Master Thesis

Reducibility of Polynomials over Finite Fields

Author: Muhammad Imran
Date: 1976-06-02
Subject: Mathematics
Level: Advance
Course code: 5MA12E
Abstract

Reducibility of certain class of polynomials over $\mathbb{F}_p$, whose degree depends on $p$, can be deduced by checking the reducibility of a quadratic and cubic polynomial. This thesis explains how can we speed up the reducibility procedure.

Key-words: Irreducible polynomials; Finite fields; Linear factors.
Acknowledgments

This thesis is written as a part of the Degree of Master of Science in Mathematics at Linnaeus University, Sweden. It is written at the Department of Computer Science, Physics and Mathematics.

This work would not be possible without the guidance provided from my supervisor, Per-Anders Svensson. I would like to thank him for being supporting throughout the whole period. He is very intelligent and knowledgeable mathematician, he is exceptionally patient with his students.

I thank to my Program Manager, Marcus Nilsson who has been very cooperative within all matters. I would also like to thank Professor Andrei Khrennikov and Professor Börje Nilsson from which I have learnt a lot. I express my deepest gratitude to my parents and elders who supported and encouraged me during my study. At last, I thank to Swedish Government for providing me the great opportunity by granting the permission to stay and study in Sweden.
### Contents

1 Introduction  

2 Preliminaries  
   2.1 Groups  
   2.2 Subgroups  
   2.3 Cyclic Groups  
   2.4 Lagrange’s Theorem  
   2.5 Fields  
   2.6 Homomorphism  

3 Finite Fields  
   3.1 Definitions and Examples  
   3.2 Polynomials  
   3.3 Factorization of Polynomials over a Field  

4 Quadratic Residues  
   4.1 Definition and Example  
   4.2 Lemma and Theorem  

5 Reducibility of Polynomials  
   5.1 Quadratic Case  
   5.2 Illustration with Examples  
   5.3 Cubic Case  

6 Conclusion  

7 References
1 Introduction

Interest in constructing irreducible polynomials over finite fields and determining the reducibility of a given polynomial stems from both mathematical theory and applications. Interest in mathematical aspects often appear in number theory, combinatorics and algebraic geometry, while practical aspects comes from the implementation of finite field arithmetic in hardware and software engineering of error correcting coding and cryptography.

Finite fields are discrete mathematical objects satisfying all the axioms of a field, such as for the real or complex numbers, except their finiteness. They are also referred to as Galois fields after the French mathematician Evariste Galois who was one of the first to show interest in them. It is easy to show that such objects exist only when the number of their elements is a power of a prime number and that any two finite fields with the same number of elements are isomorphic. Fundamental to the study of finite fields is the study of polynomials over finite fields which is the focus of this thesis.

The properties of finite fields and polynomials over them are of interest in their own right as they play a central role in many areas of pure mathematics. Polynomials over finite fields have been studied since the time of Gauss and Galois. The determination of special types of polynomials such as irreducible, primitive and permutation polynomials is a long standing and well studied problem in the theory and application of finite fields.

In our thesis, we factorized the polynomial \( g(x) = \psi(x^p) - x \), with the help of two kind of monic polynomials \( \psi(x) = x^2 + a \) and \( \psi(x) = x^3 + bx + c \) over finite field. It is seen that how many polynomials of the kind \( g(x) = \psi(x^p) - x \) that are irreducible, see [4], in case when \( \psi(x) = x^2 + a \). The aim of the thesis is to find the reducibility values of the cubic polynomial \( f(x) = x^3 + bx + c \) for different primes \( p \) and how the process of computations can speeds up to save the time.

To deal with our aim, we needs to know quiet a few mathematical concepts and definitions which are discussed in chapters 2 and 3. The definitions and theorems related to our aim are described in chapter 4 whereas the theorem through which we abled to calculate the reducibility values of cubic polynomial over finite field is stated and proved in chapter 5.
2 Preliminaries

2.1 Groups

In this section, we will define some basic definitions and properties of groups. Also we will state some theorems. For this section we have taken the material from [1].

**Definition 2.1.** Let $G$ be a non empty set and $*$ be a binary operation on $G$. Then $G$ with the binary operation $*$ is called **group** if the following three properties are satisfied.

1. $(G_1)$ $*$ is associative. That is, for all $x, y, z \in G$, we have 
   $$(x * y) * z = x * (y * z).$$

2. $(G_2)$ There is an identity element $e \in G$ such that for all $x \in G$
   $$x * e = e * x = x.$$

3. $(G_3)$ Every element in $G$ has its inverse in $G$, with respect to the operation $*$. So, for each $x \in G$, there exists an inverse element $x'$ in $G$ such that
   $$x * x' = x' * x = e.$$

If all the above properties are fulfilled then $G$ is called group under the binary operation $*$ and it is denoted by $(G, *)$.

**Definition 2.2.** Let $G$ be a group. Then $G$ is said to be **finite** if it has only finite number of elements.

**Definition 2.3.** Let $G$ be a finite group. Then the number of elements in $G$ is called the **order of group** and is denoted by $|G|$.

**Definition 2.4.** If the binary operation $*$ of a group $G$ is commutative, that is, for all $x, y \in G$
   $$x * y = y * x,$$

then the group is called **abelian** or **commutative**.

To illustrate the definition of the group, we look at the example given below.

**Example 2.1.** Consider the set of all positive rational numbers $\mathbb{Q}^+$ and the binary operation $*$ is defined on $\mathbb{Q}^+$ by $x * y = \frac{xy}{4}$. Then

1. For all $x, y, z \in \mathbb{Q}^+$
   $$(x * y) * z = \frac{xy}{4} * z = \frac{xyz}{16}$$
   and
   $$x * (y * z) = x * \frac{yz}{4} = \frac{xyz}{16}$$
   Since, $(x * y) * z = x * (y * z) = \frac{xyz}{16}$. So $*$ is associative.

2. $4 \in \mathbb{Q}^+$ is the identity element. Since
   $$4 * x = x * 4 = \frac{4x}{4} = x$$
   for each $x \in \mathbb{Q}^+$.

3. If $x'$ is the inverse of any $x \in \mathbb{Q}^+$, then $x' = \frac{16}{x}$. Since
   $$x * x' = x' * x = x.$$

Hence $\mathbb{Q}^+$ with the binary operation $*$ is a group. $(\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{Z}, +)$ are all examples of groups. Also all these are abelian groups.
2.1.1 Properties of groups

In this section, we will describe some properties of groups in terms of theorems. Cancellation laws will be stated in the first theorem.

**Theorem 2.1.** Let $G$ be a group and $*$ be the binary operation defined on $G$, then the left and right cancellation laws hold in $G$, that is for all $x, y, z \in G$

$$x * y = x * z \implies y = z,$$

and

$$y * x = z * x \implies y = z.$$  

**Proof.** Let us consider $x * y = x * z$. Then by inverse property $G_3$ of group, there exists an element $x'$ in $G$, and

$$x' * (x * y) = x' * (x * z).$$

By using the associative property ($G_1$) of group, the above equation can be written as

$$(x' * x) * y = (x' * x) * z.$$ 

By using ($G_3$) we get

$$e * y = e * z.$$ 

Now $e$ is the identity element, so by its definition in ($G_2$),

$$y = z.$$ 

Similarly, if we start with $y * x = z * x$ then we can easily prove that $y = z$. 

**Theorem 2.2.** Let $*$ be the binary operation defined on a group $G$. For any $x, y \in G$, the linear equations $x * a = y$ and $b * x = y$ have unique solutions $a$ and $b$ in $G$.

**Theorem 2.3.** If $G$ is a group with binary operation $*$, then the identity element $e$ is unique.

**Theorem 2.4.** Let $G$ be a group and $*$ be the binary operation, then for each $x \in G$ the inverse element of $x'$ of $x$ in $G$ is unique such that

2.2 Subgroups

The study of groups shows that there are sometimes such groups which are contained within larger groups. For example, the set of integers $\mathbb{Z}$ is a group under addition which is contained within the group of rational numbers $\mathbb{Q}$ under addition, which in turn is contained in the group of real numbers $\mathbb{R}$ under the same binary operation. In such case of a group contained in the other group means that the smaller group which is contained in the other group satisfies all the properties of group under the same binary operation defined on the larger group. For the group $(\mathbb{Z}, +)$ which is contained in $(\mathbb{R}, +)$, the important thing to notice that the operation $+$ on integers $x$ and $y$ as elements of $(\mathbb{Z}, +)$ produces the same element $x + y$ as would result if you were to think of $x$ and $y$ as elements in $(\mathbb{R}, +)$.

**Definition 2.5.** Let $G$ be a group and $H$ a subset of $G$. The set $H$ is called a **subgroup** of $G$ if $H$ is itself a group with respect to the operation of $G$. It is denoted by $H < G$. 

6
The set of integers \( \mathbb{Z} \) is the group under addition and is a subgroup of rational numbers \( \mathbb{Q} \). The group \( \mathbb{Q} \) in turn is a subgroup of \( \mathbb{R} \) and \( \mathbb{R} \) is subgroup of \( \mathbb{C} \). We can write all of them as:

\[
(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +).
\]

The group of nonzero rational numbers under multiplication is a subgroup of nonzero real numbers, i.e.

\[
(\mathbb{Q} \setminus \{0\}, \times) < (\mathbb{R} \setminus \{0\}, \times).
\]

2.3 Cyclic Groups

In this section cyclic group will be defined and an example will be given to understand it. We will discuss some elementary properties of cyclic group. It is already be defined the order of a finite group. Here we will define order of an element of a cyclic group.

**Definition 2.6.** A group \( G \) is a cyclic group if for some \( g \in G \), every element in \( G \) is of the form \( g^n \) where \( n \) is an integer. Thus

\[
G = \langle g \rangle = \{g^n | n \in \mathbb{Z}\}
\]

Here we say that \( g \) is called the generator of cyclic group \( G \). Now we give an example to understand the definition of the cyclic group in a simple way.

**Example 2.2.** The group \( G = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\} \) is a cyclic group with generator 3. Indeed

\[
\langle 3 \rangle = \{1 = 3^0, 3 = 3^1, 2 = 3^2, 6 = 3^3, 4 = 3^4, 5 = 3^5\} = G
\]

Note that 5 is also a generator of \( G \), but that \( \langle 2 \rangle = \{1, 2, 4\} \neq G \) so that 2 is not a generator of \( G \).

**Definition 2.7.** The order of an element \( g \) of any group is defined to be the order of the cyclic group that it generates. We denote order of \( g \) by \( o(g) \). Thus

\[
o(g) = |\langle g \rangle|.
\]

**Example 2.3.** In \( \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\} \), the order of six elements and the cyclic subgroups that they generate are:

<table>
<thead>
<tr>
<th>( g )</th>
<th>( o(g) )</th>
<th>( \langle g \rangle )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>{0}</td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>{0, 1, 2, 3, 4, 5}</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>{0, 2, 4}</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>{0, 3}</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>{0, 4, 2}</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>{0, 5, 4, 3, 2, 1}</td>
</tr>
</tbody>
</table>

2.3.1 Elementary Properties of Cyclic Groups

In this section, we will define some properties of cyclic group in terms of those theorems whose proofs can be found in [1].

**Theorem 2.5.** If \( G \) is a cyclic group, then \( G \) is abelian.

**Theorem 2.6.** Every subgroup of a cyclic group \( G \) is cyclic.
Theorem 2.7. Let $G$ be a cyclic group generated by $a$. If the order of $a$ be $n$, a positive integer i.e. $o(a) = n$. Then:

(i) $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$

(ii) $o(a^k) = \frac{n}{\gcd(n,k)}$

for all $k \in \mathbb{Z}^+$.  

Theorem 2.8. Let $G$ be a group and $a \in G$ such that $a^r = a^s$ for some integers $r$ and $s$ with $r \neq s$. Then the following statements are true:

(i) There is a smallest positive integer $n$ such that $g^n = e$.

(ii) The elements $e, a, a^2, \ldots, a^{n-1}$ are distinct and

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}.$$  

2.4 Lagrange’s Theorem

A very important corollary to the fact that the left cosets of a group partition a group is Lagrange’s theorem. This theorem gives a relationship between the order of a finite group $G$ and the order of subgroup of $G$. But before proving this theorem we will describe the concept of cosets which will help us in proving this theorem.

Definition 2.8. Let $G$ be a group and let $H < G$. A left coset of $H$ in $G$ is a subset of the form

$$gH = \{gh | h \in H\} \text{ for some } g \in G.$$  

Likewise, a right coset is a subset of the form

$$Hg = \{hg | h \in H\} \text{ for some } g \in G.$$  

Thus the left coset $gH$ consists of $g$ times everything in $H$ and $Hg$ consists of everything in $H$ times $g$.

Lemma 2.9. If $H$ is a finite subgroup of a group $G$ then for any $a \in G$

$$|aH| = H$$

i.e. the number of elements in any left coset of a subgroup $H$ are the same as the number of elements in $H$.  

Theorem 2.10. Let $G$ be a group and $H$ a subgroup of $G$. Define the relation $\sim_L$ on $G$ by

$$a \sim_L b \iff a^{-1}b \in H$$

and let $\sim_R$ be defined on $G$ by

$$a \sim_R b \iff ab^{-1} \in H$$

Then both relations $\sim_L$ and $\sim_R$ are equivalence relations on $G$.  

Note: it is important to note that the relation $\sim_L$ in Theorem 2.10 defines a partition of $G$.  

8
Theorem 2.11. **Theorem of Lagrange**

Let $G$ be a group and $H$ be a subgroup of $G$. Then the order of $H$ divides the order of $G$, i.e. $|H|$ divides $|G|$.

**Proof.** Let us consider the order of $G$ and $H$ be $m$ and $n$ respectively, i.e. $|G| = m$ and $|H| = n$. Let the distinct left cosets of $H$ in $G$ be $a_1H, a_2H, \cdots, a_rH$. Then

$$G = a_1H \cup a_2H \cup \cdots \cup a_rH,$$

since the left cosets form a partition in $G$ by Theorem 2.10. So the left cosets are pairwise disjoint and we have

$$|G| = |a_1H| + |a_2H| + \cdots + |a_rH|.$$

By Lemma 2.9, the above equation can be written as

$$|G| = |H| + |H| + \cdots + |H| \implies |G| = r \cdot |H| \implies m = r \cdot n.$$

Hence the proof is finished. \qed

**Corollary 1.** If $G$ be a group and $a \in G$ then order of $a$ divides the order of $G$.

**Proof.** Since $\langle a \rangle$ is a subgroup of $G$ then $|\langle a \rangle|$ divides $|G|$. As we know that $o(a) = |\langle a \rangle|$. Hence, $o(a)$ divides $|G|$. \qed

**Corollary 2.** If $G$ be a group and $a \in G$ then $a^{|G|} = e$.

**Proof.** If $o(a) = m$ then by Corollary 1 $o(a)$ divides $|G|$. Thus, $|G| = qm$ for some positive integer $q$. Hence,

$$a^{|G|} = a^{qm} = (a^m)^q = e^q = e.$$ \qed

2.5 **Fields**

**Definition 2.9.** Let $F$ be a set and let $+$ and $\cdot$ be two binary operations on $F$. A **field** is a triple $(F, +, \cdot)$ such that

1. $(F, +)$ is a commutative group;
2. $(F^\times, \cdot)$, where $F^\times = F \setminus \{0\}$, is a commutative group;
3. the distributive laws hold, that is

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ and } (b + c) \cdot a = b \cdot a + c \cdot a.$$ 

for all $a, b, c \in F$.

**Example 2.4.** The set of all rational numbers $\mathbb{Q}$, all real numbers $\mathbb{R}$ and all complex numbers $\mathbb{C}$ under the same binary operations addition and multiplication are the most familiar examples of fields.
2.6 Homomorphism

**Definition 2.10.** Let \( G \) and \( \hat{G} \) be groups and let \( \phi : G \to \hat{G} \) be a mapping from \( G \) into \( \hat{G} \). Then \( \phi \) is called a **(group) homomorphism** if the homomorphism property

\[
\phi(ab) = \phi(a)\phi(b)
\]

holds for all \( a, b \in G \).

The **kernel** of \( \phi \) denoted by \( \ker(\phi) \) is defined to be \( \{ a \in G \mid \phi(a) = e \} \), where \( e \) is the identity element in \( \hat{G} \).

**Example 2.5.** Let the mapping \( \phi : G \to \hat{G} \) be a group homomorphism of \( G \) onto \( \hat{G} \). If it is supposed that \( G \) is abelian, then \( \hat{G} \) must be abelian. For this, we will prove that \( \hat{a}b = b\hat{a} \) for all \( \hat{a}b \in \hat{G} \). Since \( \phi \) is the mapping from \( G \) onto \( \hat{G} \), so there exists \( a, b, \in G \) such that \( \phi(a) = \hat{a} \) and \( \phi(b) = \hat{b} \). Also \( ab = ba \), since \( G \) is abelian. Thus by using the property (2.1) we have

\[
\hat{a}b = \phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a) = b\hat{a}.
\]

**Example 2.6.** (Evaluation Homomorphism) let \( \mathbb{R} \) be the additive group of real numbers, and let \( c \) be any real number. Let \( F \) be the additive group of all functions which maps \( \mathbb{R} \) into \( \mathbb{R} \). The **evaluation homomorphism** is the map \( \phi_c : F \to \mathbb{R} \) defined by \( \phi_c(f) = f(c) \) for \( f \in F \). Since by definition, the sum of two functions \( f \) and \( g \) is the function \( f + g \) whose value at \( x \) is \( f(x) + g(x) \). So

\[
\phi_c(f + g) = (f + g)(c) = f(c) + g(c) = \phi_c(f) + \phi_c(g)
\]

which means that equation (2.1) is satisfied, so we have a homomorphism.
3 Finite Fields

3.1 Definitions and Examples

Definition 3.1. A finite field (also called Galois field) has finitely many elements. We denote a finite field with \( q \) elements by \( \mathbb{F}_q \). The number of elements in \( \mathbb{F}_q \) is always a prime power \( q = p^n \) for some prime \( p \) and positive integer \( n \). Conversely, there is a unique (up to isomorphism) finite field \( \mathbb{F}_q \) for any prime power \( q > 1 \). The prime \( p \) is called the characteristic of \( \mathbb{F}_q \).

If \( d | n \), then \( \mathbb{F}_{p^d} \) is a subfield of \( \mathbb{F}_{p^n} \). The subfield \( \mathbb{F}_p \) is called the prime field of \( \mathbb{F}_q \). A prime field is unique up to unique isomorphism.

Example 3.1. \( \mathbb{F}_2 \) is a simple and important example of a finite field. This field of order two has elements 0 and 1. The operation tables have the following form:

+ | 0 1 \\
---|---|---
0 | 0 1 \\
1 | 1 0 \\

and

. | 0 1 \\
---|---|---
0 | 0 0 \\
1 | 0 1 \\

The elements 0 and 1 are called binary elements.

3.2 Polynomials

Our aim in this section is to define some definitions related to polynomials. Here an important thing to note that a polynomial is defined over a field if all its coefficients are drawn from that field. It is also common to use the phrase polynomial over a field to convey the same meaning.

Definition 3.2. Let \( \mathbb{F} \) be a field. Any expression of the form

\[
a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0
\]

is called a polynomial over the field \( \mathbb{F} \). Where \( n \) is a nonnegative integer and \( a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{F} \) are called the coefficients of the polynomial. If \( n \) is the largest nonnegative integer with \( a_n \neq 0 \), then we say that the polynomial \( f(x) = a_nx^n + \cdots + a_0 \) has the degree \( n \) which is denoted as \( \deg f = n \) and the coefficient \( a_n \) is called the leading coefficient of \( f(x) \). The set of all polynomials over the field \( \mathbb{F} \) is denoted by \( \mathbb{F}[x] \).

Definition 3.3. The polynomial whose all coefficients are zero is called the zero polynomial.

Definition 3.4. The polynomial is said be a constant polynomial if \( a_0 \) is the leading coefficient.

Definition 3.5. If the leading coefficient is 1 of a polynomial, then it is called monic polynomial.

Definition 3.6. An element \( a \in \mathbb{F} \) is called zero of a polynomial \( f(x) \) if \( f(a) = 0 \).
Definition 3.7. A nonconstant polynomial \( f(x) \in \mathbb{F}[x] \) is said to be **irreducible** over the field \( \mathbb{F} \) or is an **irreducible polynomial** in \( \mathbb{F}[x] \) if \( f(x) \) has positive degree and \( f(x) \) cannot be expressed as a product \( g(x)h(x) \) of two polynomials \( g(x), h(x) \in \mathbb{F}[x] \) both of lower degree than the degree of \( f(x) \). If \( f(x) \in \mathbb{F}[x] \) is a nonconstant polynomial that is not irreducible over \( \mathbb{F} \), then \( f(x) \) is **reducible**.

It is to be noted that the preceding definition concerns the concept irreducible over \( \mathbb{F} \) and not merely the concept of irreducible. A polynomial \( f(x) \) may be irreducible over \( \mathbb{F} \), but it may not be irreducible if viewed over a larger field \( \mathbb{E} \) containing \( \mathbb{F} \). For example, the polynomial \( x^2 - 2 \in \mathbb{Q}[x] \) is irreducible over the field \( \mathbb{Q} \) and reducible over the field of real numbers \( \mathbb{R} \), because \( x^2 - 2 \) factors in \( \mathbb{R}[x] \) into \((x - \sqrt{2})(x + \sqrt{2})\). Also it is to be noted that

(i) All polynomials of degree 1 are irreducible.

(ii) A polynomial of degree 2 or 3 is irreducible over the field \( \mathbb{F} \) if and only if it has no zeros in \( \mathbb{F} \).

3.2.1 **The Evaluation Homomorphism**

In this section we will show that how homomorphism help us to solve a polynomial equation. Let us consider two fields \( \mathbb{E} \) and \( \mathbb{F} \) with \( \mathbb{F} \) as a subfield of \( \mathbb{E} \). In Theorem 3.1, an important homomorphism of \( \mathbb{F}[x] \) into \( \mathbb{E} \) is described. But first we define the homomorphism of rings.

**Definition 3.8.** Let \( R \) and \( S \) be rings. A **ring homomorphism** is a mapping \( \phi : R \rightarrow S \) such that for all \( x, y \in R \)

(i) \( \phi(x + y) = \phi(x) + \phi(y) \).

(ii) \( \phi(xy) = \phi(x)\phi(y) \).

If \( R \) and \( S \) are rings with 1, then

(iii) \( \phi(1_R) = 1_S \).

**Example 3.2.** (A ring homomorphism on integers modulo 2) Consider the function \( \phi : \mathbb{Z}_2 \rightarrow \mathbb{Z}_2 \) given by

\[
\phi(x) = x^2
\]

First,

\[
\phi(x + y) = (x + y)^2 = x^2 + 2xy + y^2 = \phi(x) + \phi(y).
\]

\(2xy = 0\) because 2 times anything is 0 in \( \mathbb{Z}_2 \). Next,

\[
\phi(xy) = (xy)^2 = x^2y^2 = \phi(x)\phi(y).
\]

Note also that \( \phi(1) = 1^2 = 1 \). Thus \( \phi \) is a ring homomorphism.

**Definition 3.9.** The **kernel** of a ring homomorphism \( \phi : R \rightarrow S \) is

\[
\ker \phi = \{ r \in R \mid \phi(r) = 0 \}.
\]

The **image** of a ring homomorphism \( \phi : R \rightarrow S \) is

\[
\operatorname{im} \phi = \{ \phi(r) \mid r \in R \}.
\]

12
Theorem 3.1. (The Evaluation Homomorphisms for Field Theory)
Let \( \mathbb{E} \) and \( \mathbb{F} \) be two fields with \( \mathbb{F} \) a subfield of \( \mathbb{E} \). For any \( \alpha \in \mathbb{E} \) and \( (a_0 + a_1x + \cdots + a_nx^n) \in \mathbb{F}[x] \), the map \( \phi_\alpha : \mathbb{F}[x] \to \mathbb{E} \) defined by
\[
\phi_\alpha(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1\alpha + \cdots + a_n\alpha^n
\]
is a homomorphism of \( \mathbb{F}[x] \) into \( \mathbb{E} \). Also, \( \phi_\alpha(x) = \alpha \), where \( x \) be an indeterminate. For \( a \in \mathbb{F} \), \( \phi_\alpha(a) = a \) i.e. \( \phi_\alpha \) maps \( \mathbb{F} \) isomorphically by the identity map. The homomorphism \( \phi_\alpha \) is evaluation at \( \alpha \).

Example 3.3. If we replace \( \mathbb{F} \) by \( \mathbb{Q} \) and \( \mathbb{E} \) by \( \mathbb{R} \) in Theorem 3.1 then by the evaluation homomorphism \( \phi_0 : \mathbb{Q}[x] \to \mathbb{R} \), we get
\[
\phi_0(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_10 + \cdots + a_n0^n = a_0.
\]
Which shows that every polynomial is mapped onto its constant term.

Example 3.4. In Theorem 3.1 if we replace \( \mathbb{F} \) by \( \mathbb{Q} \) and \( \mathbb{E} \) by \( \mathbb{R} \) then by the evaluation homomorphism \( \phi_2 : \mathbb{Q}[x] \to \mathbb{R} \), we get
\[
\phi_2(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_12 + \cdots + a_n2^n
\]
Here it can be noted that
\[
\phi_2(x^2 + x - 6) = 2^2 + 2 - 6 = 0
\]
So the polynomial is in the kernel \( \mathbb{N} \) of \( \phi_2 \).

3.3 Factorization of Polynomials over a Field

Theorem 3.2. (Division Algorithm for \( \mathbb{F}[x] \))
Let \( \mathbb{F} \) be a field, suppose
\[
f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0
\]
and
\[
g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0
\]
are two polynomials in \( \mathbb{F}[x] \), with \( a_n \) and \( b_m \) both nonzero elements of \( \mathbb{F} \) and \( m > 0 \). Then there are uniquely determined polynomials \( q(x), r(x) \in \mathbb{F}[x] \) such that \( f(x) = g(x)q(x) + r(x) \), where either \( r(x) = 0 \) or the degree of \( r(x) \) is less than the degree \( m \) of \( g(x) \).

Theorem 3.3. (Factor Theorem)
Let \( f(x) \) be a polynomial in \( \mathbb{F}[x] \), an element \( a \in \mathbb{F} \) is a zero of \( f(x) \) if and only if \((x - a)\) is a factor of \( f(x) \) in \( \mathbb{F}[x] \).

Proof. Suppose \( f(a) = 0 \) for \( a \in \mathbb{F} \). By Theorem 3.2 there are polynomials \( q(x), r(x) \in \mathbb{F}[x] \) such that
\[
f(x) = (x - a)q(x) + r(x),
\]
where either \( r(x) = 0 \) or the degree of \( r(x) \) is less than 1. Thus for \( c \in \mathbb{F} \), we have that \( r(x) = c \), so that
\[
f(x) = (x - a)q(x) + c.
\]
By evaluation homomorphism, \( \phi_\alpha : \mathbb{F}[x] \to \mathbb{F} \) of Theorem 3.1, we have that
\[
0 = f(a) = 0q(a) + c.
\]
so that \( c = 0 \). Then \( f(x) = (x - a)q(x) \) which shows that \( x - a \) is a factor of \( f(x) \). Conversely, suppose that for \( a \in \mathbb{F} \), \( x - a \) is a factor of \( f(x) \) in \( \mathbb{F}[x] \). Then by applying evaluation homomorphism, \( \phi_a \) to \( f(x) = (x - a)q(x) \), we have \( f(a) = 0q(a) = 0 \). 

\( \square \)
Lemma 3.4. In a finite field $\mathbb{F}$ with $p$ elements, the equation $a^p = a$ is satisfied for every $a \in \mathbb{F}$.

Proof. The result is clearly true if $a = 0$. We may therefore assume $a$ is not zero. By definition of field, the set $\mathbb{F}^\times$ of non-zero elements of $\mathbb{F}$ forms a group under multiplication. This set has $p - 1$ elements and by Corollary 2 on page number 9, we have $a^{p-1} = 1$ for any $a \in \mathbb{F}^\times$, so $a^p = a$ follows. $\square$
4 Quadratic Residues

4.1 Definition and Example

Definition 4.1. If \( m \in \mathbb{N} \) and \( a \in \mathbb{Z} \) be such that \((a,m) = 1\). Then \( a \) is called a **quadratic residue** modulo \( m \) if the congruence

\[
x^2 \equiv a \pmod{m}
\]

has a solution (i.e. if \( a \) is a perfect square modulo \( m \)), and \( a \) is called a **quadratic nonresidue** modulo \( m \) if (4.1) has no solution.

**Remarks:**
(i) Note that, by definition, integers \( a \) that do not satisfy the condition \((a,m) = 1\) are not classified as quadratic residues or nonresidues. In particular, 0 is considered neither a quadratic residue nor a quadratic nonresidue (even though, for \( a = 0 \), (4.1) has a solution, namely \( x = 0 \)).

(ii) While the definition of quadratic residues and nonresidues allows the modulus \( m \) to be an arbitrary positive integer, in the following we will focus exclusively on the case when \( m \) is an odd prime \( p \).

Example 4.1. To determine which integers are quadratic residues modulo 13, we compute the square of the integers 1, 2, 3, \ldots, 12.

<table>
<thead>
<tr>
<th>( b )</th>
<th>( 0 )</th>
<th>( 1 )</th>
<th>( 2 )</th>
<th>( 3 )</th>
<th>( 4 )</th>
<th>( 5 )</th>
<th>( 6 )</th>
<th>( 7 )</th>
<th>( 8 )</th>
<th>( 9 )</th>
<th>( 10 )</th>
<th>( 11 )</th>
<th>( 12 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( b^2 \pmod{13} )</td>
<td>( 0 )</td>
<td>( 1 )</td>
<td>( 4 )</td>
<td>( 9 )</td>
<td>( 3 )</td>
<td>( 12 )</td>
<td>( 10 )</td>
<td>( 10 )</td>
<td>( 12 )</td>
<td>( 3 )</td>
<td>( 9 )</td>
<td>( 4 )</td>
<td>( 1 )</td>
</tr>
</tbody>
</table>

From the above table, we can describe a formula

\[(p-b)^2 \equiv p^2 - 2pb + b^2 \equiv b^2 \pmod{p}\]

and we find that
1. \( 1^2 \equiv 12^2 \equiv 1 \pmod{13} \),
2. \( 2^2 \equiv 11^2 \equiv 4 \pmod{13} \),
3. \( 3^2 \equiv 10^2 \equiv 9 \pmod{13} \),
4. \( 4^2 \equiv 9^2 \equiv 3 \pmod{13} \),
5. \( 5^2 \equiv 8^2 \equiv 12 \pmod{13} \),
6. \( 6^2 \equiv 7^2 \equiv 10 \pmod{13} \).

Hence the quadratic residues modulo 13 are 1, 3, 4, 9, 10, 12 and the integers 2, 5, 6, 7, 8, 11 are quadratic nonresidues modulo 13.

It is to be noted from the example that there are 6 quadratic residues and 6 nonresidues modulo 13. Using the observation that \((p-b)^2 \equiv b^2 \pmod{p}\), we can easily verify that there are an equal number of quadratic residues and quadratic nonresidues modulo any odd prime.

4.2 Lemma and Theorem

Lemma 4.1. Let \( p \) be an odd prime and \( a \) be an integer. Then, the congruence

\[x^2 \equiv a \pmod{p}\]

has:
(i) Only the solution \( x = 0 \) if \( a = 0 \).

(ii) Exactly 0 or 2 incongruent solutions if \( p \) does not divide \( a \).

Proof. \( x = 0 \) solves \( x^2 = 0 \mod p \). Conversely, if \( x^2 = 0 \mod p \), then \( p \mid x^2 \), so \( p \mid x \), and hence \( x = 0 \mod p \).

Now suppose \( p \nmid a \). To show there are 0 or 2 solutions, there is at least one solution \( b \).

Then \( b^2 \equiv a \mod p \), so \((-b)^2 \equiv a \mod p \). We claim that \( b \) and \(-b\) are distinct.

If not, \( b \equiv -b \mod p \), so \( p \mid 2b \). Since \( p \) is an odd prime, so \( p \nmid 2 \). Therefore, \( p \mid b \), \( b \equiv 0 \mod p \), \( b^2 \equiv 0 \mod p \), and finally \( a \equiv 0 \mod p \) a contradiction \( p \nmid a \). Hence \( b \neq -b \mod p \).

To show that there are no more than two incongruent solutions. Assume that \( x = b_0 \) and \( x = b_1 \) are both solutions of \( x^2 \equiv a \mod p \). Then we have \( b_0^2 \equiv b_1^2 \equiv a \mod p \), so that \( b_0^2 - b_1^2 = (b_0 + b_1)(b_0 - b_1) \equiv 0 \mod p \). Hence, \( p \mid (b_0 + b_1) \) or \( p \mid (b_0 - b_1) \), so that \( b_1 \equiv -b_0 \mod p \) or \( b_1 \equiv b_0 \mod p \). Therefore, if there is a solution of \( x^2 \equiv a \mod p \), there are exactly two incongruent solutions modulo \( p \).

Example 4.2. Let we take \( p = 7 \).

<table>
<thead>
<tr>
<th>( b )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>( b^2 \mod 7 )</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

Thus 1, 2, 4 are quadratic residues modulo 7. Notice that there are equal number of residues and nonresidues.

Theorem 4.2. Let \( p \) be an odd prime. Then among the integers \( 1, 2, \cdots, p - 1 \) exactly half (i.e. \((p - 1)/2\)) are quadratic residues modulo \( p \) and exactly half are quadratic nonresidues modulo \( p \).

Proof. \( b \) and \(-b = p - b\) have the same square modulo \( p \). That is, 1 and \( p - 1 \) have the same square, 2 and \( p - 2 \) have the same square, \( \cdots \), and \( \frac{p - 1}{2} \) and \( \frac{p - 1}{2} + 1 \) have the same square.

Thus, the number of different squares is \( \frac{p - 1}{2} \) and these squares are the quadratic residues and the other \( \frac{p - 1}{2} \) numbers among the integers \( 1, 2, \cdots, p - 1 \) are quadratic nonresidues. 

The fact observed in the first sentence of the proof explains the symmetries in the table of squares modulo 13 and modulo 7 that we gave above.
5 Reducibility of Polynomials

This chapter presents our work to check how many polynomials of the kind \( g(x) = \psi(x^p) - x \in \mathbb{F}_p[x] \) that are irreducible, this is related to when a certain class of dynamical systems have attracting fixed points [4]. All our work is about to check how to speed up the computations when the prime \( p \) is large. Important theorems concerned when \( \psi(x) \) is a specific quadratic and cubic polynomial are described.

5.1 Quadratic Case

Using the quadratic polynomial \( \psi(x) = x^2 + a \), \( a \) is nonzero in \( \mathbb{F}_p \), we will find how many polynomials \( g(x) = \psi(x^p) - x \) that are irreducible, where \( p \) is any prime.

**Theorem 5.1.** Let \( \mathbb{F}_p \) be a prime field. For \( a \in \mathbb{F}_p \) with \( a \neq 0 \), let \( \psi(x) = x^2 + a \) be monic polynomial in \( \mathbb{F}_p[x] \). Then the polynomial \( g(x) = \psi(x^p) - x \in \mathbb{F}_p[x] \) is reducible if \( f(x) = \psi(x) - x \) is reducible.

**Proof.** For every prime \( p \) and \( 0 \neq a \in \mathbb{F}_p \), suppose that \( f(x) = \psi(x) - x = x^2 - x + a \) is reducible. Then there must exist \( b \neq 0 \) in \( \mathbb{F}_p \) such that \( x - b \) is a factor of \( f(x) \). Then by Theorem 3.3, we have that

\[
f(b) = 0
\]

\[
\implies b^2 - b + a = 0
\]

By Lemma 3.4, \( b = b^p \) for every \( b \in \mathbb{F}_p \). So, by replacing \( b \) by \( b^p \) in the above equation, we get

\[
b^{2p} - b + a = 0
\]

\[
\implies \psi(b^p) - b = 0
\]

\[
\implies g(b) = 0
\]

which shows that by Theorem 3.3, \( x - b \) divides \( g(x) \). Hence, \( g(x) \) is reducible. \( \square \)

**Theorem 5.2.** Let \( p \) be an odd prime. Let \( \psi(x) = x^2 + a \) be monic polynomial in \( \mathbb{F}_p \), where \( a \) be a nonzero element in \( \mathbb{F}_p \). Then the polynomial \( f(x) = \psi(x) - x \) is reducible over \( \mathbb{F}_p \) exactly for \( (p-1)/2 \) choices of \( a \) among the integers \( 1, 2, \cdots, p-1 \).

**Proof.** The polynomial \( f(x) = \psi(x) - x = x^2 - x + a \) is reducible over \( \mathbb{F}_p \) if and only if the congruence \( x^2 - x + a \equiv 0 \pmod p \) has solution. So, we consider this congruence

\[
x^2 - x + a \equiv 0 \pmod p
\]

\[
\implies x^2 + (p-1)x + a \equiv 0 \pmod p
\]

By completing squares, we get

\[
\left( x - \frac{p-1}{2} \right)^2 + a - \left( \frac{p-1}{2} \right)^2 \equiv 0 \pmod p
\]

\[
\iff \left( x - \frac{p-1}{2} \right)^2 \equiv \left( \frac{p-1}{2} \right)^2 - a \pmod p \tag{5.1}
\]

Here \( \left( \frac{p-1}{2} \right)^2 \) is a fixed constant for different values of \( p \). So, if we let \( y = x - \frac{p-1}{2} \) and \( c = \left( \frac{p-1}{2} \right)^2 - a \), then by a linear change of variables, the congruence (5.1) can be written as

\[
y^2 \equiv c \pmod p \tag{5.2}
\]
By Lemma 4.1 the congruence (5.2) has exactly zero or two solutions and by Theorem 4.2 there exist solutions exactly for \((p - 1)/2\) choices of \(c\). Hence the congruence \(x^2 - x + a \equiv 0 \pmod{p}\) has solutions for \((p - 1)/2\) choices of nonzero \(a \in \mathbb{F}_p\) which implies that the polynomial \(f(x) = \psi(x) - x\) is reducible over \(\mathbb{F}_p\) exactly for \((p - 1)/2\) choices of \(a\) among the integers 1, 2, \(\cdots\), \(p - 1\).

5.2 Illustration with Examples

From Theorem 5.2, it can be seen that \(f(x) = x^2 - x + a\) is reducible for half of the choices of a nonzero \(a \in \mathbb{F}_p\), for each odd prime \(p\). For instance, if we take \(p = 5\) then by Theorem 5.2 there must be two reducible \(f(x)\) and two irreducible \(f(x)\). By using mathematical computation, the factorization of the polynomials \(f(x) = \psi(x) - x\) when \(p = 5\) i.e. for \(a = 1, 2, 3, 4\) is given respectively as

\[
\begin{align*}
&x^2 + 4x + 1 \\
&x^2 + 4x + 2 \\
&(1 + x)(3 + x) \\
&\left(2 + x\right)^2
\end{align*}
\]

It comes out from the above list of polynomials, half of the \(f(x)\) are reducible, i.e. the polynomial \(f(x) = x^2 - x + a\) is reducible for half choices of nonzero \(a \in \mathbb{F}_5\).

Now among the above four polynomials \(f(x)\) we have to check how many of the corresponding polynomials \(g(x) = \psi(x^p) - x\) are irreducible, see [4]. Theorem 5.1, shows if \(f(x) = x^2 - x + a\) is reducible then \(g(x) = x^{2p} - x + a\) is reducible. This means for \(f(x) = (1 + x)(3 + x)\) and \(f(x) = (2 + x)^2\), \(g(x)\) is reducible. So for reducible \(f(x)\), there is no need to check the factorization of \(g(x)\) but for irreducible \(f(x)\) we must have to check the irreducibility of \(g(x)\). So there are half irreducible \(f(x)\) for which we will check how many polynomials \(g(x) = x^{2p} - x + a = x^{10} - x + a\) for \(p = 5\) are irreducible.

The computations show that

\[
\begin{align*}
&f(x) = x^2 - x + 1 = x^2 + 4x + 1 \text{ irreducible } \implies g(x) = x^{10} + 4x + 1 \text{ reducible} \\
&f(x) = x^2 - x + 2 = x^2 + 4x + 2 \text{ irreducible } \implies g(x) = x^{10} + 4x + 2 \text{ reducible}.
\end{align*}
\]

So, for \(p = 5\), there is no irreducible \(g(x)\).

For \(p = 11\), the list of polynomials \(f(x) = x^2 - x + a\) for \(a = 1, 2, \cdots, 10\) is given as

\[
\begin{align*}
&x^2 + 10x + 1 \\
&(x + 4)(x + 6) \\
&(x + 5)^2 \\
&x^2 + 10x + 4 \\
&(x + 2)(x + 8) \\
&x^2 + 10x + 6 \\
&x^2 + 10x + 7 \\
&(x + 1)(x + 9) \\
&(x + 3)(x + 7)
\end{align*}
\]

The above list of polynomials \(f(x)\) shows half of the \(f(x)\) are reducible following the Theorem 5.2. Now we have to check how many polynomials \(g(x)\) are irreducible among the above list of \(f(x)\). For any reducible \(f(x)\), \(g(x)\) is reducible by Theorem 5.1. For the irreducible \(f(x) = x^2 - x + a\), the corresponding polynomials \(g(x) = \psi(x^p) - x\) that must be checked for irreducibility are given below

\[
\begin{align*}
&x^{22} + 10x + 1 \\
&x^{22} + 10x + 4 \\
&x^{22} + 10x + 6
\end{align*}
\]
\[ x^{22} + 10x + 7 \\
\[ x^{22} + 10x + 8 \\
Among the above five polynomials \( g(x) \), it turns out only one \( g(x) = x^{22} + 10x + 4 \), corresponding to \( f(x) = x^2 + 10x + 4 \), is irreducible.

For other primes \( p \), for instance if \( p = 13, 17, \cdots, 41 \) there is no irreducible \( g(x) \), if \( p = 43 \) only one \( g(x) \) is irreducible, if \( p = 59 \) two \( g(x) \) are irreducible and if \( p = 79 \) it is found that three \( g(x) \) are irreducible when \( f(x) \) is irreducible. Even in some cases of primes \( p \), we may found four irreducible \( g(x) \) when \( f(x) \) is irreducible. In general, for any prime \( p \), the polynomial \( g(x) = \psi(x^p) - x \) to be irreducible is different when \( f(x) = \psi(x) - x \) is irreducible.

So, computations turn out, there are few chances of \( g(x) \) to be irreducible when \( f(x) \) is irreducible and there is no regular pattern of \( g(x) \) to be irreducible for any prime \( p \) when \( f(x) \) is irreducible.

It is noticed, in the long run of primes i.e. when \( p \) is large say 200th prime or 300th prime then computations take too much time rather than when \( p \) is small say 11, 41 or 89.

### 5.3 Cubic Case

In the next theorem we will prove the polynomial \( g(x) = \psi(x^p) - x \) is also reducible for the cubic polynomial \( \psi(x) = x^3 + bx + c \). This corresponds to Theorem 5.1 for the quadratic case.

**Theorem 5.3.** Let \( \mathbb{F}_p \) be a prime field. For \( b, c \in \mathbb{F}_p \), with \( c \neq 0 \), let \( \psi(x) = x^3 + bx + c \) be monic polynomial in \( \mathbb{F}_p[x] \). Then \( g(x) = \psi(x^p) - x = x^{3p} + bx^p - x + c \in \mathbb{F}_p[x] \) is reducible if the polynomial \( f(x) = \psi(x) - x \) is reducible

**Proof.** Suppose \( f(x) = \psi(x) - x = x^3 + (b - 1)x + c \) is reducible. Then there exist \( \alpha \neq 0 \) in \( \mathbb{F}_p \) such that \( x - \alpha \) is a factor of \( f(x) \). Then by Theorem 3.3, we have

\[
f(\alpha) = 0 \\
\implies \alpha^3 + (b - 1)\alpha + c = 0,
\]
or
\[
\alpha^3 + b\alpha - \alpha + c = 0.
\]
By Lemma 3.4, \( \alpha^p = \alpha \) for every \( \alpha \in \mathbb{F}_p \). So, by replacing \( \alpha \) by \( \alpha^p \) in the above equation, we get

\[
\alpha^{3p} + b\alpha^p - \alpha + c = 0 \\
\implies \psi(\alpha^p) - \alpha = 0 \\
\implies g(\alpha) = 0
\]
which shows that by Theorem 3.3, \( x - \alpha \ g(x) \). Hence, \( g(x) \) is reducible. \( \Box \)

In this section, we are working with the cubic polynomial \( f(x) = x^3 + bx + c \) for \( 0 \leq b \leq p - 1 \) and \( 1 \leq c \leq p - 1 \). With these values of \( b \) and \( c \), the number of possible polynomials \( f(x) = x^3 + bx + c \) are \( p(p - 1) \). But we can consider those polynomials in pairs, due the symmetry described in Theorem 5.4 below. So it thanks to Theorem 5.4, we will only have to check the reducibility for half of the \( f(x) = x^3 + bx + c \) and by this we can save our time and also speeds up the reducibility process.

**Theorem 5.4.** Let \( p \) be an odd prime and \( 0 \neq a \in \mathbb{F}_p \). If \( x + a \) divides the polynomial \( f_{+}(x) = x^3 + bx + c \) then \( x - a \) divides the polynomial \( f_{-}(x) = x^3 + bx - c \pmod{p} \), for \( b, c \in \mathbb{F}_p \) and \( c \neq 0 \).
Proof. Since \( x + a \) is a factor of \( f_+(x) = x^3 + bx + c \), then by Theorem 3.3 that \( -a \) is a zero of \( f_+(x) \), so we have
\[
    f_+(-a) = 0
    \implies (-a)^3 + b(-a) + c = 0
    \implies -a^3 - ba + c = 0
    \implies a^3 + ba - c = 0
    \implies f_-(a) = 0
\]
which shows \( x - a \) divides \( f_-(x) \). \( \Box \)

With the example given below we can understand the Theorem 5.4 in an easy way.

Example 5.1. (i) Let us consider \( p = 7 \) and \( c = 3 \). Then for \( b = 5 \), the factorization of \( f_+(x) = x^3 + 5x + c \) and \( f_-(x) = x^3 + 5x - c \) (mod 7) look like as
\[
    f_+(x) = (x + 5)(x^2 + 2x + 2)
\]
and
\[
    f_-(x) = (x + 2)(x^2 + 5x + 2) \pmod p
\]
By comparing these factorization, we can see that \( x + 5 \) is a factor of \( f_+(x) \) and at the same time \( x - 5 \equiv x + 2 \) (mod 7) is a factor of \( f_-(x) \) (mod 7). This means if \( x + 5 \) divides \( f_+(x) = x^3 + 5x + c \) then \( x - 2 \equiv x + 2 \) (mod 7) divides \( f_-(x) = x^3 + 5x - c \) which shows the symmetry in the factorization described by Theorem 5.4.

(ii) If \( p = 11 \) and \( c = 4 \) then for \( b = 7 \) we have
\[
    f_+(x) = (x + 3)(x + 4)^2
\]
and
\[
    f_-(x) = (x + 8)(x + 7)^2 \pmod p
\]
There is connection between \( x + 3 \) and \( x + 8 \) that is \( x + 3 \) divides \( f_+(x) = x^3 + 7x + c \) and \( x - 3 \equiv x + 8 \) (mod 11) divides \( f_-(x) = x^3 + 7x - c \) (mod 11). And similarly, we can see the connection between \( x + 4 \) and \( x + 7 \).

(iii) In case of \( p = 13 \) and \( c = 6 \) then for \( b = 5 \), we get
\[
    f_+(x) = (x + 1)(x + 4)(x + 8)
\]
and
\[
    f_-(x) = (x + 12)(x + 9)(x + 5) \pmod p
\]
Here we can see \( x + 1, x + 4, \) and \( x + 8 \) are respectively connected to \( x + 12, x + 9 \) and \( x + 5 \) in the same way as described in above two cases.

(iv) Now if we take \( p = 17 \) and \( c = 4 \) then for \( b = 9 \), we get
\[
    f_+(x) = x^3 + bx + c = x^3 + 9x + 4
\]
and
\[
    f_-(x) = x^3 + bx - c \equiv x^3 + 9x + 13 \pmod{17}
\]
So if \( f_+(x) \) is irreducible then \( f_-(x) \pmod p \) is also irreducible.
6 Conclusion

In quadratic case, we checked the factorization for every value of $a$ but in cubic case since $c$ varies in the interval $1 \leq c \leq (p-1)/2$ i.e. the symmetry of factorization of $f(x) = x^3 + bx + c$ takes place by Theorem 5.4 and only half of the $f(x) = x^3 + bx + c$ was checked for reducibility. By mathematica it was checked out the factorization of $f(x) = x^3 + bx + c$ for hundred many primes $p$ and the reducibility value can be found using the code:

$$t = \text{Table}[\text{Length}[\text{FactorList}[x^3\cdot b\cdot x + c, \text{Modulus} \rightarrow p]] - 1, \{b, 0, p - 1\}, \{c, 1, (p - 1)/2\}; \text{\text{\texttt{Count}}}[t, 2, 2] + \text{\texttt{Count}}[t, 3, 2]/(p(p - 1)/2)/\text{\texttt{N}}$$

The reducibility values of $f(x) = x^3 + bx + c$ found can be described by the relation:

$$r_p = \frac{\text{no. of reducible polynomials}}{p(p-1)}$$

The reducibility values $r_p$ calculated for some primes $p$ are given in the table below:

<table>
<thead>
<tr>
<th>$p$</th>
<th>$r_p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>0.6</td>
</tr>
<tr>
<td>79</td>
<td>0.66244</td>
</tr>
<tr>
<td>163</td>
<td>0.664622</td>
</tr>
<tr>
<td>229</td>
<td>0.665211</td>
</tr>
<tr>
<td>373</td>
<td>0.665773</td>
</tr>
<tr>
<td>457</td>
<td>0.665937</td>
</tr>
<tr>
<td>541</td>
<td>0.666051</td>
</tr>
<tr>
<td>631</td>
<td>0.666138</td>
</tr>
<tr>
<td>709</td>
<td>0.666197</td>
</tr>
<tr>
<td>823</td>
<td>0.666262</td>
</tr>
<tr>
<td>997</td>
<td>0.666332</td>
</tr>
</tbody>
</table>

It can be concluded from the table above that the reducibility of the cubic polynomial $f(x) = x^3 + bx + c$ is $2/3$ for different primes $p$. In the long run of primes $p$, it can also be noted that the reducibility values for the same polynomial remains approximately $2/3$ which can be checked by using the Mathematica.
7 References

References


