January 2015

General Factoring Algorithms for Polynomials over Finite Fields

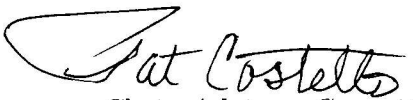
Wade Combs
Eastern Kentucky University

GENERAL FACTORING ALGORITHMS FOR POLYNOMIALS OVER FINITE FIELDS

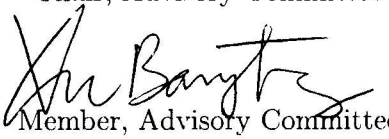
By

Wade Combs

Thesis Approved:



Chair, Advisory Committee



Member, Advisory Committee

Member, Advisory Committee

Dean, Graduate School

STATEMENT OF PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a M.S. degree at Eastern Kentucky University, I agree that the Library shall make it available to borrowers under rules of the Library. Brief quotations from this thesis are allowable without special permission, provided that accurate acknowledgment of the source is made. Permission for extensive quotation from or reproduction of this thesis may be granted by my major professor, or in his absence, by the Head of Interlibrary Services when, in the opinion of either, the proposed use of the material is for scholarly purposes. Any copying or use of the material in this thesis for financial gain shall not be allowed without my written permission.

Signature 

Date 04/06/2015

GENERAL FACTORING ALGORITHMS FOR POLYNOMIALS OVER FINITE FIELDS

By

Wade Combs

Bachelor of Science, Mathematics Teaching
Eastern Kentucky University
Richmond, Kentucky
2013

Submitted to the Faculty of the Graduate School of
Eastern Kentucky University
in partial fulfillment of the requirements
for the degree of
MASTER OF SCIENCE
May, 2015

DEDICATION

I dedicate this thesis to my parents, Harold Combs and Pamela Combs, whose love has made the many great things in my life possible.

ACKNOWLEDGEMENTS

I would like to begin by thanking my thesis advisor, Dr. Patrick Costello, for giving me the support and confidence necessary to take on the challenge of writing a paper of this magnitude. Before guiding me through the thesis writing process, Dr. Costello was very influential as my undergraduate academic advisor. He sparked my interest in mathematics and continues to ignite it every day.

I would also like to thank the other members of my thesis committee, Dr. Bangteng Xu and Dr. Rachel Bishop-Ross, for their instructive and insightful comments regarding my thesis. Any academic work is made possible in part by those who take the time to carefully read it and value it. I am extremely thankful to have had a committee that read my work with great care.

I want to thank Dr. Jeffrey Neugebauer and Dr. Kirk Jones for being excellent instructors of advanced mathematics. Both of these professors have contributed a great deal to my growth as a student and as a researcher.

Finally, I want to thank my graduate advisor, Dr. Lisa Kay, for giving me thorough and detailed guidance throughout my entire time in graduate school at Eastern Kentucky University. Dr. Kay definitely made each of the many tasks I have had to complete in graduate school as smooth and feasible as possible.

ABSTRACT

In this paper, we generate algorithms for factoring polynomials with coefficients in finite fields. In particular, we develop one deterministic algorithm due to Elwyn Berlekamp and one probabilistic algorithm due to David Cantor and Hans Zassenhaus. While some authors present versions of the algorithms that can only factor polynomials of a certain form, the algorithms we give are able to factor *any* polynomial over *any* finite field. Hence, the algorithms we give are the most general algorithms available for this factorization problem. After formulating the algorithms, we look at various ways they can be applied to more specialized inquiries. For example, we use the algorithms to develop two tests for irreducibility and a process for finding the roots of a polynomial over a finite field. We conclude our work by considering how the Berlekamp and Cantor-Zassenhaus methods can be combined to develop a more efficient factoring process.

Table of Contents

Introduction

In 1967, Elwyn Berlekamp[1] developed the first efficient method for finding factorizations of polynomials with coefficients in finite fields. His method is deterministic and primarily relies on solving systems of linear equations using row reduction of matrices. The concept behind his factoring strategy is unbelievably clever, yet very accessible to students of mathematics at all levels. Over the years, mathematicians have formulated various algorithms based on Berlekamp's factoring scheme that have the ability to completely factor polynomials over finite fields. Actually, a few researchers have been so motivated by the findings of Berlekamp that they have formulated their own separate strategies for factorization.

Citing Berlekamp as a major influence, in 1981, David Cantor and Hans Zassenhaus[2] developed a new probabilistic method for factoring. Their method is deeply rooted in the theory of fields but is ultimately easy to apply in specific problems. In their original paper, Cantor and Zassenhaus only demonstrated how to find nontrivial factorizations of polynomials using their method. Hence, they did not give a full algorithm for finding a polynomial's complete factorization. However, as Cantor and Zassenhaus probably suspected, many mathematicians and computer scientists have since used their findings to formulate various algorithms and comprehensive factoring strategies.

In this paper, our primary objective will be to thoroughly develop two factoring algorithms for polynomials over finite fields. The first will be deterministic and rely on the method of Berlekamp, while the second will be probabilistic and rely on the method of Cantor-Zassenahaus. The algorithms we present will be distinguishable by the fact that they represent the most general factoring algorithms available. What we mean by "general" is that our algorithms will have the ability to factor *any* polynomial over *any* finite field. Some authors present more specialized algorithms and exclude the generality that we will seek here. For example, Childs[3] presents a factoring technique based on Berlekamp's method that only handles polynomials over fields that have prime order. This technique excludes polynomials whose coefficients come from finite fields that have order p^v, where p is a prime number and v is a positive integer greater than 1. Further, Shoup[6] gives an algorithm based on the findings of Berlekamp that can only factor polynomials which are square-free. Hence, this algorithm cannot directly handle a polynomial that has repeated factors in its factorization.

Of course, Childs and Shoup are both aware that general versions of their algorithms can be formulated. They present such specialized algorithms because factoring generally runs much better when the input polynomial is square-free and/or has coefficients that come from fields of prime order. While our algorithms will be able to handle such specialized cases, generality will be our primary desire. With that said, over the course of the paper, we will offer various tips in regard to the best ways to factor polynomials in practice.

In order to generate factoring algorithms, we will require many preliminary results relating to finite fields and polynomials over fields. In fact, our first chapter will act as a stand-alone introduction to these concepts. Then, in Chapters 2 and 3, we will use the results from Chapter 1 to develop the algorithms.

Chapter 1

Preliminaries

Our preliminaries will build the theory that is necessary for developing factoring algorithms in later chapters. We will begin by looking at some basic properties of finite fields. Then we will consider properties of polynomials whose coefficients come from fields. Finally, we will end the chapter by using field extensions to further delve into the structure of finite fields.

Throughout all of our work, it is assumed that the reader has a good knowledge of the standard terms and theorems given in a first-semester course over group theory. However, with that said, we will explicitly state all results relating to finite fields and polynomials over fields that are used in the paper. For more information on any result given in this chapter, refer to Childs[3] and Dummit[4].

1.1 Finite Fields

We begin by formulating the definition of a field in terms of the definition of a ring.

Definition 1.1: A *ring* R is a set equipped with the binary operations $+$ and $\cdot$ (called addition and multiplication) that satisfies the following axioms:

(1) R is an abelian group under addition.

(2) Multiplication is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.

(3) Multiplication distributes over addition: for all $a, b, c \in R$,
$a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

Note that the additive identity of a ring R will always be denoted by 0, and the additive inverse of an element $a \in R$ will be denoted by $-a$. Now, we give the definition of a field.

Definition 1.2: A *field* F is a ring that satisfies the following axioms:

(1) F has a nonzero multiplicative identity, i.e., there is an element $1_F \in F$ with $1_F \neq 0$ and $1_F \cdot a = a \cdot 1_F = a$ for all $a \in F$.

(2) Every nonzero element $a \in F$ has a multiplicative inverse, i.e., there exists an element $c \in F$ with $a \cdot c = c \cdot a = 1_F$. (We will typically denote the element c by a^{-1}.)

(3) Multiplication is commutative: $a \cdot b = b \cdot a$ for all $a, b \in F$.

We will use $F^\times$ to denote the set of all nonzero elements of F. The elements of $F^\times$ will often be referred to as *units*. With respect to the first field axiom, we will generally write 1 in short for 1_F, but in cases where it may be unclear whether 1 represents an integer or a field element, we will use the notation 1_F. Also, in regard to the third field axiom, we will typically write ab instead of $a \cdot b$.

The most commonly studied infinite fields are the complex numbers $\mathbb{C}$, the real numbers $\mathbb{R}$, and the rational numbers $\mathbb{Q}$. However, we will focus our attention on fields which have finitely many elements. For every prime number p, the integers modulo p, usually denoted by $\mathbb{Z}/p\mathbb{Z}$, is a field; these are the most commonly used finite fields. In order to describe the general structure of a finite field, we require a few more definitions.

Definition 1.3: Let R be a ring. A nonzero element $a \in R$ is called a *zero divisor* if there exists a nonzero element $b \in R$ such that either $ab = 0$ or $ba = 0$.

It is not difficult to see that there are no zero divisors in a field. Let a be a nonzero element of the field F. Suppose there exists a member $b \in F$ with $ab = ba = 0$. Then $b = 1_F b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$. Hence, a is not a zero divisor.

Next, we define the characteristic of a ring.

Definition 1.4: Let R be a ring with multiplicative identity 1_R. The *characteristic* of R, denoted $\mathrm{char}(R)$, is defined to be the smallest positive integer m such that $m \cdot 1_R = 0$ if such an m exists, and 0 otherwise.

Infinite fields, such as $\mathbb{R}$ and $\mathbb{C}$, have characteristic 0. As we will see in our first major theorem regarding finite fields, the characteristic of any finite field

is a prime number. Before giving this theorem, however, we recall the following standard result from group theory:

If G is a finite abelian group of order n and p is a prime dividing n, then G contains an element of order p.

Now for the theorem:

Theorem 1.5: Let F be a finite field. Then $\text{char}(F) = p$ for some prime number p. Moreover, the order of F is p^v for some positive integer v.

***Proof*:** Since F is finite, the characteristic of F must be a positive integer. Assume, by way of contradiction, that $\text{char}(F)$ is not a prime number. By the definition of a field, $0 \neq 1_F = 1 \cdot 1_F$, and so $\text{char}(F) \neq 1$. Then $\text{char}(F)$ is composite. Say $\text{char}(F) = st$, where s and t are positive integers with $0 < s < \text{char}(F)$ and $0 < t < \text{char}(F)$. By the definition of characteristic, $s \cdot 1_F \neq 0$ and $t \cdot 1_F \neq 0$. Since F has no zero divisors, it follows that $(s \cdot 1_F)(t \cdot 1_F) \neq 0$. But, this implies

$$0 = (st) \cdot 1_F = (s \cdot 1_F)(t \cdot 1_F) \neq 0,$$

a contradiction. Thus, $\text{char}(F) = p$ for some prime p.

Next, let n be the order of F. Considering F as a group under addition, let $\text{ord}(g)$ denote the order of an element $g \in F$. Since $n \geq 2$, there must exist at least one prime number dividing n. Suppose m is a prime dividing n. Then since F is a finite abelian group under addition, by the mentioned result from group theory, there is an element $a \in F$ with $\text{ord}(a) = m$. Applying the division algorithm for integers, we can find integers q and r with $p = mq + r$ and $0 \leq r < m$. Notice that $p \cdot a = p \cdot (1_F \cdot a) = (p \cdot 1_F) \cdot a = 0 \cdot a = 0$. Now,

$$\begin{aligned}
0 &= p \cdot a \\
&= (mq + r) \cdot a \\
&= (mq) \cdot a + r \cdot a \\
&= (qm) \cdot a + r \cdot a \\
&= q(m \cdot a) + r \cdot a \\
&= q \cdot 0 + r \cdot a \\
&= 0 + r \cdot a \\
&= r \cdot a.
\end{aligned}$$

Since $r < \text{ord}(a)$, it follows that $r = 0$. Thus, $p = mq$, and m divides p. But, since p is prime and $m \neq 1$, it must be that $m = p$. Hence, p is the only prime divisor of n, which means $n = p^v$ for some positive integer v. ■

Theorem 1.5 shows us that the order of any finite field is some power of a prime number. In Section 1.3, we will establish the following related (and remarkable!) fact:

For every prime number p and positive integer v, up to isomorphism, there exists a unique finite field of order p^v.

Notice that for any element a in a ring R and any integer n, since R is closed under addition, we have that $na \in R$. Using this observation, we now present a theorem which will aid us in establishing some important results in later chapters.

Theorem 1.6: Let R be a commutative ring of prime characteristic p. Then for any elements $a, b \in R$,

$$(a + b)^p = a^p + b^p.$$

***Proof*:** Since R is commutative, we can apply the Binomial Theorem to write

$$(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k,$$

where $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ for each k. Because $\binom{p}{k}$ is an integer, $k!(p-k)!$ divides $p!$. Notice that for $k \in \{1, \cdots, p-1\}$, the prime p is a factor of neither $k!$ nor $(p-k)!$, and so p and $k!(p-k)!$ are relatively prime integers. Hence, for $k \in \{1, \cdots, p-1\}$, $k!(p-k)!$ divides $(p-1)!$, and we can write $p! = pj_k$, where $j_k = \frac{(p-1)!}{k!(p-k)!} \in \mathbb{Z}$. Since R has characteristic p, it now follows that

$$\begin{aligned}(a + b)^p &= \binom{p}{0} a^p + \sum_{k=1}^{p-1} (pj_k) a^{p-k} b^k + \binom{p}{p} b^p \\ &= a^p + \sum_{k=1}^{p-1} 0 + b^p \\ &= a^p + b^p. \quad ■\end{aligned}$$

For any integer v, it is important to see that applying Theorem 1.6 repeatedly gives that $(a+b)^{p^v} = a^{p^v} + b^{p^v}$ in R. Theorem 1.6 can always be applied to finite fields, but we will also require this theorem when dealing with commutative rings that are not fields and have prime characteristic.

To conclude our introduction to finite fields, let us recall one of the most famous theorems from number theory. Fermat's Little Theorem (FLT) says that if p is a prime number and a is a nonzero element of $\mathbb{Z}/p\mathbb{Z}$, then $a^{p-1} = 1$ in $\mathbb{Z}/p\mathbb{Z}$. We generalize this result in Theorem 1.7.

Theorem 1.7 (Generalized FLT): Let F be a field of order q. Then $a^{q-1} = 1$ for all $a \in F^\times$.

***Proof*:** Observe that $F^\times$ is a multiplicative group of order $q-1$. Then it is a consequence of Lagrange's Theorem from group theory that $a^{q-1} = 1$ for all $a \in F^\times$. ■

Multiplying both sides of the equation in Theorem 1.7 by a gives that $a^q = a$ for all $a \in F^\times$. In fact, since $0^q = 0$, we have that $a^q = a$ for all $a \in F$. We will directly cite the Generalized FLT whenever this property of the elements of F is applied.

In the upcoming section, we begin looking at polynomials over fields.

1.2 Polynomials over Fields

Let F be a field and x an indeterminate. We will use $F[x]$ to denote the set of all finite sums $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, called *polynomials*, where n is a nonnegative integer and each $a_i \in F$. If $a_n \neq 0$, then the polynomial is of *degree* n. The polynomial is called *monic* if $a_n = 1$. Notice that $F \subset F[x]$. The elements of F are called *constant polynomials* with respect to their membership in $F[x]$. We define addition in $F[x]$ to be componentwise:

$$\sum_{i=1}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=1}^{n} (a_i + b_i) x^i,$$

where some of the a_i and b_i terms may be 0, so that addition of polynomials of different degrees is defined. We define multiplication in $F[x]$ by first defining $(ax^i)(bx^j) = abx^{i+j}$ and then distributing multiplication over addition to get

$$\left(\sum_{i=0}^{n} a_i x^i\right) \cdot \left(\sum_{i=0}^{m} b_i x^i\right) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k.$$

For an arbitrary polynomial $f(x) \in F[x]$, let $\deg(f(x))$ denote the degree of $f(x)$. Here are a few straightforward properties of $F[x]$:

- $F[x]$ is a commutative ring having multiplicative identity 1_F and no zero divisors.
- The characteristic of $F[x]$ is the same as the characteristic of F.
- For nonzero polynomials $f(x), g(x) \in F[x]$, $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$.
- The elements of $F[x]$ with multiplicative inverses are precisely the elements of $F^\times$.

We now provide some standard terminology and traditional results for elements in $F[x]$.

Definition 1.8: Let $f(x), g(x) \in F[x]$. If $f(x) = g(x)h(x)$ for some $h(x) \in F[x]$, then $g(x)$ is said to *divide* $f(x)$, and we write $g(x)|f(x)$. The polynomial $g(x)$ is called a *factor* or *divisor* of $f(x)$.

Recall from elementary algebra that dividing a polynomial in $\mathbb{Q}[x]$ by another (nonzero) polynomial in $\mathbb{Q}[x]$ yields a quotient and remainder. This still holds true over any field.

Theorem 1.9 (Division Algorithm): Let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that

$$f(x) = g(x)q(x) + r(x) \qquad \text{with } r(x) = 0 \text{ or } \deg(r(x)) < \deg(g(x)). \quad (*)$$

***Proof*:** Let $g(x) \neq 0$ be fixed. We will prove that for any $f(x)$, there exist polynomials $q(x)$ and $r(x)$ satisfying $(*)$. Let $\deg(f(x)) = m$ and $\deg(g(x)) = n$. Then n is fixed, and we must show the necessary polynomials exist for all integers m.

If $m < n$, then the choices of $q(x) = 0$ and $r(x) = f(x)$ satisfy the desired conditions. For $m \geq n$, we proceed by strong induction on m. First, write $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ and $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$.

Suppose that $m = n$. Set $q(x) = a_m \cdot b_m^{-1}$ and $r(x) = f(x) - q(x)g(x)$. Observe that $q(x)$ is well-defined since $b_m \neq 0$ and that the coefficient of the x^m term vanishes in $r(x)$, which means $\deg(r(x)) = 0$ or $\deg(r(x)) < \deg(g(x))$. Now

clearly we have $f(x) = g(x)q(x) + r(x)$. This takes care of the base case.

For the inductive step, assume polynomials satisfying $(*)$ exist for all m with $n \leq m < k$, where k is a positive integer. Consider the case of $m = k$. Set $f_0(x) = f(x) - a_m b_n^{-1} x^{m-n} g(x)$. Notice that the x^m term vanishes in $f_0(x)$ so that $\deg(f_0(x)) < k$. Then, by the inductive hypothesis, there exist polynomials $q_0(x)$ and $r(x)$ such that

$$f_0(x) = g(x)q_0(x) + r(x) \qquad \text{with } r(x) = 0 \text{ or } \deg(r(x)) < n.$$

Now, letting $q(x) = q_0(x) + a_m b_n^{-1} x^{m-n}$, we get

$$f(x) = g(x)q(x) + r(x) \qquad \text{with } r(x) = 0 \text{ or } \deg(r(x)) < n.$$

So the case of $m = k$ holds. Therefore, by strong induction, there exist polynomials $q(x)$ and $r(x)$ satisfying $(*)$ for all $m \geq n$.

For uniqueness, suppose the pairs $q(x), r(x)$ and $q_1(x), r_1(x)$ both satisfy $(*)$. Then $g(x)q(x) + r(x) = g(x)q_1(x) + r_1(x)$, and we get the equation

$$g(x)(q(x) - q_1(x)) = r(x) - r_1(x).$$

If $r(x) = r_1(x) = 0$, then $q(x) = q_1(x)$ since $g(x)$ is nonzero. So, assume that either $r(x) \neq 0$ or $r_1(x) \neq 0$. This implies that both $r(x)$ and $r_1(x)$ have degree $< n$. Then $r(x) - r_1(x) = g(x)(q(x) - q_1(x))$ clearly has degree $< n = \deg(g(x))$. Since the degree of the product of two nonzero polynomials is the sum of their degrees, it must be that $q(x) - q_1(x) = 0$. Thus, $q(x) = q_1(x)$ and $r(x) = r_1(x)$. ■

Let $f(x)$ and $g(x)$ be polynomials over F with $g(x)$ non-constant. We write the congruence $f(x) \equiv h(x) \pmod{g(x)}$ for polynomials $h(x) \in F[x]$ such that $g(x) | f(x) - h(x)$. Notice that the Division Algorithm guarantees that there is a unique polynomial $r(x)$ over F which satisfies $f(x) \equiv r(x) \pmod{g(x)}$ and $\deg(r(x)) < \deg(g(x))$. The polynomial $r(x)$ is called the *least residue* of $f(x)$ mod $g(x)$. Sometimes we will simply write $f(x) (\text{mod } g(x))$ to denote the least residue.

Since a division algorithm can be established for $F[x]$, it follows that $F[x]$ has many of the same properties as the integers. This starts to become apparent when investigating the greatest common divisor of two polynomials.

Definition 1.10: The *greatest common divisor* of polynomials $f(x), g(x) \in F[x]$ with $g(x) \neq 0$ is the unique monic polynomial $d(x) \in F[x]$ satisfying:

(i) $d(x)|f(x)$ and $d(x)|g(x)$, and

(ii) if $h(x)|f(x)$ and $h(x)|g(x)$ for some $h(x) \in F[x]$, then $h(x)|d(x)$.

The greatest common divisor of $f(x)$ and $g(x) \neq 0$ will be denoted by $\gcd(f(x), g(x))$. Informally speaking, $\gcd(f(x), g(x))$ is the monic polynomial of largest degree which divides both $f(x)$ and $g(x)$. In the case $\gcd(f(x), g(x)) = 1$, we say $f(x)$ and $g(x)$ are *relatively prime*.

Considering the unique polynomials $q(x), r(x) \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$ with $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$ guaranteed by the Division Algorithm, it is easy to see that

- if $r(x) = 0$, then $\gcd(f(x), g(x)) = \alpha \cdot g(x)$, where $\alpha \in F$ is the multiplicative inverse of the leading coefficient of $g(x)$.
- if $r(x) \neq 0$, then $\gcd(f(x), g(x)) = \gcd(g(x), r(x))$.

This suggests the following iterative algorithm for finding the gcd of $f(x)$ and $g(x)$, which mirrors the Euclidean Algorithm for integers.

Euclidean Algorithm for Polynomials over F:

(1) Let $f_0(x) = f(x)$ and $g_0(x) = g(x)$.

(2) Find the unique $q(x), r(x) \in F[x]$ such that $f_0(x) = g_0(x)q(x) + r(x)$ with $r(x) = 0$ or $\deg(r(x)) < \deg(g_0(x))$.

(3) If $r(x) = 0$, then stop: $\gcd(f(x), g(x)) = \alpha \cdot g_0(x)$, where $\alpha \in F$ is the multiplicative inverse of the leading coefficient of $g_0(x)$.

(4) If $r(x) \neq 0$, then replace $f_0(x)$ by $g_0(x)$ and $g_0(x)$ by $r(x)$, and go back to (2).

This process does indeed terminate in a finite number of steps, since the degree of $g_0(x)$ decreases each time we cycle through (4). When the algorithm terminates, notice that we need to multiply the current value for $g_0(x)$ by the multiplicative inverse in F of its leading coefficient in order to meet the requirement that the gcd be monic.

We apply the Euclidean Algorithm in the upcoming example.

Example 1.11: Consider the polynomials $f(x) = x^8+3x^7+x^6+x^5+4x^3+3x^2+3$ and $g(x) = x^5 + x^4 + 3x^3 + 4x + 2$ in $(\mathbb{Z}/5\mathbb{Z})[x]$. Using polynomial long division, we find

$$\begin{aligned} f(x) &= g(x)(x^3 + 2x^2 + x + 4) + (4x^4 + 2x^3 + 2x) \\ g(x) &= (4x^4 + 2x^3 + 2x)(4x + 2) + (4x^3 + 2x^2 + 2) \\ 4x^4 + 2x^3 + 2x &= (4x^3 + 2x^2 + 2)x + 0. \end{aligned}$$

Thus, $\gcd(f(x), g(x)) = 4 \cdot (4x^3 + 2x^2 + 2) = x^3 + 3x^2 + 3$.

Since a Euclidean Algorithm can be established for $F[x]$, we can formulate a result that parallels Bézout's identity for the integers:

Theorem 1.12: Let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist polynomials $a(x), b(x) \in F[x]$ such that

$$\gcd(f(x), g(x)) = a(x)f(x) + b(x)g(x).$$

Theorem 1.12 can be proven in exactly the same manner as Bézout's identity by using the Euclidean Algorithm and backwards substitution. Utilizing this theorem, we now present a proposition that will be very valuable throughout the rest of our work.

Proposition 1.13: Let f be a polynomial in $F[x]$. If g and h are relatively prime polynomials in $F[x]$, then

$$\gcd(f, gh) = \gcd(f, g) \cdot \gcd(f, h).$$

***Proof*:** Let

$$\begin{aligned} d_0 &= \gcd(f, gh), \\ d_1 &= \gcd(f, g), \\ d_2 &= \gcd(f, h). \end{aligned}$$

By Theorem 1.12, $d_1 = a_1 f + b_1 g$ and $d_2 = a_2 f + b_2 h$ for some $a_1, b_1, a_2, b_2 \in F[x]$. Multiplying d_1 and d_2 results in the equality

$$d_1 d_2 = (a_1 a_2 f + a_1 b_2 h + b_1 a_2 g)f + (b_1 b_2)gh.$$

Note that $d_0|f$ and $d_0|gh$. So d_0 divides both terms in the sum on the right hand side of the above equation, and it follows that $d_0|d_1d_2$.

Also, since g and h are relatively prime, $\gcd(g,h) = 1$. Hence, applying Theorem 1.12 again, $1 = a_3g + b_3h$ for some $a_3, b_3 \in F[x]$. Multiplying both sides of this equation by d_0 gives

$$d_0 = a_3(d_0g) + b_3(d_0h).$$

By the definition of greatest common divisor, $d_1|d_0$ and $d_2|d_0$. Additionally, $d_1|g$ and $d_2|h$. Thus, $d_1d_2|d_0g$ and $d_1d_2|d_0h$, which implies $d_1d_2|d_0$. Now since d_0 and d_1d_2 are both monic polynomials, it must be that $d_0 = d_1d_2$. ■

Theorem 1.12 can also be used to get this significant result:

Theorem 1.14: Let $f(x), g(x), h(x)$ be polynomials in $F[x]$. If $f(x)|g(x)h(x)$ and $\gcd(f(x), g(x)) = 1$, then $f(x)|h(x)$.

The strategy of proof for Theorem 1.14 is nearly identical to the strategy used in the second part of the proof of Proposition 1.13.

Recall that any positive integer can be factored uniquely into a product of prime numbers. We will see that unique factorization also holds in $F[x]$. First, consider the definition:

Definition 1.15: Suppose $p(x)$ is a non-constant polynomial in $F[x]$. Then $p(x)$ is called *irreducible* if whenever $p(x) = a(x)b(x)$ with $a(x), b(x) \in F[x]$, either $a(x) \in F^\times$ or $b(x) \in F^\times$. Otherwise, $p(x)$ is said to be *reducible*.

Essentially, a non-constant polynomial in $F[x]$ is irreducible if it cannot be written as the product of two positive degree polynomials. For instance, the polynomial $x+1 \in (\mathbb{Z}/3\mathbb{Z})[x]$ is irreducible, since $x+1 = g(x)h(x)$ surely implies that either $g(x)$ or $h(x)$ is a unit. On the other hand, $x^2+2 \in (\mathbb{Z}/3\mathbb{Z})[x]$ is reducible, since $x^2+2 = (x+1)(x+2)$ over $\mathbb{Z}/3\mathbb{Z}$.

Irreducible elements in $F[x]$ carry many of the same properties as prime numbers. Consider, for example, the upcoming theorem, which extends Euclid's Lemma for integers to $F[x]$.

Theorem 1.16: Suppose $p(x)$ is an irreducible element of $F[x]$ and $p(x)|g(x)h(x)$ for some $g(x), h(x) \in F[x]$. Then either $p(x)|g(x)$ or $p(x)|h(x)$.

***Proof*:** Suppose $p(x) \nmid g(x)$. Then, since $p(x)$ is irreducible, $\gcd(p(x), g(x)) = 1$. By hypothesis, $p(x)|g(x)h(x)$. Thus, by Theorem 1.14, $p(x)|h(x)$. ■

Naturally, we get the following corollary.

Corollary 1.17: Suppose $p(x)$ is irreducible and $p(x)|g_1(x)g_2(x)\cdots g_n(x)$ over F. Then $p(x)|g_i(x)$ for some $i = 1, 2, \cdots, n$.

Now we are ready to establish unique factorization for $F[x]$.

Theorem 1.18: Every non-constant polynomial in $F[x]$ can be factored into a product of irreducible polynomials. The factorization is unique up to rearrangement of the irreducibles and multiplication by elements of $F^\times$.

***Proof*:** Let S be the set of all non-constant polynomials in $F[x]$ which cannot be factored into a product of irreducibles. Assume, by way of contradiction, that $S \neq \emptyset$. Let $D = \{\deg(s(x)) : s(x) \in S\}$. Since D is a non-empty set of positive integers, it follows from the well-ordering principle that D has a least element, say n. Let $p(x)$ be an element of S with $\deg(p(x)) = n$. Since $p(x)$ cannot be written as a product of irreducibles, $p(x)$ is clearly not irreducible itself. Hence, $p(x) = g(x)h(x)$ for some $h(x), g(x) \in F[x]$ with $1 \leq \deg(g(x)) < n$ and $1 \leq \deg(h(x)) < n$. Then $g(x)$, $h(x) \notin S$, and so both $g(x)$ and $h(x)$ can be written as a product of irreducibles. Say $g(x) = g_1(x)g_2(x)\cdots g_r(x)$ and $h(x) = h_1(x)h_2(x)\cdots h_t(x)$, where the $g_i(x)$ and $h_i(x)$ are irreducibles. Then

$$p(x) = g_1(x)g_2(x)\cdots g_r(x)h_1(x)h_2(x)\cdots h_s(x).$$

is a product of irreducibles, a contradiction. Therefore, $S = \emptyset$.

For uniqueness, suppose

$$a_1(x)a_2(x)\cdots a_n(x) = b_1(x)b_2(x)\cdots b_m(x), \qquad (**)$$

where the $a_i(x)$ and $b_i(x)$ are irreducibles. Now, since $a_1(x)|b_1(x)b_2(x)\cdots b_m(x)$, by Corollary 1.17, $a_1(x)|b_i(x)$ for some $1 \leq i \leq m$. If necessary, we can reindex the $b_i(x)$'s to get $a_1(x)|b_1(x)$. Since $b_1(x)$ is irreducible, it follows that $b_1(x) = \beta_1 \cdot a_1(x)$ for some $\beta_1 \in F^\times$. Then dividing both sides of the equation $(**)$ by a_1 gives

$$a_2(x)a_3(x)\cdots a_n(x) = \beta_1 b_2(x)b_3(x)\cdots b_m(x).$$

Since $a_2(x)|b_2(x)b_3(x)\cdots b_m(x)$, $a_2(x)|b_i(x)$ for some $2 \leq i \leq m$. Reindexing the $b_i(x)$'s again, if necessary, we may write $a_2(x)|b_2(x)$. Then $a_2(x) = \beta_2 \cdot b_2(x)$ for some $\beta_2 \in F^\times$. Continuing this process, we get that $a_i(x) = \beta_i \cdot b_i(x)$, $\beta_i \in F^\times$, for each $i = 1, 2, \cdots n$. In particular, this shows that $n \leq m$.

For a contradiction, suppose that $n < m$ and let $d = m - n$. Now, dividing both sides of equation $(**)$ by $a_1(x)a_2(x)\cdots a_n(x)$, we get

$$1 = (\beta_1 \cdots \beta_n) \cdot b_{n+1}(x) \cdots b_{n+d}(x).$$

But, the left hand side of this equation has degree 0, while the right hand side has positive degree. This is a contradiction. Thus, $n = m$. ■

Let $f(x)$ be a non-constant polynomial in $F[x]$. Note that for each irreducible factor $g(x)$ of $f(x)$, $g(x) = \beta \cdot h(x)$ for some monic irreducible polynomial $h(x)$ and some $\beta \in F^\times$. In view of Theorem 1.18, this suggests that $f(x)$ can be uniquely factored into the product of a nonzero constant and monic irreducibles. Collecting repeated monic irreducibles in this factorization, it follows that $f(x)$ can be written uniquely in the form

$$f(x) = \alpha \cdot f_1(x)^{k_1} f_2(x)^{k_2} \cdots f_m(x)^{k_m}, \qquad (\#)$$

where $\alpha \in F^\times$, the $f_i(x)$ are pairwise distinct monic irreducibles, and the k_i are positive integers satisfying $k_i \leq k_j$ for $i \leq j$. We will call the form $(\#)$ the *complete factorization* of $f(x)$. In particular, if $f(x)$ is monic, then $\alpha = 1$ in $(\#)$.

In Chapters 2 and 3, our primary objective will be to develop algorithms which can find the complete factorization of an arbitrary polynomial over a finite field. Before inputting a polynomial into any algorithm, however, we can often inspect the polynomial's roots to gain information about its factorization.

Proposition 1.19: Let $f(x) \in F[x]$. Then $f(x)$ has a factor of degree 1 if and only if $f(x)$ has a root in F, i.e., there exists an $\alpha \in F$ such that $f(\alpha) = 0$.

***Proof*:** Suppose $f(x)$ has a factor of degree 1. Since F is a field, we may assume the factor is monic and hence is of the form $x - \alpha$ with $\alpha \in F$. Then $f(x) = (x - \alpha)q(x)$ for some $q(x) \in F[x]$, and $f(\alpha) = 0 \cdot q(\alpha) = 0$.

For the converse, suppose $f(\alpha) = 0$ for some $\alpha \in F$. By the Division Algorithm,

$$f(x) = (x - \alpha)q(x) + r,$$

for some $q(x) \in F[x]$ and constant r. Then $0 = f(\alpha) = r$, and so $(x - \alpha)$ is a degree 1 factor of $f(x)$. ■

We now use Proposition 1.19 to establish a very useful irreducibility test for small degree polynomials.

Proposition 1.20: A polynomial of degree 2 or 3 in $F[x]$ is reducible if and only if it has a root in F.

***Proof*:** A polynomial of degree 2 or 3 is reducible if and only if it has a factor of degree 1 if and only if it has a root in F. ■

This proposition is applied in the upcoming example.

Example 1.21: Consider the polynomial $f(x) = x^3 + 2x + 1 \in (\mathbb{Z}/3\mathbb{Z})[x]$. Notice that

$$f(0) = 1$$
$$f(1) = 1$$
$$f(2) = 1.$$

So $f(x)$ has no root in $\mathbb{Z}/3\mathbb{Z}$ and hence is irreducible by Proposition 1.20.

We will end our overview of the basic properties of $F[x]$ with a powerful result known as the Chinese Remainder Theorem. Before giving the theorem, however, we need this fairly intuitive proposition.

Proposition 1.22: Let $f(x), a(x), b(x) \in F[x]$ with $a(x)$ and $b(x)$ relatively prime. Then $a(x)b(x)|f(x)$ if and only if $a(x)|f(x)$ and $b(x)|f(x)$.

***Proof*:** The first direction of the statement is trivial. For the other direction, suppose $a(x)|f(x)$ and $b(x)|f(x)$. Then $f(x) = a(x)h(x)$ for some $h(x) \in F[x]$, and $b(x)|a(x)h(x)$. Since $\gcd(a(x), b(x)) = 1$, it now follows from Theorem 1.14 that $b(x)|h(x)$. So, $a(x)b(x)|a(x)h(x)$. That is, $a(x)b(x)|f(x)$. ■

Now, we are ready for the theorem.

Theorem 1.23 (Chinese Remainder Theorem): Let $g_1(x), g_2(x), \cdots, g_n(x)$ be arbitrary polynomials, and $m_1(x), m_2(x), \cdots, m_n(x)$ be non-constant pairwise relatively prime polynomials in $F[x]$. Set $m(x) = m_1(x)m_2(x)\cdots m_n(x)$ and let $d = \deg(m(x))$. Then there exists a unique polynomial $r(x) \in F[x]$ with

$$\begin{aligned} r(x) &\equiv g_1(x) \pmod{m_1(x)} \\ r(x) &\equiv g_2(x) \pmod{m_2(x)} \\ &\vdots \\ r(x) &\equiv g_n(x) \pmod{m_n(x)}, \end{aligned}$$

and $\deg(r(x)) < d$.

***Proof*:** Since $m_i(x)$ is relatively prime to $m_j(x)$ for all $j \neq i$, $m_i(x)$ is relatively prime to the product

$$p_i(x) = \prod_{j \neq i} m_j(x).$$

Then $\gcd(m_i(x), p_i(x)) = 1$, and so, by Theorem 1.12, there exist $a_i(x), b_i(x)$ in $F[x]$ with

$$1 = a_i(x)m_i(x) + b_i(x)p_i(x).$$

Observe that $b_i(x)p_i(x)$ satisfies the congruences

$$\begin{aligned} b_i(x)p_i(x) &\equiv 1 \pmod{m_i(x)}, \\ b_i(x)p_i(x) &\equiv 0 \pmod{m_j(x)} \qquad \text{for every } j \neq i. \end{aligned}$$

Set

$$f(x) = g_1(x)b_1(x)p_1(x) + g_2(x)b_2(x)p_2(x) + \cdots + g_n(x)b_n(x)p_n(x).$$

Then clearly $f(x) \equiv g_i(x) \pmod{m_i(x)}$ for each $i = 1, 2, \cdots, n$.

Since $m_1(x), m_2(x), \cdots, m_n(x)$ are pairwise relatively prime, it follows from Proposition 1.22 that $f(x) \equiv h(x) \pmod{m_i(x)}$ for each $i = 1, 2, \cdots, n$ if and only if $f(x) \equiv h(x) \pmod{m(x)}$. By the Division Algorithm, there exists a unique polynomial $r(x)$ with $f(x) \equiv r(x) \pmod{m(x)}$ and $\deg(r(x)) < d$. Then $r(x)$ is the unique polynomial of degree less than d satisfying $r(x) \equiv g_i(x) \pmod{m_i(x)}$ for each $i = 1, 2, \cdots, n$. ■

The Chinese Remainder Theorem will be applied multiple times in Chapter 2. In particular, the theorem will be very useful in the case that the $g_i(x)$'s in the statement of theorem are constant polynomials.

1.3 Field Extensions

Here we will delve further into the structure of finite fields by looking at field extensions. Many of the results in this section can only be proven using high-powered facts from ring theory. For our purposes, there is little consequence of stating or investigating such facts. Hence, in order to naturally progress our work, we will omit quite a few proofs over the course of the section. Most omitted proofs can be found in Dummit[4], pages 509-545.

Let F be a field and $f(x)$ a polynomial in $F[x]$ of degree $n > 0$. Consider the set

$$(f(x)) = \{f(x)g(x) : g(x) \in F[x]\}.$$

In ring theory, $(f(x))$ is called the *principal ideal* of $F[x]$ generated by $f(x)$. Now, we equip the (additive) quotient group

$$F[x]/(f(x)) = \{h(x) + (f(x)) : h(x) \in F[x]\}$$

with the binary operations

$$[a(x) + (f(x))] + [b(x) + (f(x))] = [a(x) + b(x)] + (f(x))$$

and

$$[a(x) + (f(x))] \cdot [b(x) + (f(x))] = a(x)b(x) + (f(x)).$$

It is well-known that these operations are well-defined in $F[x]/(f(x))$, and that, under these operations, $F[x]/(f(x))$ is a ring (generally called a *quotient ring*). Recall from the properties of quotient groups that $h(x) + (f(x)) = g(x) + (f(x))$ iff $h(x) - g(x) \in (f(x))$ iff $h(x) \equiv g(x) \pmod{f(x)}$. By the Division Algorithm, for any $h(x) \in F[x]$, there is a unique $r(x)$ with $h(x) \equiv r(x) \pmod{f(x)}$ and $\deg(r(x)) < n$. Hence, $r(x)$ is the unique polynomial in $F[x]$ satisfying $h(x) + (f(x)) = r(x) + (f(x))$ and $\deg(r(x)) < n$. This shows that every element of $F[x]/(f(x))$ is represented by a polynomial in $F[x]$ of degree $< n$. So, when referring to the elements of $F[x]/(f(x))$, we will usually refer to their representatives of degree $< n$ in $F[x]$. Furthermore, we will do computations in

$F[x]/(f(x))$ by computing congruences mod $f(x)$. Thus, when we compute the congruence $h(x) \equiv g(x) \pmod{f(x)}$, it should be interpreted as the equality $h(x) + (f(x)) = g(x) + (f(x))$.

We now present the relationship between quotients rings and irreducible polynomials.

Proposition 1.24: Let $p(x)$ be an irreducible polynomial over F. Then the quotient ring $F[x]/(p(x))$ is a field.

We observe that the result of Proposition 1.24 does not hold for reducible polynomials. To see this, suppose that $f(x)$ is reducible over F. Then $f(x) = a(x)b(x)$ for some non-constant polynomials $a(x)$ and $b(x)$ of degree $< \deg(f(x))$. Now, $a(x)$ and $b(x)$ correspond to nonzero elements of $F[x]/(f(x))$ and satisfy $a(x)b(x) \equiv 0 \pmod{f(x)}$. This shows that $F[x]/(f(x))$ has zero divisors and hence cannot be a field.

Note that if F and L are fields with $F \subseteq L$, then we say that F is a *subfield* of L. Oftentimes, we only use the term *subfield* when we find a subset of a given field which is itself a field. On the other hand, we use the term *extension field* when we find a superset of a given field which is itself a field. This is formalized in the upcoming defintion.

Definition 1.25: If L is a field containing the subfield F, then L is said to be an *extension field* (or simply an *extension*) of F, denoted $L : F$.

Before proceeding any further, we make a few notes about vector spaces. When referencing a *vector space* V over the field F, we may use some of the following terms: *basis*, *dimension*, *linearly independent*, *scalar*, *span*, *subspace*, and *vector*. All of these terms, including *vector space*, have the same meaning as they do in a first year course in linear algebra. The only difference is that our vectors come from the arbitrary additive abelian group V rather than coming from $\mathbb{R}^n$ exclusively, and our scalars come from the arbitrary field F rather than coming from $\mathbb{R}$ exclusively. If the reader is unfamiliar with vector spaces and any related terms, a wealth of information about these concepts is available online and in standard algebra texts.

We observe that if $L : F$ is some extension of fields, then the multiplication defined in L makes L into a vector space over F.

Definition 1.26: The *degree* of a field extension $L : F$, denoted $[L : F]$, is the dimension of L as a vector space over F. The extension is called *finite* if $[L : F]$ is finite and is called *infinite* otherwise.

In the next theorem, we give a very important property of extension degrees:

Theorem 1.27: Let $F \subseteq K \subseteq L$ be fields. Then $[L : F] = [L : K][K : F]$.

Let $F = \mathbb{Z}/p\mathbb{Z}$, with p a prime number, and suppose that L is an extension of F with $[L : F] = v \in \mathbb{Z}^+$. Then since L is a v-dimensional vector space over F, there is a subset $\{l_1, l_2, \cdots, l_v\}$ of L that forms a basis for L over F. Hence, each element $l \in L$ can be written uniquely in the form $l = a_1 l_1 + a_2 l_2 + \cdots + a_v l_v$, where $a_1, a_2, \cdots, a_v \in F$. Notice that when forming an arbitrary element of L, there are p choices for each of the a_i's, $1 \leq i \leq v$. Thus, L has exactly p^v elements. This demonstrates a strategy for finding new finite fields: Starting with $\mathbb{Z}/p\mathbb{Z}$, we can find a finite field of order p^v if we can find an extension of $\mathbb{Z}/p\mathbb{Z}$ that has degree v.

Naturally, we now ask: is it possible to find extensions of $\mathbb{Z}/p\mathbb{Z}$ with specified (finite) degrees? Remarkably, the answer to this question does turn out to be "yes". In fact, we often use irreducible polynomials to construct extensions of a particular degree. To demonstrate how this is done, we start out with a result that says any irreducible polynomial over a field F has a root in some extension of F.

Theorem 1.28: Let F be a field and $p(x) \in F[x]$ an irreducible polynomial. Then there is an extension $L : F$ and an element $\theta \in L$ such that $p(\theta) = 0$.

***Proof Idea*:** Let $I = (p(x))$ and $L = F[x]/I$. By Proposition 1.24, L is a field. Define the map $\phi : F \to L$ by $\phi(a) = a + I$. It can be seen that the image of this map is isomorphic to the field F, i.e., $\phi(F) \cong F$. Hence, L contains an isomorphic copy of F, and so we can think of L as an extension of F. Let $\theta = x + I$, and suppose $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$. Then

$$\begin{aligned} p(\theta) &= (a_0 + I) + a_1(x + I) + \cdots + a_n(x + I)^n \\ &= (a_0 + a_1 x + \cdots + a_n x^n) + I \\ &= p(x) + I = 0 + I = 0 \in L. \end{aligned}$$

Now, given an irreducible $p(x)$ over F, we know the field $L = F/(p(x))$ is an extension of F which contains a root of $p(x)$. The next theorem gives the degree of the extension $L : F$ as well as a way to explicitly represent L.

Theorem 1.29: Let $p(x)$ be an irreducible polynomial of degree n over the field F, and let $L = F[x]/(p(x))$. Let $\theta = x(\text{mod } p(x)) \in L$. Then the set $\{1, \theta, \theta^2, \cdots, \theta^{n-1}\}$ is a basis for L as a vector space over F. Hence, the degree of the extension $L : F$ is n, and

$$L = \{a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} : a_0, a_1, a_2, \cdots, a_{n-1} \in F\}. \quad (\#\#)$$

Notice that Theorem 1.29 looks at the specific extension $F[x]/(p(x))$ of F and the specific root $x(\text{mod } p(x))$ of $p(x)$ in this extension. It turns out that we do not have to be so specific; we can get an extension of F identical to $(\#\#)$ by simply defining an arbitrary root of $p(x)$ in some arbitrary extension of F (note that Theorem 1.28 guarantees the existence of such a root). Before formally presenting this result, however, we give the following definition.

Definition 1.30: Let $L : F$ be an extension of fields and let $\alpha \in L$. Denote by $F(\alpha)$ the smallest subfield of L which contains both F and the element α. We call $F(\alpha)$ the field *generated* by α over F.

Now, we give the mentioned result.

Theorem 1.31: Let F be a field and $p(x)$ an irreducible polynomial over F. Let α be a root of $p(x)$ in some extension L of F. Then

$$F(\alpha) \cong F[x]/(p(x)).$$

We apply Theorem 1.31 in the upcoming example.

Example 1.32: Let $p(x) = x^4 + 2x + 2 \in (\mathbb{Z}/3\mathbb{Z})[x]$. It can be shown that $p(x)$ has no linear factors or quadratic factors over $\mathbb{Z}/3\mathbb{Z}$. So, $p(x)$ must be irreducible. Now, we let α be an arbitrary root of $p(x)$ in some extension of $\mathbb{Z}/3\mathbb{Z}$. Then, it

follows from Theorem 1.31 that

$$(\mathbb{Z}/3\mathbb{Z})(\alpha) = \{a + b\alpha + c\alpha^2 + d\alpha^3 : a, b, c \in \mathbb{Z}/3\mathbb{Z}\}$$

is a field with $3^4 = 81$ elements. Furthermore, we can do computations in $(\mathbb{Z}/3\mathbb{Z})(\alpha)$ by using the fact that α is a root of $p(x)$. Hence, we use the fact that $\alpha^4 = -2\alpha - 2 = \alpha + 1$ over $\mathbb{Z}/3\mathbb{Z}$. For instance, we multiply the elements $\alpha + 1$ and $\alpha^3 + 2$ as follows:

$$\begin{aligned}(\alpha + 1)(\alpha^3 + 2) &= \alpha^4 + \alpha^3 + 2\alpha + 2 \\ &= (\alpha + 1) + \alpha^3 + 2\alpha + 2 \\ &= \alpha^3.\end{aligned}$$

For a positive integer v, we have established that if there exists an irreducible polynomial over $\mathbb{Z}/p\mathbb{Z}$ of degree v, then there exists a corresponding finite field of order p^v, namely $(\mathbb{Z}/p\mathbb{Z})[x]/(p(x))$. However, we have not established that for every positive integer v, an irreducible polynomial over $\mathbb{Z}/p\mathbb{Z}$ of degree v actually exists. So, we have not yet shown there exists a finite field of order p^v. To get this result (as was promised in Section 1.1), we need to look at a specific class of extension fields called *splitting fields*. Preceding our look at splitting fields, we will give a few more results related to roots of polynomials.

Definition 1.33: Let $L : F$ be an extension of fields. The element $\alpha \in L$ is said to be *algebraic* over F if α is a root of some nonzero polynomial $f(x) \in F[x]$, i.e., $f(\alpha) = 0$.

The next proposition gives the relationship between algebraic elements and irreducible polynomials.

Proposition 1.34: Let $L : F$ be an extension of fields, and let $\alpha \in L$ be algebraic over F. Then there is a unique monic irreducible polynomial $m_\alpha(x) \in F[x]$ which has α as a root. Moreover, a polynomial $f(x) \in F[x]$ has α as root if and only if $m_\alpha(x)$ divides $f(x)$ in $F[x]$.

***Proof*:** Let $g(x) \in F[x]$ be a polynomial of minimal positive degree having α as root. Multiplying $g(x)$ by a unit in F, we may assume that $g(x)$ is monic. Now, for a contradiction, suppose that $g(x)$ is reducible. Then $g(x) = a(x)b(x)$ for some polynomials $a(x), b(x) \in F[x]$, both of degree smaller than the degree of

$g(x)$. Then $0 = g(\alpha) = a(\alpha)b(\alpha)$ in L. Since L has no zero divisors, it follows that $a(\alpha) = 0$ or $b(\alpha) = 0$, which contradicts the minimality of the degree of $g(x)$. Thus, $g(x)$ is irreducible.

Next, suppose that $f(x) \in F[x]$ has α as a root. By the Division Algorithm, there are polynomials $q(x), r(x) \in F[x]$ such that

$$f(x) = g(x)q(x) + r(x) \text{ with } r(x) = 0 \text{ or } \deg(r(x)) < \deg(g(x)).$$

Then $0 = f(\alpha) = g(\alpha)q(\alpha) + r(\alpha) = 0 + r(\alpha) = r(\alpha)$ in L. Now, if $r(x) \neq 0$, then $r(x)$ is a non-constant polynomial of degree less than $g(x)$ having α as root, which contradicts the minimality of the degree of $g(x)$. Hence, $r(x) = 0$, and it follows that $g(x)$ divides $f(x)$ in $F[x]$.

We have established that $g(x)$ divides any polynomial over F which has α as root. In particular, $g(x)$ would divide any other monic irreducible polynomial over F having α has a root. So, it immediately follows that $m_\alpha(x) = g(x)$ is unique. ■

Definition 1.35 The polynomial $m_\alpha(x)$ in Proposition 1.34 is called the *minimal polynomial* for α over F.

We now turn our attention to splitting fields.

Definition 1.36: Let F be a field and $f(x)$ a polynomial of degree $n > 0$ in $F[x]$. An extension K of F is called a *splitting field* for $f(x)$ (over F) if

(i) $f(x)$ factors completely into linear factors (or *splits completely*) in $K[x]$, i.e., $f(x) = c(x - a_1)(x - a_2)\cdots(x - a_n)$ for some $c, a_1, a_2, \cdots, a_n \in K$, and

(ii) $f(x)$ does not factor completely into linear factors over any proper subfield of K containing F.

Here is the major theorem regarding splitting fields.

Theorem 1.37: Let F be a field and $f(x) \in F[x]$. Then $f(x)$ has a splitting field over F which is unique up to isomorphism.

Often, when we are looking at a polynomial $f(x)$ over its splitting field K, we are interested in whether $f(x)$ has any duplicate linear factors over K. Intuitively, we say that $\alpha \in K$ is a *multiple root* of $f(x)$ if $(x - \alpha)^2 | f(x)$ in $K[x]$.

In order to test $f(x)$ for multiple roots, and hence test for duplicate linear factors, we typically inspect the value of its *derivative*.

Definition 1.38: The *derivative* of the polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$$

is defined to be the polynomial

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1 \in K[x].$$

Notice that the definition of the derivative of a polynomial over an arbitrary field is purely algebraic. Hence, the analytic notion of a limit plays no part in this definition of a derivative. The reason for this is that limits, which are continuous operations, cannot be taken in certain fields. With that said, the same differentiation formulas given in a first-year single variable Calculus course still hold true. For example, we get the following formulas for differentiating a sum and a product:

- $(f+g)'(x) = f'(x) + g'(x)$
- $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$.

We now show how derivatives can be used to test for multiple roots.

Proposition 1.39: Let $f(x)$ be a polynomial over the field K. If $f'(x)$ has no root in K, then $f(x)$ has no multiple root in K.

Proof: Suppose that $f(x)$ has a multiple root at $\alpha \in K$. Then $f(x) = (x-\alpha)^2 h(x)$ for some $h(x) \in K[x]$. Now, by the formula for differentiating a product,

$$\begin{aligned} f'(x) &= 2(x-\alpha)h(x) + (x-\alpha)^2 h'(x) \\ &= (x-\alpha)(2h(x) + (x-\alpha)h'(x)). \end{aligned}$$

Thus, α is a root of $f'(x)$. ■

In the next example, we use splitting fields to demonstrate the existence and uniqueness of a particular finite field.

Example 1.40: Consider $x^4 - x \in (\mathbb{Z}/2\mathbb{Z})[x]$. Notice that

$$x^4 - x = x(x-1)(x^2 + x + 1).$$

Since $x^2 + x + 1$ is irreducible over $\mathbb{Z}/2\mathbb{Z}$, it follows that $\mathbb{Z}/2\mathbb{Z}$ is not the splitting field for $x^4 - x$. Now, let α be an arbitrary root of $x^2 + x + 1$ in some extension of $\mathbb{Z}/2\mathbb{Z}$, and consider the field

$$(\mathbb{Z}/2\mathbb{Z})(\alpha) = \{a + b\alpha : a, b \in \mathbb{Z}/2\mathbb{Z}\}.$$

Notice that

$$x^4 - x = x(x-1)(x-\alpha)(x-(1+\alpha)).$$

Clearly $x^4 - x$ does not split completely over any proper subfield of $(\mathbb{Z}/2\mathbb{Z})(\alpha)$. Hence, $(\mathbb{Z}/2\mathbb{Z})(\alpha)$ is the splitting field for $x^4 - x$ over $\mathbb{Z}/2\mathbb{Z}$.
Moreover, we note that $(\mathbb{Z}/2\mathbb{Z})(\alpha)$ is a finite field containing 4 elements. Suppose that $\mathbb{F}$ is another finite field of order 4. Then it follows from Theorem 1.5 that $\mathbb{F}$ has characteristic 2 and hence must contain an isomorphic copy of $\mathbb{Z}/2\mathbb{Z}$ as a subfield. Furthermore, by the Generalized FLT, each element $a \in \mathbb{F}$ is a root of the polynomial $x^4 - x$ in $\mathbb{F}[x]$. Correspondingly, $x^4 - x$ has four distinct linear factors in $\mathbb{F}[x]$. Since $x^4 - x$ is also of degree 4, it must be that $\mathbb{F}$ is a splitting field for $x^4 - x$ over $\mathbb{Z}/2\mathbb{Z}$. By Theorem 1.37, splitting fields are unique up to isomorphism, and so we have that $(\mathbb{Z}/2\mathbb{Z})(\alpha) \cong \mathbb{F}$. This shows that, up to isomorphism, there exists a unique finite field of order 4.

With the strategy of Example 1.40 in mind, we prove there exists a unique finite field of any prime power order.

Theorem 1.41: For every prime number p and positive integer v, up to isomorphism, there exists a unique finite field of order p^v.

Proof: Let $q = p^v$, and consider the polynomial $x^q - x \in (\mathbb{Z}/p\mathbb{Z})[x]$. Let $\mathbb{K}$ be the splitting field for $x^q - x$ over $\mathbb{Z}/p\mathbb{Z}$. Since $\mathbb{K}$ has $\mathbb{Z}/p\mathbb{Z}$ as a subfield, $\mathbb{K}$ must have characteristic p. So, the derivative of $x^q - x$ over $\mathbb{K}$ is $qx^{q-1} - 1 = -1$. Since the derivative of $x^q - x$ has no roots, by Proposition 1.38, $x^q - x$ has no multiple roots in $\mathbb{K}$. Because $\mathbb{K}$ is also the splitting field for $x^q - x$, it follows that $x^q - x$ has exactly q distinct roots in $\mathbb{K}$. Let $\mathbb{A}$ be the set containing these q distinct roots, i.e., $\mathbb{A} = \{a \in \mathbb{K} : a^q = a\}$. We note the following properties of $\mathbb{A}$:

- For any $a, b \in \mathbb{A}$, it follows from Theorem 1.6 that $(a-b)^q = a^q - b^q = a - b$, and so $a - b \in \mathbb{A}$. This shows that $\mathbb{A}$ is closed under addition and additive inverses;

- For any $a, b \in \mathbb{A}$ with $b \neq 0$, since multiplication is commutative in the field $\mathbb{K}$, $(ab^{-1})^q = a^q(b^{-1})^q = a^q(b^q)^{-1} = ab^{-1}$, and so $ab^{-1} \in \mathbb{A}$. This establishes that $\mathbb{A}$ is closed under multiplication and multiplicative inverses.

Since $\mathbb{A}$ inherits all of the other properties of a field from $\mathbb{K}$, it follows that $\mathbb{A}$ is a subfield of $\mathbb{K}$. Clearly $\mathbb{A}$ has characteristic p, and so contains $\mathbb{Z}/p\mathbb{Z}$. Furthermore, $x^q - x$ splits completely in $\mathbb{A}$, since $\mathbb{A}$ contains all of its roots. Hence, the splitting field of $x^q - x$ over $\mathbb{Z}/p\mathbb{Z}$ is a subfield of $\mathbb{A}$; that is, $\mathbb{K}$ is a subfield of $\mathbb{A}$. Thus, $\mathbb{K} = \mathbb{A}$, and $\mathbb{K}$ is a finite field of order q.

For uniqueness, suppose that $\mathbb{F}$ is a finite field with q elements. Then, by Theorem 1.5, $\mathbb{F}$ has characteristic p and hence contains $\mathbb{Z}/p\mathbb{Z}$. Now, it follows from the Generalized FLT that $a^q - a = 0$ for all elements $a \in \mathbb{F}$. So each of the q elements of $\mathbb{F}$ is a root of $x^q - x$. Correspondingly, $x^q - x$ has q distinct linear factors in $\mathbb{F}[x]$. Since $x^q - x$ also has degree q, it must be that $\mathbb{F}$ is a splitting field for $x^q - x$ over $\mathbb{Z}/p\mathbb{Z}$. Since splitting fields are unique up to isomorphism, we have that $\mathbb{K} \cong \mathbb{F}$. Thus, up to isomorphism, $\mathbb{K}$ is the unique finite field of order q. ■

Observe that the proof of Theorem 1.41 shows us that the splitting field for the polynomial $x^q - x$ over $\mathbb{Z}/p\mathbb{Z}$ is precisely the unique field of order $q = p^v$. Throughout the remainder of our work, we will denote the unique finite field of order $q = p^v$ by $\mathbb{F}_q$. Specifically, in the case where $v = 1$, we will use the notation $\mathbb{F}_p$ in place of $\mathbb{Z}/p\mathbb{Z}$.

The final results of this section give a few additional properties of $\mathbb{F}_q$.

Proposition 1.42: The multiplicative group of nonzero elements of $\mathbb{F}_q$, denoted $(\mathbb{F}_q)^\times$, is cyclic.

Proof: Since $(\mathbb{F}_2)^\times$ contains only one element, it is clearly cyclic. So, we may assume that $q \geq 3$. Set $r = q - 1$, the order of $(\mathbb{F}_q)^\times$, and let $r = {p_1}^{w_1}{p_2}^{w_2} \cdots {p_k}^{w_k}$ be its factorization into powers of distinct primes. We will denote the order of an element a in the multiplicative group $(\mathbb{F}_q)^\times$ by $\text{ord}(a)$. Recall from group theory that if m is a positive integer with $a^m = 1$, then $\text{ord}(a)|m$. In particular, since $a^r = 1$, we have that $\text{ord}(a)|r$.

Now, for each $1 \leq i \leq k$, the polynomial $x^{r/p_i} - 1$ has at most r/p_i roots in $\mathbb{F}_q$. Then since $r/p_i < r$, there exists an element $a_i \in (\mathbb{F}_q)^\times$ which is not a root of $x^{r/p_i} - 1$. Set $b_i = {a_i}^{r/{p_i}^{w_i}}$. Then ${b_i}^{{p_i}^{w_i}} = {a_i}^r = 1$, and it follows that $\text{ord}(b_i)$

divides ${p_i}^{w_i}$. But,

$$ {b_i}^{p_i{}^{w_i-1}} = {a_i}^{r/p_i} \neq 1, $$

which shows that $\text{ord}(b_i)$ cannot be a proper divisor of ${p_i}^{w_i}$. So it must that $\text{ord}(b_i) = {p_i}^{w_i}$.

Let $b = b_1 b_2 \cdots b_k \in (\mathbb{F}_q)^\times$. Assume, by way of contradiction, that $\text{ord}(b) \neq r$. Then $\text{ord}(b)$ is a proper divisor of r and hence must divide r/p_i for some $1 \leq i \leq k$. Without loss of generality, assume that $\text{ord}(b)$ divides r/p_1. Then

$$ 1 = b^{r/p_1} = {b_1}^{r/p_1} {b_2}^{r/p_1} \cdots {b_k}^{r/p_1}. $$

Notice that for $2 \leq i \leq k$, $\text{ord}(b_i)$ divides r/p_1, which implies ${b_i}^{r/p_1} = 1$. This forces ${b_1}^{r/p_1} = 1$, and it follows that $\text{ord}(b_1)$ divides r/p_1. But, this contradicts that fact that $\text{ord}(b_1) = {p_1}^{w_1}$. Thus, $\text{ord}(b) = r = q - 1$, and b is a generator for $(\mathbb{F}_q)^\times$. This shows that $(\mathbb{F}_q)^\times$ is cyclic. ■

We can use Proposition 1.42 to establish an important result related to irreducible polynomials in $\mathbb{F}_q[x]$.

Proposition 1.43: For every positive integer n, there exists an irreducible polynomial of degree n over $\mathbb{F}_q$.

Proof: Let α be a generator of the cyclic group $(\mathbb{F}_{q^n})^\times$. Then clearly $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$. Note that since α is a root of the polynomial $x^{q^n} - x \in \mathbb{F}_q[x]$, α is algebraic over $\mathbb{F}_q$. Now, consider the minimal polynomial, $m_\alpha(x)$, of α over $\mathbb{F}_q$. By definition, $m_\alpha(x)$ is irreducible. Suppose that $\deg(m_\alpha(x)) = d$. Then $\mathbb{F}_q[x]/(m_\alpha(x)) \cong \mathbb{F}_{q^d}$. But, by Theorem 1.31,

$$ \mathbb{F}_q[x]/(m_\alpha(x)) \cong \mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}. $$

Thus, $q^d = q^n$, and $d = n$. ■

In particular, for any prime number p and positive integer v, Proposition 1.43 says that there exists an irreducible polynomial, say $f(x)$, over $\mathbb{F}_p$ of degree v. Then $\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_q$, where $q = p^v$. Now, if $f(x)$ is known, then we can use Theorem 1.29 to do computations in $\mathbb{F}_p[x]/(f(x))$, which is equivalent to doing computations in the finite field $\mathbb{F}_q$. The hard part is actually finding the irreducible polynomial $f(x)$. In Chapter 3, we will use results relating to our factoring algorithms to develop a process for finding irreducible polynomials of any given degree

over any finite field. In particular, the significance of being able to find irreducible polynomials of any degree over $\mathbb{F}_p$ is that we can do computations in any finite field of our choosing.

Now, in the following chapters, we use the theory that we have built to generate factoring algorithms for polynomials over $\mathbb{F}_q$.

Chapter 2

Berlekamp's Method

In this chapter, we will develop a deterministic algorithm for factoring polynomials over the finite field $\mathbb{F}_q$, where $q = p^v$ with p a prime number and v a positive integer. The general factoring method we will present is due to Berlekamp[1] and will provide us with a way to completely factor any polynomial over $\mathbb{F}_q$. Before generating the main algorithm, however, we offer an optional pre-processing stage called Square-Free Factorization (SFF). As mentioned in our introduction, factoring algorithms generally run much better when the input polynomial is square-free. This is so much the case that some authors actually formulate condensed algorithms that are restricted to square-free inputs. While no algorithm in this paper has such a restriction, we often recommend that SFF be employed as the initial factoring step.

We note that all algorithms we present will only accept input polynomials which are monic. We do not lose any generality with this restriction. For example, if $f(x) = \sum_{i=0}^{n} a_i x^i$ is a polynomial over $\mathbb{F}_q$ of degree n with $a_n \neq 1$, we start by factoring the monic polynomial $a_n^{-1} f(x)$. Then multiplying the factorization of $a_n^{-1} f(x)$ by a_n will give the factorization of $f(x)$.

2.1 Square-Free Factorization

Loosely speaking, a polynomial $f(x) \in \mathbb{F}_q[x]$ is *square-free* if it has no repeated non-constant factors. We give the formal definition:

Definition 2.1: A polynomial $f(x) \in \mathbb{F}_q[x]$ is *square-free* if $g(x)^2 \nmid f(x)$ for each non-constant polynomial $g(x) \in \mathbb{F}_q[x]$.

The conventional way to determine whether $f(x)$ is square-free is to inspect the value of its derivative, $f'(x)$. The major relationship between $f(x)$ and $f'(x)$ is given in the upcoming theorem.

Theorem 2.2: If $f(x)$ is a polynomial over $\mathbb{F}_q$ with $\gcd(f(x), f'(x)) = 1$, then $f(x)$ is square-free.

***Proof*:** Suppose $f(x)$ is not square-free. Then there is a non-constant polynomial $g(x) \in \mathbb{F}_q[x]$ such that $g(x)^2$ divides $f(x)$. So, $f(x) = g(x)^2 h(x)$ for some $h(x) \in \mathbb{F}_q[x]$, and applying the formula for differentiating a product, we have

$$f'(x) = 2g(x)g'(x) \cdot h(x) + g(x)^2 \cdot h'(x).$$

Clearly $g(x)$ is a common divisor of $f(x)$ and $f'(x)$. Thus, $\gcd(f(x), f'(x)) \neq 1$. ■

If $f(x)$ is a polynomial over $\mathbb{F}_q$ that is not square-free, then, by Theorem 2.2, $\gcd(f(x), f'(x)) \neq 1$. But, is it necessarily the case that $\gcd(f(x), f'(x))$ is a nontrivial factor of $f(x)$? The answer here is "no"; it may very well be the case that $\gcd(f(x), f'(x)) = f(x)$.

Consider, for example, the polynomial $f(x) = x^{14} + 3x^7 + 2$ over $\mathbb{F}_7$. Then $f'(x) = 14x^{13} + 21x^6 = 0$, and hence $\gcd(f(x), f'(x)) = f(x)$. Notice here that each exponent on x in $f(x)$ is a multiple of 7, which is the characteristic of $\mathbb{F}_7$. This observation is generalized in the following Theorem.

Theorem 2.3: Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of degree $n > 0$ such that $\gcd(f(x), f'(x)) = f(x)$. Then there exists a polynomial $g(x) \in \mathbb{F}_q[x]$ with $f(x) = g(x^p)$. Furthermore, if $g(x) = \sum_j b_j x^j$, then $f(x) = \left(\sum_j b_j^{p^{v-1}} x^j \right)^p$ so that $f(x)^{\frac{1}{p}} = \sum_j b_j^{p^{v-1}} x^j$.

***Proof*:** Since $\deg(f'(x)) < \deg(f(x))$ and $\gcd(f(x), f'(x)) = f(x)$, it must be that $f'(x) = 0$. Suppose $f(x)$ has summation representation $f(x) = \sum_{i=0}^{n} a_i x^i$, where some of the a_i values may be zero. Then $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$, and hence $i a_i = 0$ in $\mathbb{F}_q$ for all i. Since $\mathbb{F}_q$ has characteristic p, it now follows that each $i \in \{1, \cdots, n\}$ with $a_i \neq 0$ is some multiple p. Because $f(x)$ has degree n, observe, in particular, that n is some multiple of p. Let $g(x) = \sum_{j=0}^{n/p} b_j x^j$, where $b_j = a_{pj}$ for each j. Then clearly $f(x) = g(x^p)$. Moreover, applying Theorem 1.6 and the Generalized FLT,

$$\begin{aligned} \left(\sum_{j=0}^{n/p} b_j^{p^{v-1}} x^j \right)^p &= \sum_{j=0}^{n/p} b_j^{p^v} x^{jp} \\ &= \sum_{j=0}^{n/p} b_j^q (x^p)^j \end{aligned}$$

$$= \sum_{j=0}^{n/p} b_j (x^p)^j$$
$$= g(x^p)$$
$$= f(x). \quad \blacksquare$$

We will now turn our attention to finding the square-free factorization of a non-constant monic polynomial $f(x) \in \mathbb{F}_q[x]$. To begin, note that since we can combine irreducibles that are raised to the same power in the complete factorization of $f(x)$, there exist unique pairs $(g_i(x), s_i)$, $1 \leq i \leq r$, with the following properties:

- $f(x) = \prod_{i=1}^{r} g_i(x)^{s_i}$
- each $g_i(x)$ is a square-free, non-constant polynomial over $\mathbb{F}_q$
- the $g_i(x)$ are pairwise relatively prime
- $s_i < s_j$ for $i < j$.

Observe that each $g_i(x)$ is the product of all distinct irreducible factors $h(x)$ of $f(x)$ with $h(x)^{s_i} | f(x)$ and $h(x)^{s_i+1} \nmid f(x)$.

The goal of SFF is to identify the pairs $(g_i(x), s_i)$. To accomplish this goal, we need to consider two scenarios.

Scenario 1: In this scenario, we suppose $\gcd(f(x), f'(x)) \neq f(x)$. First, notice that

$$f'(x) = \sum_{i=1}^{r} [(s_i g_i(x)^{s_i - 1} g_i'(x)) \cdot \prod_{\substack{1 \leq j \leq r \\ j \neq i}} g_j(x)^{s_j}].$$

Now, for each i with $s_i \not\equiv 0 \pmod{p}$, $\gcd(g_i(x)^{s_i}, f'(x)) = g_i(x)^{s_i - 1}$. On the other hand, for each i with $s_i \equiv 0 \pmod{p}$, $\gcd(g_i(x)^{s_i}, f'(x)) = g_i(x)^{s_i}$. Since the $g_i(x)^{s_i}$ are pairwise relatively prime, we can apply Proposition 1.13 inductively to get

$$\begin{aligned} \gcd(f(x), f'(x)) &= \prod_{i=1}^{r} \gcd(g_i(x)^{s_i}, f'(x)) \\ &= \prod_{\substack{1 \leq i \leq r \\ s_i \equiv 0 (p)}} g_i(x)^{s_i} \cdot \prod_{\substack{1 \leq i \leq r \\ s_i \not\equiv 0 (p)}} g_i(x)^{s_i - 1} \quad . \end{aligned}$$

Next, set

$$d(x) = \frac{f(x)}{\gcd(f(x), f'(x))} = \prod_{\substack{1 \le i \le r \\ s_i \not\equiv 0 (p)}} g_i(x).$$

Observe that since $\gcd(f(x), f'(x)) \neq f(x)$, we have that $d(x) \neq 1$. We can now begin a process for identifying the pairs $(g_i(x), s_i)$ for i with $s_i \not\equiv 0 \pmod{p}$. Let

$$\begin{aligned} f_1(x) &= \gcd(f(x), f'(x)) \\ h_1(x) &= \gcd(f_1(x), d(x)) \\ m_1(x) &= d(x)/h_1(x). \end{aligned}$$

If $s_1 = 1$, then clearly $m_1(x) = g_1(x)$, and we get the pair $(g_1(x), 1)$. Otherwise $m_1(x) = 1$. Regardless, we go on to compute

$$\begin{aligned} f_2(x) &= f_1(x)/h_1(x) \\ h_2(x) &= \gcd(f_2(x), h_1(x)) \\ m_2(x) &= h_1(x)/h_2(x). \end{aligned}$$

If $2 \in \{s_i : 1 \le i \le r,\ s_i \not\equiv 0 (\text{mod } p)\}$, then $m_2(x) = g_i(x)$ with $i = 1$ or $i = 2$ (depending on whether $s_1 = 1$ or $s_1 \neq 1$), and we get the pair $(g_i(x), 2)$. Otherwise $m_2(x) = 1$. Regardless, we go on to compute

$$\begin{aligned} f_3(x) &= f_2(x)/h_2(x) \\ h_3(x) &= \gcd(f_3(x), h_2(x)) \\ m_3(x) &= h_2(x)/h_3(x), \end{aligned}$$

and $m_3(x)$ either gives the pair $(g_i(x), 3)$ for some $i \in \{1, 2, 3\}$ or $m_3(x) = 1$. Continuing on, in general, for the k_{th} step we get

$$\begin{aligned} f_k(x) &= f_{k-1}(x)/h_{k-1}(x) \\ h_k(x) &= \gcd(f_k(x), h_{k-1}(x)) \\ m_k(x) &= h_{k-1}(x)/h_k(x), \end{aligned}$$

where $1 < k \le s_r$. If $k \in \{s_i : 1 \le i \le r,\ s_i \not\equiv 0 (\text{mod } p)\}$, then $m_k(x) = g_i(x)$ for some $i \in \{1, \cdots, k\}$, and we get the pair $(g_i(x), k)$. Otherwise $m_k(x) = 1$.

The process terminates when we reach a k value for which $h_k(x) = 1$. By the end of the process, we will have necessarily collected the pairs $(g_i(x), s_i)$ for all i values with $s_i \not\equiv 0 \pmod{p}$.

Suppose k_0 is the largest number in $\{s_i : 1 \leq i \leq r,\ s_i \not\equiv 0 \pmod{p}\}$. Then in step k_0, we get $h_{k_0}(x) = 1$, and the process terminates. Our remaining task is to find the pairs $(g_i(x), s_i)$ for i values with $s_i \equiv 0 \pmod{p}$. To accomplish this, we need to find the SFF of the polynomial

$$f_{k_0}(x) = \frac{\gcd(f(x), f'(x))}{\prod\limits_{\substack{1 \leq i \leq r \\ s_i \not\equiv 0(p)}} g_i(x)^{s_i - 1}}.$$

If $\{i : s_i \equiv 0 \pmod{p}\} = \emptyset$, then $f_{k_0}(x) = 1$, and there is nothing left to do. However, if $\{i : s_i \equiv 0 \pmod{p}\} \neq \emptyset$, then we must handle the polynomial

$$f_{k_0}(x) = \prod_{\substack{1 \leq i \leq r \\ s_i \equiv 0(p)}} g_i(x)^{s_i},$$

whose derivative is 0 over $\mathbb{F}_q$. How we go about the SFF of such a polynomial is described in the upcoming scenario.

Scenario 2: Here we suppose that $\gcd(f(x), f'(x)) = f(x)$, which occurs precisely when $f'(x) = 0$. By Theorem 2.3, $f(x)$ is a p_{th} power. So, we can compute $z_1(x) = (f(x))^{\frac{1}{p}}$, the p_{th} root of $f(x)$. However, it is possible that $z_1(x)$ has a derivative of 0 and hence is another p_{th} power. In such a situation, we would need to compute $z_2(x) = z_1(x)^{\frac{1}{p}}$. So, we continue computing p_{th} roots until we get a polynomial whose derivative is nonzero. Say it takes w p_{th} root computations to get a polynomial with a nonzero derivative. Then we need to consider two subcases for $z_w(x)$:

(1) If $\gcd(z_w(x), z_w'(x)) = 1$, then $z_w(x)$ is square-free, and $z_w(x)^{p^w}$ will give us the SFF of $f(x)$.

(2) If $\gcd(z_w(x), z_w'(x)) \neq 1$, then we enter $z_w(x)$ into the process described in scenario 1 to begin finding the SFF of $z_w(x)$. Once the SFF of $z_w(x)$ is found, we raise $z_w(x)$ to the p^w power in order to obtain the SFF of $f(x)$.

Next we offer an iterative algorithm, developed by Shoup[6], that condenses the general strategy we have developed for SFF. Note that the algorithm takes as input a non-constant monic polynomial $f \in \mathbb{F}_q[x]$.

SFF Algorithm over $\mathbb{F}_q$:

$k \leftarrow 1$

repeat

$j \leftarrow 1, \quad d \leftarrow f/\gcd(f, f')$

repeat

$f \leftarrow f/d, \quad h \leftarrow \gcd(f, d), \quad m \leftarrow d/h$

if $m \neq 1$, then

output (m, jk)

end if

$d \leftarrow h, \quad j \leftarrow j + 1$

until $d = 1$

if $f \neq 1$, then

$f \leftarrow f^{\frac{1}{p}}, \quad s \leftarrow ps$

end if

until $f = 1$

The SFF algorithm is equivalent to the process we developed earlier for SFF and hence outputs the desired pairs $(g_i(x), s_i)$. In the upcoming example, we find the SFF of a specific polynomial over $\mathbb{F}_5$.

Example 2.4: Consider $f(x) = x^{13} + 3x^{10} + 3x^8 + 2x^6 + x^5 + 2x^3 + 2x + 3 \in \mathbb{F}_5[x]$. First, we compute

$$f'(x) = 3x^{12} + 4x^7 + 2x^5 + x^2 + 2.$$

Using the Euclidean Algorithm, we find

$$\gcd(f(x), f'(x)) = x^8 + 4x^7 + x^5 + x^3 + 4x^2 + 1.$$

Since $\gcd(f(x), f'(x)) \neq f(x)$, we enter the process described in Scenario 1. Set

$$d(x) = \frac{f(x)}{\gcd(f(x), f'(x))} = x^5 + x^4 + x^3 + 3x^2 + 2x + 3.$$

For the first step, we have

$$\begin{aligned} f_1(x) &= \gcd(f(x), f'(x)) \\ h_1(x) &= \gcd(f_1(x), d(x)) = x^3 + 4x^2 + 1 \\ m_1(x) &= d(x)/h_1(x) = x^2 + 2x + 3. \end{aligned}$$

Thus, we get the pair $(x^2 + 2x + 3, 1)$. Now, for the next step, we have

$$\begin{aligned} f_2(x) &= f_1(x)/h_1(x) = x^5 + 1 \\ h_2(x) &= \gcd(f_2(x), h_1(x)) = 1 \\ m_2(x) &= h_1(x)/h_2(x) = x^3 + 4x^2 + 1. \end{aligned}$$

This gives the pair $(x^3 + 4x^2 + 1, 2)$. Since $h_2(x) = 1$, the process terminates, and we are left with the task of finding the SFF of $f_2(x) = x^5 + 1$. For this, we enter Scenario 2. Applying Theorem 2.3, we see that $f_2(x) = (x + 1)^5$, and so $(f_2(x))^{\frac{1}{5}} = x + 1$. Now since $x + 1$ is square-free, $f_2(x) = (x + 1)^5$ is the SFF of $f_2(x)$. With respect to $f(x)$, this gives us the pair $(x + 1, 5)$. Thus,

$$f(x) = (x^2 + 2x + 3)(x^3 + 4x^2 + 1)^2(x + 1)^5$$

is the SFF of $f(x)$.

Note that this is not the complete factorization of $f(x)$ into irreducibles. In order to find the complete factorization, we need to write the square-free factors x^2+2x+3, x^3+4x^2+1, and $x+1$ as products of irreducibles. Clearly $x+1$ is itself irreducible. Since $x^2 + 2x + 3$ has no roots in $\mathbb{F}_5$, it is also irreducible. However, x^3+4x^2+1 has a root at 2, and it turns out that $x^3+4x^2+1 = (x+3)(x^2+x+2)$ is the complete factorization of this polynomial. Hence,

$$f(x) = (x^2 + 2x + 3)(x + 3)^2(x^2 + x + 2)^2(x + 1)^5$$

is the complete factorization of $f(x)$ over $\mathbb{F}_5$.

In Example 2.4, SFF alone nearly yielded a complete factorization of the given polynomial. This will not always be the case. When a polynomial has many distinct irreducible factors raised to the same power in its complete factorization, we will surely require the algorithm in the upcoming section to separate these irreducibles. With that said, however, for non-square-free high degree polynomials with few distinct irreducible factors, like the one in Example 2.4, SFF is a very powerful factoring tool.

To conclude this section, we look at polynomials which are known to be powers of a single irreducible. While our SFF process can find the complete factorization of such polynomials, it requires more work than is actually needed; we will provide a simpler factoring strategy. Suppose it is known that $f(x)$ is the power of a single irreducible. Then $f(x) = g(x)^s$ for some irreducible $g(x)$ and some positive integer s. In seeking to identify $g(x)$ and s, we consider two cases:

(i) Suppose $f'(x) \neq 0$. Then $g(x) = \dfrac{f(x)}{\gcd(f(x), f'(x))}$, and $s = \dfrac{\deg(f(x))}{\deg(g(x))}$.

(ii) Suppose $f'(x) = 0$. Then $f(x)$ is a p_{th} power, and $s = kp^w$ for some positive integers k and w with $k \not\equiv 0 \pmod{p}$. Now, we take p_{th} roots until we obtain a polynomial, say $h(x)$, which has a nonzero derivative. The number of p_{th} roots taken gives the value of w. Since $f(x) = h(x)^{p^w}$, it follows that $h(x) = g(x)^k$. So we use the strategy described in case (i) above on $h(x)$ to determine $g(x)$ and k.

In Example 2.5, we utilize this method.

Example 2.5: Given that $f(x) = x^{42}+2x^{35}+2x^{28}+3x^{21}+2x^{14}+2x^7+1 \in \mathbb{F}_7[x]$ can be expressed as the power of a single irreducible, we find the complete factorization of $f(x)$. It is easily seen that $f'(x) = 0$. So we calculate the 7_{th} root

$$h(x) = f(x)^{\frac{1}{7}} = x^6 + 2x^5 + 2x^4 + 3x^3 + 2x^2 + 2x + 1.$$

Now

$$h'(x) = 6x^5 + 3x^4 + x^3 + 2x^2 + 4x + 2 \neq 1.$$

Then we compute

$$\gcd(h(x), h'(x)) = x^4 + 6x^3 + 4x^2 + 6x + 1$$

and

$$d(x) = \frac{h(x)}{\gcd(h(x), h'(x))} = x^2 + 3x + 1.$$

Notice that $(\deg(h(x)))/(\deg(d(x))) = 3$. So $h(x) = (x^2 + 3x + 1)^3$, and we get $f(x) = (x^2 + 3x + 1)^{3 \cdot 7} = (x^2 + 3x + 1)^{21}$, which is the desired factorization.

The reader may be wondering: Under what circumstances might we know a polynomial is the power of a single irreducible before finding its factorization? Well, in the upcoming section, our General Factoring Algorithm will output polynomials of just this form. We will require the method of Example 2.5 in conjunction with our General Factoring Algorithm to have a complete factoring process over $\mathbb{F}_q$.

2.2 The General Factoring Algorithm

We will now use the method of Berlekamp[1] to develop our first large-scale factoring algorithm. This method of factoring is deterministic, and the algorithm presented here will have the ability to decompose any polynomial over $\mathbb{F}_q$ into pairwise relatively prime factors so that each factor can be expressed as the power of a single irreducible. After applying the algorithm to a polynomial, we will require the method of factoring powers of irreducibles that was presented in the previous section to find the complete factorization of the polynomial. This will be the only technique in our factoring process that is independent of the algorithm itself.

Berlekamp's method relies on polynomial long division and solving systems of equations using matrices. In particular, the efficiency of the algorithm rests on the efficiency of gcd computations using the Euclidean Algorithm and the efficiency of finding the reduced row echelon form of matrices with entries in $\mathbb{F}_q$.

Throughout this section, let $f(x) \in \mathbb{F}_q[x]$ be a non-constant monic polynomial of degree n with complete factorization $f(x) = f_1(x)^{k_1} f_2(x)^{k_2} \cdots f_m(x)^{k_m}$, where $k_1, k_2, ..., k_m$ are positive integers and $f_1(x), f_2(x), ..., f_m(x)$ are distinct monic irreducibles.

Our goal is to generate an algorithm for determining the factors $f_i(x)^{k_i}$. To accomplish this, we need to investigate polynomials $g(x) \in \mathbb{F}_q[x]$ of degree $< n$ with the property that $f(x)$ divides $g(x)^q - g(x)$. The following proposition begins to lay the framework for how such polynomials can be used as factoring tools.

Proposition 2.6: Let $g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_d x^d \in \mathbb{F}_q[x]$ be a polynomial of degree $d < n$. Let $R(h(x))$ denote the unique remainder of $h(x)$ after division by $f(x)$. The following are equivalent.

(a) $f(x)$ divides the product $\prod_{s \in \mathbb{F}_q} (g(x) - s)$.

(b) $R(g(x^q)) = g(x)$.

(c) For each $i = 1, 2, ..., m$, there is a unique $s_i \in \mathbb{F}_q$ with $g(x) \equiv s_i \pmod{f_i(x)^{k_i}}$.

Proof: Applying Theorem 1.6 and the Generalized FLT, notice

$$\begin{aligned} g(x)^q &= (b_0 + b_1 x + b_2 x^2 + \cdots + b_d x^d)^q \\ &= b_0^q + b_1^q x^q + b_2^q x^{2q} + \cdots + b_d^q x^{dq} \\ &= b_0 + b_1 x^q + b_2 x^{2q} + \cdots + b_d x^{dq} \\ &= g(x^q). \end{aligned}$$

Now, by the definition of $R(g(x^q)) = R(g(x)^q)$, we have that

$$g(x)^q = f(x)q(x) + R(g(x^q))$$

for some $q(x) \in \mathbb{F}_q[x]$. Notice that $f(x)$ divides

$$g(x)^q - g(x) = f(x)q(x) - (R(g(x^q)) - g(x))$$

if and only if $f(x)$ divides $R(g(x^q)) - g(x)$. By the Division Algorithm, $R(g(x^q)) < n = \deg(f(x))$. Since we also have $\deg(g(x)) < n$, it follows that

$$\deg[R(g(x^q)) - g(x)] < n.$$

Thus, $f(x)$ divides $R(g(x^q)) - g(x)$ iff $R(g(x^q)) - g(x) = 0$.

Recall that the polynomial $u^q - u$ has a root at each $s \in \mathbb{F}_q$. So, $u^q - u$ factors as

$$u^q - u = \prod_{s \in \mathbb{F}_q} (u - s).$$

Setting $u = g(x)$ gives

$$g(x)^q - g(x) = \prod_{s \in \mathbb{F}_q} (g(x) - s).$$

Thus, $f(x)$ divides $\prod_{s \in \mathbb{F}_q}(g(x) - s)$ iff $R(g(x)^q) = g(x)$. This shows that (a) and (b) are equivalent.

Suppose that $f(x)$ divides $\prod_{s \in \mathbb{F}_q}(g(x) - s)$. Then for each $i = 1, 2, \cdots, m$, both $f_i(x)^{k_i}$ and $f_i(x)$ divide $\prod_{s \in \mathbb{F}_q}(g(x) - s)$. Since $f_i(x)$ is irreducible, it follows from Corollary 1.17 that $f_i(x) | g(x) - s_i$ for some $s_i \in \mathbb{F}_q$. Now, if $f_i(x)^{k_i}$ does not divide $g(x) - s_i$, then it must be that $f_i(x)$ also divides $g(x) - s_{i_0}$ for some $s_{i_0} \in \mathbb{F}_q$ with $s_{i_0} \neq s_i$. However, this cannot be the case, since $g(x) - s_i$ and $g(x) - s_{i_0}$ are relatively prime. So, $f_i(x)^{k_i} | g(x) - s_i$, and hence $g(x) \equiv s_i \pmod{f_i(x)^{k_i}}$. Furthermore, this s_i is unique due to the observation that $g(x) - s_i$ and $g(x) - s_{i_0}$ are relatively prime for $s_i \neq s_{i_0}$.

Next, suppose that for each $i = 1, 2, \cdots, m$, there is an $s_i \in \mathbb{F}_q$ such that $g(x) \equiv s_i \pmod{f_i(x)^{k_i}}$. Then clearly for each $i = 1, 2, \cdots, m$, $f_i(x)^{k_i}$ divides $\prod_{s \in \mathbb{F}_q}(g(x) - s)$. Since $f_1(x)^{k_1}, f_2(x)^{k_2}, \cdots, f_m(x)^{k_m}$ are relatively prime, it now follows from Proposition 1.22 that $f_1(x)^{k_1} f_2(x)^{k_2} \cdots f_m(x)^{k_m} = f(x)$ divides $\prod_{s \in \mathbb{F}_q}(g(x) - s)$.

Thus, (a) and (c) are equivalent. ■

In the upcoming theorem, Proposition 2.6 will be used to show that the set $V = \{g(x) \in \mathbb{F}_q[x] : \deg(g(x)) < n \text{ and } g(x)^q \equiv g(x) \pmod{f(x)}\}$ is a vector space over $\mathbb{F}_q$ whose dimension is equivalent to the number of distinct irreducible factors in the complete factorization of $f(x)$.

Theorem 2.7: The set V is a vector space over $\mathbb{F}_q$ of dimension m.

Proof: To show V is a vector space over $\mathbb{F}_q$, it needs only to be shown that V is a subspace of $\mathbb{F}_q[x]$. Hence, we must show that V is non-empty, closed under addition, and satisfies $tV \subseteq V$ for each $t \in \mathbb{F}_q$. Notice that $0^q \equiv 0 \pmod{f(x)}$. So $0 \in V$, and $V \neq \emptyset$. Let $g(x), h(x) \in V$ and $t \in \mathbb{F}_q$. Then $g(x)^q \equiv g(x) \pmod{f(x)}$ and $h(x)^q \equiv h(x) \pmod{f(x)}$. Now, applying Theorem 1.6 and the Generalized FLT, we get

$$\begin{aligned}
[(g+h)(x)]^q &= [g(x)+h(x)]^q \\
&= g(x)^q + h(x)^q \\
&\equiv g(x) + h(x) \pmod{f(x)} \\
&\equiv (g+h)(x) \pmod{f(x)}
\end{aligned}$$

and

$$\begin{aligned}
[(tg)(x)]^p &= [tg(x)]^q \\
&= t^q \cdot g(x)^q \\
&= tg(x)^q \\
&\equiv tg(x) \pmod{f(x)} \\
&\equiv (tg)(x) \pmod{f(x)}.
\end{aligned}$$

Thus, $(g+h)(x), (tg)(x) \in V$. This shows that V is a subspace of $\mathbb{F}_q[x]$. Let $S = \{(s_1, s_2, \cdots, s_m) : s_i \in \mathbb{F}_q\}$. Now, construct a one-to-one correspondence between V and S as follows.

Let $g(x) \in V$. Then $f(x)$ divides $g(x)^q - g(x) = \prod_{s \in \mathbb{F}_q}(g(x) - s)$. By Proposition 2.6, for each $i = 1, 2, \cdots, m$, there exists a unique $s_i \in \mathbb{F}_q$ with $g(x) \equiv s_i \pmod{f_i(x)^{k_i}}$. To $g(x)$ correspond the unique m-tuple $(s_1, s_2, \cdots, s_m)$. Next, establish the inverse map.

Let $(s_1, s_2, \cdots, s_m) \in S$. Since $f_1(x)^{k_1}, f_2(x)^{k_2}, \cdots, f_m(x)^{k_m}$ are pairwise relatively prime, by the Chinese Remainder Theorem (Theorem 1.23), there is a unique polynomial $g(x) \in \mathbb{F}_q[x]$ of degree $< n$ with $g(x) \equiv s_i \pmod{f_i(x)^{k_i}}$ for

each $i = 1, 2, \cdots, m$. Now, by Proposition 2.6, $f(x)$ divides $\prod_{s \in \mathbb{F}_q}(g(x) - s) = g(x)^q - g(x)$. To $(s_1, s_2, \cdots, s_m) \in S$ correspond the unique element $g(x) \in V$.

Thus, there is a one-to-one correspondence between V and S. Since S is a vector space over $\mathbb{F}_q$ of dimension m, S has q^m elements. Due to the one-to-one correspondence between V and S, it follows that V also has q^m elements.

Suppose now that V has dimension w over $\mathbb{F}_q$. Then V must have q^w elements. So $q^w = q^m$, and hence $w = m$. ■

In the following corollary to Theorem 2.7, we establish that $f(x)$ is the power of a single irreducible if and only if $V = \mathbb{F}_q$.

Corollary 2.8: $f(x)$ is the power of a single irreducible polynomial over $\mathbb{F}_q[x]$ iff the vector space V over $\mathbb{F}_q$ has dimension 1 iff $V = \mathbb{F}_q$.

***Proof*:** By Theorem 2.7, $m = 1$ in the factorization of $f(x)$ if and only if the dimension of V is 1 over $\mathbb{F}_q$.

Now, for the second part of the statement, suppose that V has dimension 1 over $\mathbb{F}_q$. Since $a^q \equiv a \pmod{f(x)}$ for each $a \in \mathbb{F}_q$, any basis for V must contain a unit in $\mathbb{F}_q$. But, the dimension of V over $\mathbb{F}_q$ is 1. So any basis for V contains only a unit in $\mathbb{F}_q$, and hence $V = \mathbb{F}_q$.

For the converse, it is trivial to see that $V = \mathbb{F}_q$ only if V has dimension 1 over $\mathbb{F}_q$. ■

The vector space V gives us information about the number of irreducible factors of $f(x)$. Now, the next theorem gives us a method by which we can actually use a non-constant element of V to obtain a nontrivial factorization of $f(x)$ (in the case that $f(x)$ is divisible by two or more irreducibles).

Theorem 2.9: Let $g(x) \in \mathbb{F}_q[x]$ be a polynomial with $1 \leq \deg(g(x)) < n$ such that $f(x)$ divides $g(x)^q - g(x)$. Then $f(x) = \prod_{s \in \mathbb{F}_q} \gcd(f(x), g(x) - s)$ is a nontrivial factorization of $f(x)$ in $\mathbb{F}_q[x]$.

***Proof*:** Since $f(x)$ divides $g(x)^q - g(x)$, notice that $\gcd(f(x), g(x)^q - g(x)) = f(x)$. Now, because $g(x) - s$ and $g(x) - j$ are relatively prime for $s \neq j$, it follows from Proposition 1.13 that

$$\begin{aligned} f(x) &= \gcd(f(x), g(x)^q - g(x)) \\ &= \gcd(f(x), \prod_{s \in \mathbb{F}_q}(g(x) - s)) = \prod_{s \in \mathbb{F}_q} \gcd(f(x), g(x) - s). \qquad (*) \end{aligned}$$

Since $1 \leq \deg(g(x) - s) < n$, we clearly have that $\gcd(f(x), g(x) - s) \neq f(x)$ for each $s \in \mathbb{F}_q$. Hence, the factorization $(*)$ only involves polynomials of degree $< n = \deg(f(x))$, and so must be a nontrivial factorization of $f(x)$.■

Notice that we can utilize Theorem 2.9 to factor $f(x)$ only if we can find a non-constant polynomial in V. To demonstrate a strategy for doing this, let $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1} \in \mathbb{F}_q[x]$. Recall from Proposition 2.6 that $f(x)$ divides $g(x)^q - g(x) = \prod_{s \in \mathbb{F}_q}(g(x) - s)$ iff

$$0 = R(g(x^q)) - g(x),$$

where $R(g(x^q))$ is the unique remainder of $g(x^q)$ after division by $f(x)$. Now, we explicitly find $R(g(x^q))$. Note that $g(x^q) = b_0 + b_1x^q + b_2x^{2q} + \cdots + b_{n-1}x^{(n-1)q}$. Dividing x^{jq} by $f(x)$ for each $j = 1, 2, \cdots, n-1$, it follows from the Division Algorithm that there are polynomials $q_j(x), r_j(x) \in \mathbb{F}_q[x]$ with

$$x^{jq} = f(x)q_j(x) + r_j(x) \text{ and } \deg(r_j(x)) < n.$$

Thus,

$$\begin{aligned} g(x^q) &= b_0 + b_1[f(x)q_1(x) + r_1(x)] + \cdots + b_{n-1}[f(x)q_{n-1}(x) + r_{n-1}(x)] \\ &= [b_1q_1(x) + \cdots + b_{n-1}q_{n-1}(x)]f(x) + [b_0 + b_1r_1(x) + \cdots + b_{n-1}r_{n-1}(x)]. \end{aligned}$$

Since $\deg[(b_0 + b_1r_1(x) + \cdots b_dr_d(x))] < n$, it also is a consequence of the Division Algorithm that $R(g(x^q)) = b_0 + b_1r_1(x) + \cdots b_{n-1}r_{n-1}(x)$. Thus, $f(x)$ divides $g(x)^q - g(x)$ iff

$$0 = [b_0 + b_1r_1(x) + \cdots + b_{n-1}r_{n-1}(x)] - [b_0 + b_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1}]. \qquad (**)$$

Collecting the coefficients of $1, x, x^2, \cdots, x^{n-1}$ in this equation and setting them equal to 0 produces a homogenous system of n equations in the n unknowns $b_0, b_1, \cdots, b_{n-1}$. Finding values for the coefficients that satisfy the system will produce a polynomial $g(x)$ with degree $< n$ such that $f(x)$ divides $g(x)^q - g(x)$.

This process will be applied in the following example to factor a polynomial over $\mathbb{F}_3$.

Example 2.10: Let $f(x) = x^5 + 2x^2 + 2x + 2 \in \mathbb{F}_3[x]$. We desire to find a non-constant polynomial of the form $g(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4$ such that $f(x)$ divides $g(x)^3 - g(x)$. To accomplish this, we first find the remainder polynomials

$r_j(x)$ by computing $x^{j\cdot 3} (\text{mod } f(x))$ for $j = 1, 2, 3, 4$:

$$x^{1\cdot 3} = x^3 \equiv x^3 \text{ (mod } f(x)),$$

$$\begin{aligned} x^{2\cdot 3} &= x^6 \\ &= f(x) \cdot x + (x^3 + x^2 + x) \\ &\equiv x^3 + x^2 + x \text{ (mod } f(x)), \end{aligned}$$

$$\begin{aligned} x^{3\cdot 3} &= x^9 \\ &= x^6 \cdot x^3 \\ &\equiv (x^3 + x^2 + x)x^3 \text{ (mod } f(x)) \\ &\equiv x^6 + x^5 + x^4 \text{ (mod } f(x)) \\ &\equiv (x^3 + x^2 + x) + (x^2 + x + 1) + x^4 \text{ (mod } f(x)) \\ &\equiv x^4 + x^3 + 2x^2 + 2x + 1 \text{ (mod } f(x)), \end{aligned}$$

$$\begin{aligned} x^{4\cdot 3} &= x^{12} \\ &= x^6 x^6 \\ &= (x^3 + x^2 + x)(x^3 + x^2 + x) \text{ (mod } f(x)) \\ &= x^6 + 2x^5 + 2x^3 + x^2 \text{ (mod } f(x)) \\ &\equiv\ (x^3 + x^2 + x) + (2x^2 + 2x + 2) + 2x^3 + x^2 \text{ (mod } f(x)) \\ &\equiv x^2 + 2 \text{ (mod } f(x)). \end{aligned}$$

Thus, $r_1(x) = x^3, r_2(x) = x^3 + x^2 + x, r_3(x) = x^4 + x^3 + 2x^2 + 2x + 1$, and $r_4(x) = x^2 + 2$. Now, referring to $(**)$, $f(x)$ divides $g(x)^3 - g(x)$ iff

$$\begin{aligned} 0 = {} & b_0 + b_1x^3 + b_2(x^3 + x^2 + x) + b_3(x^4 + x^3 + 2x^2 + 2x + 1) + b_4(x^2 + 2) \\ & - [b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4]. \end{aligned}$$

Next we collect the coefficients of $1, x, x^2, x^3$, and x^4 to get a homogenous system of equations:

$$\begin{aligned} & b_0 - b_0 = 0 \\ & (2b_1 + b_2 + 2b_3)x = 0 \Rightarrow 2b_1 + b_2 + 2b_3 = 0 \\ & (2b_3 + b_4)x^2 = 0 \Rightarrow 2b_3 + b_4 = 0 \\ & (b_1 + b_2)x^3 = 0 \Rightarrow b_1 + b_2 = 0 \\ & (b_3 + 2b_4)x^4 = 0 \Rightarrow b_3 + 2b_4 = 0. \end{aligned}$$

These reduce to $b_1 = 2b_2 = b_3 = b_4$, b_0 free. Select $b_1 = b_3 = b_4 = 1$, $b_2 = 2$, and $b_0 = 0$ to form the polynomial $g(x) = x^4 + x^3 + 2x^2 + x$. Then $f(x)$ necessarily divides $g(x)^3 - g(x)$. Applying the Euclidean Algorithm, it can be found that

$$\begin{aligned}
&\gcd(f(x), g(x)) = 1 \\
&\gcd(f(x), g(x) - 1) = x^2 + 1 \\
&\gcd(f(x), g(x) - 2) = x^3 + 2x + 2.
\end{aligned}$$

And applying Theorem 2.9, we get the nontrivial factorization

$$f(x) = (x^2 + 1)(x^3 + 2x + 2).$$

In fact, since $x^2 + 1$ and $x^3 + 2x + 2$ have no roots in $\mathbb{F}_3$, we can conclude that this is the complete factorization of $f(x)$ into irreducibles.

Example 2.10 suggests the following corollary to Theorem 2.9.

Corollary 2.11: Let $h(x) \in \mathbb{F}_q[x]$ be a reducible polynomial of degree 5 with no factors of degree 1. If $g(x)$ is a polynomial of degree ≥ 1 and < 5 such that $h(x)$ divides $g(x)^q - g(x)$, then $\prod_{s \in \mathbb{F}_q} \gcd(h(x), g(x) - s)$ is the complete factorization of $h(x)$.

***Proof*:** Since $h(x)$ is a reducible polynomial over $\mathbb{F}_q$ of degree 5 and has no factors of degree 1, $h(x)$ must be the product of an irreducible quadratic polynomial and an irreducible cubic polynomial. By Theorem 2.8, $\prod_{s \in \mathbb{F}_q} \gcd(h(x), g(x) - s)$ is a nontrivial factorization of $h(x)$, which implies that at least two terms of this product must be non-constant. But, $h(x)$ is the product of precisely two irreducibles. Thus, $h(x) = \prod_{s \in \mathbb{F}_q} \gcd(h(x), g(x) - s)$ is the complete factorization of $h(x)$.■

Corollary 2.11 is a special case where Theorem 2.9 gives the complete factorization of a polynomial. However, for the general polynomial $f(x) = f_1(x)^{k_1} f_2(x)^{k_2} \cdots f_m(x)^{k_m}$, the nontrivial factorization $f(x) = \prod_{s \in \mathbb{F}_q} \gcd(f(x), g(x) - s)$ is usually not the complete factorization of $f(x)$. In particular, $\prod_{s \in \mathbb{F}_q} \gcd(f(x), g(x) - s)$ is not the complete factorization of $f(x)$ when there is an $s_0 \in \mathbb{F}_q$ such that $g(x) - s_0$ is divisible by $f_i(x)^{k_i} f_j(x)^{k_j}$ for some $i \neq j$. This situation occurs regularly.

For example, consider the product $h(x) = x(x + 1)^2(x^2 + x + 1) \in \mathbb{F}_2[x]$. If $g(x)$ is a non-constant polynomial of degree < 5 such that $h(x) | g(x)^2 - g(x)$, then Theorem 2.9 gives that $x(x+1)^2(x^2+x+1) = \gcd(h(x), g(x)) \cdot \gcd(h(x), g(x) - 1)$.

Now, one of the two gcd's on the right hand side of this equation must be divisible by two of the three factors $x, (x+1)^2$, and x^2+x+1.

So, in order to develop a process by which we can separate the factors $f_1(x)^{k_1}, f_2(x)^{k_2}, \cdots, f_m(x)^{k_m}$, we must account for the strong likelihood that the factorization $\prod_{s\in\mathbb{F}_q} \gcd(f(x), g(x)-s)$ has terms which are divisible by multiple distinct irreducibles. With this in mind, we present the following formulation of Berlekamp's algorithm.

General Factoring Algorithm:
Assume $m > 1$. Let $\{g_0(x), g_1(x), \cdots, g_{m-1}(x)\}$ be a basis for the vector space V with $g_0(x) = 1$. (We are allowed to let $g_0(x) = 1$, since $a^q \equiv a \pmod{f(x)}$ for each $a \in \mathbb{F}_q$.) Note that $g_1(x), \cdots, g_{m-1}(x)$ are non-constant. Now, complete the following steps:
Step 1) Compute $\gcd(f(x), g_1(x)-s)$ for each $s \in \mathbb{F}_q[x]$. Let A_1 be the set containing each of these factors which has degree ≥ 1. If $|A_1| = m$, then stop and output A_1. Otherwise, continue to Step 2.
Step 2) Compute $\gcd(h(x), g_2(x)-s)$ for each $h(x) \in A_1$ and $s \in \mathbb{F}_q$. Let A_2 be the set containing each of these factors which has degree ≥ 1. If $|A_2| = m$, then stop and output A_2. Otherwise, continue to Step 3.
$\vdots$
Step m-2) Compute $\gcd(h(x), g_{m-2}(x)-s)$ for each $h(x) \in A_{m-3}$ and $s \in \mathbb{F}_q$. Let A_{m-2} be the set containing each of these factors which has degree ≥ 1. If $|A_{m-2}| = m$, then stop and output A_{m-2}. Otherwise, continue to Step m-1.
Step m-1) Compute $\gcd(h(x), g_{m-1}(x)-s)$ for each $h(x) \in A_{m-2}$ and $s \in F_q$. Let A_{m-1} be the set containing each of these factors which has degree ≥ 1. Output A_{m-1}.

Theorem 2.12: Suppose the General Factoring Algorithm stops on the j_{th} step. Then the output A_j contains precisely the elements $f_1(x)^{k_1}, f_2(x)^{k_2}, \cdots, f_m(x)^{k_m}$.

***Proof*:** Suppose $j < m-1$. Then, by construction, A_j contains m relatively prime polynomials of degree ≥ 1. Applying Proposition 1.13 and Theorem 2.9, it follows that $f(x)$ must be the product of these m polynomials. Since the factorization of $f(x)$ into powers of distinct irreducibles is unique, it must be that the m polynomials in A_j are precisely $f_1(x)^{k_1}, f_2(x)^{k_2}, \cdots, f_m(x)^{k_m}$.

Now, suppose $j = m-1$. Since the elements of A_j are relatively prime and have a product which equals $f(x)$, $|A_j| \leq m$. Assume, by way of contradiction, that $|A_j| < m$. Then there exists an $h(x) \in A_j$ which is divisible by at least two of the powers of irreducibles that are factors of $f(x)$. Without loss of

generality, say both $f_1(x)^{k_1}$ and $f_2(x)^{k_2}$ divide $h(x)$. Then $f_1(x)^{k_1}$ and $f_2(x)^{k_2}$ must both divide exactly one gcd in each step of the algorithm. Thus, for each $i = 0, 1, 2, \cdots, m-1$, there exists an $s_i \in \mathbb{F}_q$ such that $g_i(x) \equiv s_i \pmod{f_1(x)^{k_1}}$ and $g_i(x) \equiv s_i \pmod{f_2(x)^{k_2}}$. Now, by the Chinese Remainder Theorem (Theorem 1.23), there exists a $g(x) \in V$ (not necessarily unique) with $g(x) \equiv 0 \pmod{f_1(x)^{k_1}}$ and $g(x) \equiv 1 \pmod{f_2(x)^{k_2}}$. Since $\{g_0(x), g_1(x), \cdots, g_{m-1}(x)\}$ forms a basis for V, there exist $c_0, c_1, \cdots, c_{m-1} \in \mathbb{F}_q$ with $g(x) = \sum_{i=0}^{m-1} c_i g_i(x)$. Let $s = \sum_{i=0}^{m-1} c_i s_i \in \mathbb{F}_q$. Then

$$\begin{aligned} s &= \sum_{i=0}^{m-1} c_i s_i \\ &\equiv \sum_{i=0}^{m-1} c_i g_i(x) \pmod{f_1(x)^{k_1}} \\ &\equiv g(x) \pmod{f_1(x)^{k_1}} \\ &\equiv 0 \pmod{f_1(x)^{k_1}}. \end{aligned}$$

This implies $s = 0$. But,

$$\begin{aligned} s &= \sum_{i=0}^{m-1} c_i s_i \\ &\equiv \sum_{i=1}^{m} c_i g_i(x) \pmod{f_2(x)^{k_2}} \\ &\equiv g(x) \pmod{f_2(x)^{k_2}} \\ &\equiv 1 \pmod{f_2(x)^{k_2}}, \end{aligned}$$

which implies $s = 1$, a contradiction. Thus, $|A_j| = m$, and A_j contains precisely the elements $f_1(x)^{k_1}, f_2(x)^{k_2}, \cdots, f_m(x)^{k_m}$. ■

The final thing we need to do before applying the General Factoring Algorithm is describe a process for determining a basis for V. Recall that determining such a basis is necessary to begin the algorithm. Consider again the equation

$$\begin{aligned} R(g(x^q)) - g(x) = &[b_0 + b_1 r_1(x) + \cdots + b_{n-1} r_{n-1}(x)] \\ &- [b_0 + b_1 x + b_2 x^2 + \cdots + b_{n-1} x^{n-1}] \end{aligned}$$

for a polynomial $g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{n-1} x^{n-1} \in \mathbb{F}_q[x]$. Set $r_0(x) = 1$.

For each $j = 0, 1, 2, \cdots, n-1$, let $r_j(x) = r_{0,j} + r_{1,j}x + \cdots + r_{n-1,j}x^{n-1}$. Form the matrices

$$B = \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{bmatrix}, Q = \begin{bmatrix} r_{0,0} & r_{0,1} & \cdots & r_{0,n-1} \\ r_{1,0} & r_{1,1} & \cdots & r_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n-1,0} & r_{n-1,1} & \cdots & r_{n-1,n-1} \end{bmatrix}, \text{ and}$$

$$I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}.$$

Then $g(x) \in V$ iff $R(g(x^q)) - g(x) = 0$ iff $(Q - I)B = 0$. Let

$$V' = \{B : B \text{ is an } n \times 1 \text{ column matrix with entries in } \mathbb{F}_q \text{ and } (Q - I)B = 0\}.$$

Clearly V' is a vector space over $\mathbb{F}_q$, called the *null space* of the matrix $Q - I$, with dimension equivalent to that of V, which was shown in Theorem 2.7 to be m. Since $Q - I$ is an $n \times n$ matrix over the field $\mathbb{F}_q$, we get the following standard relationship between the rank of $Q - I$ and the dimension of V' over $\mathbb{F}_q$:

$$\begin{aligned} n &= \text{rank}(Q - I) + \dim(V') \\ &= \text{rank}(Q - I) + m, \end{aligned}$$

which implies

$$m = n - \text{rank}(Q - I).$$

So, the number of distinct irreducible factors of $f(x)$ can be found by computing the difference between the degree of $f(x)$ and the number of linearly independent rows in the matrix $Q - I$.

Let A be the reduced row echelon form of $Q - I$. The rank of $Q - I$ can be identified by counting the number of non-zero rows in A. Furthermore, a basis for V' is most efficiently found by finding a basis for the vector space $\{B : B \text{ is an } n \times 1 \text{ column matrix with entries in } \mathbb{F}_q \text{ and } AB = 0\}$ over $\mathbb{F}_q$. We note that finding such a basis comes down to finding the free variables in a homogenous system of equations.

Finally, if

$$B_i = \begin{bmatrix} b_{0,i} \\ b_{1,i} \\ \vdots \\ b_{n-1,i} \end{bmatrix}$$

is an element in a basis for V', then $g_i(x) = b_{0,i} + b_{1,i}x + \cdots + b_{n-1,i}x^{n-1}$ is in the corresponding basis for V.

Notice that only one step of the General Factoring Algorithm would have been required to find the complete factorization of the polynomial in Example 2.10. The next example gives a situation in which we require more than one step of the algorithm.

Example 2.13: Let $f(x) = x^9 + 2x^8 + x^7 + x^4 + 2x^3 + 2x^2 + 2x + 1 \in \mathbb{F}_3[x]$. Using polynomial long division to reduce modulo $f(x)$, it is found that

$$\begin{aligned}
x^{1\cdot 3} &= x^3 \\
x^{2\cdot 3} &= x^6 \\
x^{3\cdot 3} &= x^9 \equiv x^8 + 2x^7 + 2x^4 + x^3 + x^2 + x + 2 \pmod{f(x)} \\
x^{4\cdot 3} &= x^{12} \equiv 2x^8 + 2x^5 + 2x^3 + x^2 + 2x + 1 \pmod{f(x)} \\
x^{5\cdot 3} &= x^{15} \equiv x^5 + 2x^3 + x \pmod{f(x)} \\
x^{6\cdot 3} &= x^{18} \equiv x^8 + 2x^6 + x^4 \pmod{f(x)} \\
x^{7\cdot 3} &= x^{21} \equiv x^8 + 2x^7 + 2x^6 + x^3 + 2x^2 + x + 1 \pmod{f(x)} \\
x^{8\cdot 3} &= x^{24} \equiv x^8 + 2x^7 + x^4 + x + 2 \pmod{f(x)}.
\end{aligned}$$

So form the remainder polynomials:

$$\begin{aligned}
r_0(x) &= 1 \\
r_1(x) &= x^3 \\
r_2(x) &= x^6 \\
r_3(x) &= 2 + x + x^2 + x^3 + 2x^4 + 2x^7 + x^8 \\
r_4(x) &= 1 + 2x + x^2 + 2x^3 + 2x^5 + 2x^8 \\
r_5(x) &= x + 2x^3 + x^5 \\
r_6(x) &= x^4 + 2x^6 + x^8 \\
r_7(x) &= 1 + x + 2x^2 + x^3 + 2x^6 + 2x^7 + x^8 \\
r_8(x) &= 2 + x + x^4 + 2x^7 + x^8.
\end{aligned}$$

Now the coefficient of x^j in $r_i(x)$ represents the $j+1, i+1$ entry in the following matrix Q:

$$Q = \begin{bmatrix} 1 & 0 & 0 & 2 & 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 2 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 1 & 2 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 1 & 2 & 0 & 1 & 1 & 1 \end{bmatrix}. \text{ Form } Q-I = \begin{bmatrix} 0 & 0 & 0 & 2 & 1 & 0 & 0 & 1 & 2 \\ 0 & 2 & 0 & 1 & 2 & 1 & 0 & 1 & 1 \\ 0 & 0 & 2 & 1 & 1 & 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 & 2 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 2 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Elementary row operations over $\mathbb{F}_3$ give that the reduced row echelon form of the matrix $Q - I$ is

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Notice that A has rank 5. Thus, the dimension of both V and V' is $9 - 5 = 4$. This tells us that there are exactly four powers of distinct irreducibles in the factorization of $f(x)$. Now, set

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = A \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \\ b_8 \end{bmatrix} = \begin{bmatrix} b_1 + 2b_5 + b_7 \\ b_2 + b_8 \\ b_3 + 2b_7 + b_8 \\ b_4 \\ b_6 + 2b_7 + 2b_8 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

This implies

$$\begin{aligned} b_1 &= b_5 + 2b_7 \\ b_2 &= 2b_8 \\ b_3 &= b_7 + 2b_8 \\ b_4 &= 0 \\ b_6 &= b_7 + b_8. \end{aligned}$$

Thus,

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \\ b_8 \end{bmatrix} = \begin{bmatrix} b_0 \\ b_5 + 2b_7 \\ 2b_8 \\ b_7 + 2b_8 \\ 0 \\ b_5 \\ b_7 + b_8 \\ b_7 \\ b_8 \end{bmatrix} = b_0 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + b_5 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + b_7 \begin{bmatrix} 0 \\ 2 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} + b_8 \begin{bmatrix} 0 \\ 0 \\ 2 \\ 2 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}.$$

It follows that

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 2 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \text{ and } \begin{bmatrix} 0 \\ 0 \\ 2 \\ 2 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

form a basis for V'. Correspondingly, we have that $g_0(x) = 1$, $g_1(x) = x + x^5$, $g_2(x) = 2x + x^3 + x^6 + x^7$, and $g_3(x) = 2x^2 + 2x^3 + x^6 + x^8$ form a basis for V.

Next, we use the Euclidean Algorithm to obtain the necessary gcd's for the first step of the General Factoring Algorithm. These gcd's are:

$$\begin{aligned}
&\gcd\,(f(x), g_1(x)) = x^2 + x + 2,\\
&\gcd\,(f(x), g_1(x) - 1) = x^5 + x + 2,\\
&\gcd\,(f(x), g_1(x) - 2) = x^2 + x + 1.
\end{aligned}$$

Only three of the four needed factors were found in the Step 1, so we proceed to Step 2. The necessary gcd's for this step are:

$$\begin{aligned}
&\gcd\,(x^2 + x + 2, g_2(x)) = 1,\\
&\gcd\,(x^2 + x + 2, g_2(x) - 1) = 1,\\
&\gcd\,(x^2 + x + 2, g_2(x) - 2) = x^2 + x + 2;
\end{aligned}$$

$$\begin{aligned}
&\gcd\,(x^5 + x + 2, g_2(x)) = x^5 + x + 2,\\
&\gcd\,(x^5 + x + 2, g_2(x) - 1) = 1,\\
&\gcd\,(x^5 + x + 2, g_2(x) - 2) = 1;
\end{aligned}$$

$$\begin{aligned}
&\gcd\,(x^2 + x + 1, g_2(x)) = 1,\\
&\gcd\,(x^2 + x + 1, g_2(x) - 1) = 1,\\
&\gcd\,(x^2 + x + 1, g_2(x) - 2) = x^2 + x + 1.
\end{aligned}$$

Step 2 only produced three factors as well, so we proceed to compute the necessary gcd's for the third step (which is the final possible step).

$$\begin{aligned}
&\gcd\,(x^2 + x + 2, g_3(x)) = x^2 + x + 2,\\
&\gcd\,(x^2 + x + 2, g_3(x) - 1) = 1,\\
&\gcd\,(x^2 + x + 2, g_3(x) - 2) = 1;
\end{aligned}$$

$$\begin{aligned}
&\gcd\,(x^5 + x + 2, g_3(x)) = 1,\\
&\gcd\,(x^5 + x + 2, g_3(x) - 1) = x^3 + x^2 + 2,\\
&\gcd\,(x^5 + x + 2, g_3(x) - 2) = x^2 + 2x + 1;
\end{aligned}$$

$$\begin{aligned}
&\gcd\,(x^2 + x + 1, g_3(x)) = x^2 + x + 1,\\
&\gcd\,(x^2 + x + 1, g_3(x) - 1) = 1,\\
&\gcd\,(x^2 + x + 1, g_3(x) - 2) = 1.
\end{aligned}$$

Now, by Theorem 2.12, $x^2+x+2, x^3+x^2+2, x^2+2x+1$, and x^2+x+1 are pairwise relatively prime and multiply to give $f(x)$. Further, each of these four factors can be written as the power of a single irreducible. Using the method given in Section 2.1 for factoring such polynomials, we find: x^2+x+2 and x^3+x^2+2 are both irreducible, $x^2+2x+1=(x+1)^2$, and $x^2+x+1=(x+2)^2$. Thus,

$$f(x)=(x^2+x+2)(x^3+x^2+2)(x+1)^2(x+2)^2$$

is the complete factorization of $f(x)$.

After this lengthy example, we must pose the question: Is the General Factoring Algorithm alone our best factoring tool thus far? The answer is clearly no! Practically speaking, it is strongly recommended that any polynomial undergo SFF in the first step of the factoring process. Then, if necessary, the separate square-free parts of the polynomial can be reduced using the algorithm of this section. There are many reasons for this recommendation. First, notice that implementing SFF allows us to avoid inserting polynomials into the General Factoring Algorithm which are divisible by high powers of irreducibles. Also, the algorithm works very nicely with square-free polynomials - it has the ability to directly separate all of the irreducibles of such polynomials.

Consider how implementing SFF speeds up the factoring process for the polynomial in Example 2.13. SFF gives

$$\begin{aligned} f(x) &= x^9+2x^8+x^7+x^4+2x^3+2x^2+2x+1 \\ &= (x^5+2x^4+x^2+2x+1)(x^2+2)^2 \end{aligned}$$

over $\mathbb{F}_3$. Using Corollary 2.11, we find $x^5+2x^4+x^2+2x+1=(x^2+x+2)(x^3+x^2+2)$. Searching for roots of x^2+2 in $\mathbb{F}_3$, we also see that $x^2+2=(x+1)(x+2)$. Thus,

$$f(x)=(x^2+x+2)(x^3+x^2+2)(x+1)^2(x+2)^2.$$

The process of factorization described here is a much quicker process than the application of the General Factoring Algorithm in Example 2.13.

Even though applying SFF is the recommended first step in factoring, the formulation of Berelekamp's algorithm in this section is of great theoretical interest. It has the ability to separate *any* polynomial over $\mathbb{F}_q$ into powers of distinct irreducibles. This is stronger than formulations of the algorithm which only accept square-free polynomials.

Chapter 3

The Cantor-Zassenhaus Method

The next factoring scheme we will develop is due to Cantor and Zassenhaus[2] and has two stages:

1. **Distinct Degree Factorization (DDF):** The input polynomial is decomposed into factors so that each factor can be expressed as the product of distinct irreducibles that all have the same degree (and this degree is found).

2. **Equal Degree Factorization (EDF):** Each of the "equal degree" factors produced in the DDF stage is completely factored.

The algorithm we give for DDF is deterministic, while the algorithm we give for EDF is probabilistic. Combined, the two algorithms will provide us with another method by which we can completely factor an arbitrary polynomial over $\mathbb{F}_q$, where $q = p^v$ with p a prime number and v a positive integer.

3.1 Distinct Degree Factorization

To begin this section, let $f(x)$ be a monic polynomial over $\mathbb{F}_q$ of degree ≥ 1. Formally, in order to find a distinct degree factorization of $f(x)$, we need a list of pairs

$$(g_1(x), n_1), (g_2(x), n_2), \cdots, (g_k(x), n_k)$$

such that $f(x) = g_1(x)g_2(x)\cdots g_k(x)$ and each $g_i(x)$ is the product of $\dfrac{\deg[g_i(x)]}{n_i}$ distinct irreducibles that all have degree n_i. Notice, in particular, that the degrees n_i are not necessarily pairwise distinct. In fact, if $f(x)$ is not square-free, then it will be the case that $n_i = n_j$ for some $i \neq j$.

To develop an algorithm for DDF, we start with the following proposition.

Proposition 3.1: Let r be a positive integer and $h(x)$ a monic irreducible polynomial over $\mathbb{F}_q$ of degree n. Then $h(x)$ divides $x^{q^r} - x$ in $\mathbb{F}_q[x]$ if and only if $n|r$.

***Proof*:** Suppose $h(x)$ divides $x^{q^r} - x$ in $\mathbb{F}_q[x]$. Note that $\mathbb{F}_{q^r}$ is the splitting field for $x^{q^r} - x$, and each of the q^r distinct elements of $\mathbb{F}_{q^r}$ is a root of $x^{q^r} - x$. So, we have that $x^{q^r} - x = \prod_{a \in \mathbb{F}_{q^r}} (x - a)$. Now, since $h(x)$ divides $\prod_{a \in \mathbb{F}_{q^r}} (x - a)$ in $\mathbb{F}_{q^r}[x]$ and is of degree ≥ 1, there must exist an $a' \in \mathbb{F}_{q^r}$ such that a' is a root of $h(x)$. Consider $\mathbb{F}_q(a')$, the smallest subfield of $\mathbb{F}_{q^r}$ containing $\mathbb{F}_q$ and the element a'. Since $h(x)$ is irreducible over $\mathbb{F}_q$, it follows from Theorems 1.29 and 1.31 that $\mathbb{F}_q(a') \cong \mathbb{F}_q[x]/(h(x)) \cong \mathbb{F}_{q^n}$. This shows that $\mathbb{F}_q(a')$ is a field extension of $\mathbb{F}_q$, and $[\mathbb{F}_{q^r}(a') : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. Thus, by Theorem 1.27,

$$\begin{aligned} r &= [\mathbb{F}_{q^r} : \mathbb{F}_q] \\ &= [\mathbb{F}_{q^r} : \mathbb{F}_q(a')] \cdot [\mathbb{F}_q(a') : \mathbb{F}_q] \\ &= [\mathbb{F}_{q^r} : \mathbb{F}_q(a')] \cdot n, \end{aligned}$$

and $n|r$.

Now, suppose that $n|r$. Let $\theta = x \pmod{h(x)} \in \mathbb{F}_q[x]/(h(x)) \cong \mathbb{F}_{q^n}$. Note that θ is a root of $x^{q^n} - x$. So, it follows from Proposition 1.34 that $x^{q^n} - x$ is divisible by the minimal polynomial for θ over $\mathbb{F}_q$, which is $h(x)$. Since $n|r$, $r = nj$ for some $j \in \mathbb{Z}$, and hence

$$q^r - 1 = q^{nj-1} = (q^n - 1)(q^{n(j-1)} + q^{n(j-2)} + \cdots + 1).$$

So $q^n - 1 | q^r - 1$ in $\mathbb{Z}$, and an identical argument shows that $x^{q^n-1} - 1 | x^{q^r-1} - 1$ in $\mathbb{F}_q[x]$. Thus, $x^{q^n} - x = x(x^{q^n-1} - 1)$ divides $x^{q^r} - x = x(x^{q^r-1} - 1)$. Since $h(x)|x^{q^n} - x$, it now follows that $h(x)|x^{q^r} - x$ in $\mathbb{F}_q[x]$. ■

From this proposition follows a very important theorem, which we will use to generate our DDF algorithm.

Theorem 3.2: For $n \geq 1$, let h_n denote the product of all distinct monic irreducibles in $\mathbb{F}_q[x]$ of degree n. Then for all positive integers r,

$$x^{q^r} - x = \prod_{n|r} h_n,$$

where the product is over all positive divisors of r.

***Proof*:** By Proposition 3.1, every monic irreducible polynomial over $\mathbb{F}_q$ of degree n with $n|r$ divides $x^{q^r}-x$. So $\prod_{n|r} h_n | x^{q^r}-x$. Furthermore, each monic irreducible polynomial in $\mathbb{F}_q[x]$ that divides $x^{q^r}-x$ must have degree n such that $n|r$. So, $x^{q^r}-x$ is the product of monic irreducibles whose degree divides r, and all such polynomials appear at least once in this product. Now, we compute the derivative

$$\begin{aligned}\frac{d}{dx}(x^{q^r}-x) &= q^r x^{q^r-1} - 1 \\ &= 0 - 1 \in \mathbb{F}_q[x] \\ &= -1.\end{aligned}$$

So $\gcd(x^{q^r}-x, \frac{d}{dx}(x^{q^r}-1)) = 1$, which shows that no irreducible polynomial appears more than once in the complete factorization of $x^{q^r}-x$. This means the complete factorization of $x^{q^r}-x$ consists of one copy of each of the disinct monic irreducibles over $\mathbb{F}_q$ whose degree divides r. Hence, $x^{q^r}-x = \prod_{n|r} h_n$. ■

Utilizing Theorem 3.2, we can now develop a process for finding a distinct degree factorization of $f(x)$. First, note that $x^q - x$ is the product of all distinct linear monic polynomials over $\mathbb{F}_q$. So we can compute $g(x) = \gcd(x^q - x, f(x)) = \gcd(x^q - x (\text{mod } f(x)), f(x))$ to get the product of all distinct linear factors of $f(x)$. We then remove the factor $g(x)$ from $f(x)$ to obtain a new $f(x)$. But, if the original polynomial was not square-free, $f(x)$ may still have some linear factors, and so we have to repeat the step with $x^q - x$ until we get a gcd of 1 and hence $f(x)$ has no more linear factors. Once all linear factors have been removed, we compute $\gcd(x^{q^2} - x, f(x))$, which is the product of all distinct quadratic irreducible factors of $f(x)$. Note that even though $x^{q^2} - x$ is the product of all distinct linear and quadratic monic irreducibles over $\mathbb{F}_q$, since we removed all linear factors from $f(x)$ beforehand, we know $\gcd(x^{q^2} - x, f(x))$ will only give us the product of the distinct quadratic irreducibles that divide $f(x)$. Like before, it may be necessary to repeat the step with $x^{q^2} - x$ multiple times to remove all quadratic factors from $f(x)$. In general, the strategy of our DDF algorithm will be this:

Starting with $k = 1$, once all factors of degree less than k have been removed from $f(x)$, we compute $\gcd(x^{q^k} - x, f(x))$ to get the product of all distinct degree k monic irreducible factors of $f(x)$. Following this, we may need to compute multiple gcd's with $x^{q^k} - x$ in order to remove all factors of degree k from $f(x)$. This process will be completed until no more factors can be removed from $f(x)$, which will occur when our redefined value for $f(x)$ is 1. We now give the algorithm.

DDF Algorithm over $\mathbb{F}_q$:
The input is a monic polynomial $f \in \mathbb{F}_q[x]$.

$r \leftarrow 1$
while $f \neq 1$ **do**
  $h \leftarrow x^{q^r} - x \pmod{f}$
  $g \leftarrow \gcd(h, f)$
  while $g \neq 1$ **do**
    output (g, r)
    $f \leftarrow f/g$
    $g \leftarrow \gcd(h, f)$
  end while
$r \leftarrow r + 1$
end while

The polynomials g in the outputs (g, r) in the DDF algorithm clearly multiply to give the input polynomial f. Further, each pair (g, r) represents a polynomial g which is the product of $\deg(g)/r$ distinct irreducibles of degree r.

Notice that the the degrees of the polynomials $x^{q^r} - x$ blow up very quickly. So, repeatedly computing $x^{q^r} - x(\text{mod } f) = x^{q^r}(\text{mod} f) - x(\text{mod} f)$ is one of the more difficult aspects of applying the algorithm. In view of this, we present a fairly intuitive binary exponentiation algorithm for computing $x^M(\text{mod} f)$.

Binary Exponentiation Algorithm for Computing $x^M(\text{mod} f)$:
Let $M = b_n \cdot 2^n + b_{n-1} \cdot 2^{n-1} + \cdots + b_1 \cdot 2 + b_0$ be the binary representation for M (where $b_j = 0$ or 1).

$g \leftarrow x$
$j \leftarrow n - 1$
while $j \geq 0$ **do**
  $g \leftarrow g^2 \pmod{f}$
  if $b_j = 1$, then
    $g \leftarrow g \cdot x \pmod{\text{f}}$
  end if
  $j \leftarrow j - 1$
end while
output g

We are now ready to apply the DDF algorithm.

Example 3.3: We find the DDF of the polynomial

$$f(x) = x^{11} + 2x^6 + 2x^4 + 2x^3 + x^2 + 1$$

over $\mathbb{F}_3$.

First, we use the Euclidean Algorithm to compute that

$$\gcd(x^{3^1} - x, f(x)) = x^2 + 2.$$

This gives the pair $(x^2 + 2, 1)$. Now, compute

$$f(x)/(x^2 + 2) = x^9 + x^7 + x^5 + 2x^4 + x^3 + x^2 + 2.$$

We must test this new polynomial for linear factors:

$$\gcd(x^3 - x, x^9 + x^7 + x^5 + 2x^4 + x^3 + x^2 + 2) = x + 2.$$

This gives the pair $(x + 2, 1)$, and we get that

$$(x^9 + x^7 + x^5 + 2x^4 + x^3 + x^2 + 2)/(x + 2) = x^8 + x^7 + 2x^6 + 2x^5 + 2x^3 + x + 1.$$

Testing again for linear factors:

$$\gcd(x^3 - x, x^8 + x^7 + 2x^6 + 2x^5 + 2x^3 + x + 1) = 1.$$

This shows that we have removed all of the linear factors from $f(x)$. Polynomial long division easily gives that

$$\begin{aligned} &x^{3^2} - x = x^9 - x \\ &\equiv 2x^7 + 2x^5 + x^4 + 2x^3 + 2x^2 + 2x + 1 \pmod{x^8 + x^7 + 2x^6 + 2x^5 + 2x^3 + x + 1}, \end{aligned}$$

and we use this congruence to compute the product of the distinct quadratic factors of $f(x)$:

$$\begin{aligned} &\gcd(2x^7 + 2x^5 + x^4 + 2x^3 + 2x^2 + 2x + 1, x^8 + x^7 + 2x^6 + 2x^5 + 2x^3 + x + 1) \\ &= x^2 + 1. \end{aligned}$$

This gives the pair $(x^2 + 1, 2)$. Now, compute

$$(x^8 + x^7 + 2x^6 + 2x^5 + 2x^3 + x + 1)/(x^2 + 1) = x^6 + x^5 + x^4 + x^3 + 2x^2 + x + 1.$$

Before testing again for quadratic factors, notice that

$$\begin{aligned} &x^{3^2} - x = x^9 - x \\ &\equiv 2x^7 + 2x^5 + x^4 + 2x^3 + 2x^2 + 2x + 1 \pmod{x^6 + x^5 + x^4 + x^3 + 2x^2 + x + 1} \\ &\equiv 2x^5 + x^4 + x^2 + 2x \pmod{x^6 + x^5 + x^4 + x^3 + 2x^2 + x + 1}. \end{aligned}$$

Now,

$$\gcd(2x^5 + x^4 + x^2 + 2x, x^6 + x^5 + x^4 + x^3 + 2x^2 + x + 1) = 1.$$

Hence, all of the quadratic factors have been removed from $f(x)$. Next, we let

$$p(x) = x^6 + x^5 + x^4 + x^3 + 2x^2 + x + 1$$

and use binary exponentiation to compute $x^{3^3} \pmod{p(x)}$.

Notice that $3^3 = 27 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$.

Step 1: Since 2^3 has a coefficient of 1, compute $g = x^2$, and then $g = x^2 \cdot x = x^3$.

Step 2: Since 2^2 has a coefficient of 0, compute
$g = (x^3)^2 = x^6 \equiv 2x^5 + 2x^4 + 2x^3 + x^2 + 2x + 2 \pmod{p(x)}$.

Step 3: Since 2^1 has a coefficient of 1, compute
$g = (2x^5 + 2x^4 + 2x^3 + x^2 + 2x + 2)^2 \equiv x^5 + x^4 + x^3 + x^2 + 2x + 1 \pmod{p(x)}$, and then $g = (x^5 + x^4 + x^3 + x^2 + 2x + 1) \cdot x \equiv 2 \pmod{p(x)}$.

Step 4: Since 2^0 has a coefficient of 1, compute $g = 2^2 = 1 \in \mathbb{F}_3$, and then $g = 1 \cdot x = x$.

Thus, $x^{3^3} \equiv x \pmod{p(x)}$, and so $x^{3^3} - x \equiv 0 \pmod{p(x)}$.

Clearly, $\gcd(0, p(x)) = p(x)$, which gives the pair $(p(x), 3)$. Now, $p(x)/p(x) = 1$, and the algorithm terminates.

In summary, $f(x) = (x^2 + 2)(x + 2)(x^2 + 1)(x^6 + x^5 + x^4 + x^3 + 2x^2 + x + 1)$, and these four factors are products of distinct irreducibles of degrees $1, 1, 2$, and 3, respectively. In particular, the middle two factors are themselves irreducible.

Observe that in Example 3.3, the input polynomial was not square-free since it had $x + 2$ as a repeated linear factor. This repeated linear factor forced us to compute an extra gcd when applying the DDF algorithm, giving us a total of three gcd computations before all linear factors were removed from the input polynomial.

For the general polynomial $f(x)$, suppose $g(x)^k$ is a factor of $f(x)$, where $g(x)$ is an irreducible polynomial over $\mathbb{F}_q$ of degree r, and k is the largest power on any irreducible factor of $f(x)$ with degree r. In order to remove all irreducible factors of degree r from $f(x)$ using the algorithm, we would have to compute exactly $k + 1$ gcd's with $x^{q^r} - x$. The first k of these gcd computations would actually remove all the factors of degree r, and the final gcd computation (of 1) would verify that there are no factors of degree r left. It is quite obvious that as k grows large, this process becomes extremely time consuming. The tediousness here is most likely why Cantor and Zassenhaus formulate a DDF method which only accepts square-free polynomials. As a general rule, we also suggest that a polynomial undergo SFF before being separated with our algorithm. When it is known up front that the input polynomial is square free, it is never necessary to compute gcd's in the second **while** loop of the algorithm. Hence, in such a case, we need only compute one gcd in each new degree iteration of the DDF process.

In the next section, we delve into the second stage of the Cantor-Zassenhaus factoring scheme, Equal Degree Factorization.

3.2 Equal Degree Factorization

Recall again that the an output (g, r) in the DDF algorithm represents a polynomial g which can be written as the product of distinct monic irreducibles that all have the same (known) degree, namely r. So, if we can develop an algorithm that separates the irreducible factors of such an "equal degree" polynomial, we will have generated a complete factoring process over $\mathbb{F}_q$.

Throughout this stage, let $f(x) \in \mathbb{F}_q[x]$ be a monic polynomial of degree n that is the product of $s > 1$ distinct monic irreducibles $f_i(x)$, $1 \leq i \leq s$, with $\deg(f_i(x)) = d$ for each i. Notice, in particular, that $n = sd$. Working under the assumption that d is known, our goal for the section is to use the fact that each irreducible factor of $f(x)$ has degree d to develop a method for factoring $f(x)$.

Note that a factor $p(x)$ of $f(x)$ with $0 < \deg(p(x)) < n$ will be referred to as a *proper factor* of $f(x)$. In seeking a strategy for finding proper factors of $f(x)$, we start with the following intuitive proposition (which is not dependent on the fact that the irreducible factors of $f(x)$ all have the same degree).

Proposition 3.4: Let $g(x)$ be a non-constant polynomial over $\mathbb{F}_q$ with $\deg(g(x)) < n$. If $g(x) \equiv 0 \pmod{f_{i_0}(x)}$ for some $i_0 \in \{1, \cdots, s\}$, then $\gcd(f(x), g(x))$ is a proper factor of $f(x)$.

***Proof*:** Since $g(x)$ is non-constant and $\deg(g(x)) < n$, $g(x) \not\equiv 0 \pmod{f(x)}$. Hence, $\gcd(f(x), g(x)) \neq f(x)$. Also, since $g(x) \equiv 0 \pmod{f_{i_0}(x)}$, $f_{i_0}(x)$ is a common factor of $g(x)$ and $f(x)$. So, $\gcd(f(x), g(x))$ is some multiple of $f_{i_0}(x)$, which means $\gcd(f(x), g(x)) \neq 1$. Thus, $\gcd(f(x), g(x))$ is a proper factor of $f(x)$. ■

If we can find a polynomial $g(x)$ that satisfies the conditions of Proposition 3.4, we will obtain a nontrivial factorization of $f(x)$. We first restrict ourselves to the case that $p > 2$, so that $q = p^v$ is odd. With this restriction in place, set $c = \frac{q^d-1}{2}$. Notice that the definition of c brings into play the fact that all irreducible factors of $f(x)$ have degree d. Now the next theorem will provide us with a way to efficiently generate polynomials that satisfy the hypotheses of Proposition 3.4.

Theorem 3.5: Let $h(x) \in \mathbb{F}_q[x]$ be a polynomial with $\gcd(f(x), h(x)) = 1$. Let $g(x) = h(x)^c - 1 (\text{mod } f(x))$. If $h(x)^c \not\equiv \pm 1 \pmod{f(x)}$, then $\gcd(f(x), g(x))$ is a proper factor of $f(x)$.

***Proof*:** Since $\gcd(f(x), h(x)) = 1$, $h(x) \not\equiv 0 \pmod{f_i(x)}$ for each $i \in \{1, \cdots, s\}$. Now, for each i, $\mathbb{F}_q[x]/(f_i(x))$ is a field with q^d elements, and so by the Generalized FLT,

$$(h(x)^c)^2 = h(x)^{q^d-1} \equiv 1 \pmod{f_i(x)},$$

which gives

$$(h(x)^c - 1)(h(x)^c + 1) \equiv 0 \pmod{f_i(x)}.$$

Because $\mathbb{F}_q[x]/(f_i(x))$ has no zero divisors, it follows that $h(x)^c \equiv 1 \pmod{f_i(x)}$ or $h(x)^c \equiv -1 \pmod{f_i(x)}$.

Observe that since $h(x)^c \not\equiv \pm 1 \pmod{f(x)}$, $h(x)^c$ is clearly non-constant over $\mathbb{F}_q$. In turn, $g(x)$ is also non-constant. Furthermore, since $h(x)^c \not\equiv -1 \pmod{f(x)}$, there exists an $i_0 \in \{1, \cdots, s\}$ with $h(x)^c \not\equiv -1 \pmod{f_{i_0}(x)}$. Then it must be that $h(x)^c \equiv 1 \pmod{f_{i_0}(x)}$, which means $g(x) \equiv 0 \pmod{f_{i_0}(x)}$. Hence, by Proposition 3.4, $\gcd(f(x), g(x))$ is a proper factor of $f(x)$. ■

In hopes of utilizing Theorem 3.5 to factor $f(x)$, we randomly select a polynomial $h(x)$ from the $q^n - q$ non-constant polynomials in $\mathbb{F}_q[x]$ of degree $< n$. We now will calculate the probability that $h(x)$ cannot be used with the tools that we have to find a proper factor of $f(x)$. Notice that if $\gcd(f(x), h(x)) \neq 1$, then we automatically get a proper factor of $f(x)$. Furthermore, if $\gcd(f(x), h(x)) = 1$ with $h(x)^c \not\equiv \pm 1 \pmod{f(x)}$, then we can use Theorem 3.5 to get a proper factor. It follows that $h(x)$ cannot be used to get a proper factor of $f(x)$ only if $h(x)^c \equiv \pm 1 \pmod{f(x)}$. Now, by the results of Cantor and Zassenhaus[2], for each $i \in \{1, \cdots, s\}$, there are c polynomials $p_i(x)$, of degree $< d$, such that $p_i(x)^c \equiv 1 \pmod{f_i(x)}$, and c such that $p_i(x)^c \equiv -1 \pmod{f_i(x)}$. This means there are $2c^s$ polynomials $p(x)$ of degree $< n$ in $\mathbb{F}_q[x]$ satisfying $p(x)^c \equiv \pm 1 \pmod{f(x)}$, $q - 1$ of which are constant. Since $h(x)$ was chosen to be non-constant, it follows that the probability that $h(x)^c \equiv \pm 1 \pmod{f(x)}$ is

$$\begin{aligned}
\frac{2c^s - (q-1)}{q^n - q} &= \frac{2\left(\frac{q^d-1}{2}\right)^s - (q-1)}{q^n - q} \\
&= \frac{1}{2^{s-1}} \cdot \frac{(q^d-1)^s - 2^{s-1}(q-1)}{q^n - q} \\
&< \frac{1}{2^{s-1}} \cdot \frac{q^{ds} - 2(q-1)}{q^n - q} \\
&= \frac{1}{2^{s-1}} \cdot \frac{q^n - 2(q-1)}{q^n - q} \\
&< \frac{1}{2^{s-1}} \\
&\leq \frac{1}{2}.
\end{aligned}$$

Correspondingly, the probability that we can use $h(x)$ to obtain a proper factor of $f(x)$ is $> 1 - \frac{1}{2^{s-1}}$. Notice that as the number of factors, s, of $f(x)$ grows large, the probability that $h(x)$ can be used to get a non-trivial factorization of $f(x)$ approaches 1.

Suppose now that we can use $h(x)$ along with Theorem 3.5 to get the proper factor $\gcd(f(x), h(x)^c - 1)$ of $f(x)$. Then we observe that $\gcd(f(x), h(x)^c - 1)$ and $f(x)/\gcd(f(x), h(x)^c - 1)$ are polynomials with irreducible factors that all have equal degree, namely d. So we can apply Theorem 3.5 again in conjunction with randomly selected polynomials to find proper factors of $\gcd(f(x), h(x)^c - 1)$ and $f(x)/\gcd(f(x), h(x)^c - 1)$, and hence come one step closer to finding all the irreducible factors of $f(x)$. Continuing this process iteratively suggests a full algorithm for EDF. In view of the fact that proceeding at random gives us a high probability of further separating the input polynomial $f(x)$ at each stage, the upcoming EDF algorithm is a highly efficient factoring tool.

EDF Algorithm over $\mathbb{F}_q$ with q odd:

$A \leftarrow \{f\}$
while $|A| < s$ **do**
for each $p \in A$ with $\deg(p) > d$ **do**
choose $h \in \mathbb{F}_q[x]$ with $0 < \deg(h) < \deg(p)$ at random
$g \leftarrow \gcd(p, h)$
if $g = 1$, then
$g \leftarrow h^c - 1 \pmod{p}$
end if
if $\gcd(p, g) \neq 1$ and $\gcd(p, g) \neq p$
$A \leftarrow (A - \{p\}) \cup \{\gcd(p, g), p/\gcd(p, g)\}$
end if
end while
output A

Notice that the algorithm runs until $|A| = s$. Hence, the algorithm runs until all s of the equal degree irreducible factors of f have been obtained. We apply EDF in the upcoming example.

Example 3.6: Given that $f(x) = x^6+4x^3+3x^2+2x+1 \in \mathbb{F}_5[x]$ can be written as the product of distinct irreducible polynomials of degree 2, we find the complete factorization of $f(x)$.

In this scenario, the number of irreducible factors of $f(x)$ is $s = 6/2 = 3$. Since each of these factors has degree $d = 2$, set $c = \frac{5^2-1}{2} = 12$. Note that there is a $> \frac{3}{4}$ probability that a randomly chosen non-constant polynomial over $\mathbb{F}_5$ with degree < 6 will yield a non-trivial factorization of $f(x)$. We randomly choose $x^3 + 2 \in \mathbb{F}_5[x]$. The Euclidean Algorithm can be applied to find that

$$\gcd(f(x), x^3 + 2) = 1.$$

Next, using binary exponentiation, we compute

$$(x^3 + 2)^{12} - 1 \equiv 3x^5 + 4x^3 + 3x^2 + 4 \pmod{f(x)}.$$

And we find that

$$\gcd(f(x), 3x^5 + 4x^3 + 3x^2 + 4) = x^4 + 4x^3 + 4x^2 + 2x + 3.$$

Now,

$$f(x)/(x^4 + 4x^3 + 4x^2 + 2x + 3) = x^2 + x + 2,$$

and so

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

Continuing with the algorithm, we factor the polynomial $p(x) = x^4 + 4x^3 + 4x^2 + 2x + 3$. Note that there is a $> \frac{1}{2}$ chance that a randomly chosen non-constant polynomial over $\mathbb{F}_5$ with degree < 4 will yield a non-trivial factorization of $p(x)$. We randomly select $x + 2 \in \mathbb{F}_5[x]$ and find that

$$\gcd(p(x), x + 2) = 1.$$

Then we compute the following congruence:

$$(x + 2)^{12} - 1 \equiv 3 \pmod{p(x)}.$$

(How is the congruence to 3 in the last line consistent with our previous results? Well, we know that for a polynomial $h(x)$ that is nonzero mod $p(x)$, $h(x)^{12}$ is congruent to a constant mod $p(x)$ if and only if $h(x)^{12} \equiv \pm 1 \pmod{p(x)}$ if and only if $h(x) - 1 \equiv 0 \pmod{p(x)}$ or $h(x) - 1 \equiv -2 \pmod{p(x)}$. Now $-2 = 3 \in \mathbb{F}_5$.) So it follows that

$$\gcd(p(x), 3) = 1,$$

and we must randomly choose another polynomial. We choose $x^3 + 2x^2 + 4 \in \mathbb{F}_5$, and compute

$$\gcd(p(x), x^3 + 2x^2 + 4) = 1.$$

Now,

$$(x^3 + 2x^2 + 4)^{12} - 1 \equiv x^3 + 2x^2 + 3x + 1 \pmod{p(x)}$$

and

$$\gcd(p(x), x^3 + 2x^2 + 3x + 1) = x^2 + 3.$$

Dividing we get

$$p(x)/(x^2+3) = x^2 + 4x + 1.$$

Thus,

$$f(x) = (x^2+3)(x^2+4x+1)(x^2+x+2)$$

is the complete factorization of $f(x)$ over $\mathbb{F}_5$.

Next we describe Cantor and Zassenhaus' original strategy for factoring the polynomial $f(x)$ defined at the beginning of this section in the case that $p = 2$, and hence $q = p^v$ is even.

First we treat the subcase that $q \equiv 1 \pmod 3$. We will demonstrate a strategy for finding a proper factor of $f(x)$. Recall from Proposition 1.42 that $(\mathbb{F}_q)^\times$ is a cyclic group under multiplication with $q-1$ elements. Now, since 3 divides $q-1$, it is a consequence of the fact that $(\mathbb{F}_q)^\times$ is cyclic that there exists an element $\rho \in (\mathbb{F}_q)^\times$ of (multiplicative) order 3. Note that to proceed, the element ρ must be known. Observe also that for each $i \in \{1, \cdots, s\}$, ρ is an element of order 3 in the cyclic group $(\mathbb{F}_q[x]/(f_i(x)))^\times$. So, $\{1, \rho, \rho^2\}$ is the unique subgroup of $(\mathbb{F}_q[x]/(f_i(x)))^\times$ of order 3 and hence contains all elements $p(x) (\text{mod } f_i(x)) \in \mathbb{F}_q[x]$ satisfying $p(x)^3 \equiv 1 \pmod{f_i(x)}$.

Set $c = \frac{q^d-1}{3}$ and suppose $h(x)$ is a non-constant polynomial over $\mathbb{F}_q$ satisfying $\gcd(f(x), h(x)) = 1$ and $h(x)^c \notin \{1, \rho, \rho^2\} \pmod{f(x)}$. Since $\gcd(f(x), h(x)) = 1$, $h(x) \not\equiv 0 \pmod{f_i(x)}$ for each i, and so

$$(h(x)^c)^3 = h(x)^{q^d-1} \equiv 1 \pmod{f_i(x)}.$$

Thus, $h(x)^c \in \{1, \rho, \rho^2\} \pmod{f_i(x)}$ for each i.

Let $g_1(x) = h(x)^c - 1 (\text{mod } f(x))$ and $g_2(x) = h(x)^c - \rho (\text{mod } f(x))$. Since $h(x)^c \notin \{1, \rho, \rho^2\} \pmod{f(x)}$, clearly $h(x)^c$ is non-constant over $\mathbb{F}_q$. Then g_1 and g_2 are also non-constant. Moreover, since $h(x)^c \not\equiv \rho^2 \pmod{f(x)}$, there exists an $i_0 \in \{1, \cdots, s\}$ with either $h(x)^c \equiv 1 \pmod{f_{i_0}(x)}$ or $h(x)^c \equiv \rho \pmod{f_{i_0}(x)}$. Correspondingly, either $g_1(x) \equiv 0 \pmod{f_{i_0}(x)}$ or $g_2(x) \equiv 0 \pmod{f_{i_0}(x)}$. Hence, by Proposition 3.4, either $\gcd(f(x), g_1(x))$ or $\gcd(f(x), g_2(x))$ is a proper factor of $f(x)$.

We now give an upper bound for the probability that a polynomial $h(x)$ randomly chosen from the $q^n - q$ non-constant polynomials of degree $< n$ in $\mathbb{F}_q[x]$ cannot be used in conjunction with the strategy given above to yield a proper factor of $f(x)$. To accomplish this, we need only calculate the probability that

$h(x)^c \in \{1, \rho, \rho^2\} \pmod{f(x)}$. By the results of Cantor and Zassenhaus[2], for each $j = 0, 1, 2$, there exist c polynomials $p_i(x)$, of degree $< d$, which satisfy $p_i(x)^c \equiv p^j \pmod{f_i(x)}$, $1 \leq i \leq s$. This means there are $3c^s$ polynomials $p(x)$ over $\mathbb{F}_q$ of degree $< n$ satisfying $p(x)^c \in \{1, \rho, \rho^2\} \pmod{f(x)}$, $q-1$ of which are constant. Since $h(x)$ was chosen to be non-constant, there is a

$$\begin{aligned} \frac{3c^s - (q-1)}{q^n - q} &= \frac{3(\frac{q^d-1}{3})^s - (q-1)}{q^n - q} \\ &< \frac{1}{3^{s-1}} \\ &\leq \frac{1}{3} \end{aligned}$$

probability that $h(x) \in \{1, \rho, \rho^2\} \pmod{f(x)}$. Hence, there is $> 1 - \frac{1}{3^{s-1}}$ chance that the randomly selected polynomial $h(x)$ can be used to find a proper factor of $f(x)$.

Consider the other subcase that $q \equiv 2 \pmod 3$. Since 3 does not divide $q-1$ in this case, there exists no element of order 3 in $(\mathbb{F}_q)^\times$. Notice that if there were an element $\theta \in \mathbb{F}_q$ with $\theta^2 + \theta + 1 = 0$, then $\theta^3 - 1 = (\theta - 1)(\theta^2 + \theta + 1) = 0$ would contradict the fact that $(\mathbb{F}_q)^\times$ has no element of order 3. Thus, the polynomial $x^2 + x + 1$ has no root in $\mathbb{F}_q$ and is therefore irreducible over $\mathbb{F}_q$. Let ρ be a root of $x^2 + x + 1$ in some extension of $\mathbb{F}_q$. We now factor $f(x)$ in the quadratic extension field

$$\mathbb{F}_q(\rho) = \{a + b\rho : a, b \in \mathbb{F}_q\} \cong \mathbb{F}_{q^2}.$$

It is possible that some of the equal degree factors of $f(x)$ which are irreducible over $\mathbb{F}_q$ are not irreducible over $\mathbb{F}_q(\rho)$. So, we should perform DDF as the first step in factoring $f(x)$ over $\mathbb{F}_q(\rho)$. Then, since $q^2 \equiv 2^2 \pmod 3 \equiv 1 \pmod 3$, we can use the EDF process described earlier to find all of the irreducible factors of $f(x)$ over $\mathbb{F}_q(\rho) \cong \mathbb{F}_{q^2}$, where ρ is our known element of order 3. After obtaining the irreducible factors of $f(x)$ in $\mathbb{F}_q(\rho)[x]$, we can combine factors with coefficients lying outside of $\mathbb{F}_q$ to obtain a non-trivial factorization of $f(x)$ over $\mathbb{F}_q$.

We observe that Cantor and Zassenhaus' original strategy for factoring $f(x)$ when $p = 2$ is very difficult to apply in practice, especially in the case where $q \equiv 2 \pmod 3$. So, we will develop an alternate factoring approach for the case of $p = 2$, which draws from the work of Shoup[6]. We start with the following proposition.

Proposition 3.7: Let $q = 2^v$ and $a \in \mathbb{F}_q$. Then

$$\sum_{j=0}^{v-1} a^{2^j} = 0 \qquad \text{or} \qquad \sum_{j=0}^{v-1} a^{2^j} = 1.$$

Proof: By Theorem 1.6 and the Generalized FLT,

$$\begin{aligned}
\sum_{j=0}^{v-1} a^{2^j} &= a + \sum_{j=1}^{v-1} a^{2^j} \\
&= a^{2^v} + \sum_{j=1}^{v-1} a^{2^j} \\
&= \sum_{j=1}^{v} a^{2^j} \\
&= \sum_{j=1}^{v} a^{2 \cdot 2^{j-1}} \\
&= \left(\sum_{j=1}^{v} a^{2^{j-1}} \right)^2 \\
&= \left(\sum_{j=0}^{v-1} a^{2^j} \right)^2 .
\end{aligned}$$

Hence,

$$\sum_{j=0}^{v-1} a^{2^j} \left(\sum_{j=0}^{v-1} a^{2^j} - 1 \right) = 0,$$

and so it must be that

$$\sum_{j=0}^{v-1} a^{2^j} = 0 \qquad \text{or} \qquad \sum_{j=0}^{v-1} a^{2^j} = 1. \quad \blacksquare$$

Now, we get a theorem which will give us a new strategy for finding a proper factor of $f(x)$.

Theorem 3.8: Let $q = 2^v$ and $h(x)$ a polynomial over $\mathbb{F}_q$. Set

$$g(x) = \sum_{j=0}^{vd-1} h(x)^{2^j} \pmod{f(x)}.$$

If $\sum_{j=0}^{vd-1} h(x)^{2^j} \notin \{0, 1\} \pmod{f(x)}$, then $\gcd(f(x), g(x))$ is a proper factor of $f(x)$.

Proof: For each $i \in \{1, 2, \cdots, s\}$, note that $\mathbb{F}_q[x]/(f_i(x))$ is an isomorphic copy of the finite field containing $q^d = 2^{vd}$ elements. Thus, by Proposition 3.7,

$$\sum_{j=0}^{vd-1} h(x)^{2^j} \equiv 0 \pmod{f_i(x)} \quad \text{or} \quad \sum_{j=0}^{vd-1} h(x)^{2^j} \equiv 1 \pmod{f_i(x)}.$$

Since $\sum_{j=0}^{vd-1} h(x)^{2^j} \notin \{0, 1\} (\mathrm{mod}\ f(x))$, clearly $\sum_{j=0}^{vd-1} h(x)^{2^j}$ is non-constant over $\mathbb{F}_q$. Hence, $g(x)$ is non-constant. Now, since $\sum_{j=0}^{vd-1} h(x)^{2^j} \not\equiv 1 \pmod{f(x)}$, there must exist an $i_0 \in \{1, \cdots, s\}$ with $\sum_{j=0}^{vd-1} h(x)^{2^j} \equiv 0 \pmod{f_{i_0}(x)}$. So, $g(x) \equiv 0 \pmod{f_{i_0}(x)}$, and it follows from Proposition 3.4 that $\gcd(f(x), g(x))$ is a proper factor of $f(x)$. ■

For a polynomial $h(x)$ randomly chosen from the $q^n - q$ non-constant polynomials in $\mathbb{F}_q[x]$ of degree $< n$, $q = 2^v$, Theorem 3.8 cannot be used to get a proper factor of $f(x)$ only if $\sum_{j=0}^{vd-1} h(x)^{2^j} \in \{0, 1\} \pmod{f(x)}$, which occurs precisely when $\gcd(f(x), \sum_{j=0}^{vd-1} h(x)^{2^j}) \in \{1, f(x)\}$. Using the results of Shoup, we have that for each $i \in \{1, \cdots, s\}$, there are $q^d/2$ polynomials $p_i(x)$, of degree $< d$, such that $\sum_{j=0}^{vd-1} p_i(x)^{2^j} \equiv 0 \pmod{f_i(x)}$, and $q^d/2$ such that $\sum_{j=0}^{vd-1} p_i(x)^{2^j} \equiv 1 \pmod{f_i(x)}$. This means there are $2(q^d/2)^s$ polynomials $p(x)$ of degree $< n$ in $\mathbb{F}_q[x]$ with $\sum_{j=0}^{vd-1} p_i(x)^{2^j} \in \{0, 1\} \pmod{f(x)}$, q of which are constant. Since $h(x)$ was chosen to be non-constant, it follows that there is a

$$\frac{2\left(\frac{q^d}{2}\right)^s - q}{q^n - q} < \frac{1}{2^{s-1}}$$

chance that $\sum_{j=0}^{vd-1} h(x)^{2^j} \in \{0, 1\} \pmod{f(x)}$. So, there is $> 1 - \frac{1}{2^{s-1}}$ chance that $\gcd(f(x), g(x))$ is a proper factor of $f(x)$, where $g(x) = \sum_{j=0}^{vd-1} h(x)^{2^j} \pmod{f(x)}$.

Using the strategy of finding a proper factor of $f(x)$ given in Theorem 3.8 with randomly chosen polynomials, we now present an EDF algorithm for the case of $p = 2$. Apart from the definition of the polynomial g, this algorithm is identical to the EDF algorithm for the case that q is odd.

EDF Algorithm over $\mathbb{F}_q$ with $q = 2^v$:

$A \leftarrow \{f\}$
while $|A| < s$ **do**
for each $p \in A$ with $\deg(p) > d$ **do**
choose $h \in \mathbb{F}_q[x]$ with $0 < \deg(h) < \deg(p)$ at random
$g \leftarrow \sum_{j=0}^{vd-1} h^{2^j} \pmod{p}$
if $\gcd(p, g) \neq 1$ and $\gcd(p, g) \neq p$
$A \leftarrow (A - \{p\}) \cup \{\gcd(p, g), p/\gcd(p, g)\}$
end if
end while
output A

We apply this algorithm over $\mathbb{F}_2$ in the upcoming example.

Example 3.9: Given that $f(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1 \in \mathbb{F}_2[x]$ can be written as the product of distinct irreducibles of degree $d = 4$, we find the complete factorization of $f(x)$.

Note that the number of irreducible factors of $f(x)$ is $s = 8/4 = 2$. So, there is a $> \frac{1}{2}$ probability that a randomly chosen non-constant polynomial over $\mathbb{F}_2$ of degree < 8 will yield a proper factor of $f(x)$ using the EDF algorithm. We randomly choose $x^3 + x^2 + 1 \in \mathbb{F}_2[x]$. Now, we compute

$$\begin{aligned}\sum_{j=0}^{1\cdot 4-1} (x^3 + x^2 + 1)^{2^j} &= \sum_{j=0}^{3} (x^3 + x^2 + 1)^{2^j} \\ &\equiv x^7 + x^5 + x^3 + x^2 \pmod{f(x)}.\end{aligned}$$

Observe that since $\sum_{j=0}^{3} (x^3 + x^2 + 1)^{2^j} \notin \{0, 1\} \pmod{f(x)}$, we are guaranteed to get a proper factor of $f(x)$ by applying Theorem 3.8. So, we compute

$$\gcd(f(x), x^7 + x^5 + x^3 + x^2) = x^4 + x^3 + 1,$$

and then

$$f(x)/(x^4 + x^3 + 1) = x^4 + x + 1.$$

Thus,

$$f(x) = (x^4 + x^3 + 1)(x^4 + x + 1)$$

is the complete factorization of $f(x)$ over $\mathbb{F}_2$.

This concludes our discussion of equal degree factorization. In the final section of Chapter 3, we will look at a few useful applications of the Cantor-Zassenhaus factoring method.

3.3 Applications of the Cantor-Zassenhaus Method

Our work so far in Chapter 3 has provided us with quite a few tools for gaining information about the factorization of a polynomial over $\mathbb{F}_q$. When used together, we have established that these tools result in a complete factoring process. However, we can also use our tools to answer more specialized questions about polynomials. Specifically, in this section we will develop a root finding process over $\mathbb{F}_q$, two tests for irreducibility, and a method by which we can generate irreducible polynomials of any given degree. We will then conclude the section by giving an interesting application of the Cantor-Zassenahus method to Berlekamp's method of factoring.

Let $f(x)$ be a non-constant monic polynomial over $\mathbb{F}_q$. Recall from Section 3.1 that $x^q - x$ is the product of all distinct monic polynomials of degree 1 in $\mathbb{F}_q[x]$. Then $\gcd(f(x), x^q - x)$ gives us the product of all distinct linear factors of $f(x)$. Notice that we can use our EDF algorithm to factor $\gcd(f(x), x^q - x)$ and, in turn, separate all these linear factors. This suggests the following process for finding all of the roots of $f(x)$.

Steps for Root Finding:

(1) Let $h(x) = x^q - x (\text{mod } f(x))$, and find $\gcd(f(x), h(x))$. If $\gcd(f(x), h(x)) = 1$, conclude that $f(x)$ has no roots. Otherwise, proceed to (2).

(2) Use the EDF algorithm to factor $\gcd(f(x), h(x))$.

(3) Find the roots associated with the linear factors identified in (2). This will give all the roots of $f(x)$ in $\mathbb{F}_q$.

Example 3.10: Let $f(x) = x^{12}+3x^{11}+4x^{10}+5x^8+x^6+3x^5+6x^4+6x^3+10 \in \mathbb{F}_{13}[x]$. We desire to find all of the roots of $f(x)$ in $\mathbb{F}_{13}$. Let

$$\begin{aligned} h(x) &= x^{13} - x (\text{mod } f(x)) \\ &= 5x^{11} + 12x^{10} + 8x^9 + 2x^8 + 12x^7 + 3x^5 + 12x^4 + 5x^3 + 2x + 4. \end{aligned}$$

Now, we compute

$$\gcd(f(x), h(x)) = x^4 + 3x^3 + 4x^2 + 5.$$

Finally, we use the EDF algorithm to find that

$$\begin{aligned} x^4 + 3x^3 + 4x^2 + 5 &= (x+2)(x+7)(x+8)(x+12) \\ &= (x-11)(x-6)(x-5)(x-1). \end{aligned}$$

Hence, $1, 5, 6$, and 11 are all the roots of $f(x)$ in $\mathbb{F}_{13}$.

Next we turn our attention to generating tests for irreducibility. For a positive integer r, recall that $x^{q^r} - x$ is the product of all the distinct monic irreducibles in $\mathbb{F}_q[x]$ of degree d, where d runs through all of the positive divisors of r. We will use polynomials of the form $x^{q^r} - x$ to develop a couple of methods for determining whether the arbitrary polynomial $f(x)$ is irreducible.

Note that if $f(x)$ is reducible, then it is not hard to see that $f(x)$ must have an irreducible factor of degree $\leq \deg(f(x))/2$. With this observation in mind, we give the following proposition.

Proposition 3.11 (General Irreducibility Test): Let $f(x) \in \mathbb{F}_q[x]$ be a monic polynomial of degree $n > 1$. Then $f(x)$ is irreducible over $\mathbb{F}_q$ if and only if $\gcd(f(x), x^{q^r} - x) = 1$ for all integers r with $\frac{n}{4} < r \leq \frac{n}{2}$.

***Proof*:** First, suppose that $f(x)$ is irreducible over $\mathbb{F}_q$, and let r be a positive integer with $\frac{n}{4} < r \leq \frac{n}{2}$. Note that the degree of any monic irreducible factor of $x^{q^r} - x$ must divide r. Then since $n \nmid r$, the irreducible $f(x)$ is not a factor of $x^{q^r} - x$. So it must be that $\gcd(f(x), x^{q^r} - x) = 1$.

We now prove the other direction of the statement by proving its contrapositive. Suppose that $f(x)$ is reducible. We seek to show there exists an integer r with $\frac{n}{4} < r \leq \frac{n}{2}$ such that $\gcd(f(x), x^{q^r} - x) \neq 1$. Since $f(x)$ is reducible, $f(x)$ must have an irreducible factor, say $g(x)$, of degree $k \leq \frac{n}{2}$. Clearly $g(x) | \gcd(f(x), x^{q^k} - x)$, and so $\gcd(f(x), x^{q^k} - x) \neq 1$. Hence, if the positive integer k satisfies $\frac{n}{4} < k \leq \frac{n}{2}$, then we are done. So, assume that $k \leq \frac{n}{4}$. Let $j = \left[\frac{n}{4k}\right]$, where $\left[\frac{n}{4k}\right]$ is the largest integer $\leq \frac{n}{4k}$, and let $s = (j+1)k$. Then

$$s > \frac{n}{4k} \cdot k = \frac{n}{4},$$

and

$$\begin{aligned} s &\leq \left(\frac{n}{4k} + 1\right) k \\ &= \frac{n}{4} + k \\ &\leq \frac{n}{4} + \frac{n}{4} \\ &= \frac{n}{2}. \end{aligned}$$

Now, since k divides the integer s and $g(x)$ is an irreducible of degree k, it follows that $g(x)$ is a factor of $x^{q^s} - x$. Hence, $g(x) | \gcd(f(x), x^{q^s} - x)$, and $\gcd(f(x), x^{q^s} - x) \neq 1$. ■

We now use Proposition 3.11 to develop an algorithm for irreducibility testing.

General Irreducibility Test Algorithm:
The input is a monic polynomial f over $\mathbb{F}_q$ of degree $n > 1$.

for $r = \left[\frac{n}{4}\right] + 1, \left[\frac{n}{4}\right] + 2, \cdots, \left[\frac{n}{2}\right]$ **do**
  $h \leftarrow x^{q^r} - x \pmod{f(x)}$
  $g \leftarrow \gcd(f, h)$
  if $g \neq 1$
    then output "reducible" and **STOP**
  end if
end for
output "irreducible"

The basic idea of this algorithm is that starting with $r = \left[\frac{n}{4}\right] + 1$, we compute $x^{q^r} \pmod{f(x)}$ using binary exponentiation and then take the corresponding gcd. If we reach the end of the **for** loop, then by Proposition 3.11, we know that $f(x)$ is irreducible. This algorithm is applied in Example 3.12.

Example 3.12: Consider the polynomial $f(x) = x^7 + 2x^6 + x^3 + x^2 + x + 2$ over $\mathbb{F}_3$. We seek to discover whether or not $f(x)$ is irreducible. To start the irreducibility test, notice that the only integers r satisfying $\frac{7}{4} < r \leq \frac{7}{2}$ are $r = 2$ and $r = 3$. First, we use binary exponentiation and the Euclidean Algorithm to find that

$$\begin{aligned} &x^{3^2} - x \equiv x^6 + 2x^5 + x^4 + 2x^2 + 2x + 1 \pmod{f(x)}, \text{ and} \\ &\gcd(f(x), x^6 + 2x^5 + x^4 + 2x^2 + 2x + 1) = 1. \end{aligned}$$

Next, we compute

$$x^{3^3} - x \equiv x^6 + 2x^4 + 2x^2 + x + 2 \pmod{f(x)}, \text{ and}$$
$$\gcd(f(x), x^6 + 2x^4 + 2x^2 + x + 2) = 1.$$

Thus, by the General Irreducibility Test, $f(x)$ is irreducible over $\mathbb{F}_3$.

When n is large, we observe that the General Irreducibility Test requires a great deal of gcd computations before concluding that a polynomial is irreducible. We will now formulate an alternate irreducibility test, due to Rabin[5], that does not require nearly as many gcd computations for large degree inputs.

Proposition 3.13 (Rabin's Irreducibility Test): Let $n > 1$ be an integer and $w_1, w_2, \cdots, w_k$ be all the distinct prime divisors n. Denote $n_i = n/w_i$ for $1 \leq i \leq k$. A monic polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n is irreducible in $\mathbb{F}_q[x]$ if and only if $\gcd(f(x), x^{q^{n_i}} - x) = 1$ for each $1 \leq i \leq k$, and $f(x)$ divides $x^{q^n} - x$.

***Proof*:** First, suppose $f(x)$ is irreducible over $\mathbb{F}_q$. For each n_i, the degree of each irreducible factor of $x^{q^{n_i}} - x$ divides n_i. Since $n \nmid n_i$, clearly $f(x)$ not an irreducible factor of $x^{q^{n_i}} - x$. Hence, $\gcd(f(x), x^{q^{n_i}} - x) = 1$ for each i. Furthermore, since each irreducible in $\mathbb{F}_q[x]$ of degree n divides $x^{q^n} - x$, it follows that $f(x)$ divides $x^{q^n} - x$.

Next we prove the contrapositive of the other direction of the statement. Suppose that $f(x)$ is reducible over $\mathbb{F}_q$ and $f(x)$ divides $x^{q^n} - x$. Since $f(x)$ is reducible, $f(x)$ has an irreducible factor in $\mathbb{F}_q[x]$, say $g(x)$, of degree $d < n$. Now, since $g(x)$ divides $x^{q^n} - x$ it follows that $d|n$. Suppose $n = w_1^{\alpha_1} w_2^{\alpha_2} \cdots w_k^{\alpha_k}$ is the prime factorization of the integer n, where $\alpha_1, \alpha_2, \cdots, \alpha_k$ are positive integers. Then since $d|n$, we can write $d = w_1^{\beta_1} w_2^{\beta_2} \cdots w_k^{\beta_k}$ for some nonnegative integers $\beta_1, \beta_2, \cdots, \beta_k$. Furthermore, since $d < n$, it must be that $\beta_i < \alpha_i$ for some $1 \leq i \leq k$. Then clearly $d|n_i$. Hence, $g(x)$ is a factor of $x^{q^{n_i}} - x$, and it follows that $\gcd(f(x), x^{q^{n_i}} - x) \neq 1$. ■

Using Proposition 3.13, on the next page we present an alternate algorithm for irreducibility testing.

Rabin's Irreducibility Test Algorithm:
Let $w_1, w_2, \cdots, w_k$ be all the distinct prime divisors of an integer $n > 1$ ordered so that $w_1 > w_2 > \cdots > w_k$. The input is a monic polynomial $f \in \mathbb{F}_q[x]$ of degree n.

for $j = 1, 2, \cdots, k$ **do**
  $n_j \leftarrow n/w_j$
end for
for $i = 1, 2, \cdots, k$ **do**
  $h \leftarrow x^{q^{n_i}} - x \pmod{f}$
  $g \leftarrow \gcd(f, h)$
  if $g \neq 1$
    then output "reducible" and **STOP**
  end if
end for
$g \leftarrow x^{q^n} - x \pmod{f}$
if $g \neq 0$
  then output "reducible" and **STOP**
end if
output "irreducible"

Note that the prime divisors $w_1, w_2, \cdots, w_k$ of n are ordered so that $w_1 > w_2 > \cdots > w_k$ to give $n_1 < n_2 < \cdots < n_k$. In the case that the input f is reducible, this ensures that we do not reduce $x^{q^{n_i}} - x \bmod f$ for any unnecessarily large values of n_i.

Now, let's look at an example.

Example 3.14: Let $f(x) = x^{10} + x^9 + x^7 + x^5 + x^4 + x^2 + 1 \in \mathbb{F}_2[x]$. To apply Rabin's Irreducibility Test, first notice that the only prime divisors of 10 are 5 and 2. So, we let $n_1 = 10/5 = 2$ and $n_2 = 10/2 = 5$ in the algorithm. First, we compute

$$x^{2^2} - x \equiv x^4 - x \pmod{f(x)}, \text{and}$$
$$\gcd(f(x), x^4 - x) = 1.$$

Next we compute

$$x^{2^5} - x \equiv x^7 + x^6 + x^4 \pmod{f(x)}, \text{and}$$
$$\gcd(f(x), x^7 + x^6 + x^4) = 1.$$

So, all of the necessary gcd's are 1. Now, using binary exponentiation at great length, it can be found that $x^{2^{10}} \equiv x \pmod{f(x)}$. Hence,

$$x^{2^{10}} - x \equiv 0 \pmod{f(x)},$$

which means that $f(x)$ divides $x^{2^{10}} - x$. Thus, by Rabin's Irreducibility Test, $f(x)$ is irreducible over $\mathbb{F}_2$.

A major disadvantage of Rabin's Test is that we must always compute $x^{q^n} - x \pmod{f(x)}$, where n is the degree of $f(x)$. This computation can be quite tedious, even in cases where n is not relatively large. Recall that when using the General Irreducibility Test, the highest value for r for which $x^{q^r} - x \pmod{f(x)}$ must be computed is $r = \frac{n}{2}$. So, in cases where n is not very large, the General Irreducibility Test is preferable from a computational standpoint. For example, the computations required by the General Irreducibility Test to show the degree 10 polynomial of Example 3.14 is irreducible are much less tiresome than the computations required by Rabin's Test.

Now that we have established irreducibility tests, we can potentially generate irreducible polynomials of a given degree by using trail and error. For example, if we want an irreducible of degree 7, we can begin randomly selecting degree 7 polynomials in $\mathbb{F}_q[x]$ and hope that we eventually find one that is deemed irreducible by an irreducibility test. With a little luck, this process may work sometimes, but, in general, it is not even close to being an efficient method for generating irreducibles. We seek to develop a better method.

We begin by setting

$$h_1(x) = x^q - x.$$

Then $h_1(x)$ is the product of all monic degree 1 polynomials over $\mathbb{F}_q$. We can actually separate all the monic linear polynomials by applying EDF to $h_1(x)$. Notice that since $x^{q^2} - x$ is the product of all monic degree 1 and degree 2 irreducibles, dividing $x^{q^2} - x$ by $h_1(x)$ gives the product of only the degree 2 irreducibles. Now we let

$$h_2(x) = \frac{x^{q^2} - x}{h_1(x)}.$$

Applying EDF to $h_2(x)$ will separate all degree 2 irreducibles. Further, since $x^{q^3} - x$ is the product of all monic degree 1 and degree 3 irreducibles over $\mathbb{F}_q$, dividing $x^{q^3} - x$ by $h_1(x)$ gives the product of just the degree 3 irreducibles. So,

we let

$$h_3(x) = \frac{x^{q^3} - x}{h_1(x)}.$$

We then can apply EDF to $h_3(x)$ to generate all the distinct degree 3 irreducibles. Next, since $x^{q^4} - x$ is the product of all degree 1, degree 2, and degree 4 irreducibles, dividing $x^{q^4} - x$ by $h_1(x)h_2(x)$ gives the product of all degree 4 irreducibles. Then we let

$$h_4(x) = \frac{x^{q^4} - x}{h_1(x)h_2(x)},$$

and we can apply EDF to $h_4(x)$ to separate all the distinct degree 4 irreducibles. Continuing this process recursively, for a positive integer k, we have

$$h_k(x) = \frac{x^{q^k} - x}{\prod\limits_{\substack{d|k \\ d<k}} h_d(x)},$$

where $h_k(x)$ is the product of all disinct monic irreducibles of degree k over $\mathbb{F}_q$. These irreducibles can be separated by applying EDF to $h_k(x)$.

We have now developed a process for generating all irreducibles in $\mathbb{F}_q[x]$ of any given degree. This process is applied in Example 3.15.

Example 3.15: We will find all monic irreducible polynomials of degree ≤ 5 in $\mathbb{F}_2[x]$. Applying EDF in each step of our process, we find

$$\begin{aligned} h_1(x) &= x^2 - x \\ &= x(x-1), \end{aligned}$$

$$\begin{aligned} h_2(x) &= \frac{x^4 - x}{h_1(x)} \\ &= x^2 + x + 1, \end{aligned}$$

$$\begin{aligned} h_3(x) &= \frac{x^8 - x}{h_1(x)} \\ &= (x^3 + x + 1)(x^3 + x^2 + 1), \end{aligned}$$

$$\begin{aligned} h_4(x) &= \frac{x^{16} - x}{h_1(x)h_2(x)} \\ &= (x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1), \end{aligned}$$

$$\begin{aligned} h_5(x) &= \frac{x^{32} - x}{h_1(x)} \\ &= (x^5 + x^2 + 1)(x^5 + x^3 + 1)(x^5 + x^3 + x^2 + x + 1)(x^5 + x^4 + x^2 + x + 1) \\ &\cdot (x^5 + x^4 + x^3 + x + 1)(x^5 + x^4 + x^3 + x^2 + 1). \end{aligned}$$

The factors in these five products give all monic irreducible polynomials of degree ≤ 5 over $\mathbb{F}_2$.

Recall that being able to find irreducibles allows us to explicitly construct finite fields. For example, if we can find an irreducible $g(x)$ of degree v over $\mathbb{F}_p$, then we can let α be an arbitrary root of $g(x)$ and construct the finite field

$$\begin{aligned} \mathbb{F}_p(\theta) &= \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{v-1}\alpha^{v-1} : a_0, a_1, a_2, \cdots, a_{v-1} \in \mathbb{F}_p\} \\ &\cong \mathbb{F}_{p^v} \\ &= \mathbb{F}_q. \end{aligned}$$

We can then use the fact that α is a root of $g(x)$ to perform operations in $\mathbb{F}_p(\theta)$. Computationally speaking, when $v > 1$, the field $\mathbb{F}_q$ is useless to us unless we can find irreducibles that yield concrete representations of it. Hence, the fact that we have developed a way to generate irreducibles is of great importance - it basically means we can do computations in any finite field of our choosing.

We will conclude the chapter by applying the strategies of Cantor and Zassenhaus to Berlekamp's technique for factoring. Specifically, for the case that q is odd, we will generate a probabilistic method for finding a proper factor of an arbitrary polynomial over $\mathbb{F}_q$. Note that the work we do here will closely resemble our work in Section 3.2 over EDF.

Suppose q is odd and let $f(x) \in \mathbb{F}_q[x]$ be a non-constant monic polynomial of degree n with complete factorization $f(x) = f_1(x)^{k_1} f_2(x)^{k_2} \cdots f_m(x)^{k_m}$, where $m \geq 2$. Recall from Chapter 2 that we sought to factor $f(x)$ by finding polynomials in the vector space

$$V = \{g(x) \in \mathbb{F}_q[x] : \deg(g(x)) < n \text{ and } g(x)^q \equiv g(x) \pmod{f(x)}\}$$

over $\mathbb{F}_q$. It follows from Theorem 2.7 that V has q^m elements, where m is the

number of distinct irreducibles which divide $f(x)$. We now choose a random polynomial $g(x)$ from the $q^m - 1$ nonzero polynomials contained in V (remember that selecting a random element from V amounts to randomly selecting coefficients that solve a homogenous system of equations). We seek to use $g(x)$ in some way to get a proper factor of $f(x)$. Notice that if $\gcd(f(x), g(x)) \neq 1$, then $\gcd(f(x), g(x))$ gives us a proper factor of $f(x)$. So, we assume that $\gcd(f(x), g(x)) = 1$.

By Proposition 2.6, for $i = 1, 2, \cdots, m$, we have that $g(x) \equiv g_i \pmod{f_i(x)^{k_i}}$ for some $g_i \in \mathbb{F}_q$. Set $c = \frac{q-1}{2}$. Since $\gcd(f(x), g(x)) = 1$, it follows that $g(x) \not\equiv 0 \pmod{f_i(x)^{k_i}}$ for each i, which implies $g_i \neq 0$. Thus, by the Generalized FLT,

$$\begin{aligned}(g(x)^c)^2 &= g(x)^{q-1} \\ &\equiv g_i^{q-1} \pmod{f_i(x)^{k_i}} \\ &\equiv 1 \pmod{f_i(x)^{k_i}},\end{aligned}$$

and so $g(x)^c \equiv 1 \pmod{f_i(x)^{k_i}}$ or $g(x)^c \equiv -1 \pmod{f_i(x)^{k_i}}$ for each i.

For the time being, we additionally assume that $g(x)^c \not\equiv \pm 1 \pmod{f(x)}$ (note that this automatically guarantees $g(x)$ is non-constant in $\mathbb{F}_q[x]$). In particular, since $g(x)^c \not\equiv -1 \pmod{f(x)}$, we have that $g(x)^c \not\equiv -1 \pmod{f_{i_0}(x)^{k_{i_0}}}$ for some $1 \leq i_0 \leq m$. Then $g(x)^c \equiv 1 \pmod{f_{i_0}(x)^{k_{i_0}}}$, and so $f_{i_0}(x)^{k_{i_0}}$ is a common factor of $f(x)$ and $g(x)^c - 1$. Since we also have that $g(x)^c - 1 \not\equiv 0 \pmod{f(x)}$, it follows that $\gcd(f(x), g(x)^c - 1)$ is a proper factor of $f(x)$.

Removing all of our assumptions, we now calculate the probability that for a random, nonzero element $g(x) \in V$, neither $\gcd(f(x), g(x))$ nor $\gcd(f(x), g(x)^c - 1)$ is a proper factor of $f(x)$. Considering our previous results, we need only calculate the probability that $g(x)^c \equiv \pm 1 \pmod{f(x)}$. Recall from the proof of Theorem 2.7 that there is a one-to-one correspondence between V and the set

$$S = \{(s_1, s_2, \cdots, s_m) : s_i \in \mathbb{F}_q\}.$$

The nature of this correspondence is that $s(x) \in V$ iff there exists a unique m-tuple $(s_1, s_2, \cdots, s_m) \in S$ with $s(x) \equiv s_i \pmod{f_i(x)^{k_i}}$ for each i and $\deg(s(x)) < n$. Now, as noted by Cantor and Zassenhaus[2], it can be shown that there are c^m m-tuples $(s_1, s_2, \cdots, s_m)$ such that $s_i^c = 1$ for each i, and c^m such that $s_i^c = -1$ for each i. Correspondingly, there are $2c^m$ polynomials $s(x) \in V$ with $s(x) \equiv \pm 1 \pmod{f(x)}$. Thus, the probability that neither $\gcd(f(x), g(x))$ nor $\gcd(f(x), g(x)^c - 1)$ is a proper factor of $f(x)$ is

$$\begin{aligned}\frac{2c^m}{q^m-1} &= \frac{1}{2^{m-1}} \cdot \frac{(q-1)^m}{q^m-1} \\ &< \frac{1}{2^{m-1}}.\end{aligned}$$

So, there is a $> 1 - \frac{1}{2^{m-1}}$ chance that either $\gcd(f(x), g(x))$ or $\gcd(f(x), g(x)^c - 1)$ is a proper factor of $f(x)$. As m, the number of distinct irreducible factors of $f(x)$, grows large, the probability of getting a proper factor of $f(x)$ using this method approaches 1.

Recall that for a non-constant element $g(x) \in V$, Theorem 2.9 guarantees that at least one element of the set

$$\{\gcd(f(x), g(x) - s) : s \in \mathbb{F}_q\}$$

is a proper factor of $f(x)$. Notice that if q is large, we may have to compute $\gcd(f(x), g(x) - s)$ for many values of s before finding a proper factor. However, with our new results, we know that there is a high probability that either $\gcd(f(x), g(x))$ or $\gcd(f(x), g(x)^c - 1)$ will be a proper factor of $f(x)$. So, our new probabilistic factorization technique using the elements of V only requires two gcd computations, no matter the size of q. Since there are not as many gcd computations required by this probabilistic technique, we recommend using it to get a nontrivial factorization of $f(x)$.

By meshing together the Cantor-Zassenhaus and Berlekamp methods for factoring, we got a considerable result. Hopefully, even more progess in factoring polynomials over $\mathbb{F}_q$ can be made by looking at these methods together. For example, it would be an interesting endeavor to attempt to generate a complete factoring algorithm that utilizes the probabilistic method we just formulated for finding a proper factor of the arbitrary polynomial $f(x) \in \mathbb{F}_q[x]$. Furthermore, it might be productive to explore how DDF can be used in conjunction with Berlekamp's method to formulate a better deterministic algorithm for factoring. As always, the search for new ideas goes on.

Bibliography

[1] Berlekamp, E.R. (1967). "Factoring Polynomials Over Finite Fields." *Bell System Technical Journal*, 46(8), 1853-1859.

[2] Cantor, D. & Zassenhaus, H. (1981). "A New Algorithm for Factoring Polynomials Over Finite Fields." *Mathematics of Computation*, 36(154), 587-592.

[3] Childs, L. (1995). "A Concrete Inroduction to Higher Algebra." 2nd ed. New York: Springer.

[4] Dummit, D. & Foote, R. (2004). "Abstract Algebra." 3rd ed. New Jersey: Wiley.

[5] Rabin, M. (1980). "Probabilistic Algorithms in Finite Fields." *SIAM Journal on Computing*, 9(2), 273-280.

[6] Shoup, V. (2005). "A Computational Introduction to Number Theory and Algebra." Cambridge: Cambridge University Press.