Construction of Multiplicative Groups of Polynomials with Non-Zero Identities in $\mathbb{Z}_p[x]$

Dara Varam
Advised by Dr. Ayman Badawi

Senior Thesis presented in partial fulfillment of the requirements for
Bachelor of Science in Mathematics

Department of Mathematics and Statistics
The American University of Sharjah
United Arab Emirates

Abstract

Let p be a prime integer and $\mathbb{Z}_p[x]$ be the set of all polynomials over Z_p. For a polynomial $m(x) \in Z_p[x]$ such that $degree(m(x)) \geq 2$, we define $G_m = \{f(x) \in Z_p[x] \mid degree(f(x)) < degree(m(x))\}$. We define two binary operations on G_m: Addition modulo $m(x)$ and multiplication modulo $m(x)$. If $m(x)$ is the product of distinct irreducible polynomials in $Z_p[x]$ (i.e., $m(x)$ is square-free), we show that $G_m^* = G_m - \{0\}$ is the union of disjoints multiplicative groups of G_m. If $m(x)$ is not square-free, we construct all multiplicative groups of G_m.

1 Introduction

This paper focuses on the construction of multiplicative groups of polynomials with non-zero identities. We will first define the notion of a group:

Definition 1. *A group is a non-empty set and operation, $(D, \circ)$, that satisfies the following axioms:*

1. *Closure: For any two elements $a, b \in D$, we have $a \circ b \in D$.*
2. *Associativity: The binary operation $\circ$ is associative, meaning that for any three elements a, b, and c in D, we have $(a \circ b) \circ c = a \circ (b \circ c)$*
3. *Identity: There exists an element $e \in D$ such that for any element $a \in D$, we have $e \circ a = a$*
4. *Inverse: For every element $a \in D$, there exists an element, denoted by a^{-1}, such that $a * a^{-1} = e$*

Let p be a prime integer. We recall that $Z_p[x]$ is the set of all polynomials with coefficients from Z_p. For a polynomial $m(x) \in Z_p[x]$ such that $degree(m(x)) \geq 2$, we define $G_m = \{f(x) \in Z_p[x] \mid degree(f(x)) < degree(m(x))\}$. We define two binary operations on G_m: Addition modulo $m(x)$ and multiplication modulo $m(x)$. If $m(x)$ is the product of distinct irreducible polynomials in $Z_p[x]$ (i.e., $m(x)$ is square-free), we show that $G_m^* = G_m - \{0\}$ is the union of disjoint multiplicative groups of G_m. If $m(x)$ is not square-free, we construct all multiplicative groups of G_m.

Let p be a prime integer. Recall that $f_1, f_2 \in Z_p[x]$ are associative if $f_1(x) = uf_1(x)$ for some u in Z_p^*. It is known that if $m(x) \in Z_p[x]$ of degree ≥ 2, then $m(x)$ can be written uniquely (up to associative) as

$m(x) = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdot P_k^{\alpha_k}$, where $P_1, P_2, ..., P_K \in \mathbb{Z}_p[x]$ are distinct irreducible polynomials in $Z_p[x]$ with $\alpha_i \geqslant 1 \forall i \in \{1, \ldots, k\}$.

If $m(x) = P_1(x)P_2(x) \cdots P_k(x)$, we say that $m(x)$ is square-free.

Definition 2.

1. *Let p be a prime integer and $m(x) \in Z_p[x]$ of degree ≥ 2. Write $m(x) = P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_k^{\alpha_k}$, where $P_1, P_2, ..., P_K \in \mathbb{Z}_p[x]$ are distinct irreducible polynomials in $Z_p[x]$ with $\alpha_i \geqslant 1 \forall i \in \{1, \ldots, k\}$. Then each $P_i^{\alpha}{}_i$ is called a perfect prime factor of $m(x)$. Let $d(x)$ be a product of distinct perfect prime factors of $m(x)$ or $d(x) = 1$. Then $d(x)$ is called a perfect factor of $m(x)$.*
2. *If $w(x) \in G_m$ and $w(x)^k = 0$ in G_m for some integer $k \geq 1$, we say that $w(x)$ is a nilpotent element of G_m.*
3. *If $e(x) \in G_m$ and $e(x)^2 = e(x)$ in G_m, we say $e(x)$ is an idempotent of G_m.*

2 Results

2.1 Idempotents

Lemma 1. *Assume* $e(x)$ *is an idempotent of* G_m *and* $e(x) \neq 0, 1$. *Then* $\gcd(e(x), m(x))$ *is a perfect factor of* $m(x)$.

Proof. Since $e^2(x) = e(x)$ in G_m (by definition of an idempotent), then $m(x)$ divides $e(x)(e(x)-1)$. Mathematically, $m(x) \mid (e(x))(e(x)-1)$. Since $\gcd(e(x), e(x)-1) = 1$ in G_m and $e(x) \neq 0, 1$, we conclude that $\gcd(e(x), m(x))$ is a perfect factor of $m(x)$. □

To show the existence of such idempotents (and find them), we will use the Chinese Remainder Theorem for polynomials, which states the following:

Definition 3. *For some* $m(x) = P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_k^{\alpha_k}$,

$$\begin{aligned} e_1(x) &\equiv (0 \vee 1)(mod\ P_1^{\alpha_1}) \\ e_2(x) &\equiv (0 \vee 1)(mod\ P_2^{\alpha_2}) \\ &\vdots \\ e_k(x) &\equiv (0 \vee 1)(mod\ P_k^{\alpha_k}) \end{aligned}$$

Since we have k irreducible polynomials and e is congruent either to 0 or to 1 (two options), then the total number of idempotents for G_m is 2^k. We will ignore the trivial idempotent $0 \in G_m$. Hence G_m^* has exactly $2^k - 1$ nonzero idempotents.

Define the following set of polynomials m_i with $i \in \{1, \ldots, k\}$.

$$m_1 = \frac{m}{P_1^{\alpha_1}}, m_2 = \frac{m}{P_2^{\alpha_2}}, \ldots, m_k = \frac{m}{P_k^{\alpha_k}}$$

$$\begin{aligned} m_1 &= P_2^{\alpha_2} P_3 \cdots P_k^{\alpha_k}, \\ m_2 &= P_1^{\alpha_1} P_3^{\alpha_3} \cdots P_k^{\alpha_k}, \\ &\vdots \\ m_k &= P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_{k-1}^{\alpha_{k-1}} \end{aligned}$$

Then:

$$\begin{aligned} m_1 \times m_1^{-1} &\equiv 1(mod\ m_1) \\ m_2 \times m_2^{-1} &\equiv 1(mod\ m_2) \\ &\vdots \\ m_k \times m_k^{-1} &\equiv 1(mod\ m_k) \end{aligned}$$

By the Chinese remainder Theorem, i.e., CRT, we have

$$e_i(x) = \left[m_1 m_1^{-1}(0 \vee 1) + m_2 m_2^{-1}(0 \vee 1) + \cdots + m_k m_k^{-1}(0 \vee 1)\right]\ mod\ m(x)$$

.

2.2 Main Result

The principal goal of this paper is to prove that when $m(x)$ is square-free, i.e., $m(x)$ is a product of distinct irreducible polynomials over $\mathbb{Z}_p$ for some prime p, then the set G_m^* is the union of disjoint groups under multiplication modulo $m(x)$. Mathematically:

$$G_m^* = \bigcup(U_i) = U_1 \cup U_2 \cup \cdots \cup U_k, U_i \subset G_m^* \tag{1}$$

To prove this, we will first propose the existence of one group $U_1 \subset G_m^*$ and then apply a theorem to show the existence of the others. groups.

Proposition 1. *We define U_1 to be the following set:*

$$U_1 = \{f(x) \in G_m^* \mid \gcd(f(x), m(x)) = 1\}$$

U_1 is a group under multiplication modulo m.

Proof. To prove that U_1 is a multiplicative group, we will go through the four axioms defining groups.

Identity: $e(x) = 1$ since $\gcd(f(x), m(x)) = 1$. For all functions $f(x)$ in U_1, $f(x) \times 1 = f(x)$.

Closure: Take two elements, $u_1, u_2 \in U_1$. Thus $\gcd(u_1(x), m(x)) = 1$ and $\gcd(u_2(x), m(x) = 1)$. Thus $\gcd(u_1 \times u_2, m(x)) = 1$, where the multiplication is modulo $m(x)$, showing that we have closure.

Associativity: Since we are dealing with polynomials, this is trivial.

Inverse: Let $u \in U_1$. Then $\gcd(u, m(x)) = 1$ in $\mathbb{Z}_p[x]$. This means that $1 = u_1(x)u + n(x)m(x)$ for some $u_1(x), n(x) \in \mathbb{Z}_p[x]$. Now $u_1(x)u + n(x)m(x) = u_1(x)u$ in G_m, which means $1 = u_1(x)u$ in G_m. Thus $u^{-1} = u_1(x)$. Hence U_1 is a group under multiplication modulo $m(x)$. □

Theorem 1. *Let $e(x) \in G_m^*$ be an idempotent of G_m^*. Then $e(x)U_1$ is a multiplicative group with identity $e(x)$.*

Proof. Identity: The identity element is clearly $e(x)$.

Closure: Let $w_1, w_2 \in e(x)U_1$. We show that $w_1 w_2 \in e(x)U_1$.

$w_1 = e(x)d_1, w_2 = e(x)d_2$ for some $d_1, d_2 \in U_1$. Since we have established that U_1 is a group and $d_1, d_2 \in U_1$, we conclude that $d_1 d_2 \in U_1$. Hence $w_1 w_2 = e(x)d_1 e(x)d_2 = e^2(x)d_1 d_2 = e(x)d_1 d_2 \in e(x)U_1$.

Associative: It is clear since $(G_m, .)$ is associative.

Inverse: Let $w \in e(x)U_1$. Hence $w = e(x)d$ for some $d \in U_1$. Since U_1 is a group, $d^{-1} \in U_1$ with $dd^{-1} = 1$. Therefore, $e(x)d^{-1}$ is the inverse of w. Thus $e(x)U_1$ is a group under multiplication modulo $m(x)$. □

Theorem 2. *Let $U_k = \{f(x) \in G_m^* \mid \gcd(f(x), m(x)) = k\}$, where k is a perfect factor of $m(x)$. Then U_k is a multiplicative group with identity $e_k(x) \neq 0$. Furthermore, $U_k = e_k(x)U_1$.*

Proof. First, we show that U_k has an idempotent $e(x)$. Since k is a perfect factor of $m(x)$, we conclude that the $gcd(k, m/k) = 1$. Hence by the CRT, there is a $d \in G_m$ such that $d \equiv 0 \,(mod\, k)$ and $d \equiv 1 \,(mod\, m/k)$. It is clear that such d is the idempotent $e_k(x) \in U_k$. We show $e_k(x)U_1 = U_k$. Let $c(x)$ in $e_k(x)U_1$. Then $c(x) = e(x)d(x)$

for some $d(x) \in U_1$. Since $\gcd(d(x), m(x)) = 1$ and $\gcd(e_k(x), m(x)) = k$, we conclude $\gcd(e_k(x)d(x), m(x)) = k$. Hence $c(x) \in U_k$.

$\Longleftarrow$ Let $d(x) \in U_k$. Set $v = d(x) + (e_k(x) - 1)$. We will show that $d(x) = e_k(x)v(x)$, where $v \in U_1$. Assume we have a prime factor of $m(x)$, say P, that divides $v(x)$. Observe that $d(x)(e_k(x) - 1) = 0 \in G_m$ and $\gcd(d(x), e_k(x) - 1) = 1$. Hence P must divide both $d(x)$ and $e_k(x) - 1$. This is a contradiction, since the $\gcd(d(x), e_k(x) - 1) = 1$. Therefore, such a P does not exist. Hence $\gcd(v(x), m(x)) = 1$. Since $v(x) = d(x) + (e_k(x) - 1)$, then:

$$\begin{aligned} e_k(x)v(x) &= e_k(x)d(x) + 0 \\ &\Rightarrow d(x) = e_k(x)v(x) \end{aligned}$$

Hence $d(x) \in e(x)U_1$. Therefore, by Theorem 1, U_k is a multiplicative group with identity $e_k(x)$. □

Since we have shown that the set U_1 is a multiplicative group and each set of the form $e_k(x)U_1$ is also a multiplicative group modulo $m(x)$. Hence it is clear that when $m(x)$ is a product of distinct irreducible polynomials, then the set G_m^* is made up of these disjoint partitions $U_i \forall i \in \{1, \ldots, k\}$.

Note that if $m(x)$ is not square-free, then by Lemma 1, U_k will not be a group if k is not a perfect factor of $m(x)$ (i.e., U_k will not have an identity). Using the definition of the Nilpotent set of G_m, we have the following theorem:

Theorem 3. *Assume $m(x)$ is not square-free. Let $a \in G_m \setminus Nil(G_m)$ such that a is not an element of every multiplicative group of G_m. Then there is a multiplicative group U_k of G_m for some perfect factor $k(x)$ of $m(x)$ such that $a = f + w$ for some $f \in U_k$ and $w \in Nil(G_m)$,*

Proof. Assume that $a(x) \notin Nil(G_m)$. Let $e(x)$ be the nonzero idempotent of G_m of minimum degree such that $a(x) \mid e(x)$. Hence every prime factor $p(x)$ of $e(x)$ is a prime factor of $a(x)$. Since $e_k(x)(e_k(x)-1) = 0$ in G_m and $\gcd(e_k(x), e_k(x)-1) = 1$, we conclude that $w(x) = a(x)(e(x) - 1) \in Nil(G_m)$. Since $1 = (1 - e(x) + e(x)$, we have $a(x) = a(x)(1-ex(x)) + a(x)e(x) = w(x) + e(x)f(x)$. Let $f(x) = a(x)e(x)$ and $K = gcd(e(x), n(x)) = gcd(f(x), m(x))$. Then K is a perfect factor of $m(x)$. Thus $a(x) = f(x) + w(x)$, for some $f \in U_k$ and $w \in Nil(G_m)$, where U_k is a multiplicative group of G_m for some perfect factor k of $m(x)$. □

To get the cardinality of each group, we will be using the $\phi(m(x))$ function, described in the next section.

2.3 $\phi(m(x))$ and the cardinality of U_k

Theorem 4. *Let $m(x) = P_1^{\alpha_1}$ with $P_1(x) \in \mathbb{Z}_p[x]$. then:*

$$\phi(m(x)) = [p^{\deg(P_1)\alpha_1} - p^{\deg(P_1)(\alpha_1 - 1)}] = |U_1|$$

Proof. Consider $G_m = \{f(x) \in \mathbb{Z}_p[x] \mid \deg(f) < \deg(m)\}$. Note that the degree of m, denoted $\deg(m) = \deg(P_1)\alpha_1$. Therefore the cardinality of G_m, denoted $|G_m| = p^{\deg(P_1)\alpha_1}$. Observe that $\gcd(a(x), m(x)) = 1$ or a multiple of $P_1(x)$ for every $a(x) \in G_m$. This means that $\deg(a(x)) \leqslant \deg(P_1)(\alpha_1 - 1)$ for every $a(x) \in G_m$.

Define the set $H = \{a(x) \in G_m \mid \gcd(a(x), m(x)) \neq 1\}$. It is clear that

$$\phi(m(x)) = |G_m| - |H|$$

Since $H = \{a(x) \in G_m \mid \gcd(a(x), m(x)) \neq 1\}$, we have $H = \{a(x)P_1(x) \mid \deg(a(x)) \leqslant \deg(P_1)(\alpha_1 - 1)\}$. Therefore, $|H| = p^{\deg(P_1)(\alpha_1-1)}$. Thus:

$$\phi(m(x)) = |G_m| - |H| = p^{\deg(P_1)\alpha_1} - p^{\deg(P_1)(\alpha_1-1)}$$

□

Theorem 5. *(1) Let $m(x) = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdot \cdots \cdot P_k^{\alpha_k}$. Then $|U_1|$ is given by:*

$$\phi(m(x)) = (p^{\deg(P_1)\alpha_1} - p^{\deg(P_1)(\alpha_1-1)}) \times \cdots \times (p^{\deg(P_k)\alpha_k} - p^{\deg(P_k)(\alpha_k-1)}) \quad (2)$$

(2) If k is a perfect factor of $m(x)$, then $|U_k| = \phi(m(x)/k)$

Proof. (1) It is clear that $\phi(m(x))$ is multiplicative,i.e., $\phi(m(x)) = \phi(P_1^{\alpha_1})\phi(P_2^{\alpha_2})\cdots\phi(P_k^{\alpha_k})$. Hence the claim is clear by Theorem 4.

(2) Assume k is a perfect factor of $m(x)$. Then $U_k = \{f(x) \in G_m^* \mid \gcd(f(x), m(x)) = k\}$ = $\{f(x) \in G_m^* \mid deg(f) < deg(m/k)$ and $gcd(f(x), m(x)/k) = 1\} = \phi(m(x)/k(x))$

□

3 Computational Implementation

To confirm the above results, we have developed a computational implementation that will take k irreducible polynomials in $\mathbb{Z}_p[x]$ and produce the subsequent disjoint groups that makeup G_m. This has been implemented through Python. The approach was first to generate all polynomials within a set G_m given the matrix representation of the polynomial m and the value of p. Thus, we would have $m(x) \in \mathbb{Z}_p[x]$. To generate this, we will define $\mathbb{Z}_p$ and then get the number of coefficients by determining $\deg(m)$. Then, the generation of the coefficients matrix (and thus each of the elements in G_m can be given by the following program:

```
import numpy as np
import itertools

coefficients = list(itertools.product(Z_p, repeat= len(Z_p)))
coefficients = [c for c in coefficients if sum(c) >= 0]
```

Listing 1: Generating the sets of polynomials G_m

To identify each of the idempotents in G_m, we will need to find the elements $e(x)$ where $e(x) \times e(x) = e(x)$, or in other words, $e^2(x) = e(x)$. For this, we generate a table that is $p^k \times p^k$ elements and look along the diagonal. Within this diagonal, if an element is the same as the corresponding row or column, then we have an idempotent. The following block of code describes this step:

```
table = np.zeros((card, card), dtype= object)
for i in range(card):
    for j in range(card):
        product = np.polymul(coefficients[i], coefficients[j])
        _, remainder = np.polydiv(product, modulus)
        if len(product) >= num_coefficients:
            res = np.mod(remainder,len(Z_p))
            res = [0]*(num_coefficients-len(res)) + list(res)
            table[i][j] = res
        else:
            res = np.mod(product, len(Z_p))
```

```
            res = [0]*(num_coefficients-len(res)) + list(res)
            table[i][j] = res

for i in range(card):
    for j in range(card):
        table[i][j] = [int(x) for x in table[i][j]]
```

Listing 2: Generating the multiplicative table of G_m to get the idempotents

We will then use a gcd() function that will allow us to find the $\gcd$ between two polynomials in $\mathbb{Z}_p[x]$. This was adapted from [3].

```
    EPSILON = 0.0001
def reciprocal(n, p=0):
    if p == 0:
        return 1/n
    for i in range(p):
        if (n*i) % p == 1:
            return i
    return None if n % p == 0 else 0


def gcd(f, g, p=0, verbose=False):
    if (len(f)<len(g)):
        return gcd(g,f,p, verbose)

    r = [0]*len(f)
    r_mult = reciprocal(g[0], p)*f[0]

    for i in range(len(f)):
        if (i < len(g)):
            r[i] = f[i] - g[i]*r_mult
        else:
            r[i] = f[i]
        if (p != 0):
            r[i] %= p

    while (abs(r[0])<EPSILON):
        r.pop(0)
        if (len(r) == 0):
            return g

    return gcd(r, g, p, verbose)
```

Listing 3: GCD function

Finally, to get the set U_1, we go through each element in G_m and find elements where $\gcd(f(x), m(x)) \in \mathbb{Z}_p^*$.

```
    for i, c in enumerate(coefficients):
        if (gcd(c, g, p, True) == Z_p - [0]):
        U1.append(c)}}
```

Listing 4: Identifying elements of U_1

```
    for i in range(len(U1)):
       product = np.polymul(U1[i], e_kx)
       if (len(product > num_coefficients)):
          _, remainder = np.polydiv(product, g)
          remainder = np.mod(remainder[-(num_coefficients):], p)
          remainder = remainder.astype(int)
          Uk.append(remainder)

```

```
        else:
            Uk.append(product)
```

Listing 5: Identifying elements of U_k

4 Proof of Concept and Examples

Example 4.0.1. *We take* $m(x) = P_1P_2$*, with* $P_1(x) = (x^2 + x + 1)$ *and* $P_2(x) = (x^3 + x + 1)$ *in* $\mathbb{Z}_2[x]$*. Then:*

$$m(x) = x^5 + x^4 + 1 \in \mathbb{Z}_2[x] \tag{3}$$

We will use this polynomial $m(x)$ *to construct the set* G_m*. We define* G_m *as:*

$$G_m = \{f(x) \in \mathbb{Z}_2[x] \mid \deg(f) < \deg(m)\},$$

with $\deg(m) = 5$*. Using matrix representation, we can then use our program to implement the full set* G_m*, as shown in Table 1.*

	$(a_4, a_3, a_2, a_1, a_0)$
f_1	(0, 0, 0, 0, 1)
f_2	(0, 0, 0, 1, 0)
$\vdots$	$\vdots$
f_{30}	(1, 1, 1, 1, 0)
f_{31}	(1, 1, 1, 1, 1)

Table 1: Generated table of all elements in $G_m \in \mathbb{Z}_2[x]$ where $m(x) = x^5 + x^4 + 1$

Where $f(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$*. The total number of elements in* G_m *is* 2^5*, whilst the total number of elements in* G_m^* *is* $2^5 - 1 = 31$*. The idempotent elements in this set are as follows:*

Matrix	Polynomial
$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 \end{bmatrix}$	1
$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 \end{bmatrix}$	$x^4 + x^3 + x^2$
$\begin{bmatrix} 1 & 1 & 1 & 0 & 1 \end{bmatrix}$	$x^4 + x^3 + x^2 + 1$

Table 2: Idempotents of G_m with $m(x) = x^5 + x^4 + 1$

We are expecting $2^2 - 1 = 3$ *idempotents, which is confirmed by the above. We define the set* U_1 *as* $U_1 = \{u(x) \in G_m^* \mid \gcd(u(x), x^5 + x^4 + 1) = 1 in \mathbb{Z}_2[x]\}$*. Similarly, the set* U_2 *is given by* $U_2 = \{(x^4 + x^3 + x^2)u(x) \in (\mathbb{Z}_2[x])_m \mid \gcd((x^4 + x^3 + x^2)u(x), x^5 + x^4 + 1) \in \mathbb{Z}_2^*\}$*. Finally, the set* U_3 *is defined as* $U_3 = \{(x^4 + x^3 + x^2 + 1)u(x) \in (\mathbb{Z}_2[x])_m \mid \gcd((x^4 + x^3 + x^2 + 1)u(x), x^5 + x^4 + 1) \in \mathbb{Z}_2^*\}$*.*

G_m			
	1	x	$x+1$
	x^2	x^2+1	x^2+x
	x^2+x+1	x^3	x^3+1
	x^3+x	x^3+x+1	x^3+x^2
	x^3+x^2+1	x^3+x^2+x	x^3+x^2+x+1
	x^4	x^4+1	x^4+x
	x^4+x+1	x^4+x^2	x^4+x^2+1
	x^4+x^2+x	x^4+x^2+x+1	x^4+x^3
	x^4+x^3+1	x^4+x^3+x	x^4+x^3+x+1
	$x^4+x^3+x^2$	$x^4+x^3+x^2+x$	$x^4+x^3+x^2+1$
	$x^4+x^3+x^2+x+1$		

Table 3: Full set G_m

U_1			
	1	x	$x+1$
	x^2	x^2+1	x^2+x
	x^3	x^3+x	x^3+x^2
	x^3+x^2+1	x^3+x^2+x+1	x^4
	x^4+1	x^4+x+1	x^4+x^2
	x^4+x^2+x+1	x^4+x^3	x^4+x^3+1
	x^4+x^3+x	$x^4+x^3+x^2+x$	$x^4+x^3+x^2+x+1$

Table 4: The set U_1

U_2				
	x^2+x+1	x^3+1	x^3+x^2+x	x^4+x
	x^4+x^2+1	x^4+x^3+x+1	$x^4+x^3+x^2$	

Table 5: The set U_2

U_3			
	x^3+x+1	x^4+x^2+x	$x^4+x^3+x^2+1$

Table 6: The set U_3

To confirm the elements in each of these three sets, we have presented the full sets in Tables 3, 4, 5, and 7.

It is clear that each of the disjoint subsets U_1, U_2, U_3 form up the set G_m. We can also see that all of U_1, U_2 and U_3 are groups under multiplication modulo $m(x)$, given that they are closed, associative, have an identity ($e_1(x) = 1$ for U_1, $e_2(x) = x^4 + x^3 + x^2$ for U_2 and $e_3(x) = x^4 + x^3 + x^2 + 1$ for U_3) and have an inverse for each of the elements in the set. Therefore, we have demonstrated that for the example of $m(x) = x^5 + x^4 + 1 \in \mathbb{Z}_2[x]$, the set G_m is made up of 3 disjoint subsets that each form a group under multiplication modulo $m(x)$. For the purposes of demonstration, we will show the Cayley table for U_3, since U_1 and U_2 would consume too much space.

Cayley Table for U_3	$x^3 + x + 1$	$x^4 + x^2 + x$	$x^4 + x^3 + x^2 + 1$
$x^3 + x + 1$	$x^4 + x^2 - x$	$-x^4 + x^3 - x^2 - 1$	$x^3 + x + 1$
$x^4 + x^2 + x$	$-x^4 + x^3 - x^2 - 1$	$-x^3 - x + 1$	$x^4 + x^2 + x$
$x^4 + x^3 + x^2 + 1$	$x^3 + x + 1$	$x^4 + x^2 + x$	$x^4 - x^3 + x^2 + 1$

Table 7: The set U_3

Example 4.0.2. *Assume we have some $m(x) = x^3 + 2x + x^2 + 2 \in \mathbb{Z}_3$. Clearly we can see that $m(x)$ is square-free, as it can be written as $m(x) = P_1 * P_2 = (x+1)(x^2+2)$. G_m based on this $m(x)$ would be a set that contains $3^3 = 27$ elements, since we are working in $\mathbb{Z}_3$. Additionally, since all polynomials have degree strictly less than $\deg(m(x)) = 3$, they will be of the form $f(x) = a_2x^2 + a_1x + a_0$ with $a_i \in \mathbb{Z}_3$. We will find the idempotents of G_m based on the provided algorithms. We will have $2^2 - 1 = 3$ idempotents, and they are characterized as below:*

$$
\begin{aligned}
e_1(x) &= \quad 1 \\
e_2(x) &= \quad x^2 + 2x + 1 \\
e_3(x) &= \quad 2x^2 + x
\end{aligned}
$$

Each idempotent is a perfect factor of $m(x)$, forming a group with the respective identity. The groups will be as follows: U_1 with identity 1, $U_2 = (x^2 + 2x + 1) * U_1$ with identity $(x^2 + 2x + 1)$, and finally, $U_3 = (2x^2 + x) * U_1$ with identity $2x^2 + x$.

Example 4.0.3. *Let $m(x) = P_1^2 * P_2 = (x + 1)^2(x + 2) = x^3 + x^2 + 2x + 2 \in \mathbb{Z}_3$. Clearly, we can see that $m(x)$ is not square-free, as we have at least one term where the power of P_i is not 1. In this case, then we have three perfect factors of $m(x)$: $1, k = (x + 1)^2, h = (x + 2)$. Thus G_m has exactly 3 multiplicative groups modulo $m(x)$, namely, U_1, U_k and U_h.*

5 Conclusion

Let p be a prime integer and $m(x) \in Z_p[x]$ of degree ≥ 2. In this project, we have used the Chinese Remainder Theorem to construct multiplicative groups modulo $m(x)$ in G_m, where $G_m = f(x) \in \mathbb{Z}_p[x] | \deg(f) < \deg(m)$. If $m(x) \in Z_p[x]$ is square-free, we showed that G_m^* is the union of disjoint multiplicative groups modulo $m(x)$. If $m(x)$ is not square-free, we constructed all multiplicative group modulo $m(x)$ in G_m. If U_k is a multiplicative group modulo $m(x)$ in G_m, then $|U_k|$ is determined. Through our computational implementation of this process, we can easily find out every element within the set G_m and each subsequent subset that forms a group, namely

$U_1, U_2, ..., U_k$. This removes the need for exhaustively going through the set G_m by hand and significantly reduces the restrictions on finding sets with $m(x)$ having a higher degree working in $\mathbb{Z}_p$. For future work, we consider other problems to which the Chinese Remainder Theorem applies.

References

[1] Ayman Badawi, Abstract Algebra Manual: Problems and Solutions, Nova Science Publications, USA, 2004.

[2] Joseph A. Gallian, Contemporary Abstract Algebra, Brooks/Cole, USA, 2022.

[3] Yuval, unc0mm0n, Python function to calculate polynomial gcd over finite files of prime cardinality, GitHub repository, GitHub, https://gist.github.com/unc0mm0n/117617351ecd67cea8b3ac81fa0e02a8, 2016.