Universidade Federal da Grande Dourados

Dissertação de Mestrado

UMA APLICAÇÃO DE POLINÔMIOS EM CODIFICAÇÃO

Beatriz Ibarra Dutra

Dourados-MS
2020

Universidade Federal da Grande Dourados

Beatriz Ibarra Dutra

UMA APLICAÇÃO DE POLINÔMIOS EM CODIFICAÇÃO

Dissertação apresentada ao final do Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal da Grande Dourados - UFGD como exigência parcial para obtenção do título de Mestre em Matemática.

Orientadora: Prof[a]. Dr[a]. Irene Magalhães Craveiro

Dourados-MS
2020

Dados Internacionais de Catalogação na Publicação (CIP).

D978a Dutra, Beatriz Ibarra

Uma aplicação de polinômios em codificação [recurso eletrônico] / Beatriz Ibarra Dutra. -- 2020.

Arquivo em formato pdf.

Orientadora: Irene Magalhães Craveiro.

Dissertação (Mestrado em Matemática)-Universidade Federal da Grande Dourados, 2020.

Disponível no Repositório Institucional da UFGD em:
https://portal.ufgd.edu.br/setor/biblioteca/repositorio

1. Polinômios. 2. Corpos Finitos. 3. Códigos Cíclicos. I. Craveiro, Irene Magalhães. II. Título.

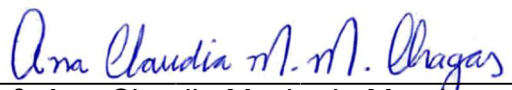
Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

MINISTÉRIO DA EDUCAÇÃO
FUNDAÇÃO UNIVERSIDADE FEDERAL DA GRANDE DOURADOS
FACULDADE DE CIÊNCIAS EXATAS E TECNOLOGIA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

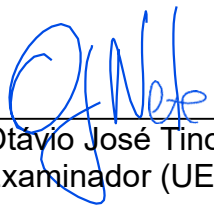
Termo de Aprovação

Após a apresentação, arguição e apreciação pela banca examinadora, foi emitido o parecer APROVADA, para a dissertação intitulada: **"Uma Aplicação de Polinômios em Codificação"**, de autoria de **Beatriz Ibarra Dutra**, apresentada ao Programa de Mestrado Profissional em Matemática da Universidade Federal da Grande Dourados.

Profª. Drª. Irene Magalhães Craveiro (Orientador-UFGD)
Presidente da Banca Examinadora



Profª. Drª. Ana Claudia Machado Mendonça Chagas
Membro Examinador (UFGD)



Prof. Dr. Otávio José Tinoco Neves dos Santos
Membro Examinador (UEMS)

Dourados/MS, 26 de março de 2020

Ao meu filho Otávio.

Agradecimentos

Agradeço primeiramente a Deus pela vida que Ele me concedeu.

Sou grato à minha família pelo apoio que sempre me deram durante toda a minha vida. A minha mãe, Elvia, que sempre me incentivou aos estudos.

Agradeço a meu marido, amigo e companheiro de estudos, Rodrigo, que me apoiou durante todo essa caminhada. Ao meu filho, Otávio, que me faz ser uma mulher cada dia mais forte.

A todo corpo docente do PROFMAT pelos ensinamentos, com destaque a professora Ana Claudia, obrigada pelas contribuições; e em especial a minha orientadora Irene a qual tenho muita admiração e carinho, a senhora é um exemplo para mim.

Resumo

Este trabalho irá apresentar uma aplicação dos polinômios em codificação, mais especificamente em códigos cíclicos. Para isso será introduzido um conceito preliminar de polinômios, já que os códigos cíclicos são gerados a partir de um. Além disso, apresentará um breve estudo a respeito da aritmética dos restos no anel de polinômios sobre $\mathbb{Z}_p$. Tratará também de corpos finitos baseados no anel de polinômios sobre $\mathbb{Z}_p$, abordando alguns conceitos como o de característica de um corpo, elemento primitivo, extensão de corpos e polinômios minimais. Por fim, apresentará algoritmos que permitem a codificação e decodificação em códigos cíclicos.

Palavras-chave: Polinômios, Corpos Finitos, Códigos Cíclicos.

Abstract

This work will present an application of polynomials in coding, more specifically in cyclic codes. For this, a preliminary concept of polynomials will be introduced, since the cyclic codes are generated from one. In addition, it will present a brief study about the arithmetic of the remainders in the polynomial ring about $\mathbb{Z}_p$. It will also deal with finite bodies based on the polynomial ring on $\mathbb{Z}_p$, addressing some concepts such as the characteristic of a body, primitive element, extension of bodies and minimal polynomials. Finally, it will present algorithms that allow the encoding and decoding of cyclic codes.

Keywords: Polynomials, Finite Bodies, Cyclic Codes .

Sumário

CAPÍTULO 1

Introdução

A transmissão de dados ou seu armazenamento, é uma ação recorrente em nosso dia a dia, por meio de um telefone celular, por exemplo, podemos enviar textos, fotos, vídeos entre outros arquivos. Mas o que muitos não sabem é que por trás de todo sistema de transmissão digital de informação estão os códigos corretores de erros, isso por que, nesse processo pode ocorrer erros.

Quando uma informação digital recebida é distinta da informação originalmente enviada dizemos que ocorreu um erro durante a transmissão de dados, tal erro é chamado de *ruído*. Os códigos corretores de erros tem a missão de adicionar informação a mensagem enviada para que posteriormente possa encontrar e corrigir possíveis erros na mensagem recebida.

A Teoria dos Códigos teve início na década de quarenta com os estudos de Richard W. Hamming, C. E. Shannon e Marcel J. E. Golay que são utilizados até hoje em nosso cotidiano em sistemas de comunicações via satélite, em redes locais de computadores, entre outros. Hoje em dia a Teoria dos Códigos Corretores de Erros é um campo de estudo muito ativo.

Este trabalho apresentará uma aplicação de polinômios em codificação, o tópico polinômios é abordado ainda no ensino básico e é essencial para tratarmos de Códigos Cíclicos. Em [1] também é dissertado o tema códigos cíclicos, que diferencia-se deste por optar em utilizar uma definição pouco convencional de polinômios, mas que permite ao leitor estudar esse assunto de forma alternativa.

Apresentaremos alguns conceitos e propriedades relacionadas a anéis de polinômios sobre o corpo das classes residuais dos inteiros módulo p, onde p é um número primo,

elementos da Teoria de Corpos Finitos, bem como sua aplicação em Teoria de Códigos, especificamente, em códigos cíclicos.

No capítulo 2, abordaremos o tópico anéis de polinômios, onde apresentaremos algumas definições e propriedades relacionadas a divisibilidade, o máximo divisor comum e irredutibilidade de polinômios.

No capítulo 3, faremos um breve estudo sobre a aritmética realizada com os restos da divisão de elementos $\mathbb{Z}_p[x]$ por um polinômio $p(x)$ sobre $\mathbb{Z}_p$.

No capítulo 4, faremos uma introdução a corpos finitos baseados no anel de polinômios $\mathbb{Z}_p[x]$, abordando os conceitos de característica de um corpo, elemento primitivo, extensão de corpos, polinômios minimais e por fim um método para encontrar polinômios irredutíveis.

E por fim, no capítulo 5, apresentaremos a matriz geradora do código cíclico, bem como os resultados que juntamente com os estudos dos capítulos anteriores nos permitem construir e decodificar um código cíclico, que possui como uma especificidade algoritmos baseados em operações com polinômios.

O conteúdo abordado neste trabalho requer do leitor familiaridade com tópicos algébricos, como por exemplo: o conceito de Espaço Vetorial, combinação linear, base, dimensão e dependência linear.

CAPÍTULO 2

Polinômios

Neste capítulo nosso objeto de estudo serão os anéis de polinômios sobre o conjunto $\mathbb{Z}_p$, onde $\mathbb{Z}_p$ é formado pelas classes residuais dos números inteiros módulo p, fica convencionado que no decorrer de todo trabalho sempre que nos referirmos ao símbolo p estaremos tratando de um número inteiro primo maior que 1. Também iremos omitir os colchetes na representação dos elementos de $\mathbb{Z}_p$, apenas escreveremos $a \in \mathbb{Z}_p$, onde a é uma classe residual módulo p. Além disso, assumiremos que $(\mathbb{Z}_p, +, \cdot)$ é um corpo, caso o leitor não tenha familiaridade com o assunto recomendamos a consulta em [2, capítulo 2]. Apresentaremos algumas definições e propriedades básicas relacionadas aos anéis de polinômios sobre $\mathbb{Z}_p$ necessárias para a compreensão dos estudos dos demais capítulos desse trabalho.

2.1 Anéis de polinômio sobre $\mathbb{Z}_p$

Considere o corpo $\mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\}$ das classes em $\mathbb{Z}$ módulo p, onde p é um número primo. Um polinômio sobre o $\mathbb{Z}_p$ é uma expressão da forma:

$$f(x) = f_n \cdot x^n + f_{n-1} \cdot x^{n-1} + \cdots + f_1 \cdot x + f_0$$

onde cada $f_i \in \mathbb{Z}_p$, com $0 \leqslant i \leqslant n$. Denotamos o conjunto dos polinômios sobre $\mathbb{Z}_p$ por $\mathbb{Z}_p[x]$, onde x é a indeterminada. Os polinômios da forma $p(x) = f_0$, com $f_0 \in \mathbb{Z}_p$ é chamado polinômio **constante**, no caso $p(x) = 0$ o chamamos de polinômio **nulo**.

Definição 2.1.1. Em $f(x) \in \mathbb{Z}_p[x]$ o coeficiente da maior potência de x do conjunto

$\{f_0, f_1, \cdots, f_n\}$ é chamado de coeficiente **líder**, quando $f_n = 1$ dizemos que o polinômio é **mônico**.

Exemplo 2.1.2. Considere o polinômio $p(x) = 5x^7 + 4x^2 + 3x + 2$ pertencente a $\mathbb{Z}_7[X]$. O coeficiente líder de $p(x)$ é 5, pois a maior potência de $p(x)$ é x^7 e 5 é seu coeficiente.

Exemplo 2.1.3. O polinômio $f(x) = x^6 + 3x + 2$ de $\mathbb{Z}_5[X]$ é mônico, pois seu coeficiente líder é 1.

Definição 2.1.4. Dois polinômios $p(x) = a_m x^m + \cdots + a_1 x + a_0$ e $q(x) = b_n x^n + \cdots + b_1 x + b_0$ em $\mathbb{Z}_p[x]$ são ditos iguais quando, $m = n$ e seus coeficientes correspondentes são iguais, isto é, $a_0 = b_0, a_1 = b_1, \cdots, a_n = b_n$.

Agora vamos definir operações soma e produto no conjunto $\mathbb{Z}_p[X]$. Sejam $p(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ e $q(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$ elementos de $\mathbb{Z}_p[X]$.

- Adição: $(p + q)(x) = p(x) + q(x) = c_s x^s + c_{s-1}x^{s-1} + \cdots + c_1 x + c_0$, onde $c_i = (a_i + b_i) \in \mathbb{Z}_p[X]$.
- Multiplicação: $(p \cdot q)(x) = p(x) \cdot q(x) = c_s x^s + c_{s-1}x^{s-1} + \cdots + c_1 x + c_0$, onde $c_i = \sum_{\alpha+\beta=i} a_\alpha \cdot b_\beta$, ou seja,

$$
\begin{aligned}
c_0 &= a_0 b_0, \\
c_1 &= a_0 b_1 + a_1 b_0, \\
c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0, \\
&\vdots \\
c_i &= a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0, \\
&\vdots \\
c_{m+n} &= a_0 b_{m+n} + a_1 b_{m+n-1} + \cdots + a_{m+n} b_0 = a_m b_n.
\end{aligned}
$$

Observação 1. Em $c_{m+n} = \sum_{i=0}^{m+n} a_i b_{m+n-i}$ temos as condições: $a_i = 0$, se $i > m$ e $b_{m+n-i} = 0$, se $i < m$. Portanto, $c_{m+n} = a_m b_n$.

Exemplo 2.1.5. Sejam os polinômios $p(x), q(x) \in \mathbb{Z}_5[X]$, onde $p(x) = 3x^2 + 3x + 2$

e $q(x) = 4x^3 + 2x^2 + 3x + 4$, então obteremos como soma:

$$\begin{aligned} p(x) + q(x) &= 4x^3 + (3+2)x^2 + (1+3)x + (4+2) \\ &= 4x^3 + 0x^2 + 4x + 1 \\ &= 4x^3 + 4x + 1 \end{aligned}$$

Para o produto vamos determinar inicialmente os coeficientes:

$$\begin{aligned} c_0 &= 4 \cdot 2 = 1; \\ c_1 &= 2 \cdot 3 + 3 \cdot 4 = 3; \\ c_2 &= 2 \cdot 3 + 3 \cdot 3 + 3 \cdot 4 = 2; \\ c_3 &= 2 \cdot 4 + 3 \cdot 2 + 3 \cdot 3 + 0 \cdot 4 = 2; \\ c_4 &= 2 \cdot 0 + 3 \cdot 4 + 3 \cdot 2 + 0 \cdot 3 + 0 \cdot 4 = 3; \\ c_5 &= 3 \cdot 4 = 2. \end{aligned}$$

E o produto será:

$$\begin{aligned} p(x) \cdot q(x) &= (3x^2 + 3x + 2) \cdot (4x^3 + 2x^2 + 3x + 4) \\ &= 2x^5 + 3x^4 + 2x^3 + 2x^2 + 3x + 1 \end{aligned}$$

Proposição 2.1.1. *Para quaisquer $p(x), q(x), r(x) \in \mathbb{Z}_p[x]$, temos que $(\mathbb{Z}_p[x], +, \cdot)$ é um* ***Anel Comutativo com unidade*** *e portanto são válidas as propriedades:*

- *Da adição:*

1. *Associativa:* $(p(x) + q(x)) + r(x) = p(x) + (q(x) + r(x))$;
2. *Comutativa:* $p(x) + q(x) = q(x) + p(x)$;
3. *Elemento neutro:* $\exists 0 \in \mathbb{Z}_p[x]$; $p(x) + 0 = p(x)$, $p(x) \in \mathbb{Z}_p[x]$;
4. *Inverso: Dado* $p(x) \in \mathbb{Z}_p[x]$, $\exists -p(x) \in \mathbb{Z}_p[x]$; $p(x) + (-p(x)) = 0$;

- *Da multiplicação:*

5. *Associativa:* $(p(x) \cdot q(x)) \cdot r(x) = p(x) \cdot (q(x) \cdot r(x))$;
6. *Comutativa:* $p(x) \cdot q(x) = q(x) \cdot p(x)$;
7. *Elemento Neutro:* $\exists 1 \in \mathbb{Z}_p[x]$; $p(x) \cdot 1 = p(x)$, $\forall p(x) \in \mathbb{Z}_p[x]$; $p(x) \neq 0$;
8. *Distributiva com relação à adição:* $p(x) \cdot (q(x) + r(x)) = p(x) \cdot q(x) + p(x) \cdot r(x)$.

Demonstração. Considere $p(x), q(x), r(x) \in \mathbb{Z}_p[x]$, tais que $p(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$, $q(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$ e $r(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c_0$. Temos que:

1. $p(x)+(q(x)+r(x)) = p(x)+(b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0 + c_k x^k + c_{k-1}x^{k-1} + \cdots + c_0) = p(x) + ((b_i + c_i)x^i + \cdots + b_0 + c_0) = ((a_j + b_j + c_j)x^j + \cdots + a_0 + b_0 + c_0 = ((a_j + b_j)x^j + \cdots + a_0 + b_0) + r(x) = (p(x) + q(x)) + r(x)$.

2. $p(x) + q(x) = (a_i + b_i)x^i + \cdots + a_0 + b_0 = (b_i + a_i)x^i + \cdots + b_0 + a_0 = q(x) + p(x)$.

3. Sejam $p(x)$ e $q(x) = 0$ polinômios pertencentes a $\mathbb{Z}_p[x]$, podemos obter:

$$p(x) + q(x) = p(x) + 0 = p(x), \text{qualquer que seja } q(x) \in \mathbb{Z}_p[x].$$

4. Dado $q(x) = 0$ e $p(x)$ elementos de $\mathbb{Z}_p[x]$. Existe $q(x) = -p(x) \in \mathbb{Z}_p[x]$, tal que: $p(x)+(-p(x)) = a_m x^m + \cdots + a_1 x + a_0 + (-a_m x^m - \cdots - a_1 x - a_0) = (a_m - a_m)x^m + \cdots + (a_1 - a_1)x + a_0 - a_0 = 0$.

5. Primeiramente considere:
   $p(x) \cdot q(x) = d_s x^s + \cdots + d_1 x + d_0$, com $d_i = \sum_{\alpha+\beta=i} a_\alpha \cdot b_\beta$,
   $(p(x) \cdot q(x)) \cdot r(x) = e_s x^s + \cdots + e_1 x + e_0$, com $e_i = \sum_{\alpha+\beta=i} d_\alpha \cdot c_\beta$,
   $q(x) \cdot r(x) = f_s x^s + \cdots + f_1 x + f_0$, com $f_i = \sum_{\alpha+\beta=i} b_\alpha \cdot c_\beta$,
   $p(x) \cdot (q(x)) \cdot r(x)) = g_s x^s + \cdots + g_1 x + g_0$, com $g_i = \sum_{\alpha+\beta=i} a_\alpha \cdot f_\beta$.
   Sendo assim, basta mostrarmos que $e_i = g_i$, para todo $i \in \mathbb{N}$. De fato,

$$e_i = \sum_{\alpha+\beta=i} d_\alpha \cdot c_\beta = \sum_{\alpha+\beta=i} \left(\sum_{\gamma+\delta=\alpha} a_\gamma \cdot b_\delta \right) \cdot c_\beta = \sum_{\gamma+\delta+\beta=i} (a_\gamma \cdot b_\delta) \cdot c_\beta =$$
$$\sum_{\gamma+\delta+\beta=i} a_\gamma \cdot (b_\delta \cdot c_\beta) = \sum_{\gamma+\lambda=i} a_\gamma \cdot \left(\sum_{\delta+\beta=\lambda} b_\delta \cdot c_\beta \right) = \sum_{\gamma+\lambda=i} a_\gamma \cdot f_\lambda = g_i.$$

6. $p(x) \cdot q(x) = (a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0)x^i + \cdots + (a_0 b_1 + a_1 b_0)x + a_0 b_0 = (b_0 a_i + b_1 a_{i-1} + \cdots + b_i a_0)x^i + \cdots + (b_0 a_1 + b_1 a_0)x + b_0 a_0 = q(x) \cdot p(x)$.

7. Sejam $p(x)$ e $r(x) = 1$ elementos de $\mathbb{Z}_p[x]$, podemos obter:

$$p(x) \cdot r(x) = p(x) \cdot 1 = (a_m x^m + \cdots + a_1 x + a_0) \cdot 1 = a_m x^m + \cdots + a_1 x + a_0 = p(x),$$

para todo $p(x) \in \mathbb{Z}_p[x]$.

8. Considere:
$p(x).(q(x)+r(x)) = t_s x^s + \cdots + t_1 x + t_0$, com $t_i = \sum_{\alpha+\beta=i} a_\alpha \cdot (b_\beta + c_\beta)$,
$p(x) \cdot q(x) = d_s x^s + \cdots + d_1 x + d_0$, com $d_i = \sum_{\alpha+\beta=i} a_\alpha \cdot b_\beta$,
$p(x) \cdot r(x) = h_s x^s + \cdots + h_1 x + h_0$, com $h_i = \sum_{\alpha+\beta=i} a_\alpha \cdot c_\beta$.

Desta forma, é equivalente mostrarmos que $t_i = d_i + h_i$, para todo $i \in \mathbb{N}$. De fato,

$$t_i = \sum_{\alpha+\beta=i} a_\alpha \cdot (b_\beta + c_\beta) = \sum_{\alpha+\beta=i} (a_\alpha \cdot b_\beta + a_\alpha \cdot c_\beta) = \sum_{\alpha+\beta=i} a_\alpha \cdot b_\beta + \sum_{\alpha+\beta=i} a_\alpha \cdot c_\beta = d_i + h_i.$$

□

Teorema 2.1.2. *$\mathbb{Z}_p[x]$ é um Anel de Integridade, ou seja, é válido nesse anel comutativo com unidade a propriedade:*

$$p(x) \cdot q(x) = 0 \Rightarrow p(x) = 0 \text{ ou } q(x) = 0.$$

Demonstração. Para tal, utilizaremos a contrapositiva: Se $p(x) \neq 0$ e $q(x) \neq 0$, então $p(x) \cdot q(x) \neq 0$.

Sejam $p(x) = a_m x^m + \cdots + a_1 x + a_o$ e $q(x) = b_n x^n + \cdots + b_1 x + b_o$ polinômios em $\mathbb{Z}_p[x]$, ambos não nulos, com $a_m \neq 0$ e $b_n \neq 0$ elementos de $\mathbb{Z}_p$. Sendo assim, temos que $a_m \cdot b_n \neq 0$. Segue da definição da multiplicação de polinômios que:

$$p(x) \cdot q(x) = c_s x^s + c_{s-1} x^{s-1} + \cdots + c_1 x + c_0, \text{ onde } c_i = \sum_{\alpha+\beta=i} a_\alpha \cdot b_\beta.$$

Note que:

$$c_{m+n} = \sum_{\alpha+\beta=m+n} a_\alpha \cdot b_\beta = a_0 b_{m+n} + a_1 b_{m+n-1} + \cdots + a_m b_n + \cdots + a_{m+n} b_0 = a_m b_n \neq 0$$

Portanto, o produto possui ao menos um coeficiente não nulo e consequentemente $p(x) \cdot q(x) \neq 0$. □

Definição 2.1.6. Seja $f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$ com $a_m \neq 0$. O grau de f é igual ao índice do coeficiente líder a_m e denotamos por $gr(f) = m$.

Observação 2. Segue da definição que $gr(f) = 0$ se e somente se $f(x) = a_0$, com $a_0 \in \mathbb{Z}_p - \{0\}$.

Proposição 2.1.3. *Sejam $f(x), g(x) \in \mathbb{Z}_p[x]$, polinômios não nulos, então:*

1. $gr(f+g) \leqslant max\{gr(f), gr(g)\}$, *onde* $f(x) \neq -g(x)$;

2. $gr(f \cdot g) = gr(f) + gr(g)$

Demonstração. 1. Sejam $f(x) = a_m x^m + \cdots + a_0$ e $g(x) = b_n x^n + \cdots + b_0$ polinômios em $\mathbb{Z}_p[x]$, com $a_m \neq 0$ e $b_n \neq 0$, como $f(x) \neq -g(x)$, então temos que $f(x) + g(x) \neq 0$. Consideremos $m > n$, da definição de adição de polinômios segue que: $f(x) + g(x) = (a_m + 0)x^m + \cdots + (a_1 + b_1)x + (a_0 + b_0)$. Note que $b_m = 0$, já que $m > n$. Portanto, $gr(f+g) = m = gr(f)$. Analogamente, temos que $gr(f+g) = n = gr(g)$, quando $m < n$.
Quando $m = n$, temos ainda duas situações: $a_m + b_n \neq 0$ ou $a_m + b_n = 0$. No primeiro caso ($a_m + b_n \neq 0$), temos que $f(x) + g(x) = (a_m + b_m)x^m + \cdots + (a_1 + b_1)x + (a_0 + b_0)$ e portanto $gr(f+g) = m = gr(f) = gr(g)$. No segundo caso, temos $f(x) + g(x) = (a_m + b_m)x^m + (a_j + b_j)x^j + \cdots + (a_1 + b_1)x + (a_0 + b_0)$, da hipótese temos $a_m + b_n = 0$, logo $a_j + b_j$ será o coeficiente líder desse polinômio, com $j < m = n$. Logo $gr(f+g) = j < gr(f) = gr(g)$. Em todos casos temos $gr(f+g) \leqslant max\{gr(f), gr(g)\}$.

2. Segue da definição do produto de polinômios:
$f(x) \cdot g(x) = c_s x^s + c_{s-1}x^{s-1} + \cdots + c_1 x + c_0$, onde $c_i = \sum_{\alpha+\beta=i} a_\alpha \cdot b_\beta$. Note que c_{m+n} será o coeficiente líder de $f(x) \cdot g(x)$, já que $a_m \neq 0$ e $b_n \neq 0$ implicam $c_{m+n} = a_m \cdot b_n \neq 0$. Portanto, segue da definição de grau de um polinômio que $gr(f \cdot g) = m + n = gr(f) + gr(g)$.

□

Exemplo 2.1.7. Sejam $f(x) = 4x^5 + 8x + 10$ e $g(x) = 7x^5 + 3x^3 + 5x^2 + 9$ em $\mathbb{Z}_{11}[x]$.

- Note que $a_5 = 4$ e $b_5 = 7$ são os coeficientes líderes dos polinômios $f(x)$ e $g(x)$, respectivamente. E portanto $gr(f) = gr(g) = 5$. Perceba que $a_5 + b_5 = 0$ em $\mathbb{Z}_{11}$, sendo assim $gr(f+g) \neq gr(f) = gr(g) = 5$. De fato, $gr(f+g) = gr(3x^3 + 5x^2 + 8x + 8) = 3$.

- Quanto ao grau do produto $f(x) \cdot g(x)$, temos $c_{5+5} = a_5 \cdot b_5 \Rightarrow c_{10} = 6$. Como c_{10} é o coeficiente líder de $f(x).g(x)$ então $gr(f \cdot g) = 10$. Fazendo a verificação, obtemos: $gr(f \cdot g) = gr(6x^{10} + x^8 + 9x^7 + x^6 + 7x^5 + 2x^4 + 4x^3 + 6x^2 + 6x + 2) = 10$.

2.2 Divisibilidade em $\mathbb{Z}_p[x]$

Definição 2.2.1. Sejam $f(x)$ e $g(x)$ polinômios em $\mathbb{Z}_p[x]$, com $f(x) \neq 0$. Dizemos que $g(x)$ é divisível por $f(x)$ ou $f(x)$ divide $g(x)$ se, e somente se, existe $k(x) \in \mathbb{Z}_p[x]$, tal que

$g(x) = k(x) \cdot f(x)$.
Notação: $f(x)|g(x)$ (lê-se: $f(x)$ divide $g(x)$).
Ou seja, em símbolos

$$f(x)|g(x) \Leftrightarrow \exists k(x) \in \mathbb{Z}_p[x], \text{tal que } g(x) = k(x) \cdot f(x).$$

Exemplo 2.2.2. O polinômio $g(x) = 6x^2 + 4x + 1$ divide $f(x) = 2x^5 + 6x^4 + 4x^2 + 5x + 3$ em $\mathbb{Z}_7[x]$, pois

$$f(x) = 2x^5 + 6x^4 + 4x^2 + 5x + 3 = (5x^3 + 3) \cdot (6x^2 + 4x + 1) = k(x) \cdot g(x)$$

, onde $k(x) = 5x^3 + 3 \in \mathbb{Z}_7[x]$.

Proposição 2.2.1. *Seja $f(x) = a_0$ um polinômio constante em $\mathbb{Z}_p[x]$, com $a_0 \in \mathbb{Z}_p - \{0\}$. $f(x)$ divide $g(x)$ qualquer que seja $g(x) \in \mathbb{Z}_p[x]$.*

Demonstração. De fato, existe $a_0^{-1} \in \mathbb{Z}_p$, tal que $a_0^{-1} \cdot a_o = 1$, já que a_0 é invertível em $\mathbb{Z}_p$. Tomemos $k(x) = a_0^{-1} g(x) \in \mathbb{Z}_p[x]$. Sendo assim temos:

$$g(x) = 1 \cdot g(x) = (a_0 \cdot a_0^{-1}) \cdot g(x) = a_0 \cdot a_0^{-1} g(x) = f(x) \cdot k(x)$$

qualquer que seja $g(x) \in \mathbb{Z}_p[x]$. □

Observação 3. Os polinômios não nulos que admitem inverso multiplicativo em $\mathbb{Z}_p[x]$ têm grau 0. De fato, seja $f(x) \in \mathbb{Z}_p[x]$ invertível em $\mathbb{Z}_p[x]$, ou seja, existe um polinômio não nulo $g(x) \in \mathbb{Z}_p[x]$, tal que $f(x) \cdot g(x) = 1$. Observe que $gr(f) + gr(g) = gr(1)$ o que implica que $gr(f) = 0$.

Segue da observação que $(\mathbb{Z}_p[x])^* = \mathbb{Z}_p - \{0\}$, onde $(\mathbb{Z}_p[x])^*$ indica o conjunto dos elementos invertíveis de $\mathbb{Z}_p[x]$

Proposição 2.2.2. *Sejam $f(x)$, $g(x)$ e $h(x)$ polinômios em $\mathbb{Z}_p[x]$ não nulos. São válidas as seguintes propriedades:*

1. *$f(x)|f(x)$;*
2. *Se $f(x)|g(x)$ e $g(x)|h(x)$, então $f(x)|h(x)$;*
3. *Se $f(x)|g(x)$ e $f(x)|h(x)$, então $f(x)|(g(x) \cdot k_1(x) + h(x) \cdot k_2(x))$ quaisquer que sejam os polinômios $k_1(x), k_2(x) \in \mathbb{Z}_p[x]$;*
4. *Se $f(x)|g(x)$, então $\alpha \cdot f(x)|g(x)$, qualquer que seja a constante $\alpha \in \mathbb{Z}_p$, com $\alpha \neq 0$;*
5. *Se $f(x)|g(x)$, então $f(x)|g(x) \cdot h(x)$, qualquer que seja $h(x) \in \mathbb{Z}_p[x]$;*

6. *Se* $f(x)|g(x)$ *e* $g(x)|f(x)$*, então* $f(x) = \alpha \cdot g(x)$*, onde* $\alpha \in \mathbb{Z}_p$.

Demonstração. 1. Basta tomarmos $k(x) = 1 \in \mathbb{Z}_p[x]$, temos que $f(x) = 1 \cdot f(x) = k(x) \cdot f(x)$. E portanto, fica demonstrada a reflexividade na divisão de polinômios em $\mathbb{Z}_p[x]$.

2. Da hipótese, temos que existem $q_1(x), q_2(x) \in \mathbb{Z}_p[x]$, tais que $g(x) = q_1(x) \cdot f(x)$ e $h(x) = q_2(x) \cdot g(x)$, assim podemos reescrever $h(x)$ como:

$$h(x) = q_2(x) \cdot g(x) = q_2(x) \cdot q_1(x) f(x) = (q_2(x) q_1(x)) \cdot f(x)$$

Logo, $f(x)|h(x)$. E portanto é válida a propriedade transitiva na divisão de polinômios em $\mathbb{Z}_p[x]$.

3. Da hipótese, segue que existem $q_1(x), q_2(x) \in \mathbb{Z}_p[x]$, tais que $g(x) = q_1(x) \cdot f(x)$ e $h(x) = q_2(x) \cdot f(x)$, dessa forma temos:

$$g(x) \cdot k_1(x) + h(x) \cdot k_2(x) = q_1(x) f(x) \cdot k_1(x) + q_2(x) f(x) \cdot k_2(x) = f(x) \cdot (q_1 k_1 + q_2 k_2)$$

Portanto, $f(x)|(g(x) \cdot k_1(x) + h(x) \cdot k_2(x))$ quaisquer que sejam os polinômios $k_1(x), k_2(x) \in \mathbb{Z}_p[x]$.

4. Se $f(x)|g(x)$ então existe $q_1(x) \in \mathbb{Z}_p[x]$, tal que $g(x) = q_1(x) \cdot f(x)$, como $\alpha \in \mathbb{Z}_p - \{0\}$, então existe $\alpha^{-1} \in \mathbb{Z}_p$, tal que $\alpha \cdot \alpha^{-1} = 1$, sendo assim, basta fazermos:

$$g(x) = \alpha^{-1} q_1(x) \cdot \alpha f(x)$$

Ou seja, $\alpha \cdot f(x)|g(x)$.

5. Se $f(x)|g(x)$ então existe $q_1(x) \in \mathbb{Z}_p[x]$, tal que $g(x) = q_1(x) \cdot f(x)$, multiplicando ambos os membros dessa equação por qualquer que seja $h(x) \in \mathbb{Z}_p[x]$, obtemos:

$$g(x) \cdot h(x) = q_1(x) h(x) \cdot f(x)$$

E portanto, $f(x)|g(x) \cdot h(x)$.

6. Se $g(x)|f(x)$, então $f(x) = q_1(x) \cdot g(x)$, para algum $q_1(x) \in \mathbb{Z}_p[x]$. E de $f(x)|g(x)$, temos que $g(x) = q_2(x) \cdot f(x)$, para algum $q_2(x) \in \mathbb{Z}_p[x]$. Sendo assim, temos:

$$\begin{aligned} f(x) &= q_1(x) \cdot g(x) \\ &= q_1(x) \cdot q_2(x) f(x) \end{aligned}$$

Note que $gr(f) = gr(q_2) + gr(q_1) + gr(f)$, ou seja, $gr(q_1) = gr(q_2) = 0$ e $q_1(x) \in \mathbb{Z}_p$. Logo, $q_1(x) = \alpha$, com $\alpha \in \mathbb{Z}_p$. Portanto $f(x) = \alpha \cdot g(x)$.

□

Proposição 2.2.3. *Sejam $f(x), g(x) \in \mathbb{Z}_p[x]$, tal que $f(x) = a(x) + b(x)$, com $a(x), b(x) \in \mathbb{Z}_p[x]$. Se $g(x)|f(x)$ e $g(x)|a(x)$ então $g(x)|b(x)$.*

Demonstração. De fato, da hipótese segue que existem $q_1(x), q_2(x) \in \mathbb{Z}_p[x]$, tais que $f(x) = q_1(x)g(x)$ e $a(x) = q_2(x)g(x)$. Desta forma, temos:

$$f(x) = a(x) + b(x) \Rightarrow q_1(x)g(x) = q_2(x)g(x) + b(x) \Rightarrow b(x) = (q_1(x) - q_2(x))g(x)$$

E portanto, $g(x)|b(x)$. □

Definição 2.2.3. Seja $p(x) \in \mathbb{Z}_p[x]$. Os divisores triviais de $p(x)$ são os polinômios constantes não nulos e os polinômios da forma $\alpha \cdot p(x)$, com $\alpha \in \mathbb{Z}_p - \{0\}$.

Exemplo 2.2.4. Os divisores triviais de $p(x) = x^3 + 2x + 4 \in \mathbb{Z}_5[X]$ são: $1, 2, 3, 4$, $x^3 + 2x + 4, 2x^3 + 4x + 3, 3x^3 + x + 2, 4x^3 + 3x + 1$.

Teorema 2.2.4. *Para todo par de polinômios $c(x)$ e $d(x)$ em $\mathbb{Z}_p[x]$, ambos não nulos, existe um único par de polinômios $q(x)$ e $r(x)$ em $\mathbb{Z}_p[x]$, tais que*

$$c(x) = q(x) \cdot d(x) + r(x), \text{ com } gr(r) < gr(d) \text{ ou } r(x) = 0,$$

onde $q(x)$ e $r(x)$ são chamados,respectivamente, de quociente e resto.

Demonstração. Existência

Considere $c(x) = a_n x^n + \cdots + a_1 x + a_0$ e $d(x) = b_m x^m + \cdots + b_1 x + b_0$, com $a_n \neq 0$ e $b_m \neq 0$, logo $gr(c) = n$ e $gr(d) = m$. Se $n < m$, então basta tomarmos $q(x) = 0$ e $r(x) = c(x)$. Observe ainda que $c(x) = 0 \cdot d(x) + c(x)$ e $gr(r) = gr(c) = n < m = gr(d)$.

Por outro lado, se $n \geqslant m$, então para prosseguirmos na demonstração iremos utilizar a Segunda Forma do Princípio de Indução [5, página 19], neste caso sobre o $gr(c) = n$.

Se $n = 0$, então temos que $c(x) = a_0$. Como $m \leqslant n = 0$, então $m = 0$ e $d(x) = b_0$, com $a_0, b_0 \in \mathbb{Z}_p - \{0\}$. Nestas condições segue que existe $b_0^{-1} \in \mathbb{Z}_p \subset \mathbb{Z}_p[x]$, tal que $b_o^{-1} \cdot b_0 = 1$, já que $\mathbb{Z}_p$ é corpo. Sendo assim, tomamos $q(x) = a_0 b_0^{-1}$ e $r(x) = 0$ e obtemos $c(x) = a_0 b_0^{-1} \cdot b_0 + 0 = q(x) \cdot d(x) + r(x)$.

Supondo que o teorema é válido para todo $0 \leqslant k < n$, onde $k = gr(h)$ e $h(x) \neq 0$. Então por hipótese de indução segue que existem $q_1(x)$ e $r_1(x)$ pertencentes a $\mathbb{Z}_p[x]$, tais que $h(x) = q_1(x) \cdot d(x) + r_1(x)$, com $r_1(x) = 0$ ou $gr(r_1) < gr(d)$.

Considere o polinômio:

$$c(x) = a_n b_m^{-1} x^{n-m} \cdot d(x) + h(x)$$

com $gr(c) = n > gr(h)$.

Observe que

$$\begin{aligned} c(x) &= a_n b_m^{-1} x^{n-m} \cdot d(x) + h(x) \\ &= a_n b_m^{-1} x^{n-m} \cdot d(x) + q_1(x) \cdot d(x) + r_1(x) \\ &= (a_n b_m^{-1} x^{n-m} + q_1(x)) \cdot d(x) + r_1(x) \end{aligned}$$

Portanto, basta tomarmos $q(x) = a_n b_m^{-1} x^{n-m} + q_1(x)$ e $r(x) = r_1(x)$, provando assim a existência dos polinômios $q(x)$ e $r(x)$, tais que $c(x) = q(x) \cdot d(x) + r(x)$, com $r(x) = 0$ ou $gr(r) < gr(d)$.

Unicidade

Vamos supor que existem $q_1(x), q_2(x), r_1(x), r_2(x) \in \mathbb{Z}_p[x]$, tais que $c(x) = q_1(x) \cdot d(x) + r_1(x) = q_2(x) \cdot d(x) + r_2(x)$, com $r_1 = 0$ ou $gr(r_1) < gr(d)$ e $r_2 = 0$ ou $gr(r_2) < gr(d)$.

Queremos provar que $q_1 = q_2$ e $r_1 = r_2$. Temos que $q_1(x) \cdot d(x) + r_1(x) = q_2(x) \cdot d(x) + r_2(x)$, ou seja,

$$(q_1(x) - q_2(x)) \cdot d(x) = r_2(x) - r_1(x) \tag{2.1}$$

Da hipótese, temos que $d(x) \neq 0$, além disso, vamos supor $q_1(x) - q_2(x) \neq 0$, ou seja, $r_1(x) \neq r_2(x)$. Portanto, da equação 2.1 segue que $q_1(x) \neq q_2(x)$.

Observe que $gr(r_2 - r_1) \leqslant max\{gr(r_1), gr(r_2)\} < gr(d)$. Enquanto $gr((q_1(x) - q_2(x)) \cdot d(x)) = gr(q_1(x) - q_2(x)) + gr(d) \geqslant gr(d)$. O que é uma contradição.

Logo,devemos ter $q_1 = q_2$ e consequentemente $r_1 = r_2$, ou seja, é único o par de polinômios $q(x)$ e $r(x)$ em $\mathbb{Z}_p[x]$, tais que $c(x) = q(x) \cdot d(x) + r(x)$, onde $gr(r) < gr(d)$ ou $r(x) = 0$. □

Exemplo 2.2.5. Considere os polinômios $c(x) = x^6 - x^5 + x^4 - x + 1$ e $d(x) = x^3 - x^2$ em $\mathbb{Z}_2[x]$. Determinemos os polinômios quociente e resto em $\mathbb{Z}_2[x]$. Para tal, façamos:

$$
\begin{array}{r|l}
x^6 - x^5 + x^4 + 0x^3 + 0x^2 - x + 1 & x^3 - x^2 \\
\cline{2-2}
-x^6 + x^5 & x^3 + x + 1 \\
\cline{1-1}
0x^6 + 0x^5 + x^4 + 0x^3 + 0x^2 - x + 1 & \\
-x^4 + x^3 & \\
\cline{1-1}
0x^4 + x^3 + 0x^2 - x + 1 & \\
-x^3 + x^2 & \\
\cline{1-1}
x^2 - x + 1 &
\end{array}
$$

Portanto, temos que $x^6 - x^5 + x^4 - x + 1 = (x^3 + x + 1) \cdot (x^3 - x^2) + x^2 - x + 1$. Ou seja, $q(x) = x^3 + x + 1$ e $r(x) = x^2 - x + 1$, são respectivamente, o quociente e o resto procurados.

2.3 O MDC entre polinômios

Definição 2.3.1. Dados $f(x), g(x) \in \mathbb{Z}_p[x]$, ambos não simultaneamente nulos. Dizemos que $d(x) \in \mathbb{Z}_p[x]$ é o Máximo Divisor Comum de $f(x)$ e $g(x)$ e denotamos por $MDC(f(x), g(x)) = d(x)$ se:

1. $d(x)$ é mônico;
2. $d(x)|f(x)$ e $d(x)|g(x)$;
3. Se existe $k(x) \in \mathbb{Z}_p[x]$, tal que $k(x)|f(x)$ e $k(x)|g(x)$, então $k(x)|d(x)$ e $gr(k) \leqslant gr(d)$.

Observação 4. Se $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}_p[x]$, com $a_n \neq 0$, então $gr(p) = n$ e além disso,

$$p(x) = a_n \cdot (x_n + \cdots + a_n^{-1} a_1 x + a_n^{-1} a_0),$$

com os coeficientes $a_n, \cdots, a_1, a_0 \in \mathbb{Z}_p$. Sendo assim, concluímos que todo polinômio não nulo está associado a um único polinômio mônico. Ou seja, $p(x) = a_n \cdot m(x)$, onde $m(x) = x_n + \cdots + a_n^{-1} a_1 x + a_n^{-1} a_0$. Observe que, necessariamente, $a_n \neq 0$ e $p(x) = a_n \cdot m(x) \Leftrightarrow a_n^{-1} \cdot p(x) = m(x)$.

O fato do MDC ser um polinômio mônico, garante sua unicidade. De fato, supondo $MDC(f(x), g(x)) = d_1(x) = d_2(x)$, temos que $d_1(x)|d_2(x)$, também $d_2(x)|d_1(x)$, logo do item 6 da proposição 2.2.2 segue que $d_1(x) = \alpha d_2(x)$, com $\alpha \in \mathbb{Z}_p$. Porém como ambos são mônicos devemos ter $\alpha = 1$ e portanto $d_1(x) = d_2(x)$.

2.3.2 O Algoritmo de Euclides no Anel $\mathbb{Z}_p[x]$

Teorema 2.3.1. *Dados dois polinômios $s(x)$ e $r(x)$ em $\mathbb{Z}_p[x]$, tais que $gr(s) \geqslant gr(r) \geqslant 0$. Considere a seguinte sucessão de divisões:*

$$\begin{aligned} s(x) &= q_1(x) \cdot r(x) + r_1(x) \\ r(x) &= q_2(x) \cdot r_1(x) + r_2(x) \\ r_1(x) &= q_3(x) \cdot r_2(x) + r_3(x) \\ &\vdots \\ r_{n-2}(x) &= q_n(x) \cdot r_{n-1}(x) + r_n(x) \\ r_{n-1}(x) &= q_{n+1}(x) \cdot r_n(x) \end{aligned}$$

Onde o processo para quando for obtido o resto zero. Então $r_n(x) = \alpha \cdot MDC(s(x), r(x))$, onde $\alpha \in \mathbb{Z}_p$.

Demonstração. Seja $d(x) = MDC(s(x), r(x))$, ou seja, $d(x)|s(x)$ e $d(x)|r(x)$. Note que:

$$s(x) = q_1(x) \cdot r(x) + r_1(x) \Rightarrow r_1(x) = s(x) - q_1(x) \cdot r(x)$$

Do item 3. da proposição 2.2.2, segue que $d(x)|r_1(x)$. Mas se $d(x)|r(x)$ e $d(x)|r_1(x)$, então $d(x)|r_2(x) = r(x) - q_2(x) \cdot r_1(x)$. Prosseguindo com esse mesmo raciocínio, temos que $d(x)|r_n(x)$.

Observe que:

$$r_{n-1}(x) = q_{n+1}(x) \cdot r_n(x) \Rightarrow r_n(x)|r_{n-1(x)}$$

E ainda,

$$\begin{aligned} r_{n-2}(x) &= q_n(x) \cdot r_{n-1}(x) + r_n(x) \\ &= q_n(x) \cdot q_{n+1}(x) r_n(x) + r_n(x) \\ &= (q_n(x) q_{n+1}(x) + 1) \cdot r_n(x) \end{aligned}$$

Ou seja, $r_n(x)|r_{n-2}(x)$. Prosseguindo com esse processo, concluímos que $r_n(x)|r(x)$ e $r_n(x)|s(x)$, mas como $d(x) = MDC(s(x), r(x))$, então $r_n(x)|d(x)$.
Portanto, segue do item 6. da proposição 2.2.2 que $r_n(x) = \alpha \cdot MDC(s(x), r(x))$, onde $\alpha \in \mathbb{Z}_p$. □

A seguir vamos apresentar alguns exemplos e como encontrar o MDC de dois polinômios dados.

Exemplo 2.3.3. 1. Sejam $f(x) = x^4 + x^3 + 3x^2 + 4x + 1$ e $g(x) = x^3 + 2x^2 + 4x + 3$ em $\mathbb{Z}_5[x]$. Temos que:

$$f(x) = (x+4) \cdot g(x) + (x^2+4)$$
$$g(x) = (x^2+4)(x+2) + 0$$

Logo, $MDC(f(x), g(x)) = x^2 + 4$.

2. Sejam $f(x) = 3x^5 + x^3 + 3x + 3$ e $g(x) = 2x^3 + x$ em $\mathbb{Z}_5[x]$. Temos que:

$$f(x) = (4x^2+1) \cdot g(x) + (2x+3)$$
$$g(x) = (x^2+x) \cdot (2x+3) + 3x$$
$$2x+3 = (4) \cdot 3x + 3$$
$$3x = (x) \cdot (3) + 0$$

Logo, $r_3(x) = 3$ é o último resto não nulo, e portanto $MDC(f(x), g(x)) = 3^{-1} \cdot 3 = 1$.

3. Sejam $p(x) = x^3 + 1$ e $g(x) = 2x^2 + 2$ polinômios de $\mathbb{Z}_3[x]$. Temos que:

$$p(x) = 2x \cdot g(x) + (2x+1)$$
$$g(x) = (x+1) \cdot (2x+1) + 1$$
$$2x+1 = (2x+1) \cdot 1 + 0$$

Portanto, o último resto não nulo das sucessivas divisões é 1, ou seja, $MDC(p(x), g(x)) = 1$.

Definição 2.3.4. Dados dois polinômios $f(x)$ e $g(x)$ em $\mathbb{Z}_p[x]$, tais que $MDC(f(x), g(x)) = 1$. Então dizemos que $f(x)$ e $g(x)$ são primos entre si.

Teorema 2.3.2. *O máximo divisor comum $d(x)$ de dois polinômios, não simultaneamente nulos, $f(x)$ e $g(x)$ em $\mathbb{Z}_p[x]$ existe. E além disso, existe $\lambda(x)$, $\mu(x) \in \mathbb{Z}_p[x]$, tais que:*

$$d(x) = \lambda(x) \cdot f(x) + \mu(x) \cdot g(x).$$

Demonstração. Considere o conjunto $S = \{\lambda(x) \cdot f(x) + \mu(x) \cdot g(x) \mid \quad \lambda(x), \mu(x) \in \mathbb{Z}_p[x]\}$. Seja $d(x) \in S$ o polinômio mônico de menor grau, note que $d(x) = \lambda(x) \cdot f(x) + \mu(x) \cdot g(x)$, para convenientes $\lambda(x), \mu(x) \in \mathbb{Z}_p[x]$.

Do teorema 2.2.4, segue que existem $q_1(x), r_1(x) \in \mathbb{Z}_p[x]$, tais que $f(x) = q_1(x) \cdot d(x) + r_1(x)$, com $r_1(x) = 0$ ou $gr(r_1) < gr(d)$. Observe que:

$$f(x) = q_1(x) \cdot (\lambda(x) \cdot f(x) + \mu(x) \cdot g(x)) + r_1(x) \Rightarrow$$

$$r_1(x) = (1 - q_1(x)\lambda(x)) \cdot f(x) - (q_1(x)\mu(x)) \cdot g(x) \Rightarrow r_1(x) \in S$$

Sendo assim, temos que $r_1(x) = 0$, já que $r_1(x) \in S$ e $gr(d)$ é o menor em S. Logo, $f(x) = q_1(x) \cdot d(x)$, ou seja, $d(x)|f(x)$.

De modo análogo, fazendo a divisão de $g(x)$ por $d(x)$, concluímos que $g(x) = q_2(x) \cdot d(x)$, com $q_2(x) \in \mathbb{Z}_p[x]$, ou seja, $d(x)|g(x)$.

Supondo que exista $k(x) \in \mathbb{Z}_p[x]$, tal que $k(x)|f(x)$ e $k(x)|g(x)$, então $k(x)|d(x)$. De fato, o terceiro item da proposição 2.2.2 nos garante.

Portanto $d(x)$ satisfaz as condições da definição 2.3.1 e $MDC(f(x), g(x)) = d(x)$. □

Proposição 2.3.3. *Sejam $f(x)$ e $g(x)$ polinômios de $\mathbb{Z}_p[x]$.*

$$MDC(f(x), g(x)) = 1 \Leftrightarrow \exists \lambda(x), \mu(x) \in \mathbb{Z}_p[x], \textit{tais que } \lambda(x) \cdot f(x) + \mu(x) \cdot g(x) = 1.$$

Demonstração. Se $MDC(f(x), g(x)) = 1$, então pelo teorema 2.3.2 segue que existem $\lambda(x), \mu(x) \in \mathbb{Z}_p[x]$, tais que $\lambda(x)f(x) + \mu(x) \cdot g(x) = 1$

Por outro lado, se existem $\lambda(x), \mu(x) \in \mathbb{Z}_p[x]$, tais que $\lambda(x)f(x) + \mu(x) \cdot g(x) = 1$, então seja $d(x) = MDC(f(x), g(x))$. Pelo item 3 da proposição 2.2.2, segue que $d(x)|1$, logo devemos ter $d(x) = 1$.

Portanto, $MDC(f(x), g(x)) = 1$. □

Proposição 2.3.4. *Sejam $f(x), g(x)e\ h(x)$ polinômios de $\mathbb{Z}_p[x]$. Se $f(x)|g(x) \cdot h(x)$ e $MDC(f(x), g(x)) = 1$, então $f(x)|h(x)$.*

Demonstração. Como $MDC(f(x), g(x)) = 1$, então pela proposição 2.3.3 segue que existem $\lambda(x), \mu(x) \in \mathbb{Z}_p[x]$, tais que $\lambda(x) \cdot f(x) + \mu(x) \cdot g(x) = 1$. Multiplicando ambos os membros da equação anterior por $h(x)$ obtemos:

$$h(x)\lambda(x)f(x) + h(x)\mu(x)g(x) = h(x)$$

Sendo assim, temos que $f(x)|f(x)$ e portanto do item 5. da proposição 2.2.2 segue que $f(x)|h(x)\lambda(x)f(x)$. Além disso, por hipótese $f(x)|g(x)h(x)$, desta forma segue que $f(x)|h(x)\mu(x)g(x)$.

Portanto o item 3. da proposição 2.2.2 nos garante que $f(x)|h(x)\lambda(x)f(x)+h(x)\mu(x)g(x)$, ou seja, $f(x)|h(x)$. □

2.4 Polinômios irredutíveis

O conceito de polinômios irredutíveis em $\mathbb{Z}_p[x]$ se assimila aos números primos no conjunto dos números inteiros $\mathbb{Z}$. Da mesma forma é possível estabelecer em $\mathbb{Z}_p[x]$ um algoritmo euclidiano. Nesta seção iremos apresentar alguns resultados relacionados a esse tópico.

Definição 2.4.1. Dizemos que $u \in \mathbb{Z}_p$ é raiz de um polinômio $p(x) \in \mathbb{Z}_p[x]$ se $p(u) = 0$.

Exemplo 2.4.2. Seja $p(x) = x^2 + x + 3 \in \mathbb{Z}_5[X]$. Temos que $u = 3$ é raiz de $p(x)$. Pois

$$p(3) = 3^2 + 3 + 3 = 0.$$

Definição 2.4.3. Seja $f(x) \in \mathbb{Z}_p[x]$. Dizemos que $f(x)$ tem um fator de grau 1 em $\mathbb{Z}_p[x]$ se $f(x) = (\alpha x + \beta) \cdot g(x)$, onde $\alpha, \beta \in \mathbb{Z}_p$, com $\alpha \neq 0$ e $g(x) \in \mathbb{Z}_p[x]$.

Teorema 2.4.1. *Seja $f(x) \in \mathbb{Z}_p[x]$. $f(x)$ possui um fator de grau 1 em $\mathbb{Z}_p[x]$ se, e somente se, $f(x)$ tem uma raiz em $\mathbb{Z}_p$.*

Demonstração. ($\Rightarrow$) Se $f(x)$ tem fator de grau 1, então seja $f(x) = (\alpha x + \beta) \cdot g(x)$, com $\alpha, \beta \in \mathbb{Z}_p$ e $g(x) \in \mathbb{Z}_p[x]$. Como $\mathbb{Z}_p$ é corpo e α é necessariamente diferente de zero, segue que $-\beta\alpha^{-1} \in \mathbb{Z}_p \subset \mathbb{Z}_p[x]$ é raiz de f. De fato,

$$f(-\beta\alpha^{-1}) = (\alpha(-\beta\alpha^{-1}) + \beta) \cdot g(-\beta\alpha^{-1}) = 0.$$

($\Leftarrow$) Seja $\alpha \in \mathbb{Z}_p$ uma raiz de $f(x)$. Do teorema 2.2.4, segue que existem $q(x), r(x) \in \mathbb{Z}_p[x]$, tais que:

$$f(x) = q(x)(x - \alpha) + r(x), \text{ com } r(x) = 0 \text{ ou } gr(r) < gr(x - \alpha) = 1.$$

Sendo assim, considere $r(x) = c$, com $c \in \mathbb{Z}_p$. Observe que:

$$0 = f(\alpha) = q(\alpha)(\alpha - \alpha) + c = c$$

Logo, $f(x) = q(x)(x - \alpha)$, ou seja, $f(x)$ tem um fator de grau 1. □

O resultado acima nos mostra que se α é raiz do polinômio $f(x)$, então necessariamente $x - \alpha$ é um divisor de $f(x)$.

Corolário 2.4.2. *Seja $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}_p[x]$, com $a_n \neq 0$. Se $u_1, u_2, \cdots, u_m$ são raízes de f, então:*

$$f(x) = (x - u_1)(x - u_2) \cdots (x - u_m) \cdot q_m(x),$$

onde $q_m(x) \in \mathbb{Z}_p[x]$ e $gr(q_m) = n - m$. Além disso, outras eventuais raízes de f são raízes de q_m.

Demonstração. Caso o leitor queira ver uma demonstração sugerimos [4, página 286]. □

Proposição 2.4.3. *Seja $f(x) \in \mathbb{Z}_p[x]$, um polinômio não nulo, com $gr(f) = n$. Então $f(x)$ tem no máximo n raízes em $\mathbb{Z}_p$.*

Demonstração. Caso o leitor queira ver uma demonstração sugerimos [3, página 27]. □

Definição 2.4.4. Seja $p(x) \in \mathbb{Z}_p[x]$, com $gr(p) \geqslant 1$. Dizemos que $p(x)$ é *irredutível* em $\mathbb{Z}_p[x]$ se $p(x) = a(x) \cdot b(x)$ implicar que $a(x)$ ou $b(x)$ é um polinômio constante em $\mathbb{Z}_p[x]$. Caso contrário, dizemos que $p(x)$ é *redutível*.

Exemplo 2.4.5. O polinômio $p(x) = x^3 + x + 1$ é irredutível em $\mathbb{Z}_5[x]$. De fato, supondo $p(x)$ redutível, então temos que $p(x) = a(x)b(x)$, com $a(x), b(x) \in \mathbb{Z}_p[x]$ e $gr(a), gr(b) \neq 0$. Observe que $gr(p) = 3 = gr(a) + gr(b)$, por simplicidade, vamos nos ater ao caso em que $gr(a) = 1$ e $gr(b) = 2$. Ou seja, $p(x)$ tem fator de grau 1 e do teorema 2.4.1, segue que $p(x)$ tem raiz em $\mathbb{Z}_5[x]$.

No entanto, fazendo os testes das possíveis raízes de $p(x)$ que seriam $0, 1, 2, 3$ ou 4, notamos que nenhuma delas o são, o que é um absurdo. Portanto, devemos ter que $p(x)$ é um polinômio irredutível em $\mathbb{Z}_5[x]$.

Observe que um polinômio $p(x) \in \mathbb{Z}_p[x]$, com $gr(p) \geqslant 1$ é irredutível se seus únicos divisores em $\mathbb{Z}_p[x]$ são os triviais. Caso haja mais divisores, temos que $p(x)$ é um polinômio redutível em $\mathbb{Z}_p[x]$.

Se ainda, $p(x) = a(x) \cdot b(x) \in \mathbb{Z}_p[x]$ é irredutível e $a(x)$ é constante, então $b(x)$ também é irredutível. De fato, pois caso $b(x)$ fosse redutível então teríamos $b(x) = a'(x) \cdot b'(x)$, com $a'(x), b'(x) \in \mathbb{Z}_p[x]$ e $0 < gr(a'), gr(b') < gr(b)$. Desta forma, $p(x) = a(x)a'(x) \cdot b'(x)$, com $0 < gr(aa'), gr(b') < gr(p)$, o que é um absurdo, já que $p(x)$ é por hipótese irredutível.

Proposição 2.4.4. *Sejam $f(x), a(x) \in \mathbb{Z}_p[x]$, onde $f(x)$ é irredutível. Se $f(x) \nmid a(x)$, então $MDC(f(x), a(x)) = 1$.*

Demonstração. Seja $d(x) = MDC(f(x), a(x))$, da definição de MDC segue que $d(x)|a(x)$ e $d(x)|f(x)$, mas como $f(x)$ é irredutível, então $gr(d) = 0$ ou $gr(d) = gr(f)$. Vamos supor $gr(d) = gr(f)$, então $f(x) = \alpha d(x)$, com $\alpha \in \mathbb{Z}_p$, segue do item 4 da proposição 2.2.2 que $\alpha d(x) = f(x)|a(x)$, o que é um absurdo, já que por hipótese $f(x) \nmid a(x)$. Sendo assim, devemos ter $gr(d) = 0$ e como $d(x)$ é mônico então $d(x) = MDC(f(x), a(x)) = 1$. □

Proposição 2.4.5. *Sejam $f(x), a(x), b(x) \in \mathbb{Z}_p[x]$, onde $f(x)$ é irredutível. Se $f(x)|a(x)b(x)$, então $f(x)|a(x)$ ou $f(x)|b(x)$.*

Demonstração. Vamos supor que $f(x) \nmid a(x)$, então da proposição acima segue que $MDC(f(x), a(x)) = 1$ e ainda da proposição 2.3.3 temos que existem $\lambda(x), \mu(x) \in \mathbb{Z}_p[x]$, tais que $\lambda(x)f(x) + \mu(x)a(x) = 1$. Observe que

$$\lambda(x)f(x) + \mu(x)a(x) = 1$$
$$b(x)\lambda(x)f(x) + b(x)\mu(x)a(x) = b(x)$$

E como $f(x)|b(x)\lambda(x)f(x)$ e $f(x)|b(x)\mu(x)a(x)$, então do item 3 da proposição 2.2.2 segue que $f(x)|b(x)$. □

Proposição 2.4.6. *Seja $p(x) \in \mathbb{Z}_p[x]$. Se $gr(p) = 1$, então $p(x)$ é irredutível.*

Demonstração. Seja $p(x) = a(x) \cdot b(x)$, com $a(x), b(x) \in \mathbb{Z}_p[x]$. Note que $gr(a) + gr(b) = gr(p) = 1$, sendo assim, temos que $gr(a) = 0$ e $gr(b) = 1$ ou vice e versa. Desta forma, sem perda de generalidade, tomemos $gr(a) = 0$, então $a(x)$ é constante e portanto $p(x)$ é irredutível. □

Proposição 2.4.7. *Seja $f(x) \in \mathbb{Z}_p[x]$, com $gr(f) = 2$ ou $gr(f) = 3$. Então $f(x)$ é redutível em $\mathbb{Z}_p[x]$ se, e somente se $f(x)$ possui raiz em $\mathbb{Z}_p[x]$.*

Demonstração. ($\Rightarrow$) Se grau de $f(x)$ igual a 2 ou 3, então supondo $f(x)$ redutível e $f(x) = a(x)b(x)$, com $a(x), b(x) \in \mathbb{Z}_p[x]$, como a soma dos graus de $a(x)$ e $b(x)$ deve ser igual a 2 ou 3 segue que pelos menos um dos polinômios deve ter grau 1. Do teorema 2.4.1, segue que este deve ter raiz em $\mathbb{Z}_p[x]$ e consequentemente $f(x)$ tem raiz em $\mathbb{Z}_p[x]$.
($\Leftarrow$) Se $f(x)$ tem raiz em em $\mathbb{Z}_p[x]$, então pelo teorema 2.4.1 $f(x)$ tem fator de grau 1 e consequentemente $f(x)$ é redutível em $\mathbb{Z}_p[x]$. □

Um interessante resultado em $\mathbb{Z}_p[x]$, similar ao Teorema Fundamental da Aritmética nos inteiros é o que segue:

Teorema 2.4.8. *Seja $p(x) = p_n x^n + \cdots + p_1 x + p_0$ um polinômio de grau n em $\mathbb{Z}_p[x]$, com $n \geqslant 1$. Então $p(x)$ se fatora de forma única (a menos da ordem dos fatores) como um produto de um $\alpha \in \mathbb{Z}_p$ vezes um produto de polinômios irredutíveis e mônicos.*

Demonstração. Existência

Para tal, vamos utilizar a Segunda Forma do Princípio de Indução [5, página 19], neste caso sobre o $gr(p) = n$.

Se $n = 1$, então a proposição 2.4.6 nos garante que o próprio $p(x) = p_1 x + p_0$ já é irredutível, sendo assim, basta tomarmos $\alpha = p_1$ e reescrevermos $p(x) = \alpha \cdot (x + \alpha^{-1} p_0)$, com $\alpha \in \mathbb{Z}_p$ e $x + \alpha^{-1} p_0$ é irredutível e mônico.

Supondo que o teorema seja válido, para todo $gr(p) = k$, com $0 < k < n$, então considere o polinômio $p(x) \in \mathbb{Z}_p[x]$, com $gr(p) = n$. Se $p(x)$ irredutível, então segue que $p(x) = \alpha_1 g(x)$, com $\alpha_1 \in \mathbb{Z}_p$ e $g(x) = g_n x^n + \cdots + g_0$, sendo assim, tomando $\alpha = \alpha_1 g_n$ e $g'(x) = x^n + \cdots + g_n^{-1} g_1 x + g_n^{-1} g_0$ obtemos $p(x) = \alpha g'(x)$ com $g'(x)$ irredutível e mônico.

Se por outro lado $p(x)$ é redutível, então $p(x) = f(x) \cdot g(x)$, com $f(x), g(x) \in \mathbb{Z}_p[x]$ e $0 < gr(f), gr(g) < n$. Sendo assim, por hipótese de indução segue que $f(x)$ e $g(x)$ se fatoram de forma única como segue:

$$f(x) = \alpha_1 a_1(x) a_2(x) \cdots a_r(x) \text{ e } g(x) = \alpha_2 a_{r+1}(x) \cdots a_l(x),$$

com $a_1, \alpha_2 \in \mathbb{Z}_p$ e os polinômios $a_i(x)$ irredutíveis e mônicos, com $i = 1, 2, \cdots, l$.

Observe que $\alpha_1 \cdot \alpha_2 \in \mathbb{Z}_p$, já que $\mathbb{Z}_p$ é corpo, considere então $\alpha = \alpha_1 \cdot \alpha_2$. Desta forma, concluímos:

$$p(x) = \alpha a_1(x)a_2(x)\cdots a_r(x)a_{r+1}(x)\cdots a_l(x)$$

, com $\alpha \in \mathbb{Z}_p$ e os polinômios $a_i(x)$ irredutíveis e mônicos, com $i = 1, 2, \cdots, l$.
Unicidade
A unicidade decorre da proposição 2.4.5. Basta supor

$$p(x) = \alpha_1 a_1(x)\cdots a_r(x) = \alpha_2 b_1(x)\cdots b_s,$$

com $r \leqslant s$, $\alpha_1, \alpha_2 \in \mathbb{Z}_p$, onde $a_i(x)$ e $b_i(x)$ são mônicos e irredutíveis. Assim temos que $a_1(x)$ divide algum $b_i(x)$, vamos supor, sem perda de generalidade, que seja $b_1(x)$, sendo assim, $b_1(x) = u_1 a_1(x)$, no entanto como $a_1(x)$ e $b_1(x)$ são mônicos e irredutíveis, segue que $u_1 = 1$. Dividindo ambos os lados da igualdade por $a_1(x)$, obtemos:

$$\alpha_1 a_2(x)\cdots a_r(x) = \alpha_2 b_2(x)\cdots b_s(x)$$

Repetindo esse mesmo processo obtemos:

$$\alpha_1 = \alpha_2 b_{r+1}(x)\cdots b_s(x)$$

Mas se isso ocorre, então $r = s$. Logo os fatores $a_i(x)$ e $b_i(x)$ mônicos e irredutíveis são os mesmos a menos da ordem e $\alpha_1 = \alpha_2$.

□

CAPÍTULO 3

A aritmética dos restos no anel de polinômios $\mathbb{Z}_p[x]$

Neste capítulo faremos um breve estudo sobre a aritmética realizada com os restos da divisão de elementos de $\mathbb{Z}_p[x]$ por um polinômio $p(x) \in \mathbb{Z}_p[x]$.

3.1 Congruências

Definição 3.1.1. Sejam $p(x), q(x), s(x) \in \mathbb{Z}_p[x]$. Dizemos que $p(x)$ é congruente a $q(x)$ módulo $s(x)$, se $p(x)$ e $q(x)$ deixam o mesmo resto quando divididos por $s(x)$ e simbolizamos por:

$$p(x) \equiv q(x) \ mod \ s(x)$$

Lê-se: $p(x)$ é côngruo a $q(x)$ módulo $s(x)$.

Da definição segue direto as seguintes propriedades:

Proposição 3.1.1. *Sejam $m(x), p(x), q(x)$ e $t(x)$ polinômios em $\mathbb{Z}_p[x]$.*

1. *reflexiva: $p(x) \equiv p(x) \ mod \ m(x)$;*
2. *simétrica: $p(x) \equiv q(x) \ mod \ m(x) \Rightarrow q(x) \equiv p(x) \ mod \ m(x)$;*
3. *transitiva: $p(x) \equiv q(x) \ mod \ m(x)$ e $q(x) \equiv t(x) \ mod \ m(x) \Rightarrow p(x) \equiv t(x) \ mod \ m(x)$.*

Exemplo 3.1.2. Sejam os polinômios $p(x) = x^6 - x^5 + x^4 - x + 1$, $q(x) = x^3 - x^2$ e $q(x) = x^2 + x + 1$ em $\mathbb{Z}_2[x]$. Observe que:

$$p(x) = (x^3 + x + 1) \cdot m(x) + (x^2 + x + 1) \text{ e } q(x) = 0 \cdot m(x) + (x^2 + x + 1)$$

Portanto, $p(x) \equiv q(x) \bmod m(x)$.

O próximo resultado caracteriza o conceito de congruências por meio de divisibilidade no anel $\mathbb{Z}_p[x]$.

Proposição 3.1.2. *Sejam $p(x)$, $q(x)$ e $m(x)$ polinômios em $\mathbb{Z}_p[x]$. Então*

$$p(x) \equiv q(x) \ mod \ m(x) \Leftrightarrow m(x)|p(x) - q(x).$$

Demonstração. ($\Rightarrow$) Da hipótese segue que $p(x)$ e $q(x)$ deixam o mesmo resto quando divididos por $m(x)$. Desta forma, sejam $p(x) = q_1(x)m(x) + r(x)$ e $q(x) = q_2(x)m(x) + r(x)$, para algum $q_1(x), q_2(x), r(x) \in \mathbb{Z}_p[x]$, com $gr(r) < gr(m)$ ou $r(x) = 0$. Fazendo $p(x) - q(x)$ obtemos:

$$\begin{aligned} p(x) - q(x) &= q_1(x)m(x) + r(x) - q_2(x)m(x) - r(x) \\ &= (q_1(x) - q_2(x)) \cdot m(x) \end{aligned}$$

Logo, $m(x)|p(x) - q(x)$.
($\Leftarrow$) Do teorema 2.2.4, segue que existem $q_1(x), q_2(x), r_1(x), r_2(x) \in \mathbb{Z}_p[x]$ tais que:

$$p(x) = q_1(x)m(x) + r_1(x), \text{ com } gr(r_1) < gr(m) \text{ ou } r_1 = 0$$

e

$$q(x) = q_2(x)m(x) + r_2(x), \text{ com } gr(r_2) < gr(m) \text{ ou } r_2(x) = 0.$$

Fazendo $p(x) - q(x)$ obtemos:

$$p(x) - q(x) = (q_1(x) - q_2(x))m(x) + (r_1(x) - r_2(x)) \tag{3.1}$$

Queremos mostrar que $r_1(x) = r_2(x)$. Da hipótese segue que $m(x)|p(x) - q(x)$, além disso, $m(x)|(q_1(x) - q_2(x))m(x)$, sendo assim da equação 3.1 e da proposição 2.2.3 segue que $m(x)|r_1(x) - r_2(x)$.

Se $r_1(x) - r_2(x) \neq 0$, então existe $l(x) \in \mathbb{Z}_p[x]$, tal que $r_1(x) - r_2(x) = m(x) \cdot l(x)$. Sendo assim, $gr(r_1 - r_2) = gr(m) + gr(l) \geqslant gr(m)$. Por outro lado, temos que $gr(r_1 - r_2) \leqslant max\{gr(r_1), gr(r_2)\}$, no entanto $gr(r_1), gr(r_2) < gr(m)$, ou seja, $gr(r_1 - r_2) < gr(m)$, o que é um absurdo.

Logo, devemos ter $r_1(x) - r_2(x) = 0$, ou seja, $r_1(x) = r_2(x)$ e $p(x) \equiv q(x) \bmod m(x)$. □

Proposição 3.1.3. *Sejam $a(x), b(x), c(x), d(x), m(x) \in \mathbb{Z}_p[x]$. Se $a(x) \equiv b(x) \ mod \ m(x)$ e $c(x) \equiv d(x) \ mod \ m(x)$, então:*

1. $a(x) + c(x) \equiv b(x) + d(x) \ mod\ m(x)$;

2. $a(x) \cdot c(x) \equiv b(x) \cdot d(x) \ mod\ m(x)$.

Demonstração. 1. Como $a(x) \equiv b(x) \bmod m(x)$ e $c(x) \equiv d(x) \bmod m(x)$, segue da proposição 3.1.2 que $m(x)|b(x) - a(x)$ e $m(x)|d(x) - c(x)$. Sendo assim, $m(x)|(b(x) - a(x)) + (d(x) - c(x))$ (item 3. da proposição 2.2.2). Observe que :

$$(b(x) - a(x)) + (d(x) - c(x)) = (b(x) + d(x)) - (a(x) + c(x)),$$

Ou seja, $m(x)|(b(x) + d(x)) - (a(x) + c(x))$ e portanto $a(x) + c(x) \equiv b(x) + d(x) \bmod m(x)$.

2. Observe que $b(x)d(x) - a(x)c(x) = d(x)(b(x) - a(x)) + a(x)(d(x) - c(x))$. Como $m(x)|d(x)(b(x)-a(x))+a(x)(d(x)-c(x))$, então $m(x)|b(x)d(x)-a(x)c(x)$. Portanto $a(x) \cdot c(x) \equiv b(x) \cdot d(x) \bmod m(x)$.

□

Proposição 3.1.4. *Sejam $a(x), b(x), c(x), m(x) \in \mathbb{Z}_p[x]$ e $d(x) = MDC(c(x), m(x))$. Temos que*

$$a(x)c(x) \equiv b(x)c(x) \quad mod\, m(x) \Leftrightarrow a(x) \equiv b(x) \quad mod\, \frac{m(x)}{d(x)}.$$

Demonstração. Considere $t(x) = \dfrac{m(x)}{d(x)}$ e $z(x) = \dfrac{c(x)}{d(x)}$. Observe que $t(x)$ e $z(x)$ são relativamente primos, ou seja, $MDC(t(x), z(x)) = 1$. Além disso,

$$a(x)c(x) \equiv b(x)c(x) \quad mod\, m(x) \Leftrightarrow m(x)|a(x)c(x) - b(x)c(x)$$

Sendo assim, existe $k(x) \in \mathbb{Z}_p[x]$, tal que

$$\begin{aligned} a(x)c(x) - b(x)c(x) &= m(x)k(x) \Leftrightarrow \\ (a(x) - b(x))c(x) &= m(x)k(x) \Leftrightarrow \\ (a(x) - b(x))\frac{c(x)}{d(x)} &= \frac{m(x)}{d(x)}k(x) \Leftrightarrow \\ (a(x) - b(x))z(x) &= t(x)k(x) \end{aligned}$$

Como $MDC(t(x), z(x)) = 1$, então a igualdade acima ocorre se, e somente se, $t(x)|(a(x) - b(x))$. □

A proposição acima também é válida no conjunto dos inteiros, ou seja, dado $a, b, c, m \in \mathbb{Z}$, $m > 1$ e $d = mdc(c, m)$, então:

$$a \cdot c \equiv b \cdot c \bmod m \quad \Leftrightarrow \quad a \equiv b \bmod \frac{m}{d}.$$

CAPÍTULO 4

Corpos Finitos baseados no Anel de polinômios $\mathbb{Z}_p[x]$

Neste capítulo faremos uma introdução a corpos finitos baseados no anel de polinômios $\mathbb{Z}_p[x]$, abordando os conceitos de característica de um corpo, elemento primitivo, extensão de corpos, polinômios minimais e por fim um método para encontrar polinômios irredutíveis. Elementos essenciais na construção de códigos, assim como para sua decodificação, assunto que abordaremos no capítulo 5.

4.1 Ideais do anel $\mathbb{Z}_p[x]$

Definição 4.1.1. Seja $I \subset \mathbb{Z}_p[x]$, um subconjunto, tal que $I \neq \emptyset$. Dizemos que I é um Ideal de $\mathbb{Z}_p[x]$ se para quaisquer $a(x), b(x) \in I$, verificarem-se as relações:

1. $a(x) - b(x) \in I$;
2. $a(x) \cdot r(x) \in I$, $\forall r(x) \in \mathbb{Z}_p[x]$.

Exemplo 4.1.2. 1. Dado o polinômio constante $a(x) = a_0 \in \mathbb{Z}_p[x]$, com $a_0 \neq 0$. Temos que $I = \{a(x)b(x); b(x) \in \mathbb{Z}_p[x]\} \subset \mathbb{Z}_p[x]$ é um ideal de $\mathbb{Z}_p[x]$. De fato, se $c(x), d(x) \in I$, então:

   (a) $c(x) - d(x) = a_0q_1(x) - a_0q_2(x) = a_0(q_1(x) - q_2(x)) \in I$;

   (b) $a(x) \cdot r(x) \in I$, $\forall r(x) \in \mathbb{Z}_p[x]$, já que $I = \{a(x)b(x); b(x) \in \mathbb{Z}_p[x]\}$.

   Neste exemplo, em particular, temos que $I = \mathbb{Z}_p[x]$. Pois $I \subset \mathbb{Z}_p[x]$, isto é claro. E se $p(x) \in \mathbb{Z}_p[x]$, como podemos reescrevê-lo como $p(x) = a_0 \cdot a_0^{-1}p(x)$, já que $a_0 \in \mathbb{Z}_p$ e $a_0 \neq 0$, segue que $p(x) \in I$, ou seja, $\mathbb{Z}_p[x] \subset I$.

2. Os ideais $I = 0$ e $I = \mathbb{Z}_p[x]$ de $\mathbb{Z}_p[x]$ são chamados os Ideais Triviais de $\mathbb{Z}_p[x]$.

Definição 4.1.3. Dado $a(x) \in \mathbb{Z}_p[x]$. Se o ideal I de $\mathbb{Z}_p[x]$, é tal que $I = \{a(x) \cdot b(x); b(x) \in \mathbb{Z}_p[x]\}$, então dizemos que I é um Ideal Principal de $\mathbb{Z}_p[x]$ e denotamos $I = (a(x))$. Um anel onde todos os seus ideais são principais é chamado de Anel de Ideais Principais.

Teorema 4.1.1. *$\mathbb{Z}_p[x]$ é um Anel de Ideais Principais.*

Demonstração. Queremos mostrar que se I é um ideal de $\mathbb{Z}_p[x]$ então I é um ideal principal, ou seja, $I = (a(x))$. Desta forma, seja I um ideal de $\mathbb{Z}_p[x]$. Se $I = \{0\}$, basta tomarmos $a(x) = 0 \in \mathbb{Z}_p[x]$ e obteremos $I = (a(x))$.

Se por outro lado, $I \neq \{0\}$, então seja $a(x) \neq 0 \in I$, onde o grau de $a(x)$ é o menor em I. Do item 2. da definição 4.1.1 segue que $(a(x)) \subset I$. Além disso, considere $b(x) \in I$do teorema 2.2.4, segue que existem $q(x)$ e $r(x)$, com $gr(r) < gr(a)$ ou $r(x) = 0$, tais que

$$b(x) = q(x)a(x) + r(x)$$

Observe que $r(x) = b(x) - q(x)a(x)$ e como $b(x), q(x)a(x) \in I$ do item 1. da definição 4.1.1 segue que $r(x) = b(x) - q(x)a(x) \in I$. Sendo assim, temos que $r(x) = 0$, pois $gr(a)$ é o menor em I, impossibilitando-nos de termos $gr(r) < gr(a)$.

Portanto $b(x) = q(x)a(x) \in (a(x))$, ou seja, $I \subset (a(x))$ e $I = (a(x))$. □

De forma mais precisa, se I é um ideal não nulo de $\mathbb{Z}_p[x]$, então é único o polinômio mônico $a(x) \in \mathbb{Z}_p[x]$, tal que $I = (a(x))$. De fato, supondo $I = (a(x)) = (b(x))$, com $a(x), b(x) \in \mathbb{Z}_p[x]$, então $a(x)|b(x)$, também $b(x)|a(x)$, mas como são ambos mônicos então $a(x) = b(x)$.

Definição 4.1.4. Seja I um ideal do anel $\mathbb{Z}_p[x]$. O conjunto

$$r(x) + I = \{r(x) + a(x); a(x) \in I\},$$

onde $r(x) \in \mathbb{Z}_p[x]$, forma uma Classe Lateral de I em $\mathbb{Z}_p[x]$.

Definição 4.1.5. O conjunto de todas as classes laterais de I em $\mathbb{Z}_p[x]$ é conhecido como conjunto Quociente de $\mathbb{Z}_p[x]$ por I e denotamos por $\mathbb{Z}_p[x]/I$.

Exemplo 4.1.6. Considere o conjunto quociente $\mathbb{Z}_3[x]/(x^2 + x + 2)$. Os elementos de $\mathbb{Z}_3[x]/(x^2+x+2)$ são as classes laterais $r_i(x)+(x^2+x+2)$, tais que $r_i(x)$ são os polinômios representantes de sua classe residual módulo x^2+x+2. Desta forma, temos que $r(x) = 0$ ou $gr(r) < gr(x^2 + x + 2) = 2$. Logo,

$$\mathbb{Z}_3[x]/(x^2 + x + 2) = \{[0], [1], [2], [x], [x + 1], [x + 2], [2x], [2x + 1], [2x + 2]\}.$$

No conjunto quociente $\mathbb{Z}_p[x]/I$ é possível definir:

- Adição: $(a(x)+I)+(b(x)+I)=(a(x)+b(x))+I$;
- Multiplicação: $(a(x)+I)(b(x)+I)=a(x)b(x)+I$;
- Elemento neutro na adição: $0+I$;
- Elemento neutro na multiplicação: $1+I$.

Definida as operações de soma e produto acima é fácil notar que $\mathbb{Z}_p[x]/I$ é um anel comutativo com unidade.

Exemplo 4.1.7. Considere o polinômio $f(x)=x^2+x+2$ em $\mathbb{Z}_3[x]$. Fazendo $\mathbb{Z}_3[x]/(x^2+x+2)$ obtemos

$$\mathbb{Z}_3[X]/(x^2+x+2)=\{[0],[1],[2],[x],[x+1],[x+2],[2x],[2x+1],[2x+2]\}.$$

As operações em $\mathbb{Z}_3[x]/(x^2+x+2)$, são descritas abaixo:

- Adição:

$+$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[0]$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[1]$	$[1]$	$[2]$	$[0]$	$[x+1]$	$[x+2]$	$[x]$	$[2x+1]$	$[2x+2]$	$[2x]$
$[2]$	$[2]$	$[0]$	$[1]$	$[x+2]$	$[x]$	$[x+1]$	$[2x+2]$	$[2x]$	$[2x+1]$
$[x]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$	$[0]$	$[1]$	$[2]$
$[x+1]$	$[x+1]$	$[x+2]$	$[x]$	$[2x+1]$	$[2x+2]$	$[2x]$	$[1]$	$[2]$	$[0]$
$[x+2]$	$[x+2]$	$[x]$	$[x+1]$	$[2x+2]$	$[2x]$	$[2x+1]$	$[2]$	$[0]$	$[1]$
$[2x]$	$[2x]$	$[2x+1]$	$[2x+2]$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$
$[2x+1]$	$[2x+1]$	$[2x+2]$	$[2x]$	$[1]$	$[2]$	$[0]$	$[x+1]$	$[x+2]$	$[x]$
$[2x+2]$	$[2x+2]$	$[2x]$	$[2x+1]$	$[2]$	$[0]$	$[1]$	$[x+2]$	$[x]$	$[x+1]$

- Multiplicação:

$\cdot$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[2]$	$[0]$	$[2]$	$[1]$	$[2x]$	$[2x+2]$	$[2x+1]$	$[x]$	$[x+2]$	$[x+1]$
$[x]$	$[0]$	$[x]$	$[2x]$	$[2x+1]$	$[1]$	$[x+1]$	$[x+2]$	$[2x+2]$	$[2]$
$[x+1]$	$[0]$	$[x+1]$	$[2x+2]$	$[1]$	$[x+2]$	$[2x]$	$[2]$	$[x]$	$[2x+1]$
$[x+2]$	$[0]$	$[x+2]$	$[2x+1]$	$[x+1]$	$[2x]$	$[2]$	$[2x+2]$	$[1]$	$[x]$
$[2x]$	$[0]$	$[2x]$	$[x]$	$[x+2]$	$[2]$	$[2x+2]$	$[2x+1]$	$[x+1]$	$[1]$
$[2x+1]$	$[0]$	$[2x+1]$	$[x+2]$	$[2x+2]$	$[x]$	$[1]$	$[x+1]$	$[2]$	$[2x]$
$[2x+2]$	$[0]$	$[2x+2]$	$[x+1]$	$[2]$	$[2x+1]$	$[x]$	$[1]$	$[2x]$	$[x+2]$

Na operação de multiplicação, quando o grau do polinômio produto é igual ou ultrapassa $gr(f) = 2$ então fazemos uma redução módulo $f(x)$. Por exemplo $[2x+2]\cdot[x+2] = [(2x+2)\cdot(x+2)] = [2x^2+1]$ e $2x^2+1 \equiv x \bmod (x^2+x+2)$. Logo, $[2x+2]\cdot[x+2] = [x]$ em $\mathbb{Z}_3[x]/(x^2+x+2)$.

4.2 O corpo $\mathbb{F}_{p^n}$

O anel $\mathbb{Z}_p[x]/I$ pode ser um corpo, desde que I seja um ideal gerado por um polinômio irredutível. É o que vamos mostrar nesta seção.

Definição 4.2.1. Seja M um ideal de $\mathbb{Z}_p[x]$. Se o único ideal de $\mathbb{Z}_p[x]$ que contém M e é diferente de M é $I = \mathbb{Z}_p[x]$, então dizemos que M é um *Ideal Maximal* de $\mathbb{Z}_p[x]$. Ou seja,

$$M \subset C \subset \mathbb{Z}_p[x] \Rightarrow I = M \text{ ou } I = \mathbb{Z}_p[x].$$

Um anel comutativo com unidade recebe o nome de corpo se todo elemento não nulo desse anel admite inverso multiplicativo. O ideal Maximal se faz importante neste contexto, já que a partir dele podemos construir corpos, como mostra o próximo teorema. Já sabemos que $\mathbb{Z}_p[x]/M$ é Anel Comutativo com Unidade.

Teorema 4.2.1. *M é um ideal maximal de $\mathbb{Z}_p[x]$ se, e somente se, $\mathbb{Z}_p[x]/M$ é um corpo.*

Demonstração. ($\Rightarrow$) Considere M um ideal maximal de $\mathbb{Z}_p[x]$. Dado $a(x) \in \mathbb{Z}_p[x] - M$, como $\mathbb{Z}_p[x]/M$ é um anel comutativo com unidade, é suficiente mostrar que $a(x) + M$ é invertível em $\mathbb{Z}_p[x]/M$. Para isso, considere

$$A = \{a(x)r(x) + m(x)\,; r(x) \in \mathbb{Z}_p[x], m(x) \in M\}.$$

Observe que todo $m(x) \in M$ pode ser escrito da forma $a(x)\cdot 0 + m(x)$, com $r(x) = 0 \in \mathbb{Z}_p[x]$, sendo assim, segue que $M \subset A$. Além disso, dados $k_1(x), k_2(x) \in A$, temos:

- $\begin{aligned} k_1(x) - k_2(x) &= a(x)r_1(x) + m_1(x) - (a(x)r_2(x) + m_2(x)) \\ &= a(x)(r_1(x) - r_2(x)) + (m_1(x) - m_2(x)) \\ &= a(x)r(x) + m(x) \in A, \text{ já que } r_1(x) - r_2(x) \in \mathbb{Z}_p[x] \text{ e} \\ &\qquad\qquad m_1(x) - m_2(x) \in M. \end{aligned}$

- $\begin{aligned} k_1(x)c(x) &= (a(x)r_1(x) + m_1(x))c(x) \\ &= a(x)r_1(x)c(x) + m_1(x)c(x) \in A, \text{qualquer que seja } c(x) \in \mathbb{Z}_p[x]. \end{aligned}$

Ou seja, A é ideal de $\mathbb{Z}_p[x]$ que contém M e como $a(x) = a(x)1 + 0 \in A$ e $a(x) \notin M$, então $A \neq M$ e portanto $A = \mathbb{Z}_p[x]$.
Em particular, como $1 \in A$, então $1 = a(x)r(x) + m(x)$, com $r(x) \in \mathbb{Z}_p[x]$ e $m(x) \in M$, então

$$\begin{aligned}(a(x) + M)(r(x) + M) &= a(x)r(x) + M \\ &= (a(x)r(x) + M) + (m(x) + M) \\ &= (a(x)r(x) + m(x)) + M \\ &= 1 + M.\end{aligned}$$

Logo, $\mathbb{Z}_p[x]/M$ é corpo.
($\Leftarrow$) Considere I um ideal de $\mathbb{Z}_p[x]$, com $I \neq M$ e $M \subset I$, para a recíproca é suficiente mostrar que $I = \mathbb{Z}_p[x]$, garante a definição 4.2.1.

Seja $a(x) \in I - M$, como $\mathbb{Z}_p[x]/M$ é corpo, existe $r(x) \in \mathbb{Z}_p[x]$ satisfazendo $(a(x) + M)(r(x) + M) = 1 + M$ e assim $a(x)r(x) + m(x) = 1$ para algum $m(x) \in M$. Como $1 = a(x)r(x) + m(x) \in I$, segue que $I = \mathbb{Z}_p[x]$. □

Teorema 4.2.2. *$\mathbb{Z}_p[x]/(m(x))$ é um corpo se, e somente se, $m(x)$ é irredutível em $\mathbb{Z}_p[x]$*

Demonstração. ($\Rightarrow$) Vamos supor $m(x) = a(x)b(x) \in \mathbb{Z}_p[x]$, com $a(x), b(x) \in \mathbb{Z}_p[x]$, do teorema 4.2.1 segue que o ideal $(m(x))$ é maximal em $\mathbb{Z}_p[x]$, já que por hipótese $\mathbb{Z}_p[x]/(m(x))$ é corpo. Observe que $(m(x)) \subset (a(x))$, da definição 4.2.1, segue que $(a(x)) = (m(x))$ ou $(a(x)) = \mathbb{Z}_p[x]$. No primeiro caso temos que $a(x) = m(x)q(x)$ para algum $q(x) \in \mathbb{Z}_p[x]$. Sendo assim,

$$\begin{aligned}m(x) &= a(x)b(x) \\ &= m(x)q(x)b(x)\end{aligned}$$

e $gr(m) = gr(m) + gr(q) + gr(b)$, desta forma segue que $gr(q) = gr(b) = 0$ e consequentemente $m(x)$ é irredutível. Se $(a(x)) = \mathbb{Z}_p[x]$ então $1 \in (a(x))$ e existe $a^{-1}(x) \in \mathbb{Z}_p[x]$, tal que $a(x)a^{-1}(x) = 1$, mas se isso ocorre então $a(x)$ é um polinômio constante e portanto $m(x)$ é irredutível.

Portanto, $m(x)$ é irredutível em $\mathbb{Z}_p[x]$.
($\Leftarrow$) Seja I um ideal de $\mathbb{Z}_p[x]$, tal que $(m(x)) \subset I \subset \mathbb{Z}_p[x]$. Como $\mathbb{Z}_p[x]$ é um anel de ideais principais, então existe $b(x) \in \mathbb{Z}_p[x]$, tal que $I = (b(x))$. Assim,

$$(m(x)) \subset (b(x)) \subset \mathbb{Z}_p[x].$$

Logo, $m(x) \in (b(x))$ e daí $m(x) = b(x)a(x)$, para algum $a(x) \in \mathbb{Z}_p[x]$. Como $m(x)$ é

irredutível, então $a(x) = \alpha \in \mathbb{Z}_p - \{0\}$ ou $b(x) = \beta \in \mathbb{Z}_p - 0$.

Se $a(x) = \alpha$, então $m(x) = \alpha b(x)$ e isso implica $\alpha^{-1}m(x) = b(x)$, logo $(m(x)) = (b(x))$. Se $b(x) = \beta$, então $1 \in (b(x))$ e portanto $(b(x)) = \mathbb{Z}_p[x]$.

Portanto $(m(x))$ é maximal e segue do teorema 4.2.1 que $\mathbb{Z}_p[x]/(m(x))$ é corpo. □

Exemplo 4.2.2. O anel quociente $\mathbb{Z}_3[x]/(x^2 + x + 2)$ é um corpo. De fato, $x^2 + x + 2$ não possui raiz em $\mathbb{Z}_3$, sendo assim, da proposição 2.4.7 segue que $x^2 + x + 2$ é irredutível em $\mathbb{Z}_3[x]$, e ainda do teorema 4.2.2, segue o resultado.

Já vimos que

$$\mathbb{Z}_3[x]/(x^2 + x + 2) = \{[0], [1], [2], [x], [x + 1], [x + 2], [2x], [2x + 1], [2x + 2]\}.$$

Não é por acaso que $|\mathbb{Z}_3[x]/(x^2 + x + 2)| = 3^2$, na verdade sempre que $\mathbb{Z}_p[x]/(g(x))$ for corpo, vamos ter $|\mathbb{Z}_p[x]/(g(x))| = p^n$, com p primo e $gr(g) = n$. Além disso, dois corpos com o mesmo número de elementos são sempre isomorfos, a demonstração dessa afirmação encontra-se em [6, página 76, teorema 4].

Afim de simplificarmos a notação, adiante vamos considerar o corpo $\mathbb{Z}_p[x]/(f(x)) = \mathbb{F}_{p^n}$, com $gr(f) = n$ e $|\mathbb{F}_{p^n}| = p^n$.

Vale observar que podemos considerar $\mathbb{F}_p = \mathbb{Z}_p$, no entanto $\mathbb{F}_{p^n} \neq \mathbb{Z}_{p^n}$, já que $\mathbb{F}_{p^n}$ é um corpo, enquanto $\mathbb{Z}_{p^n}$ não o é. Por exemplo, $\mathbb{F}_{3^2}$ é corpo e $\mathbb{Z}_9$ não é corpo.

4.2.3 A característica do corpo $\mathbb{F}_{p^n}$

Definição 4.2.4. Seja $n \in \mathbb{N}$, com $n > 0$. Se para algum n verifica-se $a(x) \cdot n = 0$, qualquer que seja $a(x) \in \mathbb{Z}_p[x]$, então existe um menor inteiro positivo r, tal que $a(x) \cdot r = 0$, $\forall a(x) \in \mathbb{Z}_p[x]$. Dizemos que r é a *característica* de $\mathbb{Z}_p[x]$ e denotamos por $c(\mathbb{Z}_p[x]) = r$.

Exemplo 4.2.5. A característica de $\mathbb{Z}_{23}[x]$ é 23. Note que em qualquer polinômio $g(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}_{23}[x]$, temos

$$23 \cdot g(x) = 23a_n x^n + \cdots + 23a_1 x + 23a_0 = 0 + \cdots + 0 + 0 = 0.$$

Além disso, não há natural menor que 23 que atenda a condição acima.

Este resultado se estende a todo anel do tipo $\mathbb{Z}_p[x]$, desde que p seja primo, veja.

Proposição 4.2.3. $c(\mathbb{Z}_p[x]) = p$.

Demonstração. De fato, $p \cdot a(x) = 0$, qualquer que seja $a(x) \in \mathbb{Z}_p[x]$. Além disso, supondo que há $p' < p$, tal que $p' \cdot a(x) = 0$, qualquer que seja $a(x) \in \mathbb{Z}_p[x]$, então seja $p' = p - n$, com $n \neq 0$. Multiplicando ambos os termos da equação anterior por $a(x) \neq 0 \in \mathbb{Z}_p[x]$, obtemos:

$$p'a(x) = pa(x) - na(x) \Rightarrow -na(x) = 0$$

Como $\mathbb{Z}_p[x]$ é um anel de integridade e $a(x) \neq 0$, segue que $n = 0$, o que contradiz a hipótese. Logo, $c(\mathbb{Z}_p[x]) = p$. □

Proposição 4.2.4. *Seja F um corpo finito de característica p. Se $a, b \in F$, temos que $(a \pm b)^p = a^p \pm b^p$.*

Demonstração. A prova deste resultado pode ser encontrada em [6, página 67]. □

Proposição 4.2.5. *Considere q uma potência de p. Se $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}_p[x]$, então*

$$f(x)^q = a_n^q x^{nq} + \cdots + a_1^q x^q + a_0^q$$

.

Demonstração. A prova deste resultado pode ser encontrada em [6, Observação 2, pg.67]. □

4.2.6 Elemento Primitivo

Para a próxima preposição considere o conjunto $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$.

Proposição 4.2.6. *Se $\alpha \in \mathbb{F}_q^*$, com $q = p^n$, então $\alpha^{q-1} = 1$.*

Demonstração. Considere a aplicação $\sigma : \mathbb{F}_q^* \longrightarrow \mathbb{F}_q^*$, dada por $\sigma(a) = \alpha a$. A aplicação σ é bijetora. De fato, se $\alpha a_1 = \alpha a_2$ então como $\mathbb{F}_q$ é corpo e $\alpha \neq 0$, segue que $a_1 = a_2$, logo σ é injetora. Além disso, $\sigma : \mathbb{F}_q^* \longrightarrow \mathbb{F}_q^*$ e como $\mathbb{F}_q^*$ é finito, então σ é sobrejetora.
Desta forma temos que $\mathbb{F}_q^* = \{a_1, a_2, \cdots, a_{q-1}\} = \{\alpha a_1, \alpha a_2, \cdots, \alpha a_{q-1}\}$ e

$$\alpha a_1 \alpha a_2 \cdots \alpha a_{q-1} = a_1 a_2 \cdots a_{q-1}$$

Portanto, $\alpha^{q-1} = 1$. □

Observe que da proposição acima, segue que todo $\alpha \in \mathbb{F}_q$ é raiz do polinômio $x^q - x \in \mathbb{Z}_p[x]$, já que $\alpha^{q-1} = 1 \Rightarrow \alpha^q = \alpha \Rightarrow \alpha^q - \alpha = 0$.

E ainda, como $gr(x^q - x) = q$ então o polinômio $x^q - x$ possui no máximo q raízes em $\mathbb{F}_q$. Mas como todo elemento de $\mathbb{F}_q$ é raiz de $x^q - x$, então do corolário 2.4.2 segue que

$$x^q - x = (x - 0)(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{q-1}).$$

Dizemos que $\mathbb{F}_q$ é um Corpo de Decomposição de $x^q - x$ sobre $\mathbb{Z}_p$.

Definição 4.2.7. Seja $\alpha \in \mathbb{F}_q^*$, onde $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$ e $\mathbb{F}_q$ um corpo finito. Dizemos que a *ordem* de α é n, se n é o menor inteiro positivo, tal que

$$\alpha^n = 1.$$

Definição 4.2.8. Seja $\alpha \in \mathbb{F}_q$, com $\alpha \neq 0$. Dizemos que α é um elemento *primitivo* se

$$\mathbb{F}_q^* = \{1, \alpha, \cdots, \alpha^{q-2}\},$$

ou seja, a ordem de α for $q-1$.

Observe que as potências do elemento primitivo geram todos os elementos não nulos de $\mathbb{F}_q$. E por se tratar de potências de mesma base, tal notação facilita o cálculo de multiplicação entre esses elementos.

Todo corpo finito possui elementos primitivos, a prova dessa afirmação pode ser encontrada em [6, página 78].

Proposição 4.2.7. *Seja $\alpha \in \mathbb{F}_{p^n}$ primitivo sobre $\mathbb{Z}_p$, tal que $\alpha^d = 1$, então $(p^n - 1)|d$.*

Demonstração. Se α é primitivo então $\alpha^{p^n-1} = 1$. Além disso, existem q e r inteiros não negativos, com $0 \leqslant r < (p^n - 1)$, tais que $d = q(p^n - 1) + r$. Desta forma, observe que

$$\alpha^d = (\alpha^{p^n-1})^q \alpha^r \Rightarrow \alpha^r = 1.$$

Mas r não pode ser ordem de α, já que $p^n - 1$ é o menor inteiro positivo, tal que $\alpha^{p^n-1} = 1$, sendo assim devemos ter $r = 0$. Logo, $p^n - 1|d$. □

Exemplo 4.2.9. Considere o corpo $\mathbb{F}_{3^2} = \mathbb{Z}_3[x]/(x^2+1)$. Temos que

$$\mathbb{F}_{3^2}^* = \{[1], [2], [x], [x+1], [x+2], [2x], [2x+1], [2x+2]\}.$$

Fazendo a verificação de cada elemento temos que os elementos primitivos de $\mathbb{F}_{3^2}$ são: $[x+1]$, $[x+2]$, $[2x+1]$, $[2x+2]$.
Para exemplificação, seja $\alpha = [x+1]$, como α é primitivo de imediato temos que $\alpha^{3^2-1} = 1$. Além disso, temos

$$\begin{aligned}
\alpha^8 &= [x+1]^8 = [1] \\
\alpha^1 &= [x+1]^1 = [x+1] \\
\alpha^2 &= [x+1]^2 = [x^2+2x+1] = [2x] \\
\alpha^3 &= [x+1]^3 = [x^3+1] = [2x+1] \\
\alpha^4 &= [x+1]^4 = [x^4+x^3+x+1] = [2] \\
\alpha^5 &= [x+1]^5 = [x^5+2x^4+x^3+x^2+2x+1] = [2x+2] \\
\alpha^6 &= [x+1]^6 = [x^6+2x^3+1] = [x] \\
\alpha^7 &= [x+1]^7 = [x^7+x^6+2x^4+2x^3+x+1] = [x+2].
\end{aligned}$$

Ou seja, $\mathbb{F}_{3^2}^* = \{\alpha^8, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}$. E ainda,

$$x^9 - x = (x)(x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^5)(x-\alpha^6)(x-\alpha^7)(x-\alpha^8).$$

Lema 4.2.8. *Se x, m, n são inteiros positivos com $x > 1$ então $(x^m - 1)|(x^n - 1) \Leftrightarrow m|n$.*

Demonstração. ($\Leftarrow$) Vamos supor $n = mq$, para algum q inteiro positivo. Da relação de congruência segue que

$$\begin{aligned} x^m &\equiv 1 \ mod\,(x^m - 1) \Rightarrow \\ x^{mq} &\equiv 1^q \ mod\,(x^m - 1) \Rightarrow \\ x^{mq} - 1 &\equiv 0 \ mod\,(x^m - 1) \Rightarrow \\ x^n - 1 &\equiv 0 \ mod\,(x^m - 1). \end{aligned}$$

Ou seja, $(x^m - 1)|(x^n - 1)$.

($\Rightarrow$) Considere $n = mq + r$, com $0 \leqslant r < m$. Observe que

$$\frac{x^n - 1}{x^m - 1} = x^r \frac{x^{mq} - 1}{x^m - 1} + \frac{x^r - 1}{x^m - 1}.$$

Da hipótese segue que $(x^m - 1)|(x^n - 1)$, além disso $(x^m - 1)|(x^{mq} - 1)$ e consequentemente $x^m - 1|x^r(x^{mq} - 1)$, desta forma temos que $x^m - 1|x^r - 1$, no entanto $r < m$, sendo assim r deve ser 0.

□

Teorema 4.2.9. *$\mathbb{F}_{p^n}$ contém um subcorpo $\mathbb{F}_{p^m}$ se, e somente se, $m|n$.*

Demonstração. ($\Rightarrow$) Considere os corpos $\mathbb{F}_{p^n}$ e $\mathbb{F}_{p^m}$, tais que $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$. Seja $\alpha \in \mathbb{F}_{p^m}$, tal que $\alpha \neq 0$, da proposição 4.2.6 segue que $\alpha^{p^m - 1} = 1$. Mas também $\alpha \in \mathbb{F}_{p^n}$, logo $\alpha^{p^n - 1} = 1$. Ou seja, as raízes de $x^{p^m} - x$ são raízes de $x^{p^n} - x$, logo $(x^{p^m} - x)|(x^{p^n} - x)$ e consequentemente $(x^{p^m - 1} - 1)|(x^{p^n - 1} - 1)$.
Portanto, do lema 4.2.8 segue que $m|n$.
($\Leftarrow$) Se $m|n$ então do lema 4.2.8 segue que $(x^{p^m - 1} - 1)|(x^{p^n - 1} - 1)$ e consequentemente $(x^{p^m} - x)|(x^{p^n} - x)$. Logo as raízes de $x^{p^m} - x$ são também de $x^{p^n} - x$, ou seja, $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$. □

Exemplo 4.2.10. Abaixo ilustramos os subcorpos de $\mathbb{F}_{5^{12}}$ e $\mathbb{F}_{7^{36}}$:

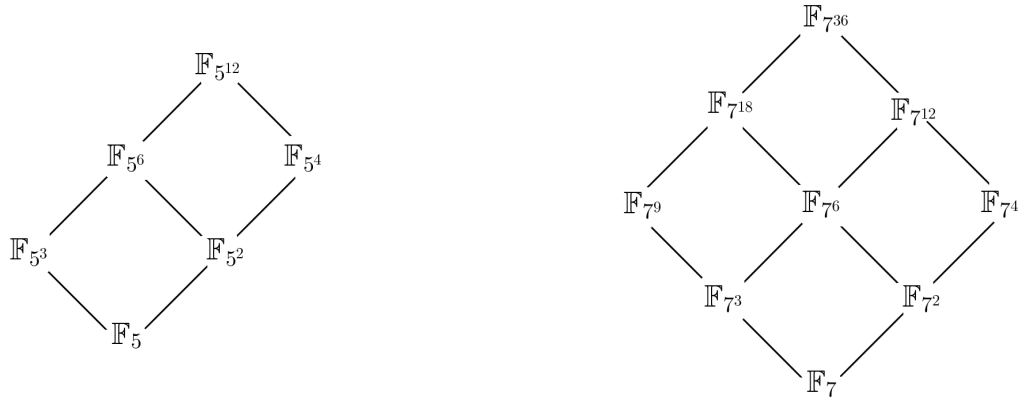


Figura 1: Subcorpos de $\mathbb{F}_5^{12}$ e $\mathbb{F}_7^{36}$.

Fonte: autora

4.3 Extensões

Definição 4.3.1. Sejam K e E corpos. Se $K \subset E$ dizemos que E é uma *extensão* de K.

Sendo assim, segue do teorema 4.2.9 que, desde que $m|n$, $\mathbb{F}_{p^n}$ é uma extensão de $\mathbb{F}_{p^m}$.

Definição 4.3.2. Seja E uma extensão do corpo K. Um número $\alpha \in E$ é dito Algébrico sobre um corpo K se existe um polinômio não nulo $f(x) \in K[x]$, tal que α é uma raiz de $f(x)$, isto é, um polinômio

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

com coeficientes $a_o, a_1, \cdots, a_n \in K$, com ao menos um coeficiente não nulo.

Exemplo 4.3.3. Sejam $f(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$ e o corpo $\mathbb{F}_{2^4} = \mathbb{Z}_2[x]/(x^4 + x + 1)$, tal que

$$\begin{aligned}\mathbb{F}_{2^4} = \{&[0], [1], [x], [x+1], [x^2], [x^2+1], [x^2+x], [x^2+x+1], [x^3], [x^3+1], [x^3+x],\\ &[x^3+x^2], [x^3+x+1], [x^3+x^2+1], [x^3+x^2+x], [x^3+x^2+x+1]\}.\end{aligned}$$

Observe que a aplicação $a \longmapsto [a]$ é um isomorfismo de $\mathbb{Z}_2$ sobre o subcorpo $\mathbb{F}_2 = \{[0], [1]\}$ de $\mathbb{F}_{2^4}$. Deste modo, podemos dizer que $\mathbb{F}_{2^4}$ é uma extensão de $\mathbb{Z}_2$.
O elemento $[x+1] \in \mathbb{F}_{2^4}$ é algébrico sobre $\mathbb{Z}_2$. De fato, tome $\alpha = [x+1]$ e $f(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$ e observe:

$$f([x+1]) = [x+1]^4 + [x+1] + 1 = [x^4 + 1 + x + 1 + 1] = [x^4 + x + 1] = [0].$$

4.4 Polinômios Minimais

Definição 4.4.1. Seja $\alpha \in \mathbb{F}_{p^n}$ algébrico sobre o corpo $\mathbb{Z}_p$ e $\mathbb{F}_{p^n}$ uma extensão de $\mathbb{Z}_p$. O único polinômio de menor grau entre os polinômios $f(x)$ em $\mathbb{Z}_p[x]$ satisfazendo:

1. $f(\alpha) = 0$;
2. $f(x)$ mônico.

É chamado o *Polinômio Minimal* de α sobre $\mathbb{Z}_p$ e denotado por $f(x) = \mathcal{M}_\alpha(x)$.

Exemplo 4.4.2. Seja $\alpha = [x] \in \mathbb{F}_{2^2} = \mathbb{Z}_2[x]/(x^2 + x + 1)$ uma raiz do polinômio $f(x) = 1 + x + x^2 \in \mathbb{Z}_2[x]$. Observe que os dois polinômios lineares x e $1 + x$ não são polinômios mínimos de α. Portanto, $\mathcal{M}_\alpha(x) = 1 + x + x^2$. Também

$$\begin{aligned} f(1+\alpha) &= 1 + (1+\alpha) + (1+\alpha)^2 \\ &= 1 + 1 + \alpha + 1 + \alpha^2 \\ &= 1 + \alpha + \alpha^2 \\ &= 0 \end{aligned}$$

E como $1 + \alpha$ não é raiz de x ou $1 + x$, então $1 + x + x^2$ também é polinômio minimal de $1 + \alpha$.

Os elementos de um corpo que possuem o mesmo polinômio minimal são denominados *conjugados*. Vamos agora apresentar algumas propriedades do polinômio minimal.

Proposição 4.4.1. *Seja $\mathcal{M}_\alpha(x)$ sobre $\mathbb{Z}_p$ e $f(x) \in \mathbb{Z}_p[x]$.*

1. *$\mathcal{M}_\alpha(x)$ é irredutível.*
2. *Se $f(\alpha) = 0$, então $\mathcal{M}_\alpha(x) | f(x)$;*
3. *$\mathcal{M}_\alpha(x) | x^{p^n} - x$;*
4. *Se $\alpha \in \mathbb{F}_{p^n}$ é um elemento primitivo, então $gr(\mathcal{M}_\alpha) = n$;*
5. *Se $\alpha, \alpha^p \in \mathbb{F}_{p^n}$, então $\mathcal{M}_\alpha(x) = \mathcal{M}_{\alpha^p}(x)$.*

Demonstração. 1. Se $\mathcal{M}_\alpha(x) = a(x)b(x)$, e supondo $gr(a), gr(b) > 0$, então

$$\mathcal{M}_\alpha(\alpha) = a(\alpha)b(\alpha) = 0 \Rightarrow a(\alpha) = 0 \text{ ou } b(\alpha) = 0.$$

O que é um absurdo, já que $gr(\mathcal{M}_\alpha)$ é o menor tal que $\mathcal{M}_\alpha(\alpha) = 0$. Logo $a(x)$ ou $b(x)$ é constante, sendo assim, $\mathcal{M}_\alpha(x)$ é irredutível.

2. Do teorema 2.2.4 segue que existem $q(x), r(x) \in K$, com $r(x) = 0$ ou $gr(r) < gr(\mathcal{M}_\alpha))$, tais que $f(x) = \mathcal{M}_\alpha(x)q(x)+r(x)$. Fazendo $f(\alpha)$, temos $f(\alpha) = \mathcal{M}_\alpha(\alpha)q(\alpha)+r(\alpha) \Rightarrow r(\alpha) = 0$. Ou seja, $r(x)$ é um polinômio onde $gr(r) < gr(\mathcal{M}_\alpha)$, tal que $r(\alpha) = 0$, o que é um absurdo. Desta forma, devemos ter $r(x) = 0$ e portanto $\mathcal{M}_\alpha(x)|f(x)$.

3. Considere $f(x) = x^{p^n} - x$, sabemos que $\alpha \in \mathbb{F}_{p^n}$ é tal que $f(\alpha) = 0$, sendo assim, do item *2*, segue que $\mathcal{M}_\alpha(x)|x^{p^n} - x$.

4. $\mathbb{F}_{p^n}$ é um espaço vetorial de dimensão n (veja em [6, página 72]), sendo assim, quaisquer $n+1$ elementos de $\mathbb{F}_{p^n}$ são linearmente dependentes ($\mathcal{L}.\mathcal{D}.$). Desta forma temos que existem $a_i \in \mathbb{Z}_p$, não todos nulos, tais que:

$$\sum_{i=0}^{n} a_i\alpha^i = 0.$$

   Ou seja, existe um polinômio de grau menor ou igual a n, cujo α é raiz. Logo, $gr(\mathcal{M}_\alpha) \leqslant n$.
   Além disso, considere o corpo $\mathbb{F}_{p^{gr(\mathcal{M}_\alpha)}} = \mathbb{Z}_p[x]/(\mathcal{M}_\alpha(x))$, como α é raiz do polinômio minimal segue que $\alpha \in \mathbb{F}_{p^{gr(\mathcal{M}_\alpha)}}$ e ainda, da hipótese, α é primitivo, logo os elementos de $\mathbb{F}_{p^n}$ são escritos em função de α e consequentemente também pertencem a $\mathbb{F}_{p^{gr(\mathcal{M}_\alpha)}}$. Desta forma, segue que $gr(\mathcal{M}_\alpha) \geqslant n$, mas também $gr(\mathcal{M}_\alpha) \leqslant n$, portanto devemos ter $gr(\mathcal{M}_\alpha) = n$.
   Dizemos que o polinômio minimal de um elemento primitivo é um *polinômio primitivo*.

5. Seja $\alpha, \alpha^p \in \mathbb{F}_{p^n}$, com os polinômios minimais $\mathcal{M}_\alpha(x)$ e $\mathcal{M}_{\alpha^p}(x)$, com $\mathcal{M}_\alpha(x) = x^n + \cdots + a_1x + a_0$. Da proposição 4.2.5,

$$\begin{aligned} 0 &= \mathcal{M}_\alpha(\alpha) \\ &= (\mathcal{M}_\alpha(\alpha))^p \\ &= (\alpha^p)^n + \cdots + a_1^p\alpha^p + a_0^p \\ &= \mathcal{M}_\alpha(\alpha^p). \end{aligned}$$

   A última igualdade é válida, pois $a_i^p \equiv a_i \, mod\, p$, $\forall a_i \in \mathbb{Z}_p$ (Pequeno Teorema de Fermat[1]) e portanto $\mathcal{M}_\alpha(\alpha^p) = 0$. Sendo assim, do item *2* temos que $\mathcal{M}_{\alpha^p}(x)|\mathcal{M}_\alpha(x)$. E como $\mathcal{M}_\alpha(x)$ é irredutível então $\mathcal{M}_\alpha(x) = \beta\mathcal{M}_{\alpha^p}(x)$, com $\beta \in \mathbb{Z}_p - \{0\}$.
   Também sabemos que $\mathcal{M}_\alpha(x)$ e $\mathcal{M}_{\alpha^p}(x)$ são mônicos, sendo assim devemos ter

[1] Para saber mais sobre o Pequeno Teorema de Fermat consulte [5, páginas 156- 158].

$\beta = 1$. Portanto $\mathcal{M}_{\alpha}(x) = \mathcal{M}_{\alpha^p}(x)$.

□

As potências de α que possuem o mesmo polinômio minimal formam conjuntos disjuntos, chamados *Classes Laterais Ciclotômicas*. Desta forma, todo α^k, tal que k varia em uma classe lateral ciclotômica tem o mesmo polinômio minimal.

Definição 4.4.3. A operação de multiplicação por p divide os inteiros $(mod\, p^n - 1)$ em conjuntos chamados Classes Laterias Ciclotômicas $(mod\, p^n - 1)$.

A classe lateral ciclotômica contendo s é dada por $C_s = \{s, ps, p^2s, p^3s, \cdots, p^{n_s-1}s\}$, onde n_s representa o menor inteiro positivo tal que $p^{n_s} \cdot s \equiv s \; mod\,(p^n - 1)$.

A classe lateral é representada por C_s, onde s é o menor número da classe lateral. Tais índices s são chamados representantes de classe lateral $(mod\, p^n - 1)$.

Exemplo 4.4.4. Classes laterais ciclotômicas:

1. Para $p = 3$ e $n = 2$, observe que

$$\begin{aligned} 0 &\equiv 0 \quad mod\, 8 \\ 3 \cdot 0 &\equiv 0 \quad mod\, 8 \end{aligned}$$

Logo, $C_0 = \{0\}$.

$$\begin{aligned} 1 &\equiv 1 \quad mod\, 8 \\ 3 \cdot 1 &\equiv 3 \quad mod\, 8 \\ 3^2 \cdot 1 &\equiv 1 \quad mod\, 8 \end{aligned}$$

Logo, $C_1 = \{1, 3\}$.

$$\begin{aligned} 2 &\equiv 2 \quad mod\, 8 \\ 3 \cdot 2 &\equiv 6 \quad mod\, 8 \\ 3^2 \cdot 2 &\equiv 2 \quad mod\, 8 \end{aligned}$$

Logo, $C_2 = \{2, 6\}$.

$$\begin{aligned} 4 &\equiv 4 \quad mod\, 8 \\ 3 \cdot 4 &\equiv 4 \quad mod\, 8 \end{aligned}$$

Logo, $C_4 = \{4\}$.

$$\begin{aligned} 5 &\equiv 5 \mod 8 \\ 3 \cdot 5 &\equiv 7 \mod 8 \\ 3^2 \cdot 5 &\equiv 5 \mod 8 \end{aligned}$$

Logo, $C_5 = \{5, 7\}$.

2. E para $p = 3$ e $n = 3$, temos:

mod $3^3 - 1$
$C_0 = \{0\}$
$C_1 = \{1, 3, 9\}$
$C_2 = \{2, 6, 18\}$
$C_4 = \{4, 10, 12\}$
$C_5 = \{5, 15, 19\}$
$C_7 = \{7, 11, 21\}$
$C_8 = \{8, 20, 24\}$
$C_{13} = \{13\}$
$C_{14} = \{14, 16, 22\}$
$C_{17} = \{17, 23, 25\}$

Seja $\mathcal{M}_{\alpha^i}(x)$, com α^i um elemento primitivo de $\mathbb{F}_{p^n}$ e $i \in C_s = \{s, ps, \cdots, p^{p_n - 1}s\}$. Do item 5 da proposição 4.4.1 temos que $\mathcal{M}_{\alpha^s}(x) = \mathcal{M}_{\alpha^{ps}}(x) = \cdots = \mathcal{M}_{\alpha^{p^{n_s-1}s}}(x)$. Note que como α^i é raiz de $\mathcal{M}_{\alpha^i}(x)$, então $(x - \alpha^i)$ é um divisor de $\mathcal{M}_{\alpha^i}(x)$, sendo assim como todo α^i, com $i \in \{s, ps, p^2s, \cdots, p^{n_s-1}s\}$, é raiz de $\mathcal{M}_{\alpha^i}(x)$ e $\alpha^r \neq \alpha^t$ (desde que $r \neq t$)[2] então:

$$(x - \alpha^s)(x - \alpha^{ps}) \cdots (x - \alpha^{p^{n_s-1}s}) = \prod_{j \in C_s} (x - \alpha^j) | \mathcal{M}_{\alpha^i}(x).$$

Outra propriedade dos polinômios minimais.

Proposição 4.4.2. *Se α^i é um elemento primitivo de $\mathbb{F}_{p^n}$, com $i \in C_s$, então*

$$\mathcal{M}_{\alpha^i}(x) = \prod_{j \in C_s} (x - \alpha^j).$$

Demonstração. Da hipótese temos que $i \in C_s = \{s, ps, p^2s, \cdots, p^{n_s-1}s\}$. Considere o polinômio mônico $f(x) = (x - \alpha^s)(x - \alpha^{ps}) \cdots (x - \alpha^{p^{n_s-1}s})$, com $\alpha^i \in \mathbb{F}_{p^n}$. Queremos

[2] Neste caso como r e t pertencem a mesma classe ciclotômica eles são necessariamente distintos.

mostrar que $f(x) = \mathcal{M}_{\alpha^i}(x)$.

Recorde que nas classes ciclotômicas $p^{n_s}s = s$, sendo assim,

$$\begin{aligned} f(x^p) =& (x^p - \alpha^s)(x^p - \alpha^{ps}) \cdots (x^p - \alpha^{p^{n_s-1}s}) \\ =& (x^p - \alpha^{p^{n_s}s})(x^p - \alpha^{ps}) \cdots (x^p - \alpha^{p^{n_s-1}s}) \\ =& (x - \alpha^{p^{n_s-1}s})^p (x - \alpha^s)^p \cdots (x - \alpha^{p^{n_s-2}s})^p \\ =& [(x - \alpha^{p^{n_s-1}s})(x - \alpha^s) \cdots (x - \alpha^{p^{n_s-2}s})]^p \\ =& f(x)^p. \end{aligned}$$

Desta forma, segue que se $f(x) = a_m x^m + \cdots + a_1 x + a_0$, então $f(x)^p = a_m^p (x^m)^p + \cdots + a_1^p x^p + a_0^p$ e portanto $a_i = a_i^p$ para todo $i = 0, \cdots, m$, mas se isso ocorre então devemos ter que $a_i \in \mathbb{Z}_p$ e consequentemente $f(x) \in \mathbb{Z}_p[x]$. Também sabemos que $f(x) | \mathcal{M}_{\alpha^i}(x)$ e como são ambos mônicos, então devemos ter $f(x) = \mathcal{M}_{\alpha^i}(x)$. Ou seja,

$$\mathcal{M}_{\alpha^i}(x) = \prod_{j \in C_s} (x - \alpha^j).$$

□

Exemplo 4.4.5. Considere o corpo $\mathbb{F}_{3^2} = \mathbb{Z}_p[x]/(x^2+x+2)$ e $\alpha = [x] \in \mathbb{F}_{3^2}$. α é primitivo sobre $\mathbb{Z}_3$, de fato, os elementos de $\mathbb{F}_{3^2}$ que as potências de α representam são:

$$\begin{aligned} \alpha^8 &= [1] \\ \alpha &= [x] \\ \alpha^2 &= [x]^2 = [2x+1] \\ \alpha^3 &= [x]^3 = [2x+2] \\ \alpha^4 &= [x]^4 = [2] \\ \alpha^5 &= [x]^5 = [2x] \\ \alpha^6 &= [x]^6 = [x+2] \\ \alpha^7 &= [x]^7 = [x+1]. \end{aligned}$$

Já conhecemos as classes ciclotômicas quando $p = 3$ e $n = 2$ (exemplo 4.4.4). Sendo assim, utilizando o resultado da proposição 4.4.2 vamos encontrar os polinômios minimais

dos elementos de $\mathbb{F}_{3^2}$. Observe que

$$\begin{aligned}
C_0 &= \{0\} \Rightarrow \mathcal{M}_{\alpha^0} = \mathcal{M}_{\alpha^8} = x - \alpha^8 = x - 1 = x + 2;\\
C_1 &= \{1, 3\} \Rightarrow \mathcal{M}_{\alpha}(x) = (x - \alpha)(x - \alpha^3) = x^2 + x + 2;\\
C_2 &= \{2, 6\} \Rightarrow \mathcal{M}_{\alpha^2}(x) = (x - \alpha^2)(x - \alpha^6) = x^2 + 1;\\
C_4 &= \{4\} \Rightarrow \mathcal{M}_{\alpha^4}(x) = (x - \alpha^4) = x + 1;\\
C_5 &= \{5, 7\} \Rightarrow \mathcal{M}_{\alpha^5}(x) = (x - \alpha^5)(x - \alpha^7) = x^2 + 2x + 2.
\end{aligned}$$

Logo,

Elemento	Polinômio Minimal
0	x
$\alpha^8 = 1$	$x + 2$
α, α^3	$x^2 + x + 2$
α^2, α^6	$x^2 + 1$
α^4	$x + 1$
α^5, α^7	$x^2 + 2x + 2$

4.5 Método para encontar polinômios irredutíveis

Teorema 4.5.1. *O produto de todos os polinômios irredutíveis sobre $\mathbb{Z}_p$, cujo grau divide n, é igual a $x^{p^n} - x$.*

Demonstração. Sabemos que $\mathbb{F}_{p^n}$ é corpo de decomposição de $x^{p^n} - x$, sendo assim, este não possui fatores múltiplos. Desta forma, seja $f(x) \in \mathbb{Z}_p[x]$ um polinômio irredutível sobre $\mathbb{Z}_p$, com $gr(f) = d$, onde $d|n$, queremos mostrar que $f(x)|x^{p^n} - x$.
Supondo $\mathbb{F}_{p^d} = \mathbb{Z}_p[x]/(f(x))$, seja $\alpha \in \mathbb{F}_{p^d}$ uma raiz de $f(x)$ então $f(x) = \mathcal{M}_{\alpha}(x)$, do item *3* da proposição 4.4.1, segue que $f(x)|x^{p^d} - x$.

Se $f(x) = x$, então é claro, que $f(x)|x^{p^n} - x$. Considere então $f(x) \neq x$, já sabemos que $f(x)|x^{p^d} - x$, em particular $f(x)|x^{p^{d-1}} - 1$.

Por hipótese $d|n$, do lema 4.2.8 $(p^d - 1)|(p^n - 1)$ e consequentemente $(x^{p^d-1} - 1)|(x^{p^n-1} - 1)$, logo $f(x)|x^{p^n} - x$.

Considere agora $f(x)$ irredutível sobre $\mathbb{Z}_p$, tal que $f(x)|(x^{p^n} - x)$ e $gr(f) = d$, queremos mostrar que $d|n$. Seja $\alpha \in \mathbb{F}^*_{p^d}$, tal que $f(\alpha) = 0$, então para algum $q(x) \in \mathbb{Z}_p[x]$, temos

$$x^{p^n} - x = q(x)f(x) \Rightarrow \alpha^{p^n} - \alpha = q(\alpha)f(\alpha) \Rightarrow \alpha^{p^n} = \alpha.$$

Considere ainda β um elemento primitivo de $\mathbb{F}_{p^d}$, tal que $\beta = a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}$, sendo assim como $\alpha^{p^n} = \alpha$ e $a_i = a_i^{p^n}$, para todo $i \in \{0, \cdots, d-1\}$ (Pequeno Teorema de

Fermat), já que $a_i \in \mathbb{Z}_p$, temos:

$$\begin{aligned}\beta &= a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} \\ &= a_0^{p^n} + a_1^{p^n}\alpha^{p^n} + \cdots + a_{d-1}^{p^n}(\alpha^{d-1})^{p^n} \\ &= \beta^{p^n}\end{aligned}$$

e ainda, como β é primitivo, então $\beta \neq 0$, sendo assim $\beta^{p^n-1} = 1$ e da proposição 4.2.7 a ordem de β, $(p^d - 1)$ deve dividir $(p^n - 1)$, sendo assim, do lema 4.2.8, segue que $d|n$. □

Teorema 4.5.2. *No corpo $\mathbb{F}_q$, $x^{q^n} - x$ é igual ao produto de todos polinômios mônicos irredutíveis sobre $\mathbb{F}_q$, cujo grau divide n.*

Demonstração. [6, página 73, proposição 11] □

Um modo de encontrar polinômios irredutíveis é fatorar o polinômio $x^{p^n} - x$, já que do teorema 4.5.1 segue que $x^{p^n} - x$ é o produto dos polinômios irredutíveis, cujo grau divide n.

Exemplo 4.5.1. Considere o corpo $\mathbb{F}_{2^n}$ e $\alpha \in \mathbb{F}_{2^n}^*$ primitivo sobre $\mathbb{Z}_2$.

1. Para n=1, temos $x^2 + x = x(x+1)$. Assim:

Elemento	Polinômio Minimal
0	x
1	$x+1$

   Ou seja, os polinômios irredutíveis em $\mathbb{F}_2$ são x e $x+1$.

2. Para n=2, temos $x^{2^2} - x = x(x+1)(x^2+x+1)$. Além disso, as classes ciclotômicas módulo $2^2 - 1 = 3$ são: $C_0 = \{0\}$ e $C_1 = \{1, 2\}$. Assim:

Elemento	Polinômio Minimal
0	x
$\alpha^3 = 1$	$x+1$
$\alpha\,, \alpha^2$	x^2+x+1

   Ou seja, os polinômios irredutíveis em $\mathbb{F}_{2^2}$ são: x, $x+1$ e x^2+x+1.

3. Para n=3, temos $x^{2^3} - x = x(x+1)(x^3+x^2+1)(x^3+x+1)$. Além disso, as classes ciclotômicas módulo $2^3 - 1 = 7$ são: $C_0 = \{0\}$, $C_1 = \{1, 2, 4\}$ e $C_3 = \{3, 6, 5\}$. Sendo assim, considerando $\mathbb{F}_{2^3} = \mathbb{Z}_p[x]/(x^3+x+1)$ e $\alpha = [x+1]$ primitivo em $\mathbb{F}_{2^3}$ temos:

Elemento	Polinômio Minimal
0	x
$\alpha^7 = 1$	$x+1$
α, α^2, α^4	x^3+x^2+1
α^3, α^6, α^5	x^3+x+1

Ou seja, os polinômios irredutíveis em $\mathbb{F}_{2^3}$ são: x, $x+1$, x^3+x+1 e x^3+x^2+1.

Os polinômios x^3+x+1 e x^3+x^2+1 do exemplo acima são ditos *polinômios recíprocos*. Um polinômio recíproco de $f(x)$ é dado por $f^{\mathtt{R}}(x) = x^{gr(f)} \cdot f(x^{-1})$, ou seja, invertendo a ordem dos coeficientes de $f(x)$. Logo se $f(x) = a_n x^n + \cdots + a_1 x + a_0$, então seu recíproco será $f^{\mathtt{R}}(x) = a_0 x^n + \cdots + a_{n-1} x + a_n$.

As raízes do polinômio recíproco são os recíprocos das raízes do polinômio original. Se um polinômio é irredutível seu recíproco também é. Além disso, se $\mathcal{M}_\alpha(x)$ é o polinômio minimal de α, então $\mathcal{M}^{\mathtt{R}}_\alpha(x) = \mathcal{M}_{\alpha^{-1}}(x)$.

4.5.2 Raízes da unidade

Definição 4.5.3. Dado m e n inteiros positivos, uma raiz n-ésima da unidade num corpo $\mathbb{F}_{p^m}$ é uma raiz em $\mathbb{F}_{p^m}$ do polinômio $x^n - 1$.

O próximo teorema nos fornece a fatoração do polinômio $x^n - 1$ em polinômios minimais, esse resultado será muito útil na construção de códigos cíclicos, que veremos no próximo capítulo.

Antes, definiremos a generalização da construção ciclotômica para $n \in \mathbb{N}$ e $mdc(n, p^m) = 1$. A classe lateral ciclotômica de p módulo n que contém s é dada por:

$$C_s = \{s, ps, p^2 s, \cdots, p^{m_s - 1} s\},$$

onde $m_s \cdot s \equiv s \bmod n$.

Teorema 4.5.3. *Sejam α um elemento primitivo de $\mathbb{F}_{p^m}$, $\mathcal{M}_{\alpha^j}(x)$ polinômio minimal de α^j e n um número inteiro positivo com $mdc(p^m, n) = 1$, onde $n|(p^m - 1)$. Vamos supor que $\{C_0, C_1, \cdots, C_t\}$ seja um conjunto completo de representantes de classes ciclotômicas de p módulo n, então o polinômio $x^n - 1$ tem fatoração em polinômios mônicos irredutíveis sobre $\mathbb{F}_{p^m}$:*

$$x^n - 1 = \prod_{i=0}^{t} \mathcal{M}_{C_{ir}}(x)$$

Onde $\mathcal{M}_{C_{ir}}(x)$ é o polinômio minimal da classe ciclotômica C_{ir} e $r = \dfrac{p^m - 1}{n}$.

Demonstração. Considere $f(x) = x^n - 1$. Note que $nr = p^m - 1$, assim:

$$\begin{aligned} f(\alpha^r) &= (\alpha^r)^n - 1 \\ &= \alpha^{p^m - 1} - 1 \\ &= 1 - 1 \qquad \text{Já que } \alpha^{p^m-1} = 1 \text{ da proposição 4.2.6.} \\ &= 0 \end{aligned}$$

Logo, α^r é uma raiz n-ésima da unidade. Sendo assim, as raízes de $x^n - 1$ serão $1, \alpha^r, \alpha^{2r}, \cdots, \alpha^{(n-1)r}$. Desta forma, pela definição de polinômios minimais 4.4.1 os polinômios $\mathcal{M}_{\alpha^{ir}}(x)$ são divisores de $x^n - 1$ para todo $0 \leqslant i \leqslant n-1$. Para determinarmos a fatoração de $x^n - 1$ basta determinarmos os polinômios minimais distintos entre $\mathcal{M}_{\alpha^0}(x), \mathcal{M}_{\alpha^r}(x), \cdots, \mathcal{M}_{\alpha^{(n-1)r}}(x)$.

Sabemos que $\mathcal{M}_{\alpha^{ir}}(x) = \mathcal{M}_{\alpha^{jr}}(x)$ se, e somente se, ir e jr estão na mesma classe ciclotômica módulo $p^m - 1 = rn$ e como $mdc(r, rn) = r$, então a proposição 3.1.4 nos garante

$$ir \equiv jr \bmod rn \Leftrightarrow i \equiv j \bmod n.$$

Logo os polinômios distintos entre $\mathcal{M}_{\alpha^0}(x), \mathcal{M}_{\alpha^r}(x), \cdots, \mathcal{M}_{\alpha^{(n-1)r}}(x)$ são $\mathcal{M}_{C_{0r}}, \mathcal{M}_{C_{1r}}, \cdots, \mathcal{M}_{C_{tr}}$, pois os índices $i's$ são representantes de classes ciclotômicas de p módulo n, logo são distintos.

□

Exemplo 4.5.4. Considere o polinômio $x^{13} - 1$ sobre $\mathbb{Z}_3$. Vamos inicialmente encontrar os representantes das classes ciclotômicas de $p = 3$ módulo 13.

$$\begin{aligned} C_0 &= \{0\} \\ C_1 &= \{1, 3, 9\} \\ C_2 &= \{2, 6, 5\} \\ C_4 &= \{4, 12, 10\} \\ C_7 &= \{7, 8, 11\} \end{aligned}$$

Logo, $\{C_0, C_1, C_2, C_4, C_7\}$ é o conjunto completo de classes ciclotômicas de $p = 3$ módulo $n = 13$. Como $mdc(3^3, 13) = 1$ e $13|(3^3 - 1)$ então tomamos $m = 3$ e consideramos o corpo $\mathbb{F}_{3^3}$. Considere o polinômio irredutível $1 + 2x + x^3$, por inspeção $\alpha = x \in \mathbb{F}_{3^3}$ é primitivo. Além disso, $r = \dfrac{3^3 - 1}{13} = 2$, sendo assim, do teorema acima procuramos

os polinômios minimais das classes ciclotômicas $C_{2\cdot 0}, C_{2\cdot 1}, C_{2\cdot 2}, C_{2\cdot 4}$ e $C_{2\cdot 7}$ de 3 módulo $3^3 - 1 = 26$, tais classes já foram determinadas no exemplo 4.4.4. Da proposição 4.4.2, segue

$$\begin{aligned}
C_0 &= \{0\} \Rightarrow \mathcal{M}_{\alpha^0}(x) = (x - \alpha^0) = x - 1 = 2 + x \\
C_2 &= \{2, 6, 18\} \Rightarrow \mathcal{M}_{\alpha^2}(x) = (x - \alpha^2)(x - \alpha^6)(x - \alpha^{18}) = 2 + x + x^2 + x^3 \\
C_4 &= \{4, 10, 12\} \Rightarrow \mathcal{M}_{\alpha^4}(x) = (x - \alpha^4)(x - \alpha^{10})(x - \alpha^{12}) = 2 + x^2 + x^3 \\
C_8 &= \{8, 20, 24\} \Rightarrow \mathcal{M}_{\alpha^8}(x) = (x - \alpha^8)(x - \alpha^{20})(x - \alpha^{24}) = 2 + 2x + 2x^2 + x^3 \\
C_{14} &= \{14, 16, 22\} \Rightarrow \mathcal{M}_{\alpha^{14}}(x) = (x - \alpha^{14})(x - \alpha^{16})(x - \alpha^{22}) = 2 + 2x + x^3
\end{aligned}$$

Do teorema 4.5.3, segue

$$\begin{aligned}
x^{13} - 1 &= \mathcal{M}_{\alpha^0}(x)\mathcal{M}_{\alpha^2}(x)\mathcal{M}_{\alpha^4}(x)\mathcal{M}_{\alpha^8}(x)\mathcal{M}_{\alpha^{14}}(x) \\
&= (2 + x)(2 + x + x^2 + x^3)(2 + x^2 + x^3)(2 + 2x + 2x^2 + x^3)(2 + 2x + x^3).
\end{aligned}$$

CAPÍTULO 5

Códigos Cíclicos

Um código cíclico é uma subclasse dos códigos lineares (para saber mais sobre os códigos lineares consulte [6, capítulo 5, página 85-111]). Estudado inicialmente por Prange [9] em 1957, os códigos cíclicos são muito utilizados nas aplicações por possuírem bons algoritmos de codificação e decodificação. Nesses códigos é possível obter uma nova palavra apenas por uma mudança cíclica em uma palavra já pertencente ao código, como veremos adiante.

Neste capítulo, considere o produto cartesiano de n cópias de $\mathbb{Z}_p$, ou seja,

$$\mathbb{Z}_p^n = \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n \text{ vezes}}.$$

$\mathbb{Z}_p^n$ é um espaço vetorial definido sobre o corpo $\mathbb{Z}_p$ (veja mais detalhes em [2, capítulo 3, páginas 31-47]). O anel $\mathbb{Z}_p[x]/(x^n-1)$ é isomorfo a $\mathbb{Z}_p^n$ através da transformação linear:

$$\begin{aligned} \mathcal{T} : \mathbb{Z}_p^n &\longrightarrow \mathbb{Z}_p[x]/(x^n-1) \\ (a_0\, a_1 \cdots a_{n-1}) &\longmapsto a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \end{aligned}$$

E denotamos por: $\mathbb{Z}_p^n \cong \mathbb{Z}_p[x]/(x^n-1)$, como espaço vetorial sobre $\mathbb{Z}_p$.

Uma base de $\mathbb{Z}_p[x]/(x^n-1)$ é $[1], [x], [x]^2, \cdots, [x]^{n-1}$, pois para todo $[p(x)] \in \mathbb{Z}_p[x]/(x^n-1)$ temos que

$$\begin{aligned} [p(x)] &= [a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}] \\ &= a_0[1] + a_1[x] + \cdots + a_{n-1}[x]^{n-1}. \end{aligned}$$

Além disso, se $a_0[1]+a_1[x]+\cdots+a_{n-1}[x]^{n-1} = [0]$, então $[a_0+a_1x+\cdots+a_{n-1}x^{n-1}] = [0]$, ou seja, $s(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in (x^n - 1)$. Se $s(x) \neq 0$, então $s(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} = (x^n - 1)t(x)$, para algum $t(x) \in \mathbb{Z}_p[x]$. Mas se isso ocorre temos uma contradição, já que $gr(s) < n$. Logo $s(x) = 0$ e $a_0 = a_1 = \cdots = a_{n-1} = 0$.

Sendo assim, é possível 'transportar' um subconjunto C de $\mathbb{Z}_p^n$ para $\mathbb{Z}_p[x]/(x^n - 1)$, veremos isso com mais detalhes no decorrer deste capítulo. Observe ainda que os elementos de $\mathbb{Z}_p[x]/(x^n-1)$ são classes residuais módulo x^n-1, no entanto iremos omitir os colchetes, a fim de simplificar a notação. Da transformação linear acima segue que vetores em $\mathbb{Z}_p^n$ correspondem a polinômios em $\mathbb{Z}_p[x]/(x^n - 1)$. Por exemplo:

Elementos de $\mathbb{Z}_3^2$	Elementos de $\mathbb{Z}_3[X]/(x^2 - 1)$
$(0\,0)$	0
$(1\,0)$	1
$(2\,0)$	2
$(0\,1)$	x
$(1\,1)$	$1 + x$
$(2\,1)$	$2 + x$
$(0\,2)$	$2x$
$(1\,2)$	$1 + 2x$
$(2\,2)$	$2 + 2x$

5.1 Códigos Cíclicos

Definição 5.1.1. Dizemos que um código $C \subset \mathbb{Z}_p^n$ é um código cíclico se:

1. C é um subespaço vetorial de $\mathbb{Z}_p^n$;
2. $\forall c = (c_0 \cdots c_{n-1}) \in C \Rightarrow (c_{n-1}\, c_0 \cdots c_{n-2}) \in C$.

Exemplo 5.1.2. $C = \{v_1, v_2, v_3, v_4\} \subset \mathbb{Z}_2^2$, com $v_1 = (0\,0)$, $v_2 = (1\,0)$, $v_3 = (0\,1)$, $v_4 = (1\,1)$ é um código cíclico, já que por inspeção temos:

$$v_1 = (0\,0) \in C \Rightarrow (0\,0) \in C$$
$$v_2 = (1\,0) \in C \Rightarrow (0\,1) \in C$$
$$v_3 = (0\,1) \in C \Rightarrow (1\,0) \in C$$
$$v_4 = (1\,1) \in C \Rightarrow (1\,1) \in C$$

Além disso, é fácil ver que C é um subespaço vetorial de $\mathbb{Z}_2^2$.

Podemos ainda caracterizar os códigos cíclicos algebricamente, pois como já dito $\mathbb{Z}_p^n$ é isomorfo a $\mathbb{Z}_p[x]/(x^n - 1)$, ou seja, podemos tratar os elementos de $\mathbb{Z}_p^n$ como polinômios

em $\mathbb{Z}_p[x]/(x^n-1)$.

Sendo assim, observe que $c(x) \in \mathbb{Z}_p[x]/(x^n-1)$ quando multiplicado por x tem seus coeficientes permutados, veja:

$$\begin{aligned} xc(x) &= x(a_o + a_1x + \cdots + a_{n-1}x^{n-1}) \\ &= a_0x + a_1x^2 + \cdots + a_{n-1}x^n \\ &= a_{n-1} + a_0x + a_1x^2 + \cdots + a_{n-2}x^{n-1} \end{aligned}$$

Acima, usamos o fato que $x^n \equiv 1 \bmod x^n - 1$. Observe que se $c = (a_0\, a_1 \cdots a_{n-1})$ é o correspondente de $c(x)$, então $xc(x)$ corresponde ao vetor $(a_{n-1}\, a_0\, a_1 \cdots a_{n-2})$, ou seja, o deslocamento cíclico das coordenadas de c é dada pela multiplicação de $c(x)$ por x. Em geral, $x^ic(x)$ corresponde ao vetor $(a_{n-1}, a_{n-(i+1)}, \cdots, a_i, a_{n-(i-1)}) \in \mathbb{Z}_p^n$, com $1 \leqslant i \leqslant n+1$.

Dado o isomorfismo

$$\begin{aligned} \mathcal{T} : \mathbb{Z}_p^n \quad &\longrightarrow \quad \mathbb{Z}_p[x]/(x^n-1) \\ (a_0\, a_1 \cdots a_{n-1}) &\longmapsto a_0 + a_1x + \cdots + a_{n-1}x^{n-1}. \end{aligned}$$

Vamos identificar $\mathcal{T}(C) = I$ com o próprio C, onde C é um subconjunto não vazio de $\mathbb{Z}_p^n$.

Teorema 5.1.1. *Um subespaço vetorial C de $\mathbb{Z}_p^n \cong \mathbb{Z}_p[x]/(x^n-1)$ é um código cíclico se, e somente se, C é um ideal de $\mathbb{Z}_p[x]/(x^n-1)$.*

Demonstração. ($\Rightarrow$) Sendo C um subespaço vetorial de $\mathbb{Z}_p^n$ segue que C é fechado para adição, satisfazendo uma condição de ideal. Além disso, sabemos que C é um código cíclico, então de $c(x) \in C$ segue que $x^ic(x) \in C$, com $i \in \mathbb{N}$. Considere $a(x) \in \mathbb{Z}_p[x]/(x^n-1)$, com $a(x) = \sum_{i=0}^{n-1} a_ix^i$, pois $1, x, \cdots, x^{n-1}$ é base de $\mathbb{Z}_p[x]/(x^n-1)$. Temos que:

$$\begin{aligned} c(x)a(x) &= \sum_{i=0}^{n-1} c(x)a_ix^i \\ &= \sum_{i=0}^{n-1} a_ic(x)x^i \end{aligned}$$

Como em C a multiplicação por escalar é fechada, segue que $c(x)a(x) \in C$, cumprindo as condições necessárias para que C seja um ideal de $\mathbb{Z}_p[x]/(x^n-1)$.
($\Leftarrow$) Segue direto da definição de ideal que C é subespaço vetorial de $\mathbb{Z}_p^n$. Também, como C é um ideal de $\mathbb{Z}_p[x]/(x^n-1)$, então para todo $c(x) \in C$ e $a(x) \in \mathbb{Z}_p[x]/(x^n-1)$ temos

que $a(x)c(x) \in C$. Em particular fazendo $a(x) = x^i$, com $i \in \mathbb{N}$, temos que $x^i c(x) \in C$. Logo, C é um código cíclico. □

Sabemos que $\mathbb{Z}_p[x]$ é um anel de ideais principais (Teorema 4.1.1), sendo assim $\mathbb{Z}_p[x]/(x^n - 1)$ também o será [8, página 80]. Desta forma, temos que todo ideal não nulo I de $\mathbb{Z}_p[x]/(x^n - 1))$ é gerado por um polinômio mônico de menor grau possível em I. Ou seja, todo código cíclico C é gerado por um único polinômio mônico de menor grau em C.

Definição 5.1.3. Se $C \subset \mathbb{Z}_p^n$ é um código cíclico, com $C = (g(x))$, então dizemos que $g(x)$ é o *polinômio gerador* de C e $h(x) = \dfrac{x^n - 1}{g(x)}$ é o *polinômio verificador* de C.

Observe que o polinômio gerador $g(x)$ é necessariamente um fator de $x^n - 1$. Caso contrário teríamos $x^n - 1 = q(x)g(x) + r(x)$, para algum $q(x)$ com $gr(r) < gr(g)$ e $r(x) \neq 0$, mas note que $x^n - 1$ equivale a zero em $\mathbb{Z}_p^n \cong \mathbb{Z}_p[x]/(x^n - 1)$ e $x^n - 1 \in C$, também $g(x)q(x) \in C$, sendo assim segue que $r(x) \in C$, mas isso é um absurdo (pois $g(x)$ tem grau mínimo em C e $gr(r) < gr(g)$), a menos que $r(x) = 0$. Portanto, segue que $g(x)|(x^n - 1)$.

Exemplo 5.1.4. Considere o subespaço vetorial $C = \{000, 110, 011, 101\}$ de $\mathbb{Z}_2^3 \cong \mathbb{Z}_2[x]/(x^3 - 1)$. Utilizando a representação polinomial obtemos $C = \{0, 1 + x, x + x^2, 1 + x^2\}$, note que C é um código cíclico, já que:

$$\begin{aligned} 0 \in C &\Rightarrow x \cdot 0 = 0 \in C, \\ (1 + x) \in C &\Rightarrow x(x + 1) = x + x^2 \in C \\ (x + x^2) \in C &\Rightarrow x(x^2 + x) = x^3 + x^2 = 1 + x^2 \in C \\ (1 + x^2) \in C &\Rightarrow x(1 + x^2) = x + x^3 = 1 + x \in C. \end{aligned}$$

Além disso, o único polinômio mônico de menor grau em C é $1 + x$ e $(1 + x)|(x^3 - 1)$, sendo assim $C = (1 + x)$. Ou seja, o polinômio gerador do código C é $g(x) = 1 + x$ e o polinômio verificador é $h(x) = \dfrac{x^3 - 1}{1 + x} = x^2 + x + 1$.

Teorema 5.1.2. *Seja $C \subset \mathbb{Z}_p[x]/(x^n - 1)$, com $C = (g(x))$ e $gr(g) = r$. Então*

$$g(x),\ xg(x),\ x^2g(x), \cdots, x^{n-r-1}g(x)$$

é uma base de C sobre $\mathbb{Z}_p$.

Demonstração. Primeiro vamos mostrar que $g(x),\ xg(x), \cdots, x^{n-r-1}g(x)$ são Linearmente

Independentes $(L.I)$. Sejam $a_0, a_1, \cdots, a_{n-1} \in \mathbb{Z}_p$, tais que:

$$a_0 g(x) + a_1 x g(x) + \cdots + a_{n-r-1} x^{n-r-1} g(x) = 0$$
$$g(x)(a_0 + a_1 x + \cdots + a_{n-r-1} x^{n-r-1}) = 0$$

Sendo assim, em $\mathbb{Z}_p[x]$, temos que existe $q(x)$, tal que:

$$g(x)(a_0 + a_1 x + \cdots + a_{n-r-1} x^{n-r-1}) = q(x)(x^n - 1)$$

Considere $h(x)$ o polinômio verificador de C. Então $h(x) = \dfrac{x^n - 1}{g(x)}$ e

$$a_0 + a_1 x + \cdots + a_{n-r-1} x^{n-r-1} = q(x)h(x)$$

Observe que no primeiro membro da equação acima temos $gr(a_0 + a_1 x + \cdots + a_{n-r-1} x^{n-r-1}) \leqslant n - r - 1$, no entanto $gr(h) = n - r$, logo devemos ter $q(x) = 0$. E

$$a_0 + a_1 x + \cdots + a_{n-r-1} x^{n-r-1} = 0 \Rightarrow a_0 = a_1 = \cdots = a_{n-r-1} = 0.$$

Além disso, qualquer que seja $f(x) \in C$, temos que $f(x) \equiv t(x)g(x) \mod (x^n - 1)$, para algum $t(x) \in \mathbb{Z}_p[x]$. E, existem $q(x), r(x) \in \mathbb{Z}_p[x]$, com $r(x) = 0$ ou $gr(r) < gr(h) = n - r$, tais que, $t(x) = q(x)h(x) + r(x)$. Logo,

$$f(x) \equiv t(x)g(x) \mod (x^n - 1)$$
$$f(x) \equiv (q(x)h(x) + r(x))g(x) \mod (x^n - 1)$$
$$f(x) \equiv q(x)(x^n - 1) + r(x)g(x) \mod (x^n - 1)$$
$$f(x) \equiv r(x)g(x) \mod (x^n - 1).$$

Ou seja, $f(x) = r(x)g(x)$ em $\mathbb{Z}_p[x]/(x^n - 1)$. Logo, tomando $r(x) = a_0 + a_1 x + \cdots + a_{n-r-1} x^{n-r-1}$, temos $f(x) = a_0 g(x) + a_1 x g(x) + \cdots + a_{n-r-1} x^{n-r-1} g(x)$.

Portanto, $g(x)$, $xg(x) \cdots, x^{n-r-1} g(x)$ é uma base de C sobre $\mathbb{Z}_p$. □

Uma vez que uma base de C é da forma $\mathcal{B} = \{g(x), xg(x), x^2 g(x), \cdots, x^{n-r-1} g(x)\}$, podemos concluir que C tem dimensão $n - r$ e denotamos por $dim(C) = n - r$.

Definição 5.1.5. Seja $C = (g(x)) \subset \mathbb{Z}_p[x]/(x^n - 1)$ um código cíclico, com $g(x) = g_0 + g_1 x + \cdots + g_r x^r$, com $g_o, g_1, \cdots, g_r \in \mathbb{Z}_p$ e $g_r \neq 0$. Considere a matriz

G de ordem $(n-r)\times n$, cujas linhas são determinadas pelos coeficientes de $g(x)$, isto é,

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_r & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_r & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & g_0 & \cdots & \dots & g_r \end{pmatrix}$$

A matriz G é chamada *Matriz Geradora* de C associada ao polinômio gerador $g(x)$.

Exemplo 5.1.6. Considere o código cíclico $C \subset \mathbb{Z}_2^3$ do exemplo 5.1.4. Como $C = (1+x)$, então a matriz geradora G do código C será:

$$G = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Proposição 5.1.3. *Considere o código cíclico $C = (g(x)) \subset \mathbb{Z}_p[x]/(x^n-1)$. Então*

$$c(x) \in C \Leftrightarrow c(x)h(x) \equiv 0 \ mod\,(x^n-1)$$

.

Demonstração. Seja $c(x) \in \mathbb{Z}_p[x]$ um polinômio qualquer. Desta forma:

$$\begin{aligned} c(x) \in C &\Leftrightarrow c(x) = q(x)g(x) \text{ para algum } q(x) \in \mathbb{Z}_p[x] \\ &\Leftrightarrow c(x)h(x) = q(x)g(x)h(x) \\ &\Leftrightarrow c(x)h(x) = q(x)(x^n-1) \\ &\Leftrightarrow c(x)h(x) \equiv 0 \bmod (x^n-1). \end{aligned}$$

□

Definição 5.1.7. Dado um código cíclico $C \subset \mathbb{Z}_p^n$, chamamos o conjunto $C^\perp$ de código dual de C, tal que

$$C^\perp = \{v \in \mathbb{Z}_p^n; < v, u >= 0, \forall u \in C\}^1.$$

Definição 5.1.8. A matriz geradora de $C^\perp$ é chamada de *Matriz Teste de Paridade* do código cíclico C.

Lema 5.1.4. *Seja $C \subset \mathbb{Z}_p^n$ um código cíclico com matriz geradora G. Então*

$$v \in C^\perp \Leftrightarrow Gv^t = 0.$$

[1] Onde $< u, v >$ é definido como segue: $< u, v >= u_0v_0 + u_1v_1 + \cdots + u_{n-1}v_{n-1}$, com $u = (u_o\, u_1 \cdots u_{n-1}) \in \mathbb{Z}_p^n$ e $v = (v_0\, v_1 \cdots v_{n-1}) \in \mathbb{Z}_p^n$.

Ou seja, $v \in C^{\perp}$ se, e somente se, v é ortogonal a cada linha de G.

Demonstração. ($\Rightarrow$) Seja g_i a i-ésima linha de G. Note que $g_i \in C$, para todo $i = 1, \cdots, n-r$.
Se $v \in C^{\perp}$, então da definição 5.1.7 segue que $< v, c >= 0$, para todo $c \in C$, em particular, v é ortogonal a g_i e como $Gv^t = \begin{pmatrix} < v, g_1 > \\ < v, g_2 > \\ \vdots \\ < v, g_{n-r} > \end{pmatrix}$, temos que $Gv^t = 0$.
($\Leftarrow$) Supondo $Gv^t = 0$, temos que $< v, g_i >= 0$, para $i = 1, \cdots, n-r$. Seja $c \in C$, então c pode ser escrito como $c = a_1 g_1 + \cdots + a_{n-r} g_{n-r}$, com $a_1, \cdots, a_{n-r} \in \mathbb{Z}_p$. E

$$\begin{aligned} < v, c > &= < v, a_1 g_1 + \cdots + a_{n-r} g_{n-r} > \\ &= < v, a_1 g_1 > + \cdots + < v, a_{n-r} g_{n-r} > \\ &= a_1 < v, g_1 > + \cdots + a_{n-r} < v, g_{n-r} > \\ &= 0 \end{aligned}$$

Logo, $v \in C^{\perp}$. □

Lema 5.1.5. *Seja $C \subset \mathbb{Z}_p^n$ um código cíclico de dimensão $n-r$, então $dim(C^{\perp}) = r$.*

Demonstração. A demonstração deste fato pode ser encontrada em [6, páginas 94-95]. □

Observe que a matriz H de ordem $(r \times n)$ com linhas linearmente independentes é uma matriz teste de paridade de C se , e somente se, $GH^t = 0$.

De fato, se H é uma matriz teste de paridade de C, então H é geradora de $C^{\perp}$ e portanto as r linhas de H (h_j) são elementos de $C^{\perp}$, deste forma segue que $< g_i, h_j >= 0$, já que $g_i \in C$. E como

$$GH^t = \begin{pmatrix} < g_1, h_1 > & < g_1, h_2 > & \cdots & < g_1, h_r > \\ < g_2, h_1 > & < g_2, h_2 > & \cdots & < g_2, h_r > \\ \vdots & \vdots & & \vdots \\ < g_{n-r}, h_1 > & < g_{n-r}, h_2 > & \cdots & < g_{n-r}, h_r > \end{pmatrix},$$

então $GH^t = 0$.

Por outro lado, se $GH^t = 0$, então $h_j \in C^{\perp}$ e $h_1, \cdots, h_r$ são linearmente independentes. Sabemos também que $dim(C^{\perp}) = r$, logo as linhas de H geram $C^{\perp}$, ou seja, H é uma matriz teste de paridade de C.

Para o próximo lema recorde que o polinômio recíproco de $f(x) \in \mathbb{Z}_p[x]$ é dado por $f^{\mathrm{R}}(x) = x^{gr(f)} f(x^{-1})$.

Lema 5.1.6. *Sejam $f(x), g(x) \in \mathbb{Z}_p[x]$, onde $g(x)|f(x)$ e $gr(f) = n$. Então polinômio recíproco de $g(x)$ divide o recíproco de $f(x)$.*

Demonstração. Da hipótese sabemos que existe $h(x) \in \mathbb{Z}_p[x]$, tal que $f(x) = g(x)h(x)$, com $n = gr(g) + gr(h)$, de modo que $f(x^{-1}) = g(x^{-1})h(x^{-1})$. Sendo assim,

$$f^{\mathtt{R}}(x) = x^{gr(f)}f(x^{-1}) = x^n g(x^{-1})h(x^{-1}) = x^{gr(g)}g(x^{-1})x^{gr(h)}h(x^{-1}) = g^{\mathtt{R}}(x)h^{\mathtt{R}}(x).$$

Logo, $g^{\mathtt{R}}(x)|f^{\mathtt{R}}(x)$. □

Do lema acima, ao considerarmos $f(x) = x^n - 1$ e $g(x)$ um divisor de $f(x)$, segue que $g^{\mathtt{R}}(x)|f(x)$. Basta notarmos que $f^{\mathtt{R}}(x) = -f(x)$.

Para o próximo teorema considere $h^{\mathtt{R}}(x)$ o polinômio recíproco do polinômio verificador $h(x)$ do código cíclico C, ou seja, $h(x) = \dfrac{x^n - 1}{g(x)}$, onde $g(x)$ é o polinômio gerador de C e $gr(g) = r$.

Teorema 5.1.7. *Se $C = (g(x)) \subset \mathbb{Z}_p[x]/(x^n - 1)$, com $g(x)|(x^n - 1)$ é um código cíclico, então $C^{\perp}$ é um código cíclico de $\mathbb{Z}_p[x]/(x^n - 1)$ e $C^{\perp} = (h^{\mathtt{R}}(x))$.*

Demonstração. Considere

$$g(x) = g_0 + g_1x + \cdots + g_rx^r \text{ e } h(x) = h_0 + h_1x + \cdots + h_{n-r}x^{n-r}.$$

Onde $g_r \neq 0$, note que necessariamente $h_{n-r} \neq 0$, já que $h(x)$ é o polinômio verificador de C e portanto $gr(h) = n - r$. Do lema 5.1.6 e do teorema 5.1.2 segue $h^{\mathtt{R}}(x)$ divide $x^n - 1$, sendo assim $(h^{\mathtt{R}}(x))$ é um código cíclico com base $\mathcal{B} = \{h^{\mathtt{R}}(x), xh^{\mathtt{R}}(x), \cdots, x^{r-1}h^{\mathtt{R}}(x)\}$, ou seja, tais termos são linearmente independentes. E a matriz geradora de $(h^{\mathtt{R}}(x))$ é dada por:

$$H = \begin{pmatrix} h_{n-r} & h_{n-r-1} & \dots & h_0 & 0 & \dots & 0 \\ 0 & h_{n-r} & h_{n-r-1} & \dots & h-0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & h_{n-r} & \cdots & \dots & h_0 \end{pmatrix}_{r\times n}$$

Além disso, a matriz geradora de C é:

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_r & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_r & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & g_0 & \cdots & \dots & g_r \end{pmatrix}_{(n-r)\times n}$$

Queremos mostrar que $GH^t = 0$. Escrevendo as linhas de G (G_i) e as colunas de H^t (H_j)

na base canônica de $\mathbb{Z}_p^n$,$\{e_1, \cdots, e_n\}$, temos que:

$$G_i = g_0 e_i + g_1 e_{i+1} + \cdots + g_r e_{i+r}, \quad \text{com } 1 \leqslant i \leqslant n-r.$$

E

$$H_j = h_{n-r} e_j + h_{n-r-1} e_{j+1} + \cdots + h_0 e_{j+n-r}, \quad \text{com } 1 \leqslant j \leqslant r.$$

Desta forma, temos:

$$GH^t = \begin{pmatrix} < G_1, H_1 > & < G_1, H_2 > & \cdots & < G_1, H_j > & \cdots & < G_1, H_r > \\ < G_2, H_1 > & < G_2, H_2 > & \cdots & < G_2, H_j > & \cdots & < G_2, H_r > \\ \vdots & \vdots & & \vdots & & \vdots \\ < G_i, H_1 & < G_i, H_2 > & \cdots & < G_i, H_j > & \cdots & < G_i, H_r > \\ \vdots & \vdots & & \vdots & & \vdots \\ < G_{n-r}, H_1 > & < G_{n-r}, H_2 > & \cdots & < G_{n-r}, H_j > & \cdots & < G_{n-r}, H_r > \end{pmatrix}_{(n-r)\times r}$$

Onde o termo $< G_i, H_j >$, supondo $i \leqslant j$, é dado por:

$$g_{j-i} h_{n-r} + g_{j-i+1} h_{n-r-1} + \cdots + g_{n-r} h_{j-i}, \text{ com } 0 \leqslant j-i \leqslant r-1.$$

Observe que $< G_i, H_j >$ equivale a $c_{n-r+j-i} = \sum_{k+t=n-r+j-i} g_k \cdot h_t$, que por sua vez é o coeficiente de $x^{(n-r)+(j-i)}$ no produto $g(x)h(x) = x^n - 1$. E supondo $n > 1$, temos

$$0 \leqslant j-i \leqslant r-1 \Rightarrow 1 < n-r+j-i \leqslant n-1,$$

desta forma ,segue que $GH^t = 0$. O caso em que $i > j$ é análogo. Logo H é a matriz geradora de $C^\perp$ e consequentemente $C^\perp = (h^{\mathrm{R}}(x))$. □

Exemplo 5.1.9. Considere o código cíclico $C = (g(x)) \subset \mathbb{Z}_3^{11}$, com $g(x) = 2 + x^2 + 2x^3 + x^4 + x^5$, a matriz geradora de C é

$$G = \begin{pmatrix} 2 & 0 & 1 & 2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 2 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 1 & 2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 2 & 1 & 1 \end{pmatrix}$$

Note que $h(x) = \dfrac{x^{11}-1}{2+x^2+2x^3+x^4+x^5} = 1 + 2x^4 + 2x^5 + x^6$ e portanto $h^{\mathrm{R}}(x) = 1 + 2x +$

$2x^2 + x^6$. Além disso, $C^{\perp} = (1 + 2x + 2x^2 + x^6)$ e a matriz teste de paridade de C é

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 2 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 2 & 1 \end{pmatrix}.$$

5.2 Codificação e Decodificação em Códigos Cíclicos

Nesta seção mostraremos a codificação e a decodificação em códigos cíclicos, esses processos são necessários para a transmissão de um dado digital, recordemos que no momento da transmissão de dados podem ocorrer ruídos alterando o dado original. Veja a ilustração do processo completo de transmissão de dados:

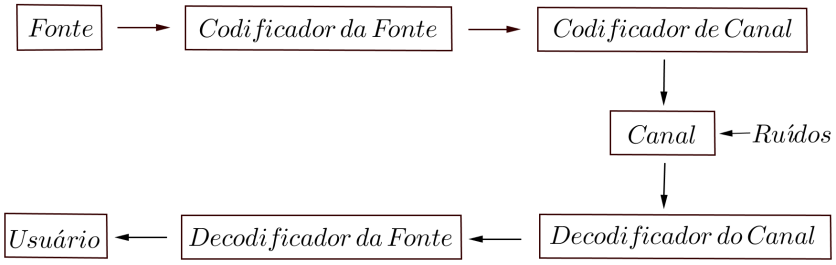


Figura 2: Sistema Digital

Fonte: autora

Quando nos referimos a codificação estamos tratando da transformação do código da fonte em código do canal, também em relação a decodificação é o processo que transforma o código do canal em código da fonte. Agora, apresentaremos meios de identificar erros na mensagem recebida, bem como em que situação é possível sua correção e como isso é feito.

Definição 5.2.1. Dizemos que uma matriz geradora G de um código cíclico $C \subset \mathbb{Z}_p[x]/(x^n - 1)$ de dimensão $n - r$ está na forma padrão se $G = (Id_{n-r}|A)$, onde Id_{n-r} é matriz identidade $(n - r) \times (n - r)$ e A é uma matriz de ordem $(n - r) \times (r)$.

Exemplo 5.2.2. A partir da matriz geradora do exemplo 5.1.9, vamos encontrar uma matriz equivalente a G que esteja na forma padrão. Para isso, vamos efetuar operações elementares de escalonamento como segue:

$$\begin{pmatrix}20121100000\\02012110000\\00201211000\\00020121100\\00002012110\\00000201211\end{pmatrix}\begin{matrix}L_1\to 2L_1\\L_2\to 2L_2\end{matrix}\quad\begin{pmatrix}10212200000\\01021220000\\00201211000\\00020121100\\00002012110\\00000201211\end{pmatrix}\begin{matrix}L_1\to L_1-L_3\\L_3\to 2L_3\\L_4\to L_2-L_4\end{matrix}\quad\begin{pmatrix}10011022000\\01021220000\\00102122000\\00020121100\\00002012110\\00000201211\end{pmatrix}\begin{matrix}L_1\to L_1+L_4\\L_2\to L_2-L_4\\L_4\to 2L_4\end{matrix}$$

$$\begin{pmatrix}10001110100\\01001102200\\00102122000\\00010212200\\00002012110\\00000201211\end{pmatrix}\begin{matrix}L_1\to L_1+L_5\\L_2\to L_2+L_5\\L_3\to L_3-L_5\\L_5\to 2L_5\end{matrix}\quad\begin{pmatrix}10000122210\\01000111010\\00100111220\\00010212200\\00001021220\\00000201211\end{pmatrix}\begin{matrix}L_1\to L_1+L_6\\L_2\to L_2+L_6\\L_3\to L_3+L_6\\L_4\to L_4-L_6\\L_6\to 2L_6\end{matrix}\quad\begin{pmatrix}10000020121\\01000012221\\00100011101\\00010011022\\00001021220\\00000102122\end{pmatrix}.$$

Logo, a uma matriz geradora de C na forma padrão é:

$$G'=\begin{pmatrix}10000020121\\01000012221\\00100011101\\00010011022\\00001021220\\00000102122\end{pmatrix}$$

.

Para o próximo teorema considere a matriz R de ordem $(n-r)\times r$ cuja i-ésima linha é dada pela representação vetorial de $-r_i(x)$, onde $r_i(x)$ é o resto da divisão de x^{r-1+i} por $g(x)$ e $gr(g)=r$.

Por exemplo se $g(x)=x^3+x+1\in\mathbb{Z}_2[x]$, com $n=7$ e $gr(g)=3$, então a matriz R terá ordem 4×3, e ainda:

Algoritmo Euclidiano	Representação Polinomial $(-r_i(x))$	Representação Vetorial $(-r_i)$
$x^3=(x^3+x+1)+(x+1)$	$1+x$	(110)
$x^4=(x^3+x+1)x+(x^2+x)$	$x+x^2$	(011)
$x^5=(x^3+x+1)(x^2+1)+(x^2+x+1)$	$1+x+x^2$	(111)
$x^6=(x^3+x+1)(x^3+x+1)+(x^2+1)$	$1+x^2$	(101)

Logo, a matriz procurada será:

$$R = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

Teorema 5.2.1. *Seja $C \subset \mathbb{Z}_p[x]/(x^n - 1)$ um código cíclico, com $C = (g(x))$ e $gr(g) = r$. Então $(R|Id_{n-r})$ é uma matriz geradora de C.*

Demonstração. A demonstração desse fato encontra-se em [6, páginas 122-123]. □

Exemplo 5.2.3. Considere o código cíclico $C \subset \mathbb{Z}_5^8$, gerado por $g(x) = x^4 + 1$ sobre $\mathbb{Z}_5$. Observe que $dim(C) = n - r = 4$. Para encontrarmos a matriz $R_{(4\times4)}$, façamos:

Algoritmo Euclidiano	Representação Polinomial $(-r_i(x))$	Representação Vetorial $(-r_i)$
$x^4 = (x^4 + 1) + (4)$	1	1000
$x^5 = (x^4 + 1)x + (4x)$	x	0100
$x^6 = (x^4 + 1)(x^2) + (4x^2)$	x^2	0010
$x^7 = (x^4 + 1)(x^3) + (4x^3)$	x^3	0001

Desta forma, do teorema 5.2.1 segue que a matriz geradora de C é dada por:

$$G' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

5.2.4 Codificação em Códigos Cíclicos

Considere um código cíclico $C \subset \mathbb{Z}_p^n$, com polinômio gerador $g(x)$ e $gr(g) = r$. Os elementos de $\mathbb{Z}_p^{n-r}$ podem ser codificados pelos elementos de C.

Suponhamos que a matriz geradora de C esteja na forma $(R|Id_{n-r})$, dado a mensagem $u = (u_0\, u_1 \cdots u_{n-r-1})$ podemos codificá-la como segue:

$$c = u(R|Id_{n-r}) = (uR|u)$$

Exemplo 5.2.5. Considere o código cíclico utilizado no exemplo acima, vamos codificar

a mensagem $m = (1\,4\,1\,3) \in \mathbb{Z}_5^4$ a partir da matriz geradora G':

$$\begin{aligned} c =& m(R|Id_{n-r}) \\ =& (1\,4\,1\,3) \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \\ =& (1\,4\,1\,3\,1\,4\,1\,3). \end{aligned}$$

A método de codificação apresentado acima é comum a qualquer código linear e para tal é necessário conhecermos a matriz geradora de C. Vamos agora apresentar um algoritmo de codificação à custa do polinômio gerador, $g(x)$, do código cíclico C.
Considere uma mensagem $u(x) = u_0 + u_1x + \cdots + u_{n-r-1}x^{n-r-1}$:

Algoritmo 1: Codificação em Códigos Cíclicos

Passo 1: Determine o resto da divisão de $x^r u(x)$ por $g(x)$, ou seja,

$$x^r u(x) = q(x)g(x) + s(x), \quad \text{com } gr(s) \leqslant r-1;$$

Passo 2: Codifique $u(x)$ por $c(x)$, onde

$$c(x) = x^r u(x) - s(x).$$

Observe no passo 2 acima que $c(x) = q(x)g(x)$, ou seja, $c(x) \in C$.

Mais detalhadamente os termos da mensagem codificada será composto por dígitos da mensagem enviada, os $n-r$ últimos termos, e dígitos de redundância, os r primeiros termos, como ilustrado abaixo.

$$c = (\underbrace{-s_0\ -s_1\ \cdots -s_{r-1}}_{\textit{dígitos de redundância}}\ \overbrace{u_0\ \cdots u_{n-r-1}}^{\textit{dígitos de mensagem}}).$$

Ou em representação polinomial,

$$c(x) = -s_0 - s_1x - \cdots - s_{r-1}x^{r-1} + u_0x^r + \cdots + u_{n-r-1}x^{n-1}.$$

Já que $s(x)$ é o resto da divisão de $x^r m(x)$ por $g(x)$, com $gr(g) = r$ e portanto $gr(s) \leqslant r-1$. Além disso, $x^r m(x) = 0 + 0x + \cdots + 0x^{r-1} + m_0x^r + \cdots + m_{n-r-1}x^{n-1}$.

Exemplo 5.2.6. Considere o código cíclico $C \subset \mathbb{Z}_5^8$ do exemplo 5.2.5, recorde que $C =$

$(1+x^4)$. Vamos codificar o elemento $m(x) \in \mathbb{Z}_5[x/(x^4-1)] \cong \mathbb{Z}_5^{8-4}$, tal que $m(x) = 1+4x+x^2+3x^3$. Note que $x^4(1+4x+x^2+3x^3) = x^4+4x^5+x^6+3x^7$. Seguindo os passos indicados acima, obtemos:

1. $3x^7+x^6+4x^5+x^4 = (3x^3+x^2+4x+1)g(x)+(2x^3+4x^2+x+4)$.
2. $c(x) = x^7+x^6+4x^5+x^4-(2x^3+4x^2+x+4) = 1+4x+x^2+3x^3+x^4+4x^5+x^6+3x^7$.

Logo a representação vetorial de $c(x)$ é dada por $(1\,4\,1\,3\,1\,4\,1\,3)$.

Teorema 5.2.2. *Seja $C \subset \mathbb{Z}_p^n$ um código cíclico de dimensão $n-r$, cuja matriz geradora $G = (R|Id_{n-r})$. Então $H = (Id_r|-R^t)$ é a matriz geradora de $C^\perp$.*

Demonstração. Seja h_i a i-ésima linha de H, com $i = 1, \cdots, r$. Como uma parte de H é composta pela matriz identidade Id_r segue que as linhas de H são linearmente independentes. E ainda,

$$GH^t = (R\ Id_{n-r}) \begin{pmatrix} Id_r \\ -R \end{pmatrix} = R\,Id_r + Id_{n-r}(-R) = R - R = 0$$

Logo, $H = (Id_r|-R^t)$ é a matriz geradora de $C^\perp$ e portanto é a matriz teste de paridade do código cíclico C. □

Definição 5.2.7. Considere $p(x) = a_0+a_1x+\cdots+a_{n-1}x^{n-1} \in \mathbb{Z}_p[x]/(x^n-1)$, chamamos de *peso* de $p(x)$ o número de coeficientes não nulos em $p(x)$. Denotamos por

$$w(p) = |\{i \in \{0, \cdots, n-1\}\,; a_i \neq 0\}|$$

O menor peso em C é denotado por $d(C)$, ou seja,

$$d(C) = min\{w(p);\, p(x) \in C\}.$$

Exemplo 5.2.8. Considere $p(x) = 6+4x+3x^5+x^7 \in \mathbb{Z}_{11}[x]/(x^8-1)$, então $w(p) = 4$.

Apresentaremos agora o conceito de síndrome, para que adiante possamos descrever um método de decodificação em códigos cíclicos.

Definição 5.2.9. Dados um código cíclico $C \subset \mathbb{Z}_p^n$ com matriz teste de paridade H e $v \in \mathbb{Z}_p^n$, com $v = (v_0\, v_1\, \cdots\, v_r)$. O vetor $S(v) = H.v^t$ é chamado de síndrome de v.

Podemos também tratar da síndrome do polinômio correspondente de v em $\mathbb{Z}_p[x]/(x^n-1)$, essa denotaremos como $S(v(x))$.

Observe que a partir do cálculo da síndrome é possível identificar se uma palavra pertence ou não a um código cíclico C, já que pelo lema 5.1.4 segue que $v \in C \Leftrightarrow Hv^t = 0$. Sendo assim, se $S(v) \neq 0$, então existe um vetor $\mathbf{e}$ erro, o qual definiremos como segue:

$$\mathbf{e} = m - c,$$

onde m é a mensagem recebida e c a mensagem transmitida. Note que o peso do vetor $\mathbf{e}$ corresponde ao número de erros cometidos entre a transmissão e a recepção da mensagem, ou seja, ao número de coordenadas distintas de m em relação a c. E ainda, $\mathbf{e}$ e m possuem a mesma síndrome, de fato

$$\begin{aligned} S(\mathbf{e}) &= H\mathbf{e}^t = H(m-c)^t \\ &= Hm^t - Hc^t = Hm^t - 0 \\ &= S(m). \end{aligned}$$

Ainda nesta seção veremos que a síndrome pode ser calculada à custa do polinômio gerador de um código cíclico C.

Lema 5.2.3. *Seja $C \subset \mathbb{Z}_p^n$ um código cíclico e $m \in \mathbb{Z}_p^n$ uma mensagem recebida, onde o número de coordenadas distintas de m em relação a mensagem enviada c é menor ou igual $\left[\frac{d(C)-1}{2}\right]$[2]. Então existe um único vetor $\boldsymbol{e}$ com $w(\boldsymbol{e}) \leqslant \left[\frac{d(C)-1}{2}\right]$, cuja síndrome é igual a síndrome de m e tal que $c = m - \boldsymbol{e}$.*

Demonstração. A demonstração desse fato pode ser encontrada em [6, página104-105]. □

Lema 5.2.4. *Dois polinômios $a(x), b(x) \in \mathbb{Z}_p[x]/(x^n - 1)$ têm a mesma síndrome se, e somente se, $a(x) \in b(x) + C = \{b(x) + t(x);\ t(x) \in C\}$.*

Demonstração.

$$S(a) = S(b) \Leftrightarrow Ha^t = Hb^t \Leftrightarrow H(a-b)^t = 0 \Leftrightarrow a - b \in C \Leftrightarrow a \in b + C.$$

Ou utilizando notação polinomial: $a(x) \in b(x) + C$. □

Analogamente podemos mostrar que $b(x) \in a(x) + C$, sendo assim segue que dois polinômios que possuem a mesma síndrome necessariamente irão pertencer a mesma classe lateral de C em $\mathbb{Z}_p[x]/(x^n - 1)$.

Definição 5.2.10. O polinômio $p(x) \in a(x) + C$ é chamado de *líder* de sua classe se, e somente se,

$$w(p) \leqslant w(t) \qquad \forall\, t(x) \in a(x) + C.$$

[2] A notação $[p]$ representa a parte inteira do número real p.

Proposição 5.2.5. *Considere uma mensagem $u \in \mathbb{Z}_p^n$. Se $w(u)) \leqslant \left[\frac{d(C)-1}{2}\right]$, então u é o único líder da classe $u + C$.*

Demonstração. Vamos supor u e v elementos líderes da classe $u + C$, observe que se $v \in u + C$, então $u - v \in C$. Note que

$$w(u-v) \leqslant w(u) + w(v) \leqslant \frac{d(C)-1}{2} + \frac{d(C)-1}{2} = d(C) - 1 < d(C)$$

Mas se isso ocorre, então segue que $u - v = 0$ e portanto $u = v$. □

Se ainda, dado $u(x) \in \mathbb{Z}_p[x]/(x^n - 1)$, com síndrome tal que $w(S(u)) \leqslant \left[\frac{d(C)-1}{2}\right]$, então $S(u(x))$ é o líder da classe $u(x) + C$.

Teorema 5.2.6. *Seja $C = (g(x)) \subset \mathbb{Z}_p^n \cong \mathbb{Z}_p[x]/(x^n - 1)$ um código cíclico com matriz geradora na forma $(R|Id_{n-r})$ e matriz teste de paridade $H = (Id_r| - R^t)$. Se $v(x) \in \mathbb{Z}_p[x]/(x^n - 1)$ com $gr(v) \leqslant n - 1$, então a síndrome de v com relação a matriz H é o resto da divisão de $v(x)$ por $g(x)$.*

Demonstração. As colunas de $-R^t$ são da forma $r_j(x) = x^{r-1+j} - q_j(x)g(x)$, com $1 \leqslant j \leqslant r - 1$ e $r_j(x)$ é o resto da divisão de x^{r-1+j} por $g(x)$, onde $gr(g) = r$. Vamos representar cada vetor coluna de $(Id_r| - R^t)$ por seu polinômio correspondente, ou seja, $(Id_r| - R^t) = (1, x, x^2, \cdots, x^{r-1}, r_1(x), \cdots, r_{n-r}(x))$. Considere $v(x) = v_0 + v_1x + \cdots + v_{n-1}x^{n-1} \in \mathbb{Z}_p[x]/(x^n - 1)$, segue da definição 5.2.9 que a síndrome de v é $S(v) = (Id_r| - R^t)v^t$. Então

$$\begin{aligned}
S(v(x)) =& (1, x, x^2, \cdots, x^{r-1}, r_1(x), \cdots, r_{n-r}(x))v^t \\
=& v_0 + v_1x + \cdots + v_{r-1}x^{r-1} + v_r r_1(x) + \cdots + v_{n-1}r_{n-r}(x) \\
=& \sum_{i=0}^{r-1} v_i x^i + \sum_{j=1}^{n-r} v_{r+j-1} r_j(x) \\
=& \sum_{i=0}^{r-1} v_i x^i + \sum_{j=1}^{n-r} v_{r+j-1}(x^{r-1+j} - q_j(x)g(x)) \\
=& \sum_{i=0}^{r-1} v_i x^i + \sum_{j=1}^{n-r} v_{r+j-1}x^{r-1+j} - g(x)\sum_{j=1}^{n-r} v_{r+j-1}q_j(x) \\
=& v(x) - g(x)\sum_{j=1}^{n-r} v_{r+j-1}q_j(x)
\end{aligned}$$

Acima usamos o fato de que $v(x) = \sum_{i=0}^{r-1} v_i x^i + \sum_{j=1}^{n-r} v_{r+j-1}x^{r-1+j}$. Dessa forma, temos que $S(v(x))$ é o resto da divisão de $v(x)$ por $g(x)$, pois $gr(S(v(x))) \leqslant r - 1 < gr(g)$, já que é o produto de matrizes de ordem $(r \times n)$ e $(n \times 1)$. □

Exemplo 5.2.11. Considere o exemplo 5.2.3, cujo o polinômio gerador é $g(x) = 1 + x^4$, do teorema 5.2.1 segue que

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 4 \end{pmatrix}$$

é a matriz teste de paridade do código C. Para encontrarmos a síndrome do vetor $v = (43012001) \in \mathbb{Z}_5^8$ em relação a H, basta fazermos a divisão de $v(x) = 4+3x+x^3+2x^4+x^7$ por $g(x) = 1 + x^4$, onde o resto de tal será a síndrome de v, neste caso, $S(v(x)) = 2 + 3x$ ou $S(v) = (2\,3\,0\,0)$.

Exemplo 5.2.12. Considere o código cíclico $C \subset \mathbb{Z}_2^7$, com polinômio gerador $g(x) = 1 + x + x^3$:

1. Determine os elementos de C e seus respectivos pesos.
   A partir do polinômio gerador, encontramos uma base de C, a saber: $\mathcal{B} = \{(1101000), (0110100), (0011010), (0001101)\}$. Logo, os elementos de C, com seus respectivos pesos serão:

Elemento de C	Peso
$0\,(1101000) + 0\,(0110100) + 0\,(0011010) + 0\,(0001101) = (0000000)$	0
$1\,(1101000) + 0\,(0110100) + 0\,(0011010) + 0\,(0001101) = (1101000)$	3
$0\,(1101000) + 1\,(0110100) + 0\,(0011010) + 0\,(0001101) = (0110100)$	3
$0\,(1101000) + 0\,(0110100) + 1\,(0011010) + 0\,(0001101) = (0011010)$	3
$0\,(1101000) + 0\,(0110100) + 0\,(0011010) + 1\,(0001101) = (0001101)$	3
$1\,(1101000) + 1\,(0110100) + 0\,(0011010) + 0\,(0001101) = (1011100)$	4
$0\,(1101000) + 1\,(0110100) + 1\,(0011010) + 0\,(0001101) = (0101110)$	3
$0\,(1101000) + 0\,(0110100) + 1\,(0011010) + 1\,(0001101) = (0010111)$	4
$1\,(1101000) + 0\,(0110100) + 1\,(0011010) + 0\,(0001101) = (1110010)$	4
$1\,(1101000) + 0\,(0110100) + 0\,(0011010) + 1\,(0001101) = (1100101)$	4
$0\,(1101000) + 1\,(0110100) + 0\,(0011010) + 1\,(0001101) = (0111001)$	4
$1\,(1101000) + 1\,(0110100) + 1\,(0011010) + 0\,(0001101) = (1000110)$	3
$1\,(1101000) + 1\,(0110100) + 0\,(0011010) + 1\,(0001101) = (1010001)$	3
$1\,(1101000) + 0\,(0110100) + 1\,(0011010) + 1\,(0001101) = (1111111)$	7
$0\,(1101000) + 1\,(0110100) + 1\,(0011010) + 1\,(0001101) = (0100011)$	3
$1\,(1101000) + 1\,(0110100) + 1\,(0011010) + 1\,(0001101) = (1001110)$	4

Figura 3: Código Gerado por $g(x) = 1 + x + x^3$.

Fonte: autora

2. Quais são os líderes das classes de $\mathbb{Z}_2^7$?
   Na figura 3 acima podemos observar que o peso mínimo em C é 3, logo os líderes de classe em $\mathbb{Z}_2^7$ devem ter peso menor ou igual a $\left[\frac{3-1}{2}\right] = 1$. São eles: (0000000), (1000000), (0100000), (0010000), (0001000), (0000100), (0000010) e (0000001).

3. Quais são as síndromes dos líderes de classe?
   Fazendo a divisão de cada um dos líderes de classe por $g(x)$, encontramos as respectivas síndromes:

Líder de Classe Lateral	Síndrome
(0000000)	(000)
(1000000)	(100)
(0100000)	(010)
(0010000)	(001)
(0001000)	(110)
(0000100)	(011)
(0000010)	(111)
(0000001)	(101)

Figura 4: Elemento Líder.

Fonte: autora

4. Decodifique a mensagem $v = (0101101) \in \mathbb{Z}_2^7$.
   Primeiro encontramos o resto da divisão do correspondente de v em $\mathbb{Z}_2[x]/(x^7 - 1)$ por $g(x)$. Neste caso $v(x) = (x^3)g(x) + (x)$, do teorema 5.2.6 segue que $S(v(x)) = x$ ou ainda $S(v) = (010)$, sendo assim, analisando a figura 4 temos que o vetor erro será $\mathbf{e}$=(0100000), então decodificamos $v(x)$ por $v(x) - \mathbf{e}(x) = x^3 + x^4 + x^6$ que corresponde a (0001101) e é palavra do código cíclico C.

5. Decodifique a mensagem $u(x) = (0011000)$.
   Observe que $u(x) = x^2 + x^3$ e $u(x) = (1)g(x) + (x^2 + x + 1)$, ou seja, $S(u(x)) = 1 + x + x^2$, ou ainda, $S(u) = (111)$, analisando a figura 4 temos que o vetor erro será $\mathbf{e} = (0000010)$.
   Sendo assim, decodificamos $u(x)$ por $u(x) - \mathbf{e}(x) = x^2 + x^3 + x^5$ que corresponde a (0011010).

A justificativa do algoritmo de decodificação utilizado nos itens 4 e 5 do exemplo acima é a que segue:

Considere os vetores m, c e $\mathbf{e}$, a mensagem recebida, a enviada e o vetor erro, respectivamente. Sabemos que $S(\mathbf{e}) = S(m)$, se $w(\mathbf{e}) \leqslant \left[\frac{d(C)-1}{2}\right]$, então da proposição 5.2.5 $\mathbf{e}$ é o único elemento líder de sua classe. Por fim, do lema 5.2.3, podemos determinar $c = m - \mathbf{e}$.

Observe ainda que se $w(S(m)) \leqslant \left[\frac{d(C)-1}{2}\right]$ (como no item 4 do exemplo acima), então como $S(S(m(x)) = S(m(x))$, temos que $S(m(x))$ e $e(x)$ possuem a mesma síndrome e portanto estão na mesma classe lateral. Mas como o elemento líder é único, segue que $e(x) = S(m(x))$. Ou seja, podemos decodificar $m(x)$ por $c(x) = m(x) - S(m(x))$.

5.2.13 A Síndrome do Desvio Cíclico

Nesta seção apresentaremos o cálculo da síndrome do desvio cíclico da mensagem recebida $m(x) \in \mathbb{Z}_p[x]/(x^n - 1)$ a partir da síndrome de $m(x)$, ou seja, um cálculo feito de forma indutiva. Veremos que é possível decodificar uma mensagem $m(x)$ desde que exista $i \in \{0, \cdots, n-1\}$, tal que $w(Sx^i m(x)) \leqslant \left[\frac{d(C)-1}{2}\right]$, ou seja, uma decodificação baseada na síndrome do desvio cíclico.

Teorema 5.2.7. *Dado $u(x) \in \mathbb{Z}_p[x]/(x^n-1)$ a síndrome do desvio cíclico de $u(x)$ é dada por*

$$S(xu(x)) = xS(u(x)) - s_{r-1}g(x),$$

onde s_{r-1} é o coeficiente do termo x^{r-1} de $S(u(x))$.

Demonstração. Considere $s(x) = S(u(x))$, do teorema 5.2.6, segue que $u(x) = q(x)g(x) + s(x)$, para algum $q(x) \in \mathbb{Z}_p[x]/(x^n-1)$ e $gr(s) < gr(g) = r$. Observe que

$$\begin{aligned} xu(x) &= xq(x)g(x) + xs(x) \\ &= xq(x)g(x) + xs(x) + s_{r-1}g(x) - s_{r-1}g(x) \\ &= (xq(x) + s_{r-1})g(x) + (xs(x) - s_{r-1}g(x)). \end{aligned}$$

Além disso, podemos escrever $s(x)$ e $g(x)$ como $s(x) = s_{r-1}x^{r-1} + s'(x)$ e $g(x) = x^r + g'(x)$, com $gr(s') < r-1$ e $gr(g') < r$, já que $gr(s) \leqslant r-1$, $gr(g) = r$ e $g(x)$ é mônico. Desta forma, temos que

$$\begin{aligned} xs(x) - s_{r-1}g(x) =& x(s_{r-1}x^{r-1} + s'(x)) - s_{r-1}(x^r + g'(x)) \\ =& s_{r-1}x^r + xs'(x) - s_{r-1}x^r - s_{r-1}g'(x) \\ =& xs'(x) - s_{r-1}g'(x). \end{aligned}$$

Note que o grau de $xs'(x)-s_{r-1}g'(x)$ é menor que r, sendo assim, $gr(xs(x)-s_{r-1}g(x)) < r$, logo do teorema 5.2.6 e da unicidade do resto segue que $S(xu(x)) = xr(x)-s_{r-1}g(x)$. □

Exemplo 5.2.14. Considere a mensagem $u(x) = x^2+x^3$ do item 5 do exemplo 5.2.12,com polinômio gerador $g(x) = 1+x+x^3$, vamos calcular as síndromes de seus desvios cíclicos utilizando o resultado do teorema 5.2.7:

$$\begin{aligned}
S(u(x)) &= x^2+x+1;\\
S(xu(x)) &= x(x^2+x+1)-1(x^3+x+1) = x^2+1;\\
S(x^2u(x)) &= x(x^2+1)-1(x^3+x+1) = 1;\\
S(x^3u(x)) &= x(1)-0(x^3+x+1) = x;\\
S(x^4u(x)) &= x(x)-0(x^3+x+1) = x^2;\\
S(x^5u(x)) &= x(x^2)-1(x^3+x+1) = x+1;\\
S(x^6u(x)) &= x(x+1)-0(x^3+x+1) = x^2+x.
\end{aligned}$$

Observe que o cálculo das síndromes dos desvios cíclicos é feito de forma indutiva, ou seja, calculamos $S(x^iu(x))$ a partir de $S(x^{i-1}u(x))$.

Definição 5.2.15. Dado $v(x) = v_0+v_1x+\cdots v_{n-1}x^{n-1}$, se existe j tal que $v_j = v_{j+1} = \cdots = v_{j+n-r-1} = 0$, onde os índices são calculados módulo n, então dizemos que $v(x)$ tem uma *sequência cíclica de n-r zeros.*

Exemplo 5.2.16.

1. $t(x) = 2+x^6 \in \mathbb{Z}_3[x]/(x^8-1)$ contém uma sequência cíclica de 5 zeros, já que $t = (2\,0\,0\,0\,0\,0\,1)$.
2. $v(x) = x^2+5x^4 \in \mathbb{Z}_7[x]/(x^9-1)$ contém uma sequência cíclica de 6 zeros, já que $x^{-2}v(x) = 1+5x^2$ tem representação polinomial $(1\,0\,5\,0\,0\,0\,0\,0\,0)$.

Lema 5.2.8. *O polinômio $v(x) \in \mathbb{Z}_p[x]/(x^n-1)$ contém uma sequência cíclica de $n-r$ zeros se, e somente se, existe $i \in \{0,\cdots,n-1\}$, tal que o grau de $x^iv(x)$ seja menor ou igual a $r-1$.*

Demonstração. $v(x) = v_0+v_1+\cdots+v_{n-1}x^{n-1}$ contém uma sequência cíclica de $n-r$ zeros se, e somente se, $x^iv(x) = u_0+u_1x+\cdots+u_{r-1}x^{r-1}+0x^r+\cdots+0x^{n-1}$, para algum $i \in \{0,\cdots,n-1\}$, o que ocorre se, e somente se, $gr(x^iv(x)) \leqslant r-1$. □

Lema 5.2.9. *Seja $\boldsymbol{e}(x) \in \mathbb{Z}_p[x]/(x^n-1)$, com $w(\boldsymbol{e}) \leqslant \left[\frac{d(C)-1}{2}\right]$, contendo uma sequência cíclica de $n-r$ zeros, então $w(S(x^i\boldsymbol{e}(x))) \leqslant \left[\frac{d(C)-1}{2}\right]$, para algum $i \in \{0,\cdots,n-1\}$.*

Demonstração. Do lema anterior segue que $gr(x^i\mathbf{e}(x)) \leqslant r-1$, para algum $i \in \{0, \cdots, n-1\}$. Então do teorema 5.2.6 $S(x^i\mathbf{e}(x)) = x^i\mathbf{e}(x)$. Note que a permutação dos coeficientes de um polinômio não alteram o seu peso, sendo assim:

$$w(S(x^i\mathbf{e}(x))) = w(x^i\mathbf{e}(x)) = w(\mathbf{e}(x)) \leqslant \left[\frac{d(C)-1}{2}\right].$$

□

5.2.17 Algoritmo de decodificação

Abaixo considere $C \subset \mathbb{Z}_p^n$ um código cíclico com polinômio gerador $g(x)$ de grau r. Dado $m(x) \in \mathbb{Z}_p[x]/(x^n-1)$ uma palavra recebida. O algoritmo de decodificação é o que segue.

Algoritmo 2: Decodificação em Códigos Cíclicos

Passo 1: Calcule $s_i(x) = S(x^i m(x))$, onde $0 \leqslant i \leqslant n-1$ é o menor inteiro, tal que $w(s_i) \leqslant \left[\frac{d(C)-1}{2}\right]$.

- Se determinar i, então vá para o passo 2.
- Caso contrário, o erro é impossível de ser corrigido.

Passo 2: Decodifique $m(x)$ por $c(x)$, onde

$$c(x) = m(x) - x^{n-i}s_i(x).$$

O algoritmo acima é justificável pelos fatos que seguem:

1. $m(x) - x^{n-i}s_i(x)$ pertence a C, já que

$$\begin{aligned} x^i(m(x) - x^{n-i}s_i(x)) &= x^i m(x) - x^n s_i(x) \\ &= q(x)g(x) + s_i(x) - x^n s_i(x) \\ &= q(x)g(x) + s_i(x)(1-x^n) \qquad \text{como } \mathbb{Z}_p^n \cong \mathbb{Z}_p[x]/(x^n-1) \\ &\equiv q(x)g(x) \mod x^n - 1. \end{aligned}$$

   Ou seja, $x^i(m(x) - x^{n-i}s_i(x)) \in C$, mas como C é um código cíclico então $m(x) - x^{n-i}s_i(x) \in C$.

2. O passo 2 do algoritmo é realizado quando o erro da mensagem possui uma sequência cíclica de $n-r$ zeros e tem peso menor ou igual a $\left[\frac{d(C)-1}{2}\right]$, nos garante o lema 5.2.9.

3. $x^{n-i}s_i(x)$ é de fato o erro $\mathbf{e}(x)$ da mensagem recebida. Sejam $c(x)$ e $m(x)$, respectivamente, as mensagens enviada e recebida, o erro é dado por $\mathbf{e}(x) = m(x) - c(x)$. Assumindo que $\mathbf{e}(x)$ possui uma sequência cíclica de $n - r$ zeros, temos que:

$$\begin{aligned} s_i(x) =& S(x^i m(x)) \\ =& S(x^i c(x)) + S(x^i \mathbf{e}(x)) \\ =& 0 + x^i \mathbf{e}(x) \\ =& x^i \mathbf{e}(x) \end{aligned}$$

Mas se $s_i(x) = x^i\mathbf{e}(x)$, então $x^{n-i}s_i(x) = x^n\mathbf{e}(x)$, além disso, $x^n \equiv 1 \mod (x^n - 1)$ e como estamos em $\mathbb{Z}_p[x]/(x^n - 1)$ temos que $x^{n-i}s_i(x) = \mathbf{e}(x)$.

Logo, o algoritmo decodifica corretamente $m(x)$ por $c(x) = m(x) - x^{n-i}s_i(x)$.

Exemplo 5.2.18. Recordando os exemplos 5.2.12 e 5.2.14 temos que a mensagem recebida foi $u(x) = x^2 + x^3$ e a síndrome $s_2 = S(x^2u(x)) = 1$ tem peso 1, sendo assim assumimos que o erro foi $x^{7-2}s_2(x) = x^5 \cdot 1 = x^5$. E como já vimos, a mensagem corrigida é $c(x) = x^2 + x^3 + x^5$.

Exemplo 5.2.19. Utilizando os resultados vistos durante esse trabalho vamos construir um código cíclico $C \subset \mathbb{Z}_3^8$.

1. Vamos determinar a fatoração do polinômio $x^8 - 1$ em polinômios irredutíveis e mônicos em $\mathbb{Z}_3[x]$, utilizando o teorema 4.5.3.
   As classes ciclotômicas de $p = 3$ módulo 8 são:

$$\begin{aligned} C_0 &= \{0\} \\ C_1 &= \{1, 3\} \\ C_2 &= \{2, 6\} \\ C_4 &= \{4\} \\ C_5 &= \{5, 7\} \end{aligned}$$

   Logo, $\{C_0, C_1, C_2, C_4, C_5\}$ é o conjunto completo de classes ciclotômicas de $p = 3$ módulo $n = 8$. Como $mdc(3^2, 8) = 1$ e $8|(3^2 - 1)$, então tomamos $m = 2$ e consideramos o corpo $\mathbb{F}_{3^2}$. Considere o polinômio irredutível $1 + x^2$, por inspeção $\alpha = x+1 \in \mathbb{F}_{3^2}$ é primitivo. Além disso, $r = \dfrac{3^2 - 1}{8} = 1$, sendo assim, procuramos os polinômios minimais das classes ciclotômicas $C_{1\cdot0}, C_{1\cdot1}, C_{1\cdot2}, C_{1\cdot4}$ e $C_{1\cdot5}$ de 3 módulo

$3^2 - 1 = 8$. Da proposição 4.4.2, segue

$$\begin{aligned}
C_0 &= \{0\} \Rightarrow \mathcal{M}_{\alpha^0}(x) = (x - \alpha^0) = x - 1 = 2 + x \\
C_1 &= \{1, 3\} \Rightarrow \mathcal{M}_{\alpha^1}(x) = (x - \alpha)(x - \alpha^3) = 2 + x + x^2 \\
C_2 &= \{2, 6\} \Rightarrow \mathcal{M}_{\alpha^2}(x) = (x - \alpha^2)(x - \alpha^6) = 1 + x^2 \\
C_4 &= \{4\} \Rightarrow \mathcal{M}_{\alpha^4}(x) = (x - \alpha^4) = 1 + x \\
C_5 &= \{5, 7\} \Rightarrow \mathcal{M}_{\alpha^5}(x) = (x - \alpha^5)(x - \alpha^7) = 2 + 2x + x^2
\end{aligned}$$

Observe que

$$x^8 - 1 = (x + 2)(x + 1)(x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2).$$

Ou seja, a fatoração de $x^8 - 1$ é dada pelos polinômios minimais: $x + 2$, $x + 1$, $x^2 + 1$, $x^2 + x + 2$ e $x^2 + 2x + 2$.

2. As condições sobre o polinômio gerador $g(x)$ é que seja mônico e que divida $x^8 - 1$. Como $x^8 - 1$ é composto por 5 polinômios minimais, temos que possui $2^5 = 32$ divisores. Vamos escolher um de seus divisores, a saber $g(x) = x^2 + 2x + 2$.

3. Definido o polinômio gerador $g(x) = 2 + 2x + x^2$ do nosso código cíclico, vamos determinar o polinômio verificador, bem como seu recíproco.

$$h(x) = \frac{x^8 - 1}{x^2 + 2x + 2} = 1 + 2x + 2x^2 + 2x^4 + 2x^5 + x^6,$$

logo $h^{\mathrm{R}}(x) = 1 + 2x + 2x^2 + 2x^4 + 2x^5 + x^6$.

4. As matrizes geradora e teste de paridade do código cíclico $C = (g(x))$ são, respectivamente:

$$G = \begin{pmatrix} 2 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 \end{pmatrix} \quad \text{e} \quad H = \begin{pmatrix} 1 & 2 & 2 & 0 & 2 & 2 & 1 & 0 \\ 0 & 1 & 2 & 2 & 0 & 2 & 2 & 1 \end{pmatrix}$$

A matriz $G' = (R|Id_{n-r})$ pode ser determinada, como vimos no teorema 5.2.1, calculando o resto da divisão de x^{2-1+i} por $g(x)$, onde $i = 1 \cdots, 8 - 2 = 6$. É isso

que vamos fazer, primeiramente determinaremos R:

Algoritmo Euclidiano	Representação Polinomial $(-r_i(x))$	Representação Vetorial $(-r_i)$
$x^2 = g(x) + (x+1)$	$2+2x$	22
$x^3 = g(x)(x+1) + (2x+1)$	$2+x$	21
$x^4 = g(x)(x^2+x+2) + (2)$	1	10
$x^5 = g(x)(x^3+x^2+2x) + (2x)$	x	01
$x^6 = g(x)(x^4+x^3+2x^2+2) + (2x+2)$	$1+x$	11
$x^7 = g(x)(x^5+x^4+2x^3+2x+2) + (x+2)$	$1+2x$	12

Logo,

$$G' = \begin{pmatrix} 2 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Do teorema 5.2.2, segue que a matriz teste de paridade é dada por $H' = (Id_r | -R^t)$, ou seja,

$$H' = \begin{pmatrix} 1 & 0 & 1 & 1 & 2 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 & 0 & 2 & 2 & 1 \end{pmatrix}$$

5. Não convém mostrarmos quais os elementos de C, já que tal é composto por $3^6 = 729$ mensagens. Vamos assumir que esse código tem peso mínimo[3] $d(C) = 3$ e portanto é capaz de corrigir até $\left[\frac{3-1}{2}\right] = 1$ erro.

6. Por fim, vamos decodificar as mensagens: $x^6 + x^4 + x^2 + 1$, $x^7 + x^5 + 2x + 1$, $x^7 + 2x^6 + x^5 + x^3 + x^2 + 2x + 1$ e $x^5 + 2x^4 + 2x^3 + 2x^2 + 2$. Efetuando a divisão das mensagens por $g(x) = 2 + 2x + x^2$ obtemos o resto $r(x)$ e se possível corrigimos

[3] A determinação do peso mínimo nesses códigos é uma questão ainda a ser respondida. No entanto, existem códigos cujos pesos mínimos possuem cotas inferiores, os Códigos BCH, para saber mais a respeito consulte [6, cap. 7, página 126].

o erro subtraindo $r(x)$ da mensagem recebida.

Mensagem recebida	Resto da divisão $r(x)$	Mensagem corrigida
$1+x^2+x^4+x^6$	0	$1+x^2+x^4+x^6$
$1+2x+x^5+x^7$	$2x$	$1+x^5+x^7$
$1+2x+x^2+x^3+x^5+2x^6+x^71$	0	$1+2x+x^2+x^3+x^5+2x^6+x^7$
$2+2x^2+2x^3+2x^4+x^5$	$2x+1$	impossível corrigir

Note que a mensagem $x^5+2x^4+2x^3+2x^2+2$ quando dividida por $g(x)$ deixa resto $r(x)=2x+1$ e como $w(2x+1)=2$ a princípio não conseguimos corrigí-la. Sendo assim, vamos utilizar o algoritmo explicitado na seção 5.2.17.

1. Iniciamos calculando as síndrome $s_i(x)$ até encontrarmos uma de peso menor ou igual a 1 (se esta existir).

$$s_o(x) = 2x+1;$$
$$s_1(x) = x(2x+1) - 2(x^2+2x+2) = -1 = 2$$

2. Como $w(s_1) \leqslant 1$, então assumimos que o erro foi $x^{8-1}s_1(x) = 2x^7$ e portanto a mensagem corrigida é $x^7+x^5+2x^4+2x^3+2x^2+2$.

CAPÍTULO 6

Conclusão

Neste trabalho, inicialmente fizemos um estudo baseado nos polinômios e mostramos como fatorar o polinômio $x^n - 1$ sobre $\mathbb{Z}_p$ em polinômios minimais, a partir disso, determinamos todos os divisores mônicos de $x^n - 1$ e consequentemente os polinômios geradores de Códigos Cíclicos.

A partir do polinômio gerador, mostramos como determinar a matriz geradora, bem como a matriz teste de paridade. Efetuando operações básicas com o polinômio gerador codificamos uma mensagem em código cíclicos, sem o auxílio de sua matriz geradora.

Também, no processo de decodificação, apresentamos o cálculo da síndrome à custa do polinômio gerador, assim como o cálculo da síndrome do desvio cíclico que nos permitiu determinar o líder da classe determinada pela síndrome da mensagem recebida.

Mostramos, portanto, uma aplicação dos polinômios em codificação, cumprindo, desta forma, o objetivo do nosso trabalho.

Referências Bibliográficas

[1] Aragão, C. R. S. *Códigos Cíclicos: uma introdução aos códigos corretores de erros.* 53f. Dissertação de Mestrado. Universidade Federal de Sergipe, 2017.

[2] Barros, A. L. *A Álgebra dos Códigos Corretores de Erros.* 88f. Dissertação de Mestrado. Universidade Federal da Grande Dourados, UFGD, 2019.

[3] Biazzi, R. N. *Polinômios Irredutíveis: Critérios e Aplicações* 72f. Dissertação de Mestrado. Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas, 2014.

[4] Domingues, H. H; Iezzi, G. *Álgebra Moderna.* 4 ed. São Paulo, 2003.

[5] Hefez, A. *Aritmética.* Coleção PROFMAT, SBM, Rio de Janeiro, 2013.

[6] Hefez, A.; Villela, M. L. T. *Códigos Corretores de Erros.* IMPA, 2008.

[7] Masuda, A.; Panario, D. *Tópicos de corpos finitos com aplicações em criptografia e teoria de códigos.* IMPA, 2007.

[8] Ventura, J. *Notas de Combinatória e Teoria de Códigos.* Instituto Superior Tecnico, Lisboa, 2014.

[9] Wikipedia contributors. *Eugene Prange.* Wikipedia, 2019. Disponível em: `http://en.wikipedia.org/w/index.php?title=Eugene_Prange&oldid=880870430`. Acessado em: 10 de Mar. de 2020.

[10] Zanoello, S. F. *Raízes polinomiais em corpos finitos.* 102f. Dissertação de Mestrado. Universidade Federal do Rio Grande do Sul, Porto Alegre, 2004.