UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA APLICADA

Raízes Polinomiais em Corpos Finitos

por

Simone Fátima Zanoello

Dissertação submetida como requisito parcial
para a obtenção do grau de

Mestre em Matemática Aplicada

Prof. Dr. Vilmar Trevisan,
Orientador

Porto Alegre, Janeiro de 2004.

CIP - CATALOGAÇÃO NA PUBLICAÇÃO

Zanoello, Simone Fátima

Raízes Polinomiais em Corpos Finitos / Simone Fátima Zanoello.—Porto Alegre: PPGMAp da UFRGS, 2004.

97 p.: il.

Dissertação (mestrado) —Universidade Federal do Rio Grande do Sul, Programa de Pós-Graduação em Matemática Aplicada, Porto Alegre, 2004.
Orientador: Trevisan, Vilmar

Dissertação: Matemática Aplicada
Modelo, Dissertação

Raízes Polinomiais em Corpos Finitos

por

Simone Fátima Zanoello

Dissertação submetida ao Programa de Pós-Graduação em Matemática Aplicada do Instituto de Matemática da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do grau de

Mestre em Matemática Aplicada

Linha de Pesquisa: Algoritmos Numéricos e Algébricos

Orientador: Prof. Dr. Vilmar Trevisan,

Banca examinadora:

Prof. Dr. Dalcidio Moraes Claudio
PUCRS

Profa. Dra. Cynthia Feijó Segatto
PPGMAp/UFRGS

Prof. Dr. Julio Cesar Ruiz Claeyssen
PPGMAp/UFRGS

Dissertação apresentada e aprovada em
06 de janeiro de 2004.

Prof. Dr. Vilmar Trevisan
Coordenador

Para meus pais

AGRADECIMENTO

Agradeço principalmente ao meu orientador, professor Vilmar Trevisan, pelas lições de saber, pela orientação constante, pela paciência, pelas sugestões e críticas que com certeza engrandeceram o meu trabalho.

Agradeço aos professores do programa de Pós Graduação em Matemática Aplicada, pela oportunidade a que me foi concedida.

Agradeço a Deus por ter me iluminado durante todo este curso.

Agradeço as pessoas que mais amo nesta vida, minha família, meus pais Lauri e Ivone, meu irmão Altair, minha cunhada Silvane e meus amados sobrinhos Gustavo e Paloma.

Agradeço aos meus amigos que sempre estiveram presentes me incentivando e animando a continuar a caminhada.

Agradeço a todos que tornaram possível este trabalho, em especial a minha grande amiga Hélia e a Dulcenéia que apesar da distância, sempre me auxiliou com o Latex.

Conteúdo

Lista de Tabelas

RESUMO

Este trabalho é um estudo sobre propriedades de decomposição de polinômios em corpos finitos. Em particular fazemos um estudo sobre métodos de fatoração e cálculos de raízes.

Procedemos inicialmente com um apanhado de conceitos e teoremas que embasam o trabalho. Com o objetivo de determinar raízes de polinômios em corpos finitos, alguns tópicos tornam-se pré-requisitos. O primeiro deles é a própria representação dos elementos dos corpos finitos. O outro é o estudo de métodos determinísticos ou probabilísticos para fatorar polinômios sobre corpos finitos. Os métodos estudados são o de Berlekamp, Cantor-Zassenhaus e Lidl-Niederreiter.

Fazemos finalmente o estudo de métodos que podem ser empregados para determinarmos as raízes de polinômios pertencentes a corpos finitos. Métodos estes que apresentam variações de acordo com o tamanho do corpo.

ABSTRACT

This work is a study about decomposition properties of polynomials over finite fields. We emphasize the study about factorization methods and computation of roots.

We initially give a number of concepts and theorems that base our work. Aiming the determination of polynomial roots in finite fields, some topics become pre-requisites. The first one being the representation of elements of finite fields. Other pre-requisite is the study of probabilistic and deterministic methods for polynomial factorization into irreducible factors over finite fields. We studied the methods of Berlekamp, Cantor-Zassenhaus and Lidl-Niederreiter.

Finally we study methods for computation of roots of polynomials over finite fields. We present methods that take into account the size and the caracteristic of the field.

APRESENTAÇÃO

O trabalho proposto consiste num estudo de polinômios sobre corpos finitos. O mesmo foi escolhido devido a sua vasta aplicação no campo da Matemática e áreas afins. Entre estas aplicações podemos citar eletro comunicações, geometria finita, combinatória, criptografia e teoria de códigos. Estas aplicações podem ser encontradas entre outros em ([13]).

Devido a amplitude do tema, delimitamos o mesmo, tendo então como objetivo a determinação das raízes de polinômios sobre corpos finitos.

Para atingirmos tal objetivo, torna-se de fundamental importância o estudo de definições e teoremas que embasem o trabalho e, a representação dos elementos de um corpo finito.

No decorrer do trabalho percebemos que para extrairmos as raízes de polinômios pertencentes a corpos finitos grandes com característica também grande precisaríamos estudar a fatoração de polinômios sobre corpos finitos. Sabendo da importância deste tema agregamos o mesmo ao nosso estudo ampliando assim o problema inicial.

Com isso o trabalho fica organizado da seguinte forma:

No capítulo 1 apresentamos alguns conceitos de álgebra, propriedades de polinômios em corpos finitos, propriedades estas que nos permitem caracterizar estes corpos. Ainda no primeiro capítulo, nos preocupamos em estudar sobre os polinômios irredutíveis, pois a partir deles dá-se a construção dos corpos finitos. Além de definirmos os mesmos, verificamos como encontrá-los e provamos que o número de polinômios irredutíveis sobre corpos finitos é elevado.

No capítulo 2 verificamos como representar os elementos de um corpo finito. Tal representação é importante para realizarmos com maior eficiência e faci-

lidade operações aritméticas com estes elementos. A representação pode ser feita na forma polinomial, vetorial, matricial e ainda como potência de um elemento.

No capítulo 3 estudamos sobre a fatoração de polinômios. Sendo que na seção 3.1 verificamos como extrair dos polinômios os fatores repetidos e nas demais seções deste capítulo apresentamos os métodos de Berlekamp, Cantor-Zassenhaus e Lidl-Niederreiter para fatorar polinômios.

No capítulo 4 descrevemos algoritmos empregados para determinarmos as raízes de polinômios sobre corpos finitos. Estes algoritmos tem significativa diferença em sua estrutura dependendo do tamanho do corpo em que o polinômio pertence.

Nos apêndices são apresentados um resumo biográfico de Evariste de Galois (matemático responsável por muitas das idéias sobre corpos finitos que temos atualmente), a descrição do Algoritmo de Euclides, exemplos da fatoração livre de quadrados e a representação dos elementos do corpo $GF(2^6)$.

1 IDÉIAS FUNDAMENTAIS SOBRE CORPOS FINITOS

Iniciaremos o nosso estudo sobre polinômios com coeficientes em corpos finitos conhecendo um pouco da estrutura destes corpos. Para isso na seção 1.1 apresentaremos alguns conceitos básicos de álgebra e propriedades de polinômios em corpos finitos. Sabendo da importância dos polinômios irredutíveis para a construção de corpos finitos, na seção 1.2 vamos nos deter em determinar o número de polinômios irredutíveis existentes em um corpo finito, bem como verificar que este número é elevado. E por fim, na seção 1.3, vamos expor alguns métodos que podem ser usados para determinar polinômios irredutíveis e consequentemente, possibilitar a construção de corpos finitos.

1.1 Caracterização de corpos finitos

A caracterização de corpos finitos mostra que cada corpo finito tem p^n elementos sendo p um primo e n um inteiro positivo. E de forma recíproca podemos dizer que com um primo p e inteiro positivo n construímos um corpo finito com p^n elementos. Estas duas afirmações e ainda o fato de que, corpos finitos com o mesmo número de elementos são isomorfos, são de fundamental importância para a classificação de corpos finitos. Isso nos mostra, essencialmente, que existe um único corpo para cada primo p e inteiro positivo n. Este corpo é chamado de corpo de Galois de ordem p.

Como já frisamos anteriormente iniciaremos esta seção expondo alguns conceitos básicos de álgebra,

Definição 1.1 Um **anel** $(A, +, .)$ é um conjunto A, juntamente com as operações de adição e multiplicação. Com relação a adição, o conjunto é associativo, comutativo, existe elemento neutro e simétrico. Com relação a multiplicação é associativo, e ain-

da a multiplicação é distributiva em relação a adição. Se a operação de multiplicação é comutativa, dizemos que o anel é comutativo.

Definição 1.2 Seja A um anel comutativo. Dizemos que um subconjunto $I \subset A$, $I \neq \emptyset$, é um **ideal** em A se,

i) $(\forall\ x\ , y)\ x, y \in I \Rightarrow x - y \in I$

ii) $(\forall\ a\ , x)\ a \in A$ e $x \in I \Rightarrow ax \in I$

Definição 1.3 Uma **relação de equivalência** R sobre um conjunto A não vazio é chamada relação de equivalência sobre A, se R é

reflexiva: a R a;

simétrica: a R $b \rightarrow b$ R a;

transitiva: a R b e b R $c \rightarrow a$ R c.

No decorrer do trabalho usaremos bastante a relação de equivalência mod m em $\mathbb{Z}$, cuja notação é $a \equiv_m b$, sendo m um inteiro positivo

$a \equiv_m b \longleftrightarrow a - b = k \cdot m$ para algum $k \in \mathbb{Z}$.

Na prática para encontrarmos a mod m, também podemos fazer da seguinte forma: a dividido por m e o resto da divisão é o b.

Exemplo 1.1 $21 \equiv 1 \bmod 5$

Toda vez que temos uma relação de equivalência R em um conjunto A, podemos agrupar os elementos em classes de equivalência. Para todo elemento $a \in A$, definimos

$[a] = \{x \in A \mid x\ R\ a\}$

A classe de equivalência mod m que contém $a \in \mathbb{Z}$ é obtida da forma

$[a] = \{a + km \mid k \in Z\}$

Exemplo 1.2 Tomando $m = 3$ obtemos as seguintes classes de equivalência de $\mathbb{Z}_3$.

$$[0] = \{\cdots, -6, -3, 0, 3, 6, \cdots\}$$

$$[1] = \{\cdots, -5, -2, 1, 4, 7, \cdots\}$$

$$[2] = \{\cdots, -4, -1, 2, 5, 8, \cdots\}$$

Ao unirmos todas as classes de equivalência obtemos um conjunto que é denominado **conjunto quociente**.

Da mesma forma, quando temos um ideal em um anel podemos separar o anel em classes de equivalência. Consideramos I um ideal em um anel A. As classes definidas pela relação de equivalência produzidas por I em A são dadas por $a + I = \{a + I \mid \forall\ i \ \in I\}$ para $\forall\ a \ \in A$. É possível definir novas operações no conjunto quociente $A \mid I = \{a + I \mid a \in A\}$ da seguinte forma:

$$(a + I) + (b + I) = (a + b) + I,$$

$$-(a + I) = -a + I,$$

$$0_{A/I} = 0 + I,$$

$$(a + I) \cdot (b + I) = a \cdot b + I,$$

$$1_{A/I} = 1 + I$$

A/I é uma imagem homomórfica de A sob o homomorfismo $a \to a + I$

A/I é um anel (comutativo se A é).

com estas operações é simples verificar que $A \mid I$ é um **anel quociente**.

Exemplo 1.3 Considerando o ideal $(5\mathbb{Z}, +, .)$ do anel $(\mathbb{Z}, +, .)$ dos inteiros, para obtermos o anel quociente $\mathbb{Z}/5\mathbb{Z}$ verificamos inicialmente quem são as classes de equivalência pertencentes a $\mathbb{Z}$ ou seja $\mathbb{Z}/5\mathbb{Z} = \{5\mathbb{Z}, 5\mathbb{Z} + 1, 5\mathbb{Z} + 2, 5\mathbb{Z} + 3, 5\mathbb{Z} + 4\}$.

Para definirmos em que classe do anel quociente o elemento x de $\mathbb{Z}$ faz parte, podemos fazer este número mod 5 (ou seja, x dividido por 5) e o resto desta divisão irá definir a classe a que o número x pertence.

Por exemplo, o número $7 \in \mathbb{Z}$ faz parte da classe de equivalência $5\mathbb{Z}+2$ pois, 7 mod 5 é igual a 2. Procedendo desta forma obteremos as classes abaixo:

$$5\mathbb{Z} = \{\dots, -10, -5, 0, 5, 10, \dots\}$$

$$5\mathbb{Z} + 1 = \{\dots, -4, 1, 6, \dots\}$$

$$5\mathbb{Z} + 2 = \{\dots, -3, 2, 7, 12, \dots\}$$

$$5\mathbb{Z} + 3 = \{\dots, -2, 3, 8, 13, \dots\}$$

$$5\mathbb{Z} + 4 = \{\dots, -1, 4, 9, 14, \dots\}$$

Podemos perceber que $\mathbb{Z}/5\mathbb{Z}$ é $\mathbb{Z}_5$. E $\forall\ m\ \in \mathbb{N}$ podemos definir um anel quociente $\mathbb{Z}_m$.

Definição 1.4 Ideal Maximal M é um ideal num anel comutativo A com a propriedade que o único ideal em A que contém M, e é diferente de M é o próprio anel A.

Definição 1.5 Um anel A, comutativo com unidade, recebe o nome de **corpo** se todo elemento não nulo de k admite inverso multiplicativo, ou seja:

$\forall\ a\ \in A, a \neq 0, \exists\ b\ \in A$ tal que $a \cdot b = 1$ sendo portanto b o inverso de a e indicado por a^{-1}.

Em outros termos, corpo é toda terna ordenada $(F, +, .)$, onde a operação de adição possui as seguintes propriedades:

1)Associativa:$(a + b) + c = a + (b + c) \forall\ a\ , b, c \in F$,

2) Admite elemento neutro: $a + 0 = 0 + a = a \forall\ a\ \in F$,

3) Todo elemento de F é inversível: $\forall\ a\ \in F, a \neq 0,\ \exists(-a) \in C\ |$ $a + a' = a' + a = 0$,

4) Comutativa: $a + b = b + a \forall\ a\ , b \in F$

e a operação de multiplicação possui as seguintes propriedades:

5) Associativa: $(a \cdot b) \cdot c = a \cdot (b \cdot c) \forall\ a\ , b, c \in F$,

6) Admite elemento unidade: $a \cdot 1 = 1 \cdot a = a \forall\ a\ \in F$,

7) Todo elemento não nulo de F é inversível: dado $a \in F$,$\exists\ a^{-1} \in F$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$

8) Comutativa: $a \cdot b = b \cdot a\ \forall\ a, b \in F$,

9) Distributiva em relação a adição: $a \cdot (b+c) = a \cdot b + a \cdot c\ \forall\ \ a\ , b, c \in F$.

Em um corpo só temos ideais triviais, ou seja, os subconjuntos $m = \{0\}$ e o próprio corpo.

Dentre alguns dos exemplos de corpos podemos citar: os números reais, os números complexos e os números racionais.

A importância de ideais maximais em anéis é verificada através do teorema seguinte que permite a construção de corpos.

Teorema 1.1 *F/M é um corpo $\Leftrightarrow$ M é maximal.*

A prova deste teorema pode ser encontrada em [14].

Definição 1.6 Um polinômio $f \in F[x]$ é chamado **irredutível** sobre F (ou irredutível em $F[x]$, ou primo em $F[x]$) se f tem grau positivo e se para toda fatoração $f = b \cdot c$ com $b, c \in F[x]$ tem-se b ou c uma constante.

Nas definições já citadas fizemos referências e exemplos ao conjunto dos números inteiros, mas é importante ressaltarmos que as mesmas também são aplicadas aos polinômios.

É fácil vermos que nos anéis polinomiais $F[x]$ os ideais maximais são os gerados pelos polinômios irredutíveis $m(x)$, e por isso temos o seguinte

Corolário 1.1 $F[x]/(m(x))$ é um corpo $\iff$ $m(x)$ é irredutível sobre F.

Seja $F[x]$ o anel de polinômios com coeficientes em um corpo F e $m(x)$ um polinômio irredutível em $F[x]$, a partir da definição de anel quociente nós concluímos que $F[x]/(m(x)) = \{a(x) + (m(x)) \mid a(x) \in F[x]\}$ sendo este um anel quociente de polinômio mod $m(x)$.

Portanto, ao generalizarmos o exemplo (1.3), podemos usar ao invés de inteiros, polinômios.

Exemplo 1.4 Considerando o anel $\mathbb{Z}_5$ e $m(x) = x^2 + x + 1$ um polinômio sobre $\mathbb{Z}_5[x]$. Para verificarmos se o anel quociente $\mathbb{Z}_5[x]/(x^2+x+1)$ é um corpo verificamos se $x^2 + x + 1$ é um polinômio irredutível sobre $\mathbb{Z}_5$.

Como nenhum elemento de $\mathbb{Z}_5$ é raiz de $m(x) = x^2 + x + 1$, podemos afirmar que $m(x) = x^2 + x + 1$ é um polinômio irredutível sobre $\mathbb{Z}_5$ e ainda pelo corolário (1.1) que o anel quociente $\mathbb{Z}_5[x]/(x^2 + x + 1)$ é um corpo.

Os elementos que compõem $\mathbb{Z}_5[x]/(x^2 + x + 1)$ são:

$\mathbb{Z}_5[x]/(x^2 + x + 1) = \{$[0], [1], [2], [3], [4], [x], [x + 1], [x + 2], [x + 3], [x + 4], [2x], [2x + 1], [2x + 2], [2x + 3], [2x + 4], [3x], [3x + 1], [3x + 2], [3x + 3], [3x + 4], 4x, [4x + 1], [4x + 2], [4x + 3], [4x + 4]$\}$, ou seja cada um destes elementos é o representante de uma classe de equivalência.

Para determinarmos em que classe de equivalência do corpo $\mathbb{Z}_5[x]/(x^2 + x + 1)$ um determinado polinômio pertence, basta dividirmos este polinômio pelo

polinômio irredutível $x^2 + x + 1$, e o resto desta divisão será um dos 25 elementos de $\mathbb{Z}_5[x]/(x^2 + x + 1)$. O polinômio dado pertencerá a classe deste elemento.

Já citamos anteriormente alguns exemplos de corpos, e podemos perceber que todos os exemplos óbvios têm um número infinito de elementos. Porém, a partir deste momento nos deteremos apenas em estudar corpos finitos, por isso começaremos definindo-os.

Definição 1.7 Um **corpo** $[F, +, .]$ **é finito** se o conjunto F é finito.

Note que o exemplo anterior pode ser generalizado. Se p é primo, consideremos um polinômio $m(\alpha)$ irredutível de grau n sobre $\mathbb{Z}_p$. Pelo corolário (1.1), sabemos que $F = \mathbb{Z}_p[x]/(m(x))$. É fácil ver que os elementos de F são classes cujos representantes podem ser caracterizadas como $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$. Ora o número de representantes é, portanto p^n, ou seja, dado n e p, é possível construir um corpo finito com p^n elementos (desde que exista um polinômio irredutível de grau n em $\mathbb{Z}_p[x]$). Veremos a seguir que esse corpo é, essencialmente o único corpo finito com p^n elementos.

O desenvolvimento inicial da teoria dos corpos finitos se deve a Evariste Galois (no apêndice A tem maiores informações sobre este matemático), por isso estes corpos também são chamados de corpos de Galois. E a notação que usaremos para representá-los é $GF(q)$.

Corpos finitos são importantes não somente na teoria de corpos mas também nas suas aplicações em eletro comunicações, geometria finita, combinatória, criptografia, teoria de códigos, entre outros.

Na seqüência, descreveremos algumas propriedades fundamentais de corpos finitos e também algumas definições que embasarão nosso trabalho posterior.

Definição 1.8 A característica de um anel A, é a ordem do 1 no grupo aditivo de A.

Desse modo, se A tem característica p, então $p \cdot 1 = 0$ e $m \cdot 1 \neq 0$ para $1 \leq m < p$. Se a característica de A não é finita, então nós dizemos que A tem característica zero.

Exemplo 1.5 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ todos tem característica zero. $\mathbb{Z}_p$ tem característica p.

Teorema 1.2 *Qualquer corpo finito tem p^n elementos para algum primo p (característica do corpo) e um inteiro positivo n (o grau do polinômio mínimo sobre Z_p de um elemento primitivo do corpo).*

Corolário 1.2 Um corpo finito tem característica prima.

Teorema 1.3 *Seja F um corpo finito. Então F^*, o grupo multiplicativo, é cíclico.*

O elemento gerador deste grupo cíclico é chamado de **elemento primitivo** do grupo. A seguir determinaremos o número de elementos primitivos que um corpo finito pode ter, mas para isso precisamos definir a função $\phi(n)$.

Definição 1.9 A função $\phi(n)$ é conhecida como função de Euler e indica o número de inteiros positivos menores e iguais a n relativamente primos a n.

Teorema 1.4 *Seja F um corpo finito com r elementos. Então F tem $\phi(r-1)$ elementos primitivos. Em particular se $\alpha \in F^*$ é primitivo, então α^i, é primitivo toda vez que $m.d.c.(i, r-1) = 1$.*

Exemplo 1.6 O número de elementos primitivos no grupo $\mathbb{Z}_7$ é dois pois se r é o número de elementos pertencentes ao $\mathbb{Z}_7$, temos r = 7, e então ϕ(r - 1) = ϕ(7 - 1)= ϕ(6)= 2

Teorema 1.5 *Dado um primo p e um inteiro positivo n, existe um corpo finito com p^n elementos.*

Teorema 1.6 *Dois corpos finitos quaisquer que têm o mesmo número de elementos são isomorfos.*

Portanto, os dois últimos teoremas descrevem uma característica fundamental de corpo finito, ou seja, para todo inteiro n e todo número primo p existe, a menos de isomorfismos, um único corpo com exatamente p^n elementos.

Definição 1.10 Seja F um corpo e $\alpha \in E$ extensão de F. α **é algébrico** sobre F se ele for raiz de um polinômio com coeficientes em F.

Definição 1.11 Seja $\alpha \in E$ algébrico sobre F. O **polinômio mínimo** de α sobre F, denotado por $m_\alpha(x)$, é o polinômio mônico de menor grau em $F[x]$ tendo α como uma raiz.

Teorema 1.7 *Um polinômio irredutível sobre um corpo F é um polinômio mínimo sobre F de qualquer uma de suas raízes.*

Teorema 1.8 *Seja $m(x)$ um polinômio irredutível sobre F. Então $E = F[x]/(m(x))$ é uma extensão de F em que $m(x)$ tem uma raiz.*

Seja $\alpha \in E$, um corpo que contém F. Denotaremos por $F[\alpha]$ o menor corpo que contém F e α. Sendo α a raiz do polinômio irredutível sobre F, podemos afirmar que

Teorema 1.9 *Se $\alpha \in E$, algébrico sobre $F \subseteq E$ com polinômio mínimo $m_\alpha(x)$ sobre F. Então*

$$F[\alpha] \equiv F[x]/(m_\alpha(x))$$

A demonstração destes resultados pode ser encontrada em muitos livros de álgebra. Em particular, podem ser encontradas no livro Elements of Algebra and Algebraic Computing de John D. Lipson [14].

Exemplo 1.7 Seja $x^4 + x + 1$ um polinômio irredutível sobre $\mathbb{Z}_2$.

Pelo teorema (1.8), $x^4 + x + 1$ tem uma raiz α em um corpo extensão de $\mathbb{Z}_2$, ou seja, em $\mathbb{Z}_2/(x^4 + x + 1)$. Pelo teorema (1.9), sabemos que o menor corpo extensão que contém α é $\mathbb{Z}_2/(x^4+x+1)$. É importante frisarmos que $\mathbb{Z}_2/(x^4+x+1)$

é um corpo pois $x^4 + x + 1$ é um polinômio irredutível. Como o polinômio tem grau 4 sobre $\mathbb{Z}_2$ podemos dizer que o corpo tem 16 elementos ou seja, 16 classes de equivalência.

Este anel quociente $\mathbb{Z}_2/(x^4 + x + 1)$ também pode ser denotado por $\mathbb{Z}_2[\alpha]$ pois, o mesmo indica o menor corpo que contém $\mathbb{Z}_2$ e α.

Então, $\mathbb{Z}_2[\alpha] = \mathbb{Z}_2[x]/(x^4 + x + 1)$.

A maneira como representamos os elementos deste corpo são de fundamental importância para realizarmos operações aritméticas com estes elementos. Por isso, no próximo capítulo veremos as diferentes formas de representar os mesmos.

1.2 Número de polinômios irredutíveis de grau d sobre $GF(p^n)$

Como a construção de um corpo finito depende inicialmente da existência de um polinômio irredutível, sobre um corpo base $F = GF(q)$, $q = p^n$, p um primo, além de sabermos encontrá-lo, é importante que saibamos quantos polinômios irredutíveis sobre o corpo base existem, pois quanto mais abundante for o número de polinômios irredutíveis mais fácil será de encontrá-lo.

Por isso, vamos iniciar esta seção determinando uma fórmula para o número de polinômios irredutíveis de grau d sobre $GF(q)$ e depois provaremos que o número de polinômios irredutíveis sobre $GF(q)$ é abundante, deixando para a próxima seção a descrição de métodos que encontrem um polinômio irredutível sobre $\mathbb{Z}_p[x]$.

Necessitamos primeiramente de alguns resultados, cujas provas podem ser encontradas, por exemplo, em [13] ou [18]. Assumimos que $q = p^n$, onde p é um número primo e n é um inteiro positivo.

Teorema 1.10 *Seja $f \in GF(q)[x]$ um polinômio irredutível sobre $GF(q)$ de grau m. Então $f(x)$ divide $x^{q^k} - x$ se e somente se m divide k.*

Teorema 1.11 *Para cada corpo finito $GF(q)$ e cada $k \in \mathbb{N}$, o produto de todos polinômios mônicos irredutíveis sobre $GF(q)$ cujo grau divide k é igual a $x^{q^k} - x$.*

Demonstração Pelo teorema (1.10) podemos concluir que ao fazermos a fatoração canônica de $g(x) = x^{q^k} - x$ obteremos polinômios irredutíveis cujo grau divide k. Já $g'(x) = -1$, pelo teorema (3.1) sabemos que g não tem raízes múltiplas no corpo decomposição sobre $GF(q)$. Portanto, cada polinômio mônico irredutível sobre $GF(q)$ cujo grau divide k aparece exatamente uma vez na fatoração de g em $GF(q)[x]$. □

Exemplo 1.8 Consideremos um polinômio mônico irredutível sobre $GF(2)$ e $k = 4$.

O primeiro passo para exemplificarmos o teorema é procurarmos quais são os polinômios mônicos irredutíveis sobre $GF(2^4)$ de grau 1, 2 ou 4, ou seja os números que dividem k (como encontrarmos um polinômio mônico irredutível descreveremos no final deste capítulo).

Os polinômios mônicos irredutíveis neste caso são: $x, x+1, x^2+x+1, x^4+x+1, x^4+x^3+1$ e $x^4+x^3+x^2+x+1$.

Partimos então para o exemplo propriamente dito:

$x^{q^k} - x = (x) \cdot (x+1) \cdot (x^2+x+1) \cdot (x^4+x+1) \cdot (x^4+x^3+1) \cdot (x^4+x^3+x^2+x+1) = (x^{16} - x)$

Vamos denotar o número de polinômios mônicos irredutíveis de grau d sobre $GF(q)$ por $N_q(d)$. Pelo resultado do teorema anterior dá-se o seguinte,

Corolário 1.3 Se $N_q(d)$ é o número de polinômios mônicos irredutíveis em $GF(q)[x]$ de grau d, então

$$q^n = \sum_{d/n} d \cdot N_q(d) \ \forall \ n \in \mathbb{N} \tag{1.1}$$

onde a soma é estendida sobre todos divisores positivos d de n.

Exemplo 1.9 Como no exemplo anterior, encontramos todos os polinômios irredutíveis sobre $GF(2)$ de grau no máximo 4, podemos contar quantos polinômios irredutíveis tem de grau 1, 2 e 4 $\in$ a $GF(2^4)$ e assim substituir na fórmula do corolário anterior exemplificando o mesmo.

$$2^4 = \sum_{d/4} d \cdot N_q(d)$$

$$16 = 1.N_q(1) + 2.N_q(2) + 4.N_q(4) = 1.2 + 2.1 + 4.3 = 16$$

Porém ainda não encontramos uma fórmula explícita que determine o número de polinômios irredutíveis sobre $GF(q)$. Para obtermos a mesma precisamos definir primeiramente a função de Moebius [1] e a inversão de Moebius.

A **função de Moebius** μ é definida por,

$$\mu(d) = \begin{cases} 1 & \text{se d = 1} \\ (-1)^j & \text{se d é o produto de j distintos primos} \\ 0 & \text{caso contrário} \end{cases}$$

De acordo com [24] esta função foi introduzida por Moebius (1832), mas a notação $\mu(d)$ foi primeiramente usada por Mertens (1874).

Lema 1.1 Para $d \in \mathbb{N}$ a função de Moebius μ satisfaz:

$$\sum_{k/d} \mu(k) = \begin{cases} 1 & \text{se } d = 1 \\ 0 & \text{se } d > 1 \end{cases}$$

Demonstração O caso $d = 1$ é óbvio. Para $d > 1$, $d \in \mathbb{N}$, seja $d = p_1^{m_1} \dots p_r^{m_r} (m_i \in \mathbb{N}, 1 \leq i \leq r)$ a fatoração prima de d. Os únicos divisores de d que produzem um somatório diferente de zero são aqueles cujos expoentes de

[1] É comum encontrarmos o nome Moebius escrito como Möbius.

p_i são 1 ou 0 ($1 \leq i \leq r$). Existem exatamente $\binom{r}{j}$ divisores de d para os quais j expoentes são 1. O restante é zero. Portanto nós temos:

$$\sum_{k/d} \mu(k) = \sum_{j=0}^{r} (-1)^j \binom{r}{j} = \sum_{j=0}^{r} \binom{r}{j} 1^{r-j} (-1)^j = (1-1)^r = 0 \square$$

Exemplo 1.10 Se $d = 12$, os divisores de d são: D(12) = {1, 2, 3, 4, 6, 12}

$$\sum_{k/12} \mu(k) = \mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) + \mu(12)$$

$$\sum_{k/12} \mu(k) = 1 - 1 - 1 + 0 + 1 + 0$$

$$\sum_{k/12} \mu(k) = 0$$

A clássica **inversão de Moebius** é dada pelo seguinte

Teorema 1.12

$$f(d) = \sum_{k/d} g(k) \Leftrightarrow g(d) = \sum_{k/d} \mu(k) \cdot f(\frac{d}{k})$$

Demonstração

$\Longrightarrow$

Por definição

$$f(d) = \sum_{k/d} g(k)$$

Fazendo mudança de variável, $d = \frac{d}{k}$ e $k = e$

$$f(\frac{d}{k}) = \sum_{e/\frac{d}{k}} g(e)$$

$$f(\frac{d}{k}) = \sum_{ek/d} g(e)$$

Voltando

$$\sum_{k/d} \mu(k) f(\frac{d}{k}) = \sum_{k/d} \mu(k) \sum_{ek/d} g(e) = \sum_{e/d} g(e) \sum_{k/\frac{d}{e}} \mu(k) = g(d)$$

$\Longleftarrow$

Por definição

$$g(d) = \sum_{k/d} \mu(k) f(\frac{d}{k})$$

Fazendo uma mudança de variável: $d = k$ e $k = e$

$$g(k) = \sum_{e/k} \mu(e) f(\frac{k}{e})$$

Portanto

$$\sum_{k/d} g(k) = \sum_{k/d} \sum_{e/k} \mu(e) f(\frac{k}{e}) = \sum_{elf=d} \mu(e) f(l) = \sum_{l/d} f(l) \sum_{e/\frac{d}{l}} \mu(e) = f(d) \square$$

Aplicando, então a inversão de Moebius na fórmula do corolário (1.3), obtemos

Teorema 1.13 *O número $N_q(d)$ de polinômios mônicos irredutíveis em $GF(q)$ de grau d é dado por*

$$N_q(d) = \frac{1}{d} \sum_{k/d} \mu(k) \cdot q^{\frac{d}{k}}$$

Demonstração Seja $f(d) = q^d$, $g(d) = d \cdot N_q(d)$ para todo $d \in \mathbb{N}$

Pela definição, $f(d) = q^d$. Pelo corolário (1.3)

$$q^d = \sum_{k/d} k \cdot N_q(k)$$

então

$$f(d) = \sum_{k/d} k \cdot N_q(k)$$

se $g(d) = d \cdot N_q(d)$ fazendo mudança de variável $d = k$, obtemos, $g(k) = k \cdot N_q(k)$ e, portanto

$$f(d) = \sum_{k/d} g(k)$$

Pela definição, temos $g(d) = d \cdot N_q(d)$

Aplicando a inversão de Moebius, obtemos

$$g(d) = \sum_{k/d} \mu(k) \cdot f(\frac{d}{k})$$

portanto

$$g(d) = d \cdot N_q(d) = \sum_{k/d} \mu(k) \cdot f(\frac{d}{k})$$

sabemos que $f(d) = q^d$, fazendo mudança de variável $d = \frac{d}{k}$

$$f(\frac{d}{k}) = q^{\frac{d}{k}}$$

portanto

$$g(d) = \sum_{k/d} \mu(k) \cdot q^{\frac{d}{k}}$$

Pela definição, $g(d) = d \cdot N_q(d)$, então

$$d \cdot N_q(d) = \sum_{k/d} \mu(k) \cdot g^{\frac{d}{k}}$$

$$N_q(d) = \frac{1}{d} \sum_{k/d} \mu(k) \cdot q^{\frac{d}{k}} \square \tag{1.2}$$

Exemplo 1.11 O número de polinômios mônicos irredutíveis em $GF(q)[x]$ de grau 20 é dado por

$N_q(20) = \frac{1}{20} \sum_{k/20} \mu(k) \cdot q^{\frac{20}{k}} = \frac{1}{20}[\mu(1) \cdot q^{20} + \mu(2) \cdot q^{10} + \mu(4) \cdot q^5 + \mu(5) \cdot q^4 + \mu(10) \cdot q^2 + \mu(20) \cdot q = \frac{1}{20}[q^{20} - q^{10} - q^4 + q^2]$

Ao exemplificarmos a fórmula dada pelo teorema (1.13) como foi feito anteriormente poderemos verificar que para cada corpo finito $GF(q)$ e cada $d \in \mathbb{N}$ existe um polinômio irredutível em $GF(q)[x]$ de grau d. De fato se usarmos a definição da função de Moebius, a estimativa irá produzir sempre $N_q(d) \geq \frac{1}{d}(q^d - q^{d-1} - q^{d-2} - \cdots - q) = \frac{1}{d}(q^d - \frac{q^d-1}{q-1}) > 0$. Ou seja, sempre existe polinômio irredutível de grau d. Essa mesma estimativa mostra que $N_q(d) \longrightarrow \frac{q^d}{d}$ (quando $d \longrightarrow +\infty$). Se observarmos que existe q^d polinômios mônicos de grau d em $GF(q)$, então obtemos o seguinte

Corolário 1.4 Um polinômio mônico randômico de grau d sobre um corpo finito é redutível com uma probabilidade próxima a $1 - \frac{1}{d}$.

Mais propriedades sobre $N_q(d)$ podem ser encontradas em Zassenhaus ([18]) e Mignotte ([15]).

Sabendo que d é o grau do polinômio irredutível e que q é o tamanho do corpo finito, observe na tabela abaixo, como o número de polinômios irredutíveis cresce velozmente com respeito a d.

Tabela 1.1: *Número de polinômios irredutíveis sobre* $GF(q)$

q	$d=1$		$d=2$		$d=3$	
	$N_q(d)$	q^d/d	$N_q(d)$	q^d/d	$N_q(d)$	q^d/d
2	2	2	1	2	2	2,66...
3	3	3	3	4,5	8	9
5	5	5	10	12,5	40	41,66...
7	7	7	21	24,5	112	114,33..

Tabela 1.1: (continuação) *Número de polinômios irredutíveis sobre* $GF(q)$

q	$d=4$		$d=5$	
	$N_q(d)$	q^d/d	$N_q(d)$	q^d/d
2	3	4	6	6,4
3	18	20,25	48	48,6
5	150	156,25	624	625
7	558	600,25	3.360	3.361,4

Observando a tabela 1.1 verificamos que o número de polinômios irredutíveis sobre um corpo finito é elevado e isso faz com que seja mais fácil encontrá-los.

Ainda podemos observar que se aplicarmos a fórmula 1.27 ou se usarmos a informação dada pela estimativa $\frac{q^d}{d}$ para encontrarmos o número de polinômios irredutíveis, os valores encontrados serão muito próximos.

1.3 Métodos para determinar um polinômio irredutível sobre $GF(p^n)$

Pelo teorema (1.13) determinamos o número de polinômios irredutíveis que existem sobre um dado corpo finito, nossa tarefa agora é encontrar um polinômio irredutível, pois como já frisamos anteriormente é a partir dele que conseguimos representar um corpo finito.

Existem diferentes métodos que podemos usar a fim de encontrarmos um polinômio irredutível sobre $GF(p^n)$.

Se o corpo primo for pequeno, um procedimento que torna-se fácil é o de encontrarmos os polinômios por tentativa e erro. Nesse caso listamos os polinômios mônicos de grau d sobre $GF(q)$. Após devemos eliminar da lista todos os polinômios que não tem um termo constante, pois se o polinômio não tiver um termo constante ele pode ser fatorado e portanto é redutível. Para os polinômios restantes devemos substituir x pelos elementos de $GF(p^n)$ um a um e fazer mod p. Se algum destes elementos de $GF(p^n)$ zerar o polinômio podemos afirmar que este é raiz do polinômio o que implica que este polinômio pode ser fatorado e portanto é redutível. Se o grau escolhido for dois, após eliminarmos os polinômios que não tem termo constante. Poderíamos tomar todos os fatores lineares sobre $GF(p^n)$ e multiplicá-los, em todos os pares possíveis, assim verificaríamos quais são quadráticos fatoráveis e eliminaríamos eles da lista. Encontrando finalmente os polinômios mônicos irredutíveis sobre $GF(p^n)$.

Se o corpo finito for grande um dos métodos que podemos aplicar é o teste de Rabin. Este algoritmo leva em consideração que existe um número elevado de polinômios irredutíveis sobre um determinado corpo finito.

O algoritmo de Rabin [5] consta das seguintes etapas,

Passo 1 Gerar um polinômio mônico, $g(x)$ aleatóriamente, de grau d sobre $GF(q)$.

Teste 1 Se este polinômio $g(x)$ dividir (x^q - x), é porque o teste um teve sucesso.

Teste 2 Verificar se $m.d.c.(g(x), x^{p^{n_i}} - x) = 1$ para todo $n_i = \mathrm{n}/k_i$ onde o k_i são todos os divisores primos de n, caso se verifique esta condição então o teste dois teve sucesso.

Deve-se repetir isto até que os testes 1 e 2 tenham sucesso.

Note que a justificativa para a correção do algoritmo é o teorema (1.10).

Observação: O máximo divisor comum de dois polinômios pode ser calculado através do algoritmo de Euclides, o qual descreveremos no apêndice B.

Exemplo 1.12 Para determinarmos os polinômios irredutíveis sobre $GF(3)$ de grau 2, podemos usar tentativa e erro já que o corpo finito é pequeno.

Iniciamos listando todos os polinômios quadráticos (pois, $n = 2$) sobre $GF(3)$.

$GF(3) = \{x^2, x^2+1, x^2+2, x^2+x, x^2+x+1, x^2+x+2, x^2+2\cdot x, x^2+2\cdot x+1, x^2+2\cdot x+2\}$.

Todos os polinômios que não tem termo constante são fatoráveis. Portanto, $x^2, x^2+x, x^2+2\cdot x$, são eliminados da lista.

Podemos saber se os polinômios que sobraram na lista são irredutíveis testando, ou seja, substituindo os valores de x pelos elementos que compõem $GF(3)$, que são, 0, 1 e 2, e fazendo mod 3.

Ao fazer isso constataremos que x^2+1, x^2+x+2 e $x^2+2\cdot x+2$ são polinômios quadráticos mônicos irredutíveis em $GF(3)$.

Exemplo 1.13 Para encontrarmos os polinômios irredutíveis de grau 4 sobre $GF(2)$, aplicando o algoritmo de Rabin escolhemos um polinômio $g(x)$.

1) O polinômio escolhido é x^4+x^3+1 sobre $GF(2^4)$.

2) Então: $g(x) = x^4+x^3+1$

$q = p^n$ como $p = 2$ e $n = 4$ então $q = 2^4$ e portanto $q = 16$

Devemos verificar se $g(x)$ divide $x^{16}-x$. Fazendo o cálculo verifica-se que divide obtendo-se o quociente $x^{12}-x^{11}+x^{10}-x^9+x^7+x^5-x^4-x$.

3) No segundo teste devemos fazer o $m.d.c.(g(x), x^{p^{n_i}}-x)$ e este deve ser um. Sabendo que $n = 4$ e $p = 2$, verificamos o valor de k_i. k_i = divisores primos de n, portanto $k_i = 2$. E $n_i = \mathrm{n}/k_i$, $n_i = 4/2$, $n_i = 2$.

Então o $m.d.c.(x^4+x^3+1, x^{2^2}-x) = m.d.c.(x^4+x^3+1, x^4-x) = m.d.c(x^4-x, x^3+x+1) = m.d.c.(x^3+x+1, -x^2) = m.d.c.(-x^2, x+1) = m.d.c(x+1, x) = m.d.c(x, 1) = m.d.c(1, 0)$.

Como o $m.d.c.$ é 1, então o teste dois também teve sucesso, e portanto x^4+x^3+1 é um polinômio irredutível sobre $GF(2^4)$.

2 REPRESENTAÇÃO DE ELEMENTOS DE CORPOS FINITOS

Este capítulo terá o intuito de demonstrar como representar os elementos de um corpo finito. Para isso considere um corpo $GF(q)$ sendo $q = p^n$ e p um número primo, para denotar um corpo finito com p^n elementos.

No decorrer do capítulo perceberemos que representar os elementos de um corpo finito será importante para realizarmos com maior eficiência e facilidade operações aritméticas com tais elementos.

A representação dos elementos deste corpo finito depende primeiramente da escolha de um polinômio irredutível sobre o corpo $GF(p)$ (como vimos no capítulo anterior). Após feita esta escolha podemos representar os elementos de $GF(p^n)$ de quatro maneiras distintas: como potência de um elemento, como polinômios, como vetores ou como matrizes.

2.1 Representação em série de um corpo finito

Pela caracterização de corpos finitos sabemos que para qualquer primo $p \geq 2$ e qualquer $n \in \mathbb{N}$ existe um corpo finito com p^n elementos. Também sabe-se que, se $GF(p^n)$ é um corpo finito com p^n elementos, então o grupo multiplicativo $GF(p^n)^*$=$\{a \in GF(p);\ a \neq 0\}$ é cíclico.

Se α é um gerador do grupo multiplicativo, então:

$GF(p^n) = \{0,\ \alpha,\ \alpha^2,\ .....,\ \alpha^{p^n-1}\}$ que é a representação do corpo em série.

2.2 Representação polinomial de um corpo finito

Para representarmos os elementos de um corpo finito em forma de polinômios, devemos inicialmente encontrar um polinômio irredutível $m(x)$ sobre $GF(q)$. Após, como já fizemos referência no capítulo 1, devemos escolher um polinômio qualquer $h(x)$ e dividi-lo pelo polinômio irredutível $m(x)$, o resto da divisão indicará a classe a que o polinômio $h(x)$ pertencerá.

Mas, poderíamos também determinar a representação polinomial de um corpo finito, tomando β como raiz do polinômio $m(x)$ e substituindo o x por β. Isolamos a maior potência de β no primeiro membro, ficando o restante do polinômio primitivo mod p no segundo membro. Chamaremos esta maior potência do polinômio primitivo de j. Como já conhecemos β^j, para encontrarmos β^{j+1}, devemos multiplicar ambos os termos da igualdade por β, sendo que devemos fazer o segundo membro mod p e ainda cada vez que aparecer β^j devemos substitui-lo pelo seu respectivo valor. Devemos fazer isso para todas as potências de β que fazem parte da representação em série.

A fim de facilitarmos nosso trabalho, é conveniente verificarmos se a raiz β é um elemento primitivo deste corpo, ou seja, se ele gera o grupo multiplicativo. Pois se isso acontecer conseguiremos fazer uma relação entre a representação polinomial e a representação em série. Relação esta que é muito útil quando estamos encontrando o polinômio mínimo de cada elemento, pois ao adicionarmos duas potências de α encontramos como resposta uma terceira potência de α; como já fizemos a representação polinomial e como esta está relacionada a representação em série, podemos substituir a terceira potência encontrada pela sua representação polinomial e assim obtermos o polinômio mínimo.

Caso β não seja um elemento primitivo deste corpo, podemos, por tentativa, procurar um elemento primitivo do corpo $GF(p^n)$, caso nosso objetivo seja o de relacionar as duas representações: polinomial e em série. Se não tivermos este objetivo, não precisamos encontrar um elemento primitivo do corpo.

Em vista disso, é importante definirmos polinômio primitivo.

Definição 2.1 Um polinômio primitivo sobre $GF(q)$ de grau n é um polinômio mônico que é irredutível sobre $GF(q)$ e tem uma raiz $\beta \in GF(q^n)$ que gera o grupo multiplicativo de $GF(q^n)$.

Isso nos mostra que para questões de representação, é conveniente que o polinômio que constrói o corpo finito seja primitivo.

2.3 Representação vetorial de elementos de um corpo finito

Os elementos de um corpo finito com p^n elementos podem ser representados por n-uplas $(v_0, v_1, \ldots v_{n-1})$, onde $v_i \in GF(p)$. Portanto $GF(p^n)$ é um espaço vetorial sobre $GF(p)$. Observe que aqui existem p^n vetores distintos sobre $GF(p)$.

Definição 2.2 Se $GF(p^n)$= $\{\beta_0, \beta_1, \ldots, \beta_{p^n-1}\}$ é um corpo finito, então: $\beta_i = (\beta_{i0}, \beta_{i1}, \ldots, \beta_{i,n-1})$ é chamado a representação vetorial do elemento β_i de $GF(p^n)$.

É importante ressaltar que a representação vetorial de elementos de um corpo finito pode ser deduzida a partir da representação polinomial e vice-versa.

Observações:

A representação em série é conveniente para multiplicações, pois como já dissemos o grupo multiplicativo é cíclico; a representação polinomial para adições, pois lembra a idéia de anel quociente onde $X^i \equiv V_i(X)$ mod $P(X)$ como vimos anteriormente, e a representação vetorial também é boa para adições e para produto interno de elementos de um corpo finito.

2.4 Representação matricial de um corpo finito

Uma outra maneira de representar os elementos de um corpo finito é através de matrizes. Em geral, a matriz companheira do polinômio mônico $f(x) = a_0 + a_1 \text{ x} + \ldots + a_{n-1}x^{n-1} + x^n$ de grau positivo n sobre um corpo é definida pela matriz $n \times n$.

$$A = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & -a_{n-1} \end{bmatrix}_{n \times n}$$

Isso é bem conhecido em álgebra linear onde A satisfaz a equação $f(A) = 0$, que é, $f(A) = a_0 I + a_1 A + \ldots + a_{n-1}A^{n-1} + A^n = 0$, onde I é a matriz identidade $n \times n$.

Desse modo, se A é a matriz companheira de um polinômio mônico irredutível f sobre $GF(q)$ de grau n, então $f(A) = 0$, e conseqüentemente A pode ter a função de raiz de f. O corpo finito $GF(q)$, $q = p^n$, pode ser representado pelo polinômio em A. Os elementos de $GF(q)$ são dados pelo polinômio em A de grau menor que n.

Exemplo 2.1 (Representação de $GF(2^4)$)

O polinômio $x^4 + x + 1$ é irredutível sobre $\mathbb{Z}_2[\equiv GF(2)]$. Pelo teorema 1.8 podemos afirmar que no corpo extensão de $\mathbb{Z}_2$, ou seja $\mathbb{Z}_2[x]$ / $(x^4 + x + 1)$, o polinômio irredutível tem uma raiz. Esta raiz chamamos de β.

Pela definição 1.11 podemos dizer que $x^4 + x + 1$ é o polinômio mínimo de β sobre $\mathbb{Z}_2$. Desse modo $\mathbb{Z}_2(\beta)$ é $GF(2^4)$, como corpo extensão de $\mathbb{Z}_2$ com 16 elementos. Abaixo representaremos a tabela de elementos de $\mathbb{Z}_2(\beta)$.

Tabela 2.1: *Representação dos elementos* $\mathbb{Z}_2(\beta)$

Representação em série	Representação polinomial	Representação vetorial
0	0	(0, 0, 0, 0)
α	β	(0, 1, 0, 0)
α^2	β^2	(0, 0, 1, 0)
α^3	β^3	(0, 0, 0, 1)
α^4	$\beta^4 \equiv \beta + 1$	(1, 1, 0, 0)
α^5	$\beta^5 \equiv \beta^2 + \beta$	(0, 1, 1, 0)
α^6	$\beta^6 \equiv \beta^3 + \beta^2$	(0, 0, 1, 1)
α^7	$\beta^7 \equiv \beta^3 + \beta + 1$	(1, 1, 0, 1)
α^8	$\beta^8 \equiv \beta^2 + 1$	(1, 0, 1, 0)
α^9	$\beta^9 \equiv \beta^3 + \beta$	(0, 1, 0, 1)
α^{10}	$\beta^{10} \equiv \beta^2 + \beta + 1$	(1, 1, 1, 0)
α^{11}	$\beta^{11} \equiv \beta^3 + \beta^2 + \beta$	(0, 1, 1, 1)
α^{12}	$\beta^{12} \equiv \beta^3 + \beta^2 + \beta + 1$	(1, 1, 1, 1)
α^{13}	$\beta^{13} \equiv \beta^3 + \beta^2 + 1$	(1, 0, 1, 1)
α^{14}	$\beta^{14} \equiv \beta^3 + 1$	(1, 0, 0, 1)
α^{15}	$\beta^{15} \equiv 1$	(1, 0, 0, 0)

Representando o exemplo 2.1, através de matrizes, obtemos,

$$A = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}_{4\times 4}$$

como $f(x) \in \mathbb{Z}_2$ então a matriz A, ou seja, a matriz companheira é:

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}_{4\times 4}$$

O corpo $GF(2^4)$ pode ser representado na forma:

$GF(16) = \{0, \text{I}, \text{A}, A^2, A^3, \text{A} + \text{I}, A^2 + \text{I}, A^2 + \text{A}, A^2 + \text{A} + \text{I}, A^3 + \text{I}, A^3 + \text{A}, A^3 + A^2, A^3 + A^2 + \text{A} + \text{I}, A^3 + A^2 + \text{I}, A^3 + \text{A} + \text{I}, A^3 + A^2 + \text{A}\}$

Aplicando-se as usuais regras da álgebra linear calculamos cada uma das matrizes do corpo $GF(2^4)$.

Considerações sobre a tabela:

• Na representação em série pela definição feita anteriormente sabemos que:

$GF(p^n) = \{0, \alpha, \alpha^2, \ldots, \alpha^{p^n-1})$, então, $GF(2^4) = \{0, \alpha, \alpha^2, \ldots, \alpha^{15}\}$

• Na representação polinomial é importante ressaltarmos que se o polinômio primitivo é $P(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$ e se β é uma raiz de P, então $\beta^4 = \beta + 1$. A tabela de multiplicação é dada pela identidade:

$\beta^5 = \beta^4 \cdot \beta = (\beta + 1) \cdot \beta = \beta^2 + \beta$

$\beta^6 = \beta^5 \cdot \beta = (\beta^2 + \beta) \cdot \beta = \beta^3 + \beta^2$ e assim por diante.

• A partir da representação polinomial escrevemos a representação vetorial. Por exemplo, a representação polinomial de $\beta^2 + \beta$, tem como representação vetorial: $(a_0, a_1, a_2, a_3) = (0, 1, 1, 0)$.

• Partindo do polinômio primitivo $P(x)$ e da tabela corpo para $GF(2^4)$ podemos computar o polinômio mínimo sobre $\mathbb{Z}_2$ para cada elemento de $GF(2^4)$.

Para calcularmos o polinômio mínimo é importante ressaltarmos primeiramente a definição de conjugado, pois é a partir dos conjugados que calculamos os polinômios mínimos.

Definição 2.3 Seja F subcorpo de E. Então $\alpha, \beta \in E$ são chamados de conjugados sobre F se eles tem um idêntico polinômio mínimo sobre F.

Teorema 2.1 *Para cada corpo finito $GF(q)$ e cada inteiro positivo d, existe um polinômio irredutível $p(x)$ de grau d sobre $GF(q)$. Seja α uma raiz de $p(x)$ em algum corpo extensão. Então podemos dizer que as raízes de $p(x)$ no corpo de decomposição (ou seja, o corpo que contém todas as raízes) são: α, α^q, α^{q^2}, ..., $\alpha^{q^{d-1}}$.*

A prova deste teorema pode ser encontrada em [20]. Sendo que o corpo decomposição de $p(x)$ é o corpo que contém todas as suas raízes.

Vamos verificar então, quais são os conjugados do exemplo anterior, ou seja de $GF(2^4)$.

conjugados de α: α,α^2,$\alpha^{2^2}\ldots$,$\alpha^{2^{4-1}}$ =α,α^2, α^4, α^8

conjugados de α^3: α^3, $(\alpha^3)^2$, $(\alpha^3)^{2^2}$ $\ldots$, $(\alpha^3)^{2^{4-1}}$ = α^3,α^6, α^{12}, α^{24}. Como $\alpha^{24} \equiv \alpha^9$ mod α^{15} então os conjugados de α^3 são: α^3,α^6, α^9 e α^{12}.

conjugados de α^5 =α^5,$(\alpha^5)^2$, $(\alpha^5)^{2^2}$, $\ldots$, $(\alpha^5)^{2^{4-1}}$ = α^5,α^{10}, α^{20}, α^{40}. Como $\alpha^{20} \equiv \alpha^5$ mod α^{15} e $\alpha^{40} \equiv \alpha^{10}$ mod α^{15}, então os conjugados de α^5 são: α^5 e α^{10}.

conjugados de α^7 =α^7,$(\alpha^7)^2$, $(\alpha^7)^{2^2}$,$\ldots$, $(\alpha^7)^{2^{4-1}}$ = α^7,α^{14}, α^{28}, α^{56}. Como $\alpha^{28} \equiv \alpha^{13}$ mod α^{15} e $\alpha^{56} \equiv \alpha^{11}$ mod α^{15}, então os conjugados de α^7 são: α^7, α^{11}, α^{13} e α^{14}.

Com isso já encontramos quatorze das dezesseis raízes que o polinômio possui, as outras duas são o zero e o $\alpha^{15} \equiv 1$ mod α^{15}.

Como α,α^2, α^4, α^8 são conjugados, então todos estes elementos têm o mesmo polinômio mínimo. Isso também acontece com o α^3,α^6, α^{12} e α^9, e os demais conjugados.

Seja $m_k(x)$ o polinômio mínimo de α^k, nós temos:

O polinômio mínimo de $\alpha, \alpha^2, \alpha^4$ e α^8 é $x^4 + x + 1$ já que α é raiz deste polinômio.

Polinômio mínimo de α^5 e α^{10}:

$m_5(x) = m_{10}(x) = (x - \alpha^5) \cdot (x - \alpha^{10}) = x^2 - \alpha^{10} \cdot x - x \cdot \alpha^5 + \alpha^{15} = x^2 - x \cdot (\alpha^{10} + \alpha^5) + \alpha^{15} = x^2 - x \cdot (\alpha^{10} + \alpha^5) + \alpha^{15} = x^2 - x \cdot 1 + 1$, então o polinômio mínimo de α^5 e α^{10} é $x^2 + x + 1$.

Polinômio mínimo de α^3, α^6, α^9 e α^{12} :

$m_3(\mathrm{x}) = m_6(x) = m_{12}(x) = m_9(x) = (x-\alpha^3)\cdot(x-\alpha^6)\cdot(x-\alpha^{12})\cdot(x-\alpha^9)$ $= (x^2-\alpha^6\cdot x-x\cdot\alpha^3+\alpha^9)\cdot(x-\alpha^{12})\cdot(x-\alpha^9) = (x^2-x\cdot(\alpha^6+\alpha^3)+\alpha^9)\cdot(x-\alpha^{12})\cdot(x-\alpha^9)$ $= (x^2-x\cdot\alpha^2+\alpha^9)\cdot(x-\alpha^{12})\cdot(x-\alpha^9) = (x^3-\alpha^{12}\cdot x^2-x^2\cdot\alpha^2+x\cdot\alpha^{14}+x\cdot\alpha^9-\alpha^{21})\cdot(x-\alpha^9)$ $= x^3-x^2\cdot(\alpha^{12}+\alpha^2)+x\cdot(\alpha^{14}+\alpha^9)-\alpha^6)\cdot(x-\alpha^9) = (x^3-x^2\cdot\alpha^7+x\cdot\alpha^4-\alpha^6)\cdot(x-\alpha^9) =$ $x^4-x^3\cdot\alpha^9-\alpha^3\cdot\alpha^7+\alpha^2\cdot\alpha^{16}+x^2\cdot\alpha^4-x\cdot\alpha^{13}-x\cdot\alpha^6+\alpha^{15} = x^4-x^3\cdot(\alpha^9+\alpha^7)+x^2\cdot(\alpha^{16}+$ $\alpha^4)-x\cdot(\alpha^{13}+\alpha^6)+\alpha^{15} = x^4-x^3\cdot\alpha^{15}+x^2\cdot\alpha^{15}-x\cdot\alpha^{15}+\alpha^{15} = x^4-x^3+x^2-x\cdot 1+1$, então o polinômio mínimo de α^3, α^6, α^9 e α^{12} é $x^4+x^3+x^2+x+1$.

Polinômio mínimo de α^7, α^{11}, α^{13} e α^{14}:

$m_7(x) = m_{14}(x) = m_{11}(x) = m_{13}(x) = (x-\alpha^7)\cdot(x-\alpha^{14})\cdot(x-\alpha^{11})\cdot$ $(x-\alpha^{13}) = (x^2-\alpha^{14}\cdot x-x\cdot\alpha^7+\alpha^{21})\cdot(x-\alpha^{11})\cdot(x-\alpha^{13}) = (x^2-x\cdot(\alpha^{14}+\alpha^7)+$ $\alpha^6)\cdot(x-\alpha^{11})\cdot(x-\alpha^{13}) = (x^2-x\cdot\alpha+\alpha^6)\cdot(x-\alpha^{11})\cdot(x-\alpha^{13}) = (x^3-\alpha^{11}\cdot x^2-x^2\cdot$ $\alpha+x\cdot\alpha^{12}+x\cdot\alpha^6-\alpha^{17})\cdot(x-\alpha^{13}) = x^3-x^2\cdot(\alpha^{11}+\alpha)+x\cdot(\alpha^{12}+\alpha^6)-\alpha^2)\cdot(x-\alpha^{13})$ $= (x^3-x^2\cdot\alpha^6+x\cdot\alpha^4-\alpha^2)\cdot(x-\alpha^{13}) = x^4-x^3\cdot\alpha^{13}-x^3\cdot\alpha^6+x^2\cdot\alpha^{19}+x^2\cdot$ $\alpha^4-x\cdot\alpha^{17}-x\cdot\alpha^2+\alpha^{15} = x^4-x^3\cdot(\alpha^{13}+\alpha^6)+x^2\cdot(\alpha^{19}+\alpha^4)-x\cdot(\alpha^{17}+\alpha^2)+1$ $= x^4-x^3\cdot\alpha^{15}+x^2\cdot 0-x\cdot 0+1 = x^4-x^3\cdot 1+0-0+1 = x^4-x^3+1$, então o polinômio mínimo de α^7, α^{11}, α^{13} e α^{14} é x^4+x^3+1.

Note que no exemplo 2.1 esgotamos a série α^i de $GF(2^4)$. Isso se deve ao fato de que escolhemos como polinômio irredutível x^4+x+1 que tem um elemento primitivo de $GF(2^4)$ como raiz. Sendo portanto, x^4+x+1, chamado de polinômio primitivo. Mas observe, que no exemplo abaixo β é uma raiz do polinômio $x^4+x^3+x^2+x+1$, mas não um elemento primitivo.

Exemplo 2.2 (Outra representação de $GF(2^4)$)

O polinômio $x^4+x^3+x^2+x+1$ é irredutível sobre $\mathbb{Z}_2$. β é uma raiz do polinômio, mas não um elemento primitivo, como podemos verificar na tabela abaixo:

Tabela 2.2: *Representação dos elementos* $\mathbb{Z}_2(\beta)$*, sendo* $x^4+x^3+x^2+x+1$ *o polinômio irredutível sobre* $\mathbb{Z}_2$*.*

Representação em série	Representação polinomial	Representação vetorial
0	0	(0, 0, 0, 0)
α	β	(0, 1, 0, 0)
α^2	β^2	(0, 0, 1, 0)
α^3	β^3	(0, 0, 0, 1)
α^4	$\beta^4 = \beta^3 + \beta^2 + \beta + 1$	(1, 1, 1, 1)
α^5	$\beta^5 = 1$	(1, 0, 0, 0)

Se continuássemos a fazer a tabela perceberíamos que a representação polinomial e conseqüentemente a representação vetorial iria começar a se repetir, o que comprova que β não é um elemento primitivo. Este fato implica em não podermos representar o corpo finito $GF(16)$ em série de β como fizemos no exemplo 2.1.

Para que possamos fazer esta representação polinomial de maneira que esta tenha uma relação com a representação em série, primeiramente devemos encontrar um elemento primitivo deste corpo.

A representação polinomial de $GF(2^4)$ é:

$GF(16) = \{0, 1, x, x^2, x^3, x+1, x^2+1, x^2+x, x^2+x+1, x^3+1, x^3+x, x^3+x^2, x^3+x^2+x, x^3+x^2+x+1, x^3+x+1, x^3+x^2+1\}$

Por tentativa encontramos um elemento primitivo deste corpo finito que é x + 1, pois como pode ser observado abaixo este elemento gera o grupo $GF(2^4)$.

$\alpha = (x+1)^1 = x+1$

$\alpha^2 = (x+1)^2 = x^2+2x+1$ como $\in GF(2) = x^2+1$

$\alpha^3 = (x+1)^3 = (x+1)^2 \cdot (x+1) = x^3+x^2+x+1$

$\alpha^4 = (x+1)^4 = x^4 + 2x^2 + 1$ como $\in GF(2)$ obtemos, $x^4 + 1$ mas $x^4 = x^3 + x^2 + x + 1$, então $x^4 + 1 = x^3 + x^2 + x + 2$ como $\in GF(2)$ obtemos $x^3 + x^2 + x$

$\alpha^5 = (x+1)^5 = x^4 + 2x^3 + 2x^2 + x$ como $\in GF(2)$ então, obtemos $x^4 + x$ mas $x^4 = x^3 + x^2 + x + 1$ portanto $x^4 + x = x^3 + x^2 + 1$

$\alpha^6 = (x+1)^6 = x^4 + 2x^3 + x^2 + x + 1$ como $\in GF(2)$ então, obtemos $x^4 + x^2 + x + 1$ como $x^4 = x^3 + x^2 + x + 1$ então $x^4 + x^2 + x + 1 = x^3$

$\alpha^7 = (x+1)^7 = x^4 + x^3$ como $x^4 = x^3 + x^2 + x + 1$ então, obtemos $x^2 + x + 1$

$\alpha^8 = (x+1)^8 = x^3 + 2x^2 + 2x + 1$ como $\in GF(2)$ então, obtemos, $x^3 + 1$

$\alpha^9 = (x+1)^9 = x^4 + x^3 + x + 1$ como $x^4 = x^3 + x^2 + x + 1$ então, obtemos x^2

$\alpha^{10} = (x+1)^{10} = x^3 + x^2$

$\alpha^{11} = (x+1)^{11} = x^4 + 2x^3 + x^2$ como $\in GF(2)$ então, obtemos $x^4 + x^2$ como $x^4 = x^3 + x^2 + x + 1$ obtemos, $x^3 + x + 1$

$\alpha^{12} = (x+1)^{12} = x^4 + x^3 + x^2 + 2x + 1$ como $\in GF(2)$ obtemos $x^4 + x^3 + x^2 + 1$ como $x^4 = x^3 + x^2 + x + 1$ então $x^4 + x^3 + x^2 + 1 = x$

$\alpha^{13} = (x+1)^{13} = x^2 + x$

$\alpha^{14} = (x+1)^{14} = x^3 + 2x^2 + x$ como $\in GF(2)$ obtemos $x^3 + x$

$\alpha^{15} = (x+1)^{15} = x^4 + x^3 + x^2 + x$ como $x^4 = x^3 + x^2 + x + 1$ obtemos, então $x^4 + x^3 + x^2 + x = 1$

Após encontrarmos o elemento primitivo podemos representar o corpo finito $GF(2^4)$. Sendo $\alpha = x + 1$, obtemos a tabela seguinte.

Tabela 2.3: *Representação dos elementos finitos de* $GF(2^4)$*, sendo* $\alpha = x + 1$ *o elemento primitivo*

Representação em série	Representação polinomial	Representação vetorial
0	0	(0, 0, 0, 0)
α	$\alpha = \mathrm{x} + 1$	(1, 1, 0, 0)
α^2	$\alpha^2 = (x+1)^2 = x^2 + 1$	(1, 0, 1, 0)
α^3	$\alpha^3 = (x+1)^3 = x^3 + x^2 + \mathrm{x} + 1$	(1, 1, 1, 1)
α^4	$\alpha^4 = (x+1)^4 = x^3 + x^2 + \mathrm{x}$	(0, 1, 1, 1)
α^5	$\alpha^5 = (x+1)^5 = x^3 + x^2 + 1$	(1, 0, 1, 1)
α^6	$\alpha^6 = (x+1)^6 = x^3$	(0, 0, 0, 1)
α^7	$\alpha^7 = (x+1)^7 = x^2 + \mathrm{x} + 1$	(1, 1, 1, 0)
α^8	$\alpha^8 = (x+1)^8 = x^3 + 1$	(1, 0, 0, 1)
α^9	$\alpha^9 = (x+1)^9 = x^2$	(0, 0, 1, 0)
α^{10}	$\alpha^{10} = (x+1)^{10} = x^3 + x^2$	(0, 0, 1, 1)
α^{11}	$\alpha^{11} = (x+1)^{11} = x^3 + \mathrm{x} + 1$	(1, 1, 0, 1)
α^{12}	$\alpha^{12} = (x+1)^{12} = \mathrm{x}$	(0, 1, 0, 0)
α^{13}	$\alpha^{13} = (x+1)^{13} = x^2 + \mathrm{x}$	(0, 1, 1, 0)
α^{14}	$\alpha^{14} = (x+1)^{14} = x^3 + \mathrm{x}$	(0, 1, 0, 1)
α^{15}	$\alpha^{15} = (x+1)^{15} = 1$	(1, 0, 0, 0)

Vamos representar o exemplo anterior também através de matriz. Sabemos que a $f(x) = x^4 + x^3 + x^2 + x + 1$ e que $\in \mathbb{Z}_2$.

$$A = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{bmatrix}_{4\times 4}$$

Como $f(x) \in \mathbb{Z}_2$ então a matriz A, ou seja a matriz companheira é:

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}_{4\times 4}$$

O corpo $GF(2^4)$ pode ser representado na forma,

$GF(16) = \{0, I, A, A^2, A^3, A+I, A^2+I, A^2+A, A^2+A+I, A^3+I, A^3+A, A^3+A^2, A^3+A^2+A+I, A^3+A^2+I, A^3+A+I, A^3+A^2+A\}$

Aplicando-se as usuais regras da álgebra linear calcula-se cada uma das matrizes do corpo $GF(2^4)$.

Após calcularemos o polinômio mínimo e como vimos no exemplo anterior devemos primeiramente encontrar os conjugados:

conjugados de α =α,α^2,α^{2^2}...,$\alpha^{2^{4-1}}$ =α,α^2, α^4, α^8

conjugados de α^3 = α^3, $(\alpha^3)^2$, $(\alpha^3)^{2^2}$ ..., $(\alpha^3)^{2^{4-1}}$ = α^3,α^6, α^{12}, α^{24}, como, $\alpha^{24} \equiv \alpha^9$ mod α^{15}, então os conjugados de α^3 são α^3, α^6, α^{12}, α^9

conjugados de α^5 =α^5,$(\alpha^5)^2$, $(\alpha^5)^{2^2}$, ..., $(\alpha^5)^{2^{4-1}}$ = α^5,α^{10}, α^{20}, α^{40}, como, $\alpha^{20} \equiv \alpha^5$ mod α^{15} e $\alpha^{40} \equiv \alpha^{10}$ mod α^{15}, então os conjugados de α^5 são α^5,α^{10}

conjugados de α^7 =α^7,$(\alpha^7)^2$, $(\alpha^7)^{2^2}$,..., $(\alpha^7)^{2^{4-1}}$ = α^7,α^{14}, α^{28}, α^{56}, como, $\alpha^{28} \equiv \alpha^{13}$ mod α^{15} e $\alpha^{56} \equiv \alpha^{11}$ mod α^{15}, então os conjugados de α^7 são α^7,α^{14}, α^{13}, α^{11}

As outras duas raízes são o zero e o $\alpha^{15} \equiv 1$ mod α^{15}.

Como já vimos α,α^2, α^4, α^8 são conjugados, portanto têm o mesmo polinômio mínimo. Isso também acontece com o α^3,α^6, α^{12} e α^9, e os demais conjugados, calculamos então os polinômios mínimos $m_k(y)$ de α^k.

Notemos que o polinômio mínimo de $\alpha^3, \alpha^6, \alpha^9$ e α^{12} é $y^4+y^3+y^2+y+1$, ou seja o próprio polinômio irredutível sobre $GF(2)$ usado na representação do corpo. É fácil verificar que $\alpha^3, \alpha^6, \alpha^9$ e α^{12} são as raízes do polinômio irredutível $y^4 + y^3 + y^2 + y + 1$. Mesmo assim vamos fazer esta verificação. Sabemos que $\alpha = x+1 \Rightarrow \alpha^3 = (x+1)^3 = x^3+x^2+x+1$. Sabemos que para α^3 ser raiz do polinômio devemos substituir o y por α^3 e ao resolver o cálculo mod $P(y)$ devemos encontrar como resto zero. Então, $y^4 + y^3 + y^2 + y + 1 = (x^3 + x^2 + x + 1)^4 + (x^3 + x^2 + x + 1)^3 + (x^3 + x^2 + x + 1)^2 + (x^3 + x^2 + x + 1) + 1$ mod $P(y) = 0$.

Se desejássemos verificar que α^6, α^9 e α^{12} são realmente raízes, procederíamos da mesma forma.

Polinômio mínimo de α^5 e α^{10}:

$m_5(y) = m_{10}(y) = (y - \alpha^5) \cdot (y - \alpha^{10}) = y^2 - \alpha^{10} \cdot y - y \cdot \alpha^5 + \alpha^{15} = y^2 - y \cdot (\alpha^{10} + \alpha^5) + \alpha^{15} = y^2 - y \cdot 1 + 1$, como $\in GF(2)$, então o polinômio mínimo de α^5 e α^{10} é $y^2 + y + 1$.

Polinômio mínimo de α, α^2, α^4 e α^8:

$m(y) = m_2(y) = m_4(y) = m_8(y) = (y-\alpha)\cdot(y-\alpha^2)\cdot(y-\alpha^4)\cdot(y-\alpha^8) = (y^2-\alpha^2\cdot y-y\cdot\alpha+\alpha^3)\cdot(y-\alpha^4)\cdot(y-\alpha^8) = (y^2-y\cdot(\alpha^2+\alpha)+\alpha^3)\cdot(y-\alpha^4)\cdot(y-\alpha^8) = (y^2-y\cdot\alpha^{13}+\alpha^3)\cdot(y-\alpha^4)\cdot(y-\alpha^8) = (y^3-\alpha^4\cdot y^2-y^2\cdot\alpha^{13}+y\cdot\alpha^{17}+y\cdot\alpha^3-\alpha^7)\cdot(y-\alpha^8) = (y^3-y^2\cdot(\alpha^4+\alpha^{13})+y\cdot(\alpha^{17}+\alpha^3)-\alpha^7)\cdot(y-\alpha^8) = (y^3-y^2\cdot\alpha^6+y\cdot\alpha^{14}-\alpha^7)\cdot(y-\alpha^8) = y^4 - y^3\cdot\alpha^8 - y^3\cdot\alpha^6 + y^2\cdot\alpha^{14} + y^2\cdot\alpha^{14} - y\cdot\alpha^{22} - y\cdot\alpha^7 + \alpha^{15} = y^4 - y^3\cdot(\alpha^8+\alpha^6) + y^2\cdot(\alpha^{14}+\alpha^{14}) - y\cdot(\alpha^{22}+\alpha^7) + \alpha^{15} = y^4 - y^3\cdot\alpha 15 + y^2\cdot 0 - y\cdot 0 + \alpha^{15} = y^4 - y^3 + 1$, como $\in GF(2)$, então o polinômio mínimo de α, α^2, α^4 e α^8 é $y^4 + y^3 + 1$.

Polinômio mínimo de α^7, α^{11}, α^{13} e α^{14}:

$m_7(y) = m_{14}(y) = m_{11}(y) = m_{13}(y) = (y-\alpha^7)\cdot(y-\alpha^{14})\cdot(y-\alpha^{11})\cdot(y-\alpha^{13}) = (y^2-\alpha^{14}\cdot y-y\cdot\alpha^7+\alpha^{21})\cdot(y-\alpha^{11})\cdot(y-\alpha^{13}) = (y^2-y\cdot(\alpha^{14}+\alpha^7)+\alpha^6)\cdot(y-\alpha^{11})\cdot(y-\alpha^{13}) = (y^2-y\cdot\alpha^5+\alpha^6)\cdot(y-\alpha^{11})\cdot(y-\alpha^{13}) = (y^3-\alpha^{11}\cdot y^2-y^2\cdot\alpha^5+y\cdot\alpha^{16}+y\cdot\alpha^6-\alpha^{17})\cdot(y-\alpha^{13}) = (y^3 - y^2\cdot(\alpha^{11}+\alpha^5) + y\cdot(\alpha^{16}+\alpha^6) - \alpha^2)\cdot(y-\alpha^{13}) = (y^3 - y^2\cdot\alpha^{13} + y\cdot\alpha^{11} - \alpha^2)\cdot(y-\alpha^{13}) = y^4 - y^3\cdot\alpha^{13} - y^3\cdot\alpha^{13} + y^2\cdot\alpha^{26} + y^2\cdot\alpha^{11} - y\cdot\alpha^{24} - y\cdot\alpha^2 + \alpha^{15} = y^4 - y^3\cdot(\alpha^{13}+\alpha^{13}) + y^2\cdot(\alpha^{26}+\alpha^{11}) - y\cdot(\alpha^{24}+\alpha^2+1 = y^4 - y^3\cdot 0 + y^2\cdot 0 - y\cdot\alpha 15 + 1 = y^4 - y + 1$, como $\in GF(2)$ então o polinômio mínimo de α^7, α^{11}, α^{13} e α^{14} é $y^4 + y + 1$.

É importante observarmos que os corpos $\mathbb{Z}_2[x]/x^4 + x + 1$ e $\mathbb{Z}_2[x]/x^4 + x^3 + x^2 + x + 1$ dos respectivos exemplos (2.1) e (2.2) são isomorfos, pois pelo teorema (1.6), dois quaisquer corpos finitos que têm o mesmo número de elementos

são isomorfos. Isso implica que eles tem a mesma representação polinomial, vetorial e também matricial, embora não haja correspondência entre elas.

3 FATORAÇÃO DE POLINÔMIOS SOBRE CORPOS FINITOS

Este capítulo abordará o tema fatoração de polinômios. Para fatorarmos um polinômio em corpos finitos existem muitos métodos, dentre os quais estudaremos o método de Berlekamp, Cantor-Zassenhaus e Lidl-Niederreiter.

3.1 Introdução

Julgamos que este tema é muito importante não somente por si, mas também para muitas aplicações em álgebra computacional, teoria de códigos, criptografia e teoria computacional de números. A fatoração de polinômios sobre corpos finitos é usada também como um sub-problema em algoritmos para fatorar polinômios sobre os inteiros, para computar logaritmo discreto, para calcular as raízes de polinômios, para estimar o número de pontos em curvas elípticas entre outras aplicações. Estas aplicações da fatoração podem ser encontradas entre outros em ([13]), ([10]) e ([11]).

Os procedimentos utilizados na fatoração de polinômios são baseados nos métodos de álgebra linear e em aritmética polinomial.

No decorrer dos anos buscou-se encontrar métodos para fatorar polinômios em corpos finitos que reduzissem cada vez mais o tempo de execução do algoritmo.

O primeiro foi introduzido por Berlekamp, em 1967 [15]. O seu algoritmo reduzia o problema para achar polinômios que formassem uma base para o espaço nulo de uma matriz $n \times n$ sobre $GF(q)$, usando para isso técnicas de álgebra linear. O algoritmo de Berlekamp foi implementado em um número de $O(n^3 + n \cdot q)$ operações em $GF(q)$, onde n é o grau do polinômio a ser fatorado.

Rabin [9] criou o seu método em 1980 com um tempo aparentemente inferior ao de Berlekamp, porém, não conseguiu provar matematicamente esta redução no tempo. Ao fazer a justificativa matemática o número de operações não teve alteração em relação ao método de Berlekamp.

Um algoritmo com diferença real foi descrito em 1981 por Cantor e Zassenhaus [22]. Este algoritmo fatora um dado polinômio em polinômios de grau distintos e depois fatora cada um em fatores irredutíveis de mesmo grau. O algoritmo pode ser implementado num tempo médio de execução de $O(n^2 \cdot q)$ operações em $GF(q)$.

Em 1992 Von Zur Gathen e Shoup [21] desenvolveram um novo algoritmo usando essencialmente técnicas criadas com o intuito de implementar o algoritmo de Cantor/Zassenhaus. O algoritmo usa um número esperado de $O(n^2 + n \cdot q)$ operações em $GF(q)$.

Em 1993 Niederreiter [13] desenvolveu uma outra alternativa para fatorar polinômios sobre corpos finitos. Porém do ponto de vista da complexidade não obteve melhoras em relação ao algoritmo original de Berlekamp.

Em 1994 Kaltofen e Lobo [9] adaptaram a técnica para resolver um sistema linear de Wiedemann(1986) para o algoritmo de Berlekamp. Utilizaram técnicas a partir de Von Zur Gathen e Shoup, e o algoritmo passou a se chamar Black Box Berlekamp e pode ser implementado em $O(n^2 + n \cdot q)$ em $GF(q)$.

A escolha do algoritmo a ser usado para fatorar polinômios em corpos finitos depende do tamanho do corpo em que o polinômio está inserido, pois alguns métodos são eficientes para a fatoração em corpos finitos pequenos, mas são ineficientes ou muito trabalhosos quando aplicados a corpos finitos grandes. Na seção 3.2 procuraremos descrever como retirar do polinômio os fatores repetidos, pois sabemos que após feito isto podemos fatorar os polinômios livre de quadrados, na seção 3.3 discutiremos sobre o método de Berlekamp, que foi o primeiro algoritmo desenvolvido para fatorar polinômios em corpos finitos. Na seção 3.4, nós discutiremos

sobre o método de Cantor-Zassenhaus que é muito eficiente para fatorar polinômios tanto em corpos finitos pequenos, quanto em corpos finitos grandes. E na seção 3.5 apresentaremos um algoritmo de Lidl-Niederreiter usado na fatoração de polinômios sobre corpos finitos pequenos.

3.2 Fatoração Livre de Quadrados

A fatoração de polinômios consiste em expressar polinômios de grau positivo na forma, $f(x) = a \cdot p_1^{e_1} \cdots p_k^{e_k}$ onde $a \in GF(q)$ e $p_1, \cdots, p_k$ são polinômios mônicos irredutíveis e distintos em $GF(q)$.

Porém, nem sempre ao fatorarmos um polinômio arbitrário encontramos somente fatores irredutíveis distintos. Como o objetivo ao fatorar um polinômio é expressá-lo na forma de produto de polinômios distintos, precisamos inicialmente, independente do método escolhido e do tamanho do corpo, verificar se o polinômio $f(x)$ tem fatores repetidos. Isso é feito através do cálculo do $m.d.c(f(x), f'(x))$.

Se o $m.d.c(f(x), f'(x))$ for igual a 1, isso indica que a $f(x)$ não tem fatores repetidos, o que é explicado pelo teorema abaixo.

Teorema 3.1 *Seja b uma raiz de $f(x) \in F[x]$. O elemento $b \in F$ é uma raiz múltipla de $f \in F[x]$ se e somente se b é uma raiz também de $f'(x)$.*

Este teorema segue imediatamente do teorema (4.1) que por razões de praticidade está demonstrado no capítulo 4. Sua prova é elementar e também pode ser encontrada, por exemplo, em [14].

Se o $m.d.c(f(x), f'(x)) \neq 1$ e também $m.d.c(f(x), f'(x)) \neq f(x)$ isso indica que o resultado do m.d.c. é um fator não trivial de $f(x)$. Retiramos este fator de $f(x)$ e repetimos o cálculo do $m.d.c.$, se der 1 então $f(x)$ não tem mais fatores repetidos.

Se o $m.d.c(f(x), f'(x)) = f(x)$ isso indica que nós temos $f'(x) = 0$. Quando isso acontecer é porque $f(x)$ tem a forma,

$$f(x) = \sum_{i=0}^{n/q} f_i \cdot x^{qi} = (\sum_{i=0}^{n/q} f_i^{\frac{1}{q}} \cdot x^i)^q,$$

ou seja, a $f(x)$ é uma potência de q. Para reduzirmos a fatoração somente a fatores irredutíveis distintos devemos fatorar apenas o termo $f_i^{\frac{1}{q}} \cdot x^i$, procedendo como no caso onde $f'(x) \neq 0$.

No apêndice C apresentaremos exemplos onde verificamos se a $f(x)$ tem fatores repetidos ou não.

Quando obtivermos a $f(x)$ sem fatores repetidos, iniciamos a fatoração propriamente dita. Sendo que a fatoração deste polinômio sem fatores repetidos nos levam diretamente a fatoração do polinômio original.

3.3 Método de Berlekamp

Em 1967 foi desenvolvido por Elwyn R. Berlekamp [15], o primeiro algoritmo para fatorar polinômios em corpos finitos. Este método tem muita tradição, e isso não se deve somente ao fato de ter sido o primeiro algoritmo desenvolvido para fatorar polinômios em corpos finitos, mas também por ser fácil de entendê-lo e por ser ainda muito usado.

Ao empregarmos o método de Berlekamp para fatorar polinômios o seguinte teorema tem fundamental importância.

Teorema 3.2 *Se $f \in GF(q)[x]$ é mônico e $h \in GF(q)[x]$ é tal que $h^q \equiv h \ mod \ f$ então*

$$f(x) = \prod_{c \in GF(q)} m.d.c.(f(x), h(x) - c) \tag{3.1}$$

Demonstração Cada máximo divisor comum do lado direito de 3.2 divide $f(x)$. Como os polinômios $h(x) - c$, $c \in GF(q)$ são relativamente primos, então são os

máximos divisores comuns com $f(x)$, e desse modo o produto desses máximos divisores comuns dividem $f(x)$. Como o produto de fatores irredutíveis é expresso por $h(x)^q$ - $h(x)$, como vimos no capítulo 1, pelo teorema(1.11), podemos afirmar então que,

$$h(x)^q - h(x) = \prod_{c \in GF(q)} (h(x) - c)$$

e como $f(x)$ divide o lado direito de 3.2 e os dois lados de 3.2 são polinômios mônicos que se dividem então eles o devem ser iguais. □

Pelo teorema acima a fatoração de $f(x)$ será obtida pelo produto do(s) $m.d.c.(f(x), h(x) - c)$, sendo que $h(x)$ é um fator irredutível mônico de f e c são todos os elementos pertencentes a $GF(q)$.

Como já frisamos anteriormente o primeiro passo que devemos seguir ao fatorar polinômios é verificar se o mesmo possui fatores repetidos.

Se assumimos que $f(x)$ não tem mais fatores repetidos, então podemos dizer que a $f(x)$ é o produto de distintos polinômios mônicos irredutíveis sobre $GF(q)$.

Pelo teorema (3.1), fica claro que para fatorarmos $f(x)$ devemos encontrar $h(x)$ e c.

Teorema 3.3 (Chinês dos Restos) *Sejam $u_1(x) \cdots u_r(x)$ polinômios sobre GF(q) com $u_j(x)$ relativamente primo a $u_k(x)$ para todo $k \neq j$. Para qualquer polinômio $w_1(x), \cdots, w_r(x) \in$ GF(q)[x] existe um único polinômio v(x) tal que*

$grau(v) < grau(u_1) + \cdots + grau(u_r)$

$v(x) = w_j(x)$ *mod* $u_j(x)$ *para* $1 \leq j \leq r$

A prova deste teorema pode ser encontrada em [14].

Se $(c_1, \cdots, c_k)$ é qualquer k-upla de elementos de $GF(q)$, então pelo teorema Chinês dos restos sabemos que existe um único $h \in GF(q)[x]$ com $h(x) \equiv c_i$ mod $f_i(x)$ para $1 \leq i \leq k$ e $grau(h) < grau(f)$.

O polinômio $h(x)$ satisfaz a condição $h(x)^q \equiv c_i^q = c_i \equiv h(x)$ mod $f_i(x)$ para $1 \leq i \leq k$. Como, $c_i \equiv h(x)$ mod $f_i(x)$ basta encontrarmos $h(x)$ que satisfaça a condição,

$$h^q \equiv h \text{ mod } f, grau(h) < grau(f) \tag{3.2}$$

Por outro lado, se h é a solução (3.2), então a identidade

$$h(x)^q - h(x) = \prod_{c \in GF(q)} (h(x) - c)$$

implica que cada fator irredutível de f divide um dos polinômios de $h(x) - c$. Para encontrarmos as soluções de (3.2) devemos reduzir $h^q \equiv h$ mod f para um sistema de equações lineares. Estas equações lineares são obtidas através do cálculo x^{iq} mod $f(x)$, sendo $0 \leq i \leq n-1$. A partir destas equações montamos uma matriz de ordem $n \times n$ a qual denominaremos de matriz B. A matriz B deve satisfazer a equação $h \cdot B$ = h ou seja, $h \cdot B - h = 0$ o que implica que $h \cdot (B - I) = 0$, sendo I a matriz identidade de ordem $n \times n$. Por isso, nosso próximo passo é calcularmos a matriz B - I. Após fazemos o escalonamento da matriz B - I para conseguirmos definir o posto da mesma, o qual será identificado por r. É necessário definirmos o posto da matriz pois só assim conseguiremos definir o número de polinômios irredutíveis mônicos distintos de f, que é dado pela fórmula $k = n - r$.

Caso $k = 1$, podemos afirmar que f é irredutível sobre $GF(q)$, não tendo portanto como fatorá-lo.

Se $k \geq 2$ devemos definir os vetores $h(x)$ que formam a base para o espaço nulo de B - I e após calcular o $m.d.c.(f(x), h(x) - c)$, sendo c todos os elementos pertencentes a $GF(q)$. É importante ressaltarmos que se houverem mais de um $h(x)$, devemos escolher um deles para realizarmos o cálculo do $m.d.c.(f(x), h(x) - c)$, pois a escolha do $h(x)$ não provocará alteração na fatoração de $f(x)$.

Assim, o algoritmo de Berlekamp usado para fatorar polinômios em corpos finitos pequenos pode ser descrito como segue.

Passo 1. Verificamos se a $f(x)$ tem fatores repetidos, como vimos anteriormente fazemos isso através do cálculo $m.d.c.(f(x), f'(x))$.

Passo 2. Calculamos x^{iq} mod $f(x)$ para $0 \leq i \leq n-1$, a fim de construirmos a matriz B.

Passo 3. Calculamos a matriz B - I, o posto e o número de fatores irredutíveis mônicos distintos de f, que é dado por $k = n - r$.

Passo 4. Caso $k = 1$, podemos afirmar que f é irredutível sobre $GF(q)$, não tendo portanto como fatorá-lo.

Se $k \geq 2$ devemos obter os vetores $h(x)$ que formam a base para o espaço nulo de B - I e após calcular o $m.d.c.(f(x), h(x) - c)$, sendo c todos os elementos pertencentes a $GF(q)$.

Exemplo 3.1 Seja $f(x) = x^8 + x^6 + x^4 + x^3 + 1$ sobre $GF(2)$. Para encontrarmos a fatoração de $f(x)$ sabemos que o primeiro passo é verificarmos se ela tem fatores repetidos, para isso calculamos o $m.d.c.(f(x), f'(x))$, ou seja, $m.d.c.(x^8 + x^6 + x^4 + x^3 + 1, 8 \cdot x^7 + 6 \cdot x^5 + 4 \cdot x^3 + 3 \cdot x^2) = m.d.c.(x^8 + x^6 + x^4 + x^3 + 1, x^2) = 1$. Como o $m.d.c.(f(x), f'(x)) = 1$ podemos concluir que $f(x)$ não tem fatores repetidos e assim começamos aplicar o método de Berlekamp.

Calculamos x^{iq} mod $f(x)$ para $q = 2$ e $0 \leq i \leq 7$, com o objetivo de definirmos as equações lineares que farão parte da matriz B. As equações serão, $x^{0 \cdot 2} = x^0 \equiv 1$; $x^{1 \cdot 2} = x^2 \equiv x^2$; $x^{2 \cdot 2} = x^4 \equiv x^4$; $x^{3 \cdot 2} = x^6 \equiv x^6$; $x^{4 \cdot 2} = x^8 \equiv x^6 + x^4 + x^3 + 1$; $x^{5 \cdot 2} = x^{10} \equiv x^5 + x^4 + x^3 + x^2 + 1$; $x^{6 \cdot 2} = x^{12} \equiv x^7 + x^6 + x^5 + x^4 + x^2$; $x^{7 \cdot 2} = x^{14} \equiv x^5 + x^4 + x^3 + x + 1$. Montamos a matriz $B_{n \times n}$, ou seja $B_{8 \times 8}$.

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}_{8\times 8}$$

e B - I é dada por,

$$B - I = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}_{8\times 8}$$

O próximo passo é fazer o escalonamento da matriz B - I, a fim de encontrarmos o número de linhas não nulas de B - I escalonada. Assim, podemos encontrar o valor de k que indica o número de fatores irredutíveis mônicos distintos de f, $k = n - r = 8 - 6 = 2$. Portanto, existem dois fatores irredutíveis mônicos distintos de f.

Os vetores que formam a base do espaço nulo de B - I são (1, 0, 0, 0, 0, 0, 0, 0) e (0, 1, 1, 0, 0, 1, 1, 1). Os polinômios correspondentes a estes vetores são, $h_1(x) = 1$ e $h_2(x) = x + x^2 + x^5 + x^6 + x^7$.

Como o $k = 2$ sabemos que f é um polinômio de base redutível por isso, devemos calcular o $m.d.c.(f(x), h_2(x) - c)$ para $c \in GF(2)$.

$m.d.c.(f(x), h_2(x)-0) = m.d.c(x^8+x^6+x^4+x^3+1, x^7+x^6+x^5+x^2+x) = x^6 + x^5 + x^4 + x + 1$

$m.d.c.(f(x), h_2(x) - 1) = m.d.c(x^8 + x^6 + x^4 + x^3 + 1, x^7 + x^6 + x^5 + x^2 + x + 1) = x^2 + x + 1$

Portanto, a fatoração de $f(x)$ é $f(x) = (x^6+x^5+x^4+x+1)\cdot(x^2+x+1)$.

O algoritmo de Berlekamp, não é tão eficiente, para fatorarmos polinômios em corpos finitos grandes, pois, torna-se muito trabalhoso encontrar $c \in GF(q)$ que satisfaça a condição $m.d.c(f(x), h(x) - c)$ não trivial o que torna o tempo de execução de tal procedimento proporcional a q, o que não será desejável para q grande. Mas, se optarmos por aplicar este algoritmo para fatorar polinômios em corpos finitos grandes devemos procurar reduzir o número de $c \in GF(q)$ de forma que este satisfaça a condição referida acima. Para isso podemos usar a teoria dos resultantes.

A partir deste momento assumiremos que ao quantificarmos o p tomaremos como medida para considerá-lo pequeno, um computador onde a palavra tem 32 bits sendo $p < 10^9$.

3.3.1 Fatoração sobre corpos finitos grandes

Definição 3.1 Seja $f(x) = a_0 \cdot x^n + a_1 \cdot x^{n-1} + \cdots + a_n \in GF(q)$ e $g(x) = b_0 \cdot x^m + b_1 \cdot x^{m-1} + \cdots + b_m \in GF(q)$ dois polinômios de grau n e m respectivamente, e com

n e $m \in \mathbb{N}$. Então a resultante $R(f,g)$ é definida pelo determinante

$$R(f,g) = \left[\begin{array}{cccccccc} a_0 & a_1 & \cdots & a_n & 0 & & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \cdots & 0 & a_0 & a_1 & & \cdots & a_n \\ b_0 & b_1 & \cdots & & b_m & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & & b_m & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \cdots & 0 & b_0 & b_1 & & \cdots & b_m \end{array}\right] \begin{array}{l} \left.\begin{array}{l} \\ \\ \\ \end{array}\right\} \text{m linhas} \\ \left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} \text{n linhas} \end{array}$$

de ordem $m+n$.

Se grau de $f = n$ (isto é, se $a_0 \neq 0$) e $f(x) = a_0(x-\alpha_1)\cdots(x-\alpha_n)$ no corpo decomposição de f sobre F, então $R(f,g)$ é também dada pela fórmula $R(f,g) = a_0^m \prod_{i=1}^{n} g(\alpha_i)$, conforme podemos verificar em [13]. Neste caso, nós obviamente temos $R(f,g) = 0$ se e somente se f e g tem uma raiz comum. Portanto, se $R(f(x), h(x)-c)$ é a resultante de $f(x)$ e $h(x)-c$, podemos afirmar que só teremos $m.d.c.(f(x), h(x)-c) \neq 1$ se $R(f(x), h(x)-c) = 0$. Isso nos leva a considerar que só teremos $m.d.c.(f(x), h(x)-c) \neq 1$ se c for uma raiz de $R(f(x), h(x)-c)$ em $GF(q)$. A partir deste momento passaremos a denominar $R(f(x), h(x)-c)$ de $F(y)$.

Abaixo descreveremos o algoritmo de Berlekamp para fatorar polinômios pertencentes a corpos finitos grandes, ressaltando que os quatro primeiros passos, são iguais a fatoração para polinômios sobre corpos finitos pequenos.

Passo 1. Verificamos se existem fatores repetidos em $f(x)$, se houverem os retiramos.

Passo 2. Calculamos x^{iq} mod $f(x)$ para $0 \leq i \leq n-1$, obtendo a matriz B.

Passo 3. Obtemos a matriz B - I, o posto da mesma e o número de fatores irredutíveis mônicos distintos de f em $GF(q)$.

Passo 4. Encontramos os vetores $h(x)$ que formam a base para o espaço nulo de B - I.

Passo 5. Calculamos o resultante, $R(f(x), h(x) - y)$, encontrando um polinômio o qual denominaremos de $F(y)$.

Passo 6. Por tentativa e erro ou pelos métodos que veremos no próximo capítulo devemos encontrar as raízes de $F(y) \in GF(q)$, as quais chamaremos de c.

Passo 7. Por fim calculamos um $m.d.c(f(x), h(x) - c)$, para cada um dos c encontrados, obtendo a fatoração de $f(x)$.

Exemplo 3.2 Seja $f(x) = x^6 - 3 \cdot x^5 + 5 \cdot x^4 - 9 \cdot x^3 - 5 \cdot x^2 + 6 \cdot x + 7$ sobre GF(23). Para fatorarmos a $f(x)$ verificamos inicialmente se existem fatores repetidos, para isso calcularmos o $m.d.c.(f(x), f'(x))$,ou seja, $m.d.c.(x^6 - 3 \cdot x^5 + 5 \cdot x^4 - 9 \cdot x^3 - 5 \cdot x^2 + 6 \cdot x + 7, 6 \cdot x^5 - 15 \cdot x^4 + 20 \cdot x^3 - 27 \cdot x^2 - 10 \cdot x + 6) = 1$. Portanto, $f(x)$ não tem fatores repetidos.

Calculamos x^{iq} mod $f(x)$ para $q = 23$ e $0 \leq i \leq 5$

$x^{0 \cdot 23} = x^0 \equiv 1$

$x^{1 \cdot 23} = x^{23} \equiv 5 - x^2 + 8 \cdot x^3 - 3 \cdot x^4 - 10 \cdot x^5$

$x^{2 \cdot 23} = x^{46} \equiv -10 + 10 \cdot x + 10 \cdot x^2 + x^4 - 9 \cdot x^5$

$x^{3 \cdot 23} = x^{69} \equiv 7 \cdot x + 9 \cdot x^2 - 8 \cdot x^3 + 10 \cdot x^4 - 11 \cdot x^5$

$x^{4 \cdot 23} = x^{92} \equiv 11 - 4 \cdot x^2 + 7 \cdot x^3 + 7 \cdot x^4 + 2 \cdot x^5$

$x^{5 \cdot 23} = x^{115} \equiv -3 - 10 \cdot x^2 + 9 \cdot x^3 + 2 \cdot x^4 - 9 \cdot x^5$

Obtendo assim a matriz $B_{6 \times 6}$.

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 5 & 0 & -1 & 8 & -3 & -10 \\ -10 & 10 & 10 & 0 & 1 & -9 \\ 0 & 7 & 9 & -8 & 10 & -11 \\ 11 & 0 & -4 & 7 & 7 & 2 \\ -3 & 0 & -10 & 9 & 2 & -9 \end{bmatrix}_{6\times 6}$$

e B - I é dada por,

$$B - I = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 5 & -1 & -1 & 8 & -3 & -10 \\ -10 & 10 & 9 & 0 & 1 & -9 \\ 0 & 7 & 9 & -9 & 10 & -11 \\ 11 & 0 & -4 & 7 & 6 & 2 \\ -3 & 0 & -10 & 9 & 2 & -10 \end{bmatrix}_{6\times 6}$$

Escalonamos a matriz B - I a fim de obtermos o número de linhas não nulas, ou seja $r = 3$. Após encontramos o número de fatores irredutíveis mônicos distintos de f em $GF(23)$, $k = n - r = 6 - 3 = 3$. Estes fatores são denominados de $h(x)$ e são: (1, 0, 0, 0, 0, 0) , (0, 4, 2, 1, 0, 0) e (0, -2, 9, 0, 1, 1), que correspondem aos polinômios: $h_1(x) = 1$, $h_2(x) = 4 \cdot x + 2 \cdot x^2 + x^3$ e $h_3(x) = -2 \cdot x + 9 \cdot x^2 + x^4 + x^5$.

Como estamos trabalhando com corpos finitos grandes, seria muito trabalho encontrar $m.d.c.(f(x), h(x) - c) \neq 1$ por isso, calcularemos o resultante

$F(y) = R(f(x), h(x) - y)$, sendo que usaremos $h(x) = 4 \cdot x + 2 \cdot x^2 + x^3$.

$$R(f,g) = \begin{bmatrix} 1 & -3 & 5 & -9 & -5 & 6 & 7 & 0 & 0 \\ 0 & 1 & -3 & 5 & -9 & -5 & 6 & 7 & 0 \\ 0 & 0 & 1 & -3 & 5 & -9 & -5 & 6 & 7 \\ 1 & 2 & 4 & -y & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 4 & -y & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 4 & -y & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 4 & -y & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 4 & -y & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & -y \end{bmatrix}_{9\times 9}$$

A ordem da matriz é 9×9. Calculamos o determinante desta matriz, obtendo, $F(y) = y^6 + 4 \cdot y^5 + 3 \cdot y^4 - 7 \cdot y^3 + 10 \cdot y^2 + 11 \cdot y + 7$.

Usando o método de tentativa e erro ou ainda algum dos métodos que veremos no próximo capítulo encontramos as raízes de $F(y)$ em $GF(23)$, que são -3, 2 e 6. De posse destas raízes calculamos $m.d.c.(f(x), h(x) - c)$.

$m.d.c.(f(x), h_2(x) + 3) = m.d.c(x^6 - 3 \cdot x^5 + 5 \cdot x^4 - 9 \cdot x^3 - 5 \cdot x^2 + 6 \cdot x + 7, x^3 + 2 \cdot x^2 + 4 \cdot x + 3) = x - 4$

$m.d.c.(f(x), h_2(x) - 2) = m.d.c(x^6 - 3 \cdot x^5 + 5 \cdot x^4 - 9 \cdot x^3 - 5 \cdot x^2 + 6 \cdot x + 7, x^3 + 2 \cdot x^2 + 4 \cdot x - 2) = x^2 - x + 7$

$m.d.c.(f(x), h_2(x) - 6) = m.d.c(x^6 - 3 \cdot x^5 + 5 \cdot x^4 - 9 \cdot x^3 - 5 \cdot x^2 + 6 \cdot x + 7, x^3 + 2 \cdot x^2 + 4 \cdot x - 6) = x^3 + 2 \cdot x^2 + 4 \cdot x - 6$

E assim obtemos a fatoração de $f(x)$ em $GF(23)$,

$f(x) = (x - 4) \cdot (x^2 - x + 7) \cdot (x^3 + 2 \cdot x^2 + 4 \cdot x - 6)$.

Exemplo 3.3 Seja $f(x) = x^5 - 9 \cdot x^4 + 3 \cdot x^3 + x^2 - 2 \cdot x + 8 \in GF(31)$. Para encontrarmos a fatoração deste polinômio iniciamos verificando se existem fatores repetidos, para isso devemos calcular o $m.d.c.(f(x), f'(x))$, ou seja, $m.d.c.(x^5 - 9 \cdot$

$x^4 + 3 \cdot x^3 + x^2 - 2 \cdot x + 8, 5 \cdot x^4 - 36 \cdot x^3 + 9 \cdot x^2 + 2 \cdot x - 2) = 1$. Portanto, $f(x)$ não tem fatores repetidos.

Calculamos x^{iq} mod f(x) para q = 31 e $0 \leq i \leq 4$

$x^{0 \cdot 31} = x^0 \equiv 1$

$x^{1 \cdot 31} = x^{31} \equiv 11 - 11 \cdot x - 11 \cdot x^2 + 12 \cdot x^3 + 11 \cdot x^4$

$x^{2 \cdot 31} = x^{62} \equiv -5 + 7 \cdot x - 14 \cdot x^2 - 10 \cdot x^3 - 4 \cdot x^4$

$x^{3 \cdot 3} = x^{93} \equiv -9 + 12 \cdot x + 7 \cdot x^2 + 13 \cdot x^3 - 11 \cdot x^4$

$x^{4 \cdot 31} = x^{124} \equiv 10 + x + 3 \cdot x^3 + 11 \cdot x^4$

Obtendo assim a matriz $B_{5\times5}$.

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 11 & -11 & -11 & 12 & 11 \\ -5 & 7 & -14 & -10 & -4 \\ -9 & 12 & 7 & 13 & -11 \\ 10 & 1 & 0 & 3 & 11 \end{bmatrix}_{5\times5}$$

e B - I é dada por,

$$B - I = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 11 & -12 & -11 & 12 & 11 \\ -5 & 7 & -15 & -10 & -4 \\ -9 & 12 & 7 & 12 & -11 \\ 10 & 1 & 0 & 3 & 10 \end{bmatrix}_{5\times5}$$

Escalonamos a matriz B - I a fim de obtermos o número de linhas não nulas, ou seja $r = 4$. Sabendo o valor de r, podemos encontrar o número de fatores irredutíveis mônicos distintos de f em $GF(31)$, $k = n - r = 5 - 4 = 1$.

Como o $k = 1$, isso indica que o espaço nulo de B - I tem dimensão 1, e portanto podemos dizer que o polinômio f é irredutível sobre $GF(31)$.

3.4 Método de Cantor-Zassenhaus

Em 1981 [22], Cantor e Zassenhaus introduziram um novo algoritmo probabilístico de fatoração, que pode ser aplicado para fatorar polinômios em qualquer corpo finito.

Para encontrar a fatoração de um polinômio $f(x)$ sobre um corpo finito usando o método de Cantor-Zassenhaus devemos seguir os seguintes passos:

Passo 1. Verificar se a $f(x)$ tem fatores repetidos, como já vimos isso deve ser feito através do cálculo do $m.d.c(f(x), f'(x))$.

Passo 2. Fatorar f no produto

$$f(x) = \prod_{i=0}^{m} h_i(x) \tag{3.3}$$

onde cada $h_i(x)$ contém somente fatores irredutíveis de grau i.

Passo 3. Devemos fatorar cada $h_i(x)$ em fatores irredutíveis, este processo é denominado fatoração de grau uniforme.

A fatoração (3.3) deve ser realizada usando o algoritmo de fatoração de grau distinto. Ao aplicarmos o mesmo procuramos decompor a $f(x)$ em $h_i(x)$ ou seja, $f(x) = h_1(x) \cdots h_i(x)$, sendo que cada $h_i(x)$ representa o produto de m fatores irredutíveis pertencentes a $GF(q)$ de grau i.

Como sabemos $h_i(x)$ é o produto de todos os polinômios mônicos de grau i sobre $GF(q)$. Pelo teorema (1.11) sabemos que o produto de todos os polinômios mônicos irredutíveis sobre $GF(q)$ de grau dividindo i é igual a $x^{q^i} - x$, então $h_i(x) = x^{q^i} - x$. Se calcularmos o $m.d.c.(f(x), x^{q^i} - x)$ obteremos somente os fatores de f, ou seja, $h_i(x)$.

Para encontrá-los começamos esta fatoração escolhendo $i = 1$ e calculando a equação $x^{q \cdot i}$ mod $f(x)$; o polinômio resultante será denominado $r_1(x)$.

Calculamos então o $m.d.c.(f(x), r_1(x) - x)$ e assim obteremos a $h_1(x)$.

Se $h_1(x) = f(x)$, o algoritmo da fatoração de grau distinto terminou, pois já descobrimos todo o conjunto de $h_i(x)$ que fatora a $f(x)$.

Caso contrário tomamos $i = 1 + i$ e encontramos a nova $f(x)$, que é obtida pela divisão da $f(x)$ por $h_1(x)$. Verificamos se esta $f(x)$ tem grau menor que $2i$; caso tenha o algoritmo está encerrado e a $f(x)$ passa a fazer parte do conjunto dos $h_i(x)$. Mas se $2i < grau f(x)$, calculamos um novo $r(x)$.

Como vimos anteriormente para encontrarmos o $r(x)$ devemos calcular $x^{q \cdot i}$ mod $f(x)$, mas dependendo do corpo em que se está trabalhando isso torna-se muito trabalhoso, por isso podemos usar outra alternativa para encontrarmos o $r(x)$. Suponha $r_{i-1}(x) = b_{n-1} \cdot x^{n-1} + \cdots + b_1 \cdot x + b_0$ um polinômio de $GF(q)[x]$, então, $(x)^q = (x^q)$. Por isso, podemos afirmar que $r_i(x) = (r_{i-1}(x))^q = b_{n-1} \cdot x^{q \cdot (n-1)} + \cdots + b_1 \cdot x^q + b_0$.

Se nós pré computarmos os valores $B_i(x) = x^{i \cdot q}$ mod $f(x)$, para $i = 0, \cdots, n-1$ e armazenarmos B_i como a i-ésima linha da matriz B de ordem $n \times n$, nós temos $r_i(x) = r_{i-1}(x) \cdot Q$, ou seja, devemos multiplicar o r(x) pela matriz B e o vetor resultante será o novo r(x).

E assim repetimos o algoritmo até obtermos o grau da $f(x) < 2i$ ou então $h_i(x) = f(x)$.

Após encontrarmos o conjuntos dos $h_i(x)$ que fatoram a $f(x)$, a próxima tarefa é encontrarmos os n fatores irredutíveis que compõem cada $h_i(x)$, para isso usamos o algoritmo de grau distinto.

Escolhemos randomicamente um polinômio $t(x)$ em $GF(q)[x]$ de grau $\leq 2i - 1$ e calculamos o novo $t(x)$ através do cálculo $(t(x))^{\frac{q^i - 1}{2}}$ mod $h_i(x)$. A

probabilidade que o polinômio $t(x)$ seja um separador é igual a 1/2, podemos ver a prova disso em [6].

Por fim calculamos a $g(x)$ através do cálculo $m.d.c(h_i(x), t(x) - 1)$. Ao obtermos a fatoração dos $h_i(x)$, encontramos a fatoração de f(x).

O algoritmo da fatoração de grau distinto pode ser descrito como segue abaixo.

Passo 1 Devemos encontrar a matriz B, como no método de Berlekamp.

Passo 2 Tomamos $i = 1$ e encontramos o valor de $r(x)$ através do cálculo $x^q \bmod f(x)$ (que é a segunda linha da matriz B).

Passo 3 Calculamos o $m.d.c(f(x), r(x) - x)$. O polinômio resultante será denominado de h_1.

Passo 4 - Se $h_1(x) = f(x)$, o algoritmo de fatoração de grau distinto terminou, pois já descobrimos todo o conjunto de $h_i(x)$ que fatoram o $f(x)$.

- Caso contrário, devemos dividir a $f(x)$ por $h_1(x)$ obtendo a nova $f(x)$ e $i = i + 1$.

Passo 5 - Se $2i > grau(f(x))$ então a $f(x)$ passa a fazer parte do conjunto dos $h_i(x)$ e o algoritmo está encerrado.

- Caso contrário, calculamos um novo $r(x)$ e retornamos ao passo 3 deste algoritmo.

O algoritmo da fatoração de grau uniforme segue os passos descritos abaixo.

Passo 1 Escolhemos randomicamente um polinômio $t(x)$ em $GF(q)[x]$ de grau $\leq 2i - 1$.

Passo 2 Calculamos o novo $t(x)$ através do cálculo $(t(x))^{\frac{q^i-1}{2}} \bmod h_i(x)$.

Passo 3 Calculamos $g(x)$ através do cálculo $m.d.c(h_i(x), t(x) - 1)$.

Exemplo 3.4 Seja $f(x) = 4 \cdot x^7 + 5 \cdot x^6 + x^5 + 4 \cdot x^4 + 3 \cdot x^3 + 4 \cdot x^2 - 4 \in GF(11)$. Para encontrarmos a fatoração deste polinômio sabemos que primeiramente devemos verificar se $f(x)$ tem fatores repetidos, para isso calculamos $m.d.c(f(x), f'(x)) = m.d.c(4 \cdot x^7 + 5 \cdot x^6 + x^5 + 4 \cdot x^4 + 3 \cdot x^3 + 4 \cdot x^2 - 4, 28 \cdot x^6 + 30 \cdot x^5 + 4 \cdot x^4 + 16 \cdot x^3 + 9 \cdot x^2 + 8 \cdot x) = 1$. Portanto a $f(x)$ não tem fatores repetidos.

Montamos a matriz $B_{7\times7}$, através do cálculo x^{iq} mod $f(x)$ sendo $0 \leq i \leq 6$.

$$B = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ -5 & -3 & -5 & 2 & 3 & 3 & -1 \\ -1 & -3 & -2 & 5 & 2 & -1 & -1 \\ 1 & -4 & 0 & 3 & 2 & -4 & -5 \\ -1 & -5 & 0 & -4 & 5 & 7 & 2 \\ -5 & 2 & 4 & -2 & -5 & -3 & 4 \\ 3 & 3 & 0 & 4 & 4 & 3 & 1 \end{bmatrix}_{7\times7}$$

Tomamos $i = 1$ e calculamos $r_1(x)$, através do cálculo x^{11} mod $f(x)$, já feito anteriormente para calcular a matriz B, então $r_1(x) = -5 \cdot x^6 - 3 \cdot x^5 - 5 \cdot x^4 + 2 \cdot x^3 + 3 \cdot x^2 + 3 \cdot x - 1$.

Calculamos $h_1(x)$ através do cálculo $m.d.c(f(x), r_1(x) - x) = m.d.c(4 \cdot x^7 + 5 \cdot x^6 + x^5 + 4 \cdot x^4 + 3 \cdot x^3 + 4 \cdot x^2 - 4, -5 \cdot x^6 - 3 \cdot x^5 - 5 \cdot x^4 + 2 \cdot x^3 + 3 \cdot x^2 + 2 \cdot x - 1) = x^3 + x^2 + 3 \cdot x + 5$.

Como $h_1(x)$ não é igual a $f(x)$, calculamos a nova $f(x)$, que é o quociente da divisão de $f(x)$ por $h_1(x)$. Portanto $(4 \cdot x^7 + 5 \cdot x^6 + x^5 + 4 \cdot x^4 + 3 \cdot x^3 + 4 \cdot x^2 - 4) : (x^3 + x^2 + 3 \cdot x + 5) = 4 \cdot x^4 + x^3 - x^2 + 4 \cdot x - 3$.

O próximo i é 2, verificamos se $2i > grau(f(x))$, como não é pois, 4 não é maior do que 4 continuamos a fatoração encontrando um novo $r(x)$, ou seja, $r_2(x) = r_1(x) \cdot B = x$.

O $h_2(x)$ é obtido através do cálculo do $m.d.c.(f(x), r_2(x) - x) = m.d.c(4 \cdot x^4 + x^3 - x^2 + 4 \cdot x - 3, x - x) = 4 \cdot x^4 + x^3 - x^2 + 4 \cdot x - 3$.

Portanto $h_2(x) = 4 \cdot x^4 + x^3 - x^2 + 4 \cdot x - 3$, como é igual a $f(x)$ o algoritmo da fatoração de grau distinto terminou. Nossa tarefa agora é fatorar os $h_i(x)$ encontrados.

Sabemos de antemão que a $f(x)$ tem três fatores irredutíveis de grau 1 e dois fatores irredutíveis de grau 2.

Começaremos encontrando a fatoração de $h_1(x)$. Para isso escolhemos randomicamente o polinômio $t(x) = x + 1 \in GF(11)$, e calculamos o novo $t(x)$ através do cálculo $(t(x))^{\frac{11^1-1}{2}} = (x+1)^5$.

Fazendo $(x+1)^5$ mod $h_1(x)$ obtemos $x^2 + 9 \cdot x + 8$.

$g(x) = m.d.c(x^3 + x^2 + 3 \cdot x + 5,\ x^2 + 9 \cdot x + 8 - 1) = x + 3$.

Como sabemos que a fatoração de $f(x)$ tem três fatores de grau 1, vamos repetir o processo, escolhendo randomicamente outro polinômio, $t(x)$, agora $t(x) = x + 3 \in GF(11)$.

Calculamos o novo $t(x)$ através do cálculo $(t(x))^{\frac{11^1-1}{2}} = (x+3)^5$.

Fazendo $(x+3)^5$ mod $h_1(x)$ obtemos $7 \cdot x^2 + 6 \cdot x + 10$.

$g(x) = m.d.c(x^3 + x^2 + 3 \cdot x + 5,\ 7 \cdot x^2 + 6 \cdot x + 10 - 1) = x + 5$.

Como já encontramos dois fatores irredutíveis de grau 1, para encontramos o terceiro basta fazermos $h_1(x)$ dividido pelo produto dos dois fatores já encontrados mod 11. Encontraremos o outro fator que é $x + 4$.

O passo agora é fatorarmos o $h_2(x)$, para isso escolhemos randomicamente o polinômio $t(x) = x + 1 \in GF(11)$ e calculamos o novo $t(x)$ através do cálculo $(t(x))^{\frac{11^2-1}{2}} = (x+1)^{60}$.

Fazendo $(x+1)^{60}$ mod $h_2(x)$ obtemos $3 \cdot x^3 - 3 \cdot x^2 - x + 1$.

$g(x) = m.d.c(4 \cdot x^4 + x^3 - x^2 + 4 \cdot x - 3,\ 3 \cdot x^3 - 3 \cdot x^2 - x) = x^2 - x - 4$.

Como existem dois fatores irredutíveis de grau 2 e já encontramos um, fazemos $h_2(x)$ dividido por $g(x)$ e assim obtemos o outro fator que é $4 \cdot x^2 + 5 \cdot x + 20$.

Portanto a fatoração de $f(x)$ é

f(x) $= (x+1) \cdot (x+3) \cdot (x+4) \cdot (4 \cdot x^2 + 5 \cdot x + 20) \cdot (x^2 - x - 4)$.

3.5 Método de Lidl- Niederreiter

Este método pode ser empregado para fatorar polinômios em corpos finitos pequenos e baseia-se na construção de famílias de polinômios, entre os quais pelo menos um dos polinômios f-redutor pode ser encontrado.

Definição 3.2 Um polinômio $h(x)$ é chamado f-redutor quando ao calcularmos $m.d.c(f(x), h(x) - c)$ verificamos que o $h(x)$ produz uma fatoração não trivial de f.

O primeiro passo para fatorarmos a $f(x)$ deve ser verificar se a mesma possui fatores repetidos. Se a $f(x)$ não tiver fatores repetidos começamos a fatoração. Caso tenha fatores repetidos devemos dividi-la pelo resultado do $m.d.c(f(x), f'(x))$. O quociente obtido será denominado a nova $f(x)$.

Assumiremos a partir daqui que a $f(x)$ não tenha fatores repetidos, ou seja, $f(x) = f_1(x) \cdots f_k(x)$ onde grau $(f_j) = n_j$ para $1 \leq j \leq k$. Iniciando em $N = 1, 2, \cdots$ calculamos seqüencialmente x^{2^N}, até encontrarmos $x^{2^N} \equiv x$ mod $f(x)$. Podemos verificar que o valor encontrado de N é o $m.m.c(n_1, \cdots, n_k)$.

Ao aplicarmos este método para fatorar a $f(x)$ sabemos que devemos encontrar um polinômio $T(x) = x + x^q + x^{q^2} + \cdots + x^{q^{N-1}} \in GF(q)[x]$ definido por $T_i(x) = T(x^i)$ para $i = 0, 1, \cdots$ que seja f-redutor. O teorema abaixo nos garante a existência deste polinômio T_i se f é redutível.

Teorema 3.4 *Se f é redutível em GF(q)[x], então pelo menos um dos polinômios* T_i, $0 \leq i \leq n-1$, *é f-redutor.*

A prova deste teorema pode ser encontrada em [13]. Encontrado o polinômio f-redutor, calculamos o $m.d.c(f(x), T_i(x) - c)$, sendo c os elementos pertencentes a $GF(q)$, a fim de definirmos os fatores irredutíveis de $f(x)$.

Se inicialmente a $f(x)$ não tinha fatores repetidos a fatoração está encerrada. Caso a $f(x)$ tinha fatores repetidos devemos ainda decompor a $g(x)$ (resultado obtido ao calcular o $m.d.c(f(x), f'(x))$) de forma que $g(x) = (a(x))^n$, obtendo assim a fatoração completa de $f(x)$.

Exemplo 3.5 Seja $f(x) = x^{17}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^5+x^4+x+1$ sobre GF(2). Para encontrarmos a fatoração deste polinômio verificamos se o mesmo tem fatores repetidos $m.d.c(x^{17}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^5+x^4+x+1,$ $17\cdot x^{16}+14\cdot x^{13}+13\cdot x^{12}+12\cdot x^{11}+11\cdot x^{10}+10\cdot x^9+9\cdot x^8+8\cdot x^7+7\cdot x^6+5\cdot x^4+4\cdot x^3+1)$ $= x^{10} + x^8 + 1$.

Como o m.d.c. não deu 1, devemos dividir $f(x)$ por $x^{10}+x^8+1$ obtendo como quociente, $f_0(x) = x^7 + x^5 + x^4 + x + 1$ e repetir o $m.d.c(f_0(x), f_0'(x)) = m.d.c(x^7 + x^5 + x^4 + x + 1, 7 \cdot x^6 + 5 \cdot x^4 + 4 \cdot x^3 + 1) = 1$. Como o resultado obtido foi 1 então, $f_0(x)$ não tem mais fatores repetidos.

Nossa tarefa é fatorar a f_0 encontrada, ou seja, $x^7+x^5+x^4+x+1$. Para isso calculamos a série x^{2^N} onde $N = 1, 2, \cdots$ até que $x^{2^N} \equiv x \bmod f_0(x)$. Temos, $x^{2^1} = x^2 \equiv x^2$; $x^{2^2} = x^4 \equiv x^4$; $x^{2^3} = x^8 \equiv x^6 + x^5 + x^2 + x$; $x^{2^4} = x^{16} \equiv x^3 + x + 1$; $x^{2^5} = x^{32} \equiv x^6 + x^2 + 1$; $x^{2^6} = x^{64} \equiv x^6 + x + 1$; $x^{2^7} = x^{128} \equiv x^6 + x^4 + x^2 + x + 1$; $x^{2^8} = x^{256} \equiv x^5 + 1$; $x^{2^9} = x^{512} \equiv x^6 + x^3 + x^2$; $x^{2^{10}} = x^{1024} \equiv x$, portanto o $N = 10$.

Devemos calcular neste momento o polinômio T_1, pois pelo teorema (3.4) pelo menos um dos T_i é f-redutor

$$T_1 = \sum_{j=0}^{N-1} x^{2^j} = \sum_{j=0}^{9} x^{2^j} = x + x^2 + x^4 + x^8 + x^{16} + x^{32} + x^{64} + x^{128} + x^{256} + x^{512}$$

Para resolver este somatório devemos adicionar cada um destes fatores mod $f_0(x)$ que foi encontrado anteriormente e ainda fazer mod 2 e assim obteremos: $x^6 + x^2 + x + 1 \bmod f_0(x)$.

Calculamos agora o $m.d.c.(f_0(x), T_1(x) - 0)$, ou seja, $m.d.c(x^7 + x^5 + x^4 + x + 1, x^6 + x^2 + x + 1) = x^5 + x^4 + x^3 + x^2 + 1$ e $m.d.c.(f_0(x), T_1(x) - 1) = m.d.c(x^7 + x^5 + x^4 + x + 1, x^6 + x^2 + x) = x^2 + x + 1$

Dessa forma obtivemos a fatoração de $f_0(x)$, que é, $f_0(x) = (x^5 + x^4 + x^3 + x^2 + 1) \cdot (x^2 + x + 1)$

Mas ainda não temos a fatoração completa de $f(x)$, pois o polinômio $x^{10} + x^8 + 1$ tinha fatores repetidos, como vimos no início deste exemplo, por isso devemos decompô-lo, ou seja, $x^{10} + x^8 + 1 = (x^5 + x^4 + 1)^2$. Para isso verificamos se $x^5 + x^4 + 1$ é divisível por um dos fatores de $f_0(x)$. Então, dividindo $(x^5 + x^4 + 1)$ por $(x^2 + x + 1)$ obtemos $(x^3 + x + 1)$. Desta forma encontramos a fatoração completa de f(x).

$$\text{f(x)} = (x^5 + x^4 + x^3 + x^2 + 1) \cdot (x^2 + x + 1)^3 \cdot (x^3 + x + 1)^2.$$

4 RAíZES DE POLINÔMIOS EM CORPOS FINITOS

Neste capítulo estudaremos algoritmos para encontrar as raízes de polinômios sobre corpos finitos, veremos que os algoritmos têm significativa diferença dependendo do tamanho do corpo em que o polinômio pertence.

4.1 Introdução

Encontrar as raízes de um polinômio em um corpo finito é um assunto da álgebra de grande interesse pois é uma operação necessária em muitas aplicações práticas da matemática ou áreas afins.

Quando procuramos as raízes de um polinômio com coeficientes em um corpo finito $GF(p^n)$ na verdade estamos procurando estas raízes no corpo $GF(p^n)$. Para conseguirmos encontrá-las, alguns resultados são de grande valia, por isso os citaremos neste momento.

Definição 4.1 Se $f(x) \in F[x]$, então um elemento a, que esteja em alguma extensão do corpo F, é denominado uma raiz de $f(x)$ se $f(a) = 0$.

Pelo teorema 1.8 sabemos que se $f(x)$ é um polinômio em $F[x]$ de grau $n \geq 1$, e é irredutível sobre F, então existe uma extensão E de F na qual $f(x)$ tem uma raíz.

Um polinômio de grau n sobre um corpo pode ter no máximo n raízes em qualquer extensão deste corpo. E existe uma extensão de grau no máximo $n!$, na qual $f(x)$ possui n raízes. E ainda, se a é uma raiz de $f(x)$ pertencente ao corpo F então $(x - a) \mid f(x)$, em $F[x]$.

É importante ressaltarmos que neste trabalho só temos interesse em procurar determinar as raízes dos polinômios pertencentes ao corpo finito em que estamos trabalhando e não no corpo extensão do mesmo.

Definição 4.2 O elemento a pertencente ao corpo é uma raiz de $f(x) \in F[x]$ de multiplicidade m se $(x-a)^m | f(x)$, enquanto $(x-a)^{m+1}$ não divide $f(x)$.

Teorema 4.1 *O polinômio $f(x) \in F[x]$ tem uma raiz múltipla se, e somente se, $f(x)$ e $f'(x)$ tem um fator comum não trivial.*

Demonstração Suponhamos que $f(x)$ tem raiz com multiplicidade α, então,

$$f(x) = (x-\alpha)^m \cdot q(x) \text{ onde } m > 1$$

$$\text{e } f'(x) = m \cdot (x-\alpha)^{m-1} \cdot q(x) + (x-\alpha)^m \cdot q'(x)$$

Isso mostra que $f(x)$ e $f'(x)$ possuem um fator comum, ou seja $(x-\alpha)$.

Reciprocamente, suponhamos que $f(x)$ não possui raiz múltipla, então:

$$f(x) = (x-\alpha_1) \cdot (x-\alpha_2) \ldots (x-\alpha_n)$$

onde os α_i são todos distintos.

$$f'(x) = \sum_{i=1}^{n} (x-\alpha_1) \ldots \widehat{(x-\alpha_i)} \ldots (x-\alpha_n)$$

onde $\widehat{(x-\alpha_i)}$ indica o termo omitido. Afirmamos que nenhuma raiz de $f(x)$ é uma raiz de $f'(x)$; de fato,

$$f'(\alpha_i) = \prod_{j \neq i} (\alpha_j - \alpha_i) \neq 0, \text{ pois as raízes são todas distintas .}$$

Contudo, se $f(x)$ e $f'(x)$ tem um fator comum não trivial, elas têm uma raiz comum, a saber, qualquer raiz deste fator comum.

Portanto, $f(x)$ e $f'(x)$ não tem nenhum fator comum não trivial.□

Exemplo 4.1 Seja $f(x) = x^2 + 2 \cdot x + 1$. Portanto, $f'(x) = 2 \cdot x + 2$. Verificamos que $f(x) = x^2 + 2 \cdot x + 1$ tem como raízes -1 e -1. E que $f'(x) = 2 \cdot x + 2$ também tem como raiz -1. O que nos permite afirmar que $f'(x)$ e $f(x)$ tem fator comum, que é o $x + 1$, observe, $f(x) = (x + 1) \cdot (x + 1)$ e $f'(x) = 2 \cdot (x + 1)$.

O teorema diz que se tem fator comum então $f(x)$ tem raízes múltiplas, o que se verifica no exemplo.

Corolário 4.1 Se $f(x) \in F[x]$ é irredutível, então:

1) Se a característica de F é zero, então $f(x)$ não tem raízes múltiplas.

2) Se a característica de F é $p \neq 0$, então $f(x)$ tem uma raíz múltipla se e somente se, $f(x)$ é da forma $f(x) = g(x^p)$.

Demonstração Como $f(x)$ é irredutível, seus únicos fatores em $F[x]$ são 1 e $f(x)$. Se $f(x)$ tem um raiz múltipla, então, pelo teorema 4.1, $f(x)$ e $f'(x)$ possuem um fator comum não trivial, donde $f(x) \mid f'(x)$. Contudo, como o grau de $f'(x)$ é menor que o de $f(x)$, a única maneira pela qual isto pode ocorrer é com $f'(x)$ sendo 0. Em característica 0 isto implica que $f(x)$ é uma constante, que não tem raízes; em característica $p \neq 0$, isto implica $f(x) = g(x^p)$.□

Exemplo 4.2 Seja $f(x) = x^2 + 1 \in \mathbb{Q}$. Verificamos que a característica de $\mathbb{Q}$ é zero. Calculando a derivada de $f(x)$ obtemos $f'(x) = 2 \cdot x$. Portanto, $f(x)$ e $f'(x)$ não tem nenhum fator comum, o que implica pelo teorema (3.1) que a $f(x)$ não tem raízes múltiplas.

Exemplo 4.3 Seja $f(x) = t^2 - x \in F$, onde F_0 é um corpo de característica 2 e seja $F = F_0(x)$ o corpo das funções racionais em x sobre F_0. Afirmamos que o polinômio $t^2 - x$ em $F[t]$ é irredutível sobre F, pois, não existe nenhuma função racional em $F_0(x)$ cujo quadrado é x. Podemos afirmar também que $t^2 - x$ tem uma raiz múltipla, pois sua derivada em função de t é $f'(x) = 2 \cdot t$ e como o corpo tem característica 2 temos que $f'(x) = 0$ e quando a $f'(x) = 0$ podemos afirmar que $f(x)$ é uma potência de p e portanto tem raízes múltiplas.

Aplicando o resultado do corolário 4.1 ao polinômio $f(x) = x^{p^n} - x$, podemos verificar que se a característica do corpo é p, então $f'(x) = -1$ e portanto, temos,

Corolário 4.2 Se F é um corpo de característica $p \neq 0$, então o polinômio $x^{p^n} - x \in F[x]$ para $n \geq 1$, tem raízes distintas.

Lembremo-nos, do teorema 1.11 do capítulo 1, o qual diz que:

"Em um corpo finito $GF(p)$, $x^{q^k} - x$ é o produto de todos os polinômios mônicos irredutíveis de grau que divide k".

Porém, quando $k = 1$ temos um caso especial, $x^q - x$. Sendo que este representa o produto de todos os polinômios mônicos lineares (ou seja, as raízes) em $GF(q)[x]$.

A idéia acima é necessária quando queremos separar a parte de $f(x)$ que contém as raízes do mesmo no corpo finito $GF(q)[x]$. Para fazermos isso realizamos o cálculo do $m.d.c.(f(x), x^q - x)$. Ou seja, as raízes de $f(x)$ sobre o corpo finito são exatamente as raízes do polinômio resultante do $m.d.c.(f(x), x^q - x)$.

Exemplo 4.4 Seja $f(x) = x^4 + x + 1 \in GF(2)$. Para separar a parte de $f(x)$ que contém as raízes, calculamos $m.d.c.(x^4 + x + 1, x^2 - x) = m.d.c.(x^2 - x, 1) = m.d.c.(1, 0) = 1$

Isso mostra que a fatoração é trivial e portanto, 0 e 1 não são raízes de $f(x)$, somente de $x^2 - x$. Assim, $f(x)$ não tem raízes em $GF(2)$, somente num corpo extensão de $GF(2)$.

Exemplo 4.5 Seja $f(x) = x^5 - 4 \cdot x^4 - 4 \cdot x^3 + 4 \cdot x \in GF(5)$, como $m.d.c.(x^5 - 4 \cdot x^4 - 4 \cdot x^3 + 4 \cdot x, x^5 - x) = m.d.c.(x^5 - x, -4 \cdot x^4 - 4 \cdot x^3) = m.d.c.(-4 \cdot x^4 - 4 \cdot x^3, x^3 - x) = m.d.c.(x^3 - x, x^2 + x) = m.d.c.(x^2 + x, 0) = x^2 + x$, então, $x^2 + x = x \cdot (x + 1)$ e as raízes de $f(x)$ em $GF(5)$ são 0 e - 1, sendo que -1 mod 5 é igual a 4. As outras três raízes não pertencem a $GF(5)$, ou seja, estão em um corpo extensão.

No restante deste capítulo nos deteremos em estudar os diferentes métodos que podem ser utilizados para extrairmos as raízes de um polinômio num corpo finito. A escolha do método mais adequado depende de algumas características do corpo onde o polinômio está inserido, como podemos observar abaixo:

1) Um corpo primo $GF(p)$ considerando p pequeno

2) Um corpo primo $GF(p)$ considerando p grande

3) Um corpo finito grande $GF(q)$ com característica p pequena

4) Um corpo finito grande $GF(q)$ com característica p grande.

Podemos encontrar a descrição de tais métodos em diverso livros, dentre eles podemos citar [13], [15] e [4].

4.2 Um corpo primo $GF(p)$ considerando p pequeno

Consideramos o primeiro caso. Seja:

$$f(x) = \prod_{i=1}^{n}(x - \alpha_i)$$

onde $\alpha_1, \ldots, \alpha_n$ são elementos de $GF(p)$.

Como p é pequeno então é possível determinar as raízes de $f(x)$ por tentativa e erro, ou seja, pelo simples cálculo do valor numérico $f(0), f(1), \cdots, f(p-1)$.

Exemplo 4.6 Seja $f(x) = x^5 - 4 \cdot x^3 - 4 \in GF(5)$ para obtermos as raízes de $f(x)$ pertencentes ao corpo $GF(5)$, calculamos o valor numérico da mesma.

Sabemos que o corpo $GF(5) = \{0,\ 1,\ 2,\ 3,\ 4\}$. Se substituirmos x por cada elemento de $GF(5)$ encontraremos, $f(0) = 1; f(1) = 2; f(2) = 9 \bmod 5 = 4; f(3) = 28 \bmod 5 = 3$ e $f(4) = 65 \bmod 5 = 0$. Portanto, o 4 é uma das cinco raízes de $f(x)$. As outras raízes estão num corpo extensão de $GF(5)$.

Exemplo 4.7 Seja $f(x) = x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+2\cdot x^9+2\cdot x^8+2\cdot x^7+2\cdot x^6+2\cdot x^5+2\cdot x^4 \in GF(3)$. Para encontrarmos as raízes de $f(x)$ já que o polinômio deste exemplo é de maior grau que o do exemplo anterior, facilitaremos o nosso trabalho se iniciarmos calculando o $m.d.c(f(x), x^p - x)$, pois sabemos que o polinômio resultante deste $m.d.c$ será a parte de $f(x)$ que contém as raízes; precisando assim substituir os elementos de $GF(3)$ num polinômio de menor grau.

Calculando o $m.d.c(x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + 2 \cdot x^9 + 2 \cdot x^8 + 2 \cdot x^7 + 2 \cdot x^6 + 2 \cdot x^5 + 2 \cdot x^4, x^3 - x)$ obteremos $x^3 + 2 \cdot x$. Devemos agora verificar quais dos elementos de $GF(3)$ são raízes de $x^3 + 2 \cdot x$ e conseqüentemente de $f(x)$. Então, f(0) = 0, f(1) = 1 + 2 = 3 mod 3 = 0 e f(2) = 8 + 4 = 12 mod 3 = 0. Portanto, 0, 1 e 2 são raízes de $f(x)$.

4.3 Um corpo primo $GF(p)$ considerando p grande

No segundo caso temos um corpo primo $GF(p)$ considerando p grande. Consideremos p ímpar e $f(x)$ como segue abaixo:

$$f(x) = \prod_{i=1}^{d}(x - \alpha_i)$$

com $\alpha_i \in GF(p)$ e sendo distintos.

Notemos que o p só pode ser ímpar, pois o único número primo e par é o dois e o dois é pequeno, como estamos considerando p grande, p é ímpar.

Primeiramente devemos separar a parte de $f(x)$ que contém as raízes, fazemos isso através do cálculo do $m.d.c.(f(x), x^p - x)$. Chamamos o polinômio resultante de $g(x)$.

Num próximo passo separamos as raízes em duas classes, ou seja, nas raízes quadradas ou não, no grupo multiplicativo $GF(p)^*$. Isso é feito através do cálculo do $m.d.c.$ como descrevemos abaixo:

$$g(x) = m.d.c.(g(x), x^{\frac{p-1}{2}} - 1)m.d.c.(g(x), x^{\frac{p-1}{2}} + 1)$$

Se o resultado deste cálculo for diferente de $\pm$ 1 mod $g(x)$ então a fatoração é chamada não trivial e a partir deste resultado encontramos uma (ou mais) raiz(es) de $g(x)$.

Se o resultado for $\equiv \pm 1$ mod $g(x)$ a fatoração é dita trivial, isso implica dizer que o valor escolhido não é raiz de $g(x)$. Devemos então substituir $g(x)$ por $g(x-a)$ sendo $a \in GF(p)$ e calcular novamente o $m.d.c.$ citado acima, tendo como objetivo encontrar uma fatoração não trivial, da qual podemos encontrar as raízes.

Este método é um algoritmo probabilístico, sendo que o mesmo depende da seleção randômica para encontrar as raízes.

O algoritmo usado para encontrar as raízes de um corpo primo $GF(p)$ considerando p grande, será descrito abaixo.

Passo 1 Calcular o $m.d.c.(f(x), x^p - x)$, encontrando o polinômio $g(x)$.

Passo 2 Separar $g(x)$ em duas classes, para isso devemos calcular $m.d.c.(f(x), x^{\frac{p-1}{2}} - 1)$ e o $m.d.c.(f(x), x^{\frac{p-1}{2}} + 1)$.

Passo 3 Se o resultado do $m.d.c.$ for 1 ou o próprio $g(x)$, devemos escolher outro valor de a, calcular $g(x-a)$, repetir para $g(x-a)$ o passo 2, ou seja, calcular o $m.d.c.$, obtendo o $g(x)$ decomposto em dois polinômios, após devemos retirar o a colocado.

Passo 4 Até que o $m.d.c.$ não resultar em um polinômio de grau 1 devemos seguir os seguintes passos: escolher um novo valor para a, trocar a $g(x)$ por $g(x-a)$, calcular o $m.d.c.$ como no passo 2 e retirar o a colocado.

Exemplo 4.8 Seja $f(x) = x^6 - 7 \cdot x^5 + 3 \cdot x^4 - 7 \cdot x^3 + 4 \cdot x^2 - x - 2 \in GF(17)$. Para encontrarmos as raízes de $f(x)$ primeiramente encontramos a parte de $f(x)$ que contém as raízes(a qual denominaremos de $g(x)$), para isso calculamos o $m.d.c.$ como abaixo:

$$g(x) = m.d.c.(x^6 - 7 \cdot x^5 + 3 \cdot x^4 - 7 \cdot x^3 + 4 \cdot x^2 - x - 2, x^{17} - x)$$

o qual resultará num $g(x) = x^4 + 6 \cdot x^3 + 12 \cdot x^2 + 7 \cdot x + 15$.

Após separamos $g(x)$ em duas classes(raízes quadradas ou não), através do cálculo $g(x) = m.d.c.(g(x), x^{\frac{p-1}{2}} - 1) \cdot m.d.c.(g(x), x^{\frac{p-1}{2}} + 1)$. Onde podemos observar que $a = 0$ pois $g(x) = g(x - 0)$.

Primeiramente devemos fazer $x^{\frac{p-1}{2}} = x^8 \bmod g(x)$. Obteremos como resultado 1. Isso quer dizer que podemos escrever $x^8 = g(x) \cdot q(x) \pm 1$, implicando que $x^8 \mp 1 = g(x) \cdot q(x)$, o que quer dizer que não conseguimos separar o $g(x)$ e portanto podemos concluir que a fatoração é trivial, ou seja, $a = 0$ não é raiz de $g(x)$.

Escolhemos um outro valor para a, $a = 1$. Se $g(x) = x^4 + 6 \cdot x^3 + 12 \cdot x^2 + 7 \cdot x + 15$, então, $g(x-1) = (x-1)^4 + 6 \cdot (x-1)^3 + 12 \cdot (x-1)^2 + 7 \cdot (x-1) + 15 = x^4 + 2 \cdot x^3 + 14 \cdot x + 15$.

Fazemos $x^8 \bmod g(x-1)$ e obtemos que, $x^8 \equiv 13 \cdot x^3 + 10 \cdot x^2 + 8 \cdot x + 12 \bmod g(x-1)$. Repetimos para $g(x-1)$ o passo (2).

$m.d.c.(g(x-1), x^8 + 1) = m.d.c.(x^4 + 2 \cdot x^3 + 14 \cdot x + 15, 13 \cdot x^3 + 10 \cdot x^2 + 8 \cdot x + 13) = x^2 + 10 \cdot x + 4$

$m.d.c.(g(x-1), x^8 - 1) = m.d.c.(x^4 + 2 \cdot x^3 + 14 \cdot x + 15, 13 \cdot x^3 + 10 \cdot x^2 + 8 \cdot x + 11) = x^2 + 9 \cdot x + 8$

$$g(x-1) = (x^2 + 10 \cdot x + 4) \cdot (x^2 + 9 \cdot x + 8)$$

Como queremos $g(x)$, retiramos aquele 1 que foi colocado:

$(x^2 + 10 \cdot x + 4)$ transformado em $((x+1)^2 + 10 \cdot (x+1) + 4) = x^2 + 12 \cdot x + 15$

$(x^2 + 9 \cdot x + 8)$ transformado em $((x+1)^2 + 9 \cdot (x+1) + 8) = x^2 + 11 \cdot x + 1$

$$g(x) = (x^2 + 12 \cdot x + 15) \cdot (x^2 + 11 \cdot x + 1)$$

Como ainda não temos polinômios de grau 1, repetimos o processo, escolhendo um novo valor para a. Façamos agora $a = 2$, e vamos procurar decompor

em fatores lineares o primeiro fator de $g(x)$, ou seja, $h_1(x) = x^2 + 12 \cdot x + 15$. Calculamos $h_1(x-2) = ((x-2)^2 + 12 \cdot (x-2) + 15) = x^2 + 8 \cdot x + 12$. Repetimos com $h_1(x-2)$ o passo (2), obtendo $x^8 \equiv 9 \cdot x + 2 \bmod h_1(x-2)$ e calculamos o $m.d.c$,

$$m.d.c.(h_1(x-2), x^8 + 1) = m.d.c.(x^2 + 8 \cdot x - 5, 9x + 3) = x + 6$$

$$m.d.c.(h_1(x-2), x^8 - 1) = m.d.c.(x^2 + 8 \cdot x - 5, 9x + 1) = x + 2$$

Novamente como queremos encontrar $h_1(x)$ e não $h_1(x-2)$, retiramos o 2 que foi colocado, obtendo $x+6 = (x+2)+6 = x+8$ e $x+2 = (x+2)+2 = x+4$. Assim, encontramos duas das raízes.

Procedemos da mesma forma para o outro fator de $g(x)$, ou seja, $h_2(x) = x^2+11 \cdot x+1$. Façamos $a = 2$. Então $h_2(x-2) = ((x-2)^2+11 \cdot (x-2)+1) = x^2+7 \cdot x$

Como podemos decompor $h_2(x-2)$ em um polinômio do primeiro grau, ou seja, $x \cdot (x+7)$, não precisamos mais calcular o $m.d.c.$, pois já é possível determinarmos as raízes.

Novamente como queremos encontrar $h_2(x)$ e não $h_2(x-2)$, retiramos o 2 que foi colocado, ou seja, $x + 7 = (x + 2) + 7 = x + 9$ e $x = x + 2$. Encontrando assim mais duas das raízes.

Portanto, $g(x) = (x + 8) \cdot (x + 4) \cdot (x + 2) \cdot (x + 9)$. Como todos os termos são do primeiro grau, então, as raízes são: -8,-4, -2, -9.

Observe que $f(x)$ é de grau seis, isso indica que devemos ter seis raízes, como só encontramos quatro, isso implica em dizer que no corpo $GF(17)$ só temos quatro das seis raízes, as outras duas estão num corpo extensão de $GF(17)$.

Exemplo 4.9 Seja $f(x) = x^5 + 6 \cdot x^4 + x^3 + x^2 + 6$ sendo $f(x) \in GF(11)$. Para encontrarmos as raízes iniciamos determinando o polinômio $g(x)$ (ou seja, a parte de $f(x)$ que contém as raízes), para isso calculamos o $m.d.c.(x^5+6 \cdot x^4+x^3+x^2+6, x^{11}-x)$ e obtemos, $g(x) = x^3 + 6 \cdot x^2 + 6$

Após separamos $g(x)$ em duas classes, através do cálculo abaixo:

$$g(x) = m.d.c.(f(x), x^{\frac{p-1}{2}} - 1)m.d.c.(f(x), x^{\frac{p-1}{2}} + 1)$$

Primeiramente fazemos x^5 mod $g(x)$, obtendo $9 \cdot x^2 + 3 \cdot x + 4$ e após calculamos o $m.d.c.$.

$$m.d.c.(x^3 + 6 \cdot x^2 + 6, 9 \cdot x^2 + 3 \cdot x + 3) = x + 2$$

$$m.d.c.(x^3 + 6 \cdot x^2 + 6, 9 \cdot x^2 + 3 \cdot x + 5) = x^2 + 4 \cdot x + 3$$

Podemos observar que um dos $m.d.c.$ já resultou em um polinômio do primeiro grau, portanto já encontrou-se uma das raízes, que é -2 fazendo mod 11 obtemos 9.

O próximo passo deve ser decompor o fator de $g(x)$ que ainda não é linear, ou seja, $h_1(x) = x^2 + 4 \cdot x + 3$. Para isso escolhemos um novo valor para a. Fazemos $a = 1$, obtendo, $h_1(x-1) = (x-1)^2 + 4 \cdot (x-1) + 3 = x^2 + 2 \cdot x = x \cdot (x+2)$. Como podemos decompor, $x^2 + 2 \cdot x$, em polinômios do primeiro grau, ou seja, $x \cdot (x + 2)$ não precisamos mais calcular o $m.d.c.$, pois já é possível determinarmos as raízes. Primeiro colocamos o 1, a fim de encontrarmos o $h_1(x)$, então obtemos, $x = x + 1$ e $x + 2 = (x + 1) + 2 = x + 3$. Calculando -1 e -3 mod 11 encontramos 10 e 8 respectivamente.

Portanto as raízes de $g(x)$ são 8, 9 e 10. E como foi ressaltado no exemplo anterior, as outras duas raízes de $f(x)$ estão no corpo extensão de $GF(11)$.

4.4 Um corpo finito grande $GF(q)$com característica p pequena

No terceiro caso temos um corpo finito grande $GF(q)$ com característica p pequena. Como anteriormente, é suficiente considerarmos o caso onde

$$f(x) = \prod_{i=1}^{m}(x - \alpha_i)$$

com distintos $\alpha_1, \alpha_2, \ldots, \alpha_n \in GF(q)$, sendo $q = p^n$.

Neste método vamos representar elementos de $GF(p^n)$, especificando β como uma raiz em $GF(p^n)$ de algum polinômio de grau m que será irredutível sobre $GF(p)$.

Definição 4.3 Para $\alpha \in E = GF(p^n)$ e $F = GF(p)$ a função traço $Tr_{E/F}(\alpha)$ de α sobre F é definida por

$$Tr_{E/F}(\alpha) = \alpha + \alpha^p + \ldots + \alpha^{p^{n-1}}.$$

Em outras palavras, a função traço de α, sobre F é a soma dos conjugados de α com respeito a F.

Encontrado um polinômio de grau n irredutível sobre $GF(p)$ e representados os elementos de $GF(p^n)$, o terceiro passo é definir o polinômio $S(x) = \sum_{i=0}^{n-1} x^{p^i}$ $= Tr_{GF(q)}(x)$.

A equação $Tr(\alpha) = s$ tem p^{n-1} soluções α, sendo $\alpha \in GF(q)$, para cada $s \in GF(p)$. Em função disto, e tendo em mente o corolário 4.2, podemos escrever a seguinte identidade,

$$x^{p^n} - x = \prod_{s \in GF(p)} (Tr(x) - s)$$

Como, $x^{p^n} - x$, pelo teorema 1.11, é o produto de todos os polinômios mônicos irredutíveis então $x^{p^n} - x \equiv 0 \bmod f(x)$, isso implica em afirmar que

$$\prod_{s \in GF(p)} (Tr(x) - s) \equiv 0 \bmod f(x)$$

Conseqüentemente, se $f(x)$ é um polinômio não linear, temos a fatoração,

$$f(x) = \prod_{s \in GF(p)} m.d.c.(f(x), Tr(x) - s).$$

Se a função traço for um escalar, outro polinômio auxiliar deve ser encontrado. Como β é a raiz de um polinômio irredutível de grau m sobre $GF(p)$ então $\beta^0, \beta, \beta^2, \ldots, \beta^{n-1}$, formam uma base para $GF(p^n)$ sobre $GF(p)$. Para $j = 0, 1, \ldots, n-1$ nós substituímos x por $\beta^j x$, obtendo a partir de,

$$x^{p^n} - x = \prod_{s \in GF(p)} (Tr(x) - s);$$

$$(\beta^j x)^{p^n} - \beta^j = \prod_{s \in GF(p)} (Tr(\beta^j x) - s)$$

Berlekamp [16], mostra que nem todos os j em

$$x^{p^n} - x = \prod_{s=0}^{p-1} (Tr(\beta^j x) - s) \ 0 \leq \text{j} \leq \text{n-1} \tag{4.1}$$

produzem uma fatoração trivial de $f(x)$, por esta razão todas as raízes de $f(x)$ são construídas a partir 4.1.

Para resumir, procuraremos apresentar a seguir o algoritmo usado para encontrar as raízes de um polinômio em um corpo finito grande $GF(p)$ com característica p pequena,

Passo 1 Representar os elementos do corpo finito dado, em série ou na forma vetorial ou ainda polinomial.

Passo 2 Calcular a função traço $Tr(x) = \sum_{i=0}^{n-1} x^{p^i}$.

- 2.1- Calcular cada termo que compõe a função traço mod $f(x)$.
- 2.2- Somar todos os termos mod $f(x)$.

Passo 3 Calcular o $m.d.c(f(x), Tr(x) - s)$ para todo $0 \leq s < p$, com o intuito de obter $f(x)$ decomposta em s fatores, sendo denominados $g(x)$.

Passo 4 Se cada um dos $g(x)$ não for um polinômio de primeiro grau, procuraremos fatorá-lo com o intuito de obter fatores de grau 1. Para isso precisaremos calcular a função traço substituindo x por βx e os valores de β pelos valores deles encontrados na representação do corpo $GF(p^n)$ feita inicialmente, e por fim calcularemos esta função mod $f(x)$.

Passo 5 Calcular o $m.d.c$ como no passo 3.

Passo 6 Repetir o passo 4 até que o resultado do m.d.c. seja polinômios de grau 1.

O método aplicado para encontrar as raízes de polinômios pertencentes a corpos finitos grandes com característica pequena é conhecido por fatoração $f(x)$ sobre $GF(p^n)$.

Exemplo 4.10 Considere $GF(64) = GF(2)(\beta)$ onde β é uma raiz do polinômio irredutível $x^6 + x + 1$ em $GF(2)[x]$ e seja:
$f(x) = x^4+(\beta^5+\beta^4+\beta^3+\beta^2)\cdot x^3+(\beta^5+\beta^4+\beta^2+\beta+1)\cdot x^2+(\beta^4+\beta^3+\beta)\cdot x+\beta^3+\beta \in GF(64)[x]$

Como já temos o polinômio irredutível sobre $GF(2)$, o primeiro passo a ser dado é fazer a representação dos elementos de $GF(2^6)$. A qual podemos ver no apêndice D.

O próximo passo é encontrar a função traço:

$$Tr(x) = \sum_{i=0}^{5} x^{2^5} = x^{2^0} + x^{2^1} + x^{2^2} + x^{2^3} + x^{2^4} + x^{2^5} = x + x^2 + x^4 + x^8 + x^{16} + x^{32}$$

Precisamos encontrar inicialmente quanto é $x + x^2 + x^4 + x^8 + x^{16} + x^{32}$ mod $f(x)$. Para isso calculamos cada um destes termos como veremos a seguir, $x \equiv x$; $x^2 \equiv x^2$; $x^4 \equiv (\beta^5 + \beta^4 + \beta^3 + \beta^2) \cdot x^3 + (\beta^5 + \beta^4 + \beta^2 + \beta + 1) \cdot x^2 + (\beta^4 + \beta^3 + \beta) \cdot x + \beta^3 + \beta$; $x^8 \equiv (\beta^4 + \beta^3 + \beta^2) \cdot x^3 + (\beta^5 + \beta + 1) \cdot x^2 + (\beta^5 + \beta + 1) \cdot x + \beta^5 + \beta^4$; $x^{16} \equiv (\beta^5 + \beta^3 + \beta) \cdot x^3 + (\beta^3 + \beta) \cdot x^2 + \beta^5 \cdot x + \beta^4 + \beta^3 + \beta^2 + \beta + 1$ e $x^{32} \equiv (\beta^5 + \beta^2 + 1) \cdot x^3 + (\beta^5 + \beta^4 + \beta^3 + \beta^2 + \beta + 1) \cdot x^2 + (\beta^4 + \beta^2) \cdot x + \beta^5 + \beta^3$.

Após substituiremos os elementos que compõem a função traço pelo seu valor mod $f(x)$.

$Tr(x) = x + x^2 + x^4 + x^8 + x^{16} + x^{32} = Tr(x) = x + x^2 + [(\beta^5 + \beta^4 + \beta^3 + \beta^2) \cdot x^3 + (\beta^5 + \beta^4 + \beta^2 + \beta + 1) \cdot x^2 + (\beta^4 + \beta^3 + \beta) \cdot x + \beta^3 + \beta] + [(\beta^4 + \beta^3 + \beta^2) \cdot x^3 + (\beta^5 + \beta + 1) \cdot x^2 + (\beta^5 + \beta + 1) \cdot x + \beta^5 + \beta^4] + [(\beta^5 + \beta^3 + \beta) \cdot x^3 + (\beta^3 + \beta) \cdot x^2 + \beta^5 \cdot x + \beta^4 + \beta^3 + \beta^2 + \beta + 1] + [(\beta^5 + \beta^2 + 1) \cdot x^3 + (\beta^5 + \beta^4 + \beta^3 + \beta^2 + \beta + 1) \cdot x^2 + (\beta^4 + \beta^2) \cdot x + \beta^5 + \beta^3$

Ao resolvermos esta soma obteremos:

$Tr(x) = (\beta^5 + \beta^3 + \beta^2 + \beta + 1) \cdot x^3 + \beta^5 \cdot x^2 + (\beta^3 + \beta^2) \cdot x + \beta^3 + \beta^2 + 1$ mod $f(x)$.

Tentaremos encontrar as raízes inicialmente com $j = 0$. Iniciamos calculando o $m.d.c.(f(x), Tr(x))$ e o $m.d.c.(f(x), Tr(x) - 1)$.

$m.d.c.(f(x), Tr(x)) = m.d.c(f(x), (\beta^5 + \beta^3 + \beta^2 + \beta + 1) \cdot x^3 + \beta^5 \cdot x^2 + (\beta^3 + \beta^2) \cdot x + \beta^3 + \beta^2 + 1) = x^3 + (\beta^4 + \beta^3 + \beta^2) \cdot x^2 + (\beta^5 + \beta^2 + 1) \cdot x + \beta^3 + \beta^2$, ao resultado deste $m.d.c.$ denominaremos de $g(x)$.

$m.d.c.(f(x), Tr(x) - 1) = m.d.c(f(x), (\beta^5 + \beta^3 + \beta^2 + \beta + 1) \cdot x^3 + \beta^5 \cdot x^2 + (\beta^3 + \beta^2) \cdot x + \beta^3 + \beta^2) = x + \beta^5$.

Então, $f(x) = g(x) \cdot (x + \beta^5)$. Sendo que β^5 já é uma das raízes procuradas.

Escolhemos agora $j = 1$ e substituímos na função traço o x por $\beta \cdot x$.

$Tr(x) = x + x^2 + x^4 + x^8 + x^{16} + x^{32}$

$Tr(\beta x) = (\beta x) + (\beta x)^2 + (\beta x)^4 + (\beta x)^8 + (\beta x)^{16} + (\beta x)^{32} = Tr(\beta x) = \beta x + \beta^2 x^2 + \beta^4 x^4 + \beta^8 x^8 + \beta^{16} x^{16} + \beta^{32} x^{32}$

Substituímos neste momento o $\beta, \beta^2, \beta^4, \beta^8, \beta^{16}, \beta^{32}$ pelos seus respectivos valores encontrados quando representamos o corpo $GF(64)$. Também substituímos os valores de $x, x^2, x^4, x^8, x^{16}, x^{32}$ pelos seus respectivos valores mod $f(x)$. Fizemos a soma, obtendo, $Tr(\beta x) = (\beta^5 + \beta^2) \cdot x^2 + \beta^3 \cdot x + \beta^5 + \beta^3 + \beta$ mod $g(x)$.

Com o intuito de obter fatores menores, calcularemos o $m.d.c.(g(x), Tr(\beta x))$ e o $m.d.c.(g(x), Tr(\beta x) - 1)$.

$m.d.c.(g(x), Tr(\beta x)) = m.d.c(x^3 + (\beta^4 + \beta^3 + \beta^2) \cdot x^2 + (\beta^5 + \beta^2 + 1) \cdot x + \beta^3 + \beta^2, (\beta^5 + \beta^2) \cdot x^2 + \beta^3 \cdot x + \beta^5 + \beta^3 + \beta) = x^2 + (\beta^3 + 1) \cdot x + \beta^4 + \beta^3 + \beta^2 + \beta$, o resultado deste $m.d.c.$ será denominado de $h(x)$.

$m.d.c.(g(x), Tr(\beta x) - 1) = m.d.c(x^3 + (\beta^4 + \beta^3 + \beta^2) \cdot x^2 + (\beta^5 + \beta^2 + 1) \cdot x + \beta^3 + \beta^2, (\beta^5 + \beta^2) \cdot x^2 + \beta^3 \cdot x + \beta^5 + \beta^3 + \beta + 1)) = x + \beta^4 + \beta^2 + 1$

Então, $g(x) = h(x) \cdot (x + \beta^4 + \beta^2 + 1)$. Sendo $\beta^4 + \beta^2 + 1$ uma das raízes.

Como $h(x)$ ainda não é de grau 1 devemos escolher outro valor para j e proceder da mesma forma que para $j = 1$. Então escolhemos $j = 2$ e substituímos na função traço o x por $\beta^2 x$.

$Tr(x) = x + x^2 + x^4 + x^8 + x^{16} + x^{32}$

$Tr(\beta^2 x) = (\beta^2 x) + (\beta^2 x)^2 + (\beta^2 x)^4 + (\beta^2 x)^8 + (\beta^2 x)^{16} + (\beta^2 x)^{32} = \beta^2 x + \beta^4 x^2 + \beta^8 x^4 + \beta^{16} x^8 + \beta^{32} x^{16} + \beta^{64} x^{32}$.

Substituímos neste momento o $\beta, \beta^2, \beta^4, \beta^8, \beta^{16}, \beta^{32}$ pelos seus respectivos valores encontrados quando representamos o corpo $GF(64)$. Também substituímos os valores de $x, x^2, x^4, x^8, x^{16}, x^{32}$ pelos seus respectivos valores mod $f(x)$. Fizemos a soma, obtendo, $Tr(\beta^2 x) = (\beta^5 + \beta^2 + 1) \cdot x + \beta^5 + \beta^3 + \beta^2$ mod $h(x)$

Novamente com o objetivo de obter fatores menores, calcularemos o $m.d.c.(h(x), Tr(\beta^2 x))$ e o $m.d.c.(f(x), Tr(\beta^2 x) - 1)$.

$m.d.c.(h(x), Tr(\beta^2 x)) = m.d.c(h(x), (\beta^5 + \beta^2 + 1) \cdot x + \beta^5 + \beta^3 + \beta^2) = x + \beta + 1$. Sendo $\beta + 1$ uma raiz de $f(x)$.

$m.d.c.(h(x), Tr(\beta^2 x) - 1) = m.d.c(h(x), (\beta^5 + \beta^2 + 1) \cdot x + \beta^5 + \beta^3 + \beta^2 + 1) = x + \beta^3 + \beta$. Sendo $\beta^3 + \beta$ uma raiz de $f(x)$.

Então, $h(x) = (x + \beta + 1) \cdot (x + \beta^3 + \beta)$. Encontramos portanto, mais duas raízes de $f(x)$.

A fatorização de $f(x)$ é, $f(x) = (x + \beta + 1) \cdot (x + \beta^3 + \beta) \cdot (x + \beta^4 + \beta^2 + 1) \cdot (x + \beta^5)$.

Portanto, as raízes de $f(x)$ são: $\beta + 1$, $\beta^3 + \beta$, $\beta^4 + \beta^2 + 1$ e β^5.

4.5 Um corpo finito grande $GF(q)$ com característica p grande

No quarto caso temos um corpo finito grande $GF(q)$ com característica p grande. Como anteriormente, é suficiente considerarmos o caso onde

$$f(x) = \prod_{i=1}^{m} (x - \gamma_i)$$

com distintos $\gamma_1, \gamma_2, \ldots, \gamma_m \in GF(q)$. Sendo $q = p^n$.

Para verificarmos se $f(x)$ tem esta forma devemos verificar a congruência $x^q \equiv x \mod f(x)$, ou seja, devemos verificar se a $f(x)$ é o produto de polinômios irredutíveis de grau 1.

A fim de encontrarmos as raízes de $f(x)$, a representamos como

$$f(x) = \sum_{j=0}^{m} \alpha_j \cdot x^j \text{ onde } \alpha_j \in GF(p^n) 0 \leq j \leq m$$

Para encontrarmos as raízes do polinômio $f(x)$ excluímos o caso trivial, assumindo $m \geq 2$ e calculamos,

$$f_k(x) = \sum_{j=0}^{m} \alpha_j^{p^k} \cdot x^j \text{ sendo } 0 \leq k \leq n-1$$

onde $\alpha_j \in GF(q)$ para $0 \leq j \leq m$.

Quando $k = 0$ a $f_k(x)$ será igual a $f(x)$ pois a

$$f(x) = \sum_{j=0}^{m} \alpha_j \cdot x^j$$

Sabendo que os distintos γ são as raízes procuradas de $f(x)$, substituímos x por $\gamma_i^{p^k}$ obtendo,

$$f_k(\gamma_i^{p^k}) = \sum_{j=0}^{m} \alpha_j^{p^k} \cdot \gamma_i^{j \cdot p^k} = (\sum_{j=0}^{m} \alpha_j \cdot \gamma_i^j)^{p^k} = (f(\gamma_i))^{p^k} = 0$$

para $1 \leq i \leq m$, $0 \leq k \leq n-1$ e então,

$$f_k(x) = \prod_{i=1}^{m} (x - \gamma_i^{p^k}) \text{ para } 0 \leq k \leq n-1$$

Isso quer dizer que as raízes de $f_k(x)$ são γ^{p^k} ou seja, as raízes de $f(x)$ elevadas na potência p^k. Ao multiplicarmos todas as f_k encontradas obtemos um polinômio $F(x)$, ou seja,

$$F(x) = \prod_{k=0}^{n-1} f_k(x)$$

ou ainda,

$$F(x) = \prod_{k=0}^{n-1} \prod_{i=1}^{m} (x - \gamma_i^{p^k}) = \prod_{i=0}^{m} \prod_{k=0}^{n-1} (x - \gamma_i^{p^k}) = \prod_{i=1}^{m} F_i(x)^{n/di}$$

sendo que $F_i(x)$ são fatores irredutíveis de $F(x)$. Alguns $F_i(x)$ podem ser idênticos, logo temos a fatoração de $F(x)$ da forma $F(x) = G_1(x), \cdots, G_r(x)$ onde G_t com $1 \leq t \leq r$ são potências de $F_i(x)$ distintos. Os $F_i(x)$ podem ser vistos como polinômios mínimos de γ_i sobre $GF(p)$ e d_i é o grau do polinômio mínimo.

Para fatorarmos a $F(x)$, ou seja encontrarmos os $G_t(x)$, devemos usar um dos algoritmos vistos no capítulo anterior, dentre os métodos relatados poderíamos usar o método de Cantor/Zassenhaus.

A fatoração de $f(x)$ é então obtida como

$$f(x) = \prod m.d.c.(f(x), G_t(x))$$

Essa fatoração geralmente é não trivial a não ser que $f(x)$ seja por si mesma uma potência irredutível.

Caso a fatoração seja não trivial, repetimos o $m.d.c.$ citado acima, trocando a $f(x)$ pelo resultado do mesmo, até encontrarmos a $f(x)$ dividida completamente em fatores lineares.

Caso a fatoração ainda seja trivial, ou seja, $m.d.c.(f(x), G_t(x)) = f(x)$ para algum t, $1 \leq t \leq r$, isso indica que as raízes de $f(x)$ são todas conjugadas. Sem perda de generalidade, podemos assumir que $r = 1$ e $f(x)$ divide $f_1(x)$. Comparando os graus, obtemos $n \leq d_1 = n$. Além disso, pode ocorrer duas possibilidades: as raízes de $f(x)$ são às de algum $f_k(x)$ ou não.

Se as raízes de $f(x)$ não forem idênticas, às de algum $f_k(x)$ ao calcularmos o $m.d.c(f(x), f_k(x))$ obteremos um fator $\neq f(x)$ e $\neq 1$ para algum k, sendo $1 \leq k < n/m$. Portanto, o resultado do $m.d.c(f(x), f_k(x))$ é um fator não trivial de $f(x)$.

Se as raízes forem idênticas ao calcularmos o $m.d.c(f(x), f_k(x))$ obteremos como resultado 1 para $1 \leq k < d = n/m$ e portanto $f(x)$ é o polinômio mínimo de γ_1. E γ_i serão exatamente todos os conjugados de γ_1. Neste caso para encontrarmos os fatores não triviais de $f(x)$ devemos transformar $f(x)$, para isso tomamos β como um elemento gerador de $GF(q)$ sobre $GF(p)$ de tal forma que $GF(q) = GF(p^d)(\beta) = GF(p^n)$ e β é algébrico de grau $\frac{n}{d} = m$ sobre $GF(p^d)$ em particular β^j não pertence a $GF(p^d)$ para $1 \leq j \leq m-1$.

Se algum coeficiente $\alpha_{j_0} \neq 0$ de $f(x)$ para $1 \leq j \leq n-1$, considere $F(x) = \beta^{-m} \cdot f(\beta x)$, que é um polinômio mônico de grau m sobre $GF(q)$. Como β^{n-j_0} não pertence $GF(p^d)$ e $\alpha_{j_0} \in GF(p^d)$, segue que o coeficiente de x^{j_0} de $\overline{f}(x)$ não pertence $GF(p^d)$. Assim, não vai ocorrer que as raízes de $\overline{f}(x)$ sejam idênticas a $\overline{f}_d(x)$. Assim o algoritmo é aplicado a $\overline{f}_d(x)$. Como recuperar as raízes de $f(x)$ a partir das raízes de $\overline{f}(x)$? É só observar que $f(x) = \beta^m \overline{f}(\beta^{-1}x)$ e, portanto, qualquer fatoração não trivial de $\overline{f}(x)$ fornece uma fatoração não trivial de $f(x)$.

Ainda falta considerar o caso em que o coeficiente de α_j de $f(x)$ são todos nulos para $1 \leq j \leq n-1$. Mas então $f(x) = x^m + \alpha_0 \in GF(p^d)(x)$, neste caso considere, $\overline{f}(x) = \beta^{-m} f(\beta x + 1)$ e segue o raciocínio anterior.

Ao encontrarmos um fator não trivial de $f(x)$ o procedimento deve ser continuado colocando este resultado no lugar de $f(x)$, até que $f(x)$ seja dividida completamente em fatores lineares.

Procuraremos apresentar a seguir o algoritmo usado para encontrar as raízes de um polinômio em um corpo finito grande $GF(p)$ com característica p grande.

Passo 1. Devemos calcular o $m.d.c.(f(x), x^q - x)$ e após encontrar $f_k(x)$ sendo $0 \leq k \leq m-1$

$$f_k(x) = \sum_{j=0}^{m} \alpha_j^{p^k} \cdot x^j$$

onde $\alpha_j \in GF(q)$ para $0 \leq j \leq m$.

Passo 2. Devemos multiplicar todas as $f_k(x)$ encontradas, obtendo $F(x)$, ou seja,

$$F(x) = \prod_{k=0}^{m-1} f_k(x)$$

Passo 3. Devemos fatorar a $F(x)$, através de um dos algoritmos vistos no capítulo anterior. Dentre os métodos relatados poderíamos usar o método de

Cantor/Zassenhaus, obtendo, $F(x) = G_1(x) \cdots G_r(x)$ onde $G_t(x)$ $1 \leq t \leq r$ é uma série de distintos $F_i(x)$.

Passo 4. Para encontrarmos os F_i devemos calcular o $m.d.c.(f(x), G_t(x))$.

A fatoração de $f(x)$ será obtida através do

$$\prod m.d.c.(f(x), G_t(x))$$

Passo 5. Geralmente essa fatoração é não trivial, mas caso seja trivial devemos calcular o $m.d.c.(f(x), f_k(x))$ para $1 \leq k < n/m$. Se isto também não produzir um fator não trivial de $f(x)$, devemos transformar a $f(x)$. Ao encontrarmos um fator não trivial de $f(x)$ o procedimento deve ser continuado colocando este resultado no lugar de $f(x)$, até que $f(x)$ seja dividida completamente em fatores lineares.

Exemplo 4.11 Seja $f(x) = x^4 + (\beta^5 + \beta^4 + \beta^3 + \beta^2) \cdot x^3 + (\beta^5 + \beta^4 + \beta^2 + \beta + 1) \cdot x^2 + (\beta^4 + \beta^3 + \beta) \cdot x + \beta^3 + \beta \in GF(2^6)$.

Para determinarmos as raízes de $f(x)$ calculamos inicialmente $m.d.c(f(x), x^q - x) = m.d.c(x^4 + (\beta^5 + \beta^4 + \beta^3 + \beta^2) \cdot x^3 + (\beta^5 + \beta^4 + \beta^2 + \beta + 1) \cdot x^2 + (\beta^4 + \beta^3 + \beta) \cdot x + \beta^3 + \beta, x^{64} - x) = f(x)$, isso indica que a $f(x)$ é o produto de fatores irredutíveis de grau 1, ou seja, tem 4 raízes no corpo $GF(2^6)$.

A seguir, calculamos as $f_k(x) = \sum_{j=0}^{6} \alpha_j^{p^k} x^j$ para $0 \leq k \leq 5$.

$k = 0$: $f_0(x) = \alpha_0 + \alpha_1 \cdot x + \alpha_2 \cdot x^2 + \alpha_3 \cdot x^3 + \alpha_4 \cdot x^4 + \alpha_5 \cdot x^5 + \alpha_6 \cdot x^6 = \beta^3 + \beta + (\beta^4 + \beta^3 + \beta) \cdot x + (\beta^5 + \beta^4 + \beta^2 + \beta + 1) \cdot x^2 + (\beta^5 + \beta^4 + \beta^3 + \beta^2) \cdot x^3 + x^4$

$k = 1$: $f_1(x) = \alpha_0^2 + \alpha_1^2 \cdot x + \alpha_2^2 \cdot x^2 + \alpha_3^2 \cdot x^3 + \alpha_4^2 \cdot x^4 + \alpha_5^2 \cdot x^5 + \alpha_6^2 \cdot x^6 = (\beta^3+\beta)^2 + (\beta^4+\beta^3+\beta)^2 \cdot x + (\beta^5+\beta^4+\beta^2+\beta+1)^2 \cdot x^2 + (\beta^5+\beta^4+\beta^3+\beta^2)^2 \cdot x^3 + x^4$

$k = 2$: $f_2(x) = \alpha_0^4 + \alpha_1^4 \cdot x + \alpha_2^4 \cdot x^2 + \alpha_3^4 \cdot x^3 + \alpha_4^4 \cdot x^4 + \alpha_5^4 \cdot x^5 + \alpha_6^4 \cdot x^6 = (\beta^3+\beta)^4 + (\beta^4+\beta^3+\beta)^4 \cdot x + (\beta^5+\beta^4+\beta^2+\beta+1)^4 \cdot x^2 + (\beta^5+\beta^4+\beta^3+\beta^2)^4 \cdot x^3 + x^4$

$k = 3$: $f_3(x) = \alpha_0^8 + \alpha_1^8 \cdot x + \alpha_2^8 \cdot x^2 + \alpha_3^8 \cdot x^3 + \alpha_4^8 \cdot x^4 + \alpha_5^8 \cdot x^5 + \alpha_6^8 \cdot x^6 =$
$(\beta^3+\beta)^8+(\beta^4+\beta^3+\beta)^8 \cdot x+(\beta^5+\beta^4+\beta^2+\beta+1)^8 \cdot x^2+(\beta^5+\beta^4+\beta^3+\beta^2)^8 \cdot x^3+x^4$

$k = 4$: $f_4(x) = \alpha_0^{16}+\alpha_1^{16} \cdot x+\alpha_2^{16} \cdot x^2+\alpha_3^{16} \cdot x^3+\alpha_4^{16} \cdot x^4+\alpha_5^{16} \cdot x^5+\alpha_6^{16} \cdot x^6 =$
$(\beta^3+\beta)^{16}+(\beta^4+\beta^3+\beta)^{16} \cdot x+(\beta^5+\beta^4+\beta^2+\beta+1)^{16} \cdot x^2+(\beta^5+\beta^4+\beta^3+\beta^2)^{16} \cdot x^3+x^4$

$k = 5$: $f_5(x) = \alpha_0^{32}+\alpha_1^{32} \cdot x+\alpha_2^{32} \cdot x^2+\alpha_3^{32} \cdot x^3+\alpha_4^{32} \cdot x^4+\alpha_5^{32} \cdot x^5+\alpha_6^{32} \cdot x^6 =$
$(\beta^3+\beta)^{32}+(\beta^4+\beta^3+\beta)^{32} \cdot x+(\beta^5+\beta^4+\beta^2+\beta+1)^{32} \cdot x^2+(\beta^5+\beta^4+\beta^3+\beta^2)^{32} \cdot x^3+x^4$

Ao multiplicarmos todas as $f_k(x)$ obtemos o polinômio $F(x) = x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{16} + x^{12} + x^7 + x^6 + x^4 + 1$. Fatoramos através do método de Cantor/Zassenhaus obtendo $F(x) = (x^6+x^4+x^2+x+1) \cdot (x^6+x^5+x^2+x+1) \cdot (x^6+x^4+x^3+x+1)^2$, ou seja $G_1(x) = x^6 + x^4 + x^2 + x + 1$, $G_2(x) = x^6 + x^5 + x^2 + x + 1$ e $G_3(x) = x^6 + x^4 + x^3 + x + 1$.

Ao calcularmos o $m.d.c(f(x), G_t(x))$ obtemos

$m.d.c.(f(x), x^6 + x^5 + x^2 + x + 1) = x + \beta^5$

$m.d.c.(f(x), x^6 + x^4 + x^2 + x + 1) = x + \beta + 1$

$m.d.c.(f(x), x^6 + x^4 + x^3 + x + 1) = x^2 + x \cdot (\beta^4 + \beta^3 + \beta^2 + \beta + 1) + \beta^2$.

Como o resultado deste $m.d.c$ não é um fator linear, calculamos novamente o $m.d.c$ substituindo a $f(x)$ por $x^2 + x \cdot (\beta^4 + \beta^3 + \beta^2 + \beta + 1) + \beta^2$ obtendo $x + \beta^3 + \beta$ e $x + \beta^4 + \beta^2 + 1$.

Portanto as raízes de $f(x)$ são β^5, $\beta + 1$, $\beta^3 + \beta$ e $\beta^4 + \beta^2 + 1$.

5 CONSIDERAÇÕES FINAIS

O trabalho que ora findamos constitui-se num esforço exercido no intuito de estudar corpos finitos. Estes podem ser chamados como corpos de Galois, uma vez que o matemático Evariste de Galois dedicou-se ao estudo e à pesquisa destes corpos. Ele é responsável por muitas das idéias que temos hoje sobre corpos finitos.

Em virtude do tema "corpos finitos" ser muito amplo, optamos pela delimitação do mesmo cuja finalidade era tornar viável nossa pesquisa. Traçamos como objetivo do trabalho determinarmos as raízes de polinômios sobre corpos finitos.

Ao nos debruçarmos sobre corpos finitos vimos que os mesmos podem, essencialmente, serem caracterizados a partir de três teoremas: o primeiro deles afirma que cada corpo finito tem p^n elementos, sendo p um primo e n um inteiro positivo, o segundo, que dado um primo p e um inteiro positivo n, existe um corpo finito com p^n elementos, e o terceiro que todos os corpos finitos que tem o mesmo número de elementos são isomorfos. Estes corpos são muito importantes em diferentes áreas da matemática, poderíamos citar, entre elas, algumas de suas aplicações na criptografia e na teoria de códigos.

Vimos que para representarmos os elementos de um corpo finito determinamos inicialmente um polinômio irredutível sobre o corpo em que estamos trabalhando e a partir dele é gerado um anel quociente. Ao optarmos pela representação dos corpos finitos visamos auxiliar na realização de operações aritméticas entre os elementos do corpo. Esta constitui-se em sua grande função que é dar maior eficiência e facilidade nas operações.

Por necessitarmos da fatoração para determinarmos as raízes de polinômios pertencentes a um determinado corpo finito, estudamos este tema que tem grande importância e aplicabilidade no campo da Matemática e áreas afins. Para o nosso trabalho bastou estudarmos os métodos de Berlekamp, Cantor-Zassenhaus

e Lidl-Niederreiter, no entanto, somos sabedores da existência de métodos mais modernos, que podem ser vistos em Kaltofen [10] e [11].

Um algoritmo de fatoração é em particular, um algoritmo para achar raízes, visto que as raízes de um polinômios sobre um corpo finito, podem ser determinadas a partir de fatores lineares, que são encontrados ao fatorarmos um polinômio. Porém as técnicas empregadas são diferentes das usadas pelos métodos para determinarmos as raízes e também esses algoritmos nem sempre são os mais eficientes.

Neste trabalho apresentamos algoritmos para determinarmos as raízes de polinômios sobre corpos finitos, sendo que os mesmos têm sua estrutura diferente dependendo do corpo em que o polinômio está inserido, ou seja, um corpo primo $GF(p)$ considerando p pequeno, um corpo primo $GF(p)$ considerando p grande, um corpo finito grande $GF(q)$ com característica p pequena e um corpo finito grande $GF(q)$ com característica p grande.

Ao findarmos este trabalho podemos afirmar que nossos objetivos foram atingidos, sendo este trabalho de grande utilidade para pesquisadores que tenham o intuito de tomarem estes conhecimentos como base para um posterior estudo de aplicações destes corpos finitos.

Bibliografia

[1] Michael Ben-Or. Probabilistc algorithms in finite fields. In *Proc 22 nd IEEE Symp. Found. Comp. Sci.* IEEE, 1981.

[2] R. Beresford. Finite - field arithmetic. site - http://www.anujseth.com, 1997.

[3] E. R. Berlekamp. *Algebraic Coding Theory.* Mc Graw-Hill, New York, 1967.

[4] E. R. Berlekamp. Factoring polynomials over large finite fields. *Mathematics of Computation*, 24(111):713–735, July 1970.

[5] J. Calmet. *Algebraic Algorithms in GF(q)*, pages 101 – 109. Descrite Mathematics, LIFIA/IMAG, Grenoble, France, 1985.

[6] D. Cantor and H. Zassenhaus. A new algorithm for factoring polynomials over finite fields. *Mathematics of Computation*, 36:587–592, January 1981.

[7] JJO' Connor and EF Robertson. Evariste galois. site - http://www - gap.dcs.st - and.ac.uk/ history/Mathematicians/Galois.html, dezembro 1996.

[8] Siret y. Davenport, J.h. and E. Tournier. *Computer Algebra-Systems and Algorithms for algebraic computation.* Academic Press Inc., San Diego, 1988.

[9] Erich Kaltofen and Victor Shoup. Subquadratic - time factoring of polynomials over finite fields. *Mathematics of Computation*, 67(223):1.179 – 1.197, 1998.

[10] Erik Kaltofen. Polynomial factorization 1982-1986. In D.V. Chudnovsky and R.D. Jenks, editors, *Computers in Mathematics*, pages 285–309. 1990.

[11] Erik Kaltofen. Polynomial factorization 1987-1991. In I. Simon, editor, *Computers in Mathematics*, pages 294–313. 1992.

[12] Donald E. Knuth. *The Art of Computer Programming , - Seminumerical Algorithms*, volume 2. Addison-Wesley, Reading Massachusetts, 1997.

[13] Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and their applications*. Cambridge University Press, New York, 1994.

[14] John D. Lipson. *Elements of Algebra and Algebraic Computing*. Addison-Wesley Publishing Company, Massachusetts, 1981.

[15] Maurice Mignotte and Doru Stefanescu. *Polynomials - An Algorithmic Approach*. Springer, Singapore, 1999.

[16] Robert T. Moenck. On the efficiency of algorithms for polynomial factoring. *Mathematics of Computation*, 31(137):235–250, January 1977.

[17] Daniel Panario. *Combinatorial and Algebraic Aspects of Polynomials over Finite Fields*. PhD thesis, University of Toronto, Estados Unidos, June 1997.

[18] M. Pohst and H. Zassenhaus. *Algorithmic Algebraic Number Theory*. Cambridge University Press, 1989.

[19] Michael O. Rabin. Probabilistic algorithms in finite fields. *SIAM J. Computation*, 9(2):273–280, May 1980.

[20] Steven Roman. *Field Theory, série: Graduate Texts in Mathematics*. Springer - Verlag, New York, 1995.

[21] Victor Shoup. Factoring polynomials over finite fields: Asymptotic complexity vs. reality. site - http://www.shoup.net/papers/lille.pdf.

[22] Vilmar Trevisan. *Univariate Polynomial Factorization*. PhD thesis, Kent State University, Estados Unidos, May 1992.

[23] Eric W. Weisstein. Evariste galois. site - http://scienceworld.wolfram.com/biography/Galois.html, 2003.

[24] Eric W. Weisstein. Function moebius. Wolfram Research - site - http://mathworld.wolfram.com/MoebiusFunction.html, 2003.

Apêndice A RESUMO BIOGRÁFICO - EVARISTE GALOIS

Evariste Galois, matemático francês, desenvolveu técnicas novas para estudar a solução de equações polinomiais por radicais. Seus trabalhos mostraram que as equações polinomiais de quinto grau ou maior não têm solução em termos de um número finito de operações aritméticas elementares e da extração de raízes.

Galois teve uma vida muito difícil, conforme está descrito em [7]. Nasceu no dia 25 de outubro de 1811, no Reino de Bourg (perto de Paris). Até os doze anos, sua única professora foi sua mãe; somente em 1823 entrou na escola. Nos seus primeiros dois anos de escola, era tido como um bom aluno, porém depois os professores admiravam sua inteligência matemática, mas queixavam-se de que não realizava as tarefas solicitadas; e só trabalhava com assuntos de nível matemático bem mais elevado. Tentou por duas vezes a admissão na escola Politécnica, mas não passou. Entrou então, na escola normal, a qual concluiu em 1829.

Galois teve seus trabalhos, por diversas vezes, ignorados ou até mesmo, perdidos. Deu a Cauchy um artigo que continha seus resultados mais importantes; mas não guardou consigo uma cópia, e Cauchy o perdeu. Após, submeteu um artigo ao prêmio da Academia de Matemática. O artigo foi enviado a Fourier, que era o então secretário da Academia, que morreu logo após. E o artigo nunca foi encontrado. Poisson convidou Galois para submeter os resultados que encontrou sobre a Teoria de Grupos à Academia, mas Poisson os considerou algo incompreensível.

Galois, sempre um radical, foi preso em maio de 1831, após ter feito um brinde, o qual foi considerado uma ameaça ao rei. Só conseguiu ser libertado em junho de 1831. E já em julho do mesmo ano, foi preso outra vez por ter estragado o uniforme de um guarda da artilharia nacional, visto como uma atitude ilegal. Além disso, Galois portava um rifle carregado, diversas pistolas e um punhal.

Em março de 1832, uma epidemia de cólera tomou conta de Paris e os prisioneiros, incluindo Galois, foram transferidos para uma pensão. Lá conheceu uma moça, Stephanie, pela qual se apaixonou.

Após ser solto da prisão, trocou cartas com Stephanie, e fez menção a ela em seus manuscritos. Provavelmente tenha sido esse o motivo do duelo com Perscheux d'Herbinville, no qual ficou muito ferido. Acabou falecendo no dia 31 de maio de 1832.

Enquanto estava encarcerado, e na noite anterior ao duelo, escreveu artigos que continham muitos conhecimentos matemáticos.

Seu irmão e o amigo Chevalier copiaram seus artigos matemáticos e os enviaram a Gauss, a Jacobi e a outros. Não se tem conhecimento de que eles tenham feito algum comentário sobre os mesmos. Mas esses artigos chegaram até Liouville, que em 1843, os anunciou para a Academia e os publicou em periódico em 1846.

A teoria que Galois esboçou nestes artigos é hoje chamada Teoria de Galois. Dentre muitos resultados desta teoria, o mais conhecido é o que se refere a um problema estudado por muitos cientistas durante séculos, ou seja, que uma equação polinomial de grau maior do que 4 não é solúvel por radicais, o que significa que não existe uma fórmula simples que contenha radicais e operações aritméticas para as raízes de um polinômio de grau ≥ 5.

Apêndice B ALGORITMO DE EUCLIDES

O matemático grego Euclides que viveu de 330 a.C. a 275 a.C. na cidade de Alexandria, na Grécia, desenvolveu um algoritmo para calcular o máximo divisor comum entre dois números (ou polinômios), que leva o seu nome Algoritmo de Euclides.

As operações são realizadas obtendo um quociente e um resto, que obedecem a propriedade do domínio Euclidiano. Se $a, b \in D$, $b \neq 0$ então a div $b = q$ e a mod $b = r$ satisfazendo $a = b \cdot q + r$, com $grau(r) < grau(b)$ ou $r = 0$.

A propriedade acima aplicada ao domínio Euclidiano $\mathbb{Z}$, é também aplicada ao domínio Euclidiano $F[x]$, onde F é um corpo. Suponha sem perder a generalidade, que $g \neq 0$. Definimos $f(x)$ div $g(x)$ e $f(x)$ mod $g(x)$ obtendo respectivamente, um único quociente $q(x)$ e resto $r(x)$ que satisfaz a propriedade: $f(x) = g(x) \cdot q(x) + r(x)$, sendo grau $r(x) <$ grau $g(x)$.

Para aplicarmos o algoritmo de Euclides devemos seguir os seguintes passos:

Passo 1 Dividimos f por g, obtendo um resto r. Reescrevemos o $m.d.c.$

$m.d.c(f, g) = m.d.c.(g, r)$.

Passo 2 Repetimos o passo 1 até encontrarmos $grau(d(x)) > grau(r(x))$.

Exemplo B.1 Seja $f(x) = x^4 + x^3 + 1$ e $g(x) = x^4 - x$. Aplicando o algoritmo de Euclides calculamos o m.d.c entre $f(x)$ e a $g(x)$ obtendo,

$$
\begin{aligned}
m.d.c.(x^4+x^3+1, x^4-x) &= m.d.c.(b, a \ mod \ b) \\
&= m.d.c(x^4-x, x^3+x+1) \\
&= m.d.c.(x^3+x+1, -x^2) \\
&= m.d.c.(-x^2, x+1) \\
&= m.d.c(x+1, x) \\
&= m.d.c(x, 1) \\
&= m.d.c(1, 0)
\end{aligned}
$$

Exemplo B.2 Seja $f(x) = x^5 - 4 \cdot x^4 - 4 \cdot x^3 + 4 \cdot x$ e $g(x) = x^5 - x$. Aplicando o algoritmo de Euclides calculamos o m.d.c entre $f(x)$ e $g(x)$ obtendo,

$$
\begin{aligned}
m.d.c.(x^5 - 4 \cdot x^4 - 4 \cdot x^3 + 4 \cdot x, x^5 - x) &= m.d.c.(x^5 - x, -4 \cdot x^4 - 4 \cdot x^3) \\
&= m.d.c.(-4 \cdot x^4 - 4 \cdot x^3, x^3 - x) \\
&= m.d.c.(x^3 - x, x^2 + x) \\
&= m.d.c.(x^2 + x, 0) \\
&= x^2 + x
\end{aligned}
$$

Apêndice C EXEMPLIFICANDO A FATORAÇÃO LIVRE DE QUADRADOS

Vimos no capítulo 3 que nem sempre ao fatorarmos um polinômio arbitrário encontramos somente fatores irredutíveis distintos. Mas que é possível reduzirmos a fatoração para encontrarmos somente estes fatores irredutíveis distintos. Considerando $f(x) \in GF(q)[x]$ calculamos primeiramente a derivada $f'(x)$.

Relembrando, o teorema afirma que se $f'(x)$ não der zero, então nós calculamos o $m.d.c.(f(x), f'(x))$. Se o resultado do $m.d.c.$ tiver grau positivo, então esse é um fator próprio de $f(x)$. Retiramos este fator de $f(x)$ e repetimos o cálculo do $m.d.c.$, se der 1 então $f(x)$ não tem mais fatores repetidos.

Se $f'(x)$ der zero, nós temos uma $f(x) = \sum_{i=0}^{n/q} f_i \cdot x^{qi} = (\sum_{i=0}^{n/q} f_i^{\frac{1}{q}} \cdot x^i)^q$,

ou seja, a $f(x)$ é uma potência de q.

Para reduzirmos a fatoração somente a fatores irredutíveis distintos devemos fatorar o termo $f_i^{\frac{1}{q}} \cdot x^i$. E após procedemos como no caso onde $f'(x) \neq 0$.

Exemplo C.1 Seja $f(x) = x^6 - 7x^5 + 3x^4 - 7x^3 + 4x^2 - x - 2 \in GF(5)$. Então a $f'(x) = 6x^5 - 35x^4 + 12x^3 - 21x^2 + 8x - 1$. Para determinarmos a parte de $f(x)$ que é composta somente por fatores irredutíveis calculamos $m.d.c.(f(x), f'(x)) = m.d.c.(x^6 - 7x^5 + 3x^4 - 7x^3 + 4x^2 - x - 2, 6x^5 - 35x^4 + 12x^3 - 21x^2 + 8x - 1) = 1$.

Como a $f'(x) \neq 0$ e o $m.d.c.$ deu 1, então $f(x)$ não tem fatores repetidos.

Exemplo C.2 Seja $f(x) = x^2+4x+4 \in GF(3)$. Então $f'(x) = 2x+4$. Para encontrarmos a parte de $f(x)$ que é composta somente por fatores irredutíveis calculamos o $m.d.c.(f(x), f'(x))$, ou seja, $m.d.c.(x^2 + 4x + 4, 2x + 4) = x + 2$.

Como o resultado foi $x + 2$, então $f(x)$ pode ser reduzida. Retiramos da $f(x)$ o $x+2$, obtendo $x+2$. Calculamos novamente o $m.d.c(f(x), f'(x))$, ou seja,

$m.d.c.(x+2,1) = 1$. Como o resultado do $m.d.c$ é 1 então $f(x)$ não tem mais fatores repetidos. A parte de $f(x)$ que é composta somente por fatores irredutíveis é $x+2$.

Exemplo C.3 Seja $f(x) = x^4 + x^2 \in GF(2)$. Então $f'(x) = 4 \cdot x^3 + 2 \cdot x$ como é mod 2, a $f'(x) = 0$. Quando a derivada é zero, podemos escrever a $f(x)$ como uma potência de q, ou seja, $(x^2 + x)^2$, nos preocupando somente com o termo do meio, que no caso é $x^2 + x$. Iniciamos calculando a derivada deste termo que é $2 \cdot x + 1$ e após calculamos, o $m.d.c.(f(x), f'(x)) = m.d.c(x^2 + x, 2 \cdot x + 1)$ como este cálculo tem como resposta 1, podemos afirmar que $f(x)$ não tem mais fatores repetidos.

Apêndice D REPRESENTAÇÃO DO CORPO $GF(2^6)$

Abaixo está representado o corpo $GF(2^6)$, onde β é uma raiz do polinômio irredutível $x^6 + x + 1$ em $GF(2)[x]$.

Tabela D.1: *Representação do corpo* $GF(2^6)$

Representação em série	Representação polinomial	Representação vetorial
0	0	(0, 0, 0, 0, 0, 0)
α	β	(0, 1, 0, 0, 0, 0)
α^2	β^2	(0, 0, 1, 0, 0, 0)
α^3	β^3	(0, 0, 0, 1, 0, 0)
α^4	β^4	(0,0, 0, 0,1, 0)
α^5	β^5	(0, 0, 0, 0, 0, 1)
α^6	$\beta^6 \equiv \beta + 1$	(1, 1, 0, 0, 0, 0)
α^7	$\beta^7 \equiv \beta^2 + \beta$	(0, 1, 1, 0, 0, 0)
α^8	$\beta^8 \equiv \beta^3 + \beta^2$	(0, 0, 1, 1, 0, 0)
α^9	$\beta^9 \equiv \beta^4 + \beta^3$	(0, 0, 0, 1, 1, 0)
α^{10}	$\beta^{10} \equiv \beta^5 + \beta^4$	(0, 0, 0, 0, 1, 1)
α^{11}	$\beta^{11} \equiv \beta^5 + \beta + 1$	(1, 1, 0, 0, 0, 1)
α^{12}	$\beta^{12} \equiv \beta^2 + 1$	(1, 0, 1, 0, 0, 0)
α^{13}	$\beta^{13} \equiv \beta^3 + \beta$	(0, 1, 0, 1, 0, 0)
α^{14}	$\beta^{14} \equiv \beta^4 + \beta^2$	(0, 0, 1, 0, 1, 0)
α^{15}	$\beta^{15} \equiv \beta^5 + \beta^3$	(0, 0, 0, 1, 0, 1)
α^{16}	$\beta^{16} \equiv \beta^4 + \beta + 1$	(1, 1, 0, 0, 1, 0)
α^{17}	$\beta^{17} \equiv \beta^5 + \beta^2 + \beta$	(0, 1, 1, 0, 0, 1)
α^{18}	$\beta^{18} \equiv \beta^3 + \beta^2 + \beta + 1$	(1, 1, 1, 1, 0, 0)
α^{19}	$\beta^{19} \equiv \beta^4 + \beta^3 + \beta^2 + \beta$	(1, 1, 1, 1, 1, 0)
α^{20}	$\beta^{20} \equiv \beta^5 + \beta^4 + \beta^3 + \beta^2$	(0, 0, 1, 1, 1, 1)
α^{21}	$\beta^{21} \equiv \beta^5 + \beta^4 + \beta^3 + \beta + 1$	(1, 1, 0, 1, 1, 1)
α^{22}	$\beta^{22} \equiv \beta^5 + \beta^4 + \beta^2 + 1$	(1, 0, 1, 0, 1, 1)
α^{23}	$\beta^{23} \equiv \beta^5 + \beta^3 + 1$	(1, 0, 0, 1, 0, 1)
α^{24}	$\beta^{24} \equiv \beta^4 + 1$	(1, 0, 0, 0, 1, 0)
α^{25}	$\beta^{25} \equiv \beta^5 + \beta$	(0, 1, 0, 0, 0, 1)
α^{26}	$\beta^{26} \equiv \beta^2 + \beta + 1$	(1, 1, 1, 0, 0, 0)
α^{27}	$\beta^{27} \equiv \beta^3 + \beta^2 + \beta$	(0, 1, 1, 1, 0, 0)

Tabela D.1: (continuação) *Representação do corpo* $GF(2^6)$

α^{28}	$\beta^{28} \equiv \beta^4 + \beta^3 + \beta^2$	(0, 0, 1, 1, 1, 0)
α^{29}	$\beta^{29} \equiv \beta^5 + \beta^4 + \beta^3$	(0, 0, 0, 1, 1, 1)
α^{30}	$\beta^{30} \equiv \beta^4 + \beta + 1$	(1, 1, 0, 0, 1, 1)
α^{31}	$\beta^{31} \equiv \beta^5 + \beta^2 + 1$	(1, 0, 1, 0, 0, 1)
β^{32}	$\beta^{32} \equiv \beta^3 + 1$	(1, 0, 0, 1, 0, 0)
β^{33}	$\beta^{33} \equiv \beta^4 + \beta$	(0, 1, 0, 0, 1, 0)
β^{34}	$\beta^{34} \equiv \beta^5 + \beta^2$	(0, 0, 1, 0, 0, 1)
β^{35}	$\beta^{35} \equiv \beta^3 + \beta + 1$	(1, 1, 0, 1, 0, 0)
β^{36}	$\beta^{36} \equiv \beta^4 + \beta^2 + \beta$	(0, 1, 1, 0, 1, 0)
α^{37}	$\beta^{37} \equiv \beta^5 + \beta^3 + \beta^2$	(0, 0, 1, 1, 0, 1)
α^{38}	$\beta^{38} \equiv \beta^4 + \beta^3 + \beta + 1$	(1, 1, 0, 1, 1, 0)
α^{39}	$\beta^{39} \equiv \beta^5 + \beta^4 + \beta^2 + \beta$	(0, 1, 1, 0, 1, 1)
α^{40}	$\beta^{40} \equiv \beta^5 + \beta^3 + \beta^2 + \beta + 1$	(1, 1, 1, 1, 0, 1)
α^{41}	$\beta^{41} \equiv \beta^4 + \beta^3 + \beta^2 + 1$	(1, 0, 1, 1, 1, 0)
α^{42}	$\beta^{42} \equiv \beta^5 + \beta^4 + \beta^3 + \beta$	(0, 1, 0, 1, 1, 1)
α^{43}	$\beta^{43} \equiv \beta^5 + \beta^4 + \beta^2 + \beta + 1$	(1, 1, 1, 0, 1, 1)
α^{44}	$\beta^{44} \equiv \beta^5 + \beta^3 + \beta^2 + 1$	(1, 0, 1, 1, 0, 1)
α^{45}	$\beta^{45} \equiv \beta^4 + \beta^3 + 1$	(1, 0, 0, 1, 1, 0)
α^{46}	$\beta^{46} \equiv \beta^5 + \beta^4 + \beta$	(0, 1, 0, 0, 1, 1)
α^{47}	$\beta^{47} \equiv \beta^5 + \beta^2 + \beta + 1$	(1, 1, 1, 0, 0, 1)
α^{48}	$\beta^{48} \equiv \beta^3 + \beta^2 + 1$	(1, 1, 1, 0, 0, 0)
α^{49}	$\beta^{49} \equiv \beta^4 + \beta^3 + \beta$	(0, 1, 0, 1, 1, 0)
α^{50}	$\beta^{50} \equiv \beta^5 + \beta^4 + \beta^2$	(0, 0, 1, 0, 1, 1)
α^{51}	$\beta^{51} \equiv \beta^5 + \beta^3 + \beta + 1$	(1, 1, 0, 1, 0, 1)
α^{52}	$\beta^{52} \equiv \beta^4 + \beta^2 + 1$	(1, 0, 1, 0, 1, 0)
α^{53}	$\beta^{53} \equiv \beta^5 + \beta^3 + \beta$	(0, 1, 0, 1, 0, 1)
α^{54}	$\beta^{54} \equiv \beta^4 + \beta^2 + \beta + 1$	(1, 1, 1, 0, 1, 1)
α^{55}	$\beta^{55} \equiv \beta^5 + \beta^3 + \beta^2 + \beta$	(0, 1, 1, 1, 0, 1)
α^{56}	$\beta^{56} \equiv \beta^4 + \beta^3 + \beta^2 + \beta + 1$	(1, 1, 1, 1, 1, 0)
α^{57}	$\beta^{57} \equiv \beta^5 + \beta^4 + \beta^3 + \beta^2 + \beta$	(0, 1, 1, 1, 1, 1)
α^{58}	$\beta^{58} \equiv \beta^5 + \beta^4 + \beta^3 + \beta^2 + \beta + 1$	(1, 1, 1, 1, 1, 1)
α^{59}	$\beta^{59} \equiv \beta^5 + \beta^4 + \beta^3 + \beta^2 + 1$	(1, 0, 1, 1, 1, 1)
α^{60}	$\beta^{60} \equiv \beta^5 + \beta^4 + \beta^3 + 1$	(1, 0, 0, 1, 1, 1)
α^{61}	$\beta^{61} \equiv \beta^5 + \beta^4 + 1$	(1, 0, 0, 0, 1, 1)
α^{62}	$\beta^{62} \equiv \beta^5 + 1$	(1, 0, 0, 0, 0, 1)
α^{63}	$\beta^{63} \equiv 1$	(1, 0, 0, 0, 0, 0)