Polinômios Irredutíveis Sobre Corpos Finitos

Construção, Contagem e Estimativas Assintóticas

Tese de Doutorado

Departamento de Matemática
UNIVERSIDADE FEDERAL DE MINAS GERAIS

Lays Grazielle Cardoso Silva de Jesus

FEVEREIRO 2020

Polinômios Irredutíveis Sobre Corpos Finitos

Construção, Contagem e Estimativas Assintóticas

Lays Grazielle Cardoso Silva de Jesus

Departamento de Matemática
UNIVERSIDADE FEDERAL DE MINAS GERAIS

Tese submetida à banca examinadora, designada pelo Programa de Pós-Graduação em Matemática da UFMG, como requisito parcial para a obtenção do título de doutora em Matemática.

Orientador: Fabio Enrique Brochero Martínez

FEVEREIRO 2020

Ficha catalográfica elaborada pela bibliotecária Belkiz Inez Rezende Costa CRB 6ª Região nº 1510

Jesus, Lays Grazielle Cardoso Silva de.

J58p Polinômios irredutíveis sobre corpos finitos: construção, contagem e estimativas assintóticas/ Lays Grazielle Cardoso Silva de Jesus— Belo Horizonte, 2020.
vi, 61 f. il.; 29 cm.

Tese (doutorado) - Universidade Federal de Minas Gerais – Departamento de Matemática.

Orientador: Fábio Enrique Brochero Martinez.

1. Matemática - Teses. 2. Polinômios - Teses. 3. Corpos finitos (Álgebra) - Teses. I. Orientador. II. Título.

CDU 51(043)

Universidade Federal de Minas Gerais
Departamento de Matemática
Programa de Pós-Graduação em Matemática

FOLHA DE APROVAÇÃO

Polinômios Irredutíveis sobre corpos finitos: Construção, contagem e estimativas assintóticas

LAYS GRAZIELLE CARDOSO SILVA DE JESUS

Tese defendida e aprovada pela banca examinadora constituída pelos Senhores:

Prof. Fabio Enrique Brochero Martínez
UFMG

Prof. Herivelto Martins Borges Filho
USP

Prof. Lucas da Silva Reis
UFMG

Profa. Luciane Quoos Conte
UFRJ

Prof. Sávio Ribas
UFOP

Belo Horizonte, 28 de fevereiro de 2020.

Av. Antônio Carlos, 6627 – Campus Pampulha - Caixa Postal: 702
CEP-31270-901 - Belo Horizonte – Minas Gerais - Fone (31) 3409-5963
e-mail: pgmat@mat.ufmg.br - home page: http://www.mat.ufmg.br/pgmat

À memória da minha amada avó Maria Benita da Silva.
Aos meus sobrinhos Anderson, Emilly, Guilherme,
Kamilly e Maria Clara.
Aos meus afilhados Bruna e Valentim Gael

AGRADECIMENTOS

A cada dia somos desafiados a vencer dificuldades e nos superar diante dos atropelos da vida. Ser otimista, ter coragem de transformar os sonhos em realidade, além disso, poder contar com pessoas que nos dão palavras de carinho, coragem, que lutam e torcem pela sua felicidade é o que nos mantém de pé diante das adversidades. Eu tive a oportunidade de encontrar várias pessoas as quais foram luz para o meu caminho e tesouro para os meus dias.

Primeiramente, agradeço a Deus e a Nossa Senhora Aparecida. É difícil transmitir com palavras a fé que sinto, essa fé guiou os meus passos e abriu estradas e caminhos. Obrigada a minha mãe Nossa Senhora Aparecida por nunca me abandonar.

Um agradecimento especial a pessoa que para mim, é um exemplo de profissionalismo com quem eu aprendi muito, o meu orientador Fabio Enrique Brochero Matínez. Nunca vou-me esquecer dos seus preciosos conselhos, a sua humanidade e a confiança que depositou em mim. Muito obrigada!

Quando olhamos para o nosso lado e vemos alguém que está sempre presente, uma pessoa que lhe dedica muito amor e carinho, que nunca te deixa desanimar, só podemos ser gratos. Muito obrigada o meu amado marido Allan Ramos.

Agradeço também a minha mãe Lêda da Silva Cardoso essa uma mulher batalhadora, guerreira que nunca mediu esforços para que os seus filhos estudassem. É um exemplo para mim. Muito obrigada pelo carinho e amor que sempre dedicou a mim.

Gratidão, a minha família, os meus pais Leandro Epifânio de Jesus e Edson Antônio Dias, os meus irmãos Livia, Leticia, Lekyson e Ivan pelo carinho, amizade e apoio. Um obrigado especial a minha tia Elanie Rodrigues que com o seu jeito meigo de ser ajudou-me tanto.

O meu agradecimento carinhoso a família que tive a oportunidade de formar durante o doutorado: Aldo, Daniele, Diego, Franciele, Guido, Izabela, Jefferson, Lázaro, Leandro, Marlon, Mayara, Moacir, Mykael, Natã, Rafael, a amizade e o apoio de vocês tornaram essa caminhada mais prazerosa. Um agradecimento especial para a minha comadre, amiga e irmã Maria de Fátima que tanto me escutou e apoiou-me nos momentos difícieis.

O meu agradecimento sincero aos meus irmãos de orientador Lilian, Lucas, Sávio, Dani-

ela, Sobral e José pelas discussões prazerosas que tanto contribuíram para construção deste trabalho.
A minha gratidão a amiga e professora Carmem Giraldo pela amizade e conversas motivadoras.
O meu sincero agradecimento ao professor Eudes Antônio da Costa por ter-me motivada a iniciar essa longa caminhada.
A minha gratidão eterna ao meu grande amigo Silvestre da Cruz Monteiro pelo seu apoio, sem ele eu não teria tido a oportunidade de fazer este doutorado.
O meu muito obrigado aos meus amigos Regina e Marcelo que tanto me ajudaram nessa caminhada.
A Coordenação de Aperfeiçoamento de Pessoal de Nível Superior-Brasil(CAPES) pelo apoio. Código de Financiamento 001.
Por fim, manifesto aqui a minha gratidão a Universidade Federal de Roraima(UFRR) e a Universidade Federal de Minas Gerais(UFMG). Em especial, as secretárias do departamento de Matemática Andreia e Kelly que sempre foram tão solistas, muito obrigada!

RESUMO

Seja $\mathbb{F}_q$ um corpo finito com q elementos. Neste trabalho serão abordados essencialmente dois tipos de problemas sobre polinômios irredutíveis. O primeiro é a construção de polinômios irredutíveis a partir da composição de um polinômio irredutível com o polinômio x^n. Este é um problema particular de um problema mais geral sobre fatoração de polinômios irredutíveis, quando fazemos composição deste com um outro polinômio ao qual conhecemos totalmente sua fatoração. Em particular, neste trabalho, impondo algumas condições sobre q, n, a ordem e o grau do polinômio f, encontramos uma fatoração de $f(x^n)$, que pode ser implementada computacionalmente para determinar explicitamente os fatores irredutíveis desta composição. Além disso, no processo também é determinada uma fórmula explícita do número de fatores irredutíveis. Este resultado generaliza os resultados encontrados em [4], [29], [7] e [37].
Como consequência, no caso em que $f(x) = x - 1$, o número de fatores irredutíveis de $x^n - 1$ é também o número de elementos normais da extensão $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.
Na segunda parte do trabalho, restringimos nosso foco ao estudo de binômios irredutíveis, pois existe um critério de irredutibilidade clássico para este tipo de polinômio. Este critério foi explorado por Heyman e Shparlinski em [17] para determinar cotas superiores e inferiores para o número total de binômios sobre $\mathbb{F}_q$ de grau limitado por T, com T suficientemente grande. No trabalho deles, também são encontradas cotas superior e inferior para o número total de binômios de grau t sobre os corpos $\mathbb{F}_q$ quando q está limitado por uma constante Q, mas achamos que este tipo de estimativa não é muito interessante, pois são contados objetos que pertencem a corpos com características distintas. Assim, nesta segunda parte são determinadas fórmulas, que são assintoticamente corretas, para o número de binômios irredutíveis sobre $\mathbb{F}_q$ e de grau menor que T, melhorando substancialmente o resultado de Heyman e Shparlinski. Também são encontradas fórmulas para cotas superior e inferior que são válidas para valores pequenos de T.
Palavras Chaves: polinômios irredutíveis, polinômios ciclotômicos e corpos finitos.

ABSTRACT

Let $\mathbb{F}_q$ be a finite field with q elements. In this thesis, we focus on two types of problems about irreducible polynomials. The first one is the construction of irreducible polynomials from the composition of an irreducible polynomial with the polynomial x^n. This is a particular case of a more general problem about finding irreducible polynomial factorization, when it composes $f(x)$ with another polynomial to which its factorization is complete known. In particular, imposing some conditions on q, n, the order and the degree of the polynomial f, we find a procedure, which can be computationally implemented in order to determine explicitly the irreducible factors of this composition $f(x^n)$. In addition, an explicit formula for the number of irreducible factors is determined in the process. This result generalizes the results found in [4], [29], [7] and [37].
Consequently, in the case when $f(x) = x - 1$, the number of irreducible factors of $x^n - 1$ is also the number of normal elements of the extension $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.
In the second part this these, we restringe our study to irreducible binomials, because there is a classic irreducibility criterion for this type of polynomial. This criterion was explored by Heyman and Shparlinski in [17] to find upper and lower bounds for the total number of binomials over $\mathbb{F}_q$ with degree $t \leq T$, where T is large enough. In their work, they also find upper and lower bounds for the total number of irreducible binomials of degree t over the field $\mathbb{F}_q$ when q is limited by a constant Q, but we think that this type of estimate is not very interesting because they count objects that are belong fields with different characteristics. Thus, in this second part, we determine formulas, which are asymptotically correct, for the number of irreducible binomials over $\mathbb{F}_q$ and degree less than T. This formulas substantially improves the result of Heyman and Shparlinski. Also found formulas for upper and lower bounds that are valid for small values of T.
Keywords: irreducible polynomials, cyclotomic polynomials, finite fields.

TABELA DE CONTEÚDO

Página

INTRODUÇÃO

A fatoração de polinômios sobre corpos finitos desempenha um papel importante em uma ampla variedade de situações tecnológicas, entre elas podemos citar os códigos de correção de erros assim como alguns sistemas criptográficos. Observamos que todo código cíclico linear de comprimento n pode ser representado por um ideal do anel $\frac{\mathbb{F}_q[x]}{(x^n-1)}$, onde $\mathbb{F}_q$ é um corpo finito com q elementos. Além disso, todo ideal pode ser gerado por um fator de x^n-1 em $\mathbb{F}_q[x]$. A fatoração x^n-1 quando n é uma potência de 2 suficientemente grande e $q \equiv 1 \pmod 4$ é consequência direta do Teorema 3.35 em [26], e neste caso basta encontrar os fatores irredutíveis de $x^{2^a}+1$, onde $a = \nu_2(q-1)$. Os primeiros trabalhos sobre os fatores irredutíveis de x^n+1, onde n é um potência de 2 e $q \equiv 3 \pmod 4$, podem ser encontrados em [4] e [29].

Em uma série de artigos posteriores, vários autores estudaram a fatoração de $x^{2^l m}-1$, com m sobre uma família bem restrita de valores tais como m potência de um primo que divide $q-1$ ([12]) , m produto de dois primos que divide $q-1$ ([25]). Nos trabalhos [7], [8], os autores determinam totalmente a fatoração de x^n-1 quando todo divisor primo de n divide $q-1$. Neste caso os fatores irredutíveis sempre são binômios ou trinômios, desta forma são encontradas famílias infinitas de binômios e trinômios irredutíveis. Finalmente em [37], Wu, Yue e Fan consideram a fatoração deste mesmo polinômio no caso que todo divisor primo de n divide q^s-1, onde s é um número primo.

Aplicações dos resultados anteriores podem ser encontrado em [24], onde os autores determinam todos os códigos cíclicos lineares minimais para uma família infinita de comprimento n, e em [31] onde o autor mostrar que se todo divisor primo de n divide $p(q-1)$, então existe elemento k-normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ para todo $1 \leq k \leq n$.

Um dos objetivos deste trabalho é fornecer a fatoração do polinômio $f(x^n)$ onde f é um polinômio irredutível, impondo algumas condições sobre a ordem e o grau de f, que são satisfeitas trivialmente no caso que $f(x) = x-1$. Além disso, são encontradas fórmulas explícitas em cada caso, para o número de fatores irredutíveis de $f(x^n)$. Esta fórmula é usada no C71orolário 2.21 para estimar a densidade mínima de elementos normais para uma família infinita de extensões do corpo $\mathbb{F}_q$.

Um segundo objetivo deste trabalho é estimar o número de binômios irredutíveis de grau $t \leq T$. Este tipo de problema foi inicialmente estudado por Heyman e Shparlinski em [17], onde os autores estimam em média o número total de binômios irredutíveis em termos de q ou t. A prova de seus resultados fazem uso de resultados fortes de teoria analítica dos números, principalmente resultados relativos à distribuição de números primos em progressões aritméticas. Em nosso trabalho, fixado q, encontramos de forma elementar cotas assintóticas exatas para o número de binômios irredutíveis de grau menor ou igual a T, assim como encontramos cotas superiores e inferiores no caso que T seja relativamente pequeno.

Esta tese está organizada da seguinte forma: No primeiro capítulo apresentamos uma breve revisão de resultados conhecidos que serão necessários para o desenvolvimento do nosso trabalho.

No segundo capítulo, considerando $f \in \mathbb{F}_q[x]$ um polinômio irredutível de grau k, ordem $\mathfrak{e}$ e impondo algumas condições sobre n que tornam o polinômio $f(x^n)$ redutível, discutimos a fatoração de $f(x^n)$ sobre $\mathbb{F}_q$. As condições impostas sobre n são uma generalização das condições imposta pelos autores em [7] e [37].

No terceiro capítulo, obtemos a ordem "exata"para ordem média do número de binômios irredutíveis da forma $x^t - a$ com $a \in \mathbb{F}_q$ em $\mathbb{F}_q[x]$ quando limitamos o valor de t. Este resultado melhora o resultado apresentado por Heyman e Shparlinski em [17]. Em particular, é mostrado que o numero de binômios de grau menor que T, se comporta assintoticamente com a função $C(\log T)^s$, onde C é uma constande adequada e s é o número de divisores primos de $\frac{q-1}{2}$, se $q \equiv 3 \pmod 4$, e o número de divisores primos de $q-1$ em outro caso (Corolário 3.8 página 53). Por fim, fornecemos uma cota inferior e superior para o número de binômios irredutíveis quando T não é necessariamente um número muito grande.

CAPÍTULO 1

PRELIMINARES

Neste capítulo, apresentaremos alguns fatos relevantes sobre a teoria de corpos finitos, isto é, um corpo com um número finito de elementos. Tais resultados serão necessários no desenvolvimento dos capítulos posteriores. Devido a maioria desses resultados serem conhecidos, muitos deles serão apresentados aqui sem demonstração. Para um estudo mais aprofudando destes resultados o leitor pode consultar o livro de Lidl e Niederreiter [26], que é principal referência deste capítulo.

1.1 Caracterização de Corpos Finitos

Neste trabalho, p sempre denotará um número primo. É conhecido que o anel dos inteiros módulo n é um corpo se, e somente se, n é um número primo. Neste caso o anel de classes $\mathbb{Z}_p$ é um corpo que também será denotado por $\mathbb{F}_p$. Dados dois corpos finitos $\mathbb{L}$ e $\mathbb{K}$ com q elementos, será mostrado que eles são isomorfos (Observação 1.5), o que nos permite denotar tais corpos por $\mathbb{F}_q$.

Seja $\mathbb{K}$ um corpo que contém o corpo $\mathbb{F}_q$. Ignorando a estrutura multiplicativa de $\mathbb{K}$, podemos olhar para $\mathbb{K}$ como um $\mathbb{F}_q$-espaço vetorial de dimensão finita. De fato:

Teorema 1.1. *Seja $\mathbb{K}$ um corpo finito e $\mathbb{F}_q$ um subcorpo de $\mathbb{K}$ contendo q elementos. Então $\mathbb{K}$ possui q^m elementos, onde m é a dimensão do espaço vetorial $\mathbb{K}$ sobre $\mathbb{F}_q$.*

Observação 1.2. *Denotaremos a dimensão do espaço vetorial $\mathbb{K}$ sobre o corpo $\mathbb{F}$ por $[\mathbb{K} : \mathbb{F}]$.*

Um invariante fundamental dos corpos finitos é sua característica.

Definição 1.3. *A característica de um corpo $\mathbb{K}$ é o menor inteiro positivo n tal que $n \cdot a = 0$ para cada $a \in \mathbb{K}$. Quando este n não existir, dizemos que a característica do corpo é zero.*

É possível mostrar, a partir da minimalidade da característica de um corpo, que ela ou é um número primo ou é zero e portanto, se p é a característica do corpo finito $\mathbb{F}_q$ e $a, b \in \mathbb{F}_q$ são elementos arbitrários então

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

Seja $f(x) \in \mathbb{F}[x]$ um polinômio não constante e $b \in \mathbb{F}$ seu coeficiente líder. Chamamos de corpo de decomposição do polinômio $f(x)$, o menor corpo $\mathbb{K}$ que contém $\mathbb{F}$ tal que existem elementos $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathbb{K}$ satisfazendo

$$f(x) = b(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n).$$

O corpo de decomposição de um polinômio sempre existe e é único a menos de isomorfismo ([26], Teorema 1.91).

Seja $\mathbb{K}$ um corpo com q elementos e característica p. Se $1 \in \mathbb{K}$ é o elemento neutro com respeito a multiplicação então o conjunto $\{0, 1, 2 \cdot 1, \cdots, (p-1) \cdot 1\}$ forma um corpo contido em $\mathbb{K}$. Este corpo é chamado de *subcorpo primo* de $\mathbb{K}$, que é o menor corpo contido em $\mathbb{K}$.

Se a ordem do corpo finito não é um número primo então, essa ordem é necessariamente uma potência de um primo, mais especificamente temos o seguinte resultado

Teorema 1.4. *Existem corpos de ordem q se, e somente se, q é uma potência de primo.*

Demonstração. Seja $\mathbb{F}_q$ um corpo com q elementos, então $\mathbb{F}_q$ possui característica prima p. Tomando $\mathbb{E}$ um subcorpo primo de $\mathbb{F}_q$ temos que $\mathbb{E}$ é isomorfo ao corpo $\mathbb{Z}_p$, portanto contém p elementos e segue do Teorema 1.1 que $q = p^n$, onde $n = [\mathbb{F}_q : \mathbb{E}]$.

Reciprocamente, tomemos $q = p^n$ e consideremos F o corpo de decomposição do polinômio $f(x) = x^q - x \in \mathbb{F}_p[x]$. Como $f^{'}(x) = -1$ o polinômio f possui q raízes distintas, Teorema1.7. Seja $S = \{a \in F; a^q - a = 0\}$ o conjunto cujos os elementos são raízes do polinômio f. Observemos que

- $0, 1 \in S$
- Para quaisquer $a, b \in S$ temos que $(a-b)^q = a^q - b^q = a - b$ logo, $a - b \in S$
- Para quaisquer $a, b \in S$ com $b \neq 0$ temos que $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$ o que implica que $ab^{-1} \in S$.

Portanto, S é um subcorpo de F. Por outro lado, S contém todas as raízes de f assim, $F = S$ ou seja F é um corpo finito com q elementos. ■

Observação 1.5. *Segue da prova do resultado anterior que, a menos de isomorfismo um corpo finito com q elementos é único, pois este é o corpo de decomposição do polinômio* $x^q - x$.

Como $\mathbb{F}_q$ é o corpo de decomposição do polinômio $x^q - x$, temos que se $a \in \mathbb{F}_q$ então $a^q = a$. No caso que $a \neq 0$ segue que $a^{q-1} = 1$, isto é, $(\mathbb{F}_q^*, \cdot)$ é um grupo multiplicativo com $q-1$ elementos. Pode ser mostrado que este grupo é ciclíco ([26], Teorema 2.8).

1.2 Raízes e Polinômios Irredutíveis

Seja $\mathbb{F}$ um corpo qualquer e $f(x) \in \mathbb{F}[x]$ um polinômio não constante. Dizemos que $f(x)$ é irredutível sobre $\mathbb{F}$ se não é possível escrevê-lo como produto de dois polinômios não constantes.

Definição 1.6. *Seja* $\alpha \in \mathbb{F}$ *uma raiz do polinômio* $f \in \mathbb{F}[x]$ *e k um inteiro positivo. Dizemos que* α *é uma raiz de multiplicidade k do polinômio* $f(x)$*, se* $f(x)$ *é divisível por* $(x-\alpha)^k$*, mas não é divisível por* $(x-\alpha)^{k+1}$*. No caso* $k = 1$*, a raiz* α *é chamada de raiz simples e se* $k \geq 2$ *dizemos que a raiz* α *é uma raiz múltipla.*

A caracterização de raiz múltipla é dada pelo seguinte resultado.

Teorema 1.7. *Um elemento* $\alpha \in \mathbb{F}$ *é uma raiz múltipla de* $f \in \mathbb{F}[x]$ *se, e somente se, é raiz dos polinômio* $f(x)$ *e da sua derivada* $f'(x)$*.*

Seja $\mathbb{F}$ um subcorpo de $\mathbb{K}$, $f(x) \in \mathbb{F}[x]$ e $\alpha \in \mathbb{K}$. Se α é raiz do polinômio $f(x)$, isto é, $f(\alpha) = 0$ dizemos que α é algébrico sobre o corpo $\mathbb{F}$. Quando cada elemento de $\mathbb{K}$ é algébrico sobre $\mathbb{F}$ dizemos que $\mathbb{K}$ é uma extensão algébrica de $\mathbb{F}$.

Suponhamos que $\alpha \in \mathbb{K}$ é algébrico sobre $\mathbb{F}$ e consideremos o conjunto

$$J = \{f \in \mathbb{F}[x]; f(\alpha) = 0\}.$$

Notemos que J é um ideal de $\mathbb{F}[x]$ e sendo $\alpha \in \mathbb{K}$ algébrico sobre $\mathbb{F}$ temos que $J \neq (0)$. Como todo ideal de $\mathbb{F}[x]$ é principal, existe um único polinômio mônico $g(x) \in \mathbb{F}[x]$ tal que $J = \langle g(x) \rangle$. Observe que o polinômio $g(x)$ é irredutível sobre $\mathbb{F}[x]$, pois se $g(x) = h_1(x)h_2(x)$ com $1 \leq gr(h_i(x)) < gr(g(x))$, $(i = 1,2)$ então $0 = g(\alpha) = h_1(\alpha)h_2(\alpha)$ o que implica que $h_1(\alpha) = 0$ ou $h_2(\alpha) = 0$, logo $h_1 \in J$ ou $h_2 \in J$ e consequentemente $h_1 = g.f_1$ ou $h_2 = g.f_2$ o que é impossível. Portanto $g(x)$ o gerador do ideal J é um polinômio irredutível.

Definição 1.8. *O único polinômio mônico que gera o ideal* $J = \{f \in \mathbb{F}[x]; f(\alpha) = 0\}$ *de* $\mathbb{F}[x]$ *é chamado de polinômio minimal de* α *sobre* $\mathbb{F}$*, e como mostrado anteriormente, o polinômio minimal é irredutível.*

Observação 1.9. *Seja* $\alpha \in \mathbb{K}$ *algébrico sobre* $\mathbb{F}$ *e* $g(x)$ *seu polinômio minimal. Para* $f(x) \in \mathbb{F}[x]$ *temos que*

$$f(\alpha) = 0 \text{ se, e somente se, } g(x) \text{ divide } f(x).$$

Segue da definição de polinômio minimal e da observação acima que

Proposition 1.10. *Seja* $f(x) \in \mathbb{F}_q[x]$ *um polinômio irredutível sobre o corpo finito* $\mathbb{F}_q$ *e* α *uma raiz de* $f(x)$ *em alguma extensão do corpo* $\mathbb{F}_q$*. Então para um polinômio* $h(x) \in \mathbb{F}_q[x]$ *temos que* $h(\alpha) = 0$ *se, e somente se,* $f(x)$ *divide* $h(x)$*.*

Seja $f \in \mathbb{F}_p[x]$ um polinômio irredutível sobre $\mathbb{F}_p$ de grau n, então $\frac{\mathbb{F}_p[x]}{(f)}$ é um corpo com $q = p^n$ elementos. Desta forma, polinômios irredutíveis de mesmo grau fornecem representações isomorfas do mesmo corpo. Assim, encontrar polinômios irredutíveis com algumas características especiais como, por exemplo, poucos monômios distintos de zero, darão representações computacionamente mais simples. A existência deste tipo de polinômios irredutíveis com características especiais explica o interesse de muitos pesquisadores em questões envolvendo polinômios irredutíveis.

Exemplo 1.11. *Seja* $\mathbb{F}_{11}$ *um corpo com onze elementos. Seja* $f(x) = x^2 - a \in \mathbb{F}_{11}[x]$ *um polinômio onde* $a \in \mathbb{F}_{11}^*$ *é um gerador do grupo cíclico* $\mathbb{F}_{11}^*$*. Observemos que* $f(x)$ *é irredutível em* $\mathbb{F}_{11}[x]$*, pois do contrário teríamos a seguinte fatoração,* $(x-b)(x+b)$ *sobre* $\mathbb{F}_{11}$*, com* $b \in \mathbb{F}_{11}$ *e* $b^2 = a$ *o que implica que* $b^{10} = (b^2)^{\frac{10}{2}} = a^{\frac{10}{2}} = 1$*, absurdo uma vez que a gera o grupo multiplicativo* $\mathbb{F}_{11}^*$*. Tomando*

$$\mathbb{K} := \frac{\mathbb{F}_{11}[x]}{(x^2 - a)},$$

pode se verificar que $\mathbb{K}$ *é um anel comutativo com unidade. Afirmamos que* $\mathbb{K}$ *é um corpo. De fato, tomemos* $\overline{g(x)} \in \mathbb{K} \setminus \{\overline{0}\}$*, como* $x^2 - a$ *é irredutível sobre* $\mathbb{F}_{11}$ *temos que* $\text{mdc}(g(x), x^2 - a) = 1$ *e segue do Teorema de Bézout que existem* $h_1(x), h_2(x) \in \mathbb{F}_{11}[x]$ *tais que* $h_1(x)g(x) + h_2(x)(x^2 - a) = 1$*. Logo* $\overline{h_1(x)g(x) + h_2(x)(x^2 - a)} = \overline{h_1(x)g(x)} = \overline{1}$ *em* $\mathbb{K}$*. Assim,* $\overline{h_1(x)} = \overline{g(x)}^{-1}$*, ou seja, todo elemento de* $\mathbb{K} \setminus \{\overline{0}\}$ *admite inverso. Portanto,* $\mathbb{K}$ *é um corpo. Como os elementos de* $\mathbb{K}$ *são da forma* $\overline{ax + b}$ *com* $a, b \in \mathbb{F}_{11}$ *temos que* $\mathbb{K}$ *é um corpo com* $11^2 = 121$ *elementos.*

Definição 1.12. *Seja $\mathbb{F}_{q^n}$ uma extensão do corpo $\mathbb{F}_q$ e $\alpha \in \mathbb{F}_{q^n}$. Os elementos $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}$ são chamados conjugados de α com respeito a $\mathbb{F}_q$.*

Agora, expomos um resultado fundamental sobre polinômios irredutíveis cuja sua importância ficará clara no decorrer do trabalho.

Teorema 1.13. *Se $f \in \mathbb{F}_q[x]$ é um polinômio irredutível de grau n, então f possui uma raiz $\alpha \in \mathbb{F}_{q^n}$; além disso, todas as raízes de f são simples e dadas pelos n elementos distintos $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}$ de $\mathbb{F}_{q^n}$.*

Segue do resultado acima que cada extensão finita $\mathbb{F}_{q^n}$ de um corpo finito $\mathbb{F}_q$ é uma extensão normal e além disso, como cada polinômio irredutível sobre um corpo finito possui apenas raízes simples, temos que cada corpo finito é um corpo perfeito.

Seja $\alpha \in \mathbb{F}_{q^n}$. Quando $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}$ são linearmente indepedentes sobre $\mathbb{F}_q$, isto é, quando o conjunto $B = \{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}\}$ constituído de todos os conjugados de $\alpha \in \mathbb{F}_{q^n}$ forma uma base para $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, dizemos que B é uma base normal e $\alpha \in \mathbb{F}_{q^n}$ é chamado elemento normal sobre $\mathbb{F}_q$.

Observemos que em geral as raízes do polinômio irredutível não são necessariamente linearmente independentes sobre $\mathbb{F}_q$, como pode ser visto no seguinte exemplo.

Exemplo 1.14. *Seja α uma raiz do polinômio $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Como $f(x)$ é irredutível sobre $\mathbb{F}_2$ temos que $\alpha \in \mathbb{F}_{2^4}$ e as demais raízes são os conjungados de α, isto é,*

$$\alpha^2,\ \alpha^4 = \alpha + 1,\ \alpha^8 = \alpha^2 + 1.$$

Uma vez que, $\alpha + \alpha^2 + \alpha^4 + \alpha^8 = \alpha + \alpha^2 + (\alpha + 1) + (\alpha^2 + 1) = 0$ em $\mathbb{F}_2$ temos que $\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$ não são linearmente independentes.

Teorema 1.15. *Um conjungado de $\alpha \in \mathbb{F}_q^*$ com respeito a qualquer subcorpo de $\mathbb{F}_q$ possui a mesma ordem de α no grupo multiplicativo $\mathbb{F}_q^*$.*

Consideremos a extensão $\mathbb{F}_{q^n}$ do corpo finito $\mathbb{F}_q$ e definimos a aplicação

$$\begin{array}{rccc} \sigma_q : & \mathbb{F}_{q^n} & \longrightarrow & \mathbb{F}_{q^n} \\ & \alpha & \longmapsto & \alpha^q. \end{array}$$

Note que σ_q é um morfismo de corpos sobre $\mathbb{F}_q$ o qual chamamos de automorfismo de Frobenius de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Em outras palavras, o automorfismo de Frobenius de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é um automorfismo de $\mathbb{F}_{q^n}$ que fixa os elementos de $\mathbb{F}_q$.

De igual forma, por abuso de notação denotaremos por σ_q o automorfismo sobre o anel de polinômios $\mathbb{F}_q[x]$, onde aplicamos o automorfismo de Frobenius sobre os coeficientes de $f(x)$, isto é, se

$$f(x) = a_0 + a_1(x) + \cdots + a_n x^n \in \mathbb{F}_{q^n}[x] \text{ então } \sigma_q(f(x)) = \sigma_q(a_0) + \sigma_q(a_1)x + \cdots + \sigma_q(a_n)x^n$$

O teorema seguinte mostra que existe uma relação entre os conjugados de $\alpha \in \mathbb{F}_{q^n}$ e os automorfismos de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Teorema 1.16. *Os automorfismos distintos de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ são exatamente as aplicações $\sigma_q^0, \sigma_q^1, \cdots, \sigma_q^{n-1}$ definidas por $\sigma_q^j(\alpha) = \alpha^{q^j}$ para $\alpha \in \mathbb{F}_{q^n}$ e $0 \leq j \leq n-1$.*

Seja T uma transformação linear em um espaço vetorial V de dimensão finita sobre um corpo arbitrário $\mathbb{F}$. Recordemos que um polinômio $f(x) = \sum_{i=1}^{m} a_i x^i \in \mathbb{F}[x]$ é aniquilado pela transformação linear T se

$$a_0 I + a_1 T + \cdots + a_m T^m = 0,$$

onde I é a transformação identidade. O polinômio mônico de menor grau que aniquila T é chamado de polinômio minimal de T. Em particular, o polinômio minimal da transformação linear T divide o polinômio característico $g(x)$ da transformação linear T o qual é dado por $g(x) = \det(xI - T)$ cujo grau é igual à dimensão do espaço vetorial V sobre o corpo $\mathbb{F}$. Recordemos ainda que, um vetor $v \in V$ é dito um vetor cíclico para a transformação linear T quando os vetores $T^k(v)$ para $k = 0, 1, ...$ geram o espaço vetorial V. É conhecido o seguinte resultado.

Teorema 1.17. *Seja V um espaço vetorial de dimensão finita e $T : V \to V$ um operador linear. Então T possui um vetor cíclico se, e somente se, os polinômios característico e minimal para T são iguais.*

Da definição de σ_q temos que σ_q é uma transformação linear do espaço vetorial de dimensão finita $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Tomemos $\alpha \in \mathbb{F}_{q^n}$ então $\sigma_q^n(\alpha) = \alpha^{q^n} = \alpha$. Assim $\sigma_q^n - I = 0$ e o polinômio $x^n - 1$ é aniquilado por σ_q. Portanto, o polinômio minimal de σ_q divide o polinômio $x^n - 1$. Afirmamos que o polinômio minimal de σ_q é o polinômio $x^n - 1$. De fato, assumindo que existe um polinômio $f(x) = \sum_{i=1}^{n-1} a_i \sigma_q^i \in \mathbb{F}_q[x]$ de grau menor que n que aniquila σ_q, isto é,

$$\sum_{i=1}^{n-1} a_i \sigma_q^i = 0,$$

então para qualquer $\alpha \in \mathbb{F}_{q^n}$ temos que

$$0 = \left(\sum_{i=1}^{n-1} a_i \sigma_q^i \right) \alpha = \sum_{i=1}^{n-1} a_i \alpha^{q^i}.$$

Logo, o polinômio $F(x) = \sum_{i=1}^{n-1} a_i x^{q^i}$ possui q^n raízes, o que é impossível uma vez que grau de $F(x)$ é menor ou igual a q^{n-1}. Portanto o polinômio de menor grau que aniquila σ_q é o polinômio $x^n - 1$, ou seja, $x^n - 1$ é o polinômio minimal da transformação linear σ_q e, sendo o polinômio característico um polinômio mônico de grau n que divide o polinômio minimal, ele coincide com o polinômio $x^n - 1$. Segue do Teorema 1.17 que existe um $\alpha \in \mathbb{F}_{q^n}$ tal que $\alpha, \sigma_q(\alpha), \sigma_q^2(\alpha), \ldots, \sigma_q^{n-1}(\alpha)$ gera o corpo $\mathbb{F}_{q^n}$ e portanto forma uma base para $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Como esta base consiste de $\alpha \in \mathbb{F}_{q^n}$ e seus conjugados, temos que $\alpha \in \mathbb{F}_{q^n}$ é um elemento normal e temos o seguinte resultado.

Teorema 1.18 (Teorema da Base Normal)**.** *Para qualquer corpo finito $\mathbb{F}_q$ e qualquer extensão $\mathbb{F}_{q^n}$ do corpo $\mathbb{F}_q$, existe uma base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.*

O teorema acima garante a existência de elemento normal, ou seja, dada qualquer extensão $\mathbb{F}_{q^n}$ do corpo finito $\mathbb{F}_q$ sempre vai existir pelo menos um elemento $\alpha \in \mathbb{F}_{q^n}$ tal que α e seus conjugados forma uma base para o espaço vetorial $\mathbb{F}_{q^n}$ sobre o corpo $\mathbb{F}_q$. A questão é determinar quando $\alpha \in \mathbb{F}_{q^n}$ e seus conjugados com respeito ao corpo $\mathbb{F}_q$ são linearmente independentes. Isso passa pela aplicação direta do seguinte teorema.

Teorema 1.19. *([26], Corolário 2.38) Sejam $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_{q^n}$. Então $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ é uma base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ se, e somente se,*

$$det \begin{bmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_n^q \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{q^{n-1}} & \alpha_2^{q^{n-1}} & \cdots & \alpha_n^{q^{n-1}} \end{bmatrix} \neq 0.$$

Segue do Teorema 1.19 que, um elemento $\alpha \in \mathbb{F}_{q^n}$ gera uma base normal se, e somente se, a matriz

$$B = \begin{bmatrix} \alpha & \alpha^q & \cdots & \alpha^{q^{n-1}} \\ \alpha^q & \alpha^{q^2} & \cdots & \alpha \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{q^{n-1}} & \alpha & \cdots & \alpha^{q^{n-2}} \end{bmatrix}$$

é não singular.

Para continuar precisaremos da seguinte proposição que pode ser encontrada em [14].

Proposition 1.20. *Seja $\mathbb{K}$ um corpo. Para quaisquer $a_0, a_1, \ldots, a_{n-1} \in \mathbb{K}$ a matriz circulante $n \times n$*

$$c[a_0, a_1, \ldots, a_{n-1}] = \begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & \cdots & a_{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{bmatrix}$$

é não singular se, e somente se, os polinômios $\sum_{i=0}^{n-1} a_i x^i$ e $x^n - 1$ são relativamente primos.

Note que, se invertermos as ordens das linhas da matriz B a partir da segunda linha da seguinte forma: A segunda linha com a última linha, a terceira linha coma penúltima linha e assim por diante, obtemos a matriz circulante $c[\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}]$ e, pelo Lema 1.20 esta é não singular se, e somente se, os polinômios $\alpha^{q^{n-1}} x^{n-1} + \cdots + \alpha^q x + \alpha$ e $x^n - 1$ são relativamente primos e, temos a seguinte caracterização para elementos normais.

Teorema 1.21. *Seja $\alpha \in \mathbb{F}_{q^n}$, α gera uma base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ se, e somente se, os polinômios $\sum_{i=0}^{n-1} \alpha^{q^i} x^i$ e $x^n - 1$ são relativamente primos.*

Exemplo 1.22. *Seja α uma raiz do polinômio $f(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$. Como $f(x)$ é irredutível em $\mathbb{F}_2$ segue do Teorema 1.13 que $\alpha \in \mathbb{F}_8$ e as demais raízes são*

$$\alpha_2 := \alpha^2 = \alpha^3 + 1 \in \mathbb{F}_8 \ \ e \ \ \alpha_3 := \alpha^4 = \alpha \cdot \alpha^3 = \alpha \cdot (\alpha^2 + 1) = \alpha^3 + \alpha = \alpha^2 + \alpha + 1 \in \mathbb{F}_8$$

e temos que

$$det \begin{bmatrix} \alpha & \alpha^2 & \alpha^4 \\ \alpha^2 & \alpha^4 & \alpha \\ \alpha^4 & \alpha & \alpha^2 \end{bmatrix} = 1.$$

Portanto, $\{\alpha, \alpha^2, \alpha^4\} = \{\alpha, \alpha^2, \alpha^2 + \alpha + 1\}$ forma uma base para espaço vetorial $\mathbb{F}_8$ sobre o corpo $\mathbb{F}_2$, o que implica que $\alpha \in \mathbb{F}_8$ é um elemento normal sobre $\mathbb{F}_2$.

Observamos que o Teorema anterior caracteriza totalmente os elementos normais de uma extensão, mas ele não nos permite determinar de forma direta, quantos elementos normais tem uma extensão. Para essa contagem, precisaremos de alguns resultados e definições que serão dadas a seguir.

Definição 1.23. *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio de grau n. Denotaremos por $\Phi_q(f)$ o número de polinômios em $\mathbb{F}_q[x]$ de grau menor que n que são relativamente primos com f. A função $\Phi_q(f)$ é chamada Função Φ de Euler para polinômios sobre corpos finitos.*

Proposition 1.24. *Sejam $f, g \in \mathbb{F}_q[x]$ polinômios não nulos. Se* $\mathrm{mdc}(f,g) = 1$ *então $\Phi_q(fg) = \Phi_q(f)\Phi_q(g)$.*

Observe que o Teorema 1.21 relaciona elementos normais e um tipo especial de polinômios primos relativos com $x^n - 1$, mas os polinômios desta forma construídos não estão em $\mathbb{F}_q[x]$. Assim, de forma imediata não podemos relacioná-los com os polinômios primos com $x^n - 1$ em $\mathbb{F}_q$. De fato estes polinômios estão relacionados, como pode ser verificado no seguinte teorema.

Teorema 1.25. *(Teorema 3.73 [26]) Em $\mathbb{F}_{q^n}$ existem exatamente $\Phi_q(x^n - 1)$ elementos α tal que $\{\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}\}$ é uma base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.*

A função $\Phi_q(f)$ depende essencialmente da fatoração de f em fatores irredutíveis. De fato, se $f(x) \in \mathbb{F}_q[x]$ é um polinômio irredutível de grau $n \geq 1$ então $\Phi_q(f) = q^n - 1$. Se $h(x) \in \mathbb{F}_q[x]$ é um polinômio cujo grau é menor que o grau do polinômio $(f(x))^l$, onde $l \in \mathbb{Z}_+$, e não relativamente primo com $(f(x))^l$, então $f(x)|h(x)$ e portanto $h(x) = f(x)g(x)$ com $gr(g(x)) < ln - n = n(l-1)$. Logo existem q^{ln-n} escolhas para $g(x)$ e daqui concluímos que $\Phi_q\left((f(x))^l\right) = q^{nl} - q^{n(l-1)} = q^{nl}\left(1 - \frac{1}{q^n}\right)$. Finalmente, se $f(x) = f_1^{l_1} f_2^{l_2} \cdots f_s^{l_s}$ é a fatoração de f em fatores irredutíveis distintos, isto é, os f_j são polinômios irredutíveis distintos de grau n_j, segue da Proposição 1.24 que :

$$\Phi_q(f) = q^n(1 - q^{-n_1}) \cdots (1 - q^{-n_r}). \tag{1.1}$$

Desta forma, para determinar o número de elementos normais de uma extensão de grau n, é suficiente determinar os fatores irredutíveis de $x^n - 1$ em $\mathbb{F}_q$.

1.3 Polinômios Ciclotômicos

Seja $\mathbb{K}$ um corpo de característica p e $g(x) = x^n - 1 \in \mathbb{K}[x]$. As raízes do polinômio $g(x)$ são chamadas raízes n-ésimas da unidade. Denotamos por E^n o conjunto de todas as raízes do polinômio $g(x)$. A multiplicação definida em $\mathbb{K}$ induz no conjunto E^n uma estrutura de grupo. Além disso, se $n = p^e m$ com $p \nmid m$, então E^n possui m elementos. Se $p \nmid n$ esse

grupo é cíclico e o gerador deste grupo é chamado de raiz n- ésima primitiva da unidade sobre $\mathbb{K}$

Seja n um inteiro positivo tal que $\text{mdc}(n,q)=1$ e $\alpha \in \overline{\mathbb{F}}_q$ uma raiz n-ésima primitiva da unidade. O polinômio

$$\Phi_n(x) = \prod_{\substack{s=1 \\ \text{mdc}(s,n)=1}}^{n} (x-\alpha^s)$$

é chamado n-ésimo polinômio ciclotômico sobre $\mathbb{F}_q$.

Afirmamos que

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

De fato, suponhamos que β é uma raiz arbitrária de $\Phi_d(x)$, logo β é uma raiz d-ésima primitiva da unidade e desta forma $\beta^d = 1$. Como $d \mid n$ segue que β é raiz de x^n-1, o que implica que $\Phi_d(x)$ divide x^n-1, pois $\Phi_d(x)$ possui apenas raízes simples. Além disso, como o $\text{mdc}(\Phi_{d_1}(x), \Phi_{d_2}(x)) = 1$ para todo $d_1 \neq d_2$, pois um elemento não pode ter duas ordens distintas, segue que

$$\prod_{d|n} \Phi_d(x) \text{ divide } x^n - 1.$$

Por outro lado, x^n-1 tem apenas raízes simples, pois $\text{mdc}(n,q)=1$ e se β é uma raiz de x^n-1, então $\beta^n = 1$ o que implica que $d := \text{ord}(\beta) \mid n$, assim β é uma raiz de $\Phi_d(x)$. Logo toda raiz de x^n-1 é raiz do produto $\prod_{d|n} \Phi_d(x)$. Portanto

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \tag{1.2}$$

Segue da Equação 1.2 que

- $\Phi_1(x) = x-1$
- $\Phi_1(x)\Phi_2(x) = x^2-1 \Rightarrow \Phi_2(x) = x+1$
- $\Phi_1(x)\Phi_3(x) = x^3-1 \Rightarrow \Phi_3(x) = x^2+x+1$

procedendo dessa forma podemos obter recursivamente todos os polinômios ciclotômicos a partir da fórmula

$$\Phi_n(x) = \frac{x^n-1}{\prod\limits_{\substack{d|n \\ d\neq n}} \Phi_d(x)}. \tag{1.3}$$

Além disso, se denotamos por $f(n)$ o grau de $\Phi_n(x)$, da Equação 1.2 obtemos a relação entre os graus $n = \sum_{d|n} f(d)$ e aplicando a fórmula de inversão de Möbius obtemos que

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d.$$

Como a função identidade é multiplicativa, segue que f também é multiplicativa e está determinada por seus valores em potência de primos.

$$f(\mathfrak{p}^k) = \sum_{d|\mathfrak{p}^k} \mu\left(\frac{\mathfrak{p}^k}{d}\right) d = \sum_{j=0}^{k} \mu(\mathfrak{p}^{k-j})\mathfrak{p}^j = \mathfrak{p}^k - \mathfrak{p}^{k-1} = \varphi(\mathfrak{p}^k),$$

onde $\mathfrak{p}$ é um primo que divide n. Desta forma concluímos que $f(n) = \varphi(n)$, ou seja, o grau do polinômio ciclotômico $\Phi_n(x)$ é igual a $\varphi(n)$.

O polinômio $\Phi_n(x) \in \mathbb{F}_q[x]$ não é necessariamente irredutível. O seguinte resultado determina o número de fatores na decomposição de $\Phi_n(x)$.

Teorema 1.26. *Seja $\mathbb{F}_q$ um corpo cuja característica não divide n e d o menor inteiro positivo tal que $q^d \equiv 1 \pmod{n}$. Então $\Phi_n(x)$ se decompõe em $\frac{\varphi(n)}{d}$ fatores irredutíveis sobre $\mathbb{F}_q[x]$, todos com o mesmo grau d.*

Observação 1.27. *O menor inteiro d tal que $q^d \equiv 1 \pmod{n}$ é chamado ordem multiplicativa de q módulo n e será denotado por $ord_n\, q$.*

Exemplo 1.28. *Considermos o polinômio $x^{27} - 1 \in \mathbb{F}_2[x]$. Segue da Equação 1.2 que*

$$x^{27} - 1 = \prod_{d|27} \Phi_d(x) \Rightarrow \frac{x^{27} - 1}{\prod_{d|3^2} \Phi_d(x)} = \Phi_{27}(x) \Rightarrow \Phi_{27}(x) = x^{18} + x^9 + 1 \ em\ \mathbb{F}_2.$$

Como a $ord_{27}\, 2 = 18$ temos que $\frac{\varphi(27)}{ord_{27}\, 2} = 1$ e a partir do Teorema 1.26 concluímos que 27-ésimo polinômio ciclotômico $\Phi_{27}(x)$ é irredutível em $\mathbb{F}_2$.

Exemplo 1.29. *Segue do Teorema 1.26 que o 15-ésimo polinômio ciclotômico Φ_{15} é redutível sobre qualquer corpo finito o qual ele está definido, pois*

$$ord_{15}\, q \mid \text{mmc}(ord_3 q, ord_5\, q) \mid \text{mmc}(\varphi(3), \varphi(5)) = 4,$$

assim toda raiz do polinômio ciclotômico é um divisor de 4

É um fato conhecido (Proposição 1.75 em [10]) que, se $\mathfrak{p}$ é um número primo ímpar e a é um inteiro positivo tal que $\text{mdc}(a, \mathfrak{p}) = 1$ e $\text{ord}_{\mathfrak{p}^2} a = \varphi(\mathfrak{p}^2) = \mathfrak{p}(\mathfrak{p} - 1)$ então $\text{ord}_{\mathfrak{p}^s} a = \varphi(\mathfrak{p}^s)$ para qualquer $s \geq 1$. Em outras palavras, se a é raiz primitiva módulo $\mathfrak{p}^2$ então a é raiz primitiva módulo $\mathfrak{p}^s$ para qualquer $s \geq 1$. Em particular, a partir do Teorema 1.26 obtemos o seguinte resultado.

Teorema 1.30. *Seja $\mathfrak{p}$ um número primo ímpar tal que $ord_{\mathfrak{p}^2} q = \varphi(\mathfrak{p}^2)$, isto é, q é raiz primitiva módulo $\mathfrak{p}^2$. Então, para qualquer $s \geq 1$ e $1 \leq i \leq s$, $\Phi_{\mathfrak{p}^i}(x)$ é irredutível sobre $\mathbb{F}_q$. Em particular, para $s \geq 1$ a fatoração em fatores irredutíveis de $x^{\mathfrak{p}^s} - 1$ sobre $\mathbb{F}_q$ é dada por*

$$x^{\mathfrak{p}^s} - 1 = (x-1) \prod_{i=1}^{s} \Phi_{\mathfrak{p}^i}(x).$$

Exemplo 1.31. *Seja $p = 3$ um primo ímpar. Como $ord_{3^2} 2 = \varphi(3^2)$ temos que os 3^i-ésimo polinômios ciclotômicos com $1 \leq i \leq 5$ são irredutíveis em $\mathbb{F}_2$. Assim, o polinômio $x^{3^5} - 1$ se decompõe sobre o corpo $\mathbb{F}_2$ da seguinte forma:*

$$x^{243}-1 = (x-1)\prod_{i=1}^{5} \Phi_{3^i}(x) = (x-1)(x^2+x+1)(x^6+x^3+1)(x^{18}+x^9+1)(x^{54}+x^{27}+1)(x^{162}+x^{81}+1).$$

1.4 Construção de Polinômios Irredutíveis

Seja $f(x) \in \mathbb{F}_q$ um polinômio mônico de grau $n \geq 1$ não divisível por x. Desta forma as classes $x^j + (f) \in \frac{\mathbb{F}_q[x]}{(f)}$ com $j = 0, 1, \cdots, q^n - 1$ são todas não nulas. Como $\frac{\mathbb{F}_q[x]}{(f)}$ contém $q^n - 1$ classes não nulas, existem inteiros r e s com $0 \leq r < s \leq q^n - 1$ tais que

$$x^s \equiv x^r \pmod{f} \Rightarrow f(x) \mid x^r(x^{s-r-1}),$$

onde $0 < s - r \leq q^n - 1$. Portanto, dado um polinômio mônico $f(x) \in \mathbb{F}_q[x]$ tal que $f(0) \neq 0$ sempre existe um inteiro positivo $\mathfrak{e} \leq q^n - 1$ tal que $f(x) \mid (x^{\mathfrak{e}} - 1)$.

Definição 1.32. *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio não nulo tal que $f(0) \neq 0$. Chamamos de ordem do polinômio $f(x)$, o qual denotaremos por $ord(f(x))$, ao menor inteiro positivo $\mathfrak{e}$ tal que $f(x)$ divide $x^{\mathfrak{e}} - 1$.*

Seja $f(x) \in \mathbb{F}_q$ um polinômio irredutível de grau n tal que $f(0) \neq 0$ e α uma raiz de $f(x)$. Segue do Teorema 1.13 que $\mathbb{F}_{q^n}$ é o corpo decomposição do polinômio $f(x)$. Pelo Teorema 1.15, as raízes de $f(x)$ possuem a mesma ordem no grupo multiplicativo $\mathbb{F}_q^*$ e $\alpha^{\mathfrak{e}} = 1$ se, e somente se, $f(x)$ divide $x^{\mathfrak{e}} - 1$ Proposição 1.10. A partir da definição de ordem de um polinômio temos o seguinte resultado.

Teorema 1.33. *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio irredutível de grau n tal que $f(0) \neq 0$. Então, a ordem de f é igual a ordem de qualquer raiz de f no grupo multiplicativo $\mathbb{F}_{q^n}^*$.*

Suponhamos que $f(x) \in \mathbb{F}_q[x]$ é um polinômio irredutível sobre $\mathbb{F}_q$ de grau n e que α é uma raiz de f. Segue do Teorema 1.13 que $\alpha \in \mathbb{F}_{q^n}$, logo $\alpha^{q^n} = \alpha$ e como $\alpha \neq 0$ temos que $\alpha^{q^n - 1} = 1$, o que implica que $\text{ord}(\alpha) \mid (q^n - 1)$ e portanto, $\text{ord}(f(x)) \mid (q^n - 1)$.

Definição 1.34. *Definimos o radical de um inteiro positivo n, o qual será denotado por* $\mathrm{rad}(n)$*, como o produto de todos os fatores primos distintos de n, ou seja, se* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *então* $\mathrm{rad}(n) = p_1 p_2 \cdots p_k$.

O problema de determinar se um determinado polinômio é irredutível não é trivial. O resultado seguinte fornece um critério para irredutibilidade de polinômios da forma $f(x^n)$.

Teorema 1.35 ([26], Teorema 3.35)**.** *Seja n um inteiro positivo e* $f(x) \in \mathbb{F}_q[x]$ *um polinômio irredutível de grau k e ordem* $\mathfrak{e}$*. Então o polinômio* $f(x^n)$ *é irredutível sobre* $\mathbb{F}_q$ *se, e somente se, as seguintes condições são satisfeitas:*

(1) $\mathrm{rad}(n)$ *divide* $\mathfrak{e}$*,*

(2) $\gcd\left(n, \frac{(q^k-1)}{\mathfrak{e}}\right) = 1$ *e*

(3) Se 4 *divide n então* $q^k \equiv 1 \pmod 4$.

Além disso, neste caso o polinômio $f(x^n)$ *possui grau* kn *e ordem* $\mathfrak{e}n$.

Como já mencionamos, determinar se um polinômio é irreduutível não é uma tarefa fácil na maioria das vezes. Quando este polinômio é um binômio, é conhecido um critério para determinar se tal binômio é irredutível.

Teorema 1.36 ([26], Teorema 3.75)**.** *Seja* $t \geq 2$ *um inteiro e* $a \in \mathbb{F}_q^*$*. Então o binômio* $x^t - a$ *é irredutível em* $\mathbb{F}_q$ *se, e somente se, as seguintes condições são satisfeitas:*

(1) $\mathrm{rad}(t)$ *divide* $ord_q\, a$*,*

(2) $\mathrm{mdc}\left(t, \frac{(q-1)}{ord_q\, a}\right) = 1$ *e*

(3) Se 4 *divide t então* $q \equiv 1 \pmod 4$.

Dado que um polinômio é irredutível sobre $\mathbb{F}_q$, uma questão útil é decidir se este polinômio continua sendo irredutível em uma extensão de $\mathbb{F}_q$. O seguinte resultado dirige-se a esta questão.

Teorema 1.37 ([26], Teorema 3.46)**.** *Seja k um inteiro positivo e f um polinômio irredutível sobre* $\mathbb{F}_q$ *de grau n. Então f se decompõe em* $\mathbb{F}_{q^k}$ *em* $d := \mathrm{mdc}(k, n)$ *polinômios irredutíveis de grau* $\frac{n}{d}$.

Como consequência imediata deste resultado obtemos o corolário abaixo.

Corolário 1.38. *Um polinômio irredutível sobre $\mathbb{F}_q$ de grau n permanece irredutível sobre $\mathbb{F}_{q^k}$ se, e somente se, k e n são relativamente primos.*

1.5 Valorização p-ádica

Definição 1.39. *A valorização p-ádica de um inteiro positivo n, a qual denotaremos por $\nu_p(n)$, é a maior potência de p que divide n. Em outras palavras, se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ é a decomposição de n em fatores primos, então $\nu_{p_i}(n) = \alpha_i$.*

O resultado seguinte fornece algumas propriedades sobre a valorização p-ádica de números da forma $a^j - 1$ com $a \equiv 1 \pmod{p}$.

Lema 1.40 (Lifting the Exponent Lemma)**.** *Seja p um primo e ν_p a valorização p-ádica. As seguintes afirmação são verdadeiras:*

(1) Se p é um primo ímpar tal que p divide $a-1$ então $\nu_p(a^k-1) = \nu_p(a-1) + \nu_p(k)$;

(2) Se $p = 2$ e a é um número ímpar, então

$$\nu_2(a^k - 1) = \begin{cases} \nu_2(a-1) & \text{se } k \text{ é ímpar,} \\ \nu_2(a^2-1) + \nu_2(k) - 1 & \text{se } k \text{ é par.} \end{cases}$$

CAPÍTULO 2

FATORAÇÃO DA COMPOSIÇÃO DE POLINÔMIOS E APLICAÇÕES

2.1 Explicitando os Fatores de $f(x^n)$

Sejam n um inteiro positivo e $f(x) \in \mathbb{F}_q[x]$ um polinômio irredutível de grau k e ordem $\mathfrak{e}$. O Teorema 1.35 fornece as condições que k, $\mathfrak{e}$, q e n devem cumprir para que o polinômio $f(x^n)$ também seja irredutível sobre $\mathbb{F}_q[x]$. Nesta seção, supondo que todo fator primo de n divide $q-1$ mostraremos, assumindo algumas condições "genéricas", como encontrar os fatores irredutíveis de $f(x^n)$ em $\mathbb{F}_q[x]$.

O principal resultado deste capítulo é uma generalização de [7], em que os autores obtêm uma fatoração explícita do binômio $x^n - 1$.

Agora, apresentamos um lema, o qual será fundamental para mostrarmos o resultado principal deste capítulo.

Lema 2.1. *Seja n um inteiro positivo tal que* $\mathrm{rad}(n)|(q-1)$*, e $f(x) \in \mathbb{F}_q[x]$ um polinômio irredutível de grau k e ordem $\mathfrak{e}$, tal que* $\mathrm{mdc}(\mathfrak{e}k, n) = 1$*; além disso, $q \equiv 1 \pmod 4$ se $8|n$. Seja r um inteiro positivo tal que $nr \equiv 1 \pmod{\mathfrak{e}}$. Se $\alpha \in \overline{\mathbb{F}}_q$ é uma raiz de $f(x)$, $\theta \in \mathbb{F}_q^*$ é um elemento de ordem d, onde $d = \mathrm{mdc}(n, q-1)$ e t é um divisor de $\frac{n}{d}$. Então,*

a) Para $t \geq 1$ $g_t(x) := \prod_{i=0}^{k-1} (x - \alpha^{trq^i})$ é um polinômio irredutível sobre $\mathbb{F}_q[x]$ com grau k e ordem $\mathfrak{e}$;

b) Para cada inteiro não negativo $u \geq 0$ tal que $\mathrm{mdc}(u,t) = 1$*, o polinômio $g_t(\theta^u x^t)$ é irredutível em $\mathbb{F}_q$ e divide $f(x^n)$.*

Demonstração. a) Como α é raiz do polinômio irredutível $f(x) \in \mathbb{F}_q[x]$ de grau k então $\alpha \in \mathbb{F}_{q^k}$, logo $\alpha^{q^k} = \alpha$. Em particular, $\sigma_q(g_t(x)) = \prod_{i=0}^{k-1}(x - \alpha^{trq^{i+1}}) = \prod_{i=0}^{k-1}(x - \alpha^{trq^i})$ e concluímos que $g_t(x) \in \mathbb{F}_q[x]$.

Resta mostrar que $g_t(x)$ é irredutível, ou seja, que o menor inteiro positivo i para o qual $\alpha^{rtq^i} = \alpha^{rt}$ é $i = k$.

Uma vez que, $\alpha^{trq^i} = \alpha^{rt}$ se, e somente se, $\alpha^{rt(q^i-1)} = 1$ e sabemos por hipótese que $\mathrm{ord}(\alpha) = \mathfrak{e}$. Segue que $rt(q^i - 1) \equiv 0 \pmod{\mathfrak{e}}$, mas por hipótese $\mathrm{mdc}(\mathfrak{e}, tr) = 1$, portanto $\mathfrak{e} \mid (q^i - 1)$ o que implica que $\mathrm{ord}_{\mathfrak{e}}\, q = k \mid i$.

b) Como $g_t(\theta^u x)$ é irredutível sobre $\mathbb{F}_q$, somente precisamos verificar que $g_t(\theta^u x)$ e t satisfaz as condições do Teorema 1.35. Observemos que cada raiz de $g_t(\theta^u x)$ é da forma $\theta^{-u}\alpha^{trq^i}$, consequentemente:

$$\mathrm{ord}\, g_t(\theta^u x) = \mathrm{ord}(\theta^{-u}\alpha^{trq^i}) = \mathrm{ord}(\alpha^{trq^i}) \cdot \mathrm{ord}(\theta^{-u}) = \frac{\mathfrak{e}d}{\mathrm{mdc}(u,d)},$$

onde a segunda igualdade segue do fato que as ordens dos elementos θ^{-u} e α^{trq^i} são coprimas, pois $\mathrm{ord}(\theta^{-u}) \mid d \mid n$, $\mathrm{ord}(\alpha^{trq^i}) \mid \mathfrak{e}$ e por hipótese $\mathrm{mdc}(\mathfrak{e}, n) = 1$.

Como $\mathrm{mdc}(u,t) = 1$ e $\mathrm{rad}(t) \mid d$, temos que $\mathrm{rad}(t) \mid \frac{d}{\mathrm{mdc}(u,d)}$. Em particular, $\mathrm{rad}(t)$ divide $\mathrm{ord}\, g_t(\theta^u x)$.

Agora, precisamos verificar que $\mathrm{mdc}\left(t, \dfrac{q^k - 1}{\mathrm{ord}\, g_t(\theta^u x)}\right) = 1$.

De fato,

$$\mathrm{mdc}\left(t, \frac{q^k - 1}{\mathfrak{e}\dfrac{d}{\mathrm{mdc}(u,d)}}\right) = \mathrm{mdc}\left(t, \frac{(q^k - 1)\mathrm{mdc}(u,d)}{\mathfrak{e}d}\right).$$

Além disso, $\mathrm{mdc}(u, t) = \mathrm{mdc}(n, \mathfrak{e}) = 1$ e $\mathrm{rad}(t) \mid d$ (que divide n). Logo, $\mathrm{mdc}(t, \mathfrak{e}) = 1$ e assim

$$\mathrm{mdc}\left(t, \frac{(q^k - 1)\mathrm{mdc}(u,d)}{\mathfrak{e}d}\right) = \mathrm{mdc}\left(t, \frac{q^k - 1}{d}\right).$$

Seja p um divisor primo de t, logo p também divide n e como o $\mathrm{mdc}(n,k) = 1$, temos que p não divide k. Em particular, $\nu_p(k) = 0$. Segue do Lema 1.40 que

$\nu_p(q^k-1) = \nu_p(q-1)+\nu_p(k) = \nu_p(q-1)$. Uma vez que $t \mid \frac{n}{d}$ temos que $\nu_p(n) > \nu_p(d)$ e sendo

$$\nu_p(d) = \nu_p(\gcd(n, q-1)) = \min\{\nu_p(n), \nu_p(q-1)\},$$

deduzimos que $\nu_p(d) = \nu_p(q-1)$ e $\nu_p\left(\frac{q^k-1}{d}\right) = 0$. Mas, p é um divisor primo arbitrário de t e concluímos que $\text{mdc}\left(t, \frac{q^k-1}{d}\right) = 1$.

Finalmente, precisamos verificar que $q \equiv 1 \pmod 4$ se $4 \mid t$.

Como $t \mid \frac{n}{\text{mdc}(n,q-1)}$ temos que $\text{rad}(t) \mid \text{rad}(n)$ (consequentemente divide $q-1$). Assim, se $4 \mid t$ temos que $\text{mdc}(n, q-1)$ é par e $\frac{n}{\text{mdc}(n,q-1)}$ é divisível por 4. Portanto, $8 \mid n$ e segue da hipótese que $q \equiv 1 \pmod 4$.

Resta mostrarmos que $g_t(\theta^u x^t)$ divide $f(x^n)$.

Suponhamos que λ é uma raiz de $g_t(\theta^u x^t)$ ou, equivalentemente, que $\lambda^t\theta^u$ é uma raiz de $g_t(x)$. Então existe $j \in \mathbb{N}$ tal que $\lambda^t\theta^u = \alpha^{trq^j}$. Em particular,

$$\alpha^{q^j} = \alpha^{nrq^j} = \left(\alpha^{trq^j}\right)^{\frac{n}{t}} = \left(\lambda^t\theta^u\right)^{\frac{n}{t}} = \lambda^n.$$

Portanto, $\lambda^n = \alpha^{q^j}$ é uma raiz de $f(x)$ e sendo λ uma raiz arbitrária segue que, qualquer raiz de $g_t(\theta^u x^t)$ é também raiz de $f(x^n)$. Uma vez que $g_t(\theta^u x^t)$ possui somente raízes simples (Teorema 1.13), concluímos que $g_t(\theta^u x^t)$ divide $f(x^n)$.

■

Observação 2.2. *Notemos que o fato de $g_t(x)$ possuir ordem $\mathfrak{e}$ segue da irredutibilidade de $g_t(x)$. Basta observarmos que a ordem da raiz α^{trq^i} do polinômio $g_t(x)$ com $i \in [0, k-1]$ é $\mathfrak{e}$.*

Agora estamos em condições para enunciar e mostrar o principal resultado deste capítulo.

Teorema 2.3. *Seja $f \in \mathbb{F}_q[x]$ um polinômio mônico irredutível de grau k e ordem $\mathfrak{e}$. Sejam q, n, r, θ e $g_t(x)$ como no Lema 2.1. Então $f(x^n)$ se decompõe em polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ da seguinte forma:*

$$f(x^n) = \prod_{t \mid m} \prod_{\substack{1 \le u \le d \\ \text{mdc}(u,t)=1}} \theta^{-uk} g_t(\theta^u x^t) \tag{2.1}$$

onde $m := \frac{n}{d} = \frac{n}{\text{mdc}(n,q-1)}$.

Demonstração. Afirmamos que os fatores de $g_t(\theta^u x^t)$ para $1 \le u \le d$ com $\mathrm{mdc}(u,t)=1$ são distintos dois a dois.

De fato, se $g_t(\theta^u x^t) = g_t(\theta^w x^t)$ para alguns $1 \le u < w \le d$ com $\mathrm{mdc}(u,t) = \mathrm{mdc}(w,t) = 1$, estes polinômios têm as mesmas raízes e como eles são irredutíveis, suas raízes são conjugadas. Como cada fator de $g_t(\theta^u x^t)$ é simples, segue que existe um inteiro não negativo i tal que $\theta^{-u}\alpha^{tr} = \theta^{-w}\alpha^{trq^i}$ isto é, $\theta^{w-u} = \alpha^{tr(q^i-1)}$. Portanto,

$$\left(\theta^{u-w}\right)^{\mathfrak{e}} = \left(\alpha^{tr(q^i-1)}\right)^{\mathfrak{e}} = 1.$$

Da última igualdade obtemos que a ordem de θ divide $(w-u)\mathfrak{e}$. Agora, por hipótese, $\mathrm{mdc}(n,\mathfrak{e}) = 1$, consequentemente $\mathrm{mdc}(d,\mathfrak{e}) = 1$ e assim d divide $w-u$. Como $|w-u| < d$, temos necessariamente que $w = u$.

Seja $h(x)$ o polinômio definido pelo duplo produto da equação (2.1). Uma vez que, cada fator deste produto é polinômio mônico, irredutível que divide $f(x^n)$, $h(x)$ é mônico e divide $f(x^n)$. Em particular, a igualdade $f(x^n) = h(x)$ é verdadeira se, e somente se, $h(x)$ e $f(x^n)$ tem o mesmo grau, isto é, $\deg(h(x)) = nk$. Como t divide m, $\mathrm{rad}(t)$ divide $\mathrm{rad}(n)$ (consequetemente divide $q-1$) e assim $\mathrm{rad}(t)$ divide d. Logo, para cada divisor t de $\frac{n}{d}$, o número de polinômios da forma $\theta^{-uk} g_t(\theta^u x^t)$ com $1 \le u \le d$ e $\gcd(u,t) = 1$ é igual a

$$\frac{d}{\mathrm{rad}(t)}\varphi(\mathrm{rad}(t)) = \frac{d\varphi(t)}{t},$$

onde φ é a *função de Euler*. Em particular, o grau de $h(x)$ é igual a

$$\sum_{t|m} \frac{d\varphi(t)}{t} tk = dk \sum_{t|m} \varphi(t) = dkm = nk.$$

Portanto, o grau de $h(x)$ é nk e desta forma $h(x) = f(x^n)$. como queríamos. ■

A partir deste resultado, podemos obter uma fórmula explícita que fornece o número total de fatores irredutíveis de $f(x^n)$ sobre $\mathbb{F}_q$.

Corolário 2.4. *Sejam $f(x)$, n e m como no Teorema 2.3. Para cada divisor t de m, o número de fatores irredutíveis de $f(x^n)$ de grau kt é $\frac{\varphi(t)}{t} \cdot \mathrm{mdc}(n, q-1)$. O número total de fatores irredutíveis de $f(x^n)$ em $\mathbb{F}_q[x]$ é igual a*

$$\mathrm{mdc}(n, q-1). \prod_{\substack{p|m \\ p \text{ primo}}} \left(1 + \nu_p(m)\frac{p-1}{p}\right).$$

Demonstração. Identificamos no Teorema 2.3 que os fatores irredutíveis de $f(x^n)$ são da forma $\theta^{-ku} g_t(\theta^u x^t)$ com $1 \le u \le d$ e $\mathrm{mdc}(u,t) = 1$, ou seja, $\mathrm{mdc}(u, \mathrm{rad}(t)) = 1$ pois $d = \mathrm{mdc}(n, q-1)$.

Particionando o intervalo $[1,d]$ em $\frac{\text{mdc}(n,q-1)}{\text{rad}(t)}$ subintervalos de tamanho $\text{rad}(t)$, em cada subintervalo temos $\varphi(\text{rad}(t))$ escolhas para u com $\text{mdc}(u,t)=1$. Desta forma o número de u que cumprem a condição é

$$\frac{\varphi(\text{rad}(t))}{\text{rad}(t)}d = \frac{\varphi(\text{rad}(t))}{\text{rad}(t)}\text{mdc}(n,q-1) = \frac{\varphi(t)}{t}\text{mdc}(n,q-1)$$

Portanto, o número total de fatores irredutíveis de $f(x^n)$ é:

$$\sum_{t|m}\frac{\varphi(t)}{t}\text{mdc}(n,q-1) = \text{mdc}(n,q-1)\sum_{t|m}\frac{\varphi(t)}{t} \tag{2.2}$$

Como $\frac{\varphi(t)}{t}$ é uma função aritmética multiplicativa, basta calcularmos para cada potência de primo, ou seja:

$$\sum_{t|p_i^s}\frac{\varphi(t)}{t} = \sum_{j=0}^{s}\frac{\varphi(p_i^j)}{p_i^j} = 1+\sum_{j=1}^{s}\frac{\varphi(p_i^j)}{p_i^j} = 1+\sum_{j=1}^{s}\frac{p_i^j-p_i^{j-1}}{p_i^j} = 1+s\cdot\frac{p_i-1}{p_i}.$$

Assim, se $m = p_1^{\alpha_1}\cdots p_l^{\alpha_l}$ então

$$\sum_{t|m}\frac{\varphi(t)}{t} = \prod_{j=1}^{l}\sum_{t|p_j^{\alpha_j}}\frac{\varphi(t)}{t} = \prod_{p_i|m}\left(1+\nu_{p_i}(m).\frac{p_i-1}{p_i}\right).$$

Segue da equação 2.2 que o número de fatores irredutíveis de $f(x^n)$ sobre $\mathbb{F}_q$ é dado por

$$\text{mdc}(n,q-1)\prod_{\substack{p_i|m\\ p_i \text{ primo}}}\left(1+\nu_{p_i}(m)\frac{p_i-1}{p_i}\right),$$

como queríamos mostrar.

■

Exemplo 2.5. *Seja* $f(x) = x^3+4x^2+6x+1 \in \mathbb{F}_{11}[x]$. *Explicitemos a decomposição do polinômio* $f(x^n)$ *com* $n = 5^a, a \geq 1$.

Observemos primeiro que $f(x)$ *é um polinômio irredutível de ordem* 14 *sobre* $\mathbb{F}_{11}$. *De fato,*

$$\Phi_{14}(x) = \frac{x^{14}-1}{(x^7-1)(x+1)} = f(x)h(x) \text{ e } ord_{14}(11) = 3,$$

onde $h(x) = x^3+6x^2+4x+1$. *Em particular,* $f(x)$ *e* n *satisfazem as condições do Teorema 2.3. Tomando* $\theta = 3$, *para* $n = 5$ *temos que* $r = 3$ *e*

$$g_1(x) = (x-\alpha^3)(x-\alpha^5)(x-\alpha^{13}) = h(x).$$

Portanto,

$$f(x^5) = \prod_{1\le u\le 5} 9^u h(3^u x).$$

Se $a \ge 2$, tomando $r = 3^a$ e para cada inteiro $0 \le b \le a-1$,

$$g_{5^b}(x) = \begin{cases} (x-\alpha)(x-\alpha^9)(x-\alpha^{11}) & \text{se } b-a \text{ é par} \\ (x-\alpha^3)(x-\alpha^5)(x-\alpha^{13}) & \text{se } b-a \text{ é ímpar.} \end{cases}$$

Logo, a decomposição do polinômio $f(x^n)$ em fatores mônicos e irredutíveis é:

$$f(x^{5^a}) = \prod_{1\le u\le 5} 9^u h(3^u x) \cdot \prod_{\substack{1\le b<a \\ b-a \text{ par}}} \prod_{u=1}^{4} 9^u f(3^u x^{5^b}) \prod_{\substack{1\le b<a \\ b-a \text{ ímpar}}} \prod_{u=1}^{4} 9^u h(3^u x^{5^b}).$$

2.1.1 Aplicações do Teorema 2.3

Nesta seção apresentamos algumas situações interessantes onde o Teorema 2.3 fornece um resultado mais explícito.

Sabemos da seção 1.3 que, para um inteiro positivo $\mathfrak{e}$ tal que $\mathrm{mdc}(\mathfrak{e}, q) = 1$, o $\mathfrak{e}$-ésimo polinômio ciclotômico $\Phi_\mathfrak{e}(x) \in \mathbb{F}_q[x]$ é definido recursivamente pela identidade

$$x^\mathfrak{e} - 1 = \prod_{m|\mathfrak{e}} \Phi_m(x).$$

O resultado seguinte nos garante que se conhecemos a fatoração do polinômio $\Phi_\mathfrak{e}(x)$ (respectivamente $x^\mathfrak{e} - 1$) sob condições adequadas do inteiro positivo n, podemos obter a fatoração de $\Phi_\mathfrak{e}(x^n)$ (respectivamente $x^{\mathfrak{e}n} - 1$).

Teorema 2.6. *Seja $\mathfrak{e}$ um inteiro positivo tal que $\mathrm{mdc}(\mathfrak{e}, q) = 1$ e sejam $k = ord_\mathfrak{e} q$ e $l = \frac{\varphi(\mathfrak{e})}{k}$. Além disso, suponhamos que n é um inteiro positivo tal que $\mathrm{rad}(n)$ divide $q-1$, $\mathrm{mdc}(n, k\mathfrak{e}) = 1$ e $q \equiv 1 \pmod 4$ se n é divisível por 8. Se $\Phi_\mathfrak{e}(x) = \prod_{1\le i\le l} f_i(x)$ é a fatoração em fatores irredutíveis de $\Phi_\mathfrak{e}(x)$ sobre $\mathbb{F}_q$, então a fatoração em fatores irredutíveis de $\Phi_\mathfrak{e}(x^n)$ sobre $\mathbb{F}_q$ é dado por:*

$$\Phi_\mathfrak{e}(x^n) = \prod_{i=1}^{l} \prod_{t|m} \prod_{\substack{1\le u\le d \\ \mathrm{mdc}(u,t)=1}} \theta^{-uk} f_i(\theta^u x^t), \tag{2.3}$$

onde $d = \mathrm{mdc}(n, q-1)$, $m = \frac{n}{d}$ e $\theta \in \mathbb{F}_q$ é um elemento de ordem d. Em particular, se $x^\mathfrak{e} - 1 = \prod_{i=1}^{N} F_i(x)$ é a fatoração de $x^\mathfrak{e} - 1$ sobre $\mathbb{F}_q$, então a fatoração de $x^{\mathfrak{e}n} - 1$ sobre $\mathbb{F}_q$ é dada por:

$$x^{\mathfrak{e}n} - 1 = \prod_{i=1}^{N} \prod_{t|m} \prod_{\substack{1\le u\le d \\ \mathrm{mdc}(u,t)=1}} \theta^{-u\cdot \deg(F_i)} F_i(\theta^u x^t). \tag{2.4}$$

Demonstração. Notemos que, para qualquer $1 \leq i \leq l$, $f_i(x)$ possui ordem $\mathfrak{e}$ e, pelo Teorema 1.26, f_i possui grau k. Em particular, das hipóteses, estamos sobre as condições do Teorema 2.3.

Para cada $t \mid m$, seja $g_{t,i}$ o polinômio de grau k e ordem $\mathfrak{e}$ associado a f_i como no Lema 2.1. Pelo Teorema 2.3, temos que:

$$f_i(x^n) = \prod_{t \mid m} \prod_{\substack{1 \leq u \leq d \\ \mathrm{mdc}(u,t)=1}} \theta^{-uk} g_{t,i}(\theta^u x^t),$$

consequentemente

$$\Phi_{\mathfrak{e}}(x^n) = \prod_{i=1}^{l} f_i(x^n) = \prod_{i=1}^{l} \prod_{t \mid m} \prod_{\substack{1 \leq u \leq d \\ \mathrm{mdc}(u,t)=1}} \theta^{-uk} g_{t,i}(\theta^u x^t).$$

Agora observemos que, para obtermos a equação (2.3) é suficiente mostrarmos que, para cada divisor $t \mid m$ vale a seguinte igualdade:

$$\prod_{i=1}^{l} g_{t,i}(x) = \prod_{i=1}^{l} f_i(x). \tag{2.5}$$

Como cada $g_{t,i}$ é irredutível de ordem $\mathfrak{e}$ e $g_{t,i}$ divide $\Phi_{\mathfrak{e}}(x) = \prod_{1 \leq i \leq l} f_i(x)$, a equação (2.5) é verdadeira se, e somente se, os polinômios $g_{t,i}$ com $1 \leq i \leq l$ são dois a dois distintos.

De fato, se $g_{t,i} = g_{t,j}$ para algum $1 \leq i < j \leq l$, então existem raízes α_i, α_j de f_i e f_j, respectivamente, tais que

$$\alpha_i^{rt} = \alpha_j^{rtq^h},$$

para algum $h \geq 0$, onde r é um inteiro positivo tal que $rn \equiv 1 \pmod{\mathfrak{e}}$. Elevando a $\frac{n}{t}$-ésima potência ambos os lados da igualdade acima, obtemos $\alpha_i = \alpha_j^{q^h}$, isto é, α_i e $\alpha_j^{q^h}$ são conjugados sobre $\mathbb{F}_q$. Portanto, eles possuem o mesmo polinômio minimal sobre $\mathbb{F}_q$, isto é, $f_i = f_j$ e desta forma $i = j$. Isto conclui a prova da equação (2.3).

Agora, verifiquemos que a equação (2.4) é verdadeira. Por hipótese,

$$x^{\mathfrak{e}n} - 1 = \prod_{i=1}^{N} F_i(x^n) = \prod_{m \mid \mathfrak{e}} \Phi_m(x^n).$$

Notemos que, para provar a veracidade da equação (2.4), somente precisamos verificar que a equação (2.3) é verdadeira quando substituímos $\mathfrak{e}$ por qualquer um de seus divisores. Se m divide $\mathfrak{e}$ então $k' := \mathrm{ord}_m\, q$ divide $k = \mathrm{ord}_{\mathfrak{e}}\, q$. Portanto, $\mathrm{mdc}(n, k\mathfrak{e}) = 1$ implica que $\mathrm{mdc}(n, k'm) = 1$. Logo, a equação (2.3) é verdadeira para Φ_m. ■

No que segue, fornecemos algumas situações especiais onde o Teorema 2.6 se aplica naturalmente. Em particular, o seguinte corolário é uma consequência imediata do Teorema 2.6 mais especificamente, equação 2.3 juntamente com o Corolário 1.30.

Corolário 2.7. *Seja n um inteiro positivo tal que* $\mathrm{rad}(n) \mid (q-1)$ *e P um número primo ímpar tal que $ord_{P^2} q = \varphi(P^2) = P(P-1)$, isto é, q é uma raiz primitiva módulo P^2. Seja $d = \mathrm{mdc}(n, q-1)$ e $m = \frac{n}{d}$. Além disso, suponhamos que* $\mathrm{mdc}(n, P-1) = 1$ *e que θ é um elemento qualquer em $\mathbb{F}_q$ de ordem d. Então, para qualquer $s \geq 1$, a fatoração de $\Phi_{P^s}(x^n)$ e $x^{P^s n} - 1$ sobre $\mathbb{F}_q$ são dadas por:*

$$\Phi_{P^s}(x^n) = \prod_{t \mid m} \prod_{\substack{1 \leq u \leq d \\ \mathrm{mdc}(u,t)=1}} \theta^{-u \cdot \varphi(P^s)} \Phi_{P^s}(\theta^u x^t),$$

e

$$x^{P^s n} - 1 = \left(\prod_{t \mid m} \prod_{\substack{1 \leq u \leq d \\ \mathrm{mdc}(u,t)=1}} (x^t - \theta^u) \right) \times \left(\prod_{1 \leq i \leq s} \prod_{t \mid m} \prod_{\substack{1 \leq u \leq d \\ \mathrm{mdc}(u,t)=1}} \theta^{u \cdot \varphi(P^i)} \Phi_{P^i}(\theta^u x^t) \right).$$

Observemos que o Corolário 2.7 extende o Lema 5.3 em [9], onde n é uma potência de um primo $r \neq P$ que divide $q-1$, mas não divide $P-1$.

Agora, exibimos alguns exemplos que são aplicações do Corolário 2.7.

Exemplo 2.8. *Seja q uma potência de primo tal que $q - 1 \equiv 3, 6 \pmod 9$ e q uma raiz primitiva módulo $25 = 5^2$. Vejamos como obter a partir do resultado acima a fatoração de $\Phi_{P^s}(x^n)$ com $P = 5$ e $n = 3^a$, $a \geq 1$.*

Primeiro, observemos que existem $2 \cdot \varphi(20) = 16$ restos módulo $225 = 9 \cdot 25$ tal que

$$\begin{cases} q - 1 \equiv 3, 6 \pmod 9 \\ q^{20} \equiv 1 \pmod{25} \end{cases}.$$

Como $d = \mathrm{mdc}(q-1, 3^a) = 3$ e $m = \frac{n}{d} = 3^{a-1}$, tomando $\theta \in \mathbb{F}_q$ um elemento qualquer de ordem 3 e aplicando o Corolário 2.7 para qualquer $s \geq 1$, obtemos:

$$x^{5^s 3^a} - 1 = \left(\prod_{t=0}^{a-1} \prod_{\substack{1 \leq u \leq 3 \\ \mathrm{mdc}(u,3^t)=1}} (x^{3^t} - \theta^u) \right) \times \left(\prod_{i=1}^{s} \prod_{t=0}^{a-1} \prod_{\substack{1 \leq u \leq 3 \\ \mathrm{mdc}(u,3^t)=1}} \theta^{-u \cdot \varphi(5^i)} \Phi_{5^i}(\theta^u x^{3^t}) \right),$$

onde $\Phi_{5^i}(x) = x^{4 \cdot 5^{i-1}} + x^{3 \cdot 5^{i-1}} + x^{2 \cdot 5^{i-1}} + x^{5^{i-1}} + 1$.

Exemplo 2.9. *Seja q uma potência de primo tal que* $\mathrm{mdc}(q-1, 25) = 5$. *Suponhamos ainda que q é uma raiz primitiva módulo 9, assim existem $4 \cdot \varphi(6) = 8$ restos módulo $225 = 25 \cdot 9$ com esta propriedade. Tomando $P = 3$ e $n = 5^a$ com $a \geq 1$ temos que, $d =$* $\mathrm{mdc}(q-1, 5^a) = 5$ *e $m = 5^{a-1}$. Seja $\theta \in \mathbb{F}_q$ um elemento qualquer de ordem 5. Aplicando o*

Corolário 2.7 para qualquer $s \geq 1$, temos que:

$$x^{5^a 3^s} - 1 = \left(\prod_{t=0}^{a-1} \prod_{\substack{1 \leq u \leq 5 \\ \mathrm{mdc}(u,5^t)=1}} (x^{5^t} - \theta^u) \right) \times \left(\prod_{i=1}^{s} \prod_{t=0}^{a-1} \prod_{\substack{1 \leq u \leq 5 \\ \mathrm{mdc}(u,5^t)=1}} \theta^{-u \cdot \varphi(3^i)} \Phi_{3^i}(\theta^u x^{5^t}) \right),$$

onde $\Phi_{3^i}(x) = x^{2 \cdot 3^{i-1}} + x^{3^{i-1}} + 1$ para $i \geq 1$.

Exemplo 2.10. *Seja q uma potência de primo tal que q é uma raiz primitiva módulo $289 = 17^2$ e $\mathrm{mdc}(q-1, 225) = 15$. Tomemos $P = 17$, $n = 3^a 5^b$. Para quaisquer $a, b, s \geq 1$ e, qualquer elemento $\theta \in \mathbb{F}_q$ de ordem $d = 15 = \mathrm{mdc}(q-1, 3^a 5^b)$, segue do Corolário 2.7 que fatoração do polinômio $x^{3^a 5^b 17^s} - 1$ é dada por:*

$$x^{3^a 5^b 17^s} - 1 = \left(\prod_{\substack{0 \leq t_1 \leq a-1 \\ 0 \leq t_2 \leq b-1}} \prod_{\substack{1 \leq u \leq 15 \\ \mathrm{mdc}(u, 3^{t_1} 5^{t_2})=1}} (x^{3^{t_1} 5^{t_2}} - \theta^u) \right) \times \left(\prod_{1 \leq i \leq s} \prod_{\substack{0 \leq t_1 \leq a-1 \\ 0 \leq t_2 \leq b-1}} \prod_{\substack{1 \leq u \leq 15 \\ \mathrm{mdc}(u, 3^{t_1} 5^{t_2})=1}} \theta^{-u \cdot \varphi(17^i)} \Phi_{17^i}(\theta^u x^{3^{t_1} 5^{t_2}}) \right),$$

onde $\Phi_{17^i}(x) = \sum_{j=0}^{16} x^{j \cdot 17^{i-1}}$ para $i \geq 1$.

Se $a = 0$ e $b \geq 1$ então $n = 5^b$ e $d = \mathrm{mdc}(q-1, 5^b) = 5$. Basta tomar $\theta \in \mathbb{F}_q$ um elemento qualquer de ordem 5 e aplicando novamente o Corolário 2.7, para qualquer $s \geq 1$ obtemos que:

$$x^{5^b 17^s} - 1 = \left(\prod_{0 \leq t \leq b-1} \prod_{\substack{1 \leq u \leq 5 \\ \mathrm{mdc}(u,5^t)=1}} (x^{5^t} - \theta^u) \right) \times \left(\prod_{1 \leq i \leq s} \prod_{0 \leq t \leq b-1} \prod_{\substack{1 \leq u \leq 5 \\ \mathrm{mdc}(u,5^t)=1}} \theta^{-u \cdot \varphi(17^i)} \Phi_{17^i}(\theta^u 5^t) \right),$$

onde $\Phi_{17^i}(x) = \sum_{j=0}^{16} x^{j \cdot 17^{i-1}}$ para $i \geq 1$.

2.2 O Caso Geral

Na seção anterior, fornecemos a fatoração de $f(x^n)$ sobre $\mathbb{F}_q$ impondo algumas condições ao polinômio f e ao número natural n; entre elas, assumimos que $\mathrm{rad}(n) \mid (q-1)$ e $q \equiv 1 \pmod 4$ se $8 \mid n$. Nesta seção, estendemos este resultado removendo estas condições sobre o número natural n.

Com este objetivo, se faz necessária a seguinte definição:

Definição 2.11. *Sejam n um inteiro positivo tal que* $\gcd(n,q)=1$ *e* $S_n = ord_{\mathrm{rad}(n)}\, q$. *Definimos o inteiro positivo s_n como:*

$$s_n := \begin{cases} 2S_n & \text{se } q^{S_n} \equiv 3 \pmod 4 \text{ e } 8|n, \\ S_n & \text{caso contrário.} \end{cases}$$

Observamos que na seção anterior $s_n = 1$.

Ao longo desta seção, fixamos $f \in \mathbb{F}_q[x]$ um polinômio irredutível de grau k e ordem $\mathfrak{e}$. Consideramos n um inteiro positivo tal que $\mathrm{mdc}(n, \mathfrak{e}k) = 1$, $s_n > 1$ e $\mathrm{mdc}(s_n, k) = 1$. Além disso, como uma extensão natural da seção anterior, $d := \mathrm{mdc}(n, q^{s_n}-1)$ e $m := \frac{n}{d} = \frac{n}{\mathrm{mdc}(n, q^{s_n}-1)}$.

Como, $\mathrm{mdc}(s_n, k) = 1$, o polinômio f permanece irredutível sobre $\mathbb{F}_{q^{s_n}}$ (ver Corolário 1.38).

Seja α uma raiz de f. Segue do Teorema 2.3 que os fatores irredutíveis de $f(x^n)$ em $\mathbb{F}_{q^{s_n}}[x]$ são os polinômios:

$$G_{t,u}(x) := \prod_{i=0}^{k-1} (x^t - \theta^{-u} \alpha^{trq^{is_n}}), \tag{2.6}$$

onde

- r é um inteiro positivo tal que $rn \equiv 1 \pmod{\mathfrak{e}}$;
- t é um divisor de m;
- $\theta \in \mathbb{F}_{q^{s_n}}^*$ é um elemento de ordem d;
- $\mathrm{mdc}(t,u) = 1$, $1 \le u \le d$.

Agora, para cada polinômio $G_{t,u}(x)$, precisamos determinar qual é a menor extensão de $\mathbb{F}_q$ que contém os seus coeficientes. Isto nós fornecerá a relação entre $G_{t,u}(x)$ e os fatores irredutíveis de $f(x^n)$ sobre $\mathbb{F}_q$ associados.

Definição 2.12. *Para t e u como acima, definimos por $l_{t,u}$ o menor inteiro positivo v tal que $G_{t,u}(x) \in \mathbb{F}_{q^v}[x]$.*

Observação 2.13. *Como $G_{t,u}(x) \in \mathbb{F}_{q^{s_n}}[x]$, $l_{t,u}$ é um divisor de s_n. Usando o automorfismo de Frobenius concluímos que cada fator irredutível de $f(x^n)$ em $\mathbb{F}_q[x]$ é da forma*

$$\prod_{j=0}^{l_{t,u}-1} \sigma_q^j(G_{t,u}(x)).$$

Segue da definição de automorfismo de Frobenius que:

$$\prod_{j=0}^{l_{t,u}-1} \sigma_q^j(G_{t,u}(x)) = \prod_{j=0}^{l_{t,u}-1} \prod_{i=0}^{k-1} (x^t - \sigma_q^j(\theta^{-u}\alpha^{trq^{is_n}})). \tag{2.7}$$

Observamos que o polinômio $\prod_{j=0}^{l_{t,u}-1} \sigma_q^j(G_{t,u}(x))$ possui peso, isto é, o número de coeficientes não nulos, limitado por

$$k \cdot l_{t,u} + 1 \leq k \cdot s_n + 1.$$

Em particular, se $f(x) = x - 1$, o peso de cada fator irredutível de $x^n - 1$ é no máximo $s_n + 1$.

Observação 2.14. *O caso $s_n = 1$ e alguns casos especiais com $s_n = 2$ são tratados em [7], onde os fatores irredutíveis são binômios e trinômios, respectivamente.*

O seguinte lema fornece uma maneira de obter o número $l_{t,u}$.

Lema 2.15. *O número $l_{t,u}$ é o menor inteiro positivo v tal que $\dfrac{\text{mdc}(n, q^{s_n} - 1)}{\text{mdc}(n, q^v - 1)}$ divide u.*

Demonstração. Por definição, $l_{t,u}$ é o menor inteiro positivo v tal que $G_{t,u} \in \mathbb{F}_{q^v}[x]$. Esta condição é equivalente a mostrar que

$$(\theta^{-u}\alpha^{-tr})^{q^v} = \theta^{-u}\alpha^{-trq^{is_n}} \text{ para algum inteiro } i,\ 0 \leq i < k. \tag{2.8}$$

Portanto, $\theta^{-u(q^v-1)} = \alpha^{-tr(q^{is_n}-q^v)}$. Em particular, temos que $\text{ord}(\theta^{-u(q^v-1)}) = \text{ord}(\alpha^{-tr(q^{is_n}-q^v)})$. Uma vez que as ordens de θ e α são relativamente primas, concluímos que:

$$\frac{d}{\text{mdc}(d, u(q^v-1))} = \frac{e}{\text{mdc}(e, tr(q^{is_n} - q^v))} = 1.$$

Em particular, $d = \text{mdc}(n, q^{s_n} - 1)$ divide $u(q^v - 1)$. Como v divide s_n, $q^v - 1$ divide $q^{s_n} - 1$ e temos que $\text{mdc}(\text{mdc}(n, q^{s_n} - 1), q^v - 1) = \text{mdc}(n, q^v - 1)$. Portanto, $\frac{\text{mdc}(n,q^{s_n}-1)}{\text{mdc}(n,q^v-1)}$ divide u. Reciprocamente, se v é um inteiro positivo tal que $\frac{\text{mdc}(n,q^{s_n}-1)}{\text{mdc}(n,q^v-1)}$ divide u, então

$$d = \text{mdc}(n, q^{s_n} - 1) = \frac{\text{mdc}(n, q^{s_n} - 1)}{\text{mdc}(n, q^v - 1)} \cdot \text{mdc}(n, q^v - 1) \mid u \cdot \text{mdc}(n, q^v - 1) \mid u(q^v - 1).$$

Uma vez que $\text{mdc}(k, s_n) = 1$, existe i tal que $is_n \equiv v \pmod{k}$ e desta forma

$$\alpha^{q^{is_n} - q^v} = 1 = \theta^{-u(q^v-1)},$$

logo $\alpha^{tr(q^{is_n}-q^v)} = \theta^{-u(q^v-1)}$ e segue da igualdade em (2.8) que $G_{t,u} \in \mathbb{F}_{q^v}[x]$. ■

Observação 2.16. *O número $l_{t,u}$ não depende de t e a partir de agora o denotaremos apenas por l_u.*

Nosso objetivo agora é contar o número de fatores irredutíveis de $f(x^n)$ sobre $\mathbb{F}_q$. Para este propósito, apresentamos a seguinte definição.

Definição 2.17. *Para cada divisor s de s_n, definimos:*

$$\Lambda_t(s) = |\{G_{t,u} \in \mathbb{F}_{q^s}[x]; G_{t,u} \text{ divide } f(x^n)\}|$$

e

$$\Omega_t(s) = |\{G_{t,u} \in \mathbb{F}_{q^s}[x]; G_{t,u} \text{ divide } f(x^n) \text{ e } G_{t,u} \notin \mathbb{F}_{q^v}[x] \text{ para qualquer } v < s\}|,$$

onde os polinômios $G_{t,u}$ são dados pela fórmula (2.6)*.*

O seguinte lema determina os valores das funções definidas anteriormente.

Lema 2.18. *Sejam $t \in \mathbb{Z}_+$ um divisor de m e $r_{n,t}$ o menor divisor inteiro positivo de s_n tal que* $\operatorname{mdc}\left(\dfrac{\operatorname{mdc}(n, q^{s_n}-1)}{\operatorname{mdc}(n, q^{r_{n,t}}-1)}, t\right) = 1$*. Para qualquer divisor s de s_n, são verdadeiras:*

(a) Se $r_{n,t}$ não divide s então $\Lambda_t(s) = \Omega_t(s) = 0$;

(b) Se $r_{n,t}$ divide s então

$$\Lambda_t(s) = \frac{\varphi(t)}{t} \operatorname{mdc}(n, q^s - 1)$$

e

$$\Omega_t(s) = \frac{\varphi(t)}{t} \sum_{r_{n,t} | v | s} \mu\left(\frac{s}{v}\right) \operatorname{mdc}(n, q^v - 1),$$

onde μ é a função de Möbius .

Demonstração. Do Lema 2.15, temos que $G_{u,t} \in \mathbb{F}_{q^s}[x]$ se, e somente se, $\frac{\operatorname{mdc}(n, q^{s_n}-1)}{\operatorname{mdc}(n, q^s-1)}$ divide u. Assim, se $G_{u,t}(x)$ está em $\mathbb{F}_{q^s}[x]$ então $\operatorname{mdc}\left(\frac{\operatorname{mdc}(n, q^{s_n}-1)}{\operatorname{mdc}(n, q^s-1)}, t\right) = 1$, pois $\operatorname{mdc}(t, u) = 1$.

Suponhamos por contradição que $r_{n,t}$ não divide s e que $\Lambda_t(s) \neq 0$. Por hipótese

$$\operatorname{mdc}\left(\frac{\operatorname{mdc}(n, q^{s_n}-1)}{\operatorname{mdc}(n, q^{r_{n,t}}-1)}, t\right) = 1 = \operatorname{mdc}\left(\frac{\operatorname{mdc}(n, q^{s_n}-1)}{\operatorname{mdc}(n, q^s-1)}, t\right)$$

Como $t \mid n$, para cada divisor primo p de t temos que $\nu_p(n) \geq 1$ e como $\operatorname{rad}(n) \mid (q^{s_n}-1)$ temos que $p \mid (q^{s_n}-1)$ e portanto:

$$\min\{\nu_p(n), \nu_p(q^{s_n}-1)\} = \min\{\nu_p(n), \nu_p(q^{r_{n,t}}-1)\} = \min\{\nu_p(n), \nu_p(q^s-1)\} \geq 1.$$

Seja $s' = \text{mdc}(r_{n,t}, s)$ então, existem inteiros positivos a e b tais que $s' = ar_{n,t} - bs$. Assim,

$$\begin{aligned} \nu_p(q^{s'} - 1) &= \nu_p(q^{ar_{n,t}-bs} - 1) = \nu_p(q^{ar_{n,t}} - q^{bs}) \\ &\geq \min\{\nu_p(q^{ar_{n,t}} - 1), \nu_p(q^{bs} - 1)\} \\ &\geq \min\{\nu_p(q^{r_{n,t}} - 1), \nu_p(q^{s} - 1)\}. \end{aligned}$$

Em particular, $\min\{\nu_p(n), \nu_p(q^{s_n} - 1)\} = \min\{\nu_p(n), \nu_p(q^{s'} - 1)\}$ para cada divisor primo p de t, o que gera uma contradição uma vez que $s' < r_{n,t}$. Portanto, se $r_{n,t} \nmid s$ então $\Lambda_t(s) = 0$.

Agora, seja s um divisor positivo de s_n tal que $r_{n,t} | s$. Sabemos que qualquer fator $G_{t,u}$ de $f(x^n)$ com coeficientes em $\mathbb{F}_{q^s}$ satisfaz as condições:

- $\text{mdc}(u,t) = 1$ com $1 \leq u \leq \text{mdc}(n, q^{s_n} - 1)$;
- $\frac{\text{mdc}(n,q^{s_n}-1)}{\text{mdc}(n,q^s-1)}$ divide u.

Assim, $u = \frac{\text{mdc}(n,q^{s_n}-1)}{\text{mdc}(n,q^s-1)} u'$ com $\text{mdc}(u',t) = 1$ e $1 \leq u' \leq \text{mdc}(n, q^s - 1)$.

Além disso, se p é um divisor primo de t então $p \mid m$ e temos que $\nu_p(n) > \nu_p(q^{s_n} - 1) \geq 1$. Entretanto, como $\text{mdc}(u,t) = 1$ temos que $p \nmid \frac{\text{mdc}(n,q^{s_n}-1)}{\text{mdc}(n,q^s-1)}$, logo p divide $q^s - 1$, o que implica que $\text{rad}(t) \mid (q^s - 1)$. Concluímos que o número de u' é igual a:

$$\Lambda_t(s) = \varphi(\text{rad}(t)) \cdot \frac{\text{mdc}(n, q^s - 1)}{\text{rad}(t)} = \frac{\varphi(t)}{t} \text{mdc}(n, q^s - 1).$$

Por fim, observamos que $\Lambda_t(s) = \sum_{v|s} \Omega_t(v)$ e aplicando a fórmula de inversão de Möbius obtemos a igualdade:

$$\Omega_t(s) = \sum_{v|s} \mu\left(\frac{s}{v}\right) \Lambda_t(v) = \sum_{r_{n,t}|v|s} \mu\left(\frac{s}{v}\right) \frac{\varphi(t)}{t} \text{mdc}(n, q^v - 1).$$

■

A partir do lema anterior, obtemos uma fórmula explicita para o número de fatores irredutíveis de $f(x^n)$ sobre $\mathbb{F}_q$.

Teorema 2.19. *Sejam $f \in \mathbb{F}_q[x]$ polinômio irredutível de grau k e ordem $\mathfrak{e}$. Seja n um inteiro positivo tal que $\text{mdc}(n, \mathfrak{e}k) = \text{mdc}(k, s_n) = 1$. Como antes, $m := \frac{n}{\text{mdc}(n,q^{s_n}-1)}$. O número de fatores irredutíveis de $f(x^n)$ em $\mathbb{F}_q[x]$ é igual a:*

$$\frac{1}{s_n} \sum_{t|m} \frac{\varphi(t)}{t} \sum_{r_{n,t}|v|s_n} \text{mdc}(n, q^v - 1) \varphi\left(\frac{s_n}{v}\right),$$

ou equivalentemente,

$$\frac{1}{s_n} \sum_{v|s_n} \text{mdc}(n, q^v - 1) \varphi\left(\frac{s_n}{v}\right) \prod_{p|m_v} \left(1 + \nu_p(m_v) \frac{p-1}{p}\right),$$

onde $m_v = \max\left\{t \,\middle|\, t \text{ divide } m \text{ e } \operatorname{mdc}\left(\frac{\operatorname{mdc}(n,q^{s_n}-1)}{\operatorname{mdc}(n,q^v-1)},t\right)=1\right\}$ *e o produto acima é sobre os divisores primos de* m_v.

Demonstração. Da demonstração do lema acima, temos que o número de fatores irredutíveis de $f(x^n)$ em $\mathbb{F}_q[x]$ é igual a:

$$\begin{aligned}
\sum_{t|m}\sum_{s|s_n}\frac{1}{s}\Omega_t(s) &= \sum_{t|m}\frac{\varphi(t)}{t}\sum_{r_{n,t}|s|s_n}\frac{1}{s}\sum_{v'|\frac{s}{r_{n,t}}}\mu\left(\frac{s}{r_{n,t}v'}\right)\operatorname{mdc}(n,q^{v'r_{n,t}}-1)\\
&= \sum_{t|m}\frac{\varphi(t)}{t}\sum_{s'|\frac{s_n}{r_{n,t}}}\frac{1}{r_{n,t}s'}\sum_{v'|s'}\mu\left(\frac{s'}{v'}\right)\operatorname{mdc}(n,q^{v'r_{n,t}}-1)\\
&= \sum_{t|m}\frac{\varphi(t)}{t}\sum_{v'|\frac{s_n}{r_{n,t}}}\frac{\operatorname{mdc}(n,q^{v'r_{n,t}}-1)}{r_{n,t}}\sum_{v'|s'|\frac{s_n}{r_{n,t}}}\frac{\mu\left(\frac{s'}{v'}\right)}{s'}\\
&= \sum_{t|m}\frac{\varphi(t)}{t}\sum_{v'|\frac{s_n}{r_{n,t}}}\frac{\operatorname{mdc}(n,q^{v'r_{n,t}}-1)}{v'r_{n,t}}\sum_{s''|\frac{s_n}{v'r_{n,t}}}\frac{\mu(s'')}{s''}\\
&= \sum_{t|m}\frac{\varphi(t)}{t}\sum_{r_{n,t}|v|s_n}\frac{\operatorname{mdc}(n,q^v-1)}{v}\sum_{s|\frac{s_n}{v}}\frac{\mu(s)}{s}\\
&= \frac{1}{s_n}\sum_{t|m}\frac{\varphi(t)}{t}\sum_{r_{n,t}|v|s_n}\operatorname{mdc}(n,q^v-1)\varphi\left(\frac{s_n}{v}\right).
\end{aligned}$$

■

Corolário 2.20. *Seja n um inteiro positivo e primo relativo com q. O número de elementos normais da extensão* $\mathbb{F}_{q^n}$ *sobre* $\mathbb{F}_q$ *é dado por:*

$$q^n\prod_{t|m}\prod_{s|s_m}\left(1-\frac{1}{q^{st}}\right)^{\frac{\varphi(t)}{t}\sum\limits_{r_{n,t}|v|s}\mu\left(\frac{s}{v}\right)\operatorname{mdc}(n,q^v-1)}.$$

Demonstração. A prova segue diretamente da fórmula 1.2 e do Lema 2.18 ■

Corolário 2.21. *Seja* $\mathbb{F}$ *um corpo finito e* $\mathscr{C}=\{n\in\mathbb{N}|s_n=1\}$. *Seja* $\kappa(x^n-1)=\dfrac{\Phi_q(x^n-1)}{q^n}$ *a densidade de elementos normais na extensão* $\mathbb{F}_{q^n}$ *sobre* $\mathbb{F}_q$. *Então* $\liminf\limits_{\substack{n\to\infty\\ n\in\mathscr{C}}}\kappa(x^n-1)$ *pertence ao intervalo* (a,b) *onde*

$$a=\exp\Big(-\sum_{\operatorname{rad}(t)|(q-1)}\frac{1}{q^t-0{,}557305}\frac{\varphi(t)}{t}(q-1)\Big)\quad e\quad b=\exp\Big(-\sum_{\operatorname{rad}(t)|(q-1)}\frac{1}{q^t-0{,}5}\frac{\varphi(t)}{t}(q-1)\Big).$$

Demonstração. No caso que $n \in \mathscr{C}$ temos que

$$\kappa(x^n-1) = \frac{\Phi_q(x^n-1)}{q^n} = \prod_{t\mid \frac{n}{\mathrm{mdc}(q-1,n)}} \left(1-\frac{1}{q^t}\right)^{\frac{\varphi(t)}{t}\mathrm{mdc}(n,q-1)}. \tag{2.9}$$

Observemos que para todo n se tem que $\mathrm{mdc}(n,q-1) \le q-1$, e a igualdade é verdadeira quando n é um múltiplo de $q-1$. Como no caso considerado todo divisor primo de n é também divisor primo de $q-1$, segue que o limite inferior de (2.9) é dado por:

$$\liminf_{\substack{n\to\infty \\ n\in\mathscr{C}_1}} \frac{\Phi_q(x^n-1)}{q^n} = \prod_{\mathrm{rad}(t)\mid(q-1)} \left(1-\frac{1}{q^t}\right)^{\frac{\varphi(t)}{t}(q-1)}$$

Agora, como um exercício direto de cálculo diferencial, é possível mostrar que para todo $k \ge q \ge 2$

$$\left(1-\frac{1}{k}\right)^{k-0.5} < \frac{1}{e} < \left(1-\frac{1}{k}\right)^{k-f(q)},$$

onde $f(q) = q + \dfrac{1}{\ln\left(\frac{q-1}{q}\right)} \in (0.5, 0.557305)$ para todo $q \ge 2$. Segue deste resultado que

$$\left(1-\frac{1}{q^t}\right)^{q^t-0{,}5} < \frac{1}{e} < \left(1-\frac{1}{q^t}\right)^{q^t-f(q)} \tag{2.10}$$

Da segunda desigualdade temos $\left(1-\frac{1}{q^t}\right) > \left(\frac{1}{e}\right)^{\frac{1}{q^t-f(q)}}$, portanto

$$\left(1-\frac{1}{q^t}\right)^{\frac{\varphi(t)}{t}(q-1)} > e^{-\frac{1}{q^t-f(q)}\frac{\varphi(t)}{t}(q-1)}$$

De forma análoga obtermos $\left(1-\frac{1}{q^t}\right)^{\frac{\varphi(t)}{t}(q-1)} < e^{-\frac{1}{q^t-0{,}5}\frac{\varphi(t)}{t}(q-1)}$. Assim:

$$\prod_{\mathrm{rad}(t)\mid(q-1)} e^{-\frac{1}{q^t-f(q)}\frac{\varphi(t)}{t}(q-1)} < \prod_{\mathrm{rad}(t)\mid(q-1)} \left(1-\frac{1}{q^t}\right)^{\frac{\varphi(t)}{t}(q-1)} < \prod_{\mathrm{rad}(t)\mid(q-1)} e^{-\frac{1}{q^t-0{,}5}\frac{\varphi(t)}{t}(q-1)}$$

■

2.3 Fatores de $f(x^n)$ quando s_n é um número primo

Nesta seção, como aplicação dos resultados anteriores, consideramos alguns casos onde s_n é um número primo. Ao longo dessa seção, para cada d com $\mathrm{mdc}(q,d) = 1$, denotaremos por $\sim_d$ a relação de equivalência definida por:

$$a \sim_d b \text{ se existe } j \in \mathbb{N} \text{ tal que } a \equiv bq^j \pmod{d},$$

isto é, $\sim_d$ define as classes q-ciclotômicas módulo d.

2.3.1 O caso $\mathrm{rad}(n) \mid (q-1)$

No Teorema 2.3 assumimos que $q \equiv 1 \pmod 4$ se $8 \mid n$. Aqui, apresentamos o caso complementar do Teorema 2.3, ou seja, assumimos que $q \equiv 3 \pmod 4$ e $8|n$, mas mantemos as demais condições, em particular a condição $\mathrm{rad}(n)|(q-1)$.

Teorema 2.22. *Sejam n um inteiro, q uma potência de primo tais que $8|n$ e $q \equiv 3 \pmod 4$. Sejam θ um elemento em $\mathbb{F}_{q^2}^*$ com ordem $d = \mathrm{mdc}(n, q^2-1)$ e $f(x)$ um polinômio irredutível de grau k e ordem $\mathfrak{e}$. Além disso, seja $g_t(x)$ como no Lema 2.1 . Então $d = 2^l \,\mathrm{mdc}(n, q-1)$, onde $l = \min\left\{\nu_2\left(\frac{n}{2}\right), \nu_2(q+1)\right\}$, e $f(x^n)$ é fatorado em fatores irredutíveis em $\mathbb{F}_q[x]$ como:*

$$f(x^n) = \prod_{\substack{t \mid m \\ t \text{ ímpar}}} \prod_{\substack{1 \leqslant w \leqslant \mathrm{mdc}(n,q-1) \\ \mathrm{mdc}(w,t)=1}} \beta^{-wk} g_t(\beta^w x^t) \prod_{t \mid m} \prod_{u \in R_t} H_u, \tag{2.11}$$

com $H_u = \theta^{-uk(q+1)} g_t(\theta^u x^t) g_t(\theta^{uq} x^t)$, $m = \frac{n}{d} = \frac{n}{\mathrm{mdc}(n,q^2-1)}$, $\beta = \theta^{2^l}$ é uma raiz $\mathrm{mdc}(n,q-1)$-ésima primitiva da unidade e $\mathscr{R}_t$ é o conjunto das q- classes ciclotômicas

$$\mathscr{R}_t = \left\{u \in \mathbb{N} | 1 \leq u \leq d, \mathrm{mdc}(u,t) = 1, 2^l \nmid u\right\} / \sim_d,$$

Além disso, o número total de fatores irredutíveis de $f(x^n)$ em $\mathbb{F}_q[x]$ é:

$$\mathrm{mdc}(n, q-1)\left(\frac{1}{2} + 2^{l-2}(2 + \nu_2(m))\right) \prod_{\substack{p \mid m \\ p \text{ primo}}} \left(1 + \nu_p(m)\frac{p-1}{p}\right).$$

Demonstração. Como $q \equiv 3 \pmod 4$ e $8|n$, da Definição 2.11 obtemos que $s_n = 2$. Assim:

$$d = \mathrm{mdc}(n, q^2-1) = 2\,\mathrm{mdc}\left(\frac{n}{2}, \frac{q-1}{2}(q+1)\right) = 2\,\mathrm{mdc}\left(\frac{n}{2}, \frac{q-1}{2}\right)\mathrm{mdc}\left(\frac{n}{2}, q+1\right),$$

onde

$$\mathrm{mdc}\left(\frac{n}{2}, q+1\right) = 2^{\min\{\nu_2(\frac{n}{2}), \nu_2(q+1)\}} = 2^l.$$

Segue do Lema 2.15 que $G_{tu}(x) = \theta^{-uk} g_t(\theta^u x^t) \notin \mathbb{F}_q[x]$ se $\dfrac{\mathrm{mdc}(n,q^2-1)}{\mathrm{mdc}(n,q-1)} = 2^l$ não divide u, isto é, a classe de u está em $\mathscr{R}_t$. Então a fatoração em (2.11) segue da Equação 2.7. Uma vez que $s_n = 2$ e $r_{n,t}$ é um divisor de s_n, para determinar quantos fatores de cada grau, é necessário analizar dois casos: $r_{n,t} = 1$ ou $r_{n,t} = 2$.

Se $r_{n,t} = 1$, temos que t satisfaz a seguinte igualdade:

$$\mathrm{mdc}\left(\frac{\mathrm{mdc}(n,q^2-1)}{\mathrm{mdc}(n,q-1)}, t\right) = \mathrm{mdc}(2^l, t) = 1.$$

Em particular, t deve ser ímpar.

Se $r_{n,t}=2$, recordando que $r_{n,t}$ é o menor divisor positivo de s_n tal que $\operatorname{mdc}\left(\frac{\operatorname{mdc}(n,q^2-1)}{\operatorname{mdc}(n,q^2-1)},t\right)=1$, concluímos que t é par. Posto isto, do Teorema 2.19 obtemos que o número de fatores irredutíveis de $f(x^n)$ em $\mathbb{F}_q[x]$ é igual a

$$\begin{aligned}
&\frac{1}{2}\sum_{v|2}\operatorname{mdc}(n,q^v-1)\varphi\left(\frac{2}{v}\right)\prod_{p|m_v}\left(1+\nu_p(m_v)\frac{p-1}{p}\right)\\
&=\frac{1}{2}\operatorname{mdc}(n,q-1)\prod_{p|m_1}\left(1+\nu_p(m)\frac{p-1}{p}\right)+\frac{1}{2}\operatorname{mdc}(n,q^2-1)\prod_{p|m_2}\left(1+\nu_p(m)\frac{p-1}{p}\right)\\
&=\frac{1}{2}\operatorname{mdc}(n,q-1)\prod_{\substack{p|m\\ p\neq 2}}\left(1+\nu_p(m)\frac{p-1}{p}\right)+\frac{1}{2}\operatorname{mdc}(n,q^2-1)\prod_{p|m}\left(1+\nu_p(m)\frac{p-1}{p}\right)\\
&=\frac{1}{2}\operatorname{mdc}(n,q-1)\left(1+2^l\left(1+\frac{1}{2}\nu_2(m)\right)\right)\prod_{\substack{p|m\\ p\neq 2}}\left(1+\nu_p(m)\frac{p-1}{p}\right).
\end{aligned}$$

■

Na próxima subseção supomos que $\operatorname{rad}(n)|(q^p-1)$ onde p é um primo ímpar.

2.3.2 Caso $\operatorname{rad}(n)|(q^p-1)$ com p primo ímpar e $\operatorname{rad}(n)\nmid(q-1)$

Nas seções anteriores, descrevemos o caso em que $\operatorname{rad}(n)|(q-1)$. Agora, iremos considerar o caso em que n tem pelo menos um fator que não divide $q-1$.

Teorema 2.23. *Sejam n um inteiro positivo tal que $\operatorname{ord}_{\operatorname{rad}(n)}q$ é um primo ímpar p e $f\in\mathbb{F}_q[x]$ um polinômio irredutível de grau k e ordem $\mathfrak{e}$ tal que $\operatorname{mdc}(k\mathfrak{e},n)=\operatorname{mdc}(k,p)=1$; além disso, suponhamos que $q\equiv 1 \pmod 4$ se $8|n$. Seja θ um elemento em $\mathbb{F}_{q^p}^*$ com ordem $d:=\operatorname{mdc}(n,q^p-1)$, $m:=\frac{n}{d}=\frac{n}{\operatorname{mdc}(n,q^p-1)}$ e $g_t(x)$ como no Lema 2.1. O polinômio $f(x^n)$ se decompõe em fatores irredutíveis sobre $\mathbb{F}_q[x]$ como*

$$\prod_{\substack{t|m\\ \operatorname{rad}(t)|(q-1)}}\prod_{\substack{1\leqslant v\leqslant d'\\ \operatorname{mdc}(v,t)=1}}\beta^{-vk}g_t(\beta^v x^t)\prod_{\substack{t|m\\ \operatorname{rad}(t)\nmid(q-1)}}\prod_{u\in R_t}H_u,$$

com $H_u=\theta^{-uk(1+\cdots+q^{p-1})}g_t(\theta^u x^t)\cdots g_t(\theta^{uq^{p-1}}x^t)$,

1) $d':=\operatorname{mdc}(n,q-1)$, $\beta:=\theta^{\operatorname{mdc}(n,\frac{q^p-1}{q-1})}$ é uma d'-ésima raiz primitiva da unidade e

$$R_t=\left\{u\in\mathbb{N}\,\middle|\,1\leq u\leq d,\quad \operatorname{mdc}\left(n,\frac{q^p-1}{q-1}\right)\nmid u,\quad \operatorname{mdc}(u,t)=1\right\}/\sim_d$$

nos casos em que $p\nmid n$ ou $p\nmid(q-1)$ ou $\nu_p(n)>\nu_p(q-1)\geq 1$.

2) $d' := p \cdot \mathrm{mdc}(\frac{n}{p}, q-1)$, $\beta := \theta^{\mathrm{mdc}\left(\frac{n}{p}, \frac{1}{p}\frac{q^p-1}{q-1}\right)}$ *é uma* d'*-ésima raiz primitiva da unidade e*

$$R_t = \left\{ u \in \mathbb{N} \,\middle|\, 1 \le u \le d, \quad \mathrm{mdc}\left(\frac{n}{p}, \frac{1}{p}\frac{q^p-1}{q-1}\right) \nmid u, \quad \mathrm{mdc}(u,t) = 1 \right\} / \sim_d$$

no caso em que p *divide* $\mathrm{mdc}(n, q-1)$ *e* $\nu_p(n) \le \nu_p(q-1)$.

Demonstração. Por hipótese o $\mathrm{mdc}(k,p) = 1$, o que implica que $f(x)$ é irredutível em $\mathbb{F}_{q^p}[x]$ (ver Corolário 1.38). Como $q \equiv 1 \pmod 4$ se $8 \mid n$ temos que $q^p \equiv 1 \pmod 4$ se $8|n$ e segue diretamente do Teorema 2.3 que a decomposição de $f(x^n)$ em fatores irredutíveis em $\mathbb{F}_{q^p}[x]$ é:

$$f(x^n) = \prod_{t|m} \prod_{\substack{1 \leqslant u \leqslant d \\ \mathrm{mdc}(u,t)=1}} \left(\theta^{-uk} g_t(\theta^u x^t)\right),$$

onde θ é um elemento em $\mathbb{F}_{q^p}^*$ com ordem $d = \mathrm{mdc}(n, q^p - 1)$.

Afirmamos que $\theta^{-uk} g_t(\theta^u x^t)$ está em $\mathbb{F}_q[x]$ se, e somente se, $d \mid u(q-1)$. De fato, como

$$\theta^{-uk} g_t(\theta^u x^t) = \prod_{i=0}^{k-1} (x^t - \theta^{-u} \alpha^{-trq^i}),$$

temos que $\theta^{-uk} g_t(\theta^u x^t) \in \mathbb{F}_q[x]$ se para cada inteiro i existe j tal que $(\theta^{-u}\alpha^{-trq^i})^q = \theta^{-u}\alpha^{-trq^j}$ ou equivalentemente $\theta^{-u(q-1)} = \alpha^{tr(q^{i+1}-q^j)}$. Em particular, temos que

$$\mathrm{ord}(\alpha^{tr(q^{i+1}-q^j)}) = \frac{\mathfrak{e}}{\mathrm{mdc}(\mathfrak{e}, tr(q^{i+1}-q^j))} = \frac{\mathfrak{e}}{\mathrm{mdc}(\mathfrak{e}, q^{i+1}-q^j)}$$

e

$$\mathrm{ord}(\theta^{-u}(q-1)) = \frac{d}{\mathrm{mdc}(d, u(q-1))}$$

são iguais. Uma vez que $\mathrm{mdc}(\mathfrak{e}, d) = 1$, estas ordens são iguais a 1 e portanto $\mathfrak{e} \mid (q^{i+1} - q^j)$ e $d \mid u(q-1)$. Como a primeira condição pode ser obtida por uma escolha adequada de j, temos que $\theta^{-uk} g_t(\theta^u x^t) \in \mathbb{F}_q[x]$ se, e somente se, $d \mid u(q-1)$. Assim, a condição deste polinômio estar no corpo $\mathbb{F}_q$ foi transformada em uma condição aritmética que pode ser analizada considerando os seguintes casos:

1. $p \nmid n$ ou $p \nmid (q-1)$; em ambos os casos temos que:

$$\mathrm{mdc}(n, q^p - 1) = \mathrm{mdc}\left(n, \frac{q^p-1}{q-1}(q-1)\right) = \mathrm{mdc}\left(n, \frac{q^p-1}{q-1}\right) . \mathrm{mdc}(n, q-1). \tag{2.12}$$

Logo, $\mathrm{mdc}(n, q^p - 1) | u(q-1)$ se, e somente se, $\mathrm{mdc}\left(n, \frac{q^p-1}{q-1}\right) | u$.

2. $p|n$ e $p|(q-1)$; temos que:

$$\begin{aligned}\mathrm{mdc}(n, q^p-1) &= \mathrm{mdc}\left(n, \frac{q^p-1}{q-1}(q-1)\right) = p\cdot\mathrm{mdc}\left(\frac{n}{p}, \frac{1}{p}\left(\frac{q^p-1}{q-1}\right)(q-1)\right)\\ &= p\cdot\mathrm{mdc}\left(\frac{n}{p}, \frac{1}{p}\frac{q^p-1}{q-1}\right)\cdot\mathrm{mdc}\left(\frac{n}{p}, q-1\right). \qquad (2.13)\end{aligned}$$

Portanto, $\mathrm{mdc}(n, q^p-1)|u(q-1)$ se, e somente se,

$$p\cdot\mathrm{mdc}\left(\frac{n}{p}, \frac{1}{p}\frac{q^p-1}{q-1}\right)\cdot\mathrm{mdc}\left(\frac{n}{p}, q-1\right)|u(q-1). \qquad (2.14)$$

que será dividido em dois subcasos:

2.1. Se $\nu_p(n) \le \nu_p(q-1)$, a condição (2.14) é equivalente a

$$\mathrm{mdc}\left(\frac{n}{p}, \frac{1}{p}\frac{q^p-1}{q-1}\right)|u.$$

2.2. Se $\nu_p(n) > \nu_p(q-1)$, a condição (2.14) é equivalente a

$$\mathrm{mdc}\left(n, \frac{q^p-1}{q-1}\right)|u.$$

Note que, nos Casos 1 e 2.2 a conclusão é a mesma. Portanto, nestes casos $\theta^{-uk}g_t(\theta^u x^t) \in \mathbb{F}_q[x]$ se, e somente se, $u = \mathrm{mdc}\left(n, \frac{q^p-1}{q-1}\right)\cdot v$ para algum inteiro positivo v.

Como $1 \le u \le \mathrm{mdc}(n, q^p-1)$, segue diretamente de 2.12 que $1 \le v \le \gcd(n, q-1)$. Além disso, uma vez que $\mathrm{mdc}(u,t) = 1$, temos que $\mathrm{mdc}(v,t) = 1$ e $\nu_{p'}(q^p-1) = \nu_{p'}(q-1)$ para cada primo $p'|t$.

Portanto, nos Casos 1 e 2.2 os números v e t satisfaz as condições $\mathrm{mdc}(v,t) = 1$ e $\mathrm{rad}(t)|(q-1)$.

Agora, no Caso 2.1 temos que $\theta^{-uk}g_t(\theta^u x^t) \in \mathbb{F}_q[x]$ se, e somente se, $u = \mathrm{mdc}\left(\frac{n}{p}, \frac{1}{p}\frac{q^p-1}{q-1}\right)v$ para algum inteiro v.

Como $1 \le u \le \gcd(n, q^p-1)$, segue da Equação 2.13 que $1 \le v \le p\cdot\mathrm{mdc}\left(\frac{n}{p}, q-1\right)$. Da mesma forma como foi analisado o caso anterior, obtemos que v e t satisfaz as condições $\mathrm{mdc}(v,t) = 1$ e $\mathrm{rad}(t)|(q-1)$. Desta forma concluímos que os fatores irredutíveis de $f(x^n)$ em $\mathbb{F}_{q^p}[x]$ que estão $\mathbb{F}_q[x]$ são da forma

$$\theta^{-uk}g_t(\theta^u x^t) = \beta^{-vk}g_t(\beta^v x^t),$$

onde $\mathrm{rad}(t)|(q-1)$ e β é um elemento de $\mathbb{F}_q^*$ de ordem d'.

Por fim, se $\mathrm{rad}(t) \nmid (q-1)$, temos que $\theta^{-uk} g_t(\theta^u x^t) \in \mathbb{F}_{q^p}[x] \setminus \mathbb{F}_q[x]$. Assim o polinômio

$$\prod_{i=0}^{p-1} \theta^{-ukq^i} g_t(\theta^{uq^i} x^t)$$

é o produto dos conjugados distintos de $\theta^{-uk} g_t(\theta^u x^t)$ pelo o automorfismo de Frobenius σ_q. Além disso, tal polinômio é mônico e irredutível sobre $\mathbb{F}_q$. ■

Admitindo as condições do Teorema 2.23, apresentamos um resultado que nos fornece informações sobre o número de fatores irredutíveis de $f(x^n)$.

Corolário 2.24. *Sejam n, m, q e $f \in \mathbb{F}_q[x]$ como no Teorema 2.23. Então o número de fatores irredutíveis $f(x^n)$ em $\mathbb{F}_q[x]$ é igual a*

$$\frac{p-1}{p}\,\mathrm{mdc}(n, q-1) \prod_{\substack{p' \mid m' \\ p' primo}} \left(1 + \nu_{p'}(m)\frac{p'-1}{p'}\right) + \frac{\mathrm{mdc}(n, q^p-1)}{p} \prod_{\substack{p' \mid m \\ p' \ primo}} \left(1 + \nu_{p'}(m)\frac{p'-1}{p'}\right),$$

onde m' é o maior divisor de m que é relativamente primo com $\begin{cases} \frac{1}{p}\frac{q^p-1}{q-1} & \text{se } \nu_p(q-1) \geq \nu_p(n) > 0 \\ \frac{q^p-1}{q-1} & \text{caso contrário.} \end{cases}$

Demonstração. Desde que $s_n = p$, segue do Teorema 2.19 que o número de fatores irredutíveis de $f(x^n)$ sobre $\mathbb{F}_q[x]$ é igual a

$$\frac{1}{p}\left(\mathrm{mdc}(n, q-1)\varphi(p) \prod_{p' \mid m_1} \left(1 + \nu_{p'}(m_1)\frac{p'-1}{p'}\right) + \mathrm{mdc}(n, q^p-1)\varphi(1) \prod_{p' \mid m_p} \left(1 + \nu_{p'}(m_p)\frac{p'-1}{p'}\right)\right)$$

$$= \frac{p-1}{p}\,\mathrm{mdc}(n, q-1) \prod_{\substack{p' \mid m_1 \\ p' \text{primo}}} \left(1 + \nu_{p'}(m_1)\frac{p'-1}{p'}\right) + \frac{\mathrm{mdc}(n, q^p-1)}{p} \prod_{\substack{p' \mid m_p \\ p' \text{ primo}}} \left(1 + \nu_{p'}(m_p)\frac{p'-1}{p'}\right),$$

onde m_p é o maior divisor t de m tal que $\mathrm{mdc}\left(\frac{\mathrm{mdc}(n,q^p-1)}{\mathrm{mdc}(n,q^p-1)}, t\right) = 1$, (o que se tem trivialmente) e m_1 é o maior divisor t de m tal que $\mathrm{mdc}\left(\frac{\mathrm{mdc}(n,q^p-1)}{\mathrm{mdc}(n,q-1)}, t\right) = 1$. Em particular, temos que $m_p = m$. Das Equações (2.12) e (2.13), obtemos a seguinte igualdade:

$$\frac{\mathrm{mdc}(n, q^p-1)}{\mathrm{mdc}(n, q-1)} = \begin{cases} \mathrm{mdc}\left(\frac{n}{p}, \frac{1}{p}\frac{q^p-1}{q-1}\right) & \text{se } \nu_p(q-1) \geq \nu_p(n) > 0, \\ \mathrm{mdc}\left(n, \frac{q^p-1}{q-1}\right) & \text{caso contrário.} \end{cases}$$

Como m_1 é relativamente primo com $\frac{\mathrm{mdc}(n,q^p-1)}{\mathrm{mdc}(n,q-1)}$, temos que $m_1 = m'$. Portanto, o resultado segue do seguinte fato: $\nu_{p'}(m') = \nu_{p'}(m)$ para cada divisor primo p' de m'. ■

2.4 $q \equiv 3 \pmod 4$ e $8 \mid n$

Nesta seção, iremos considerar o caso complementar do Teorema 2.23, isto é, $q \equiv 3 \pmod 4$ e $8 \mid n$. Aqui, $f(x) \in \mathbb{F}_q[x]$ é um polinômio irredutível de grau k e ordem $\mathfrak{e}$ com $\mathrm{mdc}(\mathfrak{e}, n) = \mathrm{mdc}(k, p(q^{2p}-1)) = 1$ e $\mathrm{rad}(n) \mid (q^p - 1)$.

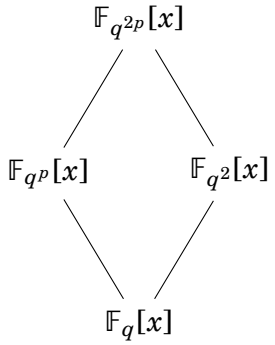
Da hipótese $q \equiv 3 \pmod 4$ temos que $q^{2p} \equiv 1 \pmod 4$ e sendo $\mathrm{mdc}(k, p(q^{2p}-1)) = 1$ concluímos que $\mathrm{mdc}(k, 2p) = 1$. Consequetemente, $f(x)$ é irredutível em $\mathbb{F}_{q^{2p}}$ (Corolário 1.38) e, pelo Teorema 2.3, $f(x^n)$ se decompõe em fatores irredutíveis sobre $\mathbb{F}_{q^{2p}}[x]$ como,

$$f(x^n) = \prod_{t \mid m} \prod_{\substack{1 \leqslant u \leqslant \mathrm{mdc}(n, q^{2p}-1) \\ \mathrm{mdc}(u,t)=1}} \theta^{-uk} g_t(\theta^u x^t) \tag{2.15}$$

onde $m = \frac{n}{\mathrm{mdc}(n, q^{2p}-1)}$ e

$$\theta^{-uk} g_t(\theta^u x^t) = \prod_{i=0}^{k-1} (x^t - \theta^{-u} \alpha^{-trq^{2pi}}) = \prod_{i=0}^{k-1} (x^t - \theta^{-u} \alpha^{-trq^i}),$$

Afirmamos que cada um dos fatores da Equação (2.15) esta em algum anel de polinômios do seguinte diagrama abaixo:



De fato, temos que $\theta^{-uk} g_t(\theta^u x^t) \in \mathbb{F}_{q^s}[x]$ onde $s \in \{1, 2, p\}$ se, e somente se, para cada inteiro i, existe um inteiro j, tal que $(\theta^{-u} \alpha^{-trq^i})^{q^s} = \theta^{-u} \alpha^{-trq^j}$, ou equivalentemente $\theta^{u(q^s-1)} = \alpha^{-tr(q^j - q^{i+s})}$.

Seguindo os mesmos passos da prova do Teorema 2.22, obtemos que a condição acima é equivalente a

I) $\mathrm{mdc}(n, q^{2p}-1) \mid u(q^s - 1)$

II) $\mathfrak{e} \mid (q^j - q^{i+s})$

Uma vez que, o item II sempre admite solução, precisamos analisar apenas o item I.

Como

$$d := \mathrm{mdc}(n, q^{2p}-1) = \mathrm{mdc}\left(n, (q^s-1)\left(\frac{q^{2p}-1}{q^s-1}\right)\right), \tag{2.16}$$

seguindo os mesmos passos da prova do Teorema 2.23, obtemos:

$$d = \begin{cases} \mathrm{mdc}(n, q^s-1)\mathrm{mdc}(\frac{n}{2}, \frac{q^{2p}-1}{q^s-1}) & \text{se } p \nmid n \text{ ou } p \nmid (q-1) \text{ e } s \in \{1, p\} \\ \mathrm{mdc}(\frac{n}{2}, q^s-1)\mathrm{mdc}(n, \frac{q^{2p}-1}{q^s-1}) & \text{se } p \nmid n \text{ ou } p \nmid (q-1) \text{ e } s = 2 \\ \mathrm{mdc}(\frac{n}{p}, q^s-1)\mathrm{mdc}(\frac{n}{2}, \frac{q^{2p}-1}{q^s-1}) & \text{se } p|n,\ p|(q-1) \text{ e } s \in \{1, p\} \\ \mathrm{mdc}(\frac{n}{2p}, q^s-1)\mathrm{mdc}(n, \frac{q^{2p}-1}{q^s-1}) & \text{se } p|n,\ p|(q-1) \text{ e } s = 2. \end{cases}$$

Do fato de que:

$$\mathrm{mdc}\left(\frac{n}{2}, \frac{q^{2p}-1}{q^p-1}\right) = \mathrm{mdc}\left(\frac{n}{2}, q^p+1\right) = 2^l,$$

onde $l = \min\{v_2(\frac{n}{2}), v_2(q+1)\}$, temos

$$\mathrm{mdc}\left(\frac{n}{2}, \frac{q^{2p}-1}{q-1}\right) = \mathrm{mdc}\left(\frac{n}{2}, \frac{q^p-1}{q-1}(q^p+1)\right) = \mathrm{mdc}\left(n, \frac{q^p-1}{q-1}\right)\mathrm{mdc}\left(\frac{n}{2}, q^p+1\right) = 2^l\,\mathrm{mdc}\left(n, \frac{q^p-1}{q-1}\right)$$

e

$$\mathrm{mdc}\left(n, \frac{q^{2p}-1}{q^2-1}\right) = \mathrm{mdc}\left(n, \frac{q^p-1}{q-1}\cdot\frac{q^p+1}{q+1}\right) = \mathrm{mdc}\left(n, \frac{q^p-1}{q-1}\right)\mathrm{mdc}\left(n, \frac{q^p+1}{q+1}\right) = \mathrm{mdc}\left(n, \frac{q^p-1}{q-1}\right).$$

Concluímos que $\theta^{-uk} g_t(\theta^u x^t) \in \mathbb{F}_{q^s}$ se, e somente se, $u = u_s v_s$, onde $v_s \in \mathbb{N}$ e,

$$u_s = \begin{cases} 2^l\,\mathrm{mdc}\left(n, \frac{q^p-1}{q-1}\right) & \text{se } s = 1 \\ \mathrm{mdc}\left(n, \frac{q^p-1}{q-1}\right) & \text{se } s = 2 \\ 2^l & \text{se } s = p \end{cases} = \begin{cases} 2^l & \text{se } p \nmid n \text{ e } s \in \{1, p\} \\ 2^l p & \text{se } p \mid n \text{ e } s = 1 \\ 1 & \text{se } p \nmid n \text{ e } s = 2 \\ p & \text{se } p \mid n \text{ e } s = 2 \end{cases} \tag{2.17}$$

Agora, definimos $\theta_s := \theta^{u_s}$ para cada $s \in \{1, 2, p, 2p\}$, temos que θ_s é uma d_s-ésima raiz primitiva da unidade, onde:

$$d_s = \begin{cases} \mathrm{mdc}(n, q^s-1) & \text{se } p \nmid n \text{ ou } p \nmid (q-1) \text{ e } s \in \{1, p\} \\ \mathrm{mdc}(\frac{n}{2}, q^s-1) & \text{se } p \nmid n \text{ ou } p \nmid (q-1) \text{ e } s = 2 \\ \mathrm{mdc}(\frac{n}{p}, q^s-1) & \text{se } p \mid n,\ p \mid (q-1) \text{ e } s \in \{1, p\} \\ \mathrm{mdc}(\frac{n}{2p}, q^s-1) & \text{se } p \mid n,\ p \mid (q-1) \text{ e } s = 2 \end{cases} \tag{2.18}$$

Além disso, como $1 \leq u \leq d$ e $\mathrm{mdc}(u,t) = 1$, segue que $1 \leq v_s \leq d_s$ e $\mathrm{mdc}(v_s,t) = 1$. Logo, t é ímpar se $s \in \{1,p\}$ e, $p \nmid t$ se $p|n$. Por fim, observemos que $\mathrm{rad}(t)|\,\mathrm{rad}(n)|(q^{2p}-1)$, mas $\mathrm{rad}(n) \nmid \frac{q^{2p}-1}{q^s-1}$, então $\mathrm{rad}(t)|(q^s-1)$.

Para simplificar a notação seja $\theta_{2p} := \theta$ e $v_{2p} = u$, desta forma o polinômio $\theta^{-uk} g_t(\theta^u x^t) = \theta_s^{-v_s k} g_t(\theta_s^{v_s} x^t)$ está contido no anel de polinômios $\mathbb{F}_{q^s}[x]$ com $s \in \{1,2,p,2p\}$ se, e somente se, as seguintes condições são satisfeitas:

a) $1 \leq v_s \leq d_s$ e $\gcd(t, v_s) = 1$,

b) $2 \nmid t$ se $s \in \{1,p\}$,

c) $p \nmid t$ se $p|n$ e $s \neq 2p$,

d) $\mathrm{rad}(t)|(q^s-1)$.

Além disso, se $\mathbb{F}_{q^s}[x]$ é o menor anel de polinômios que contém $\theta_s^{-v_s k} g_t(\theta_s^{v_s} x^t)$ então

$$G_{\theta_s,v_s}(x) := \prod_{i=0}^{s-1} \theta_s^{-v_s k q^i} g_t(\theta_s^{v_s q^i} x^t) = \theta_s^{-v_s k(1+\cdots+q^{s-1})} \prod_{i=0}^{s-1} g_t(\theta_s^{v_s q^i} x^t) \tag{2.19}$$

é invariante pelo automorfismo de Frobenius σ_q e portanto $G_{\theta_s,v_s}(x)$ é um polinômio mônico irredutível em $\mathbb{F}_q[x]$ que divide $f(x^n)$.

Com isso, concluímos o seguinte resultado:

Teorema 2.25. *Seja p um primo ímpar tal que $\mathrm{ord}_{rad(n)}\, q = p$ e $f(x) \in \mathbb{F}_q[x]$ um polinômio irredutível de grau k e ordem e tal que $\gcd(k, p(q^{2p}-1)) = \gcd(e,n) = 1$. Além disso, suponhamos que $q \equiv 3 \pmod 4$ e $8|n$, definimos u_s, d_s e $G_{v_s,\theta_s}(x)$ como nas equações (2.17), (2.18) e (2.19). Então*

1. *O polinômio $f(x^n)$ se decompõe em fatores irredutíveis sobre $\mathbb{F}_q[x]$ como:*

$$\prod_{\substack{t|m \\ \mathrm{mdc}(t,2p)=1 \\ \mathrm{rad}(t)|(q-1)}} \prod_{\substack{1 \leqslant v_1 \leqslant d_1 \\ \mathrm{mdc}(v_1,t)=1}} G_{v_1,\theta_1}(x) \cdot \prod_{\substack{t|m \\ \mathrm{mdc}(t,p)=1 \\ \mathrm{rad}(t)\nmid(q-1) \\ \mathrm{rad}(t)|(q^2-1)}} \prod_{[v_2]\in\mathscr{R}_{2,t}} G_{v_2,\theta_2}(x) \cdot \prod_{\substack{t|m \\ \mathrm{mdc}(t,2p)=1 \\ \mathrm{rad}(t)\nmid(q-1) \\ \mathrm{rad}(t)|(q^p-1)}} \prod_{[v_p]\in\mathscr{R}_{p,t}} G_{v_p,\theta_p}(x)$$
$$\cdot \prod_{\substack{t|m \\ \mathrm{rad}(t)\nmid(q^2-1) \\ \mathrm{rad}(t)\nmid(q^p-1)}} \prod_{[v_p]\in\mathscr{R}_{2p,t}} G_{v_p,\theta_p}(x)$$

onde $m = \frac{n}{\gcd(n,q^{2p}-1)}$, $\mathscr{R}_{2,t}$, $\mathscr{R}_{p,t}$ e $\mathscr{R}_{2p,t}$ são as q-classes ciclotômicas:

$$\mathscr{R}_{2,t} = \left\{ v_2 \in \mathbb{N} | 1 \leq v_2 \leq d_2, \mathrm{mdc}(v_2,t) = 1, 2^l \nmid v_2 \right\} / \sim_{2,q},$$

$$\mathscr{R}_{p,t} = \left\{ v_p \in \mathbb{N} | 1 \leq v_p \leq d_p, \operatorname{mdc}(v_p, t) = 1, \operatorname{mdc}\left(n, \frac{q^p - 1}{q-1}\right) \nmid v_p \right\} / \sim_{p,q}$$

$$\mathscr{R}_{2p,t} = \left\{ v_{2p} \in \mathbb{N} | 1 \leq v_{2p} \leq d_{2p}, \operatorname{mdc}(v_{2p}, t) = 1, 2^l \nmid v_{2p}, \operatorname{mdc}\left(n, \frac{q^p - 1}{q-1}\right) \nmid v_{2p} \right\} / \sim_{2p,q}$$

definidas pela relação de equivalência: $a \sim_{s,q} b$ se, existe $j \in \mathbb{N}$ tal que $a \equiv bq^j \pmod{d_s}$.

2. *O número de fatores irredutíveis de $f(x^n)$ em $\mathbb{F}_q[x]$ é:*

$$\frac{\gcd(n, q-1)}{2p}\left(1 + 2^l\left(1 + \nu_p(m)\frac{p-1}{p}\right)\right)\left(p - 1 + \frac{\gcd(n, q^p - 1)}{\gcd(n, q-1)}\left(1 + \frac{\nu_2(m)}{2}\right)\right) \prod_{\substack{p' | m \\ p' \notin \{2, p\}}} \left(1 + \nu_{p'}(m)\frac{p'-1}{p'}\right) \tag{2.20}$$

Demonstração. Observamos que a primeira parte do resultado já foi mostrada. Resta calcularmos o número de fatores irredutíveis. Sabemos que o número de fatores irredutíveis que aparecem na Equação (2.15) que estão em $\mathbb{F}_{q^s}[x]$ para $s \in \{1, 2, p, 2p\}$ é

$$N_s = \sum_{\substack{t | m \\ \operatorname{mdc}\left(t, \frac{2p}{s}\right) = 1}} \frac{\varphi(t)}{t} \gcd(n, q^s - 1) = \operatorname{mdc}(n, q^s - 1) \prod_{\substack{p' | m \\ \gcd(p', \frac{2p}{s}) = 1}} \left(1 + \nu_{p'}(m)\frac{p'-1}{p'}\right).$$

Portanto o número de fatores em $\mathbb{F}_{q^2}[x] \setminus \mathbb{F}_q[x]$ é $N_2 - N_1$, o número de fatores em $\mathbb{F}_{q^p}[x] \setminus \mathbb{F}_q[x]$ é $N_p - N_1$ e o número de fatores em $\mathbb{F}_{q^{2p}}[x] \setminus (\mathbb{F}_{q^2}[x] \cup \mathbb{F}_{q^p}[x])$ é $N_{2p} - N_p - N_2 + N_1$.

Agora, tomando um par de fatores adequado em $\mathbb{F}_{q^2}[x] \setminus \mathbb{F}_q[x]$ e fazendo o produto destes fatores obtemos um fator irredutível em $\mathbb{F}_q[x]$. Da mesma maneira, tomando p fatores adequados em $\mathbb{F}_{q^p}[x] \setminus \mathbb{F}_q[x]$ e $2p$ fatores adequados em $\mathbb{F}_{q^{2p}}[x] \setminus \mathbb{F}_q[x]$ geramos um fator irredutível em $\mathbb{F}_q[x]$. Portanto, o número de fatores irredutíveis de $f(x^n)$ em $\mathbb{F}_q[x]$ é

$$N_1 + \frac{1}{2}(N_2 - N_1) + \frac{1}{p}(N_p - N_1) + \frac{1}{2p}(N_{2p} - N_p - N_2 + N_1) = \left(\frac{1}{2} - \frac{1}{2p}\right)(N_1 + N_2) + \frac{1}{2p}(N_p + N_{2p}) \tag{2.21}$$

Além disso, temos que:

$$\begin{aligned} N_1 + N_2 &= \operatorname{mdc}(n, q-1) \prod_{\substack{p' | m \\ \operatorname{mdc}(p', 2p) = 1}} \left(1 + \nu_{p'}(m)\frac{p'-1}{p'}\right) + \operatorname{mdc}(n, q^2 - 1) \prod_{\substack{p' | m \\ \operatorname{mdc}(p', p) = 1}} \left(1 + \nu_{p'}(m)\frac{p'-1}{p'}\right) \\ &= \operatorname{mdc}(n, q-1)\left[1 + 2^l\left(1 + \frac{\nu_2(m)}{2}\right)\right] \prod_{\substack{p' | m \\ \operatorname{mdc}(p', 2p) = 1}} \left(1 + \nu_{p'}(m)\frac{p'-1}{p'}\right) \end{aligned} \tag{2.22}$$

e

$$N_p + N_{2p} = \mathrm{mdc}(n, q^p - 1) \prod_{\substack{p' \mid m \\ \mathrm{mdc}(p', 2) = 1}} \left(1 + \nu_{p'}(m) \frac{p' - 1}{p'}\right) + \mathrm{mdc}(n, q^{2p} - 1) \prod_{p' \mid m} \left(1 + \nu_{p'}(m) \frac{p' - 1}{p'}\right)$$

$$= \mathrm{mdc}(n, q^p - 1) \left[1 + 2^l \left(1 + \frac{\nu_2(m)}{2}\right)\right] \prod_{\substack{p' \mid m \\ \mathrm{mdc}(p', 2) = 1}} \left(1 + \nu_{p'}(m) \frac{p' - 1}{p'}\right). \tag{2.23}$$

Substituindo (2.22) e (2.23) na equação (2.21) obtemos o resultado em (2.20), como queríamos mostrar. ■

Exemplo 2.26. *Seja $q = 83 \equiv 3 \pmod 4$. Note que o polinômio ciclotômico $\Phi_{19}(x) \in \mathbb{F}_q[x]$ se decompõe da seguinte forma em $\mathbb{F}_q$*

$$(x^3 + 4x^2 - 36x - 1)(x^3 + 10x^2 - 25x - 1)(x^3 + 15x^2 - 10x - 1)$$

$$(x^3 + 24x^2 + 5x - 1)(x^3 + 36x^2 - 4x - 1)(x^3 - 5x^2 - 24x - 1)$$

Tomemos o fator $f(x) = x^3 + 4x^2 - 36x - 1$. Observe que $f(x)$ é um polinômio irredutível sobre $\mathbb{F}_q[x]$, de grau 3 e ordem 19.

Seja $n = 2^{\mathfrak{a}} \cdot 7^{\mathfrak{b}} \cdot 11^{\mathfrak{c}} \cdot 13^{\mathfrak{d}}$, onde $\mathfrak{a} \geq 5$ e $\mathfrak{b}, \mathfrak{c}, \mathfrak{d} \geq 1$. Temos que $S_n = ord_{\mathrm{rad}(n)}(q) = s_n = 20$ e $m = \frac{n}{\gcd(n, q^{20} - 1)} = 2^{\mathfrak{a}-4} \cdot 7^{\mathfrak{b}-1} \cdot 11^{\mathfrak{c}-1} \cdot 13^{\mathfrak{d}-1}$. Seguindo a mesma notação do Teorema 2.19, obtemos a seguinte tabela:

v	$\gcd(n, q^v - 1)$	$\frac{\gcd(n, q^{20} - 1)}{\gcd(n, q^v - 1)}$	m_v
1	*2*	$2^3 \cdot 7 \cdot 11 \cdot 13$	1
2	$2^3 \cdot 7$	$2 \cdot 11 \cdot 13$	$7^{\mathfrak{b}-1}$
4	$2^4 \cdot 7 \cdot 13$	11	$2^{\mathfrak{a}-4} \cdot 7^{\mathfrak{b}-1} \cdot 13^{\mathfrak{d}-1}$
5	2	$2^3 \cdot 7 \cdot 11 \cdot 13$	1
10	$2^3 \cdot 7 \cdot 11$	$2 \cdot 13$	$7^{\mathfrak{b}-1} \cdot 11^{\mathfrak{c}-1}$
20	$2^4 \cdot 7 \cdot 11 \cdot 13$	1	$2^{\mathfrak{a}-4} \cdot 7^{\mathfrak{b}-1} \cdot 11^{\mathfrak{c}-1} \cdot 13^{\mathfrak{d}-1}$

Portanto,o número de fatores irredutíveis de $f(x^n)$ sobre $\mathbb{F}_q$ é igual a

$$288\mathfrak{a}\mathfrak{b}\mathfrak{c}\mathfrak{d} + 24\mathfrak{a}\mathfrak{b}\mathfrak{c} + 144\mathfrak{a}\mathfrak{b}\mathfrak{d} + 48\mathfrak{a}\mathfrak{c}\mathfrak{d} - 576\mathfrak{b}\mathfrak{c}\mathfrak{d} + 12\mathfrak{a}\mathfrak{b} + 4\mathfrak{a}\mathfrak{c} - 24\mathfrak{b}\mathfrak{c} + 24\mathfrak{a}\mathfrak{d} - 288\mathfrak{b}\mathfrak{d} - 96\mathfrak{c}\mathfrak{d}$$
$$+ 2\mathfrak{a} - 12\mathfrak{b} - 4\mathfrak{c} - 48\mathfrak{d} - 1$$

Esta fórmula também funciona no caso em que $\mathfrak{a} \geq 3$ e $\mathfrak{b}, \mathfrak{c}, \mathfrak{d} \geq 0$.

No caso $n = 2^{\mathfrak{a}} \cdot 7^{\mathfrak{b}} \cdot 11^{\mathfrak{c}} \cdot 13^{\mathfrak{d}}$, com $\mathfrak{a} \leq 2$ e $\mathfrak{b}, \mathfrak{c}, \mathfrak{d} \geq 1$, temos que $s_n = S_n = ord_{\mathrm{rad}(n)}(q) = 20$ e $m = \frac{n}{\gcd(n, q^{10} - 1)} = 7^{\mathfrak{b}-1} \cdot 11^{\mathfrak{c}-1} \cdot 13^{\mathfrak{d}-1}$. De maneira similar obtemos a seguinte tabela:

v	$\gcd(n, q^v - 1)$	$\frac{\gcd(n, q^{20} - 1)}{\gcd(n, q^v - 1)}$	m_v
1	$2^{\min\{\mathfrak{a},1\}}$	$2^{\max\{0,\mathfrak{a}-1\}} \cdot 7 \cdot 11 \cdot 13$	1
2	$2^{\mathfrak{a}} \cdot 7$	$11 \cdot 13$	$7^{\mathfrak{b}-1}$
4	$2^{\mathfrak{a}} \cdot 7 \cdot 13$	11	$7^{\mathfrak{b}-1} \cdot 13^{\mathfrak{d}-1}$
5	$2^{\min\{\mathfrak{a},1\}}$	$2^{\max\{0,\mathfrak{a}-1\}} \cdot 7 \cdot 11 \cdot 13$	1
10	$2^{\mathfrak{a}} \cdot 7 \cdot 11$	13	$7^{\mathfrak{b}-1} \cdot 11^{\mathfrak{c}-1}$
20	$2^{\mathfrak{a}} \cdot 7 \cdot 11 \cdot 13$	1	$7^{\mathfrak{b}-1} \cdot 11^{\mathfrak{c}-1} \cdot 13^{\mathfrak{d}-1}$

e o número de fatores irredutíveis é:

$$2^{\mathfrak{a}}(36\mathfrak{b}\mathfrak{c}\mathfrak{d} + 6\mathfrak{b}\mathfrak{c} + 18\mathfrak{b}\mathfrak{d} + 6\mathfrak{c}\mathfrak{d} + 3\mathfrak{b} + \mathfrak{c} + 3\mathfrak{d}) + 2^{\mathfrak{a}-1} + 2^{\min\{\mathfrak{a}-1,0\}}$$

Esta fórmula também funciona para o caso em que $\mathfrak{b}, \mathfrak{c}, \mathfrak{d} \geq 0$.

Estas fórmulas foram comparadas com os resultados obtidos através do Software SageMath, implementando um programa que verifica o número de fatores irredutíveis de $f(x^n)$.

SageMath Code

```
          #Determine o tamanho do corpo
 sage: q=83;
         #defina um corpo finito k com q elementos e um gerador a
 sage: k=GF(q,'a');
        #defina o anel de polinômios em uma variável sobre o corpo k
 sage: R = PolynomialRing(k,'x')
        #defina o gerador do anel R (defines the generator of R)
sage: x = R.gen();
       #Encontre os fatores irredutíveis de $\Phi_{19}(x)$ em R
sage: factor(cyclotomic_polynomial(19)(x));
      #forneça a sequência onde cada termo é um fator irredutível de $f(x^{n})$
sage: A=[(x^(3*n) + 4*x^(2*n) + 47*x^n + 82).factor() for n in range (0,500)];
sage: for n in range(0,500):n, len(A[n]);
```

Este último comando gera uma sequência de pares

$$(n, \text{o número de fatores irredutíveis de } f(x^n) \text{ sobre } \mathbb{F}_q)$$

para $n = 1, \ldots, 499$.

Exemplo 2.27. *No caso* $n = 2^{\mathfrak{a}} \cdot 5^{\mathfrak{b}} \cdot 7^{\mathfrak{c}} \cdot 11^{\mathfrak{d}} \cdot 13^{\mathfrak{r}}$*, com* $\mathfrak{a} \geq 5$ *e* $\mathfrak{b} \geq 2$ $\mathfrak{c}, \mathfrak{d}, \mathfrak{r} \geq 1$*, temos* $S_n = ord_{\mathrm{rad}(n)}(q) = 20$ *e* $s_n = 40$ *e* $m = \frac{n}{\gcd(n, q^{40}-1)} = 2^{\mathfrak{a}-5} \cdot 5^{\mathfrak{b}-2} \cdot 7^{\mathfrak{c}-1} \cdot 11^{\mathfrak{d}-1} \cdot 13^{\mathfrak{r}-1}$.

v	$\gcd(n, q^v - 1)$	$\frac{\gcd(n, q^{40}-1)}{\gcd(n, q^v - 1)}$	m_v
1	*2*	$2^4 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	1
2	$2^3 \cdot 7$	$2^2 \cdot 5^2 \cdot 11 \cdot 13$	$7^{\mathfrak{c}-1}$
4	$2^4 \cdot 5 \cdot 7 \cdot 13$	$2 \cdot 5 \cdot 11$	$7^{\mathfrak{c}-1} \cdot 13^{\mathfrak{r}-1}$
5	2	$2^4 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	1
8	$2^5 \cdot 5 \cdot 7 \cdot 13$	$5 \cdot 11$	$2^{\mathfrak{a}-5} \cdot 7^{\mathfrak{c}-1} \cdot 13^{\mathfrak{r}-1}$
10	$2^3 \cdot 7 \cdot 11$	$2^2 \cdot 5^2 \cdot 13$	$7^{\mathfrak{c}-1} \cdot 11^{\mathfrak{d}-1}$
20	$2^4 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	2	$5^{\mathfrak{b}-2} \cdot 7^{\mathfrak{c}-1} \cdot 11^{\mathfrak{d}-1} \cdot 13^{\mathfrak{r}-1}$
40	$2^5 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	1	$2^{\mathfrak{a}-5} \cdot 5^{\mathfrak{b}-2} \cdot 7^{\mathfrak{c}-1} \cdot 11^{\mathfrak{d}-1} \cdot 13^{\mathfrak{r}-1}$

Portanto o número de fatores irredutíveis de $f(x^n)$ *é*

$$5760\mathfrak{abcdr} + 480\mathfrak{abcr} + 576\mathfrak{abcr} + 960\mathfrak{abdr} - 4320\mathfrak{acdr} - 11520\mathfrak{bcdr} + 48\mathfrak{abc} + 80\mathfrak{abd} - 360\mathfrak{acd}$$

$$-960\mathfrak{bcd} + 96\mathfrak{abr} + 144\mathfrak{acr} - 1152\mathfrak{bcr} - 720\mathfrak{adr} - 1920\mathfrak{bdr} + 8640\mathfrak{cdr} + 8\mathfrak{ab} + 12\mathfrak{ac} - 96\mathfrak{bc}$$

$$-60\mathfrak{ad} - 160\mathfrak{bd} + 744\mathfrak{cd} + 24\mathfrak{ar} - 192\mathfrak{br} - 288\mathfrak{cr} + 1440\mathfrak{dr} + 2\mathfrak{a} - 16\mathfrak{b} - 12\mathfrak{c} + 124\mathfrak{d} - 48\mathfrak{r} - 1$$

No caso $\mathfrak{b} = 1$ *temos*

$$7200\mathfrak{acdr} + 600\mathfrak{acd} + 1296\mathfrak{acr} + 1200\mathfrak{adr} - 14400\mathfrak{cdr} + 108\mathfrak{ac} + 100\mathfrak{ad}$$

$$-1176\mathfrak{cd} + 216\mathfrak{ae} - 2592\mathfrak{cr} - 2400\mathfrak{dr} + 18\mathfrak{a} - 204\mathfrak{c} - 196\mathfrak{d} - 432\mathfrak{r} - 33$$

CAPÍTULO 3

A Estimativa do Número de Binômios Irredutíveis

Determinar uma fórmula assintótica para o número de polinômios mônicos irredutíveis em $\mathbb{F}_q$ de grau t que satisfaçam algumas condições é uma questão interessante. Por exemplo, em [11] podem ser encontradas várias fórmulas assintóticas para o número de polinômios mônicos irredutíveis com alguns coeficientes fixos, e em [19] encontra-se uma fórmula assintótica para o número de polinômios irredutíveis que são invariantes por uma ação de $PGL(2,\mathbb{F}_q)$. Nesta direção, uma questão natural é encontrar uma função assintótica para o número de polinômios irredutíveis com peso baixo. Em particular, polinômios com apenas dois coeficientes não nulos, ou seja, que possuem peso dois. Neste caso, é bem conhecido um critério de irredutibilidade para binômios (Teorema 1.36).

Fixamos q e denotamos por $N_q(t)$ o número de elementos $a \in \mathbb{F}_q$ tal que o binômio $x^t - a$ é irredutível sobre o corpo $\mathbb{F}_q[x]$. Uma pergunta natural é, qual é a ordem de crescimento desta função, mas como esta função pode ter um comportamento não muito uniforme, se faz necessário responder outro tipo de pergunta, como por exemplo qual seu valor máximo, mínimo ou valor médio quando limitamos o valor de t. Em particular, qual é uma estimativa para $\sum_{t \le T} N_q(t)$ para T grande.

Recordando que $\mathrm{rad}(t)$ é o produto dos primos p que dividem t, definimos

$$\mathrm{rad}_4(t) = \begin{cases} \mathrm{rad}(t) & \text{se } 4 \nmid t \\ 2\,\mathrm{rad}(t) & \text{caso contrário.} \end{cases}$$

Tomando $n = (q-1)^{l+1}$, onde l é um inteiro positivo tal que $t \mid (q-1)^l$ obtemos que cada binômio da forma $x^t - a \in \mathbb{F}_q[x]$ é um fator do polinômio $x^n - 1$ [7, ver Lema 2.3]. Portanto, a partir do Corolário 2.4, o qual é essencialmente o mesmo resultado do Corolário 3.2 *b* em [7] juntamente com o teorema de irredutibilidade de binômios temos que:

Lema 3.1. *Sejam $\mathbb{F}_q$ um corpo com q elementos e $N_q(t)$ o número de binômios mônicos irredutíveis de grau t em $\mathbb{F}_q$. Então*

$$N_q(t) = \begin{cases} \frac{\varphi(t)}{t}(q-1), & \text{se } \mathrm{rad}_4(t) \mid (q-1) \\ 0, & \text{caso contrário}, \end{cases}$$

onde φ é a função de Euler.

Este resultado também pode ser encontrado em [17] Lema 7. A soma $\sum_{t \le T} N_q(t)$ foi estudada por Heyman e Shparlinski em [17] usando resultados de Teoria Analítica dos Números. Neste trabalho, os autores apresentam uma cota superior para a ordem média do número de binômios irredutíveis quando q está fixo e $t \le T$ para T suficientemente grande. O resultado mencionado é o seguinte.

Teorema 3.2 ([17], Teorema 3)**.** *Sejam $\mathbb{F}_q$ um corpo finito, A e ϵ números positivos fixos e T um número real tal que*

$$T \ge (\log(q-1))^{(1+\epsilon)A \log_3 q / \log_4 q}.$$

Então se tem que

$$\sum_{t \le T} N_q(t) \le (q-1)\frac{T}{(\log T)^A}.$$

Neste capítulo será mostrado que este limite superior não está próximo da ordem de crescimento esperada. De fato, obtivemos a ordem de crescimento "exata" para ordem média do número de binômios irredutíveis de grau menor ou igual a T com q fixo. Assim, este resultado melhora o resultado apresentado por Heyman e Shparlinski.

Ao longo deste capítulo, $\mathbb{N}_0$ e $\mathbb{N}$ denotam respectivamente o conjunto dos inteiros não negativos e o conjunto dos inteiros positivos e, $p_1 < p_2 < \cdots < p_s$ denotam números primos tais que

$$q - 1 = \begin{cases} p_1^{\alpha_1} \cdots p_s^{\alpha_s} & \text{se } q \not\equiv 3 \pmod 4 \\ 2p_1^{\alpha_1} \cdots p_s^{\alpha_s} & \text{caso contrário,} \end{cases}$$

onde $s \ge 2$. Observemos que no caso que $s = 1$, isto é, $q - 1$ tem unicamente um fator primo, temos que

$$p^k - 1 = p_1^{\alpha_1} \text{ com } k \in \mathbb{N} \tag{3.1}$$

assim:

- Se $k, \alpha_1 \geq 2$ segue do Teorema de Mihailescu (Conjectura de Catalan) [30] que a única solução de 3.1 é $p = 3$, $k = 2$, $p_1 = 2$ e $\alpha_1 = 3$.
- Se $k = 1$ segue da equação 3.1 que $p = p_1^{\alpha_1} + 1$ o que implica que $p_1 = 2$, pois se p_1 é um primo ímpar então $p_1^{\alpha_1} + 1 = 2(k_1 + 1)$ com $k_1 \geq 1$ não é um primo. Logo, $p = 2^{\alpha_1} + 1$, com $\alpha_1 = 2^{\beta}$, $\beta \in \mathbb{N}$ em outras palavras, p é um primo de Fermat (ver [10]).
- Se $\alpha_1 = 1$ então $p_1 = p^k - 1$ o que implica que $p = 2$, logo $p_1 = 2^k - 1$ com $k \in \mathbb{N}$ um número primo em outras palavras, p_1 é um primo de Mersenne (ver [10])

portanto $q = 2^R + 1$ e

$$\sum_{t \leq T} N_q(t) = \sum_{2^l \leq T} \frac{\varphi(2^l)}{2^l}(q-1) = \left(1 + \frac{\lfloor \log_2 T \rfloor}{2}\right)(q-1).$$

Além disso, para cada $\vec{v} = (v_1, \ldots, v_s) \in \mathbb{N}_0{}^s$, denotaremos por $t(\vec{v})$ o número $p_1^{v_1} \cdots p_s^{v_s}$ e por l_j o número $\log p_j$ com $j = 1, \ldots, s$.

No que segue, apresentaremos alguns resultados sobre pontos reticulares no tetraedro s-dimensional limitado pelos hiperplanos coordenados e algum outro plano. Estes resultados serão utilizados para determinarmos quantos números inteiros positivos t satisfazem $t \leq T$ com $\mathrm{rad}(t) \mid (q-1)$. Mais especificamente, queremos saber quantos números da forma $p_1^{v_1} \cdots p_s^{v_s}$ são menores ou iguais a T. Para isto, necessitamos de algumas definições e resultados, o qual passaremos a listá-los.

3.1 Alguns Resultados Sobre Pontos Reticulados

Definição 3.3. *Sejam $a_1, \ldots, a_s$ e λ números reais positivos. Denotamos por $\Omega(\lambda; a_1, \ldots, a_s)$ o conjunto de pontos do tetraedro limitado pelos hiperplanos coordenados e pelo hiperplano $a_1x_1 + \cdots + a_sx_s = \lambda$, isto é,*

$$\Omega(\lambda; a_1, \ldots, a_s) = \{(x_1, \ldots, x_s) \in \mathbb{R}^s \mid x_i \geq 0 \text{ e } a_1x_1 + \cdots + a_sx_s \leq \lambda\}, \text{ e,}$$

denotamos por $\mathcal{N}_s(\lambda; a_1, \ldots, a_s)$ o número de pontos do conjunto $\mathbb{N}_0^s \cap \Omega(\lambda; a_1, \ldots, a_s)$, isto é,

$$\mathcal{N}_s(\lambda; a_1, \ldots, a_s) = |\{(x_1, \ldots, x_s) \in \mathbb{N}_0^s \mid a_1x_1 + \cdots + a_sx_s \leq \lambda\}|.$$

A estimativa para o número de pontos reticulados no tetraedro é um resultado clássico. Se consideramos, para cada ponto de $\Omega(\lambda;a_1,\ldots,a_s)$ com coordenadas inteiras, um hipercubo de lado 1 localizado na direção positiva com respeito a todos os eixos e cada um destes pontos, o sólido $\mathscr{C}_s$ obtido pela união dos hipercubos contém $\Omega(\lambda;a_1,\ldots,a_s)$. Portanto,

$$\mathscr{N}_s(\lambda;a_1,\ldots,a_s) = Vol(\mathscr{C}_s) > Vol(\Omega(\lambda;a_1,\ldots,a_s)) = \frac{1}{s!}\prod_{j=1}^{s}\frac{\lambda}{a_j} = \frac{\lambda^s}{s!a_1\cdots a_s}. \tag{3.2}$$

Como $\mathscr{C}_s$ também está contido em $\Omega(\lambda+a_1+\cdots+a_s;a_1,\ldots,a_s)$, temos

$$\mathscr{N}_s(\lambda;a_1,\ldots,a_s) < Vol(\Omega(\lambda+a_1+\cdots+a_s;a_1,\ldots,a_s)) = \frac{(\lambda+a_1+\cdots+a_s)^s}{s!a_1\cdots a_s} \tag{3.3}$$

Uma vez que,

$$\frac{(\lambda+a_1+\cdots+a_s)^s}{s!a_1\cdots a_s} = \frac{1}{s!a_1\cdots a_s}\left(\lambda^s + \sum_{j=1}^{s}\binom{n}{k}(\lambda)^{s-j}(a_1+\cdots+a_s)^j\right) = \frac{\lambda^s}{s!a_1\cdots a_s} + O(\lambda^{s-1}).$$

A função $\mathscr{N}_s$ pode ser limitada superior e inferiormente por dois polinômios de grau s na variável λ para todo $\lambda > 0$ e, assintoticamente temos que

$$\mathscr{N}_s(\lambda;a_1,\ldots,a_s) = \frac{\lambda^s}{s!a_1\cdots a_s} + O(\lambda^{s-1}).$$

Em [21], Lehmer determina dois outros polinômios $P_{a_1,\ldots,a_s}(\lambda)$ e $Q_{a_1,\ldots,a_s}(\lambda)$ os quais fornecem uma cota mais exata para limitar inferiormente e superiomente a função $\mathscr{N}_s$ para todo $\lambda > 0$. Resultados análogos foram encontrados por Lochs [28] (equação II e equação III). No seguinte teorema, apresentamos um resumo destes resultados de uma forma simplificada:

Teorema 3.4 ([21] e [28])**.** *Sejam $a_1,\ldots,a_s$ números reais. Então,*

$$\frac{\lambda^s + \frac{s}{2}(a_2+\cdots+a_s)\lambda^{s-1}}{s!a_1\cdots a_s} < \mathscr{N}_s(\lambda;a_1,\ldots,a_s) < \frac{(\lambda+\frac{1}{2}(2a_1+\cdots+a_s))^s}{s!a_1\cdots a_s}, \quad \textit{para todo } \lambda > 0. \tag{3.4}$$

Por outro lado, em [33], Spencer encontrar uma fórmula assintótica para função $\mathscr{N}_s$ no caso em que $a_1,\ldots,a_s$ são genéricos. Uma versão elementar do resultado de Spencer pode ser encontrado em [3]. Especificamente.

Teorema 3.5 ([3, Theorem 1, Equation (1)])**.** *Sejam $a_1,\ldots,a_s$ números reais linearmente independentes sobre $\mathbb{Q}$. Então:*

$$\mathscr{N}_s(\lambda;a_1,\ldots,a_s) = \frac{\lambda^s}{s!a_1\cdots a_s} + \frac{1}{2(s-1)!}\frac{a_1+\cdots+a_s}{a_1\cdots a_s}\lambda^{s-1} + o(\lambda^{s-1}).$$

3.2 Número de Binômios Irredutíveis

Nesta seção, apresentamos o resultado principal deste capítulo, o qual fornece uma fórmula assintótica correta para o número de binômios irredutíveis sobre $\mathbb{F}_q$ de grau menor ou igual a T. Para cada inteiro positivo T, denotaremos por $\Upsilon(T)$ o conjunto dos pontos reticulados

$$\Omega(\log T; l_1, \ldots, l_s) \cap \mathbb{N}_0^s, \text{ onde } l_j = \log p_j \quad \text{para} \quad j = 1, \ldots, s,$$

por $\Upsilon^+(T)$ os elementos de $\Upsilon(T)$ em que cada coordenada é positiva, ou seja, $\Upsilon^+(T) = \Upsilon(T) \cap \mathbb{N}^s$ e, $\Upsilon_j(T)$ o subconjunto de $\Upsilon(T)$ que tem a j-ésima coordenada igual a zero e as outras coordenadas são positivas. Observemos que, pela definição de $\Upsilon(T)$,

$$\vec{v} := (v_1, \ldots, v_s) \in \Upsilon(T) \text{ se, e somente se, } t(\vec{v}) = p_1^{v_1} \cdots p_s^{v_s} \leq T.$$

Além disso, os conjuntos $\Upsilon^+(T), \Upsilon_1(T), \ldots, \Upsilon_s(T)$ são dois a dois disjuntos. Por fim, denotaremos por $\Upsilon_0(T) \subseteq \Upsilon(T)$ o subconjunto complementar

$$\Upsilon(T) \setminus (\Upsilon^+(T) \cup \Upsilon_1(T) \cup \cdots \cup \Upsilon_s(T)),$$

isto é, o subconjunto dos elementos com duas ou mais coordenadas iguais a zero.

No que segue, apresentamos um lema técnico que será util para estimar o número de binômios irredutíveis mônicos de grau $t \leq T$ com $\frac{\mathrm{rad}(q-1)}{\mathrm{rad}(t)}$ sendo igual a 1 ou um número primo. A ideia essencial é a seguinte: O número de binômios em que $\frac{\mathrm{rad}(q-1)}{\mathrm{rad}(t)} =$ é igual a 1 ou um número primo é assintoticamente maior do que outros tipos de binômios com grau menor ou igual a T.

Lema 3.6. *Seja T um inteiro com $T > \mathrm{rad}(q-1)$. Então:*

(a)

$$\sum_{\vec{v} \in \Upsilon^+(T)} \frac{\varphi(t(\vec{v}))}{t(\vec{v})} = \frac{\varphi(q-1)}{(q-1)s! l_1 \cdots l_s} (\log T)^s \left(1 - \frac{s \log(\mathrm{rad}(q-1))}{2 \log T}\right) + o\left((\log T)^{s-1}\right)$$

(b)

$$\sum_{j=1}^{s} \sum_{\vec{v} \in \Upsilon_j(T)} \frac{\varphi(t(\vec{v}))}{t(\vec{v})} = \frac{\varphi(q-1)}{(q-1)(s-1)! l_1 \cdots l_s} (\log T)^{s-1} \sum_{j=1}^{s} \frac{p_j l_j}{p_j - 1} + O((\log T)^{s-2})$$

Demonstração. **(a)** Como $\mathrm{rad}(t(\vec{v})) = \mathrm{rad}(q-1)$ para todo $\vec{v} \in \Upsilon^+(T)$, temos que:

$$\frac{\varphi(t(\vec{v}))}{t(\vec{v})} = \frac{\varphi(\mathrm{rad}(t(\vec{v})))}{\mathrm{rad}(t(\vec{v}))} = \frac{\varphi(\mathrm{rad}(q-1))}{\mathrm{rad}(q-1)} = \frac{\varphi(q-1)}{q-1}.$$

Logo,

$$\sum_{\vec{v}\in\Upsilon^+(T)} \frac{\varphi(t(\vec{v}))}{t(\vec{v})} = \frac{\varphi(q-1)}{q-1}|\Upsilon^+(T)|. \tag{3.5}$$

Por outro lado, sabemos que:

$$(v_1,v_2,\ldots,v_s)\in\Upsilon^+(T) \text{ se, e somente se, } (v_1-1,v_2-1,\ldots,v_s-1)\in\Upsilon\left(\frac{T}{p_1\cdots p_s}\right).$$

Portanto,

$$|\Upsilon^+(T)| = \left|\Upsilon\left(\frac{T}{p_1\cdots p_s}\right)\right| = \mathscr{N}_s\left(\log\left(\frac{T}{p_1\cdots p_s}\right);l_1,\ldots,l_s\right). \tag{3.6}$$

Agora, pelo Teorema 3.5 e usando o fato que

$$\left(\log\left(\frac{T}{p_1\cdots p_s}\right)\right)^k = (\log T)^k - k\log(p_1\cdots p_s)(\log T)^{k-1} + O((\log T)^{k-2})$$

para todo $k\geq 1$, concluímos que

$$\begin{aligned}
|\Upsilon^+(T)| &= \frac{1}{s!l_1\cdots l_s}\left(\log\left(\frac{T}{p_1\cdots p_s}\right)\right)^s + \frac{s}{2}(l_1+\cdots+l_s)\left(\log\left(\frac{T}{p_1\cdots p_s}\right)^{s-1}\right) + o((\log T)^{s-1}) \\
&= \frac{1}{s!l_1\cdots l_s}\left((\log T)^s - s\log(p_1\cdots p_s)(\log T)^{s-1} + \frac{s}{2}\log(p_1\cdots p_s)(\log T)^{s-1}\right) + o((\log T)^{s-1}) \\
&= \frac{(\log T)^s}{s!l_1\cdots l_s}\left(1-\frac{s\log(\mathrm{rad}(q-1))}{2\log T}\right) + o((\log T)^{s-1}).
\end{aligned}$$

O resultado segue desta última identidade e da Equação 3.5.

(b) Se $\vec{v}\in\Upsilon_j(T)$, então $\mathrm{rad}(t(\vec{v})) = \frac{\mathrm{rad}(q-1)}{p_j}$ e

$$\frac{\varphi(t(\vec{v}))}{t(\vec{v})} = \frac{\varphi\left(\frac{\mathrm{rad}(q-1)}{p_j}\right)}{\frac{\mathrm{rad}(q-1)}{p_j}} = \frac{\varphi(\mathrm{rad}(q-1))}{\mathrm{rad}(q-1)}\cdot\frac{p_j}{p_j-1} = \frac{\varphi(q-1)}{q-1}\cdot\frac{p_j}{p_j-1}.$$

Assim,

$$\sum_{j=1}^{s}\sum_{\vec{v}\in\Upsilon_j(T)} \frac{\varphi(t(\vec{v}))}{t(\vec{v})} = \frac{\varphi(q-1)}{q-1}\sum_{j=1}^{s}\frac{p_j}{p_j-1}|\Upsilon_j(T)|. \tag{3.7}$$

Como cada ponto em $\Upsilon_j(T)$ possui a j-ésima coordenada igual a zero, podemos eliminar esta coordenada e, seguindo os mesmos passos do item anterior obtemos que:

$$\begin{aligned}
|\Upsilon_j(T)| &= \mathscr{N}_{s-1}\left(\log\left(\frac{T}{p_1\cdots p_{j-1}p_{j+1}\cdots p_s}\right);l_1,\ldots,\widehat{l_j},\ldots,l_s\right) \\
&= \frac{1}{(s-1)!l_1\cdots l_{j-1}l_{j+1}\cdots l_s}(\log T)^{s-1} + O((\log T)^{s-2}),
\end{aligned} \tag{3.8}$$

onde $\widehat{l_j}$ significa que l_j não aparece como parâmetro na função. O resultado segue a partir das Equações 3.7 e 3.8. ■

Agora estamos prontos para enunciar e mostrar o resultado principal.

Teorema 3.7. *Sejam $\mathbb{F}_q$ um corpo finito com q elementos e $N_q(t)$ o número de binômios mônicos irredutíveis de grau t em $\mathbb{F}_q[x]$.*

1. *Se $q \not\equiv 3 \pmod 4$ e $q-1 = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ é a fatoração de $q-1$ em fatores primos, então*

$$\sum_{1\le t\le T} N_q(t) = \frac{\varphi(q-1)}{s!\log p_1 \cdots \log p_s}\left((\log T)^s + \frac{s}{2}\sum_{j=1}^{s}\frac{(p_j+1)\log p_j}{p_j-1}(\log T)^{s-1}\right) + o\left((\log T)^{s-1}\right).$$

2. *Se $q \equiv 3 \pmod 4$ e $q-1 = 2p_1^{\alpha_1} \dots p_s^{\alpha_s}$, então*

$$\sum_{1\le t\le T} N_q(t) = \frac{3\varphi(q-1)}{2\cdot s!\log p_1 \cdots \log p_s}\left((\log T)^s + \frac{s}{2}\left[\sum_{j=1}^{s}\frac{(p_j+1)\log p_j}{p_j-1} - \frac{\log 2}{3}\right](\log T)^{s-1}\right) + o\left((\log T)^{s-1}\right).$$

Demonstração. Suponhamos que $q \not\equiv 3 \pmod 4$, então $4 \mid (q-1)$ ou $q-1$ é ímpar.

Como $N_q(t) = 0$ se $\mathrm{rad}_4(t) \nmid (q-1)$ segue do Lema 3.1 que:

$$\sum_{t\le T} N_q(t) = \sum_{\substack{t\le T \\ \mathrm{rad}_4(t)\mid(q-1)}} N_q(t) = (q-1)\sum_{\substack{t\le T \\ \mathrm{rad}_4(t)\mid(q-1)}} \frac{\varphi(t)}{t}. \tag{3.9}$$

Uma vez que $q \not\equiv 3 \pmod 4$ temos que $q \equiv 1 \pmod 4$ ou q é par. Em ambos os casos, $\mathrm{rad}_4(t) \mid (q-1)$ e $\mathrm{rad}(t) \mid (q-1)$ são equivalentes, pois no primeiro caso $4 \mid (q-1)$ implica que $\frac{q-1}{\mathrm{rad}(t)}$ é par e no segundo caso $\mathrm{rad}(t)$ é ímpar e portanto $\mathrm{rad}_4(t) = \mathrm{rad}(t)$.

Segue da Equação 3.9 que

$$\sum_{t\le T} N_q(t) = (q-1)\sum_{\substack{t\le T \\ \mathrm{rad}(t)\mid(q-1)}} \frac{\varphi(t)}{t}. \tag{3.10}$$

As condições $t \le T$ e $\mathrm{rad}(t) \mid (q-1)$ são equivalentes a $t = p_1^{v_1}\cdots p_s^{v_s} \le T$ onde cada v_j é um inteiro não negativo. Esta última inequação é equivalente a inequação linear $v_1\log p_1 + \cdots + v_s \log p_s \le \log T$, isto é, $\vec{v} = (v_1,\dots,v_s) \in \Upsilon(T) = \Omega(\log T; l_1,\dots,l_s) \cap \mathbb{N}_0^s$. Desta forma temos que

$$\sum_{\substack{t\le T \\ \mathrm{rad}(t)\mid(q-1)}} N_q(t) = (q-1)\sum_{\vec{v}\in\Upsilon(T)} \frac{\varphi(t(\vec{v}))}{t(\vec{v})} = (q-1)(A+B+C),$$

onde

$$A := \sum_{\vec{v}\in\Upsilon^+(T)} \frac{\varphi(t(\vec{v}))}{t(\vec{v})}, \qquad B := \sum_{j=1}^{s}\sum_{\vec{v}\in\Upsilon_j(T)} \frac{\varphi(t(\vec{v}))}{t(\vec{v})} \quad \text{e} \quad C := \sum_{\vec{v}\in\Upsilon_0(T)} \frac{\varphi(t(\vec{v}))}{t(\vec{v})}. \tag{3.11}$$

Notemos, as somas A e B correspondem aos itens (a) e (b) do Lema 3.6. Logo:

$$\begin{aligned}(q-1)(A+B) &= \frac{\varphi(q-1)}{s!l_1\cdots l_s}\left[(\log T)^s - \frac{s}{2}(\log T)^{s-1}\log(\mathrm{rad}(q-1)) + s(\log T)^{s-1}\sum_{j=1}^{s}\frac{p_j l_j}{p_j-1}\right] + o\left((\log T)^{s-1}\right)\\ &= \frac{\varphi(q-1)}{s!l_1\cdots l_s}\left[(\log T)^s - \frac{s}{2}(\log T)^{s-1}\sum_{j=1}^{s} l_j + s(\log T)^{s-1}\sum_{j=1}^{s}\frac{p_j l_j}{p_j-1}\right] + o\left((\log T)^{s-1}\right)\\ &= \frac{\varphi(q-1)}{s!l_1\cdots l_s}\left((\log T)^s + \frac{s}{2}\sum_{j=1}^{s}\frac{p_j+1}{p_j-1}l_j(\log T)^{s-1}\right) + o\left((\log T)^{s-1}\right)\end{aligned}$$

Finalmente, a última soma pode ser limitada da seguinte forma

$$\sum_{\vec{v}\in\Upsilon_0(T)}\frac{\varphi(t(\vec{v}))}{t(\vec{v})} \le \sum_{\vec{v}\in\Upsilon_0(T)} 1 \le \sum_{1\le i<j\le s}|\Upsilon_{ij}(T)|, \tag{3.12}$$

onde

$$\Upsilon_{ij}(T) := |\{\vec{v}\in\Upsilon_0(T); v_i = 0 \text{ e } v_j = 0\}|. \tag{3.13}$$

Usando o fato $\Upsilon_{ij}(T) = \mathscr{N}_{s-2}(\log T; l_1,\ldots,\hat{l}_i,\ldots,\hat{l}_j,\ldots,l_s) = O((\log T)^{s-2})$ concluímos que o último termo é assintoticamente pequeno quando comparado às duas primeiras somas. Portanto

$$\sum_{\substack{t\le T\\ \mathrm{rad}_4(t)\mid(q-1)}} N_q(t) = \frac{\varphi(q-1)}{s!l_1\cdots l_s}\left((\log T)^s + \frac{s}{2}\sum_{j=1}^{s}\frac{(p_j+1)\log p_j}{p_j-1}(\log T)^{s-1}\right) + o\left((\log T)^{s-1}\right),$$

donde temos o item 1.

Agora consideremos o caso em que $q \equiv 3 \mod 4$, ou seja, $\nu_2(q-1) = 1$. Observemos que

- Se t é par então $t = 2k$ para algum $k\in\mathbb{N}$. Assim, se k for par, temos que

  $$\mathrm{rad}_4(t) = \mathrm{rad}_4(2k) = 2\,\mathrm{rad}(k)$$

  e consequetemente $4 \mid (q-1)$ absurdo. Logo, k é ímpar e $\mathrm{rad}_4(2k) = 2\,\mathrm{rad}(k)$ o que implica $\mathrm{rad}(k) \mid \frac{q-1}{2}$.

- Se t é ímpar então $\mathrm{rad}_4(t) = \mathrm{rad}(t)$ e $\mathrm{rad}(t) \mid \frac{q-1}{2}$.

Segue da Equação 3.9 que:

$$\sum_{t\le T} N_q(t) = \sum_{\substack{t\le T\\ \mathrm{rad}_4(t)\mid(q-1)}} N_q(t) = \sum_{\substack{t\le T\\ \mathrm{rad}(t)\mid\frac{q-1}{2}}} N_q(t) + \sum_{\substack{t\le T/2\\ \mathrm{rad}(t)\mid\frac{q-1}{2}}} N_q(2t).$$

Do item (1) temos que:

$$\sum_{\substack{t\leq T\\ \mathrm{rad}(t)|\frac{q-1}{2}}} N_q(t) = \frac{\varphi(q-1)}{s!l_1\cdots l_s}\left((\log T)^s + \frac{s}{2}\sum_{j=1}^{s}\frac{(p_j+1)\log p_j}{p_j-1}(\log T)^{s-1}\right) + o\left((\log T)^{s-1}\right) \quad (3.14)$$

e

$$\begin{aligned}\sum_{\substack{t\leq T/2\\ \mathrm{rad}(t)|\frac{q-1}{2}}} N_q(2t) &= (q-1)\sum_{\substack{t\leq T/2\\ \mathrm{rad}(t)|\frac{q-1}{2}}}\frac{\varphi(2t)}{2t} = \frac{(q-1)}{2}\sum_{\substack{t\leq T/2\\ \mathrm{rad}(t)|\frac{q-1}{2}}}\frac{\varphi(t)}{t}\\ &= \frac{\varphi(q-1)}{s!l_1\cdots l_s}\left(\frac{1}{2}\left(\log\frac{T}{2}\right)^s + \frac{s}{4}\sum_{j=1}^{s}\frac{(p_j+1)\log p_j}{p_j-1}\left(\log\frac{T}{2}\right)^{s-1}\right) + o\left((\log T)^{s-1}\right)\\ &= \frac{\varphi(q-1)}{s!l_1\cdots l_s}\left(\frac{1}{2}(\log T-\log 2)^s + \frac{s}{4}\sum_{j=1}^{s}\frac{(p_j+1)\log p_j}{p_j-1}(\log T-\log 2)^{s-1}\right) + o\left((\log T)^{s-1}\right)\end{aligned}$$

Agora, utizando o Teorema binômio de Newton obtemos

$$\frac{1}{2}(\log T-\log 2)^s = \frac{1}{2}\left((\log T)^s - s(\log T)^{s-1}\log 2 + \sum_{j=2}^{s}\binom{s}{j}(\log T)^{s-j}(-\log 2)^j\right) \quad \text{e}$$

$$(\log T-\log 2)^{s-1} = (\log T)^{s-1} + \sum_{j=1}^{s}\binom{s}{j}(\log T)^{s-j}(-\log 2)^j,$$

portanto,

$$\sum_{\substack{t\leq T/2\\ \mathrm{rad}(t)|\frac{q-1}{2}}} N_q(2t) = \frac{\varphi(q-1)}{s!l_1\cdots l_s}\left(\frac{1}{2}(\log T)^s - \left(\frac{s}{2}\log 2 + \frac{s}{4}\sum_{j=1}^{s}\frac{(p_j+1)\log p_j}{p_j-1}\right)(\log T)^{s-1}\right) + o\left((\log T)^{s-1}\right) \quad (3.15)$$

Somando as Equações 3.14 e 3.15 temos que

$$\sum_{\substack{t\leq T\\ \mathrm{rad}_4(t)|(q-1)}} N_q(t) = \frac{3\varphi(q-1)}{2.s!l_1\cdots l_s}\left((\log T)^s + \frac{s}{2}\left[\sum_{j=1}^{s}\frac{(p_j+1)\log p_j}{p_j-1} - \frac{2}{3}\log 2\right](\log T)^{s-1}\right) + o\left((\log T)^{s-1}\right)$$

como queríamos mostrar. ■

Como consequência direta do teorema acima temos o seguinte corolário:

Corolário 3.8. *Seja q uma potência de primo tal que* $q-1 = \begin{cases} p_1^{\alpha_1}\cdots p_s^{\alpha_s} & \text{se } q\not\equiv 3 \pmod 4\\ 2p_1^{\alpha_1}\cdots p_s^{\alpha_s} & \text{caso contrário.}\end{cases}$

Então

$$\frac{s!\log p_1\cdots\log p_s}{\varphi(q-1)}\cdot\lim_{T\to\infty}\frac{\sum_{1\leq t\leq T}N_q(t)}{(\log T)^s} = \begin{cases}1 & \text{se } q\not\equiv 3 \pmod 4\\ \frac{3}{2} & \text{caso contrário.}\end{cases}$$

3.3 Uma Cota para o Número de Binômios Irredutíveis com T pequeno

Nesta seção, fornecemos uma cota inferior e superior para o número de binômios irredutíveis quando T não é um número muito grande.

Supondo que $q \not\equiv 3 \pmod 4$, segue da Equação 3.10 que:

$$\sum_{t\leq T} N_q(t) = (q-1) \sum_{\substack{t\leq T \\ \mathrm{rad}(t)|(q-1)}} \frac{\varphi(t)}{t}.$$

Observando que $\frac{\varphi(q-1)}{q-1} \leq \frac{\varphi(t)}{t} \leq 1$ para qualquer t tal que $\mathrm{rad}(t)|(q-1)$ obtemos

$$\sum_{t\leq T} N_q(t) \geq \varphi(q-1) \sum_{\substack{t\leq T \\ \mathrm{rad}(t)|(q-1)}} 1 = \varphi(q-1)|\Upsilon(T)| = \varphi(q-1)\mathcal{N}_s(\log T; l_1+\cdots+l_s)$$

e

$$\sum_{t\leq T} N_q(t) \leq (q-1)|\Upsilon(T)| = (q-1)\mathcal{N}_s(\log T; l_1+\cdots+l_s)$$

para qualquer $T>1$, e concluímos a partir do Teorema 3.4 que:

$$\begin{aligned}\sum_{t\leq T} N_q(t) &> \frac{\varphi(q-1)}{s!\log p_1\cdots\log p_s}\left((\log T)^s + \frac{s}{2}(\log p_2+\cdots+\log p_s)\right)\\ &= \frac{\varphi(q-1)}{s!\log p_1\cdots\log p_s}(\log T)^s\left(1+\frac{s\log(\mathrm{rad}(q-1)/p_1)}{2\log T}\right)\end{aligned}$$

e

$$\begin{aligned}\sum_{t\leq T} N_q(t) &< \frac{(q-1)}{s!\log p_1\cdots\log p_s}\left((\log T)+\frac{1}{2}(2\log p_1+\log p_2+\cdots+\log p_s)\right)^s\\ &= \frac{q-1}{s!\log p_1\cdots\log p_s}(\log T)^s\left(1+\frac{\log(p_1\cdot\mathrm{rad}(q-1))}{2\log T}\right)^s\end{aligned}$$

O teorema seguinte fornece uma cota superior para o número de binômios em $\mathbb{F}_q[x]$.

Teorema 3.9. *Para qualquer $T \geq \mathrm{rad}(q-1)$, o número de binômios irredutíveis de grau menor ou igual a T em $\mathbb{F}_q[x]$ é limitado superiormente por:*

$$\frac{\varphi(q-1)}{s!\log p_1\cdots\log p_s}(\log T)^s\left(1+sM_1\frac{\log(\mathrm{rad}(q-1))}{\log T}+s(s-1)M_2\left(\frac{\log(\mathrm{rad}(q-1))}{\log T}\right)^2\right),$$

onde

$$M_1 := (\mathrm{rad}(q-1))^{-\frac{c(s-1)}{2\log T}}.\left(1+\frac{3+\log\log(s\log(s\log(s))}{s^2}\right)-\frac{1}{2}$$

e

$$M_2 := \frac{1}{8}+\frac{(s-1)(q-1)}{2s\varphi(q-1)}\cdot\left(\frac{3}{2}\right)^{s-2}.$$

Demonstração. Sabemos que o número de binômios mônicos irredutíveis é dado pela fórmula $(q-1)(A+B+C)$, onde A, B e C são definidos pela Equação 3.11. Assim, para obter uma cota superior para o número de binômios irredutíveis em $\mathbb{F}_q[x]$ é suficiente obter uma cota superior para A, B e C.

A partir das Equações 3.5, 3.6 e do Teorema 3.4 obtemos que

$$\begin{aligned}
A &= \frac{\varphi(q-1)}{q-1}\left|\Upsilon\left(\log\left(\frac{T}{\mathrm{rad}(q-1)}\right)\right)\right| = \frac{\varphi(q-1)}{q-1}\mathcal{N}_s\left(\log\left(\frac{T}{\mathrm{rad}(q-1)}\right);l_1,\ldots,l_s\right)\\
&\leq \frac{\varphi(q-1)}{q-1}\cdot\frac{\left(\log\left(\frac{T}{\mathrm{rad}(q-1)}\right)+\frac{1}{2}(l_1+\cdots+l_s)\right)^s}{s!l_1\cdots l_s}\\
&= \frac{\varphi(q-1)}{(q-1)s!l_1\cdots l_s}\left(\log T-\log(\mathrm{rad}(q-1))+\frac{1}{2}\log(\mathrm{rad}(q-1))\right)^s\\
&= \frac{\varphi(q-1)}{(q-1)s!l_1\cdots l_s}(\log T)^s\left(1-\frac{\log(\mathrm{rad}(q-1))}{2\log T}\right)^s\\
&\leq \frac{\varphi(q-1)}{(q-1)s!l_1\cdots l_s}(\log T)^s\left(1-s\frac{\log(\mathrm{rad}(q-1))}{2\log T}+s(s-1)\frac{(\log(\mathrm{rad}(q-1)))^2}{8(\log T)^2}\right). \qquad (3.16)
\end{aligned}$$

Da Equação 3.7 e do Teorema 3.4, temos que:

$$\begin{aligned}
B &= \frac{\varphi(q-1)}{q-1}\sum_{j=1}^{s}\frac{p_j}{p_j-1}|\Upsilon_j(T)|\\
&\leq \frac{\varphi(q-1)}{q-1}\sum_{j=1}^{s}\frac{p_j}{p_j-1}\frac{\left(\log\left(\frac{p_jT}{\mathrm{rad}(q-1)}\right)+\frac{1}{2}(l_1+\cdots+l_{j-1}+l_{j+1}+\cdots+l_s)\right)^{s-1}}{(s-1)!l_1\cdots l_{j-1}l_{j+1}\cdots l_s}\\
&= \frac{\varphi(q-1)}{(q-1)s!l_1\cdots l_s}(\log T)^{s-1}\sum_{j=1}^{s}\frac{sp_j\log p_j}{p_j-1}\left(1-\frac{\log\left(\frac{\mathrm{rad}(q-1)}{p_1p_j}\right)}{2\log T}\right)^{s-1}\\
&< \frac{\varphi(q-1)}{(q-1)s!l_1\cdots l_s}(\log T)^{s-1}\sum_{j=1}^{s}\frac{sp_j\log p_j}{p_j-1}\left(1-\frac{c\log(\mathrm{rad}(q-1))}{2\log T}\right)^{s-1}
\end{aligned}$$

onde $c=1-\frac{\log(p_1p_s)}{\log(\mathrm{rad}(q-1))}$.

Agora, utilizando a inequação $(1+x)\leq e^x$ obtemos

$$\sum_{j=1}^{s}\frac{sp_j\log p_j}{p_j-1}\left(1-\frac{c\log(\mathrm{rad}(q-1))}{2\log T}\right)^{s-1}\leq\sum_{j=1}^{s}\frac{sp_j\log p_j}{p_j-1}(\mathrm{rad}(q-1))^{-\frac{c(s-1)}{2\log T}}$$

uma vez que

$$\begin{aligned}\sum_{j=1}^{s}\frac{sp_j\log p_j}{p_j-1} &\le \sum_{j=1}^{s}\frac{s[(p_j-1)+1]\log p_j}{p_j-1} = \sum_{j=1}^{s}\left(s\log p_j+\frac{s\log p_j}{p_j-1}\right) = \sum_{j=1}^{s}s\log p_j+\sum_{j=1}^{s}\frac{s\log p_j}{p_j-1}\\ &\le \sum_{j=1}^{s}s\log p_j+\left(\frac{1}{s}\sum_{j=1}^{s}\log p_j\right)\left(\frac{1}{s}\sum_{j=1}^{s}s\frac{1}{p_j-1}\right) = \log(\mathrm{rad}(q-1))\left(s+\frac{1}{s}\sum_{j=1}^{s}\frac{1}{p_j-1}\right)\\ &\le \log(\mathrm{rad}(q-1))\left(s+\frac{1}{s}\left(1+\sum_{\substack{p\in\{\text{primeiros}\\(s-1)\text{ primos}\}}}\frac{1}{p}\right)\right), \qquad (3.17)\end{aligned}$$

onde na penúltima desigualdade utilizamos a inequação soma de Chebyshev (seção 2.17 de [16]).

Usando o fato que o $(s-1)$-ésimo primo é menor que $(s-1)[\ln(s-1)+\ln\ln(s-1)]$ e que $(s-1)\ln(s-1)+(s-1)\ln\ln(s-1) < s\ln(s\cdot\ln(s))$ (ver [32]), obtemos a partir da Inequação 3.17 que

$$\sum_{j=1}^{s}\frac{sp_j\log p_j}{p_j-1} \le \log(\mathrm{rad}(q-1))\left(s+\frac{1}{s}\left(1+\sum_{p\le s\ln(s)}\frac{1}{p}\right)\right) < \log(\mathrm{rad}(q-1))\left(s+\frac{1}{s}(3+\ln\ln(s\ln(s\cdot\ln(s))))\right),$$

onde na última desigualdade usamos que

$$\sum_{p\le x}\frac{1}{p} = \ln\ln(x)+B+o(1) < \ln\ln(x)+2, \quad \text{para todo } x\ge 2,$$

onde $B\approx 0.261497$ é a constante de Mertens (ver [34, Teorema 9]) . Portanto,

$$B < \frac{\varphi(q-1)}{(q-1)s!l_1\cdots l_s}(\log T)^{s-1}\log(\mathrm{rad}(q-1))\left(s+\frac{3+\log\log(s\log(s\cdot\log(s)))}{s}\right)(\mathrm{rad}(q-1))^{-\frac{c(s-1)}{2\log T}}. \qquad (3.18)$$

Finalmente, a partir das Equações 3.12 e 3.13 e usando os mesmos argumentos usados anteriormente obtemos:

$$\begin{aligned}C &\le \sum_{1\le i<j\le s}|\Upsilon_{ij}(T)|\\ &\le \sum_{1\le i<j\le s}\mathcal{N}_{s-2}(\log T;l_1,\ldots,\widehat{l_i},\ldots,\widehat{l_j},\ldots,l_s)\\ &\le \frac{1}{(s-2)!l_1\ldots l_s}(\log T)^{s-2}\sum_{1\le i<j\le s}l_il_j\left(1+\frac{\log\left(\frac{\mathrm{rad}(q-1)}{p_ip_j}\right)}{2\log T}\right)^{s-2}\\ &< \frac{1}{(s-2)!l_1\ldots l_s}(\log T)^{s-2}\cdot\sum_{1\le i<j\le s}l_il_j\cdot\left(1+\frac{\log(\mathrm{rad}(q-1))}{2\log T}\right)^{s-2}\\ &= \frac{1}{(s-2)!l_1\ldots l_s}(\log T)^{s-2}\cdot\left(1+\log(\mathrm{rad}(q-1))^{\frac{1}{2\log T}}\right)^{s-2}\sum_{1\le i<j\le s}l_il_j. \qquad (3.19)\end{aligned}$$

Usando a inequação de Maclaurin $\sum_{1\leq i<j\leq s} x_i x_j \leq \frac{s-1}{2s}\Big(\sum_{1\leq i\leq s} x_i\Big)^2$ (que se mostra a partir da desigualdade de Cauchy-Schwarz), segue da Inequação 3.19 que

$$C < \frac{1}{(s-2)!l_1\dots l_s}(\log T)^{s-2}\cdot\frac{s-1}{2s}(\log(\mathrm{rad}(q-1)))^2\cdot\left(1+\log(\mathrm{rad}(q-1))^{\frac{1}{2\log T}}\right)^{s-2} \tag{3.20}$$

Por hipótese, $\mathrm{rad}(q-1)\leq T$ o que implica que $1+\log(\mathrm{rad}(q-1))^{\frac{1}{2\log T}} \leq \frac{3}{2}$ e, concluímos a partir da 3.20 que

$$C < \frac{1}{(s-2)!l_1\dots l_s}(\log T)^{s-2}\frac{s-1}{2s}(\log(\mathrm{rad}(q-1)))^2\left(\frac{3}{2}\right)^{s-2} \tag{3.21}$$

Denotando $\omega = \mathrm{rad}(q-1)$ obtemos a partir das Equações 3.16, 3.18 e 3.21 que:

$$\begin{aligned}(q-1)(A+B+C) &\leq \frac{\varphi(q-1)}{s!l_1\cdots l_s}(\log T)^s\left[1+s\cdot\left(\omega^{-\frac{c(s-1)}{2\log T}}\cdot\left(1+\frac{3+\log\log(s\log s)}{s^2}\right)-\frac{1}{2}\right)\frac{\log(\omega)}{\log T}\right]\\ &\quad+\frac{\varphi(q-1)}{s!l_1\cdots l_s}(\log T)^s s(s-1)\left[\frac{1}{8}+\frac{(s-1)(q-1)}{2s\varphi(q-1)}\cdot\left(\frac{3}{2}\right)^{s-2}\right]\cdot\left(\frac{\log(\mathrm{rad}(q-1))}{\log T}\right)^2\\ &= \frac{\varphi(q-1)}{s!l_1\cdots l_s}(\log T)^s\left[1+s.M_1\frac{\log(\omega)}{\log T}+s(s-1)M_2\left(\frac{\log(\omega)}{\log T}\right)^2\right]\end{aligned}$$

Portanto,

$$(q-1)(A+B+C) \leq \frac{\varphi(q-1)}{s!l_1\cdots l_s}(\log T)^s\left[1+s.M_1\frac{\log(\mathrm{rad}(q-1))}{\log T}+s.(s-1)M_2\left(\frac{\log(\mathrm{rad}(q-1))}{logT}\right)^2\right],$$

onde $M_1 = (\mathrm{rad}(q-1))^{-\frac{c(s-1)}{2\log T}}\cdot\left(1+\frac{3+\log\log(s\log s)}{s^2}\right)-\frac{1}{2}$ e $M_2 = \frac{1}{8}+\frac{(s-1)(q-1)}{2s\varphi(q-1)}\cdot\left(\frac{3}{2}\right)^{s-2}$. ■

Referências Bibliográficas

[1] Bakshi G.K., Raka M. , *A class of constacyclic codes over a finite field*, Finite Fields Appl. 18 (2012) 362-377.

[2] Berlekamp, E. R. *Algebraic Coding Theory*, McGraw-Hill, New York 1968.

[3] Beukers, F. *The lattice-points of n-dimensional tetrahedra.* Indag. Math. **37** (1975), 365-372

[4] Blake, I. F., Gao, S., Mullin, R. C., *Explicit factorization of* $x^{2^k}+1$ *over* $\mathbb{F}_p$ *with* $p \equiv 3 \pmod 4$, Appl. Algebra Engrg. Comm. Comput. **4** 89-94 (1993).

[5] Brochero Martínez, F. E., Reis, L., Jesus, L, S., *Factorization of composed polynomials and applications*, Discrete Mathematics. **342** (2019).

[6] Brochero Martínez, F. E., Jesus, L, S., *The Estimation of the number of irreducible binomials*, arXiv:1909.08990. Aceito para publicação em Finite Fields Appl.

[7] Brochero Martínez, F. E., Giraldo Vergara, C. R., de Oliveira, L., *Explicit factorization of* $x^n - 1 \in \mathbb{F}_q[x]$. Des. Codes Cryptogr. **77** , no. 1, 277-286 (2015).

[8] Brochero Martínez, F. E., Giraldo Vergara, C. R., *Weight enumerator of some irreducible cyclic codes*. Des. Codes Cryptogr. **78**, 703-712 (2016).

[9] Brochero Martínez, F. E., Reis, L., *Factoring polynomials of the form* $f(x^n) \in \mathbb{F}_q[x]$, Finite Fields Appl. **49** (2018) 166-179.

[10] Brochero Martínez, F. E., Moreira, G. C., Saldanha, N., Tengan E.,*Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*, Coleção Projeto Euclides, quarta edição, Rio de Jeneiro: IMPA, 2018.

[11] Cohen, S. D., *Irreductible polynomials–Prescribed coefficients*, in Handbook of finite fields, G.L. Mullen and D. Panario, eds., CRC Press, Boca Raton, 2013

[12] Chen, B., Li, L., Tuerhong, R., *Explicit factorization of $x^{2^m p^n} - 1$ over a finite field*. Finite fields Appl. **24** 95-104 (2013).

[13] Fitzgerald, R.W., Yucas, J.L., *Explicit factorization of cyclotomic and Dickson polynomials over finite fields*. Arithmetic of Finite Fields. Lecture Notes in Comput. Sci, vol. **4547**, 1-10. Springer, Berlin (2007).

[14] Gao S., *Normal Bases over Finite Fields*. Thesis University of Waterloo Waterloo, Ontario, Canada, 1993.

[15] Golomb, S. W., *Shift Register Sequences* Holden-Day, Inc. 1967.

[16] Hardy, G. H., Littlewood, J. E., Pólya, G., *Inequalities*. Cambridge University Press London, 1934.

[17] Heyman, R., Shparlinski I. E., *Counting irreducible binomials over finite fields*. Finite Fields Appl. **38** 1-12 (2016).

[18] Huczynska S., Mullen G. L., Panario D., Thomson D., *Existence and properties of k-normal elements over finite fields*, Finite Fields Appl. **24** (2013) 170-183.

[19] H. Stichtenoth and A. Topuzoğlu. *Factorization of a class of polynomials over finite fields.* Finite Fields Appl. **18** (2012) 108-122.

[20] Lang, S. *Algebraic Number Theory*, Second edition. Graduate Texts in Mathematics, 110. Springer-Verlag, New York, 1994.

[21] Lehmer D. H., *The lattice points of an n-dimensional tetrahedron*. Duke J. Math. **7** 341-353 (1940).

[22] Lenstra, Jr., H. W., *On the Chor-Rivest knapsack cryptosystem*. J. Cryptol., **3**, 149-155 (1991).

[23] Li, F., Yue, Q., *The primitive idempotents and weight distributions of irreducible constacyclic codes.* Des. Codes Cryptogr. **86** (2018), 771-784

[24] Li, F., Cao X., *A class of minimal cyclic codes over finite fields*. Discrete Mathematics. vol. **340**, 3197-3206 (2017).

[25] Li, F., Cao X., *Explicit factorization of $x^{2^a p^b r^c} - 1$ over a finite field.* Acta Math. Sinica **58** (2015), 469-478.

[26] Lidl, R., Niederreiter, H., *Introduction to finite fields and their applications*. Cambridge University Press New York, NY, USA 1986.

[27] Liu, L., Li, L., Wang, L., Zhu, S., *Repeated-root constacyclic codes of length nlp^s*. Discrete Math. **340** (2017), 2250-2261.

[28] Lochs, G., *Über die Anzahl der Gitterpunkte in einem Tetraeder.* Revista Matemática Iberoamericana. **35**, (2019). 805-822.

[29] Meyn, H., *Factorization of the cyclotomic polynomials $x^{2^n}+1$ over finite fields*. Finite Fields Appl. **2**, 439-442 (1996).

[30] Mihailescu, P., *A class number free criterion for catalan's conjecture*. Journal of Number theory. **99**, 225-231 (2003).

[31] Reis, L., *Existence results on k-Normal elements over finite fields.* Revista Matemática Iberoamericana **35**, (2019). 805-822.

[32] Rosser, J., Schoenfeld, L. *Approximate formulas for some functions of prime numbers.* Illinois J. Math. **6** (1962) 64-94

[33] Spencer, D. C. *The lattice points of tetrahedra.* J. Math. Phys. Mass. Inst. Tech. **21** (1942), 189-197

[34] Tenenbaum, G., *Introduction to analytic and probabilistic number theory*. Cambridge University Press New York, NY, USA 2004.

[35] Tuxanidy, A., Wang, Q., *Composed products and factors of cyclotomic polynomials over finite fields*. Des. Codes Cryptogr. **69**, 203-231 (2013).

[36] Wang, L., Wang, Q., *On explicit factors of cyclotomic polynomials over finite fields*. Des. Codes Cryptogr. **63**, no. 1, 87-104 (2012).

[37] Y. Wu, Q. Yue, S. Fan. *Further Factorization of x^n-1 over a Finite Field*, Finite Fields Appl. **54**, 197-215 (2018).