Universidade Federal de Uberlândia
Faculdade de Matemática

SOBRE ELEMENTOS DISTINGUIDOS EM CORPOS FINITOS

Victor Gonzalo Lopez Neumann

Uberlândia-MG
2022

Victor Gonzalo Lopez Neumann

SOBRE ELEMENTOS DISTINGUIDOS EM CORPOS FINITOS

Tese apresentada a banca de avaliação da Universidade Federal de Uberlândia como parte dos requisitos para a promoção funcional da classe associado D nível 4 para classe E nível titular.

Área de concentração: Matemática
Linha de pesquisa: Álgebra Comutativa

Uberlândia-MG
2022

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da UFU, MG, Brasil.

N492s 2022

Neumann, Victor Gonzalo Lopez, 1974-
Sobre elementos distinguidos em corpos finitos [recurso eletrônico] / Victor Gonzalo Lopez Neumann. - 2022.

Tese (Promoção para classe E - Professor Titular) - Universidade Federal de Uberlândia, Faculdade de Matemática.
Modo de acesso: Internet.
Disponível em: http://doi.org/10.14393/ufu.te.2022.5035
Inclui bibliografia.

1. Corpos finitos (Álgebra). I. Universidade Federal de Uberlândia. Faculdade de Matemática. II. Título.

CDU: 512.624

André Carlos Francisco
Bibliotecário – CRB-6/3408

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Faculdade de Matemática
Av. João Naves de Àvila, 2121, Bloco 1F - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: +55 (34) 3239-4158/4156/4126 - www.famat.ufu.br - famat@ufu.br

ATA

ATA DA COMISSÃO ESPECIAL PARA JULGAMENTO DA DEFESA PÚBLICA DE TESE DO PROFESSOR VICTOR GONZALO LOPEZ NEUMANN, COMO REQUISITO PARA PROMOÇÃO À CLASSE DE PROFESSOR TITULAR DA FACULDADE DE MATEMÁTICA DA UNIVERSIDADE FEDERAL DE UBERLÂNDIA.

Em 19 de outubro de 2022, às 09h30, por meio remoto, utilizando a plataforma RNP, teve início a defesa pública de tese do docente Victor Gonzalo Lopez Neumann, como requisito para promoção à classe de Professor Titular. Participaram, por meio de acesso simultâneo ao ambiente virtual de transmissão da conferência, os membros da Comissão Especial, aprovada pelo Conselho da Faculdade de Matemática e designada na Portaria de Pessoal UFU Nº 4971, de 03 de outubro de 2022, a saber: Prof. Dr. Fábio Enrique Brochero Martinez (UFMG - Presidente), Profa. Dra. Luciane Quoos Conte (UFRJ), Profa. Dra. Marinês Guerreiro (UFV) e Prof. Dr. Renato Vidal da Silva Martins (UFMG). Iniciando os trabalhos, o presidente da Comissão, Prof. Dr. Fábio Enrique Brochero Martinez, cumprimentou os demais membros da Comissão Especial, o candidato e os presentes. Na sequência, a palavra foi concedida ao Prof. Dr. Victor Gonzalo Lopez Neumann, que fez a exposição da sua tese. A seguir, cada um dos membros da Comissão Especial arguiu o candidato à promoção à classe de professor titular, na seguinte ordem: Profa. Dra. Luciane Quoos Conte (UFRJ), Profa. Dra. Marinês Guerreiro (UFV), Prof. Dr. Renato Vidal da Silva Martins (UFMG) e Prof. Dr. Fábio Enrique Brochero Martinez (UFMG - Presidente). Finalizada a fase da arguição, a Comissão Especial, em sessão secreta, considerou o candidato aprovado. Nada mais havendo a tratar, os trabalhos foram encerrados às 11:16 horas e a presente ata foi lavrada por mim, Fábio Enrique Brochero Martinez, Presidente da Comissão Especial. Após lida e aprovada pela Comissão Especial, a ata será assinada por todos os seus membros.

Prof. Dr. Fábio Enrique Brochero Martinez (UFMG - Presidente)

Profa. Dra. Luciane Quoos Conte (UFRJ)

Profa. Dra. Marinês Guerreiro (UFV)

Prof. Dr. Renato Vidal da Silva Martins (UFMG)

Documento assinado eletronicamente por **Luciane Quoos Conte**, **Usuário Externo**, em 21/10/2022, às 08:30, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Fabio Enrique Brochero Martinez**, **Usuário Externo**, em 22/10/2022, às 19:43, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Renato Vidal da Silva Martins**, **Usuário Externo**, em 25/10/2022, às 15:29, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Marines Guerreiro**, **Usuário Externo**, em 25/10/2022, às 16:03, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4013769** e o código CRC **8CE43E9A**.

Para o meu pai, que sempre desejou o melhor para mim.

Para mi papá, que siempre me deseó lo mejor.

Agradecimentos

À minha esposa Adriane e filhos Matheus, Gabriel, Ana Letícia e Bárbara por manter um lar amoroso, sereno e propício aos estudos.

À minha mãe Celeste, minha filha Sofia, meus irmãos Adolfo, Maria Celeste, Elfriede e minha sobrinha Samanta, pelo apoio e carinho.

Aos meus mentores Dr. Hansen, Dr. Nelson e Zahia, que me sustentaram nos momentos de dificuldade e me mostraram o caminho certo.

Aos meus parceiros de pesquisa Abílio Lemos, Cícero Carvalho, Guilherme Tizziotti, João Paulo Guardieiro, Josimar Aguirre e Sávio Ribas a quem devo muito do trabalho realizado nesta tese.

À FAPEMIG pelo apoio financeiro ao Projeto de Pesquisa APQ-03365-18, sob minha coordenação, cuja tese é fruto de parte dos resultados desse projeto.

À Faculdade de Matemática e à Universidade Federal de Uberlândia por oferecerem um ambiente agradável para o desenvolvimento desta pesquisa.

Aos professores, funcionários e colegas da Faculdade de Matemática da UFU.

Aos membros da Comissão Julgadora.

NEUMANN, V. G. L. *.Sobre elementos distinguidos em corpos finitos*. **2022**. **122p**. **Tese** , **Universidade Federal de Uberlândia**, **Uberlândia-MG**.

Resumo

Nesta tese mostramos alguns resultados sobre elementos primitivos, elementos normais e suas generalizações. A tese começa estudando a existência de elementos primitivos normais cuja imagem por uma função racional seja primitiva. O segundo resultado se inspira em trabalhos de Cohen que estuda elementos primitivos consecutivos. Na tese tratamos de progressões aritméticas, com razão dada, nas quais todos os elementos são primitivos e um deles também é normal. A seguir procuramos fórmulas explícitas para o número de elementos k-normais em extensões de corpos finitos. Em particular, encontramos uma fórmula que depende do número de soluções de certas equações diofantinas. Já para $k = 0, 1, 2, 3$ encontramos fórmulas combinatórias fáceis de calcular. Também estudamos a existência de elementos primitivos 2-normais e finalmente estudamos elementos r-primitivos k-normais de forma geral e aplicamos os resultados para o caso particular em que o corpo é de característica 11, $r = 3$ e $k = 3$.

Palavras-chave: corpos finitos, elementos primitivos, elementos normais, elementos r-primitivos, elementos k-normais.

NEUMANN, V. G. L. ***About distinguished elements in finite fields***. **2022**. **122p**. **Thesis**, **Federal University of Uberlândia**, **Uberlândia-MG**.

Abstract

In this thesis, we show some results about primitive normal elements and their generalizations. The thesis begins by studying the existence of primitive normal elements whose image by a rational function is primitive. The second result draws on a work of Cohen which studies consecutive primitive elements. In the thesis, we deal with arithmetic progressions, with a given common difference, such that all elements are primitive and one of them is normal. Next, we look for explicit formulas for the number of k-normal elements in extensions of finite fields. In particular, we find a formula that depends on the number of solutions of certain Diophantine equations. For $k = 0, 1, 2, 3$ we find combinatorial formulas that are easy to compute. We also study the existence of 2-normal primitive elements and finally we study r-primitive k-normal elements in general, and apply these results to the particular case where the field has characteristic 11, $r = 3$ and $k = 3$.

Keywords: finite fields, primitive elements, normal elements, r-primitive elements, k-normal elements.

Sumário

Lista de Tabelas

Introdução

A teoria dos Corpos Finitos é um ramo da matemática que veio a tona nos últimos cinquenta anos por causa de suas diversas aplicações em vários segmentos da ciência, entre eles podemos citar a análise combinatória, a teoria dos códigos, o estudo matemático de circuitos comutativos, entre outros. Muitas figuras proeminentes na história da matemática compuseram esforços no desenvolvimento desta teoria, entre elas figuram Pierre de Fermat (1601-1665), Leonhard Euler (1707-1783), Joseph-Louis Lagrange (1736-1813) e Andrien-Marie Legendre (1752-1833) por exemplo. Além disso, segundo R. Lidl e H. Niederreiter (ver [27]), a teoria dos corpos finitos começou com os trabalhos de Carl Friedrich Gauss (1777-1855) e Evariste Galois (1811-1832), mas só veio a se tornar interessante para os matemáticos de áreas aplicadas nas últimas décadas, quando a matemática discreta passou a ser tratada como uma teoria séria.

Essencialmente nesta tese estudam-se elementos primitivos em corpos finitos, elementos normais em extensões de corpos finitos, as generalizações de ambos tipos de elementos e outras características. Esse tipo de elementos é foco de pesquisa na atualidade. Especificamente esta tese apresenta as contribuições originais dos seguintes artigos científicos.

- [6] On the existence of pairs of primitive and normal elements over finite fields (com Cícero Carvalho, João Paulo Guardieiro e Guilherme Tizziotti), Bulletin of the Brazilian Mathematical Society, New Series 53(3) (2022).
- [25] On arithmetic progressions in finite fields (com Abílio Lemos e Sávio Ribas), preprint (2022).
- [3] Number of k-normal elements over a finite field (com Josimar Aguirre), preprint (2022).
- [2] Existence of primitive 2-normal elements in finite fields (com Josimar Aguirre), Finite Fields and Their Applications 73 (2021).
- [1] About r-primitive and k-normal elements in finite fields (com Cícero Carvalho e Josimar Aguirre), Designs, Codes and Cryptography (2022 - aceito).

Revisão da literatura

Em 1987, Lenstra e Schoof provaram em [26] o teorema da base primitiva normal que afirma que em toda extensão de corpos finitos existe uma base normal composta por elementos primitivos. Em 2003, Cohen e Huczynska (ver [10]) demonstraram o mesmo resultado sem o uso do computador e, além de usar somas de caracteres, introduziram o método do crivo para refinar os resultados. Em 2010, os mesmos autores provaram em [11] o teorema da base primitiva normal forte que afirma que em toda extensão de corpos (com poucas exceções) existe um elemento α primitivo normal tal que α^{-1} é também primitivo normal. Na mesma linha de raciocínio, em 2014, Kapetanakis (ver [20] e [21]) provou que para toda potência de primo q e todo inteiro positivo n, com poucas exceções, e para quase toda função da forma $f(x) = \frac{ax+b}{cx+d}$ com $a, b, c, d \in \mathbb{F}_q$, existe $\alpha \in \mathbb{F}_{q^n}$ tal que α e $f(\alpha)$ são primitivos e normais sobre $\mathbb{F}_q$. Em 2017 Anju e Sharma (ver [37]), seguindo as ideias de [10] e assumindo q de característica 2, provaram que dados polinômios $f(x), g(x) \in \mathbb{F}_{q^n}[x]$, sendo $f(x)$ de grau máximo 2 e $g(x)$ de grau máximo 1, existe um elemento $\alpha \in \mathbb{F}_{q^n}$, primitivo e normal sobre $\mathbb{F}_q$, tal que $f(\alpha)/g(\alpha)$ é também primitivo, exceto para poucas combinações de $q = 2^k$, n, $f(x)$ e $g(x)$. Recentemente, Hazarika, Basnet e Cohen (ver [16]) estudaram este problema trabalhando em corpos de característica 3, considerando polinômios de grau máximo 2, no lugar de trabalhar com funções racionais. Hazarika, Basnet e Kapetanakis ([17]) também consideraram o problema de encontrar pares de elementos primitivos normais $(\alpha, f(\alpha))$, ambos em $\mathbb{F}_{q^n}$, sendo $\mathbb{F}_{q^n}$ de característica 2 e f é o quociente de um polinômio de grau máximo 2 por outro polinômio de grau máximo 1. Inspirados pelos resultados acima, trabalhamos problemas similares em corpos finitos de qualquer característica, para quocientes de funções de qualquer grau (ver [5] e [6]). Nessa tese apresentamos os resultados obtidos em [6]. Há, na literatura, diversos trabalhos que tratam do mesmo problema com algumas variantes (ver [12], [36], [35]).

Um problema similar consiste no estudo de elementos primitivos consecutivos. Nesse caso, é necessário que a quantidade de elementos consecutivos seja menor ou igual à característica do corpo finito. Em 1968 Vegh [41] respondeu a uma pergunta do seu antigo orientador A. Brauer sobre a existência de elementos primitivos consecutivos em $\mathbb{F}_p$, com p número primo. Ele provou que se $p > 3$ e $\varphi(p-1)/(p-1) > 1/3$, então existem elementos primitivos $\alpha, \alpha + 1 \in \mathbb{F}_p$. Três anos mais tarde (ver [40]) ele provou, entre outros resultados, que se $p \equiv 1 \pmod 4$, então basta ter $\varphi(p-1)/(p-1) > 1/4$ para garantir a existência de elementos primitivos consecutivos em $\mathbb{F}_p$. Esses resultados foram melhorados e ampliados para potências de primos por Cohen (ver [7, 8, 9]) em 1985. Ele provou que se $q > 7$, então $\mathbb{F}_q$ contém dois elementos primitivos consecutivos. Mais tarde, em 2015, Cohen *et al.* (ver [13, Theorem 1]) provaram que se $q > 169$ é ímpar, então sempre há 3 elementos primitivos consecutivos em $\mathbb{F}_q$. Além disso, os valores de $q \leq 169$ para os quais essa afirmação é falsa são $q = 3, 5, 7, 9, 13, 25, 29, 61, 81, 121$ e 169. Nesse mesmo artigo, o problema de 4 elementos primitivos consecutivos também foi tratado e, foi conjecturado que todo corpo com mais de 2401 elementos contém 4 elementos primitivos consecutivos. Esse resultado foi recentemente provado por Jarso e Trudgian (ver [19]). Na presente tese, tratamos os resultados de [25], no qual discutimos a existência de m termos em progressão aritmética em $\mathbb{F}_{q^n}$, todos eles primitivos e pelo menos um deles sendo normal sobre $\mathbb{F}_q$. Obtemos resultados assintóticos (para $m \geq 4$) e também resultados concretos (para $m = 2$ e $m = 3$).

Em 2013 (ver [18]) surgiu a definição de elemento k-normal, uma generalização da definição de elemento normal e nesse artigo são estudadas várias de suas propriedades. Entre outras coisas, no final desse trabalho são propostos vários problemas em aberto. Alguns resultados da tese tratam justamente desses problemas. Por exemplo, em [18] os autores apresentam uma fórmula para o número de elementos k-normais [18, Theorem 3.5], usando um resultado devido a Ore (ver [29]). Essa fórmula depende da fatoração de $x^n - 1$ em fatores irredutíveis sobre $\mathbb{F}_q$. Como a fórmula obtida não é muito fácil de ser trabalhada numericamente, Huczynska *et al.* propuseram o seguinte problema (ver [18, Problem 6.1]): Para que valores de q, n e k é possível encontrar fórmulas explícitas manipuláveis (em função de q e n) para o número de elementos k-normais em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$?

Inspirados pelo problema proposto, Saygi *et al.* (ver [34]) obtêm algumas fórmulas explícitas para certos valores particulares de q e n. Esses resultados dependem da fatoração explícita dos polinômios ciclotômicos e da solução de algumas equações Diofantinas lineares. Nessa tese apresentamos os resultados de [3], no qual são obtidas fórmulas para o número de elementos k-normais para todas as extensões $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. A seguir obtemos fórmulas explícitas para o número de elementos k-normais para $k = 0, 1, 2, 3$ e finalmente mostramos alguns resultados numéricos para verificar a eficácia das fórmulas.

Outro dos problemas formulados por Huczynska *et al.* (ver [18, Problem 6.3]) foi: Determine os pares (n, k) para os quais existem elementos primitivos k-normais em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Em [18] os autores trabalharam o caso $k = 1$ e obtiveram resultados parciais. Em 2018, Reis e Thompson (ver [33]) completaram o caso $k = 1$ e provaram o teorema do elemento primitivo 1-normal que estabelece que existem elementos primitivos 1-normais em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ para toda potência de primo q e todo $n \geq 3$ e quando $n = 2$ não existem tais elementos. Seguindo essa linha, em 2019, Reis (ver [32]) obteve condições de suficiência para a existência de elementos primitivos k-normais e provou que para todo $\varepsilon > 0$ e todo q suficientemente grande, existem elementos primitivos k-normais para $k \in [0, (\frac{1}{2} - \varepsilon)n]$, sempre que elementos k-normais existam em $\mathbb{F}_{q^n}$. Em [2] estudamos o caso $k = 2$ e provamos o teorema do elemento primitivo 2-normal.

Uma generalização natural do problema sobre a existência de elementos primitivos k-normais seria estudar a existência de elementos r-primitivos k-normais. É esse justamente outro dos problemas propostos por Huczynska *et al.* (ver [18, Problem 6.4]): Determinar a existência de elementos k-normais $\alpha \in \mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ de ordem elevado, sendo que "ordem elevado" quer dizer $\mathrm{ord}(\alpha) = N$, com N um divisor positivo grande de $q^n - 1$. Em [1] estudamos esse problema, em particular provamos resultados assintóticos para valores arbitrários de r e k, e resolvemos o problema da existência de elementos 3-primitivos 3-normais em característica 11.

Organização da tese

No capítulo 1, são abordados os conceitos, notações e resultados que serão utilizados ao longo dos capítulos seguintes. Começamos com as notações que serão utilizadas para algumas funções aritméticas e seguimos com alguns resultados importantes da teoria de corpos finitos. Estudamos também caracteres e finalmente é abordado um

apanhado de limitantes necessários para os capítulos posteriores.

No capítulo 2, mostramos os resultados de [6] que tratam sobre a existência de pares de elementos $(\alpha, f_1(\alpha)/f_2(\alpha))$, ambos em $\mathbb{F}_{q^n}$, tais que α é primitivo normal e $f_1(\alpha)/f_2(\alpha)$ é primitivo com $f_1, f_2 \in \mathbb{F}_{q^n}[x]$ polinômios de graus m_1 e m_2 (inteiros positivos quaisquer), respectivamente, satisfazendo propriedades específicas (ver Corolário 2.4). Tratamos também especificamente o caso em que $m_1 = 3$ e $m_2 = 2$.

No Capítulo 3, mostramos os resultados obtidos em [25]. Discutimos a existência de m termos em progressão aritmética em $\mathbb{F}_{q^n}$, todos eles primitivos e pelo menos um deles sendo normal sobre $\mathbb{F}_q$. Obtemos resultados assintóticos para $m \geq 4$ e resultados concretos para $m \leq 3$. Em particular, para $m = 2$ e $m = 3$ apresentamos uma lista completa das exceções quando a razão da progressão aritmética é um elemento de $\mathbb{F}_q^*$.

No Capítulo 4, mostramos os resultados obtidos em [3]. Nesse capítulo obtemos fórmulas para o número de elementos k-normais para todas as extensões $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Esses resultados dependem da solução de algumas equações Diofantinas lineares, mas não usamos a fatoração dos polinômios ciclotômicos como em [34]. A seguir obtemos fórmulas explícitas para o número de elementos k-normais para $k = 0, 1, 2, 3$. No decorrer do capítulo mostramos alguns resultados numéricos para verificar a eficácia das fórmulas.

No Capítulo 5, tratamos os resultados de [2], no qual resolvemos completamente o caso $k = 2$ e provamos que para toda potência de primo q existem elementos primitivos 2-normais em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ se, e somente se, $n \geq 5$ e $\mathrm{mdc}(q^3 - q, n) \neq 1$ ou $n = 4$ e $q \equiv 1 \pmod 4$.

No Capítulo 6, apresentamos os resultados de [1], no qual é estudada a existência de elementos r-primitivos k-normais. Em particular, provamos resultados assintóticos para valores arbitrários de r e k. Finalizamos o capítulo resolvendo o problema da existência de elementos 3-primitivos 3-normais em característica 11.

No Capítulo 7, indicamos possíveis trabalhos futuros.

Vale ressaltar que todos os resultados numéricos da tese foram obtidos usando SageMath [38].

CAPÍTULO 1

Preliminares

Neste capítulo, introduzimos algumas definições, notações e resultados básicos que serão utilizados ao longo da tese. Começamos com as definições e notações de algumas funções aritméticas que serão utilizadas posteriormente. O capítulo continua com resultados básicos de teoria de Corpos Finitos. A seguir, continuamos com o estudo de caracteres, elementos s-livres, para s um divisor positivo de $q-1$ e elementos g-livres, para um polinômio mônico g divisor de x^n-1. Finalizamos o capítulo mostrando algumas desigualdades que serão necessárias nos capítulos posteriores. A maioria dos resultados que se encontram em [27] serão apresentados sem provas, para outros resultados será apresentada uma referência para a demonstração e alguns resultados serão apresentados com provas.

Para maiores detalhes sobre a teoria dos Corpos Finitos recomendamos a leitura de [27], [28] e [15].

1.1 Notações básicas

Vamos denotar por $\mathbb{Z}$ o conjunto de números inteiros e por $\mathbb{Z}_+$ o conjunto de inteiros positivos. Dado um inteiro positivo m, denotamos por $\mathbb{Z}_m$ o conjunto de inteiros módulo m e por $\mathbb{Z}_m^*$ o conjunto de inteiros invertíveis módulo m.

Definição 1.1. *Uma função a valores reais ou complexos definida nos inteiros positivos é chamada de função aritmética. Uma função aritmética f é multiplicativa se, para todo par de inteiros positivos a, b primos entre si, tem-se $f(ab) = f(a)f(b)$.*

Definição 1.2. *Denotamos por* $\mathrm{mdc}(a,b)$ *o máximo divisor comum dos inteiros positivos a, b e denotamos por* $\mathrm{mmc}(a,b)$ *o mínimo múltiplo comum dos inteiros positivos a, b.*

Definição 1.3. *Define-se a função de Möbius $\mu : \mathbb{Z}_+ \longrightarrow \mathbb{Z}$ por*

$$\mu(m) = \begin{cases} 1 & \text{se } m = 1, \\ 0 & \text{se existe } a > 1 \text{ tal que } a^2 \mid m, \\ (-1)^k & \text{se } m \text{ é o produto de } k \text{ primos distintos.} \end{cases}$$

Dado um conjunto finito A, denotamos por $|A|$ o número de elementos do conjunto A.

Definição 1.4. *Define-se a função φ de Euler $\varphi : \mathbb{Z}_+ \longrightarrow \mathbb{Z}$ por $\varphi(m) = |\mathbb{Z}_m^*|$.*

Definição 1.5. *A função $\omega : \mathbb{Z}_+ \longrightarrow \mathbb{Z}$ conta o número de divisores primos de um inteiro positivo e a função $W : \mathbb{Z}_+ \longrightarrow \mathbb{Z}$ conta o número de divisores livres de quadrados de um inteiro positivo dado. Isto é,*

$$\omega(m) = \begin{cases} 0 & \text{se } m = 1, \\ k & \text{se } m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \text{ é a fatoração de } m \text{ como produto de primos distintos} \end{cases}$$

e

$$W(m) = \begin{cases} 1 & \text{se } m = 1, \\ 2^k & \text{se } m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \text{ é a fatoração de } m \text{ como produto de primos distintos.} \end{cases}$$

Da Definição 1.5 vemos que para todo inteiro positivo m temos $W(m) = 2^{\omega(m)}$.

Definição 1.6. *Dado um inteiro positivo m, denotamos por* $\mathrm{rad}(m)$ *o maior divisor positivo livre de quadrados de m. Em outras palavras,* $\mathrm{rad}(m)$ *é o produto dos fatores primos de m.*

Outra função importante é a função que conta o número de primos menores ou iguais a um número dado.

Definição 1.7. *Se x for um número real positivo, $\pi(x)$ denota a quantidade de números primos menores ou iguais a x.*

No decorrer da tese precisaremos também das funções piso e teto.

Definição 1.8. *Para um número real x, o teto de x é o menor inteiro $\lceil x \rceil$ que satisfaz $x \leq \lceil x \rceil$ e o piso de x é o maior inteiro $\lfloor x \rfloor$ que satisfaz $\lfloor x \rfloor \leq x$.*

1.2 Corpos Finitos

Dado um número primo p, o conjunto de inteiros módulo p é um corpo. Denotamos este corpo por $\mathbb{F}_p$. Dado qualquer polinômio irredutível $f(x)$ de grau s com coeficientes em $\mathbb{F}_p$, o quociente $\mathbb{F}_p[x]/(f(x))$ é um corpo com $q := p^s$ elementos. Existe, a menos isomorfismo, um único corpo de ordem q. O corpo finito com q elementos é denotado por $\mathbb{F}_q$ e a característica desse corpo é p. Denotamos por $\overline{\mathbb{F}}_q$ o fecho algébrico de $\mathbb{F}_q$ e, para todo inteiro positivo n, consideramos sempre $\mathbb{F}_q \subset \mathbb{F}_{q^n} \subset \overline{\mathbb{F}}_q$. Denotamos por $\mathbb{F}_q^*$ o grupo multiplicativo de elementos não nulos de $\mathbb{F}_q$.

Ao longo da tese, o número primo p nem sempre denota a característica de $\mathbb{F}_q$. Toda vez que um primo p for introduzido, as suas propriedades ficarão claras no texto.

Definição 1.9. *Para a extensão $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$, o morfismo de Frobenius $\sigma_q : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ é definido por $\sigma_q(\alpha) = \alpha^q$.*

Teorema 1.10. *O grupo de Galois da extensão $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é um grupo cíclico de ordem n gerado por σ_q.*

Definição 1.11. *Dado um elemento $\alpha \in \mathbb{F}_{q^n}$, os conjugados de α sobre $\mathbb{F}_q$ são os elementos $\sigma_q^{(i)}(\alpha) = \alpha^{q^i}$, para $i = 0, \ldots, n-1$.*

Definição 1.12. *Sejam m um divisor de n e $\alpha \in \mathbb{F}_{q^n}$.*

(i) $\mathrm{Tr}_{q^n/q^m}(\alpha) = \sum_{i=0}^{\frac{n}{m}-1} \alpha^{q^{im}}$ *é o traço de α sobre $\mathbb{F}_{q^m}$.*

(ii) $\mathrm{N}_{q^n/q^m}(\alpha) = \prod_{i=0}^{\frac{n}{m}-1} \alpha^{q^{im}} = \alpha^{\frac{q^n-1}{q^m-1}}$ *é a norma de α sobre $\mathbb{F}_{q^m}$.*

Denotamos por Tr_{q^n} *a função traço sobre $\mathbb{F}_p$ e* N_{q^n} *a função norma sobre $\mathbb{F}_p$, quando p é a característica de $\mathbb{F}_{q^n}$.*

Como $\mathbb{F}_q[x]$ é um domínio euclidiano, assim como $\mathbb{Z}$, podemos definir funções em $\mathbb{F}_q[x]$ de forma similar como foi feito em $\mathbb{Z}$.

Definição 1.13. *Dados os polinômios $f, g \in \mathbb{F}_q[x]$ (não ambos nulos), denotamos por* $\mathrm{mdc}(f, g)$ *o polinômio mônico em $\mathbb{F}_q[x]$ de maior grau que divide f e g. Se ambos polinômios não são nulos, denotamos por* $\mathrm{mmc}(f, g)$ *o polinômio mônico em $\mathbb{F}_q[x]$ de menor grau que é múltiplo de f e g. Dado o polinômio $f \in \mathbb{F}_q[x]\backslash\{0\}$, denotamos por* $\mathrm{grau}(f)$ *o grau de f.*

Definição 1.14. *Define-se a função de Möbius para polinômios $\mu_q : \mathbb{F}_q[x]\backslash\{0\} \longrightarrow \mathbb{Z}$ por*

$$\mu_q(f) = \begin{cases} 1 & \text{se } f \in \mathbb{F}_q\backslash\{0\}, \\ 0 & \text{se existe } h \in \mathbb{F}_q[x] \text{ de grau maior ou igual a } 1 \text{ tal que } h^2 \mid f, \\ (-1)^k & \text{se } f \text{ é o produto de } k \text{ polinômios irredutíveis não associados entre eles.} \end{cases}$$

Da própria definição temos que a função de Möbius para polinômios é multiplicativa, isto é, se $f, g \in \mathbb{F}_q[x]\backslash\{0\}$ são polinômios primos entre si, então $\mu_q(fg) = \mu_q(f)\mu_q(g)$.

Definição 1.15. *Define-se a função de Euler para polinômios $\phi_q : \mathbb{F}_q[x]\backslash\mathbb{F}_q \longrightarrow \mathbb{Z}$ por*

$$\phi_q(f) = \left|\left(\mathbb{F}_q[x]/(f)\right)^*\right|,$$

sendo que (f) denota o ideal gerado por f em $\mathbb{F}_q[x]$ e $\left(\mathbb{F}_q[x]/(f)\right)^*$ é o conjunto de elementos invertíveis no anel quociente $\mathbb{F}_q[x]/(f)$.

Do teorema chinês dos restos, ϕ_q é multiplicativa. Na Seção 1.5 precisaremos do seguinte resultado.

Lema 1.16. *Seja $g \in \mathbb{F}_q[x]$ um polinômio não constante. Então*

$$\prod_{\substack{r \mid g \\ r \text{ é mônico} \\ \text{e irredutível}}} \left(\frac{q^{\mathrm{grau}(r)}}{q^{\mathrm{grau}(r)} - 1}\right) = \frac{q^{\mathrm{grau}(g)}}{\phi_q(g)}.$$

Demonstração. Seja $g = \lambda r_1^{a_1} r_2^{a_2} \cdots r_k^{a_k}$ a fatoração de g em polinômios mônicos irredutíveis distintos $r_1, \ldots, r_k$, na qual $a_1, \ldots, a_k$ são inteiros positivos e $\lambda \in \mathbb{F}_q^*$. Para cada $i \in \{1, \ldots, k\}$, o anel $\mathbb{F}_q[x]/(r_i^{a_i})$ possui $q^{a_i \text{grau}(r_i)}$ elementos, dos quais $q^{(a_i-1)\text{grau}(r_i)}$ são múltiplos de r_i. Logo $\phi_q(r_i^{a_i}) = q^{(a_i-1)\text{grau}(r_i)}(q^{\text{grau}(r_i)} - 1)$ e

$$\prod_{i=1}^{k} \left(\frac{q^{\text{grau}(r_i)}}{q^{\text{grau}(r_i)} - 1} \right) = \prod_{i=1}^{k} \left(\frac{q^{a_i \text{grau}(r_i)}}{\phi_q(r_i^{a_i})} \right) = \frac{q^{\text{grau}(g)}}{\phi_q(g)}.$$

□

Definição 1.17. *Define-se a função $N : \mathbb{F}_q[x]\backslash\{0\} \longrightarrow \mathbb{Z}_+$ por $N(g) = q^{\text{grau}(g)}$.*

A partir da definição anterior, o Lema 1.16 pode ser reescrito como

$$\prod_{\substack{r \mid g \\ r \text{ é mônico} \\ \text{e irredutível}}} \left(\frac{N(r)}{\phi_q(r)} \right) = \frac{N(g)}{\phi_q(g)}.$$

Definição 1.18. *A função $\omega_q : \mathbb{F}_q[x]\backslash\{0\} \longrightarrow \mathbb{Z}$ conta o número de divisores mônicos irredutíveis de um polinômio não nulo e a função $W_q : \mathbb{F}_q[x]\backslash\{0\} \longrightarrow \mathbb{Z}$ conta o número de divisores mônicos livres de quadrados de um polinômio não nulo dado.*

Da Definição 1.18, temos $\omega_q(f) = 0$, se $f \in \mathbb{F}_q^*$, e $\omega_q(f) = k$, se $f(x) = \lambda p_1(x)^{a_1} p_2(x)^{a_2} \cdots p_k(x)^{a_k}$ é a fatoração de f como produto de fatores mônicos irredutíveis distintos, com $\lambda \in \mathbb{F}_q^*$ e $W_q(f) = 2^{\omega_q(f)}$.

Também se $f, g \in \mathbb{F}_q[x]\backslash\{0\}$ são primos entre si, então $\omega_q(fg) = \omega_q(f) + \omega_q(g)$. Em outras palavras, W_q é multiplicativa.

Definição 1.19. *Dado um polinômio não nulo $f \in \mathbb{F}_q[x]$, denotamos por $\text{rad}_q(f)$ o maior divisor mônico livre de quadrados de f. Em outras palavras, $\text{rad}_q(f)$ é o produto dos fatores mônicos irredutíveis distintos de f.*

Provemos agora um resultado interessante sobre polinômios que será utilizado no estudo de elementos k-normais.

Lema 1.20. *Sejam $f, g, h \in \mathbb{F}_q[x]$ polinômios não nulos tais que $\text{mdc}(g, h) = 1$. Então existe $\tilde{g} \in \mathbb{F}_q[x]$ tal que $\text{mdc}(f, h + \tilde{g}g) = 1$.*

Demonstração. Se f for constante, o resultado é obvio. Se f não for contante, sejam $r_1, \ldots, r_s \in \mathbb{F}_q[x]$ polinômios mônicos irredutíveis tais que $\text{rad}_q(f) = r_1 \cdots r_s$. Defina

$$\tilde{g} = \prod_{\substack{i=1 \\ r_i \nmid h}}^{s} r_i,$$

sendo que o produto percorre os elementos $i \in \{1, \ldots, s\}$ tais que $r_i \nmid h$. Para todo $i \in \{1, \ldots, s\}$, se $r_i \mid h$, então $r_i \nmid \tilde{g}g$ e, portanto, $r_i \nmid h + \tilde{g}g$ e se $r_i \nmid h$, então $r_i \nmid h + \tilde{g}g$. Isso prova $\text{mdc}(f, h + \tilde{g}g) = 1$. □

1.2.1 Ordem multiplicativa e elementos primitivos

Teorema 1.21. *Para todo corpo finito $\mathbb{F}_q$, o grupo multiplicativo $\mathbb{F}_q^*$ é cíclico.*

Definição 1.22. *Um gerador do grupo cíclico $\mathbb{F}_q^*$ é chamado de elemento primitivo de $\mathbb{F}_q$.*

Definição 1.23. *Seja $\alpha \in \overline{\mathbb{F}}_q^*$. A ordem multiplicativa de α, denotada por* $\mathrm{ord}(\alpha)$*, é o menor inteiro positivo d tal que $\alpha^d = 1$.*

Teorema 1.24. *Sejam $\alpha \in \overline{\mathbb{F}}_q^*$ e $d = ord(\alpha)$. Então $\alpha \in \mathbb{F}_{q^n}$ se, e somente se, d divide $q^n - 1$. Além disso, se d é um divisor de $q^n - 1$, então existem $\varphi(d)$ elementos $\beta \in \mathbb{F}_{q^n}$ tais que* $\mathrm{ord}(\beta) = d$.

Do teorema anterior segue que existem exatamente $\varphi(q-1)$ elementos primitivos em $\mathbb{F}_q$.

Lema 1.25. *Se α é um elemento primitivo de $\mathbb{F}_q$ e t é um inteiro positivo, então* $\mathrm{ord}(\alpha^t) = \frac{q-1}{\mathrm{mdc}(q-1,t)}$.

Definição 1.26. *Seja r um inteiro positivo tal que $r \mid (q-1)$. Um elemento $\alpha \in \mathbb{F}_q$ é chamado de r-primitivo se* $\mathrm{ord}(\alpha) = \frac{q-1}{r}$.

Do Lema 1.25 e da Definição 1.26, temos que existem $\varphi(\frac{q-1}{r})$ elementos r-primitivos em $\mathbb{F}_q^*$.

1.2.2 Elementos normais

Além da estrutura multiplicativa de $\mathbb{F}_{q^n}^*$, o corpo $\mathbb{F}_{q^n}$ possui outra estrutura algébrica importante. Podemos ver $\mathbb{F}_{q^n}$ como um espaço vetorial sobre $\mathbb{F}_q$. Em particular, dado um elemento $\alpha \in \mathbb{F}_{q^n}$, podemos considerar o espaço vetorial gerado por α e os seus conjugados.

Definição 1.27. *Um elemento $\alpha \in \mathbb{F}_{q^n}$ é normal sobre $\mathbb{F}_q$ se α e os seus conjugados geram $\mathbb{F}_{q^n}$ como $\mathbb{F}_q$-espaço vetorial. Neste caso, o conjunto $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ é uma base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.*

Observe que se $\alpha \in \mathbb{F}_{q^n}$ é normal, então os seus conjugados também são elementos normais.

Teorema 1.28 (Teorema da base normal)**.** *Para toda extensão $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, existe uma base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.*

Lema 1.29. *Sejam $f \in \mathbb{F}_q[x]$ um polinômio irredutível e α uma raiz de f em alguma extensão de $\mathbb{F}_q$. Para um polinômio $h \in \mathbb{F}_q[x]$ temos $h(\alpha) = 0$ se, e somente se, f divide h.*

Lema 1.30. *Seja $f \in \mathbb{F}_q[x]$ um polinômio irredutível de grau m. Então f divide $x^{q^n} - x$ se, e somente se, m divide n.*

Teorema 1.31. *Se f é um polinômio irredutível em $\mathbb{F}_q[x]$ de grau n, então f tem uma raiz $\alpha \in \mathbb{F}_{q^n}$. Além disso, todas as raízes de f são simples e são dadas pelos n elementos conjugados $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ de $\mathbb{F}_{q^n}$.*

Corolário 1.32. *Seja f um polinômio irredutível em $\mathbb{F}_q$ de grau n. O corpo de raízes de f sobre $\mathbb{F}_q$ é $\mathbb{F}_{q^n}$.*

Definição 1.33. *Dizemos que um corpo K é perfeito se todo polinômio irredutível em $K[x]$ é separável. Um polinômio é separável se suas raízes em um fecho algébrico de K são distintas.*

Corolário 1.34. *O corpo $\mathbb{F}_q$ é um corpo perfeito.*

Teorema 1.35. *Os conjugados de $\alpha \in \mathbb{F}_q^*$ (em relação a qualquer subcorpo de $\mathbb{F}_q$) têm todos a mesma ordem no grupo $\mathbb{F}_q^*$.*

Corolário 1.36. *Se α é primitivo em $\mathbb{F}_q$, então todos os conjugados de α, em relação a qualquer subcorpo de $\mathbb{F}_q$, são primitivos.*

Teorema 1.37. *Para $\alpha \in \mathbb{F}_{q^n}$, o conjunto $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ é uma base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ se, e somente se, os polinômios $x^n - 1$ e $\alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-2}} x + \alpha^{q^{n-1}}$ são primos entre si.*

Motivados por esse resultado, Huczynska *et al.* (ver [18]) definem elementos k-normais.

Definição 1.38. *Seja $\alpha \in \mathbb{F}_{q^n}$ e denote $g_\alpha(x)$ o polinômio $\sum_{i=0}^{n-1} \alpha^{q^i} x^{n-1-i} \in \mathbb{F}_{q^n}$. Se $\mathrm{mdc}(g_\alpha(x), x^n - 1)$ tem grau k sobre $\mathbb{F}_{q^n}$, então dizemos que α é k-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.*

Aproveitamos também para enunciar o teorema da base primitiva normal demonstrada em [26] e [10].

Teorema 1.39. *Para toda extensão $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, existe uma base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ composta por elementos primitivos.*

1.2.3 Estrutura de $\mathbb{F}_q[x]$-módulo

Em [27, Chapter 3, Section 4] é dada a noção de q-polinômio ou polinômio linearizado. Essa definição é utilizada para estudar $\mathbb{F}_{q^n}$ como $\mathbb{F}_q[x]$-módulo (ver, por exemplo, [15]).

Definição 1.40. *Um polinômio da forma*

$$L(x) = \sum_{i=0}^{m} \alpha_i x^{q^i}$$

com coeficientes em uma extensão $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$ é chamado de q-polinômio, ou polinômio linearizado, sobre $\mathbb{F}_{q^n}$.

Proposição 1.41. *Todo q-polinômio $L(x)$ sobre $\mathbb{F}_{q^n}$ induz um operador linear $\alpha \longmapsto L(\alpha)$ de $\mathbb{F}_{q^n}$ visto como espaço vetorial sobre $\mathbb{F}_q$, isto é, dados $\alpha, \beta \in \mathbb{F}_{q^n}$ e $a \in \mathbb{F}_q$ tem-se*

$$L(\alpha + \beta) = L(\alpha) + L(\beta) \quad e \quad L(a\alpha) = aL(\alpha).$$

Teorema 1.42. *Sejam $L(x)$ um q-polinômio sobre $\mathbb{F}_{q^n}$ e $\mathbb{F}_{q^s}$ uma extensão de $\mathbb{F}_{q^n}$ que contém todas as raízes de $L(x)$. Então todas as raízes de $L(x)$ têm a mesma multiplicidade, que é 1 ou uma potência de q, e essas raízes formam um subespaço $\mathbb{F}_q$-linear de $\mathbb{F}_{q^s}$.*

O produto usual de dois q-polinômios não é necessariamente um q-polinômio, mas a composição de dois q-polinômios continua sendo um q-polinômio.

Definição 1.43. *Sejam $L_1(x), L_2(x)$ dois q-polinômios sobre $\mathbb{F}_{q^n}$. Define-se a multiplicação simbólica de $L_1(x)$ e $L_2(x)$ como sendo*

$$L_1(x) \otimes L_2(x) = L_1(L_2(x)).$$

Definição 1.44. *Os polinômios*

$$f(x) = \sum_{i=0}^{m} \alpha_i x^i \quad e \quad F(x) = \sum_{i=0}^{m} \alpha_i x^{q^i}$$

sobre $\mathbb{F}_{q^n}$ são chamados de q-associados. Mais especificamente, $f(x)$ é o q-associado de $F(x)$ e $F(x)$ é o q-associado linearizado de $f(x)$.

Notação 1.45. *O polinômio q-associado linearizado de f será denotado por L_f.*

Lema 1.46. *Para todos $f, g \in \mathbb{F}_{q^n}[x]$ tem-se $L_{f+g} = L_f + L_g$ e $L_{fg} = L_f \otimes L_g$.*

Corolário 1.47. *Para todos $f, g \in \mathbb{F}_{q^n}[x]$, L_f divide simbolicamente L_g se, e somente se, f divide g.*

Teorema 1.48. *O espaço vetorial $\mathbb{F}_{q^n}$ é um $\mathbb{F}_q[x]$-módulo, com a ação dada por*

$$\begin{array}{ccc} \mathbb{F}_q[x] \times \mathbb{F}_{q^n} & \longrightarrow & \mathbb{F}_{q^n} \\ (f, \alpha) & \longmapsto & f \circ \alpha := L_f(\alpha). \end{array}$$

Demonstração. Segue da Proposição 1.41, do Lema 1.46, de $L_1(\alpha) = \alpha$ e do fato que $\mathbb{F}_{q^n}$ é um grupo abeliano. □

Dado um elemento $\alpha \in \mathbb{F}_{q^n}$, o conjunto $I_\alpha = \{f \in \mathbb{F}_q[x] \mid f \circ \alpha = 0\}$ de anuladores de α é um ideal de $\mathbb{F}_q[x]$. Como $\mathbb{F}_q[x]$ é um domínio principal, temos $I_\alpha = (f)$, para algum $f \in \mathbb{F}_q[x]$.

Definição 1.49. *O polinômio mônico de $\mathbb{F}_q[x]$ que gera I_α é chamado de $\mathbb{F}_q$-ordem de α e é denotado por* $\mathrm{Ord}(\alpha)$.

Observação 1.50. *Como $\alpha^{q^n} - \alpha = 0$, para todo $\alpha \in \mathbb{F}_{q^n}$, temos $x^n - 1 \in I_\alpha$ e, portanto,* $\mathrm{Ord}(\alpha)$ *divide $x^n - 1$.*

Pelo Teorema 1.28, existe um elemento $\alpha \in \mathbb{F}_{q^n}$ tal que todo elemento de $\mathbb{F}_{q^n}$ se escreve de forma única como $f \circ \alpha$, para algum $f \in \mathbb{F}_q[x]$ de grau menor ou igual a $n-1$. Além disso, como $(x^n - 1) \circ \alpha = \alpha^{q^n} - \alpha = 0$, temos $\mathrm{Ord}(\alpha) = x^n - 1$. Em particular, isso quer dizer que $\mathbb{F}_{q^n}$ é um $\mathbb{F}_q[x]$-módulo cíclico.

Proposição 1.51. *Seja $f \in \mathbb{F}_q[x]$ um divisor mônico de $x^n - 1$. Existem $\phi_q(f)$ elementos de $\mathbb{F}_q$-ordem f em $\mathbb{F}_{q^n}$.*

Demonstração. Pelo Teorema 1.28, existe um elemento $\alpha \in \mathbb{F}_{q^n}$ normal sobre $\mathbb{F}_q$. Por definição, isso implica que todo elemento de $\mathbb{F}_{q^n}$ se escreve de forma única como $g \circ \alpha$, para algum $g \in \mathbb{F}_q[x]$ de grau menor ou igual a $n-1$.

Sejam $\beta = g \circ \alpha$, sendo $g \in \mathbb{F}_q[x]$ de grau menor ou igual a $n-1$, e $\widetilde{g} = \mathrm{mdc}(g, x^n - 1)$. Como

$$\frac{x^n - 1}{\widetilde{g}} \circ \beta = \frac{g}{\widetilde{g}} \circ ((x^n - 1) \circ \alpha) = 0,$$

temos $\mathrm{Ord}(\beta)$ divide $\frac{x^n-1}{\widetilde{g}}$. Reciprocamente, se $h \circ \beta = 0$, então $x^n - 1$ divide gh. Dividindo por $\widetilde{g}$, como $\frac{x^n-1}{\widetilde{g}}$ e $\frac{g}{g}$ são primos entre si, temos $\frac{x^n-1}{\widetilde{g}}$ divide h. Isso implica $\mathrm{Ord}(\beta) = \frac{x^n-1}{\widetilde{g}}$. Observe que $g_1 = \frac{g}{g}$ é um polinômio de grau menor ou igual a $n - 1 - \mathrm{grau}(\widetilde{g})$. Em particular, $\mathrm{Ord}(\beta) = f$ equivale a

$$f = \frac{x^n - 1}{\widetilde{g}} \iff \mathrm{mdc}(g, x^n - 1) = \frac{x^n - 1}{f} \iff \mathrm{mdc}(\frac{fg}{x^n - 1}, f) = 1,$$

sendo $\frac{fg}{x^n-1} = \frac{x^n-1}{\widetilde{g}}\frac{g}{x^n-1} = g_1$ de grau menor do que $\mathrm{grau}(f)$.

Dessa forma, o número de elementos de $\mathbb{F}_q$-ordem f é igual ao número de polinômios em $\mathbb{F}_q[x]$ de grau menor do que $\mathrm{grau}(f)$ e primos com f. □

Na prova da Proposição 1.51 foi provado o seguinte resultado.

Corolário 1.52. *Sejam $\alpha \in \mathbb{F}_{q^n}$ um elemento normal sobre $\mathbb{F}_q$ e $g \in \mathbb{F}_q[x]$. Então* $\mathrm{Ord}(g \circ \alpha) = \frac{x^n-1}{\mathrm{mdc}(x^n-1,g)}$.

Lema 1.53. *Sejam $\beta_1, \beta_2 \in \mathbb{F}_{q^n}$ elementos de $\mathbb{F}_q$-ordem f_1 e f_2, respectivamente. Se f_1 e f_2 são primos entre si, então $\beta_1 + \beta_2$ é de $\mathbb{F}_q$-ordem $f_1 f_2$.*

Demonstração. Pelo Teorema 1.28, existe um elemento normal $\alpha \in \mathbb{F}_{q^n}$ e, da demonstração da Proposição 1.51, existem $g_1, g_2 \in \mathbb{F}_q[x]$ tais que $\mathrm{mdc}(g_i, f_i) = 1$, $\mathrm{grau}(g_i) < \mathrm{grau}(f_i)$ e $\beta_i = (\frac{x^n-1}{f_i} g_i) \circ \alpha$, para $i \in \{1, 2\}$. Daí

$$\beta_1 + \beta_2 = \left(\frac{x^n - 1}{f_1 f_2}(f_2 g_1 + f_1 g_2)\right) \circ \alpha.$$

Seja $h \in \mathbb{F}_q[x]$ um elemento irredutível. Se h divide f_1 ou f_2, então h não divide $f_2 g_1 + f_1 g_2$, já que f_1 e f_2 são primos entre si. Isso implica $\mathrm{mdc}(f_1 f_2, f_2 g_1 + f_1 g_2) = 1$, e pela prova da Proposição 1.51, $\beta_1 + \beta_2$ é de $\mathbb{F}_q$-ordem $f_1 f_2$. □

Outro resultado importante trata do número de raízes do polinômio L_f, para $f \in \mathbb{F}_q[x]$. O núcleo da aplicação linear definida por L_f será denotado por $\ker(L_g)$ e a imagem de L_f por $\mathrm{im}(L_f)$. A dimensão de um $\mathbb{F}_q$-subespaço vetorial V de $\mathbb{F}_{q^n}$ será denotada por $\dim_q V$.

Lema 1.54. *Sejam $f, g \in \mathbb{F}_q[x]$ tais que $fg = x^n - 1$. Então* $\dim_q \ker(L_f) = \mathrm{grau}(f)$, $\dim_q \mathrm{im}(L_f) = n - \mathrm{grau}(f)$, $\ker(L_f) = \mathrm{im}(L_g)$ *e* $\mathrm{im}(L_f) = \ker(L_g)$.

Demonstração. Pelo Lema 1.46, temos $L_g \circ L_f(\alpha) = L_f \circ L_g(\alpha) = L_{x^n-1}(\alpha) = 0$, para todo $\alpha \in \mathbb{F}_{q^n}$. Logo, $\mathrm{im}(L_f) \subset \ker(L_g)$ e $\mathrm{im}(L_g) \subset \ker(L_f)$. Por outro lado, como L_f tem grau $q^{\mathrm{grau}(f)}$, $\ker(L_f)$ tem dimensão menor ou igual a $\mathrm{grau}(f)$. De forma similar, $\mathrm{im}(L_f)$ tem dimensão menor ou igual a $\mathrm{grau}(g) = n - \mathrm{grau}(f)$, pois $\mathrm{im}(L_f) \subset \ker(L_g)$. O resultado segue de $n = \dim_q \mathrm{im}(L_f) + \dim_q \ker(L_f)$. □

Finalizamos a seção com dois resultados sobre elementos k-normais. O primeiro deles é [18, Theorem 3.2].

Teorema 1.55. *Seja $\alpha \in \mathbb{F}_{q^n}$. As seguintes propriedades são equivalentes:*

(i) α *é* k*-normal sobre* $\mathbb{F}_q$*;*

(ii) o conjunto $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-k-1}}\}$ *é uma base de um* $\mathbb{F}_q[x]$*-submódulo de* $\mathbb{F}_{q^n}$ *de dimensão* $n-k$ *sobre* $\mathbb{F}_q$*;*

(iii) $\text{grau}(\text{Ord}(\alpha)) = n-k$.

Em [32], Reis exibiu um método para construir elementos k-normais: *sejam* $\beta \in \mathbb{F}_{q^n}$ *um elemento normal e* $f \in \mathbb{F}_q[x]$ *um divisor de* $x^n - 1$ *de grau* k*. Então* $\alpha = L_f(\beta)$ *é* k*-normal* (ver [32, Lemma 3.1]). Na realidade, essa é a única forma de construir elementos k-normais. O seguinte resultado é uma variante de [32, Lemma 3.1] que inclui a última afirmação.

Lema 1.56. *Seja* $k \leq n$ *um inteiro não negativo. Um elemento* $\alpha \in \mathbb{F}_{q^n}$ *é* k*-normal sobre* $\mathbb{F}_q$ *se, e somente se, existem* $\beta \in \mathbb{F}_{q^n}$ *normal sobre* $\mathbb{F}_q$ *e* $f \in \mathbb{F}_q[x]$ *divisor mônico de* $x^n - 1$ *de grau* k *tais que* $\alpha = f \circ \beta$*.*

Demonstração. Suponha primeiro α k-normal. Pelo Teorema 1.55(iii), $g = \text{Ord}(\alpha)$ é de grau $n-k$. Dessa forma, $f = \frac{x^n-1}{g}$ é mônico de grau k. Pelo Teorema 1.28, existe um elemento $\gamma \in \mathbb{F}_{q^n}$ normal sobre $\mathbb{F}_q$. Por definição, isso implica que existe $h \in \mathbb{F}_q[x]$ tal que $\alpha = h \circ \gamma$. Como

$$0 = g \circ \alpha = (gh) \circ \gamma$$

e γ é de $\mathbb{F}_q$-ordem $x^n - 1$, temos $x^n - 1 \mid gh$. Dividindo essa divisibilidade por g, obtemos $f \mid h$. Seja então $\tilde{h} \in \mathbb{F}_q[x]$ tal que $h = \tilde{h}f$. Se $t = \text{mdc}(\tilde{h}, g)$, então

$$\frac{g}{t} \circ \alpha = gf \circ \left(\frac{\tilde{h}}{t} \circ \gamma\right) = 0,$$

já que $gf = x^n - 1$. Como $\text{Ord}(\alpha) = g$, segue $t = 1$. Pelo Lema 1.20, existe $\tilde{g} \in \mathbb{F}_q[x]$ tal que $\text{mdc}(x^n - 1, \tilde{h} + \tilde{g}g) = 1$. Pelo Corolário 1.52, $\beta = (\tilde{h} + \tilde{g}g) \circ \gamma$ é um elemento normal. Dessa forma,

$$f \circ \beta = (f\tilde{h} + f\tilde{g}g) \circ \gamma = h \circ \gamma = \alpha.$$

Finalmente, se $f \in \mathbb{F}_q[x]$ é um divisor mônico de $x^n - 1$ e $\beta \in \mathbb{F}_{q^n}$ é um elemento normal sobre $\mathbb{F}_q$, pelo Corolário 1.52, $\alpha = f \circ \beta$ é de $\mathbb{F}_q$-ordem $\frac{x^n-1}{f}$, isto é, α é k-normal. □

1.3 Caracteres

Definição 1.57. *Seja* G *um grupo abeliano finito. Um caracter* χ *de* G *é um homomorfismo de grupos de* G *em* $\mathbb{C}^*$*.*

O caracter χ_0 definido por $\chi_0(g) = 1$, para todo $g \in G$, é chamado de caracter trivial. Todos os outros caracteres são chamados caracteres não triviais. Para todo caracter χ de G e todo elemento $g \in G$, temos $\chi(g)^n = \chi(g^n) = \chi(1_G) = 1$, sendo 1_G a unidade de G e $n = |G|$. Assim, a imagem de χ está contida no conjunto de raízes n-ésimas da unidade. Para um caracter χ, a função $\overline{\chi} : G \longrightarrow \mathbb{C}^*$ definida por $g \longmapsto \overline{\chi(g)}$ é também um caracter de G, no qual

$\overline{\chi(g)}$ denota o conjugado complexo de $\chi(g)$. O conjunto dos caracteres de G, denotado $\widehat{G}$, é um grupo abeliano com a operação de multiplicação de caracteres definida por $(\chi_1\chi_2)(g) := \chi_1(g)\chi_2(g)$.

Teorema 1.58. *Se χ é um caracter não trivial do grupo abeliano finito G, então*

$$\sum_{g\in G}\chi(g) = 0.$$

Se $g \in G$ com $g \neq 1_G$, então

$$\sum_{\chi\in\widehat{G}}\chi(g) = 0.$$

Teorema 1.59. *O número de caracteres de um grupo abeliano finito G é igual a $|G|$.*

Um corpo finito $\mathbb{F}_q$ tem duas estruturas de grupo abeliano. Por um lado temos o grupo aditivo $\mathbb{F}_q$ e por outro lado o grupo multiplicativo $\mathbb{F}_q^*$. Cada um desses grupos tem seu respectivo grupo de caracteres.

Definição 1.60. *Um caracter $\eta : \mathbb{F}_q^* \longrightarrow \mathbb{C}^*$ do grupo multiplicativo $\mathbb{F}_q^*$ no grupo multiplicativo $\mathbb{C}^*$ é chamado de caracter multiplicativo de $\mathbb{F}_q$. O grupo de caracteres multiplicativos de $\mathbb{F}_q$ é denotado $\widehat{\mathbb{F}}_q^*$.*

Teorema 1.61. *Seja $\alpha \in \mathbb{F}_q$ um elemento primitivo. Para cada $j \in \{0, 1, \ldots, q-2\}$, a função $\eta_j : \mathbb{F}_q^* \longrightarrow \mathbb{C}^*$ definida por*

$$\eta_j(\alpha^k) = e^{2\pi ijk/(q-1)} \quad \text{para todo } k \in \{0, 1, \ldots, q-2\},$$

é uma caracter multiplicativo de $\mathbb{F}_q$. Todo caracter multiplicativo de $\mathbb{F}_q$ é obtido dessa forma.

Do Teorema 1.61, $\widehat{\mathbb{F}}_q^*$ tem uma estrutura de grupo cíclico com a operação de multiplicação de caracteres, assim como $\mathbb{F}_q^*$ tem uma estrutura de grupo cíclico. Dessa forma, podemos também definir a ordem multiplicativa de um caracter multiplicativo.

Definição 1.62. *Seja $\eta \in \widehat{\mathbb{F}}_q^*$. A ordem de η, denotada por* $\mathrm{ord}(\eta)$*, é o menor inteiro positivo d tal que $\eta^d = \eta_0$, sendo η_0 o caracter multiplicativo trivial.*

Veja que do Teorema 1.61 conclui-se que se r é um divisor primo de $q-1$, então existem exatamente $r-1$ caracteres multiplicativos de ordem r.

Teorema 1.63. *Se d é um divisor de $q-1$, então existem $\varphi(d)$ elementos $\eta \in \widehat{\mathbb{F}}_q$ tais que* $\mathrm{ord}(\eta) = d$.

Definição 1.64. *Um caracter $\psi : \mathbb{F}_q \longrightarrow \mathbb{C}^*$ do grupo aditivo $\mathbb{F}_q$ no grupo multiplicativo $\mathbb{C}^*$ é chamado de caracter aditivo de $\mathbb{F}_q$. O grupo de caracteres aditivos de $\mathbb{F}_q$ é denotado $\widehat{\mathbb{F}}_q$.*

A estrutura de grupo abeliano de $\widehat{\mathbb{F}}_q$ é dada por $(\psi_1 + \psi_2)(\alpha) := \psi_1(\alpha)\psi_2(\alpha)$, para todos $\psi_1, \psi_2 \in \widehat{\mathbb{F}}_q$ e $\alpha \in \mathbb{F}_q$.

Se p é a característica de $\mathbb{F}_q$, a função $\chi_0 : \mathbb{F}_q \longrightarrow \mathbb{C}^*$ definida por

$$\chi_0(\alpha) = \mathrm{e}^{2\pi i \mathrm{Tr}_q(\alpha)/p}, \quad \text{para todo } \alpha \in \mathbb{F}_q,$$

é um caracter aditivo, chamado de caracter aditivo canônico.

Teorema 1.65. *Para $\beta \in \mathbb{F}_q$, a função ψ_β definida por $\psi_\beta(\alpha) := \chi_0(\beta\alpha)$, para todo $\alpha \in \mathbb{F}_q$, é um caracter aditivo de $\mathbb{F}_q$. Todo caracter aditivo de $\mathbb{F}_q$ é obtido dessa forma.*

Dada a importância de [15, Theorem 13.4.1], reproduzimos aqui o seu enunciado.

Teorema 1.66. *Seja M um grupo abeliano finito (com notação aditiva) que também é um A-módulo, para algum domínio principal A. O grupo de caracteres $\widehat{M}$ de M tem uma estrutura de A-módulo dada por*

$$(a\psi)(m) := \psi(am), \quad \text{para todos } \psi \in \widehat{M}, m \in M \text{ e } a \in A.$$

Além disso, M e $\widehat{M}$ são isomorfos como A-módulos sempre que M seja um A-módulo cíclico com ideal anulador $(b) \neq \{0\}$ para algum $b \in A$.

De acordo com o teorema acima, assim como $\mathbb{F}_{q^n}$ tem uma estrutura de $\mathbb{F}_q[x]$-módulo, o grupo de caracteres aditivos $\widehat{\mathbb{F}}_{q^n}$ também tem uma estrutura de $\mathbb{F}_q[x]$-módulo. Dado $\psi \in \widehat{\mathbb{F}}_{q^n}$ e $f \in \mathbb{F}_q[x]$, define-se $f \circ \psi$ por

$$\alpha \longmapsto f \circ \psi(\alpha) := \psi(f \circ \alpha), \quad \text{para todo } \alpha \in \mathbb{F}_{q^n}.$$

Assim como foi definida a ordem de um caracter multiplicativo, no caso aditivo definimos a $\mathbb{F}_q$-ordem de um caracter aditivo.

Definição 1.67. *Seja $\psi \in \widehat{\mathbb{F}}_{q_n}$ um caracter aditivo. Definimos a $\mathbb{F}_q$-ordem de ψ, que denotamos por* $\mathrm{Ord}(\psi)$*, como sendo o polinômio mônico de menor grau que satisfaz $f \circ \psi(\alpha) = 1$, para todo $\alpha \in \mathbb{F}_{q^n}$.*

Observe que como $\widehat{\mathbb{F}}_{q^n}$ é um $\mathbb{F}_q[x]$-módulo, a $\mathbb{F}_q$-ordem de um caracter aditivo existe e como $(x^n - 1) \circ \psi(\alpha) = \psi(\alpha^{q^n} - \alpha) = \psi(0) = 1$, para todo $\alpha \in \mathbb{F}_{q^n}$, temos que a $\mathbb{F}_q$-ordem de ψ é um divisor de $x^n - 1$.

O caracter aditivo trivial será denotado por ψ_0. Dessa forma, a $\mathbb{F}_q$-ordem de um caracter aditivo ψ é o polinômio mônico $g \in \mathbb{F}_q[x]$ de menor grau que satisfaz $g \circ \psi = \psi_0$.

Do Teorema 1.66, temos $\mathbb{F}_{q^n}$ e $\widehat{\mathbb{F}}_{q^n}$ isomorfos como $\mathbb{F}_q[x]$-módulos. Logo, $\widehat{\mathbb{F}}_{q^n}$ herda todas as propriedades de $\mathbb{F}_{q^n}$ como $\mathbb{F}_q[x]$-módulo. Dessa forma, os caracteres aditivos satisfazem as propriedades a seguir.

Lema 1.68. *Seja $f \in \mathbb{F}_q[x]$ um divisor mônico de $x^n - 1$. Existem $\phi_q(f)$ caracteres aditivos de $\mathbb{F}_q$-ordem f em $\widehat{\mathbb{F}}_{q^n}$.*

Lema 1.69. *Sejam $\psi_1, \psi_2 \in \widehat{\mathbb{F}}_{q^n}$ elementos de $\mathbb{F}_q$-ordem f_1 e f_2 respectivamente. Se f_1 e f_2 são primos entre si, então $\psi_1 + \psi_2$ é de $\mathbb{F}_q$-ordem $f_1 f_2$.*

1.4 Elementos s-livres

Definição 1.70. *Seja s um divisor positivo de $q - 1$. Um elemento $\alpha \in \mathbb{F}_q^*$ é chamado s-livre se para todo inteiro positivo $d \neq 1$ de s não existe $\beta \in \mathbb{F}_q^*$ satisfazendo $\beta^d = \alpha$.*

Lema 1.71. *Dado s um divisor positivo de $q-1$, um elemento $\alpha \in \mathbb{F}_q^*$ é s-livre se, e somente se, para todo divisor primo r de s o elemento α é r-livre.*

Demonstração. Se α não é s-livre, então existem $\beta \in \mathbb{F}_q^*$ e um divisor positivo $d \neq 1$ de s tais que $\alpha = \beta^d$. Como $d \neq 1$, d possui um divisor primo r e podemos escrever $\alpha = (\beta^{d/r})^r$, logo α não é r-livre. Reciprocamente, se existe um divisor primo r de s tal que α não é r-livre, então existe $\beta \in \mathbb{F}_q^*$ tal que $\alpha = \beta^r$, o que implica que α não é s-livre. □

O critério de Vinogradov é um critério que utiliza soma de caracteres para determinar se um elemento dado é primitivo. De acordo com o parágrafo que se encontra antes de [15, Proposition 10.2.4], o critério de Vinogradov pode ser encontrado em [24, pp. 178–180]. Uma variante desse critério é a fórmula de Vinogradov que pode ser encontrada em [27, Exercise 5.14] e uma demonstração da mesma em [15, Proposition 10.2.5]. Em [15, Theorem 13.4.4] encontramos uma fórmula mais geral para A-módulos cíclicos quando A é um domínio principal. Quando vemos $\mathbb{F}_q^*$ como $\mathbb{Z}$-módulo, obtemos a equação [15, (13.9)].

Proposição 1.72. *Sejam s um divisor de $q-1$ e ρ_s a função característica dos elementos s-livres de $\mathbb{F}_q^*$. Então, para todo $\alpha \in \mathbb{F}_q^*$,*

$$\rho_s(\alpha) = \theta(s) \sum_{d|s} \frac{\mu(d)}{\varphi(d)} \sum_{\mathrm{ord}(\eta)=d} \eta(\alpha), \tag{1.1}$$

sendo $\theta(s) := \frac{\varphi(s)}{s}$ e a soma $\sum_{\mathrm{ord}(\eta)=d}$ percorre o conjunto dos caracteres multiplicativos η de $\mathbb{F}_q^*$ de ordem d.

Demonstração. Como $\mu(d) = 0$, se d não é livre de quadrados, podemos restringir a soma nos divisores de s, na soma dos divisores livres de quadrado de s. Usando que a função de Möbius e a função de Euler são multiplicativas, podemos escrever

$$\sum_{d|s} \left(\frac{\mu(d)}{\varphi(d)} \sum_{\mathrm{ord}(\eta)=d} \eta(\alpha) \right) = \prod_{\substack{r|s \\ r \text{ é primo}}} \left(1 + \frac{\mu(r)}{\varphi(r)} \sum_{\mathrm{ord}(\eta)=r} \eta(\alpha) \right),$$

já que se $d = r_1 r_2 \cdots r_k$, então $\mu(d) = \mu(r_1)\mu(r_2)\cdots\mu(r_k)$, $\varphi(d) = \varphi(r_1)\varphi(r_2)\cdots\varphi(r_k)$ e

$$\sum_{\mathrm{ord}(\eta)=d} \eta(\alpha) = \left(\sum_{\mathrm{ord}(\eta_1)=r_1} \eta_1(\alpha) \right) \left(\sum_{\mathrm{ord}(\eta_2)=r_2} \eta_2(\alpha) \right) \cdots \left(\sum_{\mathrm{ord}(\eta_k)=r_k} \eta_k(\alpha) \right).$$

Como, para um primo r, temos $\mu(r) = -1$ e $\varphi(r) = r-1$, segue

$$\sum_{d|s} \left(\frac{\mu(d)}{\varphi(d)} \sum_{\mathrm{ord}(\eta)=d} \eta(\alpha) \right) = \prod_{\substack{r|s \\ r \text{ é primo}}} \left(1 - \frac{1}{r-1} \sum_{\mathrm{ord}(\eta)=r} \eta(\alpha) \right).$$

Se α não for s-livre, pelo Lema 1.71, existe um divisor primo r de s tal que α não é r-livre. Nesse caso, existe um elemento $\beta \in \mathbb{F}_q^*$ tal que $\alpha = \beta^r$. Assim, se η for de ordem r, então $\eta(\alpha) = \eta^r(\beta) = 1$. Como existem $r-1$ caracteres de ordem r, temos

$$1 - \frac{1}{r-1} \sum_{\mathrm{ord}(\eta)=r} \eta(\alpha) = 0.$$

Isso prova que se α não é s-livre, então

$$\theta(s)\sum_{d|s}\frac{\mu(d)}{\varphi(d)}\sum_{\mathrm{ord}(\eta)=d}\eta(\alpha)=0.$$

Suponha agora α s-livre. Nesse caso, se $\beta\in\mathbb{F}_q^*$ é primitivo, então $\alpha=\beta^k$ para algum inteiro positivo k, e, pelo Lema 1.71, k deve ser primo com s. Pelo Teorema 1.61, para todo caracter multiplicativo η existe $j\in\{0,1,\ldots,q-2\}$ tal que

$$\eta(\beta)=e^{2\pi ij/(q-1)}.$$

Se η é de ordem r para algum primo r que divide s, então $j\neq 0$ e $\eta^r(\beta)=1$. Em particular, isso significa que $q-1$ é um divisor de rj e, portanto, $j\in\{t\cdot\frac{q-1}{r}\mid 1\leq t\leq r-1\}$. Seja $j_1=\frac{q-1}{r}$ e defina $\xi=e^{2\pi ij_1k/(q-1)}=e^{2\pi ik/r}$. Assim $\xi^r=1$ e, como k é primo com s, temos $\xi\neq 1$, pois r não divide k. Isso implica

$$\sum_{\mathrm{ord}(\eta)=r}\eta(\alpha)=\sum_{t=1}^{r-1}\xi^t=-1+\sum_{t=0}^{r-1}\xi^t=-1+\frac{1-\xi^r}{1-\xi}=-1.$$

Daí

$$\prod_{\substack{r|s\\ r\text{ é primo}}}\left(1-\frac{1}{r-1}\sum_{\mathrm{ord}(\eta)=r}\eta(\alpha)\right)=\prod_{\substack{r|s\\ r\text{ é primo}}}\frac{r}{r-1}=\frac{s}{\varphi(s)}$$

e, portanto,

$$\theta(s)\sum_{d|s}\frac{\mu(d)}{\varphi(d)}\sum_{\mathrm{ord}(\eta)=d}\eta(\alpha)=1.$$

□

Observação 1.73. *Por definição, um elemento $\alpha\in\mathbb{F}_q^*$ que não é primitivo não pode ser $(q-1)$-livre e vice-versa. Logo, um elemento $\alpha\in\mathbb{F}_q^*$ é primitivo se, e somente se, α é $(q-1)$-livre.*

1.5 Elementos g-livres

Definição 1.74. *Seja g um divisor mônico de x^n-1 em $\mathbb{F}_q[x]$. Um elemento $\alpha\in\mathbb{F}_{q^n}$ é chamado g-livre se, para todo divisor mônico $h\neq 1$ de g em $\mathbb{F}_q[x]$, não existe $\beta\in\mathbb{F}_{q^n}$ satisfazendo $h\circ\beta=\alpha$.*

Lema 1.75. *Dado g um divisor mônico de x^n-1 em $\mathbb{F}_q[x]$, um elemento $\alpha\in\mathbb{F}_{q^n}$ é g-livre se, e somente se, para todo fator mônico irredutível r de g o elemento α é r-livre.*

Demonstração. Se α não é g-livre, então existem $\beta\in\mathbb{F}_{q^n}$ e um divisor mônico $h\neq 1$ de g em $\mathbb{F}_q[x]$ tais que $\alpha=h\circ\beta$. Como $h\neq 1$, h possui um divisor mônico irredutível r e podemos escrever $\alpha=r\circ((h/r)\circ\beta)$. Logo, α não é r-livre. Reciprocamente, se existe um divisor mônico irredutível r de g em $\mathbb{F}_q[x]$ tal que α não é r-livre, então existe $\beta\in\mathbb{F}_{q^n}$ tal que $\alpha=r\circ\beta$, o que implica que α não é g-livre. □

Como já foi visto antes, [15, Theorem 13.4.4] é uma generalização da fórmula de Vinogradov. Esse resultado aplicado no $\mathbb{F}_q[x]$-módulo $\mathbb{F}_{q^n}$ se encontra na equação [15, (13.10)]. Mostremos antes o seguinte resultado.

Lema 1.76. *Seja $r \in \mathbb{F}_q[x]$ um polinômio mônico irredutível que divide $x^n - 1$. Então, para todo $\alpha \in \mathbb{F}_{q^n}$,*

$$\sum_{\mathrm{Ord}(\psi)=r} \psi(\alpha) = \begin{cases} -1 & \text{se } \alpha \text{ é } r\text{-livre}, \\ q^{\mathrm{grau}(r)} - 1 & \text{caso contrário}, \end{cases}$$

sendo que a soma $\sum_{\mathrm{Ord}(\psi)=r}$ percorre o conjunto dos caracteres aditivos ψ de $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$-ordem r.

Demonstração. Se α não for r-livre, existe um elemento $\beta \in \mathbb{F}_{q^n}$ tal que $\alpha = r \circ \beta$. Assim, se ψ for um caracter aditivo de $\mathbb{F}_q$-ordem r, então $\psi(\alpha) = (r \circ \psi)(\beta) = 1$. Portanto,

$$\sum_{\mathrm{Ord}(\psi)=r} \psi(\alpha) = q^{\mathrm{grau}(r)} - 1,$$

já que existem $\phi_q(r) = q^{\mathrm{grau}(r)} - 1$ caracteres de $\mathbb{F}_q$-ordem r.

Suponha agora α r-livre. Observe que o conjunto de caracteres aditivos de $\mathbb{F}_q$-ordem r juntamente com o caracter trivial formam um grupo, já que esse conjunto pode ser descrito como $V_r = \{\psi \in \widehat{\mathbb{F}}_{q^n} \mid \mathrm{Ord}(\psi)|r\}$. Dados $\psi_1, \psi_2 \in V_r$ tem-se $r \circ (\psi_1 - \psi_2)(\gamma) = (r \circ \psi_1)(\gamma)((r \circ \psi_2)(\gamma))^{-1} = 1$, para todo $\gamma \in \mathbb{F}_{q^n}$. Logo, V_r é um subgrupo de $\widehat{\mathbb{F}}_{q^n}$. Como α é r-livre, temos que existem um elemento normal $\beta \in \mathbb{F}_{q^n}$ e $g \in \mathbb{F}_q[x]$ primo com r tais que $\alpha = g \circ \beta$. Seja $\psi_1 \in \widehat{\mathbb{F}}_{q^n}$ de $\mathbb{F}_q$-ordem r. Nesse caso, temos $\psi_1(r \circ \beta) = 1$. Suponha $\psi_1(\alpha) = 1$, isto é, $\psi_1(g \circ \beta) = 1$. Como g e r são primos entre si, existem $f_1, f_2 \in \mathbb{F}_q[x]$ tais que $f_1 g + f_2 r = 1$. Logo $\psi_1(\beta) = 1$. Como β é um elemento normal, temos que ψ_1 seria o caracter trivial, mas ψ_1 é de $\mathbb{F}_q$-ordem r. Assim, $\psi_1(\alpha) \neq 1$ e

$$\psi_1(\alpha) \sum_{\psi \in V_r} \psi(\alpha) = \sum_{\psi \in V_r} (\psi_1 + \psi)(\alpha) = \sum_{\psi \in V_r} \psi(\alpha),$$

já que $\psi_1 + V_r = V_r$. Isso implica

$$0 = \sum_{\psi \in V_r} \psi(\alpha) = 1 + \sum_{\mathrm{Ord}(\psi)=r} \psi(\alpha).$$

Isso prova a igualdade

$$\sum_{\mathrm{Ord}(\psi)=r} \psi(\alpha) = -1.$$

□

Proposição 1.77. *Sejam g um divisor mônico de $x^n - 1$ em $\mathbb{F}_q[x]$ e κ_g a função característica dos elementos g-livres de $\mathbb{F}_{q^n}$. Então, para todo $\alpha \in \mathbb{F}_{q^n}$,*

$$\kappa_g(\alpha) = \Theta_q(g) \sum_{h|g} \frac{\mu_q(h)}{\phi_q(h)} \sum_{\mathrm{Ord}(\psi)=h} \psi(\alpha), \tag{1.2}$$

sendo $\Theta_q(g) := \frac{\phi_q(g)}{q^{\mathrm{grau}(g)}}$, a soma $\sum_{h|g}$ percorre os fatores mônicos h de g e a soma $\sum_{\mathrm{Ord}(\psi)=h}$ percorre o conjunto dos

caracteres aditivos ψ de $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$-ordem h.

Demonstração. Como $\mu_q(h) = 0$, se h não é livre de quadrados, podemos restringir a soma nos divisores mônicos de g na soma dos divisores mônicos livres de quadrado de g. Dessa forma,

$$\sum_{h|g} \frac{\mu_q(h)}{\phi_q(h)} \sum_{\mathrm{Ord}(\psi)=h} \psi(\alpha) = \prod_{\substack{r|g \\ r \text{ é mônico} \\ \text{e irredutível}}} \left(1 + \frac{\mu_q(r)}{\phi_q(r)} \sum_{\mathrm{Ord}(\psi)=r} \psi(\alpha)\right),$$

já que se $h = r_1 r_2 \cdots r_k$, então $\mu_q(h) = \mu_q(r_1)\mu_q(r_2)\cdots\mu_q(r_k)$, $\phi_q(h) = \phi_q(r_1)\phi_q(r_2)\cdots\phi_q(r_k)$ e, pelo Lema 1.69,

$$\sum_{\mathrm{Ord}(\psi)=h} \psi(\alpha) = \left(\sum_{\mathrm{Ord}(\psi_1)=r_1} \psi_1(\alpha)\right)\left(\sum_{\mathrm{Ord}(\Psi_2)=r_2} \psi_2(\alpha)\right)\cdots\left(\sum_{\mathrm{Ord}(\psi_k)=r_k} \psi_k(\alpha)\right).$$

Como para um polinômio mônico irredutível r temos $\mu_q(r) = -1$ e $\phi_q(r) = q^{\mathrm{grau}(r)} - 1$, segue

$$\sum_{h|g}\left(\frac{\mu_q(h)}{\phi_q(h)} \sum_{\mathrm{Ord}(\psi)=h} \psi(\alpha)\right) = \prod_{\substack{r|g \\ r \text{ é mônico} \\ \text{e irredutível}}} \left(1 - \frac{1}{q^{\mathrm{grau}(r)} - 1} \sum_{\mathrm{Ord}(\psi)=r} \psi(\alpha)\right).$$

Se α não for g-livre, pelo Lema 1.75, existe um divisor mônico irredutível r de g tal que α não é r-livre. Neste caso, pelo Lema 1.76,

$$1 - \frac{1}{q^{\mathrm{grau}(r)} - 1} \sum_{\mathrm{Ord}(\psi)=r} \psi(\alpha) = 0.$$

Isso prova que se α não é g-livre, então

$$\Theta_q(g) \sum_{h|g} \frac{\mu_q(h)}{\phi_q(h)} \sum_{\mathrm{Ord}(\psi)=h} \psi(\alpha) = 0.$$

Suponha agora α g-livre. Nesse caso α é r-livre, para todo divisor mônico irredutível de g, e, pelos Lemas 1.16 e 1.76, temos

$$\prod_{\substack{r|g \\ r \text{ é mônico} \\ \text{e irredutível}}} \left(1 - \frac{1}{q^{\mathrm{grau}(r)} - 1} \sum_{\mathrm{Ord}(\psi)=r} \psi(\alpha)\right) = \prod_{\substack{r|g \\ r \text{ é mônico} \\ \text{e irredutível}}} \left(\frac{q^{\mathrm{grau}(r)}}{q^{\mathrm{grau}(r)} - 1}\right) = \frac{q^{\mathrm{grau}(g)}}{\phi_q(g)}.$$

Conclui-se

$$\Theta_q(g) \sum_{h|g} \frac{\mu_q(h)}{\phi_q(h)} \sum_{\mathrm{Ord}(\psi)=h} \psi(\alpha) = 1.$$

□

Observação 1.78. *Por definição, um elemento $\alpha \in \mathbb{F}_{q^n}$ que não é normal não pode ser $(x^n - 1)$-livre e vice-versa. Logo, um elemento $\alpha \in \mathbb{F}_{q^n}$ é normal se, e somente se, α é $(x^n - 1)$-livre.*

1.6 Desigualdades úteis

Nessa seção apresentamos algumas cotas superiores que serão utilizadas ao longo da tese.

O próximo resultado é uma combinação de [14, Theorem 5.5] e um caso especial de [14, Theorem 5.6].

Lema 1.79. *Sejam $v(x), u(x) \in \mathbb{F}_{q^n}(x)$ funções racionais. Escreva $v(x) = \prod_{j=1}^{k} s_j(x)^{n_j}$, com $s_j(x) \in \mathbb{F}_{q^n}[x]$ polinômios irredutíveis, dois a dois não associados, e n_j são inteiros não nulos. Sejam $D_1 = \sum_{j=1}^{k} \text{grau}(s_j)$, $D_2 = \max(\text{grau}(u), 0)$, D_3 o grau do denominador de $u(x)$ e D_4 a soma dos graus dos polinômios irredutíveis que dividem o denominador de u, mas não associados a $s_j(x)$ ($j = 1, \ldots, k$). Sejam η e ψ, respectivamente, um caracter multiplicativo e um caracter aditivo não trivial de $\mathbb{F}_{q^n}$.*
a) Se $v(x)$ não é da forma $r(x)^{\text{ord}(\eta)}$ em $\overline{\mathbb{F}}_q(x)$, então

$$\left| \sum_{\substack{\alpha \in \mathbb{F}_{q^n} \\ v(\alpha) \neq 0, v(\alpha) \neq \infty}} \eta(v(\alpha)) \right| \leq (D_1 - 1) q^{\frac{n}{2}}.$$

b) Se $u(x)$ não é da forma $r(x)^{q^n} - r(x)$ em $\overline{\mathbb{F}}_q(x)$, então

$$\left| \sum_{\substack{\alpha \in \mathbb{F}_{q^n} \\ v(\alpha) \neq 0, v(\alpha) \neq \infty, \\ u(\alpha) \neq \infty}} \eta(v(\alpha)) \psi(u(\alpha)) \right| \leq (D_1 + D_2 + D_3 + D_4 - 1)\, q^{\frac{n}{2}}.$$

Observe que se η for o caracter multiplicativo trivial, então $v(x) = v(x)^{\text{ord}(\eta)}$. Logo, para aplicar o Lema 1.79(a) é necessário que η não seja o caracter multiplicativo trivial.

No Capítulo 5 precisaremos de [23, Theorem 1].

Lema 1.80. *Sejam $n \geq 2$, η um caracter multiplicativo não trivial de $\mathbb{F}_{q^n}^*$ e α um elemento de $\mathbb{F}_{q^n}$ tal que $\mathbb{F}_{q^n} = \mathbb{F}_q[\alpha]$. Então*

$$\left| \sum_{t \in \mathbb{F}_q} \eta(t - \alpha) \right| \leq (n - 1)\sqrt{q}.$$

No lema anterior, como $n \geq 2$, temos $t - \alpha \neq 0$, para todo $t \in \mathbb{F}_q$. Isso significa que não precisamos definir a imagem de 0 do caracter multiplicativo η.

O seguinte lema é uma variante de [10, Lemma 3.3] e [22, Lemma 4.1].

Lema 1.81. *Sejam u um inteiro positivo e t um número real positivo. Então $W(u) \leq A_t \cdot u^{\frac{1}{t}}$, sendo*

$$A_t = \prod_{\substack{p < 2^t \\ p \text{ é primo} \\ p^{\alpha_p} | u}} \frac{2}{\sqrt[t]{p^{\alpha_p}}},$$

o produto percorre os primos p que satisfazem $p < 2^t$ que dividem u e, para todo primo p, o expoente α_p é definido

como sendo o maior inteiro positivo tal que $p^{\alpha_p} \mid u$.

Demonstração. Seja $u = p_1^{r_1} \cdots p_k^{r_k}$ a fatoração de u como produto de fatores primos. Observe que se $2^t \leq p_i$, para algum $i \in \{1, \ldots, k\}$, então $\frac{2}{\sqrt[t]{p_i^{r_i}}} \leq 1$. Assim,

$$\frac{W(u)}{\sqrt[t]{u}} = \prod_{i=1}^{k} \frac{2}{\sqrt[t]{p_i^{r_i}}} \leq \prod_{\substack{p<2^t \\ p \text{ é primo} \\ p^{\alpha_p} \mid u}} \frac{2}{\sqrt[t]{p^{\alpha_p}}} = A_t.$$

□

Veja que a constante A_t depende também de u, mas em geral, se u é um inteiro positivo qualquer, não há nenhuma informação sobre os possíveis fatores primos de u. Nesse caso, a constante A_t usada será

$$A_t = \prod_{\substack{p<2^t \\ p \text{ é primo}}} \frac{2}{\sqrt[t]{p}}.$$

Em alguns capítulos há informações adicionais sobre a fatoração de u. Nesses casos será indicada a constante A_t utilizada.

Em outros capítulos utilizaremos o seguinte resultado inspirado de [26, Lemma 2.6].

Proposição 1.82. *Sejam r um inteiro positivo, $p_1, \ldots, p_r$ a lista dos primeiros r números primos e $\mathcal{P}_r = p_1 \cdots p_r$ o produto desses primos. Para todo inteiro positivo $u \geq \mathcal{P}_r$, temos $W(u) \leq u^t$, com t um número real positivo que satisfaz $t \geq \frac{r \log 2}{\log P_r}$.*

Demonstração. Seja $u \geq \mathcal{P}_r$ um inteiro positivo. Se $\omega(u) \leq r$, então

$$W(u) = 2^{\omega(u)} \leq 2^r \leq \mathcal{P}_r^t \leq u^t.$$

Se $\omega(u) > r$, escreva $u = u_1 u_2$, de forma que os fatores primos de u_1 sejam os menores r números primos que dividem u e u_2 seja um inteiro positivo tal que $\text{mdc}(u_1, u_2) = 1$. Então $W(u_1) \leq u_1^t$, já que $u_1 \geq \mathcal{P}_r$ e $\omega(u_1) = r$. Observe que, para todo fator primo $\tilde{p}$ de u_2, $2 < \tilde{p}^t$, já que $2^r \leq \mathcal{P}_r^t < \tilde{p}^{rt}$. Como u_2 possui $\omega(u) - r$ fatores primos, temos $W(u_2) = 2^{\omega(u)-r} \leq u_2^t$. Assim, $W(u) = W(u_1)W(u_2) \leq u_1^t u_2^t = u^t$. □

Assim como encontramos uma cota superior para $W(u)$, precisamos encontrar uma para $W_q(x^n - 1)$. Reproduzimos aqui a demonstração que pode ser encontrada em [2, Lemma 3.7] e [25, Lemma 4.3].

Lema 1.83. *Sejam q a potência de um primo e n um inteiro positivo. O número de fatores mônicos irredutíveis de*

$x^n - 1$ sobre $\mathbb{F}_q$ é no máximo $\frac{n}{a} + b$, no qual o par (a, b) pode ser escolhido dentre os seguintes pares:

$$(1,0), \quad \left(2, \frac{q-1}{2}\right), \quad \left(3, \frac{q^2+3q-4}{6}\right),$$
$$\left(4, \frac{q^3+3q^2+5q-9}{12}\right), \quad \left(5, \frac{3q^4+8q^3+15q^2+22q-48}{60}\right).$$

Demonstração. Sejam $s_{n,t}$ o número de polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$ de grau máximo t que dividem $x^n - 1$ e $T_{n,t}$ a soma dos graus desses polinômios. Observe que o número de fatores irredutíveis de $x^n - 1$ em $\mathbb{F}_q[x]$ de grau maior ou igual a $t + 1$ é, no máximo, $\frac{n-T_{n,t}}{t+1}$. Desta forma, se $W_q(x^n - 1) = 2^j$, então

$$j \leq \frac{n - T_{n,t}}{t+1} + s_{n,t} = \frac{n + (t+1)s_{n,t} - T_{n,t}}{t+1}.$$

Como cada termo na soma $T_{n,t}$ é no máximo t, temos $(t + 1)s_{n,t} - T_{n,t}$ máximo quando $s_{n,t}$ é máximo. Dessa forma, o lado direito da expressão acima é máximo quando $s_{n,t}$ é máximo. Como o número de polinômios mônicos irredutíveis de grau i que dividem $x^n - 1$ é, no máximo, igual ao número de elementos de $\mathbb{F}_{q^i}$ que não se encontram em $\mathbb{F}_{q^j}$, para todo divisor próprio j de i, dividido por i, temos que, para $t = 0$, podemos escolher $a = 1$ e $b = 0$. Para $t = 1$, o valor máximo de $s_{n,t}$ é $q - 1$ e, neste caso, $T_{n,t} = q - 1$ (ou seja $a = 2$ e $b = \frac{q-1}{2}$). Para $t = 2$, o valor máximo de $s_{n,t}$ é $q - 1 + \frac{q^2-q}{2} = \frac{q^2+q-2}{2}$ e, neste caso, $T_{n,t} = q - 1 + q^2 - q = q^2 - 1$ (ou seja $a = 3$ e $b = \frac{q^2+3q-4}{6}$). Para $t = 3$, o valor máximo de $s_{n,t}$ é $q - 1 + \frac{q^2-q}{2} + \frac{q^3-q}{3} = \frac{2q^3+3q^2+q-6}{6}$ e, neste caso, $T_{n,t} = q - 1 + q^2 - q + q^3 - q = q^3 + q^2 - q - 1$ (ou seja $a = 4$ e $b = \frac{q^3+3q^2+5q-9}{12}$). Finalmente, para $t = 4$, o valor máximo de $s_{n,t}$ é $q - 1 + \frac{q^2-q}{2} + \frac{q^3-q}{3} + \frac{q^4-q^2}{4} = \frac{3q^4+4q^3+3q^2+2q-12}{12}$ e, neste caso, $T_{n,t} = q - 1 + q^2 - q + q^3 - q + q^4 - q^2 = q^4 + q^3 - q - 1$ (ou seja $a = 5$ e $b = \frac{3q^4+8q^3+15q^2+22q-48}{60}$). □

Outra desigualdade que pode ser útil é dada em [26, Equation (2.10)].

Lema 1.84. *Sejam q a potência de um primo e n um inteiro positivo. Então*

$$\omega_q(x^n - 1) \leq \frac{1}{2}\left(n + \operatorname{mdc}(n, q-1)\right).$$

CAPÍTULO 2

Pares de elementos primitivos e normais sobre corpos finitos

Dados inteiros positivos m_1 e m_2, definimos um conjunto $\Upsilon_q(m_1, m_2)$ (ver Definição 2.1) com certas funções racionais $f_1(x)/f_2(x)$ tais que grau$(f_i(x)) \leq m_i$, para $i \in \{1, 2\}$. A seguir, determinamos condições que asseguram, para cada $f_1(x)/f_2(x) \in \Upsilon_{q^n}(m_1, m_2)$, a existência de um elemento primitivo $\alpha \in \mathbb{F}_{q^n}$ normal sobre $\mathbb{F}_q$ tal que $f_1(\alpha)/f_2(\alpha)$ é também primitivo (ver Corolário 2.4).

2.1 Preliminares

Ao longo do capítulo, p é um número primo, k, n, m_1, m_2 são inteiros positivos e $q = p^k$. Começamos definindo um conjunto com um papel importante no que se seguirá.

Definição 2.1. *Define-se $\Upsilon_q(m_1, m_2)$ como o conjunto de funções racionais $\frac{f_1}{f_2} \in \mathbb{F}_q(x)$ tais que:*

i) grau$(f_1) \leq m_1$, grau$(f_2) \leq m_2$;

ii) mdc$(f_1, f_2) = 1$;

iii) existem um inteiro positivo a e um polinômio mônico irredutível $g \in \mathbb{F}_q[x] \setminus \{x\}$ tais que mdc$(a, q-1) = 1$, *g^a divide $f_1 f_2$ e g^{a+1} não divide $f_1 f_2$.*

2.2 Resultados principais

Queremos determinar condições em q e n tais que, para todo $f \in \Upsilon_{q^n}(m_1, m_2)$, exista $\alpha \in \mathbb{F}_{q^n}$ primitivo normal sobre $\mathbb{F}_q$, tal que $f(\alpha) \in \mathbb{F}_{q^n}$ seja também um elemento primitivo. Para tal, precisamos da seguinte definição.

Definição 2.2. *Sejam e_1 e e_2 divisores de q^n-1 e g um divisor mônico de x^n-1. Dado $f \in \Upsilon_{q^n}(m_1,m_2)$, denotamos por $N_f(e_1,e_2,g)$ o número de elementos $\alpha \in \mathbb{F}_{q^n}$ tais que α é e_1-livre, $f(\alpha)$ é e_2-livre e α é g-livre.*

Pela Observação 1.73, um elemento $\alpha \in \mathbb{F}_{q^n}^*$ é primitivo se, e somente se, α é (q^n-1)-livre e, pela Observação 1.78, um elemento $\alpha \in \mathbb{F}_{q^n}$ é normal se, e somente se, α é (x^n-1)-livre. É por isso que queremos determinar condições que possam garantir $N_f(q^n-1, q^n-1, x^n-1) > 0$, para todo $f \in \Upsilon_{q^n}(m_1,m_2)$. O próximo resultado trata de um caso um pouco mais geral. Antes de começar, observe que, todo elemento em $\mathbb{F}_q$ é normal sobre $\mathbb{F}_q$ e se $\alpha \in \mathbb{F}_{q^2}^*$ não é normal sobre $\mathbb{F}_q$, então $\frac{\alpha^q}{\alpha} = \alpha^{q-1} \in \mathbb{F}_q$. Isso implica $\alpha^{(q-1)^2} = 1$ e, portanto, α não é primitivo. Logo, quando $n = 1$ ou $n = 2$, todo elemento primitivo em $\mathbb{F}_{q^n}$ é normal sobre $\mathbb{F}_q$. Assim, podemos ignorar o requerimento do elemento procurado ser normal pois, neste caso, o problema já foi resolvido em [5] e [12]. Dessa forma, daqui em diante no presente capítulo, vamos assumir $n \geq 3$.

Teorema 2.3. *Sejam e_1 e e_2 divisores de q^n-1, $g \in \mathbb{F}_q[x]$ um fator de x^n-1 e $f \in \Upsilon_{q^n}(m_1,m_2)$. Então*

$$\begin{aligned} N_f(e_1,e_2,g) \quad > \quad & \frac{\varphi(e_1)\varphi(e_2)\phi_q(g)}{e_1e_2N(g)}\left(q^n-(m_1+m_2+1)-\right. \\ & \left.(m_1+m_2+1)q^{\frac{n}{2}}(W(e_1)W(e_2)W_q(g)-1)\right) \end{aligned}$$

e, desta forma, se $q^{n/2} \geq (m_1+m_2+1)W(e_1)W(e_2)W_q(g)$, então $N_f(e_1,e_2,g) > 0$.

Demonstração. Sejam $f = \dfrac{f_1}{f_2} \in \Upsilon_{q^n}(m_1,m_2)$ e

$$S_f := \left\{\alpha \in \mathbb{F}_{q^n} \mid f_1(\alpha) = 0 \text{ or } f_2(\alpha) = 0\right\} \cup \{0\}.$$

Da definição de $N_f(e_1,e_2,g)$, da Proposição 1.72 e da Proposição 1.77, temos

$$\begin{aligned} N_f(e_1,e_2,g) &= \sum_{\alpha \in \mathbb{F}_{q^n}\setminus S_f} \rho_{e_1}(\alpha)\rho_{e_2}(f(\alpha))\kappa_g(\alpha) \\ &= \theta(e_1)\theta(e_2)\Theta_q(g) \sum_{\substack{d_1\mid e_1, d_2\mid e_2 \\ h\mid g}} \frac{\mu(d_1)\mu(d_2)\mu_q(h)}{\varphi(d_1)\varphi(d_2)\phi_q(h)} \sum_{\substack{\operatorname{ord}(\eta_1)=d_1 \\ \operatorname{ord}(\eta_2)=d_2 \\ \operatorname{Ord}(\psi)=h}} \tilde{\chi}_f(\eta_1,\eta_2,\psi), \end{aligned} \tag{2.1}$$

sendo

$$\tilde{\chi}_f(\eta_1,\eta_2,\psi) = \sum_{\alpha \in \mathbb{F}_{q^n}\setminus S_f} \eta_1(\alpha)\eta_2(f(\alpha))\psi(\alpha).$$

Para encontrar uma cota inferior de $N_f(e_1,e_2,g)$, precisamos limitar $|\tilde{\chi}_f(\eta_1,\eta_2,\psi)|$. Para tal vamos considerar cinco casos.

(i) Consideramos primeiro o caso no qual η_1, η_2 e ψ são os caracteres triviais, assim

$$\tilde{\chi}_f(\eta_1,\eta_2,\psi) = \left|\mathbb{F}_{q^n} \setminus S_f\right| \geq q^n-(m_1+m_2+1).$$

(ii) Agora lidamos com o caso em que η_1 e η_2 são os caracteres multiplicativos triviais, enquanto ψ não é o caracter aditivo trivial. Pelo Teorema 1.58, temos $\sum_{\alpha\in\mathbb{F}_{q^n}} \psi(\alpha) = 0$. Assim,

$$|\tilde{\chi}_f(\eta_1,\eta_2,\psi)| = \left|\sum_{\alpha\in\mathbb{F}_{q^n}\setminus S_f} \psi(\alpha)\right| = \left|-\sum_{\alpha\in S_f}\psi(\alpha)\right| \leq m_1+m_2+1.$$

(iii) Agora tratamos o caso em que η_1 não é o caracter trivial, enquanto η_2 e ψ são os caracteres triviais. Como $\sum_{\alpha\in\mathbb{F}_{q^n}^*} \eta_1(\alpha) = 0$ (ver Teorema 1.58), temos

$$\begin{aligned} |\tilde{\chi}_f(\eta_1,\eta_2,\psi)| &= \left|\sum_{\alpha\in\mathbb{F}_{q^n}^*}\eta_1(\alpha) - \sum_{\alpha\in\mathbb{F}_{q^n}\setminus S_f}\eta_1(\alpha)\right| = \left|\sum_{\alpha\in S_f\setminus\{0\}}\eta_1(\alpha)\right| \\ &\leq (m_1+m_2) < (m_1+m_2)q^{\frac{n}{2}}. \end{aligned}$$

Antes de continuar tratando os casos, vamos assumir que no máximo um dos caracteres é trivial e vamos reescrever a expressão $\tilde{\chi}_f(\eta_1,\eta_2,\psi)$.

Sejam η_1 e η_2 caracteres multiplicativos de ordens d_1 e d_2, respectivamente, com $d_1 \mid e_1$ e $d_2 \mid e_2$, e seja ψ um caracter aditivo de $\mathbb{F}_q$-ordem h. Pelo Teorema 1.61, sabe-se que existe um caracter η, de ordem q^n-1, que gera o grupo de caracteres multiplicativos. Para $i\in\{1,2\}$ existe um inteiro $n_i \in \{0,1,\ldots,q-2\}$ tal que $\eta_i(\alpha) = \eta(\alpha^{n_i})$, para todo $\alpha\in\mathbb{F}_{q^n}^*$, e observe que $n_i = 0$ se, e somente se, η_i é o caracter trivial. Por isso,

$$\begin{aligned} \tilde{\chi}_f(\eta_1,\eta_2,\psi) &= \sum_{\alpha\in\mathbb{F}_{q^n}\setminus S_f} \eta(\alpha^{n_1}f_1(\alpha)^{n_2}f_2(\alpha)^{-n_2})\psi(\alpha) \\ &= \sum_{\alpha\in\mathbb{F}_{q^n}\setminus S_f}\eta(v(\alpha))\psi(\alpha), \end{aligned}$$

sendo $v(x) = x^{n_1}f_1(x)^{n_2}f_2(x)^{-n_2}$.

(iv) Agora vamos assumir que ψ seja o caracter aditivo trivial e η_2 não seja o caracter multiplicativo trivial, assim $n_2 \neq 0$, e não assumimos nada quanto a η_1. Para limitar $\tilde{\chi}_f(\eta_1,\eta_2,\psi)$, vamos usar o Lema 1.79(a) e começamos mostrando que, de fato, podemos usá-lo. Assim, vamos supor o contrário, isto é, que existam $v_1(x), v_2(x) \in \overline{\mathbb{F}}_q[x]$ tais que $\mathrm{mdc}(v_1,v_2) = 1$ e $v(x) = \left(\frac{v_1(x)}{v_2(x)}\right)^{q^n-1}$. Assim,

$$x^{n_1}f_1(x)^{n_2}v_2(x)^{q^n-1} = f_2(x)^{n_2}v_1(x)^{q^n-1}.$$

Como $\frac{f_1}{f_2} \in \Upsilon_{q^n}(m_1,m_2)$, existem um polinômio mônico irredutível $t(x)\in\mathbb{F}_{q^n}[x]$, $t(x)\neq x$, e um inteiro positivo a satisfazendo $\mathrm{mdc}\,(a,q^n-1) = 1$ tais que $t(x)^a$ seja a maior potência de $t(x)$ que aparece na fatoração de $f_1(x)$ ou $f_2(x)$. Vamos supor que $t(x)^a$ apareça na fatoração de $f_2(x)$ e seja $\tilde{t}(x)$ um fator mônico irredutível de $t(x)$ em $\overline{\mathbb{F}}_q[x]$. Claramente, $\tilde{t}(x)$ é de grau 1, $\tilde{t}(x)\neq x$ e, como $\mathbb{F}_{q^n}$ é um corpo perfeito, $\tilde{t}(x)$ aparece com multiplicidade

um na fatoração de $t(x)$ em $\overline{\mathbb{F}}_q[x]$. Como $f_1(x)$ e $f_2(x)$ são coprimos em $\mathbb{F}_{q^n}[x]$, também são coprimos em $\overline{\mathbb{F}}_q[x]$. Logo, $\tilde{t}(x)^{an_2}$ é a maior potência de $\tilde{t}(x)$ que aparece na fatoração de $v_2(x)^{q^n-1}$. Podemos assim concluir $q^n - 1 \mid an_2$ e, de $\mathrm{mdc}(a, q^n - 1) = 1$, obtemos $q^n - 1 \mid n_2$, o que é uma contradição. Assim, $t(x)^a$ deve aparecer na fatoração de $f_1(x)$ e, repetindo o raciocínio acima, obtemos $q^n - 1 \mid n_2$, o que é uma contradição. Portanto, se $n_2 \neq 0$, então $v(x)$ não é da forma $\left(\frac{v_1(x)}{v_2(x)}\right)^{q^n-1}$ em $\overline{\mathbb{F}}_q(x)$.

Seja T_v o conjunto dos elementos $\beta \in \mathbb{F}_{q^n}$ tais que $v(\beta) = 0$ ou $v(\beta)$ não esteja definido. Se $0 \in T_v$, então $T_v = S_f$ e, do Lema 1.79(a), obtemos

$$\left|\tilde{\chi}_f(\eta_1, \eta_2, \psi)\right| = \left|\sum_{\alpha \in \mathbb{F}_{q^n} \setminus S_f} \eta(v(\alpha))\right| = \left|\sum_{\alpha \in \mathbb{F}_{q^n} \setminus T_v} \eta(v(\alpha))\right| \leq (m_1 + m_2)q^{\frac{n}{2}}.$$

Se $0 \notin T_v$, então

$$\left|\tilde{\chi}_f(\eta_1, \eta_2, \psi)\right| = \left|\sum_{\alpha \in \mathbb{F}_{q^n} \setminus S_f} \eta(v(\alpha))\right| = \left|\sum_{\alpha \in \mathbb{F}_{q^n} \setminus T_v} \eta(v(\alpha)) - \eta(v(0))\right|.$$

Logo, $\left|\tilde{\chi}_f(\eta_1, \eta_2, \psi)\right| \leq (m_1 + m_2 - 1)q^{\frac{n}{2}} + 1$ e, portanto, em todos os casos obtemos $|\tilde{\chi}_f(\eta_1, \eta_2, \psi)| \leq (m_1 + m_2)q^{\frac{n}{2}}$.

(v) Finalmente, consideremos que ψ não seja o caracter trivial e η_1 ou η_2 não seja o caracter trivial. Em particular, $d_1 \neq 1$ ou $d_2 \neq 1$. Obviamente, x não é da forma $r(x)^{q^n} - r(x)$ em $\overline{\mathbb{F}}_q(x)$. Logo, podemos usar o Lema 1.79(b).

Como no caso anterior, seja T_v o conjunto dos elementos $\beta \in \mathbb{F}_{q^n}$ tais que $v(\beta) = 0$ ou $v(\beta)$ não está definido. Se $0 \in T_v$, então $T_v = S_f$ e, do Lema 1.79(b), temos

$$\left|\tilde{\chi}_f(\eta_1, \eta_2, \psi)\right| = \left|\sum_{\alpha \in \mathbb{F}_{q^n} \setminus T_v} \eta(v(\alpha))\psi(\alpha)\right| \leq (m_1 + m_2 + 1)q^{\frac{n}{2}}.$$

Se $0 \notin T_v$, então

$$\left|\tilde{\chi}_f(\eta_1, \eta_2, \psi)\right| = \left|\sum_{\alpha \in \mathbb{F}_{q^n} \setminus T_v} \eta(v(\alpha))\psi(\alpha) - \eta(v(0))\psi(\alpha)\right| \leq (m_1 + m_2)q^{\frac{n}{2}} + 1$$

e, em todos os casos, obtemos $|\tilde{\chi}_f(\eta_1, \eta_2, \psi)| \leq (m_1 + m_2 + 1)q^{\frac{n}{2}}$.

Uma vez que todos os casos foram analisados, usamos as desigualdades obtidas para limitar $N_f(e_1, e_2, g)$. Sejam η_0 o caracter multiplicativo trivial e ψ_0 o caracter aditivo trivial. Escreva

$$N_f(e_1, e_2, g) = \theta(e_1)\theta(e_2)\Theta_q(g)(S_1 + S_2 + S_3 + S_4 + S_5),$$

sendo

$$S_1 = \tilde{\chi}_f(\eta_0, \eta_0, \psi_0),$$

$$S_2 = \sum_{\substack{h \mid g \\ h \neq 1}} \frac{\mu_q(h)}{\phi_q(h)} \sum_{\mathrm{Ord}(\psi) = h} \tilde{\chi}_f(\eta_0, \eta_0, \psi),$$

$$S_3 = \sum_{\substack{d_1|e_1\\ d_1\neq 1}} \frac{\mu(d_1)}{\varphi(d_1)} \sum_{\mathrm{ord}(\eta_1)=d_1} \tilde{\chi}_f(\eta_1,\eta_0,\psi_0),$$

$$S_4 = \sum_{\substack{d_1|e_1, d_2|e_2\\ d_2\neq 1}} \frac{\mu(d_1)\mu(d_2)}{\varphi(d_1)\varphi(d_2)} \sum_{\substack{\mathrm{ord}(\eta_1)=d_1\\ \mathrm{ord}(\eta_2)=d_2}} \tilde{\chi}_f(\eta_1,\eta_2,\psi_0)$$

e

$$S_5 = \sum_{\substack{d_1|e_1, d_2|e_2\\ d_1\neq 1 \text{ or } d_2\neq 1\\ 1\neq h|g}} \frac{\mu(d_1)\mu(d_2)\mu_q(h)}{\varphi(d_1)\varphi(d_2)\phi_q(h)} \sum_{\substack{\mathrm{ord}(\eta_1)=d_1\\ \mathrm{ord}(\eta_2)=d_2\\ \mathrm{Ord}(\psi)=h}} \tilde{\chi}_f(\eta_1,\eta_2,\psi).$$

Da análise realizada acima e usando que há $\varphi(d_1)$ caracteres multiplicativos de ordem d_1, $\varphi(d_2)$ caracteres multiplicativos de ordem d_2 e $\phi_q(h)$ caracteres aditivos de $\mathbb{F}_q$-ordem h, obtemos

$$\begin{aligned} |S_2+S_3+S_4+S_5| &< (m_1+m_2+1)q^{\frac{n}{2}}\Big(\sum_{\substack{d_1|e_1, d_2|e_2, h|g\\ (d_1,d_2,h)\neq(1,1,1)}} |\mu(d_1)||\mu(d_2)||\mu_q(h)|\Big)\\ &= (m_1+m_2+1)q^{\frac{n}{2}}\left(W(e_1)W(e_2)W_q(g)-1\right). \end{aligned}$$

Por conseguinte, concluímos

$$\begin{aligned} N_f(e_1,e_2,g) &> \theta(e_1)\theta(e_2)\Theta_q(g)\,(q^n-(m_1+m_2+1)-\\ &\quad (m_1+m_2+1)q^{\frac{n}{2}}(W(e_1)W(e_2)W_q(g)-1)\Big). \end{aligned} \tag{2.2}$$

Assim, se

$$\begin{aligned} q^n &\geq (m_1+m_2+1)q^{\frac{n}{2}}(W(e_1)W(e_2)W_q(g))\\ &> (m_1+m_2+1)+(m_1+m_2+1)q^{\frac{n}{2}}(W(e_1)W(e_2)W_q(g)-1), \end{aligned}$$

então $N_f(e_1,e_2,g)>0$. □

Corolário 2.4. *Se $q^{\frac{n}{2}} \geq (m_1+m_2+1)W(q^n-1)^2W_q(x^n-1)$ então, para todo $f\in\Upsilon_{q^n}(m_1,m_2)$, existe $\alpha\in\mathbb{F}_{q^n}$ primitivo normal sobre $\mathbb{F}_q$, tal que $f(\alpha)\in\mathbb{F}_{q^n}$ é também primitivo.*

O resultado seguinte apresenta uma desigualdade semelhante a outras que apareceram em trabalhos anteriores sobre elementos primitivos ou normais (ver, por exemplo, [10]).

Lema 2.5. *Sejam ℓ um divisor de q^n-1 e $\{p_1,\ldots,p_r\}$ o conjunto de todos os primos que dividem q^n-1, mas que não dividem ℓ. Sejam também $g\in\mathbb{F}_q[x]$ um divisor de x^n-1 e $\{P_1,\ldots,P_s\}\subset\mathbb{F}_q[x]$ o conjunto de todos os polinômios*

mônicos irredutíveis que dividem $x^n - 1$, mas que não dividem g em $\mathbb{F}_q[x]$. Então

$$N_f(q^n-1, q^n-1, x^n-1) \geq \sum_{i=1}^{r} N_f(p_i\ell, \ell, g) + \sum_{i=1}^{r} N_f(\ell, p_i\ell, g) + \sum_{i=1}^{s} N_f(\ell, \ell, P_i g) - (2r+s-1)N_f(\ell, \ell, g). \tag{2.3}$$

Demonstração. O lado esquerdo de (2.3) conta cada $\alpha \in \mathbb{F}_{q^n}$ tal que α é primitivo normal e $f(\alpha)$ é primitivo. Observe que se α é primitivo normal, então α é ℓ-livre, g-livre, $p_i\ell$-livre, para todo $i \in \{1, \ldots, r\}$, e $P_i g$-livre, para todo $i \in \{1, \ldots, s\}$. Além disso, se $f(\alpha)$ é primitivo, então $f(\alpha)$ é ℓ-livre e $p_i\ell$-livre, para todo $i \in \{1, \ldots, r\}$. Isso mostra que se α é primitivo normal e $f(\alpha)$ é primitivo, então α é contado uma $(2r + s - (2r + s - 1) = 1)$ vez no lado direito de (2.3). Para qualquer outro $\alpha \in \mathbb{F}_{q^n}$, temos que α ou $f(\alpha)$ não é $p_i\ell$-livre, para algum $i \in \{1, \ldots, r\}$, ou α não é $P_i g$-livre, para algum $i \in \{1, \ldots, s\}$ e, portanto, α ou $f(\alpha)$ não serão contados pelo menos uma vez em pelo menos uma das três somas do lado direito de (2.3). □

O próximo resultado será muito útil para os cálculos da próxima seção.

Lema 2.6. *Sejam ℓ um divisor de $q^n - 1$ e $\{p_1, \ldots, p_r\}$ o conjunto de primos que dividem $q^n - 1$, mas que não dividem ℓ. Sejam também $g \in \mathbb{F}_q[x]$ um divisor de $x^n - 1$ e $\{P_1, \ldots, P_s\} \subset \mathbb{F}_q[x]$ o conjunto de todos os polinômios mônicos irredutíveis que dividem $x^n - 1$, mas que não dividem g. Suponha*

$$\delta = 1 - 2\sum_{i=1}^{r} \frac{1}{p_i} - \sum_{i=1}^{s} \frac{1}{q^{\text{grau}(P_i)}} > 0$$

e seja $\Delta = \frac{2r+s-1}{\delta} + 2$. Se $q^{\frac{n}{2}} \geq (m_1 + m_2 + 1)W(\ell)^2 W_q(g)\Delta$ então, para cada $f \in \Upsilon_{q^n}(m_1, m_2)$, existe $\alpha \in \mathbb{F}_{q^n}$ primitivo normal sobre $\mathbb{F}_q$ tal que $f(\alpha) \in \mathbb{F}_{q^n}$ também é primitivo.

Demonstração. Do Lema 2.5, temos

$$N_f(q^n-1, q^n-1, x^n-1) \geq \sum_{i=1}^{r} N_f(p_i\ell, \ell, g) + \sum_{i=1}^{r} N_f(\ell, p_i\ell, g) + \sum_{j=1}^{s} N_f(\ell, \ell, P_j g) - (2r+s-1)N_f(\ell, \ell, g). \tag{2.4}$$

Como $\theta(p_i) = \dfrac{\varphi(p_i)}{p_i} = 1 - \dfrac{1}{p_i}$, para todo $i \in \{1, \ldots, r\}$ e $\Theta_q(P_j) = \dfrac{\phi_q(P_j)}{N(P_j)} = 1 - \dfrac{1}{q^{\text{grau}(P_j)}}$, para todo $j \in \{1, \ldots, s\}$,

podemos reescrever o lado direito de desigualdade acima e obtemos

$$\begin{aligned} N_f(q^n-1,q^n-1,x^n-1) \geq & \sum_{i=1}^{r}(N_f(p_i\ell,\ell,g)-\theta(p_i)N_f(\ell,\ell,g)) \\ & + \sum_{i=1}^{r}(N_f(\ell,p_i\ell,g)-\theta(p_i)N_f(\ell,\ell,g))+ \\ & \sum_{j=1}^{s}(N_f(\ell,\ell,P_jg)-\Theta_q(P_j)N_f(\ell,\ell,g))+\delta N_f(\ell,\ell,g). \end{aligned}$$

De $\theta(\ell p_i)=\theta(p_i)\theta(\ell)$ e (2.1), temos

$$N_f(p_i\ell,\ell,g)=\theta(p_i)\theta(\ell)^2\Theta_q(g)\sum_{\substack{d_1|p_i\ell,d_2|\ell\\ h|g}}\frac{\mu(d_1)\mu(d_2)\mu_q(h)}{\varphi(d_1)\varphi(d_2)\phi_q(h)}\sum_{\substack{\mathrm{ord}(\eta_1)=d_1\\ \mathrm{ord}(\eta_2)=d_2\\ \mathrm{Ord}(\psi)=h}}\tilde{\chi}_f(\eta_1,\eta_2,\psi),$$

para todo $i\in\{1,\ldots,r\}$. Por outro lado, para todo $i\in\{1,\ldots,r\}$ separamos o conjunto dos d_1's que dividem $p_i\ell$ em dois conjuntos: o primeiro contém aqueles que não têm p_i como fator, enquanto o segundo contém aqueles que são múltiplos de p_i. Isso separa a primeira soma em duas somas. Assim,

$$\begin{aligned} N_f(p_i\ell,\ell,g) &= \theta(p_i)\theta(\ell)^2\Theta_q(g)\sum_{\substack{d_1|\ell,d_2|\ell\\ h|g}}\frac{\mu(d_1)\mu(d_2)\mu_q(h)}{\varphi(d_1)\varphi(d_2)\phi_q(h)}\sum_{\substack{\mathrm{ord}(\eta_1)=d_1\\ \mathrm{ord}(\eta_2)=d_2\\ \mathrm{Ord}(\psi)=h}}\tilde{\chi}_f(\eta_1,\eta_2,\psi) \\ &+ \theta(p_i)\theta(\ell)^2\Theta_q(g)\sum_{\substack{p_i|d_1,d_1|p_i\ell,d_2|\ell\\ h|g}}\frac{\mu(d_1)\mu(d_2)\mu_q(h)}{\varphi(d_1)\varphi(d_2)\phi_q(h)}\sum_{\substack{\mathrm{ord}(\eta_1)=d_1\\ \mathrm{ord}(\eta_2)=d_2\\ \mathrm{Ord}(\psi)=h}}\tilde{\chi}_f(\eta_1,\eta_2,\psi) \end{aligned}$$

e, da expressão para $N_f(\ell,\ell,g)$ (ver (2.1)), obtemos

$$\begin{aligned} & N_f(p_i\ell,\ell,g)-\theta(p_i)N_f(\ell,\ell,g) \\ & \quad =\theta(p_i)\theta(\ell)^2\Theta_q(g)\sum_{\substack{p_i|d_1,d_1|p_i\ell,d_2|\ell\\ h|g}}\frac{\mu(d_1)\mu(d_2)\mu_q(h)}{\varphi(d_1)\varphi(d_2)\phi_q(h)}\sum_{\substack{\mathrm{ord}(\eta_1)=d_1\\ \mathrm{ord}(\eta_2)=d_2\\ \mathrm{Ord}(\psi)=h}}\tilde{\chi}_f(\eta_1,\eta_2,\psi). \end{aligned}$$

De (iv) e (v) na prova do Teorema 2.3 e de

$$\sum_{\substack{p_i|d_1,d_1|p_i\ell,d_2|\ell\\ h|g}}|\mu(d_1)||\mu(d_2)||\mu_q(h)|=W(l)^2W_q(g),$$

concluímos

$$\left|N_f(p_i\ell,\ell,g)-\theta(p_i)N_f(\ell,\ell,g)\right|\leq(m_1+m_2+1)\theta(p_i)\theta(\ell)^2\Theta_q(g)q^{\frac{n}{2}}W(\ell)^2W_q(g). \tag{2.5}$$

De forma similar, obtemos

$$\left|N_f(\ell, p_i\ell, g) - \theta(p_i)N_f(\ell, \ell, g)\right| \leq (m_1 + m_2 + 1)\theta(p_i)\theta(\ell)^2\Theta_q(g)q^{\frac{n}{2}}W(\ell)^2W_q(g), \tag{2.6}$$

para todo $i \in \{1, \ldots, r\}$.

De novo, de (2.1) e usando $\Theta_q(P_jg) = \Theta_q(P_j)\Theta_q(g)$, obtemos

$$N_f(\ell, \ell, P_jg) = \theta(\ell)^2\Theta_q(P_j)\Theta_q(g) \sum_{\substack{d_1|\ell, d_2|\ell \\ h|P_jg}} \frac{\mu(d_1)\mu(d_2)\mu_q(h)}{\varphi(d_1)\varphi(d_2)\phi_q(h)} \sum_{\substack{\mathrm{ord}(\eta_1)=d_1 \\ \mathrm{ord}(\eta_2)=d_2 \\ \mathrm{Ord}(\psi)=h}} \tilde{\chi}_f(\eta_1, \eta_2, \psi).$$

Separando o conjunto dos h's que dividem P_jg em dois conjuntos, a saber, o primeiro contém aqueles que não têm P_j como fator, enquanto que o segundo contém aqueles que são múltiplos de P_j, temos

$$\begin{aligned} N_f(\ell, \ell, P_jg) &= \theta(\ell)^2\Theta_q(P_j)\Theta_q(g) \sum_{\substack{d_1|\ell, d_2|\ell \\ h|g}} \frac{\mu(d_1)\mu(d_2)\mu_q(h)}{\varphi(d_1)\varphi(d_2)\phi_q(h)} \sum_{\substack{\mathrm{ord}(\eta_1)=d_1 \\ \mathrm{ord}(\eta_2)=d_2 \\ \mathrm{Ord}(\psi)=h}} \tilde{\chi}_f(\eta_1, \eta_2, \psi) \\ &+ \theta(\ell)^2\Theta_q(P_j)\Theta_q(g) \sum_{\substack{d_1|\ell, d_2|\ell \\ P_j|h, h|P_jg}} \frac{\mu(d_1)\mu(d_2)\mu_q(h)}{\varphi(d_1)\varphi(d_2)\phi_q(h)} \sum_{\substack{\mathrm{ord}(\eta_1)=d_1 \\ \mathrm{ord}(\eta_2)=d_2 \\ \mathrm{Ord}(\psi)=h}} \tilde{\chi}_f(\eta_1, \eta_2, \psi). \end{aligned}$$

Da expressão para $N_f(\ell, \ell, g)$ (ver (2.1)), obtemos

$$\begin{aligned} &N_f(\ell, \ell, P_jg) - \Theta_q(P_j)N_f(\ell, \ell, g) \\ &\quad = \theta(\ell)^2\Theta_q(P_j)\Theta_q(g) \sum_{\substack{d_1|\ell, d_2|\ell \\ P_j|h, h|P_jg}} \frac{\mu(d_1)\mu(d_2)\mu_q(h)}{\varphi(d_1)\varphi(d_2)\phi_q(h)} \sum_{\substack{\mathrm{ord}(\eta_1)=d_1 \\ \mathrm{ord}(\eta_2)=d_2 \\ \mathrm{Ord}(\psi)=h}} \tilde{\chi}_f(\eta_1, \eta_2, \psi). \end{aligned}$$

De (ii) e (v) na prova do Teorema 2.3 e de

$$\sum_{\substack{d_1|\ell, d_2|\ell \\ P_j|h, h|P_jg}} |\mu(d_1)||\mu(d_2)||\mu_q(h)| = W(l)^2W_q(g),$$

concluímos

$$\left|N_f(\ell, \ell, P_jg) - \Theta_q(P_j)N_f(\ell, \ell, g)\right| \leq (m_1 + m_2 + 1)\theta(\ell)^2\Theta_q(P_j)\Theta_q(g)q^{\frac{n}{2}}W(\ell)^2W_q(g). \tag{2.7}$$

Assim, substituindo os resultados de (2.5), (2.6) e (2.7) em (2.4), temos

$$\begin{aligned}
&N_f(q^n-1,q^n-1,x^n-1)\\
&\quad\geq \delta N_f(\ell,\ell,g)-(m_1+m_2+1)\theta(\ell)^2\Theta_q(g)q^{\frac{n}{2}}W(\ell)^2W_q(g)\left(2\sum_{i=1}^{r}\theta(P_i)+\sum_{j=1}^{s}\Theta_q(P_j)\right)\\
&\quad=\delta N_f(\ell,\ell,g)\\
&\qquad\qquad-(m_1+m_2+1)\theta(\ell)^2\Theta_q(g)q^{\frac{n}{2}}W(\ell)^2W_q(g)(2r+s-2\sum_{i=1}^{r}\frac{1}{p_i}-\sum_{j=1}^{s}\frac{1}{q^{\mathrm{grau}(P_j)}})\\
&\quad=\delta N_f(\ell,\ell,g)-((m_1+m_2+1)\theta(\ell)^2\Theta_q(g)q^{\frac{n}{2}}W(\ell)^2W_q(g))(\delta(\Delta-1)).
\end{aligned}$$

De (2.2), obtemos

$$\begin{aligned}
N_f(\ell,\ell,g) &> \theta(\ell)^2\Theta_q(g)\left(q^n-(m_1+m_2+1)-(m_1+m_2+1)q^{\frac{n}{2}}(W(\ell)^2W_q(g)-1)\right)\\
&> \theta(\ell)^2\Theta_q(g)(q^n-(m_1+m_2+1)q^{\frac{n}{2}}W(\ell)^2W_q(g)),
\end{aligned}$$

pois $(m_1+m_2+1)q^{\frac{n}{2}}-(m_1+m_2+1)>0$.

Da hipótese, temos $\delta>0$, portanto,

$$N_f(q^n-1,q^n-1,x^n-1)>\delta\theta(\ell)^2\Theta_q(g)(q^n-(m_1+m_2+1)q^{\frac{n}{2}}W(\ell)^2W_q(g)\Delta).$$

Desta forma, se $q^n\geq(m_1+m_2+1)q^{\frac{n}{2}}W(\ell)^2W_q(g)\Delta$, então $N_f(q^n-1,q^n-1,x^n-1)>0$. □

Definição 2.7. *Dados inteiros positivos m_1 e m_2, seja $\mathcal{B}(m_1,m_2)$ o conjunto dos pares $(q,n)\in\mathbb{Z}_+^2$, com q a potência de um primo, tais que para cada $f\in\Upsilon_{q^n}(m_1,m_2)$ existe um elemento primitivo $\alpha\in\mathbb{F}_{q^n}$ normal sobre $\mathbb{F}_q$ com $f(\alpha)$ primitivo em $\mathbb{F}_{q^n}$.*

Note que, se $n_1\leq m_1$ e $n_2\leq m_2$, então $\mathcal{B}(m_1,m_2)\subset\mathcal{B}(n_1,n_2)$, pois $\Upsilon_{q^n}(n_1,n_2)\subset\Upsilon_{q^n}(m_1,m_2)$. Terminamos a presente seção provando que existe só um número finito de pares $(q,n)\in\mathbb{Z}_+^2$ tais que q é a potência de um primo e $(q,n)\notin\mathcal{B}(m_1,m_2)$.

Proposição 2.8. *Existe somente um número finito de pares $(q,n)\in\mathbb{Z}_+^2$ tais que q é a potência de um primo e $(q,n)\notin\mathcal{B}(m_1,m_2)$.*

Demonstração. Claramente, todo elemento $\alpha\in\mathbb{F}_q^*$ é normal sobre $\mathbb{F}_q$ e é bem conhecido que se $\alpha\in\mathbb{F}_{q^2}$ é primitivo, então α também é normal sobre $\mathbb{F}_q$. Assim, para $n=1$ ou $n=2$ temos $(q,n)\in\mathcal{B}(m_1,m_2)$ se, e somente se, para todo $f\in\Upsilon_{q^n}(m_1,m_2)$, existe um elemento primitivo $\alpha\in\mathbb{F}_{q^n}$ tal que $f(\alpha)$ também é primitivo. De [12, Thm. 3.1], sabemos que uma condição de suficiência para a existência de um tal elemento é $q^{n/2}\geq(m_1+m_2)W(q^n-1)^2$. Usando o Lema 1.81 e escolhendo um número real $t>4$ podemos verificar que se $q\geq((m_1+m_2)A_t)^{\frac{2t}{(t-4)n}}$, então $(q,n)\in\mathcal{B}(m_1,m_2)$. Em particular, existe somente um número finito de pares $(q,n)\notin\mathcal{B}(m_1,m_2)$, quando $n=1$ ou $n=2$.

Vamos supor agora $n \geq 3$. Pelo Corolário 2.4, como $W_q(x^n - 1) \leq 2^n$ e usando o Lema 1.81, para algum número real $t > 4$, se $q^{\frac{n}{2}} \geq (m_1 + m_2 + 1) \cdot A_t^2 \cdot q^{\frac{2n}{t}} \cdot 2^n$, então $(q, n) \in \mathcal{B}(m_1, m_2)$. Em particular, dado um inteiro $n \geq 3$, se

$$q \geq \left(2^n \cdot (m_1 + m_2 + 1) \cdot A_t^2\right)^{\frac{2t}{(t-4)n}}, \tag{2.8}$$

então $(q, n) \in \mathcal{B}(m_1, m_2)$. Isso quer dizer que, para um número inteiro $n \geq 3$ dado, existe um número finito de potências de primos q tais que $(q, n) \notin \mathcal{B}(m_1, m_2)$.

A desigualdade $q^{\frac{n}{2}} \geq (m_1 + m_2 + 1) \cdot A_t^2 \cdot q^{\frac{2n}{t}} \cdot 2^n$ é equivalente a

$$n \geq \frac{\ln\left((m_1 + m_2 + 1) \cdot A_t^2\right)}{(\frac{t-4}{2t}) \cdot \ln q - \ln 2}, \tag{2.9}$$

para $t > \frac{4 \ln q}{\ln q - 2 \ln 2}$. Veja que a função do lado direito é uma função decrescente de $q > 2^{\frac{2t}{t-4}}$. Isso quer dizer que se escolhemos $t \geq 29$, então o lado direito de (2.9) é uma função decrescente de $q \geq 5$. Assim, se N é um inteiro positivo tal que (2.9) é válida para $q = 5$, para algum $t \geq 29$, então $(q, n) \in \mathcal{B}(m_1, m_2)$ para todas as potências de primos $q \geq 5$ e todo inteiro positivo $n \geq N$.

De [26, Lemma 2.11], para $n \geq 16$

$$W_q(x^n - 1) \leq \begin{cases} 2^{\frac{n+5}{4}} & \text{se } q = 2, \\ 2^{\frac{n+4}{3}} & \text{se } q = 3, \\ 2^{\frac{n}{3}+2} & \text{se } q = 4. \end{cases}$$

Para esses valores de q podemos mudar a desigualdade (2.9) por

$$n \geq \begin{cases} \frac{4t}{t-8}\left(\frac{\ln((m_1+m_2+1)\cdot A_t^2)}{\ln 2} + \frac{5}{4}\right) & \text{para algum } t > 8 \text{ se } q = 2, \\ \frac{\ln((m_1+m_2+1)\cdot A_t^2) + \frac{4}{3}\ln 2}{(\frac{t-4}{2t})\ln 3 - \frac{1}{3}\ln 2} & \text{para algum } t \geq 7 \text{ se } q = 3, \\ \frac{3t}{t-6}\left(\frac{\ln((m_1+m_2+1)\cdot A_t^2)}{\ln 4} + 1\right) & \text{para algum } t > 6 \text{ se } q = 4. \end{cases} \tag{2.10}$$

Das desigualdades (2.9) e (2.10), obtemos que existe um inteiro positivo M tal que se $n \geq M$, então $(q, n) \in \mathcal{B}(m_1, m_2)$, para toda potência de primo q. Para os inteiros positivos $n < M$ temos, pelo que foi feito antes, que existe um número finito de potências de primos tais que $(q, n) \notin \mathcal{B}(m_1, m_2)$. □

2.3 Exemplos numéricos

Nessa seção vamos determinar $\mathcal{B}(3, 2)$, exceto talvez para um número finito de pares (q, n), que iremos listar.

Proposição 2.9. *Sejam q a potência de um primo e $n \geq 3$ um inteiro positivo. Temos $(q, n) \in \mathcal{B}(3, 2)$ para $q \geq 3.74 \cdot 10^9$ e $n = 3$, para $q \geq 3.91 \cdot 10^7$ e $n = 4$, para $q \geq 2.5 \cdot 10^6$ e $n = 5$, e para $q \geq 23$ e $n \geq 6$.*

Demonstração. Da desigualdade (2.8), se $q \geq \left(2 \cdot \sqrt[n]{6 \cdot A_t^2}\right)^{\frac{2t}{t-4}}$ é valida, para algum número real $t > 4$, então $(q,n) \in \mathcal{B}(3,2)$. Usando essa desigualdade, construímos a Tabela 2.1, em que cada linha mostra valores de t, n e $M(n,t)$ para os quais obtemos $(q,n) \in \mathcal{B}(3,2)$, sempre que $q \geq M(n,t)$.

t	n	$M(n,t)$
6.3	3	$3.74 \cdot 10^9$
6.3	4	$3.91 \cdot 10^7$
6.4	5	$2.5 \cdot 10^6$
6.5	6, 7, 8, 9	394155
6.7	$10, 11, \ldots, 157$	9239
9	$n \geq 158$	23

Tabela 2.1: Valores de q, com n e t dados, para os quais $(q,n) \in \mathcal{B}(3,2)$.

Vamos refinar a cota inferior de q, quando $n \geq 6$. Começamos testando a desigualdade $q^{\frac{n}{2}} \geq 6W(\ell)^2 W_q(g)\Delta$, que aparece no Lema 2.6, tomando potências de primos q no intervalo $9239 \leq q < 394155$, com $\ell = \text{mdc}(q^n - 1, 2 \cdot 3 \cdot 5 \cdot 7)$, $g = 1$ e $n \in \{6,7,8,9\}$. Neste caso obtemos $(q,n) \in \mathcal{B}(3,2)$ para todos esses valores de q e n. A seguir, combinamos a condição do Corolário 2.4 com a cota no Lema 1.81, para obter a desigualdade $q^{\frac{n}{2}} \geq 6A_t^2 q^{\frac{2n}{t}} W_q(x^n - 1)$ que é válida para as potências de primos $23 \leq q < 9239$ e $65 \leq n \leq 157$, quando tomamos $t = 7$. Assim, obtemos $(q,n) \in \mathcal{B}(3,2)$ para esses valores de q e n. Tomando $t = 8$, a desigualdade é válida para as potências de primos $23 \leq q < 9239$ e n no intervalo $6 \leq n < 65$, exceto para 7713 pares (q,n). Para testar se estes pares pertencem a $\mathcal{B}(3,2)$, usamos novamente o Lema 2.6, tomando $\ell = \text{mdc}(q^n - 1, 2 \cdot 3 \cdot 5 \cdot 7)$ e $g = 1$, e obtemos uma resposta afirmativa, exceto para os pares

$$(32,31), (27,26), (27,52), (25,24), (25,48), (49,48), (23,22),$$
$$(23,44), (31,30), (37,36), (41,40), (43,42), (47,46), (53,52).$$

Para verificar se esses pares pertencem a $\mathcal{B}(3,2)$ usamos uma vez mais a condição do Lema 2.6, novamente com $\ell = \text{mdc}(q^n - 1, 2 \cdot 3 \cdot 5 \cdot 7)$, mas desta vez tomamos g como sendo o produto de todos os fatores lineares de $x^n - 1$, e obtemos que todos esses pares pertencem a $\mathcal{B}(3,2)$. □

O próximo resultado será útil no estudo do caso $n = 3$.

Lema 2.10. *Seja q a potência de um primo. Se $p \neq 3$ é um número primo tal que $p \mid q^2 + q + 1$, então $p \nmid q - 1$ e $p \equiv 1 \pmod 6$.*

Demonstração. De $\text{mdc}(q-1, q^2+q+1) = \text{mdc}(q-1, 3) \in \{1, 3\}$ e do fato que $p \neq 3$ é um divisor primo de q^2+q+1, obtemos $p \nmid q-1$. Como $p \mid q^3 - 1$ e $q \not\equiv 1 \pmod p$, temos q um elemento de ordem multiplicativa 3 em $\mathbb{F}_p^*$, portanto, $3 \mid p-1$. Por outro lado, qualquer que seja o inteiro q, q^2+q+1 é ímpar, logo $p \neq 2$. Isso implica $p \equiv 1 \pmod 6$. □

Proposição 2.11. *Seja q a potência de um primo. Então $(q,3) \in \mathcal{B}(3,2)$, exceto eventualmente para*

$$q \in \{2,4,8,16,3,9,27,81,5,25,7,49,11,121,13,17,$$
$$19,23,29,31,37,43,61,67,71,79,151,211,331\}.$$

Demonstração. Do Lema 2.9, $(q,3) \in \mathcal{B}(3,2)$, para $q \geq 3.74 \cdot 10^9$. Assim, podemos assumir $q < 3.74 \cdot 10^9$. Seja

$$q^2 + q + 1 = 3^{a_0} \cdot \prod_{i=1}^{r} p_i^{a_i}$$

a decomposição de $q^2 + q + 1$ em fatores primos. Do Lema 2.10, $p_i \nmid q - 1$ e $p_i \equiv 1 \pmod 6$ para $i \in \{1, \ldots, r\}$. Para todo número natural k, sejam $\mathcal{S}_r$ e $\mathcal{P}_r$, respectivamente, a soma dos inversos e o produto dos primeiros r números primos da forma $6j+1$. Então $\mathcal{P}_r \leq q^2 + q + 1 < 1.3988 \cdot 10^{19}$ e, como $\mathcal{P}_{11} < 2 \cdot 10^{17}$ e $2 \cdot 10^{19} < \mathcal{P}_{12}$, devemos ter $r \leq 11$. Para verificar se $(q,3) \in \mathcal{B}(3,2)$, usamos a condição $q^{\frac{n}{2}} \geq 6W(\ell)^2 W_q(g)\Delta$ que aparece no Lema 2.6, tomando $\ell = q-1$ e $g = 1$. Vamos supor $q > 10^4$. Então

$$\delta \geq 1 - 2S_r - \frac{3}{q} > 1 - 2\mathcal{S}_{11} - \frac{3}{10^4} > 0.153$$

e $\Delta = 2 + \frac{2r+s-1}{\delta} < 2 + \frac{2 \cdot 11 + 3 - 1}{0.153} < 159$. Usando a cota do Lema 1.81, obtemos que a condição acima é satisfeita se

$$q^{\frac{3}{2}} \geq 6 \cdot A_t^2 \cdot q^{\frac{2}{t}} \cdot W_q(1) \cdot 159,$$

ou, de forma equivalente, se $q \geq \left(954 \cdot A_t^2\right)^{\frac{2t}{3t-4}}$, para algum número real $t > 4/3$. Tomando $t = 3.7$, obtemos $(q,3) \in \mathcal{B}(3,2)$ para $q \geq 22282$. Para verificar se $(q,3) \in \mathcal{B}(3,2)$ para as 2563 potências de primos menores que 22282, verifica-se a condição do Lema 2.6 tomando $\ell = \text{mdc}(q^3 - 1, 2 \cdot 3 \cdot 5)$ e $g = 1$. Obtemos $(q,3) \in \mathcal{B}(3,2)$, para todas as potências de primos $q \leq 22282$, exceto possivelmente para

$$q \in \{2,4,8,16,3,9,27,81,5,25,7,49,11,121,13,17,19,$$
$$23,29,31,37,41,43,61,67,71,79,151,181,211,331\}.$$

Também obtemos $(41,3), (181,3) \in \mathcal{B}(3,2)$, verificando que a condição do Lema 2.6 é satisfeita com os dados $\ell = 2$, $g = 1$ (para o par $(41,3)$) e $\ell = 2 \cdot 3$, $g = 1$ (para o par $(181,3)$). □

Proposição 2.12. *Seja q a potência de um primo. Então $(q,4) \in \mathcal{B}(3,2)$, exceto possivelmente para*

$$q \in \{2,4,8,16,3,9,27,5,25,7,11,13,$$
$$17,19,23,29,31,37,41,43,47,83\}.$$

Demonstração. Do Lema 2.9, temos $(q,4) \in \mathcal{B}(3,2)$ para $q \geq 3.91 \cdot 10^7$. Assim, vamos assumir $q < 3.91 \cdot 10^7$. Seja

$$q^4 - 1 = 2^{a_0} \cdot 3^{a_1} \cdot 5^{a_2} \cdot 7^{a_3} \cdot 11^{a_4} \cdot 13^{a_5} \cdot \prod_{i=1}^{r} p_i^{b_i}$$

a decomposição de $q^4 - 1$ em fatores primos, sendo $p_i > 13$ para $i \in \{1, \ldots, r\}$. Sejam $\mathcal{S}_r$ e $\mathcal{P}_r$, respectivamente, a soma dos inversos e o produto dos primeiros r números primos maiores que 13. Temos $\mathcal{P}_r \leq q^4 - 1 < 2.34 \cdot 10^{30}$ e, de $\mathcal{P}_{18} < 7.92 \cdot 10^{29}$ e $7.67 \cdot 10^{31} < \mathcal{P}_{19}$, obtemos $r \leq 18$. Vamos supor $q > 10^3$. Queremos aplicar o Lema 2.6, com $\ell = \text{mdc}(q^4 - 1, 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13)$ e $g = 1$. Temos

$$\delta \geq 1 - 2\mathcal{S}_r - \frac{4}{q} > 1 - 2\mathcal{S}_{18} - \frac{4}{10^3} > 0.099$$

e $\Delta = 2 + \frac{2r+s-1}{\delta} < 2 + \frac{2 \cdot 18 + 4 - 1}{0.099} < 396$. Como $W(\ell) \leq 2^6$ e $W_q(1) = 1$, então, se $q \geq 3120 \geq (6 \cdot (2^6)^2 \cdot 396)^{\frac{1}{2}}$, $q^{\frac{4}{2}} \geq 6W(\ell)^2 W_q(g)\Delta$. Assim, do Lema 2.6, obtemos $(q,4) \in \mathcal{B}(3,2)$, para $q \geq 3120$. Há 480 potências de primos menores que 3120 e, pelo Lema 2.6 com $\ell = \text{mdc}(q^4 - 1, 2 \cdot 3 \cdot 5)$ e $g = 1$, obtemos $(q,4) \in \mathcal{B}(3,2)$, para toda potência de primo q, exceto talvez para

$$q \in \{2, 4, 8, 16, 32, 3, 9, 27, 5, 25, 7, 49, 11, 13, 17,$$
$$19, 23, 29, 31, 37, 41, 43, 47, 53, 61, 67, 73, 83\}.$$

Para esse valores usamos novamente o Lema 2.6, tomando $\ell = \text{mdc}(q^4 - 1, 2 \cdot 3)$ e $g = 1$, e obtemos $(q,4) \in \mathcal{B}(3,2)$, para $q \in \{32, 49, 53, 61, 67, 73\}$. □

Proposição 2.13. *Seja q a potência de um primo. Então $(q,5) \in \mathcal{B}(3,2)$, exceto possivelmente para $q \in \{2, 3, 4, 5, 7, 9, 11, 16\}$.*

Demonstração. Do Lema 2.9, temos $(q,5) \in \mathcal{B}(3,2)$, para $q \geq 2.5 \cdot 10^6$. Assim, assumimos $q < 2.5 \cdot 10^6$. Existem 183404 potências de primos menores que $2.5 \cdot 10^6$ e, para estas potências de primos, usamos o Lema 2.6 tomando $\ell = \text{mdc}(q^5 - 1, 2 \cdot 3 \cdot 5)$ e $g = 1$. Obtemos $(q,5) \in \mathcal{B}(3,2)$, para todas as potências de primos q, exceto possivelmente para $q \in \{2, 3, 4, 5, 7, 9, 11, 16, 31\}$. Também obtemos $(31,5) \in \mathcal{B}(3,2)$, pelo Lema 2.6, tomando agora $\ell = 2 \cdot 3$ e $g = 1$. □

Agora vamos tratar os casos em que $2 \leq q \leq 19$. No que se segue, iremos limitar $W(u)$ com $u = q^n - 1$, sendo q a potência de um primo p. Como $p \nmid q^n - 1$, podemos usar outra variante da constante A_t no Lema 1.81, isto é, definimos

$$\tilde{A}_{t,p} := \prod_{\substack{\wp < 2^t \\ \wp \neq p \\ \wp \text{ é primo}}} \frac{2}{\sqrt[t]{\wp}}. \tag{2.11}$$

Proposição 2.14. *Para $q = 2$ e $n \geq 3$, temos $(2,n) \in \mathcal{B}(3,2)$, para todo $n \in \{13, 17, 19, 21, 22, 23\}$ e todo $n \geq 25$.*

Demonstração. Para verificar se $(2,n) \in \mathcal{B}(3,2)$, começamos procedendo como no segundo parágrafo da prova da Proposição 2.8, com a diferença que, no lugar de usar A_t, usamos o número $\tilde{A}_{t,2}$ definido acima. Temos

$$\tilde{A}_{t,2} = \prod_{\substack{\wp<2^t \\ \wp\neq 2 \\ \wp \text{ é primo}}} \frac{2}{\sqrt[t]{\wp}}.$$

Dessa forma, temos $W(2^n-1) \leq \tilde{A}_{t,2} \cdot 2^{\frac{n}{t}}$ e obtemos que se

$$n > \frac{4t}{t-8}\left(\frac{\ln(6\cdot \tilde{A}_{t,2}^2)}{\ln 2} + \frac{5}{4}\right),$$

para algum $t > 8$ (ver (2.10)), então $(2,n) \in \mathcal{B}(3,2)$. Tomando $t = 9.8$, obtemos $(2,n) \in \mathcal{B}(3,2)$, para $n \geq 1237$. A seguir, obtemos que a desigualdade $2^{\frac{n}{2}} \geq 6 \cdot \tilde{A}_{t,2}^2 \cdot 2^{\frac{2n}{t}} \cdot W_2(x^n-1)$ é válida, para $156 \leq n \leq 1236$, quando tomamos $t = 8.1$. Assim, do Corolário 2.4, também temos $(2,n) \in \mathcal{B}(3,2)$, para esses valores de n. Agora verifica-se a desigualdade $2^{\frac{n}{2}} \geq 6 \cdot W(2^n-1)^2 \cdot W_2(x^n-1)$ do Corolário 2.4 e obtemos que isso é válido para $n \geq 17$, exceto para $n \in \{18,20,21,22,24,28,30,36,45\}$. Para essas exceções e para os inteiros n tais que $3 \leq n \leq 16$ usamos o Lema 2.6 com $\ell = \text{mdc}(2^n-1, 3\cdot 5)$ e g como sendo o produto dos fatores mônicos irredutíveis de x^n-1 de grau k com $2^k \leq 2\cdot n$ (isto é feito para aumentar as chances de δ ser positivo). Nesse caso, obtemos $(2,n) \in \mathcal{B}(3,2)$, para $n \in \{13,21,22,28,30,36,45\}$. □

Proposição 2.15. *Para $q = 3$ e $n \geq 3$, temos $(3,n) \in \mathcal{B}(3,2)$, para todo $n \in \{11,13,14,15\}$ e todo $n \geq 17$.*

Demonstração. Como antes, procedemos como no segundo parágrafo da prova da Proposição 2.8 e como $3 \nmid 3^n-1$, no lugar de A_t usamos $\tilde{A}_{t,3}$, de tal forma que $W(3^n-1) \leq \tilde{A}_{t,3} \cdot 3^{\frac{n}{t}}$ é válido para $t > 0$. Da desigualdade (2.10), para o caso $q = 3$ e tomando $t = 8.8$, obtemos $(3,n) \in \mathcal{B}(3,2)$, para os inteiros $n \geq 373$. Para $122 \leq n \leq 372$, a desigualdade $3^{\frac{n}{2}} \geq 6 \cdot \tilde{A}_{t,3}^2 \cdot 3^{\frac{2n}{t}} \cdot W_3(x^n-1)$ é válida, se tomamos $t = 8$. Portanto, do Corolário 2.4, obtemos $(3,n) \in \mathcal{B}(3,2)$, para n nesse intervalo. Para $3 \leq n \leq 121$, verificamos que a desigualdade $3^{\frac{n}{2}} \geq 6 \cdot W(3^n-1)^2 \cdot W_3(x^n-1)$ não é válida para $n \in \{18,20,22,24\}$. Logo, pelo Corolário 2.4, obtemos $(3,n) \in \mathcal{B}(3,2)$, para $17 \leq n \leq 121$, exceto para $n \in \{18,20,22,24\}$. Para $3 \leq n \leq 16$ e $n \in \{18,20,22,24\}$, verifica-se a desigualdade que aparece no Lema 2.6, tomando $\ell = \gcd(3^n-1, 2\cdot 5)$ e g como sendo o produto dos fatores mônicos lineares de x^n-1. Nesse caso obtemos $(3,n) \in \mathcal{B}(3,2)$, para $n \in \{11,13,14,15,18,20,22,24\}$. □

Proposição 2.16. *Para $q = 4$ e $n \geq 3$, temos $(4,n) \in \mathcal{B}(3,2)$, para $n = 11$ e todo $n \geq 13$.*

Demonstração. Mais uma vez vamos proceder como na prova da Proposição 2.8, tomando $\tilde{A}_{t,2}$ no lugar de A_t. Da desigualdade (2.10), para o caso $q = 4$ e tomando $t = 8$, obtemos $(4,n) \in \mathcal{B}(3,2)$ para $n \geq 163$. A desigualdade $4^{\frac{n}{2}} \geq 6 \cdot \tilde{A}_{t,2}^2 \cdot 4^{\frac{2n}{t}} \cdot W_4(x^n-1)$ com $t = 7$ é válida, para $(4,n) \in \mathcal{B}(3,2)$ tal que $86 \leq n \leq 162$. A desigualdade $4^{\frac{n}{2}} \geq 6 \cdot W(4^n-1)^2 \cdot W_4(x^n-1)$ se verifica para $3 \leq n \leq 85$, exceto se $n \in \{14,15,18,21,30\}$. Do Corolário 2.4, resulta $(4,n) \in \mathcal{B}(3,2)$, para esses valores de n. Finalmente, a condição $4^{\frac{n}{2}} \geq 6W(\ell)^2 W_4(g)\Delta$ do Lema 2.6 se verifica

para $n \in \{11, 14, 15, 18, 21, 30\}$, tomando $\ell = \gcd(4^n - 1, 3 \cdot 5 \cdot 7)$ e g sendo o produto de fatores lineares de $x^n - 1$. □

Proposição 2.17. *Para $q = 5$ e $n \geq 3$, temos $(5, n) \in \mathcal{B}(3, 2)$, para todo $n \geq 13$ e para $n \in \{7, 9, 10, 11\}$.*

Demonstração. De [26, Lemma 2.11], temos $W_5(x^n - 1) \leq 2^{\frac{n}{3}+6}$ e, do Lema 1.81, temos $W(5^n - 1) \leq \tilde{A}_{t,5} \cdot 5^{\frac{n}{t}}$, com um número real $t > 0$. Do Teorema 2.3, resulta que se $5^{\frac{n}{2}} \geq 6W(5^n - 1)^2 W_5(x^n - 1)$, então $(5, n) \in \mathcal{B}(3, 2)$. Dessa forma, $(5, n) \in \mathcal{B}(3, 2)$, se n satisfaz

$$5^{\frac{n}{2}} \geq 6 \cdot \tilde{A}_{t,5}^2 \cdot 5^{\frac{2n}{t}} \cdot 2^{\frac{n}{3}+6},$$

para algum número real $t > 0$. O última desigualdade é equivalente a

$$n \geq \frac{\ln\left(6 \cdot \tilde{A}_{t,5}^2\right) + 6 \ln 2}{(\frac{t-4}{2t}) \ln 5 - \frac{1}{3} \ln 2}, \tag{2.12}$$

quando $(\frac{t-4}{2t}) \ln 5 - \frac{1}{3} \ln 2 > 0$, que é válida, por exemplo, se $t > 5.62$. Para $t = 7.8$, obtemos (2.12) satisfeito para $n \geq 127$. A seguir, verificamos a condição $5^{\frac{n}{2}} \geq 6W(5^n - 1)^2 W_5(x^n - 1)$ do Corolário 2.4, para $3 \leq n \leq 126$ e obtemos $(5, n) \in \mathcal{B}(3, 2)$, para todo $n \geq 25$ e para $n \in \{11, 13, 15, 17, 19, 20, 21, 22, 23\}$. Novamente verificamos a condição $q^{\frac{n}{2}} \geq 6 \cdot W(\ell)^2 \cdot W_5(g) \cdot \Delta$ do Lema 2.6, com $\ell = \mathrm{mdc}(q^n - 1, 2 \cdot 3)$ e g sendo o produto de fatores lineares de $x^n - 1$, e obtemos $(5, n) \in \mathcal{B}(3, 2)$, para $n \in \{7, 9, 14, 16, 18, 24\}$. A mesma desigualdade com $n = 10$, $\ell = 2 \cdot 3$ e $g = 1$ mostra que $(5, 10) \in \mathcal{B}(3, 2)$. □

Proposição 2.18. *Sejam $q \in \{7, 8, 9, 11, 13, 16, 17, 19\}$ e $n \geq 3$. Temos $(q, n) \in \mathcal{B}(3, 2)$, exceto possivelmente para*

$$\begin{gathered}(7,3),(7,4),(7,5),(7,6),(7,8),(7,12),(8,3),(8,4),(8,7),(9,3),(9,4),\\(9,5),(9,6),(9,8),(11,3),(11,4),(11,5),(11,6),(13,3),(13,4),(13,6),\\(16,3),(16,4),(16,5),(17,3),(17,4),(19,3),(19,4),(19,6).\end{gathered}$$

Demonstração. Seja s o número de fatores irredutíveis mônicos de $x^n - 1 \in \mathbb{F}_q[x]$. Dessa forma, $W_q(x^n - 1) = 2^s$ e, de [26, Inequality (2.10)], conseguimos limitar s por

$$s \leq \frac{1}{2}\left(n + \mathrm{mdc}(n, q - 1)\right).$$

Suponha $n \geq 19$. Então $\mathrm{mdc}(n, q - 1) \leq n/2$ e, portanto, $W_q(x^n - 1) \leq 2^{\frac{3n}{4}}$. Seja p a característica de $\mathbb{F}_q$. Do Lema 1.81 e de $p \nmid q^n - 1$, temos $W(q^n - 1) \leq \tilde{A}_{t,p} \cdot (q^n - 1)^{\frac{1}{t}}$ e, do Corolário 2.4, temos se

$$q^{\frac{n}{2}} \geq 6 \cdot \tilde{A}_{t,p}^2 \cdot q^{\frac{2n}{t}} \cdot 2^{\frac{3n}{4}},$$

para algum número real $t > 0$, então $(q, n) \in \mathcal{B}(3, 2)$. A desigualdade acima equivale a

$$n \geq \frac{\ln\left(6 \cdot \tilde{A}_{t.p}^2\right)}{(\frac{t-4}{2t}) \ln q - \frac{3}{4} \ln 2},$$

sempre que $(\frac{t-4}{2t})\ln q - \frac{3}{4}\ln 2 > 0$. Na Tabela 2.2, mostramos os valores de q e intervalos de n para os quais essa desigualdade é válida, junto com o valor de t usado para cada caso.

t	q	n	t	q	n	t	q	n	t	q	n
10.4	7	$n \geq 649$	9.4	9	$n \geq 289$	8.6	13	$n \geq 138$	8.1	17	$n \geq 95$
9.8	8	$n \geq 403$	9	11	$n \geq 186$	8.1	16	$n \geq 100$	8	19	$n \geq 84$

Tabela 2.2: Valores de n, com q e t dados, para os quais $(q, n) \in \mathcal{B}(3, 2)$.

Para $7 \leq q \leq 19$, verificamos a condição $q^{\frac{n}{2}} \geq 6\tilde{A}_{t,p}^2 q^{\frac{2n}{t}} W_q(x^n - 1)$ com $\tilde{A}_{t,p}$ como em (2.11) e com $t = 8$. Para os pares (q, n) que não se encontram na Tabela 2.2 e para aqueles pares que essa condição não é satisfeita, verificamos a desigualdade $q^{\frac{n}{2}} \geq (m_1 + m_2 + 1)W(\ell)^2 W_q(g)\Delta$ do Lema 2.6, tomando $\ell = \mathrm{mdc}(q^n - 1, 2 \cdot 3 \cdot 5)$ e g sendo o produto de fatores lineares de $x^n - 1$. Dessa forma, obtemos $(q, n) \in \mathcal{B}(3, 2)$, com $n \geq 3$, exceto para os seguintes pares:

$$
\begin{gathered}
(7,3),(7,4),(7,5),(7,6),(7,7),(7,8),(7,9),(7,12),\\
(8,3),(8,4),(8,6),(8,7),(9,3),(9,4),(9,5),(9,6),(9,8),\\
(11,3),(11,4),(11,5),(11,6),(11,10),\\
(13,3),(13,4),(13,5),(13,6),(13,8),(13,12),\\
(16,3),(16,4),(16,5),(16,6),(16,45),\\
(17,3),(17,4),(17,6),(17,8),(19,3),(19,4),(19,6).
\end{gathered}
$$

Para esses pares, usamos novamente o Lema 2.6, com $\ell = \gcd(q^n - 1, 2 \cdot 3 \cdot 5)$ e $g = 1$, e obtemos $(q, n) \in \mathcal{B}(3, 2)$, para

$$(q, n) \in \{(7,7),(7,9),(8,6),(11,10),(13,5),(13,8),(16,6),(17,6),(17,8)\}.$$

Também obtemos $(13, 12), (16, 45) \in \mathcal{B}(3, 2)$ usando o Lema 2.6 para $q = 13$ e $n = 12$, tomamos $\ell = 2 \cdot 3 \cdot 5 \cdot 7$ e $g = (x - 1)(x + 1)$, e para $q = 16$ e $n = 45$, tomamos $\ell = 3 \cdot 5 \cdot 7$ e g como sendo o produto de fatores mônicos lineares de $x^n - 1$. □

Os próximos resultados seguem a ideia dada em [5, Propositions 3.3 and 3.4]. Para tal precisaremos do que se segue. Para uma potência de primo q e um inteiro positivo n, denotamos por $\mathfrak{N}(q, n)$ o número de elementos primitivos de $\mathbb{F}_{q^n}$ que são normais sobre $\mathbb{F}_q$.

Proposição 2.19. *Sejam q a potência de um primo e $n \geq 3$. Se $\mathfrak{N}(q, n) \leq m_1 + m_2 + 1$, então $(q, n) \notin \mathcal{B}(m_1, m_2)$.*

Demonstração. Sejam $N = \mathfrak{N}(q, n)$ e $\{\alpha_1, \ldots, \alpha_N\}$ o conjunto de todos os elementos primitivos de $\mathbb{F}_{q^n}$ que são normais sobre $\mathbb{F}_q$. Como $N \leq m_1 + m_2 + 1$, podemos escolher polinômios $f_1(x)$ e $f_2(x)$ de graus m_1 e m_2, respectivamente, tais que $f_1(\alpha_j)f_2(\alpha_j) = 0$, para todo $j = 1, \ldots, N - 1$, $f_1(\alpha_N)f_2(\alpha_N) \neq 0$ e $f(x) = \frac{f_1(x)}{f_2(x)} \in \Upsilon_{q^n}(m_1, m_2)$. Dessa forma, $f(\alpha_j)$ não é primitivo, para todo $j = 1, \ldots, N - 1$, e, tomando $\beta = \frac{1}{f(\alpha_N)}$, temos $h(x) = \beta f(x) \in \Upsilon_{q^n}(m_1, m_2)$ e $h(\alpha_N) = 1$ também não é primitivo. Isso prova que $(q, n) \notin \mathcal{B}(m_1, m_2)$. □

Proposição 2.20. *Sejam $q = 2^k$, $n \geq 3$ e $m = \max\{m_1, m_2\}$. Se*

$$\frac{\mathfrak{N}(q,n)}{m} + \varphi(q^n - 1) > q^n + 1,$$

então $(q,n) \in \mathcal{B}(m_1, m_2)$.

Demonstração. Sejam $f(x) = f_1(x)/f_2(x) \in \Upsilon_{q^n}(m_1, m_2)$ e

$$A_f = \{\alpha \in \mathbb{F}_{q^n} \mid \alpha \text{ primitivo normal sobre } \mathbb{F}_q \text{ e } f_2(\alpha) \neq 0\}.$$

Claramente $|A_f| \geq \mathfrak{N}(q,n) - m_2 \geq \mathfrak{N}(q,n) - m$. Seja $\widetilde{f} : A_f \longrightarrow \mathbb{F}_{q^n}$ definida por $\alpha \longmapsto f(\alpha)$. Dado $\beta \in \widetilde{f}(A_f)$, existem no máximo m elementos $\alpha \in A_f$ tais que $f(\alpha) = \beta$, já que α deve ser uma raiz do polinômio $f_1(x) - \beta f_2(x)$. Assim

$$|\widetilde{f}(A_f)| \geq \frac{\mathfrak{N}(q,n) - m}{m} = \frac{\mathfrak{N}(q,n)}{m} - 1.$$

Como existem $\varphi(q^n - 1)$ elementos primitivos em $\mathbb{F}_{q^n}$, temos que se $\dfrac{\mathfrak{N}(q,n)}{m} - 1 + \varphi(q^n - 1) > q^n$, pelo menos um elemento da forma $f(\alpha)$ é primitivo para algum $\alpha \in A_f$ e o resultado segue. □

Lema 2.21. *Temos $(2,3), (2,4), (2,6), (3,3), (3,4) \notin \mathcal{B}(3,2)$ e $(2,5)$, $(2,7)$, $(2,11)$, $(8,3) \in \mathcal{B}(3,2)$.*

Demonstração. Como $\mathbb{F}_8$ e $\mathbb{F}_{16}$ possuem poucos elementos, verificamos que $\mathfrak{N}(2,3) = 3$ e $\mathfrak{N}(2,4) = 4$. Assim, da Proposição 2.19, obtemos $(2,3), (2,4) \notin \mathcal{B}(3,2)$. Da mesma forma, calcula-se que $\mathfrak{N}(2,5) = 15$, $\mathfrak{N}(2,7) = 49$, $\mathfrak{N}(2,11) = 957$ e $\mathfrak{N}(8,3) = 378$. Logo, pela Proposição 2.20, obtemos $(2,5), (2,7), (2,11), (8,3) \in \mathcal{B}(3,2)$.

Usando o computador, encontramos, para $(q,n) = (2,6)$ e $f(x) = x^2 + x + 1$ (além de muitas outras funções racionais), que para todo elemento primitivo $\alpha \in \mathbb{F}_{q^n}$, normal sobre $\mathbb{F}_q$, $f(\alpha)$ não é primitivo.

Para $(q,n) = (3,3)$ e $f(x) = x^2 + x + 2$ (além de muitas outras funções racionais), temos que para todo elemento primitivo $\alpha \in \mathbb{F}_{q^n}$, normal sobre $\mathbb{F}_q$, $f(\alpha)$ não é primitivo.

Para $(q,n) = (3,4)$, $a \in \mathbb{F}_{q^n}$ tal que $a^4 - a^3 - 1 = 0$ e $f(x) = \frac{ax + 2a^3 + 2a^2 + 1}{x + 2a}$ (além de muitas outras funções racionais), temos que para todo elemento primitivo $\alpha \in \mathbb{F}_{q^n}$ normal sobre $\mathbb{F}_q$, $f(\alpha)$ não é primitivo. □

O próximo teorema resume todos os resultados anteriores.

Teorema 2.22. *Sejam q a potência de um primo e $n \geq 3$. Temos $(q,n) \in \mathcal{B}(3,2)$, exceto possivelmente para*

$$
\begin{aligned}
&n = 3 \quad e \quad q \neq 8 \text{ e } q \leq 37, \text{ ou } q \in \{43, 49, 61, 67, 71, 79, 81, 121, 151, 211, 331\};\\
&n = 4 \quad e \quad q \leq 37 \text{ ou } q \in \{41, 43, 47, 83\};\\
&n = 5 \quad e \quad q \in \{3, 4, 5, 7, 9, 11, 16\};\\
&n = 6 \quad e \quad q \in \{2, 3, 4, 5, 7, 9, 11, 13, 19\};\\
&n = 7 \quad e \quad q \in \{3, 4, 8\};\\
&n = 8 \quad e \quad q \in \{2, 3, 4, 5, 7, 9\};\\
&q = 2 \quad e \quad n \in \{9, 10, 12, 14, 15, 16, 18, 20, 24\};\\
&q = 3 \quad e \quad n \in \{9, 10, 12, 16\};\\
&q = 4 \quad e \quad n \in \{9, 10, 12\}; \quad e \quad (q,n) \in \{(5,12), (7,12)\}.
\end{aligned}
$$

Além disso, $(2,3), (2,4), (2,6), (3,3), (3,4) \notin \mathcal{B}(3,2)$.

Como foi mencionado depois da Definição 2.7, se $n_1 \leq m_1$ e $n_2 \leq m_2$, então $\mathcal{B}(m_1, m_2) \subset \mathcal{B}(n_1, n_2)$. Assim, do Teorema 2.22, também poderíamos encontrar informações sobre os conjuntos $\mathcal{B}(3,1)$, $\mathcal{B}(3,0)$, $\mathcal{B}(2,2)$, $\mathcal{B}(2,1)$, $\mathcal{B}(2,0)$, $\mathcal{B}(1,1)$ e $\mathcal{B}(1,0)$.

CAPÍTULO 3

Progressões aritméticas em corpos finitos

Seja $m \geq 2$ um inteiro positivo. Neste capítulo, discutimos a existência de m termos em progressão aritmética no corpo $\mathbb{F}_{q^n}$, cujos termos são primitivos e pelo menos um deles é normal sobre $\mathbb{F}_q$. É claro que a característica de $\mathbb{F}_q$ deve ser pelo menos m. Obtemos resultados assintóticos e resultados concretos quando $m \geq 4$ ou $m \leq 3$, respectivamente. No caso particular em que $m = 2$ ou $m = 3$ e a razão da progressão aritmética é um elemento de $\mathbb{F}_q$, obtemos a lista completa de exceções. De forma mais específica, no decorrer do capítulo iremos provar os seguintes resultados.

Teorema 3.1. *Sejam q a potência de um número primo, $m, n \geq 2$ inteiros positivos e $\beta \in \mathbb{F}_{q^n}^*$. Existe um elemento $\alpha \in \mathbb{F}_{q^n}$ tal que os elementos $\alpha, \alpha+\beta, \alpha+2\beta, \ldots, \alpha+(m-1)\beta$ são todos primitivos e pelo menos um deles é normal sempre que:*

(i) $m = 2$, *exceto possivelmente para os pares (q, n) na Tabela 3.6, se q for ímpar, e na Tabela 3.8, se q for par.*

(ii) $m = 3$ *e q é ímpar, exceto possivelmente para os pares (q, n) na Tabela 3.3, se $n \geq 7$, além dos pares (q, n) dados no Lema 3.22, se $n = 6$, Lema 3.23 se $n = 5$, Lema 3.24 se $n = 4$, Lema 3.25 se $n = 3$ e Lema 3.26 se $n = 2$.*

(iii) $m = 4$, $\mathrm{mdc}(q, 6) = 1$ *e* $q^n \geq 3.31 \cdot 10^{2821}$.

(iv) $m \geq 5$, $\mathbb{F}_q$ *é de característica maior ou igual a m e q é suficientemente grande.*

A prova baseia-se em somas de caracteres e o método do crivo que proporcionam uma condição de desigualdade que garante a existência de tais progressões aritméticas. O caso $m = 3$ estende os resultados de Cohen *et al.* (ver [13]) sobre três elementos primitivos consecutivos, bem como o caso $m = 2$ que estende os resultados de Cohen (ver [7, 8, 9]) sobre dois elementos primitivos consecutivos.

Para $\beta \in \mathbb{F}_q^*$ e $m = 3$, obtemos uma lista completa de exceções.

Teorema 3.2. *Sejam q uma potência de primo ímpar, $n \geq 2$ e $\beta \in \mathbb{F}_q^*$. Existe um elemento $\alpha \in \mathbb{F}_{q^n}$ tal que os elementos $\alpha, \alpha+\beta, \alpha+2\beta$ são todos primitivos e um deles é normal, exceto para as triplas (q,n,β) na Tabela 3.4.*

Como consequência, temos o seguinte resultado sobre 3 elementos primitivos em progressão aritmética.

Corolário 3.3. *Sejam q uma potência de primo ímpar, $n \geq 2$ e $\beta \in \mathbb{F}_q^*$. Existe um elemento $\alpha \in \mathbb{F}_{q^n}$ tal que os elementos $\alpha, \alpha+\beta, \alpha+2\beta$ são todos primitivos, exceto para as triplas (q,n,β) na Tabela 3.5.*

O caso $\beta = 1$ do corolário acima foi provado por Cohen *et al.* em [13].

Para $\beta \in \mathbb{F}_q^*$ e $m = 2$, também obtemos a lista completa de exceções.

Teorema 3.4. *Sejam q uma potência de primo, $n \geq 2$ e $\beta \in \mathbb{F}_q^*$. Existe um elemento $\alpha \in \mathbb{F}_{q^n}$ tal que os elementos α e $\alpha+\beta$ são ambos primitivos e pelo menos um deles é normal, exceto para $(q,n,\beta) = (2,4,1)$.*

De modo similar ao Corolário 3.3, obtemos o seguinte resultado.

Corolário 3.5. *Sejam q uma potência de primo, $n \geq 2$ e $\beta \in \mathbb{F}_q^*$. Existe um elemento primitivo $\alpha \in \mathbb{F}_{q^n}$ tal que $\alpha+\beta$ é também primitivo.*

O caso $\beta = 1$ do corolário acima foi provado por Cohen em [7, 8, 9].

O capítulo está organizado da seguinte forma. Na Seção 3.1, provamos algumas condições, na forma de desigualdades, que garantem a existência de progressões aritméticas formadas por elementos primitivos tais que pelo menos um elemento da progressão seja normal. Na Seção 3.2, obtemos alguns resultados assintóticos, assim como a prova do Teorema 3.1(iii),(iv). Finalmente, na Seção 3.3 apresentamos a prova dos Teoremas 3.1(ii) e 3.2 e na Seção 3.4 apresentamos a prova dos Teoremas 3.1(i) e 3.4.

3.1 Resultados gerais

Estamos interessados em encontrar condições para a existência de m termos em progressão aritmética, com uma razão dada, de elementos primitivos em $\mathbb{F}_{q^n}$ tais que pelo menos um deles seja normal sobre $\mathbb{F}_q$. Para tal, a seguinte definição exerce um papel importante.

Definição 3.6. *Para $m \geq 2$, seja N_m o conjunto de pares (q,n) tais que, para todo $\beta \in \mathbb{F}_{q^n}^*$ existe um elemento $\alpha \in \mathbb{F}_{q^n}$ para o qual os elementos do conjunto $\{\alpha + (j-1)\beta \mid 1 \leq j \leq m\} \subset \mathbb{F}_{q^n}$ são todos primitivos e pelo menos um deles é normal sobre $\mathbb{F}_q$.*

Observação 3.7. *Veja que $N_m \subset N_{m-1}$. Na realidade, se os m termos da progressão aritmética $\alpha, \alpha+\beta, \ldots, \alpha+(m-1)\beta$ são elementos primitivos e um deles é normal, então as progressões $\alpha, \alpha+\beta, \ldots, \alpha+(m-2)\beta$ e $\alpha+\beta, \alpha+2\beta, \ldots, \alpha+(m-1)\beta$ são ambas compostas de $m-1$ elementos primitivos e em pelo menos uma das progressões há um elemento normal.*

Definição 3.8. *Sejam $e_1, \ldots, e_m$ divisores positivos de $q^n - 1$, g um divisor mônico de $x^n - 1$ em $\mathbb{F}_q[x]$ e $\beta \in \mathbb{F}_{q^n}^*$. Denotemos por $N(e_1, \ldots, e_m, g)$ o número de elementos $\alpha \in \mathbb{F}_{q^n}$ tais que $\alpha + (i-1)\beta$ é e_i-livre, para todo $i \in \{1, \ldots, m\}$ e existe $j \in \{1, \ldots, m\}$ tal que $\alpha + (j-1)\beta$ é g-livre.*

Definição 3.9. *Com as notações da definição anterior e para todo $j \in \{1, \ldots, m\}$, denotemos por $N_j(e_1, \ldots, e_m, g)$ o número de elementos $\alpha \in \mathbb{F}_{q^n}$ tais que $\alpha + (i-1)\beta$ é e_i-livre, para todo $i \in \{1, \ldots, m\}$ e $\alpha + (j-1)\beta$ é g-livre.*

Denotaremos $\bar{e} = (e_1, \ldots, e_m)$ e $W(\bar{e}) = \prod_{i=1}^m W(e_i)$. Assim por exemplo, quando $\bar{e} = \overline{q^n - 1}$, temos $e_i = q^n - 1$, para todo $i \in \{1, \ldots, m\}$.

Observe que os conjuntos $N(\bar{e}, g)$ e $N_j(\bar{e}, g)$ dependem também de β.

Observação 3.10. *Das Definições 3.8 e 3.9 temos*

$$N(\bar{e}, g) \geq \frac{1}{m} \sum_{j=1}^{m} N_j(\bar{e}, g).$$

O próximo teorema é o resultado principal da seção.

Teorema 3.11. *Sejam q a potência de um primo, $n \geq 2$ um inteiro, $e_1, \ldots, e_m \in \mathbb{N}$ divisores de $q^n - 1$ e $g \in \mathbb{F}_q[x]$ um divisor mônico de $x^n - 1$. Se*

$$q^{\frac{n}{2}} \geq m W_q(g) W(\bar{e}),$$

então $N(\bar{e}, g) > 0$ para todo $\beta \in \mathbb{F}_{q^n}^*$. Em particular, se

$$q^{\frac{n}{2}} \geq m W_q(x^n - 1) W(\overline{q^n - 1}),$$

então $(q, n) \in N_m$.

Demonstração. Seja $\beta \in \mathbb{F}_{q^n}^*$. Vamos encontrar uma cota inferior para $N(\bar{e}, g)$. Das definições de ρ_s e κ_g, das Definições 3.8 e 3.9 e da Observação 3.10, temos

$$N(\bar{e}, g) \geq \frac{1}{m} \sum_{\alpha \in \mathbb{F}_{q^n} \setminus A} \left[\prod_{i=1}^{m} \rho_{e_i}(\alpha + (i-1)\beta) \sum_{j=1}^{m} \kappa_g(\alpha + (j-1)\beta) \right],$$

sendo $A = \{-(i-1)\beta \mid 1 \leq i \leq m\}$. Das Proposições 1.72 e 1.77 segue

$$N(\bar{e}, g) \geq \frac{1}{m} \Theta_q(g) \theta(\bar{e}) \sum_{\bar{d} \mid \bar{e}} \sum_{h \mid g} \frac{\mu(\bar{d})}{\varphi(\bar{d})} \frac{\mu_q(h)}{\phi_q(h)} \sum_{\substack{\operatorname{ord}(\eta_i) = d_i \\ 1 \leq i \leq m}} \sum_{\operatorname{Ord}(\psi) = h} S(\bar{\eta}, \psi), \tag{3.1}$$

com $\theta(\bar{e}) = \prod_{i=1}^m \theta(e_i)$, $\mu(\bar{d}) = \prod_{i=1}^m \mu(d_i)$, $\varphi(\bar{d}) = \prod_{i=1}^m \varphi(d_i)$, $\bar{\eta} = (\eta_1, \ldots, \eta_m)$, $\bar{d} \mid \bar{e}$ quer dizer $d_i \mid e_i$, para todo $i \in \{1, \ldots, m\}$ e

$$S(\bar{\eta}, \psi) = \sum_{\alpha \in \mathbb{F}_{q^n} \setminus A} \left(\eta_1(\alpha) \cdots \eta_m(\alpha + (m-1)\beta) \sum_{j=1}^{m} \psi(\alpha + (j-1)\beta) \right).$$

Agora vamos separar os possíveis valores de $\bar{d}$ e h em quatro casos.

- Para $\bar{d} = \bar{1}$ e $h = 1$, temos $S(\eta_{\bar{0}}, \psi_0) = m(q^n - m)$, lembrando que η_0 é o caracter multiplicativo trivial, ψ_0 é o caracter aditivo trivial e $\eta_{\bar{0}} = (\eta_0, \dots, \eta_0)$.

- Para $\bar{d} \neq \bar{1}$ and $h = 1$, considere η o gerador do grupo de caracteres multiplicativos (ver Teorema 1.61). Assim, para todo $i \in \{1, \dots, m\}$, existe um inteiro $n_i \in \{0, 1, \dots, q^n - 2\}$ tal que $\eta_i(\alpha) = \eta(\alpha^{n_i})$, para todo $\alpha \in \mathbb{F}_{q^n}^*$. Observe que $(n_1, \dots, n_m) \neq \bar{0}$, já que $\bar{d} \neq \bar{1}$. Dessa forma, temos

$$|S(\bar{\eta}, \psi_0)| = \left| m \sum_{\alpha \in \mathbb{F}_{q^n} \setminus A} \eta_1(\alpha) \cdots \eta_m(\alpha + (m-1)\beta) \right| = m \left| \sum_{\alpha \in \mathbb{F}_{q^n} \setminus A} \eta(F(\alpha)) \right|,$$

  com $F(\alpha) = \prod_{i=1}^{m} (\alpha + (i-1)\beta)^{n_i}$. Observe que não existe $G \in \overline{\mathbb{F}}_q(x)$ satisfazendo $F(x) = G(x)^{q^n - 1}$, já que existe pelo menos um $i \in \{1, \dots, m\}$ tal que $1 \leq n_i \leq q^n - 2$. Portanto, podemos aplicar o Lema 1.79(a), obtendo $|S(\bar{\eta}, \psi_0)| \leq m(m-1)q^{\frac{n}{2}}$.

- Para $\bar{d} = \bar{1}$ e $h \neq 1$, do Teorema 1.58, segue

$$|S(\eta_{\bar{0}}, \psi_h)| = \left| \sum_{j=1}^{m} \psi_h(\beta)^{j-1} \right| \cdot \left| - \sum_{\alpha \in A} \psi(\alpha) \right| \leq m^2.$$

- Para $\bar{d} \neq \bar{1}$ e $h \neq 1$, segue

$$\begin{aligned} |S(\bar{\eta}, \psi)| &= \left| \sum_{j=1}^{m} \sum_{\alpha \in \mathbb{F}_{q^n} \setminus A} \prod_{i=1}^{m} \eta_i(\alpha + (i-1)\beta)\, \psi(\alpha + (j-1)\beta) \right| \\ &\leq \sum_{j=1}^{m} \left| \psi((j-1)\beta) \sum_{\alpha \in \mathbb{F}_{q^n} \setminus A} \prod_{i=1}^{m} \eta_i(\alpha + (i-1)\beta)\, \psi(\alpha) \right| \\ &\leq m \left| \sum_{\alpha \in \mathbb{F}_{q^n} \setminus A} \eta(F(\alpha)) \psi(\alpha) \right|, \end{aligned}$$

  com $F(\alpha) = \prod_{i=1}^{m} (\alpha + (i-1)\beta)^{n_i}$ e $(n_1, \dots, n_m)$ o conjunto de inteiros positivos que definimos antes. Usando o Lema 1.79(b), com $D_1 \leq m$, $D_2 = 1$ e $D_3 = D_4 = 0$, temos $|S(\bar{\eta}, \psi)| \leq m^2 q^{\frac{n}{2}}$.

Podemos reescrever o lado direito da desigualdade (3.1) como

$$\frac{1}{m} \Theta_q(g) \theta(\bar{e}) (S_1 + S_2 + S_3 + S_4),$$

com

$$S_1 = S(\eta_{\bar{0}}, \psi_0) = m(q^n - m), \qquad S_2 = \sum_{\substack{\bar{d} \mid \bar{e} \\ \bar{d} \neq \bar{1}}} \frac{\mu(\bar{d})}{\varphi(\bar{d})} \sum_{\substack{\mathrm{ord}(\eta_i) = d_i \\ 1 \leq i \leq m}} S(\bar{\eta}, \psi_0),$$

$$S_3 = \sum_{\substack{h \mid g \\ h \neq 1}} \frac{\mu_q(h)}{\phi_q(h)} \sum_{\mathrm{Ord}(\psi) = h} S(\eta_{\bar{0}}, \psi) \text{ e } \quad S_4 = \sum_{\substack{\bar{d} \mid \bar{e} \\ \bar{d} \neq \bar{1}}} \sum_{\substack{h \mid g \\ h \neq 1}} \frac{\mu(\bar{d})}{\varphi(\bar{d})} \frac{\mu_q(h)}{\phi_q(h)} \sum_{\substack{\mathrm{ord}(\eta_i) = d_i \\ 1 \leq i \leq m}} \sum_{\mathrm{Ord}(\psi) = h} S(\bar{\eta}, \psi).$$

Das considerações acima, usando que existem $\varphi(d)$ caracteres multiplicativos de ordem d e $\phi_q(h)$ caracteres aditivos de $\mathbb{F}_q$-ordem h, obtemos

$$\begin{aligned} S_1+S_2+S_3+S_4 &\geq S_1-|S_2|-|S_3|-|S_4| \\ &\geq m(q^n-m)-m(m-1)q^{\frac{n}{2}}(W(\bar{e})-1) \\ &\quad -m^2(W_q(g)-1)-m^2q^{\frac{n}{2}}(W_q(g)-1)(W(\bar{e})-1) \\ &> mq^n-m^2q^{\frac{n}{2}}(W_q(g)W(\bar{e})-1)+mq^{\frac{n}{2}}(W(\bar{e})-1)-m^2 \\ &\geq mq^n-m^2q^{\frac{n}{2}}(W_q(g)W(\bar{e})-1), \end{aligned}$$

já que $m^2 \leq mq^{\frac{n}{2}}$. Assim, se $q^{\frac{n}{2}} \geq mW_q(g)W(\bar{e})$, então $N(\bar{e},g)>0$. Em particular, se $q^{\frac{n}{2}} \geq mW_q(x^n-1)W(q^n-1)^m$, então $N(\overline{q^n-1},x^n-1)>0$, para todo $\beta \in \mathbb{F}_{q^n}^*$. Isso implica que se essa desigualdade é válida, então $(q,n)\in N_m$. □

A técnica do crivo dos próximos dois resultados é semelhante ao do capítulo anterior e outros que apareceram em trabalhos anteriores sobre elementos primitivos ou normais.

Lema 3.12. *Sejam q a potência de um primo, $n\geq 2$ um inteiro e $j\in\{1,\dots,m\}$. Sejam e um divisor positivo de q^n-1 e $\{p_1,\dots,p_r\}$ o conjunto de todos os primos que dividem q^n-1, mas que não dividem e. Sejam também $g\in\mathbb{F}_q[x]$ um divisor mônico de x^n-1 e $\{h_1,\dots,h_s\}\subset\mathbb{F}_q[x]$ o conjunto de todos os polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$ que dividem x^n-1, mas que não dividem g. Então*

$$\begin{aligned} N_j(\overline{q^n-1},x^n-1) &\geq \sum_{i=1}^{r}N_j(p_ie_1,e_2,\dots,e_m,g)+\sum_{i=1}^{r}N_j(e_1,p_ie_2,e_3,\dots,e_m,g) \\ &\quad +\cdots+\sum_{i=1}^{r}N_j(e_1,\dots,e_{m-1},p_ie_m,g)+\sum_{i=1}^{s}N_j(\bar{e},h_ig) \\ &\quad -(mr+s-1)N_j(\bar{e},g). \end{aligned} \tag{3.2}$$

Demonstração. O lado esquerdo de (3.2) conta cada $\alpha\in\mathbb{F}_{q^n}$ para os quais $\alpha+(i-1)\beta$ é primitivo, para todo $i\in\{1,\dots,m\}$ e $\alpha+(j-1)\beta$ é normal. Observe que se α é um desses elementos, então $\alpha+(i-1)\beta$ é e_i-livre, p_te_i-livre para todo $i\in\{1,\dots,m\}$ e todo $t\in\{1,\dots,r\}$. Além disso $\alpha+(j-1)\beta$ é g-livre e h_ig-livre para todo $i\in\{1,\dots,s\}$. Assim, α é contado $(mr+s)-(mr+s-1)=1$ vez no lado direito de (3.2). Para qualquer outro $\alpha\in\mathbb{F}_{q^n}$, temos que ou $\alpha+(i-1)\beta$ não é p_te_i-livre, para algum $i\in\{1,\dots,m\}$ e algum $t\in\{1,\dots,r\}$, ou $\alpha+(j-1)\beta$ não é h_ig-livre para algum $i\in\{1,\dots,s\}$. Nesse caso α não é contado em pelo menos uma das primeiras $m+1$ somas do lado direito de (3.2). □

Proposição 3.13. *Sejam q a potência de um primo e $n\geq 2$ um inteiro. Sejam e um divisor positivo de q^n-1 e $\{p_1,\dots,p_r\}$ o conjunto de todos os primos que dividem q^n-1, mas que não dividem e. Sejam também $g\in\mathbb{F}_q[x]$ um divisor mônico de x^n-1 e $\{h_1,\dots,h_s\}\subset\mathbb{F}_q[x]$ o conjunto de todos os polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$ que dividem x^n-1, mas que não dividem g. Suponha $\delta=1-m\sum_{i=1}^{r}\frac{1}{p_i}-\sum_{i=1}^{s}\frac{1}{q^{\deg h_i}}>0$ e seja $\Delta=2+\frac{mr+s-1}{\delta}$. Se $q^{\frac{n}{2}}\geq mW_q(g)W(e)^m\Delta$, então $N(\overline{q^n-1},x^n-1)>0$.*

Demonstração. Seja $j \in \{1, \ldots, m\}$. Reescrevemos a desigualdade (3.2) na forma

$$\begin{aligned} N_j(\overline{q^n-1}, x^n-1) \geq & \sum_{i=1}^{r}\Big[N_j(p_ie_1, e_2, \ldots, e_m, g) - \theta(p_i)N_j(\bar{e}, g)\Big] \\ & + \sum_{i=1}^{r}\Big[N_j(e_1, p_ie_2, e_3, \ldots, e_m, g) - \theta(p_i)N_j(\bar{e}, g)\Big] \\ & + \cdots + \\ & + \sum_{i=1}^{r}\Big[N_j(e_1, \ldots, e_{m-1}, p_ie_m, g) - \theta(p_i)N_j(\bar{e}, g)\Big] \\ & + \sum_{i=1}^{s}\Big[N_j(\bar{e}, h_ig) - \Theta_q(h_i)N_j(\bar{e}, g)\Big] + \delta N_j(\bar{e}, g) \end{aligned}$$

com $e = e_1 = \cdots = e_m$.

Seja $i \in \{1, \ldots, r\}$. Das Proposições 1.72, 1.77, da Definição 3.9 e levando em consideração que θ é uma função multiplicativa, obtemos

$$\begin{aligned} N_j(p_ie_1, e_2, \ldots, e_m, g) &= \Theta_q(g)\theta(p_i)\theta(\bar{e}) \sum_{\substack{d_1|p_ie_1 \\ d_t|e_t \\ t\in\{2,\ldots,m\}}} \sum_{h|g} \frac{\mu(\bar{d})}{\varphi(\bar{d})}\frac{\mu_q(h)}{\phi_q(h)} \sum_{\substack{\mathrm{ord}(\eta_i)=d_i \\ 1\leq i\leq m}} \sum_{\mathrm{Ord}(\psi)=h} S_j(\bar{\eta}, \psi) \\ &= \theta(p_i)N_j(\bar{e}, g) \\ &\quad + \Theta_q(g)\theta(p_i)\theta(\bar{e}) \sum_{\substack{d_1|p_ie_1 \\ p_i|d_1 \\ d_t|e_t \\ t\in\{2,\ldots,m\}}} \sum_{h|g} \frac{\mu(\bar{d})}{\varphi(\bar{d})}\frac{\mu_q(h)}{\phi_q(h)} \sum_{\substack{\mathrm{ord}(\eta_i)=d_i \\ 1\leq i\leq m}} \sum_{\mathrm{Ord}(\psi)=h} S_j(\bar{\eta}, \psi), \end{aligned}$$

com

$$S_j(\bar{\eta}, \psi) = \sum_{\alpha\in\mathbb{F}_{q^n}\setminus A} \eta_1(\alpha)\cdots\eta_m(\alpha+(m-1)\beta)\psi(\alpha+(j-1)\beta).$$

Como na prova do Teorema 3.11, reescrevemos $\eta_1(\alpha)\cdots\eta_m(\alpha+(m-1)\beta) = \eta(F(\alpha))$, com $F(\alpha) = \prod_{i=1}^{m}(\alpha+(i-1)\beta)^{n_i}$, $(n_1, \ldots, n_m)$ o conjunto de inteiros positivos definidos nesse teorema e η um gerador do grupo de caracteres multiplicativos.

Dessa forma vemos que se ψ for o caracter aditivo trivial, do Lema 1.79(a), temos $|S_j(\bar{\eta}, \psi)| \leq (m-1)q^{\frac{n}{2}}$ e se ψ não for o caracter aditivo trivial, do Lema 1.79(b), temos $|S_j(\bar{\eta}, \psi)| \leq mq^{\frac{n}{2}}$. Assim,

$$|N_j(p_ie_1, e_2, \ldots, e_m, g) - \theta(p_i)N_j(\bar{e}, g)| \leq \Theta_q(g)\theta(p_i)\theta(\bar{e})mq^{\frac{n}{2}}W_q(g)W(\bar{e}).$$

De forma similar, para todo $t \in \{1, \ldots, m\}$, temos

$$|N_j(e_1, \ldots p_ie_t, \ldots, e_m, g) - \theta(p_i)N_j(\bar{e}, g)| \leq \Theta_q(g)\theta(p_i)\theta(\bar{e})mq^{\frac{n}{2}}W_q(g)W(\bar{e}).$$

Seja $i \in \{1, \ldots, s\}$. Mais uma vez, das Proposições 1.72, 1.77, da Definição 3.9 e levando em consideração que

Θ_q é uma função multiplicativa, temos

$$\begin{aligned} N_j(\bar{e}, h_i g) &= \Theta_q(h_i)\Theta_q(g)\theta(\bar{e}) \sum_{\bar{d}|\bar{e}} \sum_{h|h_i g} \frac{\mu(\bar{d})}{\varphi(\bar{d})} \frac{\mu_q(h)}{\phi_q(h)} \sum_{\substack{\text{ord}(\eta_i)=d_i \\ 1\le i\le m}} \sum_{\text{Ord}(\psi)=h} S_j(\bar{\eta}, \psi) \\ &= \Theta_q(h_i) N_j(\bar{e}, g) \\ &\quad + \Theta_q(h_i)\Theta_q(g)\theta(\bar{e}) \sum_{\bar{d}|\bar{e}} \sum_{\substack{h|h_i g \\ h_i|h}} \frac{\mu(\bar{d})}{\varphi(\bar{d})} \frac{\mu_q(h)}{\phi_q(h)} \sum_{\substack{\text{ord}(\eta_i)=d_i \\ 1\le i\le m}} \sum_{\text{Ord}(\psi)=h} S_j(\bar{\eta}, \psi). \end{aligned}$$

Do Lema 1.79(b), temos $|S_j(\eta_{\bar{d}}, \psi_h)| \le mq^{\frac{n}{2}}$. Logo,

$$|N_j(\bar{e}, h_i g) - \Theta_q(h_i) N_j(\bar{e}, g)| \le \Theta_q(h_i)\Theta_q(g)\theta(\bar{e}) m q^{\frac{n}{2}} W_q(g) W(\bar{e}).$$

Combinando todas as desigualdades anteriores, obtemos

$$\begin{aligned} N_j(\overline{q^n - 1}, x^n - 1) &\ge \delta N_j(\bar{e}, g) \\ &\quad - \Theta_q(g)\theta(\bar{e}) W_q(g) W(\bar{e}) m q^{\frac{n}{2}} \left(m \sum_{i=1}^{r} \theta(p_i) + \sum_{i=1}^{s} \Theta_q(h_i) \right). \end{aligned}$$

Portanto, seguindo as mesmas ideias da prova do Teorema 3.11, temos

$$N_j(\bar{e}, g) > \Theta_q(g)\theta(\bar{e})(q^n - m q^{\frac{n}{2}} W_q(g) W(\bar{e}))$$

e

$$\begin{aligned} N_j(\overline{q^n - 1}, x^n - 1) &> \Theta_q(g)\theta(\bar{e}) q^{\frac{n}{2}} \Bigg[\delta(q^{\frac{n}{2}} - m W_q(g) W(\bar{e})) \\ &\quad - m W_q(g) W(\bar{e}) \left(m \sum_{i=1}^{r} \theta(p_i) + \sum_{i=1}^{s} \Theta_q(h_i) \right) \Bigg] \\ &= \delta \Theta_q(g)\theta(\bar{e}) q^{\frac{n}{2}} \left(q^{\frac{n}{2}} - m W_q(g) W(\bar{e}) \Delta \right). \end{aligned}$$

Substituindo $W(\bar{e}) = W(e)^m$ e levando em consideração a Observação 3.10, obtemos o resultado desejado. □

O próximo resultado, sobre o caso $n = 2$, é utilizado para melhorar a cota obtida no Teorema 3.11, para esse caso particular.

Proposição 3.14. *Para toda potência de primo q, se $\alpha \in \mathbb{F}_{q^2}$ é primitivo, então α é normal sobre $\mathbb{F}_q$.*

Demonstração. Suponha que α não seja normal. Assim, $\{\alpha, \alpha^q\}$ é linearmente dependente sobre $\mathbb{F}_q$, o que implica $\frac{\alpha^q}{\alpha} \in \mathbb{F}_q$. Portanto, $\alpha^{(q-1)^2} = (\alpha^{q-1})^{q-1} = 1$. Já que $(q-1)^2 < q^2 - 1$, temos que α não é primtivo, contradição. □

Observação 3.15. *Da Proposição 3.14 e [13, Theorem 3], se $q \ge (m-1)W(q^2-1)^m$, então $(q, 2) \in N_m$ e de [13,*

Theorem 5], se $q > (m-1)\left(\frac{mr-1}{\delta}+2\right)W(e)^m$, *então* $(q,2) \in N_m$ *com* e *um divisor positivo* q^2-1 *e* $\delta = 1-m\sum_{i=1}^{r}\frac{1}{p_i} > 0$, *no qual* $p_1,\ldots,p_r$ *(para* $r \geq 0$*) são os primos que dividem* q^2-1, *mas que não dividem* e.

Na realidade, [13, Theorem 3] e [13, Theorem 5] tratam do caso $\beta = 1$, *mas se observamos atentamente a demonstração desses teoremas, vemos que os resultados funcionam para todo* $\beta \in \mathbb{F}_q^*$.

3.2 Resultados assintóticos

Para aplicar o Teorema 3.11, de forma a obter resultados assintóticos, usaremos (além de outros resultados) casos particulares da Proposição 1.82.

Corolário 3.16. *Seja* u *um inteiro positivo. Se* $u \geq 7.51 \cdot 10^{358}$, *então* $W(u) \leq u^{\frac{1}{8}}$. *Se* $u \geq 1.39 \cdot 10^{1424}$, *então* $W(u) \leq u^{\frac{1}{10}}$. *Se* $u \geq 3.31 \cdot 10^{2821}$, *então* $W(u) \leq u^{\frac{1}{11}}$.

Demonstração. Se consideramos $r = 149$, obtemos $P_{149} < 7.51 \cdot 10^{358}$ e $\frac{1}{8} > \frac{149\log 2}{\log P_{149}}$. Se consideramos $r = 473$, obtemos $P_{473} < 1.39 \cdot 10^{1424}$ e $\frac{1}{10} > \frac{473\log 2}{\log P_{473}}$. Se consideramos $r = 852$, obtemos $P_{852} < 3.31 \cdot 10^{2821}$ e $\frac{1}{11} > \frac{852\log 2}{\log P_{852}}$. O resultado segue diretamente da Proposição 1.82. □

Podemos agora enunciar os primeiros resultados assintóticos para $m = 2$ e para $m = 3$.

Proposição 3.17. *Sejam* q *a potência de um primo e* $n \geq 2$ *um inteiro. Se* $q^n \geq 7.51 \cdot 10^{358}$, *então* $(q,n) \in N_2$.

Demonstração. Do Lema 1.83, existem inteiros não negativos a, b, que dependem de q, tais que $W_q(x^n-1) \leq 2^{\frac{n}{a}+b}$ e, com o resultado do Corolário 3.16, quando $q^n \geq 7.51 \cdot 10^{358}$, temos $2W_q(x^n-1)W(q^n-1)^2 \leq 2 \cdot 2^{\frac{n}{a}+b} \cdot q^{\frac{n}{4}}$. Assim, pelo Teorema 3.11, se $q^{\frac{n}{2}} \geq 2 \cdot 2^{\frac{n}{a}+b} \cdot q^{\frac{n}{4}}$ (que equivale a $\left(\frac{q}{2^{\frac{4}{a}}}\right)^n \geq 2^{4b+4}$), então $(q,n) \in N_2$. Seja c um inteiro positivo e suponha $q \geq c = 2^{\log_2 c}$. Se $1-\frac{4}{a}\log_c 2 > 0$, obtemos

$$\frac{q}{2^{\frac{4}{a}}} \geq q^{1-\frac{4}{a}\log_c 2}.$$

Assim, se

$$(q^n)^{1-\frac{4}{a}\log_c 2} \geq 2^{4b+4} \tag{3.3}$$

e $1-\frac{4}{a}\log_c 2 > 0$, então $\left(\frac{q}{2^{\frac{4}{a}}}\right)^n \geq 2^{4b+4}$. Observe que, para $q \geq 17$, $c = 17$, $a = 1$ e $b = 0$, para $5 \leq q \leq 16$, $c = q$, $a = 2$ e $b = \frac{q-1}{2}$, para $3 \leq q \leq 4$, $c = q$, $a = 3$ e $b = \frac{q^2+3q-4}{6}$ e para $q = 2$, $c = 2$, $a = 5$ e $b = \frac{14}{5}$, temos $1-\frac{4}{a}\log_c 2 > 0$ e (3.3). Isso prova que $(q,n) \in N_2$ para todo par satisfazendo $q^n \geq 7.51 \cdot 10^{358}$. □

Proposição 3.18. *Sejam* q *a potência de um primo e* $n \geq 2$ *um inteiro. Se* $q^n \geq 1.39 \cdot 10^{1424}$, *então* $(q,n) \in N_3$.

Demonstração. Do Lema 1.83, existem inteiros negativos a, b, que dependem de q, tais que $W_q(x^n-1) \leq 2^{\frac{n}{a}+b}$. Por outro lado, pelo Corolário 3.16, se $q^n \geq 1.39 \cdot 10^{1424}$, então $W_q(q^n-1) < q^{\frac{n}{10}}$. Assim, $3W_q(x^n-1)W(q^n-1)^3 \leq$

$3 \cdot 2^{\frac{n}{a}+b} \cdot q^{\frac{3n}{10}}$. Portanto, pelo Teorema 3.11, se provarmos $q^{\frac{n}{2}} \geq 3 \cdot 2^{\frac{n}{a}+b} \cdot q^{\frac{3n}{10}}$, então $(q,n) \in N_3$. Essa última desigualdade é equivalente a $\left(\frac{q}{2^{\frac{5}{a}}}\right)^n \geq 3^5 \cdot 2^{5b}$. Como na prova da proposição anterior, seja c um inteiro positivo e suponha $q \geq c = 2^{\log_2 c}$. Se $1 - \frac{5}{a}\log_c 2 > 0$, então $\frac{q}{2^{\frac{5}{a}}} \geq q^{1-\frac{5}{a}\log_c 2}$ e, nesse caso,

$$(q^n)^{1-\frac{5}{a}\log_c 2} \geq 3^5 \cdot 2^{5b} \tag{3.4}$$

implica $q^{\frac{n}{2}} \geq 3 \cdot 2^{\frac{n}{a}+b} \cdot q^{\frac{3n}{10}}$. Se $c = 7$ e supondo $q \leq 31$, temos $n \geq \frac{\log(1.39\cdot 10^{1424})}{\log 31} > 954$, já que $q^n \geq 1.39 \cdot 10^{1424}$. Assim, $\mathrm{mdc}(n, q-1) \leq q-1 \leq \frac{30}{954}n < \frac{1}{30}n$ e, do Lema 1.84, obtemos $W_q(x^n-1) \leq 2^{\frac{31n}{60}}$. Dessa forma, para $q \geq 37$, $c = 37$, $a = 1$ e $b = 0$, para $7 \leq q \leq 16$, $c = 7$, $a = \frac{60}{31}$ e $b = 0$, para $q = 5$, $c = 5$, $a = 3$ e $b = 6$ e para $q = 3$, $c = 3$, $a = 4$, $b = 5$, temos $1 - \frac{5}{a}\log_c 2 > 0$ e (3.4). Isso conclui a prova. □

Também podemos usar a Proposição 1.82 de forma a obter resultados assintóticos para $m = 4$, o que prova o Teorema 3.1(iii).

Proposição 3.19. *Sejam q a potência de um primo ímpar não múltiplo de 3 e $n \geq 2$ um inteiro. Se $q^n \geq 3.31 \cdot 10^{2821}$, então $(q,n) \in N_4$.*

Demonstração. Como nos casos anteriores usamos o Lema 1.83, o Corolário 3.16 e o Teorema 3.11, para obter que para determinados valores de a, b e c, se $q^n \geq 3.31 \cdot 10^{2821}$, $1 - \frac{22}{3a}\log_c 2 > 0$ e

$$(q^n)^{1-\frac{22}{3a}\log_c 2} \geq 2^{\frac{22(b+2)}{3}}, \tag{3.5}$$

então $(q,n) \in N_4$. Observe primeiro que se $q \leq 157$, então $n \geq \frac{3.31\cdot 10^{2821}}{\log 157} > 1284$, já que $q^n \geq 3.31 \cdot 10^{2821}$. Assim, $\mathrm{mdc}(n, q-1) \leq q-1 \leq \frac{156}{1285}n < \frac{1}{8}n$ e, do Lema 1.84, obtemos $W_q(x^n-1) \leq 2^{\frac{9n}{16}}$, o que quer dizer que nesse caso podemos escolher $a = \frac{16}{9}$ e $b = 0$. Como não há potências de primos entre 159 e 163, verificamos que $1 - \frac{22}{3a}\log_c 2 > 0$ e (3.5) são válidos para $q \geq 163$ e $(a,b,c) = (1,0,163)$, para $19 \leq q \leq 157$ e $(a,b,c) = (\frac{16}{9},0,19)$, para $q = 17$ e $(a,b,c) = (2,8,17)$, para $q \in \{7,9,11,13\}$ e $(a,b,c) = (3, \frac{q^2+3q-4}{6}, q)$, para $q = 5$ e $(a,b,c) = (4,8,5)$ e para $q = 3$ e $(a,b,c) = (5, \frac{51}{5}, 3)$. Isso conclui a prova. □

Para $m > 4$ o resultado seguinte prova o Teorema 3.1(iv).

Proposição 3.20. *Sejam q a potência de um primo ímpar e n, m inteiros positivos tais que $n \geq 2$ e $m \geq 5$. Existem constantes $c(m)$ e $q_0(m)$, que dependem de m , para as quais se $q \geq c(m)$, $q^n \geq q_0(m)$ e a característica de $\mathbb{F}_q$ é maior ou igual a m, então $(q,n) \in N_m$.*

Demonstração. Da Proposição 1.82, existe uma constante $q_0(m)$ tal que, para todo $u \geq q_0(m)$, temos $W(u) \leq u^{\frac{1}{2(m+1)}}$ e, neste caso, $mW_q(x^n-1)W(q^n-1)^m \leq m \cdot 2^n \cdot q^{\frac{mn}{2(m+1)}}$. Como $q^{\frac{n}{2}} \geq m \cdot 2^n \cdot q^{\frac{mn}{2(m+1)}}$ é equivalente a $\left(\frac{q}{2^{2(m+1)}}\right)^n \geq m^{2(m+1)}$, do Teorema 3.11, se a última desigualdade se verifica, então $(q,n) \in N_m$. Vamos provar que se $q \geq c(m) := 2^{4(m+1)}$, então $\left(\frac{q}{2^{2(m+1)}}\right)^n \geq m^{2(m+1)}$.

Da Proposição 1.82, podemos escolher $q_0(m) = P_r$, com r um inteiro positivo que satisfaz $\frac{1}{2(m+1)} \geq \frac{r \log 2}{\log P_r}$ e, por conseguinte, $P_r \geq 2^{2r(m+1)}$. Isso implica que o r-ésimo primo p_r satisfaz $p_r \geq 2^{2(m+1)} > m^2$. De [4, Theorem 4.6], temos $\pi(2^r) > \frac{2^r}{6 \log 2^r} > r$, já que $r > 8$ (na verdade, como $m \geq 5$, da Proposição 3.19, temos $r \geq 852$). Dessa forma, $m^2 < p_r < 2^r$. Colocando todas as informações juntas, obtemos

$$\left(\frac{q}{2^{2(m+1)}}\right)^n \geq q^{\frac{n}{2}} \geq P_r^{\frac{1}{2}} \geq 2^{r(m+1)} > m^{2(m+1)},$$

para todo $q \geq c(m)$. □

3.3 O caso $m = 3$

Nessa seção vamos tomar $m = 3$. Comecemos usando a técnica do crivo para abaixar a cota inferior da Proposição 3.18. Usaremos as seguintes notações. Para inteiros positivos k e r denotamos por $\mathcal{P}(k, r)$ como sendo o produto dos r primeiros números primos maiores ou iguais a k e por $\mathcal{S}(k, r)$ a soma dos inversos desses primos.

Proposição 3.21. *Sejam q a potência de um primo ímpar e $n \geq 2$ um inteiro. Se $q^n \geq 3.422 \cdot 10^{40}$ ou se $q \geq 37$ e $q^n \geq 7.391 \cdot 10^{38}$, então $(q, n) \in N_3$.*

Demonstração. Vamos usar a notação da Proposição 3.13. Suponha $q^n < 1.39 \cdot 10^{1424}$, pois já temos $(q, n) \in N_3$, para $q^n \geq 1.39 \cdot 10^{1424}$. Sejam e o produto dos números primos menores que 353 que dividem $q^n - 1$ e r o número de primos maiores ou iguais a 353 que dividem $q^n - 1$. Como $\mathcal{P}(353, r) < q^n - 1 < 1.39 \cdot 10^{1424}$, temos $r \leq 442$. Se $u = \omega(e)$, então $u \leq 70$, já que há 70 números primos menores que 353. Defina $r(u) = \max\{r \mid \mathcal{P}_u \cdot \mathcal{P}(353, r) \leq 1.39 \cdot 10^{1424}\}$, com $\mathcal{P}_u$ o produto dos primeiros u números primos. Sejam também $\delta(353, r(u)) = 1 - 3\mathcal{S}(353, r(u))$ e $\Delta(353, r(u)) = 2 + \dfrac{3r(u) - 1}{\delta(353, r(u))}$. Sejam δ e Δ como na Proposição 3.13, com $g = x^n - 1$. Observe que $r \leq r(u) \leq r(0) = 442$ e $\delta \geq \delta(353, r(u)) \geq \delta(353, r(0)) > 0$. Assim, podemos utilizar a Proposição 3.13.

Como na Proposição 3.18, seja c um inteiro positivo e suponha $q \geq c$. Existem inteiros não negativos a, b, que dependem de q, tais que $W_q(x^n - 1) \leq 2^{\frac{n}{a}+b}$. Assim, temos $3W_q(x^n - 1)W(e)^3\Delta \leq 3 \cdot 2^{\frac{n}{a}+b} \cdot 2^{3u} \cdot \Delta(353, r(u))$. Para usar a Proposição 3.13, precisamos encontrar uma cota inferior para q^n. Desta forma, vamos estudar a desigualdade $q^{\frac{n}{2}} \geq 3 \cdot 2^{\frac{n}{a}+b+3u} \cdot \Delta(353, r(u))$.

Como $q \geq c = 2^{\log_2 c}$, se

$$3 \cdot 2^{3u+b} \cdot q^{\frac{n}{a} \log_c 2} \cdot \Delta(353, r(u)) \leq q^{\frac{n}{2}}, \tag{3.6}$$

então $q^{\frac{n}{2}} \geq 3W_q(x^n - 1)W(e)^3\Delta$. Se $a > \log_c 4$, então (3.6) é equivalente a

$$q^n \geq \left(3 \cdot 2^{3u+b} \cdot \Delta(353, r(u))\right)^{\frac{2a}{a - \log_c 4}}.$$

Do Lema 1.83, podemos escolher $(a, b, c) \in A$, com

$$A = \{(1, 0, 37), (3, 6, 5), (4, 5, 3)\} \cup \left\{\left(2, \frac{q-1}{2}, q\right) \mid 7 \leq q \leq 31\right\}.$$

Obtemos

$$\max\{\left(3 \cdot 2^{3u+b} \cdot \Delta(353, r(u))\right)^{\frac{2a}{a-\log_c 4}} \mid (a, b, c) \in A \text{ and } 0 \leq u \leq 70\} < 2.129 \cdot 10^{221}$$

e, pela Proposição 3.13, concluímos que se $q^n \geq 2.129 \cdot 10^{221}$, então $(q, n) \in N_3$.

Suponha agora $q^n < 2.129 \cdot 10^{221}$ e repita o processo, com e sendo o produto de números primos menores que 101 que dividem $q^n - 1$ e com r sendo a quantidade de números primos maiores ou iguais a 101 que dividem $q^n - 1$. Nesse caso, para $u = \omega(e)$, temos $u \leq 25$. Quando $q \leq 31$, a característica de $\mathbb{F}_q$ é menor que 101 e não divide $q^n - 1$. Isso significa que pelo menos um dos primos menores que 101 não é fator de e, ou seja, podemos supor $u \leq 24$. Dessa forma

$$\max\{\left(3 \cdot 2^{3u+b} \cdot \Delta(101, r(u))\right)^{\frac{2a}{a-\log_c 4}} \mid (a, b, c) \in A \text{ and } 0 \leq u \leq 25\} < 7.525 \cdot 10^{85}.$$

Da Proposição 3.13 obtemos que se $q^n \geq 7.525 \cdot 10^{85}$, então $(q, n) \in N_3$.

Repita agora o processo, com e sendo o produto dos números primos menores que 53 que dividem $q^n - 1$ e com r sendo a quantidade de números primos maiores ou iguais a 53 que dividem $q^n - 1$. Nesse caso

$$\max\{\left(3 \cdot 2^{3u+b} \cdot \Delta(53, r(u))\right)^{\frac{2a}{a-\log_c 4}} \mid (a, b, c) \in A \text{ and } 0 \leq u \leq 15\} < 7.871 \cdot 10^{54},$$

com $0 \leq u \leq 14$, se $c < 37$.

Repetimos esse processo várias vezes. A cada etapa escolhemos um número primo $\tilde{p}$ tal que e é o produto dos números primos menores que $\tilde{p}$ que dividem $q^n - 1$ e r é a quantidade de números primos maiores ou iguais a $\tilde{p}$ que dividem $q^n - 1$. Mas em todos essss casos, o máximo valor de $\left(3 \cdot 2^{3u+b} \cdot \Delta(\tilde{p}, r(u))\right)^{\frac{2a}{a-\log_c 4}}$ é calculado por $(a, b, c) \in \tilde{A}$, com $\tilde{A} = \{(1, 0, 37), (1, 0, 31), (3, 6, 5), (4, 5, 3)\} \cup \{(2, \frac{q-1}{2}, q) \mid 7 \leq q \leq 29\}$. A Tabela 3.1 mostra o processo para todas as potências de primos ímpares.

$q^n < M$	$\tilde{p}$	Valor máximo
$M = 7.871 \cdot 10^{54}$	41	$1.368 \cdot 10^{45}$
$M = 1.368 \cdot 10^{45}$	37	$7.379 \cdot 10^{41}$
$M = 7.379 \cdot 10^{41}$	31	$3.422 \cdot 10^{40}$

Tabela 3.1: Processo do crivo para toda potência de primo q.

A Tabela 3.2 mostra o processo do crivo para $q \geq 37$. □

$q^n < M$	$\tilde{p}$	Valor máximo
$M = 3.422 \cdot 10^{40}$	37	$1.71 \cdot 10^{39}$
$M = 1.71 \cdot 10^{39}$	31	$7.391 \cdot 10^{38}$

Tabela 3.2: Processo do crivo para $q \geq 37$.

3.3.1 Prova do Teorema 3.1(ii)

Da Proposição 3.21, se $n \geq 85$, então $(q, n) \in N_3$ para toda potência de primo ímpar q, já que $q^n \geq 3^{85} > 3.592 \cdot 10^{40} > 3.422 \cdot 10^{40}$. Dessa forma, da Proposição 3.21, verificamos a Proposição 3.13, usando $1(q, n, 3)$, para todos os inteiros n entre 7 e 84 e para toda potência de primo ímpar q entre 3 e

$$M_n = \begin{cases} \left\lceil \sqrt[n]{3.422 \cdot 10^{40}} \right\rceil & \text{se } \sqrt[n]{3.422 \cdot 10^{40}} < 31, \\ \left\lceil \sqrt[n]{7.391 \cdot 10^{38}} \right\rceil & \text{se } \sqrt[n]{7.391 \cdot 10^{38}} > 31, \\ 31 & \text{caso contrário.} \end{cases}$$

Obtemos que, para todo par (q, n) com $n \geq 7$, existem valores de g e de e tais que $q^{\frac{n}{2}} \geq 3W_q(g)W(e)^3\Delta$, exceto para os pares mostrados na Tabela 3.3.

n	q	n	q
7	3, 7	10	3, 5, 11
8	3, 5, 7, 9, 11, 13	12	3, 5, 7, 13
9	3, 7	16	3

Tabela 3.3: Possíveis exceções para o Teorema 3.1(ii).

Para finalizar a demonstração do Teorema 3.1(ii), vamos tratar cada valor de $n \in \{2, 3, 4, 5, 6\}$ separadamente.

Comecemos com o caso $n = 6$.

Lema 3.22. *Sejam q a potência de um primo ímpar e $n = 6$. Então $(q, 6) \in N_3$, exceto possivelmente para $q \in \{3, 5, 7, 9, 11, 13, 17, 19, 23, 25, 29, 31, 37, 43, 61\}$.*

Demonstração. Da Proposição 3.21, temos $(q, 6) \in N_3$, para $q \geq 3006888$. Suponha agora q a potência de um primo ímpar satisfazendo $q < M = 3006888$. Vamos usar a Proposição 3.13 com $g = 1$ e $e = (q^2 - 1)$, se $7 \nmid q^6 - 1$ ou $e = 7(q^2 - 1)$, se $7 \mid q^6 - 1$. Seja $\{p_1, \ldots, p_r\}$ o conjunto de números primos da Proposição 3.13. Para $i \in \{1, \ldots, r\}$, temos $p_i \mid q^6 - 1$ e $p_i \nmid q^2 - 1$. Logo $3 \mid \varphi(p_i) = p_i - 1$ e $p_i \neq 2$, já que $2 \mid q^2 - 1$. Isso quer dizer que o conjunto $\{p_1, \ldots, p_r\}$ está formado por números primos da forma $6j + 1$. Sejam $\mathcal{S}_r$ e $\mathcal{P}_r$, respectivamente, a soma dos inversos e o produto dos primeiros r números primos da forma $6j + 1$ maiores ou iguais a 13. Como $\{p_1, \ldots, p_r\}$ é um conjunto de primos que dividem $q^4 + q^2 + 1$ e $7 \notin \{p_1, \ldots, p_r\}$, segue $\mathcal{P}_r \leq \prod_{i=1}^{r} p_i \leq q^4 + q^2 + 1 < 8.175 \cdot 10^{25}$. Portanto, $r \leq 14$ e $\mathcal{S}_r < 0.3141$. Supondo $q > 10^4$, temos

$$\delta = 1 - 3\sum_{i=1}^{r} \frac{1}{p_i} - \sum_{i=1}^{s} \frac{1}{q^{\deg h_i}} \geq 1 - 3 \cdot \mathcal{S}_r - \frac{6}{q} > 0.0571$$

e $\Delta = 2 + \frac{3r+s-1}{\delta} < 825.118$. Veja que se $q \geq (3 \cdot 2^3 \cdot A_t^3 \cdot 825.118)^{\frac{t}{3t-6}}$ para algum número real $t > 2$, então $q^3 \geq 3 \cdot (2 \cdot A_t \cdot q^{\frac{2}{t}})^3 \cdot 825.118 > 3W_q(1)W(e)^3\Delta$, já que, do Lema 1.81, $W(e) \leq 2W(q^2 - 1) < 2 \cdot A_t \cdot q^{\frac{2}{t}}$. Portanto,

da Proposição 3.13, se $q \geq (3 \cdot 2^3 \cdot A_t^3 \cdot 825.118)^{\frac{t}{3t-6}}$, para algum número real $t > 2$, então $(q, 6) \in N_3$. Para $t = 4.53$ a condição acima se torna $q \geq 13051$.

Para $q < 13051$, usando o Algoritmo 1, obtemos que existem valores de g e de e para os quais se cumpre $q^3 \geq 3W_q(g)W(e)^3\Delta$ para todo par $(q, 6)$ com q a potência de um primo ímpar entre 3 e 13050, exceto para $q \in \{3, 5, 7, 9, 11, 13, 17, 19, 23, 25, 29, 31, 37, 43, 61\}$. □

Para $n = 5$ usamos um argumento similar ao usado no caso $n = 6$.

Lema 3.23. *Sejam q a potência de um primo ímpar e $n = 5$. Então $(q, 5) \in N_3$, exceto possivelmente para $q \in \{3, 5, 7, 9, 11, 13, 19, 31\}$.*

Demonstração. Da Proposição 3.21, temos $(q, 5) \in N_3$, para $q \geq 59393736$. Suponha agora que q é uma potência de primo ímpar tal que $q < M = 59393736$. Vamos usar a Proposição 3.13, com $g = 1$ e $e = q - 1$. Seja $\{p_1, \ldots, p_r\}$ o conjunto de primos definidos na Proposição 3.13. Para $i \in \{1, \ldots, r\}$, temos $p_i \mid q^5 - 1$ e $p_i \nmid q - 1$. Logo, $5 \mid \varphi(p_i) = p_i - 1$ e $p_i \neq 2$, já que $2 \mid q - 1$. Isso significa que o conjunto $\{p_1, \ldots, p_r\}$ está formado por números primos da forma $10j + 1$. Sejam $\mathcal{S}_r$ e $\mathcal{P}_r$, respectivamente, a soma dos inversos e o produto dos r primeiros números primos da forma $10j + 1$. Como $\{p_1, \ldots, p_r\}$ é um conjunto de primos que dividem $q^4 + q^3 + q^2 + q + 1$, segue $\mathcal{P}_r \leq \prod_{i=1}^{r} p_i \leq q^4 + q^3 + q^2 + q + 1 < 1.2445 \cdot 10^{31}$. Portanto, $r \leq 15$ e $\mathcal{S}_r < 0.2331$. Supondo $q > 435$, obtemos

$$\delta = 1 - 3\sum_{i=1}^{r} \frac{1}{p_i} - \sum_{i=1}^{s} \frac{1}{q^{\deg h_i}} \geq 1 - 3 \cdot \mathcal{S}_r - \frac{5}{q} > 0.2892$$

e $\Delta = 2 + \frac{3r+s-1}{\delta} < 171.433$. Se $q \geq (3 \cdot A_t^3 \cdot 171.433)^{\frac{2t}{5t-6}}$, para algum número real $t > 2$, então $q^{\frac{5}{2}} \geq 3 \cdot (A_t \cdot q^{\frac{1}{t}})^3 \cdot 171.433 > 3W_q(1)W(e)^3\Delta$, pois do Lema 1.81, temos $W(e) \leq W(q-1) < A_t \cdot q^{\frac{1}{t}}$. Assim, da Proposição 3.13, se $q \geq (3 \cdot A_t^3 \cdot 171.433)^{\frac{2t}{5t-6}}$, para algum número real $t > 2$, então $(q, 5) \in N_3$. Para $t = 3.4$ a desigualdade acima se torna $q \geq 439$.

Para $q < 439$, usando o Algoritmo 1, existem valores de g e de e para os quais se cumpre $q^{\frac{5}{2}} \geq 3W_q(g)W(e)^3\Delta$, para todo par $(q, 5)$, com q a potência de um primo ímpar entre 3 e 439, exceto para $q \in \{3, 5, 7, 9, 11, 13, 19, 31\}$. □

Para $n = 4$ obtemos o seguinte resultado.

Lema 3.24. *Sejam q a potência de um primo ímpar e $n = 4$. Então $(q, 4) \in N_3$, exceto possivelmente para $q \in \{3, 5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 109, 113, 127, 131, 137, 139, 149, 151, 157, 167, 169, 173, 181, 191, 197, 211, 229, 239, 281, 307, 419, 421, 463, 659, 727\}$.*

Demonstração. Da Proposição 3.21, temos $(q, 4) \in N_3$, para $q \geq 5214057313$. Assim, suponha $q < M = 5214057313$. Vamos usar a Proposição 3.13 com $g = 1$ e $e = (q^2 - 1)$, se $5 \nmid q^4 - 1$ ou $e = 5(q^2 - 1)$ se $5 \mid q^4 - 1$. Seja $\{p_1, \ldots, p_r\}$ o conjunto de primos da Proposição 3.13. Como já vimos antes, isso significa que o conjunto $\{p_1, \ldots, p_r\}$ está composto por primos da forma $4j + 1$ maiores que 5, pois $p_i \mid q^4 - 1$ e $p_i \nmid q^2 - 1$, para todo $i \in \{1, \ldots, r\}$. Sejam $\mathcal{S}_r$ e $\mathcal{P}_r$,

respectivamente, a soma dos inversos e o produto dos primeiros r primos da forma $4j+1$ maiores ou iguais a 13. Como $\{p_1, \ldots, p_r\}$ é um conjunto de primos que dividem q^2+1 e $5 \notin \{p_1, \ldots, p_r\}$, segue $\mathcal{P}_r \leq \prod_{i=1}^{r} p_i \leq \frac{q^2+1}{2} < 1.36 \cdot 10^{19}$. Portanto, $r \leq 11$. Se $q > 10^8$, então

$$\delta = 1 - 3\sum_{i=1}^{r} \frac{1}{p_i} - \sum_{i=1}^{s} \frac{1}{q^{\deg h_i}} \geq 1 - 3 \cdot \mathcal{S}_r - \frac{4}{q} > 0.0938$$

e $\Delta = 2 + \frac{3r+s-1}{\delta} < 385.796$. Observe que se $q \geq (3 \cdot 2^3 \cdot A_t^3 \cdot 385.796)^{\frac{t}{2t-6}}$, para algum número real $t > 3$, então $q^2 \geq 3 \cdot (2 \cdot A_t \cdot q^{\frac{2}{t}})^3 \cdot 385.796 > 3W_q(1)W(e)^3\Delta$, pois do Lema 1.81, $W(e) \leq 2W(q^2-1) < 2 \cdot A_t \cdot q^{\frac{2}{t}}$. Como $8 \mid q^2-1$, podemos substituir A_t do Lema 1.81 por

$$\tilde{A}_t = \frac{2}{\sqrt[t]{8}} \prod_{\substack{\wp < 2^t \\ \wp \text{ is odd} \\ \text{prime}}} \frac{2}{\sqrt[t]{\wp}}.$$

Assim, da Proposição 3.13, se $q \geq (3 \cdot 2^3 \cdot \tilde{A}_t^3 \cdot 385.796)^{\frac{t}{2t-6}}$, para algum número real $t > 3$, então $(q, 4) \in N_3$. Para $t = 5.5$ a condição acima se torna $q \geq 1.74 \cdot 10^8$.

Vamos usar novamente a Proposição 3.13 com as ideias da Proposição 3.21. Sejam e o produto dos primos menores que 29 que dividem $q^4 - 1$ e r o número de primos maiores ou iguais a 29 que dividem $q^4 - 1$. Como $16 \mid q^4 - 1$, segue $\mathcal{P}(29, r) < \frac{q^4-1}{16} < 5.729 \cdot 10^{31}$. Portanto, $r \leq 17$. Se $u = \omega(e)$, então $u \leq 9$, já que há 9 números primos menores que 29. Denotemos por $\mathcal{P}_u$ o produto dos primeiros u números primos. Defina $r(u) = \max\{r \mid 8 \cdot \mathcal{P}_u \cdot \mathcal{P}(29, r) \leq 5.729 \cdot 10^{31}\}$, já que $8 \cdot \mathcal{P}_u \cdot \mathcal{P}(29, r) \leq q^4 - 1$. Sejam δ e Δ como na Proposição 3.13 com $g = 1$ e suponha $q \geq 10^5$. Sejam também $\delta(29, r(u)) = 1 - 3\mathcal{S}(29, r(u)) - \frac{4}{10^5}$ e $\Delta(29, r(u)) = 2 + \frac{3r(u)+4-1}{\delta(29, r(u))}$. Como $3 \leq s \leq 4$ e $r \leq r(u) \leq r(0)$, temos $\delta \geq \delta(29, r(u)) \geq \delta(29, r(0)) > 0$. Assim, podemos usar a Proposição 3.13.

Como $3W_q(g)W(e)^3\Delta \leq 3 \cdot 2^{3u} \cdot \Delta(29, r(u))$, da Proposição 3.13, se $q^2 \geq 3 \cdot \Delta(29, r(u)) \cdot 2^{3u}$, então $(q, 4) \in N_3$. Dessa forma, obtemos

$$\max\{\left(3 \cdot \Delta(29, r(u)) \cdot 2^{3u}\right)^{\frac{1}{2}} \mid 0 \leq u \leq 9\} < 300350.$$

Conclui-se que se $q \geq 300350$, então $(q, 4) \in N_3$.

Para $q < 300350$, usando o Algoritmo 1, obtemos que existem valores de g e de e para os quais se cumpre $q^2 \geq 3W_q(g)W(e)^3\Delta$, para todo par $(q, 4)$, com q a potência de um primo ímpar entre 3 e 300350, exceto para os valores de q no enunciado do lema. □

Para $n = 3$ obtemos um resultado similar.

Lema 3.25. *Sejam q a potência de um primo ímpar e $n = 3$. Então $(q, 3) \in N_3$, exceto possivelmente para $q \in \{3, 5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 29, 31, 37, 41, 43, 47, 49, 53, 61, 67, 71, 73, 79, 81, 97, 103, 107, 109, 121, 127, 131, 139, 151, 157, 163, 169, 181, 191, 193, 211, 241, 277, 289, 331, 361, 373, 421, 463, 529, 541, 571, 631, 661, 691, 751, 841, 919, 961, 991, 1171, 1381, 4951\}$.*

Demonstração. Da Proposição 3.21, obtemos $(q, 3) \in N_3$, para $q \geq 9.042 \cdot 10^{12}$. Podemos assim supor que q é a potência de um primo ímpar menor que $M = 9.042 \cdot 10^{12}$. Vamos usar a Proposição 3.13, com $g = 1$ e $e = q - 1$, se $7 \nmid q^3 - 1$ ou $e = 7(q-1)$, se $7 \mid q^3 - 1$. Seja $\{p_1, \ldots, p_r\}$ o conjunto de números primos da Proposição 3.13. Como já vimos antes, isso quer dizer que o conjunto $\{p_1, \ldots, p_r\}$ está composto de números primos maiores que 7 da forma $6j + 1$, já que $p_i \mid q^3 - 1$ e $p_i \nmid q - 1$, para todo $i \in \{1, \ldots, r\}$. Sejam $\mathcal{S}_r$ e $\mathcal{P}_r$, respectivamente, a soma dos inversos e o produto dos primeiros r números primos da forma $6j + 1$ maiores ou iguais a 13. Como $\{p_1, \ldots, p_r\}$ é um conjunto de números primos que dividem $q^2 + q + 1$ e $7 \notin \{p_1, \ldots, p_r\}$, segue $\mathcal{P}_r \leq \prod_{i=1}^{r} p_i \leq q^2 + q + 1 < 8.1758 \cdot 10^{25}$. Portanto, $r \leq 14$. Se supomos $q > 10^6$, então

$$\delta = 1 - 3\sum_{i=1}^{r} \frac{1}{p_i} - \sum_{i=1}^{s} \frac{1}{q^{\deg h_i}} \geq 1 - 3 \cdot \mathcal{S}_r - \frac{3}{q} > 0.0579$$

e $\Delta = 2 + \frac{3r+s-1}{\delta} < 761.931$. Observe que se $q \geq (3 \cdot 2^3 \cdot A_t^3 \cdot 761.931)^{\frac{2t}{3t-6}}$, para algum número real $t > 2$, então $q^{\frac{3}{2}} \geq 3 \cdot (2 \cdot A_t \cdot q^{\frac{1}{t}})^3 \cdot 761.931 > 3W_q(1)W(e)^3\Delta$, já que, do Lema 1.81, $W(e) \leq 2W(q-1) < 2 \cdot A_t \cdot q^{\frac{1}{t}}$.

Assim, da Proposição 3.13, se $q \geq (3 \cdot 2^3 \cdot A_t^3 \cdot 761.931)^{\frac{2t}{3t-6}}$, para algum número real $t > 2$, então $(q, 3) \in N_3$. Para $t = 4.6$ a cota acima é $q \geq 1.5555 \cdot 10^8$.

Repetimos o mesmo processo para $q \leq 1.5555 \cdot 10^8$. Supondo $q \geq 10^6$, obtemos $r \leq 9$, $\delta > 0.19068$ e $\Delta < 154.0873$. Como acima, se $q \geq (3 \cdot 2^3 \cdot A_t^3 \cdot 154.0873)^{\frac{2t}{3t-6}}$, para algum número real $t > 2$, então $(q, 3) \in N_3$. Para $t = 4.5$ a cota obtida é $q \geq 2.301 \cdot 10^7$.

Usamos novamente a Proposição 3.13 com as ideias da Proposição 3.21. Sejam e o produto dos primos menores que 23 que dividem $q^3 - 1$ e r o número de primos maiores ou iguais a 23 que dividem $q^3 - 1$. Como $\mathcal{P}(23, r) < q^3 - 1 < 1.219 \cdot 10^{22}$, temos $r \leq 13$. Por outro lado, se $u = \omega(e)$, então $u \leq 8$, pois existem 8 primos menores que 23. Agora $\mathcal{P}_u$ denotará o produto dos u primeiros números primos. Defina $r(u) = \max\{r \mid P_u \cdot P(23, r) \leq 1.219 \cdot 10^{22}\}$. Sejam δ e Δ como na Proposição 3.13 com $g = 1$ e suponhamos $q \geq 10^5$. Sejam também $\delta(23, r(u)) = 1 - 3\mathcal{S}(23, r(u)) - \frac{3}{10^5}$ e $\Delta(23, r(u)) = 2 + \dfrac{3r(u) + 3 - 1}{\delta(23, r(u))}$. Como $2 \leq s \leq 3$ e $r \leq r(u) \leq r(0)$, temos $\delta \geq \delta(23, r(u)) \geq \delta(23, r(0)) > 0$. Dessa forma, podemos aplicar a Proposição 3.13.

Como $3W_q(g)W(e)^3\Delta \leq 3 \cdot 2^{3u} \cdot \Delta(23, r(u))$, da Proposição 3.13, temos que se $q^{\frac{3}{2}} \geq 3 \cdot 2^{3u} \cdot \Delta(23, r(u))$, então $(q, 3) \in N_3$. Como

$$\max\{\left(3 \cdot 2^{3u} \cdot \Delta(23, r(u))\right)^{\frac{2}{3}} \mid 0 \leq u \leq 8\} < 3.0884 \cdot 10^6,$$

conclui-se que se $q \geq 3.0884 \cdot 10^6$, então $(q, 3) \in N_3$.

Suponha agora $q < 3.0884 \cdot 10^6$. Sejam e o produto dos números primos menores que 19 que dividem $q^3 - 1$ e r o número de primos maiores ou iguais a 19 que dividem $q^3 - 1$. Como no caso anterior, r deve satisfazer $\mathcal{P}(19, r) < q^3 - 1 < 2.946 \cdot 10^{19}$. Seguindo o mesmo argumento do parágrafo anterior, obtemos $(q, 3) \in N_3$ se $q \geq 821257$.

Para $q < 821257$, usando o Algoritmo 1, obtemos que existem valores de g e de e para os quais se cumpre $q^2 \geq 3W_q(g)W(e)^3\Delta$ para todo par $(q, 3)$ com q a potência de um primo ímpar entre 3 e 821257, exceto para os valores

de q no enunciado do lema. □

Finalmente, para $n = 2$, usaremos a Proposição 3.14 e a Observação 3.15 para obter o seguinte resultado com o qual conclui-se a prova do Teorema 3.1(ii).

Lema 3.26. *Sejam q a potência de um primo ímpar e $n = 2$. Então $(q, 2) \in N_3$, exceto possivelmente para 1373 valores de q. Veja a Seção 3.6 para a lista completa das exceções.*

Demonstração. Da Proposição 3.21, temos $(q, 2) \in N_3$, para $q \geq 2.7187 \cdot 10^{19}$. Suponha agora q a potência de um primo ímpar tal que $q < M = 2.7187 \cdot 10^{19}$. Usamos a Observação 3.15, com $g = 1$ e com $e = q - 1$, se $5 \nmid q + 1$ ou $e = 5(q - 1)$, se $5 \mid q + 1$. Seja $\{p_1, \ldots, p_r\}$ o conjunto de números primos como na Observação 3.15. Como já vimos antes, isso implica que o conjunto $\{p_1, \ldots, p_r\}$ está composto de primos maiores que 5 da forma $4j + 1$, já que $p_i \mid q^2 - 1$ e $p_i \nmid q - 1$, para todo $i \in \{1, \ldots, r\}$. Denotamos agora $\mathcal{S}_r$ e $\mathcal{P}_r$, respectivamente, a soma dos inversos e o produto dos primeiros r números primos da forma $4j + 1$ maiores ou iguais a 13. Como $\{p_1, \ldots, p_r\}$ é um conjunto de primos que dividem $q + 1$ e $5 \notin \{p_1, \ldots, p_r\}$, segue $\mathcal{P}_r \leq \prod_{i=1}^{r} p_i \leq q + 1 < 2.7187 \cdot 10^{19}$. Portanto, $r \leq 11$. Sejam

$$\delta = 1 - 3 \sum_{i=1}^{r} \frac{1}{p_i} \geq 1 - 3 \cdot S_r > 0.0938$$

e $\Delta = 2 + \frac{3r-1}{\delta} < 343.1514$. Se $q \geq (2^4 \cdot A_t^3 \cdot 343.1514)^{\frac{t}{t-3}}$, para algum número real $t > 3$, então $q \geq 2 \cdot (2 \cdot A_t \cdot q^{\frac{1}{t}})^3 \cdot 343.1514 > 2W(e)^3\Delta$, já que, do Lema 1.81, $W(e) \leq 2W(q - 1) < 2 \cdot A_t \cdot q^{\frac{1}{t}}$. Para $t = 5.5$, a desigualdade acima se torna $q \geq 5.0381 \cdot 10^{16}$.

Usamos novamente a Observação 3.15 junto com as ideias da Proposição 3.21. Sejam e o produto dos números primos menores que 29 que dividem $q^2 - 1$ (com suas respectivas potências) e r o número de primos maiores ou iguais a 29 que dividem $q^2 - 1$. Veja que r satisfaz $\mathcal{P}(29, r) < q^2 - 1 < 2.53825 \cdot 10^{33}$, supondo $q < 5.0381 \cdot 10^{16}$. Portanto, $r \leq 18$. Se $u = \omega(e)$, então $u \leq 9$, pois há 9 primos menores que 29. Podemos supor também $8 \mid e$ e $u \geq 1$, já que $8 \mid q^2 - 1$. Se denotamos por $\mathcal{P}_u$ como sendo o produto dos primeiros u números primos, então $4\mathcal{P}_u \leq e$. Define-se $r(u) = \max\{r \mid 4 \cdot \mathcal{P}_u \cdot \mathcal{P}(29, r) \leq 2.53825 \cdot 10^{33}\}$. Sejam δ e Δ como na Observação 3.15. Sejam também $\delta(29, r(u)) = 1 - 3\mathcal{S}(29, r(u))$ e $\Delta(29, r(u)) = 2 + \dfrac{3r(u) - 1}{\delta(29, r(u))}$. Observe que $r \leq r(u) \leq r(1)$ e $\delta \geq \delta(29, r(u)) \geq \delta(29, r(1)) > 0$, logo podemos aplicar a Observação 3.15. Como $2W(e)^3\Delta \leq 2 \cdot 2^{3u} \cdot \Delta(29, r(u))$, da Observação 3.15, se $q \geq 2 \cdot 2^{3u} \cdot \Delta(29, r(u))$, então $(q, 2) \in N_3$. Obtemos

$$\max\{2 \cdot 2^{3u} \cdot \Delta(29, r(u)) \mid 1 \leq u \leq 9\} < 7.245 \cdot 10^{10}$$

e conclui-se que se $q \geq 7.245 \cdot 10^{10}$, então $(q, 2) \in N_3$.

Suponha agora $q < 7.245 \cdot 10^{10}$. Mais uma vez, sejam e o produto dos primos menores que 19 (com suas respectivas potências) que dividem $q^2 - 1$ e r o número de primos maiores ou iguais a 19 que dividem $q^2 - 1$. Usamos o mesmo argumento que anteriormente, lembrando que $\mathcal{P}(19, r) < (q^2 - 1)/8 < 6.5613 \cdot 10^{20}$ e que 8 é fator de $q^2 - 1$,

obtemos $(q, 2) \in N_3$, para $q \geq 6.615 \cdot 10^8$.

Repetimos esse processo com e sendo o produto dos primos menores que 19 (com suas respectivas potências) que dividem $q^2 - 1$ e $q < 6.615 \cdot 10^8$. Obtemos $(q, 2) \in N_3$, para $q \geq 3.0024 \cdot 10^8$.

Para $q < 3.0024 \cdot 10^8$, usando o Algoritmo 1, eliminando as linhas que envolvem polinômios e substituindo as linhas 12 e 13 por $\Delta = 2 + \frac{mr-1}{\delta}$ e $q > (m-1)W(e)^m\Delta$, obtemos que existem valores de e para os quais se cumpre $q > (m-1)W(e)^m\Delta$ para todo par $(q, 2)$ com q a potência de um primo ímpar entre 3 e $3.0024 \cdot 10^8$, exceto para os 1373 valores de q que aparecem na lista da Seção 3.6. □

3.3.2 Prova do Teorema 3.2

Usamos o Algoritmo 2 para procurar elementos $\alpha \in \mathbb{F}_{q^n}^*$ tais que α, $\alpha + \beta$ e $\alpha + 2\beta$ sejam primitivos e um deles seja normal para todo $\beta \in \mathbb{F}_q^*$ (trocando β por $-\beta$, o tempo de execução desta tarefa é reduzido pela metade). Só resta verificar a existência do elemento α, para os pares (q, n) mostrados na Tabela 3.3 com $n \geq 7$ e para as exceções dos Lemas 3.22, 3.23, 3.24, 3.25 e 3.26 com $2 \leq n \leq 6$. Só para as triplas (q, n, β) mostradas na Tabela 3.4 não existe elemento α satisfazendo as condições indicadas.

(q, n)	Valores de β
$(3, 2)$	$\beta \in \mathbb{F}_3^*$
$(5, 2)$	$\beta \in \mathbb{F}_5^*$
$(7, 2)$	$\beta \in \{\pm 2, \pm 3\}$
$(9, 2)$	$\beta \in \mathbb{F}_9^*$
$(11, 2)$	$\beta \in \mathbb{F}_{11}^*$
$(13, 2)$	$\beta \in \{\pm 1, \pm 4, \pm 5, \pm 6\}$

(q, n)	Valores de β
$(3, 3)$	$\beta \in \mathbb{F}_3^*$
$(9, 3)$	β é qualquer raiz dos polinômios $x^2 + 2x + 2, x^2 + x + 2 \in \mathbb{F}_3[x]$
$(3, 4)$	$\beta \in \mathbb{F}_3^*$
$(5, 4)$	$\beta \in \mathbb{F}_5^*$

Tabela 3.4: Exceções para a existência de progressões aritméticas de elementos primitivos com um deles normal.

3.3.3 Prova do Corolário 3.3

Este resultado segue da verificação das exceções do Teorema 3.2. Usamos o Algoritmo 2, removendo as linhas 15 e 17, para procurar $\alpha \in \mathbb{F}_{q^n}$ tal que α, $\alpha + \beta$ e $\alpha + 2\beta$ sejam primitivos para todo $\beta \in \mathbb{F}_q^*$ (trocando β e $-\beta$, o tempo de execução desta tarefa é reduzido pela metade). As únicas exceções encontradas nesse caso são as ternas (q, n, β) mostradas na Tabela 3.5.

(q, n)	Valores de β
$(3, 2)$	$\beta \in \mathbb{F}_3^*$
$(5, 2)$	$\beta \in \mathbb{F}_5^*$
$(7, 2)$	$\beta \in \{\pm 2, \pm 3\}$
$(9, 2)$	$\beta \in \mathbb{F}_9^*$
$(11, 2)$	$\beta \in \mathbb{F}_{11}^*$

(q, n)	Valores de β
$(13, 2)$	$\beta \in \{\pm 1, \pm 4, \pm 5, \pm 6\}$
$(9, 3)$	β é qualquer raiz dos polinômios $x^2 + 2x + 2, x^2 + x + 2 \in \mathbb{F}_3[x]$
$(3, 4)$	$\beta \in \mathbb{F}_3^*$

Tabela 3.5: Exceções para a existência de progressões aritméticas de elementos primitivos.

3.4 Caso $m = 2$

Tratamos agora o caso $m = 2$. Pela Observação 3.7, temos $N_3 \subset N_2$. Assim, só precisamos verificar os pares (q, n) com q ímpar que falham nos Teoremas 3.1(ii) e 3.2, além de verificar as potências de 2. Pela Proposição 3.17, para q par, só é necessário verificar as potências de 2 para as quais $q^n \leq 7.51 \cdot 10^{358}$.

3.4.1 Prova do Teorema 3.1(i) para q ímpar

Verificamos a desigualdade $q^{\frac{n}{2}} \geq 2W_q(g)W(e)^2\Delta$ (ver Proposição 3.13), usando o Algoritmo 1, para os 1532 pares (q, n) que são as possíveis exceções do Teorema 3.1(ii). Para esse pares, o Algoritmo 1 retorna verdadeiro, exceto para os 155 pares mostrados na Tabela 3.6.

n	q
12	5, 3
10	3
8	9, 5, 3
7	3
6	11, 9, 7, 5, 3
5	11, 7, 5, 3
4	43, 41, 29, 23, 19, 17, 13, 11, 9, 7, 5, 3
3	211, 121, 67, 61, 43, 37, 31, 25, 23, 19, 13, 11, 9, 7, 5, 3
2	3191, 2729, 2311, 2029, 1871, 1861, 1849, 1709, 1429, 1331, 1301, 1289, 1259, 1231, 1091, 1021, 911, 881, 859, 811, 769, 701, 659, 631, 601, 599, 571, 529, 521, 509, 491, 463, 461, 449, 439, 421, 419, 409, 389, 379, 373, 349, 337, 331, 311, 307, 293, 289, 281, 271, 269, 263, 251, 241, 239, 233, 229, 227, 223, 211, 199, 197, 191, 181, 179, 173, 169, 167, 157, 151, 149, 139, 137, 131, 127, 125, 121, 113, 109, 107, 103, 101, 97, 89, 83, 81, 79, 73, 71, 67, 61, 59, 53, 49, 47, 43, 41, 37, 31, 29, 27, 25, 23, 19, 17, 13, 11, 9, 7, 5, 3

Tabela 3.6: Possíveis exceções para o Teorema 3.1(i) com q ímpar.

3.4.2 Prova do Teorema 3.1(i) para q par

Sejam $q = 2^k$ com $1 \leq k \leq 596$ e $n \geq 2$ tais que $q^n < 7.51 \cdot 10^{358}$. Aplicamos o primeiro dos seguintes métodos para os pares (q, n) e o segundo método para aqueles pares que falham no primeiro método.

- Pelo Lema 1.83, para $q = 2$, temos $W_q(x^n - 1) \leq 2^{\frac{n+14}{5}}$; para $q = 4$, temos $W_q(x^n - 1) \leq 2^{\frac{n+41}{4}}$; para $q = 8$, temos $W_q(x^n - 1) \leq 2^{\frac{n}{3}+14}$; para $q = 16$, temos $W_q(x^n - 1) \leq 2^{\frac{n+15}{2}}$ e, para $q \geq 32$, temos $W_q(x^n - 1) \leq 2^n$. Levando em consideração $q^n - 1$ ímpar, a constante A_t que aparece no Lema 1.81 não considera o primo $p = 2$. Assim, verificamos $q^{\frac{n}{2}} \geq 2W_q(x^n - 1)A_t^2 q^{\frac{2n}{t}}$, usando as cotas para A_t e para $W_q(x^n - 1)$ e aplicamos o Teorema 3.11.

- Sejam p_1 um número primo, e o produto dos primos menores que p_1 que dividem $q^n - 1$ e $T = \frac{q^n-1}{\text{mmc}(q^n-1,e)}$. Seja $s \in \mathbb{N}$ o maior inteiro tal que $p_1 < p_2 < \cdots < p_s$ são primos consecutivos satisfazendo $p_1 p_2 \ldots p_s \leq T$. Seja também $\delta \geq \delta_T := 1-2\sum_{i=1}^{s} \frac{1}{p_i} > 0$. A seguir, verificamos se $q^{\frac{n}{2}} \geq mW_q(x^n-1)W(e)^m\Delta_T$ com $\Delta_T := 2+\frac{2s-1}{\delta_T} \geq \Delta$ e aplicamos a Proposição 3.13.

Se escolhemos $t = 10$ e $p_0 = 61$, então pelo menos um desses métodos funciona, exceto para os pares mostrados na Tabela 3.7.

q	n	q	n	q	n
	36, 30, 28, 24, 21, 20,	8	8, 7, 6, 5, 4, 3, 2	128	2
2	18, 16, 15, 14, 12, 11,	16	15, 10, 9, 7, 6, 5,	256	5, 3, 2
	10, 9, 8, 7, 6, 5, 4, 3, 2		4, 3, 2	512	2
4	18, 15, 14, 12, 10, 9,	32	4, 3, 2	1024	2
	8, 7, 6, 5, 4, 3, 2	64	6, 4, 3, 2	4096	3, 2

Tabela 3.7: Lista parcial das possíveis exceções para o Teorema 3.1(i) com q par.

A seguir, verificamos $q^{\frac{n}{2}} \geq 2W_q(g)W(e)^2\Delta$ (ver Proposição 3.13), usando o Algoritmo 1, para os pares (q, n) da Tabela 3.7. Dessa forma, obtemos $(q, n) \in N_2$, exceto possivelmente para os pares mostrados na Tabela 3.8.

q	n	q	n
2	14, 12, 10, 9, 8,	8	4, 2
	7, 6, 5, 4, 3, 2	16	3, 2
4	12, 9, 6, 5,	32	2
	4, 3, 2	64	2

Tabela 3.8: Possíveis exceções para o Teorema 3.1(i) com q par.

3.4.3 Prova do Teorema 3.4

Para provar o Teorema 3.4 só precisamos verificar os pares (q, n) mostrados nas Tabelas 3.6 e 3.8. Removemos a linha 13 e adaptamos as linhas 11, 14 e 15 do Algoritmo 2 para q ímpar e também adaptamos a linha 4 no caso em que q é par para procurar elementos primitivos $\alpha, \alpha + \beta \in \mathbb{F}_{q^n}^*$ tal que um deles seja normal. A única exceção real encontrada é $(q, n, \beta) = (2, 4, 1)$. Isso completa a prova do Teorema 3.4.

3.4.4 Prova do Corolário 3.5

Este corolário segue diretamente do Teorema 3.4 e de [9, Theorem A], já que para $\beta = 1$ lidamos com elementos consecutivos.

3.5 Algoritmos da Capítulo 3

Nessa seção apresentamos alguns algoritmos utilizados no decorrer do capítulo.

3.5.1 Algoritmo para testar todos os crivos possíveis

Dada a potência de um primo q e inteiros positivos n e m, o Algoritmo 1 verifica a Proposição 3.13, sendo $e = \prod_{p\in B} p$, $g = \prod_{h\in H} h$, $C = \{p_1, \ldots, p_r\}$ e $K = \{h_1, \ldots, h_s\}$.

O comando len(L) retorna o comprimento da lista L.

Algoritmo 1: Verifica a Proposição 3.13 para valores dados de q, n e m

Entrada: A potência de um primo q e inteiros positivos n e m
Saída: verdadeiro ou falso

$Cond \leftarrow$ verdadeiro
$L \leftarrow$ lista ordenada dos divisores primos de $q^n - 1$
$G \leftarrow$ lista ordenada de factores irredutíveis mônicos de $x^n - 1$
$i, j \leftarrow 0$
enquanto $i \leq \text{len}(L)$ *e* $Cond$ **faça**
  $B \leftarrow$ primeiros i elementos de L
  $C \leftarrow$ últimos $\text{len}(L) - i$ elementos de L
  $H \leftarrow$ primeiros j elementos de G
  $K \leftarrow$ últimos $\text{len}(G) - j$ elementos de G
  $\delta \leftarrow 1 - \left(m \cdot \sum_{p\in C} \frac{1}{p} + \sum_{h\in K} \frac{1}{q^{\text{grau}(h)}} \right)$
  se $\delta > 0$ **então**
    $\Delta \leftarrow 2 + \frac{m \cdot \text{len}(C) + \text{len}(K) - 1}{\delta}$
    $res \leftarrow \left[q^{\frac{n}{2}} \geq m \cdot 2^{m\cdot\text{len}(B)+\text{len}(H)} \cdot \Delta \right]$
    $Cond \leftarrow$ não res
  senão
    $res \leftarrow$ falso
  fim
  $j \leftarrow j + 1$
  se $j > \text{len}(G)$ **então**
    $j \leftarrow 0$
    $i \leftarrow i + 1$
  fim
fim
retorna res

3.5.2 Algoritmo para encontrar ternas de elementos primitivos sendo um dos elementos normal

O Algoritmo 2 procura um elemento $\alpha \in \mathbb{F}_{q^n}$, para todo $\beta \in \mathbb{F}_q^*$ tal que $\alpha, \alpha + \beta$ e $\alpha + 2\beta$ sejam primitivos e um deles seja normal. Para tal, considera-se um elemento primitivo $a \in \mathbb{F}_{q^n}$. Se $t = \sum_{i=0}^{n-1} q^i$, então $(a^{tj})^q = a^{tj}$, para todo $j \in \{0, \ldots, q-1\}$. Isso implica que $\beta = a^{tj}$ percorre todos os elementos não nulos de $\mathbb{F}_q$. Como $a^{j\cdot\frac{q-1}{2}} = -1$, basta

procurar valores de α para cada β definido por $j \in \{0, \ldots, \frac{q-1}{2} - 1\}$.

Algoritmo 2: Algoritmo para buscar ternas primitivas com um dos elementos normal para q ímpar

Entrada: A potência q de um primo e um inteiro positivo $n \geq 2$
Saída: A lista de valores $\beta \in \mathbb{F}_q$ para os quais não há progressões aritméticas de 3 termos de razão $\pm\beta$ com a propriedade desejada

```
1  a ← elemento primitivo de F_{q^n}
2  Lista ← ∅
3  t ← Σ_{i=0}^{n-1} q^i
4  para j = 0 até (q-1)/2 − 1 faça
5      β ← a^{tj}
6      R ←falso
7      u ← 1
8      enquanto u < q^n e R é falso faça
9          se mdc(u, q^n − 1) = 1 então
10             b ← a^u
11             se b + β ≠ 0 e b + 2β ≠ 0 então
12                 m_1 ← ordem multiplicativa de b + β
13                 m_2 ← ordem multiplicativa de b + 2β
14                 se m_1 = q^n − 1 e m_2 = q^n − 1 então
15                     se b é normal ou b + β é normal ou b + 2β é normal então
16                         R ← verdade
17                     fim
18                 fim
19             fim
20         fim
21         u ← u + 1
22     fim
23     se R é falso então
24         anexar β em Lista
25     fim
26 fim
27 retorna Lista
```

3.6 Possíveis exceções do Teorema 3.1(ii) com $n = 2$

Nesta seção são mostrados os 1373 valores de q que não satisfazem a condição $q > (m-1)W(e)^m\Delta$. Portanto, esses valores de q são as possíveis exceções do Teorema 3.1(ii) com $n = 2$. Ver o Lema 3.26.

3, 5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 79, 81, 83, 89, 97, 101, 103, 107, 109, 113, 121, 125, 127, 131, 137, 139, 149, 151, 157, 163, 167, 169, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 289, 293, 307, 311, 313, 317, 331, 337, 343, 347, 349, 353, 359, 361, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 529, 541, 547, 557, 563, 569, 571, 587, 593, 599, 601, 607, 613, 617, 619, 625, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 729, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 841, 853, 857, 859, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 961, 967, 971, 991, 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069, 1091, 1093, 1103, 1109, 1117, 1123, 1129, 1151, 1163, 1171, 1181, 1201, 1217, 1223, 1229, 1231, 1249, 1259, 1277, 1279, 1289, 1291, 1301, 1303, 1319, 1321, 1327, 1331, 1361, 1369, 1373, 1381,

1399, 1409, 1427, 1429, 1439, 1451, 1459, 1471, 1481, 1483, 1489, 1499, 1511, 1531, 1549, 1553, 1559, 1567, 1571, 1579, 1583, 1597, 1601, 1607, 1609, 1613, 1619, 1621, 1627, 1637, 1667, 1669, 1681, 1693, 1699, 1709, 1721, 1723, 1741, 1747, 1759, 1777, 1789, 1801, 1811, 1831, 1847, 1849, 1861, 1871, 1877, 1879, 1889, 1901, 1913, 1931, 1933, 1949, 1951, 1973, 1979, 1987, 1999, 2003, 2011, 2029, 2039, 2069, 2081, 2087, 2089, 2099, 2111, 2113, 2129, 2131, 2141, 2143, 2161, 2179, 2197, 2209, 2213, 2221, 2239, 2243, 2267, 2269, 2281, 2287, 2297, 2309, 2311, 2339, 2341, 2351, 2371, 2381, 2389, 2393, 2399, 2411, 2437, 2441, 2459, 2521, 2531, 2539, 2549, 2551, 2579, 2591, 2609, 2617, 2621, 2659, 2671, 2687, 2689, 2699, 2711, 2719, 2729, 2731, 2741, 2749, 2789, 2791, 2801, 2809, 2819, 2851, 2857, 2861, 2909, 2927, 2939, 2969, 2971, 3001, 3011, 3037, 3041, 3049, 3061, 3067, 3079, 3089, 3109, 3119, 3121, 3163, 3169, 3181, 3191, 3221, 3229, 3251, 3299, 3301, 3319, 3329, 3331, 3359, 3361, 3389, 3391, 3433, 3449, 3457, 3469, 3481, 3499, 3511, 3529, 3539, 3541, 3571, 3613, 3631, 3659, 3671, 3691, 3697, 3709, 3719, 3739, 3761, 3769, 3779, 3821, 3851, 3877, 3911, 3919, 3989, 4001, 4003, 4019, 4049, 4079, 4091, 4129, 4159, 4201, 4211, 4219, 4229, 4231, 4241, 4271, 4289, 4339, 4409, 4421, 4423, 4451, 4481, 4489, 4523, 4549, 4591, 4621, 4649, 4663, 4679, 4691, 4729, 4751, 4759, 4789, 4801, 4817, 4831, 4861, 4871, 4889, 4931, 4951, 4969, 4999, 5011, 5039, 5041, 5059, 5081, 5167, 5171, 5179, 5209, 5237, 5279, 5281, 5329, 5381, 5419, 5431, 5479, 5501, 5519, 5521, 5531, 5591, 5641, 5659, 5669, 5711, 5741, 5839, 5849, 5851, 5879, 5881, 5939, 5981, 6007, 6029, 6089, 6091, 6131, 6203, 6221, 6229, 6241, 6269, 6271, 6299, 6301, 6329, 6359, 6379, 6421, 6449, 6469, 6481, 6491, 6551, 6553, 6571, 6581, 6599, 6679, 6689, 6691, 6709, 6719, 6733, 6761, 6791, 6841, 6859, 6869, 6889, 6917, 6959, 6971, 6991, 7001, 7019, 7039, 7069, 7129, 7151, 7211, 7229, 7237, 7253, 7309, 7321, 7331, 7349, 7351, 7369, 7411, 7459, 7481, 7489, 7541, 7547, 7549, 7559, 7561, 7589, 7591, 7639, 7669, 7699, 7741, 7789, 7829, 7841, 7853, 7879, 7919, 7921, 7951, 8009, 8059, 8161, 8171, 8191, 8219, 8231, 8269, 8329, 8429, 8431, 8501, 8513, 8527, 8539, 8581, 8609, 8669, 8681, 8689, 8737, 8741, 8761, 8779, 8819, 8821, 8839, 8849, 8861, 8929, 8969, 8971, 9001, 9029, 9041, 9043, 9049, 9059, 9109, 9151, 9199, 9239, 9241, 9281, 9283, 9311, 9349, 9371, 9409, 9421, 9437, 9439, 9461, 9463, 9479, 9491, 9521, 9547, 9619, 9631, 9661, 9689, 9769, 9791, 9811, 9829, 9857, 9859, 9871, 9931, 9941, 10009, 10039, 10061, 10079, 10099, 10139, 10141, 10151, 10259, 10271, 10289, 10321, 10331, 10429, 10459, 10499, 10501, 10529, 10601, 10609, 10639, 10709, 10711, 10739, 10781, 10789, 10891, 10949, 10979, 11059, 11131, 11159, 11171, 11299, 11311, 11329, 11351, 11369, 11411, 11491, 11549, 11551, 11579, 11593, 11621, 11681, 11689, 11719, 11731, 11779, 11789, 11801, 11831, 11881, 11941, 11959, 11969, 11971, 12011, 12041, 12109, 12167, 12211, 12239, 12391, 12401, 12409, 12451, 12479, 12511, 12539, 12541, 12641, 12671, 12689, 12739, 12769, 12781, 12791, 12809, 12919, 12959, 12979, 13001, 13049, 13109, 13159, 13259, 13331, 13339, 13397, 13399, 13411, 13421, 13441, 13469, 13649, 13679, 13691, 13729, 13789, 13831, 13859, 13901, 13931, 14029, 14071, 14249, 14251, 14281, 14321, 14419, 14431, 14449, 14461, 14489, 14519, 14561, 14629, 14741, 14771, 14821, 14851, 14869, 14939, 14951, 15091, 15131, 15149, 15161, 15259, 15289, 15329, 15331, 15391, 15401, 15443, 15511, 15541, 15569, 15581, 15619, 15641, 15679, 15731, 15749, 15791, 15809, 15889, 15919, 15959, 16141, 16301, 16339, 16381, 16421, 16451, 16519, 16561, 16619, 16631, 16661, 16729, 16759, 16829, 16831, 16871, 17029, 17137, 17159, 17161, 17291, 17341, 17359, 17389, 17401, 17471, 17569, 17579, 17599, 17669, 17681, 17851, 17863, 17921, 18041, 18059, 18061, 18089, 18121, 18131, 18149, 18199, 18229, 18269, 18329, 18451, 18461, 18481, 18539, 18661, 18719, 18859, 18869, 18899, 19031, 19081, 19139, 19141, 19181, 19249, 19319, 19321, 19381, 19447, 19469, 19489, 19501, 19531, 19559, 19571, 19609, 19739, 19759, 19889, 19949, 19991, 20021, 20089, 20129, 20149, 20161, 20201, 20231, 20369, 20399, 20411, 20747, 20749, 20789, 20879, 20929, 21011, 21139, 21169, 21319, 21391, 21419, 21559, 21589, 21713, 21757, 21839, 21841, 21911, 22079, 22133, 22259, 22441, 22469, 22541, 22571, 22639, 22679, 22751, 22861, 22961, 23011, 23029, 23087, 23099, 23143, 23189, 23269, 23311, 23321, 23561, 23563, 23629, 23689, 23827, 23869, 23981, 24179, 24359, 24389, 24509, 24571, 24611, 24649, 24683, 24709, 24821, 24851, 25117, 25171, 25229, 25339, 25409, 25411, 25439, 25453, 25609, 25621, 25741, 25801, 25999, 26041, 26321, 26489, 26641, 26839, 26861, 26951, 27061, 27091, 27259, 27481, 27509, 27551, 27611, 27691, 28181, 28211, 28289, 28309, 28559, 28729, 28909, 29231, 29303, 29581, 29611, 29819, 30029, 30059, 30161, 30211, 30269, 30449, 30689, 30911, 30941, 31121, 31151, 31219, 31541, 31891, 32059, 32299, 32341, 32369, 32579, 32719, 32801, 32941, 32969, 33151, 33349, 33461, 33529, 33769, 33851, 34033, 34061, 34231, 34511, 34649, 34781, 35069, 35099, 35111, 35281, 35419, 35491, 35531, 35671, 35729, 35771, 35869, 36191, 36541, 36709, 36721, 36791, 36821, 36919, 37309, 37379, 37619, 38011, 38039, 38149, 38219, 38501, 38569, 38611, 38851, 39439, 39521, 39929, 40039, 40151, 40459, 40699, 40949, 41341, 41411, 41539, 41651, 41999,

42181, 42461, 42701, 42979, 43499, 43889, 43891, 44269, 44549, 44771, 45121, 45319, 45541, 46171, 46229, 46411, 46619, 47059, 47431, 47501, 47741, 48049, 48179, 48299, 48619, 49279, 49477, 49531, 49741, 49939, 50051, 50231, 51169, 51239, 51479, 51869, 51871, 52051, 52249, 52361, 53129, 53299, 53381, 53549, 53591, 53899, 54251, 54419, 54559, 54601, 54979, 55021, 55441, 55691, 55901, 55931, 56099, 56239, 56629, 56671, 57331, 58631, 59149, 59669, 60521, 60719, 60761, 61879, 61909, 62581, 62791, 62929, 63799, 64091, 65449, 65519, 65701, 66221, 66571, 66821, 67339, 67759, 67829, 68881, 69959, 70379, 70489, 71059, 71161, 72269, 73039, 73529, 74101, 75011, 75109, 75991, 76231, 76259, 76649, 77141, 77351, 77419, 78079, 78121, 78539, 78541, 78779, 80599, 80989, 81509, 81619, 81929, 82279, 83579, 83621, 84239, 84391, 84421, 84589, 84811, 85331, 85469, 85931, 88661, 88969, 89909, 90089, 90271, 90481, 91631, 91909, 93059, 93479, 93941, 94249, 95369, 96461, 97579, 100129, 102101, 102409, 102829, 103291, 104651, 104831, 105071, 105379, 106261, 106721, 106861, 107339, 108109, 108289, 110629, 111229, 111341, 111539, 112111, 114269, 114311, 114479, 115361, 115499, 116089, 116381, 116689, 117571, 117809, 118691, 118931, 119659, 120121, 120889, 122849, 123311, 123551, 125399, 128591, 131671, 132329, 132859, 133979, 133981, 134639, 135409, 135829, 136709, 137941, 138139, 141371, 141679, 142969, 143261, 144299, 145991, 146299, 146719, 147629, 148961, 149731, 150151, 151579, 153271, 154699, 154769, 158201, 158269, 158731, 161461, 162889, 164429, 166739, 166781, 167441, 167621, 169049, 169709, 172171, 173909, 174019, 174329, 174901, 175561, 176021, 178639, 180181, 180949, 181609, 183611, 183919, 184211, 188189, 195131, 195161, 195229, 195469, 196769, 197539, 197779, 199081, 200201, 201629, 202201, 203321, 204359, 204931, 206051, 206779, 207481, 208319, 211639, 213641, 214369, 216061, 216371, 217559, 224069, 225149, 225499, 231419, 234499, 236209, 239539, 242971, 244399, 244529, 245519, 251159, 259531, 262261, 266111, 268841, 269179, 276079, 286859, 298451, 298759, 303029, 303689, 304151, 307189, 314159, 315589, 316471, 318319, 325051, 326369, 328901, 336181, 336491, 339151, 340339, 347621, 361789, 366211, 366521, 372371, 374681, 410411, 415141, 435709, 483209, 609179, 614041, 620311, 647219, 650761, 690689, 786829, 1044889, 1624349, 1729001, 3847271.

CAPÍTULO 4

Número de elementos k-normais

Como explicado na Introdução, em [34] os autores obtiveram algumas fórmulas explícitas para o número de elementos k-normais para os casos particulares em que n é um potência de um primo ou da forma $n = 2^m r$ para algum primo r. Estes resultados dependem da fatoração de polinômios ciclotômicos e do número de soluções de algumas equações diofantinas lineares.

Nesta tese, segue-se outra abordagem e obtêm-se fórmulas explícitas, que também dependem de equações diofantinas lineares, para todas as extensões $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Em particular, para $k \in \{0, 1, 2, 3\}$, obtém-se fórmulas explícitas que não dependem de equações diofantinas.

4.1 Preliminares

Nesta seção apresentamos alguns resultados que serão utilizados.

A partir das definições equivalentes da noção de elementos k-normais (ver 1.55) e utilizando a função de Euler para polinômios, obtém-se a seguinte fórmula para calcular o número de elementos k-normais.

Teorema 4.1. *[18, Theorem 3.5] O número de elementos k-normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é dado por*

$$\sum_{\substack{h \mid x^n-1 \\ \text{grau}(h)=n-k}} \phi_q(h),$$

sendo que a soma percorre os divisores mônicos $h \in \mathbb{F}_q[x]$ de $x^n - 1$ de grau $n - k$.

Vemos que, nessa fórmula, o conhecimentos dos fatores irredutíveis de $x^n - 1$ é muito importante. É por isso que o próximo resultado será essencial para calcular o número de elementos k-normais.

Lema 4.2. *Sejam q a potência de um primo, n um inteiro positivo e v_d o número de fatores mônicos irredutíveis*

distintos de $x^n - 1$ de grau d sobre $\mathbb{F}_q$. Temos

$$v_d = \frac{1}{d}\sum_{r|d} \text{mdc}(q^r - 1, n) \cdot \mu\left(\frac{d}{r}\right). \tag{4.1}$$

Demonstração. Seja α um elemento primitivo em $\mathbb{F}_{q^d}$. O número de elementos da forma α^s, com $1 \leq s \leq q^d - 1$, tais que $(\alpha^s)^n = 1$ é $\text{mdc}(q^d - 1, n)$. Cada um desses elementos é raiz de algum polinômio mônico irredutível que divide $x^n - 1$ e de grau que divide d. Como cada polinômio irredutível de grau r tem r raízes em $\mathbb{F}_{q^r}$, temos $\text{mdc}(q^d - 1, n) = \sum_{r|d} r v_r$. Da fórmula de inversão de Möbius (ver [4, Theorem 2.9]) obtemos o resultado procurado. □

A partir daqui e pelo resto do capítulo, para um inteiro positivo d, v_d denota o número de fatores mônicos irredutíveis distintos de $x^n - 1$ de grau d e este valor pode ser calculado por (4.1).

Sejam p a característica de $\mathbb{F}_q$ e $n = p^s n_0$, com $\text{mdc}(n_0, p) = 1$. Observe que $x^n - 1 = (x^{n_0} - 1)^{p^s}$ e os polinômios mônicos irredutíveis que dividem $x^n - 1$ e $x^{n_0} - 1$ de grau d sobre $\mathbb{F}_q$ são os mesmos.

Corolário 4.3. *Sejam p a característica de $\mathbb{F}_q$, $n = p^s n_0$ com $\text{mdc}(n_0, p) = 1$ e d o menor inteiro positivo tal que $n_0 \mid q^d - 1$. O número de fatores irredutíveis mônicos distintos de $x^n - 1$ em $\mathbb{F}_q[x]$ é*

$$\omega_q(x^n - 1) = \frac{1}{d}\sum_{r|d} \text{mdc}(q^r - 1, n) \cdot \varphi\left(\frac{d}{r}\right).$$

Demonstração. Seja α uma raiz de $x^n - 1 = 0$. Como $x^n - 1 = (x^{n_0} - 1)^{p^s}$, temos $\alpha^{q^d - 1} = 1$ e, portanto, $\alpha \in \mathbb{F}_{q^d}$. Isso significa que se r é o menor inteiro positivo tal que $\alpha \in \mathbb{F}_{q^r}$, então $r \mid d$. Assim, se $r \nmid d$, então $v_r = 0$. Das considerações acima e do Lema 4.2, temos

$$\omega_q(x^n - 1) = \sum_{r|d} v_r = \sum_{r|d}\left(\frac{1}{r}\sum_{u|r} \text{mdc}(q^u - 1, n) \cdot \mu\left(\frac{r}{u}\right)\right).$$

Substituindo r por $v = \frac{r}{u}$, na soma, obtemos

$$\omega_q(x^n - 1) = \sum_{u|d}\sum_{v|\frac{d}{u}} \frac{1}{uv} \cdot \text{mdc}(q^u - 1, n) \cdot \mu(v) = \sum_{u|d} \frac{\text{mdc}(q^u - 1, n)}{u} \sum_{v|\frac{d}{u}} \frac{\mu(v)}{v}.$$

De [4, Theorem 2.3], temos $\sum_{v|\frac{d}{u}} \frac{\mu(v)}{v} = \frac{\varphi(\frac{d}{u})}{\frac{d}{u}}$ e, portanto,

$$\omega_q(x^n - 1) = \sum_{u|d} \frac{\text{mdc}(q^u - 1, n) \cdot \varphi(\frac{d}{u})}{d} = \frac{1}{d}\sum_{u|d} \text{mdc}(q^u - 1, n) \cdot \varphi\left(\frac{d}{u}\right).$$

□

4.2 Número de elementos k-normais

Vamos começar esta seção encontrando uma fórmula eficaz para calcular o número de elementos normais em uma extensão de corpos finitos. Vale a pena mencionar que já existem fórmulas similares na literatura (ver, por exemplo, [28, Corollary 5.2.8] ou [29, Theorem 11]). Mesmo assim, mostramos uma fórmula do número de elementos normais para exibir quais serão as ideias utilizadas na sequência.

Teorema 4.4. *Sejam p a característica do corpo $\mathbb{F}_q$ e $n = p^s n_0$ com* $\mathrm{mdc}(n_0, p) = 1$. *O número de elementos normais em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é*

$$N_0 := q^{n-n_0} \prod_{r|d} (q^r - 1)^{v_r}, \tag{4.2}$$

no qual d é o menor inteiro positivo tal que $q^d \equiv 1 \pmod{n_0}$.

Demonstração. Do Teorema 4.1, o número de elementos normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é $\phi_q(x^n - 1)$. Como $q^d \equiv 1 \pmod{n_0}$, todas as raízes de $x^{n_0} - 1$ estão em $\mathbb{F}_{q^d}$. Assim, se ξ é uma raiz de $x^{n_0} - 1$ e r é o menor inteiro positivo tal que $\xi \in \mathbb{F}_{q^r}$, então $r \mid d$. Isso quer dizer que se $v_r \neq 0$, então $r \mid d$. Sejam $g_{r,1}, \ldots, g_{r,v_r}$ os v_r fatores mônicos irredutíveis de $x^{n_0} - 1$ de grau r. Portanto,

$$x^n - 1 = \left(\prod_{r|d} \prod_{i=1}^{v_r} g_{r,i} \right)^{p^s}.$$

Como $\phi_q((g_{r,i})^{p^s}) = (q^r)^{p^s} - (q^r)^{p^s-1} = q^{r(p^s-1)}(q^r - 1)$, temos

$$\phi_q(x^n - 1) = \prod_{r|d} q^{rv_r(p^s-1)} (q^r - 1)^{v_r}.$$

Do Lema 4.2, temos

$$\sum_{r|d} rv_r = \sum_{r|d} \sum_{u|r} t_u \cdot \mu\left(\frac{r}{u}\right) = \sum_{u|d} \sum_{k|\frac{d}{u}} t_u \cdot \mu(k) = \sum_{u|d} t_u \sum_{k|\frac{d}{u}} \mu(k) = t_d = n_0.$$

Substituindo esse resultado na fórmula de $\phi_q(x^n - 1)$ e levando em consideração $n_0(p^s - 1) = n - n_0$, obtemos

$$\phi_q(x^n - 1) = q^{n-n_0} \prod_{r|d} (q^r - 1)^{v_r}.$$

□

A partir de (4.2), podemos facilmente calcular o número de elementos normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Para encontrar o valor de d, lembre-se que $d \mid \varphi(n_0)$. Ilustramos essa fórmula nas Tabelas 4.1, 4.2 e 4.3.

Computacionalmente, vemos que a fórmula é bastante eficaz, pois pode-se calcular o número de elementos normais de qualquer extensão em questão de instantes. Por exemplo, com um processador 1,4 GHz Intel Core *i*5

Dual-Core, SageMath demora 56.7ms para calcular exatamente o número de elementos normais da extensão $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ para $q = 11^{1000}$ e $n = 1000$, que é aproximadamente $4.84 \cdot 10^{1041392}$.

n	1	2	3	4	5	6	7	8	9	10
N_0	1	2	3	8	15	24	49	128	189	480
n	11	12	13	14	15	16	17	18	19	20
N_0	1023	1536	4095	6272	10125	32768	65025	96768	262143	491520

Tabela 4.1: Número de elementos normais em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ para $q = 2$.

n	1	2	3	4	5	6	7	8
N_0	2	4	18	32	160	324	1456	2048
n	9	10	11	12	13	14	15	16
N_0	13122	25600	117128	209952	913952	2119936	9447840	13107200

Tabela 4.2: Número de elementos normais em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ para $q = 3$.

n	1	2	3	4	5	6	7
N_0	3	12	27	192	675	1728	11907
n	8	9	10	11	12	13	14
N_0	49152	107163	691200	3139587	7077888	50307075	195084288

Tabela 4.3: Número de elementos normais em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ para $q = 4$.

Vejamos agora como calcular o número de elementos k-normais, generalizando a ideia utilizada no Teorema 4.4.

Teorema 4.5. *Sejam p a característica de $\mathbb{F}_q$ e $n = p^s n_0$ tal que $\operatorname{mdc}(n_0, p) = 1$. Sejam k um inteiro não negativo tal que $k < n$ e d o menor inteiro positivo tal que $q^d \equiv 1 \pmod{n_0}$. O número de elementos k-normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é*

$$N_k := \sum_{(\alpha_{r,i}) \in \mathcal{A}_d} \prod_{r|d} \prod_{\substack{i=1 \\ \alpha_{r,i}>0}}^{v_r} q^{r(\alpha_{r,i}-1)}(q^r - 1), \tag{4.3}$$

sendo $\mathcal{A}_d$ o conjunto de sequências $(\alpha_{r,i})$, para $r \mid d$ e $1 \le i \le v_r$, tais que $0 \le \alpha_{r,i} \le p^s$ e

$$\sum_{r|d} r \sum_{i=1}^{v_r} \alpha_{r,i} = n - k.$$

Em particular, se n e q são coprimos (i.e. $n = n_0$), então

$$N_k = \sum_{(a_r) \in A_d} \prod_{r|d} \binom{v_r}{a_r} (q^r - 1)^{a_r},$$

sendo A_d o conjunto de sequências $(a_r)_{r|d}$ tais que $\sum_{r|d} r a_r = n - k$ e $0 \le a_r \le v_r$.

Demonstração. Do Teorema 4.1, o número de elementos k-normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é

$$\sum_{\substack{h \mid x^n - 1 \\ \operatorname{grau}(h) = n-k}} \phi_q(h).$$

Da prova do Teorema 4.4, temos

$$x^n - 1 = \left(\prod_{r|d} \prod_{i=1}^{v_r} g_{r,i} \right)^{p^s}.$$

Se h é um fator mônico de $x^n - 1$ de grau $n - k$, então

$$h = \prod_{r|d} \prod_{i=1}^{v_r} g_{r,i}^{\alpha_{r,i}}, \tag{4.4}$$

com $(\alpha_{r,i}) \in \mathcal{A}_d$. Para esse polinômio, temos

$$\phi_q(h) = \prod_{r|d} \prod_{\substack{i=1 \\ \alpha_{r,i}>0}}^{v_r} q^{r(\alpha_{r,i}-1)}(q^r - 1),$$

logo

$$N_k = \sum_{(\alpha_{r,i})\in\mathcal{A}_d} \prod_{r|d} \prod_{\substack{i=1 \\ \alpha_{r,i}>0}}^{v_r} q^{r(\alpha_{r,i}-1)}(q^r - 1).$$

No caso em que $n = n_0$ (i.e. $s = 0$) cada $\alpha_{r,i}$ é 0 ou 1. Seja A_d o conjunto de sequências $(a_r)_{r|d}$ tais que $\sum_{r|d} r a_r = n - k$ e $0 \leq a_r \leq v_r$. Para cada a_r existem $\binom{v_r}{a_r}$ escolhas de $(\alpha_{r,1}, \ldots, \alpha_{r,v_r})$ com $\sum_{i=1}^{v_r} \alpha_{i,v_i} = a_r$. Para cada escolha de $(a_r)_{r|d}$ e $(\alpha_{r,1}, \ldots, \alpha_{r,v_r})$ existe um polinômio h da forma (4.4) e para esse polinômio temos

$$\phi_q(h) = \prod_{r|d} \prod_{\substack{i=1 \\ \alpha_{r,i}>0}}^{v_r} q^{r(\alpha_{r,i}-1)}(q^r - 1) = \prod_{r|d} (q^r - 1)^{a_r}.$$

Substituindo $\phi_q(h)$ na fórmula de elementos k-normais (ver Teorema 4.1), obtemos

$$N_k = \sum_{(a_r)\in A_d} \prod_{r|d} \binom{v_r}{a_r} (q^r - 1)^{a_r}.$$

□

A fórmula combinatória obtida para encontrar o número de elementos k-normais permite encontrar N_k para valores particulares de q e n de uma forma simples, que não depende da fatoração dos polinômios ciclotômicos, como no Teorema 4.1. Por exemplo, em [34] os autores encontraram o valor de N_k para $n = p^s$ e $q \equiv 1 \pmod{p}$, para p um número primo qualquer (ver [34, Theorem 8]). Esses resultados também poderiam ser obtidos diretamente do teorema acima.

Em [39], os autores encontram uma cota inferior para o número de elementos k-normais de $\mathbb{F}_{q^n}$ quando existem. Reencontramos o mesmo resultado usando (4.3).

Proposição 4.6. *[39, Theorem 4] Sejam $k \in \{0, 1, \ldots, n\}$ e N_k o número de elementos k-normais em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Se*

$N_k > 0$, i.e. se elementos k-normais existem em $\mathbb{F}_{q^n}$, então

$$N_k \geq \frac{N_0}{q^k}.$$

Demonstração. Temos

$$N_k = \sum_{(\alpha_{r,i})\in\mathcal{A}_d} \prod_{r|d} \prod_{\substack{i=1 \\ \alpha_{r,i}>0}}^{v_r} q^{r(\alpha_{r,i}-1)}(q^r-1) \geq \sum_{(\alpha_{r,i})\in\mathcal{A}_d} \prod_{r|d} \prod_{i=1}^{v_r} q^{r(\alpha_{r,i}-1)}(q^r-1).$$

Como

$$\sum_{r|d}\sum_{i=1}^{v_r} r(\alpha_{r,i}-1) = n-k-\sum_{r|d} rv_r = n-k-\gcd(q^d-1,n_0) = n-k-n_0,$$

e $\prod_{r|d}(q^r-1)^{v_r} = \dfrac{N_0}{q^{n-n_0}}$, obtemos $N_k \geq |\mathcal{A}_d| q^{n-k-n_0}\dfrac{N_0}{q^{n-n_0}} \geq \dfrac{N_0}{q^k}$. □

4.3 Número de elementos k-normais para pequenos valores de k

Agora mostraremos fórmulas para o número de elementos k-normais em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ para valores pequenos de k ($k = 1, 2, 3$) e daremos o valor exato desses números para valores particulares de q e n.

Proposição 4.7. *Sejam p a característica de $\mathbb{F}_q$ e $n = p^s n_0$, com* $\mathrm{mdc}(n_0, p) = 1$. *Seja d o menor inteiro positivo tal que $q^d \equiv 1 \pmod{n_0}$. O número de elementos 1-normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é*

$$N_1 = \begin{cases} v_1 q^{n-n_0-1}\displaystyle\prod_{r|d}(q^r-1)^{v_r} & \text{se } n \neq n_0, \\ v_1(q-1)^{v_1-1}\displaystyle\prod_{\substack{r|d \\ r\neq 1}}(q^r-1)^{v_r} & \text{se } n = n_0. \end{cases} \tag{4.5}$$

Demonstração. Suponha primeiro $n \neq n_0$ (assim $p^s > 1$). O conjunto $\mathcal{A}_d$, definido no Teorema 4.5, tem $v_1 = \gcd(q-1, n)$ elementos. Para todo $j \in \{1, \ldots, v_1\}$, existe um elemento $(\alpha_{r,i}) \in \mathcal{A}_d$ tal que $\alpha_{r,i} = p^s$, para $(r, i) \neq (1, j)$ e $\alpha_{1,j} = p^s - 1$. Do Teorema 4.5, obtemos

$$N_1 = \frac{v_1}{q}\prod_{r|d}\prod_{i=1}^{v_r} q^{r(p^s-1)}(q^r-1) = v_1 q^{n-n_0-1}\prod_{r|d}(q^r-1)^{v_r}.$$

Suponha agora $n = n_0$. O conjunto A_d (definido no Teorema 4.5) só tem um elemento $(a_r)_{r|d} \in A_d$ definido por $a_r = v_r$, para $r \neq 1$ e $a_1 = v_1 - 1$. Do Teorema 4.5, obtemos

$$N_1 = v_1(q-1)^{v_1-1}\prod_{\substack{r|d \\ r\neq 1}}(q^r-1)^{v_r}.$$

□

Comparando o Teorema 4.4 com a Proposição 4.7, para $n \neq n_0$, temos $N_1 = \frac{v_1}{q}N_0$ e, para $n = n_0$, $N_1 = \frac{v_1}{q-1}N_0$.

Proposição 4.8. *Sejam p a característica de $\mathbb{F}_q$ e $n = p^s n_0$, com* $\mathrm{mdc}(n_0, p) = 1$. *Seja d o menor inteiro positivo tal que $q^d \equiv 1 \pmod{n_0}$. O número de elementos 2-normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é*

$$N_2 = \begin{cases} \left(v_1 + \frac{1}{2}v_1(v_1-1) + v_2\right) q^{n-n_0-2} \prod_{r|d} (q^r-1)^{v_r} & \text{se } n \neq n_0 \text{ e } p^s > 2, \\ \left(\frac{q}{q-1}v_1 + \frac{1}{2}v_1(v_1-1) + v_2\right) q^{n-n_0-2} \prod_{r|d} (q^r-1)^{v_r} & \text{se } n \neq n_0 \text{ e } p^s = 2, \\ \left(\frac{v_1(v_1-1)}{2(q-1)^2} + \frac{v_2}{q^2-1}\right) \prod_{r|d} (q^r-1)^{v_r} & \text{se } n = n_0. \end{cases} \tag{4.6}$$

Demonstração. Suponha primeiro $n \neq n_0$ (assim $p^s > 1$). Como $p^s \sum_{r|d} r v_r = n$ (ver prova do Teorema 4.4), podemos dividir o conjunto $\mathcal{A}_d$ em três tipos de elementos.

a) Para cada $j \in \{1, \ldots, v_1\}$, existe um elemento $(\alpha_{r,i}) \in \mathcal{A}_d$ tal que $\alpha_{r,i} = p^s$ for $(r,i) \neq (1,j)$ e $\alpha_{1,j} = p^s - 2$ (sendo que consideramos dois casos: $p^s = 2$ e $p^s > 2$).

b) Para cada $\{j_1, j_2\} \subset \{1, \ldots, v_1\}$ com $j_1 \neq j_2$, existe um elemento $(\alpha_{r,i}) \in \mathcal{A}_d$ tal que $\alpha_{r,i} = p^s$ para $(r,i) \notin \{(1,j_1),(1,j_2)\}$ e $\alpha_{1,j_1} = \alpha_{1,j_2} = p^s - 1$ (só possível se $v_1 > 1$).

c) Para cada $j \in \{1, \ldots, v_2\}$, existe um elemento $(\alpha_{r,i}) \in \mathcal{A}_d$ tal que $\alpha_{r,i} = p^s$ para $(r,i) \neq (2,j)$ e $\alpha_{2,j} = p^s - 1$ (só possível se $v_2 > 0$).

Observe que $v_2 > 0$ é equivalente a $\mathrm{mdc}(q^2-1, n) > \mathrm{mdc}(q-1, n)$, que por sua vez é equivalente a $\mathrm{mdc}(q+1, n) > 2$, ou $\mathrm{mdc}(q+1, n) = 2$ e $\mathrm{mdc}(q-1, n) \mid \frac{n}{2}$.

Se $p^s > 2$, do Teorema 4.5, obtemos

$$\begin{aligned} N_2 &= \left(\frac{v_1}{q^2} + \frac{v_1(v_1-1)}{2q^2} + \frac{v_2}{q^2}\right) q^{n-n_0} \prod_{r|d} (q^r-1)^{v_r} \\ &= \left(v_1 + \frac{1}{2}v_1(v_1-1) + v_2\right) q^{n-n_0-2} \prod_{r|d} (q^r-1)^{v_r}. \end{aligned}$$

Se $p^s = 2$, do Teorema 4.5, obtemos

$$\begin{aligned} N_2 &= \left(\frac{v_1}{q(q-1)} + \frac{v_1(v_1-1)}{2q^2} + \frac{v_2}{q^2}\right) q^{n-n_0} \prod_{r|d} (q^r-1)^{v_r} \\ &= \left(\frac{q}{q-1}v_1 + \frac{1}{2}v_1(v_1-1) + v_2\right) q^{n-n_0-2} \prod_{r|d} (q^r-1)^{v_r}. \end{aligned}$$

Suponha agora $n = n_0$. O conjunto A_d tem no máximo dois elementos. Se $v_1 \geq 2$, existe um elemento $(a_r)_{r|d} \in A_d$ tal que, para $r \neq 1$, temos $a_r = v_r$ e, para $r = 1$, temos $a_1 = v_1 - 2$. Se $v_2 \geq 1$, existe um elemento $(a_r)_{r|d} \in A_d$ tal que,

para $r \neq 2$, temos $a_r = v_r$ e, para $r = 2$, temos $a_1 = v_2 - 1$. Do Teorema 4.5, obtemos

$$\begin{aligned} N_2 &= \frac{v_1(v_1-1)}{2(q-1)^2}\prod_{r|d}(q^r-1)^{v_r} + \frac{v_2}{q^2-1}\prod_{r|d}(q^r-1)^{v_r} \\ &= \left(\frac{v_1(v_1-1)}{2(q-1)^2} + \frac{v_2}{q^2-1}\right)\prod_{r|d}(q^r-1)^{v_r}. \end{aligned}$$

Observe que se $v_1 = 1$ ou $v_2 = 0$ esta fórmula continua correta. □

Proposição 4.9. *Sejam p a característica de $\mathbb{F}_q$ e $n = p^s n_0$, com* $\mathrm{mdc}(n_0, p) = 1$. *Seja d o menor inteiro positivo tal que $q^d \equiv 1 \pmod{n_0}$. O número de elementos 3-normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é*

$$N_3 = \begin{cases} \left(v_1 + \frac{1}{6}v_1(v_1-1)(v_1+4) + v_1v_2 + v_3\right)q^{n-n_0-3}\prod_{r|d}(q^r-1)^{v_r} & \text{se } p^s > 3, \\ \left(\frac{q}{q-1}v_1 + \frac{1}{6}v_1(v_1-1)(v_1+4) + v_1v_2 + v_3\right)q^{n-n_0-3}\prod_{r|d}(q^r-1)^{v_r} & \text{se } p^s = 3, \\ \left(\left(\frac{q}{q-1} + \frac{v_1-2}{6}\right)v_1(v_1-1) + v_1v_2 + v_3\right)q^{n-n_0-3}\prod_{r|d}(q^r-1)^{v_r} & \text{se } p^s = 2, \\ \left(\frac{v_1(v_1-1)(v_1-2)}{6(q-1)^3} + \frac{v_1v_2}{(q-1)(q^2-1)} + \frac{v_3}{q^3-1}\right)\prod_{r|d}(q^r-1)^{v_r} & \text{se } n = n_0. \end{cases} \tag{4.7}$$

Demonstração. Suponha primeiro $n \neq n_0$ (assim $p^s > 1$). O conjunto $\mathcal{A}_d$ do Teorema 4.5 está composto por cinco tipos de elementos.

a) Para cada $j \in \{1, \ldots, v_1\}$, existe um elemento $(\alpha_{r,i}) \in \mathcal{A}_d$ tal que $\alpha_{r,i} = p^s$, para $(r,i) \neq (1,j)$ e $\alpha_{1,j} = p^s - 3$ (devemos considerar dois casos: $p^s = 3$ e $p^s > 3$).

b) Para cada $\{j_1, j_2\} \subset \{1, \ldots, v_1\}$ com $j_1 \neq j_2$, existe um elemento $(\alpha_{r,i}) \in \mathcal{A}_d$ tal que $\alpha_{r,i} = p^s$, para $(r,i) \notin \{(1,j_1),(1,j_2)\}$, $\alpha_{1,j_1} = p^s - 2$ e $\alpha_{1,j_2} = p^s - 1$ (devemos considerar dois casos: $p_s = 2$ e $p_s > 2$).

c) Para cada conjunto $\{j_1, j_2, j_3\} \subset \{1, \ldots, v_1\}$ de três elementos distintos, existe um elemento $(\alpha_{r,i}) \in \mathcal{A}_d$ tal que $\alpha_{r,i} = p^s$, para $(r,i) \notin \{(1,j_1),(1,j_2),(1,j_3)\}$ e $\alpha_{1,j_1} = \alpha_{1,j_2} = \alpha_{1,j_3} = p^s - 1$ (existem $\frac{v_1(v_1-1)(v_1-2)}{6}$ elementos desse tipo).

d) Para cada $j_1 \in \{1, \ldots, v_1\}$ e $j_2 \in \{1, \ldots, v_2\}$, existe um elemento $(\alpha_{r,i}) \in \mathcal{A}_d$ tal que $\alpha_{r,i} = p^s$, para $(r,i) \notin \{(1,j_1),(2,j_2)\}$, $\alpha_{1,j_1} = p^s - 1$ e $\alpha_{2,j_2} = p^s - 1$.

e) Para cada $j \in \{1, \ldots, v_3\}$, existe um elemento $(\alpha_{r,i}) \in \mathcal{A}_d$ tal que $\alpha_{r,i} = p^s$, para $(r,i) \neq (3,j)$ e $\alpha_{3,j} = p^s - 1$.

Se $p^s > 3$, do Teorema 4.5, obtemos

$$\begin{aligned} N_3 &= \left(\frac{v_1}{q^3} + \frac{v_1(v_1-1)}{q^3} + \frac{v_1(v_1-1)(v_1-2)}{6q^3} + \frac{v_1v_2}{q^3} + \frac{v_3}{q^3}\right)q^{n-n_0}\prod_{r|d}(q^r-1)^{v_r} \\ &= \left(v_1 + \frac{1}{6}v_1(v_1-1)(v_1+4) + v_1v_2 + v_3\right)q^{n-n_0-3}\prod_{r|d}(q^r-1)^{v_r}. \end{aligned}$$

Se $p^s = 3$, do Teorema 4.5, obtemos

$$\begin{aligned} N_3 &= \left(\frac{v_1}{q^2(q-1)} + \frac{v_1(v_1-1)}{q^3} + \frac{v_1(v_1-1)(v_1-2)}{6q^3} + \frac{v_1v_2}{q^3} + \frac{v_3}{q^3}\right) q^{n-n_0} \prod_{r|d} (q^r-1)^{v_r} \\ &= \left(\frac{q}{q-1}v_1 + \frac{1}{6}v_1(v_1-1)(v_1+4) + v_1v_2 + v_3\right) q^{n-n_0-3} \prod_{r|d} (q^r-1)^{v_r}. \end{aligned}$$

Se $p^s = 2$, do Teorema 4.5, obtemos

$$\begin{aligned} N_3 &= \left(\frac{v_1(v_1-1)}{q^2(q-1)} + \frac{v_1(v_1-1)(v_1-2)}{6q^3} + \frac{v_1v_2}{q^3} + \frac{v_3}{q^3}\right) q^{n-n_0} \prod_{r|d} (q^r-1)^{v_r} \\ &= \left(\left(\frac{q}{q-1} + \frac{v_1-2}{6}\right) v_1(v_1-1) + v_1v_2 + v_3\right) q^{n-n_0-3} \prod_{r|d} (q^r-1)^{v_r}. \end{aligned}$$

Suponha $n = n_0$. O conjunto A_d tem no máximo três elementos. Se $v_1 \geq 3$, existe um elemento $(a_r)_{r|d} \in A_d$ tal que, para $r \neq 1$, temos $a_r = v_r$ e, para $r = 1$, temos $a_1 = v_1 - 3$. Se $v_2 \geq 1$, existe um elemento $(a_r)_{r|d} \in A_d$ tal que, para $r > 2$, temos $a_r = v_r$ e, para $r = 1$ e $r = 2$, temos $a_1 = v_1 - 1$ e $a_2 = v_2 - 1$. Se $v_3 \geq 1$, existe um elemento $(a_r)_{r|d} \in A_d$ tal que, para $r \neq 3$, temos $a_r = v_r$ e, para $r = 3$, temos $a_3 = v_3 - 1$.

Do Teorema 4.5, obtemos

$$N_3 = \left(\frac{v_1(v_1-1)(v_1-2)}{6(q-1)^3} + \frac{v_1v_2}{(q-1)(q^2-1)} + \frac{v_3}{q^3-1}\right) \prod_{r|d} (q^r-1)^{v_r}.$$

□

Ilustramos as fórmulas (4.2), (4.5), (4.6) e (4.7) nas Tabelas 4.4, 4.5 e 4.6.

n	1	2	3	4	5	6	7
N_0	24	576	13824	331776	9375000	191102976	5858625024
N_1	1	48	1728	55296	375000	47775744	244109376
N_2	0	1	72	3456	1500	4976640	0
N_3	0	0	1	96	600	276480	749952

Tabela 4.4: Número de elementos k-normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ com $0 \leq k \leq 3$ e $q = 5^2$.

n	9	10	11	12
N_0	7343167948506	190921648153600	5353168688317736	1389914829293215 68
N_1	271969183278	14686280627200	205891103396836	10295665402171968
N_2	10072932714	282428473600	0	762641881642368
N_3	373071582	0	0	42912185647968

Tabela 4.5: Número de elementos k-normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ com $0 \leq k \leq 3$ e $q = 3^3$.

n	14	15	16
N_0	67521013088256000	437893890380859375	17293822569102704640
N_1	4220063318016000	437893890380859375	1080863910568919040
N_2	281337554534400	204350482177734375	67553994410557440
N_3	32969244672000	59034583740234375	4222124650659840

Tabela 4.6: Número de elementos k-normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ com $0 \leq k \leq 3$ e $q = 2^4$.

CAPÍTULO 5

Elementos primitivos 2-normais

Como já indicamos na Introdução, Huczynska *et al.* formularam o seguinte problema (ver [18, Problem 6.3]): Determine os pares (n, k) para os quais existem elementos primitivos k-normais em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Como os casos $k = 0$ e $k = 1$ já foram completamente resolvidos, nós estudamos o caso $k = 2$ em [2]. Os resultados obtidos nesse manuscrito são mostrados neste capítulo.

Na Seção 5.1, apresentamos condições gerais para a existência de elementos primitivos k-normais em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, como também condições para casos particulares. A partir da Seção 5.2, nos concentramos no caso $k = 2$. Nessa seção, aplicamos os resultados da seção anterior estudando a existência de elementos primitivos 2-normais para $n \geq 8$ e para $q \leq 19$. Na Seção 5.3, estudamos os casos $n = 5, 6, 7$. Finalmente, na Seção 5.4, estudamos o caso $n = 4$. Como para aplicar os resultados da Seção 5.1 é necessário que $\frac{n}{2} - k > 0$, desenvolvemos novos critérios para o caso particular em que $n = 4$.

Os resultados obtidos podem ser resumidos no seguinte teorema.

Teorema 5.1 (**Teorema do elemento primitivo 2-normal**). *Sejam q a potência de um primo e n um inteiro positivo. Existe um elemento primitivo 2-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ se, e somente se, $n \geq 5$ e $\mathrm{mdc}(q^3 - q, n) \neq 1$ ou $n = 4$ e $q \equiv 1 \pmod 4$.*

Na Seção 5.5, mostramos os algoritmos usados no presente capítulo e, na Seção 5.6, são apresentadas tabelas com elementos primitivos 2-normais para casos específicos.

5.1 Resultados gerais

Pelo Teorema 4.1, sabemos que existe um elemento k-normal em $\mathbb{F}_{q^n}$ se, e somente se, $x^n - 1$ tem um divisor de grau $n - k$ (ou, equivalentemente, um divisor de grau k). Assim, se $x^n - 1$ tem um divisor de grau k em $\mathbb{F}_q[x]$ e

$$q^{\frac{n}{2}-k} \geq W(q^n - 1)W_q(x^n - 1), \tag{5.1}$$

então existe um elemento primitivo k-normal em $\mathbb{F}_{q^n}$ (ver [32, Theorem 3.3]).

Quando $k = 2$, pode-se provar que a existência de um elemento primitivo 2-normal só é possível para $n \geq 4$ (ver Teorema 1.55). Perceba que não podemos usar a desigualdade (5.1) quando $n = 4$, pois o expoente do lado direito da desigualdade é igual a zero. Dessa forma, precisamos de uma abordagem diferente para esse caso. Discutiremos esse caso na Seção 5.4. Começaremos utilizando as ideias de Huczynska *et al.* [18] e Reis [32] para aperfeiçoar a desigualdade (5.1).

Lema 5.2. *Sejam q a potência de um primo e n um inteiro positivo. Existe um elemento 2-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ se, e somente se,* $\operatorname{mdc}(q^3 - q, n) \neq 1$.

Demonstração. Como indicamos no primeiro parágrafo da seção, existe um elemento 2-normal se, e somente se, $x^n - 1$ possui um fator de grau 2 em $\mathbb{F}_q[x]$. Isso acontece se, e somente se, $x^n - 1$ tem duas raízes, não necessariamente distintas, em $\mathbb{F}_{q^2}$. As raízes são distintas quando $\operatorname{mdc}(n, q^2 - 1) \neq 1$ e as raízes são iguais quando $\operatorname{mdc}(n, q) \neq 1$. Isto é, $\operatorname{mdc}(n, q^3 - q) \neq 1$ é uma condição necessária e suficiente para a existência de um elemento 2-normal. □

Para provar o *Teorema da base primitiva normal* sem o uso do computador, os autores de [10] definiram, para $m \mid (q^n - 1)$ e $g \mid (x^n - 1)$, o número $N(m, g)$ de elementos não nulos de $\mathbb{F}_{q^n}$ que são simultaneamente m-livres e g-livres e precisaram provar que $N(q^n - 1, x^n - 1)$ é positivo. De forma similar, introduzimos a seguinte notação.

Definição 5.3. *Sejam $f, g \in \mathbb{F}_q[x]$ divisores mônicos de $x^n - 1$ tais que* $\deg f = k$ *e m um divisor positivo de $q^n - 1$. Denotamos por $N_f(g, m)$ o número de elementos g-livres $\alpha \in \mathbb{F}_{q^n}$ tais que $f \circ \alpha$ é m-livre.*

Observe que se $N_f(x^n - 1, q^n - 1) > 0$ então, pela Observação 1.78, existe um elemento $\alpha \in \mathbb{F}_{q^n}$ normal sobre $\mathbb{F}_q$ e, pela Observação 1.73, $f \circ \alpha$ é primitivo. Por outro lado, pelo Lema 1.56, $f \circ \alpha$ é k-normal. Dessa forma, nosso objetivo consiste em encontrar condições para que $N_f(x^n - 1, q^n - 1) > 0$.

Das definições de ρ_m e κ_g, temos

$$N_f(g, m) = \sum_{\alpha \in \mathbb{F}_{q^n} \setminus \ker L_f} \kappa_g(\alpha) \cdot \rho_m(L_f(\alpha)). \tag{5.2}$$

O próximo teorema generaliza [32, Theorem 3.3] usando a Definição 5.3.

Teorema 5.4. *Sejam $f, g \in \mathbb{F}_q[x]$ divisores de $x^n - 1$ tais que* $\deg f = k$ *e m um divisor positivo de $q^n - 1$. Temos $N_f(g,m) > \theta(m)\Theta_q(g)(q^n - q^{n/2+k}W(m)W_q(g))$. Em particular, se $q^{\frac{n}{2}-k} \geq W(m)W_q(g)$, então $N_f(g,m) > 0$.*

Demonstração. De (5.2) e das Proposições 1.72 e 1.77, temos

$$N_f(g,m) = \theta(m)\Theta_q(g) \sum_{\alpha \in \mathbb{F}_{q^n} \setminus \ker L_f} \sum_{\substack{d|m \\ h|g}} \frac{\mu(d)\mu_q(h)}{\varphi(d)\phi_q(h)} \sum_{\substack{\mathrm{ord}(\eta)=d \\ \mathrm{Ord}(\psi)=h}} \eta(L_f(\alpha))\psi(\alpha).$$

Se denotamos $S_f(\eta,\psi) = \sum_{\alpha \in \mathbb{F}_{q^n} \setminus \ker L_f} \eta(L_f(\alpha))\psi(\alpha)$, a equação acima pode ser reescrita como

$$\frac{N_f(g,m)}{\theta(m)\Theta_q(g)} = S_0 + S_1 + S_2 + S_3,$$

sendo $S_0 = S_f(\eta_0, \chi_0)$ (lembre que η_0 é o caráter multiplicativo trivial e χ_0 é o caráter aditivo trivial),

$$S_1 = \sum_{\substack{h|g \\ h \neq 1}} \frac{\mu_q(h)}{\phi_q(h)} \sum_{\mathrm{Ord}(\psi)=h} S_f(\eta_0,\psi), \quad S_2 = \sum_{\substack{d|m \\ d \neq 1}} \frac{\mu(d)}{\varphi(d)} \sum_{\mathrm{ord}(\eta)=d} S_f(\eta,\chi_0)$$

e

$$S_3 = \sum_{\substack{d|m \\ d \neq 1}} \sum_{\substack{h|g \\ h \neq 1}} \frac{\mu(d)\mu_q(h)}{\varphi(d)\phi_q(h)} \sum_{\substack{\mathrm{ord}(\eta)=d \\ \mathrm{Ord}(\psi)=h}} S_f(\eta,\psi).$$

Pelo Lema 1.54,

$$S_0 = \sum_{\alpha \in \mathbb{F}_{q^n} \setminus \ker(L_f)} \eta_0(L_f(\alpha))\chi_0(\alpha) = \sum_{\alpha \in \mathbb{F}_{q^n} \setminus \mathrm{Ker}\, L_f} 1 = q^n - q^k$$

e, pelo Teorema 1.58, temos

$$S_1 = \sum_{\alpha \in \mathbb{F}_{q^n} \setminus \ker(L_f)} \sum_{\substack{h|g \\ h \neq 1}} \frac{\mu_q(h)}{\phi_q(h)} \sum_{\mathrm{Ord}(\psi)=h} \psi(\alpha) = - \sum_{\alpha \in \ker(L_f)} \sum_{\substack{h|g \\ h \neq 1}} \frac{\mu_q(h)}{\phi_q(h)} \sum_{\mathrm{Ord}(\psi)=h} \psi(\alpha).$$

A última igualdade implica $|S_1| \leq q^k(W_q(g) - 1)$, já que $|\psi(\alpha)| \leq 1$, existem $\phi_q(h)$ caracteres aditivos de $\mathbb{F}_q$-ordem h e $\sum_{\substack{h|g \\ h \neq 1}} \mu_q(h) = W_q(g) - 1$.

Precisamos agora estimar as somas S_2 e S_3. Como L_f é de grau q^k e, pelo Lema 1.54, o polinômio L_f possui q^k raízes distintas, temos que L_f não tem raízes repetidas e, portanto, não pode ser da forma $G(x)^r$ para qualquer $G(x) \in \mathbb{F}_{q^n}[x]$ e $r > 1$. Portanto, pelo Lemma 1.79(a), para todo divisor positivo $d \neq 1$ de $q^n - 1$, temos

$$|S_f(\eta,\chi_0)| = \left| \sum_{\alpha \in \mathbb{F}_{q^n} \setminus \ker(L_f)} \eta(L_f(\alpha)) \right| \leq (q^k - 1)q^{\frac{n}{2}} < q^{\frac{n}{2}+k}.$$

Do Lema 1.79(b), para todo divisor $g \neq 1$ de $x^n - 1$ em $\mathbb{F}_q[x]$ e todo divisor positivo $d \neq 1$ de $q^n - 1$, tem-se

$$\left|S_f(\eta,\psi)\right| = \left|\sum_{\alpha\in\mathbb{F}_{q^n}\setminus\ker(L_f)} \eta(L_f(\alpha))\psi(\alpha)\right| \leq (q^k + 1 - 1)q^{\frac{n}{2}} = q^{\frac{n}{2}+k}.$$

Combinando todas as estimativas acima, usando que existem $\varphi(d)$ caracteres multiplicativos de ordem d, $\phi_q(h)$ caracteres aditivos de $\mathbb{F}_q$-ordem h, $\sum_{d|m}\mu(d) = W(m)$ e $\sum_{h|g}\mu_q(h) = W_q(g)$, obtemos a seguinte desigualdade:

$$\begin{aligned} N_f(g,m) &\geq \theta(m)\Theta_q(g)\left(S_0 - |S_1| - |S_2| - |S_3|\right) \\ &> \theta(m)\Theta_q(g)\left[q^n - q^k - q^k(W_q(g)-1) - q^{\frac{n}{2}+k}(W(m)-1)W_q(g)\right] \\ &> \theta(m)\Theta_q(g)(q^n - q^{\frac{n}{2}+k}W(m)W_q(g)). \end{aligned}$$

Portanto, se $W(m)W_q(g) \leq q^{\frac{n}{2}-k}$, então $N_f(g,m) > 0$. □

Nos próximos dois resultados apresentamos a técnica do crivo que segue as mesmas ideias que se encontram em [10]. Como demonstramos resultados similares nos Capítulos 2 e 3, omitimos as demonstrações neste caso. As demonstrações desses resultados podem ser encontradas em [2, Lemma 3.4] e [2, Proposition 3.5].

Lema 5.5. *Sejam $f, g \in \mathbb{F}_q[x]$ divisores de $x^n - 1$ tais que $\deg f = k$ e m um divisor positivo de $q^n - 1$. Sejam $Q_1, \ldots, Q_s$ polinômios mônicos irredutíveis e $p_1, \ldots, p_r$ números primos tais que $\operatorname{rad}(x^n - 1) = \operatorname{rad}_q(g)Q_1Q_2\cdots Q_s$ e $\operatorname{rad}(q^n - 1) = \operatorname{rad}(m)p_1p_2\cdots p_r$. Então*

$$N_f(x^n - 1, q^n - 1) \geq \sum_{i=1}^{r} N_f(g, mp_i) + \sum_{j=1}^{s} N_f(gQ_j, m) - (r + s - 1)N_f(g, m). \tag{5.3}$$

Proposição 5.6. *Sejam $f, g \in \mathbb{F}_q[x]$ divisores de $x^n - 1$ tais que $\deg f = k$ e m um divisor positivo de $q^n - 1$. Sejam $Q_1, \ldots, Q_s$ polinômios mônicos irredutíveis e $p_1, \ldots, p_r$ números primos tais que $\operatorname{rad}(x^n - 1) = \operatorname{rad}_q(g)Q_1Q_2\cdots Q_s$ e $\operatorname{rad}(q^n - 1) = \operatorname{rad}(m)p_1p_2\cdots p_r$. Suponha $\delta = 1 - \sum_{i=1}^{r}\frac{1}{p_i} - \sum_{j=1}^{s}\frac{1}{q^{\operatorname{grau}(Q_j)}} > 0$ e seja $\Delta = \frac{r+s-1}{\delta} + 2$. Se $q^{\frac{n}{2}-k} \geq W(m)W_q(g)\Delta$, então $N_f(x^n - 1, q^n - 1) > 0$.*

Quando $k \geq 2$, podemos usar o crivo para substituir a condição de existência de elementos primitivos k-normais do Teorema 5.4 por outra, na qual trocamos o fator $W_q(x^n - 1)$ por um fator linear em n.

Proposição 5.7. *Sejam $n \geq 5$ um inteiro e q a potência de um primo satisfazendo $q \geq n^2$. Se $x^n - 1$ tem um fator de grau $k \geq 2$ em $\mathbb{F}_q[x]$ e $q^{\frac{n}{2}-k} \geq (n+2)W(q^n - 1)$, então existe um elemento primitivo k-normal em $\mathbb{F}_{q^n}$.*

Demonstração. Seja $f \in \mathbb{F}_q[x]$ um fator de $x^n - 1$ de grau k. Usamos a Proposição 5.6 com $g = 1$ e $m = q^n - 1$. Sejam $Q_1, \ldots, Q_s$ polinômios mônicos irredutíveis tais que $\operatorname{rad}_q(x^n - 1) = Q_1Q_2\cdots Q_s$. Então

$$\delta = 1 - \sum_{j=1}^{s}\frac{1}{q^{\deg Q_j}} \geq 1 - \frac{n}{q} \geq 1 - \frac{1}{n} = \frac{n-1}{n} > 0,$$

já que $q \geq n^2$ e $s \leq n$. Além disto,

$$\Delta = \frac{s-1}{\delta} + 2 \leq \frac{n-1}{\frac{n-1}{n}} + 2 = n + 2.$$

Isto implica $W(m)W_q(g)\Delta \leq (n+2)W(q^n-1)$ e, da Proposição 5.6, obtemos o resultado desejado. □

5.2 Casos $n \geq 8$ e $q \leq 19$

Na presente seção começamos com o estudo do caso $k = 2$, aplicando os resultados da seção anterior, isto é, estudamos os valores de q e n para os quais existem elementos primitivos 2-normais em $\mathbb{F}_{q^n}$.

Proposição 5.8. *Sejam $q \leq 19$ a potência de um primo e $n \geq 5$ um inteiro positivo. Existe um elemento primitivo 2-normal em $\mathbb{F}_{q^n}$ se, e somente se,* $\text{mdc}(q^3 - q, n) \neq 1$.

Demonstração. Do Lema 5.2, só precisamos provar que se $x^n - 1$ possui um fator de grau 2 em $\mathbb{F}_q[x]$, então existe um elemento primitivo 2-normal em $\mathbb{F}_{q^n}$. Assim, suponha que exista um polinômio $f \in \mathbb{F}_q[x]$ de grau 2 que divida $x^n - 1$. Do Teorema 5.4, se $q^{\frac{n}{2}-2} \geq W(q^n-1)W_q(x^n-1)$, então $N_f(x^n-1, q^n-1) > 0$. Dos Lemas 1.81 e 1.83, segue $A_t \cdot q^{\frac{n}{t}} \cdot 2^{\frac{n}{a}+b} \geq W(q^n-1)W_a(x^n-1)$, sendo

$$A_t = \prod_{\substack{\wp < 2^t \\ \wp \text{ é primo} \\ \wp \neq p}} \frac{2}{\sqrt[t]{\wp}} \quad \text{e } p \text{ a característica de } \mathbb{F}_q.$$

Assim, se para algum $t > 0$, temos $q^{\frac{n}{2}-2} \geq A_t \cdot q^{\frac{n}{t}} \cdot 2^{\frac{n}{a}+b}$, então $N_f(x^n-1, q^n-1) > 0$. Para $a > \log_q 4$ e $t > \dfrac{2a}{a - \log_q 4}$, essa desigualdade é equivalente a

$$n \geq \frac{2\ln q + \ln\left(A_t \cdot 2^b\right)}{\left(\frac{1}{2} - \frac{1}{t}\right)\ln q - \frac{1}{a}\ln 2}. \tag{5.4}$$

q	a	b	(5.4) satisfeita para	q	a	b	(5.4) satisfeita para
2	5	$\frac{14}{5}$	$n \geq 69$	8	2	$\frac{7}{2}$	$n \geq 28$
3	4	5	$n \geq 46$	9	2	4	$n \geq 27$
4	3	4	$n \geq 38$	11	2	5	$n \geq 26$
5	3	6	$n \geq 35$	16	2	$\frac{15}{2}$	$n \geq 24$
7	2	3	$n \geq 31$	$\{13, 17, 19\}$	2	$\frac{q-1}{2}$	$n \geq 25$

Tabela 5.1: Valores de n que dependem de q tais que (5.4) é satisfeita com $t = 6$.

Como, para os valores de q e n da Tabela 5.1, a condição $q^{\frac{n}{2}-2} \geq W(q^n-1)W_q(x^n-1)$ é satisfeita, resta só um número finito de casos a testar para $q \leq 19$.

A Tabela 5.2 mostra os valores de q e n que não se encontram na Tabela 5.1 com $q \leq 19$ e $\text{mdc}(q^3 - q, n) \neq 1$ para os quais $q^{\frac{n}{2}-2} \geq W(q^n-1)W_q(x^n-1)$ não é satisfeita. Para os pares (q, n) da Tabela 5.2, testamos a desigualdade

q	n	q	n
2	6, 8, 9, 10, 12, 14, 15, 18, 21	9	5, 6, 8, 10
3	6, 8, 9, 10, 12, 16	11	5, 6, 8, 10, 12
4	5, 6, 8, 9, 10, 12, 15	13	6, 7, 8, 12
5	5, 6, 8, 9, 10, 12, 16	16	5, 6, 9, 10, 15
7	6, 7, 8, 9, 10, 12	17	6, 8
8	6, 7, 8, 9	19	5, 6, 8, 9, 10, 12

Tabela 5.2: Valores de q e n tais que $q \leq 19$, n não está na Tabela 5.1, $\text{mdc}(q(q-1)(q+1), n) \neq 1$ e $q^{\frac{n}{2}-2} < W(q^n-1)W_q(x^n-1)$.

$q^{\frac{n}{2}-2} \geq W(m)W_q(g)\Delta$, da Proposição 5.6, usando o Algoritmo 3 da Seção 5.5. O Algoritmo 3 retorna falso para os pares $(q,n) \in \{(2,6), (2,8), (2,9), (2,10), (2,12), (3,6), (3,8), (3,10), (3,12), (4,5), (4,6), (4,8), (4,9), (5,5), (5,6), (5,8), (5,12), (7,6), (7,8), (8,6), (8,7), (9,5), (9,6), (9,8), (11,5), (11,6), (13,6), (16,5), (16,6), (17,6), (19,5), (19,6)\}$. Para esses casos, as Tabelas 5.3, 5.4 e 5.5, da Seção 5.6, mostram de forma explícita um elemento primitivo 2-normal $\alpha \in \mathbb{F}_{q^n}$ tal que $g(\alpha) = 0$ e $g \in \mathbb{F}_p[x]$ é um polinômio irredutível e p é a característica de $\mathbb{F}_q$. □

Usamos as mesmas ideias para tratar os casos em que $n \geq 8$.

Proposição 5.9. *Seja $n \geq 8$ um inteiro positivo. Existe um elemento primitivo 2-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, para toda potência de primo q satisfazendo* $\text{mdc}(q^3 - q, n) \neq 1$.

Demonstração. Da Proposição 5.8, para toda potência de primo $q < 23$ e $n \geq 5$, existe um elemento primitivo 2-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ (sempre e quando $\text{mdc}(q^3 - q, n) \neq 1$). Assim, iremos nos concentrar em $q \geq 23$ e vamos supor que $x^n - 1$ possui um fator de grau 2 em $\mathbb{F}_q[x]$. Em outras palavras, vamos supor $\text{mdc}(q^3 - q, n) \neq 1$. Do Teorema 5.4, do Lema 1.81 e considerando $W_q(x^n - 1) \leq 2^n$, existe um elemento primitivo 2-normal em $\mathbb{F}_{q^n}$ se a desigualdade $q^{\frac{n}{2}-2} \geq 2^n \cdot A_t \cdot q^{\frac{n}{t}}$ é satisfeita para algum número real positivo t. Se $t > \dfrac{2}{1 - \log_q 4}$ e $t > \dfrac{2n}{n-4}$, então a desigualdade $q^{\frac{n}{2}-2} \geq 2^n \cdot A_t \cdot q^{\frac{n}{t}}$ é equivalente às seguintes duas desigualdades:

$$n \geq \frac{\ln(A_t) + 2\ln(q)}{\left(\frac{1}{2} - \frac{1}{t}\right)\ln(q) - \ln(2)} \quad \text{e} \quad q \geq (2^n \cdot A_t)^{\frac{2t}{(t-2)n-4t}}.$$

Para um valor fixo de $t \geq 4$, o lado direito da primeira desigualdade é uma função decrescente em $q \geq 16$. Logo, fixando $t = 7$ na primeira desigualdade, para $q \geq 23$ e $n \geq 28$, existe um elemento primitivo 2-normal em $\mathbb{F}_{q^n}$. Agora, para $14 \leq n \leq 27$, da segunda desigualdade (cujo lado direito também é uma função decrescente em n) e com $t = 6.3$, obtemos que se $n \geq 14$ e $q \geq 144$, existe um elemento primitivo 2-normal em $\mathbb{F}_{q^n}$. A seguir, verifica-se a desigualdade $q^{\frac{n}{2}-2} \geq W(q^n - 1)W_q(x^n - 1)$, para todas as potências de primos $23 \leq q < 144$ e $14 \leq n < 28$. Logo, do Teorema 5.4 e das considerações anteriores, conclui-se que existe um elemento primitivo 2-normal em $\mathbb{F}_{q^n}$ para toda potência de primo q e para todo $n \geq 14$.

Agora, vamos supor $8 \leq n \leq 13$. Da Proposição 5.7 e do Lema 1.81, existe um elemento primitivo 2-normal em $\mathbb{F}_{q^n}$ se $q \geq n^2$ e $q^{\frac{n}{2}-2} \geq (n+2)A_t \cdot q^{\frac{n}{t}}$. Define-se

$$M_t(n) = \max\left\{n^2, \left\lceil ((n+2) \cdot A_t)^{\frac{2t}{(t-2)n-4t}} \right\rceil\right\}. \tag{5.5}$$

Das desigualdades acima, se $q \geq M_t(n)$, para algum real positivo t suficientemente grande (por exemplo, para $n \geq 8$ isso significa $t > 4$), então existe um elemento primitivo 2-normal em $\mathbb{F}_{q^n}$. Para n entre 8 e 13, temos

$$M_{6.3}(8) = 6426, \quad M_6(10) = 100, \quad M_6(12) = 144,$$
$$M_6(9) = 413, \quad M_6(11) = 121, \quad M_6(13) = 169.$$

Como o Algoritmo 3 retorna verdadeiro para todas as ternas (q, n, k) tais que $8 \leq n \leq 13$, $23 \leq q < M_t(n)$ (com q a potência de um primo) e $k = 2$, a proposição está provada. □

5.3 Casos $n = 5, 6, 7$

Para $5 \leq n \leq 7$, aplicando a Proposição 5.7 e o Lema 1.81, obtemos que uma condição suficiente para a existência de um elemento primitivo 2-normal em $\mathbb{F}_{q^n}$ é $q \geq M_t(n)$, para algum número real t, com $M_t(n)$ definido por (5.5). O problema é que $M_t(n)$ é muito grande.

Para $n = 7$, a condição $\text{mdc}(q^3 - q, 7) \neq 1$ é equivalente a $q \equiv 0, \pm 1 \pmod 7$.

Proposição 5.10. *Existe um elemento primitivo* 2*-normal em* $\mathbb{F}_{q^7}$*, para toda potência de primo* q *tal que* $q \equiv 0, \pm 1 \pmod 7$.

Demonstração. Suponha primeiro $7 \mid q$. Nesse caso, $q = 7^v$ para algum inteiro $v \geq 1$. Usemos o Teorema 5.4 em combinação com o Lema 1.81. Já que $7 \nmid q^n - 1$, podemos usar a constante

$$A_t = \prod_{\substack{p \neq 7,\, p < 2^t \\ p \text{ é primo}}} \frac{2}{\sqrt[t]{p}}. \tag{5.6}$$

Do Teorema 5.4 e levando em consideração $W_q(x^7 - 1) = W_q((x-1)^7) = 2$, se a desigualdade $q^{\frac{7}{2}-2} \geq A_t \cdot q^{\frac{7}{t}} W_q(x^7 - 1) = 2A_t q^{\frac{7}{t}}$ é verdadeira, para algum número real positivo t, então $N_f(x^7 - 1, q^7 - 1) > 0$. Tomando $t = 7$, obtemos $N_f(x^7 - 1, q^7 - 1) > 0$, para $q \geq 104368$. Lembre que na Proposição 5.8 já foi provado $N_f(x^7 - 1, q^7 - 1) > 0$, para $q = 7$. Logo, resta provar esse resultado para $q \in \{7^2, 7^3, 7^4, 7^5\}$. Mas para esses valores de q, a condição $q^{\frac{7}{2}-2} \geq W(q^7 - 1) W_q(x^7 - 1)$ é satisfeita. Assim, o resultado segue do Teorema 5.4.

Se $q \equiv -1 \pmod 7$, então $7 \nmid q^7 - 1$. Dessa forma, podemos continuar usando a constante A_t dada em (5.6). Como $x^7 - 1$ tem um fator de grau 1 e 3 fatores mônicos irredutíveis de grau 2 (podemos perceber isso, por exemplo, usando o Lema 4.2), se tomamos $m = q^7 - 1$ e $g = 1$, temos $\delta = 1 - \frac{1}{q} - \frac{3}{q^2}$ e $\Delta = \frac{4-1}{\delta} + 2$. Já que se $q \geq 23$ e $q \equiv -1 \pmod 7$, então $q \geq 27$. Dessa forma, $\Delta < 5.129$ e, da Proposição 5.6, obtemos $N_f(x^7 - 1, q^7 - 1) > 0$, para as potências de primos q que satisfazem

$$q^{\frac{7}{2} - \frac{7}{t} - 2} \geq A_t \cdot 5.129 > A_t \cdot \Delta,$$

para algum número real positivo t. Tomando $t = 6.7$, obtemos $N_f(x^7 - 1, q^7 - 1) > 0$, para $q \geq 617670$. Existem

8426 potências de primos q entre 23 e 617670 tais que $q \equiv -1 \pmod 7$. Usamos o Algoritmo 5.5 para todas essas potências de primos e, em cada caso, obtemos que a desigualdade $q^{\frac{n}{2}-2} \geq W(m)W_q(g)\Delta$ é válida, para algum par de valores de m e g. Isso prova a proposição para $q \equiv -1 \pmod 7$.

Finalmente, vamos supor $q \equiv 1 \pmod 7$. Nesse caso, do Lema 1.81, podemos usar a constante

$$A_t = \frac{2}{\sqrt[t]{7^2}} \cdot \prod_{\substack{p \neq 7\,,\, p<2^t \\ p \text{ é primo}}} \frac{2}{\sqrt[t]{p}},$$

já que 7^2 aparece na fatoração de $q^7 - 1$ e $7 < 2^t$, para todo $t \geq 2.81$.

Pelo Lema 4.2, o polinômio $x^7 - 1$ se fatora em sete fatores de grau 1 em $\mathbb{F}_q[x]$. Definimos $m = q^7 - 1$ e $g = 1$ de tal forma que $\delta = 1 - \frac{7}{q}$ e $\Delta = \frac{6}{\delta} + 2 = 8 + \frac{42}{q-7}$. Supondo $q \geq 337$, temos $\Delta < 8.128$. Assim, da Proposição 5.6, obtemos que se $q^{\frac{7}{2}-2} \geq 8.128 \cdot A_t \cdot q^{\frac{7}{t}} > W(q^7 - 1)W_q(1)\Delta$, então $N_f(x^7 - 1, q^7 - 1) > 0$. Tomando $t = 6.8$, a desigualdade $q^{\frac{3}{2}-\frac{7}{t}} \geq 8.128 \cdot A_t$ é equivalente a $q \geq 2142829$, isto é, para as potências de primos maiores ou iguais a 2142829, temos $N_f(x^7 - 1, q^7 - 1) > 0$. Existem 26543 potências de primos q entre 23 e 2142829 tais que $q \equiv 1 \pmod 7$. Usamos o Algoritmo 5.5 para todas essas potências de primos e, em cada caso, obtemos que a desigualdade $q^{\frac{n}{2}-2} \geq W(m)W_q(g)\Delta$ é válida para algum par de valores de m e g. Isso prova a proposição para $q \equiv 1 \pmod 7$. □

Veja que $\text{mdc}(q^3 - q, 6) \neq 1$ é satisfeito para toda potência de primo q. Assim, das considerações do início da seção, temos $N_f(x^6 - 1, q^6 - 1) > 0$, para toda potência de primo $q \geq M_t(6)$. Para $t = 8.1$, obtemos $M_t(6) < 1.62 \cdot 10^{18}$. Logo, a partir de agora iremos supor $q < 1.62 \cdot 10^{18}$.

Veja que se q é a potência de um primo, então q é da forma 2^v, 3^v ou satisfaz $q \equiv \pm 1 \pmod 6$.

Proposição 5.11. *Existe um elemento primitivo 2-normal em $\mathbb{F}_{q^6}$ sobre $\mathbb{F}_q$, para toda potência de primo q.*

Demonstração. Consideremos primeiro $10^5 < q < 1.62 \cdot 10^{18}$ e suponha $q \equiv \pm 1 \pmod 6$. Apliquemos a Proposição 5.6, com $m = q^2 - 1$ e $g = 1$. Sejam $p_1, \ldots, p_r$ os primos dessa proposição. Pelo Lema 2.10, $p_i \equiv 1 \pmod 6$, para todo $i \in \{1, \ldots, r\}$. Sejam $\mathcal{S}_r$ e $\mathcal{P}_r$, respectivamente, a soma dos inversos e o produto dos primeiros r primos da forma $6j + 1$. Então $\mathcal{P}_r \leq p_1 \cdots p_r \leq q^4 + q^2 + 1 < 6.89 \cdot 10^{72}$, que por sua vez implica $r \leq 34$. Do Lema 4.2, se $q \equiv 1 \pmod 6$, então $x^6 - 1$ tem seis fatores mônicos de grau 1 em $\mathbb{F}_q[x]$ e se $q \equiv -1 \pmod 6$, então $x^6 - 1$ tem dois fatores mônicos de grau 1 e dois fatores mônicos irredutíveis de grau 2 em $\mathbb{F}_q[x]$. Em todos os casos, $\frac{6}{q} < \frac{2}{q} + \frac{2}{q^2}$ e $s \leq 6$ (já que $s = 4$ ou $s = 6$). Das considerações acima, obtemos $\delta \geq 1 - \mathcal{S}_{34} - \frac{6}{q}$, $r \leq 34$ e $s \leq 6$. Como $q \geq 10^5$, temos $\delta > 0.4615$ e $\Delta = 2 + \frac{r+s-1}{\delta} < 86.5$. Do Lema 1.81, temos $W(q^2 - 1) \leq A_t \cdot q^{\frac{2}{t}}$, para todo número real positivo t. Assim, se $q \geq (A_t \cdot 86.61)^{\frac{t}{t-2}}$, então da Proposição 5.6 existe um elemento primitivo 2-normal em $\mathbb{F}_{q^6}$ sobre $\mathbb{F}_q$. Para $t = 4.9$, essa desigualdade se torna $q \geq 94870$. Suponha agora $q < 94870$ e $q \equiv \pm 1 \pmod 6$. Existem 9221 potências de primos q entre 23 e 94870 tais que $q \equiv \pm 1 \pmod 6$. Usamos o Algoritmo 5.5 para todas essas potências de primos e, em cada caso, obtemos que a desigualdade $q^{\frac{n}{2}-2} \geq W(m)W_q(g)\Delta$ é válida, para algum par de valores de m e g, exceto para $q \in \{23, 25, 29, 31, 37, 41, 43, 47, 49, 59, 61, 67, 79\}$. Para essas potências de primos, a Tabela 5.6 mostra um

elemento $\alpha \in \mathbb{F}_{q^6}$ primitivo 2-normal sobre $\mathbb{F}_q$ tal que $g(\alpha) = 0$, para algum polinômio irredutível $g \in \mathbb{F}_p[x]$ com p a característica de $\mathbb{F}_q$.

Se $q = 2^v$, então $W_q(x^6 - 1) \leq 8$ (pois $x^6 - 1 = (x^3 - 1)^2$) e, se $q = 3^v$, então $W_q(x^6 - 1) = 4$ $x^6 - 1 = (x^2 - 1)^3$). Logo, do Teorema 5.4 e do Lema 1.81, verificamos a desigualdade $q \geq 8 \cdot A_t \cdot q^{\frac{6}{t}}$ com $t = 8$ e concluímos que existe um elemento primitivo 2-normal em $\mathbb{F}_{q^6}$ sobre $\mathbb{F}_q$, para $v \geq 58$ (se $q = 2^v$) e $v \geq 37$ (se $q = 3^v$). Usamos o Algoritmo 5.5 para todas as potências $q = 2^v$, com $5 \leq v \leq 57$ e $q = 3^v$, com $3 \leq v \leq 36$ (já que pela Proposição 5.8 não precisamos realizar essa verificação para $q \leq 19$) e, em cada caso, obtemos que a desigualdade $q^{\frac{n}{2}-2} \geq W(m)W_q(g)\Delta$ é válida, para algum par de valores de m e g. □

Do Lema 5.2, não existe elemento 2-normal em $\mathbb{F}_{q^5}$ sobre $\mathbb{F}_q$, se $q \equiv \pm 2 \pmod 5$. Se $5 \mid q$, então $x^5 - 1 = (x-1)^5$. Do Lema 4.2, se $q \equiv 1 \pmod 5$, então $x^5 - 1$ tem cinco fatores mônicos lineares e, se $q \equiv -1 \pmod 5$, então $x^5 - 1$ tem um fator mônico linear e dois fatores mônicos irredutíveis de grau 2.

Lema 5.12. *Seja $q \equiv 0, \pm 1 \pmod 5$ a potência de um primo. Existe um elemento primitivo 2-normal em $\mathbb{F}_{q^5}$ sobre $\mathbb{F}_q$, para $q \geq 508141$.*

Demonstração. Sejam t, u números reais positivos tais que $t + u \geq 11$ e seja

$$q^5 - 1 = q_1^{a_1} \cdots q_v^{a_v} \cdot p_1^{b_1} \cdots p_r^{b_r}$$

a fatoração de $q^5 - 1$ como produto de números primos distintos tais que $2 \leq q_i \leq 2^t$ ou $2^{t+u} \leq q_i$, para $i \in \{1, \ldots, v\}$ e $2^t < p_i < 2^{t+u}$, para $i \in \{1, \ldots, r\}$. Usemos a Proposição 5.6, com $g = 1$ e $m = q_1^{a_1} \cdots q_v^{a_v}$. Dessa forma, temos

$$\delta = 1 - \sum_{i=1}^{r} \frac{1}{p_i} - \sum_{j=1}^{s} \frac{1}{q^{\text{grau}Q_j}},$$

sendo $\text{rad}_q(x^5 - 1) = Q_1 \cdots Q_s$. Das considerações acima, temos $s \in \{1, 3, 5\}$ e $1 \leq \text{grau}Q_i \leq 2$. Agora encontremos estimativas para δ, Δ e $W(m)$.

Sejam $\mathcal{S}_{t,u}$ a soma dos inversos de todos os primos entre 2^t e 2^{t+u} e $r(t,u)$, a quantidade desses primos. Se $\mathcal{S}_{t,u} + \frac{5}{q} < 1$, então $\delta \geq 1 - \mathcal{S}_{t,u} - \frac{5}{q} > 0$. Se escolhemos $q > 10^6$ e $(t,u) = (5.8, 9.7)$, então $\mathcal{S}_{t,u} \leq 0.95566$, $\delta > 0.044335$, $r \leq r(t,u) = 4776$ e $\Delta = 2 + \frac{r+s-1}{\delta} < 2 + \frac{4776+5-1}{0.044335} \leq 107817.50$. Para estimar $W(m)$, usemos o Lema 1.81. Seja P_t o conjunto de todos os primos menores que 2^t. Do Lema 1.81, temos $W(m) \leq A_{t,u} m^{\frac{1}{t+u}} \leq A_{t,u} q^{\frac{5}{t+u}}$, com

$$A_{t,u} = \prod_{p \in P_t} \frac{2}{\sqrt[t+u]{p}} \leq 3610.54, \quad \text{já que } (t,u) = (5.8, 9.7).$$

Da Proposição 5.6, conclui-se que uma condição suficiente para a existência de um elemento primitivo 2-normal em $\mathbb{F}_{q^5}$ sobre $\mathbb{F}_q$ é $q^{\frac{1}{2}} \geq \Delta_{max} \cdot A_{t,u} \cdot q^{\frac{5}{t+u}}$ (com $\Delta_{max} = 107817.50$) ou, de forma equivalente,

$$q \geq 2.618 \cdot 10^{48} > (\Delta_{max} \cdot A_{t,u})^{\frac{2(t+u)}{t+u-10}}.$$

Vamos supor agora $q < 2.618 \cdot 10^{48}$. Aplicamos novamente a Proposição 5.6, mas desta vez com $m = q - 1$ e $g = 1$. Observe que $\mathrm{mdc}(q^4 + q^3 + q^2 + q + 1, q - 1) = 1$ ou 5. De forma similar ao Lema 2.10, se um primo diferente de 5 divide $q^4 + q^3 + q^2 + q + 1$ e não divide $q - 1$, então esse primo é da forma $10j + 1$. Assim, os primos $p_1, \ldots, p_r$ da Proposição 5.6 satisfazem $p_i \equiv 1 \pmod{10}$, para todo $i \in \{1, \ldots, r\}$. Sejam $\mathcal{S}_r$ e $\mathcal{P}_r$ a soma dos inversos e o produto, respectivamente, dos r primeiros números primos da forma $10j + 1$. Como $\mathcal{P}_r \leq q^4 + q^3 + q^2 + q + 1 < 4.698 \cdot 10^{193}$, temos $r \leq 69$ e $\mathcal{S}_r < 0.29717$. Se $q > 10^5$, então $\delta \geq 1 - \mathcal{S}_r - \frac{5}{10^5} > 0.70278$ e $\Delta = 2 + \frac{r+s-1}{\delta} < 105.874$. Usando o Lema 1.81, temos $W(q-1) \leq A_t \cdot q^{\frac{1}{t}}$, para todo número real positivo t e, portanto, se $q \geq (105.874 \cdot A_t)^{\frac{2t}{t-2}}$, para algum número real positivo $t > 2$, então $q^{\frac{1}{2}} \geq A_t \cdot q^{\frac{1}{t}} \cdot 105.874 \geq W(q-1)W_q(1)\Delta$. Dessa forma, pela Proposição 5.6 com $t = 4$, existe um elemento primitivo 2-normal em $\mathbb{F}_{q^5}$ sobre $\mathbb{F}_q$ se $q \geq 1.775 \cdot 10^{10}$.

Suponha agora $q < 1.775 \cdot 10^{10}$ e usemos novamente a Proposição 5.6, com $m = q-1$ e $g = 1$. Seguindo as mesmas ideias do parágrafo anterior, obtemos $r \leq 19$ e $\mathcal{S}_r < 0.2441801$. Para $q > 10^5$, obtemos também $\delta > 0.7558149$ e $\Delta < 32.43074$. Assim, da Proposição 5.6 e tomando $t = 4.8$, existe um elemento primitivo 2-normal em $\mathbb{F}_{q^5}$, para $q \geq 3.208 \cdot 10^8$.

Aplicamos mais uma vez a Proposição 5.6, mas desta vez com $m = \mathrm{mdc}(q^5 - 1, 2 \cdot 3 \cdot 5)$ (isto é, $W(m) \leq 8$) e $g = 1$. Sejam r e $s \leq 5$ os inteiros positivos definidos na Proposição 5.6 e sejam $\mathcal{S}_r$ e $\mathcal{P}_r$ a soma dos inversos e o produto, respectivamente, dos primeiros r números primos maiores que 5. Em particular, temos $\mathcal{P}_r \leq M^5 - 1 \leq 3.398 \cdot 10^{42}$ com $M = 3.208 \cdot 10^8$. Isso implica $r \leq 25$ e se $q \geq 10^6$, então $\delta \geq 1 - S_r - \frac{5}{q} > 0.20155$ e $\Delta \leq 145.885$. Dessa forma, a condição da Proposição 5.6 é $q^{\frac{1}{2}} \geq 1167.08 \geq 8 \cdot 145.885 \geq W(m)W_q(1)\Delta$. Logo, se $q \geq 1.363 \cdot 10^6$, então existe um elemento primitivo 2-normal em $\mathbb{F}_{q^5}$.

Voltamos a usar a Proposição 5.6, com $m = \mathrm{mdc}(q^5 - 1, 2 \cdot 3 \cdot 5)$ (isto é, $W(m) \leq 8$) e $g = 1$. Desta vez, se $q < 1.363 \cdot 10^6$, então $r \leq 19$ e $\mathcal{S}_r \leq 0.7359$. Supondo $q \geq 10^5$, obtemos $\delta \geq 0.26405$, $\Delta \leq 89.105$ e $q \geq 508141$. □

Existem 21213 potências de primos q entre 23 e 508141 tais que $q \equiv 0, \pm 1 \pmod{5}$. Se testamos o Algoritmo 3 em todas essas potências de primos, obtemos uma lista de 113 potências de primos para os quais não existem valores de m e g satisfazendo $q^{\frac{1}{2}} \geq W(m)W_q(g)\Delta$. Por esta razão, tentaremos outra abordagem.

Lema 5.13. *Seja q a potência de um primo tal que $q \equiv \pm 1 \pmod{5}$. Então $x^5 - 1 = (x-1)(x^2 - bx + 1)(x^2 + (b+1)x + 1)$, para $b \in \mathbb{F}_q$ uma raiz de $x^2 + x - 1 = 0$.*

Demonstração. Seja $\xi \neq 1$ uma raiz de $x^5 - 1$ em $\mathbb{F}_{q^2}$ e defina $b = \xi + \xi^{-1}$. Se $q \equiv 1 \pmod{5}$, então $\xi \in \mathbb{F}_q$, já que os fatores de $x^5 - 1$ são lineares em $\mathbb{F}_q[x]$. Isso implica $b \in \mathbb{F}_q$. Se $q \equiv -1 \pmod{5}$, então existe um elemento primitivo $\alpha \in \mathbb{F}_{q^2}$ tal que $\xi = \alpha^{\frac{q^2-1}{5}}$. Observe que

$$\xi^q = \alpha^{\frac{q(q-1)(q+1)}{5}} = \left(\alpha^{\frac{q+1}{5}}\right)^{q^2-q} = \left(\alpha^{\frac{q+1}{5}}\right)^{1-q} = \xi^{-1}.$$

Isso mostra que $b^q = \xi^{-1} + \xi = b$ e, consequentemente, $b \in \mathbb{F}_q$. Como $\xi^4 + \xi^3 + \xi^2 + \xi + 1 = 0$, obtemos $b^2 + b = \xi^{-2}(\xi^4 + \xi^3 + \xi^2 + \xi + 1) + 1 = 1$ e $(x^2 - bx + 1)(x^2 + (b+1)x + 1) = x^4 + x^3 + x^2 + x + 1$. □

Lema 5.14. *Sejam q a potência de um primo tal que $q \equiv \pm 1 \pmod 5$, $b \in \mathbb{F}_q$ uma raiz de $x^2 + x - 1 = 0$, α um elemento normal de $\mathbb{F}_{q^5}$ sobre $\mathbb{F}_q$ e $f = x^2 - bx + 1$. Então $L_f(\alpha) + a$ é um elemento 2-normal em $\mathbb{F}_{q^5}$, para todo $a \in \mathbb{F}_q$, exceto para um único valor de a.*

Demonstração. Escolhemos $g = (x-1)(x^2+(b+1)x+1)$ de tal forma que $fg = x^5 - 1$ e, para todo $\gamma \in \mathbb{F}_{q^5}$, tenhamos $0 = L_{fg}(\gamma) = L_g(L_f(\gamma))$. Como $x - 1$ é um fator de g, temos $L_g(a) = 0$, para todo $a \in \mathbb{F}_q$. Em particular, se α é um elemento normal em $\mathbb{F}_{q^5}$, então $L_g(L_f(\alpha) + a) = L_g(L_f(\alpha)) + L_g(a) = 0$, para todo $a \in \mathbb{F}_q$. Logo, $L_f(\alpha) + a$ tem F_q-ordem h, com h um divisor de g de grau menor ou igual a 3. Do Teorema 1.55, temos $L_f(\alpha) + a$ k-normal, para $k = 5 - \text{grau}(h) \geq 2$. Suponha grau$(h) \leq 2$. Se $x - 1 \mid h$, então $L_h(a) = 0$ e $L_h(L_f(\alpha)) \neq 0$, já que α é normal. Logo, neste caso, $L_h(L_f(\alpha)+a) \neq 0$. Isso implica que se grau$(h) \leq 2$, então $x-1 \nmid h$ e, em particular, $h \mid x^2+(b+1)x+1$. Note que $L_{x^2+(b+1)x+1}(L_f(\alpha)+a) = 0$ é equivalente a $L_{x^4+x^3+x^2+x+1}(\alpha)+L_{x^2+(b+1)x+1}(a) = 0$. Como $L_{x^2+(b+1)x+1}(a) = (b+3)a$, temos $\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = -(b+3)a$. Se $b = -3$, então $(-3)^2 + (-3) - 1 = 0$, o que é impossível, pois $5 \nmid q$. Assim, $b \neq -3$. Portanto, há um único valor de a satisfazendo $\text{Tr}_{q^5/q}(\alpha) = -(b+3)a$. Em particular, isso quer dizer que se $a \neq -(b+3)^{-1} \cdot \text{Tr}_{q^5/q}(\alpha)$, então $L_f(\alpha) + a$ é 2-normal. □

Veja que se $j \in \mathbb{F}_q$ é o único valor de $\mathbb{F}_q$ para o qual $L_f(\alpha) + j$ não é 2-normal, então $G(a) := (a - j)(L_f(\alpha) + a)$ é 2-normal, para todo $a \in \mathbb{F}_q \backslash \{j\}$ e $G(j) = 0$. Isso quer dizer que se $G(a)$ é primitivo, então $G(a)$ é 2-normal.

Dessa forma, finalizamos o caso $n = 5$ com uma abordagem computacional usando a ideia do Lema 5.14.

Proposição 5.15. *Seja q a potência de um primo. Existe um elemento primitivo 2-normal em $\mathbb{F}_{q^5}$ sobre $\mathbb{F}_q$ se, e somente se, $q \equiv 0, \pm 1 \pmod 5$.*

Demonstração. Do Lema 5.12, só precisamos provar a existência de um elemento primitivo 2-normal em $\mathbb{F}_{q^5}$, para $q \equiv 0, \pm 1 \pmod 5$ tal que $q < 508141$.

Inspirados no Lema 5.14, usamos o Algoritmo 4 para encontrar um elemento primitivo 2-normal em $\mathbb{F}_{q^5}$ sobre $\mathbb{F}_q$. Nesse algoritmo, a é um elemento primitivo de $\mathbb{F}_{q^5}$, $j \in \mathbb{F}_p$, $b \in \mathbb{F}_q$ é uma raiz de $x^2 + x - 1 = 0$ e $\beta = L_{x^2-bx+1}(a)$ para $q \equiv \pm 1 \pmod 5$. Se $5 \mid q$, então $\beta = L_{(x-1)^2}(a)$. Assim, para $q \equiv 0 \pmod 5$ ou $q \equiv \pm 1 \pmod 5$, este algoritmo retorna verdadeiro se $\beta + j$ e primitivo 2-normal em $\mathbb{F}_{q^5}$, para algum $j \in \mathbb{F}_p$, com p a característica de $\mathbb{F}_q$.

Para as 113 potências de primos q tais que $q \equiv 0, \pm 1 \pmod 5$, $q < 508141$ e o Algoritmo 3 mostrou não existir valores de m e g satisfazendo $q^{\frac{1}{2}} \geq W(m)W_q(g)\Delta$, o Algoritmo 4 encontrou sempre um elemento primitivo 2-normal, exceto para $q = 64$.

Para $q = 64$, as raízes de

$$g(x) = x^{30} + x^{27} + x^{26} + x^{23} + x^{22} + x^{21} + x^{16} + x^{14} + x^{12} + x^9 + x^6 + x^5 + x^3 + x + 1$$

em $\mathbb{F}_{q^5}$ são elementos primitivos 2-normais sobre $\mathbb{F}_q$. □

5.4 Caso $n = 4$

Em [32, Remark 3.5] é provado que não existe elemento primitivo 2-normal em $\mathbb{F}_{q^4}$, se $q \equiv 3 \pmod 4$. Vamos supor agora q uma potência de 2. Nesse caso, $x^4 - 1 = (x+1)^4$ e o único fator de grau 2 de $x^4 - 1$ é $(x+1)^2$. Logo, se β é um elemento 2-normal, então a $\mathbb{F}_q$-ordem de β deve ser $x^2 - 1$. Dessa forma, $\beta^{q^2} = \beta$, ou seja, β não é um elemento primitivo em $\mathbb{F}_{q^4}$. Portanto, se existe um elemento primitivo 2-normal em $\mathbb{F}_{q^4}$, então $q \equiv 1 \pmod 4$. Nesse caso, em $\mathbb{F}_q[x]$ podemos fatorar $x^4 - 1$ em quatro fatores lineares, isto é, $x^4 - 1 = (x+1)(x-1)(x+b)(x-b)$ com $b \in \mathbb{F}_q$ e $b^2 = -1$.

Ao longo desta seção, vamos considerar $q \equiv 1 \pmod 4$, $b \in \mathbb{F}_q$ tal que $b^2 = -1$, $f(x) = (x+1)(x+b) \in \mathbb{F}_q[x]$ um fator de $x^4 - 1$ de grau 2 e $\alpha \in \mathbb{F}_{q^4}$ um elemento normal em $\mathbb{F}_{q^4}$ sobre $\mathbb{F}_q$. Assim, $L_f(\alpha)$ é um elemento 2-normal em $\mathbb{F}_{q^4}$ (ver [32, Lemma 3.1]).

Lema 5.16. *Sejam $u, v \in \mathbb{F}_q^*$. Se $\gamma = uL_f(\alpha) + v$ é primitivo em $\mathbb{F}_{q^4}$, então γ é 2-normal em $\mathbb{F}_{q^4}$ sobre $\mathbb{F}_q$.*

Demonstração. Do Teorema 1.48, temos $L_{(x^4-1)/f}(uL_f(\alpha)+v) = uL_{x^4-1}(\alpha) + L_{(x-b)}(v^q - v) = 0$. Como $\frac{x^4-1}{f}$ é de grau 2, o conjunto $\{\gamma, \gamma^q, \gamma^{q^2}\}$ é linearmente dependente sobre $\mathbb{F}_q$. Suponha γ e γ^q linearmente dependentes. Nesse caso $\gamma^{q-1} \in \mathbb{F}_q^*$ e $\operatorname{ord}(\gamma) \leq (q-1)^2 < q^4 - 1$, contradição. Portanto, pelo Teorema 1.55, γ é 2-normal. □

Definimos $g(x) = x + \beta$ com β um elemento 2-normal em $\mathbb{F}_{q^4}$. Pelo Lema 5.16, a melhor escolha é $\beta = L_f(\alpha)$ para algum elemento normal $\alpha \in \mathbb{F}_{q^4}$, já que se $g(a)$ for primitivo, então $g(a)$ será 2-normal. Se $\beta \in \mathbb{F}_{q^2}$, então $0 = L_{\frac{x^4-1}{f}}(\beta) = \beta^{q^2} - (b+1)\beta^q + b\beta = (b+1)(\beta - \beta^q)$. Como $b^2 = -1$ e $q \equiv 1 \pmod 4$, temos $b \neq -1$. Isso implica $\beta \in \mathbb{F}_q$, o que gera uma contradição. Logo, $\beta \notin \mathbb{F}_{q^2}$.

Teorema 5.17. *Sejam m um divisor positivo de $q^4 - 1$ e $\beta = L_f(\alpha)$. Denotamos por $N_\beta(m)$ o número de elementos $a \in \mathbb{F}_q$ tais que $g(a) = a + \beta$ é m-livre. Se $q^{1/2} \geq 3W(m)$, então $N_\beta(m) > 0$.*

Demonstração. Como $\beta = L_f(\alpha) \notin \mathbb{F}_{q^2}$, temos $\mathbb{F}_{q^4} = \mathbb{F}_q(\beta)$. Portanto, do Lema 1.80, para todo caracter multiplicativo não trivial η de $\mathbb{F}_{q^4}$, temos

$$\left| \sum_{a \in \mathbb{F}_q} \eta(g(a)) \right| \leq 3\sqrt{q}. \tag{5.7}$$

Da Proposição 1.72, temos

$$N_\beta(m) = \sum_{a \in \mathbb{F}_q} \rho_m(g(a)) = \theta(m) \left(\sum_{a \in \mathbb{F}_q} \eta_0(g(a)) + \sum_{\substack{d \mid m \\ d \neq 1}} \frac{\mu(d)}{\varphi(d)} \sum_{\operatorname{ord}(\eta) = d} \sum_{a \in \mathbb{F}_q} \eta(g(a)) \right),$$

lembrando que η_0 é o caracter multiplicativo trivial de $\widehat{\mathbb{F}_q^*}$. De (5.7) e da igualdade acima,

$$\left|\frac{N_\beta(m)}{\theta(m)} - q\right| \leq \left|\sum_{\substack{d|m \\ d\neq 1}} \frac{\mu(d)}{\varphi(d)} \sum_{\mathrm{ord}(\eta)=d} \sum_{a\in\mathbb{F}_q} \eta(g(a))\right| \leq 3\sqrt{q} \sum_{\substack{d|m \\ d\neq 1}} |\mu(d)| = 3(W(m)-1)\sqrt{q}.$$

Portanto, $\frac{N_\beta(m)}{\theta(m)} \geq q - 3(W(m)-1)\sqrt{q}$ e obtemos o resultado desejado. □

A prova do seguinte resultado é similar às provas de outros resultados similares e, como na Proposição 5.6, omitimos a demonstração.

Proposição 5.18. *Sejam m um divisor positivo de q^4-1 e β o elemento 2-normal do Teorema 5.17. Sejam $p_1, \ldots, p_r$ números primos tais que $\mathrm{rad}(q^4-1) = \mathrm{rad}(m)\cdot p_1 \cdot p_2 \cdots p_r$. Suponha $\delta = 1 - \sum_{i=1}^{r} \frac{1}{p_i} > 0$ e seja $\Delta = \frac{r-1}{\delta} + 2$. Se $q^{\frac{1}{2}} \geq 3W(m)\Delta$, então $N_\beta(q^4-1) > 0$.*

Do Teorema 5.17 e da Proposição 5.18, obtemos condições de suficiência para a existência de um elemento $a \in \mathbb{F}_q$ tal que $g(a) = a+\beta$ é um elemento primitivo em $\mathbb{F}_{q^4}$. Do Lema 5.16, este elemento é também 2-normal. Dessa forma podemos concluir o caso $n = 4$.

Teorema 5.19. *Seja q a potência de um primo. Existe um elemento primitivo 2-normal em $\mathbb{F}_{q^4}$ sobre $\mathbb{F}_q$ se, e somente se, $q \equiv 1 \pmod 4$.*

Demonstração. Procedemos como no Lema 5.12. Sejam t, u números reais positivos tais que $t+u \geq 8$ e seja

$$q^4 - 1 = q_1^{a_1} \cdots q_v^{a_v} \cdot p_1^{b_1} \cdots p_r^{b_r}$$

a fatoração de q^4-1 como produto de números primos distintos tais que $2 \leq q_i \leq 2^t$ ou $2^{t+u} \leq q_i$ para $i \in \{1, \ldots, v\}$, $2^t < p_i < 2^{t+u}$ para $i \in \{1, \ldots, r\}$ e considere $m = q_1^{a_1} \cdots q_v^{a_v}$. Dessa forma, temos

$$\delta = 1 - \sum_{i=1}^{r} \frac{1}{p_i}.$$

Agora encontremos estimativas de δ, Δ e $W(m)$.

Sejam $\mathcal{S}_{t,u} < 1$ a soma dos inversos dos números primos entre 2^t e 2^{t+u} e $r(t,u)$ a quantidade desses números primos. Como no Lema 5.12, temos $r \leq r(t,u)$, $\delta \geq 1 - \mathcal{S}_{t,u}$ e $\Delta \leq 2 + \frac{r(t,u)-1}{1-\mathcal{S}_{t,u}}$. Pelo Lema 1.81, considerando $2^4 \mid q^4-1$ e $4 < t+u$, temos $W(m) < A_{t,u} \cdot q^{\frac{4}{t+u}}$, com

$$A_{t,u} = \frac{2}{\sqrt[t+u]{2^4}} \cdot \prod_{\substack{2<p<2^t \\ p \text{ é primo}}} \frac{2}{\sqrt[t+u]{p}}.$$

Pela Proposição 5.18, se $q^{\frac{1}{2}} \geq 3 \cdot A_{t,u} \cdot q^{\frac{4}{t+u}} \cdot \Delta$, então $N_\beta(q^4-1) > 0$. Essa condição é equivalente a $q \geq (3 \cdot A_{t,u} \cdot \Delta)^{\frac{2(t+u)}{t+u-8}}$. Tomando $t = 5$ e $u = 8.5$, obtemos $N_\beta(q^4-1) > 0$, para $q \geq M := 2.12 \cdot 10^{35}$.

Suponha agora $q < M$. Vamos usar a Proposição 5.18, com $m = q^2 - 1$. Sejam $p_1, \ldots, p_r$ os primos que satisfazem $\text{rad}(q^4 - 1) = \text{rad}(q^2 - 1) \cdot p_1 \cdots p_r$. Seja $i \in \{1, \ldots, r\}$. Temos p_i ímpar, $p_i \mid q^2 + 1$ e $p_i \nmid q^2 - 1$. Isso implica $4 \mid \varphi(p_i) = p_i - 1$. Seja agora $\mathcal{S}_r$ a soma dos inversos dos primeiros r números primos da forma $4j + 1$ e seja $\mathcal{P}_r$ o produto desses r números primos. Logo, de $2\mathcal{P}_r \leq q^2 + 1 < M^2 + 1$, obtemos $r \leq 33$, $\mathcal{S}_r < 0.60520004$, $\delta > 0.39479996$ e $\Delta \leq 83.054$. Como $2^3 \mid q^2 - 1$ e $3 < t$, podemos considerar

$$A_t = \frac{2}{\sqrt[t]{2^3}} \cdot \prod_{\substack{2<p<2^t \\ p \text{ é primo}}} \frac{2}{\sqrt[t]{p}}$$

como sendo a constante do Lema 1.81. Portanto, pela Proposição 5.18, se $q^{\frac{1}{2}} \geq 3 \cdot A_t \cdot q^{\frac{2}{t}} \cdot \Delta > 3W(q^2 - 1)\Delta$, então $N_\beta(q^4 - 1) > 0$. Para $t = 6.8$, obtemos $(3 \cdot A_t \cdot \Delta)^{\frac{2t}{t-4}} \leq 7.321 \cdot 10^{21}$.

Suponha agora $M := 7.321 \cdot 10^{21}$ e $q < M$. Usemos novamente a Proposição 5.18 com $m = \text{mdc}(q^4 - 1, 2 \cdot 3 \cdot 5 \cdot 7)$. Seja $\mathcal{S}_r$ a soma dos inversos dos primeiros r números primos, começando por 11, e seja $\mathcal{P}_r$ o produto desses r números primos. Observe que se $5 \nmid q^4 - 1$, então q é uma potência de 5, o que implica $3 \mid q^4 - 1$. Isso implica $2^4 \cdot 3 \mid q^4 - 1$ ou $2^4 \cdot 5 \mid q^4 - 1$. Por hipótese, r é o número de fatores primos de $q^4 - 1$ maiores que 7. Temos $r \leq 44$, já que $\mathcal{P}_r < \frac{M^4-1}{48}$. Logo, $\mathcal{S}_r < 0.7821$, $\delta > 0.2179$ e, portanto, $\Delta < 2 + \frac{44-1}{0.2179} < 199.34$. Assim, $q^{\frac{1}{2}} \geq 3W(m)\Delta$, para $q \geq 9.156 \cdot 10^7$.

Repetimos o mesmo processo com $M = 9.156 \cdot 10^7$ e $m = \text{mdc}(q^4 - 1, 2 \cdot 3 \cdot 5)$. Agora $\mathcal{S}_r$ é a soma dos inversos dos primeiros r números primos começando por 7 e $\mathcal{P}_r$ é o produto desses r números primos. Temos $\mathcal{P}_r < \frac{M^4-1}{48}$ para $r \leq 19$ e $\Delta < 70.155$. Logo, $q^{\frac{1}{2}} \geq 3 \cdot 2^3 \cdot 70.155 \geq 3W(m)\Delta$, para $q \geq 2834914$.

Repetimos esse processo uma última vez com $M = 2834914$ e $m = \text{mdc}(q^4 - 1, 2 \cdot 3 \cdot 5)$. Obtemos $r \leq 16$ e $\Delta < 51.253$. Da Proposição 5.18, temos $N_\beta(q^4 - 1) > 0$ se $q \geq 1513078 > \left(3 \cdot 2^3 \cdot 51.253\right)^2$. Do Lema 5.16, para $q \geq 1513078$ existe um elemento primitivo 2-normal em $\mathbb{F}_{q^4}$.

Existem 57731 potências de primos $q \equiv 1 \pmod 4$ menores que 1513078. Usamos uma variante do Algoritmo 3 para testar a desigualdade $q^{\frac{1}{2}} \geq 3W(m)\Delta$, para todos os valores possíveis de m. Obtemos $q^{\frac{1}{2}} \geq 3W(m)\Delta$ falso, para 918 valores de q.

Agora usamos o Algoritmo 6 para verificar, dentre os 918 valores de q, para quais valores de q existe um elemento primitivo 2-normal da forma $\beta + j$ como especificado na Subseção 5.5.3. O Algoritmo 6 retorna falso para 13, 17 e 125. A Tabela 5.7 mostra que, para esses casos, existe um elemento primitivo 2-normal $\alpha \in \mathbb{F}_{q^4}$ tal que $g(\alpha) = 0$, para algum polinômio irredutível $g \in \mathbb{F}_p[x]$, com p a característica do corpo $\mathbb{F}_q$. Isso completa a prova. □

5.5 Algoritmos do Capítulo 5

Nessa seção apresentamos alguns algoritmos utilizados no decorrer do capítulo.

5.5.1 Algoritmo para testar todos os crivos possíveis

Dada a potência de um primo q e inteiros positivos n e k satisfazendo $\frac{n}{2} > k$, o Algoritmo 3 verifica a Proposição 5.6, sendo $m = \prod_{p\in B} p$, $g = \prod_{h\in H} h$, $C = \{p_1, \ldots, p_r\}$ e $K = \{h_1, \ldots, h_s\}$.

Algoritmo 3: Verifica a Proposição 5.6 para valores dados de q, n e k

Entrada: A potência de um primo q e inteiros positivos n e k
Saída: verdadeiro ou falso

$Cond \leftarrow$ verdadeiro
$L \leftarrow$ lista ordenada dos divisores primos de $q^n - 1$
$G \leftarrow$ lista ordenada de fatores irredutíveis mônicos de $x^n - 1$
$i, j \leftarrow 0$
enquanto $i \leq \text{len}(L)$ *e* $Cond$ **faça**
  $B \leftarrow$ primeiros i elementos de L
  $C \leftarrow$ últimos $\text{len}(L) - i$ elementos de L
  $H \leftarrow$ primeiros j elementos de G
  $K \leftarrow$ últimos $\text{len}(G) - j$ elementos de G
  $\delta \leftarrow 1 - \left(\sum_{p\in C} \frac{1}{p} + \sum_{h\in K} \frac{1}{q^{\text{grau}(h)}} \right)$
  se $\delta > 0$ **então**
    $\Delta \leftarrow 2 + \frac{\text{len}(C) + \text{len}(K) - 1}{\delta}$
    $res \leftarrow \left[q^{\frac{n}{2}-k} \geq 2^{\text{len}(B)+\text{len}(H)} \cdot \Delta \right]$
    $Cond \leftarrow$ não res
  senão
    $res \leftarrow$ falso
  fim
  $j \leftarrow j + 1$
  se $j > \text{len}(G)$ **então**
    $j \leftarrow 0$
    $i \leftarrow i + 1$
  fim
fim
retorna res

5.5.2 Algoritmo para encontrar um elemento primitivo 2-normal em $\mathbb{F}_{q^5}$

Dada a potência de um primo $q \equiv 0, \pm 1 \pmod 5$, considere um elemento primitivo $a \in \mathbb{F}_{q^5}^*$ e $b \in \mathbb{F}_q$ raiz de $x^2 + x - 1$ (se q não é potência de 5). O Algoritmo 4 procura um elemento da forma $\beta + j$ com j no corpo primo que seja primitivo 2-normal em $\mathbb{F}_{q^5}$ sobre $\mathbb{F}_q$, sendo $\beta = L_{(x-1)^2}(a)$ se q é uma potência de 5 e $\beta = L_{x^2-bx+1}(a)$ se $q \equiv \pm 1 \pmod 5$.

Algoritmo 4: Verifica a existência de um elemento primitivo 2-normal em $\mathbb{F}_{q^5}$ sobre $\mathbb{F}_q$

Entrada: A potência de um primo q
Saída: verdadeiro ou falso

$a \leftarrow$ elemento primitivo de $\mathbb{F}_{q^5}$
se 5 *divide* q **então**
  $\beta \leftarrow a^{q^2} - 2a^q + a$
senão
  $b \leftarrow$ raiz de $x^2 + x - 1$
  $\beta \leftarrow a^{q^2} - ba^q + a$
fim
$(j, Verifica, Valor) \leftarrow (0, falso, verdadeiro)$
enquanto *Valor* **faça**
  $\gamma \leftarrow \beta + j$
  se γ *é primitivo* **então**
    $h \leftarrow \sum_{i=0}^{4} \gamma^{q^i} x^{4-i}$
    $k \leftarrow$ grau(mdc$(h, x^5 - 1)$)
    se $k = 2$ **então**
      $Valor \leftarrow$ falso
      $Verifica \leftarrow$ verdadeiro
    fim
  fim
  $j \leftarrow j + 1$
  se $\beta + j = \beta$ **então**
    $Valor \leftarrow$ falso
  fim
fim
retorna $Verifica$

5.5.3 Algoritmo para encontrar um elemento primitivo 2-normal em $\mathbb{F}_{q^4}$

Dada a potência de um primo $q \equiv 1 \pmod 4$, considere um elemento primitivo $a \in \mathbb{F}_{q^4}^*$. O Algoritmo 5 encontra um elemento normal $\alpha = \text{Normal}(\mathbb{F}_{q^4}, a)$. Note que um tal elemento sempre existe, logo α será encontrado para algum valor de $z \in \{1, \ldots, q^4 - 2\}$. A seguir, no Algoritmo 6 define-se $b \in \mathbb{F}_q$ que satisfaz $b^2 = -1$. Dessa forma, $x^4 - 1 = (x-1)(x+1)(x-b)(x+b)$ é a fatoração de $x^4 - 1$ em $\mathbb{F}_q[x]$. Assim, para $\beta = L_{(x+1)(x+b)}(a)$, o Algoritmo 6 procura um elemento da forma $\beta + j$ com j no corpo primo que seja primitivo em $\mathbb{F}_{q^4}$. Do Lema 5.16, se $\beta + j$ for primitivo, então $\beta + j$ será também 2-normal. A variável $Verifica$ retorna verdadeiro se tal elemento existe e falso se tal elemento não é encontrado dessa forma.

Algoritmo 5: Normal($\mathbb{F}_{q^4}, a$)

Entrada: Um elemento primitivo a no corpo $\mathbb{F}_{q^4}$
Saída: Um elemento normal α

$z \leftarrow 1$
$N \leftarrow$ verdadeiro
enquanto N **faça**
  $\alpha \leftarrow a^z$
  $g \leftarrow \sum_{i=0}^{3} \alpha^{q^i} x^{3-i}$
  $k \leftarrow \text{grau}(\text{mdc}(g, x^4 - 1))$
  se $k = 0$ **então**
    $N \leftarrow$ falso
  fim
  $z \leftarrow z + 1$
fim
retorna α

Algoritmo 6: Verifica a existência de um elemento primitivo 2-normal em $\mathbb{F}_{q^4}$ sobre $\mathbb{F}_q$

Entrada: A potência de um primo q
Saída: verdadeiro ou falso

$a \leftarrow$ elemento primitivo de $\mathbb{F}_{q^4}$
$\alpha \leftarrow \text{Normal}(\mathbb{F}_{q^4}, a)$
$b \leftarrow$ raiz de $x^2 + 1$
$\beta \leftarrow \alpha^{q^2} + (b+1)\alpha^q + b\alpha$
$(j, Verifica, Valor) \leftarrow (0, falso, verdadeiro)$
enquanto $Valor$ **faça**
  $c \leftarrow \beta + j$
  se c *é primitivo* **então**
    $Valor \leftarrow$ falso
    $Verifica \leftarrow$ verdadeiro
  fim
  $j \leftarrow j + 1$
  se $\beta + j = \beta$ **então**
    $Valor \leftarrow$ falso
  fim
fim
retorna $Verifica$

5.6 Tabelas dos casos remanescentes

(q,n)	$g(x) \in \mathbb{F}_p[x]$
$(2,6)$	$x^6+x^5+x^3+x^2+1$
$(2,8)$	$x^8+x^5+x^3+x+1$
$(2,9)$	$x^9+x^8+x^6+x^5+x^4+x^3+x^2+x+1$
$(2,10)$	$x^{10}+x^6+x^5+x^3+x^2+x+1$
$(2,12)$	$x^{12}+x^{10}+x^8+x^4+x^3+x^2+1$
$(3,6)$	$x^6+x^5+x^4+x^3+x+2$
$(3,8)$	$x^8+2x^5+x^4+2x^2+2x+2$
$(3,10)$	$x^{10}+x^8+x^7+2x^6+x^5+x^4+x^3+2x^2+x+2$
$(3,12)$	$x^{12}+x^{10}+2x^9+2x^8+x^7+x^6+2x^4+2x^3+2$

Tabela 5.3: As raízes de $g(x)$ são elementos primitivos 2-normais para $q \in \{2,3\}$.

(q,n)	$g(x) \in \mathbb{F}_p[x]$
$(4,5)$	$x^{10}+x^8+x^6+x^5+x^3+x+1$
$(4,6)$	$x^{12}+x^{11}+x^{10}+x^8+x^6+x^4+x^3+x+1$
$(4,8)$	$x^{16}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^5+x^2+1$
$(4,9)$	$x^{18}+x^{16}+x^{12}+x^{10}+x^4+x+1$
$(5,5)$	x^5+2x^3+x+2
$(5,6)$	$x^6+x^4+4x^3+x^2+2$
$(5,8)$	$x^8+4x^7+x^6+3x^4+x^3+x+3$
$(5,12)$	$x^{12}+x^{11}+3x^{10}+x^9+4x^7+3x^5+3x^3+3x^2+4x+3$
$(7,6)$	$x^6+x^4+5x^3+4x^2+6x+3$
$(7,8)$	$x^8+3x^6+6x^5+x^4+6x^3+5x^2+4x+5$
$(8,6)$	$x^{18}+x^{16}+x^{15}+x^{14}+x^{13}+x^6+x^2+x+1$
$(8,7)$	$x^{21}+x^{16}+x^{14}+x^{11}+x^7+x^6+x^5+x^3+1$

Tabela 5.4: As raízes de $g(x)$ são elementos primitivos 2-normais para $q \in \{4,5,7,8\}$.

(q,n)	$g(x) \in \mathbb{F}_p[x]$
$(9,5)$	$x^{10}+x^7+2x^6+x^5+x^4+2x^3+2$
$(9,6)$	$x^{12}+x^9+x^8+x^7+x^6+2x^4+2x^3+2x+2$
$(9,8)$	$x^{16}+2x^{14}+2x^{13}+2x^{12}+x^{11}+x^{10}+2x^9+x^8+x^5+x^4+2$
$(11,5)$	$x^5+9x^3+4x^2+9x+3$
$(11,6)$	$x^6+9x^5+x^4+3x^3+x^2+x+7$
$(13,6)$	$x^6+10x^3+11x^2+11x+2$
$(16,5)$	$x^{20}+x^{19}+x^{15}+x^{13}+x^{11}+x^{10}+x^7+x^6+x^3+x+1$
$(16,6)$	$x^{24}+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{15}+$ $x^{14}+x^{12}+x^{10}+x^8+x^7+x^3+x^2+1$
$(17,6)$	$x^6+9x^5+15x^4+6x^3+x^2+4x+14$
$(19,5)$	$x^5+2x^4+x^2+2x+16$
$(19,6)$	$x^6+17x^3+17x^2+6x+2$

Tabela 5.5: As raízes de $g(x)$ são elementos primitivos 2-normais para $q \in \{9,11,13,16,17,19\}$.

q	$g(x) \in \mathbb{F}_p[x]$
23	$x^6+3x^5+20x^4+12x^3+6x+11$
25	$x^{12}+x^{11}+3x^{10}+x^9+4x^7+3x^5+3x^3+3x^2+4x+3$
29	$x^6+14x^4+22x^3+6x^2+2x+15$
31	$x^6+19x^3+16x^2+8x+3$
37	$x^6+35x^3+4x^2+30x+2$
41	$x^6+17x^4+19x^3+9x^2+38x+17$
43	$x^6+19x^3+28x^2+21x+3$
47	$x^6+35x^4+36x^3+36x^2+19x+31$
49	$x^{12}+6x^{10}+5x^9+6x^8+6x^7+3x^6+x^5+4x^3+x^2+5x+3$
59	$x^6+13x^4+56x^3+15x^2+2x+11$
61	$x^6+49x^3+3x^2+29x+2$
67	$x^6+32x^5+58x^4+46x^3+22x^2+59x+61$
79	$x^6+19x^3+28x^2+68x+3$

Tabela 5.6: $\alpha \in \mathbb{F}_{q^6}$ é um elemento primitivo 2-normal sobre $\mathbb{F}_q$ satisfazendo $g(\alpha)=0$.

q	$g(x) \in \mathbb{F}_p[x]$
13	$x^4+11x^3+8x^2+6x+11$
17	x^4+10x^2+5x+3
125	$x^{12}+3x^{11}+4x^{10}+x^9+3x^8+2x^7+2x^5+x^4+3x^3+4x^2+x+2$

Tabela 5.7: $\alpha \in \mathbb{F}_{q^4}$ é um elemento primitivo 2-normal satisfazendo $g(\alpha)=0$.

CAPÍTULO 6

Elementos r-primitivos k-normais

Sejam q a potência de um primo, n um inteiro positivo, r um divisor positivo de $q^n - 1$ e k o grau de um polinômio em $\mathbb{F}_q[x]$ que divide $x^n - 1$. Neste capítulo, vamos apresentar resultados sobre a existência de elementos r-primitivos k-normais em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Na Seção 6.1, começamos com algumas definições e resultados sobre somas de caracteres antes de abordar o tema do capítulo. Na Seção 6.2, apresentamos resultados gerais sobre a existência de elementos r-primitivos k-normais, assim como condições para casos específicos. Na Seção 6.3, fornecemos alguns exemplos numéricos sobre corpos finitos de característica 11.

6.1 Algumas somas de caracteres

A construção de elementos k-normais dada no Lema 1.56, combinada com a seguinte definição, permitem encontrar uma forma de contar elementos r-primitivos k-normais (ver Definição 6.3).

Definição 6.1. *Para todo $\alpha \in \mathbb{F}_{q^n}$, define-se a seguinte soma de caracteres:*

$$I_0(\alpha) = \frac{1}{q^n} \sum_{\psi \in \widehat{\mathbb{F}}_{q^n}} \psi(\alpha).$$

Pelo Teorema 1.58, $I_0(\alpha) = 1$ se $\alpha = 0$ e $I_0(\alpha) = 0$, caso contrário.

Precisaremos também do seguinte resultado sobre caracteres aditivos.

Lema 6.2. *Sejam $f \in \mathbb{F}_q[x]$ um divisor de $x^n - 1$ de grau k e χ e ψ caracteres aditivos de $\mathbb{F}_{q^n}$. Então*

$$\sum_{\beta \in \mathbb{F}_{q^n}} \chi(\beta)\psi(f \circ \beta)^{-1} = \begin{cases} q^n & \text{se } \chi = f \circ \psi, \\ 0 & \text{se } \chi \neq f \circ \psi. \end{cases}$$

Além disso, para um caracter aditivo χ, o conjunto $\{\psi \in \widehat{\mathbb{F}}_{q^n} \mid \chi = f \circ \psi\}$ tem q^k elementos se $\mathrm{Ord}(\chi) \mid \frac{x^n-1}{f}$ e é o

conjunto vazio se $\mathrm{Ord}(\chi) \nmid \frac{x^n-1}{f}$.

Demonstração. Observe que, para todo $\beta \in \mathbb{F}_{q^n}$, $\chi(\beta)\psi(f\circ\beta)^{-1} = (\chi - f\circ\psi)(\beta)$. Logo, do Teorema 1.58, a soma é zero se, e somente se, $\chi \neq f\circ\psi$. Por outro lado, a soma é q^n se $\chi = f\circ\psi$.

Por definição, para todo caracter aditivo χ, temos $\mathrm{Ord}(\chi) \mid \frac{x^n-1}{f}$ se, e somente se, $\frac{x^n-1}{f}\circ\chi$ é o caracter aditivo trivial. Do Teorema 1.66, f e $\frac{x^n-1}{f}$ definem endomorfismos lineares de $\widehat{\mathbb{F}}_{q^n}$, assim como eles definem endomorfismos lineares de $\mathbb{F}_{q^n}$. Logo, dessa dualidade e do Lema 1.54, $\frac{x^n-1}{f}\circ\chi$ é o caracter aditivo trivial se, e somente se, existe um caracter aditivo ψ tal que $\chi = f\circ\psi$. Isso prova que $\{\psi \in \widehat{\mathbb{F}}_{q^n} \mid \chi = f\circ\psi\} \neq \emptyset$ se, e somente se, $\mathrm{Ord}(\chi) \mid \frac{x^n-1}{f}$.

Denotemos $\hat{L}_f$ o endomorfismo linear de $\widehat{\mathbb{F}}_{q^n}$ definido por f. Da dualidade e do Lema 1.54, $\ker\hat{L}_f$ tem q^k elementos, já que $\ker L_f$ tem q^k elementos. Logo, se $\chi \in \mathrm{im}\,\hat{L}_f$, o conjunto $\hat{L}_f^{-1}(\chi) = \{\psi \in \widehat{\mathbb{F}}_{q^n} \mid \chi = f\circ\psi\}$ tem q^k elementos, pois $\hat{L}_f^{-1}(\chi)$ é uma classe lateral de $\ker\hat{L}_f$. □

6.2 Existência de elementos r-primitivos k-normais

Como nos capítulos anteriores, encontraremos condições de existência de elementos r-primitivos k-normais usando somas de caracteres. Para tal, a próxima definição possui um papel importante.

Definição 6.3. *Sejam* $f, g \in \mathbb{F}_q[x]$ *divisores mônicos de* $x^n - 1$, *com* $\mathrm{grau} f = k$ *e* m *um divisor positivo de* $q^n - 1$. *Definimos*

$$N_{r,f}(m,g) = \sum_{\alpha\in\mathbb{F}_{q^n}^*}\sum_{\beta\in\mathbb{F}_{q^n}} \rho_m(\alpha)\kappa_g(\beta)I_0(\alpha^r - f\circ\beta).$$

Das definições de ρ_m, κ_g, I_0 e da Definição 6.3, $N_{r,f}(m,g)$ conta o número de pares $(\alpha,\beta) \in \mathbb{F}_{q^n}^* \times \mathbb{F}_{q^n}$ tais que α é m-livre, β é g-livre e $\alpha^r = f\circ\beta$. Em particular, se $N_{r,f}(q^n-1, x^n-1) > 0$, então existe um par $(\alpha,\beta) \in \mathbb{F}_{q^n}^* \times \mathbb{F}_{q^n}$ tal que α é primitivo, β é normal e $\alpha^r = f\circ\beta$. Dos Lemas 1.25 e 1.56, $\alpha^r = f\circ\beta \in \mathbb{F}_{q^n}$ é um elemento r-primitivo k-normal sobre $\mathbb{F}_q$.

Teorema 6.4. *Sejam* $f, g \in \mathbb{F}_q[x]$ *divisores mônicos de* $x^n - 1$ *com* $\mathrm{grau} f = k$ *e* m *um divisor positivo de* $q^n - 1$. *Se* $q^{\frac{n}{2}-k} \geq rW(m)W_q(\widetilde{g})$, *então* $N_{r,f}(m,g) > 0$ *com* $\widetilde{g} = \mathrm{mdc}(g, \frac{x^n-1}{f})$. *Em particular, se* $q^{\frac{n}{2}-k} \geq rW(q^n-1)W_q(\frac{x^n-1}{f})$, *então existe um elemento r-primitivo k-normal em* $\mathbb{F}_{q^n}$ *sobre* $\mathbb{F}_q$.

Demonstração. Das Definições 6.3 e 6.1 e das Proposições 1.72 e 1.77, temos

$$N_{r,f}(m,g) = \frac{\theta(m)\Theta_q(g)}{q^n}\sum_{\substack{d\mid m\\ h\mid g}}\frac{\mu(d)\mu_q(h)}{\varphi(d)\phi_q(h)}\sum_{\substack{\mathrm{ord}(\eta)=d\\ \mathrm{Ord}(\chi)=h\\ \psi\in\widehat{\mathbb{F}}_{q^n}}} S(\eta,\chi,\psi),$$

sendo

$$S(\eta,\chi,\psi) = \sum_{\alpha\in\mathbb{F}_{q^n}^*}\sum_{\beta\in\mathbb{F}_{q^n}} \eta(\alpha)\chi(\beta)\psi(\alpha^r - f\circ\beta)$$
$$= \sum_{\alpha\in\mathbb{F}_{q^n}^*} \eta(\alpha)\psi(\alpha^r)\sum_{\beta\in\mathbb{F}_{q^n}} \chi(\beta)\psi(f\circ\beta)^{-1}.$$

Denotamos novamente η_0 o caracter multiplicativo trivial e ψ_0 o caracter aditivo trivial. Escreva

$$N_{r,f}(m,g) = \frac{\theta(m)\Theta_q(g)}{q^n}\left(S_1 + S_2 + S_3 + S_4\right),$$

para $S_1 = S(\eta_0,\psi_0,\psi_0)$,

$$S_2 = \sum_{d|m}\frac{\mu(d)}{\varphi(d)}\sum_{\mathrm{ord}(\eta)=d}\sum_{\substack{\psi\in\widehat{\mathbb{F}}_{q^n}\\ \psi\neq\psi_0}} S(\eta,\psi_0,\psi), \qquad S_3 = \sum_{\substack{d|m\\ h|g\\ d\neq1 \text{ ou } h\neq1}}\frac{\mu(d)\mu_q(h)}{\varphi(d)\phi_q(h)}\sum_{\substack{\mathrm{ord}(\eta)=d\\ \mathrm{Ord}(\chi)=h}} S(\eta,\chi,\psi_0)$$

e

$$S_4 = \sum_{d|m}\sum_{\substack{h|g\\ h\neq1}}\frac{\mu(d)\mu_q(h))}{\varphi(d)\phi_q(h)}\sum_{\substack{\mathrm{ord}(\eta)=d\\ \mathrm{Ord}(\chi)=h}}\sum_{\substack{\psi\in\widehat{\mathbb{F}}_{q^n}\\ \psi\neq\psi_0}} S(\eta,\chi,\psi).$$

Temos $S_1 = (q^n-1)q^n$, já que $\eta_0(\alpha)\psi_0(\alpha^r) = 1$ e $\psi_0(\beta)\psi_0(f\circ\beta)^{-1} = 1$, para todo $\alpha\in\mathbb{F}_{q^n}^*$ e todo $\beta\in\mathbb{F}_{q^n}$.

Do Lema 6.2, para todo caracter multiplicativo η, temos

$$\sum_{\substack{\psi\in\widehat{\mathbb{F}}_{q^n}\\ \psi\neq\psi_0}} S(\eta,\psi_0,\psi) = \sum_{\substack{\psi\in\ker\hat{L}_f\\ \psi\neq\psi_0}} S(\eta,\psi_0,\psi) = (q^k-1)q^n\sum_{\alpha\in\mathbb{F}_{q^n}^*}\eta(\alpha)\psi(\alpha^r),$$

lembrando que $\ker\hat{L}_f = \{\psi\in\widehat{\mathbb{F}}_{q^n} \mid f\circ\psi = \psi_0\}$. Agora, do Lema 1.80(b) e usando que existem $\varphi(d)$ caracteres multiplicativos de ordem d, obtemos

$$|S_2| \leq \sum_{d|m}\frac{|\mu(d)|}{\varphi(d)}\sum_{\mathrm{ord}(\eta)=d} r(q^k-1)q^{\frac{3n}{2}} = r(q^k-1)q^{\frac{3n}{2}}W(m).$$

Do Teorema 1.58, temos $S(\eta,\chi,\psi_0) = 0$, se $\eta\neq\eta_0$ ou $\chi\neq\psi_0$. Logo, $S_3 = 0$.

Para obter uma cota superior para S_4, vamos utilizar $\widetilde{g} = \mathrm{mdc}(g, \frac{x^n-1}{f})$ e considerar $\hat{L}_f^{-1}(\chi) = \{\psi\in\widehat{\mathbb{F}}_{q^n} \mid \chi = f\circ\psi\}$, para todo caracter aditivo χ. Do Lema 6.2, temos $\hat{L}_f^{-1}(\chi) = \emptyset$, se $\mathrm{Ord}(\chi)\nmid\frac{x^n-1}{f}$. Logo,

$$S_4 = \sum_{d|m}\sum_{\substack{h|\widetilde{g}\\ h\neq1}}\frac{\mu(d)\mu_q(h))}{\varphi(d)\phi_q(h)}\sum_{\substack{\mathrm{ord}(\eta)=d\\ \mathrm{Ord}(\chi)=h}}\sum_{\psi\in\hat{L}_f^{-1}(\chi)} S(\eta,\chi,\psi).$$

Novamente pelo Lema 6.2, temos

$$\sum_{\psi\in\hat{L}_f^{-1}(\chi)} S(\eta,\chi,\psi) = q^{n+k}\sum_{\alpha\in\mathbb{F}_{q^n}^*}\eta(\alpha)\psi(\alpha^r),$$

para todo caracter multiplicativo η de ordem d e todo caracter aditivo χ cuja $\mathbb{F}_q$-ordem h divide $\widetilde{g}$. Logo, do Lema 1.80(b),

$$|S_4| \leq \sum_{d|m}\sum_{\substack{h|\widetilde{g}\\ h\neq 1}} \frac{|\mu(d)\mu_q(h)|}{\varphi(d)\phi_q(h)} \sum_{\substack{\mathrm{ord}(\eta)=d\\ \mathrm{Ord}(\chi)=h}} rq^{\frac{3n}{2}+k} = rq^{\frac{3n}{2}+k}W(m)(W_q(\widetilde{g})-1).$$

Portanto,

$$\begin{aligned} N_{r,f}(m,g) &\geq \frac{\theta(m)\Theta_q(g)}{q^n}\Big((q^n-1)q^n - r(q^k-1)q^{\frac{3n}{2}}W(m) \\ &\quad -rq^{\frac{3n}{2}+k}W(m)(W_q(\widetilde{g})-1)\Big) \\ &> \theta(m)\Theta_q(g)\left(q^n - rq^{\frac{n}{2}+k}W(m)W_q(\widetilde{g})\right), \end{aligned}$$

pois $rq^{\frac{n}{2}}W(m) - 1 > 0$. Assim, se $q^{\frac{n}{2}-k} \geq rW(m)W_q(\widetilde{g})$, então $N_{r,f}(m,g) > 0$.

Em particular, se $q^{\frac{n}{2}-k} \geq rW(q^n-1)W_q(\frac{x^n-1}{f})$, então existe um elemento r-primitivo k-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. □

Observação 6.5. *Veja que o último resultado com $r = k = 1$ e $f = x - 1$ generaliza resultados anteriores sobre a existência de elementos primitivos 1-normais (ver [18, Corollary 5.8]). Veja também que esse resultado com $r = 1$ é uma condição mais forte que a condição de existência de elementos primitivos k-normais dada em [32, Theorem 3.3].*

Observação 6.6. *Simultaneamente aos estudos realizados neste capítulo, em [30], os autores também estudam condições de existência de elementos r-primitivos k-normais. Eles definem $R = \frac{\mathrm{rad}(q^n-1)}{\mathrm{rad}(r)}$ e provam que se $q^{\frac{n}{2}-k} \geq r\,\mathrm{rad}(r)W(R)W_q(x^n-1)$, então existem elementos r-primitivos k-normais. Eles também usam somas de caracteres, mas utilizam outra abordagem. A título de comparação, como $W(R) = \frac{W(q^n-1)}{W(r)}$ e $\frac{\mathrm{rad}(r)}{W(r)} \geq 1$, temos $r\,\mathrm{rad}(r)W(R)W_q(x^n-1) \geq rW(q^n-1)W_q(x^n-1) \geq rW(q^n-1)W_q(\frac{x^n-1}{f})$.*

Novamente aplicamos a técnica do crivo que segue as mesmas ideias que se encontram em [10]. Como demonstramos resultados similares nos Capítulos 2 e 3, omitimos a prova de [1, Lema 3.4]. A Proposição 6.8 é uma variante de [1, Proposition 3.5], por essa razão a prova não será omitida.

Lema 6.7. *Seja $f \in \mathbb{F}_q[x]$ um divisor de $x^n - 1$ de grau k. Sejam ℓ um divisor de $q^n - 1$ e $\{p_1, ..., p_v\}$ o conjunto de todos os primos que dividem $q^n - 1$, mas que não dividem ℓ. Sejam também $g \in \mathbb{F}_q[x]$ um divisor de $x^n - 1$ e $\{P_1, ..., P_s\} \subset \mathbb{F}_q[x]$ o conjunto de todos os divisores mônicos irredutíveis de $x^n - 1$, mas que não dividem g. Então*

$$N_{r,f}(q^n-1, x^n-1) \geq \sum_{i=1}^{v} N_{r,f}(p_i\ell, g) + \sum_{i=1}^{s} N_{r,f}(\ell, P_i g) - (v+s-1)N_{r,f}(\ell, g). \tag{6.1}$$

Proposição 6.8. *Sejam ℓ um divisor positivo de q^n-1 e $\{p_1,...,p_v\}$ o conjunto de todos os primos que dividem q^n-1, mas que não dividem ℓ. Sejam $f\in\mathbb{F}_q[x]$ um divisor de x^n-1 de grau k, $\{P_1,...,P_s\}\subset\mathbb{F}_q[x]$ um conjunto de polinômios mônicos irredutíveis que dividem $\frac{x^n-1}{f}$ e $g\in\mathbb{F}_q[x]$ um divisor de x^n-1 tal que $\mathrm{rad}_q(x^n-1)=\mathrm{rad}_q(g)\cdot P_1\cdots P_s$. Suponha $\delta=1-\sum_{i=1}^{v}\frac{1}{p_i}-\sum_{i=1}^{s}\frac{1}{q^{\mathrm{grau}(P_i)}}>0$ e seja $\Delta=2+\frac{v+s-1}{\delta}$. Se $q^{\frac{n}{2}-k}\geq rW(\ell)W_q(\mathrm{mdc}(g,\frac{x^n-1}{f}))\Delta$, então $N_{r,f}(q^n-1,x^n-1)>0$.*

Demonstração. Podemos reescrever a Desigualdade (6.1) da seguinte forma

$$\begin{aligned}N_{r,f}(q^n-1,x^n-1)\geq&\sum_{i=1}^{v}\Big[N_{r,f}(p_i\ell,g)-\theta(p_i)N_{r,f}(\ell,g)\Big]\\&+\sum_{i=1}^{s}\Big[N_{r,f}(\ell,P_ig)-\Theta_q(P_i)N_{r,f}(\ell,g)\Big]+\delta N_{r,f}(\ell,g).\end{aligned}$$

Seja $i\in\{1,\dots,v\}$. Das Definições 6.3 e 6.1, das Proposições 1.72 e 1.77 e levando em consideração que θ é uma função multiplicativa, obtemos

$$\begin{aligned}N_{r,f}(p_i\ell,g)&=\frac{\theta(p_i)\theta(\ell)\Theta_q(g)}{q^n}\sum_{\substack{d\mid p_i\ell\\h\mid g}}\frac{\mu(d)\mu_q(h)}{\varphi(d)\phi_q(h)}\sum_{\substack{\mathrm{ord}(\eta)=d\\\mathrm{Ord}(\chi)=h}}\sum_{\psi\in\widehat{\mathbb{F}}_{q^n}}S(\eta,\chi,\psi)\\&=\theta(p_i)N_{r,f}(\ell,g)+\frac{\theta(p_i)\theta(\ell)\Theta_q(g)}{q^n}\sum_{\substack{d\mid p_i\ell\\p_i\mid d\\h\mid g}}\frac{\mu(d)\mu_q(h)}{\varphi(d)\phi_q(h)}\sum_{\substack{\mathrm{ord}(\eta)=d\\\mathrm{Ord}(\chi)=h}}\sum_{\psi\in\widehat{\mathbb{F}}_{q^n}}S(\eta,\chi,\psi).\end{aligned}$$

Do Lema 6.2, denotando $\widetilde{g}=\mathrm{mdc}(g,\frac{x^n-1}{f})$, temos

$$\sum_{\substack{d\mid p_i\ell\\p_i\mid d\\h\mid g}}\frac{\mu(d)\mu_q(h)}{\varphi(d)\phi_q(h)}\sum_{\substack{\mathrm{ord}(\eta)=d\\\mathrm{Ord}(\chi)=h}}\sum_{\psi\in\widehat{\mathbb{F}}_{q^n}}S(\eta,\chi,\psi)=q^n\sum_{\substack{d\mid p_i\ell\\p_i\mid d\\h\mid\widetilde{g}}}\frac{\mu(d)\mu_q(h)}{\varphi(d)\phi_q(h)}\sum_{\substack{\mathrm{ord}(\eta)=d\\\mathrm{Ord}(\chi)=h}}\sum_{\psi\in\hat{L}_f^{-1}(\chi)}\sum_{\alpha\in\mathbb{F}_{q^n}^*}\eta(\alpha)\psi(\alpha^r).\tag{6.2}$$

Do Lema 1.79(b) e utilizando que a soma em (6.2) é zero quando $\psi=\psi_0$, obtemos

$$\Big|\sum_{\substack{d\mid p_i\ell\\p_i\mid d\\h\mid\widetilde{g}}}\frac{\mu(d)\mu_q(h)}{\varphi(d)\phi_q(h)}\sum_{\substack{\mathrm{ord}(\eta)=d\\\mathrm{Ord}(\chi)=h}}\sum_{\psi\in\hat{L}_f^{-1}(\chi)}\sum_{\alpha\in\mathbb{F}_{q^n}^*}\eta(\alpha)\psi(\alpha^r)\Big|<rq^{\frac{n}{2}+k}W(\ell)W(\widetilde{g}).$$

Assim, $\big|N_{r,f}(p_i\ell,g)-\theta(p_i)N_{r,f}(\ell,g)\big|<\theta(p_i)\theta(\ell)\Theta_q(g)rq^{\frac{n}{2}+k}W(\ell)W_q(\widetilde{g})$.

Seja agora $i\in\{1,\dots,s\}$. Das Definições 6.3 e 6.1, das Proposições 1.72 e 1.77 e levando em consideração que Θ_q é uma função multiplicativa, temos

$$\begin{aligned}N_{r,f}(\ell,P_ig)&=\frac{\Theta_q(P_i)\theta(\ell)\Theta_q(g)}{q^n}\sum_{\substack{d\mid\ell\\h\mid P_ig}}\frac{\mu(d)\mu_q(h)}{\varphi(d)\phi_q(h)}\sum_{\substack{\mathrm{ord}(\eta)=d\\\mathrm{Ord}(\chi)=h}}\sum_{\psi\in\widehat{\mathbb{F}}_{q^n}}S(\eta,\chi,\psi)\\&=\Theta_q(P_i)N_{r,f}(\ell,g)+\frac{\Theta_q(P_i)\theta(\ell)\Theta_q(g)}{q^n}\sum_{\substack{d\mid\ell\\h\mid P_ig\\P_i\mid h}}\frac{\mu(d)\mu_q(h)}{\varphi(d)\phi_q(h)}\sum_{\substack{\mathrm{ord}(\eta)=d\\\mathrm{Ord}(\chi)=h}}\sum_{\psi\in\widehat{\mathbb{F}}_{q^n}}S(\eta,\chi,\psi).\end{aligned}$$

Como $P_i \mid \frac{x^n-1}{f}$ e é primo com g, segue $P_i\widetilde{g} \mid \frac{x^n-1}{f}$. Assim, do Lema 6.2, temos

$$\sum_{\substack{d\mid\ell\\ h\mid P_i g\\ P_i\nmid h}} \frac{\mu(d)\mu_q(h)}{\varphi(d)\phi_q(h)} \sum_{\substack{\mathrm{ord}(\eta)=d\\ \mathrm{Ord}(\chi)=h}} \sum_{\psi\in\widehat{\mathbb{F}}_{q^n}} S(\eta,\chi,\psi) = q^n \sum_{\substack{d\mid\ell\\ h\mid P_i\widetilde{g}\\ P_i\nmid h}} \frac{\mu(d)\mu_q(h)}{\varphi(d)\phi_q(h)} \sum_{\substack{\mathrm{ord}(\eta)=d\\ \mathrm{Ord}(\chi)=h}} \sum_{\psi\in\hat{L}_f^{-1}(\chi)} \sum_{\alpha\in\mathbb{F}_{q^n}^*} \eta(\alpha)\psi(\alpha^r).$$

Do Lema 1.79(b), obtemos

$$\Big|\sum_{\substack{d\mid\ell\\ h\mid P_i\widetilde{g}\\ P_i\nmid h}} \frac{\mu(d)\mu_q(h)}{\varphi(d)\phi_q(h)} \sum_{\substack{\mathrm{ord}(\eta)=d\\ \mathrm{Ord}(\chi)=h}} \sum_{\psi\in\hat{L}_f^{-1}(\chi)} \sum_{\alpha\in\mathbb{F}_{q^n}^*} \eta(\alpha)\psi(\alpha^r)\Big| \le rq^{\frac{n}{2}+k} W(\ell)W_q(\widetilde{g}).$$

Logo, $\left|N_{r,f}(\ell, P_i g) - \Theta_q(P_i)N_{r,f}(\ell, g)\right| \le \Theta_q(P_i)\theta(\ell)\Theta_q(g)rq^{\frac{n}{2}+k}W(\ell)W_q(\widetilde{g})$. Combinando as desigualdades acima, obtemos

$$\begin{aligned} N_{r,f}(q^n-1, x^n-1) &\ge \delta N_{r,f}(\ell, g) \\ &\quad - \theta(\ell)\Theta_q(g)W(\ell)W_q(\widetilde{g})rq^{n/2+k}\left(\sum_{i=1}^{v}\theta(p_i) + \sum_{i=1}^{s}\Theta_q(P_i)\right). \end{aligned}$$

Portanto, da prova do Teorema 6.4, temos

$$\begin{aligned} N_{r,f}(q^n-1, x^n-1) &> \delta\theta(\ell)\Theta_q(g)\left(q^n - rq^{\frac{n}{2}+k}W(\ell)W_q(\widetilde{g})\right) \\ &\quad - \theta(\ell)\Theta_q(g)W(\ell)W_q(\widetilde{g})rq^{\frac{n}{2}+k}\left(\sum_{i=1}^{v}\theta(p_i) + \sum_{i=1}^{s}\Theta_q(P_i)\right) \\ &= \delta\theta(\ell)\Theta_q(g)\Big(q^n - rq^{\frac{n}{2}+k}W(\ell)W_q(\widetilde{g})\Delta\Big). \end{aligned}$$

Da desigualdade acima decorre o resultado desejado. □

Corolário 6.9. *Se $k < n/2$, $(n-k)^2 \le q$ e $q^{\frac{n}{2}-k} \ge r(n-k+2)W(q^n-1)$, então existe um elemento r-primitivo k-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.*

Demonstração. Seja $f \in \mathbb{F}_q[x]$ um fator de x^n-1 de grau k. Vamos usar a Proposição 6.8, com $\ell = q^n-1$ e g um divisor de x^n-1 tal que $\mathrm{mdc}(g, \frac{x^n-1}{f}) = 1$ e todo fator irredutível mônico de x^n-1 divide g ou $\frac{x^n-1}{f}$. Dessa forma, o conjunto $\{P_1, \ldots, P_s\}$ está composto por todos os fatores irredutíveis mônicos que dividem $\frac{x^n-1}{f}$. Então, $\delta = 1 - \sum_{i=1}^{s}\frac{1}{q^{\mathrm{grau}(P_i)}} \ge 1 - \frac{n-k}{q} \ge 1 - \frac{1}{n-k} = \frac{n-k-1}{n-k} > 0$, pois $q \ge (n-k)^2$ e $s \le n-k$. Além disto,

$$\Delta = 2 + \frac{s-1}{\delta} \le \frac{n-k-1}{\frac{n-k-1}{n-k}} + 2 = n-k+2.$$

Isso quer dizer $W(\ell)W_q(\widetilde{g})\Delta \le (n-k+2)W(q^n-1)$ e, da Proposição 6.8, obtemos o resultado desejado. □

Definição 6.10. *Sejam t, u números reais positivos. Define-se*

$$A_{t,u} = \prod_{\substack{p<2^t \\ p \text{ é primo}}} \frac{2}{\sqrt[t+u]{p}}.$$

O próximo resultado será utilizado em casos específicos.

Lema 6.11. *Suponha $k < n/2$ e $(n-k)^2 \leq q$. Sejam t, u números reais positivos tais que $t+u > \dfrac{2n}{n-2k}$ e $\delta_{t,u} = 1 - \mathcal{S}_{t,u} - \frac{1}{n-k} > 0$, com $\mathcal{S}_{t,u}$ a soma dos inversos dos números primos entre 2^t e 2^{t+u}. Sejam $\Delta_{t,u} = 2 + \frac{v(t,u)+n-k-1}{\delta_{t,u}}$ e $v(t,u)$ a quantidade de números primos entre 2^t e 2^{t+u}. Se*

$$q \geq (rA_{t,u}\Delta_{t,u})^{\frac{2(t+u)}{(t+u)(n-2k)-2n}},$$

então existe um elemento r-primitivo k-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Demonstração. Seja

$$q^n - 1 = p_1^{a_1} \cdots p_w^{a_v} \cdot q_1^{b_1} \cdots q_v^{b_w}$$

a fatoração de $q^n - 1$ em números primos tais que $2 \leq q_i \leq 2^t$ ou $2^{t+u} \leq q_i$, para $1 \leq i \leq w$, e $2^t < p_i < 2^{t+u}$, para $1 \leq i \leq v$. Usamos a Proposição 6.8, com $\ell = q_1^{b_1} \cdots q_w^{b_w}$ e $g \in \mathbb{F}_q[x]$ um divisor de $x^n - 1$ tal que $\operatorname{mdc}(g, \frac{x^n-1}{f}) = 1$ e todo fator irredutível em $\mathbb{F}_q[x]$ de $x^n - 1$ divide g ou $\frac{x^n-1}{f}$. Dessa forma, $\{P_1, \ldots, P_s\}$ é o conjunto de todos os polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$ tais que $\operatorname{rad}_q(\frac{x^n-1}{f}) = P_1 \cdots P_s$. Então $\delta = 1 - \sum_{i=1}^{v} \frac{1}{p_i} - \sum_{i=1}^{s} \frac{1}{q^{\operatorname{grau}(P_i)}} \geq 1 - \sum_{i=1}^{v} \frac{1}{p_i} - \frac{n-k}{q} \geq \delta_{t,u} > 0$ e $\Delta = 2 + \frac{v+s-1}{\delta} \leq 2 + \frac{v(t,u)+n-k-1}{\delta_{t,u}} = \Delta_{t,u}$. Do Lema 1.81, temos $W(\ell) \leq A_{t,u}\ell^{\frac{1}{t+u}} \leq A_{t,u}q^{\frac{n}{t+u}}$. Da Proposição 6.8, conclui-se que uma condição suficiente para a existência de elementos r-primitivos k-normais em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é $q^{\frac{n}{2}-k} \geq rA_{t,u}q^{\frac{n}{t+u}}\Delta_{t,u}$ ou, equivalentemente,

$$q \geq (rA_{t,u}\Delta_{t,u})^{\frac{2(t+u)}{(t+u)(n-2k)-2n}}.$$

□

A próxima proposição apresenta um resultado assintótico sobre a existência de elementos r-primitivos k-normais em $\mathbb{F}_{q^n}$.

Proposição 6.12. *Suponha $k < n/2$ e seja t um número real tal que $t > 2n/(n-2k)$. Se*

$$q \geq \min\{U_t(n,k,r), \max\{(n-k)^2, V_t(n,k,r)\}\}, \tag{6.3}$$

então existe um elemento r-primitivo em $\mathbb{F}_{q^n}$ que é k-normal sobre $\mathbb{F}_q$, com

$$\begin{aligned} U_t(n,k,r) &= \left(r2^{n-k}A_t\right)^{\frac{2t}{t(n-2k)-2n}}, \\ V_t(n,k,r) &= (r(n-k+2)A_t)^{\frac{2t}{t(n-2k)-2n}}. \end{aligned}$$

Demonstração. Do Lema 1.81, temos

$$W(q^n-1) \leq A_t q^{n/t}.$$

Como o grau de $\frac{x^n-1}{f}$ é $n-k$, temos $W(\frac{x^n-1}{f}) \leq 2^{n-k}$. Logo, do Teorema 6.4, se

$$q^{\frac{n}{2}-k} \geq r q^{n/t} A_t 2^{n-k},$$

ou, de forma equivalente, se

$$q \geq \left(r2^{n-k}A_t\right)^{\frac{2t}{t(n-2k)-2n}},$$

então existe um elemento r-primitivo em $\mathbb{F}_{q^n}$ que é k-normal sobre $\mathbb{F}_q$. Por outro lado, se $q \geq (n-k)^2$ então, do Corolário 6.9 e do Lema 1.81, se

$$q \geq (r(n-k+2)A_t)^{\frac{2t}{t(n-2k)-2n}},$$

então existe um elemento r-primitivo em $\mathbb{F}_{q^n}$ que é k-normal sobre $\mathbb{F}_q$. □

Para cálculos numéricos, a Proposição 6.12 pode ser usada para valores grandes de n. Para valores menores de n, a Proposição 6.12 proporciona cotas muito grandes para q. Nesses casos, é melhor usar o Lema 6.11.

6.3 Exemplo numérico em característica 11

Na Proposição 6.13 e no Lema 6.14, apresentamos resultados gerais sobre a existência de elementos 3-primitivos 3-normais em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, para $\mathbb{F}_q$ um corpo finito qualquer. Já o Corolário 6.16 apresenta resultados completos quando a característica de $\mathbb{F}_q$ é 11. A característica 11 foi escolhida porque, nesse caso, os cálculos não são muito extensos e, de qualquer forma, o trabalho é similar em outras características.

Proposição 6.13. *Seja $n \geq 7$ um inteiro positivo. Para todo par (q,n) na Tabela 6.1, se $3 \mid (q^n-1)$ e x^n-1 tem um fator de grau 3 em $\mathbb{F}_q[x]$, então existe um elemento 3-primitivo 3-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.*

Demonstração. Sejam $r=3$ e $k=3$. Aplicamos a Desigualdade (6.3) e obtemos os dados da Tabela 6.1 para $n \geq 9$. Para $n=8$, usamos o Lema 6.11 com $t=6$ e $u=7$ e obtemos $q \geq 7.05 \cdot 10^{21}$. Para $n=7$, usamos também o Lema 6.11 com $t=8.5$ e $u=9.5$ e obtemos $q \geq 8.66 \cdot 10^{184}$.

Obtemos o resultado desejado pela Proposição 6.12, para $n \geq 9$, e pelo Lema 6.11, para $n=7$ e $n=8$. □

t ou (t,u)	(q,n)
$t = 7.5$	$q \geq 11$ e $n \geq 70$
$t = 7$	$q \geq 16$ e $n \geq 44$
$t = 7$	$q \geq 107$ e $n \geq 19$
$t = 6.3$	$q \geq 211$ e $n \geq 13$
$t = 6.3$	$q \geq 211$ e $n \geq 13$
$t = 6.6$	$q \geq 980$ e $n = 12$
$t = 6.8$	$q \geq 14459$ e $n = 11$
$t = 7.4$	$q \geq 3.63 \cdot 10^6$ e $n = 10$
$t = 8.2$	$q \geq 2.24 \cdot 10^{13}$ e $n = 9$
$(t,u) = (6,7)$	$q \geq 7.05 \cdot 10^{21}$ e $n = 8$
$(t,u) = (8.5,9.5)$	$q \geq 8.66 \cdot 10^{184}$ e $n = 7$

Tabela 6.1: Valores de q e n para os quais existe um elemento 3-primitivo 3-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Com o próximo lema obtemos um melhor resultado para $n = 7$.

Lema 6.14. *Seja q a potência de um primo tal que $2.132 \cdot 10^{15} \leq q < 8.66 \cdot 10^{184}$. Se $3 \mid (q^7 - 1)$ e $x^7 - 1$ tem um fator de grau 3 em $\mathbb{F}_q[x]$, então existe um elemento 3-primitivo 3-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.*

Demonstração. Sejam q a potência de um primo tal que $q < 8.66 \cdot 10^{184}$, $3 \mid (q^7 - 1)$ e $x^7 - 1$ tem um fator $f \in \mathbb{F}_q[x]$ de grau 3. Vamos usar a Proposição 6.8, com $\ell = q - 1$, e $g = f$, se $7 \nmid q$ ou $g = 1$ se $7 \mid q$ (dessa forma $s \leq 4$ e $\mathrm{mdc}(g, \frac{x^n-1}{f}) = 1$). Seja p um número primo. Se $p \mid (q^7 - 1)$, mas $p \nmid (q - 1)$, então $7 \mid \varphi(p) = p - 1$. Isso quer dizer que o conjunto $\{p_1, \ldots, p_v\}$ está composto de primos da forma $14j + 1$. Sejam $\mathcal{S}_v$ e $\mathcal{P}_v$ a soma dos inversos e o produto, respectivamente, dos primeiros v números primos da forma $14j + 1$. Como $\{p_1, \ldots, p_v\}$ é um conjunto de primos que dividem $q^6 + q^5 + q^4 + q^3 + q^2 + q + 1$, segue $\mathcal{P}_v \leq q^6 + q^5 + q^4 + q^3 + q^2 + q + 1 < 4.22 \cdot 10^{1109}$. Portanto, $v \leq 299$ e $\mathcal{S}_v < 0.19113$. Supondo $q > 10^5$, temos

$$\delta = 1 - \sum_{i=1}^{v} \frac{1}{p_i} - \sum_{i=1}^{s} \frac{1}{q^{\deg P_i}} \geq 1 - \mathcal{S}_v - \frac{4}{q} > 0.80883$$

e $\Delta = 2 + \frac{v+s-1}{\delta} < 1310.0623$. Dessa forma, se $q \geq (3 \cdot 1310.0623 \cdot A_t)^{\frac{2t}{t-2}}$, para algum número real $t > 2$, então $q^{\frac{7}{2}-3} \geq 3 \cdot A_t \cdot q^{\frac{1}{t}} \cdot 1310.0623 > 3 \cdot W(q-1) \cdot W_q(1) \cdot \Delta$. Para $t = 5.4$, pela Proposição 6.8, se $q \geq 2.132 \cdot 10^{15}$, então existe um elemento 3-primitivo 3-normal em $\mathbb{F}_{q^7}$ sobre $\mathbb{F}_q$. □

O Algoritmo 8 percorre todos os valores possíveis de ℓ e g na Proposição 6.8. Para aplicar o crivo, todos os fatores irredutíveis de $x^n - 1$ que não dividem $\frac{x^n-1}{f}$ devem dividir g. Dessa forma, para aplicar o crivo precisamos de um fator $f \in \mathbb{F}_q[x]$ de $x^n - 1$ de grau 3 para poder analisar os valores possíveis de g. Para isso utilizamos o Lema 4.2 que indica como contar o número de divisores irredutíveis mônicos de $x^n - 1$ de cada grau. Seja d um inteiro positivo. Denotamos novamente por v_d o número de divisores mônicos irredutíveis de $x^n - 1$ de grau d. A escolha de f se faz da seguinte forma.

(a) $\mathrm{mdc}(q, n) \geq 3$:

Neste caso, $(x - 1)^3$ divide $x^n - 1$ e escolhemos $f = (x - 1)^3$.

(b) $\mathrm{mdc}(q,n) \leq 2$ e $v_1 = \mathrm{mdc}(q-1,n) \geq 3$:

Neste caso, podemos escolher $f = (x-1)Q_1Q_2$, com $Q_1, Q_2 \in \mathbb{F}_q[x]$ fatores lineares mônicos de x^n-1 diferentes entre si e diferentes de $x-1$.

(c) $\mathrm{mdc}(q,n) = 2$ e $v_1 = \mathrm{mdc}(q-1,n) = 2$:

Neste caso, podemos escolher $f = (x-1)^2Q$, com $Q \in \mathbb{F}_q[x]$ um fator linear mônico de x^n-1 diferente de $x-1$.

(d) $\mathrm{mdc}(q,n) + \mathrm{mdc}(q-1,n) \leq 3$ e $\mathrm{mdc}(q^2-1,n) > \mathrm{mdc}(q-1,n)$:

Neste caso, x^n-1 possui um fator $Q \in \mathbb{F}_q[x]$ mônico irredutível de grau 2 e escolhemos $f = (x-1)Q$.

(e) $\mathrm{mdc}(q,n) + \mathrm{mdc}(q-1,n) \leq 3$, $\mathrm{mdc}(q-1,n) = \mathrm{mdc}(q^2-1,n)$ e $\mathrm{mdc}(q^2+q+1,n) > 1$:

Nesse caso, x^n-1 possui um fator $Q \in \mathbb{F}_q[x]$ mônico irredutível de grau 3 e escolhemos $f = Q$. Veja que $\mathrm{mdc}(q,n) + \mathrm{mdc}(q-1,n) \leq 3$ significa $\mathrm{mdc}(q,n) = 2$ e $\mathrm{mdc}(q-1,n) = 1$ ou $\mathrm{mdc}(q,n) = 1$ e $\mathrm{mdc}(q-1,n) \leq 2$. Como $\mathrm{mdc}(q-1, q^2+q+1) = 1$ ou 3 e todo fator de q^2+q+1 diferente de 3 é da forma $6j+1$, temos $\mathrm{mdc}(q^2+q+1,n) > 1$ implica $\mathrm{mdc}(q^3-1,n) \geq 7$ e, portanto, $v_3 > 1$.

(f) Caso nenhuma dessas condições é satisfeita, x^n-1 não possui fator de grau 3. Isso acontece quando $2 \leq \mathrm{mdc}(q,n) + \mathrm{mdc}(q-1,n) \leq 3$ e $\mathrm{mdc}(q-1,n) = \mathrm{mdc}(q^2-1,n) = \mathrm{mdc}(q^3-1,n)$.

Da lista acima podemos deduzir o lema a seguir.

Lema 6.15. *O polinômio x^n-1 tem um fator de grau 3 em $\mathbb{F}_q[x]$ se, e somente se,* $\mathrm{mdc}(q(q-1)(q+1)(q^2+q+1),n) \geq 3$.

Demonstração. Veja que nos itens (a), (b), (c), (d) e (e) acima, temos $\mathrm{mdc}(q(q-1)(q+1)(q^2+q+1),n) \geq 3$. Já no caso (f), temos duas possibilidades. Se $\mathrm{mdc}(q-1,n) = \mathrm{mdc}(q^2-1,n) = \mathrm{mdc}(q^3-1,n) = 1$, então $\mathrm{mdc}(q(q-1)(q+1)(q^2+q+1),n) = \mathrm{mdc}(q,n) \leq 2$. Se $\mathrm{mdc}(q,n) = 1$ e $\mathrm{mdc}(q-1,n) = \mathrm{mdc}(q^2-1,n) = \mathrm{mdc}(q^3-1,n) = 2$, então q^2+q+1 é ímpar e, portanto, $\mathrm{mdc}(q^2+q+1,n) = 1$. Neste caso, $\mathrm{mdc}(q(q-1)(q+1)(q^2+q+1),n) = 2$. □

Corolário 6.16. *Sejam $n \geq 7$ um inteiro positivo e $q = 11^s$ uma potência de 11. Se $3 \mid (q^n-1)$ e x^n-1 tem um fator de grau 3 em $\mathbb{F}_q[x]$, então existe um elemento 3-primitivo 3-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.*

Demonstração. Suponha primeiro $n \geq 8$. Da Proposição 6.9 e da Proposição 6.13, só precisamos verificar o Algoritmo 8 para os pares da forma $(q = 11^s, n)$ que não se encontram na Tabela 6.1 tais que $3 \mid (q^n-1)$ e $\mathrm{mdc}(q(q-1)(q+1)(q^2+q+1),n) \geq 3$. Assim, para $q = 11$ e $7 \leq n < 70$, $q = 11^2$ e $7 \leq n < 19$, $q = 11^3$ e $7 \leq n < 12$, $q \in \{11^4, 11^5, 11^6\}$ e $7 \leq n < 11$, $q \in \{11^7, 11^8, 11^9, 11^{10}, 11^{11}, 11^{12}\}$ e $7 \leq n < 10$, $n = 8$ e $11^{13} \leq q < 7.05 \cdot 10^{21}$, e $n = 7$ e $11^{13} \leq q < 2.132 \cdot 10^{15}$, o Algoritmo 8 retorna falso unicamente para os pares $(11,8)$, $(11,10)$, $(11^2,7)$, $(11^2,8)$ e $(11^4,7)$.

Para esses pares, encontramos de forma explícita um elemento 3-primitivo 3-normal em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Na extensão $\mathbb{F}_{11^8}$ sobre $\mathbb{F}_{11}$, toda raiz de $x^8 + 10x^6 + 8x^5 + 6x^4 + x^3 + 8x^2 + 3x + 2 \in \mathbb{F}_{11}[x]$ é um elemento 3-primitivo 3-normal.

Na extensão $\mathbb{F}_{11^{10}}$ sobre $\mathbb{F}_{11}$, toda raiz de $x^{10} + 8x^9 + 5x^8 + 4x^7 + 3x^6 + 9x^4 + x^3 + 4x^2 + 10x + 2 \in \mathbb{F}_{11}[x]$ é um elemento 3-primitivo 3-normal.

Na extensão $\mathbb{F}_{q^7}$ sobre $\mathbb{F}_q$, com $q = 11^2$, toda raiz de $x^{14} + 5x^{13} + 3x^{12} + 6x^{11} + 9x^{10} + 10x^9 + 4x^8 + 10x^7 + 3x^6 + 9x^5 + 8x^3 + 8x + 2 \in \mathbb{F}_{11}[x]$ é um elemento 3-primitivo 3-normal.

Na extensão $\mathbb{F}_{q^8}$ sobre $\mathbb{F}_q$, com $q = 11^2$, toda raiz de $x^{16} + 7x^{15} + 4x^{14} + x^{13} + 10x^{12} + 8x^{10} + 7x^9 + 5x^8 + 4x^7 + 6x^6 + 4x^5 + 4x^4 + 9x^3 + 2x^2 + 5x + 6 \in \mathbb{F}_{11}[x]$ é um elemento 3-primitivo 3-normal.

Na extensão $\mathbb{F}_{q^7}$ sobre $\mathbb{F}_q$, com $q = 11^4$, toda raiz de $x^{28} + 4x^{26} + 7x^{25} + x^{24} + x^{23} + 2x^{22} + 6x^{21} + 9x^{20} + 7x^{19} + 7x^{18} + 2x^{17} + 9x^{16} + 10x^{15} + 9x^{14} + 9x^{13} + 6x^{12} + x^{11} + 8x^{10} + 9x^9 + 6x^8 + 8x^6 + 9x^4 + 5x^3 + x^2 + 10x + 8 \in \mathbb{F}_{11}[x]$ é um elemento 3-primitivo 3-normal. □

Note que, para $7 \leq n \leq 9$, se q fosse a potência de um primo qualquer e não unicamente uma potência de 11, precisaríamos utilizar técnicas adicionais (como nos capítulos anteriores) para refinar as cotas da Proposição 6.13 e do Lema 6.14.

6.4 Algoritmo para verificar a existência de elementos r-primitivos k-normais

Dada a potência de um primo q e inteiros positivos r e $n \geq 7$, o Algoritmo 8 verifica a Proposição 6.8, sendo $\ell = \prod_{p \in B} p$, $g = \frac{\mathrm{rad}_q(x^n-1)}{\mathrm{rad}_q((x^n-1)/f)} \cdot \prod_{h \in H} h$, $C = \{p_1, \ldots, p_r\}$ e $K = \{h_1, \ldots, h_s\}$. O polinômio mônico f de grau 3 é encontrado usando o Algoritmo 7.

Algoritmo 7: Factorgrau3(q, n)

Entrada: A potência de um primo q e um inteiro positivo n
Saída: um fator $f \in \mathbb{F}_q[x]$ de $x^n - 1$ de grau 3

$\{g_1, \ldots, g_s\} \leftarrow$ lista de fatores mônicos irredutíveis de $x^n - 1$ em $\mathbb{F}_q[x]$ ordenada por grau
se $mdc(q, n) > 2$ **então**
  $f \leftarrow g_1^3$
senão se $mdc(q - 1, n) > 2$ **então**
  $f \leftarrow g_1 g_2 g_3$
senão se $mdc(q, n) = 2$ *e* $mdc(q - 1, n) = 2$ **então**
  $f \leftarrow g_1^2 g_2$
senão se $mdc(q^2 - 1, n) > mdc(q - 1, n)$ **então**
  $i \leftarrow \mathrm{mdc}(q - 1, n)$
  $f \leftarrow g_1 g_{i+1}$
senão se $mdc(q^3 - 1, n) > mdc(q - 1, n)$ **então**
  $i \leftarrow \mathrm{mdc}(q - 1, n)$
  $f \leftarrow g_{i+1}$
senão
  retorna $x^n - 1$ não possui fator de grau 3 em $\mathbb{F}_q[x]$
fim
retorna f

Algoritmo 8: Verifica a Proposição 6.8 para valores dados de q, n e r com $k = 3$

Entrada: A potência de um primo q e inteiros positivos n e r
Saída: verdadeiro ou falso

se *r não divide* $x^n - 1$ **então**
  retorna *não existe elemento r-primitivo*
se $\text{mdc}(q(q-1)(q+1)(q^2+q+1), n) < 3$ **então**
  retorna *não existe elemento* 3*-normal*
senão
  $f \leftarrow \text{Factorgrau3}(q, n)$
  $Cond \leftarrow$ verdadeiro
  $L \leftarrow$ lista ordenada dos divisores primos de $q^n - 1$
  $G \leftarrow$ lista de factores mônicos irredutíveis de $\frac{x^n-1}{f}$ ordenada por grau
  $i, j \leftarrow 0$
  enquanto $i \leq \text{len}(L)$ *e* $Cond$ **faça**
    $B \leftarrow$ primeiros i elementos de L
    $C \leftarrow$ últimos $\text{len}(L) - i$ elementos de L
    $H \leftarrow$ primeiros j elementos de G
    $K \leftarrow$ últimos $\text{len}(G) - j$ elementos de G
    $\delta \leftarrow 1 - \left(\sum_{p \in C} \frac{1}{p} + \sum_{h \in K} \frac{1}{q^{\text{grau}(h)}} \right)$
    se $\delta > 0$ **então**
      $\Delta \leftarrow 2 + \frac{\text{len}(C) + \text{len}(K) - 1}{\delta}$
      $res \leftarrow \left[q^{\frac{n}{2}-k} \geq r \cdot 2^{\text{len}(B)+\text{len}(H)} \cdot \Delta \right]$
      $Cond \leftarrow$ não res
    senão
      $res \leftarrow$ falso
    fim
    $j \leftarrow j + 1$
    se $j > \text{len}(G)$ **então**
      $j \leftarrow 0$
      $i \leftarrow i + 1$
    fim
  fim
  retorna *res*
fim

CAPÍTULO 7

Trabalhos futuros

Neste capítulo apresentamos possíveis trabalhos futuros motivados pelos resultados obtidos nos capítulos anteriores.

7.1 Números $\mathbb{F}_q$-práticos

Em [32], o autor introduz a noção de números $\mathbb{F}_q$-práticos.

Definição 7.1. *Um inteiro positivo n é $\mathbb{F}_q$-prático se, para todo $k \in \{1, \ldots, n-1\}$, $x^n - 1$ é divisível por um polinômio de grau k em $\mathbb{F}_q[x]$.*

Reis mostra alguns critérios sobre a existência de números $\mathbb{F}_q$-práticos e define também o polinômio enumerador de elementos k-normais. Seria interessante utilizar os resultados obtidos no Capítulo 4 para encontrar novos resultados sobre números $\mathbb{F}_q$-práticos e sobre o polinômio enumerador.

7.2 Elementos r-primitivos k-normais

No Capítulo 6, apresentamos critérios para a existência de elementos r-primitivos k-normais. No Capítulo 2, estudou-se pares de elementos primitivos e normais. Já no Capítulo 3, foram estudadas progressões aritméticas de elementos primitivos normais. Todos esses estudos sobre elementos primitivos normais podem ser feitos também com elementos r-primitivos k-normais. Tanto é que alguns resultados nesse sentido já podem ser encontrados na literatura, como por exemplo [31], que trata sobre a existência de elementos r-primitivos k-normais $\alpha \in \mathbb{F}_{q^n}$ tais que α^{-1} é também r-primitivo k-normal.

Dessa forma, podemos estudar dois aspectos dos elementos r-primitivos k-normais. Por um lado, podemos estudar a existência de progressões aritméticas de elementos r-primitivos k-normais. Por outro lado, podemos estudar

a existência de pares $(\alpha, f(\alpha))$ de elementos r-primitivos k-normais, sendo f uma função racional qualquer.

7.3 Elementos r-primitivos k-normais em extensões satisfazendo $2k \geq n$

No Capítulo 5, estudamos elementos primitivos k-normais e demos uma solução completa para a existência de elementos primitivos 2-normais. Já na Seção 5.4, precisamos criar novas estratégias para estudar o caso em que $n = 4$ e $k = 2$. De forma similar, no Capítulo 6, estudamos elementos r-primitivos k-normais com a restrição $2k < n$ e demos respostas parciais para o caso $k = 3$. Seria interessante estudar a existência de elementos primitivos k-normais para $k = \frac{n}{2}$ de forma geral. Um primeiro passo nesse sentido seria o estudo de elementos r-primitivos 3-normais para $n = 6$. Mas será possível fazer esse estudo também para $n < 2k$?

A Tabela 7.1 mostra o número de elementos r-primitivos k-normais em $\mathbb{F}_{q^n}^*$ para $q = 3$ e $n = 6$. A primeira linha corresponde ao valor de r e a primeira coluna ao valor de k. Assim, por exemplo, existem 144 elementos primitivos normais. O que se torna interessante é a existência de 24 elementos primitivos 3-normais nessa extensão de grau 6. Dessa forma, a Tabela 7.1 nos motiva a um estudo mais aprofundado de elementos r-primitivos k-normais.

$k\backslash r$	1	2	4	7	8	13	14	26	28	52	56	91	104	182	364	728
0	144	60	30	36	30	0	0	12	0	6	0	0	6	0	0	0
1	96	48	24	0	24	24	0	0	0	0	0	0	0	0	0	0
2	24	36	18	12	18	0	0	0	0	0	0	0	0	0	0	0
3	24	0	0	0	0	0	18	0	9	0	9	0	0	0	0	0
4	0	0	0	0	0	0	6	0	3	0	3	4	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	1

Tabela 7.1: Número de elementos r-primitivos k-normais para $q = 3$ e $n = 6$.

Referências Bibliográficas

[1] AGUIRRE, Josimar JR, CARVALHO, Cícero e NEUMANN, Victor GL. "**About r-primitive and k-normal elements in finite fields**". Em: ***Designs, Codes and Cryptography*** (2022), pp. 1–12.

[2] AGUIRRE, Josimar JR e NEUMANN, Victor GL. "**Existence of primitive 2-normal elements in finite fields**". Em: ***Finite Fields and Their Applications*** 73 (2021), p. 101864.

[3] AGUIRRE, Josimar JR e NEUMANN, Victor GL. "**Number of k-normal elements over a finite field**". Em: ***arXiv preprint arXiv:2202.09866*** (2022).

[4] APOSTOL, Tom M. ***Introduction to analytic number theory***. Springer Science & Business Media, 1998.

[5] CARVALHO, Cícero, GUARDIEIRO, João Paulo, NEUMANN, Victor GL e TIZZIOTTI, Guilherme. "**On special pairs of primitive elements over a finite field**". Em: ***Finite Fields and Their Applications*** 73 (2021), p. 101839.

[6] CARVALHO, Cícero, GUARDIEIRO, João Paulo, NEUMANN, Victor GL e TIZZIOTTI, Guilherme. "**On the existence of pairs of primitive and normal elements over finite fields**". Em: ***Bulletin of the Brazilian Mathematical Society, New Series*** 53.3 (2022), pp. 677–699.

[7] COHEN, Stephen D. "**Consecutive primitive roots in a finite field**". Em: ***Proceedings of the American Mathematical Society*** 93.2 (1985), pp. 189–197.

[8] COHEN, Stephen D. "**Consecutive primitive roots in a finite field. II**". Em: ***Proceedings of the American Mathematical Society*** 94.4 (1985), pp. 605–611.

[9] COHEN, Stephen D. "**Pairs of primitive roots**". Em: ***Mathematika*** 32.2 (1985), pp. 276–285.

[10] COHEN, Stephen D e HUCZYNSKA, Sophie. "**The primitive normal basis theorem–without a computer**". Em: ***Journal of the London Mathematical Society*** 67.1 (2003), pp. 41–56.

[11] COHEN, Stephen D e HUCZYNSKA, Sophie. "**The strong primitive normal basis theorem**". Em: ***Acta Aritmética*** 143.4 (2010), pp. 299–332.

[12] COHEN, Stephen D, SHARMA, Hariom e SHARMA, Rajendra. "**Primitive values of rational functions at primitive elements of a finite field**". Em: ***Journal of Number Theory*** 219 (2021), pp. 237–246.

[13] COHEN, Stephen D, SILVA, Tomás Oliveira e e TRUDGIAN, Tim. "**On consecutive primitive elements in a finite field**". Em: ***Bulletin of the London Mathematical Society*** 47.3 (2015), pp. 418–426.

[14] FU, Lei e WAN, Daqing. "**A Class of Incomplete Character Sums**". Em: ***The Quarterly Journal of Mathematics*** 65.4 (mai. de 2014), pp. 1195–1211.

[15] HACHENBERGER, Dirk e JUNGNICKEL, Dieter. ***Topics in Galois fields***. Vol. 29. Springer, 2020.

[16] HAZARIKA, Himangshu, BASNET, Dhiren Kumar e COHEN, Stephen D. "**The existence of primitive normal elements of quadratic forms over finite fields**". Em: ***Journal of Algebra and Its Applications*** 21.04 (2022), p. 2250068.

[17] HAZARIKA, Himangshu, BASNET, Dhiren Kumar e KAPETANAKIS, Giorgos. "**On the existence of primitive normal elements of rational form over finite fields of even characteristic**". Em: ***International Journal of Algebra and Computation*** 32.02 (2022), pp. 357–382.

[18] HUCZYNSKA, Sophie, MULLEN, Gary L, PANARIO, Daniel e THOMSON, David. "**Existence and properties of k-normal elements over finite fields**". Em: ***Finite Fields and Their Applications*** 24 (2013), pp. 170–183.

[19] JARSO, Tamiru e TRUDGIAN, Tim. "**Four consecutive primitive elements in a finite field**". Em: ***Math. Comp.*** 91.335 (2022), pp. 1521–1532.

[20] KAPETANAKIS, Giorgos. "**An extension of the (strong) primitive normal basis theorem**". Em: ***Applicable Algebra in Engineering, Communication and Computing*** 25.5 (2014), pp. 311–337.

[21] KAPETANAKIS, Giorgos. "**Normal bases and primitive elements over finite fields**". Em: ***Finite Fields and Their Applications*** 26 (2014), pp. 123–143.

[22] KAPETANAKIS, Giorgos e REIS, Lucas. "**Variations of the primitive normal basis theorem**". Em: ***Designs, Codes and Cryptography*** 87.7 (2019), pp. 1459–1480.

[23] KATZ, Nicholas M. "**An estimate for character sums**". Em: ***Journal of the American Mathematical Society*** 2.2 (1989), pp. 197–200.

[24] LANDAU, Edmund. ***Vorlesungen über Zahlentheorie***. Leipzig: S. Hirzel, 1927.

[25] LEMOS, Abílio, NEUMANN, Victor GL e RIBAS, Sávio. "**On arithmetic progressions in finite fields**". Em: ***arXiv preprint arXiv:2208.02876*** (2022).

[26] LENSTRA, Hendrik Willem e SCHOOF, René. "**Primitive normal bases for finite fields**". Em: ***Mathematics of Computation*** (1987), pp. 217–231.

[27] LIDL, Rudolf e NIEDERREITER, Harald. ***Finite fields***. 20. Cambridge university press, 1997.

[28] MULLEN, Gary L e PANARIO, Daniel. ***Handbook of finite fields***. Vol. 17. CRC press Boca Raton, 2013.

[29] ORE, Oystein. "**Contributions to the theory of finite fields**". Em: ***Transactions of the American Mathematical Society*** 36.2 (1934), pp. 243–274.

[30] RANI, Mamta, SHARMA, Avnish K e TIWARI, Sharwan K. "**On r-primitive k-normal elements over finite fields**". Em: ***Finite Fields and Their Applications*** 82 (2022), p. 102053.

[31] RANI, Mamta, SHARMA, Avnish K, TIWARI, Sharwan K e PANIGRAHI, Anupama. "**Inverses of r-primitive k-normal elements over finite fields**". Em: ***arXiv preprint arXiv:2201.11334*** (2022).

[32] REIS, Lucas. "**Existence results on k-normal elements over finite fields**". Em: ***Revista Matemática Iberoamericana*** 35.3 (2019), pp. 805–822.

[33] REIS, Lucas e THOMSON, David. "**Existence of primitive 1-normal elements in finite fields**". Em: ***Finite Fields and Their Applications*** 51 (2018), pp. 238–269.

[34] SAYGI, Zülfükar, TILENBAEV, Ernist e ÜRTIŞ, Çetin. "**On the number of k-normal elements over finite fields**". Em: ***Turkish Journal of Mathematics*** 43.2 (2019), pp. 795–812.

[35] SHARMA, Avnish K, RANI, Mamta e TIWARI, Sharwan K. "**Primitive normal pairs with prescribed norm and trace**". Em: ***Finite Fields and Their Applications*** 78 (2022), p. 101976.

[36] SHARMA, Hariom e SHARMA, RK. "**Existence of primitive normal pairs with one prescribed trace over finite fields**". Em: ***Designs, Codes and Cryptography*** 89.12 (2021), pp. 2841–2855.

[37] SHARMA, RK e ANJU. "**Existence of some special primitive normal elements over finite fields**". Em: ***Finite Fields and Their Applications*** 46 (2017), pp. 280–303.

[38] STEIN, William et al. ***Sage: Open source mathematical software***. 2008.

[39] TINANI, Simran e ROSENTHAL, Joachim. "**Existence and cardinality of k-normal elements in finite fields**". Em: ***International Workshop on the Arithmetic of Finite Fields***. Springer. 2020, pp. 255–271.

[40] VEGH, Emanuel. "**A note on the distribution of the primitive roots of a prime**". Em: ***Journal of Number Theory*** 3.1 (1971), pp. 13–18.

[41] VEGH, Emanuel. "**Pairs of consecutive primitive roots modulo a prime**". Em: ***Proc. Amer. Math. Soc***. Vol. 19. 1968, pp. 1169–1170.