DOUGLAS JOSÉ DE SOUZA

ELEMENTOS PRIMITIVOS ESPECIAIS EM CORPOS FINITOS

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação em Matemática, para obtenção do título de *Magister Scientiae*.

Orientador: Abílio Lemos C. Júnior

VIÇOSA - MINAS GERAIS
2021

Ficha catalográfica elaborada pela Biblioteca Central da Universidade Federal de Viçosa - Campus Viçosa

T
S729e
2021

Souza, Douglas José de, 1995-
Elementos primitivos especiais em corpos finitos / Douglas José de Souza. – Viçosa, MG, 2021.
60 f. : il. ; 29 cm.

Orientador: Abílio Lemos Cardoso Júnior.
Dissertação (mestrado) - Universidade Federal de Viçosa.
Referências bibliográficas: f. 59-60.

1. Teoria dos números. 2. Funções aritméticas. 3. Algoritmos computacionais. I. Universidade Federal de Viçosa. Departamento de Matemática. Programa de Pós-Graduação em Matemática. II. Título.

CDD 22. ed. 512.7

DOUGLAS JOSÉ DE SOUZA

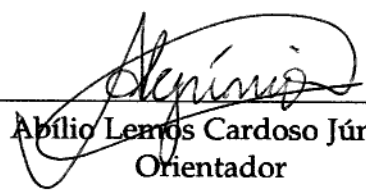
ELEMENTOS PRIMITIVOS ESPECIAIS EM CORPOS FINITOS

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação em Matemática, para obtenção do título de *Magister Scientiae*.

APROVADA: 12 de março de 2021.

Assentimento:

Douglas José de Souza
Autor



Abílio Lemos Cardoso Júnior
Orientador

Agradecimentos

Agradeço ao meu pai Jose Bosco, por ter oferecido mais do que o suporte necessário em todos esses anos que estive envolvido com o espaço acadêmico, assim como todos os anos de minha vida.

À minha querida mãe Nirlei, que já não está mais conosco neste mundo, mas que, junto com seus ensinamentos e valores, sempre esteve comigo.

Ao meu irmão Waldemar e à minha irmã Leonela, por todo suporte e carinho que sempre tiveram para comigo.

À minha namorada Jéssica, pela sensibilidade de compreensão nos momentos de minha ausência e principalmente pelo apoio psicológico nos momentos de dificuldade.

Aos meus amigos do mestrado: Amanda, Diego, Neemias, Nicolly e Renato, pela amizade construída e pelo suporte atendido sempre que foi solicitado.

Aos meus companheiros de república em Viçosa-MG, em especial o Thiago, pelo apoio e motivação de sempre.

Ao meu orientador Abílio Lemos, por ter confiado a mim para que este trabalho fosse desenvolvido, assim como pela sua ajuda, paciência e motivação.

À todos os professores que contribuíram com minha formação e em especial ao professor Anderson Araujo que, de certa forma, foi um divisor de águas em minha formação como professor de matemática.

Ao apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Resumo

SOUZA, Douglas José de, M.Sc., Universidade Federal de Viçosa, março de 2021. **Elementos especiais primitivos em corpos finitos**. Orientador: Abílio Lemos Cardoso Júnior.

Neste trabalho estamos interessados em encontrar condições suficientes que garantam a existência de um elemento primitivo $\alpha \in \mathbb{F}_q$ de forma que $f(\alpha)$ também seja um elemento primitivos em $\mathbb{F}_q$, onde $\mathbb{F}_q$ é um corpo finito de característica qualquer, ou seja, com $q = p^k$ elementos e $f(x) \in \mathbb{F}_q(x)$ é uma função racional com algumas restrições. Neste sentido, exibimos explicitamente os valores de k para os quais tal par existe sendo $p \in \{2, 3, 5, 7\}$. Por outro lado, considerando q uma potência de um primo ímpar com $q > 169$, iremos demonstrar que sempre existam três elementos primitivos consecutivos no corpo finito $\mathbb{F}_q$. Mais precisamente, existem onze valores de $q \leq 169$ para os quais isto é falso.

Palavras-chave: Elementos Primitivos. Corpos Finitos. GAP.

Abstract

SOUZA, Douglas José de, M.Sc., Universidade Federal de Viçosa, March, 2021. **Elementos especiais primitivos em corpos finitos**. Adviser: Abílio Lemos Cardoso Júnior.

In this work we are interested in finding sufficient conditions to guarantee the existence of a primitive element $\alpha \in \mathbb{F}_q$ so that $f(\alpha)$ is also a primitive element in $\mathbb{F}_q$, where $\mathbb{F}_q$ is a finite field of any characteristic, that is, with $q = p^k$ elements and $f(x) \in \mathbb{F}_q(x)$ is a rational function with some restrictions. In this sense, we explicitly determine the values of k for which such a pair exists for $p \in \{2, 3, 5, 7\}$. On the other hand, considering $q > 169$ we will demonstrate that always there are three consecutive primitive elements in the finite field $\mathbb{F}_q$. More precisely, there are eleve values of $q \leq 169$ for which this is false.

Keywords: Primitive Elements. Finite Fields. GAP.

Sumário

Introdução

No presente trabalho, estudaremos conceitos de Teoria dos Números tais como caracteres em corpos finitos, funções aritméticas e funções características afim de alcançar o objetivo principal que é encontrar elementos primitivos em um corpo finito com propriedades especiais. Mais especificamente, estamos interessados em encontrar condições suficientes que garantam a existência de pares (α, β) de elementos primitivos sobre um corpo finito $\mathbb{F}_q$ com $q = p^k$ de característica p qualquer assim como encontrar todos os corpos finitos que não possuem um elemento primitivo α tal que $\alpha + 1$ e $\alpha + 2$ também sejam primitivos.

Para compreender melhor o desenvolvimento dos resultados obtidos nessa área, vamos à origem do problema. A. Brauer perguntou ao seu ex-aluno E. Vegh sobre a existência de pares de elementos primitivos consecutivos em $\mathbb{F}_p$, ou seja, $\beta = \alpha + 1$. Vegh então provou que se $p > 3$ e $\frac{\phi(p-1)}{p-1} > \frac{1}{3}$, onde ϕ é a função de Euler, então existe o par em questão [1]. Três anos depois, ele provou que se $p \equiv 1 \pmod 4$, e $\frac{\phi(p-1)}{p-1} > \frac{1}{4}$ então tal par existe [2]. Em 1985, Cohen estendeu o resultado em uma série de três artigos provando que se $q > 7$, então existe um par de elementos primitivos consecutivos [3–5]. A partir disso, se pergunta se existem tais pares de elementos primitivos (α, β), onde β é obtido aplicando α em um polinômio. Foi então considerado por diversos autores, na maioria das vezes, polinômio de grau no máximo dois. Em 2015, Cohen, Oliveira e Silva e Thudigan provaram que se $q > 61$ existe o par de elementos primitivos (α, β) onde $\beta = a\alpha + b$ com $a, b \in \mathbb{F}_q$. Já para polinômios de grau dois, Boker, Cohen e Sutherland provaram que se $q > 211$ existe o par de elementos primitivos (α, β) onde $\beta = a\alpha^2 + b\alpha + c$, com $b^2 - 4ac \neq 0$ [6]. Neste sentido, vários autores trabalharam em busca de pares de elementos primitivos (α, β) onde β é obtido aplicando α a uma função racional. Veja, por exemplo, o caso mais simples dessa situação: $\beta = 1/\alpha$ é primitivo se, e somente se, α é primitivo. Em 2012 Wang, Cao e Feng provaram que se $q = 2^{sn}$ em que n é ímpar, $n \geq 13$ e $s > 4$, então existe um par de elementos primitivos (α, β) em que $\beta = \alpha + 1/\alpha$ [7]. Dois anos depois, este resultado foi generalizado por Cohen que provou que se q é uma potência de 2, e $q \geq 8$, então existe o par de elementos primitivos (α, β) em que $\beta = \alpha + 1/\alpha$ [8]. Naquele mesmo ano, Kapetanakis apresentou condições necessárias para que o par de elementos primitivos (α, β) exista com $\beta = \frac{a\alpha+b}{c\alpha+d}$ tal que $a, b, c, d \in \mathbb{F}_q$. Três anos depois, em 2017, Anju e Sharma encontraram condições suficientes que garantem um par de elementos primitivos (α, β) tal que $\beta = \frac{a\alpha^2+b\alpha+c}{d\alpha+e}$ com $a, b, c, d, e \in \mathbb{F}_{2^k}$. Em 2018, Sharma, Awasthi e Gupta, apresentaram condições que garantem a existência de um par de elementos primitivos (α, β) tal que $\beta = \frac{a\alpha^2+b\alpha+c}{d\alpha^2+e\alpha+f}$, com $a, b, c, d, e, f \in \mathbb{F}_{2^k}$.

E aqui entra nosso trabalho propriamente dito, que é a generalização feita por Cohen, Sharma e Sharma [9], que consiste em demonstrar condições que garantem a existência de um par (α, β) de elementos primitivos em que β é um quociente de expressões polinomiais aplicados em α sobre um corpo de característica qualquer, ou seja, com $q = p^k$ elementos. Além disso, apresentaremos resultados obtidos por Carvalho, Guardieiro, Neumann

e Tizzioti [10], que também garanta a existência de tal par ou prove que ele não existe. Também apresentamos resultados obtidos por Cohen, Oliveira e Trudgian [11] cujo principal objetivo é demonstrar que para $q > 169$ sempre existe três elementos primitivos consecutivos no corpo finito $\mathbb{F}_q$.

O primeiro capítulo trata de assuntos preliminares que são necessários para a compreensão do trabalho como um todo e, neste sentido, mencionamos alguns resultados referentes a funções aritméticas e conceitos sobre corpos finitos como, por exemplo, caracteres, que terão grande relevância na contagem de certos tipos de elementos. O conteúdo deste capítulo tem como principais referências os livros [12–14].

No segundo capítulo estaremos interessados em estudar a generalização dos resultados de Sharma, Awasthi e Gupta, encontrando condições que garantam a existência de um par (α, β) de elementos primitivos tal que β é uma função racional aplicado em α. Nosso principal resultado é o Teorema 54, que é usado para determinar os valores de k de forma que o par (α, β) existe, embora as vezes precisaremos do Lema 57 para determinar esses valores.

A primeira sessão deste capítulo contém a definição do conjunto $\Gamma_p(m_1, m_2)$ e resultados básicos que serão usados no desenvolvimento dos resultados que se seguem. Na segunda sessão, apresentaremos os principais resultados do trabalho e, junto a eles, uma série de algoritmos feitos no sistema GAP [15, 16] para aplicação destes resultados. Finalmente, na última sessão, determinaremos os conjuntos $\Gamma_p(3, 2)$ para $p = 2, 3, 5$ e 7 com auxílio dos algoritmos desenvolvidos.

Por fim, no terceiro capítulo apresentamos estimativas e resultados que garantem a existência de n elementos primitivos consecutivos sobre um corpo finito na qual sua característica seja no mínimo n e, combinado a isto, apresentamos um algoritmo em linguagem GAP para provar o Teorema 66.

Capítulo 1

Preliminares

Neste capítulo trataremos de assuntos que são pré-requisitos para a compreensão dos principais resultados. Neste sentido, falaremos sobre funções multiplicativas, corpos finitos, caracteres e elementos s-livres e, interligando todos esses, construímos nossa principal ferramenta que é a função característica dos elementos s-livres que será obtida no Corolário 49 e terá como principal objetivo servir como alicerce na demonstração dos principais resultados.

1.1 Funções Aritméticas

Definição 1. Uma função aritmética é uma função $f(n)$ na qual está definida sobre o conjunto dos número naturais.

Exemplo 2. Qualquer sequência (a_n) é uma função aritmética. Especificamente são funções aritméticas $n!$, $d(n) = \sum_{d|n} 1$ ou $r(n)$ onde $r(n)$ é o número de soluções da equação $n = x^2 + y^2$.

Definição 3. Seja $f(n)$ uma função aritmética tal que se $\text{mdc}(a, b) = 1$, e

$$f(ab) = f(a)f(b) \tag{1.1}$$

então dizemos que $f(n)$ é uma função multiplicativa. Se vale (1.1) independente da condição em que $\text{mdc}(a, b) = 1$, então dizemos que $f(n)$ é uma função completamente multiplicativa.

Desta definição, vemos que se $f(n)$ é uma função multiplicativa e se $p_1, \cdots, p_r$ são primos distintos, então

$$f(p_1^{a_1} \cdots p_r^{a_r}) = f(p_1^{a_1}) \cdots f(p_r^{a_r}),$$

de modo que $f(n)$ é determinado pelas potências dos primos. Além disso, se $f(n)$ é completamente multiplicativa, então

$$f(p_1^{a_1} \cdots p_r^{a_r}) = f(p_1)^{a_1} \cdots f(p_r)^{a_r},$$

de modo que $f(n)$ é determinado pelos números primos.

Exemplo 4. A função de Möbius é definida por:

$$\mu(n) = \begin{cases} 1 \text{ se } n = 1, \\ (-1)^r \text{ se } n \text{ é o produto de } r \text{ primos distintos}, \\ 0 \text{ se } n \text{ é divisível pelo quadrado de algum primo.} \end{cases}$$

Temos então

$$\begin{array}{lllllll} \mu(1) = 1, & \mu(2) = -1, & \mu(3) = -1, & \mu(4) = 0, & \mu(5) = -1, & \mu(6) = 1, \\ \mu(7) = -1, & \mu(8) = 0, & \mu(9) = 0, & \mu(10) = 1, & \mu(11) = -1, & \cdots \end{array}$$

Note que $\mu(n)$ é multiplicativa mas não é completamente multiplicativa.

Exemplo 5. A função totiente de Euler definida por

$$\phi(n) = \sharp\{k \in \mathbb{N} : (k, n) = 1, k \leq n\}$$

conta a quantidade de números menores ou igual a n co-primos com respeito a ele. Essa função também pode ser expressa de forma compacta pela fórmula analítica $\phi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right), n \in \mathbb{N}$. Essa função é também multiplicativa mas não é completamente multiplicativa.

Teorema 6. Seja $f(n)$ uma função multiplicativa que não é identicamente nula. Então $f(1) = 1$.

Prova. Seja a tal que $f(a) \neq 0$. Assim $f(a) = f(a \cdot 1) = f(a)f(1)$ e disso concluímos que $f(1) = 1$. ■

Teorema 7. Sejam $g(n)$ e $h(n)$ funções multiplicativas. Então a função

$$f(n) = \sum_{d|n} g(d)h\left(\frac{n}{d}\right) = \sum_{d|n} g\left(\frac{n}{d}\right)h(d) \tag{1.2}$$

é também multiplicativa.

Prova. Suponha que $\text{mdc}(a, b) = 1$. Então

$$f(ab) = \sum_{d|ab} g(d)h\left(\frac{ab}{d}\right).$$

Sejam $u = (a, d)$ e $v = (b, d)$ de modo que $uv = d$ e, portanto,

$$\begin{aligned} f(ab) &= \sum_{u|a}\sum_{v|b} g(uv)h\left(\frac{ab}{uv}\right) \\ &= \sum_{u|a} g(u)h\left(\frac{a}{u}\right)\sum_{v|b} g(v)h\left(\frac{b}{v}\right) \\ &= f(a)f(b). \end{aligned}$$

Mostremos agora a segunda igualdade de (1.2). Seja $D := \{d \in \mathbb{N} : d|n\}$. A função $j : \underset{d \mapsto \frac{n}{d}}{D \to D}$ é bijeção de D sobre D, por isso

$$\sum_{d|n} g(d)h\left(\frac{n}{d}\right) = \sum_{d\in D} g(d)h\left(\frac{n}{d}\right) = \sum_{d\in D} g(j(d))h\left(\frac{n}{j(d)}\right) = \sum_{d\in D} g\left(\frac{n}{d}\right)h(d).$$

■

Teorema 8. Seja $f(n)$ uma função multiplicativa que não é identicamente nula. Então

$$\sum_{d|n} \mu(d)f(d) = \prod_{p|n}(1 - f(p)) \tag{1.3}$$

onde p percorre os divisores primos de n.

Prova. Colocando $g(n) = \mu(n)f(n)$, $h(n) = 1$ no Teorema 7 temos

$$F(n) = \sum_{d|n} \mu(d)f(d)$$

é multiplicativa. Note que $G(n) = \prod_{p|n}(1 - f(p))$ é também multiplicativa. De fato, seja $(a, b) = 1$, então

$$G(ab) = \prod_{p|ab}(1 - f(p)) = \prod_{p|a}(1 - f(p))\prod_{p|b}(1 - f(p)) = G(a)G(b).$$

Assim $F(n)$ e $G(n)$ são multiplicativas e devido a isto, dado $n = p_1^{\alpha_1} \cdots p_r^{\alpha_k}$ fatorado em primos distintos, temos

$$F(n) = \prod_{i=1}^{k} F(p_i^{\alpha_i}) \text{ e } G(n) = \prod_{i=1}^{k} G(p_i^{\alpha_i}).$$

Assim, basta verificarmos que F e G coincidem para potência de primos e para $n = 1$.

1. Para $n = 1$, pelo Teorema 6 $F(1) = \mu(1)f(1) = f(1) = 1$, visto que f não é identicamente nula. Como 1 não possui divisor primo, segue que $G(1) = \sum_{p|1}(1 - f(p)) = 1$. Logo F(1) = G(1).

2. Para o caso em que $n = p^t$ temos $G(n) = \prod_{p|n}(1 - f(p)) = 1 - f(p)$ uma vez que apenas p é divisor primo de p^t. Por outro lado,

$$\begin{aligned} F(p^t) = \sum_{d|p^t} \mu(d)f(d) &= \sum_{i=1}^{t} \mu(p^i)f(p^i) \\ &= \mu(1)f(1) + \mu(p)f(p) + \mu(p^2)f(p^2) + \cdots + \mu(p^t)f(p^t) \\ &= \mu(1)f(1) + \mu(p)f(p) \\ &= 1 - f(p) = G(p^t). \end{aligned}$$

■

1.2 Corpos Finitos

Definição 9. Um corpo finito é um corpo que contém um número finito de elementos.

Proposição 10. Seja K um corpo finito contendo um subcorpo F com q elementos. Então K possui q^n elementos onde $n = [K : F]$.

Prova. Note que K é um espaço vetorial sobre F e uma vez que K é finito, então ele possui dimensão finita como espaço vetorial sobre F. Se $[K : F] = n$, então F tem uma base sobre K de n elementos, digamos, $v_1, \cdots, v_n$. Assim, todo elemento de K pode ser representado de uma única forma como $\alpha_1 v_1 + \cdots + \alpha_n v_n$ onde $\alpha_1, \cdots, \alpha_n \in F$. Como cada α_i pode assumir q valores, K possui exatamente q^n elementos. ■

Corolário 11. Seja F um corpo finito. Então F tem p^n elementos onde p é um número primo o qual é a característica de K e denotada por $Char(K) = p$.

Prova. Como F é finito, F possui característica p, onde p é primo. Portanto F contém um corpo F_0 isomorfo a $\mathbb{Z}_p$. Como F_0 tem p elementos, pela Proposição 10, F tem p^n elementos, onde $n = [F : F_0]$.

■

Proposição 12. Seja $\mathbb{F}_{p^n}$ um corpo finito. Então

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \text{ e } (a-b)^{p^n} = a^{p^n} - b^{p^n} \tag{1.4}$$

para todo $a, b \in \mathbb{F}_{p^n}$ e $n \in \mathbb{N}$.

Prova.

i) Observe que

$$\binom{p}{i} = p \cdot \frac{(p-1)\cdots(p-i+1)}{1 \cdot 2 \cdots i} = p \cdot l, l \in \mathbb{N}.$$

Isto é, $p \mid \binom{p}{i}$ para todo $1 \leq i \leq p-1$. Agora, como

$$(a+b)^p = a^p + \sum_{i=1}^{p-1} a^{p-i}b^i + b^p,$$

segue que $(a+b)^p \equiv a^p + b^p \pmod{p}$.

ii) Suponha que $(a+b)^{p^k} = a^{p^k} + b^{p^k}$ para algum $k > 1, k \in \mathbb{N}$.

iii) Como $(a+b)^{k+1} = \left[(a+b)^{p^k}\right]^p \overset{ii)}{=} \left(a^{p^k} + b^{p^k}\right)^p \overset{i)}{=} a^{p^{k+1}} + b^{p^{k+1}}$ para todo $k \in \mathbb{N}$.

Pelo que acabamos de mostrar, obtemos

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

e, portanto, segue a segunda identidade de (1.4). ■

Proposição 13. Se F é um corpo finito com q elementos, então $a^q = a$ para todo $a \in F$.

Prova. Se $a = 0$, segue o resultado. Por outro lado, os elementos não nulos de F formam um grupo de ordem $q-1$ em relação a multiplicação, a saber, F_q^*. Assim, $a^{q-1} = 1$ para todo $a \in F_q^*$ e, portanto, $a^q = a$.

■

Proposição 14. Seja $f(x) \in K[x]$, onde K é um corpo e $\partial(f) = n$. Então f tem no máximo n raízes em K.

Prova. Se $\partial(f) = 1$, então $f(x) = x - a$ e, por definição, $a \in K$. Suponha que qualquer polinômio $h(x) \in K[x]$ tal que $\partial(h) < n$, tem no máximo $\partial(h)$ raízes em K.

Agora, considere $f(x) \in K[x]$ tal que $\partial(f) = n$. Se f não possui raízes em K, está feito. Suponha que f tem pelo menos uma raiz em K. Seja a esta raiz. Como $K[x]$ é domínio euclidiano, seque que $f(x) = (x-a)h(x)$, onde $\partial(h) < n$. Logo, f possui no máximo $\partial(h) + 1 \leq n$ raízes em K.

■

Proposição 15. Se F é um corpo finito com q elementos, então o polinômio $x^q - x$ em $F[x]$ decompõe-se como

$$x^q - x = \prod_{a \in F} (x - a).$$

Prova. O polinômio $x^q - x$ têm no máximo q raízes em F. Pela Proposição 13, tem-se que todos elementos de F é raiz do polinômio em questão, logo

$$x^q - x = \prod_{a \in F} (x - a).$$

■

Corolário 16. Se o corpo F tem q elementos, então F é o corpo de fatoração do polinômio $x^q - x$.

Prova. Pela Proposição 15, $x^q - x$, decompõe-se em F. Note que ele não se decompõe em nenhum outro corpo menor, uma vez que tal corpo precisaria conter todas as raízes do polinômio em questão, ou seja, ele precisaria ter no mínimo q elementos. Logo segue o resultado. ■

Teorema 17. Para todo corpo finito $\mathbb{F}_q$ o grupo multiplicativo $\mathbb{F}_q^*$ de elementos não nulos de $\mathbb{F}_q$ é cíclico.

Prova. Podemos assumir que $q \geq 3$. Seja $h = q - 1 = p_1^{r_1} \cdots p_m^{r_m}$ a decomposição de fatores primos da ordem de $\mathbb{F}_q^*$. Para todo i, $1 \leq i \leq m$, o polinômio $x^{\frac{h}{p_i}} - 1$ tem no máximo $\frac{h}{p_i}$ raízes em $\mathbb{F}_q$. Uma vez que $\frac{h}{p_i} < h$, existe pelo menos um elemento não nulo em $\mathbb{F}_q$ que não é raiz desse polinômio. Seja a_i um desses elementos e defina $b_i = a_i^{h/p_i^{r_i}}$.

Note que $b_i^{p_i^{r_i}} = 1$, assim tem-se que a ordem de b_i é um divisor de $p_i^{r_i}$, ou seja, é da forma $p_i^{s_i}$ com $0 \leq s_i \leq r_i$. Como

$$b_i^{p_i^{r_i-1}} = a_i^{h/p_i} \neq 1,$$

a ordem de b_i é exatamente $p_i^{r_i}$. Afirmamos que $b = b_1 \cdots b_m$ tem ordem h. De fato, como $\text{mdc}(p_1^{r_1}, ..., p_m^{r_m}) = 1$ então

$$ord(b) = ord(b_1 \cdots b_m) = ord(b_1) \cdots ord(b_m) = p_1^{r_1} \cdots p_m^{r_m} = h$$

e, portanto, $\mathbb{F}_q^*$ é um grupo cíclico sendo b o seu gerador. ■

Definição 18. Um gerador do grupo cíclico $\mathbb{F}_q^*$ é chamado de elemento primitivo.

Observação 19. Note que sendo d um divisor da ordem de um grupo cíclico finito G, então G contém $\phi(d)$ elementos de ordem d e, consequentemente, $\mathbb{F}_q^*$ contém $\phi(q-1)$ elementos primitivos. A existência de elementos primitivos pode ser usada, em particular, para mostrar que todo corpo finito pode ser visto como uma extensão algébrica simples de seu subcorpo primo.

Teorema 20. Seja $\mathbb{F}_q$ um corpo finito e $\mathbb{F}_r$ uma extensão finita. Então $\mathbb{F}_r$ é uma extensão algébrica simples de $\mathbb{F}_q$ e todo elemento $\alpha \in \mathbb{F}_r$ satisfaz $\mathbb{F}_r = \mathbb{F}_q(\alpha)$.

Prova. Seja α um elemento primitivo de $\mathbb{F}_r$. Note que $\mathbb{F}_q(\alpha) \subseteq \mathbb{F}_r$. Por outro lado, $\mathbb{F}_q(\alpha)$ contém 0 e todas as potências de α e, portanto, todos os elementos de $\mathbb{F}_r$. Logo $\mathbb{F}_q(\alpha) = \mathbb{F}_r$.

■

Corolário 21. Seja $\mathbb{F}_q$ um corpo finito e n um inteiro positivo. Existe um polinômio irredutível em $\mathbb{F}_q[x]$ de grau n.

Prova. Seja $\mathbb{F}_r$ uma extensão finita de $\mathbb{F}_q$ de ordem q^n, assim $[\mathbb{F}_r : \mathbb{F}_q] = n$. Pelo Teorema 20 temos $\mathbb{F}_r = \mathbb{F}_q(\alpha)$ para algum $\alpha \in \mathbb{F}_r$. Então o polinômio minimal de α sobre $\mathbb{F}_q$ é um polinômio irredutível em $\mathbb{F}_q[x]$ de grau n.

■

Definição 22. Sejam $\alpha \in F = \mathbb{F}_{q^m}$ e $K = \mathbb{F}_q$. O traço $Tr_{F/K}$ de α sobre K é definido por

$$Tr_{F/K}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}}.$$

Se K é subcorpo primo de F, então $Tr_{F/K}(a)$ é chamado de traço absoluto de α e é denotado por $Tr_F(\alpha)$.

Teorema 23. Seja $F = \mathbb{F}_{q^m}$ e $K = \mathbb{F}_q$. Então a função $Tr_{F/K}$ satisfaz as seguintes propriedades:

(i) $Tr_{F/K}(\alpha + \beta) = Tr_{F/K}(\alpha) + Tr_{F/K}(\beta)$ para todo $\alpha, \beta \in F$;

(ii) $Tr_{F/K}(c\alpha) = cTr_{F/K}(\alpha)$ para todo $c \in K$, $\alpha \in F$;

(iii) $Tr_{F/K}$ é uma transformação linear de F em K, onde F e K são vistos como espaços vetoriais sobre K;

(iv) $Tr_{F/K}(a) = ma$ para todo $a \in K$;

(v) $Tr_{F/K}(\alpha^q) = Tr_{F/K}(\alpha)$ para todo $\alpha \in F$.

Prova.

(i) Sejam $\alpha, \beta \in F$. Usando o fato da característica de K ser primo p tal que $q = p^k$ tem-se:

$$\begin{aligned} Tr_{F/K}(\alpha+\beta) &= \alpha+\beta+(\alpha+\beta)^q+\cdots+(\alpha+\beta)^{q^{m-1}} \\ &= \alpha+\beta+\alpha^q+\beta^q+\cdots+\alpha^{q^{m-1}}+\beta^{q^{m-1}} \\ &= \alpha+\alpha^q+\cdots\alpha^{q^{m-1}}+\beta+\beta^q+\cdots+\beta^{q^{m-1}} \\ &= Tr_{F/K}(\alpha)+Tr_{F/K}(\beta). \end{aligned}$$

(ii) Dado $c \in K$, segue da Proposição 13 que $c^{q^j} = c$ para todo $j \geq 0$. Portanto, dado $\alpha \in F$, tem-se:

$$\begin{aligned} Tr_{F/K}(c\alpha) &= c\alpha+c^q\alpha^q+\cdots+c^{q^{m-1}}\alpha^{q^{m-1}} \\ &= c\alpha+c\alpha^q+\cdots+c\alpha^{q^{m-1}} \\ &= cTr_{F/K}(\alpha). \end{aligned}$$

(iii) As propriedades (i) e (ii) junto ao fato de que $Tr_{F/K}(\alpha) \in K$ para todo $\alpha \in F$ mostram que $Tr_{F/K}$ é uma transformação linear de F em K.

(iv) Dado $a \in K$, tem-se $Tr_{F/K}(a) = a + a^q + \cdots a^{q^{m-1}}$. Mas da Proposição 13, $a^q = a$ e, portanto, $Tr_{F/K}(a) = ma$.

(v) Dado $\alpha \in F$, segue da Proposição 13 que $\alpha^{q^m} = \alpha$ e além disso,

$$\begin{aligned} Tr_{F/K}(\alpha^q) &= \alpha^q+\alpha^{q^2}+\cdots+\alpha^{q^m} \\ &= \alpha+\alpha^q+\cdots+\alpha^{q^{m-1}} = Tr_{F/K}(\alpha). \end{aligned}$$

■

Teorema 24. Seja F uma extensão finita de $K = \mathbb{F}_q$. Então para todo $\alpha \in F$ tem-se que $Tr_{F/K}(\alpha) = 0$ se, e somente se, $\alpha = \beta^q - \beta$ para algum $\beta \in F$.

Prova. ($\Rightarrow$) Seja $\alpha \in F = \mathbb{F}_{q^m}$ tal que $Tr_{F/K}(\alpha) = 0$ e seja β alguma raiz de $x^q - x - \alpha$ em alguma extensão de F. Disso segue que $\beta^q - \beta = \alpha$ e, além disso,

$$\begin{aligned} 0 = Tr_{F/K}(\alpha) &= \alpha+\alpha^q+\cdots+\alpha^{q^{m-1}} \\ &= (\beta^q-\beta)+(\beta^q-\beta)^q+\cdots+(\beta^q-\beta)^{q^{m-1}} \\ &= (\beta^q-\beta)+(\beta^{q^2}-\beta^q)+\cdots+(\beta^{q^m}-\beta^{q^{m-1}}) \\ &= (\beta^q-\beta^q)+(\beta^{q^2}-\beta^{q^2})+\cdots+(\beta^{q^{m-1}}-\beta^{q^{m-1}})+\beta^{q^m}-\beta \\ &= \beta^{q^m}-\beta \end{aligned}$$

segue do Corolário 16 que $\beta \in F$.

($\Leftarrow$) Seja $\alpha = \beta^q - \beta$ para algum $\beta \in F$. Do Teorema 23(v), $Tr_{F/K}(\beta^q) = Tr_{F/K}(\beta)$ e, portanto, $Tr_{F/K}(\alpha) = Tr_{F/K}(\beta^q - \beta) = Tr_{F/K}(\beta^q) - Tr_{F/K}(\beta) = 0$.

■

Teorema 25. (Transitividade do Traço). Seja K um corpo finito, F uma extensão finita de K e E uma extensão finita de F. Então

$$Tr_{E/K}(\alpha) = Tr_{F/K}(Tr_{E/F}(\alpha)) \text{ para todo } \alpha \in E.$$

Prova. Seja $K = \mathbb{F}_q$, e sejam $[F : K] = m, [E : F] = n$, disso segue que $[E : K] = mn$. Então para $\alpha \in E$ tem-se que

$$\begin{aligned} Tr_{F/K}(Tr_{E/F}(\alpha)) &= \sum_{i=0}^{m-1} \left(Tr_{E/F}(\alpha)\right)^{q^i} = \sum_{i=0}^{m-1} \left(\sum_{j=0}^{n-1} \alpha^{q^{jm}}\right)^{q^i} \\ &= \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \alpha^{q^{jm+i}} \overset{*}{=} \sum_{k=0}^{mn-1} \alpha^{q^k} = Tr_{E/K}(\alpha). \end{aligned}$$

Note que é valido $*$, uma vez que, para todo $k, 0 \leq k \leq mn-1$, $k = jm + i$, com $i = 1, \cdots, m-1$ e $j = 0, \cdots, n-1$ é tal que $(n-1)m + m - 1 = nm - m + m - 1 = mn - 1$.

■

Definição 26. Dado um corpo K, dizemos que uma extensão F de K é um fecho algébrico de K quando F contém todas as raízes de polinômios com coeficientes em K.

Proposição 27. Sejam $f_1, f_2 \in \mathbb{F}_q[x]$ e seja $\mathbb{F}$ o fecho algébrico de $\mathbb{F}_q$. Se $(f_1, f_2) = 1$ em $\mathbb{F}_q[x]$ então $(f_1, f_2) = 1$ em $\mathbb{F}[x]$.

Prova. Suponha que $(f_1, f_2) \neq 1$ em $\mathbb{F}[x]$, então existe $r \in \mathbb{F}$ tal que $f_1(r) = f_2(r) = 0$. Seja

$$A := \{p(x) \in \mathbb{F}_q[x] : p(r) = 0\}.$$

Note que $f_1, f_2 \in A$ e A é um ideal de $\mathbb{F}_q[x]$ uma vez que:

1. $(A, +)$ é um subgrupo de $(\mathbb{F}_q[x], +)$;
2. Para todo $f \in \mathbb{F}_q[x]$ e para todo $g \in A$ o produto $fg \in A$.

Como $\mathbb{F}_q$ é corpo, todo ideal de $\mathbb{F}_q[x]$ é principal. Portanto existe $g_0 \in \mathbb{F}_q[x]$ tal que $A = \langle g_0 \rangle$, assim tem-se $g_0 | f_1$ e $g_0 | f_2$ e disso resulta que $f_1 = g_0 p_1$ e $f_2 = g_0 p_2$ onde $p_1, p_2 \in \mathbb{F}_q[x]$. Como $(f_1, f_2) = 1$, resulta que $g_0 = c$, onde c é uma constante não nula, pois $A \neq \{0\}$. Logo todo polinômio $f \in \mathbb{F}_q[x]$ está em A. Se g é um polinômio constante, $f = (fg^{-1})g$ é elemento de A, e $F_q[x] = A$. Absurdo! Pois se o fosse, $X, X - 1 \in A = \mathbb{F}_q[x]$ e disso teríamos $r = 0$ e $r = 1$ simultaneamente, porém $0 \neq 1$ em todo corpo.

■

Definição 28. Seja K um corpo e $f(x) \in K[x]$. Dizemos que $f(x)$ é separável sobre K, se no seu corpo de fatoração, f tiver todas as suas raízes distintas, ou seja, $f(x)$ se fatorar em fatores lineares sobre seu corpo de fatoração.

Definição 29. Um corpo K é chamado perfeito se qualquer uma das seguintes condições equivalentes se verifica:

(i) Todo polinômio irredutível sobre K tem raízes distintas;

(ii) Todo polinômio irredutível sobre K é separável;

(iii) Toda extensão finita de K é separável;

(iv) $Char(K) = 0$ ou $K^p = K$ se $Char(K) = p$, onde $K^p = \{k^p : k \in K\}$;

(v) $Char(K) = 0$ ou a aplicação $x \mapsto x^p$ é um autormorfismo de K quando $Char(K) = p$.

Teorema 30. Todo corpo finito é perfeito.

Prova. Seja F um corpo finito tal que $C(F) = p$. Considere a seguinte aplicação

$$\begin{array}{rccc} \varphi: & F & \to & F \\ & x & \mapsto & x^p \end{array}$$

e mostremos que φ é um automorfismo de corpos. Sejam $x, y \in F$, assim

- $\varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y)$;
- $\varphi(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i = x^p + y^p = \varphi(x) + \varphi(y)$.

Veja que $p|\binom{p}{i}$ se $i \in \{1, 2, \cdots, p-1\}$ e, além disso, $x^p \neq 0$ quando $x \neq 0$ e disso segue que $N(\varphi) = \{0\}$. Logo, φ é injetora e como F é finito, φ é sobrejetora. Portanto, φ é automorfismo.

■

1.3 Caracteres

Seja G um grupo abeliano finito (escrito de forma multiplicativa) de ordem $|G|$ com identidade sendo 1_G. Um caráter χ de G é um homomorfismo de G no grupo multiplicativo U dos números complexos que têm valor absoluto 1, isto é, uma função de G em U com $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$ para todo $g_1, g_2 \in G$. Uma vez que $\chi(1_G) = \chi(1_G)\chi(1_G)$ devemos ter $\chi(1_G) = 1$. Além disso,

$$(\chi(g))^{|G|} = \chi((g)^{|G|}) = \chi(1_G) = 1$$

para todo $g \in G$, assim os valores de $\chi(g)$ são $|G|$-ésimas raízes da unidade. Podemos observar que $\chi(g)\chi(g^{-1}) = \chi(gg^{-1}) = \chi(1_G) = 1$ e então, $\chi(g^{-1}) = (\chi(g))^{-1} = \overline{\chi(g)}$ para todo $g \in G$, onde a barra denota o conjugado complexo.

Entre os caracteres de G temos o caráter trivial χ_0 definido por $\chi_0(g) = 1$ para todo $g \in G$. Todos os outros caracteres são chamados de não triviais. Cada caráter χ de G está associado ao caráter conjugado $\overline{\chi}$ definido por $\overline{\chi}(g) = \overline{\chi(g)}$ para todo $g \in G$. Dados finitos caracteres $\chi_1 \cdots \chi_n$ de G podemos formar o produto de caracteres $\chi_1 \cdots \chi_n$ definindo $(\chi_1 \cdots \chi_n)(g) = \chi_1(g) \cdots \chi_n(g)$ para todo $g \in G$. Se $\chi_1 = \cdots = \chi_n = \chi$, escrevemos χ^n para $\chi_1 \cdots \chi_n$. Note que o conjunto $\hat{G}$ de caracteres de G forma um grupo abeliano sob essa multiplicação de caracteres. Uma vez que os caracteres de G podem apenas ser $|G|$-ésimas raízes da unidade, $\hat{G}$ é finito.

Depois de considerar brevemente o caso especial do grupo cíclico finito, estabeleceremos alguns fatos básicos sobre os caracteres.

Exemplo 31. Seja G um grupo cíclico finito de ordem n, e seja g um gerador de G. Para um inteiro fixado j, $0 \leq j \leq n-1$, a função

$$\chi_j(g^k) = e^{2\pi ijk/n}, \ k = 0, 1, \cdots, n-1$$

define um caráter de G. Com efeito, se χ é um caráter de G, então $\chi(g)$ deve ser uma raiz n-ésima da unidade, digamos $\chi(g) = e^{2\pi ij/n}$ para algum j, $0 \leq j \leq n-1$, e segue que $\chi = \chi_j$. Portanto, $\hat{G}$ consiste exatamente dos caracteres $\chi_0, \cdots, \chi_{n-1}$.

Teorema 32. Seja H um subgrupo de um grupo abeliano finito G e seja ψ um caráter de H. Então ψ pode ser estendido a um caráter de G; em outras palavras, existe um caráter χ de G tal que $\chi(h) = \psi(h)$ para todo $h \in H$.

Prova. Suponha que H seja um subgrupo próprio de G. Tome $a \in G$ de forma que $a \notin H$ e seja H_1 o subgrupo de G gerado por H e a. Seja m o menor inteiro positivo tal que $a^m \in H$. Então todo elemento $g \in H_1$ pode ser escrito unicamente na forma $g = a^j h$ com $0 \leq j < m$ e $h \in H$. Defina uma função ψ_1 em H_1 por $\psi_1(g) = \omega^j \psi(h)$, onde ω é um número complexo fixado satisfazendo $\omega^m = \psi(a^m)$. Para verificar que ψ_1 é de fato um caráter de H_1, considere $g_1 = a^k h_1$, $0 \leq k < m, h_1 \in H$, um outro elemento de H_1. Se $j + k < m$, então $\psi_1(gg_1) = \omega^{j+k}\psi(hh_1) = \psi_1(g)\psi_1(g_1)$ e está verificado. Se $j + k \geq m$, então

$$\begin{aligned} gg_1 &= a^{j+k-m}(a^m h h_1) \\ \psi_1(gg_1) &= \omega^{j+k-m}\psi(a^m h h_1) \\ &= \omega^{j+k-m}\psi(a^m)\psi(hh_1) \\ &= \omega^{j+k}\psi(hh_1) \\ &= \psi_1(g)\psi_1(g_1). \end{aligned}$$

Note que $\psi_1(h) = \psi(h)$ para todo $h \in H$. Se $H_1 = G$, então acabou. Caso contrário, basta continuar o processo até que se obtenha uma extensão ψ em G.

■

Corolário 33. Para quaisquer dois elementos distintos $g_1, g_2 \in G$ existe um caráter χ de G tal que $\chi(g_1) \neq \chi(g_2)$.

Prova. Sejam $g_1, g_2 \in G$ tais que $g_1 \neq g_2$. Segue que $h = g_1 g_2^{-1} \neq 1_G$. Considere $H = \langle h \rangle$ e suponha que $|H| = n$. Pelo Exemplo 31, para um inteiro fixado $j, 0 \leq j \leq n-1$, a função

$\psi_j(h^k) = e^{2\pi ijk/n}$, $k \in \{1, \cdots, n-1\}$, define um caráter de H tal que $\psi_j(h) \neq 1$, para algum j. Pelo Teorema 32, existe uma extensão χ de ψ_j. Assim

$$\begin{aligned} \psi_j(h) \neq 1 &\Rightarrow \chi(h) \neq 1_G \\ &\Rightarrow \chi(g_1 g_2^{-1}) \neq 1_G \\ &\Rightarrow \chi(g_1) \neq \chi(g_2). \end{aligned}$$

■

Teorema 34. Se χ é um caráter não trivial de um grupo abeliano finito G, então

$$\sum_{g \in G} \chi(g) = 0. \tag{1.5}$$

Se $g \in G$ com $g \neq 1_G$, então

$$\sum_{\chi \in \hat{G}} \chi(g) = 0. \tag{1.6}$$

Prova. Como χ é um caráter não trivial, existe $h \in G$ tal que $\chi(h) \neq 1$. Então

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(g),$$

uma vez que g percorre todos os elementos de G. Subtraindo as parcelas extremas das igualdades acima, obtemos

$$(\chi(h) - 1) \sum_{g \in G} \chi(g) = 0$$

e como $\chi(h) \neq 1$, segue (1.5). Na segunda parte, note que a função $\tilde{g}$ definida por $\tilde{g}(\chi) = \chi(g)$ para todo $\chi \in \hat{G}$ é um caráter do grupo abeliano finito $\hat{G}$. Esse caráter é não trivial, uma vez que, pelo Corolário 33, existe $\chi \in \hat{G}$ tal que $\chi(g) \neq \chi(1_g) = 1$. Logo, aplicando (1.5) ao grupo $\hat{G}$, temos

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

■

Observação 35. Note que se $\chi = \chi_0$, segue que $\sum_{g \in G} \chi_0(g) = |G|$ e se $g = 1_G$, então $\sum_{\chi \in \hat{G}} \chi(1_G) = |\hat{G}|$.

Teorema 36. O número de caracteres de um grupo abeliano finito G é igual a $|G|$.

Prova. Utilizando a observação anterior, as identidades (1.5) e (1.6), e definindo $1_G = g_0$, obtemos

- $|G| = \sum_{g \in G} \chi_0(g) + \sum_{g \in G} \chi_1(g) + \cdots + \sum_{g \in G} \chi_{n-1}(g) = \sum_{g \in G} \sum_{\chi \in \hat{G}} \chi(g)$;
- $|\hat{G}| = \sum_{\chi \in \hat{G}} \chi(g_0) + \sum_{\chi \in \hat{G}} \chi(g_1) + \cdots + \sum_{\chi \in \hat{G}} \chi(g_{n-1}) = \sum_{\chi \in \hat{G}} \sum_{g \in G} \chi(g)$.

Portanto, segue o resultado. ■

As demonstrações do Teorema 34 e 36 podem ser combinadas nas relações de ortogonalidade para caracteres. Sejam χ e ψ caracteres de G. Então

$$\frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\psi(g)} = \begin{cases} 0 \text{ para } \chi \neq \psi \\ 1 \text{ para } \chi = \psi. \end{cases} \tag{1.7}$$

A primeira parte segue aplicando (1.5) ao caráter $\chi\overline{\psi}$ e a segunda é imediata. Além disso, se g e h são elementos de G, então

$$\frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\chi(h)} = \begin{cases} 0 \text{ para } g \neq h \\ 1 \text{ para } g = h. \end{cases} \tag{1.8}$$

Aqui a primeira parte é obtida aplicando (1.6) ao elemento gh^{-1} e a segunda parte segue do Teorema 36.

Teoria dos caracteres é também usada para obter expressões para o número de soluções de equações em um grupo abeliano finito G. Seja $f : G^n \to G$ uma função arbitrária. Então, fixado $h \in G$, o número $N(h)$ de n-uplas $(g_1, \cdots, g_n) \in G^n$ tal que $f(g_1, \cdots, g_n) = h$ é dado por

$$N(h) = \frac{1}{|G|}\sum_{g_1\in G}\cdots\sum_{g_n\in G}\sum_{\chi\in\hat{G}}\chi(f(g_1, \cdots, g_n))\overline{\chi(h)} \tag{1.9}$$

de acordo com (1.8).

Um caráter χ de G pode ser não trivial em G, mas ainda aniquila todo um subgrupo H de G, no sentido de que $\chi(h) = 1$ para todo $h \in H$. O conjunto de todos os caracteres de G que aniquilam um subgrupo H é chamado de aniquilador de H em $\hat{G}$.

Teorema 37. Seja H um subgrupo de um grupo abeliano finito G. Então o aniquilador de H em $\hat{G}$ é um subgrupo de $\hat{G}$ de ordem $|G|/|H|$.

Prova. Seja A o aniquilador de H em $\hat{G}$. Note que da definição tem-se que A é um subgrupo de $\hat{G}$. Seja $\chi \in A$; então $\mu(gH) = \chi(g), g \in G$, é um caráter bem definido do grupo quociente G/H. Analogamente, se μ é um caráter de G/H, então $\chi(g) = \mu(gH)$, define um caráter de G aniquilando H. Elementos distintos de A correspondem a caracteres distintos de G/H. Portanto, A tem uma correspondência biunívoca com o grupo de caracteres $\widehat{G/H}$, e então, a ordem de A é igual a ordem de $\widehat{G/H}$, que é $|G/H| = |G|/|H|$ de acordo com o Teorema 36.

■

Em um corpo finito $\mathbb{F}_q$ existem dois tipos de grupos abelianos que são importantes, o grupo aditivo e o grupo multiplicativo do corpo. Portanto, iremos fazer uma importante distinção entre os caracteres que pertencem a essas duas estruturas. Em ambos os casos, fórmulas explícitas podem ser fornecidas.

Considere o grupo aditivo de $\mathbb{F}_q$. Seja p a característica de $\mathbb{F}_q$; então o corpo primo contido em $\mathbb{F}_q$ é $\mathbb{F}_p$, o qual identificamos por $\mathbb{Z}/(p)$. Seja $Tr : \mathbb{F}_q \to \mathbb{F}_p$ a função traço absoluta de $\mathbb{F}_q$ em $\mathbb{F}_p$. Então a função χ_1 definida por

$$\chi_1(c) = e^{2\pi i Tr(c)/p} \text{ para todo } c \in \mathbb{F}_q \tag{1.10}$$

é um caráter do grupo aditivo de $\mathbb{F}_q$, uma vez que para todo $c_1, c_2 \in \mathbb{F}_q$ temos $Tr(c_1+c_2) = Tr(c_1) + Tr(c_2)$ e $\chi_1(c_1 + c_2) = \chi_1(c_1)\chi_1(c_2)$. Em vez de "caráter do grupo aditivo de $\mathbb{F}_q$"chamaremos de caráter aditivo de $\mathbb{F}_q$. O caráter χ_1 em (1.10) será chamado de caráter aditivo canônico de $\mathbb{F}_q$. Todos os caracteres de $\mathbb{F}_q$ podem ser expressos em termos de χ_1.

Teorema 38. Para $b \in \mathbb{F}_q$, a função $\chi_b(c) = \chi_1(bc)$ para todo $c \in \mathbb{F}_q$ é um caráter aditivo de $\mathbb{F}_q$, e todo caráter aditivo é obtido desta forma.

Prova. Sejam $c_1, c_2 \in \mathbb{F}_q$, tem-se que

$$\chi_b(c_1 + c_2) = \chi_1(bc_1 + bc_2) = \chi_1(bc_1)\chi_1(bc_2) = \chi_b(c_1)\chi_b(c_2)$$

e a primeira parte está demonstrada. Do Teorema 23(iii), tem-se que $Tr : \mathbb{F}_q \to \mathbb{F}_p$ é uma função sobrejetora e, portanto, χ_1 é um caráter não trivial. Assim, se $a, b \in \mathbb{F}_q$ com $a \neq b$ tem-se

$$\chi_a(c)(\chi_b(c))^{-1} = \chi_1(ac)(\chi_1(bc))^{-1} = \chi_1\left((a-b)c\right) \neq 1$$

para conveniente $c \in \mathbb{F}_q$ e, assim, χ_a e χ_b são caracteres distintos. Uma vez que b percorre todos os elementos de $\mathbb{F}_q$, obtêm-se q caracteres distintos χ_b. Por outro lado, segue do Teorema 36 que $\mathbb{F}_q$ possui exatamente q caracteres aditivos e, portanto, o conjunto dos caracteres aditivos de $\mathbb{F}_q$ está completo.

■

Observação 39. Definindo $b = 0$ no Teorema anterior, obtemos o caráter aditivo trivial χ_0, o qual $\chi_0(c) = 1$ para todo $c \in \mathbb{F}_q$.

Sejam E uma extensão finita de $\mathbb{F}_q$, χ_1 o caráter canônico aditivo de $\mathbb{F}_q$ e μ_1 o caráter canônico aditivo de E definido em analogia com (1.10), onde Tr é substituído pela função traço absoluto Tr_E de E em $\mathbb{F}_p$. Então χ_1 e μ_1 estão relacionados pela identidade

$$\chi_1\left(Tr_{E/\mathbb{F}_q}(\beta)\right) = \mu_1(\beta) \text{ para todo } \beta \in E,$$

onde $Tr_{E/\mathbb{F}_q}$ é a função traço de E em $\mathbb{F}_q$. Isso decorre da relação de transitividade

$$Tr_{E/\mathbb{F}_p}(\beta) = Tr\left(Tr_{E/\mathbb{F}_q}(\beta)\right) \text{ para todo } \beta \in E,$$

que foi apresentada no Teorema 25.

Caracteres do grupo multiplicativo $\mathbb{F}_q^*$ de $\mathbb{F}_q$ são chamados caracteres multiplicativos de $\mathbb{F}_q$. Do Teorema 17, $\mathbb{F}_q^*$ é grupo cíclico de ordem $q-1$ de forma que seus caracteres podem ser facilmente determinados.

Teorema 40. Seja g um elemento primitivo fixado de $\mathbb{F}_q^*$. Para cada $j = 0, 1, \cdots, q-2$, a função ψ_j com

$$\psi_j(g^k) = e^{2\pi ijk/(q-1)} \text{ para } k = 0, 1, \cdots, q-2$$

define um caráter multiplicativo de $\mathbb{F}_q$, e todo caráter multiplicativo de $\mathbb{F}_q$ é obtido desta maneira.

Prova. Segue imediatamente do Exemplo 31.

■

O caráter ψ_0 sempre irá representar o caráter multiplicativo trivial, na qual satisfaz $\psi_0(c) = 1$ para todo $c \in \mathbb{F}_q^*$.

Corolário 41. O grupo de caracteres multiplicativos de $\mathbb{F}_q$ é cíclico de ordem $q-1$, sendo a identidade o elemento ψ_0.

Prova. Todo caráter ψ_j no Teorema 40 com j sendo primo relativo a $q-1$ é gerador do grupo em questão.

■

1.4 Elementos s-livres

Definição 42. Seja s um divisor de $q-1$. Um elemento $\alpha \in \mathbb{F}_q^*$ é chamado s-livre se para todo $d \in \mathbb{N}$ tal que $d \mid s$ e $d \neq 1$, não existe $\beta \in \mathbb{F}_q$ satisfazendo $\beta^d = \alpha$.

Assim, se $\alpha \in \mathbb{F}_q^*$ é um s-livre, então α não pode ser d-ésima potência de um elemento, onde $d \neq 1$ e $d \mid s$. A seguir, apresentaremos alguns resultados que serão usados no que se segue.

Lema 43. Seja $\alpha \in \mathbb{F}_q$, então:

1. α é primitivo se, e somente se, α é $(q-1)$-livre.
2. Se α é s-livre para algum inteiro s, então α é e-livre para todo $e \mid s$.
3. Se α é s_1-livre e s_2-livre, então α é $\text{mmc}(s_1, s_2)$-livre.
4. Sejam $p_1, \cdots, p_n$ primos. Então α é $(p_1 \cdots p_n)$-livre se, e somente se, α é $(p_1^{\alpha_1} \cdots p_n^{\alpha_n})$-livre, onde $\alpha_i > 0$ para todo i.

Prova.

1. ($\Rightarrow$) Seja α primitivo, assim $ord(\alpha) = q-1$. Considere $D = \{d \in \mathbb{N} : d \mid q-1\}$. Suponha que para algum $d \in D$, existe $\beta \in \mathbb{F}_q$ tal que $\beta^d = \alpha$. Como $d \mid q-1$, existe $s \in \mathbb{N}$ tal que $q-1 = ds$. Assim $\beta^d = \alpha \Rightarrow \beta^{ds} = \alpha^s \Rightarrow \beta^{q-1} = \alpha^s = 1$. Contradição, pois $ord(\alpha) = q-1$ e $s < q-1$. Portanto, para todo $d \in D$, não existe $\beta \in \mathbb{F}_q$ tal que $\beta^d = \alpha$. Logo α é $(q-1)$-livre.

   ($\Leftarrow$) Sejam α $(q-1)$-livre, b um gerador de $\mathbb{F}_q^*$ e $d \in \mathbb{N}$ tal que $b^d = \alpha$. Como α é $(q-1)$-livre, tem-se $d = 1$ ou d não divide $q-1$. Se $d = 1$, segue que $\alpha = b$, ou seja, α é primitivo. Suponha que d não divide $q-1$ e considere $e = (d, q-1)$. Se $e = 1$, então $ord(\alpha) = ord(b^d) = ord(b)$, uma vez que,

$$ord(b^d) = \frac{ord(b)}{(d, ord(b))} = \frac{ord(b)}{(d, q-1)} = \frac{ord(b)}{e} = ord(b)$$

   e logo α é primitivo. Note que se $e > 1$, ponha $d = ef$ e $c = b^f$ e então tem-se $c^e = c^{\frac{d}{f}} = b^d = \alpha$, ou seja, $c^e = \alpha$ o que contradiz o fato de α ser $(q-1)$-livre visto que $e > 1$ e $e \mid q-1$. De todo modo, segue o resultado.

2. Suponha que α é s-livre e seja e tal que $e \mid s$. Considere $D = \{d \in \mathbb{N} : d \mid s\}$ e $D' = \{d \in \mathbb{N} : d \mid e\}$. Como $D' \subset D$ então não existe $\beta \in \mathbb{F}_q$ tal que $\beta^d = \alpha$ para todo $d \in D'$. Portanto, α é e-livre.

3. Considere os conjuntos $D_1 = \{d \in \mathbb{N} : d \mid s_1\}$, $D_2 = \{d \in \mathbb{N} : d \mid s_2\}$ e $D_3 = \{d \in N : d \mid s_0\}$, onde $s_0 = \text{mmc}(s_1, s_2)$. Suponha que α seja s_1-livre e s_2-livre. Se $s_0 \in \{s_1, s_2\}$, então α é s_0-livre. Se $s_0 \notin \{s_1, s_2\}$, então $s_0 = \dfrac{s_1 \cdot s_2}{\text{mdc}(s_1, s_2)}$. Note que os possíveis divisores de s_0 pertencem a $D_1 \cup D_2 \cup D_3$. Sabemos por hipótese que não existe $\beta \in \mathbb{F}_q$ tal que $\beta^d = \alpha$ para todo $d \in D_1 \cup D_2$. Resta saber se existe $\beta \in \mathbb{F}_q$ tal que $\beta^{k_0} = \alpha$, onde $k_0 \in D_3$, ou seja, $k_0 = k_1 \cdot k_2$, onde $k_1 \in D_1$ e $k_2 \in D_2$. Note que não existe pois $\beta^{k_0} = \beta^{k_1 \cdot k_2} = \left(\beta^{k_1}\right)^{k_2} = \left(\beta^{k_2}\right)^{k_1} \neq \alpha$, pois caso contrário α seria s_1-livre ou s_2-livre. Portanto, α é $\text{mmc}(s_1, s_2)$-livre.

4. ($\Rightarrow$) Note que se α é p-livre, então para todo $\beta \in \mathbb{F}_q$, $\beta^p \neq \alpha$, em particular para $\beta \in \mathcal{B} = \{\beta^p, \beta^{p^2}, \cdots, \beta^{p^{\alpha_i - 1}}\}$, ou seja, $\beta^{p^j} \neq \alpha$ para todo $j \in \{1, \cdots, \alpha_i\}$ e disto segue que α é p^{α_i}-livre. Como α é $p_1 \cdots p_n$-livre, do Item 2, α é p_i-livre para todo $i \in \{1 \cdots n\}$ e, portanto, α é $p_i^{\alpha_i}$-livre. Do Item 3, temos que α é $\text{mmc}\{p_1^{\alpha_1}, \cdots, p_n^{\alpha_n}\}$-livre, ou seja, α é $p_1^{\alpha_1} \cdots p_n^{\alpha_n}$-livre.

   ($\Leftarrow$) Suponha que α é $(p_1^{\alpha_1} \cdots p_n^{\alpha_n})$-livre onde $\alpha_i > 0$ para todo $i \in \{1, \cdots, n\}$. Considerando $\alpha_1 = \cdots = \alpha_n = 1$ tem-se que α é $(p_1 \cdots p_n)$-livre.

■

Lema 44. Sejam α um elemento não primitivo de $\mathbb{F}_q$, l um divisor de $q-1$ e $\{p_1, \cdots, p_r\}$ o conjunto de todos os divisores primos de $q-1$ que não dividem l. Então α não é $p_i l$-livre para algum $i \in \{1, \cdots, r\}$.

Prova. Seja $q - 1 = p_1^{\alpha_1} \cdots p_r^{\alpha_r} l$. Suponhamos por absurdo que α é $p_i l$-livre para todo $i \in \{1, \cdots, r\}$. Pelo Item 3 da observação acima, α é $\text{mmc}\{p_1 l, \cdots, p_r l\}$-livre, ou seja, α é $(p_1 \cdots p_r)l$-livre e pelo Item 2, α é $p_1 \cdots p_r$-livre e l-livre. Uma vez que α é $(p_1 \cdots p_r)$-livre, pelo Item 4, α é $(p_1^{\alpha_1} \cdots p_n^{\alpha_r})$-livre. Utilizando o Item 3 novamente, α é $\text{mmc}\{p_1^{\alpha_1} \cdots p_r^{\alpha_r}, l\}$-livre, que é $(p_1^{\alpha_1} \cdots p_n^{\alpha_r})l$-livre, ou seja, é $(q-1)$-livre. Pelo Item 1, α é primitivo, que é uma contradição. Portanto, segue o resultado.

■

1.5 Representações de funções características

Definição 45. A ordem $\min\{k \in N : u^k \equiv 1 \pmod p\}$ de um elemento $u \in \mathbb{F}_p$ é denotada por $ord_p(u)$. Um elemento u é uma raiz primitiva se $ord_p(u) = p - 1$.

A função característica $\Phi : G \to \{1, 0\}$ de elementos primitivos é uma das ferramentas analíticas usadas para investigar as várias propriedades das raízes primitivas em grupos cíclicos G. Muitas representações equivalentes da função característica Φ de elementos primitivos são possíveis.

1.5.1 Função característica depende dos divisores

Uma representação de função característica depende da ordem do grupo cíclico G. Essa representação é sensível à decomposição de primos $|G| = q = p_1^{e_1} \cdots p_n^{e_n}$ com p_i primo

e $e_i \geq 1$.

Lema 46. Seja G um grupo cíclico finito tal que $|G| = p-1$, e seja $u = \tau^m \neq 0 \in G$ um elemento invertível do grupo. Se u não é uma q-ésima potência módulo p para todo $q \mid p-1$, onde $\text{mdc}(m, p-1) = 1$, então

$$\sum_{ord(\chi)=q} \chi(u) = \sum_{ord(\chi)=q} \chi(\tau^m) = -1.$$

Prova. Seja H um subgrupo de G tal que $|H| = q \mid p-1$ e q é primo. Note que $\hat{H} \cong H$ pois H e $\hat{H}$ são cíclicos de mesma ordem. Seja $\psi \in \hat{H}$ tal que $\langle \psi \rangle = \hat{H}$. Assim tem-se $\langle \psi^j \rangle = \hat{H}$ para todo $j \in \{1, \cdots, q-1\}$ uma vez que q é primo, ou seja, ψ^j tem ordem q em $\hat{H}$. Logo

$$\sum_{j=0}^{q-1} \psi^j(\tau^m) = 1 + \sum_{ord(\chi)=q} \chi(\tau^m). \tag{1.11}$$

Por outro lado,

$$\psi^0(\tau^m) + \psi^1(\tau^m) + \cdots + \psi^{q-1}(\tau^m) = \frac{\psi^q(\tau^m) - 1}{\psi(\tau^m) - 1}.$$

Uma vez que $\psi^0(\tau^m) = 1$ e $\psi(\tau^m) \neq 1$ pois $ord(\psi) = q, \text{mdc}(q, m) = 1$, segue de (1.11) que $\sum_{ord(\chi)=q} \chi(\tau^m) = -1$.

■

Lema 47. A função

$$f(n) = \sum_{\chi \in \hat{G}: ord(\chi)=d} \chi(u)$$

é multiplicativa.

Prova. Dados $a, b \in \mathbb{N}$ coprimos, queremos mostrar que

$$\sum_{ord(\chi)=ab} \chi(u) = \sum_{ord(\chi_1)=a} \sum_{ord(\chi_2)=b} \chi_1(u)\chi_2(u). \tag{1.12}$$

Afirmação 1: Sejam $a, b \in \mathbb{N}$ tais que $\text{mdc}(a, b) = 1$ e $f, g \in \hat{G}$ com $ord(f) = a$ e $ord(g) = b$. Então $ord(fg) = ab$.

Primeiramente, observe que $\hat{G}$ é abeliano e assim

$$(fg)^{ab} = f^{ab}g^{ab} = (f^a)^b(g^b)^a = 1^b 1^a = 1,$$

daí segue que $ord(fg) \overset{*}{\leq} ab$. Seja $n \in \mathbb{N}$ tal que $(fg)^n = 1$. Assim tem-se $f^n = g^{-n}$ pois $\hat{G}$ é abeliano. Note que $f^n \in \langle f \rangle \cap \langle g \rangle$ e sendo $f^n \in \langle f \rangle$ tem-se $ord(f^n) | a$ e de modo análogo, tem-se $ord(f^n) | b$. Assim $ord(f^n)$ divide a e b, com $(a, b) = 1$ e assim tem-se que $ord(f^n) = 1$ e $f^n = 1$, logo, $a | n$. Analogamente, tem-se que, $b | n$. Uma vez que a e b são coprimos, temos $\text{mmc}(a, b) = ab$. E como $a | n$ e $b | n$, então $\text{mmc}(a, b) | n$, ou seja, $ab | ord(fg)$, e de $(*)$ segue que $ord(fg) = ab$.

Afirmação 2: Sejam $a, b \in \mathbb{N}$ tal que $(a, b) = 1$ e $f, g, h, l \in \hat{G}$ com $(f, g) \neq (h, l)$ (i.e. $f \neq h$ ou $g \neq l$) de forma que $ord(f) = ord(h) = a$, $ord(g) = ord(l) = b$. Então $fg \neq hl$.

Se $f = h$, então $g \neq l$, logo existe $u \in G$ tal que $g(u) \neq l(u)$ e, então, $f(u)g(u) \neq h(u)l(u)$ e $fg \neq hl$. Se $g = l$, então $f \neq h$ e, de forma análoga, conclui-se que $fg \neq hl$. Seja $f \neq h$ e $g \neq l$. Suponha, por absurdo, que $fg = hl$. Assim, para todo $u \in G, f(u) = \frac{h(u)l(u)}{g(u)}$ e, portanto, $f = \frac{hl}{g} = h\frac{l}{g} = h(lg^{-1})$. Note que a ordem $ord(lg^{-1})$ divide b, pois dado $u \in G$, $((lg^{-1})(u))^b = \frac{l(u)^b}{g(u)^b} = 1$. Seja $k = ord(lg^{-1})$, e como $k|b$ segue que $(k, a) = 1$. Sendo $ord(h) = a$ e $f = h(lg^{-1})$, da afirmação 1, temos $a = ord(f) = ord(h)ord(gl^{-1}) = ak$. Segue que $k = 1$ pois $a \neq 0$, ou seja, $lg^{-1} = 1$ e, portanto, $l = g$. Sendo $l = g$ e $fg = hl$, tem-se $f = h$ contradizendo $(f, g) \neq (h, l)$.

A afirmação 1 nos diz que cada termo do lado direito de (1.12) é algum dos termos do lado esquerdo, e a afirmação 2 nos diz que esse termo do lado esquerdo é único. Junto a isso, sendo a e b coprimos tem-se

$$\phi(ab) = \sharp\{\chi \in \hat{G} : ord(\chi) = ab\} = \phi(a)\phi(b) = \sharp\{\chi_1\chi_2 \in \hat{G} : ord(\chi_1) = a, ord(\chi_2) = b\}.$$

e, portanto, f é multiplicativa. ■

Lema 48. Seja G um grupo cíclico de ordem $p - 1$. Então

$$\Psi(u) = \frac{\phi(p-1)}{p-1} \cdot \sum_{d|p-1} \frac{\mu(d)}{\phi(d)} \cdot \sum_{ord(\chi)=d} \chi(u) = \begin{cases} 1 \text{ se } ord_p(u) = p-1 \\ 0 \text{ se } ord_p(u) \neq p-1. \end{cases} \tag{1.13}$$

Prova. Assuma que $u = \tau^{rm}$ é uma r-ésima potência módulo p onde $r|p-1$, r é primo e $(m, p-1) = 1$. Então a soma interna

$$\sum_{ord(\chi)=r} \chi(u) = \sum_{ord(\chi)=r} \chi(\tau^{rm}) = \sum_{ord(\chi)=r} \chi(\tau^m)^r = \phi(r) = r - 1. \tag{1.14}$$

onde $\chi(v)^r = 1$. Substituindo esta informação, usando o Lema 47 e aplicando o Teorema 8 no produto

$$\begin{aligned} \frac{\phi(p-1)}{p-1} \cdot \sum_{d|p-1} \frac{\mu(d)}{\phi(d)} \cdot \sum_{ord(\chi)=d} \chi(u) &= \frac{\phi(p-1)}{p-1} \cdot \sum_{d|p-1} \mu(d) \cdot \sum_{ord(\chi)=d} \frac{\chi(u)}{\phi(d)} \\ &= \frac{\phi(p-1)}{p-1} \prod_{r|p-1} \left(1 - \frac{\sum_{ord(\chi)=r} \chi(u)}{r-1}\right) \\ &= \frac{\phi(p-1)}{p-1} \prod_{r|p-1} \left(1 - \frac{r-1}{r-1}\right) = 0 \end{aligned} \tag{1.15}$$

mostra que a expressão anula se o elemento $u \in G$ tem ordem $ord_p(u) = r \mid p-1$ e $r < p-1$. Assuma agora que $u = \tau^m$ não é uma r-ésima potência módulo p para todo r primo, $r \mid p-1$ e $(m, p-1) = 1$. Assim, pelo Lema 44, a soma interna

$$\sum_{ord(\chi)=r} \chi(u) = \sum_{ord(\chi)=r} \chi(\tau^m) = -1. \tag{1.16}$$

substituindo esta informação no produto

$$\begin{aligned}\frac{\phi(p-1)}{p-1}\cdot\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\cdot\sum_{ord(\chi)=d}\chi(u) &= \frac{\phi(p-1)}{p-1}\prod_{r|p-1}\left(1-\frac{\sum_{ord(\chi)=q}\chi(u)}{r-1}\right)\\ &= \frac{\phi(p-1)}{p-1}\prod_{r|p-1}\left(1-\frac{-1}{r-1}\right)\\ &= \prod_{r|p-1}\left(1-\frac{1}{r}\right)\prod_{r|p-1}\left(1-\frac{-1}{r-1}\right)\\ &= \prod_{r|p-1}\left(\frac{r-1}{r}\right)\left(\frac{r}{r-1}\right)=1, \qquad (1.17)\end{aligned}$$

assim verificamos que ambos os lados da equação se anulam se, e somente se, o elemento $u \in G$ tem ordem $ord_p(u) = r \mid p-1$ e $r < p-1$.

■

Corolário 49. Seja $\mathbb{F}_q^*$ o grupo multiplicativo de $\mathbb{F}_q$ e H_s o subconjunto de $\mathbb{F}_q^*$ formado pelos elementos s-livres. Então

$$\rho_s(u) = \frac{\phi(s)}{s}\cdot\sum_{d|s}\frac{\mu(d)}{\phi(d)}\cdot\sum_{ord(\chi)=d}\chi(u) = \begin{cases}1 \text{ se } & \text{se } u \in H_s\\ 0 \text{ se } & \text{se } u \notin H_s.\end{cases} \qquad (1.18)$$

Prova. Suponha que $u \notin H_s$, então podemos dizer que que $u = \tau^{rm}$ é uma r-ésima potência módulo p onde $r \mid s$, r é primo e $(m, s) = 1$. Então a soma interna

$$\sum_{ord(\chi)=r}\chi(u) = \sum_{ord(\chi)=r}\chi(\tau^{rm}) = \sum_{ord(\chi)=r}\chi(\tau^m)^r = \phi(r) = r-1. \qquad (1.19)$$

onde $\chi(v)^r = 1$. Substituindo esta informação, usando o Lema 47 e aplicando o Teorema 8 no produto

$$\begin{aligned}\frac{\phi(s)}{s}\cdot\sum_{d|s}\frac{\mu(d)}{\phi(d)}\cdot\sum_{ord(\chi)=d}\chi(u) &= \frac{\phi(s)}{s}\cdot\sum_{d|s}\mu(d)\cdot\sum_{ord(\chi)=d}\frac{\chi(u)}{\phi(d)}\\ &= \frac{\phi(s)}{s}\prod_{r|s}\left(1-\frac{\sum_{ord(\chi)=r}\chi(u)}{r-1}\right)\\ &= \frac{\phi(s)}{s}\prod_{r|s}\left(1-\frac{r-1}{r-1}\right)=0 \qquad (1.20)\end{aligned}$$

mostra que a equação anula se $u \notin H_s$. Assuma agora que $u \in H_s$, ou seja, $u = \tau^m$ não é uma k-ésima potência módulo p para todo $k \mid s$ e $(m, s) = 1$. Pelo Lema 44, a soma interna

$$\sum_{ord(\chi)=k}\chi(u) = \sum_{ord(\chi)=k}\chi(\tau^m) = -1. \qquad (1.21)$$

onde k é um divisor primo de s. Substituindo esta informação no produto

$$\begin{aligned}
\frac{\phi(s)}{s}\cdot\sum_{d|s}\frac{\mu(d)}{\phi(d)}\cdot\sum_{ord(\chi)=d}\chi(u) &= \frac{\phi(s)}{s}\prod_{k|s}\left(1-\frac{\sum_{ord(\chi)=k}\chi(u)}{k-1}\right)\\
&= \frac{\phi(s)}{s}\prod_{k|s}\left(1-\frac{-1}{k-1}\right)\\
&= \prod_{k|s}\left(1-\frac{1}{k}\right)\prod_{k|s}\left(1-\frac{-1}{k-1}\right)\\
&= \prod_{k|s}\left(\frac{k-1}{k}\right)\left(\frac{k}{k-1}\right)=1, \qquad (1.22)
\end{aligned}$$

assim verificamos que ambos os lados da equação se anulam se, e somente se, o elemento $u \notin H_s$.

■

Capítulo 2

Pares Especiais de Elementos Primitivos

Neste capítulo, p é primo, k é um inteiro positivo e $\mathbb{F}_q$ denotará um corpo finito com $q = p^k$ elementos.

Um par $(\alpha, \beta) \in \mathbb{F}_q^2$ é um par primitivo em $\mathbb{F}_q$ se α e β são elementos primitivos. Note que $(\alpha, \beta) \in \mathbb{F}_q^2$ é um par primitivo se, e somente se, $(\alpha, \beta^{-1}) \in \mathbb{F}_q^2$ é um par primitivo. Os seguintes conceitos desempenharão um papel crucial no trabalho.

Definição 50.

1. Sejam $f_1, f_2 \in \mathbb{F}_q[x]$, definimos $\Lambda_q(f_1, f_2)$ como sendo o conjunto de pares $(n, g) \in \mathbb{N} \times \mathbb{F}_q[x] \setminus \{x\}$ tais que $\text{mdc}(n, q-1) = 1$, g é mônico, irredutível, $g^n \mid f_1 f_2$ e $g^{n+1} \nmid f_1 f_2$.

2. Sejam $m_1, m_2 \in \mathbb{N}$. Definimos $\Upsilon_q(m_1, m_2)$ como sendo o conjunto das funções racionais $\frac{f_1}{f_2} \in \mathbb{F}_q(x)$ tais que $\partial(f_1) \leq m_1$, $\partial(f_2) \leq m_2$, $\text{mdc}(f_1, f_2) = 1$ e $\Lambda_q(f_1, f_2) \neq \emptyset$.

3. Seja $m_1, m_2 \in \mathbb{N}$. Definimos $\Gamma_p(m_1, m_2)$ como sendo o conjunto dos inteiros k tal que $\mathbb{F}_{p^k}$ contém um elemento α com $(\alpha, f(\alpha))$ um par primitivo para toda $f \in \Upsilon_{p^k}(m_1, m_2)$.

O próximo resultado nos dá algumas propriedades dos conjuntos acima.

Proposição 51. Seja p um primo e seja k, l_1, l_2, m_1, m_2 inteiros positivos. Então:

1. $\Upsilon_{p^k}(m_1, m_2) \subsetneq \Upsilon_{p^k}(m_1 + l_1, m_2 + l_2)$
2. $\Gamma_p(m_1, m_2) = \Gamma_p(m_2, m_1)$
3. $\Gamma_p(m_1 + l_1, m_2 + l_2) \subset \Gamma_p(m_1, m_2)$

Prova.

1. Se $f = \frac{f_1}{f_2} \in \Upsilon_{p^k}(m_1, m_2)$ então $\partial(f_1) \leq m_1, \partial(f_2) \leq m_2, (f_1, f_2) = 1$ e $\Lambda_q(f_1, f_2) \neq \emptyset$, assim tem-se que $\partial(f_1) \leq m_1 + l_1$ e $\partial(f_2) \leq m_2 + l_2$ logo $f \in \Upsilon_{p^k}(m_1 + l_1, m_2 + l_2)$. Tomando $f = \frac{f_1}{f_2}$ tal que f_1 é um polinômio irredutível de grau $m_1 + l_1$ e $f_2 = 1$, segue que $(f_1, f_2) = 1$ e $f \notin \Upsilon_{p^k}(m_1, m_2)$.

2. Sejam $k \in \Gamma_p(m_1, m_2)$, $f = \frac{f_1}{f_2} \in \Upsilon_{p^k}(m_1, m_2)$ e $(\alpha, f(\alpha))$ um par de elementos primitivos. Como $(\alpha, f(\alpha)) \in \mathbb{F}_{p^k}^2$ é primitivo se, e somente se, $(\alpha, f(\alpha)^{-1}) \in \mathbb{F}_{p^k}^2$ é um par primitivo, então temos $f^{-1} = \frac{f_2}{f_1} \in \Upsilon_{p^k}(m_2, m_1)$ e $k \in \Gamma_p(m_2, m_1)$. Daí segue que $\Gamma_p(m_1, m_2) = \Gamma_p(m_2, m_1)$.

3. Seja $k \in \Gamma_p(m_1 + l_1, m_2 + l_2)$. Assim existe $\alpha \in \mathbb{F}_{p^k}$ tal que $(\alpha, f(\alpha)) \in \mathbb{F}_{p^k}^2$ é par primitivo para todo $f \in \Upsilon_{p^k}(m_1 + l_1, m_2 + l_2)$ e, em particular, para todo $f \in \Upsilon_{p^k}(m_1, m_2)$, isto é, $(\alpha, f(\alpha))$ é par primitivo para todo $f \in \Upsilon_{p^k}(m_1+, m_2)$. Portanto $k \in \Gamma_p(m_1, m_2)$ e $\Gamma_p(m_1 + l_1, m_2 + l_2) \subset \Gamma_p(m_1+, m_2)$.

■

No que se segue, precisaremos do seguinte resultado, que é um caso particular de [17, Teorema 5.5].

Lema 52. Seja $h(x) \in \mathbb{F}_q(x)$ uma função racional. Escreva $h(x) = \prod_{j=1}^{r} h_j(x)^{n_j}$, onde $h_j(x) \in \mathbb{F}_q(x)$ são polinômios irredutíveis distintos e n_j são inteiros não nulos. Seja χ um caráter multiplicativo de $\mathbb{F}_q$. Suponha que a função racional $h(x)$ não é da forma $g(x)^{ord(\chi)}$ em $\mathbb{F}(x)$, onde $\mathbb{F}$ é fecho algébrico de $\mathbb{F}_q$. Então temos

$$\left| \sum_{\substack{\alpha \in \mathbb{F}_q \\ h(\alpha) \neq 0, h(\alpha) \neq \infty}} \chi(h(\alpha)) \right| \leq \left(\sum_{j=1}^{r} (\partial(h_j) - 1 \right) \cdot \sqrt{q}.$$

2.1 Principais Resultados

Sejam m_1, m_2 inteiros positivos. Nosso objetivo é determinar para quais valores de k existe $\alpha \in \mathbb{F}_{p^k}$ tal que $(\alpha, f(\alpha))$ é um par primitivo para toda $f \in \Upsilon_{p^k}(m_1, m_2)$. Para isso precisaremos dos seguintes conceitos:

Definição 53. Seja $q = p^k$ e sejam l_1, l_2 divisores de $q-1$. Dado $f \in \Upsilon_{p^k}(m_1, m_2)$ iremos denotar por $N_f(l_1, l_2)$ o número de pares $(\alpha, f(\alpha))$ tais que $\alpha \in \mathbb{F}_q$ é l_1-livre e $f(\alpha)$ é l_2-livre.

Assim para que $k \in \Gamma_p(m_1, m_2)$, devemos ter $N_f(q-1, q-1) > 0$ para toda $f \in \Upsilon_q(m_1, m_2)$.

Para um inteiro l, denotaremos por $\omega(l)$ e $W(l)$ o número de divisores primos de l e o número de divisores de l que são livre de quadrados, respectivamente. Note que $W(l) = 2^{\omega(L)}$.

Teorema 54. Seja $f = \frac{f_1}{f_2} \in \Upsilon_q(m_1, m_2)$, com $q \geq 4$. Se $\sqrt{q} > (m_1 + m_2)W(l_1)W(l_2)$, então $N_f(l_1, l_2) > 0$.

Prova. Seja $f = \frac{f_1}{f_2} \in \Upsilon_q(m_1, m_2)$ e seja

$$S_f := \{\beta \in \mathbb{F}_q : f_1(\beta) = 0 \text{ ou } f_2(\beta) = 0\} \cup \{0\}.$$

Do Corolário 49 obtemos que a função característica ρ_s do conjunto dos elementos s-livre é dado por

$$\alpha \mapsto \theta(s) \sum_{d|s} \frac{\mu(d)}{\phi(d)} \sum_{ord(\chi)=d} \chi(\alpha) \tag{2.1}$$

onde $\theta(s) = \frac{\phi(s)}{s}$, μ é a função de Möbius e $ord(\chi)$ denota a ordem do caráter multiplicativo χ.

Usando a função característica ρ_{l_1} e ρ_{l_2}, note que

$$N_f(l_1, l_2) = \sum_{\alpha \in \mathbb{F} \setminus S_f} \rho_{l_1}(\alpha) \rho_{l_2}(f(\alpha))$$

e das expressões dessas funções, obtemos

$$\begin{aligned}
N_f(l_1,l_2) &= \sum_{\alpha\in\mathbb{F}\setminus S_f} \left(\theta(l_1) \sum_{d_1|l_1} \frac{\mu(d_1)}{\phi(d_1)} \sum_{ord(\chi_1)=d_1} \chi_1(\alpha) \cdot \theta(l_2) \sum_{d_2|l_2} \frac{\mu(d_2)}{\phi(d_2)} \sum_{ord(\chi_2)=d_2} \chi_2(f(\alpha)) \right) \\
&= \sum_{\alpha\in\mathbb{F}\setminus S_f} \left(\theta(l_1)\theta(l_2) \sum_{\substack{d_1|l_1 \\ d_2|l_2}} \frac{\mu(d_1)}{\phi(d_1)} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\substack{ord(\chi_1)=d_1 \\ ord(\chi_2)=d_2}} \chi_1(\alpha)\chi_2(f(\alpha)) \right) \\
&= \theta(l_1)\theta(l_2) \sum_{\substack{d_1|l_1 \\ d_2|l_2}} \frac{\mu(d_1)}{\phi(d_1)} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\alpha\in\mathbb{F}_q\setminus S_f} \left(\sum_{\substack{ord(\chi_1)=d_1 \\ ord(\chi_2)=d_2}} \chi_1(\alpha)\chi_2(f(\alpha)) \right) \\
&= \theta(l_1)\theta(l_2) \sum_{\substack{d_1|l_1 \\ d_2|l_2}} \frac{\mu(d_1)}{\phi(d_1)} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\substack{ord(\chi_1)=d_1 \\ ord(\chi_2)=d_2}} \left(\sum_{\alpha\in\mathbb{F}_q\setminus S_f} \chi_1(\alpha)\chi_2(f(\alpha)) \right) \\
&= \theta(l_1)\theta(l_2) \sum_{\substack{d_1|l_1 \\ d_2|l_2}} \frac{\mu(d_1)}{\phi(d_1)} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\substack{ord(\chi_1)=d_1 \\ ord(\chi_2)=d_2}} \tilde{\chi}(\chi_1,\chi_2)
\end{aligned} \tag{2.2}$$

onde $\tilde{\chi}(\chi_1, \chi_2) := \sum_{\alpha\in\mathbb{F}_q\setminus S_f} \chi_1(\alpha)\chi_2(f(\alpha))$.

Sejam χ_1 e χ_2 caracteres multiplicativos de ordens d_1 e d_2, respectivamente, onde $d_1 \mid l_1$ e $d_2 \mid l_2$. Seja $i \in \{1, 2\}$. Pelo Teorema 40 existe um caráter χ de ordem $q-1$ e um inteiro $n_i \in \{0, 1, \cdots, q-2\}$ tal que $\chi_i(\alpha) = \chi(\alpha^{n_i})$ para todo $\alpha \in \mathbb{F}_q^*$. Observe que $n_i = 0$ se, e somente se, $d_i = 1$. Portanto

$$\begin{aligned}
\tilde{\chi}(\chi_1,\chi_2) = \sum_{\alpha\in\mathbb{F}_q\setminus S_f} \chi_1(\alpha)\chi_2(f(\alpha)) &= \sum_{\alpha\in\mathbb{F}_q\setminus S_f} \chi(\alpha^{n_1})\chi(f(\alpha)^{n_2}) \\
&= \sum_{\alpha\in\mathbb{F}_q\setminus S_f} \chi(\alpha^{n_1} f(\alpha)^{n_2}) \\
&= \sum_{\alpha\in\mathbb{F}_q\setminus S_f} \chi\left(\alpha^{n_1}\left(\frac{f_1(\alpha)}{f_2(\alpha)}\right)^{n_2}\right) \\
&= \sum_{\alpha\in\mathbb{F}_q\setminus S_f} \chi(\alpha^{n_1} f_1(\alpha)^{n_2} f_2(\alpha)^{-n_2}) \\
&= \sum_{\alpha\in\mathbb{F}_q\setminus S_f} \chi(h(\alpha)).
\end{aligned}$$

onde $h(x) = x^{n_1} f_1(x)^{n_2} f_2(x)^{-n_2}$. Para encontrar um limite para $N_f(l_1, l_2)$, vincularemos o somatório acima de acordo com os valores de d_1 e d_2. Consideraremos três casos:

1. Primeiramente consideraremos o caso em que $d_1 = d_2 = 1$, implicando que $n_1 = n_2 = 0$ e, portanto, $h(x) = x^0 f_1(x)^0 f_2(x)^0 = 1$, ou seja, $h = 1$, assim

$$\tilde{\chi}(\chi_1, \chi_2) = \sum_{\alpha \in \mathbb{F}_q \setminus S_f} 1 = \sharp(\mathbb{F}_q \setminus S_f) \geq q - (m_1 + m_2 + 1) \tag{2.3}$$

uma vez que $\partial(f_1) \leq m_1$, $\partial(f_2) \leq m_2$.

2. Consideramos agora o caso em que $d_1 \neq 1$ e $d_2 = 1$, implicando que $n_2 = 0$ e, portanto, $h(\alpha) = \alpha^{n_1} f_1(\alpha)^0 f_2(\alpha)^0 = \alpha^{n_1}$. Note que do Teorema 34 tem-se

$$\sum_{\alpha \in \mathbb{F}_q^*} \chi(\alpha^{n_1}) = \sum_{\alpha \in \mathbb{F}_q^*} \chi_1(\alpha) = 0$$

portanto,

$$\begin{aligned} |\tilde{\chi}(\chi_1, \chi_2)| = \left| \sum_{\alpha \in \mathbb{F}_q \setminus S_f} \chi(h(\alpha)) \right| &= \left| \sum_{\alpha \in \mathbb{F}_q \setminus S_f} \chi(\alpha^{n_1}) \right| \\ &= \left| \sum_{\alpha \in \mathbb{F}_q^*} \chi(\alpha^{n_1}) - \sum_{\alpha \in S_f \setminus \{0\}} \chi(\alpha^{n_1}) \right| \\ &= \left| \sum_{\alpha \in S_f \setminus \{0\}} \chi(\alpha^{n_1}) \right| \\ &\leq (m_1 + m_2) < (m_1 + m_2)\sqrt{q} \end{aligned} \tag{2.4}$$

e assim obtemos que $|\tilde{\chi}(\chi_1, \chi_2)| \leq (m_1 + m_2)\sqrt{q}$.

3. Por fim, consideramos o caso em que $d_2 \neq 1$, assim $n_2 \neq 0$. Utilizaremos o Lema 52, mas primeiro mostraremos que de fato o podemos fazer.

   Assuma por absurdo que $h(x) = \left(\frac{g_1(x)}{g_2(x)}\right)^{q-1}$ para algum $g_1(x), g_2(x) \in \mathbb{F}[x]$ tal que $\partial(g_1) = r_1, \partial(g_2) = r_2$, e $(g_1, g_2) = 1$, então

$$x_1^{n_1} f_1(x)^{n_2} g_2(x)^{q-1} = f_2(x)^{n_2} g_1(x)^{q-1}$$

   já que $h(x) = x^{n_1} f_1(x)^{n_2} f_2(x)^{-n_2}$.

   Uma vez que $\frac{f_1(x)}{f_2(x)} \in \Upsilon_q(m_1, m_2)$, existe um polinômio irredutível $t(x) \in \mathbb{F}_q[x]$ onde $t(x) \neq x$ e um inteiro positivo n com $(n, q-1) = 1$ tal que $t(x)^n$ aparece na fatoração de $f_1(x)$ ou $f_2(x)$, visto que $\Lambda_q(f_1, f_2) \neq \emptyset$. Suponha que $t(x)^n$ aparece na fatoração de $f_2(x)$ e seja $\tilde{t}(x)$ um fator irredutível de $t(x)$ em $\mathbb{F}[x]$, onde $\mathbb{F}$ é o fecho algébrico de $\mathbb{F}_q$. Note que $\tilde{t}(x)$ possui grau 1, uma vez que $\mathbb{F}_q$ é um corpo perfeito, nisso $\tilde{t}(x)$ aparece com multiplicidade 1 na fatoração de $t(x)$ em $\mathbb{F}[x]$.

   Lembremos que um corpo perfeito é um corpo em que todo polinômio é separável e um polinômio $p(x)$ em um corpo qualquer K é dito separável se todos os seus fatores irredutíveis tem apenas raízes simples.

   Uma vez que $f_1(x), f_2(x)$ são coprimos em $\mathbb{F}_q[x]$, da Proposição 27 eles também são coprimos em $\mathbb{F}[x]$, assim $\tilde{t}(x)^{nn_2}$ aparece na fatoração de $g_2(x)^{q-1}$ uma vez que $\tilde{t}(x)^n$ aparece na fatoração de $f_2(x)$ em $\mathbb{F}[x]$ e

$$x_1^{n_1} f_1(x)^{n_2} g_2(x)^{q-1} = f_2(x)^{n_2} g_1(x)^{q-1}.$$

Note que $\tilde{t}$ aparece exatamente nn_2 vezes na fatoração de $g_2(x)^{q-1}$ e considere m o número de vezes que $\tilde{t}$ aparece na fatoração de $g_2(x)$, logo $m(q-1) = nn_2$. Disso podemos concluir que $q-1 \mid nn_2$ e como $\mathrm{mdc}(n, q-1) = 1$ obtemos que $q-1 \mid n_2$ o que nos leva a uma contradição, uma vez que $n_2 \leq q-2$.

Assim devemos ter que $t(x)^n$ aparece na fatoração de $f_1(x)$. Analogamente, se conclui que $q-1|n_2$, o que é impossível.

Portanto, se $d_2 \neq 1$ e $n_2 \neq 0$ obtemos que $h(x)$ não é da forma $g(x)^{q-1}$ em $\mathbb{F}[x]$ e assim estamos aptos a utilizar o Lema 52.

Seja

$$T_h := \{\beta \in \mathbb{F}_q : h(\beta) = 0 \text{ ou } h(\beta) \text{ não está bem definida}\}.$$

Se $0 \in T_h$ então $T_h = S_f$. Do Lema 52 temos

$$\begin{aligned} |\tilde{\chi}(\chi_1, \chi_2)| = \left|\sum_{\alpha \in \mathbb{F}_q \setminus S_f} \chi(h(\alpha))\right| &= \left|\sum_{\alpha \in \mathbb{F}_q \setminus T_h} \chi(h(\alpha))\right| \\ &\leq (m_1 + m_2 + 1 - 1)\sqrt{q} \\ &\leq (m_1 + m_2)\sqrt{q}. \end{aligned} \tag{2.5}$$

Se $0 \notin T_h$ então $h(0) \neq 0$ e como $h(x) = x^{n_1} f_1(x)^{n_2} f_2(x)^{-n_2}$, tem-se $n_1 = 0$ e $h(x) = f_1(x)^{n_2} f_2(x)^{-n_2}$. Portanto,

$$\begin{aligned} |\tilde{\chi}(\chi_1, \chi_2)| = \left|\sum_{\alpha \in \mathbb{F}_q \setminus S_f} \chi(h(\alpha))\right| &= \left|\sum_{\alpha \in \mathbb{F}_q \setminus T_h} \chi(h(\alpha)) - \chi(h(0))\right| \\ &\leq \left|\sum_{\alpha \in \mathbb{F}_q \setminus T_h} \chi(h(\alpha))\right| + |1| \\ &\leq (m_1 + m_2 - 1)\sqrt{q} + 1 \\ &\leq (m_1 + m_2)\sqrt{q}. \end{aligned} \tag{2.6}$$

Note que aplicamos o Lema 52 na segunda desigualdade acima e de toda forma obtemos $|\tilde{\chi}(\chi_1, \chi_2)| \leq (m_1 + m_2)\sqrt{q}$.

Agora utilizaremos as estimativas acima para limitar $N_f(l_1, l_2)$. De (2.2), (2.3), (2.4), (2.5) e (2.6) obtemos

$$N_f(l_1, l_2) = \theta(l_1)\theta(l_2) \sum_{\substack{d_1 | l_1 \\ d_2 | l_2}} \frac{\mu(d_1)}{\phi(d_1)} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\substack{ord(\chi_1) = d_1 \\ ord(\chi_2) = d_2}} \tilde{\chi}(\chi_1, \chi_2)$$

$$\geq \theta(l_1)\theta(l_2) \left(q - (m_1 + m_2 + 1) + \sum_{\substack{d_1 | l_1, d_2 | l_2 \\ (d_1, d_2) \neq (1,1)}} \frac{\mu(d_1)}{\phi(d_1)} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\substack{ord(\chi_1) = d_1 \\ ord(\chi_2) = d_2}} \tilde{\chi}(\chi_1, \chi_2) \right).$$

Aqui usaremos o fato de que há $\phi(d_1)$ caracteres de ordem d_1 e $\phi(d_2)$ caracteres de ordem d_2, logo temos $\phi(d_1)\phi(d_2)$ pares de tais caracteres. Assim

$$
\begin{aligned}
N_f(l_1,l_2) &\geq \theta(l_1)\theta(l_2)\left(q-(m_1+m_2+1)+\sum_{\substack{d_1|l_1,d_2|l_2\\(d_1,d_2)\neq(1,1)}}\mu(d_1)\mu(d_2)\tilde{\chi}(\chi_1,\chi_2)\right)\\
&\geq \theta(l_1)\theta(l_2)\left(q-(m_1+m_2+1)-\sum_{\substack{d_1|l_1,d_2|l_2\\(d_1,d_2)\neq(1,1)}}|\mu(d_1)||\mu(d_2)|\tilde{\chi}(\chi_1,\chi_2)|\right)\\
&\geq \theta(l_1)\theta(l_2)\left(q-(m_1+m_2+1)-\sum_{\substack{d_1|l_1,d_2|l_2\\(d_1,d_2)\neq(1,1)}}|\mu(d_1)||\mu(d_2)|(m_1+m_2)q^{\frac{1}{2}}\right)\\
&\geq \theta(l_1)\theta(l_2)\left(q-(m_1+m_2+1)-(m_1+m_2)q^{\frac{1}{2}}\sum_{\substack{d_1|l_1,d_2|l_2\\(d_1,d_2)\neq(1,1)}}|\mu(d_1)||\mu(d_2)|\right).
\end{aligned}
$$

Note que a última soma é igual ao número de pares $(d_1,d_2)\neq(1,1)$ tais que $d_1|l_1$ e $d_2|l_2$ com d_1 e d_2 livre de quadrados, uma vez que a função de Möbius retorna 0 nesses casos. Assim temos

$$\sum_{\substack{d_1|l_1,d_2|l_2\\(d_1,d_2)\neq(1,1)}}|\mu(d_1)||\mu(d_2)|= W(l_1)W(l_2)-1$$

e, portanto, podemos concluir que

$$N_f(l_1,l_2)\geq\theta(l_1)\theta(l_2)[q-(m_1+m_2+1)-(m_1+m_2)q^{\frac{1}{2}}(W(l_1)W(l_2)-1)]. \quad (2.7)$$

Assim, se $q>(m_1+m_2+1)+(m_1+m_2)q^{\frac{1}{2}}(W(l_1)W(l_2)-1)$, então $N_f(l_1,l_2)>0$, uma vez que $\theta(l_1)\theta(l_2)>0$.

Escrevendo

$$
\begin{aligned}
&(m_1+m_2+1)+(m_1+m_2)q^{\frac{1}{2}}(W(l_1)W(l_2)-1)=\\
&\qquad (m_1+m_2)q^{\frac{1}{2}}W(l_1)W(l_2)-q^{\frac{1}{2}}\left((m_1+m_2)-q^{-\frac{1}{2}}(m_1+m_2+1)\right)
\end{aligned}
$$

e observando que

$$
\begin{aligned}
(m_1+m_2)-q^{-\frac{1}{2}}(m_1+m_2+1)\geq 0 &\iff m_1+m_2\geq\frac{(m_1+m_2+1)}{\sqrt{q}}\\
&\iff \frac{m_1\sqrt{q}+m_2\sqrt{q}-m_1-m_2-1}{\sqrt{q}}\geq 0\\
&\iff \frac{m_1(\sqrt{q}-1)+m_2(\sqrt{q}-1)-1}{\sqrt{q}}\geq 0\\
&\iff (m_1+m_2)(\sqrt{q}-1)\geq 1,
\end{aligned}
$$

temos que para um q fixado, o menor valor a esquerda ocorre quando $m_1+m_2=1$ e assim devemos ter $q\geq 4$. Portanto, se $q\geq 4$ temos $(m_1+m_2)q^{\frac{1}{2}}-(m_1+m_2+1)\geq 0$

e assim resta que $q - q^{\frac{1}{2}}(m_1+m_2)W(l_1)W(l_2) > 0$. Mas isso é dado pela hipótese, note que

$$\begin{aligned} q - q^{\frac{1}{2}}(m_1+m_2)W(l_1)W(l_2) > 0 &\iff q^{\frac{1}{2}}(q^{\frac{1}{2}} - (m_1+m_2)W(l_1)W(l_2)) > 0 \\ &\iff q^{\frac{1}{2}} > (m_1+m_2)W(l_1)W(l_2) \end{aligned}$$

e, portanto, $N_f(l_1, l_2) > 0$.

■

Corolário 55. Se $q = p^k \geq 4$ e $q^{\frac{1}{2}} \geq (m_1+m_2)[W(q-1)]^2$ então $k \in \Gamma_p(m_1, m_2)$. Em outras palavras, para toda $f = \frac{f_1}{f_2} \in \Upsilon_q(m_1, m_2)$ com q satisfazendo as hipóteses acima, existe um elemento $\alpha \in \mathbb{F}_q^*$ tal que $(\alpha, f(\alpha))$ é um par primitivo.

Lema 56. Seja l um divisor de $q-1$ e seja $\{p_1, \cdots, p_r\}$ o conjunto de todos os divisores primos de $q-1$ mas que não dividem l. Então

$$N_f(q-1, q-1) \geq \sum_{i=1}^{r} N_f(p_i l, l) + \sum_{i=1}^{r} N_f(l, p_i l) - (2r-1)N_f(l, l). \tag{2.8}$$

Prova. Observe que $N_f(q-1, q-1)$ conta os elementos $\alpha \in \mathbb{F}_q$ para os quais α e $f(\alpha)$ são primitivos, $(q-1)$-livres e consequentemente $p_i l$-livres, uma vez que $p_i l \mid q-1$ e da mesma forma são l-livres pois $l \mid p_i l$. Portanto, o par $(\alpha, f(\alpha)$ é contado $r + r - (2r-1) = 1$ vez do lado direito da equação. Portanto, se $(\alpha, f(\alpha))$ é um par de elementos primitivos em $\mathbb{F}_q^2$ vale a desigualdade. Por outro lado, seja $\alpha \in \mathbb{F}_q$ tal que α ou $f(\alpha)$ não é primitivo, do Lema 44, temos que α ou $f(\alpha)$ não é $p_i l$-livre para algum $i \in \{1, \cdots, r\}$, então note que o lado direito será contado no máximo $r + (r-1) - (2r-1) = 0$ vezes e, portanto, segue o resultado.

■

Lema 57. Seja l um divisor de $q-1$ e seja $\{p_1, \cdots, p_r\}$ o conjunto de todos os divisores primos de $q-1$ mas que não dividem l. Suponha que $\delta = 1 - 2\sum_{i=1}^{r} \frac{1}{p_i} > 0$ e seja $\Delta = \frac{2r-1}{\delta} + 2$. Se $q^{\frac{1}{2}} \geq (m_1+m_2)W(l)^2\Delta$, então $k \in \Gamma_p(m_1, m_2)$.

Prova. Podemos escrever o lado direito de (2.8) como

$$\begin{aligned} N_f(q-1, q-1) \geq &\sum_{i=1}^{r} (N_f(p_i l, l) - \theta(p_i)N_f(l, l)) \\ &+ \sum_{i=1}^{r} (N_f(l, p_i l) - \theta(p_i)N_f(l, l)) + \delta N_f(l, l). \end{aligned} \tag{2.9}$$

De fato, lembre-se que

$$\theta(p_i) = \frac{\phi(p_i)}{p_i} = \prod_{p \mid p_i} \left(1 - \frac{1}{p}\right) = 1 - \frac{1}{p_i} \text{ para todo } i \in \{1, \cdots, r\}.$$

Assim, desenvolvendo o lado direito de (2.9) temos

$$\begin{aligned}
& \sum_{i=1}^{r}(N_f(p_il,l)-\theta(p_i)N_f(l,l))+\sum_{i=1}^{r}(N_f(l,p_il)-\theta(p_i)N_f(l,l))+\delta N_f(l,l)\\
= & \sum_{i=1}^{r}N_f(p_il,l)+\sum_{i=1}^{r}N_f(l,p_il)-2\sum_{i=1}^{r}\theta(p_i)N_f(l,l)+\delta N_f(l,l)\\
= & \sum_{i=1}^{r}N_f(p_il,l)+\sum_{i=1}^{r}N_f(l,p_il)-2\left[\sum_{i=1}^{r}\left(1-\frac{1}{p_i}\right)\right]N_f(l,l)+\delta N_f(l,l)\\
= & \sum_{i=1}^{r}N_f(p_il,l)+\sum_{i=1}^{r}N_f(l,p_il)-2rN_f(l,l)+2\sum_{i=1}^{r}\frac{1}{p_i}N_f(l,l)+\delta N_f(l,l)\\
= & \sum_{i=1}^{r}N_f(p_il,l)+\sum_{i=1}^{r}N_f(l,p_il)+\left[-2r+2\sum_{i=1}^{r}\frac{1}{p_i}+\delta\right]N_f(l,l)\\
= & \sum_{i=1}^{r}N_f(p_il,l)+\sum_{i=1}^{r}N_f(l,p_il)+\left[-2r+2\sum_{i=1}^{r}\frac{1}{p_i}+1-2\sum_{i=1}^{r}\frac{1}{p_i}\right]N_f(l,l)\\
= & \sum_{i=1}^{r}N_f(p_il,l)+\sum_{i=1}^{r}N_f(l,p_il)-(2r-1)N_f(l,l)
\end{aligned}$$

e, portanto, vale (2.9). Uma vez que

$$\theta(p_il)=\frac{\phi(p_il)}{p_il}=\frac{\phi(p_i)\phi(l)}{p_il}=\theta(p_i)\theta(l) \text{ para todo } i\in\{1,\cdots,r\},$$

da Equação (2.2) obtemos

$$N_f(p_il,l)=\theta(p_i)\theta(l)^2\sum_{\substack{d_1|p_il\\ d_2|l}}\frac{\mu(d_1)}{\phi(d_1)}\frac{\mu(d_2)}{\phi(d_2)}\sum_{\substack{ord(\chi_1)=d_1\\ ord(\chi_2)=d_2}}\tilde{\chi}(\chi_1,\chi_2)$$

para todo i.

Iremos subdividir o conjunto dos d_1's em dois subconjuntos da seguinte maneira: O primeiro subconjunto conterá aqueles que não possuem p_i como um fator, enquanto que o segundo conterá aqueles que são múltiplos de p_i. Isso dividirá o primeiro somatório em duas somas, e assim obtemos

$$\begin{aligned}
N_f(p_il,l)=&\,\theta(p_i)\theta(l)^2\sum_{d_1|l,d_2|l}\frac{\mu(d_1)}{\phi(d_1)}\frac{\mu(d_2)}{\phi(d_2)}\sum_{\substack{ord(\chi_1)=d_1\\ ord(\chi_2)=d_2}}\tilde{\chi}(\chi_1,\chi_2)\\
&+\theta(p_i)\theta(l)^2\sum_{p_i|d_1,d_1|p_il,d_2|l}\frac{\mu(d_1)}{\phi(d_1)}\frac{\mu(d_2)}{\phi(d_2)}\sum_{\substack{ord(\chi_1)=d_1\\ ord(\chi_2)=d_2}}\tilde{\chi}(\chi_1,\chi_2).
\end{aligned}$$

E como

$$N_f(l,l)=\theta(l)^2\sum_{d_1|l,d_2|l}\frac{\mu(d_1)}{\phi(d_1)}\frac{\mu(d_2)}{\phi(d_2)}\sum_{\substack{ord(\chi_1)=d_1\\ ord(\chi_2)=d_2}}\tilde{\chi}(\chi_1,\chi_2),$$

segue que

$$\begin{aligned} N_f(p_il,l)-\theta(p_i)N_f(l,l) &= \theta(p_i)\theta(l)^2 \sum_{p_i|d_1,d_1|p_il,d_2|l} \frac{\mu(d_1)}{\phi(d_1)}\frac{\mu(d_2)}{\phi(d_2)} \sum_{\substack{ord(\chi_1)=d_1\\ord(\chi_2)=d_2}} \tilde{\chi}(\chi_1,\chi_2) \\ &= \theta(p_i)\theta(l)^2 \sum_{p_i|d_1,d_1|p_il,d_2|l} \mu(d_1)\mu(d_2)\tilde{\chi}(\chi_1,\chi_2) \\ &\Downarrow \\ |N_f(p_il,l)-\theta(p_i)N_f(l,l)| &\leq \theta(p_i)\theta(l)^2 \sum_{p_i|d_1,d_1|p_il,d_2|l} |\mu(d_1)\mu(d_2)||\tilde{\chi}(\chi_1,\chi_2)|. \end{aligned}$$

Observe também que dos Casos 2 e 3 na prova do Teorema 54 que $|\tilde{\chi}(\chi_1,\chi_2)|\leq (m_1+m_2)\sqrt{q}$ e, além disso,

$$\sum_{p_i|d_1,d_1|p_il,d_2|l} |\mu(d_1)||\mu(d_2)|= W(l)^2,$$

logo podemos concluir que

$$|N_f(p_il,l)-\theta(p_i)N_f(l,l)|\leq (m_1+m_2)\theta(p_i)\theta(l)^2W(l)^2q^{\frac{1}{2}}.$$

Analogamente, podemos concluir que

$$|N_f(l,p_il)-\theta(p_i)N_f(l,l)|\leq (m_1+m_2)\theta(p_i)\theta(l)^2W(l)^2q^{\frac{1}{2}}$$

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

Substituindo esses resultados na Inequação (2.9), obtemos

$$\begin{aligned} N_f(q-1,q-1) &\geq -2\sum_{i=1}^{r}|N_f(p_il,l)-\theta(p_i)N_f(l,l)|+\delta N_f(l,l) \\ &\geq -2\sum_{i=1}^{r}(m_1+m_2)\theta(p_i)\theta(l)^2W(l)^2q^{\frac{1}{2}}+\delta N_f(l,l) \\ &\geq \delta N_f(l,l)-2(m_1+m_2)\theta(l)^2W(l)^2q^{\frac{1}{2}}\sum_{i=1}^{r}\theta(p_i). \end{aligned}$$

Como

$$\sum_{i=1}^{r}\theta(p_i)=\sum_{i=1}^{r}\left(1-\frac{1}{p_i}\right)=r-\sum_{i=1}^{r}\frac{1}{p_i}=r+\frac{\delta-1}{2}=\frac{\delta}{2}\left[\frac{2r-1}{\delta}+1\right]=\frac{\delta}{2}(\Delta-1)$$

uma vez que $\Delta=\frac{2r-1}{\delta}+2$, obtemos

$$N_f(q-1,q-1)\geq \delta N_f(l,l)-(m_1+m_2)\delta(\Delta-1)\theta(l)^2W(l)^2q^{\frac{1}{2}}. \tag{2.10}$$

Da Inequação (2.7) sabemos que

$$N_f(l,l)>\theta(l)^2\left(q-(m_1+m_2+1)-(m_1+m_2)q^{\frac{1}{2}}(W(l)^2-1)\right). \tag{2.11}$$

Substituindo (2.11) em (2.10) obtemos

$$\begin{aligned} N_f(q-1,q-1)\geq{}& \delta\theta(l)^2[(q-(m_1+m_2+1) \\ &-(m_1+m_2)q^{\frac{1}{2}}(W(l)^2-1))]-(m_1+m_2)\delta(\Delta-1)\theta(l)^2W(l)^2q^{\frac{1}{2}} \end{aligned}$$

$$
\begin{aligned}
&\geq \delta\theta(l)^2[(q-(m_1+m_2+1)-(m_1+m_2)q^{\frac{1}{2}}(W(l)^2-1))-(m_1+m_2)q^{\frac{1}{2}}(\Delta-1)W(l)^2] \\
&\geq \delta\theta(l)^2[(q-(m_1+m_2+1)-(m_1+m_2)q^{\frac{1}{2}}((W(l)^2-1)+(\Delta-1)W(l)^2)] \\
&\geq \delta\theta(l)^2[(q-(m_1+m_2+1)-(m_1+m_2)q^{\frac{1}{2}}(W(l)^2(1+(\Delta-1))-1] \\
&\geq \delta\theta(l)^2[(q-(m_1+m_2+1)-(m_1+m_2)q^{\frac{1}{2}}[W(l)^2\Delta-1] \\
&\geq \delta\theta(l)^2[(q-(m_1+m_2+1)+(m_1+m_2)q^{\frac{1}{2}}-(m_1+m_2)q^{\frac{1}{2}}\Delta W(l)^2].
\end{aligned}
$$

Portanto,

$$N_f(q-1,q-1) \geq \delta\theta(l)^2[(q-(m_1+m_2+1)+(m_1+m_2)q^{\frac{1}{2}}-(m_1+m_2)q^{\frac{1}{2}}\Delta W(l)^2]. \quad (2.12)$$

Como $\delta > 0$ e $(m_1+m_2)q^{\frac{1}{2}} - (m_1+m_2+1) > 0$, segue que se $q^{\frac{1}{2}} \geq (m_1+m_2)W(l)^2\Delta$, então $N_f(q-1,q-1) > 0$ e, portanto, $k \in \Gamma_p(m_1,m_2)$.

■

Observação 58. O resultado apresentado acima é um método de crivo [18].

Proposição 59. Se $\phi(q-1) \leq m_1+m_2+1$, então $k \notin \Gamma_p(m_1,m_2)$.

Prova. Seja $\{\alpha_1,\cdots,\alpha_{\phi(q-1)}\}$ o conjunto de todos os elementos primitivos de $\mathbb{F}_q$. Note que se $\phi(q-1) \leq m_1+m_2+1$, podemos escolher polinômios $f_1(x), f_2(x)$ tais que $\partial f_1 \leq m_1$ e $\partial f_2 \leq m_2$ de forma que $f_1(\alpha_j)f_2(\alpha_j) = 0$, para todo $j \in \{1,\cdots,\phi(q-1)-1\}$, $f_1(\alpha_{\phi(q-1)}), f_2(\alpha_{\phi(q-1)}) \neq 0$ com $f = \frac{f_1}{f_2} \in \Upsilon_q(m_1,m_2)$. Suponha que $\phi(q-1) \leq m_1+m_2+1$ e tome

$$
\begin{aligned}
f_1(x) &= (x-\alpha_1)\cdots(x-\alpha_l),\ l \leq m_1 \\
f_2(x) &= (x-\alpha_{l+1})\cdots(x-\alpha_v),\ v \leq m_2,\ l+v \leq \phi(q-1)-1.
\end{aligned}
$$

Assim $(\alpha_j, f(\alpha_j))$ não é um par primitivo para todo $j \in \{1,\cdots,\phi(q-1)-1\}$. Tomando $\beta = \frac{1}{f(\alpha_{\phi(q-1)})}$, temos $h(x) = \beta f(x) \in \Upsilon_q(m_1,m_2)$ e $(\alpha_{\phi(q-1)}, h(\alpha_{\phi(q-1)}) = (\alpha_{\phi(q-1)}, 1)$ também não é um par de elementos primitivos. Assim, $(\alpha, h(\alpha_i))$ não é um par de elementos primitivos para todo $i \in \{1,\cdots,\phi(q-1)\}$. Portanto, $k \notin \Gamma_p(m_1,m_2)$.

■

Quando $p = 2$, podemos usar os seguintes resultados para obter informações sobre o conjunto $\Gamma_2(m_1,m_2)$.

Proposição 60. Sejam $m = max\{m_1,m_2\}$ e $k > 1$. Se 2^k-1 é um número primo e $2^k-2 > m_1+m_2+m$, então $k \in \Gamma_2(m_1,m_2)$.

Prova. Assuma que 2^k-1 é primo, então temos um total de $\phi(2^k-1) = 2^k-2$ elementos primitivos em $\mathbb{F}_{2^k}$, uma vez que todo $\alpha \in \mathbb{F}_{2^k}^* \setminus \{1\}$ é primitivo. Seja $f(x) = \frac{f_1(x)}{f_2(x)} \in \Upsilon_{2^k}(m_1,m_2)$ e assuma que $2^k-2 > m_1+m_2+m$. Uma vez que $f_1(x)$ e $f_2(x)$ tem no máximo m_1 e m_2 raízes respectivamente (note que todas distintas, uma vez que $(f_1,f_2) = 1$) e $f_1(x)-f_2(x)$ tem no máximo m raízes, onde $m = max\{m_1,m_2\}$, então existe $\alpha \in \mathbb{F}_{2^k}$ tal que $f_1(\alpha) \neq 0$, $f_2(\alpha) \neq 0$ e $f_1(\alpha)-f_2(\alpha) \neq 0$ donde obtemos $f_1(\alpha) \neq f_2(\alpha)$. Assim, $f(\alpha) = \frac{f_1(\alpha)}{f_2(\alpha)} \in \mathbb{F}_{2^k}^* \setminus \{1\}$, ou seja, $f(\alpha)$ é primitivo. Portanto, para toda $f(x) \in \Upsilon_{2^k}(m_1,m_2)$ existe um $\alpha \in \mathbb{F}_{2^k}$ primitivo tal que $(\alpha, f(\alpha))$ é um par primitivo, ou seja, $k \in \Gamma_2(m_1,m_2)$.

■

Proposição 61. Seja $q = 2^k$ e $m = max\{m_1, m_2\}$. Se

$$\phi(q-1) + \frac{1}{m}\phi(q-1) > q$$

então $k \in \Gamma_2(m_1, m_2)$.

Prova. Seja $f(x) = \frac{f_1(x)}{f_2(x)} \in \Upsilon_q(m_1, m_2)$ e defina

$$A_f = \{\alpha \in \mathbb{F}_q^* : \alpha \text{ é primitivo e } f_2(\alpha) \neq 0\}.$$

Considere a função $f : A_f \to \mathbb{F}_q$ dada por $\alpha \mapsto f(\alpha)$. Seja $B_f = Im(f)$. Dado $\beta \in B_f$, observe que

$$\begin{aligned} & f(x) = \beta \\ \Rightarrow \quad & \frac{f_1(x)}{f_2(x)} = \beta \\ \Rightarrow \quad & f_1(x) = \beta f_2(x) \\ \Rightarrow \quad & f_1(x) - \beta f_2(x) = 0. \end{aligned}$$

Assim existem no máximo m elementos $\alpha \in A_f$ tais que $f(\alpha) = \beta$ uma vez que α deve ser raiz do polinômio $f_1(x) - \beta f_2(x)$. Note que $|A_f| \geq \phi(q-1) - m$, o que implica $|B_f| \geq \frac{\phi(q-1)-m}{m}$, uma vez que, para cada elemento da imagem, existem no máximo m pré-imagens. Assim, se

$$\phi(q-1) + \frac{\phi(q-1) - m}{m} > q - 1$$

então existe pelo menos um elemento na interseção dos conjuntos dos elementos primitivos e B_f, ou seja, existe pelo menos um elemento de B_f, digamos $f(\alpha)$, que é primitivo e, portanto, $(\alpha, f(\alpha))$ é um par primitivo e $k \in \Gamma_2(m_1, m_2)$.

■

O resultado acima não pode ser estendido ao caso onde p é primo ímpar, uma vez que nesse caso tem-se $q-1$ par e consequentemente $\phi(q-1) + \frac{1}{m}\phi(q-1) < q$ para todo $m \geq 1$. De fato, considerando $m = 1$ o lado direito esquerdo da inequação atinge seu máximo, e assim tem-se

$$\begin{aligned} 2 \cdot \phi(q-1) &= 2 \cdot (q-1) \prod_{p_i | q-1} \left(1 - \frac{1}{p_i}\right) \\ &= 2(q-1)\left(1 - \frac{1}{2}\right) \prod_{\substack{p_i | q-1 \\ p_i \neq 2}} \left(1 - \frac{1}{p_i}\right) \\ &= (q-1) \underbrace{\prod_{\substack{p_i | q-1 \\ p_i \neq 2}} \left(1 - \frac{1}{p_i}\right)}_{\leq 1} \\ &< q. \end{aligned}$$

Proposição 62. Sejam p primo, $q = p^k, m_1, m_2$ inteiros positivos, $t > 4$ um número real positivo e

$$A_t = \prod_{\substack{s \text{ primo} \\ s \leq 2^t}} \frac{2}{\sqrt[t]{s}}.$$

Se $q \geq ((m_1 + m_2) \cdot A_t^2)^{\frac{2t}{t-4}}$ então $k \in \Gamma_p(m_1, m_2)$.

Prova. Note inicialmente que

$$\begin{aligned} q \geq \left((m_1 + m_2) \cdot A_t^2\right)^{\frac{2t}{t-4}} &\iff q^{\frac{t-4}{2t}} \geq (m_1 + m_2) \cdot A_t^2 \\ &\iff q^{\frac{t-4}{2t}} q^{\frac{2}{t}} \geq \left((m_1 + m_2) \cdot A_t^2\right) q^{\frac{2}{t}} \iff q^{\frac{1}{2}} \overset{*}{\geq} (m_1 + m_2) \cdot (A_t \cdot q^{\frac{1}{t}})^2 \end{aligned}$$

Seja $q - 1 = p_1^{\alpha_1} \cdots p_l^{\alpha_l}$ decomposto em fatores primos distintos. Então $W(q-1) = 2^l$. Se $p > 2^t$, então $\frac{2}{\sqrt[t]{p}} < 1$ e assim obtemos

$$\begin{aligned} &\frac{W(q-1)}{q^{\frac{1}{t}}} < \frac{W(q-1)}{(q-1)^{\frac{1}{t}}} = \frac{2^l}{(p_1^{\alpha_1} \cdots p_l^{\alpha_l})^{\frac{1}{t}}} = \frac{2^l}{p_1^{\frac{\alpha_1}{t}} \cdots p_l^{\frac{\alpha_l}{t}}} = \frac{2^l}{\sqrt[t]{p_1^{\alpha_1}} \cdots \sqrt[t]{p_l^{\alpha_l}}} \\ \Rightarrow \quad &\frac{W(q-1)}{q^{\frac{1}{t}}} < \frac{2^l}{\sqrt[t]{p_1} \cdots \sqrt[t]{p_l}} \leq \prod_{\substack{2 \leq p_i \leq 2^t \\ 1 \leq i \leq l}} \frac{2}{\sqrt[t]{p_i}} \leq A_t. \end{aligned}$$

Assim temos $A_t \cdot q^{\frac{1}{t}} > W(q-1)$. Substituindo essa informação em $*$ obtemos $q^{\frac{1}{2}} \geq (m_1 + m_2) \cdot W(q-1)^2$. Do Corolário 55 obtemos $k \in \Gamma_p(m_1, m_2)$.

■

Observação 63. Para exemplificar o resultado acima, tomemos, por exemplo, $t = 6$ e obtemos para qualquer primo p, que:

1. Se $q = p^k \geq 5.6 \times 10^{21}$ então $k \in \Gamma_p(2, 1)$.
2. Se $q = p^k \geq 3.2 \times 10^{22}$ então $k \in \Gamma_p(2, 2)$.
3. Se $q = p^k \geq 1.2 \times 10^{23}$ então $k \in \Gamma_p(3, 2)$.

Para que esses resultados sejam facilmente verificados, desenvolvemos uma série de algoritmos no sistema GAP que nos auxiliará não só nesta observação como em outros resultados que veremos a seguir.

Algoritmo 1: Recebe como entrada os valores referentes a t na Proposição 62 e m_1, m_2 referente ao conjunto $\Gamma_p(m_1, m_2)$ e devolve um valor na qual q precisa superar de tal forma que $k \in \Gamma_p(m_1, m_2)$.

```
1  Proposicao58q := function(t,m1,m2)
2  local A, aux1, aux2, P, D, q;
3  aux1:= Filtered([1,2..2^t-1],IsPrime);
4  aux2:= Size(aux1);
5  P:= Product(aux1);
6  D:= Float(1/t);
7  A:= 2^(aux2) / P^D;
8  q:= ((m1 + m2)*A^2)^((2*t)/(t-4));
9  return q;
10 end;
```

Algoritmo 2: Retorna o valor de k referente ao valor de $q = p^k$ do algoritmo anterior.

```
1  Proposicao58k := function(t,p,m1,m2)
2  local q, k;
3  k:= 1;
4  q:= Proposicao58q(t,m1,m2);;
5  while Float(q) >= Float(p^(k)) do
6  |  k:= k+1;
7  end
8  return k;
9  end;
```

Algoritmo 3: Aplicação do Corolário 55 onde as entradas são respectivamente o valor máximo que k que será testado e $p, m1, m2$ os valores de $\Gamma_p(m_1, m_2)$. O algoritmo retorna o conjunto composto pelos $k's$ tais que $k \in \Gamma_p(m_1, m_2)$.

```
1  Corolario52:= function(k,p,m1,m2)
2  local A, q, u, aux1, aux2, w, W;
3  A:=[];
4  for i in [4,5..k] do
5  |  q:= p^(i);
6  |  u:= PrimeDivisors(q-1);
7  |  w:= Size(u);
8  |  W:= 2^(w);
9  |  aux1:= p^(Float(i/2));
10 |  aux2:= Float((m1 + m2) * W^(2));
11 |  if  aux1 > aux2 then
12 |  |  AddSet(A,i);
13 |  end
14 end
15 return A;
16 end;
```

Os próximos três algoritmos juntos tratam do Lema 57.

Algoritmo 4: Retorna o conjunto $\{p_1, \cdots, p_r\}$ referente ao lema e as entradas (p, k, l) são referentes a $q = p^k$ e l um divisor de $q - 1$.

```
1  Lema541:= function(p,k,l)
2  local q, A, B, C1;
3  A:=[];
4  q:= p^(k);
5  C1:= [];
6  B:= DivisorsInt(l);
7  A:= PrimeDivisors(q-1);
8  for i in [1..Size(A)] do
9  |  AddSet(C1, A[i]);
10 end
11 for i in [1..Size(A)] do
12 |  if (A[i] in B) = true then
13 |  |  RemoveSet(C1,A[i]);
14 |  end
15 end
16 return C1;
17 end;
```

Algoritmo 5: Testa se o Lema 57 é verdadeiro ou falso dados valores específicos para $\{p, k, l, m1, m2\}$.

```
1  Lema542 := function(p,k,l,m1,m2)
2  local q, d, D, A, a, aux, W, w, u;
3  q:= p^k;
4  aux:= 0;
5  A:= Lema541(p,k,l);
6  for i in [1..Size(A)] do
7  |  aux:= aux + (1/A[i]);
8  end
9  u:= PrimeDivisors(l);
10 w:= Size(u);
11 W:= 2^w;
12 d:= 1 - 2*aux;
13 if (d <= 0) then
14 |  return false;
15 end
16 D:= (2*Size(A) - 1)/d + 2;
17 if (q^(Float(1/2)) >= Float( (m1+m2)*W^(2)*D)) then
18 |  return true;
19 else
20 |  return false;
21 end
22 end;
```

Algoritmo 6: E por fim, dado um conjunto de $k's$, digamos K, este algoritmo testa todos os divisores l e $q-1$ relacionado a cada k, e caso o Lema 57 seja verdadeiro para alguns deles, o algoritmo imprime o menor valor de l juntamente com o k correspondente. Caso não exista nenhum l que satisfaça o lema, então ele imprime um espaço vazio.

```
1  Lema54:= function(K,p,m1,m2)
2  local L, A, q, B, C, a;
3  C:= K;
4  for i in [1..Size(C)] do
5  |  a:=C[i];
6  |  q:= p^a;
7  |  L:= DivisorsInt(q-1);
8  |  B:= [];
9  |  Print(a,"\t");
10 |  for j in [1..Size(L)] do
11 |  |  if  Lema562(p,a,L[j],m1,m2) = true then
12 |  |  |  AddSet(B,L[j]);
13 |  |  end
14 |  end
15 |  if  Size(B) >= 1 then
16 |  |  Print(B[1],"\n");
17 |  else
18 |  |  Print("\n");
19 |  end
20 end
21 end;
```

2.2 Trabalhando Exemplos

Em [19] os autores definiram um conjunto de matrizes $\mathcal{M}_q$ e para cada $A \in \mathcal{M}_q$ eles associaram uma função racional $\lambda_A(x) \in \mathbb{F}_q(x)$ na qual é um quociente de polinômios de grau no máximo 2 por outro de no máximo 1. Naquele artigo, eles trabalharam sobre corpos finitos com 2^k elementos e eles queriam investigar a existência de elementos primitivos α tal que $f(\alpha)$ também fosse primitivo. Note que se $f \in \Upsilon_q(2,1)$ então existe $A \in \mathcal{M}$ tal que $f = \lambda_A$. Analogamente, se $A \in \mathcal{M}$, então $\lambda_A \in \Upsilon_q(2,1)$ a menos que $\lambda_A = x, x^2$ ou βx^{-1} para algum $\beta \in \mathbb{F}_q$. Observe que se $\alpha_A(x) = x, x^2$ ou βx^{-1} então existe $\alpha \in \mathbb{F}_q$ tal que $(\alpha, f(\alpha))$ é par primitivo. Eles também definiram um conjunto $\mathcal{B}$ de potências de 2 que satisfaz uma condição semelhante a dos elementos de $\Gamma_2(2,1)$ e obtiveram que $q = 2^k \in \mathcal{B}$ se, e somente se, $k \in \Gamma_2(2,1)$ e de [19, Teorema 2.1] obtêm-se que $\Gamma_p(2,1) = \mathbb{N} \setminus \{1,2,4\}$. Em [20] os autores definiram um conjunto de matrizes $\mathcal{N}_{2\times 3}(\mathbb{F}_q)$ de maneira similar feita em [19] com a diferença de que neste caso a função racional $\lambda_A(x)$ é um quociente de polinômios de grau 2. Eles também queriam estudar a existência de elementos primitivos α tal que $f(\alpha)$ também o seja. Pode-se ver que se $f \in \Upsilon_q(2,2)$ e $f \notin \Upsilon q(2,1) \cup \Upsilon_q(1,2)$, então existe uma matriz $A \in \mathcal{N}_{2\times 3}(\mathbb{F}_q)$ tal que $f = \lambda_A(x)$. Observe também que $\Upsilon_q(2,1) \cup \Upsilon_q(1,2) \subset \Upsilon_q(2,2)$, assim $\Gamma_2(2,2) \subset \mathbb{N} \setminus \{1,2,4\}$. Analogamente, se $A \in \mathcal{N}_{2\times 3}(\mathbb{F}_q)$ então $\lambda_A \in \Upsilon_q(2,2)$ e de [20, Teorema 1.5] obtemos $\mathbb{N}\setminus\{1,2,4,6,8,10,12\} \subset \Gamma_2(2,2)$. Também em [20] os autores concluíram que $k \in \Gamma_2(2,2)$

para todo inteiro positivo k, com exceção de $k \in \{1, 2, 4, 6, 8, 10, 12\}$, um resultado que pode ser recuperado da Proposição 51(3). Eles também provaram que $1, 2, 4 \notin \Gamma_2(2, 2)$ e conjecturaram que $6, 8, 9, 10, 12 \in \Gamma_2(2, 2)$. Da Proposição 60 obtemos que $9 \in \Gamma_2(2, 2)$. Agora iremos estudar o conjunto $\Gamma_p(3, 2)$ para $p \in \{2, 3, 5, 7\}$ e começaremos com o caso onde $p = 2$.

Proposição 64. $\mathbb{N} \setminus \{1, 2, 3, 4, 6, 8, 10, 12\} \subset \Gamma_2(3, 2)$ e $\{1, 2, 3, 4\} \cap \Gamma_2(3, 2) = \emptyset$.

Prova. Usando $t = 6$ na Proposição 62, obtemos que $k \in \Gamma_2(3, 2)$ para todo $k \geq 77$. Do Corolário 55, obtêm-se que para todo $k \in \{5, 6, \cdots, 76\} \setminus \{11, 14, 15, 16, 18, 20, 24, 28, 36\}$, $k \in \Gamma_2(3, 2)$.

Usando o Lema 57, com $q = 2^k$ e para $k \in \{11, 14, 15, 16, 18, 20, 24, 28, 36\}$ obtemos que $k \in \Gamma_2(3, 2)$. A Tabela 2.1 resume esses resultados.

Tabela 2.1: Dados que satisfazem o Lema 57.

k	l	$\{p_1, p_2, \cdots, p_r\}$	k	l	$\{p_1, p_2, \cdots, p_r\}$
11	1	$\{23, 89\}$	20	3	$\{5, 11, 31, 41\}$
14	1	$\{3, 43, 127\}$	24	15	$\{7, 13, 17, 241\}$
15	1	$\{7, 31, 151\}$	28	3	$\{5, 29, 43, 113, 127\}$
16	3	$\{5, 17, 257\}$	36	15	$\{7, 13, 19, 37, 73, 109\}$
18	3	$\{7, 19, 73\}$			

Da Proposição 59 obtemos que $1, 2, 3 \notin \Gamma_2(3, 2)$. Em [19] é mostrado que para qualquer elemento primitivo $\beta \in \mathbb{F}_{16}$ tem-se que $f(\beta)$ não é primitivo onde $f = \frac{\alpha x+1}{x+\alpha} \in \mathbb{F}_{16}[x]$ e $\alpha \in \mathbb{F}_{16}$ é um elemento primitivo fixado, assim $4 \notin \Gamma_2(1, 1)$ e, em particular, $4 \notin \Gamma_2(3, 2)$.

Finalmente, da Proposição 60 tem-se que $5, 7 \in \Gamma_2(3, 2)$ e da Proposição 61 tem-se que $9 \in \Gamma_2(3, 2)$.

■

Agora passaremos a estudar os conjuntos $\Gamma_3(3, 2)$, $\Gamma_5(3, 2)$ e $\Gamma_7(3, 2)$.

Teorema 65. Para os conjuntos $\Gamma_3(3, 2)$, $\Gamma_5(3, 2)$ e $\Gamma_7(3, 2)$ são válidos os seguintes resultados.

i) $1, 2 \notin \Gamma_3(3, 2)$ e $\{9, 10, 11\} \cup \{k \in \mathbb{N} : k \geq 13\} \subset \Gamma_3(3, 2)$;

ii) $1 \notin \Gamma_5(3, 2)$ e $\{k \in \mathbb{N} : k \geq 7\} \subset \Gamma_5(3, 2)$;

iii) $1 \notin \Gamma_7(3, 2)$ e $\{k \in \mathbb{N} : k \geq 7\} \subset \Gamma_7(3, 2)$.

Prova. Usando $t = 6$ na Proposição 62 obtemos que $k \in \Gamma_3(3, 2)$ para todo $k \geq 49$, $k \in \Gamma_5(3, 2)$ para todo $k \geq 34$ e $k \in \Gamma_7(3, 2)$ para todo $k \geq 28$.

A tabela a seguir contém os valores de k que são satisfeitos no Corolário 55, em relação a $p = 3, 5, 7$.

Tabela 2.2: Aplicação do Corolário 55 para $p = 3, 5, 7$.

p	$k \in \Gamma_p(3, 2)$
3	$11 \leq k \leq 48$, exceto $k = 12, 18$
5	$7 \leq k \leq 33$, exceto $k = 8, 10, 12$
7	$8 \leq k \leq 27$

As próximas tabelas resumem os resultados obtidos usando o Lema 57 para $p = 3, 5, 7$.

Tabela 2.3: Para $p = 3$, obtemos $9, 10, 18 \in \Gamma_3(3, 2)$.

k	l	$\{p_1, p_2, \cdots, p_r\}$
9	2	$\{13, 757\}$
10	2	$\{11, 61\}$
18	2	$\{7, 13, 19, 37, 757\}$

Tabela 2.4: Para $p = 5$, obtemos $7, 8, 10, 12 \in \Gamma_5(3.2)$.

k	l	$\{p_1, p_2, \cdots, p_r\}$
7	2	$\{19531\}$
8	2	$\{3, 13, 313\}$
10	2	$\{3, 11, 71, 521\}$
12	6	$\{7, 13, 31, 601\}$

Tabela 2.5: Para $p = 7$, obtemos $7 \in \Gamma_7(3, 2)$.

k	l	$\{p_1, p_2, \cdots, p_r\}$
7	2	$\{3, 29, 4733\}$

Finalmente, da Proposição 59 obtemos que $1, 2 \notin \Gamma_3(3, 2)$, $1 \notin \Gamma_5(3, 2)$ e $1 \notin \Gamma_7(3, 2)$. ■

Capítulo 3

Elementos Primitivos Consecutivos em Corpos Finitos

Para $q = p^k$ com p ímpar e $q > 169$, mostraremos que sempre existem três elementos consecutivos em $\mathbb{F}_q$. Além disso, há precisamente 11 valores de q com $q \leq 169$ na qual $\mathbb{F}_q$ não possui esse trio em questão. Finalmente melhoraremos o limite superior de $q_0(n)$ para todo $n \geq 3$. Cohen [3–5] provou que para qualquer $q > 7$, $\mathbb{F}_q$ contém dois elementos primitivos consecutivos. Estamos interessados em determinar $q_0(n)$ tal que $\mathbb{F}_{p^k}, p \geq n$ tenha n elementos primitivos consecutivos distintos para todo $q = p^k > q_0(n)$.

Carlitz [21] mostrou que $q_0(n)$ existe para todo n. Tanti e Thangadurai [22] mostraram que

$$q_0(n) \leq \exp(2^{5.54n}), \text{para todo } n \geq 2. \tag{3.1}$$

Quando $n = 3$, obtém-se um limite superior enorme: 10^{43743}.

Teorema 66. O corpo finito $\mathbb{F}_q$ contém três elementos primitivos consecutivos para todo q ímpar, $q > 169$. Na verdade, os únicos corpos $\mathbb{F}_q$ (q ímpar) os quais não possui três elementos consecutivos são aqueles para quais $q \in \{3, 5, 7, 9, 13, 25, 29, 61, 81, 121, 169\}$.

Quando $n \geq 4$, faremos estimativas para $q_0(n)$ com o seguinte teorema.

Teorema 67. O corpo $\mathbb{F}_q$, assumindo ter característica pelo menos n, contém n elementos primitivos consecutivos desde que $q > q_0(n)$, onde os valores de $q_0(n)$ são dados na terceira coluna da Tabela 3.1 para $4 \leq n \leq 10$ e $q_0(n) = \exp(2^{2.77n})$ para $n \geq 11$.

Provamos o Teorema 67 e discutimos a construção da Tabela 3.1 na Seção 3.3.

Note que o expoente externo do limite no Teorema 67 é a metade de (3.1). Isto é devido a desigualdade de aprimoramento usado no Teorema 73.

Ainda sim, tem-se que o expoente duplo nos fornece valores muito grandes de $q_0(n)$. Deve-se estender a Tabela 3.1 de acordo com a Seção 3.3.

Na Seção 3.4, apresentaremos um algoritmo juntamente com o Teorema 67 para provar o Teorema 66 .

Tabela 3.1: Intervalo dos valores de q dado n

n	Limite para $\omega(q-1)$	Limite para q $(q_0(n))$
3	13	3.49×10^{15}
4	23	3.29×10^{32}
5	37	4.22×10^{61}
6	59	4.61×10^{113}
7	100	3.75×10^{220}
8	171	2.27×10^{425}
9	301	1.01×10^{836}
10	533	6.69×10^{1638}

3.1 Estimativas

A presente investigação se refere à existência de $n \geq 2$ elementos consecutivos distintos em $\mathbb{F}_q$, ou seja, se existe $g \in \mathbb{F}_q$ de forma que $\{g, g+1, g+2, \cdots, g+n-1\}$ seja um conjunto de n elementos primitivos distintos consecutivos de $\mathbb{F}_q$. Como $q = p^n$, então, necessariamente, $n \leq p$, mas estamos particularmente interessados em $n \geq 3$, ou seja, assumiremos que $3 \leq n \leq p$.

Sejam $l_1, \cdots, l_n$ divisores de $q-1$. Definimos $N(l_1, \cdots, l_n)$ como sendo o número de elementos $g \in \mathbb{F}_q$ tais que $g+k-1$ é l_k-livre onde $k \in \{1, \cdots, n\}$. Baseado na Equação (2.2) tem-se o próximo lema.

Lema 68. Seja $3 \leq n \leq p$ e $l_1, \cdots, l_n$ divisores de $q-1$. Então

$$N(l_1, \cdots, l_n) = \theta(l_1) \cdots \theta(l_n) \sum_{d_1 | l_1, \cdots, d_n | l_n} \frac{\mu(d_1)}{\phi(d_1)} \cdots \frac{\mu(d_n)}{\phi(d_n)} \sum_{ord(\chi_1)=d_1, \cdots, ord(\chi_n)=d_n} \tilde{\chi}(\chi_1, \cdots, \chi_n), \tag{3.2}$$

onde

$$\tilde{\chi}(\chi_1, \cdots, \chi_n) = \sum_{g \in \mathbb{F}_q} \chi_1(g)\chi_2(g+1) \cdots \chi_n(g+n-1).$$

Agora forneceremos um limite do valor de $\tilde{\chi}(\chi_1, \cdots, \chi_n)$. Para tal, enunciaremos o próximo teorema [13, Teorema 5.41] que será utilizado na demonstração no lema posterior.

Teorema 69. Seja ψ um caráter multiplicativo de $\mathbb{F}_q$ de ordem $d > 1$ e seja $f \in \mathbb{F}_q[x]$ um polinômio mônico de grau positivo que não é uma d-ésima potência de um outro polinômio em $\mathbb{F}_q[x]$. Seja n o número de raízes distintas de f no fecho algébrico de $\mathbb{F}_q$. Então para todo $a \in \mathbb{F}_q$ tem-se

$$\left| \sum_{\alpha \in \mathbb{F}_q} \psi(a \cdot f(c)) \right| \leq (n-1)\sqrt{q}.$$

Definição 70. Seja $f \in \mathbb{F}_q[x]$. Escreva $f = f_1^{\alpha_1} \cdots f_n^{\alpha_n}$, sendo $f_1, \cdots, f_n$ polinômios irredutíveis distintos e α_i com $i \in \{1, \cdots, n\}$, inteiros não nulos. Definimos por radical de f e denotamos por $\mathrm{Rad}(f)$, o produto de todos os polinômios irredutíveis, ou seja, $\mathrm{Rad}(f) = f_1 \cdots f_n$.

Lema 71. Sejam $d_1, \cdots, d_n$ ordens dos caracteres $\chi_1, \cdots, \chi_n$, respectivamente. Suponha que $d_1, \cdots, d_n$ sejam divisores de $q-1$ livres de quarado. Então

$$\tilde{\chi}(\chi_1, \cdots, \chi_n) = q - n \text{ se } d_1 = \cdots = d_n = 1.$$

Caso contrário,

$$\tilde{\chi}(\chi_1, \cdots, \chi_n) \leq (n-1)\sqrt{q}.$$

Prova. Assumindo que nem todos os divisores $d_1, \cdots, d_n$ assumam valor 1, defina

$$d := \text{mmc}(d_1, d_2, \cdots, d_n).$$

Observe que d é também um divisor livre de quadrados de $q-1$ e $d > 1$. Pelo Teorema 40 aplicado a um subgrupo H de $\mathbb{F}_q$, existe um caráter χ de ordem d e inteiros $c_i \in \{0, 1, \cdots, d-2\}$ tais que $\chi_i(\alpha) = \chi(\alpha^{c_i})$ para todo $\alpha \in \mathbb{F}_q$. Logo

$$\begin{aligned}
\tilde{\chi}(\chi_1, \cdots, \chi_n) &= \sum_{g \in \mathbb{F}_q} \chi_1(g)\chi_2(g+1)\cdots\chi_n(g+n-1) \\
&= \sum_{g \in \mathbb{F}_q} \chi(g^{c_1})\chi[(g+1)^{c_2}]\cdots\chi[(g+n-1)^{c_n}] \\
&= \sum_{g \in \mathbb{F}_q} \chi(g^{c_1} \cdot (g+1)^{c_2}\cdots(g+n-1)^{c_n}) \\
&= \sum_{g \in \mathbb{F}_q} \chi(f(g))
\end{aligned}$$

onde $f(x) = x^{c_1} \cdot (x+1)^{c_2} \cdot (x+2)^{c_3} \cdots (x+n-1)^{c_n}$. Note que o radical de f é igual a n e f não é uma d-ésima potência de um polinômio uma vez que $d \nmid c_i$ para todo $i \in \{1, \cdots, n\}$. Segue do Teorema 69 que

$$|\tilde{\chi}(\chi_1, \cdots, \chi_n)| = \left| \sum_{g \in \mathbb{F}_q} \chi(f(g)) \right| \leq (n-1)\sqrt{q}.$$

Quando $d_1 = \cdots = d_n = 1$, tem-se $c_1 = \cdots = c_n = 0$ e, portanto,

$$\tilde{\chi}(\chi_1, \cdots, \chi_n) = \sum_{g \in \mathbb{F}_q \setminus S_f} 1 = \sharp(\mathbb{F}_q \setminus S_f) = q - n$$

onde $S_f := \{\beta \in \mathbb{F}_q : f(\beta) = 0\}$. ■

Quando $l_1 = l_2 = \cdots = l_n = l$ denotaremos $N(l_1, \cdots, l_n)$ por $N_n(l)$. Obtemos um limite inferior para $N_n(l)$ no lema seguinte.

Lema 72. Sejam $3 \leq n \leq p$ e l um divisor de $q-1$. Então

$$N_n(l) > \theta(l)^n \left[q - (n-1)W(l)^n\sqrt{q}\right]. \tag{3.3}$$

Prova. Note que precisamos apenas nos preocupar com os divisores livres de quadrados $d_1, \cdots, d_n$ de l devido a presença da função de Möbius. Do Lema 68 tem-se

$$N_n(l) = \theta(l)^n \sum_{d_1|l, \cdots, d_n|l} \frac{\mu(d_1)}{\phi(d_1)} \cdots \frac{\mu(d_n)}{\phi(d_n)} \sum_{ord(\chi_1)=d_1, \cdots, ord(\chi_n)=d_n} \tilde{\chi}(\chi_1, \cdots, \chi_n).$$

Subdividindo o somatório em dois na equação acima de modo que o primeiro englobe o caso onde $d_1 = \cdots = d_n = 1$ e o segundo englobe os casos restantes e, aplicando o Lema 71, tem-se

$$\begin{aligned}
N_n(l) &= \theta(l)^n \sum_{d_1|l,\cdots,d_n|l} \frac{\mu(d_1)}{\phi(d_1)} \cdots \frac{\mu(d_n)}{\phi(d_n)} \sum_{ord(\chi_1)=d_1,\cdots,ord(\chi_n)=d_n} \tilde{\chi}(\chi_1,\cdots,\chi_n) \\
&= \theta(l)^n \left[q-n+ \sum_{\substack{d_1|l,\cdots,d_n|l \\ (d_1,\cdots,d_n)\neq(1,\cdots,1)}} \frac{\mu(d_1)}{\phi(d_1)} \cdots \frac{\mu(d_n)}{\phi(d_n)} \sum_{\substack{ord(\chi_1)=d_1,\cdots,ord(\chi_n)=d_n \\ (d_1,\cdots,d_n)\neq(1,\cdots,1)}} \tilde{\chi}(\chi_1,\cdots,\chi_n) \right] \\
&= \theta(l)^n \left[q-n+ \sum_{\substack{d_1|l,\cdots,d_n|l \\ (d_1,\cdots,d_n)\neq(1,\cdots,1)}} \mu(d_1)\cdots\mu(d_n)\tilde{\chi}(\chi_1,\cdots,\chi_n) \right] \\
&\geq \theta(l)^n \left[q-n- \sum_{\substack{d_1|l,\cdots,d_n|l \\ (d_1,\cdots,d_n)\neq(1,\cdots,1)}} |\mu(d_1)|\cdots|\mu(d_n)||\tilde{\chi}(\chi_1,\cdots,\chi_n)| \right] \\
&\geq \theta(l)^n \left[q-n-(n-1)\sqrt{q} \sum_{\substack{d_1|l,\cdots,d_n|l \\ (d_1,\cdots,d_n)\neq(1,\cdots,1)}} |\mu(d_1)|\cdots|\mu(d_n)| \right]. \qquad (3.4)
\end{aligned}$$

Note que a última soma é igual ao número de n-uplas $(d_1,\cdots,d_n) \neq (1,\cdots,1)$ tal que $d_1,\cdots,d_n \mid l$, com $d_1,\cdots,d_n$ livres de quadrados, ou seja,

$$\sum_{\substack{d_1|l,\cdots,d_n|l \\ (d_1,\cdots,d_n)\neq(1,\cdots,1)}} |\mu(d_1)|\cdots|\mu(d_n)| = W(l)^n - 1. \qquad (3.5)$$

Substituindo (3.5) em (3.4) tem-se

$$\begin{aligned}
N_n(l) &\geq \theta(l)^n \left[q-n-(n-1)\sqrt{q}(W(l)^n-1)\right] \\
&\geq \theta(l)^n \left[q-n-(n-1)W(l)^n\sqrt{q}+(n-1)\sqrt{q}\right].
\end{aligned}$$

Note que $(n-1)\sqrt{q}-n>0$ uma vez que $n\geq 3$ e $q\geq 3$ e, portanto,

$$N_n(l) > \theta(l)^n[q-(n-1)W(l)^n\sqrt{q}].$$

■

Aplicando o Lema 72 para $l = q-1$ obtemos um critério básico que nos garante a existência de n elementos primitivos consecutivos em $\mathbb{F}_q$ para q suficientemente grande. De fato, precisamos que

$$\begin{aligned}
& q-(n-1)W(q-1)^n q^{\frac{1}{2}} > 0 \\
\Leftrightarrow\ & q^{\frac{1}{2}}(q^{\frac{1}{2}}-(n-1)W(q-1)^n) > 0 \\
\Leftrightarrow\ & q^{\frac{1}{2}} > (n-1)W(q-1)^n \\
\Leftrightarrow\ & q > (n-1)^2 W(q-1)^{2n} \\
\Leftrightarrow\ & q > (n-1)^2 2^{2n\omega(q-1)}.
\end{aligned}$$

E assim obtemos o próximo teorema.

Teorema 73. Seja $3 \leq n \leq p$. Suponha que

$$q > (n-1)^2 W(q-1)^{2n} = (n-1)^2 2^{2n\omega(q-1)}. \tag{3.6}$$

Então existe um conjunto com n elementos primitivos consecutivos em $\mathbb{F}_q$.

Como aplicação do Teorema 73, consideremos o caso $n = 3$. Defina P_m como sendo o produto dos m primeiros números primos. Pode-se ver que para $m \geq 50$ tem-se $P_m + 1 \geq 2^{2+6m}$. Assim, segue que $\mathbb{F}_q$ possui três elementos primitivos consecutivos quando $\omega(q-1) \geq 50$ ou quando $q \geq 2^{2+6\cdot 50}$. Melhoraremos isso significativamente.

Antes de apresentarmos o próximo teorema, faremos uma observação que é de suma importância para a compreensão do mesmo.

Observação 74. Dado um caráter multiplicativo χ de $\mathbb{F}_q$, observe que $\chi(-1) = \pm 1$. Considere m a ordem de χ, isto é, m é o menor inteiro positivo tal que $\chi^m = \chi_0$. Então m divide $q-1$ uma vez que $\chi^{q-1} = \chi_0$. Os valores de χ são raízes m-ésimas da unidade, em particular, -1 pode aparecer como valor de χ se m é par. Se g é um elemento primitivo de $\mathbb{F}_q$, então $\chi(g) = \xi$ é uma rais m-ésima da unidade. Se m é par, então precisamente q é ímpar, segue então que $\chi(-1) = \chi(g^{\frac{q-1}{2}}) = \xi^{\frac{q-1}{2}}$ na qual é -1 se precisamente $\frac{q-1}{2} \equiv \frac{m}{2} \pmod{m}$, ou seja, $\frac{q-1}{m} \equiv 1 \pmod 2$. Portanto, $\chi(-1) = -1$ se, e somente se, m é par e $\frac{q-1}{m}$ é ímpar. Caso contrário, $\chi(-1) = 1$.

O próximo passo é apresentar uma melhora na discussão acima quando $q \equiv 3 \pmod 4$. A melhora nesse caso se deve à Observação 74.

Note que no Lema 68, podemos substituir g por $-g-(n-1)$ na definição de $\tilde{\chi}(\chi_1, \cdots, \chi_n)$, obtendo

$$\begin{aligned}
\tilde{\chi}(\chi_1, \cdots, \chi_n) &= \sum_{g \in \mathbb{F}_q} \chi_1(g)\chi_2(g+1)\cdots\chi_n(g+n-1) \\
&= \sum_{g \in \mathbb{F}_q} \chi_1(-g-n+1)\chi_2(-g-n+2)\cdots\chi_n(-g) \\
&= \sum_{g \in \mathbb{F}_q} \chi_1(-1)\chi_1(g+n-1)\chi_2(-1)\chi_2(g+n-2)\cdots\chi_n(-1)\chi_n(g) \\
&= (\chi_1\chi_2\cdots\chi_n)(-1)\tilde{\chi}(\chi_n, \cdots, \chi_1).
\end{aligned}$$

Seja χ_m um caráter de ordem m. Note que como $q \equiv 3 \pmod 4$ tem-se que 2 aparece apenas uma vez na fatoração de $q-1$, ou seja, $q-1 = 2 \cdot p_1^{r_1} \cdots p_s^{r_s}$ onde os p_i's são primos ímpares e, portanto, $\frac{q-1}{m}$ é ímpar se m é par. Segue da Observação 74 que $\chi_m(-1) = -1$ se m é par e $\chi_m(-1) = 1$ se m é ímpar.

Neste sentido, se da lista $d_1, \cdots, d_n$ pudermos obter uma sublista $d_{i_1}, \cdots, d_{i_j}$ de modo que j seja ímpar e todos $d'_{i_t}s$ com $t \in \{i_1, \cdots, i_j\}$ sejam pares, então $\tilde{\chi}(\chi_n, \cdots, \chi_1) = -\tilde{\chi}(\chi_1, \cdots, \chi_n)$, caso contrário, $\tilde{\chi}(\chi_n, \cdots, \chi_1) = \tilde{\chi}(\chi_1, \cdots, \chi_n)$. Como consequência, no Lema 68, se $l_1 = \cdots = l_n = l$ é par, então do lado direito da Equação (3.2) os termos correspondentes aos divisores $(d_1, \cdots, d_n)$ com um número ímpar de divisores pares se cancelam, ou seja, metade das n-uplas $(d_1, \cdots, d_n)$ se cancelam uma vez que metade dos divisores de $q-1$ são pares pois $q-1 = 2 \cdot p_1^{r_1} \cdots p_s^{r_s}$. Nessa situação, obtemos o seguinte melhoramento do Lema 72 e Teorema 73.

Teorema 75. Seja $3 \leq n \leq p$ e l um divisor par de $q-1$, onde $q \equiv 3 \pmod 4$ e $q \geq 7$. Então

$$N_n(l) \geq \theta(l)^n \left(q - \frac{n-1}{2} W(l)^n \sqrt{q} \right).$$

Além disso, se

$$q \geq \frac{(n-1)^2}{4} W(q-1)^{2n} = (n-1)^2 2^{2(n\omega(q-1)-1)},$$

então existe um conjunto com n elementos primitivos consecutivos em $\mathbb{F}_q$.

3.2 Aprimorando desigualdades e estimativas

Como antes, seja $3 \leq n \leq p$ e seja l um divisor de $q-1$. Dado inteiros positivos m, j, k com $1 \leq j,\ k \leq n$ defina

$$m_{jk} = \begin{cases} m, \text{ se } j = k \\ 1 \text{ caso contrário.} \end{cases} \tag{3.7}$$

Lema 76. Seja $3 \leq n \leq p$ e l um divisor de $q-1$. Seja e um divisor primo de $q-1$ que não divide l. Então para todo $j \in \{1, \cdots, n\}$,

$$|N(e_{j1}l, \cdots, e_{jn}l) - \theta(e)N_n(l)| \leq \left(1 - \frac{1}{e}\right) \theta(l)^n (n-1) W(l)^n \sqrt{q}.$$

Prova. Primeiramente observe que, de acordo com (3.7), para j fixado, apenas um elemento do conjunto $\{e_{j1}l, e_{j2}l, \cdots, e_{jn}l\}$ é exatamente el, o restante é igual a l. Sem perda de generalidade, consideremos que el apareça na primeira entrada de $N(e_{j1}l, \cdots, e_{jn}l)$, ou seja, $N(e_{j1}l, \cdots, e_{jn}l) = N(el, l, \cdots, l)$. Portanto

$$N(e_{j1}l, \cdots, e_{jn}l) = \theta(e)\theta(l)^n \sum_{d_1 | el, d_2 | l, \cdots, d_n | l} \frac{\mu(d_1)}{\phi(d_1)} \cdots \frac{\mu(d_n)}{\phi(d_n)} \sum_{ord(\chi_1)=d_1, \cdots, ord(\chi_n)=d_n} \tilde{\chi}(\chi_1, \cdots, \chi_n).$$

Subdividindo o conjunto dos d_1's em dois, o primeiro conterá aqueles divisores que não possuem e como fator, ou seja, todos os divisores de l, e o segundo aqueles que possuem e como fator, ou seja, aqueles d_1's em que $e \mid d_1$. Portanto

$$\begin{aligned} N(e_{j_1}l, \cdots, e_{j_n}l) = \theta(e)\theta(l)^n & \sum_{d_1 | l, d_2 | l, \cdots, d_n | l} \frac{\mu(d_1)}{\phi(d_1)} \cdots \frac{\mu(d_n)}{\phi(d_n)} \sum_{ord(\chi_1)=d_1, \cdots, ord(\chi_n)=d_n} \tilde{\chi}(\chi_1, \cdots, \chi_n) \\ + \theta(e)\theta(l)^n & \sum_{e | d_1, d_1 | el, d_2 | l \cdots, d_n | l} \frac{\mu(d_1)}{\phi(d_1)} \cdots \frac{\mu(d_n)}{\phi(d_n)} \sum_{ord(\chi_1)=d_1, \cdots, ord(\chi_n)=d_n} \tilde{\chi}(\chi_1, \cdots, \chi_n). \end{aligned}$$

Além disso, observe que

$$\theta(e)N_n(l) = \theta(e)\theta(l)^n \sum_{d_1 | l, d_2 | l, \cdots, d_n | l} \frac{\mu(d_1)}{\phi(d_1)} \cdots \frac{\mu(d_n)}{\phi(d_n)} \sum_{ord(\chi_1)=d_1, \cdots, ord(\chi_n)=d_n} \tilde{\chi}(\chi_1, \cdots, \chi_n),$$

logo tem-se que

$$\begin{aligned} N(e_{j1}l,\cdots,&e_{jn}l)-\theta(e)N_n(l)= \\ &=\theta(e)\theta(l)^n \sum_{e|d_1,d_1|el,d_2|l\cdots,d_n|l} \frac{\mu(d_1)}{\phi(d_1)}\cdots\frac{\mu(d_n)}{\phi(d_n)} \sum_{ord(\chi_1)=d_1,\cdots,ord(\chi_n)=d_n} \tilde{\chi}(\chi_1,\cdots,\chi_n) \\ &=\theta(e)\theta(l)^n \sum_{e|d_1,d_1|el,d_2|l\cdots,d_n|l} \mu(d_1)\cdots\mu(d_n)\tilde{\chi}(\chi_1,\cdots,\chi_n). \end{aligned}$$

Portanto, temos

$$|N(e_{j1}l,\cdots,e_{jn}l)-\theta(e)N_n(l)|\leq \theta(e)\theta(l)^n \sum_{e|d_1,d_1|el,d_2|l\cdots,d_n|l} |\mu(d_1)|\cdots|\mu(d_n)||\tilde{\chi}(\chi_1,\cdots,\chi_n)|.$$

Do Lema 71 temos $|\tilde{\chi}(\chi_1,\cdots,\chi_n)|\leq (n-1)\sqrt{q}$ e, além disso,

$$\sum_{e|d_1,d_1|el,d_2|l\cdots,d_n|l} |\mu(d_1)|\cdots|\mu(d_n)|= W(l)^n.$$

Portanto,

$$|N(e_{j_1}l,\cdots,e_{j_n}l)-\theta(e)N_n(l)|\leq \theta(e)\theta(l)^n W(l)^n(n-1)\sqrt{q}.$$

Note que $\theta(e)=\left(1-\frac{1}{e}\right)$ pois e é primo, ou seja,

$$|N(e_{j_1}l,\cdots,e_{j_n}l)-\theta(e)N_n(l)|\leq \left(1-\frac{1}{e}\right)\theta(l)^n W(l)^n(n-1)\sqrt{q}.$$

■

Definição 77. Seja $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}\geq 1$, fatorado em primos distintos. Definimos por radical de n e denotamos por $\mathrm{Rad}(n)$, o produto de todos os fatores primos distintos de n, ou seja, $\mathrm{Rad}(n)=p_1\cdots p_r$.

Isso nos leva ao principal resultado de melhoramento. Seja l um divisor de $q-1$. No que se segue, se $\mathrm{Rad}(l)=\mathrm{Rad}(q-1)$ defina $s=0$ e $\delta=1$. Caso contrário, sejam $p_1,\cdots,p_s, s\geq 1$ os divisores primos de $q-1$ que não dividem l e defina $\delta=1-n\sum_{i=1}^{s}\frac{1}{p_i}$. É essencial escolher l de forma que $\delta>0$.

Lema 78. Seja $3\leq n\leq p$ e l um divisor de $q-1$. Então, com as notações acima

$$N_n(q-1)\geq \left(\sum_{j=1}^{n}\sum_{i=1}^{s} N(p_{ij1}l,p_{ij2}l,\cdots,p_{ijn}l)\right)-(ns-1)N_n(l), \tag{3.8}$$

onde p_{ijk} significa $(p_i)_{jk}$ como em (3.7). Consequentemente

$$N_n(q-1)\geq \delta N_n(l)+\sum_{i=1}^{s}\left(\sum_{j=1}^{n} N(p_{ij1}l,p_{ij2}l,\cdots,p_{ijn}l)-\theta(p_1)N_n(l)\right). \tag{3.9}$$

Prova. Note que $N_n(q-1)$ conta a quantidade de elementos $g\in\mathbb{F}_q^*$ tais que $g, g+1,\cdots,g+n-1$ são $(q-1)$-livres, ou seja, primitivos. Observe que $p_{ijk}l=p_il$ ou $p_{ijk}l=l$. Se $g\in\mathbb{F}_q^*$ é $(q-1)$-livre então g é l-livre e p_il-livre. Portanto, se a n-upla $(g,g+1,\cdots,g+n-1)$ é uma n-upla de elementos primitivos, então ela será contada $ns-(ns-1)=1$ vez e vale

a Desigualdade (3.8). Por outro lado, se $g \in \mathbb{F}_q^*$ é tal que pelo menos um dos elementos do conjunto $\{g, g+1, \cdots, g+n-1\}$ não é primitivo, então do Lema 44, este elemento não será $p_i l$-livre para algum $i \in \{1, \cdots, s\}$ e, portanto, o lado direito de (3.8) será contado no máximo $ns - 1 - (ns-1) = 0$ vezes e está demonstrada a Desigualdade (3.8).

Em relação a Desigualdade (3.9), uma vez que $\theta(p_i) = \left(1 - \frac{1}{p_i}\right)$ tem-se

$$\begin{aligned}
N_n(q-1) &\geq \sum_{i=1}^{s}\sum_{j=1}^{n} N(p_{ij1}l, p_{ij2}l, \cdots, p_{ijn}l) - (ns-1)N_n(l) \\
&\geq \sum_{i=1}^{s}\sum_{j=1}^{n} N(p_{ij1}l, p_{ij2}l, \cdots, p_{ijn}l) + \left[-ns + n\sum_{i=1}^{s}\frac{1}{p_i} + 1 - n\sum_{i=1}^{s}\frac{1}{p_i}\right] N_n(l) \\
&\geq \sum_{i=1}^{s}\sum_{j=1}^{n} N(p_{ij1}l, p_{ij2}l, \cdots, p_{ijn}l) + \left[-ns + n\sum_{i=1}^{s}\frac{1}{p_i} + \delta\right] N_n(l) \\
&\geq \sum_{i=1}^{s}\sum_{j=1}^{n} N(p_{ij1}l, p_{ij2}l, \cdots, p_{ijn}l) - nsN_n(l) + n\sum_{i=1}^{s}\frac{1}{p_i}N_n(l) + \delta N_n(l) \\
&\geq \sum_{i=1}^{s}\sum_{j=1}^{n} N(p_{ij1}l, p_{ij2}l, \cdots, p_{ijn}l) - n\sum_{i=1}^{s}\left(1 - \frac{1}{p_i}\right) N_n(l) + \delta N_n(l) \\
&\geq \sum_{i=1}^{s}\left(\sum_{j=1}^{n} N(p_{ij1}l, p_{ij2}l, \cdots, p_{ijn}l) - \left(1 - \frac{1}{p_i}\right) N_n(l)\right) + \delta N_n(l) \\
&\geq \sum_{i=1}^{s}\left(\sum_{j=1}^{n} N(p_{ij1}l, p_{ij2}l, \cdots, p_{ijn}l) - \theta(p_i)N_n(l)\right) + \delta N_n(l).
\end{aligned}$$

Portanto, vale (3.9).

■

Agora podemos fornecer uma condição de forma que, se satisfeita, é suficiente para provar a existência de n elementos consecutivos.

Teorema 79. Seja $3 \leq n \leq p$ e l um divisor de $q-1$. Se $\mathrm{Rad}(l) = \mathrm{Rad}(q-1)$ então defina $s = 0$ e $\delta = 1$. Caso contrário, seja $p_1, \cdots, p_s, s \geq 1$, divisores primos de $q-1$ mas que não dividem l e defina $\delta = 1 - n\sum_{i=1}^{s}\frac{1}{p_i}$. Assuma $\delta > 0$. Se

$$q > \left((n-1)\left(\frac{ns-1}{\delta} + 2\right) W(l)^n\right)^2, \tag{3.10}$$

então existem n elementos primitivos consecutivos em $\mathbb{F}_q$.

Prova. A Desigualdade (3.9) nos diz que

$$N_n(q-1) \geq \delta N_n(l) + \sum_{i=1}^{s}\left(\sum_{j=1}^{n} N(p_{ij1}l, p_{ij2}l, \cdots, p_{ijn}l) - \theta(p_1)N_n(l)\right).$$

Como $N(p_{ij1}l, p_{ij2}l, \cdots, p_{ijn}l) \geq 0$ e $\theta(p_1)N_n(l) \geq 0$ para todo $i \in \{1, \cdots, s\}$ e para todo $j \in \{1, \cdots, n\}$ segue que

$$N(p_{ij1}l, p_{ij2}l, \cdots, p_{ijn}l) - \theta(p_1)N_n(l) \geq -|N(p_{ij1}l, p_{ij2}l, \cdots, p_{ijn}l) - \theta(p_1)N_n(l)|$$

e, consequentemente

$$N_n(q-1) \geq \delta N_n(l) + \sum_{j=1}^{n}\left(\sum_{i=1}^{s}|N(p_{ij1}l, p_{ij2}l, \cdots, p_{ijn}l) - \theta(p_1)N_n(l)|\right). \tag{3.11}$$

Aplicando o Lema 76 em (3.11) obtemos

$$N_n(q-1) \geq \delta N_n(l) - n\sum_{i=1}^{s}\left(1-\frac{1}{p_i}\right)\theta(l)^n W(l)^n(n-1)\sqrt{q}. \tag{3.12}$$

Por outro lado, observe que

$$\sum_{i=1}^{s}\left(1-\frac{1}{p_i}\right) = s - \sum_{i=1}^{s}\frac{1}{p_i} = s + \frac{\delta-1}{n} = \frac{\delta}{n}\left(\frac{ns-1}{\delta}+1\right) \tag{3.13}$$

e do Lema 72 segue que

$$N_n(l) \geq \theta(l)^n\left[q-(n-1)W(l)^n\sqrt{q}\right]. \tag{3.14}$$

Substituindo (3.13) e (3.14) em (3.12) temos

$$\begin{aligned}
N_n(q-1) \quad \geq \quad & \delta\theta(l)^n\left[q-(n-1)W(l)^n\sqrt{q}\right] - n\frac{\delta}{n}\left(\frac{ns-1}{\delta}+1\right)\theta(l)^n W(l)^n(n-1)\sqrt{q} \\
& \delta\theta(l)^n\left[q-(n-1)W(l)^n\sqrt{q} - W(l)^n(n-1)\sqrt{q}\left(\frac{ns-1}{\delta}+1\right)\right] \\
& \delta\theta(l)^n\left[q-(n-1)W(l)^n\sqrt{q}\left(1+\left(\frac{ns-1}{\delta}+1\right)\right)\right] \\
& \delta\theta(l)^n\left[q-(n-1)W(l)^n\sqrt{q}\left(\frac{ns-1}{\delta}+2\right)\right].
\end{aligned}$$

Uma vez que, por hipótese, $\delta > 0$, para que $N_n(q-1)$ seja maior que zero, é necessário que

$$\begin{aligned}
& q-(n-1)W(l)^n\sqrt{q}\left(\frac{ns-1}{\delta}+2\right) > 0 \\
\Leftrightarrow \quad & q^{\frac{1}{2}}\left[q^{\frac{1}{2}} - (n-1)W(l)^n\left(\frac{ns-1}{\delta}+2\right)\right] > 0 \\
\Leftrightarrow \quad & q^{\frac{1}{2}} > (n-1)W(l)^n\left(\frac{ns-1}{\delta}+2\right) \\
\Leftrightarrow \quad & q > \left((n-1)W(l)^n\left(\frac{ns-1}{\delta}+2\right)\right)^2.
\end{aligned}$$

E o teorema está demonstrado. ■

Concluímos esta seção com uma ligeira melhora quando $q \equiv 3 \pmod 4$. Quando l é par, pela Observação 74, as expressões de soma de caracteres para os termos

$$\sum_{j=1}^{n} N(p_{ij1}l, p_{ij2}l, \cdots, p_{ijn}l) - \theta(p_1)N_n(l)$$

em (3.9) se cancelam a menos que um número par de divisores $(d_1, \cdots, d_n)$ sejam pares. Logo temos uma redução pela metade no limite do Lema 76 e, por conseguinte, uma melhora no Teorema 79.

Teorema 80. Suponha $q \equiv 3 \pmod 4$, $q \geq 7$, $3 \leq n \leq p$ e l um divisor de $q-1$. Se $\mathrm{Rad}(l) = \mathrm{Rad}(q-1)$ então defina $s = 0$ e $\delta = 1$. Caso contrário, seja $p_1, \cdots, p_s, s \geq 1$, divisores primos de $q-1$ mas que não dividem l e defina $\delta = 1 - n\sum_{i=1}^{s}\left(\frac{1}{p_i}\right)$. Assuma $\delta > 0$. Se

$$q > \left((n-1)\left(\frac{ns-1}{\delta}+2\right)W(l)^n\right)^2,$$

então existe n elementos primitivos consecutivos em $\mathbb{F}_q$.

Observação 81. Nos Teoremas 79 e 80 o melhor (maior) valor de δ é obtido quando os maiores fatores primos de $q-1$ são usados para calcular δ.

3.3 Aplicação dos Teoremas 73 e 79 para n genérico; prova do Teorema 67

Como uma aplicação do Teorema 79 considere o caso $n = 3$. Mostramos após o Teorema 73 que $\mathbb{F}_q$ contém três elementos primitivos consecutivos para todo q satisfazendo $\omega(q-1) \geq 50$. Para $14 \leq \omega(q-1) \leq 49$ verificamos que vale (3.10) com $s = 8$. Como exemplo, considere $\omega(q-1) = 14$ e $s = 8$ donde

$$\delta = 1 - 3\left(\frac{1}{17}+\frac{1}{19}+\frac{1}{23}+\frac{1}{29}+\frac{1}{31}+\frac{1}{37}+\frac{1}{41}+\frac{1}{43}\right) > 0.1109.$$

Segue que o lado direito de (3.10) é ligeiramente maior do que 12 039 747 811 470 119 o qual é menor do que P_{14}. Observe que $\omega(q-1) = 14$ implica que $q-1 \geq P_{14}$. Segue que $\mathbb{F}_q$ tem três elementos consecutivos quando $\omega(q-1) = 14$. Por outro lado, não podemos proceder diretamente quando $\omega(q-1) \leq 13$. Por exemplo, quando $\omega(q-1) = 13$, não há valor de s tal que $1 \leq s \leq 13$ que satisfaça com que o lado direito (3.10) seja menor do que P_{13}. Se escolhermos $s = 7$ no Teorema 79, obtemos que q precisa superar 3.48914×10^{15} para que existam três elementos consecutivos primitivos, ou seja, precisamos apenas considerar $\omega(q-1) \leq 13$ e $q \leq 3.49 \times 10^{15}$.

Continuamos esse procedimento para valores maiores de n. Usamos o Teorema 73 para obtermos um limite inicial para $\omega(q-1)$ e então utilizamos o Teorema 79 para valores convenientes de s de forma a reduzir o máximo possível o limite. Portanto, reduzimos o problema de encontrar n elementos primitivos consecutivos em $\mathbb{F}_q$ de forma computacional para valores finitos em um determinado intervalo. Esse intervalo é dado na Tabela 3.1.

Agora usamos o Teorema 73 para obter um limite $q_0(n)$ para um valor genérico de n. Para encontrar um limite para $\omega(q-1)$, usamos um resultado de Robin [23, Teorema 11], que nos diz que $\omega(n) \leq 1.38402\log(n)/\log(\log(n))$ para todo $n \geq 3$. Uma vez que a função $\log(x)/\log(\log(x))$ é crescente para $x \geq e^e$ temos

$$\omega(q-1) \leq \frac{1.38402\log(q)}{\log(\log(q))} \tag{3.15}$$

para todo $q \geq 17$. Não é difícil verificar que vale (3.15) para $3 \leq q \leq 17$. Substituindo

(3.15) em (3.6) obtemos

$$\begin{aligned} q &\geq (n-1)^2 \cdot 2^{2n\omega(q-1)} \\ \log(q) &\geq \log(n-1)^2 + \log 2^{2n\omega(q-1)} \\ &\geq 2 \cdot \log(n-1) + 2n\omega(q-1) \cdot \log(2) \\ &\geq 2\log(n-1) + 2n\log(2) \cdot \frac{1.38402\log(q)}{\log(\log(q))} \\ &\geq 2\log(n-1) + \frac{2.76804n\log(2)\log(q)}{\log(\log(q))} \\ \log(q) - \frac{2.76804n\log(2)\log(q)}{\log(\log(q))} &\geq 2\log(n-1) \\ \log(q)\left(1 - \frac{2.76804n\log(2)}{\log(\log(q))}\right) &\geq 2\log(n-1). \end{aligned} \tag{3.16}$$

Para resolver (3.16) observe que $\left(1 - \frac{2.76804n\log(2)}{\log(\log(q))}\right)$ está limitado inferiormente por d, para algum $d \in (0,1)$. Logo obtemos

$$\begin{aligned} d &\leq 1 - \frac{2.76804n\log(2)}{\log(\log(q))} \\ -d &\geq -1 + \frac{2.76804n\log(2)}{\log(\log(q))} \\ 1-d &\geq \frac{2.76804n\log(2)}{\log(\log(q))} \\ \log(\log(q))(1-d) &\geq 2.76804n\log(2) \\ \log\left[\log(q)^{1-d}\right] &\geq \log(2^{2.76804n}) \\ \log(q)^{1-d} &\geq 2^{2.76804n} \\ \log(q) &\geq 2^{\frac{2.76804n}{1-d}} \\ q &\geq \exp\left(2^{\frac{2.76804n}{1-d}}\right). \end{aligned}$$

Por outro lado, insistimos que $d\log(q) \geq 2\log(n-1)$, ou seja, $q \geq (n-1)^{\frac{2}{d}}$ e, portanto, para garantir a validade de (3.6) tomamos

$$q \geq \max\{(n-1)^{\frac{2}{d}}, \exp\left(2^{\frac{2.76804n}{1-d}}\right)\}. \tag{3.17}$$

Escolhendo $d = 0.0001$, exigimos que $q \geq \exp(2^{2.77n})$ para todo $n \geq 6$. E isso prova o Teorema 67.

3.4 Três Elementos Consecutivos Primitivos

Para provar o Teorema 66, verificamos numericamente a existência de 3 elementos primitivos consecutivos para todo valor de q remanescente do Teorema 79. Como visto na seção anterior, para $n = 3$, precisamos apenas considerar os casos onde $\omega(q-1) \leq 13$. Para cada possível valor de $\omega(q-1)$ o Teorema 79 foi usado para para computar um limite do valor de q na qual a existência de elementos primitivos consecutivos não foi assegurado para $q \leq q_0(n)$. Esse limite é apresentado na segunda coluna da Tabela 3.3.

Algoritmo 7: Enumerar todos os inteiros ímpares $m+1$ tais que $m < M$ e $\omega(m) = w$. E então testar m+1 utilizando o Teorema 79.

```
1  Algoritmo1:= function(limit,w,L,J)
2  local A, C, j, d, aux, v1, v2, I, M, V, del;
3  aux:= 0; C:=[]; I:=[]; M:=[]; v2:=[]; v1:=[]; V:=[];
4  A:= Filtered([1,3..L],IsPrimePowerInt);
5  for i in [1..Size(A)] do
6  |  Add(v1,A[i]);
7  |  Add(v2,PrimeDivisors(A[i])[1]);
8  end
9  Add(v1,infinity); Add(v2,0);
10 for k in [1..J] do
11 |  M[1]:= 2^k; d:= 2; I:=[]; I[1]:= 1;
12 |  if  w = 1 then
13 |  |  if Teorema74(M[1],w) = false then
14 |  |  |  Add(V,M[1]+1);
15 |  |  end
16 |  else
17 |  |  I[2]:= 0; while d>1 do
18 |  |  |  while d=d do
19 |  |  |  |  I[d]:= I[d]+1;  j:= 2;
20 |  |  |  |  while  j<d and v2[I[j]] <> v2[I[d]] do
21 |  |  |  |  |  j:= j + 1;
22 |  |  |  |  end
23 |  |  |  |  if j=d then
24 |  |  |  |  |  break;
25 |  |  |  |  end
26 |  |  |  end
27 |  |  |  if M[d-1]*v1[I[d]]^(w + 1 - d) >= limit then
28 |  |  |  |  d:= d-1;
29 |  |  |  else
30 |  |  |  |  M[d]:= M[d-1]*v1[I[d]];
31 |  |  |  |  if d = w then
32 |  |  |  |  |  if Teorema74(M[d],w) = false then
33 |  |  |  |  |  |  Add(V,M[d]+1);
34 |  |  |  |  |  end
35 |  |  |  |  else
36 |  |  |  |  |  d:= d+1;  I[d]:= I[d-1];
37 |  |  |  |  end
38 |  |  |  end
39 |  |  end
40 |  end
41 end
42 return V;
43 end;
```

Algoritmo 8: Verificação do Teorema 79 para $m+1$ e w em questão. Esse algoritmo é chamado nas linhas 32 e 13 do Algoritmo 7.

```
1  Teorema5:= function(m,w)
2  local q, d, s, f;
3  q:= m+1; f:= PrimeDivisors(m);
4  for s in [0..w] do
5  |  d:= 1-3*Sum([0..s-1], x->1/f[w-x]);
6  |  if  (d > 0) and q >((3-1)*((3*s-1)/d+2)*2^(3*(w-s)))^2 then
7  |  |  return true;
8  |  end
9  end
10 return false;
11 end;
```

Algoritmo 9: Algoritmo utilizado para verificar a existência de três elementos consecutivos nos corpos cujas quais ordens falharam no teste do Teorema 79.

```
1  CsRoot3:= function(n)
2  local g;
3  g:= Z(n);
4  for i in [1..n-1] do
5  |  if (Order(g^i) = n-1) and (Order(g^i + 1) = n-1) and (Order(g^i + 2) =
   |   n-1) then
6  |  |  return true;
7  |  end
8  end
9  return false;
10 end;
```

Tabela 3.2: Valores de entrada para o Algoritmo 7

$\omega(q-1)=w$	M = limit	$L = M - 1/\prod_{i=1}^{w-1} p_i$	$J = \log(M-1)/\log(2)$
1	256	255	7
2	16 384	8191	13
3	802 816	133 801	19
4	31 719 424	1 057 313	24
5	368 212 715	1 753 393	28
6	9 777 432 663	4 232 653	33
7	48 913 046 416	1 628 805	35
8	3 273 635 059 78	641 247	38
9	6 245 429 709 655	643 879	42
10	22 053 999 260 750	98 855	44
11	117 121 857 096 884	18 103	46
12	1 307 042 588 523 590	6515	50
13	3 489 135 957 826 319	469	51

Tabela 3.3: Limites e números de testes realizados quando $n = 3$.

$\omega(q-1)$	Limite superior de q	m + 1 testes	m + 1 sobreviventes	Potência de primos
1	256	7	7	4
2	16 384	2425	805	172
3	802 816	172 827	21 350	4811
4	31 719 424	5 459 954	149 265	33 463
5	368 212 715	30 738 954	695 172	159 854
6	9 777 432 663	278 578 984	1 680 653	381 389
7	48 913 046 416	262 182 675	2 131 439	478 499
8	3 273 635 059 78	218 209 768	2 162 062	476 772
9	6 245 429 709 655	479 005 331	897 028	194 339
10	22 053 999 260 750	68 795 792	262 534	55 952
11	117 121 857 096 884	9 250 747	93 920	19 316
12	1 307 042 588 523 590	2 378 985	6566	1294
13	3 489 135 957 826 319	11 547	964	187

O Algoritmo 7 foi utilizado para construir os elementos $m + 1$ de forma que $m < M$ e $\omega(m) = w$ para $w \in \{1, \cdots, 13\}$. A quantidade desses elementos é mostrada na terceira coluna da Tabela 3.3. Ao criar esses elementos, utilizamos o Algoritmo 8 para ver se o Teorema 79 consegue lidar com $m + 1$, ou seja, se ele consegue garantir a existência de três elementos primitivos consecutivos e então retorne um conjunto com aqueles valores de $m + 1$ que falharam, ou seja, aqueles que são mostrados na coluna 4 da Tabela 3.3. Desses números que falharam, façamos uma filtragem daqueles que são potência de primos, ou seja, aqueles cujo os quais são permitidos ser ordem de um corpo finito. Sua quantidade é mostrada na quinta coluna da Tabela 3.3. Por fim, utilizamos o Algoritmo 9 para verificar quais dessas possíveis ordens de um corpo finito falha para a existência de três elementos primitivos. O resultado é precisamente os valores de $q \in \{3, 5, 9, 7, 13, 29, 25, 81, 61, 121, 169\}$ o que prova o Teorema 66.

O Algoritmo 7 levou cerca de 21h:30m para retornar os números que falharam no Teorema 79. O Algoritmo 9 levou cerca de 4h:45m para retornar as ordens que não possuem um trio de elementos primitivos consecutivos. Estes testes foram feitos utilizando o GAP na versão 4.11.0 de 29/Fev/2020 em um notebook Acer Nitro 5 AN515-51-50U2.

Referências Bibliográficas

[1] VEGH, E. Pairs of consecutive primitive roots modulo a prime. **Proc. Amer. Math. Soc.** Vol. 19. 1968.

[2] VEGH, E. A note on the distribution of the primitive roots of a prime. **Journal of Number Theory** 3.1 (1971): 13-18.

[3] COHEN, S. D. Consecutive primitive roots in a finite field. **Proceedings of the American Mathematical Society** (1985): 189-197.

[4] COHEN, S. D. Consecutive primitive roots in a finite field. II. **Proceedings of the American Mathematical Society** 94.4 (1985): 605-611.

[5] COHEN, S. D. Pairs of primitive roots. **Mathematika** 32 (1985) 276–285.

[6] BOOKER, A.; COHEN, S.; SUTHERLAND, N.; TRUDGIAN, T. Primitive values of quadratic polynomials in a finite field. **Mathematics of Computation.** 88.318 (2019): 1903-1912.

[7] WANG, P.; CAO, X.; FENG, R. On the existence of some specific elements in finite fields of characteristic 2. **Finite fields and their applications** 18.4 (2012): 800-813.

[8] COHEN, S. D. Pairs of primitive elements in fields of even order. **Finite Fields and Their Applications** 28 (2014): 22-42.

[9] COHEN, S. D; SHARMA, H.; SHARMA, R. Primitive values of rational functions at primitive elements of a finite field. **Journal of Number Theory** 219 (2021): 237-246.

[10] CARVALHO, C.; SOUZA, J.P.G.; NEUMANN V.G.L.; TIZZIOTTI G. On existence of some special pair of primitive elements over finite fields. **arXiv preprint arXiv:2002.01867** (2020).

[11] COHEN, S. D; OLIVEIRA E SILVA, T.; TRUDGIAN, T. On consecutive primitive elements in a finite field. **Bulletin of the London Mathematical Society** 47.3 (2015): 418-426.

[12] KENG, H. L. **Introduction to Number Theory**. Translated from the Chinese by Peter Shiu, Springer-Verlag, Berlin, 1982.

[13] LIDL R.; NIEDERREITER H. **Finite fields**. Cambridge university press; 1997.

[14] MARTINEZ, F. B.; MOREIRA, C. G.; SALDANHA, N.; TENGAN, E. **Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro**, 2010.

[15] SOUZA, D. J. **Álgebra com enfoque computacional - O sistema GAP.** Trabalho de Conclusão de Curso (Licenciatura em Matemática) - Departamento de Ciências Exatas, Universidade Federal de Lavras, 2018.

[16] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.11.0*; 2020, `https://www.gap-system.org`.

[17] FU, L.; WAN, D. A class of incomplete character sums. **Quart. J. Math**. 65 (2014): 1195–1211.

[18] COLÓQUIO BRASILEIRO DE MATEMÁTICA, 29. ANDRADE J. Introdução aos métodos de crivos em teoria dos números. IMPA 2013.

[19] SHARMA, R. K. Existence of some special primitive normal elements over finite fields. **Finite Fields and Their Applications** 46 (2017): 280-303.

[20] SHARMA, R. K.; AWASTHI, A.; GUPTA, A. Existence of pair of primitive elements over finite fields of characteristic 2. **Journal of Number Theory** 193 (2018): 386-394.

[21] CARLITZ, L. Sets of primitive roots. **Compositio Mathematica** 13 (1956): 65-70.

[22] TANTI, J.; THANGADURAI, R. Distribution of residues and primitive roots. **Proceedings-Mathematical Sciences** 123.2 (2013): 203-211.

[23] ROBIN, G. Estimation de la fonction de Tchebychef θ sur le k-i‘eme nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n, **Acta Arith.** 42 (1983) 367–389.