Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Somas Curtas de Caracteres e o Teorema de Burgess

por

Thiago Gonçalves Dias

Brasília
2009

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Somas Curtas de Caracteres e o Teorema de Burgess

por

Thiago Gonçalves Dias*

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de

MESTRE EM MATEMÁTICA

Brasília, 9 de julho de 2009.

Comissão Examinadora:

Prof. Dr. Nigel John Edward Pitt - UnB (Orientador)

Prof. Dr. Ivan Marques de Toledo Camargo - UnB (Membro)

Prof. Dr. Kenneth Dean McLaughlin - UnB (Membro)

*O autor foi bolsista CNPq durante a elaboração deste trabalho.

A minha filha Isabella Ferreira Gonçalves Dias,
a minha irmã Lívia Cristina Gonçalves Dias e ao meu avô Orcidino Gonçalves da Silva.

“Com organização e tempo, acha-se o segredo de fazer tudo e bem feito.”
Pitágoras.

Agradecimentos

Agradeço primeiramente a DEUS, se não fosse por ele não teria alcançado essa conquista.

Aos meus pais, Mantoel Dias Rocha e Rosa Helena Gonçalves Silva Rocha, pela compreensão e apoio ininterruptos, por mesmo estando a quilômetros de distância, se fizeram próximos. Obrigado, amo muito vocês!

A Dayanne , meu amor, pelo companheirismo, compreensão, e por toda a ajuda nos diversos momentos difíceis que passamos juntos, noites sem dormir, mas tudo isso nos tornou vencedores.

A minha pequena, Isabella, que me fez forte e confiante para lutar por esse sonho. Tudo o que fiz e ainda vir a fazer é por você e para você minha filha!! Você é tudo, tudo, tudo para o papai!!!

Ao meu orientador, professor Dr. Nigel Pitt, pela orientação, paciência e pela forma sempre respeitosa com que me tratou e chamou minha atenção quando necessário. Aprendi muito com você professor!!

Ao professor Dr. Hemar Godinho pelas considerações feitas, ao professor Dr. Ivan Marques e ao professor Dr. Kenneth McLaughlin, por tamanho interrese em meu trabalho e pelas importantes conversas que tivemos, meu muito obrigado.

A todos do departamento de matemática que me acompanharam e ajudaram durante todo esse período.

Aos professores da UFG/CAJ, em Jataí, pela minha formação como professor de matemática. Vocês, Jaqueline Araújo, Iron Felisberto, Claudiney Goulart, e principalmente Fabiano Fortunato, muitissímo obrigado por todo o incentivo e créditos dados a mim.

Agradeço todos que se alegraram com minha conquista, aos que torceram por mim, amigos, familiares, colegas, e peço desculpas se esqueci de citar algum nome aqui, mais tenham certeza, estão todos em meu coração.

Resumo

Neste trabalho estudamos somas incompletas de caracteres e como estimar estas usando métodos analíticos para relacioná-las com somas completas associadas, para as quais existem métodos de estimação vindos de geometria algébrica. Estabelecemos um método analítico geral para completar somas, e mostramos que o método falha para somas mais curtas que $q^{1/2}$, que é uma barreira natural. Em seguida mostramos como ultrapassar esta barreira no caso mais clássico, que resulta no Teorema de Burgess.

Palavras-chave: Somas de Caracteres, Somas Incompletas, Teorema de Burgess.

Abstract

In this work we study incomplete character sums and how to estimate these using analytic methods to relate with associated complete sums, for which them exist estimation methods from algebraic geometry. We establish a general analytic method to complete sums, and show that the method fails for sums shorter than $q^{1/2}$ which is a natural barrier. We then show how to pass this of barrier in the most classical case, which leads to Burgess's Theorem.

Keywords: Character Sums, Incomplete Sums, Burgess's Theorem.

Sumário

Introdução

Dada qualquer função oscilatória $a(n)$, digamos com $|a(n)| \leq 1$, é natural perguntar qual o tamanho da soma

$$\sum_{n=N+1}^{N+H} a(n) \ ,$$

isto é, se existe uma estimativa menor que a trivial de $O(H)$. Exemplos incluem caracteres multiplicativos $a(n) = \chi(n)$ ou aditivos $a(n) = \psi(n)$, ou mais geralmente os produtos

$$a(n) = \chi(P(n))\psi(Q(n))$$

onde P e Q são funções apropriadas. São estes exemplos que vamos expor nesta dissertação. É importante ressaltar que o intervalo de soma é independente do módulo q dos caracteres; e que nosso tema envolve intervalos de comprimento H que são mais curtos de q, em geral.

O objetivo nessa dissertação é apresentar métodos de completar somas envolvendo caracteres, como as descritas acima. Por somas incompletas entendemos somas que não estão sobre todos os inteiros módulo q e quando dizemos completar somas, estamos nos referindo à relacioná-las com somas completas do mesmo tipo. Sendo assim, para conseguir estimar as somas incompletas, precisamos de meios para estimar somas completas, uma vez que estas serão relacionadas.

Para completar somas vamos usar conceitos analíticos, no entanto, para estimar as somas completas relacionadas à estas, vamos trabalhar com conceitos algébricos geométricos.

No primeiro capítulo vamos trabalhar com alguns conceitos preliminares e dois Teoremas tratados em Schmidt ([4]), que são bem gerais no que diz respeito a estimativa de somas completas, vamos demonstrar apenas um destes, e para isso será discutido conceitos de geometria algébrica, onde vamos relacionar as somas completas com as L-funções de Dirichlet definidas

por

$$L(S,\chi) = \sum_n \frac{\chi(n)}{n^s},$$

através de propriedades destas; escreva $s = \sigma + it$, um número complexo qualquer.

Não está no objetivo desta dissertação entrar em detalhes de como fica estabelecida à relação entre essas L-funções e a Hipótese de Riemann para curvas sobre corpos finitos, a saber

$$N_\nu - q^\nu \ll q^{\nu/2},$$

onde N_ν representa o número de soluções de $Y^d = P(X)$, mais vamos usar este fato.

No que segue apresentamos um método bastante geral de completar somas definidas como

$$S(N,H) = \sum_{n=N+1}^{N+H} \chi(P(n))\psi(Q(n)),$$

usando análise harmônica, onde $q^{1/2} < H < q$: ou seja um intervalo relativamente curto. Consideramos casos particulares de $P(n)$ e $Q(n)$ para ilustrar a partir deste metódo, o Teorema de Pólya e Vinogradov, e a partir do que foi estudado até aqui percebemos que $q^{1/2}$ é uma barreira para este método.

Logo após consideramos a soma quando $P(n) \equiv n$ e $Q(n) \equiv 0$ para mostrar que

$$S(N,H) = \sum_{n=N+1}^{N+H} \chi(n) \ll H^{1-\frac{1}{k}} q^{\frac{k+1}{4k^2}+\varepsilon}$$

onde $H < q^{1/2}$ e a constante implícita depende de k e ε, este é o Teorema de Burgess, e neste precisamos de alguma maneira para criar uma outra variável apropriada(definida em um intervalo "mais comprido"), para completar a soma, e a necessidade e suficiência de termos $H \gg q^{1/4+\delta}$. Faremos estas discuções para q primo, o que é suficiente para ilustrar estes resultados.

Capítulo 1

Preliminares

1.1 Caracteres

Para qualquer $q \in \mathbb{N}$, um caracter multiplicativo módulo q é um homomorfismo

$$\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$$

estendido a ser uma função $\chi : \mathbb{Z} \to \mathbb{C}$ por periodicidade módulo q e a convenção que $\chi(n) = 0$ se $(n,q) > 1$. Observe que se q' é multiplo de q, então χ induz um caracter χ' módulo q', por

$$\chi'(n) = \begin{cases} \chi(n) & \text{se } (n,q') = 1 \\ 0 & \text{se } (n,q') > 1 \end{cases}$$

(ver [5]) Quando $\chi(n) = 1$ para todo n, $(n,q) = 1$, chamamos este de caracter principal ou trivial, e o denotamos por χ_0. Um caracter $\chi(n)$ é dito primitivo quando não está induzido por um caracter de módulo menor, ou seja, se para qualquer divisor D de q, $0 < D < q$, existir algum inteiro a tal que

$$a \equiv 1 (\mathrm{mod}\, D), \quad (a,q) = 1, \quad \chi(a) \neq 1,$$

Caracteres multiplicativos deste tipo são chamados de caracteres de Dirichlet.

Por exemplo se q é primo, então qualquer caracter não principal módulo q é primitivo, pois o único divisor que satisfaz a condição acima é $D = 1$. Enquanto que para $q > 1$, o caracter principal módulo q é impróprio, pois 1 é um divisor de q. Um caracter é dito impróprio quando não é primitivo.

Um exemplo de um caracter é o símbolo de Legendre $\left(\frac{n}{q}\right)$, definido para módulos primos q. Este caracter é definido a ser ± 1, conforme n é ou não é resíduo quadrático módulo q. (Lembramos que n é resíduo quadrático módulo q se a congruência $x^2 \equiv n(\mathrm{mod}\, q)$ tiver solução, caso contrário, dizemos que n é um não-resíduo quadrático módulo q.) Que $\chi(n) = (n/q)$ realmente é um caracter é conseqüência da fórmula

$$\left(\frac{n}{q}\right) \equiv n^{\frac{q-1}{2}} (\mathrm{mod}\, q),$$

(que por sua vez é conseqüência do pequeno teorema de Fermat; que

$$n^{q-1} \equiv 1(\mathrm{modq}),$$

para $(n,q) = 1$ e a definiçãoo de resíduo quadrático.) Logo se $(ab,q) = 1$ tem-se

$$\left(\frac{ab}{q}\right) = \left(\frac{a}{q}\right)\left(\frac{b}{q}\right).$$

Os caracteres de qualquer grupo abeliano multiplicativo G formam um grupo, onde o elemento identidade será representado pelo caracter principal χ_0, e o elemento inverso é dado por χ^{-1}, que definimos como $\chi^{-1}(x) = \overline{\chi}(x)$. Para χ_1 e χ_2 caracteres de G, definimos a aplicação $\chi_1\chi_2$ por $(\chi_1\chi_2)(x) = \chi_1(x)\chi_2(x)$. Este grupo de caracteres será denotado por G'. Em relação as grupos G e G', temos o seguinte resultado.

Teorema 1.1. *Dado um grupo finito abeliano G, seu grupo G' de caracteres é isomorfo a G. ([4])*

Um dos resultados preliminares que envolvem caracteres, mais especificamente, somas de caracteres, é o seguinte teorema.

Teorema 1.2. *Seja G um grupo abeliano finito de ordem $|G|$.*

$$\sum_{x\in G} \chi(x) = \begin{cases} |G| & se\ \ \chi = \chi_0 \\ 0 & se\ \ \chi \neq \chi_0 \end{cases} \qquad \sum_{\chi\in G'} \chi(x) = \begin{cases} |G| & se\ \ x = 1 \\ 0 & se\ \ x \neq 1 \end{cases}$$

Demonstração: No caso $\chi = \chi_0$ o resultado segue de estarmos somando sobre todos os elementos de G. Mais se $\chi \neq \chi_0$, então existe $x_1 \in G$ com $\chi(x_1) \neq 1$. Como x percorre todos elementos

de G, o mesmo acontece para xx_1, por isso

$$S = \sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(xx_1) = \chi(x_1) \sum_{x \in G} \chi(x) = \chi(x_1)S.$$

Donde $S = 0$.

A primeira igualdade do segundo item segue do fato de G e seu grupo de caracteres serem isomorfos. Para estabelecermos a segunda igualdade vamos considerar a função x' dada por $x'(\chi) = \chi(x)$ para $\chi \in G'$, assim $x' \in G'$. Agora do item anterior aplicado para o grupo de caracteres temos,

$$\sum_{\chi \in G'} \chi(x) = \sum_{\chi \in G'} x'(\chi) = 0$$

. □

1.2 Somas de Gauss

Quando são trabalhados meios de completar uma soma, é natural pensar em como estima-lá após terminado o completamento. Dentre as somas completas que irão surgir no decorrer desta dissertação, estão as somas de Gauss, que definimos para qualquer caracter χ módulo q, como

$$G(n, \chi) = \sum_{m=1}^{q} \chi(m) e_q(mn), \tag{1.1}$$

dizemos que essas somas de Gauss são associadas à χ, a notação $e_q(mn)$ representa a exponencial $e^{2\pi imn/q}$. Escreveremos ainda

$$\tau(\chi) = G(1, \chi). \tag{1.2}$$

Já definimos o complexo conjugado de um caracter χ, assim $|\chi(n)|^2 = \chi(n)\overline{\chi}(n) = 1$ e daí para qualquer r tem-se

$$\chi(r) = \overline{\chi}(n)\chi(n)\chi(r) = \overline{\chi}(n)\chi(nr).$$

Quando r percorre um sistema completo de resíduos módulo q, o mesmo acontece com nr, sempre que $(n, q) = 1$, conseqüentemente a soma (1.1) pode ser escrita como segue

$$\begin{aligned} G(n,\chi) &= \sum_{r \pmod q} \chi(r) e^{2\pi i n r/q} = \overline{\chi}(n) \sum_{r \pmod q} \chi(nr) e^{2\pi i n r/q} \\ &= \overline{\chi}(n) \sum_{m \pmod q} \chi(m) e^{2\pi i m/q} = \overline{\chi}(n)\tau(\chi) \end{aligned}$$

assim acabamos de demonstrar o resultado que se segue, e que será importante no desenvolvimento subseqüente.

Teorema 1.3. *Seja χ um caracter módulo q, então*

$$G(n,\chi) = \begin{cases} \overline{\chi}(n)\tau(\chi), & se \quad (n,q) = 1 \\ 0, & se \quad (n,q) > 1. \end{cases}$$

Observe que do Teorema (1.2), temos que as somas de Gauss são nulas se um dos caracteres envolvidos é principal e o outro não. A estimativa menos trivial das somas de Gauss, é o caso em que ambos os caracteres multiplicativo e aditivo são não triviais e $n = 1$.

Teorema 1.4. *Seja χ um caracter módulo q não principal, então*

$$|\tau(\chi)|^2 = q.$$

Demonstração: Temos que:

$$|\tau(\chi)|^2 = \tau(\chi)\overline{\tau(\chi)} = \tau(\chi) \sum_{m=1}^{q} \overline{\chi}(m) e^{-2\pi i m/q}$$

passando $\tau(\chi)$ para dentro do somatório e em vista do Teorema (1.3),

$$\begin{aligned} |\tau(\chi)|^2 &= \sum_{m=1}^{q} G(m,\chi) e^{-2\pi i m/q} \\ &= \sum_{m=1}^{q} \sum_{r=1}^{q} \chi(r) e^{2\pi i m r/q} e^{-2\pi i m/q} \\ &= \sum_{r=1}^{q} \chi(r) \sum_{m=1}^{q} e^{2\pi i m(r-1)/q}. \end{aligned}$$

Da soma geométrica interior obtemos;

$$\sum_{m=1}^{q} e^{2\pi i m(r-1)/q} = \begin{cases} 0 & \text{se } q \nmid (r-1) \\ q & \text{se } q \mid (r-1), \end{cases}$$

ou seja, a soma sobre m é 0 a não ser que $q \mid (r-1)$. Mas $|r-1| \leq q$, portanto $q \mid (r-1)$ se, e só se , $r = 1$. Conseqüentemente o único termo que não é nulo acontece quando $r = 1$, então

$$|G(1,\chi)|^2 = q\chi(1) = q.$$

□

Quando χ é um caracter principal e $n \equiv 0 (\mathrm{mod}\, q)$, isto é, o caracter aditivo envolvido também e trivial, as somas de Gauss são:

$$G(n,\chi) = q.$$

Como o símbolo de Legendre é um caracter, podemos escrever a somas de Gauss da seguinte forma:

$$G\left(n, \left(\frac{\cdot}{q}\right)\right) = \sum_{m=1}^{q} \left(\frac{m}{q}\right) e^{2\pi i m n/q} = \sum_{m=1}^{q} \left\{ \left(\left(\frac{m}{q}\right) + 1 \right) \right\} e^{2\pi i m n/q} - \sum_{m=1}^{q} e^{2\pi i m n/q},$$

com $(n,q) = 1$, e então a última soma é igual a zero. Se m for um não-resíduo quadrático módulo q, $G(n,\chi) = 0$. Por outro lado, se m é um resíduo quadrático módulo q, obtemos

$$G\left(n, \left(\frac{\cdot}{q}\right)\right) = 2 \sum_{m=1}^{q} e^{2\pi i m n/q} = \sum_{x=1}^{q} e^{2\pi i x^2 n/q},$$

que é a fórmula que foi inicialmente considerada por Gauss.

1.3 Somas de Caracteres associadas à Corpos Finitos

Seja $\mathbb{F}_p$ o corpo com p elementos, p primo. O grupo multiplicativo então é $\mathbb{F}_p^* \cong (\mathbb{Z}/p\mathbb{Z})^*$, logo os caracteres de Dirichlet já definidos, podem ser vistos como caracteres multiplicativos $\chi : \mathbb{F}_p^* \to \mathbb{C}^*$. De forma análoga um caracter aditivo de $\mathbb{F}_p$ é um homomorfismo do grupo

aditivo de $\mathbb{F}_p$ sobre o corpo dos números complexos, vamos denotar este tipo de caracter por ψ. Quando for $\psi(x) = 1$, para qualquer x, diremos que este caracter aditivo é principal e escrevemos $\psi = \psi_0$.

Agora, vamos ampliar este conceito aos demais corpos finitos. No que se segue, $\mathbb{F}_q$ é um corpo finito cuja ordem é potência de um número primo p, ou seja, $q = p^\nu$, onde p é a característica do corpo.

Pode-se estender a definição de caracter multiplicativo à $\mathbb{F}_q$ em vez de $\mathbb{F}_q^*$, se necessário, pondo

$$\chi(0) = \begin{cases} 0 & \text{se } \chi \neq \chi_0, \\ 1 & \text{se } \chi = \chi_0. \end{cases}$$

Podemos também, trabalhar a noção de caracteres multiplicativos e aditivos da extensão $\mathbb{F}_{q^\nu}$ de $\mathbb{F}_q$, usando duas importantes funções entre o corpo finito $\mathbb{F}_{q^\nu}$ e seu subcorpo principal $\mathbb{F}_q$, que são o traço e a norma.

A função traço $\mathscr{T}_\nu : \mathbb{F}_{q^\nu} \to \mathbb{F}_q$ de x é dada por

$$\mathscr{T}_\nu(x) = x^{q^0} + x^q + \ldots + x^{q^{\nu-1}},$$

enquanto a norma $\mathscr{N}_\nu : \mathbb{F}_{q^\nu} \to \mathbb{F}_q$ de x é dada por

$$\mathscr{N}_\nu(x) = x^{q^0} \cdot x^q \cdot \ldots \cdot x^{q^{\nu-1}},$$

onde x^{q^0}, x^q, $x^{q^2}, \ldots,$ $x^{q^{\nu-1}}$ são as imagens de x sob a ação do grupo de Galois, ou seja, os conjugados de x em relação à $\mathbb{F}_q$. Note que o traço de um elemento x sobre $\mathbb{F}_q$ é obtido a partir da soma dos seus conjugados, enquanto a norma é dada pelo produto desses conjugados.

Da aditividade da função traço e da multiplicatividade da função norma, podemos definir caracteres χ_ν e ψ_ν como caracteres multiplicativo e aditivo respectivamente do corpo de extensão $\mathbb{F}_{q^\nu}$, dados χ, ψ em $\mathbb{F}_q$. Para isso, pomos

$$\chi_\nu(x) = \chi(\mathscr{N}_\nu(x)) \qquad \text{para } x \in {\mathbb{F}^*}_{q^\nu}$$

e

$$\psi_\nu(x) = \psi(\mathscr{T}_\nu(x)) \qquad \text{para } x \in \mathbb{F}_{q^\nu},$$

onde $\mathscr{N}_\nu$ e $\mathscr{T}_\nu$ são funções norma e traço de $\mathbb{F}_{q^\nu}$ sobre $\mathbb{F}_q$.

Antes de prosseguir, vale ressaltar um resultado a cerca de um número de soluções de um determinado polinômio sobre um corpo de extensão, a saber

Teorema 1.5. *Seja $f \in \mathbb{F}_q[x]$, de grau $n \geq 0$. Então a equação $f(x) = 0$ tem no máximo n soluções em $\mathbb{F}_q[x]$ e em qualquer extensão deste corpo.([7])*

Como os caracteres multiplicativos de um corpo finito $\mathbb{F}_q$ formam um grupo cíclico, vão atender a $\chi^{q-1} = \chi_0$. Dizemos que χ é de ordem d se $\chi^d = \chi_0$ e se d é o menor inteiro positivo com está propriedade. Dizemos que χ tem expoente d, caso este não seja o menor inteiro positivo tal que $\chi^d = \chi_0$.

1.4 Hipótese de Riemann para Curvas sobre Corpos Finitos

Como já mencionado, é importante ter ferramentas para trabalhar a estimativa de uma soma completa, tendo sido ela obtida a partir de uma soma incompleta, se não de nada adiantaria relacionar somas incompletas com somas completas do mesmo tipo. Nesta seção são discutidos dois Teoremas de Schmidt([4]) a respeito de somas completas, que são

Teorema 1.6. *Seja χ um caracter multiplicativo de ordem $d > 1$. Suponha que $P(x) \in \mathbb{F}_q[x]$ tem m zeros distintos entre suas raízes, e que não é uma d-ésima potência. Então*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(P(x)) \right| \leq (m-1)q^{1/2}.$$

O segundo e mais geral, que envolve caracteres multiplicativo e aditivo simultaneamente, é o

Teorema 1.7. *Seja χ, ψ respectivamente, um caracter multiplicativo de ordem d com $d \mid (q-1)$ e um caracter aditivo de $\mathbb{F}_q$, ambos não triviais. Sejam $P(x) \in \mathbb{F}_q[X]$ com precisamente m raízes distintas, e $Q(x) \in \mathbb{F}_q[X]$ de grau n. Suponha que $(d, \text{grau de} P) = (n,q) = 1$. Então*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(P(x))\psi(Q(x)) \right| \leq (m+n-1)q^{1/2}.$$

Vamos considerar o Teorema (1.6) em detalhes, vendo que supor a Hipótese de Riemann para curvas é crucial para tal resultado. A demonstração do Teorema (1.7) segue de maneira similar, mas não pretendemos entrar em detalhes.

Para estudar a soma do Teorema (1.6), vamos relacioná-la com a L-função relacionada à curva do tipo $Y^d - P(X)$, onde d é o expoente do caracter envolvido. Para definir esta L-função, começamos com o polinômio $P(X)$, visto que este por hipótese tem m raízes distintas, em alguma extensão de $\mathbb{F}_q$, ele pode ser fatorado e, então escrito na forma

$$P(X) = (X+\gamma_1)^{\alpha_1} \cdot \ldots \cdot (X+\gamma_m)^{\alpha_m},$$

onde $\gamma_1, \ldots, \gamma_m$ pertencem ao fecho algébrico de $\mathbb{F}_q$.

Consideramos agora, o conjunto de valores

$$\{r\} = r(\gamma_1)^{\alpha_1} \cdot \ldots \cdot r(\gamma_m)^{\alpha_m}, \tag{1.3}$$

onde cada r é uma função racional da forma h_1/h_2, onde h_1, h_2 são polinômios mônicos que não se anulam em $\gamma_1, \ldots, \gamma_m$. Sendo assim, $\{r\} \neq 0$, como $\{r\} \in \mathbb{F}_q$ e usando a multiplicatividade de χ, vemos que

$$\chi(\{r_1 r_2\}) = \chi(\{r_1\})\chi(\{r_2\}).$$

Seja G o grupo das funções racionais h_1/h_2, com h_1 e h_2 polinômios mônicos em $\mathbb{F}_q$, e H um subgrupo tal que se $h_1 h_2 \in H$, então h_1 e $h_2 \in H$. Se pormos

$$\mathscr{X}(r) = \chi(\{r\}), \tag{1.4}$$

$\mathscr{X}$ será um caracter de H. Quando for necessário podemos estender este conceito, pondo $\mathscr{X}(h) = 0$ se h não pertencer à H. Usando este $\mathscr{X}$, podemos definir para cada $s = \sigma + it$, podemos definir

$$L(s, \mathscr{X}) = \sum_h \mathscr{X}(h)\mathbf{N}(h)^{-s}. \tag{1.5}$$

onde $\mathbf{N}(h) = q^d$ se d é o grau de h, e h é mônico com coeficientes em $\mathbb{F}_q$. As L-funções definidas acima tem expansão em produto de Euler, isto é, para $\sigma > 1$,

$$L(s, \mathscr{X}) = \prod_{h \text{irredutvel}} (1 - \mathscr{X}(h)\mathbf{N}(h)^{-s})^{-1}. \tag{1.6}$$

Considere $\{h_j\}_{j=1}^{\infty}$, o conjunto de todos os polinômios irredutíveis em $\mathbb{F}_q$. Qualquer polinômio $h \in \mathbb{F}_q$, pode ser escrito de modo único como potências de polinômios irredutíveis, digamos

$$h = h_1^{a_1} \cdot h_2^{a_2} \cdot \ldots \cdot h_k^{a_k}.$$

Usando meios análogos aos usados para mostrar que a função zeta de Riemann admite produto de Euler, vamos mostrar (1.6).

Para começar observe que da característica multiplicativa do caracter $\mathscr{X}$ e de $\mathbf{N}$, subtraindo de $L(s,\mathscr{X})$, o produto $\mathscr{X}(h_1)\mathbf{N}(h_1)^{-s}L(s,\mathscr{X})$, obtemos

$$\begin{aligned}\left(1-\mathscr{X}(h_1)\mathbf{N}(h_1)^{-s}\right)L(s,\mathscr{X}) &= \sum_{h}\left(1-\mathscr{X}(h_1)\mathbf{N}(h_1)^{-s}\right)\mathscr{X}(h)\mathbf{N}(h)^{-s}\\ &= \sum_{h}\mathscr{X}(h)\mathbf{N}(h)^{-s}-\sum_{h}\left(\mathscr{X}(h_1h)\mathbf{N}(h_1h)^{-s}\right)\\ &= \sum_{\substack{h\\(h_1,h)=1}}\mathscr{X}(h)\mathbf{N}(h)^{-s},\end{aligned}$$

pois subtraimos do conjunto dos polinômios h, todos aqueles que são divisíveis por h_1. Agora, multiplicando o resultado anterior por $\mathscr{X}(h_2)\mathbf{N}(h_2)^{-s}$, e este resultado, subtraindo de (1.5), tem-se

$$\begin{aligned}\prod_{i=1}^{2}\left(1-\mathscr{X}(h_i)\mathbf{N}(h_i)^{-s}\right)L(s,\mathscr{X}) &= \sum_{\substack{h\\(h_1,h)=1}}\mathscr{X}(h)\mathbf{N}(h)^{-s}-\sum_{\substack{h\\(h_1,h)=1}}\left(\mathscr{X}(h_1h_2h)\mathbf{N}(h_1h_2h)^{-s}\right)\\ &= \sum_{\substack{h\\(h_1h_2,h)=1}}\mathscr{X}(h)\mathbf{N}(h)^{-s}.\end{aligned}$$

Seguindo este raciocínio sucessivas vezes, obtemos

$$\prod_{1\leq i\leq k}\left(1-\mathscr{X}(h_i)\mathbf{N}(h_i)^{-s}\right)L(s,\mathscr{X})=\sum_{\substack{h\\(h_1h_2\ldots h_k,h)=1}}\mathscr{X}(h)\mathbf{N}(h)^{-s}.$$

Conseqüentemente

$$L(s,\mathscr{X})=\prod_{1\leq i\leq k}\left(1-\mathscr{X}(h_i)\mathbf{N}(h_i)^{-s}\right)^{-1}\cdot\sum_{\substack{h\\(h_1h_2\ldots h_k,h)=1}}\mathscr{X}(h)\mathbf{N}(h)^{-s},$$

para qualquer k. Afirmamos que no limite não sobra nenhum h na série, pois quando k é suficientemente grande, continuando com o método descrito acima, teremos subtraído todos os fatores da decomposição de h. Logo

$$L(s,\mathscr{X}) = \prod_{h \text{ irred.}} \left(1 - \mathscr{X}(h)\mathbf{N}(h)^{-s}\right)^{-1}.$$

Para analisar $L(s,\mathscr{X})$ com mais detalhes, abrimos o somatório, de acordo com o grau do polinômio h, isto é

$$L(s,\mathscr{X}) = \sum_{\substack{h \\ \textit{grau de } h=0}} \mathscr{X}(h)\mathbf{N}(h)^{-s} + \sum_{\substack{h \\ \textit{grau de } h=1}} \mathscr{X}(h)\mathbf{N}(h)^{-s} + \sum_{\substack{h \\ \text{grau de } h=2}} \mathscr{X}(h)\mathbf{N}(h)^{-s} + \ldots.$$

Lembrando que $\mathbf{N}(h) = q^d$, onde d é o grau de h, o primeiro termo da soma acima, sobre os h de grau zero, é igual a 1, pois h é mônico, logo

$$L(s,\mathscr{X}) = 1 + \sum_{\substack{h \\ \textit{grau de } h=1}} \mathscr{X}(h)q^{-s} + \sum_{\substack{h \\ \textit{grau de } h=2}} \mathscr{X}(h)q^{-2s} + \ldots.$$

Introduzimos a notação $\mathscr{U} = q^{-s}$ e

$$\zeta_t = \sum_{\substack{h \\ \textit{grau de } h=t}} \mathscr{X}(h), \tag{1.7}$$

daí a equação acima se torna

$$L(s,\mathscr{X}) = 1 + \zeta_1\mathscr{U} + \zeta_2\mathscr{U}^2 + \ldots. \tag{1.8}$$

As somas ζ_t dadas em (1.7) vão refletir no nosso propósito, por meio de propriedades que veremos posteriormente. Primeiro note que a priori a soma em (1.8) pode ter uma infinidade de termos.

Queremos relacionar a soma do teorema (1.6) com as L-funções. Os resultados e considerações seguintes vão servir para mostrar que a soma acima tem na verdade um número finito de termos e que um de seus coeficientes é a soma em que estamos interessados.

Seja $\overline{H}$ o subgrupo de G, formado por elementos da forma $h_1(x)/h_2(x)$, que satisfazem as

condições

$$h_1(x) = \sum_{i=0}^{k} a_i x^{k-i} \quad \text{e} \quad h_2(x) = \sum_{j=0}^{v} c_j x^{v-j}$$

com $a_1 = c_1, \ldots, a_n = c^n$. Observe que em h_1 e h_2 existem os termos a_0 e c_0, mas estes são ambos iguais a 1, visto que h_1 e h_2 são mônicos.

Considere ainda, o subgrupo $\overline{\overline{H}}$ de H, consistindo de funções $r(x) = h_1/h_2$ com $h_1(\gamma i) = h_2(\gamma i)$, e ambos não se anulam em γi para $i = 1, \ldots, m$.

A partir destas dois subgrupos, $\overline{H}$ e $\overline{\overline{H}}$ de H vamos definir um terceiro, pondo $H' = \overline{H} \cap \overline{\overline{H}}$, para trabalhar alguns resultados que envolvem os elementos das classes laterais de H' em H.

Teorema 1.8. *Suponha $l \geq 0$. Então toda classe lateral de H' em H contem exatamente q^l polinômios de grau $m+l$.*

Teorema 1.9. *Suponha que χ é um caracter não principal de expoente d e $Y^d - P(X)$ absolutamente irredutível. Então o caracter $\mathscr{X}$ é não principal.*

Demonstração: Como definimos o caracter $\mathscr{X}$ pondo

$$\mathscr{X}(u) = \chi(\{u\}),$$

então é suficiente mostrar que existe $u \in H$ tal que $\chi(\{u\}) \neq 1$.

Por ser χ um caracter não trivial, suponha que ele tem ordem o, e portanto o/d, e como o polinômio $Y^d - P(X)$ é absolutamente irredutível, pelo menos um dos expoentes $\alpha_1, \ldots, \alpha_m$ não é múltiplo de o. Digamos então que α_i seja tal elemento, dessa forma dados $b_2, \ldots, b_m \in \mathbb{F}_q$, existe $b_1 \in \mathbb{F}_q^*$ tal que o elemento $b_1^{\alpha_1} b_2^{\alpha_2} \cdot \ldots \cdot b_m^{\alpha_m}$ não é uma o-ésima potência não nula, e portanto $\chi(b_1^{\alpha_1} b_2^{\alpha_2} \cdot \ldots \cdot b_m^{\alpha_m}) \neq 1$. Como os elementos $b_1, \ldots, b_m$ estão em $\mathbb{F}_q^*$ e $u(x) \in \mathbb{F}_q[x]$, tal que $u(\gamma_i) = b_i$ para $i = 1, \ldots, m$. (ver [4]).

Portanto $\{u\} = b_1^{\alpha_1} b_2^{\alpha_2} \cdot \ldots \cdot b_m^{\alpha_m}$, e o resultado segue. □

Teorema 1.10. *Suponha que χ é um caracter não principal de expoente d e que $Y^d - P(X)$ é absolutamente irredutível. Suponha ainda $l \geq 0$, então*

$$\sum_{\substack{h \in H \\ h \text{ pol.mônico} \\ \text{grau de } h = m+l}} \mathscr{X}(h) = 0$$

.

Demonstração: O subgrupo $H' = \overline{H} \cap \overline{\overline{H}}$ é tal que se $r \in H'$ então $\mathscr{X}(r) = 1$, pela definição de $\overline{\overline{H}}$, e pelo teorema anterior, vimos que $\mathscr{X}$ é um caracter não principal de H, conseqüentemente $\mathscr{X}$ é um caracter não trivial sobre os elementos do grupo finito H/H'.

Além disso, como h percorre todos os polinômios de grau $m+l$, segue do teorema (1.8) que cada classe lateral deH/H' terá q^l polinômios, como estes são todos os polinômios, o teorema segue do Teorema (1.2).

□

Com o resultado obtido no Teorema (1.10), temos que a expressão dada em (1.8) é nula quando $t \geq m$, conseqüentemente a expressão (1.8) se torna

$$L(s, \mathscr{X}) = 1 + \zeta_1 \mathscr{U} + \ldots + \zeta_{m-1} \mathscr{U}^{m-1}, \tag{1.9}$$

o que prova a primeira parte do próximo Teorema.

Teorema 1.11. *Seja $\chi \neq \chi_0$ um caracter de expoente d com (grau de P, d) $= 1$. Sendo m o número de zeros distintos de $P(X)$ e pondo $\mathscr{U} = q^{-s}$, temos*

$$L(s, \mathscr{X}) = 1 + \zeta_1 \mathscr{U} + \ldots + \zeta_{m-1} \mathscr{U}^{m-1}.$$

Se $\chi \neq \chi_0$ ou se $\chi = \chi_0$ com $P(X) = 1$, então

$$\zeta_1 = \sum_{x \in F_q} \chi(P(X)).$$

Demonstração:

Que $L(s, \mathscr{X})$ é um polinômio em $\mathscr{U}$ de grau no máximo $m-1$, já foi provado. Observe que, a segunda parte, se resume em escrever a soma dada no Teorema (1.6) como ζ_1, mas

$$\zeta_1 = \sum_{\substack{h \in H \\ \text{grau de } h1}} \mathscr{X}(h) = \sum_x \mathscr{X}(X + x),$$

daí por (1.4) tem-se

$$\sum_x \mathscr{X}(X + x) = \sum_x \chi(\{X + x\}) = \sum_x \chi((\gamma_1 + x)^{\alpha_1} \ldots (\gamma_m + x)^{\alpha_m}),$$

que, como dito anteriormente, é a fatorização de $P(x)$, logo

$$\sum_{\substack{x \\ P(x)\neq 0}} \chi(P(x)) = \sum_{x} \chi(P(x)).$$

□

Estamos interessados na prova do Teorema (1.6) não apenas no corpo $\mathbb{F}_q$, queremos algo mais geral, isto é, mostrar que o resultado segue também, em qualquer extensão finita $\mathbb{F}_{q^\nu}$ de $\mathbb{F}_q$. Para isso vamos fazer considerações análogas as já feitas, e de alguma maneira, através de propriedades e teoremas relacioná-los.

Como já observado no tópico 1.3, podemos estender o conceito de caracter para a extensão $\mathbb{F}_{q^\nu}$, pondo

$$\chi_\nu(x) = \chi(\mathscr{N}_\nu(x)) \quad \text{e} \quad \psi_\nu(x) = \psi(\mathscr{T}_\nu(x))$$

respectivamente para definir o caracter multiplicativo e aditivo de $\mathbb{F}_{q^\nu}$.

Com a fatorização de um polinômio é única ainda temos para $P(X) \in \mathbb{F}_q[X]$,

$$P(X) = (X+\gamma_1)^{\alpha_1} \cdot \ldots \cdot (X+\gamma_m)^{\alpha_m},$$

no fecho algébrico de $\mathbb{F}_q[X]$. Seja G_ν o grupo das funções racionais $r(x) = h_1(x)/h_2(x)$, onde h_1, h_2 mônicos, agora estão em $\mathbb{F}_{q^\nu}$.

Os outros conjuntos, H_ν, $\overline{H}_\nu$, $\overline{\overline{H}}_\nu$ e H' são definidos como os ja trabalhados no corpo principal $\mathbb{F}_q$, e $\{r\}$ será como em (1.3), logo podemos definir o caracter de H_ν, pondo

$$\mathscr{X}_\nu(r) = \chi_\nu(\{r\}).$$

Com o caracter definido acima, podemos definir as L-funções associados ao corpo $\mathbb{F}_{q^\nu}$, pondo

$$L_\nu(s, \mathscr{X}) = \sum_{h \in \mathbb{F}_{q^\nu}[X]} \mathscr{X}_\nu(h) \mathbf{N}_\nu(h)^{-s}, \tag{1.10}$$

onde $\mathbf{N}_\nu(h) = q^{\nu d}$, se d é o grau de h.

As L-funções definidas em (1.5) têm polinômio em $\mathscr{U} = q^{-s}$, uma pergunta natural é se as L-funções definidas em (1.10) também terá. A resposta para essa pergunta é positiva, mais em (1.5) dependem de $\mathscr{X}$ e $\mathbf{N}$, enquanto (1.10) dependem de $\mathscr{X}_\nu$ e $\mathbf{N}_\nu$, então precisamos de alguma maneira de relacionar essas funções.

Proposição 1.12. *Seja $h(x) = x^d + a_1 x^{d-1} + \ldots + a_d$ um polinômio mônico irredutível em $\mathbb{F}_q[X]$,*

e fatorável em $\mathbb{F}_q^v$ em r polinômios irredutíveis de grau d/r.

$$h(x) = h_1(x) \cdot \ldots \cdot h_r(x), \tag{1.11}$$

onde $r = mdc(d, v)$. Então

$$N_v(h_i) = N(h)^{v/r} \quad e \quad \mathscr{X}_v(h_i) = \mathscr{X}(h)^{v/r}$$

Demonstração: Pela definição de $\mathbf{N}_v$, e como o grau de cada fator h_i é d/r, tem-se

$$\mathbf{N}_v(h_i) = (q^v)^{d/r} = (q^d)^{v/r} = \mathbf{N}(h)^{v/r}.$$

Como $h(x) \in \mathbb{F}_q[X]$, pode ser escrito como em (1.11), temos que

$$\mathscr{X}(h)^{v/r} = \chi(\{h\})^{v/r} = \chi(\{h_1\} \cdot \ldots \cdot \{h_r\})^{v/r},$$

onde $\{h_1\}, \ldots, \{h_r\}$ estão em $\mathbb{F}_{q^r}$ e são conjugados sobre $\mathbb{F}_q$. (ver [4]). Se for $\mathscr{N}^r$ a norma de $\mathbb{F}_{q^r}$ para $\mathbb{F}_q$, obtemos

$$\{h\} = \mathscr{N}_r(\{h_i\}), \quad \forall\, i = 1, \ldots, r.$$

Consequentemente,

$$\mathscr{X}_v(h_i) = \chi_v(\{h_i\}) = \chi(\mathscr{N}_v(\{h_i\})),$$

e de $\mathscr{N}_v(\{h_i\}) = \mathscr{N}_r(\{h_i\})^{v/r}$, obtemos

$$\mathscr{X}_v(h_i) = \chi\left((\mathscr{N}_r(\{h_i\}))^{v/r}\right) = \chi(\{h\})^{v/r} = \mathscr{X}(h)^{v/r}.$$

e a proposição está provada.

□

Ainda para relacionarmos as L-funções dadas em (1.5) com as da equação (1.10), vamos precisar do seguinte resultado.

Lema 1.13. *Sejam v, m números naturais. Denotando por (v, m) o maior divisor comum entre v e m, temos*

$$\prod_{u=1}^{v} \left(1 - e^{(mu/v)} X\right) = \left(1 - X^{\frac{v}{(v,m)}}\right)^{(v,m)}.$$

Agora sim, podemos enunciar:

Teorema 1.14. *Suponha $h(x)$ como na Proposição (1.12). Então*

$$L_\nu(s,\mathscr{X}) = \prod_{u=1}^{\nu} L\left(s - \frac{2\pi i u}{\nu \log q}, \mathscr{X}\right).$$

Demonstração: Como por hipótese $h(x) \in \mathbb{F}_q[X]$ é separável em $\mathbb{F}_{q^\nu}$, digamos

$$h(x) = l_1 \cdot \ldots \cdot l_r,$$

onde $r = mdc(d,\nu)$ e cada $l_i(x) \in \mathbb{F}_{q^\nu}[X]$ é mônico irredutível.

Da equação (1.6), temos

$$L_\nu(s,\mathscr{X}) = \prod_{\substack{l \text{ irred} \\ mnico}} (1 - \mathscr{X}_\nu(l)\mathbf{N}_\nu(l)^{-s})^{-1},$$

e pela fatorização que $h(x)$ assume em $\mathbb{F}_{q^\nu}$, da equação acima, tem-se

$$L_\nu(s,\mathscr{X}) = \prod_{\substack{h \in F_q[X] \\ irred, mnico}} \prod_{\substack{l \in F_q^\nu[X] \\ l/h}} (1 - \mathscr{X}_\nu(l)\mathbf{N}_\nu(l)^{-s})^{-1},$$

os polinômios mônicos irredutíveis $l_i(x)$ aparecem na fatorização de apenas um polinômio mônico $h(x) \in \mathbb{F}_q$. Consequentemente, a última expressão se torna

$$\prod_{\substack{h \in F_q[X] \\ irrd, mnico}} \prod_{i=1}^{r} (1 - \mathscr{X}_\nu(l_i)\mathbf{N}_\nu(l_i)^{-s})^{-1}$$

e está, pela Proposição (1.12)

$$L_\nu(s,\mathscr{X}) = \prod_{\substack{h \in F_q[X] \\ irrd, mnico}} \prod_{i=1}^{r} (1 - \left[\mathscr{X}(h)\mathbf{N}(h)^{-s}\right])^{-\nu/r}$$

e abrindo o produtório interno, tem-se

$$L_\nu(s,\mathscr{X}) = \prod_{\substack{h \in F_q[X] \\ irred, mnico}} (1 - [\mathscr{X}(h)\mathbf{N}(h)^{-s}]^{-\nu/r})^{-r}.$$

Se denotarmos por X o produto $\mathscr{X}(h)\mathbf{N}(h)$ e $r=(v,m)$, aplicando o Lema (1.13), obtemos

$$L_v(s,\mathscr{X}) = \prod_{\substack{h \\ irred,mnico}} \prod_{u=1}^{v} \left(1 - e\left(\frac{u\cdot d}{v}\right)\mathscr{X}(h)\mathbf{N}(h)^{-s}\right)^{-1},$$

agora de $d=$ grau de h, usando a definição de $\mathbf{N}(h)$ que

$$d = \frac{1}{\log q}\cdot \log \mathbf{N}(h),$$

ainda aplicando exponencial e elevando ambos os lados a $\frac{2\pi iu}{v}$, vem

$$e^{\frac{2\pi iud}{v}} = \mathbf{N}(h)^{\frac{2\pi iu}{v\log q}},$$

substituindo este resultado na última expressão de $L_v(s,\mathscr{X})$, obtemos

$$L_v(s,\mathscr{X}) = \prod_{u=1}^{v} \prod_{\substack{h\in\mathbb{F}_q[X] \\ irred,mnico}} \left(1 - \mathscr{X}(h)\mathbf{N}(h)^{-\left(s-\left(\frac{2\pi iu}{v\log q}\right)\right)}\right)^{-1}$$

Mas o produtório interno é por definição uma L-função associada ao corpo $\mathbb{F}_q$, como desejávamos e portanto

$$L_v(s,\mathscr{X}) = \prod_{u=1}^{v} L\left(s - \frac{2\pi iu}{v\log q}, \mathscr{X}\right).$$

□

Sobre as hipóteses do Teorema (1.11), vimos que as L-funções têm um polinômio, em $\mathscr{U}=q^{-s}$, com termo constante igual a 1. Então existe números complexos $\lambda_1,\ldots,\lambda_k$ tais que possamos escrever

$$L(s,\mathscr{X}) = (1-\lambda_1\mathscr{U})\cdot\cdots\cdot(1-\lambda_k\mathscr{U}), \tag{1.12}$$

Considerando que estabelecemos uma relação entre as L-funções dadas em (1.5) e (1.10) levando em conta que essas primeiras podem ser escritos como em (1.12), então é natural pensar em escrever as segundas de tal forma. Neste caminho temos o seguinte resultado.

Teorema 1.15. *Considere $L(s,\mathscr{X})$ como em (1.12), com $\mathscr{U}=q^{-s}$, então*

$$L_v(s,\mathscr{X}) = (1-\lambda_1^v\mathscr{U})\cdot\cdots\cdot(1-\lambda_k^v\mathscr{U}),$$

onde $\mathscr{U}_\nu = q^{-\nu s}$.

Para simplificar notações, vamos escrever

$$S_\nu = \sum_{x \in \mathbb{F}_{q^\nu}} \chi_\nu(P(x)),$$

quando nos referirmos a soma dada no Teorema (1.6) em alguma extensão $\mathbb{F}_{q^\nu}$ de $\mathbb{F}_q$,estimada essa soma, o teorema estará provado, bastando considerar o caso particular, quando $\nu = 1$.

Teorema 1.16. *Suponha que* χ *é um caracter não trivial de expoente d e* $Y^d - P(X)$ *é absolutamente irredutível, ou que* χ *é trivial com* $P(X) = 1$. *Então a soma* S_ν *pode ser escrita como*

$$S_\nu = -\lambda_1^\nu - \ldots - \lambda_{m-1}^\nu.$$

Demonstração: Do Teorema (1.11), tem-se

$$L_\nu(s, \mathscr{X}) = 1 + \zeta_{\nu,1}\mathscr{U}_\nu + \ldots + \zeta_{\nu,m-1}\mathscr{U}_\nu^{m-1},$$

onde $\zeta_{\nu,1} = S_\nu$.

As L-funções associadas ao corpo $\mathbb{F}_{q^\nu}$ têm um polinômio em $\mathscr{U} = q^{-\nu s}$, assim da mesma forma que para as L-funções dadas em (1.5), este polinômio também tem uma forma fatorada, e usado o resultado anterior obtemos

$$L_\nu(s, \mathscr{X}) = (1 - \lambda_1^\nu \mathscr{U}_\nu) \cdot \ldots \cdot (1 - \lambda_{m-1}^\nu \mathscr{U}_\nu).$$

Se desenvolvemos o lado direito da equação acima e igualamos os coeficientes correspondentes, àquela equação que tem os coeficientes $\zeta_{\nu,t}$ com $t = 1, \ldots, m-1$, chegamos a

$$\zeta_{\nu,1} = -\lambda_1^\nu - \ldots - \lambda_{m-1}^\nu,$$

como queríamos. □

Nos passos seguintes vamos considerar S_ν para cada caracter χ, para depois relacionar a expressão encontrada, com o numero N_ν de soluções de $Y^d = P(X)$, e então usar a hipótese de Riemann para curvas sobre corpos finitos, para estimar a soma.

Se para cada caracter χ definimos $S_\nu = S_{\chi\nu}$, então pelo Teorema (1.16) com χ não principal,

$$S_{\chi\nu} = -\lambda_{\chi,1}^{\nu} - \ldots - \lambda_{\chi,m-1}^{\nu}, \tag{1.13}$$

no caso em que χ é principal temos

$$S_{\chi_0\nu} = q^{\nu}. \tag{1.14}$$

Considerando a soma de $S_{\chi\nu}$ sobre os caracteres de expoente d, ganhamos

$$\sum_{\substack{\chi\neq\chi_0 \\ \text{de expoente d}}} S_{\chi\nu} = -\sum_{\substack{\chi\neq\chi_0 \\ \text{de expoente d}}} \sum_{j=1}^{m-1} \lambda_{\chi j}^{\nu}. \tag{1.15}$$

Denotando por N_ν o número de soluções em $\mathbb{F}_{q^\nu}$ de $Y^d = P(X)$, tem-se

$$N_\nu = \sum_{\substack{\chi \\ \text{de expoente d}}} \sum_{x\in\mathbb{F}_{q^\nu}} \chi_\nu(P(x)),$$

mas pela forma que definimos, a soma interna é $S_{\chi\nu}$, logo

$$N_\nu = \sum_{\substack{\chi \\ \text{de expoente d}}} S_{\chi\nu}, \tag{1.16}$$

ver [4]. Como estamos supondo que $Y^d - P(X)$ é absolutamente irredutível, segue da Hipótese de Riemann para curvas sobre corpos finitos, ver [4], que

$$N_\nu - q^{\nu} \ll q^{\frac{\nu}{2}}.$$

Pela expressão de N_ν em (1.16) e visto que $q^{\nu} = S_{\chi_0\nu}$, a diferença acima é a soma sobre todos os caracteres não principais de expoente d, mas isso é o conteúdo da equação (1.15), assim obtemos

$$\sum_{\substack{\chi\neq\chi_0 \\ \text{de expoente d}}} \sum_{j=1}^{m-1} \lambda_{\chi j}^{\nu} \ll q^{\frac{\nu}{2}}. \tag{1.17}$$

Observe que na expressão acima, o somando são os números complexos envolvidos em (1.13), ou seja, se estimarmos os valores absolutos de cada um dos $(m-1)$ inteiros, o Teorema estará provado. Para isso veja o seguinte lema.

Lema 1.17. *Sejam $\lambda_1, \ldots, \lambda_m$ números complexos, e seja $B > 0$ tais que*

$$\lambda_1^s + \ldots + \lambda_m^s \leq B^s \quad para \ \ s = 1, 2 \ldots \tag{1.18}$$

Então $|\lambda_j| \leq B$ para $1 \leq j \leq m$.

Demonstração: Seja z uma variável complexa. Para valores suficientemente pequenos de $|z|$, temos

$$log(1 - \lambda_j z) = -\sum_{s=1}^{\infty} \frac{1}{s} \lambda_j^s z^s \quad \text{para} 1 \leq j \leq m,$$

daí segue que

$$log((1 - \lambda_1 z) \ldots (1 - \lambda_m z)) = -\sum_{s=1}^{\infty} \frac{1}{s} (\lambda_1^s + \ldots + \lambda_m^s) z^s. \tag{1.19}$$

Da equação (1.18) vemos que a série da direita é convergente se $|Bz| < 1$, ou seja, na região $|z| < B^{-1}$, visto que $B > 0$. Conseqüentemente a função da esquerda é analítica em $|z| < B^{-1}$, segue que, $1 - \lambda_j z \neq 0$, e portanto $|\lambda_j| \leq B$ para $1 \leq j \leq m$. □

Agora de (1.17) e do lema acima segue que $|\lambda_{\chi j}| \leq q^{1/2}$ para todo χ e j considerados. Logo de (1.13)

$$\left| \sum_{x \in \mathbb{F}_{q^\nu}} \chi_\nu(P(x)) \right| \leq (m-1) q^{\frac{\nu}{2}},$$

e no caso do corpo $\mathbb{F}_q$, isto é, quando $\nu = 1$, temos

$$\left| \sum_{x \in \mathbb{F}_q} \chi(P(x)) \right| \leq (m-1) q^{\frac{1}{2}},$$

o que demonstra o teorema (1.6).

Toda a teoria desenvolvida nesta seção não ajudaria na demonstração do Teorema (1.6), se não pudéssemos supor a famosa hipótese de Riemann, o caso mais geral tratado no Teorema (1.7) pode ser trabalhado de forma parecida, tendo apenas que considerar algumas hipóteses a mais.

Estes dois resultados serão utilizados nesta dissertação, nos capítulos subseqüentes, na estimativa de somas completas que irão surgir.

Capítulo 2

Completando Somas

Seja χ um caracter módulo q e por $e_q(x)$ vamos denotar a função $e^{2\pi ix/q}$. Uma classe de problemas centrais na teoria analítica dos números é entender como a variação no sinal do somando implica em cancelamento quando trabalhamos com somas do tipo

$$S(N,H) = \sum_{n=N+1}^{N+H} \chi(P(n))e_q(Q(n)), \tag{2.1}$$

onde P e Q são funções racionais sobre $\mathbb{Z}$. No capítulo anterior trabalhamos com somas completas, e vimos algumas propriedades algébricas.

Por somas incompletas entendemos somas sobre intervalos ou somas que não estejam sobre um sistema completo de resíduos módulo q, enquanto que por completar uma soma, queremos dizer que vamos escrever a soma incompleta (2.1) em termos de somas completas relacionadas, de maneira que as propriedades estudadas possam ser usadas na estimativa dessas.

2.1 A desigualdade de Pólya-Vinogradov

Seja χ um caracter não principal módulo q. Considere o caso $P(n) \equiv n$ e $Q(n) \equiv 0$ para todo n. Isto é, considere

$$S(N,H) = \sum_{n=N+1}^{N+H} \chi(n). \tag{2.2}$$

Sendo que $|\chi(n)| \leq 1$, é evidente que $|S(N,H)| \leq H$, que chamaremos de cota trivial. Por

volta de 1919 Pólya e Vinogradov mostraram o primeiro resultado não-trivial, a saber

$$S(N,H) \ll q^{\frac{1}{2}} \log q \tag{2.3}$$

esta cota superior pode ser demonstrada de maneira muito elementar.

Para qualquer caracter $\chi(n)$ módulo q, $q > 1$, considere a equação (1.2), quando $(n,q) = 1$, tem-se

$$\chi(n)\tau(\overline{\chi}) = \sum_{m \bmod q} \chi(n)\overline{\chi}(m)e_q(m) = \sum_{m \bmod q} \chi(n\overline{m})e_q(m) = \sum_{a \bmod q} \overline{\chi}(a)e_q(na)$$

pois enquanto m varia sobre classes de resíduos mod q, $\overline{a} \equiv n\overline{m}$ também o fará, e ainda $\tau(\overline{\chi}) \neq 0$ pelo Teorema (1.4), portanto vamos considerar esta última relação para começarmos nossos argumentos afim de mostrar que a soma $S(N,H)$ tem cancelamento.

Assim

$$\sum_{n=N+1}^{N+H} \chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{a \bmod q} \overline{\chi}(a) \sum_{n=N+1}^{N+H} e_q(na),$$

observe que a soma interior é uma progressão geométrica, logo

$$\sum_{n=N+1}^{N+H} e_q(na) = \sum_{n=0}^{H-1} [e_q(a)]^{N+n+1} = [e_q(a)]^{N+1} \sum_{n=0}^{H-1} [e_q(a)]^n$$

mas de

$$\sum_{n=0}^{H-1} [e_q(a)]^n = \frac{1-[e_q(a)]^H}{1-[e_q(a)]}$$

obtemos

$$\sum_{n=N+1}^{N+H} e_q(na) = e_q(a(N+1)) \frac{[e_q(a)]^{H-1/2} - [e_q(a)]^{-1/2}}{[e_q(a)]^{1/2} - [e_q(a)]^{-1/2}} = e_q\Big(aN + \frac{aH}{2} + \frac{a}{2}\Big) \frac{\sin\left(\frac{\pi aH}{q}\right)}{\sin\left(\frac{\pi a}{q}\right)}.$$

Portanto dessa igualdade, da equação (2.2) e de $|\chi(n)| \leq 1$ temos

$$\left| \sum_{n=N+1}^{N+H} \chi(n) \right| \leq q^{-\frac{1}{2}} \sum_{a=1}^{q-1} \frac{1}{|\sin \pi a/q|}$$

mais quando $0 \leq \beta \leq 1/2$, $\sin(\pi\beta) \geq 2\beta$, daí $|\sin(\pi\beta)| \geq 2\langle\beta\rangle$, e

$$\left|\sum_{n=N+1}^{N+H}\chi(n)\right| \leq q^{-\frac{1}{2}}\sum_{a=1}^{q-1}\frac{1}{2\left\langle\frac{a}{q}\right\rangle}$$

onde $\left\langle\frac{a}{q}\right\rangle$ é a distância de $\frac{a}{q}$ ao número inteiro mais próximo.

Conseqüentemente, tem-se

$$\left|\sum_{n=N+1}^{N+H}\chi(n)\right| \ll q^{1/2}\sum_{a=1}^{q-1}\frac{1}{a} \ll q^{1/2}\log q,$$

pois

$$\sum_{a=1}^{A}\frac{1}{a} = \log A+\gamma+O(A^{-1}),$$

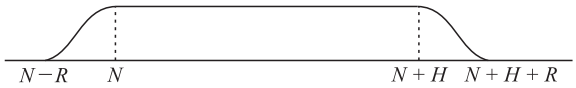
onde $0 \leq \gamma \leq 1$ é a constante de Euler.

Tanto para a busca de generalizações quanto para um entendimento mais profundo dessa fórmula, vale a pena investigar mais a soma dada por (2.1).

2.2 Completando Somas usando Análise Harmônica

O método que apresentamos aqui pode ser encarado como um processo geral de relacionar somas incompletas com somas completas, usando análise harmônica. Observamos que a soma completa precisa ser estimada, e que usa métodos bem diferentes dos que discutiremos posteriormente. Considere o problema de estimar (2.1). O somando é oscilatório e como em (2.2), queremos entender como essas variações implicam em cancelamento.

Para simplificar estimativas posteriores é conveniente introduzir uma função teste suavizante $g(t)$ de classe C^∞, que seja identicamente 1 em $[N,N+H]$, que se anula fora do intervalo $[N-R,N+H+R]$, com $1 \leq R < N$, como descrito no gráfico a seguir,



e

$$g^{(\nu)}(t) \ll R^{-\nu}, \quad \nu = 0,1,2,\ldots.$$

Usando g para definir

$$S_g = \sum_n g(n)\chi(P(n))e_q(Q(n)),$$

a contribuição do intervalo $N < n \leq N+H$ é igual à $S(N,H)$ e a dos intervalos $N-R < n \leq N$ e $N+H < n \leq N+H+R$ é $O(R)$, portanto

$$S_g = S + O(R),$$

assim, para R arbitrariamente pequeno é suficiente estimar S_g em vez de S. Quebrando em classes de resíduos, tem-se

$$S_g = \sum_{x(\mathrm{mod}\, q)} \chi(P(x))e_q(Q(x)) \sum_{n \equiv x(\mathrm{mod}\, q)} g(n) = \sum_{x(\mathrm{mod}\, q)} \chi(P(x))e_q(Q(x)) \sum_r g(rq+x).$$

Assim, note que a variável x varia sobre um conjunto completo de classes de resíduos módulo q, mas a soma interior ainda depende de x, não permitindo que utilizemos a estrutura completa de x.

Para eliminar esta limitação vamos aplicar a fórmula do somatório de Poisson, que afirma que

$$\sum_{n=-\infty}^{+\infty} f(n) = \sum_{l=-\infty}^{+\infty} \int_{-\infty}^{+\infty} f(y)e(-ly)\mathrm{d}y.$$

Portanto

$$\sum_r g(rq+x) = \sum_l \int_{-\infty}^{+\infty} g(yq+x)e(-ly)\mathrm{d}y,$$

e por uma mudança de variáveis tem-se

$$\sum_r g(rq+x) = \frac{1}{q}\sum_l e_q(lx) \int_{-\infty}^{+\infty} g(\xi)e_q(-l\xi)\mathrm{d}\xi = \frac{1}{q}\sum_l e_q(lx)\hat{g}\left(\frac{l}{q}\right),$$

onde $\hat{g}\left(\frac{l}{q}\right) = \int_{-\infty}^{+\infty} g(\xi)e_q(-l\xi)\mathrm{d}\xi$ é a transformada de Fourier de g.

Agora

$$S_g = \frac{1}{q}\sum_l \hat{g}\left(\frac{l}{q}\right) W(P,Q,l),$$

onde $W(P,Q,l) = \sum_{x(\mathrm{modq})} \chi(P(x))e_q(Q(x)+lx)$ e considerando o valor absoluto obtemos

$$\left|\frac{1}{q}\sum_l \hat{g}\left(\frac{l}{q}\right) \sum_{x(\mathrm{modq})} \chi(P(x))e_q(Q(x)+lx)\right| \leq \frac{1}{q}\sum_l \left|\hat{g}\left(\frac{l}{q}\right)\right| |W(P,Q,l)|\,. \tag{2.4}$$

Observe que, em efeito ao método usado, a variável completa x foi separada da outra variável. Para prosseguir vamos trabalhar em (2.4) as propriedades de $\hat{g}(l/q)$ para diferentes valores de l e deixaremos a soma completa para uma próxima seção.

No caso em que $l = 0$, temos

$$\hat{g}(0) = \int_{-\infty}^{+\infty} g(t)\mathrm{dt} = \int_{N-R}^{N} g(t)\mathrm{dt} + \int_{N}^{N+H} \mathrm{dt} + \int_{N+H}^{N+H+R} g(t)\mathrm{dt} = H + O(R) \tag{2.5}$$

note que para $2R < H$, $\hat{g}(0)$ é não nulo.

Se $l \neq 0$, integrando por partes uma vez, obtemos

$$\hat{g}\left(\frac{l}{q}\right) = \lim_{R_1\to\infty} -\frac{qg(t)}{2\pi il}e\left(-\frac{lt}{q}\right)\Bigg|_{-R_1}^{+R_1} + \frac{q}{2\pi il}\int_{-\infty}^{+\infty} g'(t)e\left(-\frac{lt}{q}\right)\mathrm{dt} = \frac{q}{2\pi il}\int_{-\infty}^{+\infty} g'(t)e\left(-\frac{lt}{q}\right)\mathrm{dt}$$

pois fora do intervalo $[N-R, N+H+R]$ a função $g(t)$ se anula. Então

$$\left|\frac{q}{2\pi il}\int_{-\infty}^{+\infty} g'(t)e\left(-\frac{lt}{q}\right)\mathrm{dt}\right| \leq \frac{q}{2\pi|l|}\int_{-\infty}^{+\infty} \left|g'(t)\right|\mathrm{dt},$$

mas $g'(t) \ll R^{-1}$ e a integral acima é nula no intervalo $N < n \leq N+H$ e os outros dois intervalos novamente contribuem com $O(R)$, donde

$$\hat{g}\left(\frac{l}{q}\right) \ll \left(\frac{q}{|l|}\right). \tag{2.6}$$

Como $g \in \mathbb{C}^\infty$, podemos integrar por partes quantas vezes quisermos, digamos ν-vezes, $\nu \geq 1$ e assim

$$\hat{g}\left(\frac{l}{q}\right) = \left(\frac{2\pi i l}{q}\right)^{-\nu} \int_{-\infty}^{+\infty} g^{(\nu)}(t) e\left(-\frac{tl}{q}\right) \mathrm{dt}$$

pelos mesmos argumentos vistos anteriormente, de $g^{(\nu)}(t) \ll R^{-\nu}$, segue que

$$\hat{g}\left(\frac{l}{q}\right) \ll \left(\frac{q}{|l|}\right)^{\nu} R^{1-\nu}, \quad \nu = 1, 2, \ldots \tag{2.7}$$

a relação acima é válida de fato se ν é pelo menos 1, pois as derivadas de qualquer ordem de g não se anulam apenas nos dois intervalos de tamanho R.

Escrevendo

$$S_g = S_0 + S_1 + S_2,$$

onde

$$S_0 = \frac{1}{q}\hat{g}(0) W(P,Q,0), \quad S_1 = \frac{1}{q} \sum_{1 \leq |l| \leq L} \hat{g}\left(\frac{l}{q}\right) W(P,Q,l), \quad S_2 = \frac{1}{q} \sum_{|l| > L} \hat{g}\left(\frac{l}{q}\right) W(P,Q,l), \tag{2.8}$$

tem-se de (2.5) que

$$S_0 = \frac{1}{q}\{H + O(R)\} W(P,Q,0),$$

de (2.6) que

$$S_1 \ll \sum_{1 \leq |l| \leq L} \frac{1}{|l|} |W(P,Q,l)|$$

e de (2.7) que

$$S_2 \ll q^{\nu-1} R^{1-\nu} \sum_{|l| > L} \frac{1}{|l|^{\nu}} |W(P,Q,l)|.$$

Observe que a estimativa final de S_g depende da consideração $W(P,Q,l)$, e posteriormente a estimativa de $S(N,H)$ depende da escolha final de R e L, que consideramos nos exemplos a seguir.

2.3 Aplicações

Nesta seção vamos considerar dois exemplos das somas estudadas na seção 2.2, e usaremos as mesmas definições de g, R, L. Primeiro considere $P(x) \equiv x$ e $Q(x) \equiv 0$, tal que

$$S(N,H) = \sum_{n=N+1}^{N+H} \chi(n),$$

ou seja, o caso de Pólya-Vinogradov. A soma $W(P,Q,l)$ é

$$W(P,Q,l) = \sum_{x(\mathrm{mod}q)} \chi(x) e_q(lx),$$

que é uma soma de Gauss, e do capítulo 1,

$$W(P,Q,l) = \begin{cases} q^{\frac{1}{2}} & \text{se } l \not\equiv 0 \mathrm{mod}\, q,\ \chi \neq \chi_0; \\ q & \text{se } l \equiv 0 \mathrm{mod}\, q,\ \chi = \chi_0; \\ 0, \quad c.c. & \end{cases}$$

Assim,

$$S_0 = \frac{1}{q}\{H + O(R)\} W(P,Q,0) = 0;$$

e como

$$S_1 \ll \sum_{1 \leq |l| \leq L} \frac{1}{|l|} |W(P,Q,l)|,$$

podemos ter casos em que $l \equiv 0 \mathrm{mod}\, q$, nestes casos $W(P,Q,l) = 0$ e este é $\leq q^{1/2}$, daí

$$S_1 \ll q^{\frac{1}{2}} \sum_{1 \leq |l| \leq L} \frac{1}{|l|} \ll q^{1/2} \sum_{1 \leq l \leq L} \frac{1}{l},$$

conseqüentemente em S_1 tem-se

$$S_1 \ll q^{\frac{1}{2}} \sum_{1 \leq l \leq L} \frac{1}{l} = q^{\frac{1}{2}} \left(\log L + \gamma + O\left(\frac{1}{L}\right) \right),$$

onde $0 \leq \gamma \leq 1$ é a constante de Euler. Mas os termos $q^{\frac{1}{2}}\gamma$ e $q^{\frac{1}{2}} O\left(\frac{1}{L}\right)$ são no máximo $q^{\frac{1}{2}}$, que é sempre menor que $q^{\frac{1}{2}} \log L$ para q suficientemente grande, portanto

$$S_1 \ll q^{\frac{1}{2}} \log L.$$

E ainda

$$S_2 \ll q^{\nu-1}R^{1-\nu}\sum_{|l|>L}\frac{1}{|l|^{\nu}}\,|W(P,Q,l)| = q^{\nu-1/2}R^{1-\nu}\sum_{|l|>L}\frac{1}{|l|^{\nu}},$$

para que a série seja convergente, ν deve ser pelo menos dois, aí

$$S_2 \ll q^{\nu-1/2}R^{1-\nu}L^{1-\nu} + q^{\nu-1/2}R^{1-\nu}O\left(\frac{1}{L^{\nu}}\right),$$

o último termo é bastante pequeno, assim

$$S_2 \ll q^{\nu-1/2}R^{1-\nu}L^{1-\nu} = q^{-1/2}RL\left(\frac{q}{RL}\right)^{\nu},$$

note que se for $RL < q$ não conseguimos estimar S_2, se $RL > q$ o termo fica arbitrariamente pequeno, enquanto se colocarmos $RL = q$ a estimação de S_2 nem ao menos depende de ν, daí

$$S_2 \ll q^{\frac{1}{2}}.$$

Com as contribuições de S_0, S_1 e S_2 obtemos

$$S_g \ll q^{\frac{1}{2}}\log L + q^{\frac{1}{2}} \ll q^{\frac{1}{2}}\log(q/R) \ll q^{\frac{1}{2}}\log q,$$

pois $1 \leq R$.

Agora que já estudamos o teorema de Pólya-Vinogradov, vamos considerar um caso menos trivial, com $P(n) \equiv n^2+1$, ainda será $Q(n) \equiv 0$, ou seja, estamos com a soma

$$S(N,H) = \sum_{n=N+1}^{N+H}\chi(n^2+1).$$

Pelo método trabalhado na seção anterior, obtemos neste caso

$$S_g = \frac{1}{q}\sum_{l}\hat{g}\left(\frac{l}{q}\right)W(P,Q,l),$$

onde, agora

$$W(P,Q,l) = \sum_{x(\mathrm{mod}\,q)}\chi(x^2+1)e_q(lx).$$

Considere $S_g = S_0 + S_1 + S_2$, onde S_0, S_1 e S_2 são dadas como em (2.8). Agora vamos

estimar $W(P,Q,l)$. A começar por S_0, temos

$$W(P,Q,l) = \sum_{x\in\mathbb{F}_q} \chi(x^2+1),$$

do Teorema (1.5) temos que $f(x) = x^2+1$ tem no máximo duas soluções em $\mathbb{F}_q$ ou em qualquer extensão deste, e como χ é uma caracter não principal, segue do Teorema (1.6) que

$$W(P,Q,l) \ll q^{1/2}.$$

Em S_1 e S_2, tem-se

$$W(P,Q,l) = \sum_{x\in\mathbb{F}_q} \chi(x^2+1)e_q(lx),$$

e novamente pelo Teorema (1.5), agora combinado agora com o Teorema (1.7), temos

$$W(P,Q,l) \leq 2q^{1/2},$$

assim, em todo caso

$$W(P,Q,l) \ll q^{1/2}.$$

Agora substituindo esta estimativa em S_0, S_1 e S_2, e usando os resultados das equações (2.5), (2.6) e (2.7), obtemos

$$S_0 = q^{-1/2}\{H+O(R)\}, \quad S_1 \ll q^{1/2} \sum_{1\leq|l|\leq L} \frac{1}{|l|} \ \ e \ \ S_2 \ll q^{\nu-1/2}R^{1-\nu} \sum_{|l|>L} \frac{1}{|l|^{\nu}}.$$

Então a estimativa de S_g é dada por

$$S_g = q^{-1/2}\{H+O(R)\} + q^{1/2}\left(\log L+\gamma+O\left(\frac{1}{L}\right)\right) + q^{\nu-1/2}R^{1-\nu}\left(\frac{L^{1-\nu}}{\nu-1}+O\left(\frac{1}{L^{\nu}}\right)\right).$$

Pelas mesmas considerações feitas na estimativa de S_g na aplicação anterior, podemos escrever

$$S_g \ll q^{-1/2}H + q^{-1/2}O(R) + q^{1/2}\log q + q^{1/2},$$

como por hipótese $H < q$, e o segundo termo é muito pequeno para q arbitrariamente grande, tem-se

$$S_g \ll q^{\frac{1}{2}}\log q.$$

Mais uma vez vimos que com este método não se consegue quebrar a barreira de $q^{1/2}$. O teorema de Pólya-Vinogradov mostra que somas do tipo (2.1) sobre intervalos de mais que $q^{1/2}$ inteiros mostram cancelamento, ou seja, seu valor absoluto é menor que o número de termos.

Capítulo 3

Somas Curtas e o Teorema de Burgess

A função divisor denotada por $d(n)$ é o número de divisores positivos do inteiro positivo n. Note que esta não é completamente multiplicativa, mesmo sendo multiplicativa, pois $d(4) = 3$, e $d^2(2) = 4$. Esta função é tal que para qualquer $\varepsilon > 0$, $d(n) \ll n^{\varepsilon}$.

Neste capítulo tratamos de somas curtas, isto é, somas sobre intervalos de comprimento $H < q^{1/2}$. De fato, consideramos somas da forma (2.1) com $P(n) \equiv n$ e $Q(n) \equiv 0$, isto é

$$S(N,H) = \sum_{n=N+1}^{N+H} \chi(n), \tag{3.1}$$

com $H < q^{1/2}$. Observe que se completarmos esta soma da maneira do capítulo anterior, obtemos ainda

$$S(N,H) \ll q^{1/2} \log q,$$

ou seja, temos uma estimativa não-trivial somente se $H \gg q^{1/2} \log q$. Por esta razão precisamos de uma outra maneira para criar alguma "variável mais comprida". E a partir do deste novo método obtemos uma prova do Teorema de Burgess, que enunciamos agora:

Teorema 3.1. *Seja $q \geq 1$ e χ um caracter módulo q, não principal. Considere ainda $N \geq 1$ e $1 \leq H \leq q$. Então para qualquer $\varepsilon > 0$ arbitrário*

$$S(N,H) \ll_{\varepsilon,k} H^{1-\frac{1}{k}} q^{\frac{k+1}{4k^2}+\varepsilon},$$

para $k = 1,2,3$. Além disso se q é livre de cubos, o resultado segue para todo $k \in \mathbb{N}$.

Note primeiro que para qualquer $s \in \mathbb{N}$,

$$\begin{aligned} S(N,H) &= \sum_{N-s<n\leq N+H-s} \chi(n+s) \\ &= \sum_{N<n\leq N+H} \chi(n+s) + \sum_{N-s<n\leq N} \chi(n+s) - \sum_{N+H-s<n\leq N+H} \chi(n+s) \\ &= \sum_{N<n\leq N+H} \chi(n+s) + \sum_{N<n\leq N+s} \chi(n) - \sum_{N+H<n\leq N+H+s} \chi(n) \\ &= \sum_{N<n\leq N+H} \chi(n+s) + S(N,s) - S(N+H,s), \end{aligned} \tag{3.2}$$

por incluir e exluir. Supondo que $s < H$, as somas no segundo e terceiro membros são mais curtas que a soma original, permitindo uma demonstração por indução. Em [8], aproveitando uma idéia de Karatsuba, o autor, Friedlander, calcula a média de (3.2) sobre os inteiros $s = ab$, onde $1 \leq a \leq A$, $1 \leq b \leq B$, com $AB < H$, para escrever

$$S(N,H) = T(N,H) + \frac{1}{AB}\sum_{a,b} S(N,ab) - \frac{1}{AB}\sum_{a,b} S(N+H,ab),$$

onde

$$T(N,H) = \frac{1}{AB}\sum_{a,b}\sum_{N<n\leq N+H} \chi(n+ab).$$

Se $(a,q) = 1$, temos

$$\sum_{N<n\leq N+H} \chi(n+ab) = \chi(a) \sum_{N<n\leq N+H} \chi(\overline{a}n+b),$$

portanto

$$T(N,H) = \frac{1}{AB}\sum_{a}\sum_{b}\sum_{n} \chi(a)\chi(\overline{a}n+b).$$

A soma em n ainda está sobre o intervalo $[N, N+H]$, que é curto. Porém, note que por ser $1 \leq a \leq A$, $a \in \mathbb{N}$, $\overline{a}n$ assume AH valores módulo q, ou seja, mais valores do que n assume, e procuramos usar este número maior de valores para criar uma soma mais comprida.

Assim queremos usar os valores $\overline{a}n$ como uma variável só; para isso reordenamos, e esti-

mando obtemos

$$|T(N,H)| \leq \frac{1}{AB} \sum_{1\leq a\leq A} \sum_{N<n\leq\leq N+H} \left| \sum_{1\leq b\leq B} \chi(\bar{a}n+b) \right|.$$

Veja que a soma sobre b depende somente de $\bar{a}n$ e não dos valores de a e n separadamente. Agora, considere a substituição $\bar{a}n \equiv y$, onde y percorre todo um conjunto de classes de resíduos módulo q. Desta forma, conseguimos uma única variável de comprimento maior que o de n, mas esta é irregular.

Afim de usar a desigualdade de Hölder, precisamos de um produto. Para isso vamos definir por $\nu(y)$ o número de pares (a,n), com $1 \leq a \leq A$, $N < n \leq N+H$, $(a,q) = 1$ e $\bar{a}n \equiv y \pmod{q}$, assim

$$|T(N,H)| \leq \frac{1}{AB} \sum_{y\,(\mathrm{mod}q)} \nu(y) \left| \sum_{1\leq b\leq B} \chi(y+b) \right|.$$

Observe que não temos garantia a priori de que os AH valores que $\bar{a}n$ assumem, são todos distintos, isto é, dependendo dos valores assumidos, podemos ter $\bar{a}_1 n_1 \equiv \bar{a}_2 n_2$, e ainda que fossem todos distintos, como $AH < q$ algumas vezes teremos $\nu(y) = 0$. Em outras palavras, por a e n variarem uma quantia mais curta que q, muitas das classes de resíduos não serão representadas por $\bar{a}n$.

Agora temos o produto que precisávamos para usar a desigualdade de Holder, e desta maneira completar a soma interior que depende em b, assim obtemos

$$|T(N,H)| \leq \frac{1}{AB} \left\{ \sum_{y(\mathrm{mod}q)} \nu(y)^{\frac{2k}{2k-1}} \right\}^{\frac{2k-1}{2k}} \left\{ \sum_{y(\mathrm{mod}q)} \left| \sum_{1\leq b\leq B} \chi(y+b) \right|^{2k} \right\}^{\frac{1}{2k}}, \tag{3.3}$$

onde $k > 1$ é um número natural.

Para estimar $T(N,H)$ trabalhamos os dois fatores acima. Na estimativa do primeiro fator usamos métodos algébricos, observando primeiro que 2 é uma cota superior para $\frac{2k}{2k-1}$ e como

$\nu(y) \in \mathbb{N} \cup \{0\}$, tem-se

$$\sum_{y(\mathrm{mod} q)} \nu(y)^{\frac{2k}{2k-1}} \leq \sum_{y(\mathrm{mod} q)} \nu(q)^2 = \sum_{y(\mathrm{mod} q)} \left\{ \sum_{\substack{1\leq a\leq A \\ N<n\leq N+H \\ \bar{a}n\equiv y(\mathrm{mod} q) \\ (a,q)=1}} 1 \right\}^2 = \sum_{\substack{1\leq a_1,a_2\leq A \\ N<n_1,n_2\leq N+H \\ \bar{a}_1 n_1 \equiv \bar{a}_2 n_2 (\mathrm{mod}\, q) \\ (a_1 a_2, q)=1}} 1,$$

nessa última, observe que a congruência $\bar{a}_1 n_1 \equiv \bar{a}_2 n_2$, é equivalente à $a_2 n_1 \equiv a_1 n_2$, além disso se considerarmos não somente o caso em que $(a_1 a_2, q) = 1$, a soma acima é menor ou igual a

$$\sum_{\substack{1\leq a_1,a_2\leq A \\ N<n_1,n_2\leq N+H \\ a_2 n_1 \equiv a_1 n_2 (\mathrm{mod}\, q)}} 1 = \sum_{\substack{1\leq a_1,a_2\leq A \\ N<n_1,n_2\leq N+H \\ (a_2-a_1) n_1 \equiv (n_2-n_1) a_1 (\mathrm{mod}\, q)}} 1,$$

pois $a_2 n_1 \equiv a_1 n_2$ se e somente se $(a_2 - a_1) n_1 \equiv (n_2 - n_1) a_1$. O número de possibilidades para $(a_2 - a_1) n_1$ são $2AH$ e cada um desses valores determina $a_1(n_2 - n_1)$ módulo q. E a última expressão acima é igual a

$$\sum_{\substack{1\leq a\leq A \\ N<n\leq N+H}} 1 + 2 \sum_{\substack{1\leq a_1,a_2\leq A \\ N<n_1,n_2\leq N+H \\ (a_2-a_1) n_1 \equiv (n_2-n_1) a_1 (\mathrm{mod}\, q) \\ a_2>a_1}} 1.$$

Como os valores de $a_1(n_2 - n_1)$ estão no intervalo $[-AH, AH]$ e $AH < q$, ser determinado módulo q é o mesmo que estar determinado absolutamente, ou seja, a congruência anterior se torna uma igualdade, pois $2AH < q$. Se escrevemos $b = a_2 - a_1$ e $m = n_2 - n_1$, tem-se

$$AH + 2 \sum_{\substack{1\leq a_1\leq A \\ N<n_1\leq N+H}} \sum_{\substack{1-a_1\leq b\leq A-a_1 \\ 0<m\leq N+H-1 \\ bn_1 = ma_1}} 1$$

de a_2 ser maior que a_1 temos que $1 \leq b$, observe que como a_1 é pelo menos 1 então A é uma cota superior para $A - a_1$. Agora reordenando os índices, obtemos

$$AH + 2 \sum_{\substack{1\leq a_1\leq A \\ N<n_1\leq N+H}} \sum_{\substack{1\leq b\leq A-a_1 \\ 0<m\leq N+H-1 \\ bn_1 = ma_1}} 1 \leq AH + 2 \sum_{\substack{1\leq a_1\leq A \\ N<n_1\leq N+H}} \sum_{\substack{1\leq b\leq A \\ 0<m\leq N+H-1 \\ bn_1 = ma_1}} 1 \leq AH + 2 \sum_{\substack{1\leq b\leq A \\ N<n_1\leq N+H}} \sum_{m | bn_1} 1,$$

esta soma interior é a função divisor de bn_1, isto é, $d(bn_1)$, e esta como já mencionada é tal que para $\varepsilon > 0$, tem-se $d(n) = O(n^{\varepsilon})$, logo

$$\sum_{y(\mathrm{mod}q)} v(q)^2 = AH + 2 \sum_{\substack{1\leq b\leq A \\ N<n_1\leq N+H}} d(bn_1) \ll AH + \sum_{\substack{1\leq b\leq A \\ N<n_1\leq N+H}} (bn_1)^{\varepsilon},$$

mais $b \leq A$ e $\varepsilon > 0$, logo $b^{\varepsilon} \leq A^{\varepsilon}$, o mesmo para n_1, isto é, $n_1^{\varepsilon} \leq N^{\varepsilon}$, portanto $(bn_1)^{\varepsilon} \leq (AN)^{\varepsilon}$, conseqüentemente

$$\sum_{y(\mathrm{mod}q)} v(q)^2 \ll AH + (AN)^{\varepsilon} \sum_{\substack{1\leq b\leq A \\ N<n_1\leq N+H}} 1,$$

agora de ambos, A e N serem menores que q, temos

$$\sum_{y(\mathrm{mod}q)} v(q)^2 \ll AH + AHq^{\varepsilon} \ll AHq^{\varepsilon}. \tag{3.4}$$

Para obter cancelamento para $T(N,H)$ e conseqüentemente para $S(N,H)$, falta investigar uma estimativa para o segundo membro de (3.3), que é um resultado de Burgess, obtido por meios de combinatória.

Lema 3.2. *Para um caracter χ não principal módulo q, q-primo e k um inteiro positivo, temos*

$$\sum_{y(mod q)} \left| \sum_{1\leq b\leq B} \chi(y+b) \right|^{2k} \ll_k B^{2k} q^{1/2} + B^k q.$$

Demonstração: Abrindo a 2k-ésima potência, a equação é

$$\sum_{y(\mathrm{mod}q)} \left| \sum_{1\leq b\leq B} \chi(y+b) \right|^{2k} = \sum_{1\leq b_1,\ldots,b_{2k}\leq B} \sum_{y(\mathrm{mod}q)} \chi((y+b_1)\cdots(y+b_k)(y+b_{k+1})^{q-2}\cdots(y+b_{2k})^{q-2})$$

e daí, menor ou igual à

$$\sum_{1\leq b_1,\ldots,b_{2k}\leq B} \left| \sum_{y(\mathrm{mod}q)} \chi((y+b_1)\cdots(y+b_k)(y+b_{k+1})^{q-2}\cdots(y+b_{2k})^{q-2}) \right|.$$

Sejam d a ordem de χ, e

$$P(y) = (y+b_1)\cdots(y+b_k)(y+b_{k+1})^{q-2}\cdots(y+b_{2k})^{q-2}.$$

Se existe b_j que difere de todos os demais b_l, então $P(y)$ não é uma d-ésima potência, pois a ordem do zero $-b_j$ de $P(y)$ ou é 1 ou é $q-2$. Portanto

$$\sum_{y(\mathrm{mod}q)} \chi((y+b_1)\cdots(y+b_k)(y+b_{k+1})^{q-2}\cdots(y+b_{2k})^{q-2}) \ll q^{\frac{1}{2}}$$

pelo Teorema (1.6), pois o número máximo de zeros para $P(y)$ é $2k$.

Por outro lado, se não existe b_j diferente dos demais b_l, então os $b_j's$ que agrupam em pares iguais e existem $O_k(B^k)$ $2k$-uplas $(b_1,\ldots,b_{2k})$ com esta propriedade, e para estes a soma

$$\sum_{y(\mathrm{mod}q)} \chi((y+b_1)\cdots(y+b_k)(y+b_{k+1})^{q-2}\cdots(y+b_{2k})^{q-2}) \ll q.$$

Consequentemente

$$\sum_{y(\mathrm{mod}q)} \left| \sum_{1\le b\le B} \chi(y+b) \right|^{2k} \ll_k B^{2k}q^{1/2} + B^k q.$$

□

Combinando as estimativas de (3.4) e Lema (3.2) acima, temos

$$\begin{aligned} T(N,H) &\ll_{k,\varepsilon} (AB)^{-1}(AHq^{\varepsilon})^{1-\frac{1}{2k}}\cdot(B^{2k}q^{\frac{1}{2}} + B^k q)^{\frac{1}{2k}} \\ &\ll_{k,\varepsilon} (AB)^{-1}(AHq^{\varepsilon})^{1-\frac{1}{2k}}\cdot(Bq^{\frac{1}{4k}} + B^{\frac{1}{2}}q^{\frac{1}{2k}}). \end{aligned}$$

Escolhemos $AB = H/8 < H$. Daí

$$\begin{aligned} T(N,H) &\ll_{k,\varepsilon} \frac{1}{AB}\left[\frac{H^{1-\frac{1}{2k}}}{B^{1-\frac{1}{2k}}}H^{1-\frac{1}{2k}}q^{\varepsilon}\right]\cdot(Bq^{\frac{1}{4k}} + B^{\frac{1}{2}}q^{\frac{1}{2k}}) \\ &\ll_{k,\varepsilon} H^{1-\frac{1}{k}}q^{\varepsilon}\cdot(B^{\frac{1}{2k}}q^{\frac{1}{4k}} + B^{-\frac{1}{2}+\frac{1}{2k}}q^{\frac{1}{2k}}). \end{aligned}$$

Esta estimativa depende de B, e para minimizar a cota superior escolhemos B de tal modo que $B^{\frac{1}{2k}} = B^{-\frac{1}{2}+\frac{1}{2k}}$. Observe que estas expressões são crescente e decrescente respectivamente,

por isso escolhemos B para mediar esse crescimento e decrescimento. Assim, $B = q^{\frac{1}{2k}}$ e

$$\begin{aligned} T(N,H) &\ll_{k,\varepsilon} H^{1-\frac{1}{k}}\left[(q^{\frac{1}{2k}})^{\frac{1}{2k}}q^{\frac{1}{4k}} + (q^{\frac{1}{2k}})^{-\frac{1}{2}+\frac{1}{2k}}q^{\frac{1}{2k}}\right]q^{\varepsilon} \\ &= H^{1-\frac{1}{k}}\left(q^{\frac{1}{4k^2}+\frac{1}{4k}} + q^{-\frac{1}{4k}+\frac{1}{4k^2}+\frac{1}{2k}}\right)q^{\varepsilon} \\ &\ll_{k,\varepsilon} H^{1-\frac{1}{k}}\, q^{\frac{k+1}{4k^2}+\varepsilon}. \end{aligned}$$

Ou seja,

$$|T(N,H)| \leq C_{k,\varepsilon}H^{1-\frac{1}{k}}q^{\frac{k+1}{4k^2}+\varepsilon},$$

para alguma constante positiva C que depende de k e ε. A partir de $C_{k,\varepsilon}$, definimos uma outra constante,

$$D_{k,\varepsilon} = \frac{C_{k,\varepsilon}}{1-2^{\frac{3}{k}-2}}. \tag{3.5}$$

Para concluir a demonstração do Teorema(3.1), trabalhamos por indução, observando primeiro que se H é suficientemente pequeno, então o resultado do Teorema(3.1) segue, pois

$$H < q^{\frac{k+1}{4k^2}+\varepsilon},$$

para todo $\varepsilon > 0$, e a estimativa é trivial.

Agora pela nossa hipótese de indução supomos que o Teorema(3.1) vale para todo $H_1 < H$, em particular para qualquer número $H_1 = ab < H/8$, e podemos estimar

$$|S(N,ab)|, |S(N+H,ab)| \leq D_{k,\varepsilon}(H')^{1-\frac{1}{k}}q^{\frac{k+1}{4k^2}+\varepsilon}.$$

Consequentemente

$$|S(N,H)| \leq C_{k,\varepsilon}H^{1-\frac{1}{k}}q^{\frac{k+1}{4k^2}+\varepsilon} + 2D_{k,\varepsilon}(H')^{1-\frac{1}{k}}q^{\frac{k+1}{4k^2}+\varepsilon},$$

e

$$\begin{aligned} |S(N,H)| &\leq C_{k,\varepsilon}H^{1-\frac{1}{k}}q^{\frac{k+1}{4k^2}+\varepsilon} + 2^{\frac{3}{k}-2}D_{k,\varepsilon}H^{1-\frac{1}{k}}q^{\frac{k+1}{4k^2}+\varepsilon} \\ &= \left(C_{k,\varepsilon} + 2^{\frac{3}{k}-2}D_{k,\varepsilon}\right)H^{1-\frac{1}{k}}q^{\frac{k+1}{4k^2}+\varepsilon}, \end{aligned}$$

observe que da maneira como $D_{k,\varepsilon}$ foi definida, obtemos

$$C_{k,\varepsilon} + 2^{\frac{3}{k}-2} D_{k,\varepsilon} = D_{k,\varepsilon}.$$

Portanto

$$S(N,H) \ll H^{1-\frac{1}{k}} q^{\frac{k+1}{4k^2}+\varepsilon},$$

o que prova o Teorema de Burgess.

Vale a pena considerar quando esta cota é não trivial, isto acontece quando $H^{1-\frac{1}{k}} q^{\frac{k+1}{4k^2}} < H$, o que é equivalente à

$$H > q^{\frac{k+1}{4k}},$$

daqui vemos que é necessário e suficiente ter $H \gg q^{\frac{1}{4}+\delta}$ para algum $\delta > 0$, por tomar k suficientemente grande. Para ilustrar, considere o caso em que $H = q^{\frac{1}{3}}$, então nossa estimativa é

$$S(N, q^{\frac{1}{3}}) \ll q^{\frac{1}{3}-\frac{1}{12k}+\frac{1}{4k^2}},$$

utilizando os valores de $k = 2, 3, 4, 5, 6, 7$, obtemos respectivamente os expoentes $\frac{17}{48} \cong 0,3542$, $\frac{1}{3} \cong 0,3333$, $\frac{21}{64} \cong 0,3281$, $\frac{49}{150} \cong 0,3267$, $\frac{47}{144} \cong 0,3264$, $\frac{16}{49} \cong 0,3265$. Observamos a partir destes expoentes suspeitamos que $k = 6$ pode resultar na melhor estimativa para a soma $S(N,H)$ quando $H = q^{\frac{1}{3}}$.

Afirmamos que existe um determinado valor, tal que para k maior que este, a estimativa é não trivial, e mais ainda, que existe um k que nos dá a melhor estimativa.

No exemplo de $H = q^{\frac{1}{3}}$, observe que em

$$\frac{1}{3} - \frac{1}{12k} + \frac{1}{4k^2},$$

para $k > 1$, temos um expoente maior que $\frac{1}{3}$, o próprio $\frac{1}{3}$ e os demais menores, mais quando olhamos no limite para k arbitrariamente grande, este é igual a $\frac{1}{3}$, ou seja, deve haver um ponto de mínimo.

No caso geral, com $H = q^{\alpha}$, para a estimativa ser não trivial, devemos ter

$$\alpha > \frac{k+1}{4k},$$

ou seja, dado α, a partir do valor de k que satisfaz a inequação acima, teremos uma estimativa não trivial.

Substituindo $H = q^{\alpha}$ na estimativa geral, e como queremos uma estimativa não trivial, obtemos o seguinte expoente para q,

$$\frac{k+1}{4k^2} - \frac{\alpha}{k} = \left(\frac{1}{4} - \alpha\right)\frac{1}{k} + \frac{1}{4k^2},$$

como já observamos vai existir um valor de mínimo, e para encontrar esse valor de k, suponha por um momento que k seja uma variável real, então se calculamos a derivada, temos

$$\left(\alpha - \frac{1}{4}\right)\frac{1}{k^2} - \frac{1}{2k^3} = 0,$$

o que dá

$$k = \frac{2}{4\alpha - 1},$$

observe que o melhor k é o dobro do valor para o qual a estimativa se torna não trivial, se necessário consideramos o valor inteiro anterior ou sucessor ao encontrado aqui, visto que k é inteiro inicialmente.

Se usando esses resultados, calcularemos novamente para $\alpha = \frac{1}{3}$, para a estimativa ser não trivial deveremos ter $k > 3$, e a melhor estimativa se da quando $k = 6$, como havíamos encontrado.

Note que se ao invés da desigualdade de Hölder, tivéssemos usado a desigualdade de Cauchy, (3.3) teríamos,

$$|T(N,H)| \leq \frac{1}{AB}\left\{\sum_{y(\mathrm{mod}q)} \nu(y)^2\right\}^{\frac{1}{2}}\left\{\sum_{y(\mathrm{mod}q)}\left|\sum_{1\leq b\leq B}\chi(y+b)\right|^2\right\}^{\frac{1}{2}},$$

isto é, a desigualdade de Hölder para $k = 1$. Assim com os resultados encontrados, tem-se

$$T(N,H) \ll_{\varepsilon} (AB)^{-1}(AHq^{\varepsilon})^{\frac{1}{2}} \cdot (B^2 q^{\frac{1}{2}} + Bq)^{\frac{1}{2}}.$$

E terminando com o mesmo raciocínio, obteríamos

$$\begin{aligned} S(N,H) &\ll_{\varepsilon} \frac{1}{AB}(A^{\frac{1}{2}}H^{\frac{1}{2}}q^{\varepsilon}) \cdot (Bq^{\frac{1}{4}} + B^{\frac{1}{2}}q^{\frac{1}{2}}) \\ &= q^{\varepsilon}\left(\frac{H^{\frac{1}{2}}}{A^{\frac{1}{2}}}q^{\frac{1}{4}} + \frac{(AHB)^{\frac{1}{2}}}{AB}q^{\frac{1}{2}}\right), \end{aligned}$$

de $B = H/4A$ temos $AB = H/4$, logo

$$S(N,H) \ll_\varepsilon q^\varepsilon \left(\frac{H^{\frac{1}{2}}}{A^{\frac{1}{2}}} q^{\frac{1}{4}} + q^{\frac{1}{2}} \right) \ll_\varepsilon q^{\frac{1}{2}} \varepsilon.$$

Observe que este resultado é trivial se $H < q^{1/2}$, e se fosse $H > q^{1/2}$ teríamos usado o método do capítulo anterior.

Referências Bibliográficas

[1] L. Ruolf, *Finite Fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Gian - Carlo Rota, 1983.

[2] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Clarendon Press. Oxford, Fifth Edition, 1979.

[3] K. Chandrasekharan, *Introduction to Analytic Number Theory*, Springer - Verlag, Berlin Heidelberg New York, 1968.

[4] Wolfgang M. Schmidt, *Equations over Finite Fields an Elementary Approach*, Lecture Notes in Mathematics, Springer - Verlag, Berlin Heidelberg New York, 1976.

[5] Harold Davenport, *Multiplicative Number Theory*, Graduate Texts in Mathematics, Springer - Verlag, Berlin Heidelberg New York, Second Edition.

[6] Niven, I. Zuckerman, H.S. Montgomery, H.L. *An Introduction to the Theory of Numbers*, John Wiley & Sons, Inc., 5ªed, New York.

[7] Gonçalves, Adilson. *Introdução a Álgebra*, ed.:IMPA., 5ªed, Rio de Janeiro, 2006.

[8] Friedlander. J, *Primes In Arithmetic Progressions and Related Topics*, Analytic Number Theory and Diophantine Problems, Oklahoma State University, 1984.