UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

OTÁVIO ARAÚJO DE AGUIAR

SOBRE O PROBLEMA DE LINNIK NA ESFERA

FORTALEZA
2021

OTÁVIO ARAÚJO DE AGUIAR

SOBRE O PROBLEMA DE LINNIK NA ESFERA

Dissertação apresentada ao Programa de Pós-graduação em Matemática do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Mestrado em Matemática. Área de concentração: Teoria dos Números.

Orientador: Prof. Dr. Ramon Moreira Nunes.

FORTALEZA

2021

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

A23s Aguiar, Otávio Araújo de.
Sobre o problema de Linnik na esfera / Otávio Araújo de Aguiar. – 2021.
74 f. : il.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Programa de Pós-Graduação em Matemática, Fortaleza, 2021.
Orientação: Prof. Dr. Ramon Moreira Nunes.

1. Formas modulares. 2. Estimativa não trivial de coeficientes de Fourier. 3. Problema de Linnik. I. Título.

CDD 510

OTÁVIO ARAÚJO DE AGUIAR

O PROBLEMA DE LINNIK NA ESFERA

Dissertação apresentada ao Programa de Pós-graduação em Matemática do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática. Área de concentração: Teoria dos Números.

Aprovada em: 14 / 09 / 2021.

BANCA EXAMINADORA

Prof. Dr. Ramon Moreira Nunes (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Kevin Langlois
Universidade Federal do Ceará (UFC)

Prof. Dr. Cayo Rodrigo Felizardo Dória
Universidade Federal de Goiás (UFG)

Prof. Dr. Davi Dos Santos Lima (Suplente)
Universidade Federal de Alagoas (UFAL)

Dedico aos meus pais, Francisco Pereira e Francisca Araújo, por sempre me apoiarem.

AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Ao Prof. Dr. Ramon Moreira Nunes, pela excelente orientação.

Aos professores participantes da banca examinadora Kevin Langlois, Cayo Rodrigo e Davi Dos Santos, por aceitarem o convite.

Aos colegas das turmas de mestrado e doutorado, cuja a convivência me permitiu amadurecer como pessoa.

"Sem a escuridão, a luz não só seria irreconhecível, como não poderia existir."(BARDON, 1956)

RESUMO

O objetivo deste trabalho é apresentar uma demonstração do fato de que o conjunto das projeções das soluções inteiras da equação $x^2 + y^2 + z^2 = n$, $n \in \mathbb{Z}$ livre de quadrados, sobre $\mathbb{S}^2$ é uniformemente distribuída sobre essa esfera quando $n \to +\infty$. Para isso, será esboçada uma estimativa não trivial dos coeficientes de Fourier de formas modulares de peso meio inteiro produzida por Iwaniec em 1987, que implicará diretamente no resultado anterior.

Palavras-chave: formas modulares; estimativa não trivial de coeficientes de Fourier; problema de Linnik.

ABSTRACT

Objective of this work is to present a demonstration of the fact that the set of projections of the integer solutions of the equation $x^2+y^2+z^2 = n$, $n \in \mathbb{Z}$ square free, about $\mathbb{S}^2$ is equidistributed over this sphere when $n \to +\infty$. For that, a non-trivial estimate of the Fourier coefficients of modular half-weight shapes produced by Iwaniec in 1987 will be outlined, which will directly imply the previous result.

Keywords: modular forms; non-trivial bound of Fourier coefficients; Linnik problem.

LISTA DE SÍMBOLOS

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	Representam, respectivamente, o conjunto dos números inteiros, racionais, reais e complexos.
$Re(z), Im(z)$	Dado $z \in \mathbb{C}$, escrevemos $z = Re(z) + iIm(z)$, onde $Re(z), Im(z) \in \mathbb{R}$.
$\mathbb{S}^2$	$\{(x,y,z) \in \mathbb{R}^3; x^2+y^2+z^2 = 1\}$.
$\frac{1}{2}\mathbb{Z} - \mathbb{Z}$	Representa o conjunto $\{\frac{2n+1}{2}; n \in \mathbb{Z}\}$ dos números meio inteiros.
$[a,b]$	Denota o mínimo múltiplo comum dos inteiros a e b.
$e(x)$	$e^{2\pi ix}$, onde e é a constante de Euler base do logaritmo natural.
O_3	Representa o conjunto das matrizes ortogonais do $\mathbb{R}^3$.
${}^t m$	Representa a transposta da matriz m.
$\ll$	$f(x) \ll g(x)$ significa que existem constantes $C > 0$ e x_0 independentes da variável x que satisfazem $\lvert f(x)\rvert \leq C\lvert g(x)\rvert$ sempre que $x \geq x_0$. $f(x) \gg g(x)$ significa o mesmo que $g(x) \ll f(x)$.
$\asymp$	$f(x) \asymp g(x)$ significa que $f(x) \ll g(x)$ e $g(x) \ll f(x)$ simultaneamente.
$\ll_\varepsilon$	$f(x) \ll_\varepsilon g(x)$ significa que a constante implícita depende da variável ε. $f(x) \gg_\varepsilon g(x)$ significa o mesmo que $g(x) \ll_\varepsilon f(x)$.
Big O	$f(x) = O(g(x))$ significa o mesmo que $f(x) \ll g(x)$. $f(x) = O_\varepsilon(g(x))$ significa o mesmo que $f(x) \ll_\varepsilon g(x)$.
$\sum_{x \, mod(c)} f$	$\sum_{n=0}^{c-1} f(n)$, onde f é uma função periódica módulo c.
$\mu(n)$	Representa a função de Möbius, definida como 0 se n não é livre de quadrados e $(-1)^k$ quando n é livre de quadrados com k fatores primos distintos em sua fatoração.
$\tau(n)$	$\sum_{d\mid n} 1$, representa o número de divisores positivos de um inteiro n.
$\omega(n)$	$\sum_{p\mid n} 1$, é o número de inteiros primos que dividem n.
$\delta_{m,n}$	Delta de Kronecker, é definido como 0 se $m \neq n$, e 1 caso $m = n$.
$a \mid b^\infty$	Significa que todos os fatores primos que dividem o inteiro a também dividem o inteiro b.
$p^n \parallel a$	Dados inteiros a, n, p, com n positivo e p primo, $p^n \parallel a$ significa que p^n divide a, mas p^{n+1} não divide a.

SUMÁRIO

1 INTRODUÇÃO

O comportamento de algumas equações diofantinas já desafiou muitos matemáticos durante a história, e isso não foi diferente com a equação de aparência inicialmente simpática $x^2 + y^2 + z^2 = n$. O primeiro comportamento a intrigar os estudiosos envolvia descobrir quais eram os inteiros positivos n que permitiam a equação ter solução inteira, problema esse que rondou a mente de matemáticos notáveis como Fermat, Cauchy e Legendre, até ser completamente demonstrada por Gauss em 1801. Gauss foi além e obteve uma fórmula para o número de soluções, mostrando como consequência que a equação teria solução se, e somente se, n não fosse do tipo $4^a(8k + 7)$, $a, k \in \mathbb{Z}_{\geq 0}$. Depois de mais de um século, outra questão desafiou os matemáticos: Como se distribuem as soluções inteiras de $x^2 + y^2 + z^2 = n$ na esfera centrada na origem e de raio $\sqrt{n}$?

A resposta desse problema é que, desde que n deixe resto 1,2,3,5 ou 6 quando dividido por 8, o conjunto $\Omega'(n) = \{(x, y, z) \in \mathbb{Z}^3; x^2 + y^2 + z^2 = n\}$ será cada vez mais bem "distribuído"na esfera quando $n \to +\infty$. A noção intuitiva do que essa ideia representa é que, se tomarmos $E \subset \mathbb{S}^2$ aleatório suficientemente regular e considerarmos $E_n = \sqrt{n}E$ a projeção do conjunto E na esfera de raio $\sqrt{n}$ centrada na origem, obtemos

$$\frac{\#(\Omega'(n) \cap E_n)}{\#(\Omega'(n))} \to \frac{A(E)}{4\pi}$$

quando $n \to +\infty$, onde $A(E)$ representaria a "área"do conjunto E sobre a esfera unitária. De outra forma, Duke mostrou que é verdade que os conjuntos $\Omega(n) = \{(x, y, z)/\sqrt{n}; (x, y, z) \in \Omega'(n)\}$, $n \equiv 1, 2, 3, 4$ ou $6 \mod 8$), tornam-se *equidistribuídos*, ou *uniformemente distribuídos* em $\mathbb{S}^2$, isto é, se tomarmos a medida de Lebesgue normalizada μ na esfera, temos a seguinte relação

$$\lim_{n\to+\infty} \frac{1}{\#\Omega(n)} \sum_{x\in\Omega(n)} f(x) \to \int_{\mathbb{S}^2} f d\mu \tag{1.1}$$

para toda função contínua $f : \mathbb{S}^2 \to \mathbb{R}$.

O matemático soviético Linnik foi o primeiro a discutir o problema, e também foi o primeiro a obter um avanço significativo na direção desse resultado, em seu livro de 1968 *Ergodic Properties of Algebraic Fields* (21), ao provar, usando métodos de teoria ergódica, que a afirmação era válida se n é livre de quadrados, não deixa resto 7 quando dividido por 8, e o símbolo de Lagrange $\left(\frac{-n}{p}\right)$ valer 1 para algum primo ímpar p fixo. Já no ano de 1977, Arenstorf e Johnson em (1) concluíram que é possível atacar esse problema usando a teoria de formas modulares, e que a solução de uma versão onde a restrição era n ser livre de quadrados e incongruente a 7 módulo 8 dependia apenas da obtenção de uma *estimativa não trivial dos coeficientes de Fourier* de formas modulares de peso meio inteiro.

Heuristicamente falando, usando uma terminologia que será definida no decorrer deste trabalho, essa ligação vem do fato da função θ_P, P indica um polinômio harmônico esfé-

rico de grau par, definida como

$$\theta_P(z) = \sum_{m\in\mathbb{Z}^3} P(m/|m|)e(|m|^2 z) = \sum_{n=1}^{\infty}\left(\sum_{|m|^2=n} P(m/|m|)\right) e(|m|^2 z),$$

ser um tipo específico de forma modular de peso meio inteiro, chamada de *forma cuspidal*, e do fato de esse último somatório explicitar a sua *série de Fourier*. No contexto das formas modulares, uma forma modular de peso $k = \lambda + \frac{1}{2}, \lambda$ inteiro, pode ser representada através da sua série de Fourier

$$f(z) = \sum_{i=0}^{\infty} a_n e^{2\pi i n z}.$$

Levando em consideração esse fato, Arenstorf e Johnson já tinham conhecimento de que os coeficientes a_n satisfaziam $a_n = O_\epsilon(n^{\frac{k}{2}-\frac{1}{4}+\epsilon})$ desde que f fosse cuspidal, e que essa estimativa era a melhor possível. O que foi chamado de estimativa não trivial dos coeficientes de Fourier nesse cenário seria uma eventual estimativa do tipo $a_n = O_\epsilon(n^{\frac{k}{2}-\frac{1}{4}-\sigma+\epsilon})$, para algum $\sigma > 0$, quando se impõe que n seja livre de quadrados. Um resultado do gênero foi finalmente demonstrado por Iwaniec em 1987, que mostrou em (15) que $a_n = O_\epsilon(n^{\frac{k}{2}-\frac{1}{4}-\frac{1}{28}+\epsilon})$ desde que o peso k fosse maior que 2, o que não somente validou o que foi provado por Arenstorf e Johnson, como também implicou que (1.1) era válido, como mostrado logo depois por Duke (7) em 1988 .

Esse trabalho tem como objetivo apresentar uma demonstração do fato de que (1.1) vale desde que imposta a restrição de n ser livre de quadrados. Para isso, será antes esboçada a prova de Iwaniec para a estimativa não trivial dos coeficientes de Fourier de formas cuspidais de peso meio inteiro.

No capítulo 2, serão citados alguns conceitos e resultados preliminares que serão usados no decorrer do texto. No capítulo 3 será feita uma breve explanação sobre formas modulares, onde será citada suas principais propriedades, e também serão introduzidas as importantes noções de séries de Eisenstein e Poincaré. Será citado que o conjunto das séries de Poincaré gera o subespaço vetorial das formas cuspidais, e no fim será obtida uma fórmula para os coeficientes de Fourier de séries de Poincaré. No capítulo 4 será obtida a famosa *fórmula de Petersson*, que relaciona os coeficientes de Fourier de elementos de uma base ortonormal do espaço das formas cuspidais com um tipo especial de soma exponencial, chamada *soma de Kloosterman*. Depois de estudar algumas propriedades dessas somas, será esboçada a demonstração da estimativa não trivial dos coeficientes de Fourier de formas cuspidais de peso meio-inteiro, que será obtida procurando estimativas envolvendo soma de somas de Kloosterman que, quando combinada com a fórmula de Petersson, resulta na estimativa não trivial. Por último, será apresentada no capítulo 5 como a estimativa de Iwaniec implica na conclusão do artigo de Arenstorf e Johnson, isto é, que os conjuntos $\Omega(n)$ tornam-se equidistribuidos na esfera quando $n \not\equiv 7 (\mathrm{mod}\ 8)$ é livre de quadrados.

2 PRELIMINARES

2.1 Harmônicos esféricos

Uma função duas vezes diferenciável $f : \mathbb{R}^d \to \mathbb{R}$ é dita *harmônica* se satisfaz

$$\Delta f = \frac{\partial^2 f}{\partial x_1^2} + \frac{\partial^2 f}{\partial x_2^2} + ... + \frac{\partial^2 f}{\partial x_d^2} = 0.$$

Um polinômio homogêneo que satisfaz a equação diferencial acima é chamado de *polinômio harmônico*, e quando seu domínio é restrito a $\mathbb{S}^{d-1}$ este é chamado de *polinômio harmônico esférico*. O subespaço de $L^2(\mathbb{S}^{d-1})$ formado pelos polinômios harmônicos esféricos na esféra d-dimensional será denotado por $\mathcal{H}^d$, e o espaço dos polinômios harmônicos esféricos de grau $n \geq 0$ de $\mathcal{H}_n^d$. Veja que $\mathcal{H}^d$ é a soma direta de todos os $\mathcal{H}_n^d$, $n \geq 0$.

Proposição 2.1 *Seja μ a medida de Lebesgue normalizada em $\mathbb{S}^{d-1}$. Sobre os espaços vetoriais citados anteriormente, as seguintes afirmações são válidas*

(1) Para cada $n \geq 0$, $\mathcal{H}_n^d$ tem dimensão finita e, se caso $d \geq 3$, essa dimensão valerá $D(d,n) = \frac{2n+d-2}{n+d-2}\binom{n+d-2}{d-2}$.

(2) Dados $m \neq n$, $F \in \mathcal{H}_n^d$, $G \in \mathcal{H}_m^d$, então $\int_{\mathbb{S}^{d-1}} FGd\mu = 0$, e em particular $\int_{\mathbb{S}^{d-1}} Fd\mu = 0$ caso $n > 0$.

(3) Existe um conjunto ortonormal $\bigcup_{i=0}^{\infty}\{P_i^{(1)}, P_i^{(2)}, ..., P_i^{(D(d,i))}\}$ de polinômio harmônicos esféricos, onde $P_0^1 \equiv 1$, cada polinômio P_i^j tem grau i, e que gera um espaço vetorial denso em $L^2(\mathbb{S}^{d-1})$.

(4) Se $f : \mathbb{S}^2 \to \mathbb{R}$ é contínua, então existe uma sequência de reais a_i^j tais que, tomando $F_i = \sum_{j=1}^{D(d,i)} a_i^{(j)} P_i^{(j)}$ a projeção de f em $\mathcal{H}_i^d$, a série

$$\sum_{i=0}^{\infty} F_i$$

converge uniformemente para f, isto é, os polinômio harmonicos esféricos geram um subespaço denso em $C^0(\mathbb{S}^2)$.

Prova: Todos esses resultados podem ser vistos em (11). □

2.2 Equidistribuição

Intuitivamente, um conjunto S ser equidistribuído em um espaço X significa que se duas regiões de X têm a mesma "área", então elas devem conter o mesmo número de pontos de S. Se tomarmos X como o intervalo $[0,1]$ esta ideia pode ser traduzida matematicamente da seguinte forma: Uma sequência $w = (x_n)_{n=1}^{\infty} \subset [0,1]$ é dita equidistribuída em $[0,1]$ se para todo $a, b \in [0,1](b > a)$, tivermos

$$\frac{\#(\{x_1, x_2, ..., x_n\} \cap [a,b])}{n} \to b - a,$$

quando $n \to \infty$. Essa afirmação é equivalente a dizer que para toda função contínua f em $[0,1]$ vale

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} f(x_i) = \int_0^1 f(x)dx.$$

Pode-se usar uma ideia similar para analisar o comportamento de sequência de subconjuntos finitos $\{X_n\}_{n=1}^{\infty}$. Por exemplo, se tomarmos novamente o intervalo $[0,1]$ como referência, uma sequência de subconjuntos $\{X_n\}_{n=1}^{\infty} \subset [0,1]$ será equidistribuído se

$$\lim_{n\to\infty} \frac{1}{\#X_n} \sum_{x\in X_n} f(x) = \int_0^1 f(x)dx.$$

Será necessária usar uma definição que generalize essa ideia anterior de equidistribuição para um espaço de Hausdorff compacto para que seja possível entender matematicamente o que significa uma sequência de conjuntos tornar-se equidistribuídos em $\mathbb{S}^2$ (Veja (20, p.171)).

Definição 2.1 *Seja X um espaço compacto de Hausdorff. Faça μ uma medida de Borel regular de probabilidade em X. Seja $C^0(X)$ o conjunto de todas as funções contínuas em X que assumam valores reais. Então a sequência de subconjuntos finitos de X, $\{X_n\}_{n=1}^{\infty}$, tornam-se equidistribuídos em X, com respeito à medida μ, se*

$$\lim_{n\to\infty} \frac{1}{\#X_n} \sum_{x\in X_n} f(x) = \int_X f(x)d\mu,$$

para todo $f \in C^0(X)$.

A esfera $\mathbb{S}^2$ com a topologia induzida do $\mathbb{R}^3$ é um espaço compacto de Hausdorff, assim só nos falta definir uma medida que satisfaça as condições da definição acima.

Definição 2.2 *Será denominada de medida de Lesbegue normalizada em $\mathbb{S}^2$, μ, a única medida de Borel de $\mathbb{S}^2$, em relação à topologia induzida do $\mathbb{R}^3$, que satisfaz*
(1) $\mu(gE) = \mu(E)$, para todo elemento E da álgebra de Borel de $\mathbb{S}^2$ e para todo $g \in O_3$.
(2) $\mu(\mathbb{S}^2) = 1$.

Por último, apresentaremos um critério que nos será bastante útil mais adiante.

Proposição 2.2 *(Critério de Weyl na esfera) A sequência de subconjuntos finitos $\{X_n\}_{n=1}^{\infty}$ de $\mathbb{S}^2$ tornam-se equidistribuídos se, e somente se,*

$$\lim_{n\to\infty} \frac{1}{\#X_n} \sum_{x\in X_n} P(x) = 0$$

Para todo polinômio harmônico esférico P em $\mathbb{S}^2$ de grau positivo.

Prova: Pelo item (2) da proposição 2.1, se $\{X_n\}_{n=1}^{\infty}$ é equidistribuído em $\mathbb{S}^2$,

$$\lim_{n\to\infty}\frac{1}{\#X_n}\sum_{x\in X_n}P(x)=0=\int_{\mathbb{S}^2}P(x)d\mu.$$

Caso $\lim_{n\to\infty}\frac{1}{\#X_n}\sum_{x\in X_n}P(x)=0$ para todo polinômio harmônico esférico P de grau positivo, fixemos f uma função real contínua em $\mathbb{S}^2$ e $\epsilon>0$. Pelo item (4) da proposição 2.1 existem polinômios harmônicos esféricos $P_0,P_1,...,P_t$, com o grau de P_i sendo i, tais que

$$\parallel f-(P_0+...+P_t)\parallel_{\infty}<\epsilon,$$

onde $\parallel f\parallel_{\infty}=\max_{x\in\mathbb{S}^2}|f(x)|$ denota a norma do máximo. Note que P_0 é uma função constante, digamos $P_0\equiv c$. Por simplicidade, será denotado

$$S_i(n)=\frac{1}{\#X_n}\sum_{x\in X_n}P_i(x)$$

Então

$$\int_{\mathbb{S}^2}P_0(x)\mu=c=S_0(n)\ \ \forall n\geq 0$$

Do enunciado

$$\lim_{n\to\infty}S_i(n)=0$$

Para todo $i=1,..,t$. Portanto podemos tomar um n_0 suficientemente grande tal que (observe que nessa situação t é um inteiro fixo) $|S_i(n)|<\frac{\epsilon}{3t}\ \ \forall n\geq n_0$. Assim, quando $n\geq n_0$

$$\left|\int_{\mathbb{S}^2}f\mu-\frac{1}{\#X_n}\sum_{x\in X_n}f(x)\right|=$$

$$\left|\int_{\mathbb{S}^2}f\mu-\frac{1}{\#X_n}\sum_{x\in X_n}f(x)+\int_{\mathbb{S}^2}(P_0+...+P_t)\mu-\int_{\mathbb{S}^2}(P_0+...+P_t)\mu+\sum_{i=0}^{t}S_i(n)-\sum_{i=0}^{t}S_i(n)\right|$$

$$\leq\left|\int_{\mathbb{S}^2}(f-(P_0+...+P_t))\mu\right|+\left|\frac{1}{\#X_n}\sum_{x\in X_n}[f(x)-(P_0+...+P_t)]\right|+\sum_{i=0}^{t}\left|\int_{\mathbb{S}^2}P_i\mu-S_i(n)\right|$$

$$\leq\parallel f-(P_0+...+P_t)\parallel_{\infty}+\frac{1}{\#X_n}\sum_{x\in X_n}\parallel f-(P_0+...+P_t)\parallel_{\infty}+\sum_{i=1}^{t}|S_i(n)|$$

$$\leq\frac{\epsilon}{3}+\frac{\epsilon}{3}+t\frac{\epsilon}{3t}=\epsilon$$

O que mostra que

$$\lim_{n\to\infty}\frac{1}{\#X_n}\sum_{x\in X_n}f(x)=\int_{\mathbb{S}^2}f(x)\mu$$

para uma função contínua arbitrária f. Portanto $\{X_n\}_{n=1}^{\infty}$ tornam-se equidistribuídos em $\mathbb{S}^2$. □

2.3 $\mathbf{SL_2}(\mathbb{R})$

O semiplano de Poincaré $\mathbb{H}$ consiste no conjunto

$$\mathbb{H} = \{z = x + iy \in \mathbb{C}; Im(z) = y > 0\}$$

equipado com a métrica não euclidiana

$$ds^2 = y^{-2}(dx^2 + dy^2)$$

tem-se também uma medida derivada diretamente dessa métrica, que pode ser escrita em termos da medida de Lebesgue como

$$d\sigma(z) = y^{-2}dxdy.$$

Outros fatos importantes sobre $\mathbb{H}$ são (Veja [3, p.11-35)):

(1) As isometrias de $\mathbb{H}$ são as transformações de Möbius, i.e., são as funções do tipo

$$g(z) = \frac{az + b}{cz + d}, \quad a, b, c, d \in \mathbb{R}, ad - bc = 1,$$

ou as transformações do tipo

$$g(z) = \frac{a\overline{z} + b}{c\overline{z} + d}, \quad a, b, c, d \in \mathbb{R}, ad - bc = 1.$$

(2) A medida $d\sigma$ definida anteriormente é também invariante por transformações de Möbius.

(3) As geodésicas de $\mathbb{H}$ são as retas perpendiculares ao eixo real e os semicírculos com centro no eixo real.

(4) Dados dois pontos z_1, z_2 pertencentes a $\mathbb{H}$, existe uma isometria de $\mathbb{H}$ que satisfaz $gz_1 = z_2$.

$SL_2(\mathbb{R})$ é definido como o conjunto de todas as matrizes 2×2 de entradas reais de determinante 1 agindo em $\mathbb{C} \cup \{\infty\}$ através da ação

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z \to \frac{az + b}{cz + d},$$

onde definimos, dado $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$, que $\gamma(-d/c) = \infty$ se $c \neq 0$, $\gamma(\infty) = \infty$ se $c = 0$, e $\gamma(\infty) = a/c$ se $c \neq 0$.

Definição 2.3 *Será dito que um elemento $\alpha \in SL_2(\mathbb{R})$ é:*

(1) Elíptico se a equação $\alpha z = z$ tem duas soluções $z_0, \bar{z_0}$, com $z_0 \in \mathbb{H}$.

(2) Parabólico se a equação $\alpha z = z$ tem uma única raiz em $\mathbb{R} \cup \{\infty\}$.

(3) Hiperbólico se a equação $\alpha z = z$ tem duas raízes em $\mathbb{R} \cup \{\infty\}$.

***Obs**: Observe que uma manipulação em $\alpha z = z$ resultará em uma equação polino-*

mial de segundo grau com coeficientes reais em z, portanto α vai se enquadrar em exatamente um dos casos citados na definição.

Seja Γ um subgrupo de $SL_2(\mathbb{R})$. Dados z, w pertencentes a $\mathbb{H}\cup\mathbb{R}\cup\{\infty\}$, definimos $\Gamma_z = \{\alpha \in \Gamma; \alpha z = z\}$ se z pertence a $\mathbb{H}$, $\Gamma_\infty = \{\alpha \in \Gamma; \alpha(\infty) = \infty\}$, e $\Gamma_{z,w} = \Gamma_z \cap \Gamma_w$. Dizemos também que um elemento z_0 de $\mathbb{H} \cup \mathbb{R} \cup \{\infty\}$ é um ponto elíptico, parabólico ou hiperbólico de Γ se existir α pertencente a Γ elíptico, parabólico ou hiperbólico, respectivamente, tal que α pertence a Γ_{z_0}. Chamamos um ponto parabólico também de cúspide ou ponto cuspidal de Γ.

Dado $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ pertencente a $\mathrm{SL}_2(\mathbb{R})$ um elemento arbitrário, podemos munir $SL_2(\mathbb{R})$ com a norma $|\alpha|^2 = a^2 + b^2 + c^2 + d^2$, e como $|\alpha| = |-\alpha|$, esta induzirá uma distância em $PSL_2(\mathbb{R}) = SL_2(\mathbb{R})/\{I_d, -I_d\}$.

Definição 2.4 *Um subgrupo Γ de $SL_2(\mathbb{R})$ é discreto se Γ é um subconjunto discreto de $SL_2(\mathbb{R})$, isto é, dado $r > 0$ real, o conjunto $\{\alpha \in \Gamma; |\alpha| < r\}$ é um conjunto finito. Como consequência dessa definição, todo subgrupo discreto é enumerável.*

Dado X espaço topológico de Hausdorff e Γ um grupo de homeomorfismos de X agindo em X, dizemos que Γ age em X *descontinuamente* se, dado $x \in X$, a órbita Γx não tem uma sequência convergindo em X. Ou de forma equivalente, todo subconjunto compacto Y de X é disjunto de wY, para todo w pertencente a Γ, com a exceção de um conjunto finito de elementos de Γ.

Proposição 2.3 *Seja Γ um subgrupo de $SL_2(\mathbb{R})$, e defina $Z(\Gamma) = \{I_d, -I_d\} \cap \Gamma$. Faça $\Gamma' = \Gamma/Z(\Gamma)$ visto como um subgrupo de $PSL_2(\mathbb{R})$. Então Γ é um subgrupo discreto de $SL_2(\mathbb{R})$ se, e somente se, Γ' age descontinuadamente em $\mathbb{H}$.*

Prova: A demonstração desse resultado pode ser vista em ([23], p.17). □

Definição 2.5 *Dizemos que um subgrupo Γ de $PSL_2(\mathbb{R})$ é um grupo Fuchsiano se Γ é discreto (ou, de forma equivalente, Γ' age descontinuadamente em $\mathbb{H}$).*

Proposição 2.4 *Seja Γ um grupo Fuchsiano e $z \in \mathbb{C} \cup \{\infty\}$. Então, sobre o estabilizador Γ_z, podemos afirmar que*

(1) É ciclico e finito se $z \notin \mathbb{R} \cup \{\infty\}$.

(2) Todos os elementos de Γ_z são parabólicos e

$$\Gamma_z/Z(\Gamma) \backsim \mathbb{Z},$$

se $z \in \mathbb{R} \cup \{\infty\}$ é uma cúspide de Γ.

(3)

$$\Gamma_{z_1,z_2}/Z(\Gamma) \backsim \mathbb{Z},$$

se $z_1, z_2 \in \mathbb{R} \cup \{\infty\}$ satisfazem $\Gamma_{z_1,z_2} \neq Z(\Gamma)$.

Prova:A demonstração desse resultado pode ser vista em (23, p.18-19). □

Dado Γ subgrupo de $SL_2(\mathbb{R})$, dizemos que z, w pertencentes a $\mathbb{H}$ são equivalentes em relação a Γ se existir α pertencente a Γ com $\alpha z = w$, ou, de forma equivalente, w pertence a Γz .

Definição 2.6 *Um subconjunto $\mathcal{F} \subset \mathbb{H}$ é chamado de domínio fundamental de um subgrupo Γ de $SL_2(\mathbb{R})$ se*
(1) $\mathcal{F}$ é fechado e conexo em relação à topologia usual de $\mathbb{C} \cup \{\infty\}$.
(2) int($\mathcal{F}$) é aberto e conexo em relação à topologia usual de $\mathbb{C} \cup \{\infty\}$.
(3) $\lambda int(\mathcal{F}) \cap int(\mathcal{F}) = \emptyset$ para todo $\lambda \in \Gamma - Z(\Gamma)$.
(4) Toda órbita de Γ contém um ponto em $\mathcal{F}$.

Proposição 2.5 *Todo grupo Fuchsiano Γ tem um domínio fundamental.*

Prova: Veja (23, p.21-24). □

Proposição 2.6 *Se Γ é um grupo Fuchsiano com domínio fundamental $\mathcal{F}$ e que satisfaz*

$$\int_{\mathcal{F}} \frac{dxdy}{y^2} < \infty$$

então podemos escolher $\mathcal{F}$ de modo que cada um de seus vértices que pertence a $\mathbb{R} \cup \{\infty\}$ seja uma cúspide de Γ, e que cada cúspide de Γ seja equivalente a algum vértice de $\mathcal{F}$ que pertence a $\mathbb{R} \cup \{\infty\}$.

Prova: Veja (23, p.36).

2.4 $\mathbf{SL_2}(\mathbb{Z})$

$SL_2(\mathbb{Z})$ é definido como o conjunto de todas as matrizes 2×2 com entradas inteiras que possuem determinante igual a 1. Será esse o subgrupo de $SL_2(\mathbb{R})$ que vamos nos concentrar a partir deste ponto, uma vez que este e seus subgrupos de índice finito são necessários para se construir a definição de forma modular.

Proposição 2.7 $\mathrm{SL}_2(\mathbb{Z})$ *é gerado pelos elementos* $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *e* $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Prova: Ponha $\tau = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ e $\omega = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, e seja D o subgrupo gerado por τ e ω. Suponha $D \neq SL_2(\mathbb{Z})$. Como

$$\omega \tau^{-1} \omega^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

e

$$\omega^2 = -I_d$$

todos os elementos $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$ que pertencem a $SL_2(\mathbb{Z})$ pertencerão a D, uma vez que $a = d = \pm 1$ e $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$ para todo inteiro n. Se

$$b_0 = \min \{|b|; \exists \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) - D\}$$

então b_0 é maior que zero. Faça um elemento $y_0 = \begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix}$ de $SL_2(\mathbb{Z}) - D$, e um inteiro n tal que $|a_0 - nb_0| < b_0$. Assim

$$y_0\omega^{-1}\tau^n = \begin{pmatrix} -b_0 & a_0 - nb_0 \\ -d_0 & c_0 - nd_0 \end{pmatrix}.$$

Portanto $y_0\omega^{-1}\tau^n$ pertence a D pela definição de b_0. Porém, isso implicará que y_0 pertence a D, contradição. □

Proposição 2.8 *O conjunto de todas as cúspides de $SL_2(\mathbb{Z})$ é dado por $\mathbb{Q} \cup \{\infty\}$, e todas elas são equivalentes à cúspide ∞.*

Prova: Denote por $X \subset \mathbb{R} \cup \{\infty\}$ o conjunto das cúspides de $SL_2(\mathbb{Z})$. Primeiro observe que, se x pertence a X, então existe um elemento $\lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ pertencente a $SL_2(\mathbb{Z})$ tal que a equação $\lambda z = z$ tem apenas x como solução em $\mathbb{R} \cup \{\infty\}$.Caso $c \neq 0$, $cz^2 + (d-a)z - b = 0$ tem $\Delta = 0$ e sua única raiz será $x = \frac{a-d}{2c}$, que é racional. Caso $c = 0$, temos claramente que ∞ será o único ponto fixo de λ. Portanto X estará contido em $\mathbb{Q} \cup \{\infty\}$. Observe que ∞ é o único ponto fixo de $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, assim ∞ pertence a X. 0 também pertencerá a D, uma vez que é o único ponto fixo de $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$. Dado agora um racional não nulo $r = \frac{q}{s}$, q, s inteiros primos entre si, pode-se observar que r será o único ponto fixo de $\begin{pmatrix} qs+1 & -q^2 \\ s^2 & -qs+1 \end{pmatrix}$ pertencente a $SL_2(\mathbb{Z})$. Assim $X = \mathbb{Q} \cup \{\infty\}$.

Por último, observe que 0 é equivalente a ∞, uma vez que 0 é levado ao ∞ por $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. E se $r = \frac{p}{q}$, p e q inteiros primos entre si,um racional não nulo, o teorema de Bézout garantirá a existência de inteiros a e b que satisfazem $ap + bq = 1$, e portanto $\lambda = \begin{pmatrix} a & b \\ -q & p \end{pmatrix}$ pertence a $SL_2(\mathbb{Z})$. Note que $\lambda r = \infty$, portanto r será equivalente a ∞. Daí todo racional é equivalente a ∞. □

A observação de que, para cada par de quádruplas $(a_1, b_1, c_1, d_1), (a_2, b_2, c_2, d_2)$ distintas em $\mathbb{Z}^4$, se tem

$$\sqrt{(a_1 - a_2)^2 + (b_1 - b_2)^2 + (c_1 - d_2)^2 + (d_1 - d_2)^2} \geq 1$$

implica que $SL_2(\mathbb{Z})$ não tem pontos de acumulação, ou seja, é um conjunto discreto de $SL_2(\mathbb{R})$, logo um grupo Fuchsiano pela definição 2.5. Assim, de acordo com a proposição 2.7, $SL_2(\mathbb{Z})$ possui um domínio fundamental.

Proposição 2.9 *O conjunto* $\mathcal{F} = \{z \in \mathbb{H} : |z| \geq 1, |Re(z)| \leq 1/2\}$ *é um domínio fundamental de* $SL_2(\mathbb{Z})$.

Prova: Note que $\mathcal{F}$ satisfaz as condições (1) e (2) da definição 2.6. Para comprovar a condição (3), considere

$$U = \{z \in \mathbb{H}; |z| > 1, |Re(z)| < \frac{1}{2}\}$$

o interior de $\mathcal{F}$. Queremos verificar que $\lambda U \cap U = \emptyset$ para $\lambda \neq \{I_d, -I_d\}$. Seja $\lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ um elemento de Γ que satisfaz $\lambda U \cap U \neq \emptyset$, e considere z pertencente a U tal que λz pertence a U. Pode-se assumir que $Im(\lambda z) \geq Im(z)$ por fazermos a mudança de variável $u = \lambda z$ se necessário. Então, observando que $Im(\lambda z) = \frac{Im(z)}{|cz+d|^2}$ implica em $|cz + d| \leq 1$, obteremos

$$|c|Im(z) \leq \sqrt{(cRe(z) + d)^2 + (cIm(z))^2} = |cz + d| \leq 1. \tag{2.2}$$

Como z pertence a U, temos $Im(z) > \frac{\sqrt{3}}{2}$ e portanto $|c| < \frac{2}{\sqrt{3}}$. Sendo c um inteiro, temos então que $|c| = 1$ ou $c = 0$. No primeiro caso, concluímos que $|z \pm d| \leq 1$ por (2.2). Daí

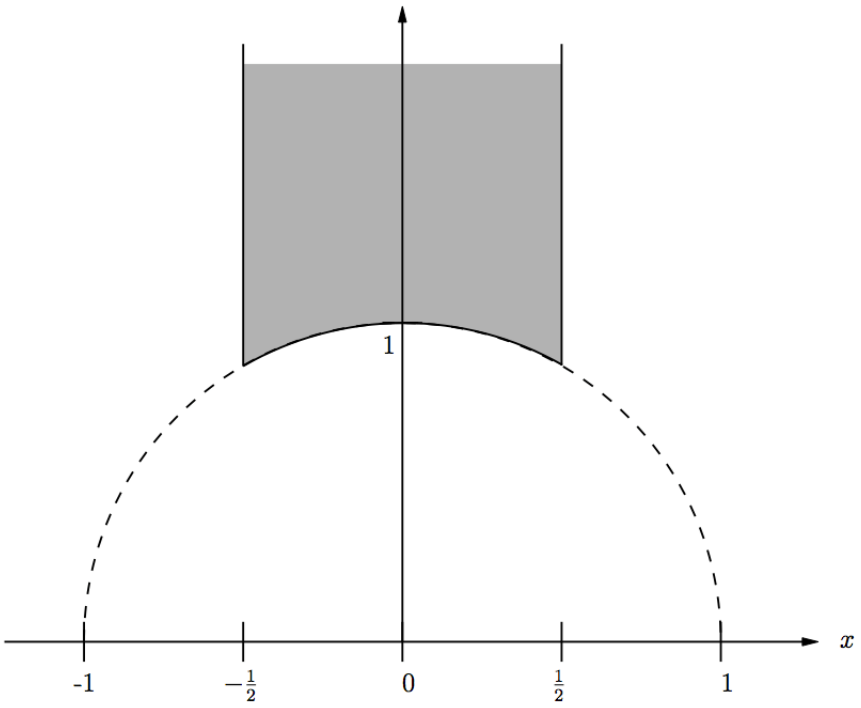
$$1 \geq |z \pm d|^2 = (Re(z) + d)^2 + Im(z)^2 = Re(z)^2 + Im(z)^2 + d^2 \pm 2Re(z)d > 1 + d^2 - d \geq 1,$$

uma vez que $|Re(z)| < \frac{1}{2}$ e d pertence a $\mathbb{Z}$, absurdo. Devemos então ter $c = 0$, nesse caso $\lambda = \pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ e $\lambda z = z + b$. Mas para termos ambos z e $z + b$ pertencentes a U temos que ter necessariamente $b = 0$. Daí $\lambda = \pm I_d$. Para verificar (4), fixemos $z_0 \in \mathbb{H}$. O conjunto

$$\left\{ j(\lambda, z_0) = |cz_0 + d|; \lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \right\}$$

possuirá um elemento mínimo $j(\lambda_0, z_0)$. Pode-se concluir isso escolhendo $\lambda_0 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ tal que $|cRe(z_0) + d|$ seja o menor possível. Então $z_1 = \lambda_0 z_0$ satisfaz $Im(\lambda z_1) \leq Im(z_1)\ \forall \lambda \in SL_2(\mathbb{Z})$, pois $Im(\lambda z_1) = Im(\lambda\lambda_0 z_0) = \frac{Im(z_0)}{j(\lambda\lambda_0, z_0)^2} \leq \frac{Im(z_0)}{j(\lambda_0, z_0)^2} = Im(z_1)$. Mais do

Figura 1 - Domínio fundamental de $SL_2(\mathbb{Z})$



Fonte: FLENG, 2018, p. 61.

que isso, podemos supor que z_1 satisfaz $|Re(z_1)| \leq 1/2$, já que $Im\left(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} z_1\right) = Im(z_1 + b) = Im(z_1)$ e podemos escolher $b \in \mathbb{Z}$ satisfazendo $|Re(z_1 + b)| = |Re(z_1) + b| \leq 1/2$. Portanto, escolhendo z_1 satisfazendo $|Re(z_1)| \leq 1/2$, observe que $Im(-1/z_1) = Im(z_1)/|z_1|^2 \leq Im(z_1)$ e daí $|z_1| \geq 1$. Concluímos então que z_1 está na mesma órbita de z_0, que pertence a $\mathcal{F}$. □

O grupo $SL_2(\mathbb{Z})$ e seus subgrupos de índice finito são chamados de *grupos modulares*. Alguns exemplos de grupos modulares importantes são os grupos de congruência modulares, que vamos definir agora. Dado N inteiro positivo, definimos o grupo de congruência modular principal $\Gamma(N)$ por

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) | b \equiv c \equiv 0 \; mod \; N, \; a \equiv d \equiv 1 \; mod \; N \right\}.$$

Um grupo modular é dito um *grupo modular de congruência* se ele contém algum grupo de congruência modular principal. Assim, são grupos de congruência modulares os seguintes gru-

pos

$$\begin{aligned}\Gamma_0(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) | c \equiv 0 \; mod \; N \right\} \\ \Gamma_1(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) | c \equiv 0 \; mod \; N, \; a \equiv d \equiv 1 \; mod \; N \right\}.\end{aligned}$$

Proposição 2.10 *Se $N \geq 2$ é um inteiro, então*

$$[SL_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N} (1 + 1/p).$$

Prova: Veja (23, p.106).

Corolário 2.1 *Se N, q são inteiros positivos maiores que 2, q primo, então*

$$[\Gamma_0(N) : \Gamma_0(qN)] \leq q + 1.$$

Seja Γ um subgrupo de congruência de $SL_2(\mathbb{Z})$ de índice m. Uma ideia que será importante quando formos tratar de séries de Poincaré é a de que, se $\mathcal{F}$ é o domínio fundamental de $SL_2(\mathbb{Z})$, podemos tomar um conjunto de representantes γ_i do quociente $SL_2(\mathbb{Z})/\Gamma$ de forma que

$$\mathcal{F}_\Gamma = \bigcup_{r=1}^{m} \gamma_r \mathcal{F}.$$

Seja um domínio fundamental de Γ. Observe que o conjunto $\mathbb{Q} \cup \{\infty\}$ das cúspides de $SL_2(\mathbb{Z})$ é também o conjunto de todas as cúspides de Γ, que pode ser particionado em um número finito de subconjuntos tais que dois elementos de um mesmo subconjunto são equivalentes em Γ, mas dois elementos que pertencem a subconjuntos distintos são inequivalentes em relação a Γ .

2.5 Função de Bessel

A equação diferencial de segunda ordem

$$z^2 \frac{d^2 f(z)}{dz^2} + z \frac{df(z)}{dz} + (z^2 - v^2) f(z) = 0,$$

onde v representa um número real, é chamada de *equação de Bessel*, e o número real v é chamado de ordem da equação de Bessel, e as soluções de uma equação de Bessel são chamadas de *funções de Bessel*. Será suposto aqui que v não é um inteiro. Nesse caso, existe uma base $\{J_v, J_{-v}\}$ do conjunto solução da equação de Bessel de ordem v cujo os elementos são chama-

dos de equações de Bessel de primeiro tipo, e estas são expressas como

$$J_v(z) = \sum_{n=0}^{\infty} (-1)^n \frac{(\frac{z}{2})^{2n+v}}{n!\Gamma(n+v+1)} \tag{2.3}$$

$$J_{-v}(z) = \sum_{n=0}^{\infty} (-1)^n \frac{(\frac{z}{2})^{2n-v}}{n!\Gamma(n-v+1)}.$$

Através de combinações lineares dessas duas soluções podemos obter outras funções de Bessel, como as seguintes

$$\begin{aligned} Y_v(z) &= (\sin v\pi)^{-1}[J_v(z)\cos v\pi - J_{-v}(z)] \\ H_v^{(1)}(z) &= J_v(z) + iY_v(z) = (i\sin v\pi)^{-1}[J_{-v}(z) - J_v(z)e^{-iv\pi}] \\ H_v^{(2)}(z) &= J_v(z) - iY_v(z) = (i\sin v\pi)^{-1}[J_v(z)e^{iv\pi} - J_{-v}(z)]. \end{aligned}$$

A função Y_v é chamada de função de Bessel de segundo tipo de ordem v. Já $H_v^{(1)}, H_v^{(2)}$ são chamadas de funções de Bessel de terceiro tipo de ordem v, ou simplesmente por funções de Hankel. Da definição, veja ver que as equações de Hankel safisfazem a relação

$$J_v(z) = \frac{1}{2}[H_v^{(1)} + H_v^{(2)}].$$

Um fato que pode ser visto em [2] e que vai ser usado futuramente neste trabalho é a seguinte forma integral de J_v

$$2\pi i J_v(\alpha z) = z^v \int_{c-i\infty}^{c+i\infty} e^{\frac{1}{2}\alpha(t-z^2t^{-1})} t^{-v-1} dt, \tag{2.4}$$

válida sempre que α for um real positivo e v for maior que -1.

As funções de Hankel admitem uma forma especial quando $v = l + \frac{1}{2}, l$ inteiro, for um múltiplo inteiro de $\frac{1}{2}$, que pode ser escritas como

$$H_{l+\frac{1}{2}}^{(1)}(z) = (\frac{1}{2}\pi z)^{-\frac{1}{2}} i^{-l-1} e^{iz} \sum_{n=0}^{l} \frac{i^n(l+n)!}{(l-n)!n!(2z)^n}$$

$$H_{l+\frac{1}{2}}^{(2)}(z) = (\frac{1}{2}\pi z)^{-\frac{1}{2}} i^{l+1} e^{-iz} \sum_{n=0}^{l} \frac{(-i)^n(l+n)!}{(l-n)!n!(2z)^n}.$$

Tais formas serão úteis quando se for estimar os coeficientes de Fourier de uma forma modular de peso meio inteiro, no final do capítulo 4.

2.6 Símbolo de Jacobi e Kronecker

Veremos nessa seção um pouco sobre o clássico símbolo de Legendre e de suas extensões, os símbolos de Jacobi e Kronecker.

Definição 2.7 *Considere $p \in \mathbb{Z}$ um primo maior que 2. O símbolo de Legendre $\left(\frac{a}{p}\right)$ de um inteiro a é definido por*

$$\begin{cases} \left(\frac{a}{p}\right) = 1, \textit{ se a é resíduo quadrático módulo p} \\ \left(\frac{a}{p}\right) = -1, \textit{ se a não é resíduo quadrático módulo p} \\ \left(\frac{a}{p}\right) = 0, \textit{ se p } |a \end{cases}$$

Proposição 2.11 *Dado p>2 primo, o símbolo de Legendre irá satisfazer as seguintes propriedades*

(1) Se $a \equiv b (\mathrm{mod}\ p)$ então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

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

(3) (Critério de Euler) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\ p)$.

(4) (Lei da reciprocidade quadrática de Gauss) Sejam p, q primos ímpares distintos, então $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

(5) (Suplemento à lei da reciprocidade quadrática) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Prova: A prova de todos esses resultados podem ser conferidas em (22, p.88-94).□

Podemos estender o símbolo de Legendre para inteiros ímpares m, que chamamos de símbolo de Jacobi. Para isso, primeiro definimos que $\left(\frac{a}{1}\right) = 1\ \forall a \in \mathbb{Z}$, $\left(\frac{a}{-1}\right) = 1$ se $a \geq 0$ e $\left(\frac{a}{-1}\right) = -1$ se $a < 0$. Assim, dado um ímpar m cuja sua decomposição em fatores primos positivos seja $wp_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ ($w = \pm 1$ indica o sinal de m) e $a \in \mathbb{Z}$

$$\left(\frac{a}{m}\right) := \left(\frac{a}{w}\right)\left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2}...\left(\frac{a}{p_k}\right)^{\alpha_k}.$$

Dessa definição podemos concluir que, quando m é primo, o símbolo de Jacobi coincide com o simbolo de Legendre. As propriedades do símbolo de Jacobi que iremos citar a seguir podem ser observadas diretamente da definição ou usando propriedades do símbolo de Legendre

(i) $\left(\frac{a}{m}\right) = 0$ se $(a, m) \neq 1$.

(ii) Se $a_1 \equiv a_2 (\mathrm{mod}\ m)$ então $\left(\frac{a_1}{m}\right) = \left(\frac{a_2}{m}\right)$.

(iii) Se b_1, b_2 são ímpares, $\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)$.

(iv) $\left(\frac{a_1 a_2}{m}\right) = \left(\frac{a_1}{m}\right)\left(\frac{a_2}{m}\right)$.

(v) Se m, n são ímpares primos entre si então $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$.

(vi) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$.

(vii) $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.

(viii) Se b_1 e b_2 são ímpares satisfazendo $b_1 \equiv b_2 (\mathrm{mod}\ 4a)$ então $\left(\frac{a}{b_1}\right) = \left(\frac{a}{b_2}\right)$.

Por último, podemos estender o símbolo de Jacobi para qualquer inteiro de forma similar ao que fizemos para estender o símbolo Lagrange definindo

$$\left(\frac{a}{2}\right) = \begin{cases} 0, \text{ se } a \text{ é par} \\ 1 \text{ se } a \equiv \pm 1 (\mathrm{mod}\ 8) \\ -1, \text{ se } a \equiv \pm 3 (\mathrm{mod}\ 8)) \end{cases}$$

$$\left(\frac{a}{0}\right) = \begin{cases} 1, \text{ se } a < 0 \\ 0, \text{ em outro caso} \end{cases}$$

e

$$\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$$

para todos os inteiros m e n.

Dado um inteiro q, uma função $\chi : \mathbb{Z} \to \mathbb{C}$ é um caráter de Dirichlet (ou simplesmente caráter) módulo q se satisfazer as seguintes propriedades:

(1) χ é periódica módulo q, i.e., $\chi(n+q) = \chi(q)$ para todo $n \in \mathbb{Z}$.

(2) χ é completamente multiplicativa,i.e.,$\chi(mn) = \chi(m)\chi(n)$ para todos $n, m \in \mathbb{Z}$.

(3) $\chi n \neq 0$ se, e somente se, $(n, q) = 1$.

Assim, denotando a extensão do símbolo de Jacobi por símbolo de Kronecker, essa extensão possuirá as seguintes propriedades

(i) $\left(\frac{a}{m}\right) = 0$ se $(a, m) \neq 1$.

(ii) A função $x \to \left(\frac{x}{a}\right)$ é um caráter módulo $|a|$.

(iii) A função $x \to \left(\frac{a}{x}\right)$ é um caráter módulo igual a $4|a|$, caso $a \equiv 3 (\mathrm{mod}\ 4)$, e módulo $|a|$, caso $a \equiv 1 (\mathrm{mod}\ 4)$ ou quando 4 divide a.

Os símbolos de Legendre, Jacobi e Kronecker, e suas propriedades, serão muito úteis no decorrer do capítulo 4.

2.7 Discriminante de um corpo de números e número de classes

Faremos várias afirmações nessa seção cujas demonstrações podem ser vistas em (24). Dado $K/\mathbb{Q}$ extensão finita, dizemos que o *anel de inteiros* de K é o conjunto dos elementos de K que são raizes de algum polinômio mônico de $\mathbb{Z}[x]$, e o denotamos por O_K. Por (24, p.12-13) sabemos existir uma $\mathbb{Z}$-base de O_K, visto como um $\mathbb{Z}$-módulo, que também é uma base de K, visto como um espaço vetorial sobre $\mathbb{Q}$. Denotando por $\{\sigma_i\}_{1 \leq i \leq n}$, $n = [K : \mathbb{Q}]$, os mergulhos de K sobre $\mathbb{C}$ que fixam $\mathbb{Q}$ e por $\{\alpha_1, ..., \alpha_n\}$ uma $\mathbb{Z}$-base de O_K, considere

$$d(\alpha_1, ..., \alpha_n) = \mathrm{Det}([\sigma_i(\alpha_j)])^2.$$

Este número é independente da $\mathbb{Z}$-base de O_K escolhida, e é chamado de *discriminante* do corpo numérico K, d_K. O conjunto dos O_K-submódulos finitamente gerados de K podem ser equipados com as operações de soma e produto

$$A + B = \{a + b | a \in A, b \in B\}$$

$$AB = \{\sum_i a_i b_i | a_i \in A, b_i \in B\},$$

e este conjunto, equipado com a operação de produto, é um grupo abeliano, o grupo ideal J_K de K. O conjunto P_K dos conjuntos do tipo aO_K,$a \in K^*$, é um subgrupo de J_K, chamado de grupo de ideais principais de O_K. Pode-se provar (veja ([24], p.36)) que o grupo quociente $J_K/P_K = Cl_K$ é finito, e o índice

$$h_K = [J_K : P_K]$$

é chamado de *número de classe* de K. Com esses conceitos já estabelecidos, podemos citar dois fatos que serão fundamentais neste trabalho. Em Disquisitiones([9]), Gauss provou que $r_3(n) = \#\{(x, y, z) \in \mathbb{Z}^3; x^2 + y^2 + z^2 = n\}$ está relacionado à classe de número h_n da extensão quadrática $\mathbb{Q}(\sqrt{-n})$,n inteiro positivo. Mais exatamente, se d denota o discriminante de $\mathbb{Q}(\sqrt{-n})$, Gauss mostrou que, se n é livre de quadrados

$$r_3(n) = \frac{24h_n}{W(n)}\left(1 - \left(\frac{d}{2}\right)\right),$$

onde $\left(\frac{d}{2}\right)$ denota o símbolo de Kronecker e $W(n)$ o número de raízes da unidade em $\mathbb{Q}(\sqrt{-n})$, que tem cardinalidade

$$W(n) = \begin{cases} 4, \text{ se } n = 1 \\ 6, \text{ se } n = 3 \\ 2, \text{ se } n = 2 \text{ ou } n > 3 \end{cases}$$

O outro resultado que será importante aqui é o que Siegel provou, e que pode também ser visto em ([14]):

$$h_n \gg_\epsilon |d|^{1/2-\epsilon}.$$

Por último, é conhecido que o valor de d para $\mathbb{Q}(\sqrt{-n})$ é dado por

$$d = \begin{cases} n, \text{ quando } n \equiv 1 (\text{mod } 4) \\ 4n, \text{ quando } n \equiv 2, 3 (\text{mod } 4) \end{cases}$$

2.8 Alguns resultados de análise

Será enunciado em sequência uma série de resultados bem conhecidos que usaremos no decorrer deste trabalho, veja ([12], p.56) para ver a prova do primeiro resultado e ([27]) para ver

a prova do restante.

Definição 2.8 *Uma função de contradomínio $\mathbb{C}$ é denominada função aritmética se seu domínio é o conjunto dos números inteiros positivos, $\mathbb{Z}_{>0}$.*

Teorema 2.1 *(Soma por partes) Considere $a : \mathbb{Z}_{>0} \to \mathbb{C}$ função aritmética, $0 < y < x$ reais e $f : [y, x] \to \mathbb{C}$ uma função com derivada f' contínua em $[y, x]$. Então*

$$\sum_{y<n\leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt,$$

onde $A(t) = \sum_{n\leq t} a(n)$.

Definição 2.9 *Dados $x = (x_1, ..., x_d)$ e $a = (a_1, a_2, ..., a_d)$ em $\mathbb{R}^d$, com cada inteiro $a_i \geq 0$, definimos*

$$x^a = x_1^{a_1} x_2^{a_2} ... x_d^{a_d} \in \mathbb{R}.$$

Definimos também o operador

$$\left(\frac{\partial}{\partial x}\right)^a = \frac{\partial^{s_a}}{\partial x_1^{a_1} \partial x_2^{a_2} ... \partial x_d^{a_d}},$$

onde $s_a = a_1 + ... + a_d$.

Definição 2.10 *O espaço das funções Schwartz em $\mathbb{R}^d$ o é conjunto das funções infinitamente diferenciáveis $f : \mathbb{R}^d \to \mathbb{C}$ que satisfazem*

$$\sup_{x\in\mathbb{R}^d} \left| x^a \left(\frac{\partial}{\partial x}\right)^b f(x) \right| < \infty$$

para cada $a = (a_1, ...a_d)$ e $b = (b_1, ..., b_d)$ em $\mathbb{R}^d$, com a_i, b_i maiores que 0 para cada i. Chamamos uma função desse conjunto de função de classe Schwartz.

Definição 2.11 *A transformada de Fourier de uma função de classe Schwartz f em $\mathbb{R}^d$ é definida por*

$$\hat{f}(\xi) = \int_{\mathbb{R}^d} f(x)e^{-2\pi i\langle x,\xi\rangle} dx,$$

onde $<, >$ denota o produto interno canônico do $\mathbb{R}^d$.

Teorema 2.2 *(Fórmula de inversão de Fourier- Versão contínua) Se f é uma função de classe Schwartz em $\mathbb{R}^d$, então $\hat{f}$ também será de classe Schwartz, e*

$$f(x) = \int_{\mathbb{R}^d} \hat{f}(\xi)e^{2\pi i\langle x,\xi\rangle} d\xi.$$

Teorema 2.3 *(Fórmula do somatório de Poisson) Se f é uma função de classe Schwartz em $\mathbb{R}^d$*

então

$$\sum_{m\in\mathbb{Z}^d} f(m) = \sum_{m\in\mathbb{Z}^d} \hat{f}(m).$$

Definição 2.12 *Seja $F : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$, $N > 0$ inteiro positivo. A transformada discreta de Fourier de F é definida por*

$$\hat{F}(m) = \frac{1}{N}\sum_{n=0}^{N-1} F(n)e^{-2\pi inm/N} \ \ \forall m \in \mathbb{Z}/N\mathbb{Z}.$$

Teorema 2.4 *(Fórmula de inversão de Fourier-Versão discreta) Seja $F : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$, $N > 0$ inteiro positivo. Então*

$$F(n) = \sum_{m=0}^{N-1} \hat{F}(m)e^{2\pi inm/N}.$$

3 FORMAS MODULARES

Será apresentada nesse capítulo a noção de forma modular. Primeiramente apresentaremos a definição e as propriedades básicas de formas modulares de peso inteiro e de peso meio inteiro. Logo após, serão definidas as séries de Eisenstein e de Poincaré, e concluiremos que o conjunto dessas últimas geram o espaço das formas cuspidais. Tendo em mente o objetivo de estimar os coeficientes de Fourier de formas cuspidais, será apresentada no fim uma fórmula para os coeficientes de Fourier de séries de Poincaré.

3.1 Formas modulares de peso inteiro

Para cada $\lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ definimos

$$J(\lambda, z) := cz + d.$$

Uma conta simples nos permitirá ver que as seguintes relações são válidas para todos os α, β pertencentes a $SL_2(\mathbb{Z})$ e z em $\mathbb{H}$

(i) $J(\alpha\beta, z) = J(\alpha, \beta z)J(\beta, z)$
(ii) $J(\alpha^{-1}, z) = J(\alpha, \alpha^{-1}z)^{-1}$
(iii) $Im(\alpha z) = Im(z)/|J(\alpha, z)|^2$.

Dados k inteiro, $f : \mathbb{H} \to \mathbb{C}$ e $\lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ elemento de $SL_2(\mathbb{Z})$, definimos também

$$f|_k\lambda(z) := J(\lambda, z)^{-k} f(\lambda z) \ \ \forall z \in \mathbb{H},$$

por (i) se pode concluir que

$$f|_k\alpha\beta = (f|_k\alpha)|_k\beta \ \ \forall \alpha, \beta \in SL_2(\mathbb{Z}).$$

Se $f : \mathbb{H} \to \mathbb{C}$ é holomorfa e k um inteiro par, dizemos que f é uma *função modular*, ou *forma modular*, de peso k em relação a $SL_2(\mathbb{Z})$ se $f(\gamma z) = J(\gamma, z)^k f(z)$ para todo γ em $SL_2(\mathbb{Z})$ e $f(z)$ é uniformemente limitado quando $Im(z)$ tende ao infinito, isto é, dado $\epsilon > 0$, existe $M_\epsilon > 0$ tal que $|f(z)| < \epsilon \ \forall z$ satisfazendo $Im(z) > M_\epsilon$.

Uma função modular satisfaz a relação $f(z+1) = f(z)$ para todo z em $\mathbb{H}$, uma vez que $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ pertence a $SL_2(\mathbb{Z})$, logo toda função modular em relação a $SL_2(\mathbb{Z})$ f pode ser escrita da forma $f(z) = g(e^{2\pi iz})$, onde g é uma função holomorfa em $\mathbb{D} - \{0\} = \{z \in \mathbb{C}; 0 < |z| < 1\}$. A expansão de Laurent de g no ponto $z = 0$ fornecerá uma série $\sum_{-\infty}^{\infty} a_n z^n$ cujo os coeficientes a_{-n}, $n > 0$, são nulos, uma vez que a definição de função modular implicará que g terá de ser limitada nas vizinhanças do ponto $z = 0$.

Definição 3.1 *Seja $f(z) = g(e(z))$ uma função modular. Se $g(z) = \sum_{n=0}^{\infty} a_n z$ é a expansão de Laurent de g em $z = 0$, definimos a série de Fourier de f como*

$$f(z) = g(e(z)) = \sum_{n=0}^{+\infty} a_n e(nz).$$

É comum também a série de Fourier de f ser chamada de *q-expansão* e ser denotada do seguinte modo

$$f(z) = \sum_{n=0}^{+\infty} a_n q^n,$$

onde $q = e^{2\pi iz}$. Dizemos que uma função holomorfa $f : \mathbb{H} \to \mathbb{C}$ se *anula* no infinito se $f(z)$ tende uniformemente para 0 quando $Im(z)$ tende a ∞ , o que é equivalente a dizer que o termo a_0 de sua q-expansão é 0.

Definição 3.2 *Considere Γ um grupo de congruência e k um inteiro par. Uma função holomorfa $f : \mathbb{H} \to \mathbb{C}$ irá satisfazer a condição de modularidade de peso k em relação a Γ se para todo α pertencente a Γ*

$$f(\alpha z) = J(\alpha, z)^k f(z).$$

Definição 3.3 *Uma função f que satisfaz a condição de modularidade de peso k em relação ao grupo de congruência Γ é holomorfa na cúspide p de Γ se, dado $\alpha \in SL_2(\mathbb{Z})$ satisfazendo $\alpha(\infty) = p$, a função*

$$z \mapsto f|_k\alpha(z) = J(\alpha, z)^{-k} f(\alpha(z))$$

for uniformemente limitada no infinito. Dizemos que f se anula na cúspide p se $f|_k\alpha(z)$ tende a zero quando $Im(z) \to \infty$.

Com o definição acima em mãos, podemos estender o conceito de forma modulares dado anteriormente para subgrupos de congruência.

Definição 3.4 *Seja $f : \mathbb{H} \to \mathbb{C}$ holomorfa, k um inteiro par e Γ um subgrupo de congruência de $SL_2(\mathbb{Z})$. Dizemos então que f é uma forma modular, de peso k em relação a Γ se ela satisfaz as seguintes condições:*
(1) Satisfaz a condição de modularidade de peso k em relação a Γ.
(2) f é holomorfa em cada uma de suas cúspides.
Denotamos o conjunto dessas funções por $M_k(\Gamma)$.

Uma forma modular f que se anula em todas as suas cúspides é chamada de *forma cuspidal*, e denotamos o conjunto das formas cuspidais de peso inteiro k de Γ por $S_k(\Gamma)$. O fato de existir N inteiro tal que Γ contenha $\Gamma(N)$ implica que Γ_∞ contém algum elemento diferente da identidade, por exemplo $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$. Faça $m = min \left\{ n \in \mathbb{Z}_{>0}; \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in \Gamma \right\}$. Se

f pertence a $M_k(\Gamma)$, temos que $f(z+m) = f(z)$ para todo elemento z de $\mathbb{H}$, e logo $f^*(z) = f(mz)$ terá período 1. A exemplo do que se fez antes, podemos tomar $f^*(z) = \sum_{n=0}^{\infty} a_n e(nz)$, e uma mudança simples de variável nos dará

$$f(z) = \sum_{n=0}^{+\infty} a_n e^{2\pi niz/m} = \sum_{n=0}^{+\infty} a_n q^n,$$

e dizemos que essa é a série de Fourier de f no infinito. Considere p uma cúspide de Γ e $\alpha \in SL_2(\mathbb{Z})$ novamente satisfazendo $\alpha(\infty) = p$. A função $f|_k\alpha(z) = J(\alpha, z)^{-k} f(\alpha z)$ será modular de peso k em relação a $\alpha^{-1}\Gamma\alpha$, sendo possível então construir sua série de Fourier no infinito exatamente como foi feito anteriormente. Assim, será dito que a série de Fourier de f em relação à cúspide p é a série de Fourier de $f|_k\alpha$ no infinito, dada por

$$f|_k\alpha(z) = \sum_{n=0}^{\infty} a_n^{(p)} e(\frac{nz}{h}),$$

onde $h = min\left\{n \in \mathbb{Z}_{>0}; \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in \alpha^{-1}\Gamma\alpha\right\}$. De forma equivalente ao que foi proposto anteriormente, f se anulará na cúspide p se, e só se, $a_0^{(p)} = 0$. É importante ressaltar que essa série está bem definida, isto é, a série independe do α tomado satisfazendo $\alpha(\infty) = p$ e depende apenas da classe da cúspide p em relação a Γ (veja ([23], p.39)).

Proposição 3.1 *Seja $f : \mathbb{H} \to \mathbb{C}$ função que satisfaz a condição de modularidade de peso k em Γ, k inteiro par. Então f é cuspidal se, e somente se, $f(z)Im(z)^{\frac{k}{2}}$ é limitado em $\mathbb{H}$.*

Prova: Considere p uma cúspide de Γ e $\alpha \in SL_2(\mathbb{Z})$ satisfazendo $\alpha(\infty) = p$, e $m = min\left\{n \in \mathbb{Z}_{>0}; \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in \alpha^{-1}\Gamma\alpha\right\}$. Suponha primeiro que $f(z)Im(z)^{\frac{k}{2}}$ seja limitado por uma constante $M > 0$ em $\mathbb{H}$. Então, usando que $Im(\alpha z) = J(\alpha, z)^{-2} Im(z) \forall z \in \mathbb{H}$

$$|f|_k\alpha(z)| = |J(\alpha, z)^{-k} f(\alpha z)| = |J(\alpha, z)^{-k} Im(\alpha z)^{-\frac{k}{2}} f(\alpha z)(Im(\alpha z))^{\frac{k}{2}}|$$

$$\leq Im(z)^{-\frac{k}{2}} M \to 0$$

quando $Im(z) \to \infty$, e como p é uma cúspide arbitrária isso mostra que f é cuspidal. Suponha agora que f é cuspidal, e tomemos $g(z) = |f(z)|Im(z)^{\frac{k}{2}}$. Para todo $\gamma \in \Gamma$ temos $g(\lambda z) = |f(\lambda z)|Im(\lambda z)^{\frac{k}{2}} = |f(z)|Im(z)^{\frac{k}{2}} = g(z)$, logo só precisaremos analisar o comportamento de g em relação a um domínio fundamental $\mathcal{F}$ de Γ, que podemos supor contido numa faixa $-N \leq |Re(z)| \leq N$ para algum $N > 0$. Uma vez que Γ possui um número finito de cúspides não equivalentes e que as "vizinhanças"do infinito seriam faixas do tipo $\{|Re(z)| \leq N, Im(z) > C\}$, basta mostrar que f é limitada nas proximidades das cúspides de Γ. De fato, retirando vizinhanças de cada cúspide do domínio $\mathcal{F}$, obtemos um conjunto compacto, onde f é limitado por ser holomorfa. Assim, tomando a cúspide arbitrária p e $\sum_{n=1}^{\infty} a_n e(\frac{nz}{m})$ a série de Fourier de

f em relação à cúspide p, e novamente usando que $Im(\alpha z) = |J(\alpha, z)|^{-2} Im(z) \forall z \in \mathbb{H}$

$$\begin{aligned} g(\alpha z) &= |f(\alpha z)| Im(\alpha z)^{\frac{k}{2}} \\ &= |f|_k \alpha(z)| Im(z)^{\frac{k}{2}} \\ &= \left| \sum_{n=1}^{\infty} a_n e\left(\frac{(n-1)z}{m}\right) \right| e^{\frac{-2\pi Im(z)}{m}} Im(z)^{\frac{k}{2}} \to 0 \end{aligned}$$

quando $Im(z) \to \infty$, o que prova que g é limitada nas proximidades que qualquer uma das cúspide de Γ.$\square$

Vamos enunciar agora a nossa primeira estimativa a envolver coeficientes de séries de Fourier de formas cuspidais.

Proposição 3.2 *Seja k um inteiro par e seja f em $S_k(\Gamma)$ uma forma modular com coeficientes de Fourier a_n em relação a uma cúspide p de Γ. Então*

$$a_n \ll n^{k/2}.$$

Prova: Suponha $p = \infty$. Pela proposição anterior, $\exists M > 0$ satisfazendo $|f(z)| \leq M Im(z)^{-\frac{k}{2}}$. Portanto, se $f(z) = \sum_{n=1}^{\infty} a_n e(\frac{nz}{m})$

$$|a_n| = \frac{1}{2m} \left| \int_0^{2m} f(x+iy) e^{\frac{-\pi i n(x+yi)}{m}} dx \right| \leq M y^{-\frac{k}{2}} e^{\frac{\pi n y}{m}}$$

Fazendo $y = \frac{2}{n}$, obtemos $|a_n| \leq L n^{\frac{k}{2}}$ com $L = M e^{\frac{2\pi}{m}} 2^{-\frac{k}{2}}$. Cálculo análogo pode ser feito para concluir que os coeficientes de Fourier em relação as outras cúspides satisfazem a mesma relação. $\square$

Essa não é a melhor estimativa possível para os coeficientes de Fourier de formas cuspidais de peso inteiro. Ramanujan conjecturou, em um caso particular, que $a_n = O_\epsilon(n^{\frac{k-1}{2}+\epsilon})$. Este fato foi posteriormente demonstrado por Deligne em (5).

As formas modulares de peso inteiro são um caso particular de funções chamadas *formas automorfas*, que estende o conceito de funções modulares a grupos fuchsianos quaisquer de $SL_2(\mathbb{R})$. O conjunto das formas automorfas de peso inteiro k em relação a um subgrupo fuchsiano Γ é um espaço vetorial de dimensão finita sobre $\mathbb{C}$ (veja (23, p.57-61)). O argumento usado para mostrar isto usa o fato de que se pode dar ao domínio fundamental de Γ uma estrutura de superfície de Riemann, e nesse contexto é possível aplicar o *teorema de Riemann-Roch*. Tal argumento pode ser adaptado até mesmo para provar a finitude da dimensão do conjunto das *formas modulares de peso meio-inteiro* de peso k em relação a $\Gamma_0(4N)$, N inteiro, funções essas que serão definidas na próxima seção.

3.2 Formas modulares de peso meio inteiro

Antes de mais nada, é importante evitar problemas ao se falar de raízes quadradas nos complexos. E é esse o motivo que fez essa ser a primeira definição desta seção.

Definição 3.5 *Seja $z \in \mathbb{C}$ com forma polar $z = r(\cos\theta + i\sin\theta)$, onde $r > 0$ e $\theta \in (-\pi, \pi]$. Definimos a raiz quadrada do complexo z por*

$$\sqrt{z} = \sqrt{r}(\cos(\theta/2) + i\sin(\theta/2)).$$

Se n é inteiro, definimos $z^{\frac{n}{2}} = (\sqrt{z})^n$.

Dado γ em $\Gamma_0(4)$, definimos o fator automórfico $j(\gamma, z)$ por

$$j(\gamma, z) := \frac{\theta(\gamma z)}{\theta(z)},$$

onde a função theta θ é definida por

$$\theta(z) = \sum_{n=-\infty}^{+\infty} e(n^2 z).$$

Pode ser visto que, se $\lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, então (veja ([25], p.11-12))

$$j(\gamma, z) = \left(\frac{c}{d}\right) \varepsilon_d^{-1} (cz + d)^{\frac{1}{2}},$$

onde $\left(\frac{c}{d}\right)$ indica o símbolo de Kronecker e $\varepsilon_d = i^{(\frac{d-1}{2})^2}$ é igual a 1 ou i dependendo se $d \equiv 1$ ou $3 \pmod 4$, respectivamente. Dizemos que uma função $f : \mathbb{H} \to \mathbb{C}$ satisfaz a *condição de modularidade de peso k*, k meio inteiro, em relação a Γ, subgrupo de índice finito de $\Gamma_0(4)$, se $f(\lambda z) = j(\lambda, z)^{2k} f(z)$ para todo λ em Γ. Definiremos a partir de agora a série de Fourier de uma função f que satisfaz a condição de modularidade de peso k, k meio inteiro, em relação a $\Gamma(N)$, N inteiro múltiplo de 4, e para isso vamos fazer uma construção um pouco mais complexa daquela feita para formas modulares de peso inteiro. Tal construção pode ser vista com mais detalhes em ([17], p.177-182) ou em ([26]). Considere $GL_2(\mathbb{Q})^+$ o grupo das matrizes 2×2 de determinante positivo e entradas racionais agindo em $\mathbb{H} \cup \mathbb{R} \cup \{\infty\}$ da forma $\lambda z = \frac{az+b}{cz+d}$ para todo $\lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ em $GL_2(\mathbb{Q})^+$. Dados $\lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ pertencentes a $GL_2(\mathbb{Q})^+$ e $t \in \{\pm 1\}$, considere uma função holomorfa ϕ que satisfaz

$$\phi(z)^2 = t\frac{cz + d}{\sqrt{ad - bc}}.$$

Observe que, para cada λ em $GL_2(\mathbb{Q})^+$, temos exatamente 4 possibilidades para a função ϕ.

Considere agora o seguinte conjunto G

$$G = \{(\lambda, \phi); \lambda \in GL_2(\mathbb{Q})^+\}.$$

Pode-se mostrar (veja ([17], p.179)) que G equipado com a seguinte operação

$$(\lambda_1, \phi_1)(\lambda_2, \phi_2) = (\lambda_1\lambda_2, \phi_1(\lambda_2 z)\phi_2(z))$$

é um grupo, e a função $P : G \to GL_2(\mathbb{Q})^+$ definida pela projeção $(\lambda, \phi) \to \lambda$ é um homomorfismo entre esses dois grupos. Dado $\xi = (\alpha, \phi) \in G$ e $h : \mathbb{H} \to \mathbb{C}$, definamos

$$\begin{aligned} h|_k[\xi] &= \phi(z)^{-2k} h(\alpha z) \\ h(\xi z) &= h(\alpha z). \end{aligned}$$

Uma conta simples nos mostra que $h|_k[\xi_1\xi_2] = h|_k[\xi_1]|_k[\xi_2]$. Dado Γ subgrupo de $\Gamma_0(4)$, defina os seguintes subgrupos de G

$$\begin{aligned} G^1 &= \{(\lambda, \phi); \lambda \in SL_2(\mathbb{Z})\} \\ G^1_\infty &= \{(\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, t); n \in \mathbb{Z}\} \\ \Gamma^* &= \{(\lambda, j(\lambda, z)); \lambda \in \Gamma\} \\ \Gamma^*_s &= \{\omega \in \Gamma^*; \omega s = s\}. \end{aligned}$$

Seja agora s uma cúspide de Γ e $\xi = (\alpha, \phi)$ em G^1 tal que $\alpha\infty = s$. O conjunto $\xi^{-1}\Gamma^*_s\xi$ está claramente contido em G^1_∞, e pode-se mostrar (veja ([17], p.181)) que existe $(\begin{pmatrix} 1 & l \\ 0 & 1 \end{pmatrix}, t)$ em G^1_∞ com $l > 0$ tal que

$$\pm\xi^{-1}\Gamma^*_s\xi = \{(\pm \begin{pmatrix} 1 & l \\ 0 & 1 \end{pmatrix}, t)^j; j \in \mathbb{Z}\},$$

e mais que isso, tal elemento gerador depende apenas da classe da cúspide s em relação a Γ . Se $s = \infty$, então $\pm\Gamma_\infty = \{\pm \begin{pmatrix} 1 & l \\ 0 & 1 \end{pmatrix}^j, j \in \mathbb{Z}\}$ onde $l > 0$, e como f satisfaz a condição de modularidade de peso k em Γ temos que $f(z + l) = f(z)$ para todo z em $\mathbb{H}$, e portanto podemos tomar a série de Fourier de f em relação a ∞ como

$$f(z) = \sum_{n=-\infty}^{+\infty} a_n e^{2\pi n i z/l} = \sum_{n=-\infty}^{+\infty} a_n q^n.$$

No caso particular $\Gamma = \Gamma(4N)$, como $\Gamma(4N)_\infty = \{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^j ; j \in \mathbb{Z}\}$, a série de Fourier de f

no infinito torna-se

$$f(z) = \sum_{n=-\infty}^{+\infty} a_n e^{2\pi niz} = \sum_{n=-\infty}^{+\infty} a_n q^n.$$

Caso $s \neq \infty$ faça $g(z) = f|_k[\xi](z)$. Observe que, pela definição de Γ^* , temos $f|k[\omega] = f \ \forall \omega \in \Gamma^*$. Portanto, dado $\pm\xi^{-1}\omega\xi$ em $\pm\xi^{-1}\Gamma^*\xi$

$$g|_k[\pm\xi^{-1}\omega\xi] = f|_k[\pm\xi\xi^{-1}\omega\xi] = f|_k[\omega\xi] = f|_k[\xi] = g,$$

logo g é invariante por $\pm\xi^{-1}\Gamma^*\xi$, e consequentemente é invariante por $(\begin{pmatrix} 1 & l \\ 0 & 1 \end{pmatrix}, t)$:

$$g(z) = g|_k[(\begin{pmatrix} 1 & l \\ 0 & 1 \end{pmatrix}, t)](z) = t^{-2k} g(z + l).$$

Por último, tomando $t^{2k} = e^{2\pi ir}$ onde $r = 0, \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$, e $F(z) = e^{-2\pi irz/l} g(z)$

$$F(z + l) = t^{-2k} e^{-2\pi irz/l} g(z + l) = e^{-2\pi irz/l} g(z) = F(z).$$

Assim, definimos a série de Fourier de f em relação à cúspide s como a série obtida através da função $F(z)$, que pode ser escrita como $F(z) = \sum_{n=-\infty}^{+\infty} a_n e^{2\pi inz/l}$:

$$g(z) = \sum_{n=-\infty}^{+\infty} a_n e^{2\pi in(z+r)/l} = e^{2\pi irz/l} \sum_{n=-\infty}^{+\infty} a_n q^n.$$

Em particular, se $\Gamma = \Gamma(4N)$, N inteiro, temos

$$g(z) = \sum_{n=-\infty}^{+\infty} a_n e^{2\pi in(z+r)}.$$

Dizemos que f é meromorfa em s se existe um inteiro m tal que $a_n = 0$ para todo $n < m$, holomorfa em s se $a_n = 0$ para todo $n < 0$, e que f se anula em s se $a_n = 0$ para todo $n \leq 0$. Agora temos condições de definir o que é uma forma modular de peso meio inteiro k, como faremos a seguir.

Definição 3.6 *Seja $f : \mathbb{H} \to \mathbb{C}$ uma função holomorfa e $k \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$. Dizemos que f é uma função modular, ou forma modular, de peso k em relação a $\Gamma_0(4N)$, N inteiro, se*
(1) $f(\gamma z) = (j(\gamma, z))^{2k} f(z)$, para $\gamma \in \Gamma_0(4N)$
(2) f(z) é holomorfa em cada cúspide.

Novamente chamamos uma função modular de peso meio inteiro k que se anula em cada cúspide de *forma cuspidal*. Conforme fizemos com as formas de peso inteiro, denotamos o conjunto das funções modulares de $\Gamma_0(4N)$ de peso k por $M_k(\Gamma_0(4N))$, tal como o conjunto das

formas cuspidais de $M_k(\Gamma_0(4N))$ por $S_k(\Gamma_0(4N))$. Usando um raciocínio análogo ao feito nas proposições 3.1 e 3.2, observando que a função $G(z) = |Im(z)^{\frac{k}{2}} f(z)|$ é invariante em $\Gamma_0(4N)$ para todo f em $M_k(\Gamma_0(4N))$, concluímos que também são válidas as seguintes afirmações para o caso meio inteiro

Proposição 3.3 *Seja $f : \mathbb{H} \to \mathbb{C}$ função que satisfaz a condição de modularidade de peso meio inteiro k em $\Gamma_0(4N)$. Então f é cuspidal se, e somente se, $f(z)Im(z)^{\frac{k}{2}}$ é limitado em $\mathbb{H}$.*

Proposição 3.4 *Seja $f \in S_k(\Gamma(4N))$, k meio inteiro com coeficientes de Fourier a_n em relação a uma cúspide p de Γ. Então*

$$a_n \ll n^{k/2}.$$

Considerando $S_k(\Gamma)$ como um espaço vetorial sobre $\mathbb{C}$, podemos tomar nele um produto interno chamado *produto interno de Petersson*. Dados f, g elementos de $S_k(\Gamma)$ e $\mathcal{F}$ o domínio fundamental de Γ, esse produto interno é definido por

$$\langle f, g \rangle = \int_{\mathcal{F}} f(z)\overline{g(z)} Im(z)^k \frac{dxdy}{y^2}.$$

Observe que $f(z)\overline{g(z)}Im(z)^k$ é invariante por Γ, logo a integral acima independe do domínio fundamental escolhido. Mais ainda, pode-se concluir que esta integral converge.

É possível generalizar a noção de função theta para um polinômio harmônico esférico P de grau $v \geq 0$ em $\mathbb{R}^n$. Dado $r > 0$ inteiro, definimos

$$\theta_P(z) = \sum_{m \in \mathbb{Z}^r} P(m) e(|m|^2 z) = \sum_{t=0}^{t=\infty} \left(\sum_{|m|^2 = t} P(m) \right) e(tz). \tag{3.5}$$

Proposição 3.5 *Se P for um polinômio harmônico esférico de grau $v > 0$ par, a função θ_P definida acima é uma forma modular cuspidal de peso $\frac{r}{2} + v$.*

Prova: Considere A uma matriz $r \times r$ simétrica cujo todos seus autovalores são positivos (positiva definida). Um polinômio homogêneo de grau v, $P(x_1, ..., x_r)$, com coeficientes complexos é dito um polinômio esférico de grau v com respeito a A se ele satisfazer a relação

$$\Delta_A P = \sum_{i,j=1}^{r} b_{i,j} \frac{\partial P}{\partial x_i \partial x_j} = 0,$$

onde $A^{-1} = [b_{i,j}]$. Tomemos também h um vetor coluna de tamanho r e um inteiro N que satisfaçam

(1) NA^{-1} é uma matriz com coordenadas inteiras.

(2) Ah é um vetor coluna de tamanho r onde cada elemento é um inteiro múltiplo de N.

Definimos a função

$$\theta^*(z;h,A,N,P)=\sum_{m\equiv h(\mathrm{mod}\ N)} P(m)e\left(\frac{{}^tmAm}{2N^2}z\right).$$

Se $k=r/2+v$, pode-se usar a fórmula do somatório de Poisson para se concluir que (veja (23, p.185-191) ou (26)) θ^* é holomorfa em $\mathbb{H}$ e que satisfaz as seguintes relações:
(1)

$$\theta^*(-1/z;h,A,N,P)=(-i)^v(Det(A))^{-1/2}(-iz)^k \sum_{\substack{l\in\mathbb{Z}/\mathbb{Z}^r\\ Al\equiv 0\ mod\ N}} e\left(\frac{{}^tlAl}{2N^2}\right)\theta^*(z;h,A,N,P)$$

(2)

$$\theta^*(z+2;h,A,N,P)=e\left(\frac{{}^thAh}{N^2}\right)\theta^*(z;h,A,N,P)$$

(3) Se $\lambda=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL_2(\mathbb{Z})$ satisfaz $2|b$ e $2N|c$, então

$$\theta^*(\lambda z;h,A,N,P)=e\left(ab\frac{{}^thAh}{2N^2}\right)\left(\frac{Det(A)}{d}\right)\left(\frac{2c}{d}\right)^r\varepsilon_d^{-r}(cz+d)^k\theta^*(z;ah,A,N,P),$$

onde $\left(\frac{x}{y}\right)$ indica o símbolo de Jacobi.

Observando que o conjunto $W_N=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL_2(\mathbb{Z});2|b,2N|c\right\}$ satisfaz

$$\sigma\Gamma_0(4N)\sigma^{-1}=W_N,\ \ \sigma=\begin{pmatrix}\sqrt{2} & 0\\ 0 & \frac{\sqrt{2}}{2}\end{pmatrix},$$

pois

$$\sigma\begin{pmatrix}a & b\\ c & d\end{pmatrix}\sigma^{-1}=\begin{pmatrix}a & 2b\\ \frac{c}{2} & d\end{pmatrix},$$

podemos concluir por (3) que a função $\theta(z;h,A,N,P)=\theta^*(2z;h,A,N,P)$ satisfaz $\forall\lambda=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\Gamma_0(4)$

$$\theta(\lambda z;h,A,N,P)=e\left(ab\frac{{}^thAh}{N^2}\right)\left(\frac{Det(A)}{d}\right)\left(\frac{c}{d}\right)^r\varepsilon_d^{-r}(cz+d)^k\theta(z;ah,A,N,P).$$

Observando que $\theta_P(z)=\theta(z;0,I_d,1,P)$ e usando o fato de $2v$ ser múltiplo de 4 , concluímos da afirmação acima que θ_P satisfaz a condição de modularidade para $k=\frac{r}{2}+v$ e $\Gamma=\Gamma_0(4)$. A definição de θ_P em (3.5) nos dá sua série de Fourier em relação ao ∞, mostrando que ela se

anula no infinito se $v > 0$. (1) nos dá que

$$\theta_P(-1/4z) = (-4iz)^k \theta_P(z). \tag{3.6}$$

Defina a função $g(z) = |Im(z)^{\frac{k}{2}}\theta_P(z)|$, ela é invariante em $\Gamma_0(4)$ por θ_P satisfazer a condição de modularidade de peso k em $\Gamma_0(4)$. Pela proposição 3.3, para provar que θ_P é cuspidal basta provar que g é limitada em um domínio fundamental de $\Gamma_0(4)$, que podemos supor estar contido na faixa $-\frac{1}{2} \leq |Re(z)| \leq \frac{1}{2}$. Se $\theta_P(z) = \sum_{n=1}^{\infty} a_n e^{2\pi inz}$ então $g(z) = |Im(z)^{\frac{k}{2}} e^{-2\pi Im(z)}| \, |\sum_{n=0}^{\infty} a_{n+1} e^{2\pi inz}| \to 0$ se $Im(z) \to \infty$, portanto existe uma faixa $\{-\frac{1}{2} \leq |Re(z)| \leq \frac{1}{2}, Im(z) > M_1\}$ onde g é limitada. Já da relação (3.6),

$$\begin{aligned} g(z) &= |Im(z)^{\frac{k}{2}} 4^{-k} z^{-k} \theta_P(-1/4z)| \\ &= |Im(z)^{\frac{k}{2}} 4^{-k} z^{-k}| |\sum_{n=1}^{\infty} a_n e^{-\pi in/2z}| \\ &= |Im(z)^{\frac{k}{2}} 4^{-k} z^{-k} e^{-\pi Im(z)/2|z|^2}| |\sum_{n=0}^{\infty} a_{n+1} e^{-\pi in/2z}| \to 0 \end{aligned}$$

uniformemente na faixa $-\frac{1}{2} \leq |Re(z)| \leq \frac{1}{2}$ quando $Im(z) \to 0$. Assim existe uma faixa $\{-\frac{1}{2} \leq |Re(z)| \leq \frac{1}{2}, 0 < Im(z) < M_2\}$, com $M_2 < M_1$ aonde g é limitada. Por último, g é limitado no compacto $\{-\frac{1}{2} \leq |Re(z)| \leq \frac{1}{2}, M_1 \leq Im(z) \leq M_2\}$ por ser contínua em $\mathbb{H}$. Portanto g é limitada em toda a faixa $\{-\frac{1}{2} \leq |Re(z)| \leq \frac{1}{2}; Im(z) > 0\}$, e assim também em todo $\mathbb{H}$. $\square$

Como vimos na proposição 3.4, os coeficientes de Fourier a_n de uma forma cuspidal f de peso meio-inteiro k também satisfazem $a_n = O(n^{\frac{k}{2}})$. Com um certo trabalho, usando a fórmula de Petersson, que veremos no início do capítulo 4, e usando diretamente a estimativa de Weil para somas de Kloosterman, somas essas que definiremos no início do capítulo 4, pode-se provar que $a_n = O_\epsilon(n^{\frac{k}{2}-\frac{1}{4}+\epsilon})$, o que infelizmente ainda não é suficiente para resolver o problema de Linnik na esfera. Essa estimativa é o melhor resultado que se pode obter no caso meio-inteiro, diferentemente das formas modulares de peso inteiro. De fato, se denotarmos por ψ um cárater de Dirichlet módulo 4 com $\psi(-1) = -1$ pode-se mostrar que a função

$$\theta(z, \psi) = \sum_{m=-\infty}^{m=\infty} \psi(m) m e(m^2 z)$$

é uma forma cuspidal de $\Gamma_0(8)$ de peso $\frac{3}{2}$ que satisfaz $|a_v| = 2\sqrt{v}$ sempre que $v \in \mathbb{Z}$ for um quadrado perfeito ímpar. No capítulo 4, adicionando as restrições $k > 2$ e n livre de quadrados, melhoraremos essa estimativa para $a_n = O_\epsilon(n^{\frac{k}{2}-\frac{2}{7}+\epsilon})$, para assim podermos aplicar-la no problema de Linnik, no capítulo 5.

3.3 Séries de Eisenstein

Seja Γ um subgrupo de congruência, k um meio inteiro maior que 2, p uma cúspide de Γ e σ em $SL_2(\mathbb{Z})$ satisfazendo $\sigma(\infty) = p$. Suponha que $\sigma\Gamma_p\sigma^{-1} = \{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}; n \in \mathbb{Z}\}$ para cada cúspide p de Γ. Definimos a *série de Eisenstein* de Γ em relação a uma cúspide p como

$$E_k^p(z) = \sum_{\lambda \in \Gamma_p \backslash \Gamma} (j(\sigma^{-1}\lambda, z))^{-2k}.$$

Em particular, se $p = \infty$, a série se tornará

$$E_k^\infty(z) = \sum_{\lambda \in \Gamma_\infty \backslash \Gamma} (j(\lambda, z))^{-2k}.$$

Para analisar a convergência dessas séries, definamos a série "espectral"de Eisenstein. Fixe $s \in \mathbb{C}$ com $re(s) > 1$, defina

$$E(z, s) = \sum_{\lambda \in \Gamma_\infty \backslash \Gamma} (im(\lambda z))^s,$$

a demonstração da convergência absoluta de $E(z, s)$ em $\mathbb{H}$, quando vista como função em z, pode ser vista em (19, p.12). Para provar a convergência de E_k^∞ observe que

$$Im(z)^{\frac{k}{2}} |E_k^\infty(z)| \leq \sum_{\lambda \in \Gamma_\infty \backslash \Gamma} |cz + d|^{-k} Im(z)^{\frac{k}{2}} = E(z, k/2), \tag{3.7}$$

portanto $E_k^\infty(z)$ converge absolutamente para $k > 2$, e segue que $E_k^\infty(z)$ é holomorfa em $\mathbb{H}$. De forma similar podemos verificar a convergência e o holomorfismo de $E_k^p(z)$. Podemos observar que E_k^p satisfaz a condição de modularidade da seguinte forma: para todos γ, λ em $SL_2(\mathbb{Z})$ temos $j(\lambda, \gamma z) = \frac{j(\lambda\gamma, z)}{j(\gamma, z)}$, como consequência, dado γ em Γ

$$\begin{aligned} E_k^p(\gamma z) &= \sum_{\lambda \in \Gamma_p \backslash \Gamma} (j(\sigma^{-1}\lambda, \gamma z))^{-2k} \\ &= \sum_{\lambda \in \Gamma_p \backslash \Gamma} (\frac{j(\sigma^{-1}\lambda\gamma, z)}{j(\gamma, z)})^{-2k} \\ &= (j(\gamma, z))^{2k} \sum_{\lambda \in \Gamma_p \backslash \Gamma} (j(\sigma^{-1}\lambda\gamma, z))^{-2k}, \end{aligned}$$

observando que $\lambda\gamma$ varia entre representantes de todas as classes de $\Gamma_p \setminus \Gamma$ enquanto λ também o faz, concluímos que $E_k^p(\gamma z) = (j(\gamma, z))^{2k} E_k^p(z)$. Para analisar o holomorfismo nas cúspides, considere $p_1 = \infty, p_2, ..., p_m$ cúspides inequivalentes de Γ de forma que toda cúspide de Γ seja equivalente a uma dessas cúspides. Dado $i \in \{1, ..., m\}$, pode-se mostrar que $E_k^{p_j}(z)$ se anula

na cúspide p_i se $j \neq i$, e

$$\begin{cases} \lim_{z\to p_i} E_k^{p_i}(z) = 2, se - I_d \in \Gamma \\ \lim_{z\to p_i} E_k^{p_i}(z) = 1, se - I_d \notin \Gamma \end{cases}$$

Esse resultado, que pode ser visto em (25, p.18) tem como consequência direta o fato de que cada elemento de $M_k(\Gamma)$ pode ser escrito da forma $g+h$, onde $g \in S_k(\Gamma)$ e h é uma combinação linear finita das séries de Eisenstein de Γ em relação a cada uma de suas cúspides. É possível, por exemplo, verificar esse resultado para $E_k^{\infty}(z)$ no caso em que $p_i = p_j = \infty$. Supondo, sem perda de generalidade, que $-I_d$ pertence a Γ, a convergência absoluta de E_k^{∞} em $\mathbb{H}$ nos garante que

$$\lim_{Im(z)\to\infty} E_k^{\infty}(z) = \sum_{\lambda\in\Gamma_\infty\backslash\Gamma} \lim_{Im(z)\to\infty} (j(\lambda,z))^{-2k} = 2,$$

pois $\lim_{z\to\infty}(j(\lambda,z))^{-2k} \neq 0$ somente quando λ pertence a $\Gamma_\infty I_d$ ou $\Gamma_\infty(-I_d)$, e nessas exceções temos o limite valendo 1.

3.4 Séries de Poincaré

Dado N inteiro múltiplo de 4 e $k > 2$ meio inteiro, a *série de Poincaré* de $\Gamma_0(N)$ em relação ao infinito é dada por

$$P_m(z,k) = \sum_{\lambda\in(\Gamma_0(N))_\infty\backslash\Gamma_0(N)} (j(\lambda,z))^{-2k} e(m\lambda z),$$

onde $m \geqq 0$ é um inteiro. Observe que obtemos a série de Eisenstein de $\Gamma_0(N)$ em relação ao infinito fazendo $m = 0$. Se $m \geqq 1$, $P_m(z,k)$ será majorada por $E_k^{\infty}(z)$, a série de Eisenstein de $\Gamma_0(N)$ no ∞, assim ela será absolutamente convergente. Usando uma conta similar ao que fizemos anteriormente para séries de Eisenstein, podemos concluir que $P_m(\sigma z,k) = (j(\sigma,z))^{2k} P_m(z,k)$ para todo $\sigma \in \Gamma_0(N)$. Novamente usando essa majoração por séries de Eisenstein, pode-se concluir que P_m se anula em cada cúspide inequivalente ao infinito. Já no caso ∞, temos

$$\lim_{Im(z)\to\infty} \sum_{\lambda\in(\Gamma_0(N))_\infty\backslash\Gamma_0(N)} (j(\lambda,z))^{-2k} e(m\lambda z) =$$

$$\sum_{\lambda\in(\Gamma_0(N))_\infty\backslash\Gamma_0(N)} \lim_{Im(z)\to\infty} (j(\lambda,z))^{-2k} e(m\lambda z) = 0,$$

logo P_m se anula no infinito também. Concluímos daí que, se $m \geqq 1$, P_m será uma forma cuspidal de peso k em relação a $\Gamma_0(N)$.

Proposição 3.6 *Sejam f um elemento de $S_k(\Gamma_0(N))$ e $m \geq 1$ inteiro. Então*

$$< P_m, f >= \overline{a_m}\frac{\Gamma(k-1)}{(4\pi m)^{k-1}},$$

onde $f(z) = \sum_{n=1}^{\infty} a_n e(nz)$ é a série de Fourier de f no infinito e $\Gamma(z)$ indica a função gamma. Em particular, o conjunto das séries de Poincaré P_m,$m = 1, 2, ...$, geram $S_k(\Gamma_0(N))$.

Prova: Seja $\mathcal{F}$ um domínio fundamental de $\Gamma_0(N)$. Usando o produto interno de Petersson

$$\begin{aligned}
\langle P_m, f\rangle &= \int_{\mathcal{F}} P_m(z)\overline{f(z)}Im(z)^k\frac{dxdy}{y^2} \\
&= \int_{\mathcal{F}} \sum_{\lambda\in\Gamma_\infty\backslash\Gamma} ((j(\lambda,z))^{-2k}(\overline{(j(\lambda,z))})^{-2k}e(m\lambda z)\overline{f(\lambda z)}y^k\frac{dxdy}{y^2} \\
&= \int_{\mathcal{F}} \sum_{\lambda\in\Gamma_\infty\backslash\Gamma} e(m\lambda z)\overline{f(\lambda z)}|(cz+d)|^{-2k}y^k\frac{dxdy}{y^2} \\
&= \int_{\mathcal{F}} \sum_{\lambda\in\Gamma_\infty\backslash\Gamma} e(m\lambda z)\overline{f(\lambda z)}Im(\lambda z)^k\frac{dxdy}{y^2} \\
&= \int_0^\infty\int_0^1 e(mz)\overline{f(z)}y^{k-2}dxdy = \frac{\overline{a_m}}{(4\pi m)^{k-1}}\Gamma(k-1),
\end{aligned}$$

onde usamos no penúltimo passo que podemos escolher representantes λ das classes de $\Gamma_\infty\backslash\Gamma$ de modo que $\cup_\lambda \lambda\mathcal{F} = \{z \in \mathbb{H}; -\frac{1}{2} \leq Re(z) \leq \frac{1}{2}\}$. Daí $\langle P_m, f\rangle = 0$ para todo $m \in \mathbb{Z}_{>0}$ se, e somente se, $a_m = 0$ para todo $m \in \mathbb{Z}_{>0}$, que é equivalente a dizer que $f \equiv 0$. Portanto o conjunto $\{P_m, m \geq 1\}$ gera o espaço vetorial de dimensão finita $S_k(\Gamma_0(N))$.□

Calculemos agora o n-ésimo coeficiente de Fourier $\hat{P}_m(n)$ de $P_m(z,k)$. Para isso, faça aqui $\Gamma = \Gamma_0(N)$ e observe que $\Gamma_\infty = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}; n \in \mathbb{Z} \right\}$. Veja também que

$$\begin{cases} \Gamma_\infty\alpha\Gamma_\infty = \Gamma_\infty, \text{ se } \alpha \in \pm\Gamma_\infty \\ \Gamma_\infty\alpha\Gamma_\infty = \bigcup_{s\in\mathbb{Z}} \left(\alpha \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \right), \text{ se } \alpha \notin \pm\Gamma_\infty \end{cases}.$$

Assim

$$\begin{aligned}
\hat{P}_m(n) &= \int_0^1 P_m(z,k)e(-nz)dz \\
&= \int_0^1 \sum_{\lambda\in\Gamma_\infty\backslash\Gamma} (j(\lambda,z)^{-2k}e(m\lambda z)e(-nz)dz \\
&= 2\int_0^1 e(mz)e(-nz)dz + \sum_{\substack{c\neq 0\\ \lambda\in\Gamma_\infty\backslash\Gamma/\Gamma_\infty}} \sum_{s\in\mathbb{Z}} \int_0^1 j(\lambda\begin{pmatrix}1 & s\\ 0 & 1\end{pmatrix},z)^{-2k}e\left(m\lambda\begin{pmatrix}1 & s\\ 0 & 1\end{pmatrix}z - nz\right) \\
&= 2\delta_{m,n} + \sum_{\substack{c\neq 0\\ \lambda\in\Gamma_\infty\backslash\Gamma/\Gamma_\infty}} \int_{-\infty}^{\infty} j(\lambda,z)^{-2k}e(m\lambda z - nz)dz,
\end{aligned}$$

onde tomamos $\lambda = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$. Uma conta simples pode nos mostrar que as classes de $\Gamma_\infty\backslash\Gamma/\Gamma_\infty$ são os conjuntos das matrizes $\begin{pmatrix}* & *\\ c & d\end{pmatrix} \in \Gamma$, onde c e $d(\mathrm{mod}\ c)$ estão fixados. Assim, continuando nosso cálculo e observando que $\lambda z = \frac{a}{c} - \frac{1}{c(cz+d)}$

$$\begin{aligned}
&2\delta_{m,n} + \sum_{\substack{c\neq 0\\ \lambda\in\Gamma_\infty\backslash\Gamma/\Gamma_\infty}} \int_{-\infty}^{\infty} j(\lambda,z)^{-2k}e(m\lambda z - nz)dz \\
&= 2\delta_{m,n} + 2\sum_{\substack{c>0\\ \lambda\in\Gamma_\infty\backslash\Gamma/\Gamma_\infty}} \varepsilon_d^{-2k}\left(\frac{c}{d}\right)^{2k}\int_{-\infty}^{\infty}(cz+d)^{-k}e\left(\frac{ma}{c} - \frac{m}{c(cz+d)} - nz\right)dz \\
&= 2\delta_{m,n} + 2\sum_{\substack{c>0\\ N|c}}\sum_{\substack{d(\mathrm{mod}\ c)\\ (c,d)=1}} \varepsilon_d^{-2k}\left(\frac{c}{d}\right)^{2k}\int_{-\infty}^{\infty}(cz+d)^{-k}e\left(\frac{ma}{c} - \frac{m}{c(cz+d)} - nz\right)dz \\
&= 2\delta_{m,n} + 2\sum_{\substack{c>0\\ N|c}} c^{-k}\sum_{\substack{d(\mathrm{mod}\ c)\\ (c,d)=1}} e\left(\frac{ma}{c}\right)\varepsilon_d^{-2k}\left(\frac{c}{d}\right)^{2k}\int_{-\infty}^{\infty}(z+\frac{d}{c})^{-k}e\left(\frac{-m}{c^2(z+d/c)} - nz\right)dz \\
&= 2\delta_{m,n} + 2\sum_{\substack{c>0\\ N|c}} c^{-k}\sum_{\substack{d(\mathrm{mod}\ c)\\ (c,d)=1}} \left(\frac{c}{d}\right)^{2k}\varepsilon_d^{-2k}e\left(\frac{ma}{c}\right)\int_{-\infty}^{\infty} z^{-k}e\left(\frac{-m}{c^2z} - n(z-\frac{d}{c})\right)dz \\
&= 2\delta_{m,n} + 2\sum_{\substack{c>0\\ N|c}} c^{-k}\left(\sum_{\substack{d(\mathrm{mod}\ c)\\ (d,c)=1}} \left(\frac{c}{d}\right)^{2k}\varepsilon_d^{-2k}e\left(\frac{ma+nd}{c}\right)\int_{-\infty}^{\infty} z^{-k}e\left(\frac{-m}{c^2z} - nz\right)dz\right).
\end{aligned}$$

Então, usando uma variação da representação da função de Bessel enunciada em (2.4), encon-

tramos que

$$\hat{P}_m(n) = 2\frac{m^{(k-1)/2}}{n^{(k-1)/2}} \left\{ \delta_{m,n} + 2\pi i^{-k} \sum_{\substack{c>0 \\ N|c}} J_{k-1}\left(\frac{4\pi\sqrt{mn}}{c}\right) \frac{K(m,n,c)}{c} \right\},$$

onde

$$K(m,n,c) = \sum_{\substack{d(\mathrm{mod}\ c) \\ (d,c)=1}} \left(\frac{c}{d}\right)^{2k} \varepsilon_d^{-2k} e\left(\frac{m\overline{z} + nd}{c}\right).$$

Fazendo $n = m$ obtemos

Proposição 3.7 *Se $\hat{P}_m(n, \Gamma_0(N))$ denota o n-ésimo coeficiente de Fourier da m-ésima série de Poincaré de $\Gamma_0(N)$ relativa ao peso meio inteiro k, $k > 2$ e $4|N$, então, para $n \geq 1$*

$$\hat{P}_n(n, \Gamma_0(N)) = 1 + 2\pi i^{-k} \sum_{\substack{c>0 \\ N|c}} J_{k-1}\left(\frac{4\pi n}{c}\right) \frac{K(n,n,c)}{c}.$$

.

4 UMA ESTIMATIVA NÃO TRIVIAL DE IWANIEC

Nesse capítulo iremos fazer um esboço da prova da estimativa não trivial para coeficientes de Fourier de formas cuspidais de peso meio inteiro obtida por Iwaniec em (15). Nesse artigo, Iwaniec trabalha principalmente procurando estimar formas bilineares do tipo

$$\mathcal{B}(X,Y)=\sum_{A<a\leq 2A}\sum_{\substack{B<b\leq 2B\\(a,b)=1}}X_aY_be^{2\pi in(\frac{\overline{a}}{b}-\frac{\overline{b}}{a})},$$

onde $\overline{a}$ e $\overline{b}$ indicam os inversos multiplicativos de a e b módulo b e módulo a, respectivamente. Esse tipo de forma é obtida quando somas de Kloosterman são somadas, e isso é feito com o objetivo de se explorar cancelamento de termos entre as somas.

Teorema 4.1 *(Iwaniec(15),1987) Seja N inteiro com $4|N$ e k um meio inteiro maior que 2. Fixe $f\in S_k(\Gamma_0(N))$, e seja a_n o n-ésimo coeficiente de Fourier de f. Se n é um inteiro livre de quadrados, então*

$$a_n\ll_\epsilon n^{k/2-2/7+\epsilon}.$$

Para começarmos a prova desse teorema, primeiro escolheremos uma base ortonormal $f_1,f_2,...,f_R$ de $S_k(\Gamma_0(N))$ em relação ao produto interno de Petersson. Pela proposição 3.6, se denotarmos por P_m a m-ésima série de Poincaré de $\Gamma_0(N)$

$$\langle P_m,f_i\rangle=\overline{a_i(m)}\frac{\Gamma(k-1)}{(4\pi m)^{k-1}},$$

onde

$$f_j(z)=\sum_{n=1}^{\infty}a_j(n)e(nz).$$

O fato de $f_1,f_2,...,f_R$ formarem uma base ortonormal implica que

$$\begin{aligned}P_m(z)&=\sum_{j=1}^{R}\langle P_m,f_j\rangle f_j(z)\\&=\sum_{j=1}^{R}\langle P_m,f_j\rangle\left(\sum_{n=1}^{\infty}a_j(n)e(nz)\right)\\&=\sum_{n=1}^{\infty}\left(\sum_{j=1}^{R}\langle P_m,f_j\rangle a_j(n)\right)e(nz).\end{aligned}$$

Concluímos então que

$$\hat{P}_m(n)=\sum_{j=1}^{R}\langle P_m,f_j\rangle a_j(n)=\frac{\Gamma(k-1)}{(4\pi m)^{k-1}}\sum_{j=1}^{R}\overline{a_j(m)}a_j(n).\tag{4.8}$$

Usando a proposição 3.7, encontramos a *fórmula de Petersson* para quando $m = n$

$$\frac{\Gamma(k-1)}{(4\pi n)^{k-1}} \sum_{j=1}^{R} |a_j(n)|^2 = 1 + 2\pi i^{-k} \sum_{\substack{c>0 \\ N|c}} \frac{K(n,n,c)}{c} J_{k-1}\left(\frac{4\pi n}{c}\right). \tag{4.9}$$

É através dessa importante relação que estimamos $|a_j(n)|$, e como esses são os coeficientes de Fourier de uma base ortonormal de $S_k(\Gamma_0(N))$, será suficiente provar a estimativa do teorema 4.1 para esses coeficientes.

4.1 Somas de Kloosterman

Dados t inteiro ímpar e m, n, c inteiros, a soma de Kloosterman generalizada $K_t(m,n;c)$ e a soma de Salié $S(m,n;c)$ são definidas como

$$\begin{aligned} K_t(m,n;c) &= \sum_{d(\mathrm{mod}\ c)} \varepsilon_d^{-t} \left(\frac{c}{d}\right) e\left(\frac{md+n\overline{d}}{c}\right) \\ S(m,n;c) &= \sum_{d(\mathrm{mod}\ c)} \left(\frac{d}{c}\right) e\left(\frac{md+n\overline{d}}{c}\right), \end{aligned}$$

onde $\overline{d}$ indica o inverso multiplicativo de d módulo c. Na sequência deste capítulo usaremos com frequência a notação $\overline{u}$ para indicar o inverso multiplicativo de u com respeito a algum módulo v sem mencionarmos qual v é considerado, isto será facilmente indicado pelo contexto. Por exemplo, na fração $\frac{a\overline{x}}{y}$, $\overline{x}$ sempre significará que $\overline{x}x \equiv 1(\mathrm{mod}\ y)$.

Proposição 4.1 *Seja $c = qr$ com $4|r$ e $mdc(q,r) = 1$. Então*

$$K_t(m,n;c) = K_{t-q+1}(m\overline{q}, n\overline{q}; r) S(m\overline{r}, n\overline{r}; q).$$

Prova: Se $r = 4w$ com $w \in \mathbb{Z}$, então, dado l inteiro ímpar

$$\left(\frac{r}{l}\right) = \left(\frac{4w}{l}\right) = \left(\frac{4}{l}\right)\left(\frac{w}{l}\right) = \left(\frac{4}{l+4w}\right)\left(\frac{w}{l+4w}\right) = \left(\frac{r}{l+r}\right).$$

Portanto, se $l' \equiv l(\mathrm{mod}\ r))$, $\left(\frac{r}{l'}\right) = \left(\frac{r}{l}\right)$. Quando x e y percorrem, respectivamente, todas as classes de $(\mathbb{Z}/q\mathbb{Z})^\times$ e $(\mathbb{Z}/r\mathbb{Z})^\times$, $d = xr\overline{r} + yq\overline{q}$ percorre todas as classes de $(\mathbb{Z}/c\mathbb{Z})^\times$. Veja que d também é ímpar, tal como q. Assim, usando a lei da reciprocidade quadrática e o que vimos acima

$$\left(\frac{c}{d}\right) = \left(\frac{q}{d}\right)\left(\frac{r}{d}\right) = (-1)^{\frac{d-1}{2}\frac{q-1}{2}} \left(\frac{d}{q}\right)\left(\frac{r}{d}\right) = (-1)^{\frac{y-1}{2}\frac{q-1}{2}} \left(\frac{x}{q}\right)\left(\frac{r}{y}\right).$$

Observe que, como $d \equiv y(\mathrm{mod}\ 4)$, $\varepsilon_d = \varepsilon_y$ e que

$$\varepsilon_y^{q-1} = (\varepsilon_y^2)^{\frac{q-1}{2}} = (-1)^{\frac{y-1}{2}\frac{q-1}{2}}.$$

temos

$$\begin{aligned}
K_{t-q+1}(m\overline{q}, n\overline{q}; r)S(m\overline{q}, n\overline{q}; r) &= \\
\left(\sum_{y(\mathrm{mod}\ r)} \varepsilon_y^{-t+q-1}\left(\frac{r}{y}\right) e\left(\frac{m\overline{q}y + n\overline{qy}}{r}\right)\right)\left(\sum_{x(\mathrm{mod}\ q)}\left(\frac{x}{q}\right) e\left(\frac{m\overline{r}x + n\overline{rx}}{q}\right)\right) &= \\
\sum_{\substack{x(\mathrm{mod}\ q)\\ y(\mathrm{mod}\ r)}} \varepsilon_d^{-t}\varepsilon_y^{q-1}\left(\frac{r}{y}\right)\left(\frac{x}{q}\right) e\left(\frac{m(q\overline{q}y + r\overline{r}x) + n(m(q\overline{qy} + r\overline{rx})}{qr}\right) &= \\
\sum_{d(\mathrm{mod}\ c))} \varepsilon_d^{-t}\left(\frac{c}{d}\right) e\left(\frac{md + n\overline{d}}{c}\right) &= K_t(m, n; c)\ \square
\end{aligned}$$

Usando uma prova similar (e mais simples) que a da proposição anterior, pode-se concluir que

Proposição 4.2 *Seja q ímpar,* $q = uv$ *com* $(u, v) = 1$. *Então*

$$S(m, n; q) = S(m\overline{u}, n\overline{u}; v)S(m\overline{v}, n\overline{v}; u).$$

As somas de Salié possuem as seguintes propriedades:

Proposição 4.3 *Sejam m,n,q inteiros satisfazendo* $(m, q) = (n, q) = 1$. *então*
(1) $S(m, n; q) = \left(\frac{m}{q}\right) S(1, mn; q)$*;*
(2) Se $\left(\frac{m}{q}\right) = -1$*, então* $S(1, m; q) = 0$*;*
(3)

$$S(1, n^2, q) = \varepsilon_q\sqrt{q} \sum_{x^2 \equiv 1(\mathrm{mod}\ q)} e^{\frac{4\pi i x n}{q}}.$$

Prova: Para provar (1) faça $y = mx, x = \overline{m}y$ e $\overline{x} = m\overline{y}$, então

$$\begin{aligned}
S(m, n; q) &= \sum_{x(\mathrm{mod}\ q)}\left(\frac{x}{q}\right) e\left(\frac{mx + n\overline{x}}{q}\right) \\
&= \sum_{y(\mathrm{mod}\ q)}\left(\frac{\overline{m}y}{q}\right) e\left(\frac{y + nm\overline{y}}{q}\right) \\
&= \left(\frac{m}{q}\right) S(1, mn, q).
\end{aligned}$$

Para provar (2)

$$\begin{aligned} S(1,m;q) &= \sum_{x(\mathrm{mod}\ q)} \left(\frac{x}{q}\right) e\left(\frac{x+m\overline{x}}{q}\right) \\ &= \sum_{x(\mathrm{mod}\ q)} \left(\frac{\overline{x}}{q}\right) e\left(\frac{\overline{x}+mx}{q}\right) \\ &= S(m,1;q) \\ &= \left(\frac{m}{q}\right) S(1,m;q), \end{aligned}$$

portanto $\left(\frac{m}{q}\right) = -1$ implica em $S(1,m;q) = 0$. Provar (3) vai ser um pouco mais trabalhoso. Primeiro lembremos do clássico resultado sobre soma de Gauss (Veja (4, p.12-16))

$$\sum_{n=0}^{q-1} e\left(\frac{an^2}{q}\right) = \left(\frac{a}{q}\right) \varepsilon_q \sqrt{q},$$

onde q é um inteiro positivo ímpar e $(a,q) = 1$. Definindo, para $m, s \in \mathbb{Z}$

$$c_s(m) = \sum_{\substack{0 \le \lambda < s \\ (\lambda,s)=1}} e\left(\frac{m\lambda}{s}\right) \text{ e } n_s(m) = \sum_{\lambda=0}^{s-1} e\left(\frac{m\lambda}{s}\right),$$

observe que $n_s(m)$ é s, se s divide m, e é 0 caso contrário. Agora, observando que

$$n_s(m) = \sum_{\lambda=0}^{s-1} e\left(\frac{m\lambda}{s}\right) = \sum_{d|s} \sum_{\substack{\lambda(\mathrm{mod}\ d) \\ (d,\lambda)=1}} e\left(\frac{m\lambda}{d}\right) = \sum_{d|s} c_d(m).$$

Fixando m e considerando $c_s(m)$ como uma função aritmética em s, usamos a inversão de Möbius para concluir que

$$c_s(m) = \sum_{d|s} \mu(s/d) n_d(m) = \sum_{\substack{d|s \\ d|m}} \mu(s/d) d, \tag{4.10}$$

onde μ é a função de Möbius. Agora sim podemos começar a prova de (3). Seja

$$h(n) = S(1,n^2;q) = \sum_{x(\mathrm{mod}\ q)} \left(\frac{x}{q}\right) e\left(\frac{x+n^2\overline{x}}{q}\right)$$

uma função com domínio $n = 0, 1, ..., q-1$. Calculando a transformada discreta de Fourier de

h, temos

$$\begin{aligned}
\hat{h}(l) &= \sum_{n(\mathrm{mod}\ q)} \left(\sum_{x(\mathrm{mod}\ q)} \left(\frac{x}{q}\right) e\left(\frac{x+n^2\overline{x}}{q}\right)\right) e\left(\frac{-ln}{q}\right) \\
&= \sum_{x(\mathrm{mod}\ q)} e\left(\frac{x}{q}\right)\left(\frac{x}{q}\right) \sum_{n(\mathrm{mod}\ q)} e\left(\frac{\overline{x}(n^2-xln)}{q}\right) \\
&= \sum_{x(\mathrm{mod}\ q)} \left(\frac{x}{q}\right) e\left(\frac{x}{q}\right) e\left(\frac{-\overline{4}xl^2}{q}\right) \sum_{n(\mathrm{mod}\ q)} e\left(\frac{\overline{x}(n-\overline{2}xl)^2}{q}\right) \\
&= \sum_{x(\mathrm{mod}\ q)} \left(\frac{x}{q}\right) e\left(\frac{x}{q}\right) \sum_{n(\mathrm{mod}\ q)} e\left(\frac{-\overline{4}xl^2}{q}\right) \epsilon_q\sqrt{q}\left(\frac{\overline{x}}{q}\right),
\end{aligned}$$

onde usamos o resultado sobre soma de Gauss na última passagem. Daí

$$\hat{h}(m) = \varepsilon_q\sqrt{q} \sum_{(x,q)=1} e\left(\frac{x}{q}(1-\overline{4}m^2)\right) = \varepsilon_q\sqrt{q}c_q(1-\overline{4}m^2).$$

Usando a fórmula de inversão de Fourier e observando que q é ímpar, temos

$$\begin{aligned}
h(n) &= \frac{1}{q} \sum_{m(\mathrm{mod}\ q)} \hat{h}(m) e\left(\frac{mn}{q}\right) \\
&= \frac{1}{q} \sum_{m(\mathrm{mod}\ q)} e\left(\frac{mn}{q}\right) \varepsilon_q\sqrt{q}c_q(1-\overline{4}m^2) \\
&= \frac{\varepsilon_q}{\sqrt{q}} \sum_{m(\mathrm{mod}\ q)} e\left(\frac{mn}{q}\right) \sum_{\substack{d|q \\ d|m^2-4}} \mu(q/d)d,
\end{aligned}$$

onde concluímos que

$$h(n) = \frac{\varepsilon_q}{\sqrt{q}} \sum_{d|q} d\mu(q/d) \sum_{\substack{m(\mathrm{mod}\ q) \\ m^2\equiv 4(\mathrm{mod}\ d)}} e\left(\frac{mn}{q}\right). \tag{4.11}$$

Fixe $d|q$ com $d \neq q$. Olhemos agora para a soma

$$\Omega(n,d,q) := \sum_{\substack{m(\mathrm{mod}\ q) \\ m^2\equiv 4(\mathrm{mod}\ d)}} e\left(\frac{mn}{q}\right).$$

Considere $q = db, b > 1$. Para cada $m_0(\mathrm{mod}\ d)$ solução de $m^2 \equiv 4(\mathrm{mod}\ d)$ temos que $m \equiv m_0 + \lambda d(\mathrm{mod}\ q)$, $\lambda \in \mathbb{Z}/b\mathbb{Z}$, serão b soluções distintas de $m^2 \equiv 4(\mathrm{mod}\ d)$ módulo q.

Portanto

$$\Omega(n,d,q)=\sum_{m^2\equiv 4(\mathrm{mod}\ d)}\sum_{\lambda(\mathrm{mod}\ b)} e\left(\frac{(m+\lambda d)n}{db}\right)=\sum_{m^2\equiv 4(\mathrm{mod}\ d)} e\left(\frac{mn}{db}\right)\sum_{\lambda(\mathrm{mod}\ b)} e\left(\frac{\lambda n}{b}\right).$$

Observe que $(n,b)=1$ implica

$$\sum_{\lambda(\mathrm{mod}\ b)} e\left(\frac{\lambda n}{b}\right)=\sum_{\lambda(\mathrm{mod}\ b)} e\left(\frac{\lambda}{b}\right)=0,$$

portanto

$$\sum_{\substack{m(\mathrm{mod}\ q)\\ m^2\equiv 4(\mathrm{mod}\ d)}} e\left(\frac{mn}{q}\right)=0.$$

Logo, segue de (4.11)

$$h(n)=\frac{\varepsilon_q}{\sqrt{q}}\sum_{\substack{m(\mathrm{mod}\ q)\\ m^2\equiv 4(\mathrm{mod}\ q)}} e\left(\frac{mn}{q}\right). \quad \square$$

Um corolário importante que podemos concluir dessa proposição é que, se q é ímpar e $(n,q)=1$, temos

$$S(n,n;q)=\left(\frac{n}{q}\right)\varepsilon_q\sqrt{q}\sum_{\substack{ab=q\\(a,b)=1}} e\left(2n\left(\frac{\overline{a}}{b}-\frac{\overline{b}}{a}\right)\right). \tag{4.12}$$

De fato, usando a proposição 4.3, obtemos

$$S(n,n;q)=\left(\frac{n}{q}\right)S(1,n^2;q)=\left(\frac{n}{q}\right)\varepsilon_q\sqrt{q}\sum_{x^2\equiv 1(\mathrm{mod}\ q)} e(2xn/q).$$

Usando o teorema chinês dos restos e o fato de que $x^2\equiv 1(\mathrm{mod}\, p^\alpha)$ tem somente duas soluções módulo p^α quando p é primo e α inteiro positivo, pode-se concluir que os conjuntos $\{(a\overline{a}-b\overline{b})mod\ q;(a,b)=1,ab=q\}$ e $\{x;x\in\mathbb{Z}/q\mathbb{Z},x^2\equiv 1(\mathrm{mod}\ q)\}$ são iguais. Portanto

$$\sum_{x^2\equiv 1(\mathrm{mod}\ q)} e(2xn/q)=\sum_{\substack{ab=q\\(a,b)=1}} e\left(2n\left(\frac{\overline{a}}{b}-\frac{\overline{b}}{a}\right)\right),$$

de onde concluímos o corolário.

A partir deste ponto, k sempre denotará um meio inteiro maior que 2. Com isso em mente, o próximo resultado visa obter uma fórmula para $K_{2k}(n,n,c)$ similar à formula obtida para $S(n,n,c)$.

Proposição 4.4 *Sejam n,c,q,r inteiros que satisfazem* $c = qr$, $(2n, q) = 1$, $r|(2n)^\infty$, $8|r$. *Então*

$$K_{2k}(n,n;c) = \sqrt{q} \sum_{s(\mathrm{mod}\ r/2)} \varepsilon_s^{-2k} f_r(2s)[(1+i^s)\left(\frac{nr}{q}\right) + (1-i^s)\left(\frac{-nr}{q}\right)]$$

$$\times \sum_{\substack{ab=q \\ (a,b)=1}} e\left(2n(\frac{\overline{ar}}{b} - \frac{\overline{br}}{a} + \frac{s\overline{ab}}{r})\right),$$

onde

$$f_r(2s) = \sum_{\substack{d(\mathrm{mod}\ r) \\ d+\overline{d}\equiv 2s(\mathrm{mod}\ r)}} \left(\frac{r}{d}\right).$$

Prova: Pela proposição 4.1 e pelo item (3) da proposição 4.3

$$\begin{aligned} K_{2k}(n,n;c) &= K_{2k-q+1}(n\overline{q}, n\overline{q}; r) S(n\overline{r}, n\overline{r}; q) && (4.13)\\ &= K_{2k-q+1}(n\overline{q}, n\overline{q}; r)(\varepsilon_q q^{\frac{1}{2}} \left(\frac{n\overline{r}}{q}\right) \sum_{\substack{ab=1 \\ (a,b)=1}} e\left(2n(\frac{\overline{a}}{b} - \frac{\overline{b}}{a})\right) && (4.14)\\ &= K_{2k-q+1}(n\overline{q}, n\overline{q}; r)(\varepsilon_q q^{\frac{1}{2}} \left(\frac{nr}{q}\right) \sum_{\substack{ab=1 \\ (a,b)=1}} e\left(2n(\frac{\overline{a}}{b} - \frac{\overline{b}}{a})\right). && (4.15) \end{aligned}$$

Faça $w = 2k - q - 1$. Veja que

$$\begin{aligned} K_w(n\overline{q}, n\overline{q}; r) &= \sum_{\substack{d(\mathrm{mod}\ r) \\ (d,r)=1}} \varepsilon_d^{-w} \left(\frac{r}{d}\right) e\left(\frac{n\overline{q}(d+\overline{d})}{r}\right) \\ &= 2 \sum_{\substack{s(\mathrm{mod}\ r/2) \\ 2\nmid s}} \varepsilon_s^{-w} \left(\sum_{\substack{d(\mathrm{mod}\ r) \\ d+\overline{d}\equiv 2s(\mathrm{mod}\ r)}} \left(\frac{r}{d}\right) \right) e\left(2n\frac{\overline{q}s}{r}\right) \\ &= 2 \sum_{\substack{s(\mathrm{mod}\ r/2) \\ 2\nmid s}} \varepsilon_s^{-w} f_r(2s) e\left(2n\frac{\overline{q}s}{r}\right), \end{aligned}$$

onde usamos o fato de que $\varepsilon_d = \varepsilon_{\frac{d+\overline{d}}{2}}$, pois $d \equiv \overline{d}(\mathrm{mod}\ 8)$. Pode-se mostrar com uma conta simples que

$$2\varepsilon_q \varepsilon_s^{q-1} = (1+i^s) + (1-i^s)\left(\frac{-1}{q}\right).$$

Portanto, por (4.15)

$$K_{2k}(n,n;c) = \left(2\sum_{\substack{s(\mathrm{mod}\ r/2)\\ 2\nmid s}} \varepsilon_s^{-w} f_r(2s) e\left(\frac{2n\overline{q}s}{r}\right)\right) \times \left(\varepsilon_q q^{\frac{1}{2}} \left(\frac{nr}{q}\right) \sum_{\substack{ab=q\\(a,b)=1}} e\left(2n\overline{r}(\frac{\overline{a}}{b}-\frac{\overline{b}}{a})\right)\right)$$

$$= q^{\frac{1}{2}} \left(\sum_{\substack{s(\mathrm{mod}\ r/2)\\ 2\nmid s}} \varepsilon_q \varepsilon_s^{q-1} \varepsilon_s^{-2k} f_r(s) \left(\frac{nr}{q}\right)\right) \times \left(\sum_{\substack{ab=q\\(a,b)=1}} e\left(2n(\frac{\overline{ar}}{b}-\frac{\overline{br}}{a})+\frac{2n\overline{q}s}{r})\right)\right)$$

$$= \sqrt{q} \sum_{s(\mathrm{mod}\ r/2)} \varepsilon_s^{-2k} f_r(2s)[(1+i^s)\left(\frac{nr}{q}\right)+(1-i^s)\left(\frac{-nr}{q}\right)] \times \sum_{\substack{ab=q\\(a,b)=1}} e\left(2n(\frac{\overline{ar}}{b}-\frac{\overline{br}}{a}+\frac{s\overline{ab}}{r})\right).$$

□

Proposição 4.5 *Se n é um inteiro livre de quadrados e $4|c$, então $K(n,n;c)=0$ a menos que*

$$(c,n)^2|c$$

Prova: Suponha que $(c,n)^2 \nmid c$. Então existe um primo $p>2$ que satisfaz $p \parallel n$ e $p \parallel c$, ou seja, $(n/p,p)=(c/p,p)=1$. Faça $w_p=(-1)^{\frac{p-1}{2}}$. Daí, pelo teorema chinês dos restos e do fato de $x \equiv y(\mathrm{mod}\ c/p)$ implicar $x \equiv y(\mathrm{mod}\ 4)$, teremos

$$\begin{aligned} K_{2k}(n,n;c) &= \sum_{d(\mathrm{mod}\ c))} \varepsilon_d^{-t} \left(\frac{c}{d}\right) e\left(\frac{n(d+\overline{d})}{c}\right) \\ &= \sum_{\substack{w(\mathrm{mod}\ c/p)\\ x(\mathrm{mod}\ p)}} \varepsilon_w^{-t} \left(\frac{c/w_p p}{w}\right)\left(\frac{w_p p}{x}\right) e\left(\frac{(n/p)(w+\overline{w})}{c/p}\right) \\ &= \left(\sum_{w(\mathrm{mod}\ c/p)} \varepsilon_w^{-t} \left(\frac{cw_p/p}{w}\right) e\left(\frac{(n/p)(w+\overline{w})}{c/p}\right)\right)\left(\sum_{x(\mathrm{mod}\ p)} \left(\frac{w_p p}{x}\right)\right) \\ &= 0. \end{aligned}$$

Uma vez que, já que $x \to \left(\frac{w_p p}{x}\right)$ é carácter módulo p, o somatório de símbolos de Kronecker se anula. □

Proposição 4.6 *Para $q \geq 1$ e $X \geq 1$ temos*

$$\left|\sum_{1\leq x\leq X} e\left(m\frac{\overline{x}}{q}\right)\right| \leq (m,q)^{\frac{1}{2}} q^{\frac{1}{2}} \tau(q) \log 2q + (m,q) q^{-1} \tau(q) X.$$

Prova: A conhecida estimativa de Weil (veja (13, p.399)) nos dá

$$\left|\sum_{x(\mathrm{mod}\ q)} e\left(\frac{m\overline{x}+dx}{q}\right)\right| \leq (m,d,q)^{\frac{1}{2}} q^{\frac{1}{2}} \tau(q). \tag{4.16}$$

Usando a fórmula de inversão de Fourier para uma função f periódica em $x(\mathrm{mod}\ q)$ obtemos

$$\begin{aligned}\sum_{1\leq x\leq X} f(x) &= \sum_{1\leq x\leq X} \sum_{u(\mathrm{mod}\ q)} \hat{f}(u) e\left(\frac{ux}{q}\right) \\ &= \sum_{1\leq x\leq X} \sum_{u(\mathrm{mod}\ q)} e\left(\frac{ux}{q}\right) \frac{1}{q} \sum_{y(\mathrm{mod}\ q)} f(y) e\left(\frac{-uy}{q}\right) \\ &= \sum_{-q/2\leq u\leq q/2} \left(\frac{1}{q}\sum_{1\leq x\leq X} e\left(\frac{ux}{q}\right)\right)\left(\sum_{y(\mathrm{mod}\ q)} f(y) e\left(\frac{-uy}{q}\right)\right).\end{aligned}$$

Seja

$$\lambda(u) = q^{-1} \sum_{1\leq x\leq X} e\left(\frac{ux}{q}\right),$$

então $\lambda(u) = \left(\frac{e(Xu/q)-1}{e(u/q)-1}\right) e(\frac{u}{q}) q^{-1}$ caso $u \neq 0$, e $\lambda(0) = X/q$. Logo, se $1 \leq |u| \leq q/2$, observando que $|e(\pi x) - 1| = |\sin \pi x|$ e que $|\sin \pi y| \geq 2y$ quando $0 \leq y \leq 1/2$

$$|\lambda(u)| = \frac{|\sin \pi X u/q|}{|\sin \pi u/q|} q^{-1} \leq \frac{q^{-1}}{|\sin \pi u/q|} \leq \frac{1}{2|u|}.$$

Portanto

$$\begin{aligned}\left|\sum_{1\leq x\leq X} f(x) - \frac{1}{q}\sum_{x(\mathrm{mod}\ q)} f(x)\right| &= \left|\sum_{1\leq |u|\leq q/2} \lambda(u) \sum_{x(\mathrm{mod}\ q)} f(x)\right| \\ &\leq \sum_{1\leq |u|\leq q/2} \frac{1}{2|u|} \left|\sum_{x(\mathrm{mod}\ q)} f(x) e\left(\frac{ux}{q}\right)\right|. \end{aligned} \tag{4.17}$$

Tomando $f(x) = e\left(\frac{m\overline{x}}{q}\right)$, observe que

$$\left|\sum_{x(\mathrm{mod}\ q)} f(x)\right| = \left|\sum_{x(\mathrm{mod}\ q)} e\left(\frac{m\overline{x}}{q}\right)\right| = |c_q(m)|,$$

onde $c_s(m)$ é como a definida na proposição 4.3. Usando (4.10), concluímos que

$$\left|\sum_{x(\mathrm{mod}\ q)} f(x)\right| = |c_q(m)| = \left|\sum_{v|(m,q)} v\mu(\frac{q}{v})\right| \leq (m,q)\tau(q) \tag{4.18}$$

Logo, por (4.16),(4.17) e (4.18), temos

$$\begin{aligned}\left|\sum_{\substack{1\le x\le X\\(x,q)=1}} e\left(\frac{m\overline{x}}{q}\right)\right| &\le \sum_{1\le|u|\le q/2}\frac{1}{2|u|}\left|\sum_{x(\mathrm{mod}\ q)} e\left(\frac{m\overline{x}+ux}{q}\right)\right| + \frac{X}{q}\left|\sum_{x(\mathrm{mod}\ q)} e\left(\frac{m\overline{x}}{q}\right)\right| \\ &\le \sum_{1\le|u|\le q/2}\frac{1}{2|u|}(m,u,q)^{\frac{1}{2}}q^{\frac{1}{2}}\tau(q)+\frac{X}{q}(m,q)\tau(q) \\ &\le (m,q)^{\frac{1}{2}}q^{\frac{1}{2}}\tau(q)\log 2q+(m,q)\tau(q)Xq^{-1}.\ \square\end{aligned}$$

Proposição 4.7 *Seja n inteiro livre de quadrados e c um múltiplo de 8. Então*

$$|K_t(n,n;c)| \ll (n,c)^{1/2}c^{1/2}\tau(c).$$

Prova: Seja $c=2^\alpha q=2^\alpha uv$, com q ímpar e $(u,n)=(u,v)=1$. Das proposições 4.1 e 4.2, concluímos

$$K_t(n,n;c)=K_{t-q+1}(n\overline{q},n\overline{q};2^\alpha)S(n\overline{2^\alpha},n\overline{2^\alpha};q) \tag{4.19}$$

e

$$S(n\overline{2^\alpha},n\overline{2^\alpha};q)=S(n\overline{2^\alpha}\overline{v},n\overline{2^\alpha}\overline{v};u)S(n\overline{2^\alpha}\overline{u},n\overline{2^\alpha}\overline{u};v). \tag{4.20}$$

Primeiro voltemos a atenção a $K_{t-q+1}(n\overline{q},n\overline{q};2^\alpha)=K_s(n',n';2^\alpha)$ e façamos $\alpha=2\beta+r_2$, onde $r_2=0$ ou 1 é o resto da divisão de α por 2. Observe que a função $\eta(d)=\varepsilon_d^{-s}\left(\frac{2^\alpha}{d}\right)=\varepsilon_d^{-s}\left(\frac{2^{r_2}}{d}\right)$ é periódica com período de tamanho 8. Se $\beta<3$, então $|K_s(n',n';2^\alpha)|\le 2^5=32$. Se $\beta\ge 3$, então $\eta(2^{\beta+r_2}x_2+x_1)=\eta x_1$, onde x_2 varia módulo 2^β e x_1 varia módulo $2^{\beta+r_2}$. Todo elemento de $\mathbb{Z}/2^\alpha\mathbb{Z}$ pode ser escrito da forma $2^{\beta+r_2}x_2+x_1$, este cujo o inverso módulo 2^α pode ser expresso como $\overline{2^{\beta+r_2}x_2+x_1}=-\overline{x_1}+2^{\beta+r_2}x_2\overline{x_1}(\mathrm{mod}\ 2^\alpha)$. Portanto

$$\begin{aligned}K_s(n',n';2^\alpha) &= \sum_{d(\mathrm{mod}\ 2^\alpha)}\eta(d)e\left(\frac{n(d+\overline{d})}{2^\alpha}\right) \\ &= \sum_{x_1(\mathrm{mod}\ 2^{\beta+r_2})}\left(\eta(x_1)e\left(\frac{n(x_1+\overline{x_1})}{2^\alpha}\right)\sum_{x_2(\mathrm{mod}\ 2^\beta)}e\left(\frac{n(1-\overline{x_1}^2)x_2}{2^\beta}\right)\right) \\ &= 2^\beta\sum_{\substack{x(\mathrm{mod}\ 2^{\beta+r_2})\\2^\beta|n(1-\overline{x}^2)}}\eta(x)e\left(\frac{n(x+\overline{x})}{2^\alpha}\right).\end{aligned}$$

Sendo n livre de quadrados, $2^\beta|n(1-\overline{x}^2)$ implica em $\overline{x}^2-1\equiv 0(\mathrm{mod}\ 2^{\beta-1})$, de modo que $\overline{x}\equiv\pm 1(\mathrm{mod}\ 2^{\beta-2})$. Portanto, poderão haver no máximo 16 soluções módulo $2^{\beta+r_2}$ que satisfazem $n(1-\overline{x}^2)\equiv 0(\mathrm{mod}\ 2^\beta)$, e assim

$$|K_s(n',n';2^\alpha)|\ll 2^\beta\le 2^{\alpha/2}. \tag{4.21}$$

Por (4.12), observando que $1 = (n, u) = (\overline{2^\alpha}\overline{v}n, u)$, obtemos

$$|S(n\overline{2^\alpha}\overline{v}, n\overline{2^\alpha}\overline{v}; u)| \leq u^{1/2}\tau(u). \tag{4.22}$$

Por outro lado, sendo n livre de quadrados e pela definição de v, $(n, c) \geq (n, v) = v$. Assim, por (4.19),(4.20),(4.21) e (4.22)

$$|K_t(n, n; c)| \ll 2^{\alpha/2}u^{1/2}\tau(u)v \leq (n, c)^{1/2}c^{1/2}\tau(c). \ \square$$

Obs: Pode-se mostrar que esse fato é bem mais forte que o demonstrado aqui. De fato, Iwaniec em (16) cita que, para todos os inteiro positivos n e c, vale

$$K_t(n, n; c) \leq (n, c)^{1/2}c^{1/2}\tau(c).$$

4.2 Somatório de somas de Kloosterman

Iremos supor a partir daqui que n é um inteiro livre de quadrados. Focaremos agora em procurar uma estimativa que envolva

$$K_Q^{(v)}(x) = \sum_{\substack{c \leq x \\ Q|c}} c^{-\frac{1}{2}} K_{2k}(n, n; c) e\left(\frac{2vn}{c}\right),$$

com $v = -1, 0, 1$ e $8|Q$, e, enquanto o valor de v não for fixado, denotaremos $K_Q^{(v)}$ apenas por K_Q. Usando a proposição 4.7 obtemos

$$|K_Q(x)| \leq \sum_{\substack{c \leq x \\ Q|c}} c^{-\frac{1}{2}} |K_{2k}(n, n; c)| \ll \sum_{\substack{c \leq x \\ Q|c}} (n, c)^{\frac{1}{2}}\tau(c) \leq \sum_{d|n} d^{\frac{1}{2}} \sum_{\substack{c \leq x \\ [d,Q]|c}} \tau(c). \tag{4.23}$$

Usando que $\tau(x) \ll_\epsilon x^\epsilon$

$$\sum_{d|n} d^{\frac{1}{2}} \frac{\tau([d, Q])}{[d, Q]} \ll_\epsilon n^\epsilon Q^\epsilon \sum_{d|n} \frac{d^{1/2}}{[d, Q]} = \frac{n^\epsilon Q^\epsilon}{Q} \sum_{d|n} \frac{(d, Q)}{d^{1/2}},$$

e observando que $(d, Q) \leq d$

$$\sum_{d|n} d^{\frac{1}{2}} \frac{\tau([d, Q])}{[d, Q]} \ll_\epsilon \frac{n^\epsilon Q^\epsilon}{Q}\tau(n)(n, Q)^{\frac{1}{2}} \ll_\epsilon \frac{n^\epsilon Q^\epsilon}{Q}(n, Q)^{\frac{1}{2}}. \tag{4.24}$$

Assim, usando (4.23) e o fato de que $\sum_{b\leq x}\tau(b) \ll x\log x$ e de que $\tau(ab)\leq\tau(a)\tau(b)$

$$\begin{aligned}|K_Q(x)| &\ll \sum_{d|n} d^{\frac{1}{2}} \sum_{\substack{c\leq x\\ [d,Q]|c}} \tau(c)\\ &\leq \sum_{d|n} d^{\frac{1}{2}}\tau([d,Q]) \sum_{\frac{c}{[d,Q]}\leq\frac{x}{[d,Q]}} \tau(\frac{c}{[d,Q]})\\ &\ll \sum_{d|n} d^{\frac{1}{2}}\tau([d,Q])(\frac{x}{[d,Q]})\log\frac{x}{[d,Q]},\end{aligned}$$

e combinando com a estimativa (4.24)

$$\begin{aligned}|K_Q(x)| &\ll x\log x\sum_{d|n}\frac{d^{\frac{1}{2}}\tau([d,Q])}{[d,Q]}\\ &\ll_\epsilon (n,Q)^{\frac{1}{2}}xQ^{-1}(nQx)^\epsilon.\end{aligned}$$

Em particular, a restrição de K_Q para quando $n|c$ pode ser estimada usando a estimativa anterior

$$\begin{aligned}|K_{[n,Q]}(x)| &\ll_\epsilon (n,[n,Q])^{\frac{1}{2}}[n,Q]^{-1}x(nQx)^\epsilon\\ &\ll_\epsilon n^{\frac{1}{2}}\tau(nQ)n^{-1}Q^{-1}(n,Q)x(nQx)^\epsilon\\ &= \frac{(n,Q)}{n^{\frac{1}{2}}Q}x(nQx)^\epsilon. \qquad (4.25)\end{aligned}$$

Faça

$$K_Q^*(y)=\sum_{\substack{y<c\leq 2y\\ n\nmid c, Q|c}} c^{-\frac{1}{2}}K_{2k}(n,n;c)e\left(\frac{2vn}{c}\right),$$

com $4<y\leq x$. Observe que $K_Q(x)$ pode ser decomposta em $O(\log x)$ parcelas da forma $K_Q^*(y)$, fazendo y igual a $\frac{x}{2^n}$, com n variando de 1 até o menor valor inteiro possível de n que satisfaz $\frac{x}{2^n}>4$, mais uma parcela igual a $K_{[n,Q]}(x)$. Seja agora $Q=LM$ com $8|L$, $L|(2n)^\infty$, $(M,2n)=1$. Seja também $c=qr$ como na proposição 4.4 e com as restrições adicionais $Q|c,(n,c)^2\nmid c$. Observe que $Q|c$ implica $LM|qr$ que implica em $L|r$ e $M|q$. Também temos que, como $(c,n)^2|c$, $(2n,q)=1$ se e só se $(r,n)^2|r$. Por último, $n\nmid c$ se e só se $n\nmid r$. Assim, tomando os conjuntos

$$\mathscr{R}=\{r; L|r, n\nmid r, (r,n)^2|r, r|(2n)^\infty\}$$

$$\mathscr{Q}=\{q; M|q, (2n,q)=1\}.$$

Como consequência da unicidade da fatoração em primos, cada inteiro positivo c que satisfaça $Q|c, n\nmid c, (n,c)^2|c$ pode ser representado de forma única como produto de um elemento de $\mathscr{R}$

com um elemento de $\mathscr{Q}$. Usando a proposição 4.4 e a proposição 4.5 temos

$$K_Q^*(y) = \sum_{\substack{y<c\leq 2y \\ n\nmid c, Q|c, (n,c)^2|c}} c^{-\frac{1}{2}} K_{2k}(n,n;c) e\left(\frac{2vn}{c}\right)$$

$$= \sum_{\substack{y<c\leq 2y \\ n\nmid c, Q|c, (n,c)^2|c}} r^{-\frac{1}{2}} K_{2k}(n,n;c) e\left(\frac{2vn}{c}\right)$$

$$= \sum_{\substack{y<qr\leq 2y \\ q\in\mathscr{Q}, r\in\mathscr{R}}} r^{-\frac{1}{2}} e\left(\frac{2vn}{qr}\right) \left(\sum_{\substack{s(\mathrm{mod}\ r/2) \\ 2\nmid s}} \varepsilon_s^{-t} f_r(2s)[(1+i^s)\left(\frac{nr}{q}\right) + (1-i^s)\left(\frac{-nr}{s}\right)] \right)$$

$$\times \left(\sum_{\substack{ab=q \\ (a,b)=1}} e\left(2n\left(\frac{\overline{ar}}{b} - \frac{\overline{br}}{a} + \frac{s\overline{ab}}{r}\right)\right) \right)$$

$$= \sum_{\substack{y<qr\leq 2y \\ q\in\mathscr{Q}, r\in\mathscr{R}}} r^{-\frac{1}{2}} \sum_{\substack{s(\mathrm{mod}\ r/2) \\ 2\nmid s}} \varepsilon_s^{-t} f_r(2s)[(1+i^s)F_{r,s}^+(M) + (1-i^s)F_{r,s}^-(M)],$$

onde

$$F_{r,s}^{\pm}(M) = \sum_{\substack{y<abr\leq 2y \\ ab\in\mathscr{Q}, (a,b)=1}} \left(\frac{\pm nr}{ab}\right) e\left[2n\left(\frac{\overline{ar}}{b} - \frac{\overline{br}}{a} + s\frac{\overline{ab}}{r} + \frac{v}{abr}\right)\right].$$

O próximo objetivo será obter uma estimativa envolvendo $F_{r,s}^{\pm}(M)$. Para tal, será útil definir a soma parcial $F^{\pm}(A,B;M)$ que será dada como uma restrição da soma $F_{r,s}^{\pm}(M)$ através da adição das seguintes condições ao somatório

$$A < a \leq 2A, \quad B < b \leq 2B,$$

onde A, B satisfazem

$$y < rAB \leq 2y, \quad A, B \geq \frac{1}{2},$$

ou seja

$$F^{\pm}(A,B;M) = \sum_{\substack{A<a\leq 2A \\ B<b\leq 2B \\ ab\in\mathscr{Q}, (a,b)=1}} \left(\frac{\pm nr}{ab}\right) e\left[2n\left(\frac{\overline{ar}}{b} - \frac{\overline{br}}{a} + s\frac{\overline{ab}}{r} + \frac{v}{abr}\right)\right].$$

É possível verificar que podemos decompor $F_{r,s}^{\pm}(M)$ em $O(\log y)$ dessas somas parciais. Por último, daqui pra frente denotaremos $F^+(A,B;M)$ e $F^-(A,B;M)$ somente por $F(A,B;M)$

enquanto o sinal não interferir na estimativa. A fórmula de reciprocidade

$$\frac{\overline{\alpha}}{\beta}+\frac{\overline{\beta}}{\alpha}\equiv\frac{1}{\alpha\beta}(\mathrm{mod}\ 1) \tag{4.26}$$

será usada para concluir que

$$\begin{aligned} e\left[2n\left(\frac{\overline{ar}}{b}-\frac{\overline{br}}{a}+s\frac{\overline{ab}}{r}+\frac{v}{abr}\right)\right] &= e\left[2n\frac{\overline{a}}{br}(r\overline{r}+sb\overline{b}+1)+2n\left(-\frac{\overline{br}}{a}-\frac{\overline{a}}{br}+\frac{v}{abr}\right)\right] \\ &= e[2n\frac{\overline{a}}{br}(r\overline{r}+sb\overline{b}+1)]e\left(2n\frac{(v-1)}{abr}\right), \end{aligned}$$

de onde obtemos

$$\begin{aligned} F(A,B;M) &= \sum_{\substack{A<a\leq 2A\\ B<b\leq 2B\\ ab\in\mathscr{Q},(a,b)=1}}\left(\frac{\pm nr}{ab}\right)e\left[2n\left(\frac{\overline{ar}}{b}-\frac{\overline{br}}{a}+s\frac{\overline{ab}}{r}+\frac{v}{abr}\right)\right] \\ &= \sum_{B<b\leq 2B}\sum_{\substack{A<a\leq 2A\\ ab\in\mathscr{Q},(a,b)=1}}\left(\frac{\pm nr}{ab}\right)e[2n\frac{\overline{a}}{br}(r\overline{r}+sb\overline{b}+1)]e\left(2n\frac{(v-1)}{abr}\right) \\ &= \sum_{B<b\leq 2B}\sum_{\substack{A<a\leq 2A\\ (a,b)=1,(ab,2n)=1}}\left(\frac{\pm nr}{ab}\right)e[2n\frac{\overline{a}}{br}(r\overline{r}+sb\overline{b}+1)]e\left(2n\frac{(v-1)}{abr}\right). \end{aligned}$$

Fixando b, usamos soma por partes em

$$\sum_{\substack{A<a\leq 2A\\ (a,b)=1,(ab,2n)=1}}\left(\frac{\pm nr}{ab}\right)e[2n\frac{\overline{a}}{br}(r\overline{r}+sb\overline{b}+1)]e\left(2n\frac{(v-1)}{abr}\right)$$

Faça $f(a)=\xi_b(a)\left(\frac{\pm nr}{ab}\right)e[2n\frac{\overline{a}}{br}(r\overline{r}+sb\overline{b}+1)]$, onde $\xi_b(a)=1$ se $(a,b)=(ab,2n)=1$, e $\xi_b(a)=0$ caso contrário. Também façamos $F(x)=\sum_{a\leq x}f(a+A)$. Seja $A'>0$ satisfazendo $|F(A')|\geq|F(x)|$ para todo $x\in(0,A]$, então

$$\begin{aligned} \sum_{\substack{A<a\leq 2A\\ (a,b)=1,(ab,2n)=1}}\left(\frac{\pm nr}{ab}\right)e[2n\frac{\overline{a}}{br}(r\overline{r}+sb\overline{b}+1)]e\left(2n\frac{(v-1)}{abr}\right) &= \sum_{x\leq A}f(x+A)e\left(\frac{C}{x+A}\right) \\ &= F(x)e\left(\frac{C}{2A}\right)-\int_1^A F(y)(-\frac{C}{(y+A)^2})e\left(\frac{C}{y+A}\right)dy, \end{aligned}$$

daí

$$\begin{aligned}\left|\sum_{x\leq A} f(x+A)e\left(\frac{C}{x+A}\right)\right| &\leq |F(x)| + \int_1^A |F(y)|\left(\frac{C}{(y+A)^2}\right)dy \\ &\leq |F(A')| + |F(A')|\int_1^A \frac{C}{(y+A)^2}dy \\ &\leq |F(A')|\left(1+\frac{C}{2A}\right) \\ &\ll |F(A')|\left(1+\frac{n}{y}\right).\end{aligned}$$

Logo

$$|F(A,B;M)| \ll \left(1+\frac{n}{y}\right)\sum_{B<b\leq 2B}\left|\sum_{\substack{A<a\leq A+A' \\ (a,b)=1,(ab,2n)=1}}\left(\frac{\pm nr}{ab}\right)e[2n\frac{\overline{a}}{br}(r\overline{r}+sb\overline{b}+1)]\right|.$$

Sendo $M_b = M/(b,M)$ e mudando a variável a por aM_b, tomando $m \in \mathbb{Z}$ satisfazendo $mM_b \equiv r\overline{r}+sb\overline{b}+1 (\mathrm{mod}\ br)$ e fazendo $A_1 = \lceil A/M_b \rceil$, $A_2 = \lfloor (A+A')/M_b \rfloor$, temos

$$|F(A,B;M)| \ll \left(1+\frac{n}{y}\right)\sum_{\substack{B<b\leq 2B \\ (b,2nM_b)=1}}\left|\sum_{\substack{A_1<a\leq A_2 \\ (a,b)=1}}\left(\frac{\pm nr}{a}\right)e[2nm\frac{\overline{a}}{br}]\right|. \tag{4.27}$$

Faça agora $\Delta_1 = n/(n,r)$ e $\Delta_2 = r/(n,r)$, o somatório interno da soma acima será agora escrito como

$$\sum_a = \sum_{\substack{A_1<a\leq A_2 \\ (a,b)=1}}\left(\frac{\pm nr}{a}\right)e[2nm\frac{\overline{a}}{br}] = \sum_{A_1<a\leq A_2}\left(\frac{\pm\Delta_1\Delta_2}{a}\right)e\left(2m\frac{\Delta_1\overline{a}}{\Delta_2 b}\right).$$

Observe que cada parcela do somatório acima tem período igual a $D = \Delta_1\Delta_2 b$ em relação à variável a, logo podemos usar (4.17) para concluir que

$$\left|\sum_a\right| \leq \sum_{1\leq d\leq D}\frac{1}{d}\left|\sum_{x(\mathrm{mod}\ D)}\left(\frac{\pm\Delta_1\Delta_2}{x}\right)e\left(2m\frac{\Delta_1\overline{x}}{\Delta_2 b}+\frac{dx}{D}\right)\right|.$$

Note que Δ_1, Δ_2, b são dois a dois primos entre si, $4|\Delta_2$,$(b,m)=1$ e que Δ_1 é livre de quadrados. Faça

$$\begin{cases}\Delta_1' = \Delta_1, \Delta_2' = \Delta_2, \text{ caso } \Delta_1 \equiv 1(\mathrm{mod}\ 4). \\ \Delta_1' = -\Delta_1, \Delta_2' = -\Delta_2, \text{ caso } \Delta_1 \equiv 3(\mathrm{mod}\ 4).\end{cases}$$

Isso garantirá que $\Delta_1' \equiv 1 (\mathrm{mod}\ 4)$. Portanto, o condutor de $\mathbb{Q}(\sqrt{\Delta_1'})$ será $|\Delta_1'| = \Delta_1$, o que garante que

$$x \to \left(\frac{\Delta_1'}{x}\right)$$

é um caráter multiplicativo de ordem 2 não trivial módulo Δ_1 (veja ([26], p.442)), e o mesmo é válido para Δ_2' (ser caráter módulo Δ_2) por ser múltiplo de 4. Logo

$$\sum_{x(\mathrm{mod}\ D)} \left(\frac{\pm\Delta_1\Delta_2}{x}\right) e\left(2m\frac{\Delta_1\overline{x}}{\Delta_2 b} + \frac{dx}{D}\right) = \left(\sum_{x(\mathrm{mod}\ \Delta_1)} \left(\frac{\Delta_1'}{x}\right) e\left(\frac{d\overline{\Delta_2 bx}}{\Delta_1}\right)\right)$$

$$\left(\sum_{x(\mathrm{mod}\ \Delta_2)} \left(\frac{\pm\Delta_2'}{x}\right) e\left(\frac{2m\Delta_1\overline{bx} + \overline{\Delta_1}bdx}{\Delta_2}\right)\right)\left(\sum_{x(\mathrm{mod}\ b)} e\left(\frac{2m\overline{\Delta_2 x} + \overline{\Delta_2}x}{b}\right)\right).$$

Nesse ponto, usando a fórmula da soma de Gauss no primeiro caso, a estimativa para somas de Salié no segundo caso ([18], p.26) e a estimativa de Weil no terceiro caso, obtemos

$$\begin{aligned}
\sum_{x(\mathrm{mod}\ \Delta_1)} \left(\frac{\Delta_1'}{x}\right) e\left(\frac{d\overline{\Delta_2 bx}}{\Delta_1}\right) &\ll \Delta_1^{\frac{1}{2}} \\
\sum_{x(\mathrm{mod}\ \Delta_2)} \left(\frac{\pm\Delta_2'}{x}\right) e\left(\frac{2m\Delta_1\overline{bx} + \overline{\Delta_1}bdx}{\Delta_2}\right) &\ll (d,\Delta_2)^{\frac{1}{2}}\Delta_2^{\frac{1}{2}}\tau(\Delta_2) \\
\sum_{x(\mathrm{mod}\ b)} e\left(\frac{2m\overline{\Delta_2 x} + \overline{\Delta_2}x}{b}\right) &\ll b^{\frac{1}{2}}\tau(b),
\end{aligned}$$

de onde

$$\begin{aligned}
\left|\sum_a\right| &\leq \sum_{1\leq d\leq D} \frac{1}{d}\Delta_1^{\frac{1}{2}}\Delta_2^{\frac{1}{2}}b^{\frac{1}{2}}(d,\Delta_2)^{\frac{1}{2}}\tau(b)\tau(\Delta_2) \\
&= (bnr)^{\frac{1}{2}}(n,r)^{-1}\tau(b)\tau(\Delta_2)\sum_{1\leq d\leq D}\frac{(d,\Delta_2)^{\frac{1}{2}}}{d} \\
&\ll (bnr)^{\frac{1}{2}}(n,r)^{-1}\tau(b)\tau(r)^2\log bnr.
\end{aligned}$$

Voltando à estimativa de $|F(A,B;M)|$ em (4.27), concluímos

$$F(A,B;M) \ll (1+\frac{n}{y})(nr)^{\frac{1}{2}}\tau(r)^2\log ny\sum_{B<b\leq 2B} b^{\frac{1}{2}}\tau(b).$$

Por último, observando que podemos usar soma por partes e a desigualdade $\sum_{b\leq x}\tau(b) \ll$

$x \log x$ para concluir que $\sum_{B \leq b \leq 2B} b^{\frac{1}{2}} \tau(b) \ll B^{\frac{3}{2}} \log B$. Finalmente, concluímos que

$$|F(A,B;M)| \ll_\epsilon B^{\frac{3}{2}} \left(1 + \frac{n}{y}\right) (nr)^{\frac{1}{2}} \tau(r)^2 n^\epsilon y^\epsilon. \tag{4.28}$$

De forma análoga, concluímos

$$|F(A,B;M)| \ll_\epsilon A^{\frac{3}{2}} \left(1 + \frac{n}{y}\right) (nr)^{\frac{1}{2}} \tau(r)^2 n^\epsilon y^\epsilon. \tag{4.29}$$

4.3 Uma estimativa para *F(A,B;M)* em média

As estimativas (4.28) e (4.29) serão usadas quando B ou A forem pequenos, respectivamente. Agora, estabeleceremos uma estimativa em média com respeito à variável M, que será usada quando A ou B forem suficientemente grandes. Fixe M_0 um inteiro relativamente primo com $2n$ e, dado $P > 0$, $\mathscr{P} = \{p; p \text{ inteiro primo}, P < p \leq 2P, p \nmid 2n\}$. Desejamos estimar

$$F_P(A,B) = \sum_{p \in \mathscr{P}} |F(A,B;pM_0)|.$$

Se $\lambda_p = \frac{\overline{F(A,B;pM_0)}}{|F(A,B;pM_0)|}$, onde nesse caso, a barra indica conjugado complexo, uma inversão na ordem dos somatórios é usada para concluir que

$$F_P(A,B) = \sum_{\substack{A < a \leq 2A \\ y < abr \leq 2y}} \sum_{\substack{B < b \leq 2B \\ (a,b)=1}} \sum_{\substack{P < p \leq 2P \\ pM_0 | ab}} \lambda_p \left(\frac{\pm nr}{ab}\right)$$

$$\times e\left[2n\left(\frac{\overline{ar}}{b} - \frac{\overline{br}}{a} + \frac{s\overline{ab}}{r} + \frac{v}{abr}\right)\right].$$

Há duas possibilidades para cada $p \in \mathscr{P}$: $p|a$ ou $p|b$. Assim, podemos escrever $F_P(A,B)$ como

$$F_P(A,B) = F(A/P, B) + F(A, B/P),$$

onde $F(A/P,B)$ tem a restrição adicional de $p|a$ no somatório que define $F_P(A,B)$, e $F(A,B/P)$ tem a restrição adicional de $p|b$ no somatório que define $F_p(A,B)$. Iremos tratar de $F(A/P,B)$ primeiro, o caso $F(A,B/P)$ é análogo. Dado $M = pM_0$ com $p \in \mathscr{P}$, mudando a variável a para ap, encontramos

$$|F(A/P,B)| \leq \sum_{A/2P < a \leq A/P} \sum_{B < b \leq 2B} \left| \sum_{P_1 < p \leq P_2} \lambda_p e\left[2n\left(\frac{\overline{ar}}{b} - \frac{\overline{br}}{a} + \frac{s\overline{ab}}{r} + \frac{v}{abr}\right)\right] \right|,$$

onde $P_1 = \max(P, y/abr)$ e $P_2 = \min(2P, 2y/abr)$. Observe que, nessa nova configuração, $y < apbr \leq 2y$. Usando Cauchy-Schwarz, expandido o quadrado e trocando a ordem das

somas, vemos que

$$|F(A/P,B)| \ll ABP^{-1} \sum_{A/2P<a\leq A/P} \sum_{B<b\leq 2B} \left| \sum_{P_1<p\leq P_2} \lambda_p e[2n\left(\frac{\overline{ar}}{b} - \frac{\overline{br}}{a} + \frac{s\overline{ab}}{r} + \frac{v}{abr}\right)] \right|^2$$
$$\leq ABP^{-1} \sum_{P_1<p_1\leq P_2} \sum_{P_1<p_2\leq P_2} G(A/P,B), \tag{4.30}$$

onde

$$G(A/P,B) = \left| \sum_{A/2P<a\leq A/P} \sum_{B<b\leq 2B} e\left[2n(p_2-p_1)\left(\frac{\overline{ap_1p_2r}}{b} - \frac{\overline{br}}{ap_1p_2} + s\frac{\overline{ap_1p_2b}}{r} + \frac{v}{ap_1p_2br}\right)\right] \right|.$$

Usando a fórmula de reciprocidade (4.26)

$$e\left[2n(p_2-p_1)\left(\frac{\overline{ap_2p_1r}}{b} - \frac{\overline{br}}{ap_1p_2} + s\frac{\overline{ap_1p_2b}}{r} + \frac{v}{ap_1p_2br}\right)\right]$$

$$= e[2n(p_2-p_1)\left(\frac{\overline{ap_2p_1r}}{b} - \frac{\overline{br}}{ap_1p_2} - \frac{\overline{ap_1p_2}}{br} + \frac{\overline{ap_1p_2}}{br} + s\frac{\overline{ap_1p_2b}}{r} + \frac{1}{ap_1p_2br}\right)]e\left(\frac{2n(v-1)(p_2-p_1)}{abrp_1p_2}\right)$$
$$= e\left[2n(p_2-p_1)\overline{p_1p_2}(r\overline{r}+1+s\overline{b}\overline{b})\frac{\overline{a}}{br}\right] e\left(\frac{2n(v-1)(p_2-p_1)}{abrp_1p_2}\right).$$

Aplicando soma por partes de forma similar a usada para concluir (4.27) para eliminar o termo $e\left(\frac{2n(v-1)(p_2-p_1)}{abrp_1p_2}\right)$, chegamos em

$$\sum_{A/2P<a\leq A/P} e\left[2n(p_2-p_1)\overline{p_1p_2}(r\overline{r}+1+s\overline{b}\overline{b})\frac{\overline{a}}{br}\right] e\left(\frac{2n(v-1)(p_2-p_1)}{abrp_1p_2}\right)$$

$$\ll (1+\frac{n}{y}) \left| \sum_{A/2P<a\leq A'} e\left[2n(p_2-p_1)\overline{p_1p_2}(r\overline{r}+1+s\overline{b}\overline{b})\frac{\overline{a}}{br}\right] \right|,$$

onde A' é o inteiro no intervalo $[A/2P, 2A/P]$ que maximiza a norma do somatório. Usando a proposição 4.6 com $q = br/(n,r)$ e $m = 2n(p_2-p_1)\overline{p_1p_2}(r\overline{r}+1+s\overline{b}\overline{b})/(n,r)$ quando $p_1 \neq p_2$, e observando, usando a definição, que

$$(m,q) \leq (\frac{2n(p_2-p_1,br)}{(n,r)}, \frac{br}{(n,r)})(r\overline{r}+1+s\overline{b}\overline{b},b)(r\overline{r}+1+s\overline{b}\overline{b},r) \leq (p_2-p_1,br)(s+1,r),$$

temos

$$\left| \sum_{A/2P<a\leq A'} e\left(\frac{\overline{a}m}{q}\right) \right| \ll (m,q)^{\frac{1}{2}} q^{\frac{1}{2}} \tau(q) \log 2q + (m,q) q^{-1} \tau(q) A'$$

$$\begin{aligned} &\ll (s+1)^{\frac{1}{2}}(p_2-p_1,br)^{\frac{1}{2}}b^{\frac{1}{2}}r^{\frac{1}{2}}(n,r)^{-\frac{1}{2}}\tau(br)\log br+(s+1,r)(p_2-p_1,br)(n,r)b^{-1}r^{-1}\tau(br)\frac{A}{P} \\ &\ll (s+1,r)\tau(br)\log br\left[\frac{(p_2-p_1,br)^{\frac{1}{2}}b^{\frac{1}{2}}r^{\frac{1}{2}}}{(n,r)^{\frac{1}{2}}}+\frac{(p_2-p_1,br)(n,r)A}{brP}\right]. \end{aligned}$$

Assim

$$\sum_{A/2P<a\leq A/P} e\left[2n(p_2-p_1)\overline{p_1p_2}(r\overline{r}+1+s\overline{b}\overline{b})\frac{\overline{a}}{br}\right]e\left(\frac{2n(v-1)(p_2-p_1)}{abrp_1p_2}\right)$$

$$\ll (1+\frac{n}{y})(s+1,r)\tau(br)\log br\left[\frac{(p_2-p_1,br)^{\frac{1}{2}}b^{\frac{1}{2}}r^{\frac{1}{2}}}{(n,r)^{\frac{1}{2}}}+\frac{(p_2-p_1,br)(n,r)A}{brP}\right].$$

Como consequência, procuraremos estimar agora

$$\sum_{\substack{P_1<p_1,p_2\leq P_2\\ p_2\neq p_1}}\sum_{B<b\leq 2B}\tau(br)\log br\left[\frac{(p_2-p_1,br)^{\frac{1}{2}}b^{\frac{1}{2}}r^{\frac{1}{2}}}{(n,r)^{\frac{1}{2}}}+\frac{(p_2-p_1,br)(n,r)A}{brP}\right], \tag{4.31}$$

uma vez que, incluindo na condição de soma do somatório

$$\sum_{P<p_1,p_2\leq 2P}\left|\sum_{A/2P<a\leq A/P}\sum_{B<b\leq 2B} e[2n(p_2-p_1)(\frac{\overline{ap_1p_2r}}{b}-\frac{\overline{br}}{ap_1p_2}+s\frac{\overline{ap_1p_2b}}{r}+\frac{v}{ap_1p_2br})]\right|$$

a condição $p_1=p_2$, temos

$$\sum_{P<p\leq 2P}\left|\sum_{A/2P<a\leq A/P}\sum_{B<b\leq 2B}1\right|\ll AB. \tag{4.32}$$

Observe que

$$\begin{aligned} \sum_{p_1\neq p_2}(p_2-p_1,br) &\leq \sum_{p_2\neq p_2}\sum_{\substack{e|br\\ e|p_2-p_1}} e \\ &\leq \sum_{p_2}\sum_{e|br} e\sum_{\substack{P_1\leq n\leq P_2\\ e|n-p_2}}1 \\ &\ll \sum_{p_2}\sum_{e|br} e\frac{P}{e} \\ &\ll P^2\tau(br). \end{aligned}$$

Também precisaremos de uma outra desigualdade envolvendo a função τ

$$\sum_{b\leq B}\tau(b)^2\ll B(\log B)^3.$$

Usando soma por partes e a desigualdade acima, podemos concluir também que

$$\sum_{b\leq B}\frac{\tau(b)^2}{b}\ll(\log B)^4.$$

Estimemos agora a primeira e a segunda parcela da soma (4.31) separadamente usando essas três desigualdades anteriormente citadas. Na primeira parcela

$$\begin{aligned}\sum_{\substack{P_1<p_1,p_2\leq P_2\\ p_2\neq p_1}}\sum_{B<b\leq 2B}\tau(br)\log br\frac{(p_2-p_1,br)^{\frac{1}{2}}b^{\frac{1}{2}}r^{\frac{1}{2}}}{(n,r)^{\frac{1}{2}}} &\leq \tau(r)\log y\frac{r^{\frac{1}{2}}}{(n,r)^{\frac{1}{2}}}\sum_b b^{\frac{1}{2}}\tau(b)\sum_{p_1,p_2}(p_2-p_1)^{\frac{1}{2}}\\ &\ll \tau(r)^2\log y\frac{r^{\frac{1}{2}}}{(n,r)^{\frac{1}{2}}}P^2B^{\frac{1}{2}}\sum_b\tau(b)^2\\ &\ll_\epsilon \frac{r^{\frac{1}{2}}}{(n,r)^{\frac{1}{2}}}B^{\frac{3}{2}}\tau(r)^2P^2y^\epsilon,\end{aligned}$$

e então, usando um processo análogo para estimar a segunda parcela

$$\begin{aligned}\sum_{p_1\neq p_2}\sum_b\frac{(n,r)A}{brP}(p_2-p_1,br)\tau(br)\log br &\leq \tau(r)\log y\frac{(n,r)A}{rP}\sum_b\frac{\tau(b)}{b}\sum_{p_1,p_2}(p_2-p_1)\\ &\ll \tau(r)^2\log y\frac{(n,r)A}{rP}P^2\sum_b\frac{\tau(b)^2}{b}\\ &\ll_\epsilon \tau(r)^2\frac{(n,r)A}{r}Py^\epsilon.\end{aligned}$$

Assim, combinando as duas estimativas anteriores com (4.32), obtemos

$$\sum_{P_1<p_1\leq P_2}\sum_{P_1<p_2\leq P_2}\left|\sum_{A/2P<a\leq A/P}\sum_{B<b\leq 2B}e[2n(p_2-p_1)(\frac{\overline{ap_1p_2r}}{b}-\frac{\overline{br}}{ap_1p_2}+s\frac{\overline{ap_1p_2b}}{r}+\frac{v}{ap_1p_2br})]\right|$$

$$\ll_\epsilon AB+(1+\frac{n}{y})(s+1,r)\tau(r)^2\left[\frac{r^{\frac{1}{2}}}{(n,r)^{\frac{1}{2}}}B^{\frac{3}{2}}P^2+\frac{(n,r)}{r}AP\right]y^\epsilon.$$

Por (4.30) e por $1\leq(n,r)\leq r^{\frac{1}{2}}$

$$F(A/P,B)^2\ll_\epsilon A^2B^2P^{-1}+(1+\frac{n}{y})(s+1,r)\tau(r)^2\left[r^{\frac{1}{2}}AB^{\frac{5}{2}}P+r^{\frac{1}{2}}A^2B\right]y^\epsilon,$$

para finalmente encontrarmos que

$$F(A/P,B)\ll_\epsilon ABP^{-\frac{1}{2}}+(1+\frac{n}{y})^{\frac{1}{2}}(s+1,r)^{\frac{1}{2}}\tau(r)(r^{\frac{1}{4}}A^{\frac{1}{2}}B^{\frac{5}{4}}P^{\frac{1}{2}}+r^{-\frac{1}{4}}AB^{\frac{1}{2}})y^\epsilon. \qquad (4.33)$$

Podemos encontrar outra estimativa para $F(A/P,B)$ procedendo de forma análoga ao que fizemos para obter (4.33). De fato, podemos usar a fórmula de reciprocidade para con-

cluir que

$$e[2n(p_2-p_1)(\frac{\overline{ap_1p_2r}}{b}-\frac{\overline{br}}{ap_1p_2}+s\frac{\overline{ap_1p_2b}}{r}+\frac{v}{ap_1p_2br})]$$

$$=e[2n(p_2-p_1)(\frac{\overline{ap_1p_2r}}{b}+\frac{\overline{b}}{ap_1p_2r}-\frac{\overline{b}}{ap_1p_2r}-\frac{\overline{br}}{ap_1p_2}+s\frac{\overline{ap_1p_2b}}{r}-\frac{1}{ap_1p_2br})]e\left(\frac{2n(v+1)(p_2-p_1)}{abrp_1p_2}\right)$$

$$=e[2n(p_2-p_1)(s\overline{ap_1p_2}ap_1p_2-1-r\overline{r})\frac{\overline{b}}{ap_1p_2r}]e\left(\frac{2n(v+1)(p_2-p_1)}{abrp_1p_2}\right),$$

logo, usando soma por partes para retirar o fator $e\left(\frac{2n(v+1)(p_2-p_1)}{abrp_1p_2}\right)$, temos

$$\sum_{A/2P<a\leq A/P} e\left[2n(p_2-p_1)(s\overline{ap_1p_2}ap_1p_2-1-r\overline{r})\frac{\overline{b}}{ap_1p_2r}\right]e\left(\frac{2n(v-1)(p_2-p_1)}{abrp_1p_2}\right)$$

$$\ll(1+\frac{n}{y})\left|\sum_{A/2P<a\leq A'} e\left[2n(p_2-p_1)(s\overline{ap_1p_2}ap_1p_2-1-r\overline{r})\frac{\overline{b}}{ap_1p_2r}\right]\right|,$$

e assim, tomando $m=2n(p_2-p_1)\overline{b}(s\overline{ap_1p_2}ap_1p_2-1-r\overline{r})/(n,r)$, $q=ap_1p_2r/(n,r)$ e observando que $(m,q)\leq(p_2-p_1,ap_1p_2r)(s-1,r)=(p_2-p_1,ar)(s-1,r)$, podemos repetir o processo que usamos para obter (4.33) para se obter

$$F(A/P,B)\ll_\epsilon ABP^{-\frac{1}{2}}+(1+\frac{n}{y})^{\frac{1}{2}}(s-1,r)^{\frac{1}{2}}\tau(r)[r^{\frac{1}{4}}B^{\frac{1}{2}}A^{\frac{5}{4}}P^{\frac{1}{4}}+r^{-\frac{1}{4}}BA^{\frac{1}{2}}P^{-\frac{1}{2}}]y^\epsilon. \quad (4.34)$$

Como $min\{A^{\frac{1}{2}}B^{\frac{5}{4}}P^{\frac{1}{2}},A^{\frac{5}{4}}B^{\frac{1}{2}}P^{\frac{1}{4}}\}\leq(AB)^{\frac{7}{8}}P^{\frac{3}{8}}$ e $rAB\leq 2y$, (4.33) e (4.34) implicam que

$$F(A/P,B)\ll_\epsilon yr^{-1}P^{-\frac{1}{2}}+(1+\frac{n}{y})^{\frac{1}{2}}(s^2-1,r)^{\frac{1}{2}}\tau(r)[y^{\frac{7}{8}}r^{-\frac{5}{8}}P^{\frac{3}{8}}+(A^{-\frac{1}{2}}+B^{-\frac{1}{2}})yr^{-\frac{5}{4}}]y^\epsilon.$$

De forma análoga podemos obter uma desigualdade idêntica para $F(A,B/P)$. Assim

$$F_P(A,B)\ll_\epsilon yr^{-1}P^{-\frac{1}{2}}+(1+\frac{n}{y})^{\frac{1}{2}}(s^2-1,r)^{\frac{1}{2}}\tau(r)[y^{\frac{7}{8}}r^{-\frac{5}{8}}P^{\frac{3}{8}}+(A^{-\frac{1}{2}}+B^{-\frac{1}{2}})yr^{-\frac{5}{4}}]y^\epsilon. \quad (4.35)$$

4.4 Uma estimativa para $\mathbf{K_Q(x)}$ em média

Agora temos as ferramentas necessárias para produzir uma estimativa para $K_Q(x)$ em média com respeito à variável Q. Primeiro, suponha que $min\{A,B\}$ seja menor que

$$(1+\frac{n}{y})^{-\frac{1}{4}}n^{-\frac{1}{4}}r^{-\frac{7}{8}}y^{\frac{1}{2}}P^{-\frac{1}{2}}.$$

Temos por (4.28) ou (4.29) que

$$\sum_{p\in\mathscr{P}}|F^{\pm}(A,B;pM_0)|\ll_\epsilon(1+\frac{n}{y})^{\frac{5}{8}}P^{\frac{1}{4}}n^{\frac{1}{8}}r^{-\frac{13}{16}}y^{\frac{3}{4}}\tau(r)^2n^\epsilon y^\epsilon.$$

Caso contrário, se $min\{A,B\}$ for maior ou igual que $(1+\frac{n}{y})^{-\frac{1}{4}}n^{-\frac{1}{4}}r^{-\frac{7}{8}}y^{\frac{1}{2}}P^{-\frac{1}{2}}$, temos $(A^{-\frac{1}{2}}+B^{-\frac{1}{2}})\leq(1+\frac{n}{y})^{\frac{1}{8}}n^{\frac{1}{8}}r^{\frac{7}{16}}y^{-\frac{1}{4}}P^{\frac{1}{4}}$ e daí por (4.35)

$$\sum_{p\in\mathscr{P}}|F^{\pm}(A,B;pM_0)|\ll_\epsilon yr^{-1}P^{-\frac{1}{2}}+(1+\frac{n}{y})^{\frac{5}{8}}(s^2-1,r)^{\frac{1}{2}}\tau(r)[y^{\frac{7}{8}}r^{-\frac{5}{8}}P^{\frac{3}{8}}+n^{\frac{1}{8}}r^{-\frac{13}{16}}y^{\frac{3}{4}}P^{\frac{1}{4}}]y^{\epsilon}.$$

Assim, é válido para quaisquer A e B

$$\sum_{p\in\mathscr{P}}|F^{\pm}(A,B;pM_0)|\ll_\epsilon yr^{-1}P^{-\frac{1}{2}}+(1+\frac{n}{y})^{\frac{5}{8}}(s^2-1,r)^{\frac{1}{2}}\tau(r)^2[y^{\frac{7}{8}}r^{-\frac{5}{8}}P^{\frac{3}{8}}+n^{\frac{1}{8}}r^{-\frac{13}{16}}y^{\frac{3}{4}}P^{\frac{1}{4}}]n^{\epsilon}y^{\epsilon}.$$

Consequentemente

$$\sum_{p\in\mathscr{P}}|F^{\pm}_{r,s}(pM_0)|\ll_\epsilon yr^{-1}P^{-\frac{1}{2}}\log y+(1+\frac{n}{y})^{\frac{5}{8}}(s^2-1,r)^{\frac{1}{2}}\tau(r)^2[y^{\frac{7}{8}}r^{-\frac{5}{8}}P^{\frac{3}{8}}+n^{\frac{1}{8}}r^{-\frac{13}{16}}y^{\frac{3}{4}}P^{\frac{1}{4}}]n^{\epsilon}y^{\epsilon}. \tag{4.36}$$

Serão necessárias duas proposições auxiliares para obtermos a estimativa que desejamos.

Proposição 4.8

$$\sigma_r=\sum_{s(\mathrm{mod}\ r/2)}|f_r(2s)|(s^2-1,r)^{\frac{1}{2}}\ll r\tau(r)^2.$$

Prova: Da definição de $f_r(2s)$

$$\sigma_r\leq\sum_{s(\mathrm{mod}\ r/2)}\ \sum_{\substack{d(\mathrm{mod}\ r)\\ d+\overline{d}=2s(\mathrm{mod}\ r)}}((d+\overline{d})^2-4,r)^{\frac{1}{2}}=\sum_{\substack{d(\mathrm{mod}\ r)\\ (d,r)=1}}((d^2-1)^2,r)^{\frac{1}{2}}.$$

Suponha que $r=p^\alpha$, p primo. Definindo λ_p por $\lambda_p=4$ se $p=2$ e $\lambda_p=2$ caso contrário, temos

$$\begin{aligned}\sum_{\substack{d(\mathrm{mod}\ r)\\ (d,r)=1}}((d^2-1)^2,r)^{\frac{1}{2}} &\leq \sum_{0\leq l\leq\alpha}p^{\frac{l}{2}}|\{d(\mathrm{mod}\ p^\alpha);d^2\equiv 1(\mathrm{mod}\ p^{\lceil\frac{l+1}{2}\rceil})\}|\\ &\leq \lambda_p(\alpha+1)p^\alpha,\end{aligned}$$

onde usamos que $x^2\equiv 1(\mathrm{mod}\ p^\alpha)$ tem no máximo λ_p soluções módulo p^α. No caso r genérico, as multiplicidades das funções de domínios inteiros $x\to\sum_{\substack{d(\mathrm{mod}\ x)\\ (d,x)=1}}((d^2-1)^2,x)^{\frac{1}{2}}$ e $x\to x\tau(x)^2$ garantem que

$$\sigma_r\ll r\tau(r)^2.\ \square$$

Proposição 4.9

$$\sum_{r\in\mathscr{R}}r^{-\frac{1}{8}}\tau(r)^4\ll_\epsilon(ny)^{\epsilon}.$$

Prova: A definição de r diz que todos os fatores primos que dividem r também dividem $2n$. além disso, $r \leq 2y$. Portanto

$$\sum_{r\in\mathscr{R}} r^{-\frac{1}{8}}\tau(r)^4 \ll_\epsilon y^\epsilon \prod_{p|2n}(1+p^{-1/8}+p^{-2/8}+...) = y^\epsilon \prod_{p|2n}\left(\frac{1}{1-p^{-1/8}}\right).$$

Observando que $\frac{1}{1-p^{-1/8}} < 2$ sempre que $p > 2^8$ e que $2^{\omega(2n)} \leq \tau(2n)$, concluímos que

$$\sum_{r\in\mathscr{R}} r^{-\frac{1}{8}}\tau(r)^4 \ll_\epsilon y^\epsilon 2^{\omega(2n)} \ll_\epsilon n^\epsilon y^\epsilon. \ \square$$

Fixe Q_0, faça $Q_0 = L_0M_0$ $(8|L_0, L_0|(2n)^\infty, (M_0, L_0) = 1)$ e defina o conjunto $\mathbb{P} = \{pQ_0; p \text{ primo}, P < p \leq 2P, p \nmid 2n\}$. Tomando, para cada $Q \in \mathbb{P}$, $Q = LM$ com $8|L, L|(2n)^\infty$ e $(M, L) = 1$, obtemos usando (4.36)

$$\sum_{Q\in\mathbb{P}} |K_Q^*(y)| \leq \sum_{Q\in\mathbb{P}}\sum_{r\in\mathscr{R}} r^{-\frac{1}{2}} \sum_{\substack{s(\text{mod } r/2)\\ 2\nmid s}} 2|f_r(2s)|(|F_{r,s}^+(M)| + |F_{r,s}^-(M)|)$$

$$= 2\sum_{r\in\mathscr{R}} r^{-\frac{1}{2}} \sum_{\substack{s(\text{mod } r/2)\\ 2\nmid s}} |f_r(2s)| \sum_{p\in\mathscr{P}} |F_{r,s}^{\pm}(pM_0)|$$

$$\ll_\epsilon \sum_{r\in\mathscr{R}} r^{-\frac{1}{2}} \sum_{\substack{s(\text{mod } r/2)\\ 2\nmid s}} |f_r(2s)|$$

$$\times(yr^{-1}P^{-\frac{1}{2}}\log y + (1+\frac{n}{y})^{\frac{5}{8}}(s^2-1,r)^{\frac{1}{2}}\tau(r)^2[y^{\frac{7}{8}}r^{-\frac{5}{8}}P^{\frac{3}{8}} + n^{\frac{1}{8}}r^{-\frac{13}{16}}y^{\frac{3}{4}}P^{\frac{1}{4}}])n^\epsilon y^\epsilon$$

$$= X_1 + X_2 + X_3,$$

onde

$$X_1 = yP^{-\frac{1}{2}}\log y \sum_{r\in\mathscr{R}} r^{-\frac{3}{2}} \sum_{s(\text{mod } r/2)} |f_r(2s)|$$

$$X_2 = (1+\frac{n}{y})^{\frac{5}{8}} y^{\frac{7}{8}} P^{\frac{3}{8}} \left[\sum_{r\in\mathscr{R}} r^{-\frac{9}{8}}\tau(r)^2 \sum_{s(\text{mod } r/2)} |f_r(s)|(s^2-1,r)^{\frac{1}{2}}\right] O_\epsilon(n^\epsilon y^\epsilon)$$

$$X_3 = (1+\frac{n}{y})^{\frac{5}{8}} n^{\frac{1}{8}} y^{\frac{3}{4}} P^{\frac{1}{4}} \left[\sum_{r\in\mathscr{R}} r^{-\frac{21}{16}}\tau(r)^2 \sum_{s(\text{mod } r/2)} |f_r(s)|(s^2-1,r)^{\frac{1}{2}}\right] O_\epsilon(n^\epsilon y^\epsilon).$$

Usando em cada uma dessas parcelas as proposições 4.8 e 4.9, obtemos

$$\begin{aligned} X_1 &\ll yP^{-\frac{1}{2}}\log y\sum_{r\in\mathscr{R}} r^{-\frac{1}{2}}\tau(r)^2 \ll_\epsilon yP^{-\frac{1}{2}}n^\epsilon y^\epsilon \\ X_2 &\ll_\epsilon (1+\frac{n}{y})^{\frac{5}{8}}y^{\frac{7}{8}}P^{\frac{3}{8}}n^\epsilon y^\epsilon\sum_{r\in\mathscr{R}} r^{-\frac{1}{8}}\tau(r)^4 \ll_\epsilon (1+\frac{n}{y})^{\frac{5}{8}}y^{\frac{7}{8}}P^{\frac{3}{8}}n^\epsilon y^\epsilon \\ X_3 &\ll_\epsilon (1+\frac{n}{y})^{\frac{5}{8}}n^{\frac{1}{8}}y^{\frac{3}{4}}P^{\frac{1}{4}}n^\epsilon y^\epsilon\sum_{r\in\mathcal{R}} r^{-\frac{5}{16}}\tau(r)^4 \ll_\epsilon (1+\frac{n}{y})^{\frac{5}{8}}n^{\frac{1}{8}}y^{\frac{3}{4}}P^{\frac{1}{4}}n^\epsilon y^\epsilon, \end{aligned}$$

portanto

$$\sum_{Q\in\mathbb{P}}|K_Q^*(y)| \ll_\epsilon yP^{-\frac{1}{2}}n^\epsilon y^\epsilon + (1+\frac{n}{y})^{\frac{5}{8}}[y^{\frac{7}{8}}P^{\frac{3}{8}} + n^{\frac{1}{8}}y^{\frac{3}{4}}P^{\frac{1}{4}}]y^\epsilon n^\epsilon.$$

Por último, tendo em vista que $|K_Q(x)| \ll \log x|K_Q^*(x)| + |K_{[Q,n]}(x)|$ e observando por (4.25) que

$$\begin{aligned} \sum_{Q\in\mathbb{P}}|K_{[Q,n]}(x)| &\ll_\epsilon \sum_{p\in\mathscr{P}}\frac{(n,pQ_0)}{n^{\frac{1}{2}}pQ_0}x(xpQ_0n)^\epsilon \\ &\ll_\epsilon \frac{(n,Q_0)}{n^{\frac{1}{2}}Q_0}x(xPQ_0n)^\epsilon \\ &\ll_\epsilon xn^{-\frac{1}{2}}O_\epsilon(n^\epsilon x^\epsilon P^\epsilon), \end{aligned}$$

onde usamos no último passo que $Q_0 \leq x$, podemos finalmente chegar na estimativa que é o objetivo dessa seção:

Teorema 4.2 *Seja n um inteiro livre de quadrados, Q_0 um múltiplo de 8 e $\mathbb{P} = \{pQ_0, p$ primo, $P < p \leq 2P, p \nmid 2n\}$. Então*

$$\sum_{Q\in\mathbb{P}}|K_Q(x)| \ll_\epsilon [xP^{-\frac{1}{2}} + xn^{-\frac{1}{2}} + (x+n)^{\frac{5}{8}}(x^{\frac{1}{4}}P^{\frac{3}{8}} + n^{\frac{1}{8}}x^{\frac{1}{8}}P^{\frac{1}{4}})]n^\epsilon x^\epsilon P^\epsilon.$$

4.5 Demonstração do teorema 4.1

Voltemos ao contexto do início deste capítulo. Nosso objetivo é provar que a estimativa do teorema 4.1 vale para os coeficientes de Fourier em relação ao infinito das funções da base ortonormal $f_1, f_2, ..., f_R$ de $S_k(\Gamma_0(N))$, tal afirmação que sabemos ser equivalente a demonstrar o teorema 4.1. Para podermos usar o teorema 4.2, iremos supor inicialmente que N é múltiplo de 8, pois no caso $N \equiv 4 (\mathrm{mod}\ 8)$ basta aplicarmos o que iremos demonstrar para $2N$. Seja $a_j(n)$ o n-ésimo coeficiente de Fourier de f_j, denote por $\hat{P}_m(n,\Gamma)$ o n-ésimo coeficiente de Fourier da m-ésima série de Poincaré de um determinado subgrupo de congruência Γ , Considere p um primo e faça $Q = pN$. Se $f \in S_k(\Gamma_0(N))$ é normalizada pela norma induzida pelo produto interno de Petersson em relação a $S_k(\Gamma_0(N))$, então $[\Gamma_0(N) : \Gamma_0(Q)]^{-\frac{1}{2}}f(z)$ pertencerá a $S_k(\Gamma_0(Q))$ e terá norma 1 pela norma induzida pelo produto interno de Petersson em relação a $S_k(\Gamma_0(Q))$. Portanto, se denotarmos $f_i^* = [\Gamma_0(N) : \Gamma_0(Q)]^{\frac{1}{2}}f_i\ \forall i \in \{1, 2, .., R\}$

, obtemos que $f_1^*, f_2^*, ..., f_R^*$ formam um conjunto ortonormal de $S_k(\Gamma_0(Q))$. Tendo em vista que $S_k(\Gamma_0(Q))$ tem dimensão finita, e denotamos o valor dessa dimensão por R_Q, podemos completar esse conjunto ortonormal para formar uma base ortonormal $\{f_1^*, ..., f_R^*, ..., f_{R_Q}^*\}$ de $S_k(\Gamma_0(Q))$. Denotando por $a_i^*(n)$ o n-ésimo coeficiente de Fourier de f_i^*, concluímos que $a_i^*(n) = [\Gamma_0(N) : \Gamma_0(Q)]^{-\frac{1}{2}} a_i(n)$ sempre que $1 \leq i \leq R$. Portanto, por (4.8)

$$\begin{aligned}
\hat{P}_n(n, \Gamma_0(N)) &= \frac{\Gamma(k-1)}{(4\pi n)^{k-1}} \sum_{j=1}^{R} |a_j(n)|^2 \\
&= [\Gamma_0(N) : \Gamma_0(Q)] \frac{\Gamma(k-1)}{(4\pi n)^{k-1}} \sum_{j=1}^{R} |a_j^*(n)|^2 \\
&\leq [\Gamma_0(N) : \Gamma_0(Q)] \frac{\Gamma(k-1)}{(4\pi n)^{k-1}} \sum_{j=1}^{R_Q} |a_j^*(n)|^2 \\
&= [\Gamma_0(N) : \Gamma_0(Q)] \hat{P}_n(n, \Gamma_0(Q)).
\end{aligned}$$

Usando o fato de que $[\Gamma_0(N) : \Gamma_0(Q)] \leq p + 1$ (corolário 2.1), chegamos em

$$\frac{1}{p+1} \hat{P}_n(n, \Gamma_0(N)) \leq \hat{P}_n(n, \Gamma_0(Q)) = 1 + 2\pi i^{-k} \sum_{Q|c} c^{-1} K(n, n, c) J_{k-1}(\frac{4\pi}{c}).$$

Tomando $P > (4 \log 2n)^2$, denote por $\mathbb{P} = \{pN; p \text{ primo}, P < p \leq 2P, p \nmid c\}$. Por Chebyshev, $\#\mathbb{P} \asymp P/\log P$. Assim

$$\begin{aligned}
\frac{\hat{P}_n(n, \Gamma_0(N))}{\log P} &\ll \sum_{Q \in \mathbb{P}} \frac{\hat{P}_n(n, \Gamma_0(N))}{p+1} \\
&\leq \sum_{Q \in \mathbb{P}} \hat{P}_n(n, \Gamma_0(Q)) \\
&\ll \frac{P}{\log P} + \sum_{Q \in \mathbb{P}} \left| \sum_{Q|c} c^{-1} K(n, n; c) J_{k-1}(\frac{4\pi n}{c}) \right|.
\end{aligned}$$

Olhemos para o somatório que está dentro do módulo. Se $k = (2l+1)/2$, podemos tomar como vimos na seção 2.4 do capítulo 2, que

$$J_{k-1}(2\pi z) = (2/z)^{\frac{1}{2}} [e(z) H_1(2/z) + e(-z) H_{-1}(2/z)],$$

onde H_1, H_{-1} são polinômios de grau menor ou igual a l. Desmembremos essa soma em duas, para o caso $c \leq n$ e para o caso $c > n$, e usemos soma por partes. No caso $c \leq n$ temos

$$\sum_{\substack{Q|c \\ c \leq n}} c^{-1} K(n, n; c) J_{k-1}(\frac{4\pi n}{c}) = n^{-\frac{1}{2}} \sum_{\substack{Q|c \\ c \leq n}} c^{-\frac{1}{2}} K(n, n; c) \left[e\left(\frac{2n}{c}\right) H_1(c/n) + e\left(\frac{-2n}{c}\right) H_{-1}(c/n) \right]$$

$$= n^{-\frac{1}{2}} H_1(1) K_Q^{(1)}(n) + n^{-\frac{1}{2}} H_{-1}(1) K_Q^{(-1)}(n) - n^{-\frac{3}{2}} \int_1^n H_1'(\frac{x}{n}) K_Q^{(1)}(x) dx$$

$$-n^{-\frac{3}{2}} \int_1^n H_{-1}'(\frac{x}{n}) K_Q^{(-1)}(x) dx.$$

Já no caso $c > n$

$$\sum_{\substack{Q|c \\ c>n}} c^{-1} K(n,n;c) J_{k-1}(\frac{4\pi n}{c})$$

$$= -n^{-\frac{1}{2}} J_{k-1}(4\pi) K_Q^{(0)}(n) + \int_n^\infty \left(x^{-\frac{1}{2}} J_{k-1}(\frac{4\pi n}{x}) \right)' K_Q^{(0)}(x) dx.$$

Uma vez que H_v e H_v' são contínuas no intervalo compacto $[0,1]$, existe uma constante C tal que $H_v(1) \leq C$, $H_v'(\frac{x}{n}) \leq C$ quando $x \leq n$. Também é possível concluir que $\left(x^{-1/2} J_{k-1}(4\pi/x)\right)' \ll nx^{-\frac{5}{2}}$, quando $x > n$, usando a expansão em série de J_k apresentada em (2.3). Portanto

$$\left| \sum_{\substack{Q|c \\ c\leq n}} c^{-1} K(n,n;c) J_{k-1}(\frac{4\pi n}{c}) \right| \ll n^{-\frac{1}{2}} (|K_Q^{(1)}(n)| + |K_Q^{(-1)}(n)|) + n^{-\frac{3}{2}} \int_1^n (|K_Q^{(1)}(x)| + |K_Q^{(-1)}(x)|) dx$$

e

$$\left| \sum_{\substack{Q|c \\ c>n}} c^{-1} K(n,n;c) J_{k-1}(\frac{4\pi n}{c}) \right| \ll n^{-\frac{1}{2}} |K_Q^{(0)}(n)| + \int_n^\infty nx^{-\frac{5}{2}} |K_Q^{(0)}(x)| dx.$$

Portanto

$$\sum_{Q\in\mathbb{P}} \left| \sum_{Q|c} c^{-1} K(n,n;c) J_{k-1}(\frac{4\pi n}{c}) \right|$$

$$\begin{aligned}
&\ll n^{-\frac{1}{2}} \left(\sum_{Q\in\mathbb{P}} |K_Q^{(1)}(n)| + \sum_{Q\in\mathbb{P}} |K_Q^{(-1)}(n)| \right) + n^{-\frac{3}{2}} \int_1^n \left(\sum_{Q\in\mathbb{P}} |K_Q^{(1)}(x)| + \sum_{Q\in\mathbb{P}} |K_Q^{(-1)}(x)| \right) dx \\
&+ n^{-\frac{1}{2}} \sum_{Q\in\mathbb{P}} |K_Q^{(0)}(n)| + \int_n^\infty nx^{-\frac{5}{2}} \sum_{Q\in\mathbb{P}} |K_Q^{(0)}(x)| dx \\
&\leq n^{-\frac{1}{2}} \sum_{v=-1}^{1} \left(\sum_{Q\in\mathbb{P}} |K_Q^{(v)}(n)| \right) + n \int_1^\infty (x+n)^{-\frac{5}{2}} \sum_{v=-1}^{1} \left(\sum_{Q\in\mathbb{P}} |K_Q^{(v)}(n)| \right) dx,
\end{aligned}$$

onde, pelo teorema 4.2, temos

$$\sum_{Q\in\mathbb{P}} \left| \sum_{Q|c} c^{-1} K(n,n;c) J_{k-1}(\frac{4\pi n}{c}) \right|$$

$$\begin{aligned}
&\ll_\epsilon \quad n^{-\frac{1}{2}}(nP^{-\frac{1}{2}} + n^{\frac{1}{2}} + n^{\frac{5}{8}}[n^{\frac{1}{4}}P^{\frac{3}{8}} + n^{\frac{1}{4}}P^{\frac{1}{4}}])n^\epsilon P^\epsilon \\
&+ \quad n\tau(n)\int_1^\infty (x+n)^{-\frac{5}{2}}[xP^{-\frac{1}{2}} + xn^{-\frac{1}{2}} + (x+n)^{\frac{5}{8}}(x^{\frac{1}{4}}P^{\frac{3}{8}} + n^{\frac{1}{8}}x^{\frac{1}{8}}P^{\frac{1}{4}})]n^\epsilon x^\epsilon P^\epsilon dx \\
&\ll_\epsilon \quad (n^{\frac{1}{2}}P^{-\frac{1}{2}} + n^{\frac{3}{8}}P^{\frac{3}{8}})n^\epsilon P^\epsilon,
\end{aligned}$$

e assim, fazendo $P = n^{\frac{1}{7}}$

$$\frac{\Gamma(k-1)}{(4\pi n)^{k-1}}\sum_{j=1}^{R}|a_j(n)|^2 = \hat{P}_n(n, \Gamma_0(N))$$

$$\ll P + \sum_{Q\in\mathbb{P}}\left|\sum_{Q|c} c^{-1}K(n,n;c)J_{k-1}(\frac{4\pi n}{c})\right| \log P \ll_\epsilon n^{\frac{3}{7}+\epsilon},$$

de onde finalmente concluímos que

$$a_j(n) \ll_\epsilon n^{\frac{k}{2}-\frac{2}{7}+\epsilon}$$

para todo $j \in \{1, ..., R\}$, o que mostra o teorema 4.1 quando $8|N$.

5 UMA APLICAÇÃO DA ESTIMATIVA DE IWANIEC AO PROBLEMA DE LINNIK NA ESFERA

Será usada nesse capítulo a notação $\Omega(n) = \{\frac{(x,y,z)}{\sqrt{n}}; x^2+y^2+z^2 = n)\}$ e $r_3(n) = \#\Omega(n)$. De acordo com a definição 2.1, demonstrar que a sequência de conjuntos $\{\Omega(n_i)\}_{i=1}^{\infty}$ ($\{n_i\}$ a sequência crescente de inteiros positivos livre de quadrados incongruentes a 7 módulo 8) tornam-se equidistribuídos na medida de Lebesgue normalizada μ em $\mathbb{S}^2$ significa mostrar que

$$\lim_{i\to\infty} \frac{1}{r_3(n_i)} \sum_{x\in\Omega_{n_i}} f(x) = \int_{\mathbb{S}^2} f(x)d\mu$$

para toda função real contínua f de $\mathbb{S}^2$. A teoria de formas modulares será aplicada nesse contexto usando o fato da função

$$\theta_P(z) = \sum_{m\in\mathbb{Z}^r} P(m)e(|m|^2 z) = \sum_{t=0}^{+\infty} \left(\sum_{|m|^2=t} P(m) \right) e(tz)$$

ser uma forma modular de peso meio inteiro quando seu grau é par, de modo a obter uma estimativa para seus n-ésimos coeficientes de Fourier, n livre de quadrados, simultaneamente ao fato de que é possível relacionar esses coeficientes com somas de Weyl do tipo $\frac{1}{r_3(n)}\sum_{x\in\Omega(n)} P(x)$, P polinômio harmônico esférico. Usaremos essa estratégia para provar o

Teorema 5.1 *A sequência de conjuntos $\Omega(n)$, $n \not\equiv 7 (\mathrm{mod}\ 8)$ e livre de quadrados, tornam-se equidistribuídos em $\mathbb{S}^2$.*

Prova: Considere um polinômio harmônico esférico P de grau positivo em $\mathbb{S}^2$. Se o grau de P for ímpar, o fato de P ser homogêneo implica que $P(-x) = -P(x) \forall x \in \mathbb{S}^2$. O conjunto $\Omega(n)$ é claramente simétrico (i.e. $x \in \Omega(n) \Longrightarrow -x \in \Omega(n)$), logo

$$\frac{1}{r_3(n)} \sum_{x\in\Omega(n)} P(x) = 0 \tag{5.37}$$

para todo n livre de quadrados e P polinômio harmônico esférico de grau ímpar.

Agora suponha que o grau de P, v, seja par. Pela proposição 3.5

$$\theta_P(x) = \sum_{m\in\mathbb{Z}^3} P(m)e(|m|^2 z) = \sum_{n=1}^{\infty} a_n e(nz),$$

com $a_n = \sum_{|m|^2=n} P(m)$, é uma forma cuspidal de peso $\frac{3}{2}+v$ em $\Gamma_0(4)$. Supondo n livre de quadrados e incongruente a 7 módulo 8, o teorema 4.2 nos dá que

$$|a_n| \ll_\epsilon n^{\frac{3}{4}+\frac{v}{2}-\frac{2}{7}+\epsilon}. \tag{5.38}$$

O fato de P ser homogêneo de grau v implica

$$P(m/|m|) = |m|^{-v}P(m),$$

assim

$$a_n = n^{\frac{v}{2}} \sum_{|m|^2=n} P(m/|m|),$$

de onde concluímos, por (5.38), que

$$\sum_{|m|^2=n} P(m/|m|) \ll_\epsilon n^{13/28+\epsilon}. \tag{5.39}$$

Por outro lado, o teorema de Gauss que citamos na seção 2.7 nos diz que, caso $n > 3$

$$r_3(n) = 12h_n \left(1 - \left(\frac{d}{2}\right)\right), \tag{5.40}$$

onde h_n é o número de classe de $\mathbb{Q}(\sqrt{-n})$ e d é o discriminante de $\mathbb{Q}(\sqrt{-n})$. Como n é livre de quadrados e incongruente a 7 módulo 8, portanto não é da forma $4^a(8b+7)$, temos $r_3(n) > 0$ e logo $\left(\frac{d}{2}\right) = -1$. O resultado de Siegel enunciado na seção 2.7 nos diz que $h_n \gg_\epsilon |d|^{\frac{1}{2}-\epsilon}$. Combinando esses resultados com (5.40)

$$r_3(n) = 24h_n \gg_\epsilon |d|^{\frac{1}{2}-\epsilon} \asymp n^{\frac{1}{2}-\epsilon}$$

$$\implies \frac{1}{r_3(n)} \ll_\epsilon n^{-\frac{1}{2}+\epsilon}.$$

Segue por (5.39) que para todo polinômio harmônico esférico de grau par positivo e n livre de quadrados

$$\frac{1}{r_3(n)} \sum_{|m|^2=n} P(m/|m|) = \frac{1}{r_3(n)} \sum_{x\in\Omega(n)} P(x) \ll_\epsilon n^{-\frac{1}{28}+\epsilon}, \tag{5.41}$$

o que mostra, junto com (5.37), o critério de Weyl para a sequência de conjuntos $\{\Omega(n_i)\}_i^\infty$, onde $\{n_i\}_{i=1}^\infty$ denota a sequência crescente dos inteiros positivos livres de quadrados. □

6 CONCLUSÃO

Nesta dissertação apresentamos a noção de forma modular de peso meio inteiro, e depois apresentamos uma estimativa para os coeficientes de Fourier dessas formas modulares com o intuito de aplicá-la na demonstração do problema de Linnik na esfera para o caso em que n é livre de quadrados. Como vimos inicialmente, pode-se mostrar que esse resultado vale para $n \equiv 1, 2, 3, 5, 6 (\mathrm{mod}\ 8)$. A demonstração dessa versão geral pode ser visto em (10), onde Golubeva e Formenko usam a *correspondência de Shimura*, uma correspondência que relaciona formas modulares de meio inteiro $k + \frac{1}{2}$ e formas modulares de peso inteiro $2k$ (veja (26)), para obter uma estimativa geral para os coeficientes de Fourier de formas modulares de peso meio inteiro. Por exemplo, usando essa correspondência, o teorema de Deligne e a estimativa de Iwaniec, é possível mostrar que, se $f \in S_k(N)$ satisfaz $\langle f, f \rangle = 1$, o tn^2-ésimo coeficiente de Fourier a_{tn^2}, t livre de quadrados e $(n, N) = 1$, de f satisfaz, por exemplo

$$a_{tn^2} \ll_\epsilon (tn^2)^{\frac{k}{2} - \frac{1}{4} - \frac{1}{96} + \epsilon},$$

como é citado em (10, p.3042).

REFERÊNCIAS

1 ARENSTORF, R. F.; JOHNSON, D. Uniform distribution of integral points on 3-dimensional spheres via modular forms. **Journal of Number Theory,** [Belgium], v. 11, p. 218-238, 1979.

2 BATEMAN, H. **Higher transcendental functions II**. New York: McGraw-Hill, 1953.

3 BONAHON, F. **Low-dimensional geometry**: from Euclidean surfaces to hyperbolic knots. Providence, R. I.: American Mathematical Society; Princeton, N. J.: Institute for Advanced Study, 2009.

4 DAVENPORT, H. **Multiplicative number theory**. 2nd. ed. New York: Springer-Verlag, 1980.

5 DELIGNE, P. La conjecture de Weil I. **Publ. Math. Inst. Hautes Etud. Sci.,** [Germany], v. 43, p. 273-307, 1974.

6 DUKE,W. **An introduction to the Linnik problems**. Califórnia, 2006. Pré-publicação.

7 DUKE, W. Hyperbolic distribution problems and half-integral weight Maass forms. **Invent Math**, [Germany], v. 92, p. 73–90, 1988.

8 FLEIG, P. et al. **Eisenstein series and automorphic representations: With applications in string theory**. Cambridge Studies in Advanced, 2018.

9 GAUSS, C. F. **Disquisitiones Arithmeticae**. New York: Springer-Verlag, 1986.

10 GOLUBEVA, E.; FOMENKO, O. Asymptotic distribution of integral points on the three-dimensional sphere. **J Math Sci,** [Netherlands], v. 52, p. 3036–3048, 1990.

11 GROEMER, H. **Geometric applications of Fourier series and spherical harmonics.** Cambridge: Cambridge University Press, 1996.

12 HILDEBRAND, Adolf J. **Introduction to analytic number theory math 531.** Fall 2005. Notas de curso proferido na Universidade de Illinois. Disponível em: http://www.math.uiuc.edu/~hildebr/ant. Acesso em: 15 de maio 2021.

13 HOOLEY, C. An asymptotic formula in the theory of numbers. **Proc. London Math. Soc**., London, v. 7, n. 27, p. 396–413, 1957.

14 IWANIEC, H.; KOWALSKI, E. **Analitic number theory**. Providence, RI: American Mathematical Society, 2004. (Mathematical Society Colloquium Publications, v. 53).

15 IWANIEC, H. Fourier coefficients of modular forms of half integral weight. **Inv. Mat.**, [Germany], v. 87, n. 2, p. 385-401, 1987.

16 IWANIEC, H. **Topics in classical automorphic forms**. Providence, R. I.: American Mathematical Society, 1997. (Graduate Studies in Mathematics,v. 17).

17 KOBLITZ, N. **Introduction to elliptic curves and modular forms**. New York: Springer-Verlag, 1984. (Graduate Texts in Mathematics, v. 97).

18 KOWALSKI, E. **Exponential sums over finite fields, I**: elementary methods. Zurich, 2010. Disponível em: www.math.ethz.ch/kowalski/exp-sums.pdf. Acesso em: 12 abr. 2021.

19 KUBOTA, T. **Elementary theory of Eisenstein series**. Tokyo: Kodansha; New York: Wiley, 1973.

20 KUIPERS, L.; NEIDERREITE, H. **Uniform distribution of sequences**. New York: John Wiley & Sons, 1974.

21 LINNIK,Y. V. **Ergodic properties of algebraic fields**. New York: Springer-Verlag, 1968.

22 MARTINEZ, F. B.; MOREIRA, C. G.; SALDANHA, N.; TENGAN, E. **Teoria dos números**: um passeio com primos e outros números familiares pelo mundo inteiro. 4. ed. Rio de Janeiro: IMPA, 2010.

23 MIYAKE, T. **Modular forms**. New York: Springer-Verlag, 1989.

24 NEUKIRCH, J. **Algebraic number theory**. Berlim: Springer-Verlag, 1999. (Grundlehren der mathematischen Wissenschaften, v. 322).

25 SARNAK, P. **Some applications of modular forms**. Cambridge: Cambridge Univ. Press, 1990.

26 SHIMURA, G. On modular forms of half integral weight. **Ann. Math,** Princeton, v. 97, n. 3, p. 440-481, May 1973.

27 STEIN, E.; SHAKARCHI, R. **Fourier analysis**: an introduction. Princeton: Princeton University Press, 2011.