Universidade Federal do Rio Grande do Sul

Instituto de Matemática

Programa de Pós-Graduação em Matemática

A fórmula de Hardy-Ramanujan-Rademacher das partições de um inteiro positivo

Eduardo Casagrande Stabel

Dissertação de Mestrado

Porto Alegre, 7 de Março de 2007.

Dissertação submetida por Eduardo Casagrande Stabel[1] como requisito parcial para a obtenção do grau de Mestre em Matemática pelo Programa de Pós-Graduação em Matemática do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.

Professor Orientador:

Dr. Artur Oscar Lopes (UFRGS)

Banca Examinadora:

Dr. Alexandre Tavares Baraviera (UFRGS)

Dr. Amílcar Pacheco (UFRJ)

Dr. Eduardo Henrique de Mattos Brietzke (UFRGS)

Data da Apresentação: 7 de Março de 2007.

[1]Bolsista do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq

Sumário

Agradecimentos

Agradeço aos professores (da banca) Alexandre Baraviera, Eduardo Brietzke e Amílcar Pacheco pelas correções em pontos da dissertação e/ou pela ajuda na compreensão das demonstrações. Agradeço também ao professor Luiz Fernando Rocha por haver estudado o assunto em meu auxílio.

Também agradeço ao professor Artur Lopes pela paciência, orientação e sincera preocupação comigo ao longo de toda a graduação e o mestrado. Muito obrigado!

Em especial, agradeço a minha mãe, que me apoiou de todas as formas que estavam ao seu alcance nos meus inúmeros (!) interesses durante a vida (quais mais virão?). Em particular, na minha participação nas olimpíadas de matemática (tarefa que se mostrou difícil) e na minha escolha da matemática como carreira. Você é muito especial para mim e desejo toda a felicidade para sua vida!

Finalmente, e não menos importante, agradeço a todos (amigos e mestres) aqueles que me inspiraram de alguma forma a ser uma pessoa melhor e, conseqüentemente, me ajudaram a ver a matemática como um meio pelo qual o bem pode ser realizado...

Resumo

Neste trabalho será obtida a série de Rademacher que determina o valor para a função partição irrestrita p(n). Será usado o método do círculo com o caminho de integração descrito através dos círculos de Ford; e será demonstrada a equação funcional de Dedekind — peça chave na demonstração — para a função eta de Dedekind $\eta(\tau)$.

Abstract

In this work, we prove the Rademacher's series for the unrestricted partition function. We will use the circle method described through the Ford circles; and the Dedekind's functional equation for the Dedekind eta function $\eta(\tau)$ — a key element in the proof — is also obtained.

Capítulo 1

Introdução

Em matemática, quando se subdivide algo em partes menores, é costume se utilizar o termo *partição*. No contexto que será trabalhado aqui, uma partição é uma expressão de um inteiro positivo n como soma de inteiros positivos quaisquer, sendo irrelevante a ordem em que as parcelas são somadas. Estaremos interessados em determinar a quantidade de partições que possui um dado n. Mais formalmente:

Definição 1.1. *Dado $n > 0$ um inteiro, denota-se por $\mathsf{p}(n)$ à quantidade de seqüências finitas ordenadas de inteiros positivos $(a_1, \ldots, a_k)$ que satisfazem às propriedades $a_1 \geq \ldots \geq a_k$ e $n = \sum_{i=1}^{k} a_i$. Por convenção, define-se $\mathsf{p}(0) = 1$.*

Exemplo 1.1. *O número inteiro 4 possui as seguintes partições*

$$\begin{aligned} 4 &= 4 \\ &= 3+1 \\ &= 2+2 \\ &= 2+1+1 \\ &= 1+1+1+1, \end{aligned}$$

portanto $\mathsf{p}(4) = 5$. Alguns outros valores da função partição são $\mathsf{p}(10) = 42$ e $\mathsf{p}(100) = 190569292$.

Costuma-se denominar também de função partição irrestrita à função $\mathsf{p}(n)$ que acabamos de definir, pelo fato de não termos exigido qualquer tipo de restrição nas parcelas das somas. A função partição cresce muito rapidamente. Uma expressão assintótica para ela é a seguinte:

$$\mathsf{p}(n) \sim \frac{1}{4n\sqrt{3}}\, e^{\pi\sqrt{2n/3}}.$$

Lembramos que isto significa que o quociente (a divisão) entre as duas funções tende a 1 quando n tende ao infinito; neste caso, elas são ditas assintoticamente equivalentes.

Neste trabalho, demonstraremos uma expressão exata para $\mathsf{p}(n)$. Ela foi demonstrada pelo matemático Rademacher, no ano de 1937, quando preparava notas de aula sobre o trabalho conjunto dos matemáticos Hardy e Ramanujan, realizado cerca de duas décadas antes. A expressão (bastante complicada) envolve o número π, raízes quadradas, raízes complexas da unidade, derivadas de funções hiperbólicas e uma série.

1.1 Requisitos mínitos e as fontes do trabalho

Na parte final deste capítulo será exibido um roteiro de toda a dissertação. Como veremos, para o cálculo de $\mathsf{p}(n)$, teremos de calcular a integral de uma função de variável complexa. O caminho de integração é descrito no Capítulo 2, e envolve conhecimentos de matemática elementar. Utilizaremos a equação funcional de Dedekind, demonstrada no Capítulo 3, para podermos calcular a integral que mencionamos. São utilizados conhecimentos de variável complexa: um conhecimento sobre os zeros e pólos das funções trigonométricas; a convergência do produtório infinito de funções analíticas; a teoria dos resíduos de Cauchy. Uma referência da bibliografia é [5]. Também será utilizado o teorema da convergência limitada de Arzelà (conferir [6, página 405]). Neste capítulo, também se estuda o grupo modular. Finalmente, no Capítulo 4, demonstra-se o resultado.

A fonte principal de pesquisa para a dissertação é [7]. Mais sobre a história deste resultado está na referência [3, capítulo 5]. Mais sobre o grupo modular pode ser estudado em [4].

1.2 Um roteiro da demonstração

A ferramenta mais fundamental no estudo das partições tem demonstrado ser a função geradora. No caso da função partição $\mathsf{p}(n)$, a *função geradora* é a seguinte série formal: $F(x) = \sum_{n=0}^{\infty} \mathsf{p}(n)x^n$. Felizmente F é mais do que uma série formal em x.

Teorema 1.1 (Euler)**.** *O somatório que define $F(x)$ converge se $|x| < 1$ e além disso vale a igualdade*

$$F(x) = \prod_{m=1}^{\infty} \frac{1}{(1-x^m)}.$$

Em particular, a função $F(x)$ é analítica em $|x| < 1$.

Antes da demonstração, uma observação. Um resultado tradicional de variável complexa (ver referência [5], página 163) diz o seguinte

Lema 1.1. *Seja G uma região de $\mathbb{C}$ e $\{f_n\}$ uma seqüência de funções analíticas em G, nenhuma delas identicamente nula. Se $\sum_{n=1}^{\infty}[f_n(z)-1]$ converge absoluta e uniformemente nos subconjuntos compactos de G então $\prod_{n=1}^{\infty} f_n(z)$ converge para uma função analítica $f(z)$. Mais ainda, se a é um zero de f então a é zero de somente um número finito das f_n e a multiplicidade de a, como zero de f, é igual a soma das multiplicidades de a, como zero dessas f_n das quais a é zero.*

Este resultado garante que o produtório $\prod_{n=1}^{\infty}(1-x^n)$ converge para uma função analítica definida no disco unitário $|x| < 1$, pois o somatório $\sum_{n=1}^{\infty} x^n$ — a série geométrica — converge absoluta e uniformemente nas partes compactas do domínio $|x| < 1$. Mais ainda, como nenhuma das funções $(1-x^n)$ tem um zero em $|x| < 1$, o produtório $\prod_{n=1}^{\infty}(1-x^n)$ é não-nulo para todo x que satisfaz $|x| < 1$. Portanto $\prod_{m=1}^{\infty} \frac{1}{(1-x^m)}$ é também analítica em $|x| < 1$, sem raízes. Agora vamos à demonstração do Teorema 1.1:

Demonstração: Consideremos, sem perda de generalidade, que $0 < x < 1$ e que x está fixado a partir deste ponto. Truncamos a expressão do produtório em $m = k$, daí a expressão $\prod_{m=1}^{k} \frac{1}{(1-x^m)}$ pode ser pensada como

$$\begin{aligned}
\prod_{m=1}^{k} \frac{1}{(1-x^m)} = \prod_{m=1}^{k}\left(\sum_{n=0}^{\infty} x^{nm}\right) &= \prod_{m=1}^{k}\left(1 + x^m + x^{2m} + x^{3m} + \ldots\right) \\
&= \left(1 + x^1 + x^2 + x^3 + \ldots\right) \\
&\times \left(1 + x^2 + x^4 + x^6 + \ldots\right) \\
&\times \ \ldots \times \\
&\times \left(1 + x^k + x^{2k} + x^{3k} + \ldots\right).
\end{aligned}$$

Como cada série $\sum_{n=0}^{\infty} x^{nm}$ converge absolutamente, podemos efetuar o produto termo a termo do produtório acima e somar em qualquer ordem. O resultado pode ser expresso como uma série de potências em x, $\sum_{i=0}^{\infty} c_i x^i$.

Vamos identificar quem são os coeficientes c_i. Eles estão ligados às partições. Tem-se $c_0 = 1 = \mathsf{p}(0)$. Afirmo que $\mathsf{p}(1) = c_1, \mathsf{p}(2) = c_2, \ldots, \mathsf{p}(k) = c_k$ e que $c_i \leq \mathsf{p}(i)$ se $i > k$. De fato, pois o produtório resultará num somatório de todos os termos do tipo $x^{i_1 1 + i_2 2 + \ldots + i_k k}$, onde cada i_m é livremente um número inteiro ≥ 0. Portanto o coeficiente de x^i — que é c_i — será igual à quantidade de maneiras de se escrever i como soma dos números $1, 2, \ldots, k$ – possivelmente com repetições. Logo $c_i \leq \mathsf{p}(i)$, valendo a igualdade para $i \leq k$, pois todas as partições de $1, 2, \ldots, k$ só envolvem termos $\leq k$.

Por um lado, já que $c_i = \mathsf{p}(i)$ se $i \leq k$, temos

$$\sum_{n=0}^{k} \mathsf{p}(n)x^n = \sum_{n=0}^{k} c_n x^n < \sum_{n=0}^{\infty} c_n x^n = \prod_{m=1}^{k} \frac{1}{(1-x^m)} \leq \prod_{m=1}^{\infty} \frac{1}{(1-x^m)} < \infty.$$

Como $\prod_{m=1}^{\infty} \frac{1}{(1-x^m)}$ é finito (conseqüência da observação feita antes de começar a demonstração) e independente de k, a seqüência $\{\sum_{n=0}^{k} \mathsf{p}(n)x^n\}_k$ é limitada. Ela também é crescente pois $\mathsf{p}(n)x^n > 0$. Logo, deve convergir. Isto implica que

$$\sum_{n=0}^{\infty} \mathsf{p}(n)x^n \leq \prod_{m=1}^{\infty} \frac{1}{(1-x^m)}.$$

Por outro lado, pelo fato de que $c_i \leq \mathsf{p}(i)$,

$$\sum_{n=0}^{\infty} \mathsf{p}(n)x^n \geq \sum_{n=0}^{\infty} c_n x^n = \prod_{m=1}^{k} \frac{1}{(1-x^m)},$$

podemos tomar o limite em k, obtendo

$$\sum_{n=0}^{\infty} \mathsf{p}(n)x^n \geq \prod_{m=1}^{\infty} \frac{1}{(1-x^m)}.$$

O que implica que para $0 < x < 1$ vale a igualdade $\sum_{n=0}^{\infty} \mathsf{p}(n)x^n = \prod_{m=1}^{\infty} \frac{1}{(1-x^m)}$. Como a série de potências $F(x) = \sum_{n=0}^{\infty} \mathsf{p}(n)x^n$ é convergente para $0 < x < 1$, seu raio de convergência é pelo menos 1, logo ela é convergente para qualquer complexo x que satisfaz $|x| < 1$. Portanto $F(x)$ é analítica em $|x| < 1$. Pela observação anterior à demonstração, $\prod_{m=1}^{\infty} \frac{1}{(1-x^m)}$ também é analítica em $|x| < 1$. Como essas duas funções analíticas coincidem no segmento real $(0, 1)$ – que possui pontos de acumulação – elas devem coincidir em todo o domínio $|x| < 1$, o que conclui a demonstração. □

A fórmula de Euler fornece uma expressão, de certa forma, mais simples da função $F(x)$ do que a expressão original que envolvia os $\mathsf{p}(n)$. A teoria dos resíduos de Cauchy permite calcular os coeficientes da expansão analítica de $F(x)$ — o coeficiente de x^n é precisamente quem queremos calcular, $\mathsf{p}(n)$. Esta será a abordagem. Escrevemos

$$\frac{F(x)}{x^{n+1}} = \sum_{k=0}^{\infty} \frac{\mathsf{p}(k)x^k}{x^{n+1}}$$

para $0 < |x| < 1$. Esta última série é a expansão de Laurent de $F(x)/x^{n+1}$ no disco perfurado $0 < |x| < 1$. Esta função possui um pólo de ordem $n+1$ em $x = 0$ cujo resíduo (coeficiente de x^{-1}) é $\mathsf{p}(n)$, portanto pelo teorema dos resíduos de Cauchy, para qualquer curva bem comportada C em $0 < |x| < 1$ que dá uma volta em torno da origem e é orientada positivamente

$$\mathsf{p}(n) = \frac{1}{2\pi i} \int_C \frac{F(x)}{x^{n+1}} dx.$$

É preciso encontrar uma curva adequada C que nos possibilite calcular efetivamente essa integral. O método do círculo consiste em escolher uma curva próxima aos pontos tais que $x = 1$, $x^2 = 1$, $x^3 = 1$, ..., que anulam os denominadores do produtório de $F(x)$, dado pela expressão de Euler. O método do círculo escolhe uma (na verdade, uma para cada N inteiro positivo) curva $C = C_N$ de "raio" aproximadamente 1 que é dividida em curvas $\gamma(h, k)$ perto da raiz da unidade $e^{2\pi i h/k}$, onde (h/k) percorre todas as frações irredutíveis de denominador $\leq N$ do intervalo $[0,1]$ — essas são as chamadas frações de Farey de ordem N. A integral ao longo de $C = C_N$ pode ser escrita como uma soma de integrais ao longo desses arcos

$$\int_C \frac{F(x)}{x^{n+1}}dx = \sum_{(h,k)=1, 0<k\leq N} \int_{\gamma(h,k)} \frac{F(x)}{x^{n+1}}dx.$$

Em cada arco $\gamma(h,k)$, a função $F(x)$ no integrando é substituída por uma função elementar $\Psi_{(h,k)}(x)$, que tem essencialmente o mesmo comportamento de $F(x)$ perto de $e^{2\pi i h/k}$. Esta função elementar $\Psi_{(h,k)}$ surge naturalmente da equação funcional satisfeita pela função eta de Dedekind $\eta(\tau)$. As funções F e η estão relacionadas pela equação

$$F(e^{2\pi i\tau}) = e^{\pi i\tau/12}/\eta(\tau),$$

e a equação funcional para η dá uma fórmula que descreve o comportamento de F perto de cada raiz da unidade $e^{2\pi i h/k}$. A substituição de F por $\Psi_{(h,k)}$ tem um erro, que precisa ser estimado. Finalmente, as integrais de $\Psi_{(h,k)}$ ao longo de $\gamma(h,k)$ são calculadas, e suas somas ao longo dos h's são termos $R_k(n)$ da série de Rademacher, que dá a expressão para a partição

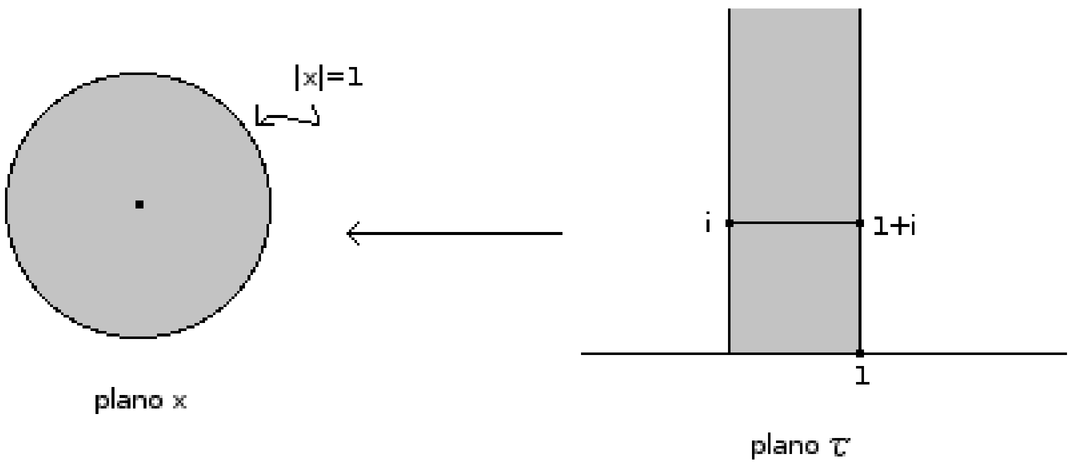
$$\mathsf{p}(n) = \sum_{k=1}^{\infty} R_k(n).$$

Em 1943 (6 anos depois de Rademacher ter obtido este resultado pela primeira vez), ele próprio modificou o método do círculo, substituindo o caminho C por um outro caminho do plano τ, através da mudança de variáveis $x = e^{2\pi i\tau}$. Este novo caminho usa os círculos de Ford e uma importante propriedade que os relaciona às frações de Farey — algo que só foi estudado em 1938, um ano após o primeiro resultado de Rademacher. Este caminho de integração é o que será utilizado aqui.

Capítulo 2

O caminho de integração

O caminho de integração C utilizado para o cálculo de $\int_C \frac{F(x)}{x^{n+1}}dx$ não será descrito diretamente em $|x| < 1$. Ele será descrito no semi-plano superior $H = \{\tau \in \mathbb{C} : \Im(\tau) > 0\}$. A mudança de variáveis $\tau \mapsto x = e^{2\pi i\tau}$ aplica uma faixa de largura 1 do semi-plano superior H no disco perfurado $0 < |x| < 1$, como mostra a figura abaixo.



A construção do caminho é muito interessante. O caminho ligará os pontos i e $i+1$ do plano τ e todo seu interior pertencerá ao quadrado de vértices 0, 1, $i+1$ e i. Na verdade, para cada N inteiro positivo construiremos um caminho $C = C_N$. Serão desenhados vários círculos que se tangenciam desde i até $i+1$, dentro deste quadrado. Os arcos superiores desses círculos serão escolhidos e este será o caminho — passando de um arco para outro através dos pontos de tangência. Cada círculo — usado para construir C_N — está ligado a uma fração irredutível do intervalo unitário $[0,1]$ — uma das frações de Farey de ordem N.

Nosso estudo, neste capítulo, será primeiro das frações de Farey, depois dos círculos de Ford e por fim a apresentação do caminho de integração.

2.1 Frações de Farey

Definição 2.1. *O conjunto das frações de Farey de ordem n, denotado por F_n, é a seqüência finita ordenada de todas as frações irredutíveis do intervalo fechado $[0,1]$, cujos denominadores são $\leq n$, listadas em ordem crescente.*

Exemplo 2.1. *Vejamos alguns exemplos ilustrativos.*
F_1: $(\frac{0}{1}, \frac{1}{1})$ F_2: $(\frac{0}{1}, \frac{1}{2}, \frac{1}{1})$ F_3: $(\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1})$ F_4: $(\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1})$

Os conjuntos F_n crescem com n, isto é, $F_n \subset F_{n+1}$. Há mais duas propriedades sobre as frações de Farey que serão necessárias. Dois lemas serão provados inicialmente como auxílio para a prova do teorema central deste seção. Antes uma definição:

Definição 2.2. *Dadas duas frações racionais irredutíveis $a/b < c/d$, com $b > 0$ e $d > 0$, a fração mediante das duas é definida como $(a + c)/(b + d)$.*

Lema 2.1. *Sejam $a/b < c/d$ duas frações irredutíveis. A fração mediante das duas está entre elas, isto é,*

$$\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}.$$

Demonstração: Das desigualdades

$$\frac{a+c}{b+d} - \frac{a}{b} = \frac{bc-ad}{b(b+d)} > 0 \quad \text{e} \quad \frac{c}{d} - \frac{a+c}{b+d} = \frac{bc-ad}{d(b+d)} > 0$$

conclui-se o enunciado. □

Lema 2.2. *Sejam $0 \leq a/b < c/d \leq 1$ duas frações que satisfazem a relação $bc - ad = 1$ — esta é chamada de relação unimodal. Então:*

- *As frações a/b e c/d são consecutivas em F_n se e somente se*

$$\max(b, d) \leq n \leq b + d - 1.$$

- *Se h/k é a fração mediante das duas então valem novamente as relações unimodais*

$$bh - ak = 1 \quad \text{e} \quad ck - dh = 1.$$

Demonstração: A relação $bc - ad = 1$ implica que as frações a/b e c/d são irredutíveis. A desigualdade $\max(b, d) \leq n$ é equivalente a $b \leq n$ e $d \leq n$ ou ainda que a/b e c/d pertencem a F_n.

Suponhamos que $n \leq b + d - 1$ e, por hipótese de absurdo, que elas não são consecutivas em F_n. Então existe uma fração h/k entre as duas, isto é, $a/b < h/k < c/d$. Os fatos de que $a/b < h/k$ e $h/k < c/d$ implicam que $ck - dh \geq 1$ e $bh - ak \geq 1$. A identidade

$$k = (bc - ad)k = b(ck - dh) + d(bh - ak)$$

implica que $k = b(ck - dh) + d(bh - ak) \geq b + d$, uma contradição, pois h/k não pode pertencer a F_n já que $n \leq b + d - 1 < b + d$. O que demonstra que de fato a/b e c/d são consecutivas em F_n com as hipóteses do enunciado.

Se as frações a/b e c/d são consecutivas em F_n então $n \leq b + d - 1$, pois a fração mediante $(a + c)/(b + d)$ está entre as duas em F_{b+d}.

Agora, o segundo item. Seja $h/k = (a + c)/(b + d)$ a fração mediante das frações $a/b < c/d$ e suponha que valha a relação unimodal $bc - ad = 1$. Como $a/b < h/k < c/d$, conclui-se que $ck - dh \geq 1$ e $bh - ak \geq 1$. Finalmente, a relação $b + d = k = b(ck - dh) + d(bh - ak)$ implica que $ck - dh = 1$ e $bh - ak = 1$.

□

Agora o resultado central sobre as frações de Farey que será utilizado:

Teorema 2.1. *Para todo n, vale a inclusão $F_n \subset F_{n+1}$. Sempre que $a/b < c/d$ sejam frações consecutivas em F_n, vale a relação unimodal $bc - ad = 1$. Mais ainda, se $a/b < c/d$ são frações consecutivas em F_n e separadas em F_{n+1}, então a fração mediante $(a + c)/(b + d)$ está entre elas, e nenhuma outra fração separa a/b e c/d, em F_{n+1}.*

Demonstração: Será utilizada indução em n. Quando $n = 1$, as frações $0/1$ e $1/1$ são consecutivas e satisfazem a relação unimodal. Na passagem de F_1 para F_2, insere-se a fração mediante das duas anteriores, $1/2 = (0+1)/(1+1)$, e nenhuma outra fração separa $0/1$ de $1/1$, em F_2. As relações unimodais ainda valem em F_2, pois $1 \times 1 - 0 \times 1 = 1$ e $2 \times 1 - 1 \times 1 = 1$. Agora o passo de indução. Suponhamos o teorema válido para n e vamos mostrar que ele é válido para $n+1$.

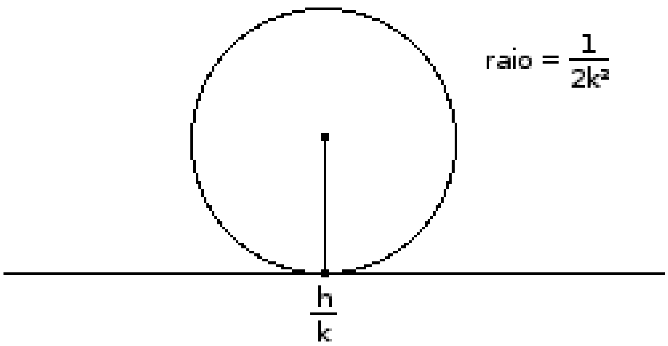
Sejam a/b e c/d frações consecutivas em F_n, e que satisfazem a relação unimodal $bc - ad = 1$, pela hipótese de indução. Seja h/k a mediante das duas, ou seja, $h = a + c$ e $k = b + d$. Pelo Lema 2.2, sabe-se que vale a relação unimodal $ck - dh = 1$, logo h e k são primos entre si. Se as frações a/b e c/d não são consecutivas em F_{n+1}, então $(n+1) > b + d - 1$, pelo Lema 2.2. Como a/b e c/d não são consecutivas em F_{b+d} (pois $h/k = (a+c)/(b+d)$ está entre elas), conclui-se que $(n+1) \leq (b+d)$. Logo $(n+1) = (b+d) = k$. Os dois pares de frações $a/b < h/k$ e $h/k < c/d$ são consecutivos em F_{n+1}, segundo o Lema 2.2, pois $k = \max(b,k)$ e $k = \max(d,k)$. As relações unimodais $ck - dh = 1$ e $bh - ak = 1$ são satisfeitas, também pelo Lema. Isto mostra que na passagem de F_n para F_{n+1}, cada nova fração que surge tem de ser a mediante de duas frações que eram consecutivas em F_n, e que os novos pares satisfazem as relações unimodais. O que finaliza o passo de indução.

□

2.2 Círculos de Ford

O matemático L. R. Ford foi quem primeiro estudou as propriedades dos chamados círculos de Ford, em 1938, por isso receberam seu nome.

Definição 2.3. *Dado um número racional irredutível h/k, o círculo de Ford correspondente a esta fração é denotado por $C(h,k)$: é o círculo do plano complexo de raio $1/(2k^2)$ cujo centro está no ponto $(h/k) + i/(2k^2)$.*

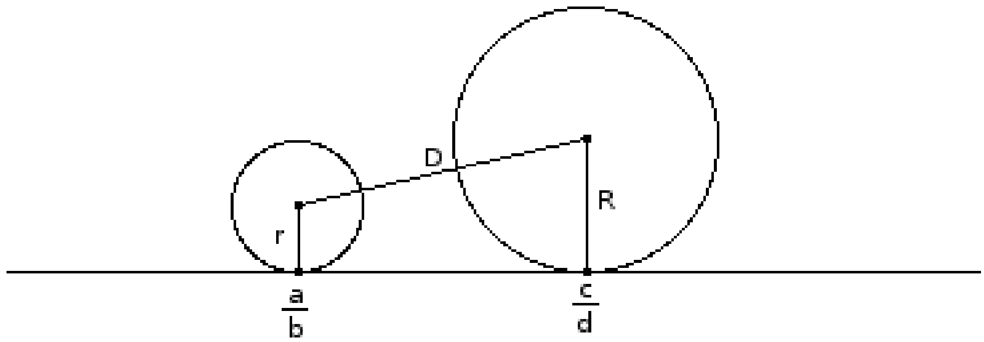


Um círculo de Ford qualquer $C(h,k)$ localiza-se no fecho do semi-plano superior H e tangencia o eixo real no ponto h/k, pois a medida de seu raio é igual à medida de sua parte imaginária. Considere F_n o conjunto das frações de Farey de ordem n. Se dispusermos os círculos de Ford correpondentes a cada uma das frações de F_n, os círculos de Ford correspondentes à frações de Farey consecutivas corresponderão à círculos tangentes e exteriores um ao outro. Esse é o conteúdo do primeiro teorema desta seção.

Teorema 2.2. *Dois círculos de Ford $C(a,b)$ e $C(c,d)$ ou se tangenciam ou não se intersectam. Eles se tangenciam se, e somente se, $bc - ad = \pm 1$. Em particular, frações de Farey de mesma ordem consecutivas correspondem a círculos de Ford tangentes.*

Demonstração: Vamos supor, sem perda de generalidade, que $a/b < c/d$. Seja r o raio do círculo $C(a,b)$ e R o raio do círculo $C(c,d)$. Da definição, sabemos as coordenadas dos centros dos dois círculos, logo podemos determinar a distância D que os separa

$$D^2 = \left(\frac{a}{b} - \frac{c}{d}\right)^2 + \left(\frac{1}{2b^2} - \frac{1}{2d^2}\right)^2.$$



Por outro lado, sabemos a soma do raio dos dois círculos (elevarei ao quadrado para assemelhar-se à fórmula de D^2)

$$(r + R)^2 = \left(\frac{1}{2b^2} + \frac{1}{2d^2}\right)^2.$$

Calcularemos a diferença $D^2 - (r + R)^2$. Se ela for igual a zero, os círculos são tangentes; e se ela for positiva, eles não se intersectam. Essa diferença vale:

$$D^2 - (r + R)^2 = \left(\frac{a}{b} - \frac{c}{d}\right)^2 + \left(\frac{1}{2b^2} - \frac{1}{2d^2}\right)^2 - \left(\frac{1}{2b^2} + \frac{1}{2d^2}\right)^2 = \frac{(ad - bc)^2 - 1}{b^2 d^2} \geq 0.$$

Portanto ou os dois círculos se tangenciam ou eles não se tocam. Se as frações a/b e c/d são consecutivas em F_n, pelo Teorema 2.1, vale a relação unimodal, portanto os círculos de Ford $C(a, b)$ e $C(c, d)$ se tangenciam exteriormente. $\square$

As coordenadas dos pontos de tangência podem ser calculadas.

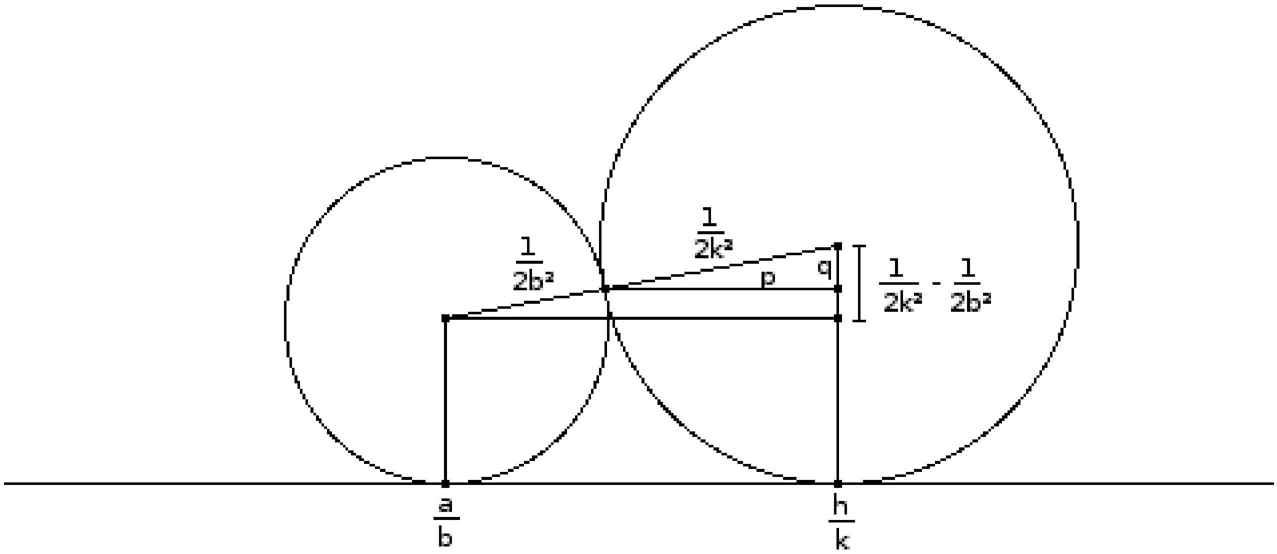
Teorema 2.3. *Sejam $a/b < h/k < c/d$ três frações de Farey de ordem n consecutivas. Os pontos de tangência dos círculos $C(a, b)$ e $C(h, k)$ e dos círculos $C(h, k)$ e $C(c, d)$ são, respectivamente,*

$$\alpha_1 = \frac{h}{k} - \frac{b}{k(k^2 + b^2)} + \frac{1}{k^2 + b^2} i$$

e

$$\alpha_2 = \frac{h}{k} + \frac{d}{k(k^2 + d^2)} + \frac{1}{k^2 + d^2} i.$$

Demonstração: Uma figura auxiliará a demonstração.



Conforme a figura, tem-se

$$\alpha_1 = \left(\frac{h}{k} - p\right) + i\left(\frac{1}{2k^2} - q\right) \tag{2.1}$$

Através da semelhança dos triângulos retângulos, determina-se p e q. Primeiro

$$\frac{p}{\frac{h}{k} - \frac{a}{b}} = \frac{\frac{1}{2k^2}}{\frac{1}{2k^2} + \frac{1}{2b^2}} = \frac{b^2}{k^2 + b^2}$$

portanto

$$p = \frac{b}{k(k^2 + b^2)}.$$

Usando de novo a semelhança, chega-se à

$$\frac{q}{\frac{1}{2k^2}} = \frac{\frac{1}{2k^2} - \frac{1}{2b^2}}{\frac{1}{2k^2} + \frac{1}{2b^2}} = \frac{b^2 - k^2}{b^2 + k^2}$$

portanto

$$q = \frac{1}{2k^2}\frac{b^2 - k^2}{b^2 + k^2}.$$

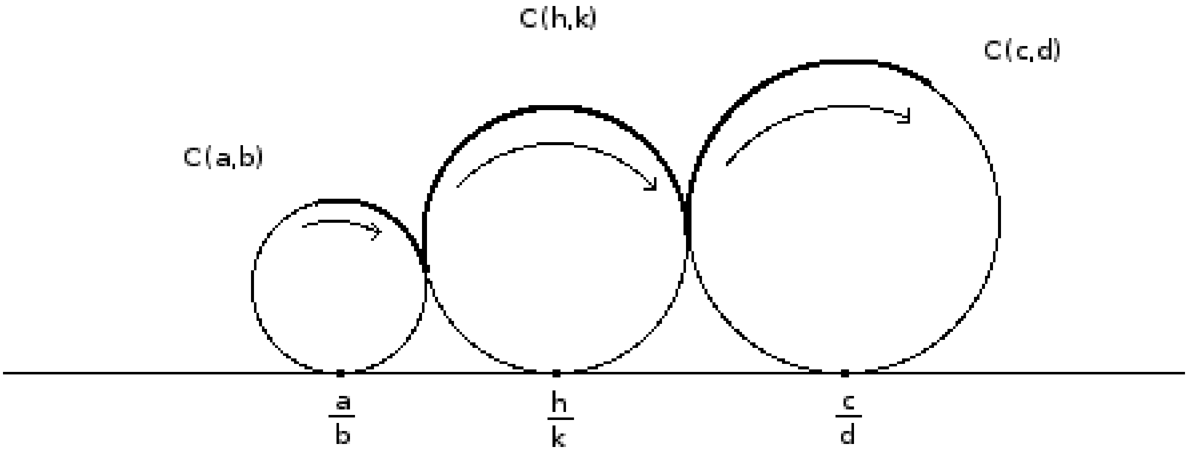
Substituindo os valores de p e q na expressão de α_1, na fórmula 2.1, chega-se na fórmula desejada. A fórmula para α_2 é obtida de modo análogo.

$\square$

2.3 Construção do caminho

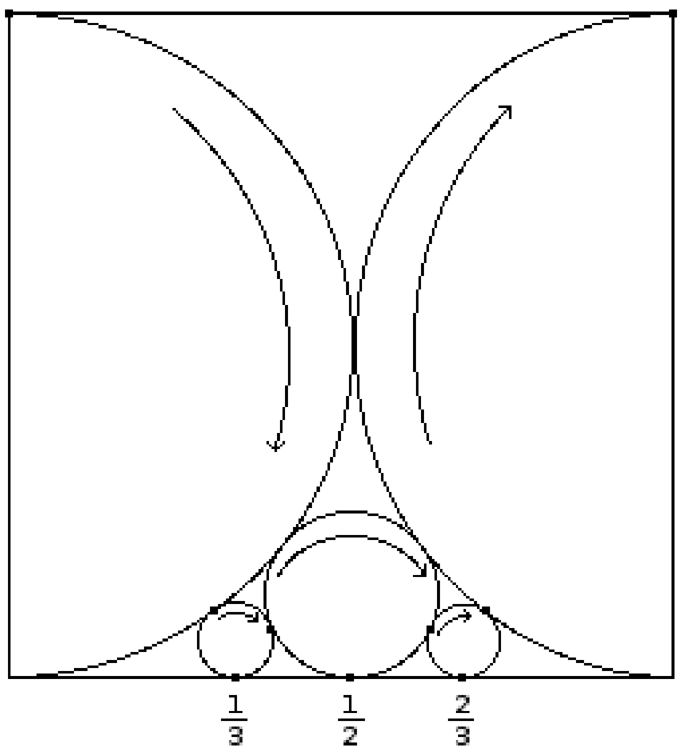
Para cada inteiro positivo N, será construído um caminho C_N que liga os pontos i e $i + 1$. Consideraremos os círculos de Ford correspondentes às frações de Farey de ordem N, F_N. Frações consecutivas correspondem à círculos tangentes, segundo o Teorema 2.2. Se $a/b < h/k < c/d$ são frações de Farey de ordem N consecutivas (até o final desta seção, estas frações desempenham o mesmo papel), são considerados os círculos respectivos de Ford $C(a, b)$, $C(h, k)$ e $C(c, d)$. Os pontos de tangência de $C(a, b)$ com

$C(h,k)$ e de $C(h,k)$ com $C(c,d)$ dividem o círculo $C(h,k)$ em dois arcos, um superior e um inferior. O arco superior $\gamma(h,k)$ faz parte do caminho C_N, como mostra a figura:



O caminho C_N é a união de todos esses arcos superiores. Com a exceção de que para as frações $0/1$ e $1/1$ são consideradas a parte do arco que está dentro do quadrado de vértices 0, 1, i e $i+1$.

Exemplo 2.2. *O caminho C_3 é descrito na figura seguinte.*

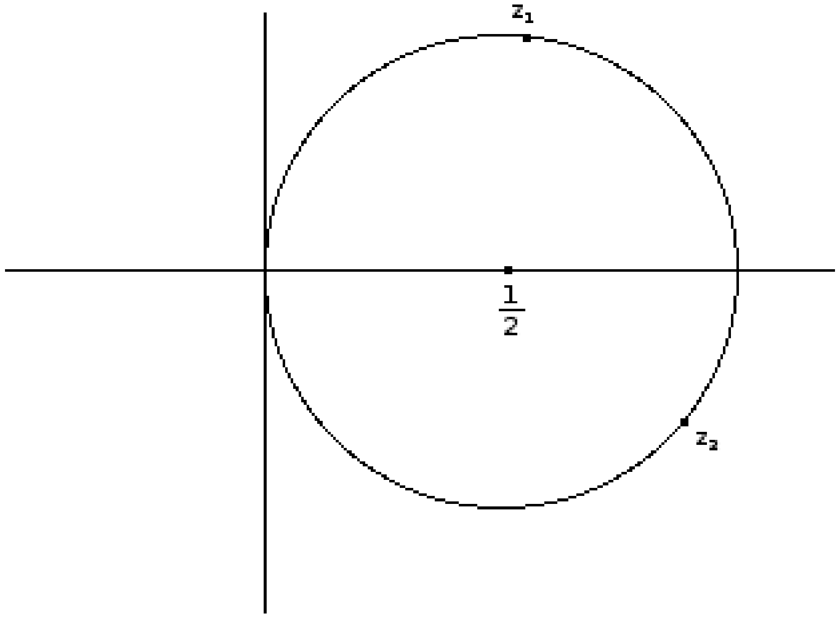


É conveniente estudarmos, neste ponto, o efeito de uma certa mudança de variáveis sobre $C(h,k)$.

Teorema 2.4. *A mudança de variáveis*

$$z = -ik^2\left(\tau - \frac{h}{k}\right)$$

mapeia o círculo de Ford $C(h,k)$ do plano τ num círculo K do plano z de raio $1/2$ em torno do ponto $z = 1/2$.



Os pontos de tangência das frações de Farey consecutivas α_1 e α_2, descritos no Teorema 2.3, são aplicados respectivamente nos pontos

$$z_1 = \frac{k^2}{k^2+b^2} + i\frac{kb}{k^2+b^2}$$

e

$$z_2 = \frac{k^2}{k^2+d^2} + i\frac{kd}{k^2+d^2}.$$

O arco superior que une α_1 a α_2 é aplicado no arco de K que não toca o eixo imaginário de z.

Demonstração: A translação $\tau-(h/k)$ leva o círculo $C(h,k)$ para a esquerda h/k unidades, portanto move seu centro para o ponto do eixo imaginário $i/(2k^2)$. A multiplicação por $-ik^2$ expande o raio para $1/2$ e rotaciona o círculo de $\pi/2$ no sentido horário. As expressões para z_1 e z_2 seguem diretamente das expressões α_1 e α_2 do Teorema 2.3, aplicando a expressão da mudança de variáveis. Finalmente, o arco superior de $C(h,k)$ é aplicado no arco de K que não toca o eixo imaginário, pois o ponto h/k (pertencente ao arco inferior) é levado na origem (pertencente ao arco que toca o eixo imaginário). $\square$

As seguinte estimativas de módulo serão utilizadas.

Teorema 2.5. *Tem-se*

$$|z_1| = \frac{k}{\sqrt{k^2+b^2}} \quad \text{e} \quad |z_2| = \frac{k}{\sqrt{k^2+d^2}}.$$

Se z está na corda (segmento de reta) que une z_1 a z_2, então

$$|z| < \frac{\sqrt{2}k}{N}.$$

O comprimento desta corda é $\leq \frac{2\sqrt{2}k}{N}$.

Demonstração: Basta calcular

$$|z_1|^2 = \frac{k^4+k^2b^2}{(k^2+b^2)^2} = \frac{k^2}{k^2+b^2}.$$

E de modo análogo se obtém a expressão de $|z_2|$. Agora a segunda parte do teorema. Considere z pertencente à corda que une z_1 a z_2. Queremos mostrar que $|z| < \frac{\sqrt{2}k}{N}$. Temos $|z| \leq \max\{|z_1|, |z_2|\}$. Então basta mostrar essa desigualdade para $z = z_1$ e $z = z_2$, faremos o primeiro caso, o segundo sendo análogo. Da expressão obtida para $|z_1|$ e da desigualdade que relaciona a média aritmética com a média quadrática

$$\frac{k+b}{2} \leq \sqrt{\frac{k^2+b^2}{2}},$$

obtém-se

$$|z_1| = \frac{k}{\sqrt{k^2+b^2}} \leq \frac{k}{\frac{k+b}{\sqrt{2}}} \leq \frac{k}{\frac{N+1}{\sqrt{2}}} < \frac{\sqrt{2}k}{N}.$$

Repare que $N+1 \geq k+b$, pois as frações a/b e h/k são consecutivas em F_N. Da análise do triângulo $\triangle 0 z_1 z_2$ conclui-se que o comprimento do segmento que une z_1 a z_2 é $\leq |z_1| + |z_2|$, e a desigualdade $|z| < \frac{\sqrt{2}k}{N}$ pode ser aplicada para $z = z_1$ e $z = z_2$, o que finaliza a demonstração. $\square$

Capítulo 3

A equação funcional de Dedekind

Esta equação (na verdade uma formulação equivalente) será muito importante para o cálculo da integral no método do círculo. Para sua demonstração – o objetivo deste capítulo –, precisamos estudar antes alguns assuntos.

Eis um roteiro deste capítulo. Primeiro, estudaremos o grupo modular Γ, que é um grupo de transformações que agem sobre o semi-plano superior $H = \{\tau \in \mathbb{C} : \Im(z) > 0\}$, que são aplicações analíticos inversíveis de H sobre si mesmo. Em seguida, estudaremos as somas de Dedekind $s(h,k)$ e algumas de suas propriedades — essas somas tem a ver com a fração h/k do caminho $\gamma(h,k)$. Depois, introduziremos a função eta $\eta(\tau)$ de Dedekind, que é uma função analítica definida no semi-plano superior H. Finalmente, veremos o que ocorrerá quando compusermos a função η com as transformações do grupo modular, o que dará origem a uma equação funcional — é nesta equação em que aparecem as somas de Dedekind.

3.1 Grupo modular Γ

Estamos interessados em transformações de Möbius (unimodulares)

$$f(z) = \frac{az+b}{cz+d},$$

onde a, b, c e d são inteiros que satisfazem a relação $ad - bc = 1$. Esta transformação é analítica (exceto por um pólo em $z = -d/c \in \mathbb{R}$) em todo plano complexo $\mathbb{C}$, mas só estaremos interessados no semi-plano superior $H \subset \mathbb{C}$, onde ela é analítica em todo ponto. Transformações de Möbius unimodulares são inversíveis. A inversa é também uma transformação de Möbius unimodular

$$f^{-1}(z) = \frac{dz-b}{-cz+a}.$$

Lema 3.1. *Toda transformação unimodular $f(\tau) = (a\tau+b)/(c\tau+d)$ deixa invariante o semi-plano superior H.*

Demonstração: Temos

$$\Im\left(f(\tau)\right) = \Im\left(\frac{(a\tau+b)(c\bar{\tau}+d)}{|c\tau+d|^2}\right) = \frac{\Im(ac\tau\bar{\tau}+ad\tau+cd\bar{\tau}+bd)}{|c\tau+d|^2} = \frac{\Im(\tau)}{|c\tau+d|^2},$$

portanto se $\tau \in H$ então $f(\tau) \in H$, lembrando que H é caracterizado pelos complexos cuja parte imaginária é positiva. □

O conjunto de automorfismos de H em que estamos interessados em estudar é Γ, o conjunto de todas as transformações de Möbius unimodulares restritas ao domínio H. Este conjunto Γ munido da operação de composição resulta um grupo. Vejamos uma outra interpretação de $f(\tau)$, que dá uma outra caracterização útil de Γ.

A transformação $f(\tau) = (a\tau + b)/(c\tau + d)$ está ligada à matriz $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Sem apelar para um excesso de notação: o que ocorre é que a composição de transformações de Γ corresponde ao produto das matrizes correspondentes. É preciso fazer um parênteses. A transformação $f(\tau)$ está ligada à duas matrizes, A e $-A$. De fato, pois $f(\tau) = (-a\tau - b)/(-c\tau - d)$. Agora podemos enunciar a outra caracterização. O conjunto de matrizes 2×2 de coeficientes inteiros e determinante 1 quociente pela relação de equivalência que identifica matrizes simétricas $A \sim -A$, munido da operação de produto, é um grupo (denota por $\mathsf{PSL}_2(\mathbb{Z})$). A correspondência descrita há pouco entre essas matrizes (na verdade, é a classe da matriz, mas omitiremos esse preciosismo) e Γ é um isomorfismo de grupos, considerando Γ com a operação de composição. A definição explícita é:

Definição 3.1. *O grupo modular Γ é composto de todas as transformações $f(\tau) = (a\tau + b)/(c\tau + d) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}(z)$ — onde a, b, c e d são inteiros que satisfazem a relação $ad - bc = 1$ — restritas ao domínio H. A operação considerada é a composição.*

Teorema 3.1. *O grupo modular Γ é gerado pelas transformações $S(\tau) = -1/\tau$ e $T(\tau) = \tau + 1$. Vale a relação $S^2 = I$.*

Demonstração: Será mostrado, analogamente ao enunciado, que qualquer matriz $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ é igual a um produto (não necessariamente único) de matrizes do tipo

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ e } S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

A demonstração será por indução em c, que podemos supor, sem perder generalidade, que satisfaz $c \geq 0$.

Se $c = 0$ então $ad = 1$, portanto $a = d = \pm 1$ e

$$A = \begin{pmatrix} \pm 1 & b \\ 0 & \pm 1 \end{pmatrix} = \begin{pmatrix} 1 & \pm b \\ 0 & 1 \end{pmatrix} = T^{\pm b}.$$

Se $c = 1$ então $ad - b = 1$, portanto $b = ad - 1$ e

$$A = \begin{pmatrix} a & ad-1 \\ 1 & d \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} = T^a S T^d.$$

Agora o passo de indução. Assumimos que a afirmação está provada para todos $c \leq c_0$, onde $c_0 \geq 1$, e vamos provar que ela vale para $c = c_0 + 1$. Como $ad - bc = 1$, tem-se $(c, d) = 1$. Pelo algoritmo da divisão euclidiana, existem q e r satisfazendo $0 < r < c$ e $d = cq + r$. Daí

$$AT^{-q} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & -aq+b \\ c & r \end{pmatrix}$$

e

$$AT^{-q}S = \begin{pmatrix} a & -aq+b \\ c & r \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -aq+b & -a \\ r & -c \end{pmatrix},$$

que, pela hipótese de indução, pode ser escrita como produto das matrizes S e T, já que $r \leq c - 1 = c_0$, o que finaliza a demonstração. □

3.2 Somas de Dedekind

As somas de Dedekind $s(h, k)$ surgirão na equação funcional da função eta $\eta(\tau)$, que será estudada na próxima seção. Até o final desta seção, será assumido que h e k são inteiros, $k > 0$ e $(h, k) = 1$. Primeiro, a definição das somas de Dedekind.

Definição 3.2. *Se h e k são inteiros, $k > 0$ e $(h,k) = 1$, a soma de Dedekind $s(h,k)$ é definida através da expressão*

$$s(h,k) = \sum_{r=1}^{k-1} \frac{r}{k}\left(\frac{hr}{k} - \left\lfloor \frac{hr}{k} \right\rfloor - \frac{1}{2}\right).$$

Como de costume, o símbolo $\lfloor x \rfloor$ representa a parte inteira de x, ou seja, o único inteiro k tal que $k \leq \lfloor x \rfloor < k+1$. Outra notação que será utilizada é a seguinte, $((x))$ definida da seguinte maneira:

$$((x)) = \begin{cases} x - \lfloor x \rfloor - \frac{1}{2} & \text{se } x \text{ não é inteiro;} \\ 0 & \text{se } x \text{ é inteiro.} \end{cases}$$

A função $((x))$ é periódica, com período 1, e ímpar, isto é, $((-x)) = -((x))$. O seguinte somatório anula-se

$$\sum_{r=0}^{k-1} \left(\left(\frac{r}{k}\right)\right) = 0,$$

pelo argumento que segue. Neste somatório, r está percorrendo todas as classes módulo k. Podemos substituir os r's, devido à periodicidade de $((x))$, por outros representantes da mesma classe módulo k. Para um certo r, se a classe de $-r$ módulo k for diferente, então $((\frac{r}{k})) + ((-\frac{r}{k})) = 0$, pois a função $((x))$ é ímpar. Pode, então, restar no somatório um único r que está na mesma classe de $-r$ módulo k. Mas neste caso $((r)) = 0$ pois $-((r)) = ((-r)) = ((r))$. O que conclui o argumento.

Utilizando-se desse argumento das classes módulo k, se obtém uma expressão mais geral

$$\sum_{r=0}^{k-1} \left(\left(\frac{hr}{k}\right)\right) = 0,$$

sempre que $(h,k) = 1$, pois hr percorre todas as classes módulo k.

Feitas essas observações, é possível encontrar uma outra expressão para a soma de Dedekind, que será útil.

$$\sum_{r=1}^{k-1} \frac{r}{k}\left(\left(\frac{hr}{k}\right)\right) = \sum_{r=0}^{k-1}\left(\frac{r}{k} - \frac{1}{2}\right)\left(\left(\frac{hr}{k}\right)\right) = \sum_{r=0}^{k-1}\left(\left(\frac{r}{k}\right)\right)\left(\left(\frac{hr}{k}\right)\right),$$

ou seja,

$$s(h,k) = \sum_{r=0}^{k-1}\left(\left(\frac{r}{k}\right)\right)\left(\left(\frac{hr}{k}\right)\right). \tag{3.1}$$

Teorema 3.2. *Se $h \equiv \pm h' (\textit{mod } k)$ então $s(h,k) = \pm s(h',k)$.*

Demonstração: É uma conseqüência da fórmula 3.1. □

Não existe uma fórmula simples para $s(h,k)$. Contudo, existe uma lei de reciprocidade que relaciona $s(h,k)$ e $s(k,h)$ de uma maneira simples. Esta lei será necessária adiante. A demonstração não é a original de Dedekind, é devida a Rademacher e Whiteman, e consiste em calcular a expressão $\sum_{r=1}^{k}\left(\left(\frac{hr}{k}\right)\right)^2$ de duas maneiras diferentes.

Teorema 3.3 (Lei da reciprocidade para somas de Dedekind)**.** *Se $h > 0$, $k > 0$ e $(h,k) = 1$ então*

$$12hks(h,k) + 12hks(k,h) = h^2 + k^2 - 3hk + 1.$$

Demonstração: Tem-se

$$\sum_{r=1}^{k}\left(\left(\frac{hr}{k}\right)\right)^2 = \sum_{r=1}^{k}\left(\left(\frac{r}{k}\right)\right)^2 = \sum_{r=1}^{k-1}\left(\frac{r}{k} - \frac{1}{2}\right)^2,$$

que, ao ser expandida, resulta

$$\frac{1}{k^2}\sum_{r=1}^{k-1} r^2 - \frac{1}{k}\sum_{r=1}^{k-1} r + \frac{1}{4}\sum_{r=1}^{k-1} 1,$$

por outro lado

$$\begin{aligned}
\sum_{r=1}^{k}\left(\left(\frac{hr}{k}\right)\right)^2 &= \sum_{r=1}^{k-1}\left(\frac{hr}{k}-\left\lfloor\frac{hr}{k}\right\rfloor-\frac{1}{2}\right)^2 \\
&= \sum_{r=1}^{k-1}\left(\frac{h^2r^2}{k^2}+\left\lfloor\frac{hr}{k}\right\rfloor^2+\frac{1}{4}-\frac{hr}{k}+\left\lfloor\frac{hr}{k}\right\rfloor-\frac{2hr}{k}\left\lfloor\frac{hr}{k}\right\rfloor\right) \\
&= 2h\sum_{r=1}^{k-1}\frac{r}{k}\left(\frac{hr}{k}-\left\lfloor\frac{hr}{k}\right\rfloor-\frac{1}{2}\right)+ \\
&\quad \sum_{r=1}^{k-1}\left\lfloor\frac{hr}{k}\right\rfloor\left(\left\lfloor\frac{hr}{k}\right\rfloor+1\right)-\frac{h^2}{k^2}\sum_{r=1}^{k-1}r^2-\frac{1}{4}\sum_{r=1}^{k-1}1.
\end{aligned}$$

As duas expressões juntas, já feito ajustes, resultam

$$2hs(h,k)+\sum_{r=1}^{k-1}\left\lfloor\frac{hr}{k}\right\rfloor\left(\left\lfloor\frac{hr}{k}\right\rfloor+1\right)=\frac{h^2+1}{k}\sum_{r=1}^{k-1}r^2-\frac{1}{k}\sum_{r=1}^{k-1}r. \tag{3.2}$$

No somatório, do lado esquerdo da igualdade 3.2, separamos os termos para os quais $\left\lfloor\frac{hr}{k}\right\rfloor$ tem um valor igual. Como $0<r<k$, tem-se $0<\frac{hr}{k}<h$ e se pode escrever

$$\left\lfloor\frac{hr}{k}\right\rfloor = v-1,$$

onde $v=1,2,\ldots,h$. Para cada v destes, seja $N(v)$ a quantidade de valores de r para os quais se tem $\left\lfloor\frac{hr}{k}\right\rfloor=v-1$. Esta última expressão é equivalente à $v-1<\frac{hr}{k}<v$ ou ainda

$$\frac{k(v-1)}{h}<r<\frac{kv}{h},$$

a igualdade $v-1=\frac{hr}{k}$ é excluída pois ela equivale a $(v-1)k=hr$, entretanto $0<r<k$ e $(h,k)=1$, ou seja, hr não pode ser mútiplo de k, uma contradição — para o caso $k=1$, este argumento não funciona, só que este é um caso onde o somatório é vazio. Portanto $\left\lfloor\frac{hr}{k}\right\rfloor=v-1$ para r de $\lfloor k(v-1)/h\rfloor+1$ até $\lfloor kv/h\rfloor$, logo

$$N(v)=\lfloor kv/h\rfloor-\lfloor k(v-1)/h\rfloor,$$

isto se $1\le v\le h-1$. Para $v=h$, tem-se de excluir o caso $r=k$, portanto

$$N(h)=k-1-\lfloor k(h-1)/h\rfloor.$$

Agora, temos

$$\begin{aligned}
\sum_{r=1}^{k-1}\left\lfloor\frac{hr}{k}\right\rfloor\left(\left\lfloor\frac{hr}{k}\right\rfloor+1\right) &= \sum_{v=1}^{h}(v-1)vN(v) \\
&= \left\{\sum_{v=1}^{h-1}(v-1)v\left(\left\lfloor\frac{kv}{h}\right\rfloor-\left\lfloor\frac{k(v-1)}{h}\right\rfloor\right)\right\}+h(h-1)N(h) \\
&= \left\{\sum_{v=1}^{h-1}\left\lfloor\frac{kv}{h}\right\rfloor\{(v-1)v-v(v+1)\}\right\}+(k-1)h(h-1) \\
&= -2\left\{\sum_{v=1}^{h-1}v\left\lfloor\frac{kv}{h}\right\rfloor\right\}+(k-1)h(h-1).
\end{aligned}$$

Por outro lado, da definição,

$$2hs(k,h)=2\sum_{v=1}^{h-1}v\left(\frac{kv}{h}-\left\lfloor\frac{kv}{h}\right\rfloor-\frac{1}{2}\right)=-2\sum_{v=1}^{h-1}v\left\lfloor\frac{kv}{h}\right\rfloor+\frac{2k}{h}\sum_{v=1}^{h-1}v^2-\sum_{v=1}^{h-1}v.$$

Logo

$$\sum_{r=1}^{k-1}\left\lfloor\frac{hr}{k}\right\rfloor\left(\left\lfloor\frac{hr}{k}\right\rfloor+1\right)=2hs(k,h)-\frac{2k}{h}\sum_{v=1}^{h-1}v^2+\sum_{v=1}^{h-1}v+h(h-1)(k-1)$$

Substituindo esta expressão, na equação 3.2, chegamos à lei da reciprocidade. □

3.3 A equação funcional

A função eta de Dedekind $\eta(\tau)$ foi estudada pela primeira vez em 1877, por Dedekind. Ela está ligada à função geradora das partições $F(x)$ pela equação $\eta(\tau)F(e^{2\pi i\tau})=e^{\pi i\tau/12}$. Vejamos uma definição.

Definição 3.3. *A função eta de Dedkind $\eta(\tau)$ é definida para cada $\tau\in H$ (lembrando que $H=\{\tau\in\mathbb{C}:\Im(\tau)>0\}$ é o semi-plano superior), pela expressão*

$$\eta(\tau)=e^{\pi i\tau/12}\prod_{n=1}^{\infty}(1-e^{2\pi in\tau}).$$

Conforme a explicação dada antes da demonstração do Teorema 1.1, sabemos que o produtório $\prod_{n=1}^{\infty}(1-x^n)$ converge para uma função analítica, sem zeros, definida no disco unitário $|x|<1$.

Se $\tau\in H$ então $x=e^{2\pi i\tau}$ satisfaz $|x|<1$. A expressão que define a função η envolve o produtório $\prod_{n=1}^{\infty}(1-x^n)$, com este x. Concluímos daí que a função η é composição de duas funções analíticas, logo é analítica em todo o domínio H.

Agora estudaremos o que acontece quando fazemos uma composição da função η com uma transformação do grupo modular Γ. Para $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\Gamma$, encontraremos uma expressão que relaciona $\eta\left\{(a\tau+b)/(c\tau+d)\right\}$ com $\eta(\tau)$. Essa expressão envolve as somas de Dedekind e é chamada de *equação funcional de Dedekind*.

A equação funcional é a seguinte: para $c>0$

$$\eta\left(\frac{a\tau+b}{c\tau+d}\right)=\epsilon(A)\{-i(c\tau+d)\}^{1/2}\eta(\tau),$$

onde

$$\epsilon(A)=\exp\left\{\pi i\left(\frac{a+d}{12c}-s(d,c)\right)\right\}$$

e $s(d,c)$ é uma soma de Dedekind.

A demonstração que apresentaremos tem duas partes. A primeira demonstra diretamente que a equação funcional é válida para os casos $A=T$ e $A=S$, recordando que $T(\tau)=\tau+1$ e $S(\tau)=-1/\tau$ — o primeiro caso sendo fácil e o segundo bem mais difícil. A segunda parte da demonstração usa o fato de que o grupo modular Γ é gerado por S e T. Finalmente, se mostrará que se a equação funcional vale para A então ela também vale para AS e AT. Isto implicará que ela vale para quaisquer produtos de S e T, que, como sabemos, é todo o grupo modular Γ.

3.3.1 Casos T e S

Para o gerador $T(\tau)=\tau+1$, tem-se

$$\eta(\tau+1)=e^{\pi i(\tau+1)/12}\prod_{n=1}^{\infty}(1-e^{2\pi in(\tau+1)}),$$

mas $e^{2\pi in(\tau+1)}=e^{2\pi in\tau}$, logo

$$\eta(\tau+1)=e^{\pi i/12}\eta(\tau).$$

Mais geralmente

$$\eta(T^b(\tau)) = e^{\pi i b/12}\eta(\tau).$$

Para o outro gerador S, a demonstração é bem mais difícil. A prova apresentada aqui é devida a C. L. SIEGEL, ver na bibliografia [1].

Teorema 3.4. *Para cada $\tau \in H$, tem-se*

$$\eta(\tau + b) = e^{\pi i b/12}\eta(\tau) \quad \text{e} \quad \eta\left(\frac{-1}{\tau}\right) = (-i\tau)^{1/2}\eta(\tau).$$

O ramo do logaritmo, usado para extrair a raiz quadrada, é o tradicional: $\log(z) > 0$ para $z > 0$.

Na demonstração que segue, será utilizado o seguinte resultado (conferir referência [6, página 405])

Lema 3.2 (Teorema da Convergência Limitada de Arzelà)**.** *Sejam $\{f_n\}_{n\in\mathbb{N}}$ funções reais Riemann-integráveis definidas no intervalo fechado $[a,b]$. Suponha que f_n converge pontualmente a uma função f também Riemann-integrável e que $\{f_n\}_{n\in\mathbb{N}}$ é uniformemente limitada em $[a,b]$. Nestas condições*

$$\lim_{n\longrightarrow\infty}\int_a^b f_n(x)dx = \int_a^b \lim_{n\longrightarrow\infty} f_n(x)dx = \int_a^b f(x)dx.$$

Demonstração: A primeira parte está pronta. Queremos demonstrar a expressão $\eta(-1/\tau) = (-i\tau)^{1/2}\eta(\tau)$ para todo $\tau \in H$. O lado direito e o lado esquerdo desta equação são funções analíticas na variável τ, definidas no semi-plano superior. A estratégia da prova será demonstrar que a equação é válida para $\tau = iy$ com $y > 0$. Por continuação analítica, as duas funções devem ser iguais em todo H e portanto a equação é válida em geral.

Para $\tau = iy$ com $y > 0$, a equação se torna $\eta(i/y) = y^{1/2}\eta(iy)$, que é equivalente a

$$\log\eta(i/y) - \log\eta(iy) = \frac{1}{2}\log y.$$

De fato, o logaritmo pode ser tomado, pois da expressão que define $\eta(\tau)$, vemos que ela é um número real e positivo se τ é da forma iy com $y > 0$. Então

$$\begin{aligned}
\log\eta(iy) &= -\frac{\pi y}{12} + \log\prod_{n=1}^{\infty}(1 - e^{-2\pi n y}) = -\frac{\pi y}{12} + \sum_{n=1}^{\infty}\log(1 - e^{-2\pi n y}) \\
&= -\frac{\pi y}{12} - \sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\frac{e^{-2\pi m n y}}{m} \\
&= -\frac{\pi y}{12} - \sum_{m=1}^{\infty}\frac{1}{m}\frac{e^{-2\pi m y}}{1 - e^{-2\pi m y}} = -\frac{\pi y}{12} + \sum_{m=1}^{\infty}\frac{1}{m}\frac{1}{1 - e^{2\pi m y}}
\end{aligned}$$

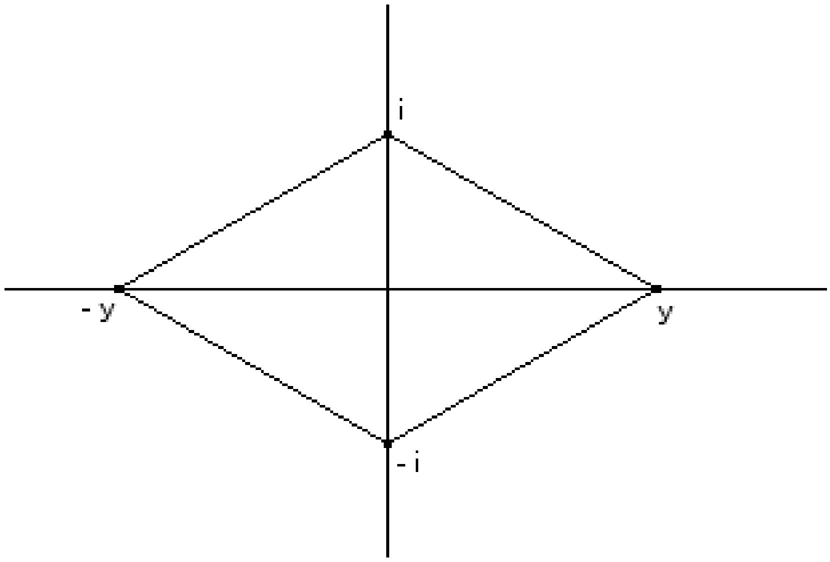
Ou seja, queremos demonstrar que

$$\sum_{m=1}^{\infty}\frac{1}{m}\frac{1}{1 - e^{2\pi m y}} - \sum_{m=1}^{\infty}\frac{1}{m}\frac{1}{1 - e^{2\pi m/y}} - \frac{\pi}{12}\left(y - \frac{1}{y}\right) = -\frac{1}{2}\log y.$$

Iremos provar esta última expressão através da teoria de resíduos de variável complexa. Seja $y > 0$ fixo, a partir daqui. Para cada n inteiro positivo, colocamos $m = n + \frac{1}{2}$, e definimos a função auxiliar

$$F_n(z) = -\frac{1}{8z}\cot\pi i m z \cot\frac{\pi m z}{y}.$$

Seja G o paralelogramo de vértices y, i, $-y$ e $-i$, conforme a figura:



Vejamos quais são as singularidades de F_n no interior da região G. Como $\cot = \cos / \sin$, estamos interessados nos zeros das funções $\cos$ e $\sin$. Os únicos zeros da função $\sin$ são da forma πz para z inteiro; e de $\cos z$, da forma $\pi z + \frac{\pi}{2}$ para z inteiro.

Para cada k inteiro, $z = ik/m$ é um pólo simples, pois é um pólo de $\cot \pi imz$ mas não é um zero de $\cot \frac{\pi mz}{y}$. Os pólos interiores a G são aqueles com $k = \pm 1, \pm 2, \ldots, \pm n$. De modo análogo, se conclui que $z = ky/m$ é um pólo simples de $F_n(z)$, para $k = \pm 1, \pm 2, \ldots, \pm n$. O número $z = 0$ é um pólo simples tanto de $\frac{-1}{8z}$ como de $\cot \pi imz$ como de $\cot \pi mz/y$, portanto é um pólo triplo de $F_n(z)$. Essas são todas as singularidades em G.

Pela teoria dos resíduos, podemos determinar o resíduo de F_n no ponto $z = 0$ definindo $g(z) = z^3[F_n(z)]$ e calculando $\frac{1}{2!}g''(0)$, que resulta $i(y - y^{-1})/24$, fazendo as contas. De modo similar, se conclui que para cada k, como do parágrafo anterior, o resíduo de $z = ik/m$ é $\frac{1}{8\pi k} \cot \frac{\pi ik}{y}$, que é uma função par em k, portanto

$$\sum_{(0 \neq k)=n}^{n} \mathrm{Res}_{ik/m}(F_n(z)) = 2 \sum_{k=1}^{n} \frac{1}{8\pi k} \cot \frac{\pi ik}{y}.$$

Mas

$$\cot i\theta = i\frac{e^{-\theta} + e^{\theta}}{e^{-\theta} - e^{\theta}} = \frac{1}{i}\left(1 - \frac{2}{1 - e^{2\theta}}\right).$$

Se escolhemos $\theta = \pi k/y$, obtemos

$$\sum_{(0 \neq)k=-n}^{n} \mathrm{Res}_{ik/m}(F_n(z)) = \frac{1}{4\pi i} \sum_{k=1}^{n} \frac{1}{k} - \frac{1}{2\pi i} \sum_{k=1}^{n} \frac{1}{k} \frac{1}{1 - e^{2\pi k/y}}.$$

E de modo similar para as singularidades $z = ky/m$, chegamos a

$$\sum_{(0 \neq)k=-n}^{n} \mathrm{Res}_{ky/m}(F_n(z)) = \frac{-1}{4\pi i} \sum_{k=1}^{n} \frac{1}{k} + \frac{1}{2\pi i} \sum_{k=1}^{n} \frac{1}{k} \frac{1}{1 - e^{2\pi ky}}.$$

Multiplicamos os resíduos por $2\pi i$ e os somamos, em seguida fazemos $n \longrightarrow \infty$. Pelo teorema dos resíduos de Cauchy, teremos

$$\lim_{n \longrightarrow \infty} \int_{\delta G} F_n(z) dz = \sum_{m=1}^{\infty} \frac{1}{m} \frac{1}{1 - e^{2\pi my}} - \sum_{m=1}^{\infty} \frac{1}{m} \frac{1}{1 - e^{2\pi m/y}} - \frac{\pi}{12}\left(y - \frac{1}{y}\right).$$

Por outro lado, se mostrarmos que $\lim_{n\longrightarrow\infty}\int_{\delta G} F_n(z)dz = -\frac{1}{2}\log y$, a demonstração estará completa.

Definimos como sendo $C = \delta G$ a curva da fronteira do paralelogramo G. Vamos estudar o que ocorre com a função $zF_n(z)$ nos lados do paralelogramo quando n tende ao infinito. Os pontos do lado pertencente ao primeiro quadrante — segmento $[i, y]$ — são da forma $ti + (1-t)y$ onde $0 \le t \le 1$. Para estes pontos, o limite é $\frac{1}{8}$ – isto pode se obtido através da fórmula $\cot(z) = i(1+e^{2iz})/(-1+e^{2iz})$. O mesmo para o segmento $[-y, -i]$ já que a função $\cot$ é uma função ímpar. Nos outros dois segmentos, o limite é $-\frac{1}{8}$. Mais ainda, a função $F_n(z)$ é uniformemente limitada em G – também pela expressão de $\cot$, deduz-se este resultado. Pelo teorema da convergência limitada de Arzelà,

$$\begin{aligned}
\lim_{n\longrightarrow\infty}\int_C F_n(z)dz &= \int_C \lim_{n\longrightarrow\infty} zF_n(z)\frac{dz}{z} \\
&= \frac{1}{8}\left\{-\int_{-i}^{y} + \int_{y}^{i} - \int_{i}^{-y} + \int_{-y}^{-i}\right\}\frac{dz}{z} \\
&= \frac{1}{4}\left\{-\int_{-i}^{y} + \int_{y}^{i}\right\}\frac{dz}{z} \\
&= \frac{1}{4}\left\{-\left(\log y + \frac{\pi i}{2}\right) + \left(-\log y + \frac{\pi i}{2}\right)\right\} = -\frac{1}{2}\log y
\end{aligned}$$

E a prova está terminada.

□

3.3.2 Caso geral

Teorema 3.5 (Equação funcional de Dedekind). *Se* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ *e* $c > 0$, *então para cada* $\tau \in H$, *vale*

$$\eta\left(\frac{a\tau + b}{c\tau + d}\right) = \epsilon(A)\{-i(c\tau + d)\}^{1/2}\eta(\tau),$$

onde

$$\epsilon(A) = \exp\left\{\pi i\left(\frac{a+d}{12c} - s(d,c)\right)\right\}$$

e $s(d,c)$ *é uma soma de Dedekind.*

A demonstração que apresentaremos é devida a Basil Gordon. Nós já sabemos que o teorema vale nos casos especiais $A = T^m$ e $A = S$, basta substituir os respectivos coeficientes a, b, c e d para verificar este fato. Sabemos também que qualquer transformação $A \in \Gamma$ pode ser escrita como um produto (possivelmente envolvendo várias repetições) das transformações S e T. O que será demonstrado é que se a equação funcional é válida para uma certa transformação unimodular $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, com $c > 0$, então ela também é valida para AT^m e AS. A restrição $c > 0$ não diminui a generalidade do teorema, pois caso $c = 0$, então da relação $ad - bc = 1$, conclui-se que $a = d = 1$ e que $A = T^b$; e se $c < 0$ podemos substituir a matriz A por $-A$, pois elas são equivalentes (correspondem à mesma transformação de Möbius). Estes dois fatos reunidos provarão a equação funcional de Dedekind no caso geral.

A demonstração será feita através de três lemas. Os dois primeiros relacionam $\epsilon(A)$ com $\epsilon(AT^m)$ e $\epsilon(AS)$. O último concluirá o argumento explicado no parágrafo anterior.

Lema 3.3. *Se* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ *e* $c > 0$, *então para qualquer inteiro* m, *tem-se*

$$\epsilon(AT^m) = e^{\pi i m/12}\epsilon(A).$$

Demonstração: Temos

$$AT^m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & am+b \\ c & cm+d \end{pmatrix},$$

portanto

$$\epsilon(AT^m) = \exp\left\{\pi i \left(\frac{a+cm+d}{12c} - s(cm+d,c)\right)\right\}.$$

Mas, pelo Teorema 3.2, $s(cm+d,c) = s(d,c)$; separando o termo $(cm)/(12c)$, chega-se ao resultado. □

Lema 3.4. *Se* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ *e* $c > 0$, *então*

$$\epsilon(AS) = \begin{cases} e^{-\pi i/4}\epsilon(A) & \text{se } d > 0, \\ e^{\pi i/4}\epsilon(A) & \text{se } d < 0. \end{cases}$$

Demonstração: Suponhamos, primeiro, que $d > 0$. Temos

$$AS = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}.$$

Daí

$$\epsilon(AS) = \exp\left\{\pi i \left(\frac{b-c}{12d} - s(-c,d)\right)\right\} = \exp\left\{\pi i \left(\frac{b-c}{12d} + s(c,d)\right)\right\} \tag{3.3}$$

pois $-s(-c,d) = s(c,d)$, pelo Teorema 3.2. A lei da reciprocidade de Dedekind implica que

$$s(c,d) + s(d,c) = \frac{c}{12d} + \frac{d}{12c} - \frac{1}{4} + \frac{1}{12cd}.$$

Substituímos o 1 da última fração por $ad - bc$, rearranjamos as frações obtendo

$$\frac{b-c}{12d} + s(c,d) = \frac{a+d}{12c} - s(d,c) - \frac{1}{4}.$$

Se substituirmos esta expressão, em 3.3, obteremos $\epsilon(AS) = e^{-\pi i/4}\epsilon(A)$, que é a primeira parte do lema.

No caso $d < 0$, usamos a matriz simétrica da anterior $\begin{pmatrix} -b & a \\ -d & c \end{pmatrix}$ (equivalente à AS) Essencialmente as mesmas contas obtém a expressão $\epsilon(AS) = e^{\pi i/4}\epsilon(A)$. □

Lema 3.5. *Se a equação funcional de Dedekind*

$$\eta(A(\tau)) = \epsilon(A)\{-i(c\tau + d)\}^{1/2}\eta(\tau) \tag{3.4}$$

é satisfeita para algum $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, *com* $c > 0$, *então ela é satisfeita para* AT^m *e para* AS.

Demonstração: Suponhamos que a equação seja satisfeita para A e substituamos τ por $T^m(\tau)$ em 3.4,

$$\begin{aligned} \eta(A[T^m(\tau)]) &= \epsilon(A)\{-i(cT^m(\tau) + d)\}^{1/2}\eta(T^m(\tau)) \\ &= \epsilon(A)\{-i(c\tau + mc + d)\}^{1/2}e^{\pi i m/12}\eta(T(\tau)) \\ &= \epsilon(AT^m)\{-i(c\tau + mc + d)\}^{1/2}\eta(T(\tau)) \end{aligned}$$

para a última passagem, foi usado o Lema 3.3. Portanto a equação funcional de Dedekind é satisfeita para AT^m se é satisfeita para A. Agora a segunda parte, suponhamos ela satisfeita para A, e substituindo τ por $S(\tau)$, em 3.4, obtém-se

$$\begin{aligned} \eta(A[S(\tau)]) &= \epsilon(A)\{-i(cS(\tau)+d)\}^{1/2}\eta(S(\tau)) \\ &= \epsilon(A)\{-i(cS(\tau)+d)\}^{1/2}\{-i\tau\}^{1/2}\eta(\tau) \end{aligned} \tag{3.5}$$

pelo Teorema 3.4. Suponhamos inicialmente que $d > 0$, reescrevemos

$$cS(\tau) + d = -\frac{c}{\tau} + d = \frac{d\tau - c}{\tau}$$

daí

$$i(cS(\tau) + d) = \frac{-i(-d\tau + c)}{-i\tau} e^{-\pi i/2}$$

pois $e^{\pi i/2} = i$. Finalmente

$$\{-i(cS(\tau)+d)\}^{1/2}\{-i\tau\}^{1/2} = e^{\pi/4}\{-i(-d\tau+c)\}^{1/2}.$$

Substituindo esta expressão em 3.5 e usando o Lema 3.4, concluímos que a equação funcional de Dedekind é satisfeita para AS. O caso $d < 0$ é análogo. □

3.4 A equação funcional em termos de $F(x)$

A equação funcional para a função η precisa ser reescrita em termos da função $F(x)$.

Teorema 3.6. *Seja* $F(x) = \prod_{m=1}^{\infty}(1 - x^m)^{-1}$,

$$x = \exp\left(\frac{2\pi i h}{k} - \frac{2\pi z}{k^2}\right) \qquad e \qquad x' = \exp\left(\frac{2\pi i H}{k} - \frac{2\pi}{z}\right),$$

onde $\Re(z) > 0$, $k > 0$, $(h,k) = 1$ *e* $hH \equiv -1 \mod k$. *Então*

$$F(x) = e^{\pi i s(h,k)}\left(\frac{z}{k}\right)^{1/2}\exp\left(\frac{\pi}{12z} - \frac{\pi z}{12k^2}\right)F(x').$$

Se $|z|$ é pequeno, então x estará muito próximo da raiz da unidade $e^{2\pi i h/k}$ enquanto x' estará muito próximo da origem, onde $F(0) = 1$. A expressão então descreve o comportamento de $F(x)$ quando x está próximo da raiz da unidade $e^{2\pi i h/k}$, e a função se comporta, a menos de uma multiplicação por costante, como

$$z^{1/2}\exp\left(\frac{\pi}{12z}\right).$$

Demonstração: Se $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ com $c > 0$, a equação funcional para $\eta(\tau)$ pode ser escrita como

$$\frac{1}{\eta(\tau)} = \frac{1}{\eta(\tau')}\{-i(c\tau+d)\}^{1/2}\exp\left\{\pi i\left(\frac{a+d}{12c} + s(-d,c)\right)\right\}$$

onde $\tau' = (a\tau + b)/(c\tau + d)$. Como $F(e^{2\pi i\tau}) = e^{\pi i\tau/12}/\eta(\tau)$, e da equação acima, temos

$$\begin{aligned} F(e^{2\pi i\tau}) &= F(e^{2\pi i\tau'})\exp\left(\frac{\pi i(\tau - \tau')}{12}\right)\{-i(c\tau+d)\}^{1/2} \\ &\quad \times \exp\left\{\pi i\left(\frac{a+d}{12c} + s(-d,c)\right)\right\}. \end{aligned} \tag{3.6}$$

Agora definimos $a = H$, $c = k$, $d = -h$, $b = -\frac{hH+1}{k}$ e $\tau = \frac{iz+h}{k}$. Da expressão $\tau' = (a\tau+b)/(c\tau+d)$, concluímos que

$$\tau' = \frac{iz^{-1} + H}{k}$$

e a equação 3.6 transforma-se em

$$\begin{aligned} F\left(\exp\left(\frac{2\pi ih}{k} - \frac{2\pi z}{k}\right)\right) &= F\left(\exp\left(\frac{2\pi iH}{k} - \frac{2\pi}{kz}\right)\right) z^{1/2} \\ &\quad \times \exp\left\{\frac{\pi}{12kz} - \frac{\pi z}{12k} + \pi is(h,k)\right\}. \end{aligned}$$

Se substituirmos z por z/k, temos a fórmula do enunciado do teorema. □

Capítulo 4

A demonstração final

Teorema 4.1. *Seja $n \geq 1$ um inteiro. A função partição* $\mathsf{p}(n)$ *é dada pela fórmula*

$$\mathsf{p}(n) = \frac{1}{\pi\sqrt{2}} \sum_{k=1}^{\infty} A_k(n)\sqrt{k}\frac{d}{dn}\left(\frac{\sinh\left\{\frac{\pi}{k}\sqrt{\frac{2}{3}\left(n-\frac{1}{24}\right)}\right\}}{\sqrt{n-\frac{1}{24}}}\right)$$

onde

$$A_k(n) = \sum_{0 \leq h < k}^{(h,k)=1} e^{\pi i s(h,k) - 2\pi i n h/k}.$$

e $s(h,k)$ *é uma soma de Dedekind, dada por*

$$s(h,k) = \sum_{r=1}^{k-1} \frac{r}{k}\left(\frac{hr}{k} - \left\lfloor \frac{hr}{k} \right\rfloor - \frac{1}{2}\right).$$

Demonstração: Já sabemos que

$$\mathsf{p}(n) = \frac{1}{2\pi i}\int_C \frac{F(x)}{x^{n+1}}dx$$

onde

$$F(x) = \prod_{m=1}^{\infty}(1-x^m)^{-1} = \sum_{n=0}^{\infty}\mathsf{p}(n)x^n$$

e C é qualquer curva bem comportada em $0 < |x| < 1$, que dá uma volta em torno da origem $x = 0$. A mudança de variáveis

$$x = e^{2\pi i \tau}$$

aplica o disco unitário perfurado $0 < |x| < 1$ numa faixa vertical de largura 1 no plano τ, como mostra a figura da página 5.

Se x percorre um círculo de raio $e^{-2\pi}$ com centro em $x = 0$, o ponto τ percorre o segmento que une os pontos i e $i+1$. Neste ponto da demonstração, substituímos este caminho pelo caminho de Rademacher C_N, construído na seção 2.3, que é composto dos arcos superiores dos círculos de Ford correspondentes às frações de Farey de ordem N. Daí

$$\mathsf{p}(n) = \int_{C_N} F(e^{2\pi i\tau})e^{-2\pi i n\tau}d\tau.$$

A partir deste ponto, n será mantido fixo, mas N não. Podemos subdividir o caminho C_N em vários caminhos $\gamma(h,k)$ — correspondente a cada fração de Farey h/k de ordem N. Por simplicidade de notação, denotarei F_N o conjunto das frações de Farey de ordem N. Então

$$\mathsf{p}(n) = \int_{C_N} F(e^{2\pi i\tau})e^{-2\pi i n\tau}d\tau = \sum_{(h/k)\in F_N}\int_{\gamma(h,k)} F(e^{2\pi i\tau})e^{-2\pi i n\tau}d\tau.$$

Para calcularmos a integral $\int_{\gamma(h,k)}$, fazemos a mudança de variável descrita no Teorema 2.4,

$$\tau = \frac{h}{k} + \frac{zi}{k^2}.$$

O Teorema 2.4 mostra que essa mudança aplica o círculo de Ford $C(h,k)$ em um círculo K de raio $1/2$ em torno de $z = 1/2$. O arco $\gamma(h,k)$ é levado no arco de extremidades $z_1 = z_1(h,k)$ e $z_2 = z_2(h,k)$, descrito no Teorema. Temos

$$\begin{aligned}
\mathsf{p}(n) &= \sum_{(h/k)\in F_N} \int_{z_1(h,k)}^{z_2(h,k)} F\left(\exp\left(\frac{2\pi ih}{k} - \frac{2\pi z}{k^2}\right)\right) \frac{i}{k^2} e^{-2\pi inh/k} e^{2n\pi z/k^2} dz \\
&= \sum_{(h/k)\in F_N} ik^{-2} e^{-2\pi inh/k} \int_{z_1(h,k)}^{z_2(h,k)} e^{2n\pi z/k^2} F\left(\exp\left(\frac{2\pi ih}{k} - \frac{2\pi z}{k^2}\right)\right) dz.
\end{aligned}$$

Agora usamos a equação funcional de Dedekind reescrita para $F(x)$, descrita no Teorema 3.6. Para

$$x = \left(\exp\left(\frac{2\pi ih}{k} - \frac{2\pi z}{k^2}\right)\right),$$

existe um H tal que $hH \equiv -1 \mod k$. Daí

$$F(x) = e^{\pi is(h,k)} \left(\frac{z}{k}\right)^{1/2} \exp\left(\frac{\pi}{12z} - \frac{\pi z}{12k^2}\right) F(x')$$

para

$$x' = \exp\left(\frac{2\pi iH}{k} - \frac{2\pi}{z}\right).$$

As contas começam a ficar muito grandes, a partir daqui. Vamos simplificar as coisas, definindo

$$\Psi_k(z) = z^{1/2} \exp\left(\frac{\pi}{12z} - \frac{\pi z}{12k^2}\right).$$

Sabemos que $F(0) = 1$; vamos usar um truque comum em análise, que é o de escrever $F(x')$ como $1 + \{F(x') - 1\}$, aí a integral se reparte em duas integrais, e cada uma delas será tratada diferentemente. Obtemos, então,

$$\mathsf{p}(n) = \sum_{(h/k)\in F_N} ik^{-5/2} e^{\pi is(h,k)} e^{-2\pi inh/k} \left(I_1(h,k) + I_2(h,k)\right) \tag{4.1}$$

onde

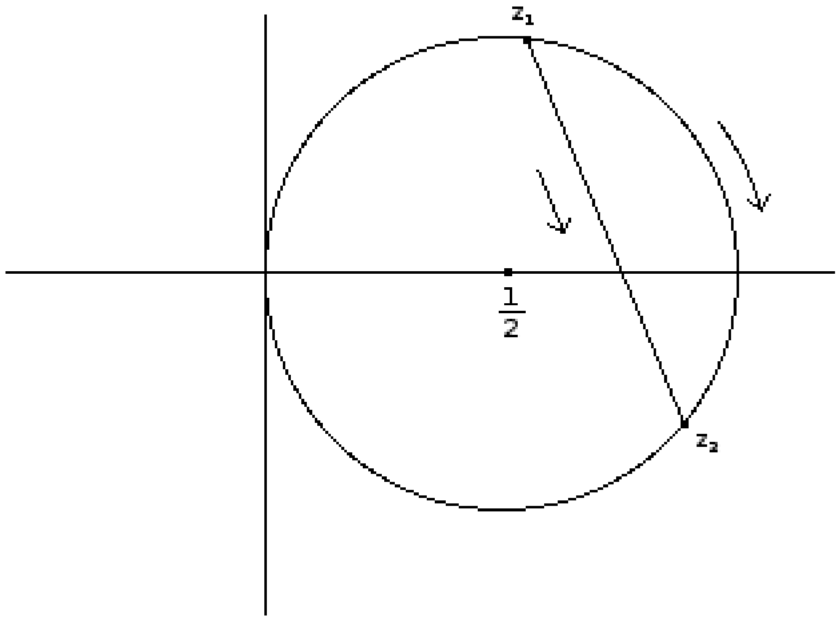
$$I_1(h,k) = \int_{z_1(h,k)}^{z_2(h,k)} \Psi_k(z) e^{2n\pi z/k^2}$$

e

$$I_2(h,k) = \int_{z_1(h,k)}^{z_2(h,k)} \Psi_k(z) \left\{F\left(\exp\left(\frac{2\pi iH}{k} - \frac{2\pi}{z}\right)\right) - 1\right\} e^{2n\pi z/k^2} dz.$$

Vamos tratar primeiramente de I_2; mostraremos que se tomarmos N suficientemente grande, I_2 torna-se arbitrariamente pequeno, ou seja, este termo, de certa forma, desaparecerá do nosso cálculo. Vamos ao trabalho.

Podemos mudar o caminho de integração, dentro da expressão de I_2, pela corda que une z_1 a z_2, conforme a figura seguinte, e isto não influenciará no cálculo da integral, pois não há singularidades no interior da região formada pelas duas curvas.



Já estimamos o comprimento deste segmento no Teorema 2.5; ele não é maior que $2\sqrt{2}k/N$. Para cada z que está na corda que liga z_1 a z_2, vale a desigualdade $|z| \leq \sqrt{2}k/N$.

Os pontos no círculo e no interior dele são da forma $z = \frac{1}{2} + re^{i\theta}$ onde $0 \leq r \leq \frac{1}{2}$. Precisaremos tratar de $\Re(1/z)$; usando o fato que $1/z = \bar{z}/|z|^2$, temos

$$\Re\left(\frac{1}{z}\right) = \frac{\Re(1/2 + r\cos\theta - r\sin\theta i)}{(1/2 + r\cos\theta)^2 + (r\sin\theta)^2} = \frac{1/2 + r\cos\theta}{1/4 + r\cos\theta + r^2} \geq 1,$$

pois $1/2 + r\cos\theta - (1/4 + r\cos\theta + r^2) = 1/4 - r^2 \geq 0$, já que $0 \leq r \leq \frac{1}{2}$. Para $r = \frac{1}{2}$, isto é, quando z está sobre o círculo K, $\Re(1/z) = 1$.

Ou seja, para cada z no círculo K ou no interior deste círculo, temos $0 < \Re(z) \leq 1$ e $\Re(1/z) \geq 1$, e para z no círculo vale a igualdade $\Re(1/z) = 1$. Agora vamos às estimativas do integrando em I_2:

$$\begin{aligned}
&\left|\Psi_k(z)\left\{F\left(\exp\left(\frac{2\pi i H}{k} - \frac{2\pi}{z}\right)\right) - 1\right\} e^{2n\pi z/k^2} dz\right| \\
&= |z|^{1/2} \exp\left\{\frac{\pi}{12}\Re\left(\frac{1}{z}\right) - \frac{\pi}{12k^2}\Re(z)\right\} e^{2n\pi\Re(z)/k^2} \left|\sum_{m=1}^{\infty} \mathsf{p}(m) e^{2\pi i H m/k} e^{-2\pi m/z}\right| \\
&\leq |z|^{1/2} \exp\left\{\frac{\pi}{12}\Re\left(\frac{1}{z}\right)\right\} e^{2n\pi/k^2} \sum_{m=1}^{\infty} \mathsf{p}(m) e^{-2\pi m \Re(1/z)} \\
&< |z|^{1/2} e^{2n\pi} \sum_{m=1}^{\infty} \mathsf{p}(m) e^{-2\pi(m-(1/24))\Re(1/z)} \\
&\leq |z|^{1/2} e^{2n\pi} \sum_{m=1}^{\infty} \mathsf{p}(m) e^{-2\pi(m-(1/24))} \\
&= |z|^{1/2} e^{2n\pi} \sum_{m=1}^{\infty} \mathsf{p}(m) e^{-2\pi(24m-1)/24} \\
&< |z|^{1/2} e^{2n\pi} \sum_{m=1}^{\infty} \mathsf{p}(24m-1) e^{-2\pi(24m-1)/24} \\
&= c|z|^{1/2}
\end{aligned}$$

onde

$$c = e^{2n\pi} \sum_{m=1}^{\infty} \mathsf{p}(24m-1) e^{-2\pi(24m-1)/24}.$$

Este número c não depende de N ou de z, apenas de n, mas este está fixado desde o começo da demonstração. Já estimamos o integrando de I_2, ele é $< c|z|^{1/2}$, onde c é uma constante; como z está na corda que une z_1 a z_2, $|z| < \sqrt{2}k/N$. Também sabemos que o comprimento de toda a corda é $< 2\sqrt{2}k/N$. Juntando a estimativa do integrando e do tamanho do caminho de integração,

$$|I_2(h,k)| < Ck^{3/2}N^{-3/2}$$

para alguma constante C que não nos interessa. Agora relembrando a fórmula 4.1, temos

$$\begin{aligned} \left|\sum_{(h/k)\in F_N} ik^{-5/2}e^{\pi is(h,k)}e^{-2\pi inh/k}I_2(h,k)\right| &< \sum_{k=1}^{N}\sum_{0\le h<k}^{(h,k)=1} Ck^{-1}N^{-3/2} \\ &\le CN^{-3/2}\sum_{k=1}^{N}1 = CN^{-1/2}. \end{aligned} \tag{4.2}$$

Agora vamos cuidar de I_1; também é uma integral de $z_1(h,k)$ até $z_2(h,k)$ ao longo de um arco do círculo K. Vamos integrar no círculo todo K, e mostraremos que o erro entre essas duas integrais também é da ordem de $N^{-1/2}$. Omitimos o integrando para simplificar as contas,

$$I_1(h,k) = \int_{K(-)} - \int_0^{z_1(h,k)} - \int_{z_2(h,k)}^{0} = \int_{K(-)} -J_1 - J_2.$$

A notação $K(-)$ indica que o círculo é percorrido no sentido negativo, ou seja, horário. Para estimar $|J_1|$, vemos que o comprimento do arco que une 0 a $z_1(h,k)$ é menor do que

$$\pi|z_1(h,k)| < \pi\sqrt{2}\frac{k}{N}.$$

Já estimamos o tamanho do caminho de integração em J_1, agora vamos estimar o integrando. Já sabemos que $\Re(1/z) = 1$ e $0 < \Re(z) \le 1$ se z está no círculo K, portanto

$$\begin{aligned} |\Psi_k(z)e^{2n\pi z/k^2}| &= e^{2n\pi\Re(z)/k^2}|z|^{1/2}\exp\left\{\frac{\pi}{12}\Re\left(\frac{1}{z}\right) - \frac{\pi}{12k^2}\Re(z)\right\} \\ &\le \frac{e^{2n\pi}2^{1/4}k^{1/2}e^{\pi/12}}{N^{1/2}}. \end{aligned}$$

Daí concluímos que

$$|J_1| < C_1k^{3/2}N^{-3/2},$$

multiplicando o comprimento do caminho pela cota do integrando; e C_1 é uma constante. De modo similar, se obtém uma estimativa

$$|J_2| < C_2k^{3/2}N^{-3/2}.$$

Agora lembramos que na expressão 4.1 de $\mathsf{p}(n)$, surgiu $I_1(h,k)$ dentro de um somatório $\sum_{(h/k)\in F_N*}$. Fazendo essencialmente a mesma conta que em 4.2, concluímos que a influência destes termos J, já feito o somatório, na fórmula de $\mathsf{p}(n)$ é da ordem de $N^{-1/2}$. E portanto quando N for tomado suficientemente grande, ele se tornará insignificante. Temos, então, a expressão

$$\mathsf{p}(n) = \sum_{k=1}^{N}\sum_{0\le h<k}^{(h,k)=1} ik^{-5/2}e^{\pi is(h,k)}e^{-2\pi inh/k}\int_{K(-)}\Psi_k(z)e^{2n\pi z/k^2}dz + O(N^{-1/2}).$$

Tomamos o limite $N \longrightarrow \infty$,

$$\mathsf{p}(n) = i\sum_{k=1}^{\infty}A_k(n)k^{-5/2}\int_{K(-)} z^{1/2}\exp\left\{\frac{\pi}{12z} + \frac{2\pi z}{k^2}\left(n - \frac{1}{24}\right)\right\}dz,$$

onde

$$A_k(n) = \sum_{0\le h<k}^{(h,k)=1} e^{\pi is(h,k) - 2\pi inh/k}.$$

Só o que falta é calcular esta integral. O que se faz é uma mudança de variáveis, primeiramente, e em seguida, a integral que se obtém é calculada em termos de funções de Bessel. Os detalhes estão em [7, pág. 109] e [2, pág. 181]. Por fim, chega-se à fórmula de Rademacher

$$\mathsf{p}(n) = \frac{1}{\pi\sqrt{2}} \sum_{k=1}^{\infty} A_k(n)\sqrt{k}\frac{d}{dn}\left(\frac{\sinh\left\{\frac{\pi}{k}\sqrt{\frac{2}{3}\left(n-\frac{1}{24}\right)}\right\}}{\sqrt{n-\frac{1}{24}}}\right).$$

□

Referências Bibliográficas

[1] Siegel Carl L. A simple proof of $\eta(-1/\tau) = \eta(\tau)\sqrt{\tau/i}$. *Mathematika*, 1(4), 1952.

[2] Watson G. N. *A Treatise on the Theory of Bessel Functions, Second Edition*. Cambridge University Press, Cambridge, 1962.

[3] Andrews George E. *The Theory of Partitions*. Cambridge University Press, Cambridge, 1984.

[4] Serre Jean-P. *Cours d'Arithmétique, 2ed.* Presses Universitaires de France, Paris, 1977.

[5] Conway John. *Functions of One Complex Variable*. Springer Verlag, New York, 1973.

[6] Apostol Tom M. *Mathematical Analysis*. Addison-Wesley Publishing Company, Inc., Massachusetts, 1958.

[7] Apostol Tom M. *Modular Functions and Dirichlet Series in Number Theory, Second Edition*. Springer Verlag, New York, 1990.