A conjectura de Bateman-Horn e o Λ-cálculo de Golomb

Pedro Henrique Pontes

Dissertação apresentada
ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para
obtenção do título
de
Mestre em Ciências

Programa: Mestrado em Matemática

Orientador: Prof. Dr. Paulo Agozzini Martin

O presente trabalho foi realizado com apoio do CNPq, Conselho Nacional de Desenvolvimento Científico e Tecnológico - Brasil

São Paulo, julho de 2012

A Conjectura de Bateman-Horn e o Λ-Cálculo de Golomb

Esta versão da dissertação contém as correções e alterações sugeridas pela Comissão Julgadora durante a defesa da versão original do trabalho, realizada em 02/07/2012. Uma cópia da versão original está disponível no Instituto de Matemática e Estatística da Universidade de São Paulo.

Comissão Julgadora:

- Prof. Dr. Paulo Agozzini Martin (orientador) - IME-USP
- Prof. Dr. Paulo Domingos Cordaro - IME-USP
- Prof. Dr. Nigel John Edward Pitt - Unb

Agradecimentos

Gostaria de agradecer ao meu orientador, Prof. Dr. Paulo Agozzini Martin, porque eu realmente lhe devo muito. Foi graças a ele que comecei a estudar Teoria dos Números, e ele soube muito bem me manter engajado no assunto, sugerindo problemas e textos interessantes e diversos. Agradeço a ele e ao Prof. Dr. Paulo Domingos Cordaro pelas aulas, sempre muito bem preparadas e esclarecedoras, que tiveram grande impacto sobre a minha formação como matemático. Essa influência sem dúvida aparece nesta dissertação. Também gostaria de agradecer ao Dr. Daniel M. Martin pela complicada obtenção da tese de doutoramento de Solomon W. Golomb, que foi essencial para o desenvolvimento deste texto.

Também gostaria de agradecer aos meus pais, Benedito Antonio Pontes e Cléa Magda Pontes pelo incrível apoio que sempre me deram nos meus intensos estudos. Não deve ter sido fácil me aguentar por tanto tempo simultaneamente próximo e ausente. Tudo o que faço hoje foi possível somente graças a eles.

Finalmente, gostaria de agradecer aos meus colegas de curso Gabriel Cueva Candido Soares de Araújo, Henrique Meretti Camargo, Bruno de Paula Jacóia, Max Reinhold Jahnke, Ivã Passoni, Luis Fernando Ragognette, e Lucas Kaufmann Sacchetto. Nunca teria conseguido terminar este texto sem a sua companhia. A Matemática não significa nada se não se pode compartilhá-la com amigos, mas como ela me permitiu estudar e conviver com cada um de vocês, este trabalho tem um significado verdadeiramente especial para mim.

Resumo

PONTES, P. H. **A conjectura de Bateman-Horn e o Λ-cálculo de Golomb**. 2012. 131 f. Dissertação (Mestrado) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2012.

A Conjectura de Bateman-Horn dá condições sobre uma família de polinômios com coeficientes inteiros $f_1(X), \ldots, f_k(X)$ para que hajam infinitos $n \in \mathbb{N}$ tais que $f_1(n), \ldots, f_k(n)$ sejam todos primos, e determina qual deve ser o comportamento assintótico de tais inteiros n. Neste texto, vamos estudar essa conjectura, assim como um método desenvolvido por Solomon W. Golomb que pode ser usado para demonstrá-la. Veremos que esse cálculo prova a Conjectura de Bateman-Horn a menos da troca de um limite com uma série infinita, que é o único passo ainda não provado desse método. Também estudaremos uma tentativa para solucionar esse problema por meio do uso de teoremas abelianos de regularidade, e provaremos que teoremas tão gerais não são suficientes para provar a troca do limite com a série.

Palavras-chave: Conjectura de Bateman-Horn, Λ-cálculo de Golomb, teoremas abelianos.

Abstract

PONTES, P. H. **The Bateman-Horn conjecture and Golomb's Λ-method**. 2012. 131 f. Dissertação (Mestrado) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2012.

Given a family of polynomials with integer coefficients $f_1(X), \ldots, f_k(X)$, one would like to answer the following question: does there exist infinitely many $n \in \mathbb{N}$ such that $f_1(n), \ldots, f_k(n)$ are all primes? Schinzel conjectured that if these polynomials satisfy certain simple conditions, then the answer to this question is affirmative. Assuming these conditions, Bateman and Horn proposed a formula for the asymptotic density of the integers $n \in \mathbb{N}$ such that $f_1(n), \ldots, f_k(n)$ are all primes. In this text, we shall study the Bateman-Horn Conjecture, as well as a method proposed by Solomon W. Golomb that may be used to prove this conjecture. We shall see that Golomb's Λ-method would prove the Bateman-Horn Conjecture, except for a single unproved step, namely, the commutation of a limit with an infinite series.

Keywords: Bateman-Horn conjecture, Golomb's Λ-method, Abelian theorems.

Sumário

1 Introdução **3**

1.1 Conjecturas sobre números primos 3

1.2 A densidade assintótica dos números primos 4

1.3 O Λ-cálculo de Golomb 6

1.4 Este texto 6

2 As conjecturas de Schinzel e de Bateman-Horn **9**

2.1 A Conjectura de Schinzel 9

2.2 Famílias apropriadas 10

2.3 A Conjectura de Bateman-Horn 11

2.4 Exemplos notáveis 21

3 A convergência do produto $C(\mathbf{f})$ **25**

3.1 Propriedades da função N_g 25

3.2 Demonstração da convergência de $C(\mathbf{f})$ 27

3.3 A função ζ de Dedekind 29

4 Uma demonstração do TNP **31**

4.1 Funções aritméticas 31

4.2 O Teorema de Hardy-Littlewood 32

4.3 Um teorema abeliano 35

4.4 Demonstração do Teorema dos Números Primos 36

5 O Λ-cálculo com séries de potências **37**

5.1 A equivalência entre $\pi_{\mathbf{f}}(x)$ e $\psi_{\mathbf{f}}(x)$ 37

5.2 A Identidade de Golomb 44

5.3 A Hipótese F 45

5.4 O Λ-cálculo 49

6 Demonstração da igualdade $S(\mathbf{f}) = C(\mathbf{f})$ **53**

6.1 As funções $L_{\mathbf{f}}(s)$ 53

6.2 Demonstração da convergência da série $S(\mathbf{f})$ 58

6.3 Demonstração da igualdade $S(\mathbf{f}) = C(\mathbf{f})$ 63

7 A não-regularidade do Λ-cálculo **67**
7.1 Transformações regulares 67
7.2 Transformações semelhantes 70
7.3 Uma variante do método da regularidade 71
7.4 Um problema inverso 75

8 O Teorema de Bateman-Stemmler **79**
8.1 Estimativas para $\theta_{\mathbf{f}}(x)$ e $\psi_{\mathbf{f}}(x)$ 82

9 O Λ-cálculo usando séries de Dirichlet **85**
9.1 Caso a): $F(s)$ é analítica em $s = 1$ 86
9.2 Caso b): $F(s)$ tem um polo em $s = 1$ 87

A O Critério de Kummer **91**

B Teoremas Abelianos **97**
B.1 Introdução 97
B.2 Métodos de somabilidade 98
B.3 Regularidade 99
B.4 Outro tipo de transformação 104
B.5 Um terceiro método 105
B.6 Os métodos de Abel e de Lambert 106

C Tauberianos para Séries de Dirichlet **109**
C.1 Outro tipo de teorema tauberiano 115

Referências Bibliográficas **119**

Índice Remissivo **121**

Notações

$\mathbb{N} \doteq \{1, 2, 3, \dots\}$. Por *número primo* queremos sempre dizer primo *positivo*. Dados $a, b \in \mathbb{Z}$, escrevemos $a \mid b$ quando, e somente quando a *divide* b. Escrevemos $a \nmid b$ se, e somente se a *não divide* b. Dado $n \in \mathbb{N}$, o símbolo $\sum_{d|n}$ denota uma soma sobre os divisores positivos d de n. Sempre que escrevermos $\prod_p$, quer dizer que estamos tomando o produto infinito sobre o conjunto de todos os números p primos (positivos).

Escrevemos $f = O(g)$ para duas funções a valores complexos f, g quando existirem $M, R > 0$ tais que $|f(x)| \leq M|g(x)|$ se $|x| \geq R$. Usamos essa notação com certa flexibilidade: por exemplo, quando quisermos considerar o limite de f com relação a g quando $x \to 0$, a igualdade $f = O(g)$ terá o seguinte significado: existem $M, \varepsilon > 0$ tais que $|f(x)| \leq M|g(x)|$ se $|x| \leq \varepsilon$. Mantemos a mesma notação $f = O(g)$ pois a definição que usamos estará clara pelo contexto. Também escrevemos $a_n = O(b_n)$ para duas sequências a valores complexos $(a_n)_{n\in\mathbb{N}}$ e $(b_n)_{n\in\mathbb{N}}$ se existir $M > 0$ tal que $|a_n| \leq M|b_n|$ para todo $n \in \mathbb{N}$.

Escrevemos também $f \ll g$ com o mesmo significado de $f = O(g)$, e escrevemos

$$f(x) = g(x) + O\big(h(x)\big)$$

se, e somente se $f - g = O(h)$. Escrevemos $f = o(g)$ quando

$$\lim_{x\to+\infty} \frac{f(x)}{g(x)} = 0.$$

Temos $f = g + o(h)$ por definição quando $f - g = o(h)$. Escrevemos $f(x) \sim g(x)$ quando

$$\lim_{x\to+\infty} \frac{f(x)}{g(x)} = 1.$$

Relembramos a definição das seguintes funções aritméticas básicas da Teoria dos Números:

- Dado $n \in \mathbb{N}$, denotamos por $\omega(n)$ o número de fatores primos de n, isto é;

  $$\omega(n) \doteq \#\{p \in \mathbb{N} \text{ primo} : p \mid n\},$$

  em que tomamos $\omega(1) = 0$.

- A função de von Mangoldt, $\Lambda(n)$, é dada por:

  $$\Lambda(n) = \begin{cases} \log p, & \text{se } n = p^k, \text{ com } p \text{ primo} \\ 0, & \text{caso contrário.} \end{cases}$$

  Em particular, $\Lambda(1) = 0$.

- A função de Möbius, $\mu(n)$, é dada por

  $$\mu(n) = \begin{cases} (-1)^{\omega(n)}, & \text{se } n \text{ é livre de quadrados, ou } n = 1 \\ 0, & \text{caso contrário.} \end{cases}$$

Definimos assim $\mu(1) = 1$.

Capítulo 1

Introdução

1.1 Conjecturas sobre números primos

Muito pouco se sabe sobre a existência de primos de uma forma específica dada. Por exemplo, algumas conjecturas em aberto que tratam da existência de primos de uma forma específica são:

Conjectura 1. *Existem infinitos primos p da forma $p = n^2 + 1$, com $n \in \mathbb{N}$.*

Conjectura 2 (dos primos gêmeos)**.** *Existem infinitos primos p tais que $p + 2$ também é primo.*

Dois primos p, q tais que $q = p + 2$ são ditos *primos gêmeos*.

Apesar da dificuldade desses problemas, é fácil e instrutivo generalizar as Conjecturas 1 e 2.

Uma extensão natural da Conjectura 1 seria propor uma pergunta da seguinte forma: dado um polinômio $f(X) \in \mathbb{Z}[X]$, será que existem infintos primos $p = f(n)$ com $n \in \mathbb{N}$?

Além disso, se escrevermos $f_1(X) \doteq X$ e $f_2(X) \doteq X + 2$, então a Conjectura 2 pergunta se existem infinitos $n \in \mathbb{N}$ tais que $f_1(n)$ e $f_2(n)$ são *simultaneamente* primos. Logo, podemos generalizar também essa pergunta substituindo $f_1(X), f_2(X)$ por dois polinômios quaisquer de $\mathbb{Z}[X]$. Mais ainda, podemos nos perguntar: dados $f_1(X), \ldots, f_k(X)$ polinômios com coeficientes inteiros, existem infinitos $n \in \mathbb{N}$ tais que $f_1(n), \ldots, f_k(n)$ são todos simultaneamente primos?[1]

Em geral, a resposta a essa pergunta será *não*. Por exemplo, se algum dos polinômios $f_i(X)$ for o produto de dois outros polinômios de $\mathbb{Z}[X]$, então decorre facilmente que $f_i(n)$ não será primo para nenhum $n \in \mathbb{N}$ suficientemente grande. Isso sugere exigir que todos os polinômios $f_1(X), \ldots, f_k(X)$ sejam irredutíveis, mas será que isso é suficiente?

Questão 1. Que condições devemos impor sobre os polinômios $f_1(X), \ldots, f_k(X) \in \mathbb{Z}[X]$ para que existam infinitos $n \in \mathbb{N}$ tais que

$$f_1(n), \ldots, f_k(n) \quad \text{sejam todos primos?}$$

Até hoje só foi provado um único resultado relacionado à Questão 1, que é o caso em que $k = 1$ e $\operatorname{gr} f_1(X) = 1$; o seguinte Teorema de Dirichlet:

Teorema 1.1 (Dirichlet)**.** *Se $a, b \in \mathbb{N}$ são relativamente primos, então existem infinitos números primos na progressão aritmética $\{an + b : n \in \mathbb{N}\}$.*

É importante notar que o Teorema 1.1 é o único Teorema já provado sobre a existência de primos de uma certa forma específica *no contexto da Questão 1*. Se, por exemplo, considerarmos polinômios com mais variáveis, temos também outros resultados, como o seguinte Teorema de Fermat:

[1] É importante observar que, ao contrário da notação usual deste texto, aqui contaremos também os primos *negativos* caso algum polinômio em questão assuma um tal valor. Esse problema será resolvido logo, pois restringiremos a nossa atenção aos polinômios que só assumem valores *positivos*.

Teorema 1.2 (Fermat)**.** *Seja p um número primo ímpar. Então existem $x, y \in \mathbb{N}$ tais que $p = x^2 + y^2$ se, e somente se $p \equiv 1 \pmod 4$.*

Em particular, segue dos Teoremas 1.1 e 1.2 que existem infinitos números primos p da forma $p = a^2 + b^2$ com $a, b \in \mathbb{N}$.

Para citar um resultado mais recente (e em que o comportamento não é equivalente ao de nenhum polinômio linear, como é o caso do Teorema 1.2), tem-se também o seguinte Teorema (veja [FI98]):

Teorema 1.3 (Friedlander, Iwaniec)**.** *Existem infinitos números primos da forma $p = a^2 + b^4$, com $a, b \in \mathbb{N}$.*

No entanto, neste texto vamos nos concentrar em polinômios de *uma* variável.

1.2 A densidade assintótica dos números primos

Paralelamente ao que foi feito na Seção 1.1, além de perguntar sobre a existência de números primos podemos também nos perguntar qual a *densidade* dos números primos dentre os números naturais. O primeiro resultado nesse sentido é o Teorema dos Números Primos. Denotando por

$$\pi(x) \doteq \#\{n \in \mathbb{N},\, n \leq x \,:\, n \text{ é primo}\},$$

o Teorema dos Números Primos se enuncia da seguinte forma:

Teorema 1.4 (dos Números Primos)**.** *Para $x \to +\infty$ vale*

$$\pi(x) \sim \frac{x}{\log x}.$$

Podemos dizer que esse Teorema dá a *densidade assintótica* dos números primos dentre os números naturais. De fato, ele é equivalente a

$$\frac{\pi(x)}{x} \sim \frac{1}{\log x}.$$

Agora, o quociente $\pi(n)/n$ pode ser visto como a proporção de números primos menores ou iguais a n (representados pelo valor $\pi(n)$) dentre todos os números naturais menores ou iguais a n (daí a divisão por n, que é a quantidade de números naturais menores ou iguais a n).

Notemos que o Teorema 1.4 inclui o fato de que existem infinitos números primos: como $x/\log x \to +\infty$ quando $x \to +\infty$ temos também que $\pi(x) \to +\infty$ quando $x \to +\infty$.

Também existe uma generalização do Teorema 1.4 que leva em conta o Teorema 1.1: fixemos $a, b \in \mathbb{N}$ e denotemos por

$$\pi_{aX+b}(x) \doteq \#\{n \in \mathbb{N},\, n \leq x \,:\, an + b \text{ é primo}\}.$$

Então o Teorema de Dirichlet diz que se $\operatorname{mdc}(a, b) = 1$, então $\pi_{aX+b}(x) \to +\infty$ quando $x \to +\infty$. A generalização do Teorema 1.4 é o seguinte resultado:

Teorema 1.5. *Se $a, b \in \mathbb{N}$ são relativamente primos, então*

$$\pi_{aX+b}(x) \sim \frac{a}{\varphi(a)} \cdot \frac{x}{\log x}.$$

No enunciado do Teorema 1.5, denotamos por φ a função de Euler, dada por

$$\varphi(n) \doteq \#\big\{m \in \mathbb{N},\, m \leq n \,:\, \operatorname{mdc}(m, n) = 1\big\}.$$

Tem-se também

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right), \tag{1.1}$$

onde o produto é tomado sobre os primos p que dividem n. (Na fórmula (1.1), temos $\varphi(1) = 1$ pois o produto vazio tem valor 1 por definição.) Uma demonstração de (1.1) pode ser encontrada em [Apo76, Seção 2.5].

Em vista da Conjectura 1, podemos definir também

$$\pi_{X^2+1}(x) \doteq \#\{n \in \mathbb{N},\, n \leq x \,:\, n^2 + 1 \text{ é primo}\}.$$

Dessa forma, a Conjectura 1 pergunta se $\pi_{X^2+1}(x)$ é uma função limitada, ou se $\pi_{X^2+1}(x) \to +\infty$ quando $x \to +\infty$. Agora supondo que essa Conjectura é verdadeira, será que podemos obter um resultado como o Teorema 1.5 para a função $\pi_{X^2+1}(x)$?

Usando o método do círculo, Hardy e Littlewood usaram argumentos heurísticos e analíticos para elaborar a seguinte Conjectura:

Conjectura 3 (Hardy-Littlewood)**.** *Para $x \to +\infty$ vale*

$$\pi_{X^2+1}(x) \sim \frac{1}{2} \prod_{p>2} \left(1 - \frac{(-1)^{(p-1)/2}}{p-1}\right) \cdot \frac{x}{\log x}.$$

Podemos fazer o mesmo com relação à Conjectura 2: definimos

$$\pi_{X,X+2} \doteq \#\{n \in \mathbb{N},\, n \leq x \,:\, n \text{ e } n+2 \text{ são primos}\}.$$

Hardy e Littlewood também propuseram uma conjectura análoga à Conjectura 3 para esse caso:

Conjectura 4 (Hardy-Littlewood)**.** *Para $x \to +\infty$ vale*

$$\pi_{X,X+2}(x) \sim 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \cdot \frac{x}{\log^2 x}.$$

É interessante notar que, apesar do polinômio X^2+1 ter grau maior do que 1, o comportamento assintótico da função $\pi_{X^2+1}(x)$ associada é o mesmo da função $\pi_{aX+b}(x)$ (a menos de uma constante multiplicativa; veja o Teorema 1.5). Por outro lado, $\pi_{X,X+2}(x)$ tem um comportamento assintótico diferente, apesar de ambos os polinômios $X, X+2$ serem lineares. No final, o crescimento do polinômio não é muito importante para as funções $\pi_{X^2+1}(x)$ e $\pi_{X,X+2}(x)$ associadas em cada caso. Veremos no Capítulo 2 um argumento heurístico que justifica mais precisamente por quê as Conjecturas 3 e 4 são razoáveis.

Agora, já tentamos generalizar as Conjecturas 1 e 2 através da Questão 1. Poderíamos então tentar generalizar também as Conjecturas 3 e 4: fixemos $f_1(X), \ldots, f_k(X) \in \mathbb{Z}[X]$, e seja $\mathbf{f} \doteq (f_1, \ldots, f_k)$. Definimos

$$\pi_{\mathbf{f}}(x) \doteq \#\{n \in \mathbb{N},\, n \leq x \,:\, f_1(n), \ldots, f_k(n) \text{ são todos primos}\}.$$

Chegamos então ao seguinte problema:

Questão 2. Existe $F(x)$ relativamente simples tal que

$$\pi_{\mathbf{f}}(x) \sim F(x)$$

para $x \to +\infty$? Que função seria essa $F(x)$?

As Questões 1 e 2 estão interligadas, pois para que a Questão 2 faça sentido (não tenha uma resposta trivial), temos de supor que $\pi_{\mathbf{f}}(x) \to +\infty$ quando $x \to +\infty$, o que supõe uma resposta à Questão 1.

Veremos a seguir (Conjectura 5) que Schinzel propôs uma resposta à Questão 1 que dá condições suficientes (conjecturalmente) para que valha $\pi_{\mathbf{f}}(x) \to +\infty$ quando $x \to +\infty$. Supondo essas mesmas condições, Bateman e Horn, usando de argumentos heurísticos de probabilidades, propuseram em [BH62] uma resposta à Questão 2 que ficou conhecida como a Conjectura de Bateman-Horn (a Conjectura 6).

1.3 O Λ-cálculo de Golomb

Em sua tese de doutoramento [Gol56], Golomb propôs um novo método da Teoria Analítica dos Números que ele aplicou à Conjectura dos Primos Gêmeos, e que depois foi chamado Λ-cálculo de Golomb. (As linhas gerais desse método também podem ser encontradas em [Gol70].) Golomb falha em demonstrar a Conjectura 4 por falta de uma única etapa analítica, a saber uma comutação de um limite com uma série infinita.

Mesmo em [Gol70], Golomb nota que seu método poderia ser aplicado a outras conjecturas, mas nesse caso ainda mais problemas técnicos surgem. Um desses problemas foi resolvido por Baier em [Bai02], em que ele generaliza a função ψ de Chebychef para o caso da Conjectura de Bateman-Horn. Com isso, Conrad em [Con03] consegue estender o método de Golomb de modo que ele se aplique à Conjectura de Bateman-Horn completa (e não só a casos especiais, como a Conjectura dos Primos Gêmeos).

Conrad considera em [Con03] como função geradora a série de Dirichlet

$$\sum_{n=1}^{+\infty} \frac{\Lambda\big(f_1(n)\big)\cdots\Lambda\big(f_k(n)\big)}{n^s}.$$

Em [HR05], Hindry e Rivoal seguem basicamente o mesmo método de [Con03], mas usando como função geradora a série de potências

$$\sum_{n=0}^{+\infty} \Lambda\big(f_1(n)\big)\cdots\Lambda\big(f_k(n)\big) z^n.$$

Seguiremos neste texto primeiramente este último método para expor o Λ-cálculo de Golomb, e veremos que todos os problemas técnicos foram resolvidos para a demonstração da Conjectura de Bateman-Horn, a menos da comutação do limite com a série. Somente depois de ver completamente o Λ-cálculo com a série de potências veremos o método aplicado à série de Dirichlet, como variante.

1.4 Este texto

Nosso primeiro objetivo será detalhar as Conjecturas de Schinzel e de Bateman-Horn e suas hipóteses. Provaremos que essas hipóteses são *necessárias* para que haja $\pi_{\mathbf{f}}(x) \to +\infty$, mas não custa lembrar que não se sabe em nenhum caso, à exceção do caso do Teorema de Dirichlet, se essas condições são suficientes para termos $\pi_{\mathbf{f}}(x) \to +\infty$.

Um passo importante para o enunciado da Conjectura 6 é a convergência do produto infinito

$$C(\mathbf{f}) \doteq \prod_p \left[\left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{N_f(p)}{p}\right) \right].$$

Provaremos essa convergência no Capítulo 3 por meio de resultados da Teoria Algébrica dos Números. Algumas definições e resultados básicos dessa teoria serão usados sem referência, mas podem ser encontrados em [Rib01]. Também usaremos o Critério de Kummer, cujos enunciado e demonstração encontram-se no Apêndice A.

No Capítulo 4 faremos uma demonstração do Teorema dos Números Primos por meio do Teorema Tauberiano de Hardy-Littlewood (o Teorema 4.4). Veremos que essa demonstração pode ser

estendida de forma natural ao Λ-cálculo de Golomb.

No Capítulo 5 aplicamos o método de Golomb à Conjectura de Bateman-Horn. Começamos usando o argumento de Baier [Bai02] para estender a função ψ de Chebychef ao caso em questão. Depois provamos a Identidade de Golomb (o Teorema 5.8) e vemos as linhas gerais do método de Golomb. Esbarramos então com um problema de comutação de um limite com uma série (a equação (5.30)), problema esse que continua em aberto e é o *único* passo não justificado do método de Golomb. Supondo provada essa etapa, veremos que esse método de fato prova a conjectura de Bateman-Horn, só que no lugar da constante $C(\mathbf{f})$ conjecturada aparece a série $S(\mathbf{f})$. De fato, provamos no Capítulo 6 que $S(\mathbf{f}) = C(\mathbf{f})$, de modo que o método de Golomb dá a mesma constante que Bateman e Horn conjecturaram usando argumentos heurísticos.

Agora, o problema da comutação do limite com a série também aparece na demonstração do Teorema dos Números Primos no Capítulo 4, e é resolvido com o uso de um teorema abeliano de regularidade. (O Apêndice B é dedicado a teoremas desse tipo.) Faz sentido então perguntar se esse mesmo método não pode ser aplicado para provar a etapa que falta no caso geral.

Golomb prova em [Gol56] que esse método não pode ser usado para resolver o problema no caso da Conjectura dos Primos Gêmeos pois nesse caso o método de somabilidade associado não é *regular* (veja o Apêndice B). No Capítulo 7 faremos uma extensão da demonstração de Golomb para provar que o método não é regular em *nenhum* caso interessante da Conjectura de Bateman-Horn, e assim a comutação do limite com a série não pode ser demonstrada dessa forma. Esse é um resultado inédito, e foi provado pelo autor. Depois faremos uma análise do que pode ser provado usando o Λ-cálculo de Golomb, mesmo à vista do resultado da não-regularidade.

No Capítulo 8 veremos o Teorema de Bateman-Stemmler, como demonstrado por Hindry e Rivoal em [HR05]. (Por sua vez, a demonstração de Hindry e Rivoal é basicamente a original de Bateman e Stemmler feita em [BS62]). Esse é um resultado interessante para a Conjectura de Bateman-Horn, que prova que a função $\pi_{\mathbf{f}}(x)$ não pode ter uma ordem de crescimento maior do que a esperada. Além disso, ele serve de aplicação das técnicas desenvolvidas nos capítulos anteriores.

Finalmente, faremos no Capítulo 9 a variante do Λ-cálculo de Golomb com séries de Dirichlet, como feito por Conrad em [Con03]. Esse método não deixa de ser interessante mesmo em vista do método com a série de potências pois surgem problemas completamente diferentes, e é possível que esses problemas sejam mais tangíveis do que a dificuldade encontrada no estudo da série de potências (assim como também pode ser mais fácil estudar as séries de potências do que as séries de Dirichlet).

Capítulo 2

As conjecturas de Schinzel e de Bateman-Horn

2.1 A Conjectura de Schinzel

Schinzel propôs uma resposta à Questão 1:

Conjectura 5 (Schinzel)**.** *Sejam $f_1(X), \ldots, f_k(X)$ polinômios não-constantes com coeficientes inteiros tais que*

i) $f_1(X), \ldots, f_k(X)$ são irredutíveis sobre $\mathbb{Q}$; e

ii) para todo primo p existe $n \in \mathbb{N}$ tal que $p \nmid f_1(n) \cdot f_2(n) \cdots f_k(n)$.

Então

$$\lim_{x \to +\infty} \pi_{\mathbf{f}}(x) = +\infty.$$

Como a condição ii) é um pouco mais técnica, vamos motivá-la um pouco com alguns exemplos:

Exemplo (Teorema de Dirichlet)*.* No caso de uma família com um único polinômio de grau 1, $f(X) \doteq aX + b$, a condição ii) é equivalente a $\text{mdc}(a, b) = 1$. Essa condição é exatamente a condição do Teorema 1.1 para a existência de infinitos números primos na progressão aritmética $\{an + b : n \in \mathbb{N}\}$.

Exemplo. Consideremos a família de dois polinômios $X, X + 1$. Para todo $n \in \mathbb{N}$ temos que n é par, ou $n + 1$ é par. Logo se $n > 2$ então não podem ser ambos n e $n + 1$ primos. Portanto $\pi_{X,X+1}(x) \not\to +\infty$. Agora, a condição "$n$ é par, ou $n + 1$ é par, para todo $n \in \mathbb{N}$", escrita de outra forma, é $2 \mid n(n + 1)$, para todo $n \in \mathbb{N}$. Assim vemos que a família $X, X + 1$ não satisfaz a condição ii) da Conjectura 5.

Notemos que as condições da Conjectura 5 são *necessárias* para termos $\pi_{\mathbf{f}}(x) \to +\infty$. De fato, se tivéssemos algum $f_j(X)$ redutível sobre $\mathbb{Q}$, então existiriam polinômios $g(X), h(X) \in \mathbb{Z}[X]$ não-constantes tais que $f_j(X) = g(X) \cdot h(X)$. Seja então $N > 0$ tal que

$$\text{se } n \geq N, \quad \text{então} \quad |g(n)| > 1, \text{ e } |h(n)| > 1.$$

Assim se $n \geq N$ temos que $f_j(n)$ não é primo, pois então $f_j(n) = g(n)h(n)$, com $g(n), h(n) \in \mathbb{Z}$ diferentes de ± 1. Assim, se $n \geq N$, nunca temos $f_1(n)$, $\ldots$, $f_k(n)$ simultaneamente primos, e portanto $\pi_{\mathbf{f}}(x) \leq N$ para todo $x \geq 1$. Isto é; $\pi_{\mathbf{f}}(x) \not\to +\infty$.

Suponhamos agora que existe um primo p tal que $p \mid f_1(n) \cdot f_2(n) \cdots f_k(n)$ para todo $n \in \mathbb{N}$. Como $|g(n)| \to +\infty$ quando $n \to +\infty$ para todo polinômio $g(X)$ não-constante, existe $N > 0$ tal que

$$\text{se } n \geq N, \quad \text{então} \quad |f_1(n)| > p, |f_2(n)| > p, \ldots, |f_k(n)| > p. \tag{2.1}$$

Seja $n \geq N$. Se tivéssemos $f_1(n), \dots, f_k(n)$ simultaneamente primos, como temos $p \mid f_1(n) \cdot f_2(n) \cdots f_k(n)$ por hipótese, então para algum $j \in \{1, \dots, k\}$ teríamos $f_j(n) = p$, absurdo, pois por (2.1) temos $|f_j(n)| > p$. Dessa forma $f_1(n), \dots, f_k(n)$ não são simultaneamente primos para $n \geq N$, e $\pi_{\mathbf{f}}(x) \not\to +\infty$.

Notemos também que ii) é equivalente a

ii') para todo primo p existem infinitos $n \in \mathbb{N}$ tais que $p \nmid f_1(n) \cdots f_k(n)$.

De fato, se $n \in \mathbb{N}$ é tal que $p \nmid f_1(n) \cdots f_k(n)$, então para todo $m \in \mathbb{N}$ temos

$$f_1(n + mp) \cdots f_k(n + mp) \equiv f_1(n) \cdots f_k(n) \not\equiv 0 \pmod{p},$$

isto é; $p \nmid f_1(n + mp) \cdots f_k(n + mp)$.

2.2 Famílias apropriadas

Neste texto, vamos estudar uma tentativa de demonstração da Conjectura 5, mas vamos antes colocar mais hipóteses sobre os polinômios $f_1(X), \dots, f_k(X)$ para que o estudo se torne mais fácil:

Definição. Sejam $f_1(X), \dots, f_k(X)$ polinômios não-constantes com coeficientes inteiros. Diremos que $\mathbf{f} \doteq (f_1, \dots, f_k)$ é uma família *apropriada* se esses polinômios satisfazem as seguintes propriedades:

i) $f_1(X), \dots, f_k(X)$ são todos distintos;

ii) $f_1(X), \dots, f_k(X)$ são irredutíveis sobre $\mathbb{Q}$;

iii) para todo primo p existe $n \in \mathbb{N}$ tal que $p \nmid f_1(n) \cdot f_2(n) \cdots f_k(n)$;

iv) para todo $n \geq 0$, temos $f_1(n) > 1$, $f_2(n) > 1$, $\dots$, $f_k(n) > 1$; e

v) $f_1(X), \dots, f_k(X)$ são estritamente crescentes em $(-1, +\infty)$.

As propriedades iv) e v) não são de fato restritivas. Se $f_1(X), \dots, f_k(X)$ são polinômios que satisfazem as propriedades i) a iii), podemos considerar ao invés de $\mathbf{f}$ uma família $\mathbf{g} \doteq (g_1, \dots, g_k)$ em que

$$g_1(X) \doteq \pm f_1(X + c), \quad g_2(X) \doteq \pm f_2(X + c), \quad \dots, \quad g_k(X) \doteq \pm f_k(X + c), \tag{2.2}$$

em que tomamos os sinais $\pm$ e o inteiro c de tal modo que $g_j(n) > 1$ para todo $n \in \mathbb{N}$ e $g_j(X)$ é estritamente crescente em $(-1, +\infty)$, para todo $j \in \{1, \dots, k\}$. Podemos também remover alguns polinômios da família $\mathbf{g}$ para evitar repetições (e assim $\mathbf{g}$ satisfaz i)).

Dessa forma a família $\mathbf{g}$ é apropriada, e como todos os polinômios de $\mathbf{g}$ são translações de polinômios de $\mathbf{f}$ (no sentido acima), a diferença $\pi_{\mathbf{f}}(x) - \pi_{\mathbf{g}}(x)$ é limitada. Portanto o comportamento assintótico da função $\pi_{\mathbf{f}}(x)$ é o mesmo comportamento da função $\pi_{\mathbf{g}}(x)$, no seguinte sentido: $\pi_{\mathbf{f}}(x) \to +\infty$ se, e somente se $\pi_{\mathbf{g}}(x) \to +\infty$, e nesse caso $\pi_{\mathbf{f}}(x) \sim \pi_{\mathbf{g}}(x)$.

Definição. Dado $g(X) \in \mathbb{Z}[X]$ definimos para $d \in \mathbb{N}$, $d \geq 2$,

$$N_g(d) \doteq \#\big\{n \in \mathbb{N},\, n \leq d \,:\, g(n) \equiv 0 \pmod{d}\big\}.$$

Colocamos também $N_g(1) \doteq 1$ pois assim a função $d \mapsto N_g(d)$ se torna multiplicativa (Lema 3.2).

Fixemos $f_1(X), \dots, f_k(X)$ uma família de polinômios apropriada para o resto desta Seção.
Definindo $f(X) \doteq f_1(X) \cdot f_2(X) \cdots f_k(X)$, podemos substituir a condição iii) por

iii') para todo primo p, vale $N_f(p) < p$.

Provemos que iii) e iii') são equivalentes.

iii) $\Rightarrow$ iii'): Suponhamos que existe um número primo p tal que $N_f(p) = p$. Seja $n \in \mathbb{N}$. Seja $m \in \mathbb{N}$, $m \leq p$, tal que $n \equiv m \pmod p$. Então $N_f(p) = p$ implica que $f(m) \equiv 0 \pmod p$. Como $n \equiv m \pmod p$ temos

$$f(n) \equiv f(m) \equiv 0 \pmod p .$$

Isto é; $p \mid f(n)$. Como $n \in \mathbb{N}$ é arbitrário temos que não vale iii).

iii') $\Rightarrow$ iii): Suponhamos que existe um número primo p tal que $p \mid f(n)$ para todo $n \in \mathbb{N}$. Então $f(n) \equiv 0 \pmod p$ para todo $n \in \mathbb{N}$, e assim $N_f(p) = p$.

Observação. É importante notar que $f(n) \equiv 0 \pmod p$ pode ter no máximo $h \doteq \operatorname{gr} f$ soluções para $n \in \mathbb{N}$, $n \leq p$. De fato, isso ocorre pois essas soluções são as raízes do polinômio correspondente a $f(X)$ em $\mathbb{Z}/p\mathbb{Z}$, que é um corpo quando p é primo.

Portanto para todo p primo vale $N_f(p) \leq h$. Assim se $p > h$ temos $N_f(p) < p$ de modo que a condição iii') está automaticamente verificada para primos maiores do que h. Esse fato torna verificar iii') mais fácil, pois basta testar iii') para os primos de 2 a h; uma quantidade finita de testes.

Um Lema bastante simples e útil é o seguinte:

Lema 2.1. *Dados $i, j \in \{1, \ldots, k\}$ distintos, tem-se (em $\mathbb{Q}[X]$)*

$$\operatorname{mdc}(f_i, f_j) = 1.$$

Demonstração. Como $\mathbf{f} = (f_1, \ldots, f_k)$ é uma família apropriada, temos que $f_i(X)$ e $f_j(X)$ são irredutíveis, logo $\operatorname{mdc}(f_i, f_j) = 1$ ou $\operatorname{mdc}(f_i, f_j) = f_i$ no caso de serem $f_i(X)$ e $f_j(X)$ polinômios associados.

Se fosse $f_i(X)$ associado a $f_j(X)$, teríamos $f_i(X) = (a/b)f_j(X)$ com $a, b \in \mathbb{Z}$ primos entre si, $b \neq 0$. Temos $a/b \neq \pm 1$ pois da definição de família apropriada temos $f_i(X) \neq \pm f_j(X)$.

Se $b \neq \pm 1$, seja p primo tal que $p \mid b$. Temos que $(a/b)f_j(X) = f_i(X) \in \mathbb{Z}[X]$, de modo que p divide todos os coeficientes de $af_j(X)$. Mas sendo a, b relativamente primos, de fato p divide todos os coeficientes de $f_j(X)$. Mas assim $p \mid f_j(n)$ para todo $n \in \mathbb{N}$ e $N_f(p) = p$, absurdo.

Se $b = \pm 1$, temos que $a \neq \pm 1$ (pois $a/b \neq \pm 1$). Seja então p divisor primo de a. Logo p divide $\pm af_j(n) = f_i(n)$ para todo $n \in \mathbb{N}$ de modo que novamente $N_f(p) = p$, absurdo. Portanto não podemos ter $f_i(X)$ associado a $f_j(X)$. □

2.3 A Conjectura de Bateman-Horn

Usando argumentos heurísticos e de probabilidade, Bateman e Horn propuseram em [BH62] uma resposta à Questão 2 considerando que as condições razoáveis que devemos colocar sobre os polinômios para termos $\pi_{\mathbf{f}}(x) \to +\infty$ são aquelas da Conjectura 5:

Conjectura 6 (Bateman-Horn)**.** *Seja $f_1(X), \ldots, f_k(X)$ uma família apropriada de polinômios. Então*

$$\pi_{\mathbf{f}}(x) \sim \frac{C(\mathbf{f})}{h_1 h_2 \cdots h_k} \cdot \frac{x}{\log^k x},$$

em que $h_1, \ldots, h_k$ são os graus dos polinômios $f_1(X), \ldots, f_k(X)$ respectivamente, e

$$C(\mathbf{f}) \doteq \prod_p \left[\left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{N_f(p)}{p}\right) \right],$$

em que o produto é tomado sobre todos os p primos.

Ainda precisamos provar a convergência do produto $C(\mathbf{f})$, o que faremos a seguir, no Capítulo 3. Por enquanto, notemos somente que como $N_f(p) < p$ para todo primo p, nenhum fator do produto

$C(\mathbf{f})$ é nulo, e assim $C(\mathbf{f}) \neq 0$. Em particular, a Conjectura 6 implica que $\pi_{\mathbf{f}}(x) \to +\infty$ se $\mathbf{f}$ é uma família apropriada.

Vamos aqui reproduzir um argumento heurístico semelhante ao de Bateman e Horn para justificar o enunciado da Conjectura 6. Não seguiremos o mesmo argumento do artigo original [BH62] pois é preferível detalhar melhor o surgimento da constante $C(\mathbf{f})$. Vamos descrever uma variante do argumento com que Tao justifica a Conjectura dos Primos Gêmeos assintótica (a Conjectura 4) em [Tao09, Seção 3.1].

Começamos com o caso de uma família apropriada de um único polinômio $f(X)$. Fixamos um inteiro $N > 0$ suficientemente grande. A base do argumento heurístico para a Conjectura 6 é ver a razão $\pi_f(N)/N$ como uma probabilidade. De fato, dados os N primeiros valores do polinômio $f(X)$:

$$f(1), \quad f(2), \quad f(3), \quad \ldots, \quad f(N), \tag{2.3}$$

a função $\pi_f(N)$ nos diz quantos desses valores são números primos. Assim se escolhermos um inteiro dentre os de (2.3) aleatoriamente, a probabilidade dele ser um número primo é exatamente $\pi_f(N)/N$. Escrevendo simbolicamente, temos que

$$\mathrm{P}\left(\{n \leq N \,:\, f(n) \text{ é primo}\}\right) = \frac{\pi_f(N)}{N}. \tag{2.4}$$

Em (2.4), o que escrevemos foi a probabilidade de se escolher um $n \leq N$ tal que $f(n)$ é primo. Essa probabilidade é igual à probabilidade que queríamos, de se escolher um número primo dentre os valores de (2.3). A diferença é que o modo como está escrito em (2.4) é mais prático para as contas que faremos a seguir.

Vamos tentar calcular a probabilidade de (2.4) de outra maneira.

Se $M > 0$ é grande, temos analogamente (caso $f(X) = X$) que, escolhendo um $m \leq M$ aleatoriamente, a probabilidade de m ser primo é $\pi(M)/M$, em que $\pi(x) = \#\{n \leq x \,:\, n \text{ é primo}\}$. Pelo Teorema dos Números Primos, temos uma expressão assintótica para a razão $\pi(M)/M$:

$$\mathrm{P}\left(\{m \leq M \,:\, m \text{ é primo}\}\right) = \frac{\pi(M)}{M} = \frac{1 + o(1)}{\log M}. \tag{2.5}$$

É importante notar, e usaremos a seguir que como $f(X)$ é, por hipótese, estritamente crescente em $\mathbb{N}$, temos que os valores de (2.3) estão todos entre 1 e $f(N)$.

Agora vamos tentar seguir o modo mais ingênuo de pensar, que é ignorar o fato de que os valores de (2.3) vêm de um polinômio. Vamos assim supor que um valor $m = f(n)$ de (2.3) não passa de um inteiro *qualquer* entre 1 e $M \doteq f(N)$. Mas a equação (2.5) nos dá a probabilidade de um inteiro qualquer m entre 1 e M ser primo, que é $\pi(M)/M$. Isso sugere que a probabilidade de $f(n)$ ser primo é $\pi(f(N))/f(N)$. Ou seja,

$$\mathrm{P}\left(\{n \leq N \,:\, f(n) \text{ é primo}\}\right) = \frac{\pi\big(f(N)\big)}{f(N)} = \frac{1 + o(1)}{\log f(N)} = \frac{1 + o(1)}{h \log N},$$

em que h é o grau do polinômio $f(X)$. Junto com (2.4), temos que

$$\frac{\pi_f(N)}{N} = \frac{1 + o(1)}{h \log N}. \tag{2.6}$$

O problema é que esse argumento já parece falho quando substituímos, por exemplo, $f(X) = 2X + 1$, pois sabemos do Teorema 1.5 que vale

$$\frac{\pi_{2X+1}(N)}{N} = \frac{2 + o(1)}{\log N},$$

mas essa equação não condiz com (2.6) quando $N \to +\infty$. O problema é que, ao propor a equação (2.6), estamos considerando os N primeiros valores do polinômio $f(X) = 2X + 1$ como

inteiros quaisquer entre 1 e $f(N) = 2N + 1$. Mas os N primeiros valores

$$3, \quad 5, \quad 7, \quad 9, \quad \ldots, \quad 2N + 1$$

do polinômio $f(X) = 2X + 1$ não podem ser considerados como inteiros quaisquer entre 1 e $2N + 1$, pois são todos números ímpares, e a paridade de um número é muito relevante para sabermos se ele é primo ou não, já que não existem números primos pares (exceto pelo número 2).

Voltemos então ao caso de um polinômio apropriado qualquer $f(X)$. Em vista do exemplo anterior com o polinômio $2X + 1$, vamos tentar consertar o argumento acima que levou à equação (2.6) levando em conta a paridade dos valores (2.3). Gostaríamos então primeiramente de saber quais valores de (2.3) são ímpares, e quais são pares.

Na linguagem de congruências, dado $n \leq N$ gostaríamos de saber quando $f(n) \equiv 0 \pmod 2$, e quando $f(n) \equiv 1 \pmod 2$. Agora, se $n \equiv m \pmod 2$, então $f(n) \equiv f(m) \pmod 2$. Assim se $n \equiv 1 \pmod 2$, então $f(n) \equiv f(1) \pmod 2$, de modo que os valores

$$f(1), \quad f(3), \quad f(5), \quad f(7), \quad f(9), \quad \ldots \tag{2.7}$$

têm todos a mesma paridade, que é a paridade de $f(1)$; se $f(1)$ é par, então todos os elementos de (2.7) são pares, e se $f(1)$ é ímpar, então todos os elementos de (2.7) são ímpares. Analogamente, temos que os inteiros $f(2)$, $f(4)$, $f(6)$, ..., também têm todos a mesma paridade, que é a paridade de $f(2)$.

Assim determinamos quando $f(n)$ é par ou ímpar, basta ver se $n \equiv 1 \pmod 2$, e nesse caso a paridade de $f(n)$ é a mesma de $f(1)$; ou se $n \equiv 2 \pmod 2$, e então a paridade é a mesma de $f(2)$. Para tratar desses dois casos simultaneamente, fixemos $i \in \{1, 2\}$, e analisemos o que acontece quando $n \equiv i \pmod 2$. Queremos novamente calcular a probabilidade de $f(n)$ ser primo, com $n \leq N$, mas agora nos restringimos ao caso em que $n \equiv i \pmod 2$. Isto é; vamos calcular a probabilidade *condicional*

$$\mathrm{P}\big(f(n) \text{ é primo} \mid n \equiv i \pmod 2\big) \doteq \mathrm{P}\big(\{n \leq N : f(n) \text{ é primo}\} \mid \{n \leq N : n \equiv i \pmod 2\}\big),$$

isto é; a probabilidade de escolhermos $n \leq N$ tal que $f(n)$ é primo, dado que $n \equiv i \pmod 2$. Calculando essas probabilidades para $i = 1, 2$, podemos obter de volta a probabilidade que queríamos originalmente usando a lei da probabilidade total:

$$\mathrm{P}\big(f(n) \text{ é primo}\big) = \sum_{i=1}^{2} \mathrm{P}\big(f(n) \text{ é primo} \mid n \equiv i \pmod 2\big) \cdot \mathrm{P}\big(n \equiv i \pmod 2\big). \tag{2.8}$$

(Aqui estamos cometendo um abuso de notação para encurtar a escrita, mas basta lembrar que o que estamos escolhendo aleatoriamente é um natural $n \leq N$, e N é um número grande e fixado.) Podemos calcular explicitamente a probabilidade $\mathrm{P}(\{n \leq N : n \equiv i \pmod 2\})$; por exemplo, para $i = 2$ temos

$$\mathrm{P}\big(n \equiv 2 \pmod 2\big) = \begin{cases} (N-1)/2N & \text{se } N \text{ é ímpar} \\ 1/2 & \text{se } N \text{ é par} \end{cases}.$$

Em particular, vale $\mathrm{P}(n \equiv 2 \pmod 2) = (1 + o(1))/2$. O mesmo vale quando $i = 1$, e assim substituindo em (2.8) temos

$$\mathrm{P}\big(f(n) \text{ é primo}\big) = \sum_{i=1}^{2} \mathrm{P}\big(f(n) \text{ é primo} \mid n \equiv i \pmod 2\big) \cdot \frac{1 + o(1)}{2}. \tag{2.9}$$

Calculemos então a probabilidade $\mathrm{P}(f(n) \text{ é primo} \mid n \equiv i \pmod 2)$. Lembrando que quando $n \equiv i \pmod 2$, temos $f(n) \equiv f(i) \pmod 2$, logo basta ver o que acontece quando $f(i)$ é par, e quando $f(i)$ é ímpar.

a) $f(i) \equiv 0 \pmod 2$: nesse caso, para todo $n \leq N$, $n \equiv i \pmod 2$, temos que $f(n)$ é par. Assim

$f(n)$ só pode ser um número primo se $f(n) = 2$. Mas como $f(X)$ é estritamente crescente em $\mathbb{N}$, a igualdade $f(n) = 2$ pode ocorrer no máximo uma vez em $\mathbb{N}$. Se a igualdade $f(n) = 2$ não ocorre, então simplesmente

$$\mathrm{P}\left(f(n) \text{ é primo} \mid n \equiv i \pmod 2\right) = 0.$$

Se a igualdade $f(n) = 2$ ocorre uma vez para $n \in \mathbb{N}$, digamos $f(n_0) = 2$, então

$$\mathrm{P}\left(f(n) \text{ é primo} \mid n \equiv i \pmod 2\right) \leq \mathrm{P}\left(\{n \leq N \,:\, f(n) = 2\}\right) = \mathrm{P}\left(\{n \leq N \,:\, n = n_0\}\right) \leq \frac{1}{N}.$$

De qualquer forma, ocorrendo a igualdade $f(n) = 2$ para $n \in \mathbb{N}$ ou não, é sempre verdade que vale $\mathrm{P}(f(n) \text{ é primo} \mid n \equiv i \pmod 2) = O(1/N)$. Assim, colocamos

$$\mathrm{P}\left(f(n) \text{ é primo} \mid n \equiv i \pmod 2\right) = \frac{0 + o(1)}{h \log N}. \tag{2.10}$$

Poderíamos ter sido mais precisos no cálculo dessa probabilidade, mas preferimos a equação (2.10) para ficar com uma fórmula mais parecida com a do caso seguinte.

b) $f(i) \equiv 1 \pmod 2$: Seja N_1 o maior inteiro $n \leq N$ tal que $n \equiv i \pmod 2$. Queremos então calcular a probabilidade de escolhermos um número primo dentre os valores

$$f(i), \quad f(i+2), \quad f(i+4), \quad f(i+6), \quad \ldots, \quad f(N_1), \tag{2.11}$$

que são todos números ímpares entre 1 e $f(N)$. Vamos agora fazer a mesma hipótese "ingênua" que fizemos anteriormente, ignorando o fato de que os valores (2.11) vêm do polinômio $f(X)$, mas com um refinamento: agora levaremos em conta que todos esses valores são números ímpares. Vamos assim supor que um valor $m = f(n)$ de (2.11) não passa de um inteiro *ímpar qualquer* entre 1 e $M \doteq f(N)$. Logo a probabilidade de um valor de (2.11) ser primo é a mesma de um inteiro ímpar qualquer entre 1 e M ser primo. Simbolicamente, isto é

$$\mathrm{P}\left(f(n) \text{ é primo} \mid n \equiv i \pmod 2\right) = \mathrm{P}\left(\{m \leq M,\, m \text{ ímpar} \,:\, m \text{ é primo}\}\right). \tag{2.12}$$

Vamos então calcular a probabilidade da direita de (2.12).

Seja $M_1 \doteq 2l - 1$ o maior número ímpar menor ou igual a M. Então a probabilidade $\mathrm{P}(\{m \leq M,\, m \text{ ímpar} \,:\, m \text{ é primo}\})$ é a chance de escolhermos um número primo dentre os inteiros

$$1, \quad 3, \quad 5, \quad 7, \quad \ldots, \quad M_1. \tag{2.13}$$

Escrevendo esses números de outra forma, temos

$$2 \cdot 1 - 1, \quad 2 \cdot 2 - 1, \quad 2 \cdot 3 - 1, \quad 2 \cdot 4 - 1, \quad \ldots, \quad 2l - 1. \tag{2.14}$$

Isto é; os inteiros de (2.13) são simplesmente os l primeiros valores do polinômio $2X - 1$. Então temos que a probabilidade de escolhermos um número primo dentre os elementos de (2.14) é $\pi_{2X-1}(l)/l$. Dessa forma,

$$\mathrm{P}\left(\{m \leq M,\, m \text{ ímpar} \,:\, m \text{ é primo}\}\right) = \frac{\pi_{2X-1}(l)}{l} = \frac{2}{\varphi(2)} \cdot \frac{1 + o(1)}{\log l}. \tag{2.15}$$

Em (2.15) usamos $\pi_{2X-1}(x) \sim (2/\varphi(2))x/\log x$, que segue do Teorema 1.5 aplicando uma translação no polinômio $2X + 1$. Se M é par temos $l = M/2$, logo segue de (2.15) que

$$\mathrm{P}\left(\{m \leq M,\, m \text{ ímpar} \,:\, m \text{ é primo}\}\right) = \frac{2}{\varphi(2)} \cdot \frac{1 + o(1)}{\log M - \log 2} = 2 \cdot \frac{1 + o(1)}{\log M}.$$

Se M é ímpar, temos $l = (M + 1)/2$ e analogamente chegamos à mesma fórmula. Isto é; vale em

geral que

$$\mathrm{P}\left(\{m \leq M,\, m \text{ ímpar} : m \text{ é primo}\}\right) = \frac{2+o(1)}{\log M}.$$

Substituindo em (2.12) temos finalmente

$$\mathrm{P}\left(f(n) \text{ é primo} \mid n \equiv i \pmod 2\right) = \frac{2+o(1)}{\log M} = \frac{2+o(1)}{\log f(N)} = \frac{2+o(1)}{h\log N}.$$

Em resumo, obtivemos

$$\mathrm{P}\left(f(n) \text{ é primo} \mid n \equiv i \pmod 2\right) = \frac{a_i+o(1)}{h\log N}, \tag{2.16}$$

onde $a_i \doteq 0$ se $f(i) \equiv 0 \pmod 2$, e $a_i \doteq 2$ se $f(i) \equiv 1 \pmod 2$. Substituindo esses valores em (2.9) obtemos

$$\mathrm{P}\left(f(n) \text{ é primo}\right) = \sum_{i=1}^{2} \frac{a_i+o(1)}{h\log N} \cdot \frac{1+o(1)}{2} = \sum_{i=1}^{2} \frac{a_i+o(1)}{2h\log N}.$$

Vamos organizar essa soma (de apenas dois fatores) de outra forma, separando a soma de acordo com os valores de a_i:

$$\begin{aligned}\mathrm{P}\left(f(n) \text{ é primo}\right) &= \sum_{i\in\{1,2\},\, a_i=0} \frac{0+o(1)}{2h\log N} + \sum_{i\in\{1,2\},\, a_i=2} \frac{2+o(1)}{2h\log N} \\ &= n_0 \cdot \frac{0+o(1)}{2h\log N} + n_1 \cdot \frac{2+o(1)}{2h\log N} = n_1 \cdot \frac{2+o(1)}{2h\log N}\end{aligned} \tag{2.17}$$

em que n_0 é o número de elementos $i \in \{1,2\}$ tais que $a_i = 0$, ou seja; $f(i) \equiv 0 \pmod 2$, e n_1 é o número de elementos $i \in \{1,2\}$ tais que $a_i = 2$, ou seja; $f(i) \equiv 1 \pmod 2$. Agora, $n_0 + n_1 = 2$, e lembrando a definição da função N_f, de fato temos $n_0 = N_f(2)$. Assim $n_1 = 2 - N_f(2) > 0$, e portanto segue de (2.17) que

$$\mathrm{P}\left(f(n) \text{ é primo}\right) = \frac{2-N_f(2)}{2} \cdot \frac{2+o(1)}{h\log N} = \left(1-\frac{N_f(2)}{2}\right)\cdot\left(1-\frac{1}{2}\right)^{-1} \cdot \frac{1+o(1)}{h\log N}.$$

Chegamos assim à conclusão de que (lembrando de (2.4)) vale

$$\frac{\pi_f(N)}{N} = \left(1-\frac{N_f(2)}{2}\right)\cdot\left(1-\frac{1}{2}\right)^{-1} \cdot \frac{1+o(1)}{h\log N}. \tag{2.18}$$

Assim conseguimos consertar o problema da paridade dos valores de (2.3); agora se substituirmos $f(X) = 2X + 1$, a equação (2.18) nos dá o resultado esperado pelo Teorema de Dirichlet assintótico. Mas ainda temos outros problemas com essa equação. No argumento anterior, levamos em conta apenas a paridade dos valores de $f(X)$, isto é; analisamos como estão distribuídos os valores de $f(X)$ nas classes de congruência módulo 2. O problema é que não levamos em consideração as classes de congruência módulo 3, que são tão importantes quanto as classes módulo 2 (da mesma forma como antes, não existem números primos congruentes a 0 módulo 3, exceto pelo próprio número 3). Por exemplo, se substituirmos $f(X) = 3X + 1$, a equação (2.18) não dá o comportamento correto quando $N \to +\infty$, em vista do Teorema 1.5. Precisamos então começar novamente o argumento levando em conta as classes de congruência módulo 2 e módulo 3. Consideraremos ambas as classes simultaneamente, simplesmente analisando as congruências módulo $6 = 2 \cdot 3$.

A partir daqui deve estar claro que também precisaríamos analisar todas as classes de congruência módulo p, para todo número primo p. Faremos apenas a análise levando em conta $p = 2$ e $p = 3$ para ilustrar as técnicas usadas, e deixaremos indicado depois o que acontece quando se

considera simultaneamente uma quantidade finita de números primos.

Novamente temos um polinômio apropriado $f(X)$ e um inteiro $N > 0$ suficientemente grande. Assim como no caso anterior, temos que $n \equiv m \pmod 6$ implica $f(n) \equiv f(m) \pmod 6$. Logo, para determinar em que classe de congruência módulo 6 um valor $f(n)$, basta determinar o inteiro $i \in \{1, 2, \ldots, 6\}$ tal que $n \equiv i \pmod 6$, e então $f(n)$ estará na mesma classe de $f(i)$. Assim (também como no caso anterior) vamos calcular a probabilidade $\mathrm{P}(f(n)$ é primo$)$ usando probabilidades condicionais:

$$\mathrm{P}\big(f(n) \text{ é primo}\big) = \sum_{i=1}^{6} \mathrm{P}\big(f(n) \text{ é primo} \mid n \equiv i \pmod 6\big) \cdot \mathrm{P}\big(n \equiv i \pmod 6\big).$$

De modo análogo ao que fizemos anteriormente, vemos que $\mathrm{P}(n \equiv i \pmod 6) = (1 + o(1))/6$ para todo $i \in \{1, \ldots, 6\}$, logo

$$\mathrm{P}\big(f(n) \text{ é primo}\big) = \sum_{i=1}^{6} \mathrm{P}\big(f(n) \text{ é primo} \mid n \equiv i \pmod 6\big) \cdot \frac{1 + o(1)}{6}. \tag{2.19}$$

Resta então calcular as probabilidades $\mathrm{P}(f(n)$ é primo $\mid n \equiv i \pmod 6)$. Assim como no caso anterior, basta considerar cada possibilidade para $f(i)$ nas classes de congruência módulo 6:

a) $f(i) \equiv b \pmod 6$, onde $b \in \{0, 2, 3, 4\}$: Em todos esses casos $b = 0, 2, 3, 4$, temos que os valores

$$f(i), \quad f(i + 6), \quad f(i + 2 \cdot 6), \quad f(i + 3 \cdot 6), \quad \ldots$$

estão todos na progressão aritmética $\{6n + b : n \geq 0\} = \{m \in \mathbb{N} : m \equiv b \pmod 6\}$. Mas como $\mathrm{mdc}(6, b) > 1$, a progressão $\{6n+b : n \geq 0\}$ só passa por uma quantidade finita de números primos. Portanto, assim como no item a) do caso anterior temos que $\mathrm{P}(f(n)$ é primo $\mid n \equiv i \pmod 6) = O(1/N)$. Em particular,

$$\mathrm{P}\big(f(n) \text{ é primo} \mid n \equiv i \pmod 6\big) = \frac{0 + o(1)}{h \log N}. \tag{2.20}$$

b) $f(i) \equiv b \pmod 6$, onde $b \in \{1, 5\}$: Seja N_b o maior valor congruente a b módulo 6, menor ou igual a N. Assim queremos calcular a probabilidade de obtermos um número primo, escolhendo um número aleatoriamente dentre os valores

$$f(i), \quad f(i + 6), \quad f(i + 2 \cdot 6), \quad f(i + 3 \cdot 6), \quad \ldots, \quad f(N_b), \tag{2.21}$$

que são todos inteiros entre 1 e $f(N)$, congruentes a b módulo 6. Aqui fazemos novamente uma hipótese "ingênua" aprimorada; vamos ignorar que os valores (2.21) vêm de um polinômio, mas vamos nos lembrar que são todos congruentes a b módulo 6. Assim vamos supor que um valor $m = f(n)$ de (2.21) é um inteiro qualquer entre 1 e $M \doteq f(N)$, congruente a b módulo 6. Logo a probabilidade de um inteiro de (2.21) ser primo é a mesma de um inteiro qualquer entre 1 e M, congruente a b módulo 6, ser primo. Isto é;

$$\mathrm{P}\big(f(n) \text{ é primo} \mid n \equiv i \pmod 6\big) = \mathrm{P}\big(\{m \leq M,\, m \equiv b \pmod 6 \,:\, m \text{ é primo}\}\big). \tag{2.22}$$

Calculando a probabilidade à direita de (2.22) como fizemos no item b) do caso anterior (mas agora aparece a progressão aritmética $\{6n + b : n \geq 0\}$, que passa por infinitos números primos pois $\mathrm{mdc}(6, b) = 1$), temos que

$$\mathrm{P}\big(f(n) \text{ é primo} \mid n \equiv i \pmod 6\big) = \frac{6}{\varphi(6)} \cdot \frac{1 + o(1)}{\log M} = \frac{6}{\varphi(6)} \cdot \frac{1 + o(1)}{h \log N}.$$

Em resumo, temos

$$\mathrm{P}\big(f(n) \text{ é primo} \mid n \equiv i \pmod 6\big) = \frac{6}{\varphi(6)} \cdot \frac{a_i + o(1)}{h \log N},$$

onde $a_i \doteq 0$ se $\mathrm{mdc}(6, f(i)) > 1$, e $a_i = 1$ se $\mathrm{mdc}(6, f(i)) = 1$. Substituindo em (2.19) temos

$$\mathrm{P}\big(f(n) \text{ é primo}\big) = \sum_{i=1}^{6} \frac{6}{\varphi(6)} \cdot \frac{a_i + o(1)}{h \log N} \cdot \frac{1 + o(1)}{6} = \sum_{i=1}^{6} \frac{6}{\varphi(6)} \cdot \frac{a_i + o(1)}{6h \log N} \tag{2.23}$$

Vamos organizar a soma em (2.23) de outra forma:

$$\begin{aligned} \mathrm{P}\big(f(n) \text{ é primo}\big) &= \sum_{i \in \{1,\ldots,6\},\, a_i = 0} \frac{6}{\varphi(6)} \cdot \frac{0 + o(1)}{6h \log N} + \sum_{i \in \{1,\ldots,6\},\, a_i = 1} \frac{6}{\varphi(6)} \cdot \frac{1 + o(1)}{6h \log N} \\ &= n_0 \cdot \frac{6}{\varphi(6)} \cdot \frac{0 + o(1)}{6h \log N} + n_1 \cdot \frac{6}{\varphi(6)} \cdot \frac{1 + o(1)}{6h \log N} = n_1 \cdot \frac{(6/\varphi(6)) + o(1)}{6h \log N}, \end{aligned} \tag{2.24}$$

em que n_0 é o número de elementos $i \in \{1, 2, \ldots, 6\}$ tais que $a_i = 0$, isto é; $\mathrm{mdc}(6, f(i)) > 1$, e n_1 é o número de elementos $i \in \{1, 2, \ldots, 6\}$ tais que $a_i = 1$, isto é; $\mathrm{mdc}(6, f(i)) = 1$. Agora, uma outra forma de escrever n_1 é

$$n_1 = \#\big\{i \leq 6 \,:\, f(i) \not\equiv 0 \pmod 2 \text{ e } f(i) \not\equiv 0 \pmod 3\big\}.$$

Aplicando o Teorema Chinês dos Restos, vemos que

$$n_1 = \#\big\{i \leq 2 \,:\, f(i) \not\equiv 0 \pmod 2\big\} \cdot \#\big\{i \leq 3 \,:\, f(i) \not\equiv 0 \pmod 3\big\} = \big(2 - N_f(2)\big) \cdot \big(3 - N_f(3)\big).$$

Substituindo em (2.24) temos que

$$\mathrm{P}\big(f(n) \text{ é primo}\big) = C_6 \cdot \frac{1 + o(1)}{h \log N}, \tag{2.25}$$

em que

$$C_6 \doteq \frac{\big(2 - N_f(2)\big) \cdot \big(3 - N_f(3)\big)}{6} \cdot \frac{6}{\varphi(6)}. \tag{2.26}$$

Podemos deixar a expressão de C_6 um pouco mais familiar; como a função φ é multiplicativa, temos $\varphi(6) = \varphi(2) \cdot \varphi(3) = (2-1) \cdot (3-1)$. Assim,

$$\frac{6}{\varphi(6)} = \frac{2 \cdot 3}{(2-1) \cdot (3-1)} = \frac{1}{(1 - 1/2) \cdot (1 - 1/3)}.$$

Substituindo em (2.26) temos

$$C_6 = \prod_{p=2,3} \left(1 - \frac{N_f(p)}{p}\right) \cdot \left(1 - \frac{1}{p}\right)^{-1}. \tag{2.27}$$

Concluímos finalmente de (2.25) que

$$\frac{\pi_f(N)}{N} = \prod_{p=2,3} \left[\left(1 - \frac{N_f(p)}{p}\right) \cdot \left(1 - \frac{1}{p}\right)^{-1}\right] \cdot \frac{1 + o(1)}{h \log N}.$$

Assim consertamos o problema das classes módulo 2 e 3, mas também é necessário analisar as classes de congruência módulo 5, 7, 11, ..., de todos os outros primos. Com argumentos análogos, vemos que se levarmos em conta as classes de congruência de todos os primos até o primo P,

teremos que

$$\frac{\pi_f(N)}{N} = \prod_{p=2}^{P} \left[\left(1 - \frac{N_f(p)}{p}\right) \cdot \left(1 - \frac{1}{p}\right)^{-1} \right] \cdot \frac{1+o(1)}{h \log N}.$$

Isso sugere que, se levarmos em conta todos os números primos simultaneamente, deve valer

$$\frac{\pi_f(N)}{N} = \prod_{p} \left[\left(1 - \frac{N_f(p)}{p}\right) \cdot \left(1 - \frac{1}{p}\right)^{-1} \right] \cdot \frac{1+o(1)}{h \log N} = C(f) \cdot \frac{1+o(1)}{h \log N} \tag{2.28}$$

com o produto infinito percorrendo todos os números primos. Ou seja, esse argumento sugere que devemos conjecturar

$$\frac{\pi_f(x)}{x} \sim \frac{C(f)}{h \log x},$$

que é exatamente a Conjectura 6 para uma família de um único polinômio.

Vejamos agora como deduzir a Conjectura 6 para uma família de k polinômios. Seja então $f_1(X), \ldots, f_k(X)$ uma família apropriada de polinômios, de graus respectivamente $h_1, \ldots, h_k$. Seja também $f(X) \doteq f_1(X) \cdots f_k(X)$. Assim como no caso de um único polinômio, vamos fixar $N > 0$ suficientemente grande e tentar calcular a probabilidade $\mathrm{P}(\{n \leq N : f_1(n), \ldots, f_k(n) \text{ são primos}\})$. Vamos utilizar novamente a notação mais compacta

$$\mathrm{P}\left(f_1(n), \ldots, f_k(n) \text{ são primos}\right) \doteq \mathrm{P}\left(\{n \leq N : f_1(n), \ldots, f_k(n) \text{ são primos}\}\right).$$

Se os eventos "$f_1(n)$ é primo", ..., "$f_k(n)$ é primo" fossem independentes, então teríamos

$$\begin{aligned} \mathrm{P}\left(f_1(n), \ldots, f_k(n) \text{ são primos}\right) &= \mathrm{P}\left(f_1(n) \text{ é primo}\right) \cdots \mathrm{P}\left(f_k(n) \text{ é primo}\right) \\ &= \frac{C(f_1) \cdots C(f_k)}{h_1 \cdots h_k} \cdot \frac{1+o(1)}{\log^k N}, \end{aligned}$$

usando a probabilidade (2.28) que calculamos no caso anterior para cada polinômio $f_j(X)$. Logo

$$\frac{\pi_{\mathbf{f}}(N)}{N} = \mathrm{P}\left(f_1(n), \ldots, f_k(n) \text{ são primos}\right) = \frac{C(f_1) \cdots C(f_k)}{h_1 \cdots h_k} \cdot \frac{1+o(1)}{\log^k N}.$$

Mas é errado supor livremente que os eventos "$f_1(n)$ é primo", ..., "$f_k(n)$ é primo" são independentes, pois isso implicaria, por exemplo, que a família $X, X+1$ passa por infinitos números primos. Mas já vimos que essa família $X, X+1$ não pode passar por infinitos números primos, pois para todo $n \in \mathbb{N}$ temos que n é par, ou $n+1$ é par. Pois bem, então precisamos levar em conta esse fenômeno da paridade ao calcular a probabilidade de $f_1(n), \ldots, f_k(n)$ serem todos primos. Isso nos levaria novamente a estudar quando os valores $f_j(n)$ são números pares, para $j \in \{1, \ldots, k\}$ e $n \in \mathbb{N}$, e com essa análise precisaríamos garantir que existem $n \in \mathbb{N}$ tais que nenhum dos valores $f_1(n), \ldots, f_k(n)$ seja par. (É esse o problema do caso $X, X+1$; não existe $n \in \mathbb{N}$ tal que n e $n+1$ não sejam pares.)

Já fizemos uma análise parecida no caso de um único polinômio quando levamos em conta a paridade dos valores $f(1), \ldots, f(N)$. Vamos seguir a mesma ideia desse caso, e separar a probabilidade $\mathrm{P}(f_1(n), \ldots, f_k(n) \text{ são primos})$ usando probabilidades condicionais módulo 2:

$$\mathrm{P}\left(f_1(n), \ldots, f_k(n) \text{ são primos}\right) = \sum_{i=1}^{2} \mathrm{P}\left(f_1(n), \ldots, f_k(n) \text{ são primos} \mid n \equiv i \pmod 2\right) \cdot \frac{1+o(1)}{2}.$$

(Já usamos aqui que $\mathrm{P}(n \equiv i \pmod 2) = (1+o(1))/2$ para todo $i \in \{1, 2\}$.) Vamos assim supor que, quando olhamos localmente nas classes módulo 2 e separamos essa probabilidade $\mathrm{P}(f_1(n), \ldots, f_k(n) \text{ são primos})$ em probabilidades condicionais, "consertamos" o problema da paridade, de modo que agora os eventos "$f_1(n)$ é primo", ..., "$f_k(n)$ é primo" são *condicionalmente*

independentes, dado que $n \equiv i \pmod 2$. Com essa hipótese, segue que

$$\mathrm{P}\left(f_1(n),\dots,f_k(n) \text{ são primos} \mid n \equiv i \pmod 2\right) = \prod_{j=1}^{k} \mathrm{P}\left(f_j(n) \text{ é primo} \mid n \equiv i \pmod 2\right).$$

Portanto

$$\mathrm{P}\left(f_1(n),\dots,f_k(n) \text{ são primos}\right) = \sum_{i=1}^{2} \frac{1+o(1)}{2} \cdot \prod_{j=1}^{k} \mathrm{P}\left(f_j(n) \text{ é primo} \mid n \equiv i \pmod 2\right). \quad (2.29)$$

Fixemos $i \in \{1,2\}$. Veremos em breve que vale

$$\mathrm{P}\left(f_j(n) \text{ é primo} \mid n \equiv i \pmod 2\right) = \frac{0+o(1)}{h_j \log N}, \quad \text{se } f_j(i) \equiv 0 \pmod 2,$$

e

$$\mathrm{P}\left(f_j(n) \text{ é primo} \mid n \equiv i \pmod 2\right) = \frac{C(f_1)}{(1-N_{f_j}(2)/2)(1-1/2)^{-1}} \frac{2+o(1)}{h_j \log N}, \quad \text{se } f_j(i) \not\equiv 0 \pmod 2,$$

para todo $j \in \{1,\dots,k\}$. É no cálculo dessas probabilidades que usaremos o caso que fizemos anteriormente para uma família apropriada de um único polinômio. Vamos assumir, por um momento, a validade dessas igualdades. Para reduzir a expressão, dado um número primo p denotaremos por

$$C_{j,p} \doteq \left(1-\frac{N_{f_j}(p)}{p}\right)\cdot\left(1-\frac{1}{p}\right)^{-1}, \quad j=1,2,\dots,k.$$

Tomando o produto dessas fórmulas, vemos que

$$\prod_{j=1}^{k} \mathrm{P}\left(f_j(n) \text{ é primo} \mid n \equiv i \pmod 2\right) = \frac{0+o(1)}{h_1\cdots h_k \log N}, \quad \text{se } f(i) \equiv 0 \pmod 2$$

(pois $f(i) = f_1(i)\cdots f_k(i)$), e

$$\prod_{j=1}^{k} \mathrm{P}\left(f_j(n) \text{ é primo} \mid n \equiv i \pmod 2\right) = \frac{C(f_1)\cdots C(f_k)}{C_{1,2}\cdots C_{k,2}} \cdot \frac{2^k+o(1)}{h_1\cdots h_k \log N}, \quad \text{se } f(i) \equiv 0 \pmod 2.$$

Agora, na soma de (2.29), temos que ocorre a equivalência $f(i) \equiv 0 \pmod 2$ uma quantidade $N_f(2)$ vezes em i, enquanto $f(i) \not\equiv 0 \pmod 2$ ocorre $2 - N_f(2)$ vezes. Assim, substituindo as fórmulas dos produtos acima em (2.29), obtemos

$$\begin{aligned}
&\mathrm{P}\left(f_1(n),\dots,f_k(n) \text{ são primos}\right) \\
&\quad = N_f(2)\frac{1+o(1)}{2}\cdot\frac{0+o(1)}{h_1\cdots h_k\log N} + \big(2-N_f(2)\big)\frac{1+o(1)}{2}\cdot\frac{C(f_1)\cdots C(f_k)}{C_{1,2}\cdots C_{k,2}}\cdot\frac{2^k+o(1)}{h_1\cdots h_k\log N} \\
&\qquad = \frac{C(f_1)\cdots C(f_k)}{C_{1,2}\cdots C_{k,2}}\cdot\left[\left(1-\frac{N_f(2)}{2}\right)\left(1-\frac{1}{2}\right)^{-k}\right]\cdot\frac{1+o(1)}{h_1\cdots h_k\log N}.
\end{aligned}$$

Portanto,

$$\frac{\pi_{\mathbf{f}}(N)}{N} = \frac{C(f_1)\cdots C(f_k)}{C_{1,2}\cdots C_{k,2}}\cdot\left[\left(1-\frac{N_f(2)}{2}\right)\left(1-\frac{1}{2}\right)^{-k}\right]\cdot\frac{1+o(1)}{h_1\cdots h_k\log N}.$$

Mas esse argumento ignora as congruências módulo 3. Por exemplo, ele implicaria que a família

$X, X+2, X+4$ passa por infinitos números primos, o que é impossível pois para todo $n \in \mathbb{N}$, um dos valores $n, n+2, n+4$ é divisível por 3. Precisamos, da mesma forma como fizemos com a paridade, considerar as congruências módulo 3, 5, 7, ... para todos os outros números primos. Considerando todas as congruências até o primo P e procedendo de modo análogo ao que fizemos anteriormente, resulta

$$\frac{\pi_{\mathbf{f}}(N)}{N} = C(f_1)\cdots C(f_k)\cdot \prod_{p=2}^{P}\left\{\frac{1}{C_{1,p}\cdots C_{k,p}}\cdot\left[\left(1-\frac{N_f(p)}{p}\right)\left(1-\frac{1}{p}\right)^{-k}\right]\right\}\cdot\frac{1+o(1)}{h_1\cdots h_k\log N}.$$

Isso sugere que, se considerarmos todos os números primos simultaneamente, teremos

$$\frac{\pi_{\mathbf{f}}(N)}{N} = C(f_1)\cdots C(f_k)\cdot \prod_{p}\left\{\frac{1}{C_{1,p}\cdots C_{k,p}}\cdot\left[\left(1-\frac{N_f(p)}{p}\right)\left(1-\frac{1}{p}\right)^{-k}\right]\right\}\cdot\frac{1+o(1)}{h_1\cdots h_k\log N}, \tag{2.30}$$

em que o produto é tomado sobre todos os números primos. Agora, lembramos que $C(f_j) = \prod_p C_{j,p}$, de modo que podemos cancelar os $C(f_j)$ e os $C_{j,p}$ em (2.30), e obtemos

$$\frac{\pi_{\mathbf{f}}(N)}{N} = \frac{C(\mathbf{f})+o(1)}{h_1\cdots h_k\log N}.$$

Finalmente, esse argumento probabilístico sugere que devemos conjecturar

$$\frac{\pi_{\mathbf{f}}(x)}{x} \sim \frac{C(\mathbf{f})}{h_1\cdots h_k}\cdot\frac{1}{\log x},$$

que é exatamente a Conjectura de Bateman-Horn.

Resta somente calcular as probabilidades $\mathrm{P}(f_j(n)$ é primo $\mid n \equiv i \pmod 2)$ com $i \in \{1,2\}$ e $j \in \{1,\ldots,k\}$ fixados, como prometido anteriormente.

a) Se $f_j(i) \equiv 0 \pmod 2$: nesse caso $f_j(n)$ é par para todo $n \equiv i \pmod 2$, logo $f_j(n)$ não será um número primo, exceto se $f_j(n) = 2$. Assim, $\mathrm{P}(f_j(n)$ é primo $\mid n \equiv i \pmod 2) = O(1/N)$, e segue então que

$$\mathrm{P}\left(f_j(n) \text{ é primo} \mid n \equiv i \pmod 2\right) = \frac{0+o(1)}{h_j\log N}.$$

b) Se $f_j(i) \not\equiv 0 \pmod 2$: vamos supor $i = 1$ por simplicidade. O caso $i = 2$ é inteiramente análogo. Assim, $f_j(1) \not\equiv 0 \pmod 2$. Seja $N_1 = 2l-1$ o maior inteiro congruente a 1 módulo 2, menor do que N. Queremos então calcular a probabilidade de se obter um primo, escolhendo aleatoriamente um inteiro de

$$f_j(1), \quad f_j(3), \quad f_j(5), \quad f_j(7), \quad \ldots, \quad f_j(N_1).$$

Escrevendo de outra forma, esses valores são

$$f_j(2\cdot 1-1), \quad f_j(2\cdot 2-1), \quad f_j(2\cdot 3-1), \quad f_j(2\cdot 4-1), \quad \ldots, \quad f_j(2l-1). \tag{2.31}$$

Mas os valores de (2.31) são simplesmente os l primeiros valores do polinômio $g_j(X) \doteq f_j(2X-1)$. O polinômio $g_j(X)$ também é irredutível sobre $\mathbb{Q}$ pois $f_j(X)$ é irredutível. Fazendo uma translação como em (2.2) para tornar $g_j(X)$ um polinômio apropriado (se necessário) temos, do argumento probabilístico para um único polinômio que fizemos anteriormente, que vale

$$\frac{\pi_{g_j}(l)}{l} = \frac{C(g_j)+o(1)}{h_j\log l}.$$

Assim, como $\mathrm{P}(f_j(n)$ é primo $\mid n \equiv 1 \pmod 2)$ é a probabilidade de se escolher um valor primo

em (2.31), e essa probabilidade é por outro lado $\pi_{g_j}(l)/l$, temos que

$$\mathrm{P}\left(f_j(n) \text{ é primo} \mid n \equiv i \pmod 2\right) = \frac{C(g_j)+o(1)}{h_j \log l} = \frac{C(g_j)+o(1)}{h_j \log N}, \tag{2.32}$$

pois $l = N/2$ ou $l = (N+1)/2$. Resta só calcular $C(g_j)$.

Precisamos então calcular os valores $N_{g_j}(p)$ para todo número primo p. Se $p = 2$, temos que $N_{g_j}(2) = 0$, pois se $n \in \mathbb{N}$ vale

$$g_j(n) = f_j(2n-1) \equiv f_j(-1) \equiv f_j(1) \not\equiv 0 \pmod 2.$$

Seja $p > 2$ um número primo. Denotaremos por $\overline{n} \doteq n + p\mathbb{Z}$ a classe de congruência de $n \in \mathbb{N}$ módulo p. Como $p > 2$, temos que $\overline{2}$ é invertível no anel quociente $\mathbb{Z}/p\mathbb{Z}$, logo a seguinte aplicação

$$\begin{aligned} \phi : \mathbb{Z}/p\mathbb{Z} &\to \mathbb{Z}/p\mathbb{Z} \\ \overline{n} &\mapsto \overline{2}\cdot\overline{n} - \overline{1} \end{aligned}$$

é uma bijeção. Agora, a função ϕ leva raízes módulo p de $g_j(X) = f_j(2X-1)$ em raízes módulo p de $f_j(X)$, e reciprocamente ϕ^{-1} leva raízes de $f_j(X)$ em raízes de $g_j(X)$. Como também ϕ é bijetora, segue que o número de raízes de $g_j(X)$ módulo p é igual ao número de raízes de $f_j(X)$ módulo p. Isto é; vale $N_{g_j}(p) = N_{f_j}(p)$.

Em resumo,

$$N_{g_j}(p) = \begin{cases} 0, & \text{se } p = 2 \\ N_{f_j}(p), & \text{se } p > 2. \end{cases}$$

Mas então isso implica que

$$C(g_j) = \frac{1}{1 - N_{f_j}(2)/2} C(f_j) = \frac{C(f_j)}{(1 - N_{f_j}(2)/2)(1-1/2)^{-1}} \cdot 2.$$

Substituindo em (2.32) temos

$$\mathrm{P}\left(f_j(n) \text{ é primo} \mid n \equiv i \pmod 2\right) = \frac{C(f_j)}{(1 - N_{f_j}(2)/2)(1-1/2)^{-1}} \cdot \frac{2+o(1)}{h_j \log N},$$

como queríamos demonstrar.

2.4 Exemplos notáveis

Provemos que a Conjectura de Bateman-Horn condiz com o único caso já provado, que é o do Teorema 1.5.

Proposição 2.2. *Sejam $a, b \in \mathbb{N}$ relativamente primos. Então temos que*

$$C(aX+b) = \frac{a}{\varphi(a)}.$$

Portanto a Conjectura 6 inclui o Teorema 1.5.

Demonstração. Seja $f(X) \doteq aX + b$. Temos que

$$N_{aX+b}(p) = \begin{cases} 0, & \text{se } p \mid a \\ 1, & \text{se } p \nmid a. \end{cases}$$

De fato, i) se $p \mid a$, então $p \nmid b$ pois $\mathrm{mdc}(a,b) = 1$, e dado $n \in \mathbb{N}$, $n \leq p$, temos

$$an + b \equiv 0n + b \equiv b \not\equiv 0 \pmod p,$$

de modo que $N_f(p) = 0$. ii) Se $p \nmid a$, então a é invertível em $\mathbb{Z}/p\mathbb{Z}$; existe $c \in \mathbb{N}$ tal que $a.c \equiv 1 \pmod p$. Então dado $n \in \mathbb{N}$, temos $an + b \equiv 0 \pmod p$ se, e somente se $n \equiv -cb \pmod p$, e portanto $f(n) \equiv 0 \pmod p$ possui uma única solução para $n \in \mathbb{N}$, $n \leq p$. Isto é; $N_f(p) = 1$.

Dessa forma, separando os primos que dividem a dos que não dividem a no produto que define $C(\mathbf{f})$, temos

$$\begin{aligned} C(aX+b) &= \prod_{p|a}\left[\left(1-\frac{1}{p}\right)^{-1}\left(1-\frac{0}{p}\right)\right]\cdot\prod_{p\nmid a}\left[\left(1-\frac{1}{p}\right)^{-1}\left(1-\frac{1}{p}\right)\right] \\ &= \prod_{p|a}\left(1-\frac{1}{p}\right)^{-1}\cdot 1 = \frac{a}{\varphi(a)}, \end{aligned}$$

usando (1.1). A igualdade $C(aX + b) = a/\varphi(a)$ de fato condiz com o Teorema 1.5. □

A Conjectura 6 também engloba várias outras conjecturas anteriores, como as Conjecturas 3 e 4 formuladas por Hardy e Littlewood. Provaremos esse fato nesta Seção.

Provemos primeiramente que a Conjectura 6 inclui a Conjectura 3. Para isso, precisamos saber o valor de $N_{X^2+1}(p)$ para todo primo p. De fato, temos $N_{X^2+1}(2) = 1$ e

$$N_{X^2+1}(p) = 1 + (-1)^{(p-1)/2}, \quad \text{para todo primo } p > 2, \tag{2.33}$$

o que segue diretamente de [Apo76, Teorema 9.4]. Com isso temos a seguinte Proposição:

Proposição 2.3. *Vale*

$$C(X^2+1) = \prod_{p>2}\left(1-\frac{(-1)^{(p-1)/2}}{p-1}\right).$$

Portanto a Conjectura 6 inclui a Conjectura 3.

Demonstração. Segue de (2.33) que

$$C(X^2+1) = \left(1-\frac{1}{2}\right)^{-1}\left(1-\frac{1}{2}\right)\cdot\prod_{p>2}\left[\left(1-\frac{1}{p}\right)^{-1}\left(1-\frac{1+(-1)^{(p-1)/2}}{p}\right)\right]. \tag{2.34}$$

Agora para todo primo $p > 3$ temos

$$\left(1-\frac{1}{p}\right)^{-1}\left(1-\frac{1+(-1)^{(p-1)/2}}{p}\right) = \frac{p-1-(-1)^{(p-1)/2}}{p-1} = 1-\frac{(-1)^{(p-1)/2}}{p-1}.$$

Substituindo em (2.34) provamos o resultado. □

Provemos agora o mesmo resultado para a Conjectura 4. É preciso observar que a família $(X, X+2)$ não é apropriada pois ela não satisfaz a condição iv) de família apropriada. Entretanto, essa condição foi colocada meramente para facilitar o estudo abstrato que faremos nos próximos capítulos; essa hipótese não é necessária *de fato* na Conjectura 6; portanto não nos preocuparemos com essa condição no momento.

Temos $N_{X(X+2)}(2) = 1$, e, se $p > 2$ é primo, então a equação $n(n+2) \equiv 0 \pmod p$ tem sempre duas soluções distintas módulo p. Portanto

$$N_{X(X+2)}(p) = 2, \quad \text{para todo primo } p > 2. \tag{2.35}$$

Concluímos assim que:

Proposição 2.4. *Vale*

$$C(X, X+2) = 2\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right).$$

Portanto a Conjectura 6 inclui a Conjectura 4.

Demonstração. Segue de (2.35) que

$$C(X, X+2) = \left(1-\frac{1}{2}\right)^{-2}\left(1-\frac{1}{2}\right)\cdot\prod_{p>2}\left[\left(1-\frac{1}{p}\right)^{-2}\left(1-\frac{2}{p}\right)\right]. \tag{2.36}$$

Agora se $p > 2$ é primo temos

$$\frac{1-2/p}{(1-1/p)^2} = \frac{p^2-2p}{(p-1)^2} = \frac{(p-1)^2-1}{(p-1)^2} = 1-\frac{1}{(p-1)^2}.$$

Substituindo em (2.36) obtemos o resultado. □

Capítulo 3

A convergência do produto $C(\mathbf{f})$

Antes de provarmos a convergência do produto $C(\mathbf{f})$, precisaremos entender melhor a função N_g para um dado polinômio $g(X) \in \mathbb{Z}[X]$ qualquer.

3.1 Propriedades da função N_g

Lema 3.1. *Seja $f_1(X), \ldots, f_k(X)$ uma família de polinômios apropriada. Então exceto para uma quantidade finita de primos p, vale a seguinte igualdade:*

$$N_f(p) = N_{f_1}(p) + N_{f_2}(p) + \cdots + N_{f_k}(p). \tag{3.1}$$

Demonstração. Sejam $i, j \in \{1, \ldots, k\}$ distintos. Como $\mathrm{mdc}(f_i, f_j) = 1$ (Lema 2.1), existem $u_{ij}(X), v_{ij}(X) \in \mathbb{Z}[X]$ e $c_{ij} \in \mathbb{Z}$, $c_{ij} \neq 0$ tais que

$$u_{ij}(X)f_i(X) + v_{ij}(X)f_j(X) = c_{ij}. \tag{3.2}$$

Seja p um número primo. Provaremos que vale (3.1) se $p \nmid \prod_{1 \leq i < j \leq k} c_{ij}$. De fato, nesse caso segue de (3.2) que

$$p \nmid \mathrm{mdc}(f_i(n), f_j(n)) \quad \text{para todo } n \in \mathbb{N}.$$

Dessa forma, dados $i, j \in \{1, \ldots, k\}$ distintos, os conjuntos $\{n \in \mathbb{N},\, n \leq p \,:\, f_i(n) \equiv 0 \pmod p\}$ e $\{n \in \mathbb{N},\, n \leq p \,:\, f_j(n) \equiv 0 \pmod p\}$ são disjuntos.

Como p é primo, temos que $p \mid f(n)$ se, e somente se, $p \mid f_i(n)$ para algum $i \in \{1, \ldots, k\}$. Dessa forma,

$$\big\{n \in \mathbb{N},\, n \leq p \,:\, f(n) \equiv 0 \pmod p\big\} = \bigcup_{i=1}^{k} \big\{n \in \mathbb{N},\, n \leq p \,:\, f_i(n) \equiv 0 \pmod p\big\}$$

onde temos uma união de conjuntos dois a dois disjuntos. Calculando o número de elementos desses conjuntos, temos

$$N_f(p) = N_{f_1}(p) + N_{f_2}(p) + \cdots + N_{f_k}(p). \qquad \square$$

Fixemos agora $g(X)$ um polinômio não-constante de coeficientes inteiros para o resto desta Seção.

Lema 3.2. *Sejam $a, b \in \mathbb{N}$ relativamente primos. Então vale*

$$N_g(ab) = N_g(a)N_g(b).$$

Isto é; a função $d \mapsto N_g(d)$ é multiplicativa.

Demonstração. Eliminando os casos triviais, a demonstração do Lema será uma simples aplicação do Teorema Chinês dos Restos.

Se $a = 1$ ou $b = 1$, o resultado é trivial. Suponha então $a \neq 1$ e $b \neq 1$.

Para cada $c \in \mathbb{N}$, $c \geq 2$, defina

$$B_c \doteq \big\{ n \in \mathbb{N},\, n \leq c \,:\, g(n) \equiv 0 \pmod{c} \big\}.$$

Dessa forma, $N_g(c) = \#B_c$.

Se $B_a = \varnothing$, então $a \nmid g(n)$ para todo $n \in \mathbb{N}$, mas então também vale $ab \nmid g(n)$ para todo $n \in \mathbb{N}$, e assim $B_{ab} = \varnothing$. Portanto $N_g(ab) = 0 = N_g(a)N_g(b)$. O caso $B_b = \varnothing$ é análogo.

Suponhamos então que B_a, B_b são não-vazios. Dados $k \in B_a$ e $m \in B_b$, o Teorema Chinês dos Restos implica que existe um único $n_{km} \in \mathbb{N}$, $n_{km} \leq ab$ tal que

$$n_{km} \equiv k \pmod{a} \quad \text{e} \quad n_{km} \equiv m \pmod{b}.$$

Além disso $n_{km} \in B_{ab}$ pois

$$g(n_{km}) \equiv g(k) \equiv 0 \pmod{a},$$

dado que $k \in B_a$. Assim $a \mid g(n_{km})$ e analogamente $b \mid g(n_{km})$. Como a, b são relativamente primos, segue que $ab \mid g(n_{km})$, e $n_{km} \in B_{ab}$. Temos assim uma aplicação

$$\begin{aligned} \phi : B_a \times B_b &\to B_{ab} \\ (k, m) &\mapsto n_{km}. \end{aligned}$$

Provemos que ϕ é injetora. De fato, se $\phi(k, m) = \phi(k', m') = n$, temos

$$n \equiv k \pmod{a} \quad \text{e} \quad n \equiv k' \pmod{a},$$

logo $k \equiv k' \pmod{a}$. Como $k, k' \leq a$, segue que $k = k'$. Analogamente prova-se que $m = m'$, e assim ϕ é injetora.

Provemos que ϕ é sobrejetora. Seja $n \in B_{ab}$. Então sejam $k, m \in \mathbb{N}$, $k \leq a$, $m \leq b$ tais que

$$n \equiv k \pmod{a} \quad \text{e} \quad n \equiv m \pmod{b}.$$

Então $k \in B_a$ pois $g(k) \equiv g(n) \equiv 0 \pmod{a}$, dado que $ab \mid g(n)$. Analogamente, $m \in B_b$ e assim $\phi(k, m) = n$. Portanto ϕ é sobrejetora.

Vimos assim que $\phi : B_a \times B_b \to B_{ab}$ é bijetora, de modo que

$$N_g(ab) = \#B_{ab} = \#(B_a \times B_b) = \#B_a \cdot \#B_b = N_g(a)N_g(b). \qquad \square$$

Seja $\alpha \in \mathbb{C}$ uma raiz de $g(X)$, e sejam $K \doteq \mathbb{Q}(\alpha)$ e $\mathcal{O}_K$ o anel de inteiros algébricos do corpo K. Se I é um ideal de $\mathcal{O}_K$, denotaremos por $\mathrm{N}(I) \doteq \#(\mathcal{O}_K/I)$ a *norma* de I. Dado um primo p, seja

$$A_{p,K} \doteq \#\big\{ P \text{ ideal primo de } \mathcal{O}_K \,:\, \mathrm{N}(P) = p \big\}.$$

Quando não houver dúvida sobre o corpo K, escreveremos simplesmente A_p em lugar de $A_{p,K}$.

Com esses conceitos, vamos obter uma expressão alternativa para $N_g(p)$ que é fundamental no desenvolvimento da teoria:

Proposição 3.3. *Com exceção de uma quantidade finita de números primos $p \in \mathbb{N}$, vale*

$$A_{p,K} = N_g(p).$$

Demonstração. Provemos o resultado primeiramente para o caso em que $g(X)$ é mônico. Nesse caso, seja p um número primo que não divide a norma do condutor de $\mathbb{Z}[\alpha]$ em $\mathcal{O}_K$ (para a definição de condutor, veja o Apêndice A). Então estamos nas condições de aplicar o Teorema A.2 do Apêndice A. Se φ é a mesma aplicação do enunciado desse Teorema, escrevemos

$$\varphi(g) = g_1^{a_1} g_2^{a_2} \cdots g_m^{a_m} \tag{3.3}$$

com $a_1, \ldots, a_m \in \mathbb{N}$ e $g_1(X), \ldots, g_m(X) \in (\mathbb{Z}/p\mathbb{Z})[X]$ polinômios mônicos, irredutíveis, não-constantes, e distintos. Sejam $n_1, \ldots, n_m$ os graus dos polinômios $g_1(X), \ldots, g_m(X)$, respectivamente. Temos que

$$p\mathcal{O}_K = P_1^{a_1} P_2^{a_2} \cdots P_m^{a_m} \tag{3.4}$$

em que $P_1, \ldots, P_m$ são ideais primos de $\mathcal{O}_K$ distintos, com $\mathrm{N}(P_i) = p^{n_i}$ para cada $i \in \{1, \ldots, m\}$.

Seja P um ideal primo de $\mathcal{O}_K$ tal que $\mathrm{N}(P) = p$. Então $p \in P$ e assim $P \mid p\mathcal{O}_K$. Segue então de (3.4) que existe $i \in \{1, \ldots, m\}$ tal que $P = P_i$. Dessa forma, temos que

$$A_p = \#\big\{i \in \{1, \ldots, m\} : \mathrm{N}(P_i) = p\big\} = \#\big\{i \in \{1, \ldots, m\} : n_i = 1\big\} = N_g(p)$$

pois $N_g(p)$ é o número de soluções de $\varphi(g)$ em $\mathbb{Z}/p\mathbb{Z}$. Isto é; $N_g(p)$ é igual ao número de fatores lineares (isto é, de grau 1) distintos que aparecem na decomposição de $\varphi(g)$ em (3.3).

Para o caso em que $g(X) = aX^n + a_1X^{n-1} + \cdots + a_n$ não é mônico, defina

$$h(X) \doteq a^{n-1} g\left(\frac{X}{a}\right) = X^n + a_1X^{n-1} + a_2aX^{n-2} + \cdots + a_na^{n-1}.$$

Temos que $h(X)$ é um polinômio com coeficientes inteiros, irredutível sobre $\mathbb{Q}$, e mônico. Seja então $\beta \doteq a\alpha$. Temos que $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ e, pelo caso que já fizemos, vale $A_{p,K} = N_h(p)$ para todo primo p suficientemente grande.

Agora, se p é primo tal que $p \nmid a$, então $\overline{a} \doteq a + p\mathbb{Z}$ é invertível no corpo $\mathbb{Z}/p\mathbb{Z}$ e assim

$$\varphi(g)(X) = \overline{a}^{1-n} \varphi(h)(\overline{a}X).$$

Com isso vemos que $\varphi(g)$ tem tantas raízes em $\mathbb{Z}/p\mathbb{Z}$ quanto $\varphi(h)$, isto é; $N_g(p) = N_h(p)$. Portanto se p é também suficientemente grande, temos $N_g(p) = N_h(p) = A_p$. □

3.2 Demonstração da convergência de $C(\mathbf{f})$

A demonstração da convergência de $C(\mathbf{f})$ se baseará na seguinte propriedade geral sobre convergência de produtos infinitos, que lembramos aqui:

Lema 3.4. *Seja $(a_n)_{n\in\mathbb{N}}$ uma sequência de números reais tal que as séries*

$$\sum_{n=1}^{+\infty} a_n \quad \text{e} \quad \sum_{n=1}^{+\infty} a_n^2$$

são ambas convergentes. Então o produto $\prod_{n=1}^{+\infty}(1 - a_n)$ é convergente.

Demonstração. Lembramos que $-\log(1-x) - x \sim \frac{1}{2}x^2$ quando $x \to 0$. Como $\sum_n a_n$ é convergente, temos que $a_n \to 0$. Então,

$$-\log(1 - a_n) - a_n \sim \frac{1}{2}a_n^2 \tag{3.5}$$

quando $n \to +\infty$. Como $\sum_n a_n$ e $\sum_n a_n^2$ são convergentes, segue de (3.5) que $\sum_{n\geq m} \log(1 - a_n)$ é convergente para algum $m \in \mathbb{N}$ grande o suficiente para que $1 - a_n > 0$ para todo $n \geq m$, o que implica a convergência do produto $\prod_n(1 - a_n)$. □

Fixemos $f_1(X), \ldots, f_k(X)$ uma família apropriada de polinômios. Como sempre, definimos $f(X) \doteq f_1(X)f_2(X)\cdots f_k(X)$ e $\mathbf{f} \doteq (f_1, \ldots, f_k)$. Para cada $j \in \{1, \ldots, k\}$, sejam α_j uma raiz de $f_j(X)$ e $K_j \doteq \mathbb{Q}(\alpha_j)$. Dessa forma, para todo primo p suficientemente grande, temos

$$N_{f_j}(p) = A_{p,K_j}$$

pela Proposição 3.3.

Para cada primo p seja a_p tal que

$$1 - a_p = \left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{N_f(p)}{p}\right),$$

de modo que $C(\mathbf{f}) = \prod_p (1 - a_p)$. Lembramos que para $|z| < 1$ vale

$$\frac{1}{(1-z)^k} = 1 + kz + k(k+1)z^2 + \cdots = 1 + kz + O(z^2).$$

Para todo primo p temos então

$$1 - a_p = \left(1 + k\frac{1}{p} + O\left(\frac{1}{p^2}\right)\right)\left(1 - \frac{N_f(p)}{p}\right) = 1 + \frac{k - N_f(p)}{p} + O\left(\frac{1}{p^2}\right),$$

Assim

$$a_p = \frac{N_f(p) - k}{p} + O\left(\frac{1}{p^2}\right).$$

Dessa forma, $a_p = O(1/p)$ e $a_p^2 = O(1/p^2)$, de modo que $\sum_p a_p^2$ é convergente. Se provarmos que $\sum_p a_p$ é convergente, seguirá do Lema 3.4 que $C(\mathbf{f})$ é convergente.

Para provar que $\sum_p a_p$ é convergente, basta mostrar que a série

$$\sum_p \frac{N_f(p) - k}{p} \tag{3.6}$$

é convergente. Agora, para p suficientemente grande, temos (do Lema 3.1 e da Proposição 3.3) que

$$\begin{aligned} N_f(p) - k &= (N_{f_1}(p) - 1) + (N_{f_2}(p) - 1) + \cdots + (N_{f_k}(p) - 1) \\ &= (A_{p,K_1} - 1) + (A_{p,K_2} - 1) + \cdots + (A_{p,K_k} - 1). \end{aligned}$$

Dessa forma, existe $m \in \mathbb{N}$ tal que

$$\sum_{p \geq m} \frac{N_f(p) - k}{p} = \sum_{p \geq m} \frac{A_{p,K_1} - 1}{p} + \cdots + \sum_{p \geq m} \frac{A_{p,K_k} - 1}{p}. \tag{3.7}$$

Assim a série (3.6) será convergente e a demonstração da convergência de $C(\mathbf{f})$ estará terminada se provarmos o seguinte Lema:

Lema 3.5. *Para todo corpo de números K, a série*

$$\sum_p \frac{A_{p,K} - 1}{p}$$

é convergente.

Para demonstrar esse Lema precisaremos do conceito da função ζ de Dedekind, que estará relacionada com os números $A_{p,K}$. (A demonstração do Lema 3.5 é de fato a parte mais complicada da demonstração da convergência de $C(\mathbf{f})$.)

É interessante notar que não é possível "escapar" da demonstração do Lema 3.5, pois, no caso $k = 1$, demonstrar a convergência da série (3.6) é exatamente demonstrar o Lema 3.5, em vista da Proposição 3.3. Isto é; com a igualdade (3.7) nós reduzimos a demonstração da convergência de (3.6) à prova do caso $k = 1$.

3.3 A função ζ de Dedekind

Sejam K um corpo de números algébricos e $\mathcal{O}_K$ o seu anel de inteiros algébricos. A função ζ de Dedekind associada ao corpo K é a série de Dirichlet dada por

$$\zeta_K(s) \doteq \sum_I \frac{1}{\mathrm{N}(I)^s} = \prod_P \frac{1}{1-\mathrm{N}(P)^{-s}} \tag{3.8}$$

em que a soma $\sum_I$ é tomada sobre os ideais inteiros I de $\mathcal{O}_K$, e o produto $\prod_P$ é tomado sobre os ideais primos P de $\mathcal{O}_K$. A abcissa de convergência absoluta da série é 1, e a segunda igualdade em (3.8) vale se $\mathrm{Re}(s) > 1$. Além disso, a função $\zeta_K(s)$ possui um prolongamento meromorfo a todo o $\mathbb{C}$, com um único polo simples em $s = 1$. A demonstração desse fato pode ser encontrada em [Lan94, Cap. XIII].

Usaremos também o seguinte fato sobre a função $\zeta_K(s)$:

Teorema 3.6. *Existe uma constante $C_K > 0$ tal que $\zeta_K(s)$ não se anula no aberto*

$$\{s = \sigma + it \in \mathbb{C},\, \sigma, t \in \mathbb{R} \,:\, \sigma > 1 - C_K/\log(|t|+2)\}$$

que contém o semiplano fechado $\mathrm{Re}(s) \geq 1$*, e nesse mesmo aberto tem-se*

$$\frac{1}{\zeta_K(s)} \ll \log(|t|+2).$$

A demonstração do Teorema 3.6 para o caso $K = \mathbb{Q}$ pode ser encontrada em [Ten95] (Teoremas 15 e 16). Hindry e Rivoal notam em [HR05] que essa demonstração pode ser facilmente adaptada ao caso geral. Note que, se $K = \mathbb{Q}$, temos $\zeta_K(s) = \zeta(s)$, a função ζ de Riemann.

A propriedade da função $\zeta_K(s)$ que mais nos interessa se encontra no seguinte Lema, pois ele relaciona essa função com as quantidades A_p (e portanto, com $N_f(p)$):

Lema 3.7. *Existe uma função $R_K(s)$ holomorfa em* $\mathrm{Re}(s) > 1/2$*, que não se anula nesse aberto, tal que, se* $\mathrm{Re}(s) > 1$*, então*

$$\zeta_K(s) = \prod_p \left(\frac{1}{1-p^{-s}}\right)^{A_p} \cdot R_K(s). \tag{3.9}$$

Demonstração. Para cada ideal primo P de $\mathcal{O}_K$, seja $f_P \in \mathbb{N}$ tal que $\mathrm{N}(P) = p^{f_P}$ para algum número primo p. Se $\mathrm{Re}(s) > 1$,

$$\zeta_K(s) = \left(\prod_{P;\, f_P=1} \frac{1}{1-\mathrm{N}(P)^{-s}}\right) \cdot \left(\prod_{P;\, f_P\geq 2} \frac{1}{1-\mathrm{N}(P)^{-s}}\right) = \prod_p \left(\frac{1}{1-p^{-s}}\right)^{A_p} \cdot R_K(s)$$

onde $R_K(s) \doteq \prod_{P;\, f_P\geq 2} 1/(1-\mathrm{N}(P)^{-s})$. Provemos que $R_K(s)$ assim definida satisfaz as propriedades necessárias.

Para cada primo p, defina

$$B_p \doteq \#\big\{P \text{ ideal primo de } \mathcal{O}_K \,:\, p \mid \mathrm{N}(P)\big\}.$$

Então $B_p = \#\big\{P \text{ ideal primo de } \mathcal{O}_K \,:\, \mathrm{N}(P) = p^{f_P}\big\}$. Agora se P é um ideal primo de $\mathcal{O}_K$ tal que $\mathrm{N}(P) = p^{f_P}$, então P é um divisor de $p\mathcal{O}_K$. Seja $n \doteq [K:\mathbb{Q}]$. Como $\mathrm{N}(p\mathcal{O}_K) = |\,\mathrm{N}(p)| = p^n$, temos que $p\mathcal{O}_K$ não pode ter mais do que n divisores primos. Portanto $B_p \leq n$.

Defina

$$\tilde{R}_K(s) \doteq \prod_{P;\, f_P\geq 2} \left(1 - \frac{1}{\mathrm{N}(P)^s}\right) = \frac{1}{R_K(s)}.$$

Fixemos $\varepsilon > 0$. Se $s = \sigma + it$, $\sigma, t \in \mathbb{R}$, $\sigma \geq 1/2 + \varepsilon$, temos

$$\sum_{P;\, f_P \geq 2} \left| \frac{1}{\mathrm{N}(P)^s} \right| \leq \sum_{P;\, f_P \geq 2} \frac{1}{\mathrm{N}(P)^\sigma} = \sum_p \sum_{k \geq 2} \sum_{P;\, \mathrm{N}(P) = p^k} \frac{1}{p^{k\sigma}}$$
$$\leq \sum_p \sum_{P;\, p \mid \mathrm{N}(P)} \frac{1}{p^{2\sigma}} = \sum_p \frac{B_p}{p^{2\sigma}} \leq \sum_p \frac{n}{p^{2\sigma}} \leq \sum_p \frac{n}{p^{1+2\varepsilon}} < \infty.$$

Dessa forma, o produto que define $\tilde{R}_K(s)$ é normalmente convergente em $\mathrm{Re}(s) > 1/2$ e a função $\tilde{R}_K(s)$ é holomorfa nesse aberto. Além disso, nenhum dos fatores do produto que define $\tilde{R}_K(s)$ se anula se $\mathrm{Re}(s) > 1/2$, assim a função $\tilde{R}_K(s)$ não se anula nesse aberto. Portanto $R_K(s) = 1/\tilde{R}_K(s)$ é uma função holomorfa em $\mathrm{Re}(s) > 1/2$ e que não se anula nesse aberto. □

Podemos agora demonstrar o Lema 3.5.

Demonstração do Lema 3.5. Como $R_K(s)$ é uma função holomorfa e não se anula em $\mathrm{Re}(s) > 1/2$, existe um logaritmo $\log R_K(s)$ de $R_K(s)$ nesse aberto. Assim (3.9) implica, para $\mathrm{Re}(s) > 1$,

$$\log \zeta_K(s) = \sum_p (-A_p) \log\left(1 - \frac{1}{p^s}\right) + \log R_K(s) = \sum_p \frac{A_p}{p^s} + \sum_p \sum_{m \geq 2} \frac{A_p}{m p^{ms}} + \log R_K(s), \quad (3.10)$$

em que usamos a expansão em série de potências da função $z \mapsto -\log(1-z)$. Analogamente, para $K = \mathbb{Q}$ temos

$$\log \zeta(s) = \sum_p \frac{1}{p^s} + \sum_p \sum_{m \geq 2} \frac{1}{m p^{ms}} \quad (3.11)$$

pois $R_{\mathbb{Q}}(s) = 1$. Subtraindo (3.11) de (3.10) obtemos

$$\sum_p \frac{A_p - 1}{p^s} = \log\left(\frac{\zeta_K(s)}{\zeta(s)}\right) - \sum_p \sum_{m \geq 2} \frac{A_p - 1}{m p^{ms}} - \log R_K(s). \quad (3.12)$$

Segue do Teorema 3.6 que $\zeta_K(s)/\zeta(s)$ é analítica em um aberto que contém o semiplano fechado $\mathrm{Re}(s) \geq 1$ (os polos simples das funções $\zeta_K(s)$ e $\zeta(s)$ "se cancelam" quando tomamos o quociente $\zeta_K(s)/\zeta(s)$), e essa função não se anula nesse aberto. Assim $\log(\zeta_K(s)/\zeta(s))$ possui uma extensão analítica a um aberto que contém o semiplano fechado $\mathrm{Re}(s) \geq 1$.

A função $(-\log(1-z) - z)/z^2$ possui uma extensão analítica à bola aberta de centro 0 e raio 1 pois a singularidade em $z = 1$ é removível. Assim, existe $M > 0$ tal que

$$\text{se } |z| \leq \frac{1}{\sqrt{2}}, \quad \text{então} \quad \left| -\log(1-z) - z \right| \leq M z^2.$$

Fixemos $\varepsilon > 0$. Notando também que $A_p \leq B_p \leq n$ temos, para $s = \sigma + it$, com $\sigma, t \in \mathbb{R}$, $\sigma \geq 1/2 + \varepsilon$;

$$\sum_p \sum_{m \geq 2} \left| \frac{A_p - 1}{m p^{ms}} \right| \leq \sum_p \sum_{m \geq 2} \frac{n+1}{m p^{m\sigma}} = (n+1) \sum_p \left(-\log\left(1 - \frac{1}{p^\sigma}\right) - \frac{1}{p^\sigma} \right)$$
$$\leq (n+1) \sum_p \frac{M}{p^{2\sigma}} \leq (n+1) \sum_p \frac{M}{p^{1+2\varepsilon}} < \infty.$$

Portanto a série $\sum_p \sum_{m \geq 2} (A_p - 1)/(m p^{ms})$ define uma função analítica no semiplano aberto $\mathrm{Re}(s) > 1/2$.

Dessa forma, todos os termos do lado direito de (3.12) possuem uma extensão analítica a um aberto contendo o semiplano fechado $\mathrm{Re}(s) \geq 1$. Como também $A_p \leq n$ para todo primo p, pelo uso de um teorema tauberiano (o Corolário C.4 do apêndice C) temos que a série $\sum_p (A_p - 1)/p$ é convergente. □

Capítulo 4

Uma demonstração do Teorema dos Números Primos

Neste Capítulo, veremos uma demonstração do Teorema dos Números Primos (o Teorema 1.4) que serve de motivação para o Λ-cálculo de Golomb.

4.1 Funções aritméticas

Paramos um momento para lembrar a definição de algumas funções usuais da Teoria dos Números, e algumas de suas propriedades básicas. As demonstrações de todas essas propriedades podem ser encontradas em [Apo76].

- Dado $n \in \mathbb{N}$, denotamos por $\omega(n)$ o número de fatores primos de n, isto é;

$$\omega(n) \doteq \#\{p \in \mathbb{N} \text{ primo} : p \mid n\},$$

  em que tomamos $\omega(1) = 0$.

- A função de von Mangoldt, $\Lambda(n)$, é dada por:

$$\Lambda(n) = \begin{cases} \log p, & \text{se } n = p^k, \text{ com } p \text{ primo} \\ 0, & \text{caso contrário.} \end{cases}$$

  Em particular, $\Lambda(1) = 0$.

- A função de Möbius, $\mu(n)$, é dada por

$$\mu(n) = \begin{cases} (-1)^{\omega(n)}, & \text{se } n \text{ é livre de quadrados, ou } n = 1 \\ 0, & \text{caso contrário.} \end{cases}$$

  Definimos assim $\mu(1) = 1$.

Ou seja, escrevendo $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m} > 1$, com $p_1, \ldots, p_m$ primos distintos e $k_1, \ldots, k_m \in \mathbb{N}$, temos $\omega(n) = m$, e

$$\Lambda(n) = \begin{cases} \log p_1, & \text{se } n = p_1^{k_1} \\ 0, & \text{se } m > 1. \end{cases} \qquad \mu(n) = \begin{cases} (-1)^m, & \text{se } n = p_1 p_2 \cdots p_m \\ 0, & \text{se existe } k_j > 1. \end{cases}$$

A função de Möbius possui a seguinte propriedade importante: para $n \in \mathbb{N}$, vale

$$\sum_{d \mid n} \mu(d) = \begin{cases} 0, & \text{se } n > 1 \\ 1, & \text{se } n = 1, \end{cases} \tag{4.1}$$

em que a notação $\sum_{d|n}$ significa que a soma é tomada sobre todos os divisores $d \in \mathbb{N}$ de n. Além disso, a função μ é *multiplicativa*, isto é; se $m, n \in \mathbb{N}$ são relativamente primos, então $\mu(mn) = \mu(m)\mu(n)$.

Para $n \in \mathbb{N}$, temos a seguinte expressão de Λ:

$$\Lambda(n) = \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right). \tag{4.2}$$

Escrevendo $\log(n/d) = \log n - \log d$ em (4.2) e usando (4.1) temos, para $n > 1$,

$$\Lambda(n) = \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d = -\sum_{d|n} \mu(d) \log d. \tag{4.3}$$

Para $x > 1$, a função ψ de Chebyshev é dada por

$$\psi(x) = \sum_{n \leq x} \Lambda(n),$$

A função $\psi(x)$ está intimamente relacionada à função $\pi(x)$, de modo que vale o Teorema:

Teorema 4.1. *Vale:*

$$\pi(x) \sim \frac{x}{\log x} \quad \textit{se, e somente se,} \quad \psi(x) \sim x.$$

Esse Teorema é um resultado clássico da Teoria dos Números, cuja demonstração usual pode ser encontrada em [Apo76]. Demonstraremos depois o Teorema 4.1 de um modo bem diferente. (O Teorema 4.1 é um caso particular do Teorema 5.1.)

Em alguns casos é mais simples tratar dessa função $\psi(x)$ do que da função $\pi(x)$, e, de fato, provaremos o Teorema dos Números Primos demonstrando $\psi(x) \sim x$, e não diretamente $\pi(x) \sim x/\log x$.

A função ζ de Riemann é dada por

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}},$$

para $\mathrm{Re}(s) > 1$. Lembramos que a função $\zeta(s)$ possui uma extensão meromorfa a todo o plano complexo $\mathbb{C}$, tendo apenas um polo simples em $s = 1$ com resíduo 1. Assumiremos também os resultados básicos sobre Séries de Dirichlet que podem ser encontrados em [Apo76, Cap. 11].

4.2 O Teorema de Hardy-Littlewood

O ponto de partida da demonstração que faremos do Teorema dos Números Primos é o Teorema Tauberiano de Hardy-Littlewood (o Teorema 4.4). Dedicamos esta Seção ao seu enunciado e à sua demonstração, que foi tirada de [Tit39].

Para $f : [0, 1] \to \mathbb{R}$ limitada, definimos

$$\|f\|_\infty = \sup_{x \in [0,1]} |f(x)|.$$

Vamos usar o seguinte conhecido Teorema de Weierstrass:

Teorema 4.2 (Weierstrass)**.** *Seja $f : [0, 1] \to \mathbb{R}$ contínua. Dado $\varepsilon > 0$ existe um polinômio p de coeficientes reais tal que $\|f - p\|_\infty < \varepsilon$.*

Mais precisamente, vamos utilizar um Corolário do Teorema 4.2. Nesse enunciado, dizemos que

uma função g tem *uma descontinuidade de tipo 1* em $c \in [0,1]$ se existirem os limites

$$g(c-) \doteq \lim_{x \to c^-} g(x) \quad \text{e} \quad g(c+) = \lim_{x \to c^+} g(x)$$

mas $g(c-) \neq g(c+)$.

Corolário 4.3. *Seja $g : [0,\,1] \to \mathbb{R}$ contínua, ou contínua a menos de uma única descontinuidade de tipo 1 em $[0,\,1]$. Dado $\varepsilon > 0$ existem polinômios reais p e P tais que*

$$p(x) \leq g(x) \leq P(x), \quad \textit{para todo } x \in [0,\,1], \tag{4.4}$$

e

$$0 \leq \int_0^1 \big[g(\xi) - p(\xi)\big]\,\mathrm{d}\xi \leq \varepsilon \quad e \quad 0 \leq \int_0^1 \big[P(\xi) - g(\xi)\big]\,\mathrm{d}\xi \leq \varepsilon. \tag{4.5}$$

Demonstração. a) Façamos primeiramente o caso em que g é contínua. Pelo Teorema 4.2 existe um polinômio q tal que $\|g - q\|_\infty < \varepsilon/2$. Então, sejam $p(x) = q(x) - \varepsilon/2$ e $P(x) = q(x) + \varepsilon/2$ polinômios. Assim vale (4.4) e também $\|p - g\|_\infty < \varepsilon$ e $\|P - g\|_\infty < \varepsilon$, logo vale (4.5).

b) Suponhamos agora que g possui uma descontinuidade de tipo 1 em $c \in [0,\,1]$. Provemos o resultado para $c \in]0,1[$. Os casos $c = 0$ e $c = 1$ são análogos.

Seja $\delta > 0$ com $\delta < \min\{c, 1-c\}$. Sejam l_δ, L_δ funções afins ($l(x) = ax + b$) tais que

$$l_\delta(c-\delta) = g(c-\delta), \quad L_\delta(c+\delta) = g(c+\delta), \quad \text{e}$$
$$l_\delta(c) = L_\delta(c) = \max\{g(c-), g(c+), g(c)\}.$$

(Tomamos $\delta > 0$ suficientemente pequeno para termos $c - \delta$ e $c + \delta$ em $[0,1]$.) Defina

$$f_\delta(x) = \begin{cases} g(x), & \text{se } x \leq c-\delta \text{ ou } x \geq c+\delta \\ \max\{g(x), l_\delta(x)\}, & \text{se } c-\delta < x \leq c \\ \max\{g(x), L_\delta(x)\}, & \text{se } c < x < c+\delta \end{cases}$$

Então $g(x) \leq f_\delta(x) \leq \|g\|_\infty$ para todo $x \in [0,1]$, e pelo Teorema da Convergência Dominada de Lebesgue existe $\delta > 0$ tal que

$$0 \leq \int_0^1 \big[f_\delta(\xi) - g(\xi)\big]\,\mathrm{d}\xi \leq \frac{\varepsilon}{2}. \tag{4.6}$$

Como também f_δ é contínua, pelo caso a) existe um polinômio P tal que $f_\delta(x) \leq P(x)$ para $x \in [0,\,1]$ e

$$0 \leq \int_0^1 \big[P(\xi) - f_\delta(\xi)\big]\,\mathrm{d}\xi \leq \frac{\varepsilon}{2}. \tag{4.7}$$

Assim sendo, temos $g(x) \leq f_\delta(x) \leq P(x)$ para $x \in [0,\,1]$ e de (4.6) e (4.7),

$$0 \leq \int_0^1 \big[P(\xi) - g(\xi)\big]\,\mathrm{d}\xi \leq \varepsilon.$$

Analogamente obtemos também um polinômio p com as propriedades desejadas. □

Agora podemos demonstrar o Teorema:

Teorema 4.4 (Hardy-Littlewood)**.** *Seja $(a_n)_{n\geq 0}$ uma sequência de números não-negativos tal que a série de potências $\sum_{n=0}^\infty a_n x^n$ tem raio de convergência maior ou igual a 1, e*

$$\lim_{x \to 1^-} (1-x) \sum_{n=0}^{\infty} a_n x^n = A. \tag{4.8}$$

Então

$$\frac{1}{N}\sum_{n=0}^{N} a_n \to A \quad \textit{quando } N \to +\infty.$$

Demonstração. Basta demonstrar o Teorema para o caso $A = 1$. O caso geral segue desse tomando $a'_n = a_n/A$ para todo $n \in \mathbb{N}$ e aplicando o caso $A = 1$ à sequência $\{a'_n\}_{n\geq 0}$.

Provemos primeiramente que

$$\lim_{x\to 1^-} (1-x)\sum_{n=0}^{\infty} a_n x^n p(x^n) = \int_0^1 p(\xi)\,\mathrm{d}\xi \tag{4.9}$$

para um polinômio qualquer p. Pela linearidade da expressão em p, basta considerar o caso $p(x) = x^k$. Nesse caso,

$$\begin{aligned}(1-x)\sum_{n=0}^{+\infty} a_n x^n p(x^n) &= (1-x)\sum_{n=0}^{+\infty} a_n x^n x^{nk} = (1-x)\sum_{n=0}^{+\infty} a_n (x^{k+1})^n \\ &= \frac{1-x}{1-x^{k+1}}\cdot(1-x^{k+1})\sum_{n=0}^{+\infty} a_n (x^{k+1})^n, \end{aligned}\tag{4.10}$$

e como $x^{k+1} \in [0,\, 1)$, temos a convergência da série $\sum a_n x^n p(x^n)$. De (4.8) (com $A = 1$), temos

$$\lim_{x\to 1^-} (1-x^{k+1})\sum_{n=0}^{+\infty} a_n (x^{k+1})^n = 1.$$

Agora fazemos $x \to 1^-$ em (4.10) e notando que $\lim_{x\to 1^-}(1-x)/(1-x^{k+1}) = 1/(k+1)$ temos

$$\lim_{x\to 1^-} (1-x)\sum_{n=0}^{+\infty} a_n x^n p(x^n) = \frac{1}{k+1}\cdot 1 = \int_0^1 p(\xi)\,\mathrm{d}\xi.$$

Assim provamos (4.9).

Provemos agora que se $g : [0,\, 1] \to \mathbb{R}$ é contínua a menos de, possivelmente, uma única descontinuidade de tipo 1, então

$$\lim_{x\to 1^-} (1-x)\sum_{n=0}^{+\infty} a_n x^n g(x^n) = \int_0^1 g(\xi)\,\mathrm{d}\xi. \tag{4.11}$$

Como vimos no Corolário 4.3, dado $\varepsilon > 0$ existem p e P polinômios satisfazendo (4.4) e (4.5) para a g dada. Assim, como $(1-x)a_n x^n \geq 0$ e $g(x) \leq P(x)$ para todo $x \in [0, 1]$, temos

$$(1-x)\sum_{n=0}^{+\infty} a_n x^n g(x^n) \leq (1-x)\sum_{n=0}^{+\infty} a_n x^n P(x^n)$$

para todo $x \in]0,\, 1[$. Fazendo então $x \to 1^-$ temos, usando (4.9) e (4.5),

$$\limsup_{x\to 1^-}(1-x)\sum_{n=0}^{+\infty} a_n x^n g(x^n) \leq \int_0^1 P(\xi)\,\mathrm{d}\xi \leq \int_0^1 g(\xi)\,\mathrm{d}\xi + \varepsilon.$$

Analogamente temos

$$\int_0^1 g(\xi)\,\mathrm{d}\xi - \varepsilon \leq \int_0^1 p(\xi)\,\mathrm{d}\xi \leq \liminf_{x\to 1^-}(1-x)\sum_{n=0}^{+\infty} a_n x^n g(x^n).$$

E assim, como $\varepsilon > 0$ é arbitrário, temos (4.11).

Vamos aplicar a igualdade (4.11) à função

$$g(x) = \begin{cases} 0, & \text{se } 0 \le x < 1/e \\ 1/x, & \text{se } 1/e \le x \le 1. \end{cases}$$

Agora se $x > 0$, temos $g(x^n) \neq 0$ se, e somente se $n \le -1/\log x$. Logo

$$(1-x)\sum_{n=0}^{+\infty} a_n x^n g(x^n) = (1-x)\sum_{n \le -1/\log x} a_n x^n \frac{1}{x^n} = (1-x)\sum_{n \le 1/\log(1/x)} a_n.$$

Escolhemos então $x = e^{-1/N}$. Assim

$$(1-x)\sum_{n=0}^{+\infty} a_n x^n g(x^n) = (1-e^{-1/N})\sum_{n \le N} a_n.$$

Fazendo $N \to +\infty$, temos $x = e^{-1/N} \to 1$ e de (4.11) segue que

$$\lim_{N\to+\infty}(1-e^{-1/N})\sum_{n=0}^{N} a_n = \int_0^1 g(\xi)\,\mathrm{d}\xi = \int_{1/e}^1 \frac{1}{\xi}\,\mathrm{d}\xi = -\log(e^{-1}) = 1. \tag{4.12}$$

Agora, vale $1 - e^{-1/N} \sim 1/N$ quando $N \to +\infty$. Dessa forma (4.12) implica de fato

$$\lim_{N\to+\infty}\frac{1}{N}\sum_{n=0}^{N} a_n = 1. \qquad \square$$

4.3 Um teorema abeliano

Vamos usar também um teorema do tipo abeliano, mais precisamente, a regularidade da transformada de Lambert (a Proposição B.12), que enunciamos da seguinte forma:

Teorema 4.5. *Seja $(a_n)_{n\in\mathbb{N}}$ uma sequência de números reais tal que a série $\sum_{n=1}^{+\infty} a_n$ é convergente. Então existe $Y > 0$ tal que $\sum_{n=1}^{+\infty} a_n n y e^{-ny}/(1-e^{-ny})$ converge, para todo $y \in (0, Y]$, e*

$$\lim_{y\to0^+}\sum_{n=1}^{+\infty} a_n \frac{nye^{-ny}}{1-e^{-ny}} = \sum_{n=1}^{+\infty}\lim_{y\to0^+}\left(a_n\frac{nye^{-ny}}{1-e^{-ny}}\right) = \sum_{n=1}^{+\infty} a_n.$$

Na realidade, vamos usar um Corolário do Teorema 4.5 que se adapta melhor ao nosso caso:

Corolário 4.6. *Seja $(a_n)_{n\in\mathbb{N}}$ uma sequência de números reais tal que a série $\sum_{n=1}^{+\infty} a_n/n$ é convergente. Então existe $X < 1$ tal que $\sum_{n=1}^{+\infty} a_n x^n/(1+x+\cdots+x^{n-1})$ converge para todo $x \in [X, 1)$, e*

$$\lim_{x\to1^-}\sum_{n=1}^{+\infty} a_n \frac{x^n}{1+x+\cdots+x^{n-1}} = \sum_{n=1}^{+\infty}\lim_{x\to1^-}\left(a_n\frac{x^n}{1+x+\cdots+x^{n-1}}\right) = \sum_{n=1}^{+\infty}\frac{a_n}{n}.$$

Demonstração. Colocando $x = e^{-y}$, temos

$$\sum_{n=1}^{+\infty} a_n \frac{x^n}{1+x+\cdots+x^{n-1}} = \sum_{n=1}^{+\infty} a_n \frac{(1-x)x^n}{1-x^n} = \frac{1-e^{-y}}{y}\sum_{n=1}^{+\infty}\frac{a_n}{n}\frac{nye^{-ny}}{1-e^{-ny}}.$$

De $\lim_{y\to0^+}(1-e^{-y})/y = 1$, aplicando o Teorema 4.5 temos o resultado. $\square$

4.4 Demonstração do Teorema dos Números Primos

No momento evitaremos explicar detalhadamente todas as passagens da demonstração a seguir, pois essas passagens serão justificadas futuramente em um contexto mais geral. Para melhor referência, assinalaremos por $(\star)$ as passagens que serão justificadas depois.

Em vista da relação entre $\pi(x)$ e $\psi(x)$ expressa no Teorema 4.1, queremos provar que $\psi(x) \sim x$, isto é; que $\lim_{x\to+\infty} \psi(x)/x = 1$. Como $\psi(x) = \sum_{n\leq x} \Lambda(n)$, provar $\psi(x) \sim x$ é equivalente a provar

$$\lim_{N\to+\infty} \frac{1}{N} \sum_{n=0}^{N} \Lambda(n) = 1. \tag{4.13}$$

Vamos usar o Teorema 4.4 para provar a igualdade (4.13). Para aplicar esse Teorema, precisamos provar que a série de potências

$$\sum_{n=1}^{+\infty} \Lambda(n) x^n \tag{4.14}$$

tem raio de convergência maior ou igual a 1, e provar que

$$\lim_{x\to1^-} (1-x) \sum_{n=1}^{+\infty} \Lambda(n) x^n = 1.$$

Agora,

$$\limsup_{n\to+\infty} \sqrt[n]{\Lambda(n)} \leq \limsup_{n\to+\infty} \sqrt[n]{\log n} = \lim_{n\to+\infty} \exp\left(\frac{1}{n}\log\log n\right) = e^0 = 1,$$

logo a série (4.14) tem raio de convergência maior ou igual a 1.

Usando (4.3) temos, para $0 < x < 1$,

$$\begin{aligned}\sum_{n=1}^{+\infty} \Lambda(n) x^n &= \sum_{n=1}^{+\infty} \left(-\sum_{d|n} \mu(d)\log d\right) x^n \overset{(\star)}{=} -\sum_{d=1}^{+\infty} \mu(d)\log d \sum_{k=1}^{+\infty} x^{kd} \\ &= -\sum_{d=1}^{+\infty} \mu(d)\log(d)\frac{x^d}{1-x^d} = -\sum_{d=1}^{+\infty} \frac{\mu(d)\log(d)x^d}{(1-x)(1+x+\cdots+x^{d-1})}.\end{aligned}$$

Dessa forma,

$$\lim_{x\to1^-} (1-x)\sum_{n=1}^{+\infty} \Lambda(n)x^n = \sum_{d=1}^{+\infty} \lim_{x\to1^-} \left(\frac{-\mu(d)\log(d)x^d}{1+x+\cdots+x^{d-1}}\right) = \sum_{d=1}^{+\infty} \frac{-\mu(d)\log d}{d},$$

sendo que podemos trocar o limite com a série usando o Corolário 4.6 e pois a série $\sum_{d=1}^{+\infty} \mu(d)\log d/d$ é convergente, como será justificado futuramente. Dessa forma

$$\begin{aligned}\lim_{x\to1^-} (1-x)\sum_{n=1}^{+\infty} \Lambda(n)x^n &= \sum_{d=1}^{+\infty} \frac{-\mu(d)\log d}{d} \overset{(\star)}{=} \lim_{\sigma\to1^+} \sum_{d=1}^{+\infty} \frac{-\mu(d)\log d}{d^\sigma} \\ &= \lim_{\sigma\to1^+} \left(\frac{1}{\zeta(\sigma)}\right)' = \lim_{\sigma\to1^+} \frac{-\zeta'(\sigma)}{\zeta^2(\sigma)} = 1.\end{aligned}$$

Temos que $\lim_{\sigma\to1^+} -\zeta'(\sigma)/\zeta^2(\sigma) = 1$ simplesmente pelo fato de que $\zeta(s)$ possui em $s = 1$ um polo simples com resíduo 1. Portanto, aplicando o Teorema 4.4 temos $\psi(n) \sim n$. □

Capítulo 5

O Λ-cálculo de Golomb com séries de potências

Voltemos agora à Conjectura de Bateman-Horn. Seja $f_1(X), \ldots, f_k(X)$ uma família apropriada de polinômios. Vamos nos basear na demonstração que fizemos do Teorema dos Números Primos para tentar demonstrar a Conjectura 6.

Um passo importante da demonstração foi substituir a análise da função $\pi(x)$ pela da função $\psi(x)$. A função equivalente à $\psi(x)$ para o nosso caso com k polinômios é a seguinte função

$$\psi_{\mathbf{f}}(x) \doteq \sum_{n \leq x} \Lambda\big(f_1(n)\big)\Lambda\big(f_2(n)\big)\ldots\Lambda\big(f_k(n)\big).$$

Precisamos então demonstrar uma equivalência análoga à do Teorema 4.1.

5.1 A equivalência entre $\pi_{\mathbf{f}}(x)$ e $\psi_{\mathbf{f}}(x)$

Fixemos $f_1(X), \ldots, f_k(X)$ uma família apropriada de polinômios para o resto desta Seção. Fixemos também $\mathbf{f} \doteq (f_1, \ldots, f_k)$.

Vamos aqui seguir o artigo de Baier [Bai02] para demonstrar o seguinte Teorema:

Teorema 5.1. *Vale a seguinte equivalência:*

$$\pi_{\mathbf{f}}(x) \sim \frac{C(\mathbf{f})}{h_1 \cdots h_k} \cdot \frac{x}{\log^k x} \quad \textit{se, e somente se,} \quad \psi_{\mathbf{f}}(x) \sim C(\mathbf{f})x$$

Definimos, além da função $\psi_{\mathbf{f}}$, a função $\theta_{\mathbf{f}}$ dada por

$$\theta_{\mathbf{f}}(x) \doteq \sum_{n \leq x;\, f_1(n),\ldots,f_k(n) \text{ são todos primos}} \log f_1(n) \cdot \log f_2(n) \cdot \cdots \cdot \log f_k(n).$$

A função $\theta_{\mathbf{f}}(x)$ serve de função intermediária entre $\pi_{\mathbf{f}}(x)$ e $\psi_{\mathbf{f}}(x)$ do mesmo modo como no caso clássico do Teorema dos Números Primos temos a função θ de Chebyshev dada por

$$\theta(x) \doteq \sum_{p \leq x} \log p.$$

De fato, não provaremos diretamente o Teorema 5.1; provaremos primeiro uma equivalência entre as funções $\pi_{\mathbf{f}}(x)$ e $\theta_{\mathbf{f}}(x)$ (o Teorema 5.3), e depois uma equivalência entre as funções $\theta_{\mathbf{f}}(x)$ e $\psi_{\mathbf{f}}(x)$ (o Teorema 5.7). Juntando essas duas equivalências obtemos o Teorema 5.1.

Vamos usar o seguinte Lema, cuja demonstração (em um caso mais geral, que não usaremos aqui) pode ser encontrada em [Apo76]:

Lema 5.2 (Identidade de Abel)**.** *Sejam $g : (0, +\infty) \to \mathbb{R}$ uma função com derivada contínua e $(c_n)_{n\in\mathbb{N}}$ uma sequência de números reais. Seja $C(x) \doteq \sum_{n\leq x} c_n$ (de modo que $C(t) = 0$ se $t < 1$). Então vale a igualdade*

$$\sum_{n\leq x} c_n g(n) = g(x)C(x) - \int_1^x g'(t)C(t)\,\mathrm{d}t.$$

Teorema 5.3. *Vale:*

$$\pi_{\mathbf{f}}(x) \sim \frac{C(\mathbf{f})}{h_1\cdots h_k}\cdot\frac{x}{\log^k x} \quad \textit{se, e somente se,} \quad \theta_{\mathbf{f}}(x) \sim C(\mathbf{f})x.$$

Demonstração. Definimos

$$a_n \doteq \begin{cases} 1, & \text{se } f_1(n),\ldots,f_k(n) \text{ são todos primos} \\ 0, & \text{caso contrário} \end{cases}$$

e para $x \geq 0$ seja

$$g(x) \doteq \log f_1(x)\cdot\log f_2(x)\cdot\cdots\cdot\log f_k(x).$$

Temos assim $\pi_{\mathbf{f}}(x) = \sum_{n\leq x} a_n$ e $\theta_{\mathbf{f}}(x) = \sum_{n\leq x} a_n g(n)$. Então, pelo Lema 5.2,

$$\theta_{\mathbf{f}}(x) = g(x)\pi_{\mathbf{f}}(x) - \int_1^x g'(t)\pi_{\mathbf{f}}(t)\,\mathrm{d}t. \tag{5.1}$$

Por outro lado, se $b_n \doteq a_n g(n)$, temos $\theta_{\mathbf{f}}(x) = \sum_{n\leq x} b_n$ e $\pi_{\mathbf{f}}(x) = \sum_{n\leq x} a_n = \sum_{n\leq x} b_n/g(n)$. Assim, usando novamente o Lema 5.2 temos

$$\pi_{\mathbf{f}}(x) = \frac{1}{g(x)}\theta_{\mathbf{f}}(x) + \int_1^x \frac{g'(t)}{g(t)^2}\theta_{\mathbf{f}}(t)\,\mathrm{d}t. \tag{5.2}$$

Vale também a seguinte igualdade:

$$\frac{g'(x)}{g(x)} = \sum_{i=1}^{k} \frac{f_i'(x)}{\big(\log f_i(x)\big)\cdot f_i(x)}. \tag{5.3}$$

Segue que $g'(x)/g(x) > 0$ para todo $x \geq 0$ pois para todo $i \in \{1,\ldots,k\}$, temos $f_i(x)$ estritamente crescente para $x > -1$, e $f_i(x) > 1$ para todo $x \geq 0$.

($\Rightarrow$): Suponhamos que vale

$$\pi_{\mathbf{f}}(x) \sim \frac{C(\mathbf{f})}{h_1\ldots h_k}\cdot\frac{x}{\log^k x}. \tag{5.4}$$

Queremos provar que $\theta_{\mathbf{f}}(x)/x \to C(\mathbf{f})$. Então dividimos (5.1) por x, e obtemos

$$\frac{\theta_{\mathbf{f}}(x)}{x} = \frac{\pi_{\mathbf{f}}(x)g(x)}{x} - \frac{1}{x}\int_1^x g'(t)\pi_{\mathbf{f}}(t)\,\mathrm{d}t. \tag{5.5}$$

Como $g(x) \sim h_1\cdots h_k \log^k x$ (pois é fácil ver que $\log f_j(x) \sim h_j \log x$ para cada $j \in \{1,\ldots,k\}$), segue de (5.4) que

$$\lim_{x\to+\infty} \frac{\pi_{\mathbf{f}}(x)g(x)}{x} = C(\mathbf{f}). \tag{5.6}$$

Assim, se provarmos que

$$\int_1^x g'(t)\pi_{\mathbf{f}}(t)\,\mathrm{d}t = o(x), \tag{5.7}$$

tomando o limite para $x \to +\infty$ em (5.5) temos que (5.6) implica $\theta_{\mathbf{f}}(x) \sim C(\mathbf{f})x$, como queríamos demonstrar.

Provemos então que vale (5.7). Por (5.6), temos

$$\pi_{\mathbf{f}}(x) \ll \frac{x}{g(x)}.$$

Logo, usando (5.3),

$$\int_1^x g'(t)\pi_{\mathbf{f}}(t)\,\mathrm{d}t \ll \int_1^x g'(t)\frac{t}{g(t)}\,\mathrm{d}t = \sum_{i=1}^k \int_1^x \frac{tf_i'(t)}{\big(\log f_i(t)\big)\cdot f_i(t)}\,\mathrm{d}t$$
$$\ll \sum_{i=1}^k \int_1^x \frac{1}{\log f_i(t)}\,\mathrm{d}t,$$

em que usamos que $tf_i'(t)/f_i(t) \ll 1$ para todo $i \in \{1,\dots,k\}$. De fato, se $f_i(t)$ é polinômio de grau h_i, então $f_i'(t)$ tem grau $h_i - 1$, de modo que $tf_i'(t)$ tem o mesmo grau de $f_i(t)$, o que implica que existe o limite de $tf_i'(t)/f_i(t)$ quando $t \to +\infty$. Em particular, $tf_i'(t)/f_i(t) \ll 1$. Agora,

$$\int_1^x g'(t)\pi_{\mathbf{f}}(t)\,\mathrm{d}t \ll \sum_{i=1}^k \int_1^x \frac{1}{\log f_i(t)}\,\mathrm{d}t = o(x) \tag{5.8}$$

pois é fácil ver, usando a Regra de l'Hôpital, que

$$\int_1^x \frac{1}{\log f_i(t)}\,\mathrm{d}t = o(x)$$

para todo $i \in \{1,\dots,k\}$. (De fato temos

$$\lim_{x\to+\infty}\int_1^x \frac{1}{\log f_i(t)}\,\mathrm{d}t = +\infty$$

pois $\log f_i(t) \sim h_i \log t \le h_i.t$ e assim, para algum $x_0 > 1$ e alguma constante $C > 0$, temos

$$\int_{x_0}^x \frac{1}{\log f_i(t)}\,\mathrm{d}t \ge C\int_{x_0}^x \frac{1}{t}\,\mathrm{d}t \to +\infty$$

quando $x \to +\infty$.) Dessa forma, (5.8) implica (5.7) que, por sua vez, implica $\theta_{\mathbf{f}}(x) \sim C(\mathbf{f})x$.

($\Leftarrow$): Suponhamos que vale

$$\theta_{\mathbf{f}}(x) \sim C(\mathbf{f})x. \tag{5.9}$$

Então de (5.2) temos

$$\frac{\pi_{\mathbf{f}}(x)g(x)}{x} = \frac{\theta_{\mathbf{f}}(x)}{x} + \frac{g(x)}{x}\int_1^x \theta_{\mathbf{f}}(t)\frac{g'(t)}{g(t)^2}\,\mathrm{d}t. \tag{5.10}$$

Assim, se provarmos que

$$\int_1^x \theta_{\mathbf{f}}(t)\frac{g'(t)}{g(t)^2}\,\mathrm{d}t = o\left(\frac{x}{g(x)}\right), \tag{5.11}$$

fazendo $x \to +\infty$ em (5.10) veremos que

$$\lim_{x\to+\infty}\frac{\pi_{\mathbf{f}}(x)g(x)}{x} = \lim_{x\to+\infty}\frac{\theta_{\mathbf{f}}(x)}{x} = C(\mathbf{f}).$$

Então usando $g(x) \sim h_1 \dots h_k \log^k x$ teremos de fato que

$$\pi_{\mathbf{f}}(x) \sim \frac{C(\mathbf{f})}{h_1\cdots h_k}\cdot\frac{x}{\log^k x}$$

como queríamos demonstrar.

Provemos então que vale (5.11). De (5.9) temos em particular que $\theta_{\mathbf{f}}(x) \ll x$. Logo, usando também (5.3),

$$\int_1^x \theta_{\mathbf{f}}(t)\frac{g'(t)}{g(t)^2}\,\mathrm{d}t \ll \int_1^x \frac{t}{g(t)}\frac{g'(t)}{g(t)}\,\mathrm{d}t = \sum_{i=1}^{k}\int_1^x \frac{t}{g(t)}\frac{f_i'(t)}{\big(\log f_i(t)\big)\cdot f_i(t)}\,\mathrm{d}t$$
$$\ll \sum_{i=1}^{k}\int_1^x \frac{1}{g(t)\log f_i(t)}\,\mathrm{d}t$$

em que usamos, como no caso anterior, $tf_i'(t)/f_i(t) \ll 1$ para todo $i \in \{1,\dots,k\}$. Agora, provemos que

$$\int_1^x \theta_{\mathbf{f}}(t)\frac{g'(t)}{g(t)^2}\,\mathrm{d}t \ll \sum_{i=1}^{k}\int_1^x \frac{1}{g(t)\log f_i(t)}\,\mathrm{d}t = o\left(\frac{x}{g(x)}\right). \tag{5.12}$$

Fixemos $i \in \{1,\dots,k\}$. Então $g(t)\log f_i(t) \sim h_1\cdots h_k.h_i.\log^{k+1} t \ll t$ e, de modo análogo ao caso anterior, vale

$$\lim_{x\to+\infty}\int_1^x \frac{1}{g(t)\log f_i(t)}\,\mathrm{d}t = +\infty.$$

Assim, aplicando a Regra de l'Hôpital, temos

$$\lim_{x\to+\infty}\frac{\int_1^x (g(t)\log f_i(t))^{-1}\,\mathrm{d}t}{x/g(x)} = \lim_{x\to+\infty}\frac{1/(g(x)\log f_i(x))}{(g(x)-xg'(x))/g(x)^2} = \lim_{x\to+\infty}\frac{1}{\log f_i(x)}\cdot\frac{g(x)}{g(x)-xg'(x)}$$
$$= \lim_{x\to+\infty}\frac{1}{\log f_i(x)}\cdot\frac{1}{1-\dfrac{xg'(x)}{g(x)}} = 0,$$

sendo que é fácil ver que

$$\lim_{x\to+\infty}\frac{xg'(x)}{g(x)} = 0$$

usando (5.3). Dessa forma, de fato vale (5.12) o que, como vimos, implica

$$\pi_{\mathbf{f}}(x) \sim \frac{C(\mathbf{f})}{h_1\cdots h_k}\cdot\frac{x}{\log^k x}. \qquad \square$$

A equivalência que queremos provar agora,

$$\theta_{\mathbf{f}}(x) \sim C(\mathbf{f})x \quad \text{se, e somente se,} \quad \psi_{\mathbf{f}}(x) \sim C(\mathbf{f})x,$$

diz basicamente que, no cálculo de $\psi_{\mathbf{f}}(x)$, a contribuição dos n tais que $f_1(n),\dots,f_k(n)$ são potências maiores do que 1 de primos é pequena. Para prová-la, estimaremos então os seguintes números:

Definição. Sejam $f_0(X) \in \mathbb{Z}[X]$ e $k \in \mathbb{N}$, $k \geq 2$. Definimos

$$Z_k(f_0;x) \doteq \#\big\{n \in \mathbb{N},\, n \leq x \,:\, \text{existe } m \in \mathbb{Z} \text{ tal que } f_0(n) = m^k\big\}.$$

Lema 5.4. *Sejam $b \in \mathbb{N}$, $b \geq 2$ livre de quadrados e A o anel de inteiros algébricos do corpo $\mathbb{Q}(\sqrt{b})$. Denotemos por $\mathrm{N} : \mathbb{Q}(\sqrt{b}) \to \mathbb{Q}$ a função norma no corpo $\mathbb{Q}(\sqrt{b})$. Seja $D \in \mathbb{N}$. Supomos que a equação*

$$\mathrm{N}(\beta) = \pm D \tag{5.13}$$

possui alguma solução $\beta \in A$. Então existem u_0 unidade de A e $S \subseteq A$ finito tais que toda solução β da equação (5.13) é da forma

$$\beta = \pm u_0^j\gamma$$

com $j \in \mathbb{Z}$ e $\gamma \in S$.

Demonstração. Como existe $\beta \in A$ tal que $\mathrm{N}(\beta) = \pm D$, temos $\mathrm{N}(\beta A) = |\mathrm{N}(\beta)| = D$, isto é, existe um ideal inteiro I de A com norma D. Sejam $I_1, \dots I_l$ todos os ideais inteiros de A com norma igual a D (só pode existir uma quantidade finita desses ideais). Sejam $x_1 A, \dots, x_m A$ os ideais principais dentre os ideais $I_1, \dots, I_l$, e seja $S \doteq \{x_1, \dots, x_m\}$.

Pelo Teorema das Unidades de Dirichlet, existe $u_0 \in A$, unidade, tal que toda unidade u de A é da forma

$$u = \pm u_0^j$$

para algum $j \in \mathbb{Z}$.

Seja então $\beta \in A$ tal que $\mathrm{N}(\beta) = \pm D$. Então $\mathrm{N}(\beta A) = |\mathrm{N}(\beta)| = D$, e, portanto, existe $\gamma \in S$ tal que $\beta A = \gamma A$. Dessa forma, existe $u \in A$ unidade tal que $\beta = \gamma u$. Assim, existe $j \in \mathbb{Z}$ tal que $\beta = \pm u_0^j \gamma$. □

Usaremos também o seguinte resultado da Geometria Diofantina. Stephan Baier, em [Bai02, p. 6], nota que sua demonstração segue do Teorema D.8.3 e do Exercício D.6.(b) de [HS00]:

Teorema 5.5. *Seja $f_0(X) \in \mathbb{Q}[X]$ irredutível de grau $d \geq 2$. Seja $k \in \mathbb{N}$, $k \geq 2$. Suponhamos que $d \geq 3$ ou $k \geq 3$. Então existe apenas uma quantidade finita de pares de inteiros (m, n) tais que $f_0(n) = m^k$.*

Aplicando o Lema 5.4 e o Teorema 5.5, provamos a

Proposição 5.6. *Seja $f_0(X) = a_d X^d + \cdots + a_0 \in \mathbb{Z}[X]$ irredutível, estritamente crescente em $(-1, +\infty)$ e com $f_0(0) > 0$. Então existe $M > 0$ (que só depende de $f_0(X)$) tal que dado $k \in \mathbb{N}$, $k \geq 2$, vale*

$$Z_k(f_0; x) \leq M\sqrt{x},$$

para todo $x \geq 0$.

Demonstração. Dividimos a demonstração em três casos:

Caso 1: $d \geq 3$. Separamos esse caso em mais duas partes:

a) $k \geq 2d$. Para $x \geq 1$, se $n \in \mathbb{N}$, $n \leq x$, temos

$$\begin{aligned}\sqrt[k]{f_0(n)} &\leq \sqrt[k]{|a_d|n^d + |a_{d-1}|n^{d-1} + \cdots + |a_0|} \leq \sqrt[k]{|a_d|}n^{d/k} + \cdots + \sqrt[k]{|a_0|} \\ &\leq |a_d|n^{d/k} + \cdots + |a_0| \leq \big(|a_d| + \cdots + |a_0|\big)n^{d/k} \leq M_1\sqrt{x}\end{aligned}$$

em que usamos $d/k \leq 2$, e com $M_1 \doteq |a_d| + \cdots + |a_0|$ só dependendo de $f_0(X)$. Assim, se $\sqrt[k]{f_0(n)}$ fosse um inteiro, ele estaria entre 1 e $[M_1\sqrt{x}]$, a parte inteira de $M_1\sqrt{x}$, de modo que só haveria $[M_1\sqrt{x}]$ possibilidades para valores de $\sqrt[k]{f_0(n)}$. Como também $n \mapsto f_0(n)$ é injetora por hipótese, só pode haver no máximo $[M_1\sqrt{x}]$ valores de n para os quais $\sqrt[k]{f_0(n)}$ é inteiro. Portanto,

$$Z_k(f_0; x) \leq M_1\sqrt{x}.$$

b) $2 \leq k < 2d$. Pelo Teorema 5.5, existe M_k tal que

$$Z_k(f_0; x) \leq M_k$$

para todo $x \geq 0$.

Tomando então $M \doteq \max\{M_1, M_2 \dots M_{2d-1}\}$, temos de fato

$$Z_k(f_0; x) \leq M\sqrt{x}$$

para todo $x \geq 0$.

Caso 2: $d = 2$.

a) Como no caso anterior, existe $M_1 > 0$ tal que, se $k \geq 2d = 4$, temos $Z_k(f_0; x) \leq M_1\sqrt{x}$ para todo $x \geq 0$.

b) Se $k = 3$, pelo Teorema 5.5 existe $M_3 > 0$ tal que $Z_3(f_0; x) \leq M_3$ para todo $x \geq 0$.

c) Resta o caso $d = k = 2$. Como $d = 2$, temos $f_0(X) = aX^2 + bX + c$, com $a, b, c \in \mathbb{Z}$, sendo que a, b, c são positivos pois $f_0(0) > 0$ e $f_0(X)$ é estritamente crescente em $(-1, +\infty)$. Queremos estudar as soluções de

$$f_0(X) - Y^2 = 0, \tag{5.14}$$

para X, Y inteiros. Completando os quadrados, obtemos

$$\begin{aligned} f_0(X) - Y^2 = aX^2 + bX + c - Y^2 &= \frac{1}{4a}\left(4a^2X^2 + 4abX + 4ac - 4aY^2\right) \\ &= \frac{1}{4a}\left((2aX + b)^2 - b^2 + 4ac - a(2Y)^2\right) \\ &= \frac{1}{4a}(U^2 - aV_0^2 - D), \end{aligned} \tag{5.15}$$

se $U \doteq 2aX + b$, $V_0 \doteq 2Y$ e $D \doteq b^2 - 4ac$ é o discriminante de $f_0(X)$. Como $f_0(X)$ é irredutível, temos $D \neq 0$. Podemos melhorar (5.15) mais um pouco escrevendo $a = qa_0^2$, com $a_0, q \in \mathbb{N}$ e q livre de quadrados. Então

$$f_0(X) - Y^2 = \frac{1}{4a}(U^2 - qV^2 - D)$$

em que $V \doteq a_0V_0 = 2a_0Y$. Dessa forma, existe uma injeção que leva cada solução de (5.14) a uma solução de

$$U^2 - qV^2 = D \tag{5.16}$$

para U, V inteiros. Como queremos estimar $Z_2(f_0; x)$, de fato só estamos interessados nas soluções de (5.14) para X, Y inteiros e com $0 < X \leq x$. Essa restrição se traduz, em termos de U, V, na condição $b < U \leq 2ax + b$ (pois $U = 2aX + b$). Dessa forma, se

$$Z_2^*(f_0; x) \doteq \#\big\{n \in \mathbb{N},\, b < n \leq 2ax + b \,:\, \text{existe } m \geq 0 \text{ tal que } n^2 - qm^2 = D\big\},$$

temos

$$Z_2(f_0; x) \leq Z_2^*(f_0; x). \tag{5.17}$$

i) Se $q = 1$, dados $m, n \geq 0$ tais que $n^2 - qm^2 = D$, temos $(n - m)(n + m) = D$. Assim, temos uma aplicação injetora $(m, n) \mapsto (n-m, n+m)$ que leva soluções (m, n) de $n^2-m^2 = D$ a divisores de D. Portanto, se S é o conjunto dos divisores de D, temos que

$$Z_2^*(f_0; x) \leq \#\big(S \times S\big) = \big(\#S\big)^2 < \infty$$

para todo $x \geq 0$. Logo

$$Z_2(f_0; x) \leq Z_2^*(f_0; x) \leq M_2$$

com $M_2 \doteq (\#S)^2$ de que segue o resultado para esse caso.

ii) Supomos agora $q \geq 2$. Seja A o anel de inteiros algébricos do corpo $\mathbb{Q}(\sqrt{q})$. A norma do corpo $\mathbb{Q}(\sqrt{q})$ sobre $\mathbb{Q}$ é dada por

$$\mathrm{N}(r_1 + r_2\sqrt{q}) = (r_1 + r_2\sqrt{q})(r_1 - r_2\sqrt{q}) = r_1^2 - qr_2^2,$$

para todos $r_1, r_2 \in \mathbb{Q}$.

Se $\mathrm{N}(\beta) = D$ não tem soluções para $\beta \in A$, em particular $n^2 - qm^2 = D$ não tem soluções para $m, n \in \mathbb{Z}$, pois se tivéssemos $m, n \in \mathbb{Z}$ tais que $n^2 - qm^2 = D$, então tomando $\beta \doteq n + m\sqrt{q} \in \mathbb{Z}[\sqrt{q}] \subseteq A$, teríamos $\mathrm{N}(\beta) = D$, absurdo. Portanto nesse caso, $Z_2^*(f_0; x) = 0$ para todo $x \geq 0$.

Suponhamos então que $\mathrm{N}(\beta) = D$ possui soluções para $\beta \in A$. Assim, pelo Lema 5.4 existem u_0 unidade de A e $S \subseteq A$ tais que, se $\beta \in A$ e $\mathrm{N}(\beta) = D$, então $\beta = \gamma u_0^j$ com $\gamma \in S$ e $j \in \mathbb{Z}$. Em particular, se $n \in \mathbb{N}$, $m \geq 0$ são tais que $n^2 - qm^2 = D$, então $n + m\sqrt{q} \in A$, e $\mathrm{N}(n + m\sqrt{q}) = D$.

Logo existem $j \in \mathbb{Z}$ e $\gamma \in S$ tais que $n + m\sqrt{q} = u_0^j \gamma$. Desse fato provaremos então que $Z_2^*(f_0; x) = O(\log x)$.

Notemos primeiramente que podemos supor $|u_0| > 1$, pois se tivéssemos $|u_0| = 1$, teríamos $u_0 = \pm 1$, o que contradiz o fato do Teorema das Unidades de Dirichlet (usado na demonstração do Lema 5.4) de que u_0 não é raiz da unidade. Se tivéssemos $|u_0| < 1$, poderíamos tomar a unidade $u_0' \doteq 1/u_0$, que possui a mesma propriedade que usamos de u_0, mas $|u_0'| = 1/|u_0| > 1$.

Fixemos $x \geq 1$ e definimos

$$C = C(f_0; x) \doteq \big\{ n \in \mathbb{N},\, b < n \leq 2ax + b \,:\, \text{existe } m \geq 0 \text{ tal que } n^2 - qm^2 = D \big\}.$$

Podemos então definir $\phi : C \to \mathbb{Z} \times S$ por

$$\phi(n) \doteq (j, \gamma)$$

em que j, γ são escolhidos tais que, se $m \geq 0$ é tal que $n^2 - qm^2 = D$, então $n + m\sqrt{q} = u_0^j \gamma$. Temos que ϕ é injetora, pois se $n + m\sqrt{q} = u_0^j \gamma = n' + m'\sqrt{q}$ com n, m, n', m' inteiros, então $n = n'$. Dessa forma, $Z_2^*(f_0; x) = \#C = \#\phi[C]$.

Notemos que existe $N > 0$ tal que, se $(j, \gamma) \in \phi[C]$, então $j \geq -N$. De fato, sejam $n \in C$ e $(j, \gamma) = \phi(n)$. Seja $m \geq 0$ tal que $n^2 - qm^2 = D$. Então como $n \geq 1$, temos $1 \leq n + m\sqrt{q} = u_0^j \gamma$, logo $1 \leq |u_0|^j |\gamma|$. Aplicando o logaritmo, vemos que

$$j \geq -\frac{\log |\gamma|}{\log |u_0|}.$$

Tomando então $N > 0$ tal que $N > \log|\gamma| / \log|u_0|$ para todo $\gamma \in S$ (lembrando que S é finito), temos que $j \geq -N$. Assim temos que, para todo par $(j, \gamma) \in \phi[C]$, vale $j \geq -N$.

Provemos também que existe $K > 0$ que não depende de x tal que, se $(j, \gamma) \in \phi[C]$, então $j \leq K \log x$. Sejam $n \in C$, $m \geq 0$ tal que $n^2 - qm^2 = D$ e $(j, \gamma) \doteq \phi(n)$. Logo $0 < n + m\sqrt{q} = u_0^j \gamma$.

Como $n \leq 2ax + b$, temos

$$qm^2 = n^2 - D \leq (2ax + b)^2 - D.$$

Tirando a raiz quadrada, vemos que existe $r \in \mathbb{N}$, que só depende de a, b, D, tal que

$$m\sqrt{q} \leq rx.$$

Dessa forma, se $a' \doteq 2a + r > 0$, temos

$$0 < u_0^j \gamma = n + m\sqrt{q} \leq (2ax + b) + rx = a'x + b.$$

Assim $|u_0|^j |\gamma| \leq |a'x + b| = a'x + b$ e, aplicando o logaritmo, vemos que

$$j \leq \frac{\log(a'x + b) - \log|\gamma|}{\log|u_0|} \leq K \log x$$

para algum $K > 0$ que não depende de x.

Em resumo, provamos que se $(j, \gamma) \in \phi[C]$, então $-N \leq j \leq K \log x$, com N, K que não dependem de x. Dessa forma, $\phi[C] \subseteq ([-N, K \log x] \cap \mathbb{Z}) \times S$, de modo que

$$Z_2^*(f_0; x) = \#\phi[C] \leq (K \log x + N).\#S = O(\log x).$$

De (5.17) temos que $Z_2(f_0; x) = O(\log x)$ o que, juntamente com os outros casos, implica o resultado para $d = 2$.

Caso 3: $d = 1$. Nesse caso sempre temos $k \geq 2d$, e o resultado segue como em a) do Caso 1. □

Teorema 5.7. *Vale:*

$$\psi_{\mathbf{f}}(x) \sim C(\mathbf{f})x \quad \textit{se, e somente se,} \quad \theta_{\mathbf{f}}(x) \sim C(\mathbf{f})x.$$

Demonstração. Vamos estimar a diferença $\psi_{\mathbf{f}}(x) - \theta_{\mathbf{f}}(x)$. Todo $n \leq x$ que contribui um termo não-nulo para essa diferença (isto é, que aparece na soma de $\psi_{\mathbf{f}}$ mas não na de $\theta_{\mathbf{f}}$) é tal que para algum $i \in \{1, \ldots, k\}$ tem-se $f_i(n) = p^m$ com p primo e $m > 1$. Assim, se $\sum^*$ representa a soma sobre tais n, temos

$$\psi_{\mathbf{f}}(x) - \theta_{\mathbf{f}}(x) = \sum_{n\leq x}{}^{*} \Lambda\big(f_1(n)\big) \cdots \Lambda\big(f_k(n)\big) \leq \log f_1(x) \cdots \log f_k(x) \sum_{n\leq x}{}^{*} 1.$$

Todo n contado pela soma $\sum_{n\leq x}{}^{*}$ é tal que existe $i \in \{1, \ldots, k\}$ tal que $f_i(n) = p^m$ com p primo $m > 1$. Em particular, esse n é contado no valor de $Z_m(f_i; x)$. Além disso podemos dizer que $2 \leq m \leq \log_2 f_i(x)$ pois $f_i(n) = p^m \geq 2^m$ e tomando o logaritmo de base 2 temos $\log_2 f_i(x) \geq \log_2 f_i(n) \geq m$. Dessa forma

$$\psi_{\mathbf{f}}(x) - \theta_{\mathbf{f}}(x) \leq \log f_1(x) \cdots \log f_k(x) \sum_{i=1}^{k} \sum_{2\leq m\leq \log_2 f_i(x)} Z_m(f_i; x).$$

Logo, usando a Proposição 5.6 temos

$$\psi_{\mathbf{f}}(x) - \theta_{\mathbf{f}}(x) = O(x^{1/2} \log^{k+1} x), \tag{5.18}$$

o que implica a equivalência entre $\psi_{\mathbf{f}}(x) \sim C(\mathbf{f})x$ e $\theta_{\mathbf{f}}(x) \sim C(\mathbf{f})x$. □

5.2 A Identidade de Golomb

Demonstrado o Teorema 5.1, o Teorema 4.4 sugere que, para demonstrar a Conjectura de Bateman-Horn, bastaria considerar a seguinte série de potências, análoga à série (4.14):

$$\sum_{n=1}^{+\infty} \Lambda\big(f_1(n)\big) \cdots \Lambda\big(f_k(n)\big) z^n. \tag{5.19}$$

Golomb demonstrou uma identidade que generaliza (4.3), que vamos usar para obter uma outra expressão da série (5.19), assim como usamos (4.3) para obter outra expressão da série (4.14). Essa simplificação constitui a base do Λ-cálculo:

Teorema 5.8 (Identidade de Golomb)**.** *Sejam $a_1, \ldots, a_k \in \mathbb{N}$, $a_1, \ldots, a_k > 1$ dois a dois relativamente primos. Então vale*

$$\Lambda(a_1) \cdot \Lambda(a_2) \cdots \Lambda(a_k) = \frac{(-1)^k}{k!} \sum_{d\mid a_1 a_2 \cdots a_k} \mu(d) \log^k d.$$

Demonstração. Escrevendo cada divisor d de $a_1 \cdots a_k$ como produto $d = d_1 \cdots d_k$ de divisores d_1 de a_1, d_2 de a_2, …, d_k de a_k, temos

$$\begin{aligned} \sum_{d\mid a_1 \cdots a_k} \mu(d) \log^k d &= \sum_{d_1\mid a_1,\, d_2\mid a_2,\, \ldots,\, d_k\mid a_k} \mu(d_1 d_2 \cdots d_k) \log^k (d_1 d_2 \cdots d_k) \\ &= \sum_{d_1\mid a_1,\, d_2\mid a_2,\, \ldots,\, d_k\mid a_k} \mu(d_1 d_2 \cdots d_k) \big(\log d_1 + \cdots + \log d_k\big)^k \end{aligned}$$

Como $a_1, \ldots, a_k$ são dois a dois relativamente primos, usando a multiplicidade de μ temos

$$\sum_{d|a_1\cdots a_k} \mu(d)\log^k d = \sum_{d_1|a_1,\ldots,d_k|a_k} \mu(d_1)\cdots\mu(d_k) \sum_{i_1+\cdots+i_k=k} \frac{k!}{i_1!\cdots i_k!}(\log^{i_1} d_1)\cdots(\log^{i_k} d_k),$$

em que $\sum_{i_1+\cdots+i_k=k}$ denota que a soma é sobre os inteiros $i_1, \ldots, i_k \geq 0$ tais que $i_1+i_2+\cdots+i_k = k$, e $\log^0 1 = 1$ por definição. Assim,

$$\sum_{d|a_1\cdots a_k} \mu(d)\log^k d = \sum_{i_1+\cdots+i_k=k} \frac{k!}{i_1!\cdots i_k!} \sum_{d_1|a_1,\cdots,d_k|a_k} \mu(d_1)\cdots\mu(d_k)(\log^{i_1} d_1)\cdots(\log^{i_k} d_k),$$

de modo que

$$\sum_{d|a_1\cdots a_k} \mu(d)\log^k d = \sum_{i_1+\cdots+i_k=k} \frac{k!}{i_1!\cdots i_k!} \prod_{j=1}^{k} \sum_{d_j|a_j} \mu(d_j)\log^{i_j} d_j. \tag{5.20}$$

Se em algum termo da primeira soma do lado direito de (5.20) tivermos algum $i_m = 0$, então $\sum_{d_m|a_m} \mu(d_m)\log^{i_m} d_m = \sum_{d_m|a_m} \mu(d_m) = 0$ usando (4.1), de modo que podemos eliminar os termos em que aparece algum $i_m = 0$. Isto é; a soma é tomada sobre os termos $i_1, \ldots, i_k \geq 1$ tais que $i_1 + \cdots + i_k = k$, mas isso só é possível se $i_1 = i_2 = \cdots = i_k = 1$, portanto

$$\sum_{d|a_1\cdots a_k} \mu(d)\log^k d = k! \prod_{j=1}^{k} \sum_{d_j|a_j} \mu(d_j)\log d_j = k! \prod_{j=1}^{k} (-1)\Lambda(a_j) = (-1)^k k! \prod_{j=1}^{k} \Lambda(a_j),$$

usando (4.3), o que implica o Teorema. □

5.3 A Hipótese F

Para simplificarmos a expressão da série (5.19) usando o Teorema 5.8, suporemos que os valores $f_1(n), \ldots, f_k(n)$ são dois a dois relativamente primos para todo $n \in \mathbb{N}$. Diremos que uma família $\mathbf{f}$ que possui essa propriedade satisfaz a *hipótese F* (seguiremos a terminologia do artigo [HR05]).

Exemplo (Conjectura dos Primos Gêmeos). A família de dois polinômios $2X + 3, 2X + 5$, é uma família apropriada que satisfaz a hipótese F. Verifica-se diretamente que essa família é apropriada; provemos somente que ela satisfaz a hipótese F. Suponhamos que existam $n \in \mathbb{N}$ e p um número primo tais que $p \mid 2n + 3$ e $p \mid 2n + 5$. Então p divide a diferença dos valores $2n + 5$ e $2n + 3$, isto é; $p \mid 2$. Logo $p = 2$, o que é um absurdo, pois $p \mid 2n + 3$, e $2n + 3$ é ímpar. Portanto $\text{mdc}(2n + 3, 2n + 5) = 1$, para todo $n \in \mathbb{N}$.

A hipótese F pode parecer restritiva, mas para provar a Conjectura 6 é suficiente demonstrá-la para famílias apropriadas que satisfazem essa hipótese:

Teorema 5.9. *Se a Conjectura 6 vale para toda família apropriada que satisfaz a hipótese F, então essa Conjectura também vale para* toda *família apropriada.*

Fixemos $\mathbf{f} = (f_1, \ldots, f_k)$ uma família apropriada de polinômios, e $f(X) \doteq f_1(X)\cdots f_k(X)$. Então para todos $i, j \in \{1, 2, \ldots, k\}$ distintos, segue do Lema 2.1 que existem $c_{ij} \in \mathbb{Z}$, $c_{ij} \neq 0$ e $u_{ij}(X), v_{ij}(X) \in \mathbb{Z}[X]$ tais que

$$u_{ij}(X)f_i(X) + v_{ij}(X)f_j(X) = c_{ij}. \tag{5.21}$$

Se $\mathbf{f}$ não satisfaz a hipótese F, então existem $n \in \mathbb{N}$, $i, j \in \{1, 2, \ldots, k\}$ distintos, e p primo tais que $p \mid f_i(n)$ e $p \mid f_j(n)$. Logo segue de (5.21) que $p \mid c_{ij}$. Assim todos os primos que impedem a

validade da hipótese F para a família $\mathbf{f}$ estão no conjunto

$$\mathcal{P} \doteq \left\{ p \in \mathbb{N} \text{ primo} : p \text{ divide } \prod_{1 \leq i < j \leq k} c_{ij} \right\}.$$

Precisamos então evitar os valores de $f(n)$ que são múltiplos de algum elemento de $\mathcal{P}$. Isto é; gostaríamos de considerar só os $n \in \mathbb{N}$ tais que $f(n) \not\equiv 0 \pmod p$ para todo $p \in \mathcal{P}$. Fixado $p \in \mathcal{P}$, se $b \in \mathbb{N}$ é tal que $f(b) \not\equiv 0 \pmod p$, temos que $f(pn + b) \equiv f(b) \not\equiv 0 \pmod p$. Portanto, todo valor de $f(m)$ com m na progressão aritmética $\{pn + b : n \in \mathbb{N}\}$ evita os múltiplos de p, como queríamos.

Podemos generalizar esse fato para evitar todos os valores múltiplos de $\mathcal{P}$ de uma só vez: definimos $N_0 \doteq \prod_{p \in \mathcal{P}} p$, e tomamos n_0 no conjunto

$$\mathcal{N}_0 \doteq \{b \in \mathbb{N},\, b \leq N_0 : f(b) \not\equiv 0 \pmod p \text{ para todo } p \in \mathcal{P}\}.$$

(O conjunto $\mathcal{N}_0$ é não-vazio se N_0 é primo pois então $N_f(N_0) < N_0$. No caso geral, esse fato segue do caso em que N_0 é primo usando o Teorema Chinês dos Restos.) Dessa forma,

$$f(N_0 n + n_0) \equiv f(n_0) \not\equiv 0 \pmod p \qquad \text{para todos } n \in \mathbb{N},\, p \in \mathcal{P}. \tag{5.22}$$

Isto é; nenhum valor de $f(n)$ com n na progressão aritmética $\{N_0 m + n_0 : m \in \mathbb{N}\}$ é múltiplo de nenhum elemento de $\mathcal{P}$.

Considere então a família $\mathbf{f}_{n_0} = (f_{1,n_0}, \ldots, f_{k,n_0})$ dada por

$$f_{i,n_0}(X) \doteq f_i\big(N_0(X+1) + n_0\big) \qquad \text{para todo } i \in \{1, \ldots, k\}.$$

Temos que $g_{n_0}(X) \doteq f_{1,n_0}(X) \cdots f_{k,n_0}(X)$ faz o papel do polinômio $f(X)$ para a família $\mathbf{f}_{n_0}$. (De fato, $g_{n_0}(X) = f(N_0(X+1) + n_0)$.) Como conseguimos evitar todos os valores problemáticos para a hipótese F, podemos provar o seguinte resultado:

Lema 5.10. *A família $\mathbf{f}_{n_0}$ é apropriada e satisfaz a hipótese F.*

Demonstração. De fato, como $f_1(X), \ldots, f_k(X)$ são irredutíveis sobre $\mathbb{Q}$ temos que os polinômios $f_{1,n_0}(X)$, …, $f_{k,n_0}(X)$ também são irredutíveis. Analogamente valem as condições i), iv) e v) da definição de família apropriada para $\mathbf{f}_{n_0}$. Provemos que para todo primo p vale

$$N_{g_{n_0}}(p) = \begin{cases} 0, & \text{se } p \in \mathcal{P} \\ N_f(p) & \text{se } p \notin \mathcal{P}. \end{cases} \tag{5.23}$$

Em particular a desigualdade $N_f(p) < p$ implicará $N_{g_{n_0}}(p) < p$, de modo que $\mathbf{f}_{n_0}$ satisfaz a propriedade iii') de família apropriada.

Seja $p \geq 2$ primo.

a) Se $p \in \mathcal{P}$, temos $N_{g_{n_0}}(p) = 0$ pela equação (5.22).

b) Se $p \notin \mathcal{P}$, sejam

$$A \doteq \big\{ n \in \mathbb{N},\, n \leq p : f(n) \equiv 0 \pmod p \big\}$$

e

$$B \doteq \big\{ n \in \mathbb{N},\, n \leq p : g_{n_0}(n) \equiv 0 \pmod p \big\}$$

Assim $N_f(p) = \#A$ e $N_{g_{n_0}}(p) = \#B$. Como $p \notin \mathcal{P}$, isto é; $p \nmid N_0$, existe $N_1 \in \mathbb{N}$ tal que $N_0 N_1 \equiv 1 \pmod p$. Assim, se $n \in A$, seja $m_n \in \mathbb{N}$, $1 \leq m_n \leq p$ tal que $m_n \equiv N_1(n - n_0) - 1 \pmod p$. Temos

$$g_{n_0}(m_n) \equiv f\big(n_0 + N_0 N_1 (n - n_0)\big) \equiv f\big(n_0 + (n - n_0)\big) \equiv f(n) \equiv 0 \pmod p.$$

Logo $m_n \in B$. Além disso, se $n, n' \in A$ e $m_n = m_{n'}$, então

$$N_1(n - n_0) - 1 \equiv m_n = m_{n'} \equiv N_1(n' - n_0) - 1 \pmod{p}.$$

Multiplicando por N_0, vemos que $n \equiv n' \pmod{p}$, e como $1 \leq n, n' \leq p$, temos $n = n'$. Assim, a aplicação $n \mapsto m_n$ de A em B é injetora. Provemos que é bijetora. Seja $m \in B$. Então seja $n \in \mathbb{N}$, $n \leq p$ tal que $n \equiv n_0 + N_0(m+1) \pmod{p}$, de modo que

$$f(n) \equiv f\big(n_0 + N_0(m+1)\big) = g_{n_0}(m) \equiv 0 \pmod{p},$$

e assim $n \in A$. Além disso, $m \equiv N_1(n-n_0)-1 \pmod{p}$ (pois $n \equiv n_0+N_0(m+1) \pmod{p}$), e como $1 \leq m \leq p$, temos $m = m_n$. Portanto $n \mapsto m_n$ é uma aplicação bijetora entre A e B, de modo que $N_f(p) = \#A = \#B = N_{g_{n_0}}(p)$.

Provemos agora que $\mathbf{f}_{n_0}$ satisfaz a hipótese F. Suponhamos por absurdo que existam $n \in \mathbb{N}$, e $p \geq 2$ primo tais que $p \mid f_{i,n_0}(n)$ e $p \mid f_{j,n_0}(n)$, com $i, j \in \{1, \ldots, k\}$ e $i < j$. Então $p \mid c_{ij}$, pois

$$p \mid u_{ij}\big(n_0 + N_0(n+1)\big) f_{i,n_0}(n) + v_{ij}\big(n_0 + N_0(n+1)\big) f_{j,n_0}(n) = c_{ij},$$

usando (5.21). Assim temos $p \in \mathcal{P}$. Como $p \mid f_{i,n_0}(n)$ temos que $p \mid g_{n_0}(n)$, absurdo pois vimos que $N_{g_{n_0}}(p) = 0$ para todo $p \in \mathcal{P}$. Portanto $\mathbf{f}_{n_0}$ satisfaz a hipótese F. □

Podemos assim considerar a relação entre as funções $\pi_{\mathbf{f}}(x)$ e $\pi_{\mathbf{f}_{n_0}}(x)$. De fato, como $\mathbf{f}_{n_0}$ é igual à família $\mathbf{f}$, só que percorrendo só os termos da progressão aritmética $\{N_0 n + n_0 : n \in \mathbb{N}\}$, temos que $\pi_{\mathbf{f}_{n_0}}(x)$ não conta todos os termos que $\pi_{\mathbf{f}}(x)$ conta. Para obter de volta a função $\pi_{\mathbf{f}}(x)$ precisaríamos contar todas as funções $\pi_{\mathbf{f}_{n_0}}(x)$ para todo $n_0 \in \mathbb{N}$, $n_0 \leq N_0$, pois todo $n \in \mathbb{N}$ está em alguma dessas progressões, para algum $n_0 \in \mathbb{N}$.

De fato, não precisamos contar absolutamente todas as progressões aritméticas $\{N_0 n + n_0 : n \in \mathbb{N}\}$ para todo $n_0 \in \mathbb{N}$, $n_0 \leq N_0$, pois só queremos contar os inteiros $n \in \mathbb{N}$ tais que $f_1(n), \ldots, f_k(n)$ são todos primos, e de fato algumas dessas funções $\pi_{\mathbf{f}_{n_0}}(x)$ podem até ser limitadas. De fato, basta contar as progressões com termos n_0 no conjunto $\mathcal{N}_0$:

Lema 5.11. *A menos de uma quantidade finita de exceções, para todo $n \in \mathbb{N}$ tal que $f_1(n)$, …, $f_k(n)$ são todos primos existe $n_0 \in \mathcal{N}_0$ tal que $n \equiv n_0 \pmod{N_0}$ (em que n_0 depende de n).*

Demonstração. Como $\mathcal{P}$ é finito, existe $M \in \mathbb{N}$ tal que,

$$\text{se } m \geq M, \quad \text{então} \quad f_1(m) > \sup \mathcal{P}, \ \ldots, \ f_k(m) > \sup \mathcal{P}.$$

Seja agora $n \geq M$ tal que $f_1(n), \ldots, f_k(n)$ são todos primos. Seja $n_1 \in \mathbb{N}$, $n_1 \leq N_0$ tal que $n \equiv n_1 \pmod{N_0}$, e suponhamos por absurdo que $n_1 \notin \mathcal{N}_0$. Então existe $p \in \mathcal{P}$ tal que $f(n_1) \equiv 0 \pmod{p}$. Como $n \equiv n_1 \pmod{N_0}$ e $p \mid N_0$, temos $n \equiv n_1 \pmod{p}$, e assim $f(n) \equiv f(n_1) \equiv 0 \pmod{p}$, portanto $p \mid f(n)$. Dessa forma, $p \mid f_i(n)$ para algum $i \in \{1, \ldots, k\}$, mas como $f_i(n)$ é primo, segue que $p = f_i(n)$, absurdo, pois $f_i(n) > \sup \mathcal{P} \geq p$ dado que $n \geq M$. Logo, as exceções à afirmação são todas estritamente menores do que M, sendo portanto em quantidade finita. □

Podemos agora provar a seguinte Proposição, que implica diretamente o Teorema 5.9:

Proposição 5.12. *Se a Conjectura 6 é verdadeira para toda família $\mathbf{f}_{n_0}$ com $n_0 \in \mathcal{N}_0$, que são famílias apropriadas que satisfazem a hipótese F, então essa conjectura também vale para a família $\mathbf{f}$.*

Demonstração. Dado $n_0 \in \mathcal{N}_0$, como a Conjectura 6 é verdadeira para $\mathbf{f}_{n_0}$ temos que

$$\pi_{\mathbf{f}_{n_0}}(x) \sim \frac{C(\mathbf{f}_{n_0})}{h_1 h_2 \cdots h_k} \cdot \frac{x}{\log^k x}. \tag{5.24}$$

Agora notemos que segue do Lema 5.11 que

$$\pi_{\mathbf{f}}(x) = \sum_{n_0 \in \mathcal{N}_0} \pi_{\mathbf{f}_{n_0}}\left(\frac{x-n_0}{N_0} - 1\right) + O(1). \tag{5.25}$$

De fato, fixado $x \geq 0$, se $n \in \mathbb{N}$, $n \leq x$ é tal que $f_1(n), \ldots, f_k(n)$ são todos primos, a menos que n seja uma das exceções do Lema 5.11 (que são finitas), existem $m \in \mathbb{Z}$ e $n_0 \in \mathcal{N}_0$ univocamente determinados tais que $n = n_0 + N_0(m+1)$. Para termos $m > 0$, supomos também $n > \sup \mathcal{N}_0 + N_0$. Assim,

$$0 < m = \frac{n-n_0}{N_0} - 1 \leq \frac{x-n_0}{N_0} - 1.$$

Portanto $f_{j,n_0}(m) = f_j(n)$ é primo para todo $j \in \{1, \ldots, k\}$, e m é contado pela função $\pi_{\mathbf{f}_{n_0}}(x)$.

Por outro lado, se $n_0 \in \mathcal{N}_0$ e $m \leq (x-n_0)/N_0 - 1$ são tais que $f_{1,n_0}(m), \ldots, f_{k,n_0}(m)$ são todos primos, então tomando $n \doteq n_0 + N_0(m+1)$ temos $n \in \mathbb{N}$,

$$n \leq n_0 + \frac{N_0(x-n_0)}{N_0} = x$$

e $f_j(n) = f_{j,n_0}(m)$ é primo para todo $j \in \{1, \ldots, k\}$, de modo que n é contado por $\pi_{\mathbf{f}}(x)$. Note que a aplicação $m \mapsto n$ que definimos assim é injetora, pois se tivéssemos $n_0 + N_0(m+1) = n = n_0' + N_0(m'+1)$, então seria $n_0 \equiv n_0' \pmod{N_0}$ o que implica $n_0 = n_0'$ pois $1 \leq n_0, n_0' \leq N_0$. Logo também teríamos $m = m'$. Dessa forma, de fato vale (5.25).

Notemos que $C(\mathbf{f}_{n_0})$ não depende de n_0 em si mas somente de $\mathcal{P}$, por (5.23). Fixemos $n_0 \in \mathcal{N}_0$. Usando (5.23) obtemos (lembrando que $\mathcal{P}$ é finito)

$$C(\mathbf{f}_{n_0}) = \prod_{p \in \mathcal{P}} \left[\left(1-\frac{1}{p}\right)^{-k}\left(1-\frac{0}{p}\right)\right] \cdot \prod_{p \notin \mathcal{P}} \left[\left(1-\frac{1}{p}\right)^{-k}\left(1-\frac{N_f(p)}{p}\right)\right].$$

Assim temos

$$\begin{aligned} C(\mathbf{f}_{n_0}) &= \left[\prod_{p \in \mathcal{P}}\left(1-\frac{N_f(p)}{p}\right)\right]^{-1} \cdot \prod_{p} \left[\left(1-\frac{1}{p}\right)^{-k}\left(1-\frac{N_f(p)}{p}\right)\right] \\ &= \left[\prod_{p \in \mathcal{P}}\left(1-\frac{N_f(p)}{p}\right)\right]^{-1} \cdot C(\mathbf{f}). \end{aligned} \tag{5.26}$$

Agora lembrando que $N_0 = \prod_{p \in \mathcal{P}} p$, vale

$$\prod_{p \in \mathcal{P}}\left(1-\frac{N_f(p)}{p}\right) = \prod_{p \in \mathcal{P}} \frac{p - N_f(p)}{p} = \frac{1}{N_0} \prod_{p \in \mathcal{P}} \big(p - N_f(p)\big).$$

Segue do Teorema Chinês dos Restos que vale $\prod_{p \in \mathcal{P}} \big(p - N_f(p)\big) = \#\mathcal{N}_0$, de modo que temos

$$\prod_{p \in \mathcal{P}}\left(1-\frac{N_f(p)}{p}\right) = \frac{\#\mathcal{N}_0}{N_0}.$$

Portanto segue de (5.26) que

$$C(\mathbf{f}_{n_0}) = \frac{N_0}{\#\mathcal{N}_0} C(\mathbf{f}).$$

Substituindo esse valor em (5.24) temos

$$\pi_{\mathbf{f}_{n_0}}\left(\frac{x-n_0}{N_0}-1\right) \sim \frac{N_0 C(\mathbf{f})/\#\mathcal{N}_0}{h_1h_2\cdots h_k}\cdot\frac{(x-n_0)/N_0-1}{\log^k[(x-n_0)/N_0-1]}$$
$$\sim \frac{1}{\#\mathcal{N}_0}\cdot\frac{C(\mathbf{f})}{h_1h_2\cdots h_k}\cdot\frac{x}{\log^k x}.$$

Logo usando essa relação assintótica em (5.25) obtemos

$$\pi_{\mathbf{f}}(x) \sim \#\mathcal{N}_0\frac{1}{\#\mathcal{N}_0}\frac{C(\mathbf{f})}{h_1h_2\cdots h_k}\cdot\frac{x}{\log^k x}$$
$$\sim \frac{C(\mathbf{f})}{h_1h_2\cdots h_k}\cdot\frac{x}{\log^k x},$$

de modo que vale a Conjectura 6 para a família $\mathbf{f}$. □

5.4 O Λ-cálculo

Finalmente desenvolvemos a parte principal do Λ-método.

Seja $f_1(X), \ldots, f_k(X)$ uma família apropriada de polinômios que satisfaz a hipótese F. Sejam $f(X) \doteq f_1(X)f_2(X)\cdots f_k(X)$ e $h_1, \ldots, h_k$ respectivamente os graus desses polinômios. Seja $\mathbf{f} \doteq (f_1, \ldots, f_k)$.

Em resumo, queremos estudar o comportamento da série (5.19) quando $z \to 1^-$ com o objetivo de usar o Teorema 4.4 para provar que $\psi_{\mathbf{f}}(x) \sim C(\mathbf{f})x$ e, com isso, provar a Conjectura 6. Seja então

$$G(z) \doteq \sum_{n=1}^{+\infty}\Lambda\big(f_1(n)\big)\cdots\Lambda\big(f_k(n)\big)z^n.$$

Procedemos de modo inteiramente análogo ao da nossa demonstração do Teorema dos Números Primos. A série $G(z)$ tem raio de convergência maior ou igual a 1 por causa do seguinte Lema:

Lema 5.13. *Vale*

$$\Lambda\big(f_1(n)\big)\cdot\Lambda\big(f_2(n)\big)\cdots\Lambda\big(f_k(n)\big) = O(\log^k n).$$

Demonstração. Como $\log f_i(n) \sim h_i \log n$, temos que

$$\Lambda\big(f_1(n)\big)\cdots\Lambda\big(f_k(n)\big) \leq \log f_1(n)\cdots\log f_k(n) \sim h_1\cdots h_k\cdot\log^k n,$$

logo $\log f_1(n)\cdots\log f_k(n) = O(\log^k n)$. □

Com o Lema 5.13, temos que existe $M > 0$ tal que

$$\limsup_{n\to+\infty}\sqrt[n]{\Lambda\big(f_1(n)\big)\cdots\Lambda\big(f_k(n)\big)} \leq \limsup_{n\to+\infty}\sqrt[n]{M\log^k n} = 1.$$

Dessa forma de fato $G(z)$ tem raio de convergência maior ou igual a 1.

Usando o Teorema 5.8 temos, para $0 < z < 1$,

$$G(z) = \frac{(-1)^k}{k!}\sum_{n=1}^{+\infty}\left(\sum_{d|f(n)}\mu(d)\log^k d\right)z^n. \tag{5.27}$$

Vamos trocar a ordem das somas no lado direito da igualdade (5.27). Para que as somas sejam

ambas tomadas sobre todo o $\mathbb{N}$, definimos

$$\chi_{d,f(n)} \doteq \begin{cases} 1, & \text{se } d \mid f(n) \\ 0, & \text{caso contrário.} \end{cases}$$

para $d, n \in \mathbb{N}$. Então

$$\sum_{n=1}^{+\infty} \left(\sum_{d \mid f(n)} \mu(d) \log^k d \right) z^n = \sum_{n=1}^{+\infty} \sum_{d=1}^{+\infty} \chi_{d,f(n)} \big(\mu(d) \log^k d\big) z^n. \tag{5.28}$$

Provemos que é possível trocar a ordem das séries da direita de (5.28).

Lema 5.14. *Fixe $z \in \mathbb{R}$ com $|z| < 1$. Vale*

$$\sum_{n=1}^{+\infty} \sum_{d=1}^{+\infty} \chi_{d,f(n)} \big(\mu(d) \log^k d\big) z^n = \sum_{d=1}^{+\infty} \sum_{n=1}^{+\infty} \chi_{d,f(n)} \big(\mu(d) \log^k d\big) z^n.$$

Demonstração. O Lema segue do Teorema de Fubini se provarmos que a série

$$\sum_{n=1}^{+\infty} \sum_{d=1}^{+\infty} \left| \chi_{d,f(n)} \big(\mu(d) \log^k d\big) z^n \right| \tag{5.29}$$

é convergente. De fato,

$$\begin{aligned} \sum_{n=1}^{+\infty} \sum_{d=1}^{+\infty} \left| \chi_{d,f(n)} \big(\mu(d) \log^k d\big) z^n \right| &= \sum_{n=1}^{+\infty} \sum_{d \mid f(n)} \left| \big(\mu(d) \log^k d\big) z^n \right| \leq \sum_{n=1}^{+\infty} \sum_{d \leq f(n)} \log^k f(n) \cdot |z|^n \\ &\leq \sum_{n=1}^{+\infty} f(n) \log^k f(n) \cdot |z|^n < \infty, \end{aligned}$$

sendo que a última série é convergente pois $f(n) = O(n^h)$, em que $h = \operatorname{gr} f$, e pois $|z| < 1$. Isso prova a convergência de (5.29). □

Podemos então trocar as duas séries da direita de (5.28), e assim obtemos

$$\begin{aligned} \sum_{n=1}^{+\infty} \left(\sum_{d \mid f(n)} \mu(d) \log^k d \right) z^n &= \sum_{d=1}^{+\infty} \sum_{n=1}^{+\infty} \chi_{d,f(n)} \big(\mu(d) \log^k d\big) z^n \\ &= \sum_{d=1}^{+\infty} \sum_{n=1;\, f(n) \equiv 0 \,(\mathrm{mod}\, d)}^{+\infty} \big(\mu(d) \log^k d\big) z^n. \\ &= \sum_{d=1}^{+\infty} \mu(d) \log^k d \sum_{n \leq d;\, f(n) \equiv 0 \,(\mathrm{mod}\, d)} \sum_{l=0}^{+\infty} z^{n+ld}, \end{aligned}$$

em que usamos o fato de que toda solução de $f(n) \equiv 0 \pmod d$ em $n \in \mathbb{N}$ é equivalente a uma

solução $m \in \mathbb{N}$, $m \leq d$, módulo d, isto é; existe $l \geq 0$ tal que $n = m + ld$. Dessa forma,

$$\begin{aligned}\sum_{n=1}^{+\infty}\left(\sum_{d|f(n)}\mu(d)\log^k d\right)z^n &= \sum_{d=1}^{+\infty}\mu(d)\log^k d \sum_{n\leq d;\, f(n)\equiv 0 \,(\mathrm{mod}\, d)} z^n \sum_{l=0}^{+\infty} z^{ld} \\ &= \sum_{d=1}^{+\infty}\frac{\mu(d)\log^k d}{1-z^d}\sum_{n\leq d;\, f(n)\equiv 0 \,(\mathrm{mod}\, d)} z^n \\ &= \frac{1}{1-z}\sum_{d=1}^{+\infty}\frac{\mu(d)\log^k d}{1+z+\cdots+z^{d-1}}\sum_{n\leq d;\, f(n)\equiv 0 \,(\mathrm{mod}\, d)} z^n.\end{aligned}$$

Juntando com (5.27) e tomando o limite quando $z \to 1^-$, temos então

$$\lim_{z\to 1^-}(1-z)G(z) = \frac{(-1)^k}{k!}\lim_{z\to 1^-}\sum_{d=1}^{+\infty}\frac{\mu(d)\log^k d}{1+z+\cdots+z^{d-1}}\sum_{n\leq d;\, f(n)\equiv 0 \,(\mathrm{mod}\, d)} z^n.$$

Se pudéssemos então comutar o limite com a soma infinita, passo esse que é *o único* passo não justificado desse método, obteríamos

$$\begin{aligned}&\lim_{z\to 1^-}(1-z)\sum_{n=1}^{+\infty}\Lambda\big(f_1(n)\big)\cdots\Lambda\big(f_k(n)\big)z^n \\ &\qquad \stackrel{?}{=} \frac{(-1)^k}{k!}\sum_{d=1}^{+\infty}\lim_{z\to 1^-}\left(\frac{\mu(d)\log^k d}{1+z+\cdots+z^{d-1}}\sum_{n\leq d;\, f(n)\equiv 0 \,(\mathrm{mod}\, d)} z^n\right) \\ &\qquad = \frac{(-1)^k}{k!}\sum_{d=1}^{+\infty}\frac{\mu(d)\log^k d}{d}N_f(d). \quad (5.30)\end{aligned}$$

Definimos então

$$S(\mathbf{f}) \doteq \frac{(-1)^k}{k!}\sum_{d=1}^{+\infty}\frac{\mu(d)\log^k d}{d}N_f(d).$$

Dessa forma, (supondo a troca da ordem do limite com a série) concluímos de (5.30) aplicando o Teorema 4.4 que vale

$$\psi_{\mathbf{f}}(x) \sim S(\mathbf{f})x.$$

Ainda precisamos provar a convergência da série $S(\mathbf{f})$.

Também veremos que vale

$$S(\mathbf{f}) = C(\mathbf{f}), \quad (5.31)$$

exatamente como esperado pela Conjectura de Bateman-Horn. Isto é, incrivelmente a constante $S(\mathbf{f})$ obtida pelo Método de Golomb corresponde àquela encontrada por meio de argumentos heurísticos por Bateman e Horn. Nesse sentido, a igualdade (5.31) é talvez a maior evidência que temos a favor da validade do Método de Golomb.

Portanto (a menos do passo que falta) o Λ-cálculo demonstra a Conjectura 6.

No caso da demonstração que fizemos do Teorema dos Números Primos, o Corolário 4.6 realmente nos permite trocar a ordem do limite com a soma, depois de provada a convergência da série resultante. Exceto para o caso de um único polinômio linear, ainda não foi encontrado um teorema abeliano apropriado para justificar a comutação do limite com a soma.

Capítulo 6

Demonstração da igualdade $S(\mathbf{f}) = C(\mathbf{f})$

Fixemos para todo este Capítulo $f_1(X), \ldots, f_k(X)$ uma família apropriada de polinômios, $f(X) \doteq f_1(X)f_2(X)\cdots f_k(X)$ e $\mathbf{f} \doteq (f_1, \ldots, f_k)$. Para cada $j \in \{1, \ldots, k\}$, seja α_j uma raiz de $f_j(X)$, e seja $K_j \doteq \mathbb{Q}(\alpha_j)$.

O objetivo deste Capítulo é demonstrar a igualdade $S(\mathbf{f}) = C(\mathbf{f})$. Vamos primeiramente provar a convergência da série $S(\mathbf{f})$, e essa demonstração também nos dará uma outra expressão para o valor dessa série, expressão essa que por fim nos permitirá provar a igualdade desejada. Essa demonstração é a mesma feita em [HR05].

6.1 As funções $L_{\mathbf{f}}(s)$

A existência de teoremas do tipo tauberiano para séries de Dirichlet (veja o Apêndice C) sugere o estudo da seguinte série:

$$D(s) \doteq \sum_{d=1}^{+\infty} \frac{\mu(d)\log^k d}{d^s} N_f(d). \tag{6.1}$$

Se conseguirmos provar que $D(s)$ tem boas propriedades analíticas, de modo a satisfazer as hipóteses de algum teorema tauberiano, obteremos daí a convergência da série $S(\mathbf{f})$. É importante notar que além da convergência de $S(\mathbf{f})$, obteremos também a seguinte igualdade:

$$S(\mathbf{f}) = \frac{(-1)^k}{k!} D(1).$$

Uma expressão desse tipo será essencial na demonstração de $S(\mathbf{f}) = C(\mathbf{f})$.

De fato, não vamos estudar a série $D(s)$ acima, mas uma série de Dirichlet um pouco mais simples:

$$L_{\mathbf{f}}(s) \doteq \sum_{d=1}^{+\infty} \frac{\mu(d)N_f(d)}{d^s}.$$

Basta estudar $L_{\mathbf{f}}(s)$ para obter o resultado desejado, pois derivando (por enquanto, formalmente) essa série k vezes, obtemos

$$L_{\mathbf{f}}^{(k)}(s) \doteq (-1)^k \sum_{d=1}^{+\infty} \frac{\mu(d)N_f(d)\log^k d}{d^s} = (-1)^k D(s).$$

A série $L_{\mathbf{f}}(s)$ é melhor para nós do que a série $D(s)$ definida em (6.1) pelo fato de que os

coeficientes de $L_{\mathbf{f}}(s)$ formam uma função multiplicativa. Desse fato, obtemos a igualdade

$$L_{\mathbf{f}}(s) = \prod_p \left(1 - \frac{N_f(p)}{p^s}\right)$$

nos pontos s em que a série que define $L_{\mathbf{f}}(s)$ é absolutamente convergente. (Toda série de Dirichlet com coeficientes multiplicativos possui uma expressão como produto de Euler sobre os números primos; veja [Apo76, Cap. 11].) Vejamos então qual é o semiplano de convergência absoluta da série $L_{\mathbf{f}}(s)$:

Proposição 6.1. *A abcissa de convergência absoluta da série $L_{\mathbf{f}}(s)$ é menor ou igual a 1. Isto é; a série que define $L_{\mathbf{f}}(s)$ é absolutamente convergente se $\mathrm{Re}(s) > 1$, e a convergência é uniforme em todo semiplano fechado $\mathrm{Re}(s) \geq 1 + \varepsilon$ com $\varepsilon > 0$.*

Demonstração. Como $N_f(p) \leq h \doteq \operatorname{gr} f$ para todo $p \in \mathbb{N}$ primo, temos que

$$\big|\mu(d)N_f(d)\big| \leq |\mu(d)|h^{\omega(d)}, \quad \text{para todo } d \in \mathbb{N}. \tag{6.2}$$

De fato, se $d \in \mathbb{N}$ não é livre de quadrados, então $\mu(d) = 0$ e a desigualdade (6.2) vale trivialmente. Se d é livre de quadrados, então $d = p_1 \cdots p_n$ com $p_1, \ldots, p_n \in \mathbb{N}$ primos distintos. Nesse caso, usando o Lema 3.2 obtemos

$$\big|\mu(d)N_f(d)\big| = \big|\mu(d)N_f(p_1)N_f(p_2)\cdots N_f(p_k)\big| \leq |\mu(d)|h^n = |\mu(d)|h^{\omega(d)}.$$

Dessa forma, se $s = \sigma + it$, $\sigma > 1$;

$$\sum_{d=1}^{N} \left|\frac{\mu(d)N_f(d)}{d^s}\right| \leq \sum_{d=1}^{N} \frac{|\mu(d)|h^{\omega(d)}}{d^\sigma} \leq \prod_{p \leq N} \left(1 + \frac{h}{p^\sigma}\right) \tag{6.3}$$

para todo $N \in \mathbb{N}$. A segunda desigualdade de (6.3) vale pois o produto de Euler da série de Dirichlet $\sum_{d=1}^{+\infty} |\mu(d)|h^{\omega(d)}/d^s$ é $\prod_p (1 + h/p^s)$. Mas o produto em (6.3) converge absolutamente quando $N \to +\infty$ pois como $\sigma > 1$ a série $\sum_p 1/p^\sigma$ converge absolutamente. Portanto fazendo $N \to +\infty$ em (6.3) temos que

$$\sum_{d=1}^{+\infty} \left|\frac{\mu(d)N_f(d)}{d^s}\right| \leq \prod_p \left(1 + \frac{h}{p^\sigma}\right) < \infty.$$

Dessa forma, a série $\sum_{d=1}^{+\infty} \mu(d)N_f(d)/d^s$ de fato converge absolutamente se $\mathrm{Re}(s) > 1$. □

Precisamos agora provar que $L_{\mathbf{f}}(s)$ possui uma extensão analítica a um aberto que contém o semiplano fechado $\mathrm{Re}(s) \geq 1$ para usar um teorema tauberiano (o teorema que usaremos é o Teorema C.2). O Lema seguinte é o principal passo para obter essa extensão:

Lema 6.2. *Existem $\varepsilon_{\mathbf{f}} > 0$ e uma função $M_{\mathbf{f}}(s)$ holomorfa para $\mathrm{Re}(s) > 1/2$ que não se anula em $\mathrm{Re}(s) > 1 - \varepsilon_{\mathbf{f}} > 1/2$ e tal que*

$$L_{\mathbf{f}}(s) = \frac{1}{\zeta_{K_1}(s)\cdots\zeta_{K_k}(s)} M_{\mathbf{f}}(s)$$

em $\mathrm{Re}(s) > 1$. (Onde $\zeta_{K_j}(s)$ é a função ζ de Dedekind do corpo K_j.)

Demonstração. Fixemos $s = \sigma + it$ com $\sigma > 1$. Com o Lema 3.7 temos os seguintes produtos infinitos:

$$L_{\mathbf{f}}(s) = \prod_p \left(1 - \frac{N_f(p)}{p^s}\right) \quad \text{e} \quad \zeta_{K_i}(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-A_{p,K_i}} \cdot R_{K_i}(s)$$

para $i = 1, \ldots, k$. Combinando o Lema 3.1 e a Proposição 3.3 temos que existe um primo p_0 tal que

$$\text{se } p \geq p_0 \text{ é primo,} \quad \text{então} \quad N_f(p) = A_{p,K_1} + \cdots + A_{p,K_k}. \tag{6.4}$$

Assim, fazendo o produto das funções ζ associadas aos corpos $K_1, \ldots, K_k$ temos

$$\zeta_{K_1}(s) \cdots \zeta_{K_k}(s) = \prod_{p \geq p_0} \left(1 - \frac{1}{p^s}\right)^{-N_f(p)} \cdot P_0(s) \cdot R_{K_1}(s) \cdots R_{K_k}(s) \tag{6.5}$$

em que

$$P_0(s) \doteq \prod_{p < p_0} \left(1 - \frac{1}{p^s}\right)^{-A_{p,K_1} - \cdots - A_{p,K_k}}.$$

Para que a expressão de (6.5) fosse um pouco mais simples, seria melhor que o produto infinito fosse tomado sobre todos os primos, ao invés de ser o somente o produto sobre os primos maiores ou iguais a p_0. Podemos obter isso definindo $P(s) \doteq P_0(s) \cdot \prod_{p<p_0} (1 - p^{-s})^{N_f(p)}$ pois então temos

$$\zeta_{K_1}(s) \cdots \zeta_{K_k}(s) = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-N_f(p)} \cdot P(s) \cdot R_{K_1}(s) \cdots R_{K_k}(s). \tag{6.6}$$

Usando a expressão do binômio de Newton temos, para todo primo p, que

$$\left(1 - \frac{1}{p^s}\right)^{N_f(p)} = 1 - \frac{N_f(p)}{p^s} + O\left(\frac{1}{p^{2\sigma}}\right)$$

em que a constante O depende apenas de $N_f(p)$. Segue então que

$$\frac{1 - N_f(p)/p^s}{(1 - 1/p^s)^{N_f(p)}} = 1 + O\left(\frac{1}{p^{2\sigma}}\right).$$

Assim, definindo

$$E_p(s) \doteq \frac{1 - N_f(p)/p^s}{(1 - 1/p^s)^{N_f(p)}} = 1 + O\left(\frac{1}{p^{2\sigma}}\right)$$

temos que a segunda igualdade sugere que o produto $E(s) \doteq \prod_p E_p(s)$ é normalmente convergente (provaremos esse fato com mais detalhes a seguir, pois não basta ser somente $E_p(s) = 1 + O(p^{-2\sigma})$, é preciso que a constante em O não dependa de p e nem de σ). Então, usando o produto de Euler de $L_{\mathbf{f}}(s)$ e (6.6) temos que

$$E(s) = \prod_p \frac{1 - N_f(p)/p^s}{(1 - 1/p^s)^{N_f(p)}} = L_{\mathbf{f}}(s) \cdot \frac{\zeta_{K_1}(s) \cdots \zeta_{K_k}(s)}{P(s) \cdot R_{K_1}(s) \cdots R_{K_k}(s)}.$$

Isso sugere definir

$$M_{\mathbf{f}}(s) \doteq P(s) \cdot R_{K_1}(s) \cdots R_{K_k}(s) \cdot E(s). \tag{6.7}$$

Basta então demonstrar as propriedades necessárias para essa função $M_{\mathbf{f}}(s)$.

Já vimos que as funções $R_{K_1}(s), \ldots, R_{K_k}(s)$ são holomorfas e não se anulam para $\mathrm{Re}(s) > 1/2$. A função $P(s)$ é também holomorfa e não se anula nesse mesmo semiplano pois se $\mathrm{Re}(s) > 1/2$ vale $1 - p^{-s} \neq 0$ para todo primo p. Portanto para terminar a demonstração basta provar que $E(s)$ é holomorfa em $\mathrm{Re}(s) > 1/2$ e que existe $\varepsilon_{\mathbf{f}} > 0$ tal que $E(s)$ não se anula no semiplano $\mathrm{Re}(s) > 1 - \varepsilon_{\mathbf{f}}$.

Segue do binômio de Newton que

$$1 - \frac{N_f(p)}{p^s} = \left(1 - \frac{1}{p^s}\right)^{N_f(p)} - \sum_{m=2}^{N_f(p)} \binom{N_f(p)}{m} \frac{(-1)^m}{p^{ms}} = \left(1 - \frac{1}{p^s}\right)^{N_f(p)} \cdot \left[1 + g_p\left(\frac{1}{p^s}\right)\right]$$

em que

$$g_p(z) \doteq -(1-z)^{-N_f(p)} \cdot \sum_{m=2}^{N_f(p)} \binom{N_f(p)}{m} (-z)^m.$$

(Se $N_f(p) \leq 1$, definimos $g_p(z) \doteq 0$.) Assim

$$E_p(s) = 1 + g_p\left(\frac{1}{p^s}\right).$$

Como queremos provar que $E(s) = \prod_p E_p(s)$ é normalmente convergente para $\mathrm{Re}(s) > 1/2$, precisamos estimar $g_p(p^{-s})$. Se $s = \sigma + it$ com $\sigma > 1/2$, temos que

$$|p^{-s}| = p^{-\sigma} \leq 2^{-\sigma} \leq 2^{-1/2}.$$

Portanto, basta estimar $g_p(z)$ na bola fechada de centro 0 e raio $2^{-1/2}$. De fato, se $|z| \leq 2^{-1/2} < 1$ e $N_f(p) \geq 2$, temos

$$\begin{aligned} |g_p(z)| &\leq \frac{1}{|1-z|^{N_f(p)}} \sum_{m=2}^{N_f(p)} \binom{N_f(p)}{m} |z|^m \\ &\leq \left(\frac{1}{(1-2^{-1/2})^{N_f(p)}} \sum_{m=2}^{N_f(p)} \binom{N_f(p)}{m} \right) |z|^2 \leq \frac{2^{N_f(p)}}{(1-2^{-1/2})^{N_f(p)}} |z|^2 \\ &\leq \frac{2^h}{(1-2^{-1/2})^h} |z|^2 \end{aligned}$$

pois $N_f(p) \leq h$ para todo primo p. Assim, provamos que existe uma constante $C > 0$ que não depende nem de p nem de z tal que

$$|g_p(z)| \leq C|z|^2 \qquad \text{se } |z| \leq 2^{-1/2}. \tag{6.8}$$

Portanto, dado $\delta > 0$, se $s = \sigma + it$ com $\sigma \geq 1/2 + \delta$ temos

$$\sum_p \left| g_p\left(\frac{1}{p^s}\right) \right| \leq \sum_p \frac{C}{p^{2\sigma}} \leq \sum_p \frac{C}{p^{1+2\delta}} < \infty.$$

Assim $E(s) = \prod_p E_p(s)$ de fato define uma função holomorfa no semiplano aberto $\mathrm{Re}(s) > 1/2$.

Resta provar que existe $\varepsilon_{\mathbf{f}} > 0$ tal que $E(s) \neq 0$ se $\mathrm{Re}(s) > 1 - \varepsilon_{\mathbf{f}}$, o que é equivalente a encontrar $\delta_{\mathbf{f}} < 1$ tal que $E(s)$ não se anula em $\mathrm{Re}(s) > \delta_{\mathbf{f}}$.

Seja $s = \sigma + it$ com $\sigma > 1/2$ tal que $E(s) = 0$. Então existe um primo p tal que $E_p(s) = 0$. Isto é: $1 - N_f(p)p^{-s} = 0$. Em particular, $N_f(p) \neq 0$. Temos então $p^s = N_f(p)$ e, calculando o módulo dessa igualdade vemos que

$$\sigma = \frac{\log N_f(p)}{\log p} \leq \frac{\min\{\log h, \log(p-1)\}}{\log p}, \tag{6.9}$$

pois $N_f(p) < p$ e $N_f(p) \leq h$. Basta então notar que

$$\delta_{\mathbf{f}} \doteq \sup_p \left\{ \frac{\min\{\log h, \log(p-1)\}}{\log p} \right\} < 1.$$

De fato, para todo primo p, vale $\log(p-1)/\log p < 1$. Assim

$$\sup_{p\le h}\left\{\frac{\min\{\log h,\,\log(p-1)\}}{\log p}\right\} = \max_{p\le h}\left\{\frac{\log(p-1)}{\log p}\right\} < 1.$$

Por outro lado,

$$\sup_{p>h}\left\{\frac{\min\{\log h,\,\log(p-1)\}}{\log p}\right\} \le \frac{\log h}{\log(h+1)} < 1.$$

Portanto, de fato $\delta_{\mathbf{f}} < 1$. Temos que $E(s)$ não se anula em $\mathrm{Re}(s) > \delta_{\mathbf{f}}$, pois vimos em (6.9) que todo zero de $E(s)$ tem parte real menor do que $\delta_{\mathbf{f}}$. □

Teorema 6.3. *Existe $B_{\mathbf{f}} > 0$ tal que $L_{\mathbf{f}}(s)$ possui um prolongamento analítico ao aberto*

$$U_{\mathbf{f}} \doteq \big\{s = \sigma + it \in \mathbb{C},\, \sigma, t \in \mathbb{R} \,:\, \sigma > 1 - B_{\mathbf{f}}/\log(|t|+2)\big\}$$

e, nesse aberto, $L_{\mathbf{f}}(s)$ não possui zeros nem polos, exceto por um zero de ordem k em $s = 1$. Além disso, para $s = \sigma + it \in U_{\mathbf{f}}$ vale

$$L_{\mathbf{f}}(s) \ll \log^k(|t|+2).$$

Demonstração. Pelo Teorema 3.6 existe $B_{\mathbf{f}} > 0$ tal que $\zeta_{K_1}(s), \ldots, \zeta_{K_k}(s)$ não se anulam em um mesmo aberto

$$U_{\mathbf{f}} \doteq \big\{s = \sigma + it \,:\, \sigma > 1 - B_{\mathbf{f}}/\log(|t|+2) > 1/2\big\}.$$

Assim $1/\zeta_{K_1}(s), \ldots, 1/\zeta_{K_k}(s)$ são holomorfas em $U_{\mathbf{f}}$. Então o Lema 6.2 fornece uma extensão analítica de $L_{\mathbf{f}}(s)$ a $U_{\mathbf{f}}$.

Supondo que $B_{\mathbf{f}} > 0$ é suficientemente pequeno para termos

$$U_{\mathbf{f}} \subseteq \{s = \sigma + it \,:\, \sigma > 1 - \varepsilon_{\mathbf{f}}\},$$

temos também que $M_{\mathbf{f}}(s)$ não se anula em $U_{\mathbf{f}}$, de modo que o único zero de $L_{\mathbf{f}}(s)$ em $U_{\mathbf{f}}$ é o polo comum das funções $\zeta_{K_1}(s), \ldots, \zeta_{K_k}(s)$ em $s = 1$. Como para todo $i \in \{1, \ldots, k\}$ o polo de $\zeta_{K_i}(s)$ em $s = 1$ é simples, temos que a função $L_{\mathbf{f}}(s)$ tem em $s = 1$ um zero de ordem k.

Provemos que $M_{\mathbf{f}}(s)$ é limitada em todo semiplano fechado $\mathrm{Re}(s) \ge 1/2 + \varepsilon$ com $\varepsilon > 0$. Lembramos que

$$M_{\mathbf{f}}(s) \doteq P(s) \cdot R_{K_1}(s) \cdots R_{K_k}(s) \cdot E(s).$$

Então basta mostrar que cada uma das funções $P(s)$, $R_{K_1}(s), \ldots, R_{K_k}(s)$ e $E(s)$ é limitada em $\mathrm{Re}(s) \ge 1/2 + \varepsilon$.

Se $s = \sigma + it$, temos

$$|P(s)| = \prod_{p<p_0} \frac{|1-p^{-s}|^{N_f(p)}}{|1-p^{-s}|^{A_{p,K_1}+\cdots+A_{p,K_k}}} \le \prod_{p<p_0} \frac{(1+p^{-\sigma})^{N_f(p)}}{(1-p^{-\sigma})^{A_{p,K_1}+\cdots+A_{p,K_k}}} \doteq Q(\sigma).$$

Agora, $Q(\sigma) \to 1$ quando $\sigma \to +\infty$, portanto essa função $Q(\sigma)$ é limitada no conjunto $[1/2+\varepsilon,\, +\infty[$. Segue daí que $P(s)$ é limitada em $\mathrm{Re}(s) > 1/2 + \varepsilon$.

Para cada corpo de números K temos, $s = \sigma + it$ com $\sigma \ge 1/2 + \varepsilon$;

$$\begin{aligned}\frac{1}{|R_K(s)|} &= \prod_{P;\, f_P \ge 2} \left|1 - \frac{1}{N(P)^s}\right| \ge \prod_{P;\, f_P \ge 2} \left(1 - \frac{1}{N(P)^\sigma}\right) \\ &\ge \prod_{P;\, f_P \ge 2} \left(1 - \frac{1}{N(P)^{1/2+\varepsilon}}\right) > 0.\end{aligned}$$

Portanto $R_K(s)$ é limitada no semiplano fechado $\sigma \ge 1/2 + \varepsilon$. Analogamente, a igualdade $E_p(s) =$

$1 + g_p(p^{-s})$ implica, usando (6.8), que

$$|E(s)| = \prod_p \left|1 + g_p\left(\frac{1}{p^s}\right)\right| \leq \prod_p \left(1 + \frac{C}{p^{2\sigma}}\right) \leq \prod_p \left(1 + \frac{C}{p^{1+2\varepsilon}}\right) < \infty. \tag{6.10}$$

Portanto $E(s)$ é limitada nesse mesmo semiplano. Isso conclui a prova de que $M_{\mathbf{f}}(s)$ é limitada em $\mathrm{Re}(s) > 1/2 + \varepsilon$.

Dessa forma, usando a estimativa das funções $1/\zeta_{K_i}(s)$ para $i = 1 \ldots, k$ dada pelo Teorema 3.6 e a igualdade

$$L_{\mathbf{f}}(s) = \frac{1}{\zeta_{K_1}(s) \ldots \zeta_{K_k}(s)} M_{\mathbf{f}}(s)$$

temos que $L_{\mathbf{f}}(s) \ll \log^k(|t| + 2)$ em $U_{\mathbf{f}}$. □

6.2 Demonstração da convergência da série $S(\mathbf{f})$

Pela Proposição 6.1 temos, para $\mathrm{Re}(s) > 1$, que

$$L_{\mathbf{f}}^{(l)}(s) = (-1)^l \sum_{d=1}^{+\infty} \frac{\mu(d) \log^l(d) N_f(d)}{d^s},$$

para todo $l \geq 0$. O nosso objetivo agora é usar o Teorema C.2 para justificar a igualdade

$$L_{\mathbf{f}}^{(l)}(1) = (-1)^l \sum_{d=1}^{+\infty} \frac{\mu(d) \log^l(d) N_f(d)}{d} \tag{6.11}$$

para todo $l \geq 0$. Em particular, se $l = k$ a equação (6.11) demonstra a convergência da série $S(\mathbf{f})$. Assim, precisamos considerar as somas dos coeficientes da série $L_{\mathbf{f}}^{(l)}(s)$ para cada $l \geq 0$. Definimos

$$S_l(x) \doteq \sum_{d \leq x} \mu(d) \log^l(d) N_f(d).$$

Para usar o Teorema C.2, resta apenas provar que $S_l(x) = o(x)$. Agora, pelo Lema 5.2 temos

$$S_l(x) = \sum_{d \leq x} \mu(d) N_f(d) \log^l(d) = S_0(x) \log^l x - \int_1^x S_0(t) \frac{l \log^{l-1} t}{t} \, \mathrm{d}t. \tag{6.12}$$

Assim, se provarmos que $S_0(x) = O(x/\log^{l+1} x)$, teremos

$$S_l(x) \ll \frac{x}{\log x} + l \int_2^x \frac{1}{\log^2 t} \, \mathrm{d}t + l \int_1^2 S_0(t) \frac{\log^{l-1} t}{t} \, \mathrm{d}t = o(x),$$

e poderemos aplicar o Teorema C.2. De fato provaremos mais do que $S_0(x) = O(x/\log^N x)$ para todo $N \in \mathbb{N}$:

Teorema 6.4. *Existe $c(\mathbf{f}) > 0$ tal que*

$$S_0(x) \ll x \exp\left(-c(\mathbf{f}) \sqrt{\log x}\right)$$

para $x \to +\infty$.

Demonstração. Como na demonstração da Proposição 6.1 temos, para $s = \sigma + it$, $\sigma > 1$, que

$$|L_{\mathbf{f}}(s)| \leq \sum_{d=1}^{+\infty} \frac{|\mu(d)| N_f(d)}{d^\sigma} \leq \sum_{d=1}^{+\infty} \frac{|\mu(d)| h^{\omega(d)}}{d^\sigma} = M(\sigma) \tag{6.13}$$

onde

$$M(s) \doteq \sum_{d=1}^{+\infty} \frac{|\mu(d)|h^{\omega(d)}}{d^s}.$$

Vimos na demonstração da Proposição 6.1 que a série que define $M(s)$ converge absolutamente se $\sigma > 1$.

Vamos estender a função $M(s)$ comparando o seu produto de Euler com o da função $\zeta(s)$. (O "truque" para fazer isso é o mesmo da demonstração do Lema 6.2.) Se $\sigma > 1$ temos

$$M(s) = \prod_p \left(1 + \frac{h}{p^s}\right) = \zeta(s)^h Z(s)$$

em que

$$Z(s) \doteq \prod_p \left[\left(1 + \frac{h}{p^s}\right)\left(1 - \frac{1}{p^s}\right)^h\right].$$

Fixe p primo e s. Expandindo $(1 - p^{-s})^h$ temos

$$\begin{aligned}\left(1 + \frac{h}{p^s}\right)\left(1 - \frac{1}{p^s}\right)^h &= \sum_{j=0}^{h} \binom{h}{j} \frac{(-1)^j}{p^{js}} + \frac{h}{p^s} \sum_{j=0}^{h} \binom{h}{j} \frac{(-1)^j}{p^{js}} \\ &= 1 - \frac{h}{p^s} + \frac{h}{p^s} + O\left(\frac{1}{p^{2\sigma}}\right) = 1 + O\left(\frac{1}{p^{2\sigma}}\right)\end{aligned}$$

em que a constante em O não depende de p nem de s, só de h (só dos coeficientes binomiais). Portanto, o produto que define $Z(s)$ é normalmente convergente se $\sigma > 1/2$, de modo que $Z(s)$ é uma função holomorfa nesse aberto. Além disso prova-se que $Z(s)$ é limitada em todo semiplano fechado $\sigma \geq 1/2+\varepsilon$ da mesma forma como fizemos anteriormente com outras funções. (Por exemplo, como demonstramos a mesma propriedade para a função $E(s)$ em (6.10).)

Como $M(s) = \zeta(s)^h Z(s)$, temos então que a função $M(s)$ possui uma extensão analítica ao aberto $\sigma > 1/2$ com um polo de ordem h em $s = 1$. Como $(\sigma - 1)\zeta(\sigma)$ e $Z(\sigma)$ são limitadas se $1/2 + \varepsilon \leq \sigma \leq 2$, nesse conjunto temos

$$|M(s)| \leq M(\sigma) = \zeta(\sigma)^h Z(\sigma) \ll \frac{1}{(\sigma - 1)^h} \tag{6.14}$$

desde que seja $\sigma \neq 1$. Tomando $\varepsilon > 0$ e $B_{\mathbf{f}} > 0$ do Teorema 6.3 de tal modo que valha

$$U_{\mathbf{f}} \subseteq \{s = \sigma + it \in \mathbb{C} \,:\, \sigma \geq 1/2 + \varepsilon\},$$

segue de (6.13) e (6.14) que também vale

$$L_{\mathbf{f}}(s) \ll \frac{1}{(\sigma - 1)^h} \tag{6.15}$$

para todo $s \in U_{\mathbf{f}}$ com $\sigma \neq 1$.

A fórmula de Perron implica (veja [Ten95, capítulo II.2]), para $\kappa > 1$;

$$\int_1^x S_0(t)\,\mathrm{d}t = \frac{1}{2\pi i} \int_{\kappa - i\infty}^{\kappa + i\infty} L_{\mathbf{f}}(s) \frac{x^{s+1}}{s(s+1)}\,\mathrm{d}s.$$

Assim o nosso objetivo agora é majorar a integral da direita. Começamos truncando a integral e estimando o resto. Fixamos $\kappa \doteq 1 + 1/\log x$. Então

$$\int_1^x S_0(t)\,\mathrm{d}t = \frac{1}{2\pi i} \int_{\kappa - iT}^{\kappa + iT} L_{\mathbf{f}}(s) \frac{x^{s+1}}{s(s+1)}\,\mathrm{d}s + R(x, T) \tag{6.16}$$

em que o resto é

$$R(x,T) \doteq \frac{1}{2\pi i}\int_{\kappa+iT}^{\kappa+i\infty} L_{\mathbf{f}}(s)\frac{x^{s+1}}{s(s+1)}\,\mathrm{d}s + \frac{1}{2\pi i}\int_{\kappa-i\infty}^{\kappa-iT} L_{\mathbf{f}}(s)\frac{x^{s+1}}{s(s+1)}\,\mathrm{d}s.$$

Majorando essas duas integrais da mesma forma e usando (6.15) temos

$$\begin{aligned} R(x,T) &\ll \int_{\kappa+iT}^{\kappa+i\infty} \frac{1}{(\kappa-1)^h}\frac{x^{\kappa+1}}{|s|^2}\,|\mathrm{d}s| \ll \frac{x^{\kappa+1}}{(\kappa-1)^h}\int_T^{+\infty}\frac{1}{t^2}\,\mathrm{d}t \\ &\ll \frac{x^{\kappa+1}}{(\kappa-1)^h}\cdot\frac{1}{T}, \end{aligned}$$

para $x, T \to +\infty$. Agora como $\kappa = 1 + 1/\log x$, temos $x^\kappa = x^{1/\log x}x = ex$ e assim

$$R(x,T) \ll \frac{x^2\log^h x}{T}. \tag{6.17}$$

Sejam $c_2 > 0$ e $\kappa_1 \doteq 1 - (c_2/\log T)$; $0 < \kappa_1 < 1$ para todo $T > 2$. Seja Γ o caminho retangular formado pelos pontos $\kappa \pm iT$, $\kappa_1 \pm iT$ percorrido no sentido anti-horário. Escolhemos c_2 pequeno o suficiente de tal modo que Γ esteja contido em $U_{\mathbf{f}}$ para todo $T > 2$. Então como $L_{\mathbf{f}}(s)$ é holomorfa em $U_{\mathbf{f}}$ ($L_{\mathbf{f}}(s)$ não possui polos!), temos

$$\int_\Gamma L_{\mathbf{f}}(s)\frac{x^{s+1}}{s(s+1)}\,\mathrm{d}s = 0. \tag{6.18}$$

Vamos agora majorar as integrais da função $L_{\mathbf{f}}(s)x^{s+1}/s(s+1)$ sobre as retas $[\kappa+iT, \kappa_1+iT]$, $[\kappa_1+iT, \kappa_1-iT]$ e $[\kappa_1-iT, \kappa-iT]$ e usar (6.18) para obter uma majoração para a integral sobre a reta $[\kappa-iT, \kappa+iT]$.

Usando a estimativa do Teorema 6.3 temos (com $s = \sigma + it$),

$$\begin{aligned} \int_{\kappa_1-iT}^{\kappa_1+iT} L_{\mathbf{f}}(s)\frac{x^{s+1}}{s(s+1)}\,\mathrm{d}s &\ll x^{\kappa_1+1}\int_{\kappa_1-iT}^{\kappa_1+iT}\frac{\log^k(|t|+2)}{|s|^2}\,|\mathrm{d}s| \\ &\ll x^2 x^{-c_2/\log T}\int_{\kappa_1-iT}^{\kappa_1+iT}\frac{\log^k(|t|+2)}{4^{-1}+t^2}\,|\mathrm{d}s| \\ &\ll x^2 e^{-c_2\log x/\log T} \end{aligned} \tag{6.19}$$

para $x, T \to +\infty$, e usamos $\int_{-\infty}^{+\infty}\log^k(|t|+2)/(4^{-1}+t^2)\,\mathrm{d}t < \infty$.

Estimando analogamente temos

$$\int_{\kappa_1+iT}^{\kappa+iT} L_{\mathbf{f}}(s)\frac{x^{s+1}}{s(s+1)}\,\mathrm{d}s \ll \log^k T\int_{\kappa_1+iT}^{\kappa+iT}\frac{x^{\sigma+1}}{T^2}\,|\mathrm{d}s| = \frac{\log^k T}{T^2}\int_{\kappa_1}^{\kappa} x^{\sigma+1}\,\mathrm{d}\sigma.$$

Calculando essa última integral e majorando $x^{\kappa_1+1} \ll x^{\kappa+1} = ex^2 \ll x^2$, temos

$$\int_{\kappa_1+iT}^{\kappa+iT} L_{\mathbf{f}}(s)\frac{x^{s+1}}{s(s+1)}\,\mathrm{d}s \ll \frac{\log^k T}{T^2}\cdot\frac{x^2}{\log x} \ll x^2\frac{\log^k T}{T^2}. \tag{6.20}$$

Analogamente, obtemos

$$\int_{\kappa_1-iT}^{\kappa-iT} L_{\mathbf{f}}(s)\frac{x^{s+1}}{s(s+1)}\,\mathrm{d}s \ll x^2\frac{\log^k T}{T^2}. \tag{6.21}$$

Usando (6.19), (6.20) e (6.21), obtemos de (6.18) que

$$\int_{\kappa-iT}^{\kappa+iT} L_{\mathbf{f}}(s)\frac{x^{s+1}}{s(s+1)}\,\mathrm{d}s \ll x^2\frac{\log^k T}{T^2} + x^2\exp\left(-c_2\frac{\log x}{\log T}\right).$$

Logo, de (6.16) e (6.17) temos

$$\int_1^x S_0(t)\,\mathrm{d}t \ll x^2\frac{\log^k T}{T^2} + x^2\exp\left(-c_2\frac{\log x}{\log T}\right) + x^2\frac{\log^k x}{T}.$$

Colocando então $T = \exp(\sqrt{\log x})$, vale

$$\begin{aligned}\int_1^x S_0(t)\,\mathrm{d}t &\ll x^2\frac{\sqrt{\log^{k+h} x}}{e^{(2-c_2)\sqrt{\log x}}}\exp\left(-c_2\sqrt{\log x}\right) + x^2\exp\left(-c_2\sqrt{\log x}\right)\\ &\ll x^2\exp\left(-c_2\sqrt{\log x}\right).\end{aligned} \tag{6.22}$$

Vamos agora estimar uma integral semelhante usando a função $M(s)$ ao invés da $L_{\mathbf{f}}(s)$. Ao invés da soma $S_0(x)$, aparecerá a função

$$B(x) \doteq \sum_{n\leq x}|\mu(n)|h^{\omega(n)}.$$

Usando a majoração $\zeta(s) \ll \log|t|$ para $s = \sigma + it$ com $\sigma \geq 1 - B_{\mathbf{f}}/\log|t|$ e $|t| \geq 3$ (é o Teorema 7 de [Ten95, Cap. II.3]), temos

$$M(s) = \zeta(s)^h Z(s) \ll \log^h|t| \tag{6.23}$$

se $s = \sigma + it$ com $|t| \geq 3$, usando novamente que $Z(s)$ é limitada em $U_{\mathbf{f}}$. Usando também (6.14), obtemos uma majoração para $\int_1^x B(t)\,\mathrm{d}t$ exatamente da mesma forma como obtivemos (6.22), com uma pequena diferença apenas na majoração da integral

$$\begin{aligned}\int_{\kappa_1-iT}^{\kappa_1+iT} M(s)\frac{x^{s+1}}{s(s+1)}\,\mathrm{d}s &= \left(\int_{\kappa_1-3i}^{\kappa_1+3i} + \int_{\kappa_1-iT}^{\kappa_1-i3} + \int_{\kappa_1+3i}^{\kappa_1+iT}\right) M(s)\frac{x^{s+1}}{s(s+1)}\,\mathrm{d}s\\ &\ll \int_{\kappa_1-3i}^{\kappa_1+3i}\frac{1}{|\kappa_1-1|^h}\frac{|x^{s+1}|}{|s(s+1)|}\,|\mathrm{d}s| + \int_{\kappa_1+3i}^{\kappa_1+iT}\log^h|t|\frac{|x^{s+1}|}{|s(s+1)|}\,|\mathrm{d}s|\end{aligned}$$

Logo, como fizemos em (6.19), temos

$$\begin{aligned}\int_{\kappa_1-iT}^{\kappa_1+iT} M(s)\frac{x^{s+1}}{s(s+1)}\,\mathrm{d}s &\ll x^{\kappa_1+1}\log^h T\int_{-3}^{3}\frac{1}{4^{-1}+t^2}\,\mathrm{d}t + x^2e^{-c_2\log x/\log T}\\ &\ll x^2e^{-c_2\log x/\log T}\log^h T + x^2e^{-c_2\log x/\log T}.\end{aligned}$$

Colocando então $T = \exp(\sqrt{\log x})$, teremos

$$\begin{aligned}\int_{\kappa_1-iT}^{\kappa_1+iT} M(s)\frac{x^{s+1}}{s(s+1)}\,\mathrm{d}s &\ll x^2e^{-c_2\sqrt{\log x}}(\log x)^{h/2} + x^2e^{-c_2\sqrt{\log x}}\\ &\ll x^2\exp\left(-c_3\sqrt{\log x}\right)\end{aligned}$$

para algum $c_3 > 0$, $c_3 < c_2$.

Além dessa diferença, ao invés de (6.18) teremos

$$\int_\Gamma M(s)\frac{x^{s+1}}{s(s+1)}\,\mathrm{d}s = \Phi(x),$$

onde $\Phi(x)$ é o resíduo da função $s \mapsto M(s)x^{s+1}/s(s+1)$ em $s = 1$, de modo que, por fim, teremos

$$\int_1^x B(t)\,\mathrm{d}t = \Phi(x) + O\left(x^2e^{-c_3\log x/\log T}\right). \tag{6.24}$$

Provemos que $\Phi(x) = x^2Q(\log x)$ com $Q(x)$ polinômio de grau menor ou igual a h. Fixamos x e

definimos

$$g(s) \doteq (s-1)^h \frac{M(s)x^{s+1}}{s(s+1)},$$

de modo que temos

$$\Phi(x) = \lim_{s\to 1} g^{(h)}(s).$$

Agora, se $f(s) \doteq (s-1)^h M(s)/s(s+1)$, temos $g(s) = x^{s+1}f(s)$. Logo

$$g^{(h)}(s) = \sum_{l=0}^{h} \binom{h}{l} f^{(h-l)}(s) \frac{\mathrm{d}^l}{\mathrm{d}s^l}(x^{s+1}) = \sum_{l=0}^{h} \binom{h}{l} f^{(h-l)}(s) \log^l x \cdot x^{s+1}.$$

Fazendo $s \to 1$ isso prova que de fato existe $Q(X)$ polinômio de grau menor ou igual a h, cujos coeficientes independem de x, tal que $\Phi(x) = x^2 Q(\log x)$.

Calculando explicitamente as derivadas, vemos que, se $l \geq 0$, vale

$$\frac{\mathrm{d}^2}{\mathrm{d}x^2}\left(x^2 \log^l x\right) = O(\log^l x).$$

Dessa forma, como $\Phi(x) = x^2 Q(\log x)$, temos que

$$\Phi''(x) = O(\log^h x). \tag{6.25}$$

Vamos finalmente obter uma estimativa para $S_0(x)$ a partir de (6.22) e (6.24). Para isso escrevemos, para $u > 0$,

$$S_0(x) = \frac{1}{u}\int_x^{x+u} S_0(t)\,\mathrm{d}t + O\left(\frac{1}{u}\int_x^{x+u} |S_0(t) - S_0(x)|\,\mathrm{d}t\right). \tag{6.26}$$

Essa igualdade vale pois

$$S_0(x) - \frac{1}{u}\int_x^{x+u} S_0(t)\,\mathrm{d}t = \frac{1}{u}\int_x^{x+u} \big(S_0(x) - S_0(t)\big)\,\mathrm{d}t.$$

Agora

$$\begin{aligned}\int_x^{x+u} |S_0(t) - S_0(x)|\,\mathrm{d}t &\leq \int_x^{x+u} \left(\sum_{x<u\leq t} |\mu(n)N_f(n)|\right)\,\mathrm{d}t \\ &\leq \int_x^{x+u} \left(\sum_{x<u\leq t} |\mu(n)|h^{\omega(n)}\right)\,\mathrm{d}t.\end{aligned}$$

Isto é;

$$\begin{aligned}\int_x^{x+u} |S_0(t) - S_0(x)|\,\mathrm{d}t &\leq \int_x^{x+u} \big(B(t) - B(x)\big)\,\mathrm{d}t = \int_x^{x+u} B(t)\,\mathrm{d}t - uB(x) \\ &\leq \int_x^{x+u} B(t)\,\mathrm{d}t - \int_{x-u}^{x} B(x)\,\mathrm{d}t \\ &\leq \int_x^{x+u} B(t)\,\mathrm{d}t - \int_{x-u}^{x} B(t)\,\mathrm{d}t\end{aligned}$$

Então usando (6.24) temos

$$\int_x^{x+u} |S_0(t) - S_0(x)| \, \mathrm{d}t \leq \Phi(x+u) - \Phi(x) - \big(\Phi(x) - \Phi(x-u)\big) + O\left(x^2 e^{-c_3\sqrt{\log x}}\right).$$

Aplicando então o Teorema do Valor Médio três vezes, às funções Φ e Φ', vemos que

$$\int_x^{x+u} |S_0(t) - S_0(x)| \, \mathrm{d}t \leq 2u^2 \max_{t\in[x-u,x+u]} \Phi''(t) + O\left(x^2 e^{-c_3\sqrt{\log x}}\right).$$

Logo de (6.25) temos

$$\int_x^{x+u} |S_0(t) - S_0(x)| \, \mathrm{d}t \ll u^2 \log^h(x+u) + x^2 e^{-c_3\sqrt{\log x}}.$$

Colocando $u = xe^{-c_4\sqrt{\log x}}$, com $c_4 > 0$ e $2c_4 < c_3$, temos $u = xe^{-c_4\sqrt{\log x}} \leq x$ para x suficientemente grande, e obtemos

$$\begin{aligned}\int_x^{x+u} |S_0(t) - S_0(x)| \, \mathrm{d}t &\ll x^2 e^{-2c_4\sqrt{\log x}} \log^h(2x) + x^2 e^{-c_3\sqrt{\log x}} \\ &\ll x^2 e^{-c_5\sqrt{\log x}}\end{aligned}$$

para algum $c_5 > c_4 > 0$, $c_5 < 2c_4$. Colocando também $u = xe^{-c_4\sqrt{\log x}}$ em (6.26) e usando (6.22) obtemos finalmente

$$\begin{aligned}S_0(x) &\ll \frac{1}{u}\left(4x^2 e^{-c_3\sqrt{\log x}} + x^2 e^{-c_3\sqrt{\log x}}\right) + xe^{-(c_5-c_4)\sqrt{\log x}} \\ &\ll xe^{-c_6\sqrt{\log x}}\end{aligned}$$

para algum $c_6 > 0$. □

6.3 Demonstração da igualdade $S(\mathbf{f}) = C(\mathbf{f})$

Vamos usar um Teorema que nos permitirá relacionar $C(\mathbf{f})$ com a função $L_{\mathbf{f}}(s)$:

Teorema 6.5. *Vale a seguinte igualdade*

$$C(\mathbf{f}) = \lim_{\sigma\to 1^+} \prod_p \left[\left(1 - \frac{1}{p^\sigma}\right)^{-k} \left(1 - \frac{N_f(p)}{p^\sigma}\right)\right]. \tag{6.27}$$

Provemos primeiro que $S(\mathbf{f}) = C(\mathbf{f})$ assumindo valer o Teorema 6.5. Usando a fórmula do produto de Euler das séries de Dirichlet $\zeta(s)$ e $L_{\mathbf{f}}(s)$, segue de (6.27) que

$$\begin{aligned}C(\mathbf{f}) &= \lim_{\sigma\to 1^+} \prod_p \left[\left(1 - \frac{1}{p^\sigma}\right)^{-k} \left(1 - \frac{N_f(p)}{p^\sigma}\right)\right] = \lim_{\sigma\to 1^+} \left[\zeta(\sigma)^k L_{\mathbf{f}}(\sigma)\right] \\ &= \lim_{\sigma\to 1^+} \left\{[(\sigma-1)\zeta(\sigma)]^k \cdot \frac{L_{\mathbf{f}}(\sigma)}{(\sigma-1)^k}\right\} = 1 \cdot \lim_{\sigma\to 1^+} \frac{L_{\mathbf{f}}(\sigma)}{(\sigma-1)^k} = \frac{1}{k!} L_{\mathbf{f}}^{(k)}(1) \\ &= \frac{(-1)^k}{k!} \sum_{d=1}^{+\infty} \frac{\mu(d)\log^k(d) N_f(d)}{d} = S(\mathbf{f})\end{aligned}$$

usando as propriedades já demonstradas da função $L_{\mathbf{f}}(s)$, em especial a igualdade (6.11). Assim $C(\mathbf{f}) = S(\mathbf{f})$. □

Demonstração do Teorema 6.5. Para $\sigma > 1$, usando os produtos de Euler de $\zeta(\sigma)$ e $L_{\mathbf{f}}(\sigma)$ temos

que

$$\prod_p \left[\left(1 - \frac{1}{p^\sigma}\right)^{-k} \left(1 - \frac{N_f(p)}{p^\sigma}\right) \right] = \zeta(\sigma)^k L_{\mathbf{f}}(\sigma).$$

Queremos então calcular

$$\lim_{\sigma \to 1^+} \prod_p \left[\left(1 - \frac{1}{p^\sigma}\right)^{-k} \left(1 - \frac{N_f(p)}{p^\sigma}\right) \right] = \lim_{\sigma \to 1^+} \zeta(\sigma)^k L_{\mathbf{f}}(\sigma).$$

Usando o Lema 6.2 temos, para $\sigma > 1$,

$$\zeta(\sigma)^k L_{\mathbf{f}}(\sigma) = M_{\mathbf{f}}(\sigma) \cdot \frac{\zeta(\sigma)}{\zeta_{K_1}(\sigma)} \cdot \frac{\zeta(\sigma)}{\zeta_{K_2}(\sigma)} \cdots \frac{\zeta(\sigma)}{\zeta_{K_k}(\sigma)}.$$

Agora, o valor $M_{\mathbf{f}}(1)$ está bem definido, e as funções $Z_j(s) \doteq \zeta_{K_j}(s)/\zeta(s)$ para $j = 1, \ldots, k$ podem ser estendidas analiticamente a um aberto contendo o semiplano fechado $\mathrm{Re}(s) \geq 1$, de modo que $Z_j(1)$ está bem definido. Dessa forma,

$$\lim_{\sigma \to 1^+} \zeta(\sigma)^k L_{\mathbf{f}}(\sigma) = \frac{M_{\mathbf{f}}(1)}{Z_1(1) \cdot Z_2(1) \cdots Z_k(1)}.$$

Basta provar então que $M_{\mathbf{f}}(1)/(Z_1(1) \cdot Z_2(1) \cdots Z_k(1)) = C(\mathbf{f})$.

Vamos provar a seguir (Lema 6.6) que

$$Z_j(1) = \prod_p \left(1 - \frac{1}{p}\right)^{-A_{p,K_j}+1} \cdot R_{K_j}(1)$$

para todo $j = 1, \ldots, k$. Assim, usando (6.7) (e com a notação da demonstração do Lema 6.2) temos que

$$\frac{M_{\mathbf{f}}(1)}{Z_1(1) \cdots Z_k(1)} = \frac{P(1) \cdot E(1)}{\prod_p (1 - 1/p)^{-A_{p,K_1} - \cdots - A_{p,K_k} + k}} \tag{6.28}$$

Agora

$$P(1) = \prod_{p < p_0} \left(1 - \frac{1}{p}\right)^{-A_{p,K_1} - \cdots - A_{p,K_k} + N_f(p)}$$

e usando (6.4) temos

$$\begin{aligned} E(1) &= \prod_p \left[\left(1 - \frac{N_f(p)}{p}\right) \left(1 - \frac{1}{p}\right)^{-N_f(p)} \right] \\ &= \prod_{p < p_0} \left[\left(1 - \frac{N_f(p)}{p}\right) \left(1 - \frac{1}{p}\right)^{-N_f(p)} \right] \cdot \prod_{p \geq p_0} \left[\left(1 - \frac{N_f(p)}{p}\right) \left(1 - \frac{1}{p}\right)^{-A_{p,K_1} - \cdots - A_{p,K_k}} \right]. \end{aligned}$$

Substituindo essas expressões para $P(1)$ e $E(1)$ em (6.28) temos que

$$\frac{M_{\mathbf{f}}(1)}{Z_1(1) \cdots Z_k(1)} = C(\mathbf{f}). \qquad \square$$

Lema 6.6. *Sejam K um corpo de números e $Z(s) \doteq \zeta_K(s)/\zeta(s)$. Então $Z(s)$ possui uma extensão analítica a um aberto contendo o semiplano fechado* $\mathrm{Re}(s) \geq 1$*, e vale*

$$Z(1) = \prod_p \left(1 - \frac{1}{p}\right)^{-A_{p,K}+1} \cdot R_K(1).$$

Demonstração. Vamos usar aqui o que vimos na demonstração do Lema 3.5. Lembre que usamos o Corolário C.4 em (3.12) para provar o Lema 3.5. De fato, obtivemos assim não só a convergência da série $\sum_p (A_p - 1)/p$, mas também a igualdade

$$\begin{aligned}\sum_p \frac{A_p - 1}{p} &= \log Z(1) - \sum_p \sum_{m \geq 2} \frac{A_p - 1}{m p^m} - \log R_K(1) \\ &= \log Z(1) + \sum_p \left\{ (A_p - 1) \left[\log\left(1 - \frac{1}{p}\right) + \frac{1}{p} \right] \right\} - \log R_K(1).\end{aligned}$$

Como já sabemos que $\sum_p (A_p - 1)/p$ é convergente, podemos separar a série à direita, obtendo

$$\sum_p \frac{A_p - 1}{p} = \log Z(1) + \sum_p \left[(A_p - 1) \log\left(1 - \frac{1}{p}\right) \right] + \sum_p \frac{A_p - 1}{p} - \log R_K(1).$$

Dessa forma

$$\log Z(1) = -\sum_p \left[(A_p - 1) \log\left(1 - \frac{1}{p}\right) \right] + \log R_K(1)$$

e, exponenciando, obtemos o resultado. □

Capítulo 7

A não-regularidade do Λ-cálculo

Fixemos para todo este Capítulo $f_1(X), \ldots, f_k(X)$ uma família apropriada satisfazendo a Hipótese F, e seja $f(X) \doteq f_1(X)f_2(X)\cdots f_k(X)$. Denotemos por h o grau do polinômio $f(X)$.

7.1 Transformações regulares

Como fizemos no caso da Seção 4.4, podemos tentar demonstrar a troca problemática do limite com a série de (5.30) utilizando o conceito de transformação regular (Apêndice B). Lembramos que a série que aparece é

$$\begin{aligned}(1-z)G(z) &= \sum_{d=1}^{+\infty} \frac{\mu(d)\log^k d}{1+z+\ldots z^{d-1}} \sum_{n\leq d;\, f(n)\equiv 0 \,(\mathrm{mod}\, d)} z^n \\ &= \sum_{d=1}^{+\infty} (\mu(d)\log^k d)\frac{1-z}{1-z^d} \sum_{n\leq d;\, f(n)\equiv 0 \,(\mathrm{mod}\, d)} z^n.\end{aligned}$$

Para sermos mais precisos, sejam $d_1 < d_2 < d_3 < \ldots$ os elementos do conjunto $\{d \in \mathbb{N} : N_f(d) \neq 0\}$. Então

$$(1-z)G(z) = \sum_{i=1}^{+\infty} (\mu(d_i)\log^k d_i)\frac{1-z}{1-z^{d_i}} \sum_{n\leq d_i;\, f(n)\equiv 0 \,(\mathrm{mod}\, d_i)} z^n.$$

Apesar de termos restringido os índices da série $(1-z)G(z)$, nem a convergência, nem o valor da série são alterados. Definindo então

$$\phi_i(z) \doteq \frac{d_i}{N_f(d_i)}\frac{1-z}{1-z^{d_i}} \sum_{n\leq d_i;\, f(n)\equiv 0 \,(\mathrm{mod}\, d_i)} z^n,$$

temos que

$$(1-z)G(z) = \sum_{i=1}^{+\infty} \frac{\mu(d_i)\log^k d_i N_f(d_i)}{d_i}\phi_i(z).$$

Isso nos leva a considerar em geral a transformação

$$\phi(x) \doteq \sum_{i=1}^{+\infty} a_i\phi_i(x), \quad \text{para } 0 < x < 1,$$

para qualquer sequência $a_i \in \mathbb{C}$. Se provássemos que a transformação (ϕ) é regular segundo a Seção B.5, seguiria então que a comutação do limite com a soma em (5.30) estaria justificada, pois já vimos que a série resultante é convergente.

Infelizmente esse resultado é falso. Provaremos neste Capítulo que essa transformação *não é*

regular se $h > 1$ (isto é, com exceção do caso de um único polinômio linear), pois verificaremos que a condição 2 do Teorema B.10 não é satisfeita. Isto é; veremos que não existe limitação uniforme para a série

$$\sum_{i=1}^{+\infty} |\phi_i(x) - \phi_{i+1}(x)|, \quad 0 < x < 1. \tag{7.1}$$

Em [HR05, p. 35], Hindry e Rivoal afirmam que a transformação (ϕ) *provavelmente* não é regular *em geral*. O Teorema 7.3 responde assim a essa questão, inclusive especificando que o único caso em que (ϕ) pode ser regular é quando $h = 1$.

A demonstração que faremos do Teorema 7.3 é basicamente uma extensão ao caso da Conjectura de Bateman-Horn da demonstração feita por Golomb em sua tese de doutoramento [Gol56] de que a transformação relacionada à Conjectura dos Primos Gêmeos não é regular.

Observação. Ao contrário do que é feito na Seção B.5, consideraremos o limite quando $x \to 1^-$ (em B.5 fazemos $x \to 0^+$), mas essa diferença claramente não altera a conclusão do Teorema B.10.

É importante notar que precisamos supor $N_f(d_i) \neq 0$ e colocar a constante $d_i/N_f(d_i)$ na definição de $\phi_i(x)$ para termos

$$\phi_i(x) \to 1 \quad \text{quando } x \to 1^-,$$

para todo $i \in \mathbb{N}$. Essa é uma condição necessária para a regularidade de (ϕ) segundo o Teorema B.10.

Para provar que a série (7.1) não é uniformemente limitada, usaremos o seguinte Lema:

Lema 7.1. *Seja $(\alpha_n)_{n\in\mathbb{N}}$ uma sequência de números positivos tais que $\alpha_n \to 0$. Então*

$$\sum_{n=1}^{+\infty} |\alpha_n - \alpha_{n+1}| \geq \max_{n\in\mathbb{N}} \alpha_n.$$

Demonstração. Como $\alpha_n \to 0$, temos que existe N tal que $\alpha_n < \alpha_1/2$ para todo $n \geq N$. Assim,

$$\max_{n\in\mathbb{N}} \alpha_n = \max_{n\leq N} \alpha_n,$$

portanto, esse máximo de fato existe. Seja $n_0 \in \mathbb{N}$ tal que $\alpha_{n_0} = \max_{n\in\mathbb{N}} \alpha_n$.

Podemos supor que $\sum_{n=1}^{+\infty} |\alpha_n - \alpha_{n+1}|$ é finito, pois o caso em que $\sum_{n=1}^{+\infty} |\alpha_n - \alpha_{n+1}| = \infty$ é trivial.

Agora, dado $k \in \mathbb{N}$ com $k > n_0$ temos

$$\sum_{n=1}^{k} |\alpha_n - \alpha_{n+1}| \geq \sum_{n=n_0}^{k} |\alpha_n - \alpha_{n+1}| \geq \left| \sum_{n=n_0}^{k} (\alpha_n - \alpha_{n+1}) \right| = |\alpha_{n_0} - \alpha_{k+1}|.$$

Fazendo $k \to +\infty$ e usando que $\alpha_n \to 0$, segue que

$$\sum_{n=1}^{+\infty} |\alpha_n - \alpha_{n+1}| \geq |\alpha_{n_0}| = \alpha_{n_0} = \max_{n\in\mathbb{N}} \alpha_n. \qquad \square$$

O objetivo é aplicar o Lema 7.1 para a sequência $\phi_i(x)$ para x fixado. Precisamos então provar o seguinte resultado:

Lema 7.2. *Fixado $x \in]0, 1[$, temos que*

$$\phi_i(x) \to 0 \quad \textit{quando} \quad i \to +\infty.$$

Demonstração. Para todo $i \in \mathbb{N}$, temos

$$0 < \phi_i(x) = \frac{d_i}{N_f(d_i)} \frac{1}{1 + x + \cdots + x^{d_i - 1}} \sum_{n \leq d_i,\, f(n) \equiv 0 \,(\mathrm{mod}\, d_i)} x^n \leq \frac{d_i}{N_f(d_i)} N_f(d_i) x^{n_0} \leq d_i x^{n_0}$$

onde $n_0 \in \mathbb{N}$, $n_0 \leq d_i$ é a menor solução de $f(n) \equiv 0 \pmod{d_i}$. Assim $d_i \mid f(n_0)$. Logo, existe uma constante $C' > 0$, que só depende do polinômio $f(X)$, tal que $d_i \leq f(n_0) \leq C' n_0^h$. Portanto, existe uma constante $C > 0$, que também só depende de $f(X)$, tal que $n_0 \geq C d_i^{1/h}$. Dessa forma,

$$0 < \phi_i(x) \leq d_i x^{n_0} \leq d_i x^{C d_i^{1/h}} = d_i (x^C)^{d_i^{1/h}}. \tag{7.2}$$

Agora como $0 < x < 1$ e $C > 0$, temos também que $0 < x^C < 1$, de modo que fazendo $i \to +\infty$ (isto é, $d_i \to +\infty$) segue que (7.2) que $\phi_i(x) \to 0$ quando $i \to +\infty$. □

Podemos agora provar o resultado principal deste Capítulo:

Teorema 7.3. *Se $h > 1$, então a transformação* (ϕ) não *é regular, pois a série*

$$\sum_{i=1}^{+\infty} |\phi_i(x) - \phi_{i+1}(x)|, \quad 0 < x < 1$$

não *é uniformemente limitada.*

Demonstração. Podemos supor que a Conjectura de Bateman-Horn é verdadeira neste caso (para esta família $\mathbf{f}$), pois se o método (ϕ) fosse regular ele implicaria que a conjectura é verdadeira, como vimos anteriormente.

Vamos encontrar uma sequência $(x_j)_{j \in \mathbb{N}}$ de números reais com $x_j \to 1^-$ associada a índices $(i_j)_{j \in \mathbb{N}}$ tal que $\phi_{i_j}(x_j) \to +\infty$ quando $j \to +\infty$. Usando o Lema 7.1, isso implicará que

$$\sum_{i=1}^{+\infty} |\phi_i(x_j) - \phi_{i+1}(x_j)| \geq \phi_{i_j}(x_j) \to +\infty$$

quando $j \to +\infty$ e portanto não pode haver limitação uniforme para a série (7.1).

É importante que tenhamos $x_j \to 1^-$, pois se a série (7.1) fosse uniformemente limitada em algum intervalo $]1 - \delta, 1[$ para algum $\delta \in]0, 1]$, isso bastaria para termos a troca do limite com a série (5.30).

Como supusemos que a Conjectura de Bateman-Horn é verdadeira, existem infinitos $n_0 \in \mathbb{N}$ tais que $f(n_0) = p_1 p_2 \cdots p_k$ com $p_1, p_2, \ldots, p_k$ primos. Além disso, esses primos são distintos pela Hipótese F. Nesse caso, usando o Lema 3.2 temos que

$$N_f\big(f(n_0)\big) = N_f(p_1) \cdot N_f(p_2) \cdots N_f(p_k) \leq h^k. \tag{7.3}$$

Escrevamos $n_1 < n_2 < n_3 < \ldots$ para cada um de tais elementos n_0.

Para cada $j \in \mathbb{N}$, seja $i_j \in \mathbb{N}$ tal que $d_{i_j} = f(n_j)$. Podemos escolher tal d_{i_j} se $N_f(d_{i_j}) \neq 0$, mas isso vale trivialmente pois $f(n_j) \equiv 0 \pmod{f(n_j)}$. Seja também

$$x_j \doteq 1 - \frac{1}{d_{i_j}^{1/h}}.$$

Então usando (7.3) temos

$$\phi_{i_j}(x_j) \geq \frac{d_{i_j}}{h^k}\frac{1-x_j}{1-x_j^{d_{i_j}}}x_j^{n_j} \geq \frac{d_{i_j}}{h^k}(1-x_j)x_j^{n_j} \geq \frac{d_{i_j}}{h^k}d_{i_j}^{-1/h}x_j^{n_j}$$
$$\geq \frac{d_{i_j}^{1-1/h}}{h^k}\left(1-\frac{1}{d_{i_j}^{1/h}}\right)^{n_j} = \frac{d_{i_j}^{1-1/h}}{h^k}\left(1-\frac{1}{f(n_j)^{1/h}}\right)^{n_j}$$

em que usamos que $f(n_j) \equiv 0 \pmod{d_{i_j}}$. Provaremos então que existe $C_f > 0$ que só depende de $f(X)$ tal que

$$\left(1-\frac{1}{f(y)^{1/h}}\right)^{y} \geq C_f, \quad \text{para todo } y > 1. \tag{7.4}$$

Assim teremos que

$$\phi_{i_j}(x_j) \geq \frac{d_{i_j}^{1-1/h}}{h^k}C_f,$$

e como $d_{i_j} \to +\infty$ quando $j \to +\infty$, segue que $\phi_{i_j}(x_j) \to +\infty$. (Aqui usamos a hipótese $h \geq 2$.)

Provemos então que vale (7.4). Temos

$$\log\left[\left(1-\frac{1}{f(y)^{1/h}}\right)^{y}\right] = y\log\left(1-\frac{1}{f(y)^{1/h}}\right)$$
$$= \frac{\log\left(f(y)^{1/h}-1\right) - \frac{1}{h}\log f(y)}{1/y}.$$

Vamos aplicar a Regra de L'Hospital:

$$\frac{\frac{1}{f(y)^{1/h}-1}\cdot\frac{1}{h}f(y)^{1/h-1}f'(y) - \frac{1}{h}\cdot\frac{1}{f(y)}f'(y)}{-1/y^2}$$
$$= \frac{-1}{h}\frac{f'(y)y^2}{f(y)}\left(\frac{f(y)^{1/h}}{f(y)^{1/h}-1}-1\right) = \frac{1}{h}\frac{f'(y)y^2}{f(y)(1-f(y)^{1/h})}$$
$$= \frac{-1}{h}\cdot\frac{f'(y)y^2}{f(y)f(y)^{1/h}}\cdot\frac{1}{1-f(y)^{-1/h}} \to B_f$$

para algum $B_f \in \mathbb{R}$ que só depende de $f(X)$. Assim

$$\left(1-\frac{1}{f(y)^{1/h}}\right)^{y} \to e^{B_f} > 0$$

o que prova (7.4). □

7.2 Transformações semelhantes

Um modo que poderíamos ter usado para tentar obter uma transformação regular (ϕ) seria escolher $d_1, d_2, d_3, \ldots$ os elementos que definem $\phi_i(x)$ como sendo aqueles $d \in \mathbb{N}$ tais que

$$N_f(d) \neq 0 \quad \text{e} \quad d \text{ é livre de quadrados,}$$

pois, na série que define $G(z)$, os termos associados aos índices d que não são livres de quadrados são anulados por causa do termo $\mu(d)$. Apesar disso, a nova transformação (ϕ) associada a esses novos d_i também não seria regular, pela mesma demonstração que fizemos para o Teorema 7.3, dado que a sequência de índices $(i_j)_j$ que obtivemos está associada a elementos d_{i_j} que de fato são

livres de quadrados.

Um terceiro modo pelo qual poderíamos obter uma transformação regular, sugerido por Hindry e Rivoal em [HR05, p. 35] seria definir $\psi_d(x)$ para $d \in \mathbb{N}$ da seguinte forma:

$$\psi_d(x) = \begin{cases} \frac{d}{N_f(d)} \frac{1-x}{1-x^d} \sum_{n \leq d;\, f(n) \equiv 0 \,(\mathrm{mod}\, d)} x^n & \text{se } N_f(d) \neq 0 \\ g_d(x) & \text{se } N_f(d) = 0, \end{cases}$$

em que $g_d(x)$ seriam funções que poderiam de alguma forma ajudar na regularidade de uma transformação (ψ) dada por

$$\psi(x) = \sum_{d=1}^{+\infty} a_d \psi_d(x) \quad \text{para } 0 < x < 1.$$

A definição das funções $g_d(x)$ não importa muito, porque estamos interessados na equação (5.30) e na série

$$\sum_{d=1}^{+\infty} \frac{\mu(d) \log^k dN_f(d)}{d},$$

que anula os termos em que $g_d(x)$ aparece.

Apesar dessa liberdade de escolha para as funções $g_d(x)$, as contas que fizemos anteriormente também provam que mesmo essa transformação (ψ) não poderá ser regular. De fato, sejam novamente $d_1 < d_2 < d_3 < \ldots$ os elementos $d \in \mathbb{N}$ tais que $N_f(d) \neq 0$. Então o Lema 7.2 implica que, para $x \in]0,1[$ fixado,

$$\psi_{d_i}(x) \to 0 \quad \text{quando} \quad i \to +\infty.$$

Assim se $k \in \mathbb{N}$ temos

$$\begin{aligned} \sum_{d=1}^{+\infty} |\psi_d(x) - \psi_{d+1}(x)| &\geq \sum_{d=k}^{d_i-1} |\psi_d(x) - \psi_{d+1}(x)| \geq \left| \sum_{d=k}^{d_i-1} \big(\psi_d(x) - \psi_{d+1}(x)\big) \right| \\ &\geq |\psi_k(x) - \psi_{d_i}(x)| \end{aligned}$$

para todo $i \in \mathbb{N}$ tal que $d_i - 1 > k$. Fazendo $i \to +\infty$ segue que

$$\sum_{d=1}^{+\infty} |\psi_d(x) - \psi_{d+1}(x)| \geq |\psi_k(x)| \quad \text{para todos } k \in \mathbb{N},\ x \in]0,1[.$$

Mas então podemos demonstrar a não-regularidade de (ψ) usando o mesmo argumento da demonstração do Teorema 7.3.

7.3 Uma variante do método da regularidade

O resultado do Teorema 7.3 implica que se quisermos provar a troca do limite com a série (5.30), não é suficiente usar somente a convergência da série $S(\mathbf{f})$; é preciso usar alguma propriedade mais específica dessa série.

Nesse sentido, uma variante mais abrangente do Teorema B.10, sugerida por Hindry e Rivoal em [HR05], que pode vir a ser usada para resolver o problema de (5.30) é o seguinte Teorema:

Teorema 7.4. *Sejam $(\phi_n)_n$ uma sequência de funções definidas em $]0,1[$, e $(r(n))_n$ uma sequência decrescente de números positivos. Suponhamos que*

1. *$\phi_1(x)$ é limitado em $]0,1[$, e vale*

$$\lim_{x \to 1^-} \phi_n(x) = 1 \quad \textit{para todo } n \in \mathbb{N};\ \textit{e}$$

2. existe $H > 0$ constante uniforme tal que

$$\sum_{n=1}^{+\infty} r(n)\big|\phi_n(x) - \phi_{n+1}(x)\big| \leq H \quad \text{para todo } x \in]0,1[.$$

Então dada uma série convergente $\sum_{n=1}^{+\infty} a_n$ tal que

$$\sum_{n>N} a_n = o\big(r(N)\big),$$

temos que a série $\sum_{n=1}^{+\infty} a_n\phi_n(x)$ também é convergente para todo $x \in]0,1[$, e vale

$$\lim_{x\to 1^-} \sum_{n=1}^{+\infty} a_n\phi_n(x) = \sum_{n=1}^{+\infty} a_n. \tag{7.5}$$

Demonstração. Notemos primeiramente que basta provar o resultado supondo $\sum_{n=1}^{+\infty} a_n = 0$. De fato, se $\sum_{n=1}^{+\infty} a_n \neq 0$, definimos $b_1 \doteq a_1 - \sum_{n=1}^{+\infty}$ e $b_n = a_n$ para $n > 1$. Assim $\sum_{n=1}^{+\infty} b_n = 0$. Adimitindo valer o Teorema para a sequência $(b_n)_n$, temos então

$$0 = \lim_{x\to 1^-} \sum_{n=1}^{+\infty} b_n\phi_n(x) = \lim_{x\to 1^-} \left[\sum_{n=1}^{+\infty} a_n\phi_n(x) - \phi_1(x)\sum_{n=1}^{+\infty} a_n\right].$$

Assim segue de $\phi_1(x) \to 1$ quando $x \to 1^-$ que vale (7.5) para a série $\sum_{n=1}^{+\infty} a_n$.

Provemos então que vale o Teorema supondo $\sum_{n=1}^{+\infty} a_n = 0$. Assim se $(S_N)_N$ é a sequência de somas parciais de $\sum_{n=1}^{+\infty} a_n$, temos

$$S_N \doteq \sum_{n=1}^{N} a_n = \sum_{n=1}^{+\infty} a_n - \sum_{n>N} a_n = -\sum_{n>N} a_n = o\big(r(N)\big).$$

Fixemos $x \in]0,1[$. Notemos que

$$\begin{aligned}\sum_{n=1}^{N} a_n\phi_n(x) &= a_1\phi_1(x) + \sum_{n=2}^{N}(S_n - S_{n-1})\phi_n(x)\\ &= S_N\phi_N(x) + \sum_{n=1}^{N-1} S_n\big(\phi_n(x) - \phi_{n+1}(x)\big).\end{aligned} \tag{7.6}$$

Provemos que o termo $S_N\phi_N(x)$ converge para 0 quando $N \to +\infty$. De fato, temos

$$\begin{aligned}|S_N\phi_N(x)| \leq S_N\big|\phi_N(x)\big| &= S_N\left|\sum_{n=1}^{N-1}\big(\phi_{n+1}(x) - \phi_n(x)\big) + \phi_1(x)\right|\\ &\leq S_N|\phi_1(x)| + \frac{S_N}{r(N)}\sum_{n=1}^{N-1} r(N)\big|\phi_n(x) - \phi_{n+1}(x)\big|.\end{aligned}$$

Agora como $r(n)$ é decrescente segue que

$$|S_N\phi_N(x)| \leq S_N|\phi_1(x)| + \frac{S_N}{r(N)}\sum_{n=1}^{N-1} r(n)\big|\phi_n(x) - \phi_{n+1}(x)\big|.$$

Usando o fato de ser $\phi_1(x)$ limitada, a condição 2. do Teorema, e $S_N = o(r(N))$, temos que $S_N\phi_N(x) \to 0$ quando $N \to +\infty$.

Assim, se provarmos que $\sum_{n=1}^{+\infty} S_n(\phi_n(x)-\phi_{n+1}(x))$ é absolutamente convergente, segue de (7.6) fazendo $N \to +\infty$ que $\sum_{n=1}^{+\infty} a_n\phi_n(x)$ é convergente. De fato, como $S_N = o(r(N))$ existe $M \in \mathbb{N}$ tal que $|S_n| \le r(n)$ para todo $n \ge M$. Logo

$$\begin{aligned}\sum_{n=1}^{+\infty}\Big|S_n\big(\phi_n(x)-\phi_{n+1}(x)\big)\Big| &\le \sum_{n=1}^{M-1}\Big|S_n\big(\phi_n(x)-\phi_{n+1}(x)\big)\Big| + \sum_{n=M}^{+\infty} r(n)\big|\phi_n(x)-\phi_{n+1}(x)\big| \\ &\le \sum_{n=1}^{M-1}\Big|S_n\big(\phi_n(x)-\phi_{n+1}(x)\big)\Big| + H < \infty.\end{aligned}$$

Isso termina a prova de que $\sum_{n=1}^{+\infty} a_n\phi_n(x)$ é convergente.

Provemos agora que vale (7.5). Fixemos $\varepsilon > 0$. Como $S_n = o(r(n))$, existe $N \in \mathbb{N}$ tal que

$$|S_n| \le \varepsilon r(n) \quad \text{para todo } n \ge N.$$

Também temos da condição 1. que existe $\delta < 1$ tal que

$$\text{se } x \in]\delta, 1[\quad \text{então} \quad \sum_{n=1}^{N-1} |S_n|\big|\phi_n(x)-\phi_{n+1}(x)\big| < \varepsilon.$$

Assim fazendo $N \to +\infty$ em (7.6) temos

$$\begin{aligned}\left|\sum_{n=1}^{+\infty} a_n\phi_n(x)\right| &= \left|\sum_{n=1}^{+\infty} S_n\big(\phi_n(x)-\phi_{n+1}(x)\big)\right| \\ &\le \sum_{n=1}^{N-1} |S_n|\big|\phi_n(x)-\phi_{n+1}(x)\big| + \sum_{n=N}^{+\infty} \varepsilon r(n)\big|\phi_n(x)-\phi_{n+1}(x)\big| \\ &\le \varepsilon + \varepsilon H\end{aligned}$$

para todo $x \in]\delta, 1[$. Como $\varepsilon > 0$ é arbitrário, temos que vale (7.6). □

Agora, para utilizar o Teorema 7.4 ficamos com o problema de obter uma função $r(N)$ tal que

$$\sum_{d \ge N} \frac{\mu(d)\log^k d\, N_f(d)}{d} = o\big(r(N)\big).$$

Veremos a seguir que o Teorema 6.4 nos permite tomar, para alguma constante $c > 0$, a função $r(N) = \exp(-c\sqrt{\log N})$. Depois ainda temos o problema de verificar a validade da condição 2. do Teorema 7.4, problema esse que ainda não foi resolvido. De fato não sabemos se a função $r(N)$ obtida é pequena o suficiente para valer essa condição. Apesar disso, é interessante a demonstração do Lema 7.5 pois ela mostra como obter uma função $r(N)$ a partir de uma estimativa para $S_0(x)$ como a do Teorema 6.4. Hindry e Rivoal notam em [HR05] que é possível que a estimativa $r(N) = \exp(-c\sqrt{\log N})$ possa ser melhorada com o uso da Hipótese de Riemann generalizada para funções ζ de Dedekind.

Lema 7.5. *Existe $c > 0$ tal que*

$$\sum_{d \ge x} \frac{\mu(d)\log^k d\, N_f(d)}{d} = o\big(\exp(-c\sqrt{\log x})\big)$$

Demonstração. Recuperando a notação da Seção 6.2, temos de (6.12) que

$$S_k(x) \doteq \sum_{d\le x} \mu(d) N_f(d) \log^k(d) = S_0(x)\log^k x - \int_1^x S_0(t)\frac{l\log^{k-1} t}{t}\,\mathrm{d}t.$$

Usando o Teorema 6.4 temos que $S_0(x) = O(x/\log^k x)$, logo

$$\begin{aligned} S_k(x) &= S_0(x)\log^k x - \int_2^x S_0(t)\frac{l\log^{k-1} t}{t}\,\mathrm{d}t - \int_1^2 S_0(t)\frac{l\log^{k-1} t}{t}\,\mathrm{d}t \\ &\ll x e^{-c(\mathbf{f})\sqrt{\log x}}\log^k x + \int_2^x e^{-c(\mathbf{f})\sqrt{\log t}}\log^{k-1} t\,\mathrm{d}t. \end{aligned} \tag{7.7}$$

Agora, se $c_1 \doteq c(\mathbf{f})/2 > 0$, temos

$$\int_2^x e^{-c(\mathbf{f})\sqrt{\log t}}\log^{k-1} t\,\mathrm{d}t \ll \int_2^x e^{-c_1\sqrt{\log t}}\,\mathrm{d}t \sim x e^{-c_1\sqrt{\log x}},$$

o que pode ser verificado diretamente usando a Regra de L'Hôpital. Assim segue de (7.7) que

$$S_k(x) \ll x e^{-c_1\sqrt{\log x}}. \tag{7.8}$$

Usando a Identidade de Abel, temos

$$\sum_{d\le x} \frac{\mu(d)\log^k d\, N_f(d)}{d} = \frac{S_k(x)}{x} + \int_1^x \frac{S_k(t)}{t^2}\,\mathrm{d}t \tag{7.9}$$

para todo $x > 1$. Como $S_k(x) = o(x)$, fazendo $x \to +\infty$ obtemos

$$\sum_{d=1}^{+\infty} \frac{\mu(d)\log^k d\, N_f(d)}{d} = \int_1^{\infty} \frac{S_k(t)}{t^2}\,\mathrm{d}t.$$

Subtraindo (7.9) temos que

$$\sum_{d>x} \frac{\mu(d)\log^k d\, N_f(d)}{d} = -\frac{S_k(x)}{x} + \int_x^{\infty} \frac{S_k(t)}{t^2}\,\mathrm{d}t.$$

Agora se $c \doteq c_1/2$, segue de (7.8) que $S_k(x)/x = o(e^{-c\sqrt{\log x}})$, de modo que basta provar que

$$\int_x^{\infty} \frac{S_k(t)}{t^2}\,\mathrm{d}t = o\big(e^{-c\sqrt{\log x}}\big).$$

Mas isso é fácil de demonstrar usando (7.8), pois então

$$\int_x^{\infty} \frac{S_k(t)}{t^2}\,\mathrm{d}t \ll \int_x^{\infty} \frac{e^{-2c\sqrt{\log t}}}{t}\,\mathrm{d}t.$$

Usando a Regra de L'Hospital, temos $\int_x^{\infty} e^{-2c\sqrt{\log t}} t^{-1}\,\mathrm{d}t = o(e^{-c\sqrt{\log x}})$. (Pode-se provar diretamente que a integral $\int_x^{\infty} e^{-2c\sqrt{\log t}} t^{-1}\,\mathrm{d}t$ é convergente.) □

7.4 Um problema inverso

Um problema interessante relacionado à Conjectura de Bateman-Horn foi proposto em [Bai02]: supondo valer

$$\pi_{\mathbf{f}}(x) \sim \frac{D(\mathbf{f})}{h_1 \cdots h_k} \cdot \frac{x}{\log^k x}$$

para *alguma* constante $D(\mathbf{f}) > 0$, será que é possível provar que $D(\mathbf{f}) = C(\mathbf{f})$? Ou, equivalentemente, será que

$$\psi_{\mathbf{f}}(x) \sim D(\mathbf{f})x \quad \text{implica} \quad D(\mathbf{f}) = C(\mathbf{f})?$$

Podemos tentar seguir o caminho oposto ao que desenvolvemos no Capítulo 5 para resolver esse problema. Começamos com a seguinte Proposição, que é o inverso do Teorema 4.4:

Proposição 7.6. *Seja $(a_n)_n$ uma sequência de números reais não-negativos tal que a série de potências $\sum_{n=0}^{+\infty} a_n x^n$ tem raio de convergência maior ou igual a 1. Supomos que*

$$\sum_{n=0}^{N} a_n \sim A \cdot N$$

para alguma constante $A > 0$. Então vale

$$\lim_{x \to 1^-} (1-x) \sum_{n=0}^{+\infty} a_n x^n = A.$$

A demonstração da Proposição 7.6 é bem simples, e será feita em breve.

Dessa forma, se $\psi_{\mathbf{f}}(x) \sim D(\mathbf{f})x$, temos da Proposição 7.6 que

$$\lim_{z \to 1^-} (1-z)G(z) = \lim_{z \to 1^-} (1-z) \sum_{n=1}^{+\infty} \Lambda\big(f_1(n)\big) \cdots \Lambda\big(f_k(n)\big) z^n = D(\mathbf{f}). \tag{7.10}$$

Agora, como no início deste Capítulo, temos

$$(1-z)G(z) = \sum_{i=1}^{+\infty} \frac{\mu(d_i) \log^k d_i N_f(d_i)}{d_i} \phi_i(z).$$

Vimos que a transformação (ϕ) dada pelas funções $\phi_i(z)$ não é regular (Teorema 7.3) pois a série $\sum_{i=1}^{+\infty} |\phi_i(x) - \phi_{i+1}(x)|$ não é uniformemente limitada para $x \in]0,1[$. Apesar disso é possível que exista alguma sequência $(x_n)_n$ de elementos em $]0,1[$ tais que $x_n \to 1^-$ e com

$$\sum_{i=1}^{+\infty} |\phi_i(x_n) - \phi_{i+1}(x_n)| < H \quad \text{para todo } n \in \mathbb{N} \tag{7.11}$$

para alguma constante H independente de n. Então teríamos que a transformação discreta

$$\sum_{i=1}^{+\infty} a_i \phi_i(x_n)$$

é regular. Isto é; se $\sum_{i=1}^{+\infty} a_i$ é convergente de valor s, então

$$\lim_{n \to +\infty} \sum_{i=1}^{+\infty} a_i \phi_i(x_n) = s.$$

Pode-se demonstrar esse fato adaptando a demonstração do Teorema 7.4 colocando $r(I) = 1$ para

todo $I \in \mathbb{N}$.

No caso que nos interessa, teríamos

$$\lim_{n\to+\infty}(1-x_n)G(x_n) = \lim_{n\to+\infty}\sum_{i=1}^{+\infty}\frac{\mu(d_i)\log^k d_i N_f(d_i)}{d_i}\phi_i(x_n) = C(\mathbf{f}).$$

Por outro lado, segue de (7.10) que

$$\lim_{n\to+\infty}(1-x_n)G(x_n) = D(\mathbf{f}).$$

Assim, provaríamos que $D(\mathbf{f}) = C(\mathbf{f})$.

A conclusão é: apesar de termos visto que a transformação (ϕ) não é regular em $]0,1[$, se ao menos provássemos que ela é "regular" sobre alguma sequência $x_n \to 1^-$, teríamos como resultado (mais fraco) que $D(\mathbf{f}) = C(\mathbf{f})$. Isso seria, de qualquer modo, um resultado interessante que confirmaria o argumento heurístico de Bateman e Horn.

Ainda mais, podemos adaptar a demonstração do Teorema 7.4 para o caso de uma sequência $x_n \to 1^-$ para relaxar a condição (7.11). Assim, se provássemos que $\sum_{i>I}^{+\infty}\mu(d_i)\log^k d_i N_f(d_i)/d_i = r(I)$ para alguma sequência decrescente $(r(I))_I$ (por exemplo aquela dada pelo Lema 7.5), e existisse $H > 0$ constante tal que

$$\sum_{i=1}^{+\infty} r(i)|\phi_i(x_n) - \phi_{i+1}(x_n)| < H \quad \text{para todo } n \in \mathbb{N},$$

teríamos pelo mesmo argumento que $D(\mathbf{f}) = C(\mathbf{f})$.

Demonstração da Proposição 7.6. Seja $(s_n)_n$ a sequência de somas parciais da sequência $(a_n)_n$. Assim, por hipótese, $s_n \sim An$. Dessa forma, $\sum_{n=0}^{+\infty} s_n x^n$ também é convergente em $]0,1[$, e temos

$$(1-x)\sum_{n=0}^{+\infty} s_n x^n = \sum_{n=0}^{+\infty} s_n x^n - \sum_{n=1}^{+\infty} s_{n-1}x^n = \sum_{n=0}^{+\infty} a_n x^n. \tag{7.12}$$

Analogamente, vale

$$(1-x)\sum_{n=0}^{+\infty} nx^n = \sum_{n=0}^{+\infty} x^n = \frac{1}{1-x}. \tag{7.13}$$

Fixemos $\varepsilon > 0$. Como $s_n \sim An$, existe $N \in \mathbb{N}$ tal que

$$|s_n - An| \le \varepsilon An \quad \text{para todo } n > N. \tag{7.14}$$

(Dividindo por An temos a definição do limite $s_n/An \to 1$.) Fixado N, escolhemos $\delta > 0$ tal que

$$\text{se } x \in]1-\delta, 1[, \quad \text{então} \quad \sum_{n=0}^{N}|s_n - An| < \varepsilon\sum_{n=0}^{+\infty} nx^n. \tag{7.15}$$

Isso é sempre possível pois $\sum_{n=0}^{+\infty} nx^n \to +\infty$ quando $x \to 1^-$. Dessa forma, usando (7.12) e (7.13) temos, para $x \in]1-\delta, 1[$, que

$$\begin{aligned}\left|\sum_{n=0}^{+\infty} a_n x^n - A\sum_{n=0}^{+\infty} x^n\right| &\le (1-x)\sum_{n=0}^{+\infty}|s_n x^n - Anx^n| \\ &\le (1-x)\sum_{n=0}^{N}|s_n - An| + (1-x)\sum_{n=N+1}^{+\infty}\varepsilon Anx^n.\end{aligned}$$

Em que usamos também (7.14). Com (7.15) obtemos

$$\left|\sum_{n=0}^{+\infty} a_n x^n - A\sum_{n=0}^{+\infty} x^n\right| \leq \varepsilon(A+1)(1-x)\sum_{n=0}^{+\infty} nx^n = \frac{\varepsilon(A+1)}{1-x},$$

usando (7.13) novamente. Multiplicando por $1-x$ temos

$$\left|(1-x)\sum_{n=0}^{+\infty} a_n x^n - A\right| \leq \varepsilon(A+1) \quad \text{para todo } x \in]1-\delta, 1[. \qquad \square$$

Capítulo 8

O Teorema de Bateman-Stemmler

Fixemos $f_1(X), \dots, f_k(X)$ uma família apropriada pelo resto deste Capítulo. Sejam $f(X) \doteq f_1(X) \cdots f_k(X)$ e $\mathbf{f} \doteq (f_1, \dots, f_k)$.

O objetivo deste Capítulo é demonstrar o seguinte Teorema de Bateman e Stemmler:

Teorema 8.1 (Bateman-Stemmler)**.** *Vale*

$$\pi_{\mathbf{f}}(x) \leq k! 2^k C(\mathbf{f}) \cdot \frac{x}{\log^k x} + o\left(\frac{x}{\log^k x}\right).$$

Observação. Aqui estamos escrevendo $f(x) \leq g(x) + o(h(x))$ para simbolizar que existe uma função $G(x)$ tal que $f(x) \leq G(x)$ e $G(x) = g(x) + o(h(x))$.

O Teorema de Bateman-Stemmler é importante pois é uma evidência em favor da Conjectura de Bateman-Horn. De fato, decorre dele que $\pi_{\mathbf{f}}(x) \ll x/\log^k x$, logo $\pi_{\mathbf{f}}(x)$ não pode crescer mais rapidamente do que o que foi conjecturado. Usaremos também o limite superior para o crescimento da função $\psi_{\mathbf{f}}(x)$, que decorre do Teorema 8.1, no Capítulo 9.

A demonstração do Teorema 8.1 que faremos aqui é basicamente aquela encontrada em [HR05]. O passo principal da demonstração será o uso de uma forma do grande crivo que pode ser encontrada em [Ten95, Corolário 6.1 do Capítulo I.4]. Dada a complexidade da notação desse resultado, o reenunciaremos aqui:

Teorema 8.2. *Sejam $x_{M+1}, \dots, x_{M+M'} \in \mathbb{C}$,*

$$\omega_p \doteq \#\{d \in \mathbb{N},\, d \leq p \,:\, x_n = 0 \text{ para todo } n \equiv d \pmod p\,,\, n \in [M+1, M+M']\},$$

e também

$$b_n \doteq |\mu(n)| \prod_{p|n} \frac{\omega_p}{p - \omega_p}.$$

Então para todo $Q \geq 1$ vale

$$\left| \sum_{M < n \leq M+M'} x_n \right|^2 \leq \frac{M' - 1 + Q^2}{L_0(Q)} \cdot \sum_{M < n \leq M+M'} |x_n|^2 \tag{8.1}$$

em que $L_0(Q) \doteq \sum_{n \leq Q} b_n$.

Não provaremos o Teorema 8.2 aqui.

Vamos primeiramente adaptar o Teorema 8.2 para o nosso caso. Para $N \in \mathbb{N}$, definimos

$$X_N(\mathbf{f}) \doteq \#\{n \in \mathbb{N} \cap]2\sqrt{N}, N] \,:\, f_1(n), \dots, f_k(n) \text{ são todos primos}\}.$$

Vamos então estimar o valor de $X_N(\mathbf{f})$. Fixemos também

$$L(Q) \doteq \sum_{n\leq Q} a_n \quad \text{e} \quad a_n \doteq |\mu(n)| \prod_{p|n} \frac{N_f(p)}{p - N_f(p)}.$$

Então temos

Corolário 8.3. *Para todos $N \in \mathbb{N}$ suficientemente grande e $Q \geq 1$ com $Q \leq \sqrt{N}$, vale*

$$X_N(\mathbf{f}) \leq \frac{N + Q^2}{L(Q)}$$

Demonstração. Seja $M \doteq [2\sqrt{N}]$ o maior inteiro menor ou igual a $2\sqrt{N}$. Defina

$$x_n \doteq \begin{cases} 1, & \text{se } f_1(n), \ldots, f_k(n) \text{ são todos primos} \\ 0, & \text{caso contrário} \end{cases}$$

para $n \in \{M+1, M+2, \ldots, N-M\}$. Substituindo em (8.1) obtemos

$$X(\mathbf{f}) \leq \frac{N + Q^2}{L_0(Q)}. \tag{8.2}$$

Agora tomemos $N \in \mathbb{N}$ suficientemente grande para que valha

$$f_i(n) > Q \quad \text{para todos } n \geq 2\sqrt{N},\ i \in \{1, \ldots, k\}. \tag{8.3}$$

Sempre é possível obter tal N pois, para todo $i \in \{1, \ldots, k\}$, existe $c_i \geq 1$ tal que $f_i(n) \sim c_i n^{h_i}$ onde $h_i \doteq \operatorname{gr} f_i$, e pois $\sqrt{N} \geq Q$.

Com tal N fixado, provemos que, se $p \leq Q$ é primo, então $N_f(p) \leq \omega_p$. De fato, seja $d \in \mathbb{N}$, $d \leq p$ tal que $f(d) \equiv 0 \pmod p$. Provaremos que se $n \in \mathbb{N}$, $M < n \leq N - M$, satisfaz $n \equiv d \pmod p$ então $a_n = 0$. Dessa forma teremos que cada d contado por $N_f(p)$ é também contado em ω_p, de modo que $N_f(p) \leq \omega_p$.

Seja então $n \in \mathbb{N}$, $M < n \leq N - M$, tal que $n \equiv d \pmod p$. Suponhamos por absurdo que $a_n = 1$. Então $f_1(n), \ldots, f_k(n)$ são primos. Mas como $f(n) \equiv f(d) \equiv 0 \pmod p$ temos que existe $i \in \{1, \ldots, k\}$ tal que $p = f_i(n)$. Mas isso contradiz (8.3) pois $p \leq Q$, absurdo.

Agora, para todo p a função $x \mapsto x/(p-x)$ é crescente em $]-\infty, p[$ (basta derivar a função). Portanto, para todo $p \leq Q$, vale

$$\frac{N_f(p)}{p - N_f(p)} \leq \frac{\omega_p}{p - \omega_p}$$

pois $N_f(p) \leq \omega_p$. Mas então segue que, se $(b_n)_{n\leq Q}$ é como no enunciado do Teorema 8.2, então $a_n \leq b_n$ para todo $n \leq Q$. Dessa forma $L(Q) \leq L_0(Q)$ e assim o resultado final segue de (8.2). □

Em vista do Corolário anterior, precisamos estimar o valor $L(Q)$, o que é feito no seguinte Lema:

Lema 8.4. *Para $Q \to +\infty$ vale*

$$L(Q) \doteq \sum_{n\leq Q} a_n \sim \frac{1}{k! C(\mathbf{f})} \cdot \log^k Q.$$

Demonstração. Para obter o comportamento assintótico de $L(Q)$, vamos primeiro considerar a série de Dirichlet

$$P(s) \doteq \sum_{n=1}^{+\infty} \frac{a_n}{n^s}.$$

Como $n \mapsto a_n$ é multiplicativa, temos que $P(s)$ possui o seguinte produto de Euler:

$$P(s) = \prod_p \left(1 + \frac{N_f(p)}{p - N_f(p)} \cdot \frac{1}{p^s}\right) = \prod_p \left(1 + \frac{N_f(p)}{p^{s+1}} \cdot \frac{1}{1 - N_f(p)/p}\right).$$

Agora $N_f(p) < p$ e $N_f(p) < \operatorname{gr} f$ para todo primo p, de modo que

$$\frac{N_f(p)}{1 - N_f(p)/p} = O(1).$$

Portanto, a série que define $P(s)$ é absolutamente convergente para $\operatorname{Re}(s) > 0$. Vamos determinar uma extensão analítica dessa função a um aberto contendo $\operatorname{Re}(s) \geq 0$.

Multiplicando $P(s)$ por $L_{\mathbf{f}}(s+1) = \prod_p (1 - N_f(p)p^{-(s+1)})$ temos

$$\begin{aligned} L_{\mathbf{f}}(s+1)P(s) &= \prod_p \left(1 + \frac{N_f(p)}{p^{s+1}} \cdot \frac{1}{1 - N_f(p)/p} - \frac{N_f(p)}{p^{s+1}} - \frac{N_f(p)^2}{p^{2s+2}} \cdot \frac{1}{1 - N_f(p)/p}\right) \\ &= \prod_p \left(1 + \frac{N_f(p)}{p^{s+1}} \cdot \frac{N_f(p)/p}{1 - N_f(p)/p} - \frac{N_f(p)^2}{p^{2s+2}} \cdot \frac{1}{1 - N_f(p)/p}\right). \end{aligned}$$

Logo

$$L_{\mathbf{f}}(s+1)P(s) = \prod_p \left[1 + \frac{N_f(p)^2}{1 - N_f(p)/p} \cdot \frac{1}{p^2} \cdot \left(\frac{1}{p^s} - \frac{1}{p^{2s}}\right)\right].$$

Concluímos daí que o produto $R(s) \doteq L_{\mathbf{f}}(s+1)P(s)$ é absolutamente convergente para $\operatorname{Re}(s) > -1/2$. De fato, como $N_f(p) < p$ e $N_f(p) < \operatorname{gr} f$ para todo primo p, temos que

$$\frac{N_f(p)^2}{1 - N_f(p)/p} = O(1).$$

Dessa forma, a série

$$\sum_p \frac{N_f(p)^2}{1 - N_f(p)/p} \cdot \frac{1}{p^2} \cdot \left(\frac{1}{p^s} - \frac{1}{p^{2s}}\right) = \sum_p \frac{N_f(p)^2}{1 - N_f(p)/p} \cdot \frac{p^s - 1}{p^{2s+2}}$$

é absolutamente convergente se $\operatorname{Re}(s) > -1/2$.

Assim concluímos que

$$P(s) = \frac{1}{L_{\mathbf{f}}(s+1)} \cdot R(s)$$

com $R(s)$ holomorfa em $\operatorname{Re}(s) > -1/2$, e $L_{\mathbf{f}}(s+1)$ não se anula em um aberto contendo $\operatorname{Re}(s) \geq 0$, exceto por um zero de ordem k em $s = 0$. Agora segue de (6.27) que

$$C(\mathbf{f}) = \lim_{\sigma \to 1^+} [\zeta(\sigma)^k L_{\mathbf{f}}(\sigma)] = \lim_{\sigma \to 1^+} \frac{L_{\mathbf{f}}(\sigma)}{(\sigma - 1)^k}.$$

Como também $R(0) = 1$, temos que

$$\sigma^k P(\sigma) = \frac{\sigma^k}{L_{\mathbf{f}}(\sigma + 1)} R(\sigma) \to \frac{1}{C(\mathbf{f})}$$

quando $\sigma \to 0^+$. Assim o resultado segue do Teorema C.6. □

Podemos finalmente demonstrar o Teorema de Bateman-Stemmler:

Demonstração do Teorema 8.1. Usando a estimativa do Corolário 8.3, temos que para todos $N \in$

$\mathbb{N}$, $Q \geq 1$ com $Q \leq \sqrt{N}$ vale

$$\pi_{\mathbf{f}}(N) \leq 2\sqrt{N} + X_N(\mathbf{f}) \leq 2\sqrt{N} + \frac{N+Q^2}{L(Q)} \tag{8.4}$$

Tomemos $Q \doteq \sqrt{N/\log N} \leq \sqrt{N}$, $N > 2$. Provaremos que com essa escolha vale

$$2\sqrt{N} + \frac{N+Q^2}{L(Q)} = k!\, C(\mathbf{f}) 2^k \cdot \frac{N}{\log^k N} + o\left(\frac{N}{\log^k N}\right), \tag{8.5}$$

o que, com (8.4), prova o resultado.

A equação (8.5) é equivalente a

$$\frac{\log^k N}{N}\left(2\sqrt{N} + \frac{N+Q^2}{L(Q)} - k!\, C(\mathbf{f}) 2^k \cdot \frac{N}{\log^k N}\right) \to 0 \tag{8.6}$$

quando $N \to +\infty$. Agora

$$\begin{aligned}\frac{\log^k N}{N}&\left(2\sqrt{N} + \frac{N+Q^2}{L(Q)} - k!\, C(\mathbf{f}) 2^k \cdot \frac{N}{\log^k N}\right) \\ &= 2\frac{\log^k N \cdot \sqrt{N}}{N} + \frac{\log^k N}{N} \cdot \frac{Q^2}{L(Q)} + \frac{\log^k N}{L(Q)} - k!\, C(\mathbf{f}) 2^k. \end{aligned} \tag{8.7}$$

Do Lema 8.4 temos que

$$L(Q) \sim \frac{\log^k Q}{k! C(\mathbf{f})} = \frac{1}{k! C(\mathbf{f}) 2^k} \cdot (\log N - \log\log N)^k \sim \frac{1}{k! C(\mathbf{f}) 2^k} \cdot \log^k N.$$

Substituindo em (8.7), temos que de fato vale (8.6). □

8.1 Estimativas para $\theta_{\mathbf{f}}(x)$ e $\psi_{\mathbf{f}}(x)$

Como corolários do Teorema de Bateman-Stemmler, obtemos também estimativas para as funções $\theta_{\mathbf{f}}(x)$ e $\psi_{\mathbf{f}}(x)$, como faremos a seguir. No entanto, o objetivo desta Seção é obter uma estimativa para a função $\psi_{\mathbf{f}}(x)$ que será usada no Capítulo 9, de modo que não seremos cuidadosos a ponto de obter um resultado preciso como o do Teorema 8.1; aqui vamos simplesmente estudar a ordem de crescimento das funções $\theta_{\mathbf{f}}(x)$ e $\psi_{\mathbf{f}}(x)$:

Corolário 8.5. *Vale*

$$\theta_{\mathbf{f}}(x) = O(x).$$

Demonstração. Basta repetir parte da demonstração do Teorema 5.3. Seja

$$g(x) \doteq \log f_1(x) \cdots \log f_k(x) \sim h_1 \cdots h_k \cdot \log^k x.$$

Então vimos que segue da Identidade de Abel que

$$\frac{\theta_{\mathbf{f}}(x)}{x} = \frac{\pi_{\mathbf{f}}(x) g(x)}{x} - \frac{1}{x}\int_1^x g'(t)\pi_{\mathbf{f}}(t)\,\mathrm{d}t \tag{8.8}$$

(como fizemos para provar (5.5)). Agora segue do Teorema 8.1 que

$$\pi_{\mathbf{f}}(x) \ll \frac{x}{\log^k x} \ll \frac{x}{g(x)}.$$

Dessa forma podemos provar

$$\int_1^x g'(t)\pi_{\mathbf{f}}(t)\,\mathrm{d}t = o(x)$$

assim como provamos (5.7). Agora como $\pi_{\mathbf{f}}(x) \ll x/g(x)$, segue de (8.8) que

$$\frac{\theta_{\mathbf{f}}(x)}{x} = O(1). \qquad \square$$

Corolário 8.6. *Vale*

$$\psi_{\mathbf{f}}(x) = O(x).$$

Demonstração. Segue do Corolário 8.5 e de (5.18). $\square$

Capítulo 9

Variante: o Λ-cálculo de Golomb usando séries de Dirichlet

Fixemos $f_1(X), \ldots, f_k(X)$ uma família apropriada e que satisfaz a Hipótese F pelo resto deste Capítulo. Sejam $f(X) \doteq f_1(X) \cdots f_k(X)$ e $\mathbf{f} \doteq (f_1, \ldots, f_k)$.

Neste capítulo, vamos descrever o método de Golomb usando séries de Dirichlet como feito em [Con03]. Isto é; ao invés de considerarmos a série de potências

$$G(z) \doteq \sum_{n=0}^{+\infty} \Lambda\big(f_1(n)\big) \cdots \Lambda\big(f_k(n)\big) z^n$$

como fizemos no Capítulo 5, vamos estudar a seguinte série de Dirichlet:

$$F(s) \doteq \sum_{n=1}^{+\infty} \frac{\Lambda\big(f_1(n)\big) \cdots \Lambda\big(f_k(n)\big)}{n^s}.$$

Veremos que no caso dessa série de Dirichlet, obtemos o mesmo resultado que conseguimos usando a série de potências: a menos de alguns problemas analíticos, prova-se a Conjectura de Bateman-Horn com exatamente a mesma constante $C(\mathbf{f})$ conjecturada.

O teorema tauberiano que usaremos para tentar obter a Conjectura de Bateman-Horn a partir da análise de $F(s)$ será o Teorema C.3. Precisamos então verificar as hipóteses desse Teorema. De fato, a série $F(s)$ é absolutamente convergente se $\mathrm{Re}(s) > 1$, o que decorre diretamente do Lema 5.13. Além disso, temos

$$\sum_{n \leq v} \Lambda\big(f_1(n)\big) \cdots \Lambda\big(f_k(n)\big) = O(v)$$

pelo Corolário 8.6. Portanto resta apenas obter um prolongamento analítico de $F(s)$ a um aberto contendo o semiplano fechado $\mathrm{Re}(s) \geq 1$, com possivelmente um polo em $s = 1$. Se $F(s)$ possuir um polo em $s = 1$, esse polo será obrigatoriamente um polo simples da função:

Lema 9.1. *Suponhamos que a função $F(s)$ possua um prolongamento analítico a um aberto contendo o semiplano fechado $\mathrm{Re}(s) \geq 1$, com um polo em $s = 1$. Então $s = 1$ é um polo simples de $F(s)$.*

Demonstração. Fixemos $\sigma > 1$. Usando a Identidade de Abel (o Lema 5.2), temos que, para todo $x \geq 1$, vale

$$\sum_{n \leq x} \frac{\Lambda\big(f_1(n)\big) \cdots \Lambda\big(f_k(n)\big)}{n^\sigma} = \frac{\psi_{\mathbf{f}}(x)}{x^\sigma} + \sigma \int_1^x \frac{\psi_{\mathbf{f}}(t)}{t^{\sigma+1}} \, \mathrm{d}t.$$

Como $\sigma > 1$ e $\psi_{\mathbf{f}}(x) \ll x$, temos que $\psi_{\mathbf{f}}(x) = o(x^\sigma)$. Assim fazendo $x \to +\infty$ obtemos

$$\sum_{n=1}^{+\infty} \frac{\Lambda\big(f_1(n)\big)\cdots\Lambda\big(f_k(n)\big)}{n^\sigma} = \sigma \int_1^{+\infty} \frac{\psi_{\mathbf{f}}(t)}{t^{\sigma+1}}\,\mathrm{d}t.$$

Logo

$$F(\sigma) = \sigma \int_1^{+\infty} \frac{\psi_{\mathbf{f}}(t)}{t^{\sigma+1}}\,\mathrm{d}t \ll \sigma \int_1^{+\infty} \frac{t}{t^{\sigma+1}}\,\mathrm{d}t = \frac{\sigma}{\sigma-1},$$

para todo $\sigma \to 1^+$. Portanto $\sigma \mapsto (\sigma-1)F(\sigma)$ é limitada numa região à direita e próxima de $\sigma = 1$, e dessa forma nenhuma extensão de $F(s)$ pode ter em $s = 1$ um polo de ordem maior do que 1. □

Dessa forma, a menos que a extensão de $F(s)$ possua uma singularidade essencial em $s = 1$, sempre podemos aplicar o Teorema C.3. (Não trataremos neste texto da possibilidade de $F(s)$ ter em $s = 1$ uma singularidade essencial.) Supondo então que $F(s)$ possui uma extensão analítica a um aberto contendo o semiplano $\mathrm{Re}(s) \geq 1$ com no máximo um polo em $s = 1$, podem ocorrer duas coisas: a) $F(s)$ é analítica em $s = 1$, ou b) $F(s)$ possui um polo simples em $s = 1$. Vamos tratar desses dois casos separadamente, e veremos que é bastante improvável que o caso a) ocorra. Veremos também que o caso b) implica a Conjectura de Bateman-Horn, supondo uma troca de limite com uma série.

9.1 Caso a): $F(s)$ é analítica em $s = 1$

Supomos que $F(s)$ é analítica em $s = 1$. Como a série de Dirichlet que define $F(s)$ tem coeficientes não-negativos, o fato de $F(s)$ ser analítica em $s = 1$ (e em uma vizinhança de $s = 1$) implica que de fato a série $F(s)$ é absolutamente convergente em algum semiplano $\mathrm{Re}(s) \geq 1 - \delta$, com $\delta > 0$. Esse resultado é conhecido como Lema de Landau (veja [Apo76, Teorema 11.13]).

Vejamos como isso implica em uma estimativa para $\psi_{\mathbf{f}}(x)$:

Proposição 9.2. *Se $F(s)$ é analítica em uma vizinhança de $s = 1$, então existe $\delta > 0$ tal que*

$$\psi_{\mathbf{f}}(x) = O(x^{1-\delta}).$$

Demonstração. Seja $\delta > 0$ tal que a série de Dirichlet que define $F(s)$ é convergente em $s = 1 - \delta$. Seja

$$a_n \doteq \Lambda\big(f_1(n)\big)\cdots\Lambda\big(f_k(n)\big), \quad \text{para todo } n \in \mathbb{N}.$$

Assim $\psi_{\mathbf{f}}(x) = \sum_{n\leq x} a_n$. Seja $S(x) \doteq \sum_{n\leq x} a_n/n^{1-\delta}$ a soma parcial da série $F(1-\delta)$, que vimos ser convergente. Dessa forma $S(x) = O(1)$. Segue do Lema 5.2 que

$$\psi_{\mathbf{f}}(x) = \sum_{n\leq x} \frac{a_n}{n^{1-\delta}} \cdot n^{1-\delta} = S(x)x^{1-\delta} - \int_1^x S(t)(1-\delta)t^{-\delta}\,\mathrm{d}t. \tag{9.1}$$

Agora como $S(x) = O(1)$ temos

$$\int_1^x S(t)t^{-\delta}\,\mathrm{d}t \ll \int_1^x t^{-\delta}\,\mathrm{d}t = \frac{x^{1-\delta}-1}{1-\delta} \ll x^{1-\delta}.$$

(Aqui precisaríamos tratar separadamente o caso $\delta = 1$, mas nesse caso o resultado da Proposição decorre diretamente do fato de ser $\psi_{\mathbf{f}}(x) = S(x) = O(1)$.) Substituindo em (9.1) e usando novamente $S(x) \ll 1$ temos

$$\psi_{\mathbf{f}}(x) \ll x^{1-\delta} + x^{1-\delta} \ll x^{1-\delta}.$$ □

Como o resultado da Proposição 9.2 certamente não é um resultado esperado em vista da Conjectura de Bateman-Horn, o mais provável é que a série $F(s)$ não seja analítica em $s = 1$.

9.2 Caso b): $F(s)$ tem um polo em $s = 1$

Daqui em diante, vamos supor que $F(s)$ possui uma extensão analítica a um aberto contendo o semiplano fechado $\mathrm{Re}(s) \geq 1$, com um polo simples em $s = 1$. Temos então do Teorema C.3 que

$$\psi_{\mathbf{f}}(x) \sim \operatorname*{Res}_{s=1} F(s) \cdot x.$$

Logo precisamos calcular $\mathrm{Res}_{s=1} F(s)$, o resíduo de $F(s)$ em $s = 1$, e esperamos obter

$$\operatorname*{Res}_{s=1} F(s) = C(\mathbf{f}).$$

Fixemos $s = \sigma + it \in \mathbb{C}$ com $\sigma, t \in \mathbb{R}$ e $\sigma > 1$. Da Identidade de Golomb (Teorema 5.8) temos que

$$F(s) = \frac{(-1)^k}{k!} \sum_{n=1}^{+\infty} \left(\sum_{d \mid f(n)} \mu(d) \log^k d \right) \frac{1}{n^s}.$$

Ou seja, definindo

$$\chi_{d,n} = \begin{cases} 1, & \text{se } d \mid f(n) \\ 0, & \text{caso contrário,} \end{cases}$$

para $d, n \in \mathbb{N}$, temos

$$F(s) = \frac{(-1)^k}{k!} \sum_{n=1}^{+\infty} \sum_{d=1}^{+\infty} \left(\chi_{d,n} \mu(d) \log^k d \cdot \frac{1}{n^s} \right). \tag{9.2}$$

Provemos que é possível inverter a ordem dessas duas séries.

Lema 9.3. *Para* $\mathrm{Re}(s) > 1$*, vale*

$$\sum_{n=1}^{+\infty} \sum_{d=1}^{+\infty} \left(\chi_{d,n} \mu(d) \log^k d \cdot \frac{1}{n^s} \right) = \sum_{d=1}^{+\infty} \sum_{n=1}^{+\infty} \left(\chi_{d,n} \mu(d) \log^k d \cdot \frac{1}{n^s} \right).$$

Demonstração. O resultado segue diretamente do Teorema de Fubini, se provarmos que a série

$$\sum_{n=1}^{+\infty} \sum_{d=1}^{+\infty} \left| \chi_{d,n} \mu(d) \log^k d \cdot \frac{1}{n^s} \right| \tag{9.3}$$

é convergente. De fato, temos

$$\sum_{n=1}^{+\infty} \sum_{d=1}^{+\infty} \left| \chi_{d,n} \mu(d) \log^k d \cdot \frac{1}{n^s} \right| = \sum_{n=1}^{+\infty} \sum_{d \mid f(n)} \left| \mu(d) \log^k d \cdot \frac{1}{n^s} \right| \leq \sum_{n=1}^{+\infty} \sum_{d \mid f(n)} \log^k \big(f(n) \big) \cdot \frac{1}{n^\sigma}.$$

Dessa forma

$$\sum_{n=1}^{+\infty} \sum_{d=1}^{+\infty} \left| \chi_{d,n} \mu(d) \log^k d \cdot \frac{1}{n^s} \right| \leq \sum_{n=1}^{+\infty} \frac{\log^k \big(f(n) \big)}{n^\sigma} \cdot d\big(f(n) \big) \tag{9.4}$$

em que $d(n) \doteq \sum_{d \mid n} 1$ é o número de divisores de n.

Agora, para todo $\varepsilon > 0$ vale

$$d(n) = O(n^\varepsilon)$$

(veja [Apo76, Exercício 13 do Capítulo 13]). Seja $h \doteq \mathrm{gr}\, f$. Assim temos $f(n) = O(n^h)$, de modo que $d(f(n)) = O(n^{h\varepsilon})$ para todo $\varepsilon > 0$. Também temos $\log^k(f(n)) = O(n^\varepsilon)$, portanto, dado $\varepsilon > 0$ existe $M_\varepsilon > 0$ tal que

$$\log^k \big(f(n) \big) \cdot d\big(f(n) \big) \leq M_\varepsilon n^{\varepsilon + h\varepsilon} \quad \text{para todo } n \in \mathbb{N}.$$

Sejam $\delta > 0$ tal que $\sigma = 1 + 2\delta$, e $\varepsilon > 0$ tal que $(1+h)\varepsilon = \delta$. Então temos $M = M_\varepsilon > 0$ tal que

$$\log^k\big(f(n)\big) \cdot d\big(f(n)\big) \leq Mn^\delta \quad \text{para todo } n \in \mathbb{N}.$$

Assim segue de (9.4) que

$$\sum_{n=1}^{+\infty}\sum_{d=1}^{+\infty}\left|\chi_{d,n}\mu(d)\log^k d \cdot \frac{1}{n^s}\right| \leq \sum_{n=1}^{+\infty}\frac{Mn^\delta}{n^{1+2\delta}} = \sum_{n=1}^{+\infty}\frac{M}{n^{1+\delta}} < \infty.$$

Isto é; a série (9.3) converge. □

Portanto, podemos trocar a ordem das séries de (9.2) e então obtemos

$$\begin{aligned} F(s) &= \frac{(-1)^k}{k!}\sum_{d=1}^{+\infty}\sum_{n=1;\, f(n)\equiv 0 \,(\mathrm{mod}\, d)}^{+\infty}\frac{\mu(d)\log^k d}{n^s} \\ &= \frac{(-1)^k}{k!}\sum_{d=1}^{+\infty}\left(\mu(d)\log^k d \cdot \sum_{n=1;\, f(n)\equiv 0 \,(\mathrm{mod}\, d)}^{+\infty}\frac{1}{n^s}\right). \end{aligned}$$

Assim o cálculo do resíduo de $F(s)$ em $s = 1$ é

$$\begin{aligned} \operatorname*{Res}_{s=1} F(s) &= \lim_{\sigma\to 1^+}(\sigma-1)F(\sigma) \\ &= \lim_{\sigma\to 1^+}(\sigma-1)\frac{(-1)^k}{k!}\sum_{d=1}^{+\infty}\left(\mu(d)\log^k d \cdot \sum_{n=1;\, f(n)\equiv 0 \,(\mathrm{mod}\, d)}^{+\infty}\frac{1}{n^\sigma}\right). \end{aligned}$$

Supondo novamente que podemos trocar a ordem do limite com a série, mais um passo que não podemos justificar no momento, obtemos

$$\operatorname*{Res}_{s=1} F(s) \stackrel{?}{=} \frac{(-1)^k}{k!}\sum_{d=1}^{+\infty}\left[\mu(d)\log^k d \cdot \lim_{\sigma\to 1^+}\left((\sigma-1)\sum_{n=1;\, f(n)\equiv 0 \,(\mathrm{mod}\, d)}^{+\infty}\frac{1}{n^\sigma}\right)\right]. \tag{9.5}$$

Agora, esse último limite podemos calcular da seguinte forma:

Lema 9.4. *Seja $d \in \mathbb{N}$ fixo. Então*

$$\lim_{s\to 1}(s-1)\cdot\sum_{n=1;\, f(n)\equiv 0 \,(\mathrm{mod}\, d)}^{+\infty}\frac{1}{n^s} = \frac{N_f(d)}{d}.$$

Demonstração. Sejam $m \doteq N_f(d)$ e $a_1, \ldots, a_m$ as soluções de

$$f(n) \equiv 0 \ (\mathrm{mod}\, d) \tag{9.6}$$

compreendidas entre 1 e d. Dessa forma, se n é solução da equação (9.6), então existe um único $i \in \{1, \ldots, m\}$ tal que $n \equiv a_i \ (\mathrm{mod}\, d)$. Reciprocamente, se $n \equiv a_i \ (\mathrm{mod}\, d)$ para algum $i \in \{1, \ldots, m\}$, então n é solução de (9.6). Dessa forma temos

$$\sum_{n=1;\, f(n)\equiv 0 \,(\mathrm{mod}\, d)}^{+\infty}\frac{1}{n^s} = \sum_{i=1}^{m}\sum_{n\geq 1,\, n\equiv a_i \,(\mathrm{mod}\, d)}\frac{1}{n^s}. \tag{9.7}$$

Fixemos $i \in \{1, \ldots, m\}$. Então

$$\sum_{n \geq 1,\, n \equiv a_i \,(\mathrm{mod}\, d)} \frac{1}{n^s} = \sum_{l=0}^{+\infty} \frac{1}{(dl + a_i)^s} = \frac{1}{d^s} \sum_{l=0}^{+\infty} \frac{1}{(l + b_i)^s} = \frac{\zeta(s, b_i)}{d^s}$$

em que $b_i \doteq a_i/d \leq 1$ e $\zeta(s, b_i)$ é uma função ζ de Hurwitz (veja [Apo76, Cap. 12]). Assim segue de (9.7) que

$$\sum_{n=1;\, f(n) \equiv 0 \,(\mathrm{mod}\, d)}^{+\infty} \frac{1}{n^s} = \sum_{i=1}^{m} \frac{\zeta(s, b_i)}{d^s}.$$

O resultado do Lema segue então do fato de que $\zeta(s, b)$ tem em $s = 1$ um polo simples com resíduo 1 para todo $b \in]0, 1]$ (veja [Apo76, Teorema 12.4]). □

Dessa forma, segue de (9.5) que

$$\operatorname*{Res}_{s=1} F(s) \stackrel{?}{=} \frac{(-1)^k}{k!} \sum_{d=1}^{+\infty} \frac{\mu(d) \log^k d}{d} N_f(d) = S(\mathbf{f}) = C(\mathbf{f}).$$

Concluímos assim que: se $F(s)$ possui uma extensão analítica a um aberto contendo o semiplano fechado $\mathrm{Re}(s) \geq 1$ com um único polo simples em $s = 1$, e se vale a troca do limite com a série de (9.5), então vale a Conjectura de Bateman-Horn.

Apêndice A

O Critério de Kummer

Enunciaremos e demonstraremos aqui um resultado da Teoria Algébrica dos Números que usamos no texto, a saber, o Critério de Kummer. Para a parte básica dessa teoria, veja [Rib01]. Os resultados enunciados aqui foram adaptados de [Nar04, Seção 4.3].

Para esta seção, fixamos $f(X) \in \mathbb{Z}[X]$ um polinômio mônico irredutível, e $\alpha \in \mathbb{C}$ uma raiz de $f(X)$. Sejam $K \doteq \mathbb{Q}(\alpha)$ e $\mathcal{O}_K$ o anel de inteiros do corpo de números K. Como $f(X)$ é mônico, temos $\alpha \in \mathcal{O}_K$, e assim $R \doteq \mathbb{Z}[\alpha]$ é um subanel de $\mathcal{O}_K$. Seja $\mathfrak{f}$ o *condutor* de R em $\mathcal{O}_K$, isto é; $\mathfrak{f}$ é o maior ideal de $\mathcal{O}_K$ contido em R. Esse ideal não é nulo devido ao seguinte Lema:

Lema A.1. *Existe $k \in \mathbb{Z}$, $k \neq 0$ tal que $k\mathcal{O}_K \subseteq R$.*

Demonstração. Sejam $n \doteq [K : \mathbb{Q}]$ e $\{a_1, \ldots, a_n\}$ uma base integral de K. Fixemos $i \in \{1, \ldots, n\}$. Como $a_i \in \mathbb{Q}(\alpha)$, existem $p_{1i}, \ldots, p_{ni}, q_{1i}, \ldots, q_{ni} \in \mathbb{Z}$ com $q_{1i}, \ldots, q_{ni} \neq 0$ tais que

$$a_i = \frac{p_{1i}}{q_{1i}}\alpha^{n-1} + \frac{p_{2i}}{q_{2i}}\alpha^{n-2} + \cdots + \frac{p_{ni}}{q_{ni}}.$$

Assim, se $k_i \doteq q_{1i} \cdots q_{ni} \neq 0$, temos $k_i a_i \in R$.

Definimos $k \doteq k_1 \cdots k_n \neq 0$. Então $ka_i \in R$ para todo $i \in \{1, \ldots, n\}$, de modo que $k\mathcal{O}_K \subseteq R$. □

O objetivo deste Apêndice é demonstrar o seguinte Teorema:

Teorema A.2 (Critério de Kummer)**.** *Seja p um número primo tal que $p \nmid \mathrm{N}(\mathfrak{f})$. Seja $\varphi : \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$ dada por*

$$\varphi(c_k X^k + c_{k-1}X^{k-1} + \cdots + c_0) = \overline{c_k}X^k + \overline{c_{k-1}}X^{k-1} + \cdots + \overline{c_0}$$

em que $\overline{c_j} \doteq c_j + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}$.

Decompondo $\varphi(f)$ em polinômios irredutíveis:

$$\varphi(f) = f_1^{a_1} f_2^{a_2} \cdots f_m^{a_m}$$

com $a_1, \ldots, a_m \in \mathbb{N}$ e $f_1(X), \ldots, f_m(X) \in (\mathbb{Z}/p\mathbb{Z})[X]$ polinômios mônicos irredutíveis (sobre $\mathbb{Z}/p\mathbb{Z}$) não-constantes e distintos, temos que o ideal $p\mathcal{O}_K$ também se decompõe como $\varphi(f)$:

$$p\mathcal{O}_K = P_1^{a_1} P_2^{a_2} \cdots P_m^{a_m}$$

em que $P_1, \ldots, P_m$ são ideais primos de $\mathcal{O}_K$ distintos e $\mathrm{N}(P_i) = p^{n_i}$, em que n_i é o grau do polinômio $f_i(X)$.

Para demonstrar o Teorema A.2, precisamos do seguinte Lema:

Lema A.3. *Seja p um número primo. São equivalentes:*

a) $p\mathcal{O}_K \cap R = pR$*;*

b) a imersão de R *em* $\mathcal{O}_K$ *induz um isomorfismo entre* $\mathcal{O}_K/p\mathcal{O}_K$ *e* $R/(R \cap p\mathcal{O}_K)$ *isto é; cada classe de equivalência de* $\mathcal{O}_K/p\mathcal{O}_K$ *possui um elemento de* R*;*

c) a imersão de R *em* $\mathcal{O}_K$ *induz isomorfismos entre* $\mathcal{O}_K/p^m\mathcal{O}_K$ *e* $R/(R \cap p^m\mathcal{O}_K)$ *para todo* $m \in \mathbb{N}$*;*

d) $p^m\mathcal{O}_K \cap R = p^m R$ *para todo* $m \in \mathbb{N}$*; e*

e) $p \nmid \mathrm{N}(\mathfrak{f})$.

Demonstração. a) $\Rightarrow$ b): Temos um homomorfismo canônico $\phi : R \to \mathcal{O}_K/p\mathcal{O}_K$ dada pela composição dos homomorfismos canônicos $R \to \mathcal{O}_K$ e $\mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K$. Dessa forma $\ker\phi = R \cap p\mathcal{O}_K$. Assim, temos um isomorfismo $R/(R \cap p\mathcal{O}_K) \simeq \operatorname{Im}\phi \subseteq \mathcal{O}_K/p\mathcal{O}_K$. Provemos que $\operatorname{Im}\phi = \mathcal{O}_K/p\mathcal{O}_K$. De fato,

$$\left|\frac{\mathcal{O}_K}{p\mathcal{O}_K}\right| = \mathrm{N}(p\mathcal{O}_K) = |\,\mathrm{N}(p)| = p^n.$$

Por outro lado, usando a), temos

$$|\operatorname{Im}\phi| = \left|\frac{R}{R \cap p\mathcal{O}_K}\right| = \left|\frac{R}{pR}\right| = \left|\frac{\mathbb{Z}[\alpha]}{p\mathbb{Z}[\alpha]}\right| = p^n = \left|\frac{\mathcal{O}_K}{p\mathcal{O}_K}\right|.$$

Portanto $\operatorname{Im}\phi = \mathcal{O}_K/p\mathcal{O}_K$ e $R/(R \cap p\mathcal{O}_K) \simeq \mathcal{O}_K/p\mathcal{O}_K$.

b) $\Rightarrow$ c): Faremos por indução sobre $m \in \mathbb{N}$. Para $m = 1$, o resultado vale por hipótese. Suponhamos agora $\mathcal{O}_K/p^m\mathcal{O}_K \simeq R/(R \cap p^m\mathcal{O}_K)$ para $m \geq 1$. Seja $a \in \mathcal{O}_K$. Precisamos encontrar um elemento de R na mesma classe de equivalência de a em $\mathcal{O}_K/p^{m+1}\mathcal{O}_K$.

Por hipótese de indução, existe $r \in R$ tal que $a \equiv r \pmod{p^m\mathcal{O}_K}$, isto é, existe $b \in \mathcal{O}_K$ tal que $a = r + p^m b$. Por sua vez, existe $r_1 \in R$ tal que $b \equiv r_1 \pmod{p\mathcal{O}_K}$ isto é, existe $b_1 \in \mathcal{O}_K$ tal que $b = r_1 + pb_1$. Assim

$$a = r + p^m r_1 + p^{m+1} b_1 \equiv r + p^m r_1 \left(\mathrm{mod}\, p^{m+1}\mathcal{O}_K\right),$$

com $r + p^m r_1 \in R$, como queríamos.

c) $\Rightarrow$ d): Temos que por c) vale

$$\left|\frac{R}{R \cap p^m\mathcal{O}_K}\right| = \left|\frac{\mathcal{O}_K}{p^m\mathcal{O}_K}\right| = \mathrm{N}(p^m\mathcal{O}_K) = |\,\mathrm{N}(p^m)| = p^{mn}.$$

Por outro lado,

$$\left|\frac{R}{p^m R}\right| = \left|\frac{\mathbb{Z}[\alpha]}{p^m\mathbb{Z}[\alpha]}\right| = p^{mn}.$$

Agora $p^m R \subseteq R \cap p^m\mathcal{O}_K$, de modo que

$$p^{mn} = \left|\frac{R}{R \cap p^m\mathcal{O}_K}\right| = \left|\frac{R/p^m R}{(R \cap p^m\mathcal{O}_K)/p^m R}\right| = \frac{p^{mn}}{\left|(R \cap p^m\mathcal{O}_K)/p^m R\right|}$$

portanto $\left|(R \cap p^m\mathcal{O}_K)/p^m R\right| = 1$ e $R \cap p^m\mathcal{O}_K = p^m R$.

d) $\Rightarrow$ a): Trivial.

d) $\Rightarrow$ e): Pelo Lema A.1 existe $k \in \mathbb{Z}$ tal que $k\mathcal{O}_K \subseteq R$. Escrevemos $k = p^m d$ em que $p \nmid d$. Provemos que $d\mathcal{O}_K \subseteq R$. De fato, se $m = 0$ acabou. Se $m \geq 1$, temos $k\mathcal{O}_K = p^m d\mathcal{O}_K \subseteq p^m\mathcal{O}_K$, logo $p^m d\mathcal{O}_K = k\mathcal{O}_K \subseteq R \cap p^m\mathcal{O}_K = p^m R$ usando d). "Dividindo" por p^m vemos que $d\mathcal{O}_K \subseteq R$. Assim $d\mathcal{O}_K \subseteq \mathfrak{f}$, de modo que $\mathfrak{f} \mid d\mathcal{O}_K$ e portanto $\mathrm{N}(\mathfrak{f}) \mid \mathrm{N}(d\mathcal{O}_K) = d^n$. Como $p \nmid d$, segue que $p \nmid \mathrm{N}(\mathfrak{f})$.

e) $\Rightarrow$ b): Notemos que $\mathrm{mdc}(\mathfrak{f}, p\mathcal{O}_K) = \mathcal{O}_K$. De fato, se I é um ideal inteiro de $\mathcal{O}_K$ tal que $I \mid \mathfrak{f}$ e $I \mid p\mathcal{O}_K$, então $\mathrm{N}(I) \mid \mathrm{N}(p\mathcal{O}_K) = |\mathrm{N}(p)| = p^n$ e $\mathrm{N}(I) \mid \mathrm{N}(\mathfrak{f})$, mas como $p \nmid \mathrm{N}(\mathfrak{f})$, segue que $\mathrm{N}(I) = 1$ e $I = \mathcal{O}_K$.

Dessa forma, $\mathcal{O}_K = \mathrm{mdc}(\mathfrak{f}, p\mathcal{O}_K) = \mathfrak{f} + p\mathcal{O}_K$. Portanto, se $a \in \mathcal{O}_K$, existem $b \in \mathfrak{f}$ e $c \in p\mathcal{O}_K$ tais que $a = b + c$. Isto é; $a \equiv b \pmod{p\mathcal{O}_K}$, mas como $b \in \mathfrak{f} \subseteq R$, segue que vale b). □

Demonstração do Teorema A.2. Provaremos que para todo $i \in \{1, \ldots, m\}$,

$$P_i = p\mathcal{O}_K + F_i(\alpha)\mathcal{O}_K$$

em que $F_i(X) \in \mathbb{Z}[X]$ é um polinômio qualquer tal que $\varphi(F_i) = f_i$.

Fixemos $i \in \{1, \ldots, m\}$. Seja k_i o seguinte corpo:

$$k_i \doteq \frac{(\mathbb{Z}/p\mathbb{Z})[X]}{\langle f_i(X)\rangle}$$

em que $\langle f_i(X)\rangle$ é outra notação para o ideal gerado por $f_i(X)$ em $(\mathbb{Z}/p\mathbb{Z})[X]$. Definimos $\varphi_i : (\mathbb{Z}/p\mathbb{Z})[X] \to k_i$ da seguinte forma:

$$\varphi_i\big(g(X)\big) = g(X) + \langle f_i(X)\rangle\,.$$

Então seja $\Phi_i \doteq \varphi_i \circ \varphi : \mathbb{Z}[X] \to k_i$, isto é, Φ_i é dada por

$$\Phi_i(c_k X^k + \cdots + c_0) = \overline{c_k}X^k + \overline{c_{k-1}}X^{k-1} + \cdots + \overline{c_0} + \langle f_i(X)\rangle\,.$$

Seja $I_i \doteq p\mathbb{Z}[X] + F_i(X)\mathbb{Z}[X]$. Provemos que $\ker\Phi_i = I_i$. É fácil ver que $I_i \subseteq \ker\Phi_i$ (pois $\varphi(F_i) = f_i$). Por outro lado, se $V \in \ker\Phi_i$, então $0 = \Phi_i(V) = \varphi_i(\varphi(V))$, logo $\varphi(V) \in \ker\varphi_i$ e assim $\varphi(V) = gf_i$ para algum $g \in (\mathbb{Z}/p\mathbb{Z})[X]$. Seja $G \in \mathbb{Z}[X]$ tal que $\varphi(G) = g$. Então definindo $H \doteq V - GF_i$, temos

$$\varphi(H) = \varphi(V) - \varphi(G)\varphi(F_i) = gf_i - gf_i = 0,$$

logo $H \in p\mathbb{Z}[X]$, e assim $V = H + F_iG \in I_i$. Portanto $I_i = \ker\Phi_i$, e o epimorfismo Φ_i induz um isomorfismo $\mathbb{Z}[X]/I_i \simeq k_i$.

Temos que $\langle f(X)\rangle \subseteq I_i$ pois $\varphi(f) = f_1^{a_1}\cdots f_m^{a_m} \in \ker\varphi_i$. Assim, podemos definir um epimorfismo

$$\begin{aligned} \frac{\mathbb{Z}[X]}{\langle f(X)\rangle} &\to \frac{\mathbb{Z}[X]}{I_i} \\ g(X) + \langle f(X)\rangle &\mapsto g(X) + I_i. \end{aligned} \tag{A.1}$$

Agora como $\mathbb{Z}[X]/\langle f(X)\rangle \simeq \mathbb{Z}[\alpha]$ e $\mathbb{Z}[X]/I_i \simeq k_i$, a aplicação dada por (A.1) induz um epimorfismo $\psi_i : \mathbb{Z}[\alpha] \to k_i$. De fato, ψ_i é dado por

$$\psi_i(c_1\alpha^{n-1} + c_2\alpha^{n-2} + \cdots + c_n) = \overline{c_1}X^{n-1} + \cdots + \overline{c_n} + \langle f_i(X)\rangle\,.$$

Assim,

$$\ker\psi_i = \{V(\alpha) \,:\, V(X) \in I_i\} = p\mathbb{Z}[\alpha] + F_i(\alpha)\mathbb{Z}[\alpha].$$

Definimos agora $\Psi_i : \mathcal{O}_K \to k_i$ da seguinte forma: dado $b \in \mathcal{O}_K$, podemos escolher $V(X) \in \mathbb{Z}[X]$ tal que $b \equiv V(\alpha) \pmod{p\mathcal{O}_K}$ (o que é possível por b) do Lema A.3) e assim definimos

$$\Psi_i(b) = \psi_i\big(V(\alpha)\big).$$

A aplicação Ψ_i está bem definida pois se $V(\alpha) \equiv 0 \pmod{p\mathcal{O}_K}$, então $V(\alpha) \in p\mathcal{O}_K \cap \mathbb{Z}[\alpha] = p\mathbb{Z}[\alpha]$, por a) do Lema A.3, e assim $V(\alpha) \in \ker\psi_i$.

Como ψ_i é sobrejetora, temos que Ψ_i também o é. Definimos $P_i \doteq \ker\Psi_i$. Temos então $\mathcal{O}_K/P_i \simeq k_i$ corpo, de modo que P_i é um ideal maximal de $\mathcal{O}_K$, e portanto P_i é um ideal primo de $\mathcal{O}_K$. Além

disso,

$$\begin{aligned} P_i &= \left\{ b \in \mathcal{O}_K \,:\, b \equiv V(\alpha) \pmod{p\mathcal{O}_K},\, V(\alpha) \in \ker \psi_i = p\mathbb{Z}[\alpha] + F_i(\alpha)\mathbb{Z}[\alpha] \right\} \\ &= p\mathcal{O}_K + p\mathbb{Z}[\alpha] + F_i(\alpha)\mathbb{Z}[\alpha] = p\mathcal{O}_K + F_i(\alpha)\mathbb{Z}[\alpha], \end{aligned}$$

sendo que vale a última igualdade pois $p\mathbb{Z}[\alpha] \subseteq p\mathcal{O}_K$. Além disso, por b) do Lema A.3, temos em particular que $\mathcal{O}_K = \mathbb{Z}[\alpha] + p\mathcal{O}_K$. Assim,

$$\begin{aligned} F_i(\alpha)\mathcal{O}_K &= F_i(\alpha)\big(\mathbb{Z}[\alpha] + p\mathcal{O}_K\big) = F_i(\alpha)\mathbb{Z}[\alpha] + F_i(\alpha)p\mathcal{O}_K \\ &\subseteq F_i(\alpha)\mathbb{Z}[\alpha] + p\mathcal{O}_K \end{aligned}$$

de modo que

$$p\mathcal{O}_K + F_i(\alpha)\mathcal{O}_K \subseteq p\mathcal{O}_K + F_i(\alpha)\mathbb{Z}[\alpha] \subseteq p\mathcal{O}_K + F_i(\alpha)\mathcal{O}_K$$

isto é;

$$P_i = p\mathcal{O}_K + F_i(\alpha)\mathbb{Z}[\alpha] = p\mathcal{O}_K + F_i(\alpha)\mathcal{O}_K.$$

Provemos que $P_1, \ldots, P_m$ são distintos. Suponhamos que existam $i, j \in \{1, \ldots, m\}$ distintos tais que $P_i = P_j$. Então como $\mathrm{mdc}(f_i, f_j) = 1$ existem $g, h \in (\mathbb{Z}/p\mathbb{Z})[X]$ tais que $gf_i + hf_j = \overline{1}$. Assim, tomando $G, H \in \mathbb{Z}[X]$ tais que $\varphi(G) = g$ e $\varphi(H) = h$, temos

$$\varphi(GF_i + HF_j - 1) = gf_i + hf_j - \overline{1} = 0.$$

Portanto $L \doteq GF_i + HF_j - 1 \in p\mathbb{Z}[X]$, de modo que

$$GF_i + HF_j - L = 1.$$

Calculando em α, temos

$$1 = G(\alpha)F_i(\alpha) + H(\alpha)F_j(\alpha) - L(\alpha) \in P_i$$

pois $F_i(\alpha) \in P_i$, $F_j(\alpha) \in P_j = P_i$ e $L(\alpha) \in p\mathbb{Z}[\alpha] \subseteq p\mathcal{O}_K \subseteq P_i$. Logo $1 \in P_i$ e $P_i = \mathcal{O}_K$ absurdo, pois então $k_i \simeq \mathcal{O}_K/P_i = (1)$, mas k_i possui mais do que um único elemento. Portanto $P_1, \ldots, P_m$ são todos distintos.

Notemos que $F_1(\alpha)^{a_1} \cdots F_m(\alpha)^{a_m} \in p\mathcal{O}_K$. De fato,

$$\varphi(F_1^{a_1} \cdots F_m^{a_m}) = f_1^{a_1} \cdots f_m^{a_m} = \varphi(f),$$

logo $G \doteq F_1^{a_1} \cdots F_m^{a_m} - f \in \ker \varphi = p\mathbb{Z}[X]$ e assim

$$F_1(\alpha)^{a_1} \cdots F_m(\alpha)^{a_m} = G(\alpha) + f(\alpha) = G(\alpha) + 0 = G(\alpha) \in p\mathbb{Z}[\alpha] \subseteq p\mathcal{O}_K.$$

Seja então P um ideal primo que divide $p\mathcal{O}_K$. Temos $F_1(\alpha)^{a_1} \cdots F_m(\alpha)^{a_m} \in p\mathcal{O}_K \subseteq P$ de modo que, como P é primo, existe $i \in \{1, \ldots, m\}$ tal que $F_i(\alpha) \in P$. Como também $p \in P$, segue que $P_i \subseteq P$, logo $P = P_i$. Isto é, provamos que os únicos divisores primos do ideal $p\mathcal{O}_K$ são os ideais $P_1, \ldots, P_m$, de modo que existem $e_1, \ldots, e_m \geq 0$ tais que $p\mathcal{O}_K = P_1^{e_1} \cdots P_m^{e_m}$.

Como vimos, $\mathcal{O}_K/P_i \simeq k_i$, logo

$$\mathrm{N}(P_i) = \left| \frac{\mathcal{O}_K}{P_i} \right| = k_i = \left| \frac{(\mathbb{Z}/p\mathbb{Z})[X]}{\langle f_i(X) \rangle} \right| = p^{n_i}$$

para todo $i \in \{1, \ldots, m\}$. Resta provar que $e_i = a_i$ para todo $i \in \{1, \ldots, m\}$. Agora como $F_1(\alpha)^{a_1} \cdots F_m(\alpha)^{a_m} \in p\mathcal{O}_K$, temos $F_1(\alpha)^{a_1} \cdots F_m(\alpha)^{a_m}\mathcal{O}_K \subseteq p\mathcal{O}_K$, logo

$$P_1^{e_1} \cdots P_m^{e_m} = p\mathcal{O}_K \mid \big(F_1(\alpha)\mathcal{O}_K\big)^{a_1}\big(F_2(\alpha)\mathcal{O}_K\big)^{a_2} \cdots \big(F_m(\alpha)\mathcal{O}_K\big)^{a_m}.$$

Lembrando que $P_1, \ldots, P_m$ são distintos, temos que cada P_i só pode dividir o fator $F_i(\alpha)\mathcal{O}_K$ do produto $(F_1(\alpha)\mathcal{O}_K)^{a_1} \cdots (F_m(\alpha)\mathcal{O}_K)^{a_m}$ (pois se tivéssemos $j \neq i$ tal que $P_i \mid F_j(\alpha)\mathcal{O}_K$, então $F_j(\alpha) \in P_i$, e assim $P_j = P_i$). Fixemos $i \in \{1, \ldots, m\}$. Temos $P_i^{e_i} \mid F_i(\alpha)^{a_i}\mathcal{O}_K$ logo $F_i(\alpha)^{a_i}\mathcal{O}_K \subseteq P_i^{e_i}$, e como também $p\mathcal{O}_K \subseteq P_i^{e_i}$ (pois $P_i^{e_i} \mid p\mathcal{O}_K$), temos $p\mathcal{O}_K + F_i(\alpha)^{a_i}\mathcal{O}_K \subseteq P_i^{e_i}$. Portanto

$$\begin{aligned} P_i^{a_i} &= \left(p\mathcal{O}_K + F_i(\alpha)\mathcal{O}_K\right)^{a_i} = \operatorname{mdc}\left(p\mathcal{O}_K, F_i(\alpha)\mathcal{O}_K\right)^{a_i} \\ &= \operatorname{mdc}\left(p^{a_i}\mathcal{O}_K, F_i(\alpha)^{a_i}\mathcal{O}_K\right) = p^{a_i}\mathcal{O}_K + F_i(\alpha)^{a_i}\mathcal{O}_K \\ &\subseteq p\mathcal{O}_K + F_i(\alpha)^{a_i}\mathcal{O}_K \subseteq P_i^{e_i} \end{aligned}$$

de modo que $e_i \leq a_i$.

Por outro lado,

$$\begin{aligned} p^n &= |\operatorname{N}(p)| = \operatorname{N}(p\mathcal{O}_K) = \operatorname{N}(P_1^{e_1} \cdots P_m^{e_m}) = \operatorname{N}(P_1)^{e_1} \cdots \operatorname{N}(P_m)^{e_m} \\ &= p^{n_1 e_1} \cdots p^{n_m e_m} = p^{n_1 e_1 + \cdots + n_m e_m} \end{aligned}$$

logo $n = n_1 e_1 + \cdots + n_m e_m$. Além disso,

$$\begin{aligned} n &= \operatorname{gr}\varphi(f) = \operatorname{gr}(f_1^{a_1} \cdots f_m^{a_m}) = a_1 \operatorname{gr} f_1 + \cdots + a_m \operatorname{gr} f_m \\ &= a_1 n_1 + \cdots + a_m n_m \geq e_1 n_1 + \cdots + e_m n_m = n, \end{aligned}$$

isto é;

$$n = a_1 n_1 + a_2 n_2 + \cdots + a_m n_m = e_1 n_1 + e_2 n_2 + \cdots + e_m n_m$$

com $e_1 \leq a_1$, …, $e_m \leq a_m$, mas isso só é possível se $e_1 = a_1$, $e_2 = a_2$, …, $e_m = a_m$. □

Apêndice B

Teoremas Abelianos

Neste Apêndice, vamos demonstrar alguns teoremas de tipo abeliano, mais especificamente de regularidade de métodos de somabilidade, como visto em [Har92].

Esses teoremas são importantes para a teoria não só porque usamos um teorema abeliano na demonstração do Teorema dos Números Primos (Capítulo 4, Teorema 4.5) como também é possível que um teorema desse tipo possa resolver o problema da inversão do limite com a série de (5.30).

B.1 Introdução

Em termos gerais, um *teorema abeliano* é um teorema segundo o qual uma certa "regularidade" de uma sequência (ou função) implica uma "regularidade" de uma *média* dessa sequência (função). Um exemplo de teorema abeliano bem simples é o seguinte:

Proposição B.1. *Seja $(s_n)_n$ uma sequência de números complexos. Se $s_n \to s$, então a sequência $(\sigma_m)_m$ dada por*

$$\sigma_m \doteq \frac{s_0 + s_1 + \cdots + s_m}{m+1} \qquad \text{para todo } m \geq 0$$

também converge para o mesmo limite s.

Na Proposição B.1, a sequência $(\sigma_m)_m$ é vista como uma "média" da sequência $(s_n)_n$ (pois σ_m é a média aritmética dos $m+1$ primeiros termos da sequência $(s_n)_n$). A convergência da sequência $(s_n)_n$ é vista como uma "regularidade" dessa sequência, e a partir dela obtemos uma "regularidade" da sua "média" $(\sigma_m)_m$, a saber, a convergência dessa sequência de médias para o mesmo limite.

A denominação "teorema abeliano" vem do seguinte teorema de Abel sobre séries de potências:

Proposição B.2 (Abel)**.** *Se a série de números complexos $\sum_{n=0}^{+\infty} a_n$ é convergente, então a série de potências $\sum_{n=0}^{+\infty} a_n x^n$ tem raio de convergência maior ou igual a 1, e vale*

$$\lim_{x \to 1^-} \sum_{n=0}^{+\infty} a_n x^n = \sum_{n=0}^{+\infty} a_n. \tag{B.1}$$

Essa Proposição também é um exemplo da relação entre teoremas abelianos e teoremas de inversão de limite com séries, pois podemos escrever a equação (B.1) como uma inversão de um limite com uma série:

$$\lim_{x \to 1^-} \sum_{n=0}^{+\infty} a_n x^n = \sum_{n=0}^{+\infty} \lim_{x \to 1^-} a_n x^n.$$

Faremos as demonstrações das Proposições B.1 e B.2 mais adiante, como consequências de teoremas abelianos mais gerais.

B.2 Métodos de somabilidade

Usualmente, uma sequência de números complexos $(a_n)_n$ é dita *somável* se a sequência das suas somas parciais $s_n \doteq a_0 + a_1 + \cdots + a_n$ para $n \geq 0$ é convergente. Por exemplo, $(1/n^2)_n$ é somável, mas $((-1)^n)_n$ não é somável. Dizemos então que a série $\sum_{n=0}^{+\infty}(-1)^n$ é *divergente*. Podemos desenvolver métodos para dar algum valor a esse tipo de série. Para isso, estendemos o conceito de convergência de sequências, e usamos essa extensão de convergência para a sequência de somas parciais $(s_n)_n$.

Vejamos um exemplo: seja $s_n \doteq a_0 + a_1 + \cdots + a_n$, $n \geq 0$, a sequência das somas parciais de uma sequência de números complexos $(a_n)_n$. Definimos o método de Cesàro (C) da seguinte forma: seja $(\sigma_m)_m$ a sequência dada pela média aritmética dessas somas parciais:

$$\sigma_m \doteq \frac{s_0 + s_1 + \cdots + s_m}{m+1} \qquad \text{para todo } m \geq 0.$$

Diremos que a sequência $(s_n)_n$ converge (C) para s quando $\sigma_m \to s$. Nesse caso, dizemos que a série $\sum_{n=0}^{+\infty} a_n$ é *somável* (C) com valor s, e escrevemos

$$s_m \to s \ \ (C), \qquad \text{e também} \qquad \sum_{n=0}^{+\infty} a_n = s \ \ (C).$$

Para o caso da sequência $((-1)^n)_n$, temos que as suas somas parciais são

$$s_n = \begin{cases} 1, & \text{se } n \text{ é par} \\ 0, & \text{se } n \text{ é ímpar} \end{cases}$$

para todo $n \geq 0$. Logo

$$\sigma_m \doteq \frac{s_0 + \cdots + s_m}{m+1} = \begin{cases} 1/2, & \text{se } m \text{ é ímpar} \\ (m+2)/(2m+2) & \text{se } m \text{ é par} \end{cases}$$

para todo $m \geq 0$. Portanto $\sigma_m \to 1/2$ e assim dizemos que

$$s_m \to \frac{1}{2} \ \ (C), \qquad \text{e que} \qquad \sum_{n=0}^{+\infty}(-1)^n = \frac{1}{2} \ \ (C).$$

Note que os σ_m do caso anterior têm a seguinte forma:

$$\sigma_m = \frac{1}{m+1}s_0 + \frac{1}{m+1}s_1 + \cdots + \frac{1}{m+1}s_m.$$

Por esse e outros exemplos é natural considerar, mais geralmente, transformações T que levam uma sequência $(s_n)_n$ em outra sequência $(t_m)_m$ dada por

$$t_m = \sum_{n=0}^{\infty} c_{m,n}s_n, \quad \text{para todo } m \geq 0 \tag{B.2}$$

para certos $c_{m,n}$, $m, n \geq 0$, números complexos fixados. Por enquanto consideraremos apenas transformações da forma (B.2).

A partir de uma transformação T como acima, obtemos um método de somabilidade (T) da seguinte forma: dizemos que uma sequência $(s_n)_n$ converge (T) para s quando $t_m \to s$, ou seja

$$s_m \to s \ \ (T) \qquad \text{se, e somente se} \qquad t_m \to s,$$

em que $(t_m)_m$ é dada por (B.2). Suponhamos agora que $(s_n)_n$ é a sequência de somas parciais da

sequência $(a_n)_n$. Se $s_n \to s\ (T)$ então também dizemos que a série $\sum_{n=0}^{+\infty} a_n$ é somável (T) com valor s, e escrevemos

$$\sum_{n=0}^{+\infty} a_n = s\ (T).$$

B.3 Regularidade

Como queremos *estender* o conceito de somabilidade (ou de limite de uma sequência), é importante saber quais transformações T da forma de (B.2) mantêm a convergência usual intacta. Isto é; quando

$$s_n \to s \quad \text{implica} \quad s_n \to s\ (T)$$

para qualquer sequência $(s_n)_n$ de números complexos.

Definição. Dizemos que o método (T) é *regular* se para toda sequência $(s_n)_n$ convergente, o valor t_m de (B.2) está bem definido para todo $m \geq 0$ (a série que define t_m é convergente), e vale

$$\lim s_n = \lim t_m.$$

Um teorema da forma "T é regular" pode ser considerado um teorema abeliano, pois sempre que $s_n \to s$ temos que a "média" $(t_m)_m$ da sequência $(s_n)_n$ converge para o mesmo limite. Por exemplo, a Proposição B.1 simplesmente diz que o método (C) é regular.

Seja $\mathcal{I}_r$ a classe das transformações da forma de (B.2) que são regulares. Seja também $\mathcal{I}_c$ a classe das transformações da mesma forma que levam sequências convergentes em sequências convergentes. Isto é; $T \in \mathcal{I}_c$ se, para toda sequência $(s_n)_n$ convergente, t_m está bem definido para todo $m \geq 0$ e a sequência $(t_m)_m$ é convergente (sendo que é possível ocorrer $\lim t_m \neq \lim s_n$). Temos então $\mathcal{I}_r \subseteq \mathcal{I}_c$. Nessa situação, vale o seguinte Teorema:

Teorema B.3. *T pertence a $\mathcal{I}_c$ se, e somente se*

1. *existe $H < \infty$ tal que $\gamma_m \doteq \sum_{n=0}^{+\infty} |c_{m,n}| < H$ para todo $m \geq 0$;*
2. *para todo $k \geq 0$ existe δ_k tal que $c_{m,k} \to \delta_k$ quando $m \to +\infty$; e*
3. *existe δ tal que $c_m \doteq \sum_{n=0}^{+\infty} c_{m,n} \to \delta$ quando $m \to +\infty$.*

Nesse caso $\sum_{n=0}^{+\infty} \delta_n$ converge absolutamente e, se $s_n \to s$, vale

$$t_m \to t = \delta s + \sum_{n=0}^{+\infty} \delta_n (s_n - s) = s\left(\delta - \sum_{n=0}^{+\infty} \delta_n\right) + \sum_{n=0}^{+\infty} \delta_n s_n. \tag{B.3}$$

Se

$$\delta_{ij} \doteq \begin{cases} 1, & \text{se } i = j \\ 0, & \text{se } i \neq j \end{cases}$$

vemos que, no Teorema B.3, as condições 2 e 3 são respectivamente equivalentes a

2'. para cada k, tem-se $\delta_{nk} \to \delta_k\ (T)$ (com $n \to \infty$); e

3'. $s_n \equiv 1 \to \delta\ (T)$.

Ou seja, as condições do Teorema B.3 são simplesmente uma limitação uniforme dos coeficientes $c_{m,n}$, mais o fato de o método (T) funcionar para algumas sequências simples.

Demonstração do Teorema B.3. Provemos que as condições são suficientes. Suponhamos que $s_n \to s$. Então $(s_n)_n$ é limitada, e existe $M > 0$ tal que $|s_n| < M$ para todo $n \geq 0$. Da condição 1 do Teorema temos que

$$\sum_n |c_{m,n} s_n| \leq \sum_n |c_{m,n}| M \leq H \cdot M < \infty.$$

Portanto a série $t_m = \sum_n c_{m,n} s_n$ converge absolutamente para todo $m \geq 0$ sempre que $(s_n)_n$ é convergente (de fato, sempre que $(s_n)_n$ é limitada).

As séries em (B.3) também são absolutamente convergentes, pois das condições 2 e 1 temos

$$\sum_{n=0}^{N} |\delta_n| = \sum_{n=0}^{N} \lim_{m \to +\infty} |c_{m,n}| = \lim_{m \to +\infty} \sum_{n=0}^{N} |c_{m,n}| \leq H,$$

logo $\sum_{n=0}^{+\infty} |\delta_n| \leq H$. Além disso, como no caso da convergência absoluta dos t_m, as outras séries de (B.3) convergem absolutamente (são somas de um produto de duas sequências, em que uma sequência tem soma absolutamente convergente, e a outra é limitada).

Provemos agora que vale a equação (B.3) se $s = 0$. Ou seja, provemos que $t_m \to \sum_{n=0}^{+\infty} \delta_n s_n$ se $s_n \to 0$. Fixemos $\varepsilon > 0$. Temos

$$\left| t_m - \sum_{n=0}^{+\infty} \delta_n s_n \right| \leq \sum_{n=0}^{+\infty} |c_{m,n} - \delta_n| |s_n|. \tag{B.4}$$

Como $s_n \to 0$ existe $N_0 > 0$ tal que $|s_n| < \varepsilon$ para todo $n \geq N_0$. Além disso, $|s_n| < M$ para todo $n \geq 0$. Assim separamos a série de (B.4) em duas partes, uma para $n \geq N_0$ em que podemos usar $|s_n| < \varepsilon$, e outra para $n < N_0$ em que usamos $|s_n| < M$, obtemos

$$\begin{aligned} \left| t_m - \sum_{n=0}^{+\infty} \delta_n s_n \right| &\leq M \sum_{n=0}^{N_0 - 1} |c_{m,n} - \delta_n| + \varepsilon \sum_{n=0}^{+\infty} (|c_{m,n}| + |\delta_n|) \\ &\leq M \sum_{n=0}^{N_0 - 1} |c_{m,n} - \delta_n| + \varepsilon K, \end{aligned} \tag{B.5}$$

em que $K \doteq H + \sum_{n=0}^{+\infty} |\delta_n| < \infty$. Como também $c_{m,n} \to \delta_n$ quando $m \to +\infty$ para todo $n \geq 0$, segue de (B.5) que de fato $t_m \to \sum_{n=0}^{+\infty} \delta_n s_n$.

Se agora $s_n \to s \neq 0$, definimos $s'_n \doteq s_n - s$ para $n \geq 0$, de modo que $s'_n \to 0$. Seja $t'_m \doteq \sum_{n=0}^{+\infty} c_{m,n} s'_n$ para todo $m \geq 0$. Do caso anterior temos $t'_m \to \sum_{n=0}^{+\infty} \delta_n s'_n$. Assim vemos que

$$t'_m = \sum_{n=0}^{+\infty} c_{m,n} s'_n = t_m - s \sum_{n=0}^{+\infty} c_{m,n}.$$

Dessa forma, usando a condição 3 do Teorema temos

$$t_m = t'_m + s \sum_{n=0}^{+\infty} c_{m,n} \to \sum_{n=0}^{+\infty} \delta_n s'_n + s\delta = \sum_{n=0}^{+\infty} \delta_n (s_n - s) + s\delta$$

quando $m \to +\infty$, como queríamos demonstrar.

Provemos que as condições são necessárias. Supomos $T \in \mathcal{I}_c$.

Fixemos $k \geq 0$ e seja $s_n = \delta_{nk}$ para $n \geq 0$. Temos $s_n \to 0$, de modo que por hipótese temos $t_m = \sum_{n=0}^{+\infty} c_{m,n} s_n = c_{m,k}$ convergente, e $\delta_k \doteq \lim_{m \to +\infty} t_m = \lim_{m \to +\infty} c_{m,k}$. Dessa forma, a condição 2 do Teorema é necessária. Analogamente prova-se que a condição 3 é necessária, tomando $s_n = 1$ para todo $n \geq 0$.

Resta provar que a condição 1 é necessária.

Provemos primeiramente que $\sum_{n=0}^{+\infty} |c_{m,n}|$ converge para cada $m \geq 0$. Suponha por absurdo que

exista $m \geq 0$ tal que $\sum_{n=0}^{+\infty} |c_{m,n}| = \infty$. Vamos criar uma sequência convergente s_n tal que $t_m = \infty$, o que é um absurdo pois, por hipótese, $T \in \mathcal{I}_c$ e assim t_m deve ser finito para todo m sempre que s_n é convergente.

Seja $N \geq 0$ o menor inteiro tal que $c_{m,N} \neq 0$, e defina

$$\varepsilon_n \doteq \begin{cases} 1, & \text{se } n < N \\ 1/\left(\sum_{\nu=N}^{n} |c_{m,\nu}|\right), & \text{se } n \geq N. \end{cases}$$

Então $\varepsilon_n \to 0$ pois $\sum_{\nu=0}^{+\infty} |c_{m,\nu}| = \infty$. Assim, se $s_n = \varepsilon_n \operatorname{sgn} \overline{c_{m,n}}$,[1] temos $s_n \to 0$.

Agora se $N_1 > N_0 > N$ temos

$$\sum_{n=N_0}^{N_1} \varepsilon_n |c_{m,n}| = \sum_{n=N_0}^{N_1} \frac{|c_{m,n}|}{\sum_{\nu=N}^{n} |c_{m,\nu}|} \geq \sum_{n=N_0}^{N_1} \frac{|c_{m,n}|}{\sum_{\nu=N}^{N_1} |c_{m,\nu}|} \geq 1 - \frac{\sum_{n=N}^{N_0-1} |c_{m,n}|}{\sum_{\nu=N}^{N_1} |c_{m,\nu}|}.$$

Como $\sum_{\nu=0}^{+\infty} |c_{m,\nu}| = \infty$, fazendo $N_1 \to +\infty$ temos $\sum_{n=N_0}^{\infty} \varepsilon_n |c_{m,n}| \geq 1$. Assim, como $N_0 > N$ é arbitrário temos que $\sum_{n=N}^{\infty} \varepsilon_n |c_{m,n}|$ não pode convergir (pois então, para N_0' suficientemente grande, teríamos $\sum_{n=N_0'}^{\infty} \varepsilon_n |c_{m,n}| < 1/2$). Dessa forma,

$$t_m = \sum_{n=0}^{+\infty} \varepsilon_n \operatorname{sgn}(\overline{c_{m,n}}) \cdot c_{m,n} = \sum_{n=0}^{+\infty} \varepsilon_n |c_{m,n}| = \infty,$$

o que é um absurdo, como discutido anteriormente. Portanto para todo $m \geq 0$ vale $\sum_{n=0}^{+\infty} |c_{m,n}| < \infty$.

Resta provar que a sequência $\gamma_m \doteq \sum_{n=0}^{+\infty} |c_{m,n}|$, $m \geq 0$, é limitada. Suponhamos por absurdo que ela não seja limitada. Seja $d_n \doteq \sum_{\nu=0}^{n} |\delta_\nu|$.

Vamos construir duas sequências crescentes $m_1, m_2, \ldots,$ e $n_1, n_2, \ldots,$ começando de algum n_1 arbitrário. Supondo definidos $m_1, \ldots, m_{r-1}$ e $n_1, \ldots, n_r$, vamos construir m_r e n_{r+1}. Como γ_m não é limitada, existe $m_r > m_{r-1}$ tal que

$$\gamma_{m_r} > 2r d_{n_r} + r^2 + 2r + 2. \tag{B.6}$$

Como

$$\sum_{n=0}^{n_r} |c_{m,n}| \to \sum_{n=0}^{n_r} |\delta_n| = d_{n_r}, \qquad \text{quando } m \to +\infty,$$

podemos supor que m_r é grande o suficiente para termos também

$$\sum_{n=0}^{n_r} |c_{m_r,n}| < d_{n_r} + 1. \tag{B.7}$$

Seja então $n_{r+1} > n_r$ tal que

$$\sum_{n=n_{r+1}+1}^{\infty} |c_{m_r,n}| < 1. \tag{B.8}$$

[1] A função sinal $\operatorname{sgn} : \mathbb{C} \to \mathbb{C}$ é dada por

$$\operatorname{sgn} z \doteq \begin{cases} 0, & \text{se } z = 0 \\ \frac{z}{|z|}, & \text{se } z \neq 0. \end{cases}$$

Assim de (B.6), (B.7) e (B.8) temos

$$\sum_{n=n_r+1}^{n_{r+1}} |c_{m_r,n}| = \sum_{n=0}^{+\infty} |c_{m_r,n}| - \sum_{n=0}^{n_r} |c_{m_r,n}| - \sum_{n=n_{r+1}+1}^{\infty} |c_{m_r,n}|$$
$$> 2rd_{n_r} + r^2 + 2r + 2 - d_{n_r} - 1 - 1 > rd_{n_r} + r^2 + 2r. \tag{B.9}$$

Tomemos então

$$s_n \doteq \begin{cases} 0, & \text{se } n \leq n_1, \\ \frac{1}{r} \operatorname{sgn} \overline{c_{m_r,n}}, & \text{se } n_r < n \leq n_{r+1}. \end{cases}$$

para $n \geq 0$. Com essa sequência $(s_n)_n$ temos

$$|t_{m_r}| = \left| \sum_{n=0}^{n_r} c_{m_r,n} s_n + \sum_{n=n_r+1}^{n_{r+1}} |c_{m_r,n}| \frac{1}{r} + \sum_{n=n_{r+1}+1}^{\infty} c_{m_r,n} s_n \right|$$
$$\geq \frac{1}{r} \sum_{n=n_r+1}^{n_{r+1}} |c_{m_r,n}| - \left| \sum_{n=0}^{n_r} c_{m_r,n} s_n \right| - \left| \sum_{n=n_{r+1}+1}^{\infty} c_{m_r,n} s_n \right|$$
$$\geq \frac{1}{r} \sum_{n=n_r+1}^{n_{r+1}} |c_{m_r,n}| - \sum_{n=0}^{n_r} |c_{m_r,n}||s_n| - \sum_{n=n_{r+1}+1}^{\infty} |c_{m_r,n}||s_n|$$

para todo $r \geq 1$. Assim, usando $|s_n| < 1$ para todo $n \geq 0$ e (B.7), (B.8) e (B.9), temos

$$|t_{m_r}| \geq \frac{1}{r}(rd_{n_r} + r^2 + 2r) - (d_{n_r} + 1) - 1 = r.$$

Logo $(t_{m_r})_r$ não converge. Mas então $(t_m)_m$ não é convergente, absurdo pois $s_n \to 0$ e $T \in \mathcal{I}_c$. □

Do Teorema B.3 obtemos um resultado para transformações regulares:

Teorema B.4 (Schur-Toeplitz)**.** *T é regular se, e somente se*

1. *existe $H < \infty$ tal que $\gamma_m \doteq \sum_{n=0}^{+\infty} |c_{m,n}| < H$ para todo m;*
2. *para todo $k \geq 0$ tem-se $c_{m,k} \to 0$ quando $m \to +\infty$; e*
3. *$c_m \doteq \sum_{n=0}^{+\infty} c_{m,n} \to 1$ quando $m \to +\infty$.*

Demonstração. Basta usar o Teorema B.3, substituindo em (B.3) os valores $\delta_k = 0$ para todo $k \geq 0$ e $\delta = 1$. □

Agora é fácil demonstrar a Proposição B.1. Vamos reenunciá-la da seguinte forma:

Proposição B.5. *O método (C) é regular.*

Demonstração. Nos termos do Teorema B.4, a transformação que define o método (C) é aquela com

$$c_{m,n} = \begin{cases} 1/(m+1), & \text{se } n \leq m \\ 0, & \text{se } n > m. \end{cases}$$

Dessa forma $\gamma_m = \sum_{n=0}^{m} 1/(m+1) = 1$ para todo $m \geq 0$. Temos $c_{m,k} \to 0$ quando $m \to +\infty$ e $c_m \equiv 1$. Assim, pelo Teorema B.4 o método (C) é regular. □

Temos também a seguinte variação do Teorema B.4:

Teorema B.6. *Para que $s_n \to 0$ sempre implique t_m estar bem definido para todo $m \geq 0$ e com $t_m \to 0$, é necessário e suficiente que valham*

1. *existe* $H < \infty$ *tal que* $\gamma_m = \sum_{n=0}^{+\infty} |c_{m,n}| < H$ *para todo* m*; e*
2. *para cada* $n \geq 0$ *tem-se* $c_{m,n} \to 0$ *quando* $m \to +\infty$*.*

Demonstração. Basta seguir os mesmos argumentos utilizados na demonstração do Teorema B.3. □

Um resultado interessante que segue de B.3 é o seguinte:

Teorema B.7. *A série* $\sum_{n=0}^{+\infty} \chi_n a_n$ *é convergente sempre que* $\sum_{n=0}^{+\infty} a_n$ *é convergente se, e somente se*

$$\sum_{n=0}^{+\infty} |\Delta\chi_n| \doteq \sum_{n=0}^{+\infty} |\chi_n - \chi_{n+1}| < \infty. \tag{B.10}$$

Demonstração. Seja t_m a m-ésima soma parcial da série $\sum_{n=0}^{+\infty} \chi_n a_n$ para todo $m \geq 0$, isto é; $t_m = \sum_{n=0}^{m} \chi_n a_n$ para todo $m \geq 0$. Seja $(s_n)_n$ a sequência de somas parciais de $(a_n)_n$. Substituindo $a_n = s_n - s_{n-1}$ para $n \geq 1$ na definição de t_m obtemos

$$\begin{aligned} t_m &= \sum_{n=1}^{m} \chi_n s_n - \sum_{n=1}^{m} \chi_n s_{n-1} + \chi_0 s_0 = \sum_{n=0}^{m-1} (\chi_n - \chi_{n+1}) s_n + \chi_m s_m \\ &= \sum_{n=0}^{m-1} \Delta\chi_n s_n + \chi_m s_m = \sum_{n=0}^{+\infty} c_{m,n} s_n \end{aligned}$$

para todo $n \geq 0$, em que

$$c_{m,n} \doteq \begin{cases} \Delta\chi_n, & \text{se } 0 \leq n \leq m-1 \\ \chi_m, & \text{se } n = m \\ 0, & \text{se } n > m. \end{cases}$$

Assim temos uma transformação $t_m = \sum_{n=0}^{+\infty} c_{m,n} s_n$, $m \geq 0$, e podemos usar o Teorema B.3 para avaliar a convergência de $(t_m)_m$. Nos termos desse Teorema temos

$$\gamma_m = \sum_{n=0}^{m-1} |\Delta\chi_n| + |\chi_m| \quad \text{e} \quad c_m = \sum_{n=0}^{m-1} \Delta\chi_n + \chi_m = \chi_0.$$

Suponhamos que $\sum_{n=0}^{+\infty} \chi_n a_n$ seja convergente sempre que $\sum_{n=0}^{+\infty} a_n$ é convergente (ou seja, sempre que $(s_n)_n$ é convergente). Então a transformação definida por $t_m = \sum_{n=0}^{+\infty} c_{m,n} s_n$, $m \geq 0$, pertence a $\mathcal{I}_c$ por definição e assim, pelo Teorema B.3, existe $H > 0$ tal que $\gamma_m < H$ para todo $m \geq 0$. Portanto

$$\sum_{n=0}^{m} |\Delta\chi_n| \leq \gamma_{m+1} < H,$$

e fazendo $m \to +\infty$ temos (B.10).

Por outro lado, se temos (B.10) então $\sum_{n=0}^{+\infty} (\chi_n - \chi_{n+1})$ é convergente, de modo que $(\chi_n)_n$ é convergente. Isso ocorre pois, se $M > N$ temos

$$\left| \sum_{n=0}^{M} (\chi_n - \chi_{n+1}) - \sum_{n=0}^{N} (\chi_n - \chi_{n+1}) \right| = |\chi_{N+1} - \chi_{M+1}|.$$

Assim, as somas parciais de $\sum_{n=0}^{+\infty} (\chi_n - \chi_{n+1})$ formam uma sequência de Cauchy se, e somente se $(\chi_n)_n$ é uma sequência de Cauchy. Em particular, existe $M < \infty$ tal que $|\chi_n| < M$ para todo $n \geq 0$ e assim

$$\gamma_m = \sum_{n=0}^{m-1} |\Delta\chi_n| + |\chi_m| \leq M + \sum_{n=0}^{+\infty} |\Delta\chi_n| < \infty,$$

de modo que a transformação $t_m = \sum_{n=0}^{+\infty} c_{m,n} s_n$ satisfaz a condição 1 do Teorema B.3. Como $c_{m,k} \to \Delta\chi_k$ e $c_m = \chi_0$ para todo $m \geq 0$, t_m também satisfaz as condições 2 e 3 do Teorema B.3. Portanto $(t_m)_m$ é convergente sempre que $(s_n)_n$ é convergente, ou seja, $\sum_{n=0}^{+\infty} \chi_n a_n$ é convergente sempre que $\sum_{n=0}^{+\infty} a_n$ é convergente. □

B.4 Outro tipo de transformação

Vamos agora considerar um outro tipo de transformação T, dada por

$$t(x) = \sum_{n=0}^{+\infty} c_n(x) s_n, \tag{B.11}$$

para $x \geq 0$ real. Nesse caso, essa tranformação induz um método (T) de somabilidade da seguinte forma: $s_n \to s$ (T) se, e somente se $t(x) \to s$ quando $x \to +\infty$. Diremos, de modo análogo ao caso anterior, que T é *regular* quando $s_n \to s$ implica que $t(x)$ está definida para todo $x \geq 0$, e que $t(x) \to s$ quando $x \to +\infty$. Para esse tipo de transformação, temos um resultado como o Teorema B.4 e que de fato é um corolário dele:

Teorema B.8. *Se T é dada como em* (B.11)*, temos que T é regular se, e somente se*

1. $\sum_{n=0}^{+\infty} |c_n(x)| < \infty$ *para todo* $x \geq 0$*, e existem* $H < \infty$ *e* $x_0 \geq 0$ *tais que para* $x \geq x_0$*, vale* $\gamma(x) \doteq \sum_{n=0}^{+\infty} |c_n(x)| < H$*;*
2. *para todo* $n \geq 0$ *tem-se* $c_n(x) \to 0$ *quando* $x \to +\infty$*; e*
3. $c(x) \doteq \sum_{n=0}^{+\infty} c_n(x) \to 1$ *quando* $x \to +\infty$*;*

Demonstração. Suponhamos que T satisfaz as condições 1, 2 e 3. Seja $(x_m)_m$ uma sequência de números reais não-negativos tal que $x_m \to +\infty$. Definindo $c_{m,n} = c_n(x_m)$ para $m, n \geq 0$, temos

$$t_m \doteq \sum_{n=0}^{+\infty} c_{m,n} s_n \doteq \sum_{n=0}^{+\infty} c_n(x_m) s_n = t(x_m)$$

para $m \geq 0$, o que define uma transformação da forma de (B.2) que satisfaz as condições Teorema B.4. Segue então desse Teorema que, se $s_n \to s$, temos $t_m = t(x_m)$ bem definido para todo $m \geq 0$, com $t(x_m) \to s$. Como $x_m \to +\infty$ é uma sequência arbitrária, temos que $t(x) \to s$ e que $t(x)$ está bem definido para todo $x \geq 0$.

Provemos que as condições do Teorema são necessárias. Tomando novamente uma sequência $x_m \to +\infty$ de números reais não negativos, temos que $t_m = t(x_m)$ define uma transformação regular como anteriormente, e assim pelo Teorema B.4 tem-se $c_n(x_m) \to 0$ para todo $n \geq 0$ fixo, e $\sum_{n=0}^{+\infty} c_n(x_m) \to 1$ quando $m \to +\infty$. Como $x_m \to +\infty$ é arbitrária, temos então que T satisfaz as condições 2 e 3 do Teorema B.8.

Quando à condição 1: se $x \geq 0$, tomando $x_m \doteq x + m$, temos novamente uma transformação regular dada por $t_m = t(x_m)$, logo pela condição 1 do Teorema B.4, temos $\sum_{n=0}^{+\infty} |c_n(x)| = \sum_{n=0}^{+\infty} |c_n(x_0)| < \infty$.

Se não existe $x_0 \geq 0$ tal que $\gamma(x) = \sum_{n=0}^{+\infty} |c_n(x)|$ é limitada para $x \geq x_0$, então existe $x_m \to +\infty$ tal que $\gamma(x_m) \to +\infty$. Absurdo, pois então $t_m = t(x_m)$ não satisfaz a condição 1 do Teorema B.4. □

Observação. Podemos alterar o Teorema B.8 de modo a fazermos $x \to 0^+$ ao invés de $x \to +\infty$, e obtemos outro teorema de demonstração análoga.

Vamos usar um análogo do Teorema B.6 para transformações da forma de (B.11), que decorre do Teorema B.6 assim como o Teorema B.8 decorre do Teorema B.4:

Teorema B.9. *Seja*

$$t(x) = \sum_{n=0}^{+\infty} c_n(x) s_n$$

com as funções c_n definidas em $(0,\, X]$. Para que $s_n \to 0$ implique que $t(x)$ está bem definido em $(0,\, X]$ e que $t(x) \to 0$ quando $x \to 0^+$, é necessário e suficiente que se tenha

1. *$\sum_{n=0}^{+\infty} |c_n(x)| < \infty$ para todo $x \in (0,\, X]$, e existem $X_0 > 0$ e $H < \infty$ tal que, se $0 < x \leq X_0$, então $\gamma(x) = \sum_{n=0}^{+\infty} |c_n(x)| < H$; e*

2. *para todo $n \geq 0$ tem-se $c_n(x) \to 0$ quando $x \to 0^+$.*

B.5 Um terceiro método

Definimos

$$\phi(x) = \sum_{n=0}^{+\infty} a_n \phi_n(x),$$

com $x \in (0,\, X]$, para algum $X > 0$. Se para alguma sequência $(a_n)_n$ fixada tem-se $\phi(x) \to s$ quando $x \to 0^+$, dizemos que $(a_n)_n$ é somável (ϕ) com soma s, e escrevemos $\sum_{n=0}^{+\infty} a_n = s\ (\phi)$. Dizemos que o método (ϕ) é *regular* se sempre que $\sum_{n=0}^{+\infty} a_n = s \in \mathbb{C}$ temos $\phi(x)$ bem definido para todo $x \in (0,\, X]$ e $\phi(x) \to s$ quando $x \to 0^+$. Nessas condições, temos o seguinte Teorema:

Teorema B.10. *Para que o método (ϕ) seja regular é necessário e suficiente que ocorram*

1. *para todo $n \geq 0$ vale $\phi_n(x) \to 1$ quando $x \to 0^+$; e*

2. *$\sum_{n=0}^{+\infty} |\phi_n(x) - \phi_{n+1}(x)| < \infty$ para todo $x \in (0,\, X]$ e existem $X_0 > 0$ e $H < \infty$ tais que $\sum_{n=0}^{+\infty} |\phi_n(x) - \phi_{n+1}(x)| < H$ para todo $x \in (0,\, X_0]$.*

Em particular, a condição 2 é satisfeita se vale

$$0 \leq \phi_{n+1}(x) \leq \phi_n(x), \qquad \text{para todos } x \in (0, X],\ n \geq 0. \tag{B.12}$$

Demonstração. Provemos que as condições são suficientes. Temos da condição 1 que existem H_1 e $\xi > 0$ tais que $|\phi_0(x)| \leq H_1$ para todo $x \in (0,\, \xi]$. Assim, da condição 2,

$$\begin{aligned} |\phi_n(x)| &= \left| \sum_{\nu=0}^{n-1} [\phi_{\nu+1}(x) - \phi_\nu(x)] + \phi_0(x) \right| \leq |\phi_0(x)| + \sum_{\nu=0}^{n-1} |\phi_{\nu+1}(x) - \phi_\nu(x)| \\ &\leq H + H_1 \doteq K \end{aligned}$$

para $x \in (0,\, \xi]$. (Podemos supor $\xi < X_0$.)

Suponhamos primeiramente que $s_n \to 0$, em que $(s_n)_n$ é a sequência de somas parciais de $(a_n)_n$. Podemos deixar a expressão de ϕ mais parecida com a transformação do Teorema B.9 substituindo $a_n = s_n - s_{n-1}$ para $n \geq 1$, pois então obtemos

$$\sum_{n=0}^{N} a_n \phi_n(x) = \sum_{n=0}^{N-1} s_n [\phi_n(x) - \phi_{n+1}(x)] + s_N \phi_N(x). \tag{B.13}$$

Como $|\phi_N(x)| \leq K$ para $x \in (0,\, \xi]$, temos nesse caso que

$$|s_N \phi_N(x)| \leq |s_N| K \to 0$$

quando $N \to +\infty$. Assim, fazendo $N \to +\infty$ em (B.13), temos

$$\phi(x) = \sum_{n=0}^{+\infty} a_n \phi_n(x) = \sum_{n=0}^{+\infty} s_n [\phi_n(x) - \phi_{n+1}(x)] = \sum_{n=0}^{+\infty} s_n c_n(x) \tag{B.14}$$

para $x \in (0,\, \xi]$, tomando $c_n(x) = \phi_n(x) - \phi_{n+1}(x)$. Pela condição 1, temos que $c_n(x) \to 0$ quando $x \to 0^+$, e pela condição 2 vale $\sum_{n=0}^{+\infty} |c_n(x)| < \infty$ para $x \in (0,\, X]$ e $\sum_{n=0}^{+\infty} |c_n(x)| < H$ para $x \in (0,\, X_0]$. Assim, pelo Teorema B.9 temos $\phi(x) = \sum_{n=0}^{+\infty} a_n \phi_n(x)$ bem definido em $(0,\, X]$ e $\phi(x) \to 0$ quando $x \to 0^+$.

Para o caso em que $s_n \to s$ com s não necessariamente nulo, definimos $a'_0 \doteq a_0 - s$ e $a'_n \doteq a_n$ para $n > 0$. Nesse caso $s'_n \doteq \sum_{\nu=0}^{n} a'_\nu \to 0$, e assim

$$\phi(x) - s\phi_0(x) = \sum_{n=0}^{+\infty} a'_n \phi_n(x) \to 0$$

quando $x \to 0^+$. Como $\phi_0(x) \to 1$ segue que $\phi(x) \to s$, como queríamos demonstrar.

Provemos que as condições são necessárias. Fixemos $k \geq 0$. Tomando $a_n \doteq \delta_{nk}$ para $n \geq 0$, temos $\sum_{n=0}^{+\infty} a_n = 1$ e portanto $\phi_k(x) = \phi(x) \to 1$. Assim, a condição 1 é necessária.

Fixemos $x \in (0,\, X]$. Como (ϕ) é regular, a série $\sum_{n=0}^{+\infty} a_n \phi_n(x)$ é convergente sempre que $s_n \to s$. Assim, pelo Teorema B.7 temos $\sum_{n=0}^{+\infty} |\phi_n(x) - \phi_{n+1}(x)| < \infty$, e isso vale para todo $x \in (0,\, X]$. Como na demonstração do Teorema B.7, isso implica que para esse x fixado a série $\sum_{n=0}^{+\infty} [\phi_n(x) - \phi_{n+1}(x)]$ é convergente, logo a sequência $(\phi_n(x))_n$ é de Cauchy e portanto é limitada. Dessa forma, quando $s_n \to 0$ chegamos a (B.14) da mesma forma como no caso anterior. Portanto, do Teorema B.9 temos $\sum_{n=0}^{+\infty} |c_n(x)| < H$ para $x \in (0,\, X_0]$ ou seja; temos a condição 2.

Suponhamos agora que vale (B.12). Como antes, $|\phi_0(x)| < H_1$ para $x \in (0,\, \xi]$, com $\xi < X$. Para $x \in (0,\, \xi]$ fixado, temos que $(\phi_n(x))_n$ é decrescente e limitada, logo é convergente. Assim sendo, para $x \in (0,\, \xi]$ temos

$$\sum_{n=0}^{+\infty} |\phi_n(x) - \phi_{n+1}(x)| = \sum_{n=0}^{+\infty} [\phi_n(x) - \phi_{n+1}(x)] = \phi_0(x) - \lim_{n \to +\infty} \phi_n(x) \leq \phi_0(x) < H_1.$$

Também, para $x \in (0,\, X]$ temos

$$\sum_{n=0}^{+\infty} |\phi_n(x) - \phi_{n+1}(x)| = \sum_{n=0}^{+\infty} [\phi_n(x) - \phi_{n+1}(x)] = \phi_0(x) - \lim_{n \to +\infty} \phi_n(x) < \infty.$$

Portanto, vale a condição 2. □

B.6 Os métodos de Abel e de Lambert

Definimos o método de Abel (A) da seguinte forma: a série $\sum_{n=0}^{+\infty} a_n$ tem soma (A) igual a s se a série de potências $\sum_{n=0}^{+\infty} a_n x^n$ tem raio de convergência maior ou igual a 1, e

$$\lim_{x \to 1^-} \sum_{n=0}^{+\infty} a_n x^n = s.$$

Nesse caso, escrevemos $\sum_{n=0}^{+\infty} a_n = s \ \ (A)$. Nessas condições, demonstramos a Proposição B.2:

Proposição B.11. *O método (A) é regular.*

Demonstração. Aqui utilizamos um resultado análogo ao Teorema B.10, mas para $x \to 1^-$ ao invés de $x \to 0^+$.

Na notação do Teorema B.10, temos $\phi_n(x) = x^n$ para $x \in [0,1)$ e $n \geq 0$, logo $\phi_n(x) \to 1$ quando $x \to 1^-$, e os ϕ_n satisfazem (B.12). Portanto, pelo Teorema B.10, temos que o método (A) é regular. □

O método de Lambert diz que $\sum_{n=0}^{+\infty} a_n$ tem soma (L) igual a s se

$$\sum_{n=0}^{+\infty} a_n \frac{nye^{-ny}}{1-e^{-ny}}$$

está bem definida para $y \in (0,\, 1]$, e

$$\lim_{y\to 0^+} \sum_{n=0}^{+\infty} a_n \frac{nye^{-ny}}{1-e^{-ny}} = s.$$

Nesse caso, escrevemos $\sum_{n=0}^{+\infty} a_n = s \ \ (L)$.

Proposição B.12. *O método (L) é regular.*

Demonstração. Vamos mostrar que o método (L) satisfaz o caso particular do Teorema B.10, provando que

$$f(x) = \frac{xe^{-x}}{1-e^{-x}}$$

é não-crescente para $x > 0$, e que $f(x) \to 1$ quando $x \to 0^+$. Isto é suficiente pois nos termos do Teorema B.10 temos $\phi_n(x) = f(nx)$.

De fato,

$$\lim_{x\to 0^+} f(x) = \lim_{x\to 0^+} \frac{x}{e^x - 1} = \lim_{x\to 0^+} \frac{1}{e^x} = 1.$$

Também,

$$f'(x) = \frac{(e^{-x} - xe^{-x})(1-e^{-x}) - xe^{-x}e^{-x}}{(1-e^{-x})^2} = \frac{e^{-x}}{(1-e^{-x})^2} \cdot (1 - e^{-x} - x).$$

Se $g(x) = 1 - e^{-x} - x$, temos então

$$f'(x) = \frac{e^{-x}}{(1-e^{-x})^2} \cdot g(x).$$

Como $g(0) = 0$, e

$$g'(x) = e^{-x} - 1 \leq 0,$$

para $x \geq 0$, temos que g é não-crescente em $[0,\, +\infty)$ e portanto $g(x) \leq 0$ para todo $x \in [0,\, +\infty)$. Assim, $f'(x) \leq 0$ para todo $x \in [0,\, +\infty)$ e dessa forma f é não-crescente. □

Apêndice C

Teoremas Tauberianos para Séries de Dirichlet

Enunciamos e demonstramos aqui alguns teoremas tauberianos para séries de Dirichlet, seguindo o texto [Kor02, Seções 7 e 8]. Dada uma série de Dirichlet $D(s) \doteq \sum_{n=1}^{+\infty} a_n/n^s$ absolutamente convergente para $\mathrm{Re}(s) > 1$, suponhamos que a função $D(s)$ possui um prolongamento analítico a um aberto que contém o semiplano fechado $\mathrm{Re}(s) \geq 1$. Os teoremas que estudaremos nesta seção dão algumas condições sobre a sequência dos a_n suficientes para a convergência da série $\sum_{n=1}^{+\infty} a_n/n$, e para que o seu valor seja tal que

$$D(1) = \sum_{n=1}^{+\infty} \frac{a_n}{n}.$$

(O valor $D(1)$ é dado pela extensão de $D(s)$ a $\mathrm{Re}(s) \geq 1$, logo esse valor não precisa ser, a princípio, igual a $\sum_{n=1}^{+\infty} a_n/n$.)

Começamos com um teorema tauberiano sobre a transformada de Laplace:

Teorema C.1. *Seja $\alpha : \mathbb{R} \to \mathbb{C}$ uma função mensurável limitada e tal que $\alpha(t) = 0$ para $t < 0$. Dessa forma a sua transformada de Laplace*

$$F(z) = \mathcal{L}\alpha(z) \doteq \int_0^{+\infty} \alpha(t) e^{-zt} \, \mathrm{d}t$$

está bem-definida e é analítica no semiplano $\mathrm{Re}(z) > 0$. Suponhamos que $F(z)$ possui uma extensão analítica a um aberto contendo o semiplano fechado $\mathrm{Re}(z) \geq 0$. Então a integral imprópria $\int_0^{+\infty} \alpha(t) \, \mathrm{d}t$ existe, e vale

$$\int_0^{+\infty} \alpha(t) \, \mathrm{d}t = F(0).$$

Demonstração. Notemos primeiramente que podemos supor $F(0) = 0$. De fato, se $F(0) \neq 0$, seja $\tilde{\alpha}(t) \doteq \alpha(t) - F(0)\chi_{[0,1]}(t)$, em que

$$\chi_{[0,1]}(t) = \begin{cases} 1, & \text{se } t \in [0,1] \\ 0, & \text{caso contrário.} \end{cases}$$

Assim,

$$\begin{aligned} \tilde{F}(z) \doteq \mathcal{L}\tilde{\alpha}(z) &= \int_0^{+\infty} \tilde{\alpha}(t) e^{-zt} \, \mathrm{d}t = \int_0^{+\infty} \alpha(t) e^{-zt} \, \mathrm{d}t - F(0) \int_0^1 e^{-zt} \, \mathrm{d}t \\ &= F(z) - F(0) \frac{1 - e^{-z}}{z}, \end{aligned}$$

com $(1 - e^{-z})/z$ função inteira. Então como $F(z)$ possui uma extensão analítica a um aberto contendo o semiplano fechado $\mathrm{Re}(z) \geq 0$, temos que $\tilde{F}(z)$ também possui uma extensão analítica a esse mesmo aberto, e com $\tilde{F}(0) = F(0) - F(0).1 = 0$.

Dessa forma, se provarmos que

$$\int_0^{+\infty} \tilde{\alpha}(t)\,\mathrm{d}t = \tilde{F}(0) = 0,$$

então

$$0 = \int_0^{+\infty} \tilde{\alpha}(t)\,\mathrm{d}t = \int_0^{+\infty} \alpha(t)\,\mathrm{d}t - F(0)$$

e teremos provado o resultado em geral.

Fixamos então $F(0) = 0$. Dividindo $\alpha(t)$ por uma constante se necessário, podemos supor $\sup|\alpha(t)| \leq 1$. Definamos, para $B > 0$,

$$F_B(z) \doteq \int_0^B \alpha(t)e^{-zt}\,\mathrm{d}t.$$

Precisamos mostrar que

$$\int_0^{+\infty} \alpha(t)\,\mathrm{d}t = \lim_{B\to+\infty} \int_0^B \alpha(t)\,\mathrm{d}t = \lim_{B\to+\infty} F_B(0) \stackrel{?}{=} 0.$$

Se $z = x + iy$ com $x, y \in \mathbb{R}$ e $x > 0$, temos

$$|F_B(z) - F(z)| \leq \int_B^{+\infty} |\alpha(t)||e^{-zt}|\,\mathrm{d}t \leq \int_B^{+\infty} e^{-xt}\,\mathrm{d}t \leq \frac{e^{-Bx}}{x}. \tag{C.1}$$

Se $x < 0$, então

$$|F_B(z)| \leq \int_0^B e^{-xt}\,\mathrm{d}t = \frac{e^{-Bx}}{-x} - \frac{1}{-x} \leq \frac{e^{-Bx}}{|x|}. \tag{C.2}$$

Para $R > 0$ fixado, seja Γ o caminho formado pelo círculo $|z| = R$ percorrido no sentido anti-horário. Sejam $\Gamma_1, \Gamma_2, \sigma$ os caminhos da figura C.1. Isto é; a curva Γ_1 percorre a circunferência Γ do ponto $-iR$ ao ponto iR em $\mathrm{Re}(z) \geq 0$; a curva Γ_2 percorre a circunferência de iR a $-iR$ por $\mathrm{Re}(z) \leq 0$; enquanto σ percorre o eixo imaginário de iR a $-iR$.

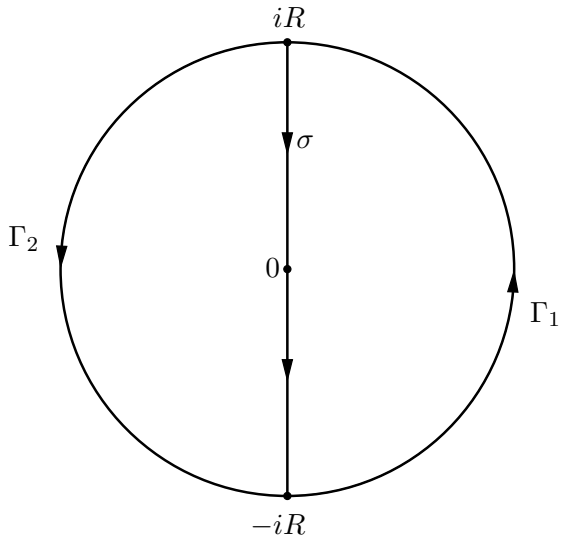

Figura C.1: *Caminho da demonstração do Teorema C.1.*

Podemos tentar continuar esta demonstração usando a Fórmula Integral de Cauchy usando as curvas $\Gamma, \Gamma_1, \Gamma_2, \sigma$; temos

$$F_B(0) = \frac{1}{2\pi i}\int_\Gamma \frac{F_B(z)}{z}\,\mathrm{d}z$$

pois $F_B(z)$ é uma função inteira. Podemos comparar a função $F_B(z)$ com $F(z)$ na curva Γ_1, mas $F(z)$ não está necessariamente definida em toda a Γ_2.

$$F_B(0) = \frac{1}{2\pi i}\int_{\Gamma_1} \frac{F_B(z)-F(z)}{z}\,\mathrm{d}z + \frac{1}{2\pi i}\int_{\Gamma_1}\frac{F(z)}{z}\,\mathrm{d}z + \frac{1}{2\pi i}\int_{\Gamma_2}\frac{F_B(z)}{z}\,\mathrm{d}z. \tag{C.3}$$

Completando o caminho Γ_1 com a reta σ na integral de $F(z)/z$, obtemos um caminho fechado, logo

$$\frac{1}{2\pi i}\int_{\Gamma_1}\frac{F(z)}{z}\,\mathrm{d}z = -\frac{1}{2\pi i}\int_\sigma \frac{F(z)}{z}\,\mathrm{d}z.$$

Substituindo em (C.3) obtemos

$$F_B(0) = \frac{1}{2\pi i}\int_{\Gamma_1} \frac{F_B(z)-F(z)}{z}\,\mathrm{d}z + \frac{1}{2\pi i}\int_{\Gamma_2}\frac{F_B(z)}{z}\,\mathrm{d}z - \frac{1}{2\pi i}\int_\sigma \frac{F(z)}{z}\,\mathrm{d}z. \tag{C.4}$$

E agora podemos começar a estimar essas integrais separadamente. Agora, observando as nossas estimativas (C.1) e (C.2) vemos que, do modo como está, não conseguiremos ir muito longe. Por exemplo, ao final de (C.1) obtivemos e^{-Bx}/x, que não é uma boa estimativa quando x está próximo de zero. A solução será integrar essas funções $F(z)$ e $F_B(z)$ contra uma outra função, que será melhor estimada.

Esse kernel especial será

$$z \mapsto e^{Bz}\left(\frac{1}{z}+\frac{z}{R^2}\right).$$

A propriedade mais importante dele é a seguinte: se $z = x+iy$ com $x, y \in \mathbb{R}$ e $|z| = R$, então

$$\frac{1}{z}+\frac{z}{R^2} = \frac{\overline{z}}{z\overline{z}}+\frac{z}{R^2} = \frac{z+\overline{z}}{R^2} = \frac{2x}{R^2}. \tag{C.5}$$

Assim, poderemos cancelar o termo $1/x$ nas estimativas de $F(z)$ e $F_B(z)$. Também multiplicamos esta função por e^{Bz} para cancelar os fatores e^{-Bx} e para permitir uma estimativa da integral sobre σ (veremos a seguir). Também mantemos a propriedade essencial da Fórmula Integral de Cauchy:

$$F_B(0) = F_B(0)e^0 = \frac{1}{2\pi i}\int_\Gamma F_B(z)e^{Bz}\left(\frac{1}{z}+\frac{z}{R^2}\right)\mathrm{d}z.$$

Dessa forma, do mesmo modo como obtivemos (C.4) conseguimos

$$\begin{aligned} F_B(0) = {} & \frac{1}{2\pi i}\int_{\Gamma_1}\big(F_B(z)-F(z)\big)e^{Bz}\left(\frac{1}{z}+\frac{z}{R^2}\right)\mathrm{d}z \\ & + \frac{1}{2\pi i}\int_{\Gamma_2} F_B(z)e^{Bz}\left(\frac{1}{z}+\frac{z}{R^2}\right)\mathrm{d}z - \frac{1}{2\pi i}\int_\sigma F(z)e^{Bz}\left(\frac{1}{z}+\frac{z}{R^2}\right)\mathrm{d}z \\ & \doteq T_1+T_2+T_3. \end{aligned} \tag{C.6}$$

Vamos então estimar as integrais T_1, T_2, e T_3.

Usando (C.1) e (C.5) temos, para $z = x+iy \in \Gamma_1$ com $x > 0$,

$$|F_B(z)-F(z)||e^{Bz}|\left|\frac{1}{z}+\frac{z}{R^2}\right| \le \frac{e^{-Bx}}{x}e^{Bx}\frac{2x}{R^2} = \frac{2}{R^2}.$$

Logo

$$|T_1| = \left| \frac{1}{2\pi i} \int_{\Gamma_1} \big(F_B(z) - F(z)\big) e^{Bz} \left(\frac{1}{z} + \frac{z}{R^2} \right) \mathrm{d}z \right| \leq \frac{1}{2\pi} \frac{2}{R^2} \pi R = \frac{1}{R}. \tag{C.7}$$

Usando (C.2) e (C.5) temos, para $z = x + iy \in \Gamma_2$ com $x < 0$,

$$|F_B(z)||e^{Bz}| \left| \frac{1}{z} + \frac{z}{R^2} \right| \leq \frac{e^{-Bx}}{|x|} e^{Bx} \frac{2|x|}{R^2} = \frac{2}{R^2}.$$

Logo, procedendo como para T_1 obtemos

$$|T_2| \leq \frac{1}{2\pi} \frac{2}{R^2} \pi R = \frac{1}{R}. \tag{C.8}$$

Agora,

$$T_3 = \frac{-1}{2\pi i} \int_{\sigma} F(z) e^{Bz} \left(\frac{1}{z} + \frac{z}{R^2} \right) \mathrm{d}z = \frac{-1}{2\pi i} \int_{R}^{-R} F(iy) e^{Biy} \left(\frac{1}{iy} + \frac{iy}{R^2} \right) i \, \mathrm{d}y = \frac{1}{2\pi} \int_{-R}^{R} f(y) e^{iBy} \, \mathrm{d}y,$$

em que

$$f(y) \doteq F(iy) \left(\frac{1}{iy} + \frac{iy}{R^2} \right).$$

Nesses termos, é natural que seja $T_3 \to 0$ quando $B \to +\infty$ (e R fixado) em vista do Lema de Riemann-Lebesgue, mas vamos provar esse limite de uma outra forma. Como $F(z)/z$ é holomorfa em um aberto contendo $\mathrm{Re}(z) \geq 0$, temos que $f(y)$ é infinitamente diferenciável em $\mathbb{R}$, logo

$$\begin{aligned} T_3 &= \frac{1}{2\pi} \int_{-R}^{R} f(y) e^{iBy} \, \mathrm{d}y = \frac{1}{2\pi} \int_{-R}^{R} f(y) \left(\frac{1}{iB} e^{iBy} \right)' \mathrm{d}y \\ &= \frac{1}{2\pi} f(y) \frac{e^{iBy}}{iB} \bigg|_{-R}^{R} - \frac{1}{2\pi} \int_{-R}^{R} f'(y) \frac{e^{iBy}}{iB} \, \mathrm{d}y \\ &= \frac{1}{2\pi i B} \big(f(R) e^{iBR} - f(-R) e^{-iBR} \big) - \frac{1}{2\pi i B} \int_{-R}^{R} f'(y) e^{iBy} \, \mathrm{d}y. \end{aligned}$$

Assim, para $R > 0$ fixado temos

$$T_3 = T_3(R, B) \to 0, \quad \text{quando} \quad B \to +\infty. \tag{C.9}$$

Com isso já podemos provar que $F_B(0) \to 0$ quando $B \to +\infty$. Seja $\varepsilon > 0$. Tomamos $R \doteq 1/3\varepsilon$ e para esse R, seja $B_0 > 0$ tal que

$$\text{se } B \geq B_0, \quad \text{então} \quad |T_3| < \frac{1}{3\varepsilon},$$

sendo que tal B_0 existe por (C.9). Assim, usando (C.6), (C.7) e (C.8) temos, se $B \geq B_0$, que $|F_B(0)| \leq \varepsilon$. Como $\varepsilon > 0$ é arbitrário, de fato $F_B(0) \to 0 = F(0)$ quando $B \to +\infty$. □

Vejamos agora como esse teorema tauberiano relativo à transformada de Laplace se aplica às séries de Dirichlet:

Teorema C.2. *Seja $D(s) \doteq \sum_{n=1}^{+\infty} a_n/n^s$ uma série de Dirichlet absolutamente convergente para $\mathrm{Re}(s) > 1$. Supomos que a função $D(s)$ possui um prolongamento analítico a um aberto contendo o semiplano fechado $\mathrm{Re}(s) \geq 1$, e que os coeficientes da série satisfazem*

$$S(v) \doteq \sum_{n \leq v} a_n = o(v).$$

Então a série $\sum_{n=1}^{+\infty} a_n/n$ *é convergente, de valor*

$$D(1) = \sum_{n=1}^{+\infty} \frac{a_n}{n}.$$

Demonstração. Se $\mathrm{Re}(s) \geq 0$ e $x > 1$, pela Identidade de Abel temos

$$\sum_{n \leq x} \frac{a_n}{n^{s+1}} = \frac{1}{x^s}\frac{S(x)}{x} + (s+1)\int_1^x \frac{S(u)}{u^{s+2}}\,\mathrm{d}u.$$

Fazendo a mudança de variáveis $u = e^t$ na integral temos

$$\sum_{n \leq x} \frac{a_n}{n^{s+1}} = \frac{1}{x^s}\frac{S(x)}{x} + (s+1)\int_0^{\log x} \frac{S(e^t)}{e^{t(s+2)}}e^t\,\mathrm{d}t = \frac{1}{x^s}\frac{S(x)}{x} + (s+1)\int_0^{\log x} \frac{S(e^t)}{e^t}e^{-st}\,\mathrm{d}t$$

Isso sugere definir

$$\alpha(t) \doteq \begin{cases} e^{-t}S(e^t), & \text{se } t \geq 0, \\ 0, & \text{se } t < 0. \end{cases}$$

Então $\alpha(t)$ é limitada, pois $S(e^t) = o(e^t)$. Com essa notação, temos

$$\sum_{n \leq x} \frac{a_n}{n^{s+1}} = \frac{1}{x^s}\frac{S(x)}{x} + (s+1)\int_0^{\log x} \alpha(t)e^{-st}\,\mathrm{d}t. \tag{C.10}$$

Dessa forma, se $\mathrm{Re}(s) > 0$, fazendo $x \to +\infty$ em (C.10) e usando $S(x) = o(x)$ temos

$$D(s+1) = \sum_{n=1}^{+\infty} \frac{a_n}{n^{s+1}} = (s+1)\int_0^{+\infty} \alpha(t)e^{-st}\,\mathrm{d}t = (s+1)\mathcal{L}\alpha(s).$$

Assim, para $\mathrm{Re}(s) > 0$,

$$\mathcal{L}\alpha(s) = \frac{D(s+1)}{s+1}.$$

Agora, como $D(s)$ é analítica em um aberto contendo o semiplano fechado $\mathrm{Re}(s) \geq 1$, segue que $\mathcal{L}\alpha(z)$ possui um prolongamento analítico ao semiplano fechado $\mathrm{Re}(z) \geq 0$. Assim, pelo Teorema C.1 temos

$$\int_0^{+\infty} \alpha(t)\,\mathrm{d}t = \mathcal{L}\alpha(0) = \frac{D(1)}{1} = D(1).$$

Por outro lado, colocando $s = 0$ em (C.10) e fazendo $x \to +\infty$, temos

$$\sum_{n=1}^{+\infty} \frac{a_n}{n} = \int_0^{+\infty} \alpha(t)\,\mathrm{d}t = D(1). \qquad \square$$

Teorema C.3. *Seja* $D(s) \doteq \sum_{n=1}^{+\infty} a_n/n^s$ *uma série de Dirichlet absolutamente convergente para* $\mathrm{Re}(s) > 1$. *Suponhamos que os coeficientes* a_n, $n \in \mathbb{N}$ *sejam reais, que existe* $C > 0$ *tal que* $a_n \geq -C$ *para todo* $n \in \mathbb{N}$ *e que*

$$S(v) \doteq \sum_{n \leq v} a_n = O(v).$$

Supomos também que existe $A \in \mathbb{R}$ *tal que* $F(s) \doteq D(s) - A\zeta(s)$ *possui uma extensão analítica para um aberto contendo o semiplano fechado* $\mathrm{Re}(s) \geq 1$. *Então*

$$\frac{S(u)}{u} \to A$$

quando $u \to +\infty$, a série $\sum_{n=1}^{+\infty}(a_n - A)/n$ converge, e vale

$$F(1) = \sum_{n=1}^{+\infty} \frac{a_n - A}{n}.$$

Demonstração. Notemos primeiramente que basta provar o resultado supondo $a_n > 0$ para todo $n \in \mathbb{N}$ e $A > 0$. De fato, se a série $D(s) \doteq \sum_{n=1}^{+\infty} a_n/n^s$ satisfaz as hipóteses do Teorema, existe $C' > 0$ tal que $b_n \doteq a_n + C' > 0$ para todo $n \in \mathbb{N}$ e $B \doteq A + C' > 0$. Definindo então $\tilde{D}(s) \doteq \sum_{n=1}^{+\infty} b_n/n^s = D(s) + C'\zeta(s)$ e $\tilde{S}(v) \doteq \sum_{n \le v} b_n = S(v) - [v]C'$, em que $[v]$ denota a parte inteira do real v, temos $\tilde{D}(s) - B\zeta(s) = D(s) - A\zeta(s) = F(s)$ e assim a série $\tilde{D}(s)$ satisfaz as hipóteses do Teorema, com $b_n > 0$ para todo $n \in \mathbb{N}$, e $B > 0$.

Se então vale $\tilde{S}(u)/u \to B$ e $F(1) = \sum_{n=1}^{+\infty}(b_n - B)/n$, temos $S(u)/u = \tilde{S}(u)/u - C'[u]/u$, de modo que $S(u)/u \to B - C' = A$, e

$$\sum_{n=1}^{+\infty} \frac{a_n - A}{n} = \sum_{n=1}^{+\infty} \frac{b_n - B}{n} = F(1).$$

Assim sendo, seja $D(s) \doteq \sum_{n=1}^{+\infty} a_n/n^s$ uma série de Dirichlet satisfazendo as hipóteses do Teorema e também com $a_n > 0$ para todo $n \in \mathbb{N}$ e $A > 0$. Definimos

$$\alpha(t) \doteq \frac{S(e^t) - A[e^t]}{e^t} = \frac{1}{e^t} \sum_{n \le e^t} (a_n - A),$$

se $t \ge 0$, e $\alpha(t) \doteq 0$ se $t < 0$. Como $S(v) = O(v)$, temos que a função $\alpha(t)$ é limitada.

Para $\mathrm{Re}(s) > 0$, o Lema 5.2 implica

$$\begin{aligned}
\sum_{n \le x} \frac{a_n - A}{n^{s+1}} &= \frac{\sum_{n \le x}(a_n - A)}{x^{s+1}} + (s+1)\int_1^x \frac{\sum_{n \le x}(a_n - A)}{v^{s+2}}\,\mathrm{d}v \\
&= \frac{1}{x^s}\left(\frac{S(x)}{x} - A\frac{[x]}{x}\right) + (s+1)\int_0^{\log x} \frac{\sum_{n \le e^t}(a_n - A)}{(e^t)^{s+2}} e^t\,\mathrm{d}t \\
&= \frac{1}{x^s}O(1) + (s+1)\int_0^{\log x} \alpha(t)e^{-st}\,\mathrm{d}t. \qquad \text{(C.11)}
\end{aligned}$$

Fazendo $x \to +\infty$ temos $F(s+1) = D(s+1) - A\zeta(s+1) = (s+1)\mathcal{L}\alpha(s)$, logo

$$\mathcal{L}\alpha(s) = \frac{F(s+1)}{s+1}$$

de modo que $\mathcal{L}\alpha(s)$ possui um prolongamento analítico em um aberto contendo $\mathrm{Re}(s) \ge 0$. Pelo Teorema C.1 temos então

$$\int_1^{+\infty} \frac{S(v) - A[v]}{v^2}\,\mathrm{d}v = \int_0^{+\infty} \alpha(t)\,\mathrm{d}t = F(1). \qquad \text{(C.12)}$$

Provemos agora que vale $S(u) \sim Au$. Suponhamos por absurdo que seja $\limsup(S(u)/u) > A$. Então existem $\varepsilon > 0$ e $u_1, u_2, u_3, \ldots$, com $u_n \to +\infty$, tais que

$$S(u_n) > (A + 2\varepsilon)u_n \qquad \text{para todo } n \in \mathbb{N}.$$

Como $a_n > 0$ para todo $n \in \mathbb{N}$, temos que $S(v)$ é não-decrescente. Seja $\rho \doteq (A + 2\varepsilon)/(A + \varepsilon) > 1$. Então se $u_n < v < \rho u_n$,

$$S(v) \ge S(u_n) > (A + 2\varepsilon)u_n > (A + \varepsilon)v \ge (A + \varepsilon)[v]$$

de modo que, para todo $n \in \mathbb{N}$,

$$\int_{u_n}^{\rho u_n} \frac{S(v) - A[v]}{v^2}\,\mathrm{d}v > \int_{u_n}^{\rho u_n} \frac{\varepsilon/2}{v}\,\mathrm{d}v = \frac{\varepsilon}{2}\log\rho > 0,$$

o que contradiz a convergência da integral $\int_1^{+\infty}(S(v) - A[v])/v^2\,\mathrm{d}v$, vista em (C.12). Portanto, $\limsup(S(u)/u) \leq A$.

Suponhamos agora que $\liminf(S(u)/u) < A$. Então existem $\varepsilon > 0$ e uma sequência $(u_n)_n$, com $u_n \to +\infty$, tais que

$$S(u_n) < (A - 2\varepsilon)u_n \qquad \text{para todo } n \in \mathbb{N}.$$

Como $A > 0$ podemos supor $0 < 2\varepsilon < A$. Seja $\rho \doteq (A - 2\varepsilon)/(A - \varepsilon)$; $0 < \rho < 1$. Se então $\rho u_n < v < u_n$,

$$S(v) \leq S(u_n) < (A - 2\varepsilon)u_n < (A - \varepsilon)v.$$

Dessa forma, para todo $n \in \mathbb{N}$,

$$\begin{aligned}\int_{\rho u_n}^{u_n} \frac{S(v) - A[v]}{v^2}\,\mathrm{d}v &\leq \int_{\rho u_n}^{u_n} \frac{(A - \varepsilon)v - A[v]}{v^2}\,\mathrm{d}v \leq \int_{\rho u_n}^{u_n} A\frac{v - [v]}{v^2}\,\mathrm{d}v - \varepsilon\int_{\rho u_n}^{u_n}\frac{1}{v}\,\mathrm{d}v \\ &\leq A\int_{\rho u_n}^{+\infty}\frac{1}{v^2}\,\mathrm{d}v + \varepsilon\log\rho \leq \frac{A}{\rho u_n} + \varepsilon\log\rho.\end{aligned}$$

Como $u_n \to +\infty$, se n é suficientemente grande temos

$$\int_{\rho u_n}^{u_n} \frac{S(v) - A[v]}{v^2}\,\mathrm{d}v \leq \frac{A}{\rho u_n} + \varepsilon\log\rho \leq \frac{\varepsilon}{2}\log\rho < 0,$$

o que também contradiz a convergência da integral $\int_1^{+\infty}(S(v) - A[v])/v^2\,\mathrm{d}v$, vista em (C.12). Portanto, $\liminf(S(u)/u) \geq A$, o que conclui a prova de $S(u) \sim Au$.

Como em (C.11), o Lema 5.2 implica

$$\sum_{n\leq x}\frac{a_n - A}{n} = \frac{S(x) - A[x]}{x} + \int_0^{\log x}\alpha(t)\,\mathrm{d}t. \tag{C.13}$$

Agora $(S(x) - A[x])/x \to 0$ pois $S(x) \sim Ax$, logo fazendo $x \to +\infty$ em (C.13) temos que

$$\sum_{n=1}^{+\infty}\frac{a_n - A}{n} = \int_0^{+\infty}\alpha(t)\,\mathrm{d}t = F(1). \qquad \square$$

De fato não usaremos tanto o Teorema C.3, mas uma versão mais fraca dele:

Corolário C.4. *Seja $D(s) = \sum_{n=1}^{+\infty} a_n/n^s$ uma série de Dirichlet com coeficientes reais e tais que*

$$a_n = O(1).$$

Então a série $D(s)$ é absolutamente convergente para $\mathrm{Re}(s) > 1$, e suponhamos que $D(s)$ possui uma extensão analítica a um aberto contendo o semiplano fechado $\mathrm{Re}(s) \geq 1$. Então $\sum_{n=1}^{+\infty} a_n/n$ converge, e

$$D(1) = \sum_{n=1}^{+\infty}\frac{a_n}{n}.$$

C.1 Outro tipo de teorema tauberiano

Aqui vamos demonstrar um teorema de tipo tauberiano diferente dos vistos anteriormente neste Apêndice. De fato, a demonstração desse Teorema é basicamente a mesma do Teorema 4.4, só que

aqui trataremos de séries de Dirichlet ao invés de séries de potências. Mais ainda, o Teorema que provaremos é um caso especial de um resultado mais geral, que pode ser encontrado em [Ten95, Teorema 5 do Capítulo II.7].

Como na demonstração do Teorema 4.4, precisaremos de um Lema sobre integrais:

Lema C.5. *Seja $g : [0, 1] \to \mathbb{R}$ contínua, ou contínua a menos de uma única descontinuidade de tipo 1 em $[0, 1]$. Seja $k \in \mathbb{N}$. Dado $\varepsilon > 0$ existem polinômios reais p e P tais que*

$$p(x) \leq g(x) \leq P(x), \quad \text{para todo } x \in [0, 1], \tag{C.14}$$

que satisfazem

$$0 \leq \int_0^{+\infty} \big(P(e^{-t}) - g(e^{-t})\big) e^{-t} t^{k-1} \, \mathrm{d}t \leq \varepsilon \tag{C.15}$$

e

$$0 \leq \int_0^{+\infty} \big(g(e^{-t}) - p(e^{-t})\big) e^{-t} t^{k-1} \, \mathrm{d}t \leq \varepsilon.$$

Não é necessário detalhar a demonstração desse resultado, já que ela é completamente análoga à demonstração do Corolário 4.3 (a única coisa que muda é a fórmula da integral final).

Teorema C.6. *Seja $D(s) = \sum_{n=1}^{\infty} a_n/n^s$ uma série de Dirichlet com coeficientes não-negativos que converge absolutamente no semiplano $\mathrm{Re}(s) > 0$. Suponhamos que existam $C \in \mathbb{C}$ e $k \in \mathbb{N}$ tais que*

$$\lim_{\sigma \to 0^+} \sigma^k D(\sigma) = C.$$

Então para $x \to +\infty$ vale

$$\sum_{n \leq x} a_n \sim \frac{C}{k!} \log^k x.$$

Demonstração. Provemos primeiramente que se P é um polinômio, então para $\sigma \to 0^+$ vale

$$\sigma^k \sum_{n=1}^{+\infty} \frac{a_n}{n^\sigma} P\left(\frac{1}{n^\sigma}\right) \to \frac{C}{(k-1)!} \int_0^{+\infty} P(e^{-t}) e^{-t} t^{k-1} \, \mathrm{d}t. \tag{C.16}$$

De fato, basta provar para $P(x) = x^m$ com $m \geq 0$ pela linearidade em P da expressão (C.16). Nesse caso, temos

$$\sigma^k \sum_{n=1}^{+\infty} \frac{a_n}{n^\sigma} P\left(\frac{1}{n^\sigma}\right) = \sigma^k D\big((m+1)\sigma\big) = \frac{1}{(m+1)^k} \big((m+1)\sigma\big)^k D\big((m+1)\sigma\big).$$

Portanto

$$\sigma^k \sum_{n=1}^{+\infty} \frac{a_n}{n^\sigma} P\left(\frac{1}{n^\sigma}\right) \to \frac{1}{(m+1)^k} \cdot C \quad \text{quando } \sigma \to 0^+.$$

Apesar dessa fórmula parecer mais simples do que (C.16), ela possui uma desvantagem importante: ela não é linear em P como é (C.16). Por isso usamos a seguinte expressão

$$\frac{C}{(m+1)^k} = \frac{C}{\Gamma(k)} \int_0^{+\infty} e^{-tm} e^{-t} t^{k-1} \, \mathrm{d}t = \frac{C}{(k-1)!} \int_0^{+\infty} P(e^{-t}) e^{-t} t^{k-1} \, \mathrm{d}t$$

que pode ser provada substituindo $u = (m+1)t$ na integral. Assim obtemos (C.16).

Agora seja $g : [0, 1] \to \mathbb{R}$ dada por

$$g(x) = \begin{cases} 0, & \text{se } 0 \leq x < 1/e \\ 1/x, & \text{se } 1/e \leq x \leq 1. \end{cases}$$

Assim como provamos (4.11), temos que usando o Lema C.5 e (C.16) vale

$$\sigma^k \sum_{n=1}^{+\infty} \frac{a_n}{n^\sigma} g\left(\frac{1}{n^\sigma}\right) \to \frac{C}{(k-1)!} \int_0^{+\infty} g(e^{-t}) e^{-t} t^{k-1} \, \mathrm{d}t \quad \text{quando } \sigma \to 0^+. \tag{C.17}$$

(Aqui usamos o fato de ser $a_n \geq 0$ para todo $n \in \mathbb{N}$.)

Agora $g(n^{-\sigma}) \neq 0$ se, e somente se $n^{-\sigma} \geq 1/e$, isto é; $n \leq e^{1/\sigma}$. Nesse caso, $g(n^{-\sigma}) = n^\sigma$. Substituindo também o valor de g na integral de (C.17), segue que

$$\sigma^k \sum_{n \leq e^{1/\sigma}} a_n \to \frac{C}{(k-1)!} \int_0^1 t^{k-1} \, \mathrm{d}t = \frac{C}{k!} \quad \text{quando } \sigma \to 0^+.$$

Escrevendo $x = e^{1/\sigma}$ obtemos o resultado. □

Referências Bibliográficas

[Apo76] Tom M. Apostol. *Introduction to analytic number theory*. Springer-Verlag, New York, 1976. Undergraduate Texts in Mathematics.

[Bai02] Stephan Baier. On the Bateman-Horn conjecture. *J. Number Theory*, 96(2):432–448, 2002.

[BH62] Paul T. Bateman e Roger A. Horn. A heuristic asymptotic formula concerning the distribution of prime numbers. *Math. Comp.*, 16:363–367, 1962.

[BS62] Paul T. Bateman e Rosemarie M. Stemmler. Waring's problem for algebraic number fields and primes of the form $(p^r - 1)/(p^d - 1)$. *Illinois J. Math.*, 6:142–156, 1962.

[Con03] Keith Conrad. Hardy-Littlewood constants. Em *Mathematical properties of sequences and other combinatorial structures (Los Angeles, CA, 2002)*, páginas 133–154. Kluwer Acad. Publ., Boston, MA, 2003.

[FI98] John Friedlander e Henryk Iwaniec. The polynomial $X^2 + Y^4$ captures its primes. *Ann. of Math. (2)*, 148(3):945–1040, 1998.

[Gol56] Solomon W. Golomb. *Problems in the Distribution of the Prime Numbers*. Tese de Doutorado, Harvard University, 1956.

[Gol70] Solomon W. Golomb. The lambda method in prime number theory. *J. Number Theory*, 2:193–198, 1970.

[Har92] G. H. Hardy. *Divergent series*. American Mathematical Society, 1992.

[HR05] Marc Hindry e Tanguy Rivoal. Le Λ-calcul de Golomb et la conjecture de Bateman-Horn. *Enseign. Math. (2)*, 51(3-4):265–318, 2005.

[HS00] Marc Hindry e Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[Kor02] J. Korevaar. A century of complex Tauberian theory. *Bull. Amer. Math. Soc. (N.S.)*, 39(4):475–531, 2002.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, segunda edição, 1994.

[Nar04] Władysław Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, terceira edição, 2004.

[Rib01] Paulo Ribenboim. *Classical theory of algebraic numbers*. Universitext. Springer-Verlag, New York, 2001.

[Tao09] Terence Tao. *Poincaré's legacies, pages from year two of a mathematical blog. Part I*. American Mathematical Society, Providence, RI, 2009.

[Ten95] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 46 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 1995. Translated from the second French edition (1995) by C. B. Thomas.

[Tit39] E. C. Titchmarsh. *The theory of functions*. Oxford University Press, segunda edição, 1939.

Índice Remissivo

(A), 106
(C), 98
(L), 107
A_p, 26
$A_{p,K}$, 26
$C(\mathbf{f})$, 6, 11
$M_{\mathbf{f}}(s)$, 54
$N_g(d)$, 10
$R_K(s)$, 29
$S(\mathbf{f})$, 51
$U_{\mathbf{f}}$, 57
$X(\mathbf{f})$, 79
$Z_k(f_0; x)$, 40
$\Lambda(n)$, 1, 31
$L_{\mathbf{f}}(s)$, 53, 57
$\mathcal{O}_K$, 26
$\mathcal{I}_c$, 99
$\mathcal{I}_r$, 99
$\mu(n)$, 1, 31
$\omega(n)$, 1, 31
$\pi(x)$, 4
$\pi_{\mathbf{f}}(x)$, 5
$\psi(x)$, 6, 32
$\psi_{\mathbf{f}}(x)$, 37
sgn, 101
$\zeta(s)$, 32
ζ_K, 29
$d(n)$, 87

Conjectura
  de Bateman-Horn, 6, 11
  de Schinzel, 6, 9
  dos primos gêmeos, 3, 6, 45
  $p = n^2 + 1$, 3

Descontinuidade
  de tipo 1, 33

Família apropriada, 10
Função
  multiplicativa, 25, 32
  ζ de Dedekind, 29
  ζ de Hurwitz, 89
  ζ de Riemann, 32

Hipótese
  de Riemann, 73
Hipótese F, 45

Identidade
  de Abel, 37
  de Golomb, 44

Λ-cálculo de Golomb, 6

Método
  de Abel (A), 106
  de Cesàro (C), 98
  de Lambert (L), 107
    regularidade do, 35, 107
  regular, 7, 99, 104, 105

Norma
  de um ideal, 26

Primos
  gêmeos, 3

Série
  divergente, 98
Sequência
  somável, 98

Teorema
  abeliano, 97
  de Bateman-Stemmler, 79
  de Dirichlet, 4, 9
  de Weierstrass, 32
  dos Números Primos, 4
    demonstração do, 36
  tauberiano, 109
    de Hardy-Littlewood, 6, 33
    para séries de Dirichlet, 109
Transformada
  de Laplace, 109