UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE CIÊNCIAS EXATAS E DA NATUREZA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Ricardo Francisco da Silva

O Teorema de Hooley e a Conjectura de Artin para Raízes Primitivas

Recife

2018

Ricardo Francisco da Silva

O Teorema de Hooley e a Conjectura de Artin para Raízes Primitivas

Dissertação apresentada ao Programa de Pós-graduação em Matemtica da Universidade Federal de Pernambuco como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. **EDUARDO SHIRLIPPE GOES LEANDRO**

Recife

2018

Catalogação na fonte
Bibliotecária Monick Raquel Silvestre da S. Portes, CRB4-1217

S586t Silva, Ricardo Francisco da
O teorema de Hooley e a conjectura de Artin para raízes primitivas / Ricardo Francisco da Silva. – 2018.
74 f.: il., fig., tab.

Orientador: Eduardo Shirlippe Goes Leandro.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CCEN, Matemática, Recife, 2018.
Inclui referências e apêndices.

1. Teoria dos números. 2. Raízes primitivas. I. Leandro, Eduardo Shirlippe Goes (orientador). II. Título.

512.7 CDD (23. ed.) UFPE- MEI 2018-092

RICARDO FRANCISCO DA SILVA

O TEOREMA DE HOOLEY E A CONJECTURA DE ARTIN PARA RAÍZES PRIMITIVAS

Dissertação apresentada ao Programa de Pós-Graduação do Departamento de Matemática da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre em Matemática.

Aprovado em: 27/02/2018.

BANCA EXAMINADORA

_____

Prof. Dr. Eduardo Shirlippe Goes Leandro (Orientador)
Universidade Federal de Pernambuco

_____

Prof. Dr. Manoel José Machado Soares Lemos (Examinador Interno)
Universidade Federal de Pernambuco

_____

Prof. Dr. Hemar Teixeira Godinho (Examinador Externo)
Universidade de Brasília

Agradecimentos

A Deus pelo dom da vida, pela paz, saúde e sabedoria.

À minha família, principalmente meus pais, por acreditar em mim sempre e por serem exemplos de perseverança e de luta.

Aos meus amigos pelo apoio, encorajamento e motivação e pelos bons momentos que tivemos juntos.

Ao professor Eduardo Leandro, pelo suporte, auxílio e acompanhamento neste trabalho.

Ao professor Antonio Carlos pela oportunidade em estudar Teoria dos Números com ele e pela paciência para comigo em seus ensinamentos e orientações.

Aos professores do Departamento de Matemática que contribuíram na minha formação.

Aos membros da banca pela gentileza em participar da avaliação desse trabalho.

Ao CNPQ pelo apoio financeiro.

Resumo

Desde que Artin formulou sua conjectura em 1927, muitos matemáticos tentaram demonstrá-la, mas não obtiveram um resultado significativo. Entretanto, em 1967 houve um avanço notório em torno da conjectura de Artin com o trabalho de Hooley. De fato, o teorema de Hooley foi o primeiro resultado de grande importância no que diz respeito à conjectura, fornecendo uma prova rigorosa para a mesma, assumindo a Hipótese de Riemann Generalizada para funções zeta de Dedekind de certos corpos de números. Temos por objetivo, neste trabalho, apresentar os detalhes da demonstração do teorema de Hooley. Detalharemos o raciocínio heurístico que levou Artin a formular a sua conjectura. Veremos que a relação com a Hipótese de Riemann aparece quando Hooley usa uma versão efetiva do teorema de Chebotarev, que também é um resultado de grande relevância em Teoria dos Números. Além disso, veremos também como o trabalho de Hooley tem relação com os métodos de crivos, demonstrando a famosa desigualdade de Brun-Titchmarsh via crivo de Selberg.

Palavras-Chave: Teoria dos Números. Métodos de Crivos. Conjectura de Artin. Raízes Primitivas.

Abstract

Since Artin formulated his conjecture in 1927, many mathematicians attempted to demonstrate it, but did not obtain a significant result. However, in 1967 there was a notable advance around the Artin conjecture, with Hooley's work. In fact, Hooley's theorem was the first major result with respect to this conjecture, providing rigorous proof for it, assuming the Generalized Riemann Hypothesis for the Dedekind's zeta functions of certain number fields. The purpose of this work is to present the details of the proof of Hooley's theorem. We will detail the heuristic reasoning that led Artin to formulate his conjecture. We will see that the relation with the Riemann Hypothesis appears when Hooley uses an effective version of Chebotarev's theorem, which is also a result of great relevance in Number Theory. In addition, we will also see how Hooley's work relates to sieve methods, demonstrating the famous Brun-Titchmarsh inequality via the Selberg sieve.

Keywords: Number Theory. Sieve Methods. Artin's Conjecture. Primitive Roots.

Sumário

1 Introdução

A conjectura de Artin para raízes primitivas é um dos problemas mais famosos da Teoria dos Números. É bem verdade que antes de Artin formular formalmente essa conjectura, Gauss já tinha estudado o problema quando analisava o tamanho dos períodos das expansões decimais de frações com denominador primo.

Ao longo dos anos, vários trabalhos foram publicados em torno dessa conjectura, como por exemplo, em [4], Bilharz demonstrou a versão para corpos de funções, assumindo a Hipótese de Riemann para funções zeta de tais corpos, que foi demonstrada depois, em 1948, por André Weil. Em 1967, Hooley (ver [14]), assumindo a Hipótese de Riemann para funções zeta para corpos de números da forma $\mathbb{Q}(b^{\frac{1}{k_1}}, \zeta_k)$, onde k é um inteiro livre de quadrados, k_1 um divisor de k e ζ_k uma k-ésima raiz primitiva da unidade, mostrou que a conjectura de Artin é verdadeira. Em [9], Gupta e Ram Murty demonstraram que dados três primos distintos q, r e s, o conjunto

$$S = \{qs^2, q^3r^2, q^2r, r^3s^2, r^2s, q^2s^3, qr^3, q^3rs^2, rs^3, q^2r^3s, q^3s, qr^2s^3, qrs\}$$

tem pelo menos um elemento para o qual a conjectura de Artin é verdadeira. E em [11], Heath-Brown mostrou que dados três inteiros não-nulos q, r e s multiplicativamente independentes (ou seja, se $q^e r^f s^g = 1$ com $e, f, g \in \mathbb{Z}$, então $e = f = g = 0$) e supondo que nenhum dos números $q, r, s, -3qr, -3qs, -3rs$ ou qrs seja um quadrado, a conjectura de Artin é válida para pelo menos um dos números q, r, s.

Neste trabalho temos por objetivo estudar detalhadamente o teorema de Hooley. No Capítulo 1, mostramos a origem da conjectura e como Artin raciocinou para formular sua conjectura.

No Capítulo 2, nos voltamos para a Teoria Analítica dos Números, onde veremos um pouco sobre Métodos de Crivos. Nesse capítulo, mostraremos o Crivo de Selberg e o usaremos para demonstrar a desigualdade de Brun-Titchmarsh.

No Capítulo 3, demonstraremos uma versão efetiva do Teorema de Chebotarev (isto é, o teorema com um termo de resto) para corpos da forma $\mathbb{Q}(b^{\frac{1}{k_1}}, \zeta_k)$. Para isso, assumiremos que a Hipótese de Riemann é verdadeira para funções zeta de Dedekind de tais corpos. Também assumiremos a equação funcional para funções zeta de Dedekind e a fórmula explícita, uma vez que as demonstrações estão além de nossos objetivos.

No Capítulo 4, demonstraremos o Teorema de Hooley, usando os resultados obtidos ao longo dos capítulos.

Por fim, queremos deixar claro que estaremos assumindo conceitos e resultados básicos da Teoria Elementar e Algébrica dos Números e alguns teoremas conhecidos da Teoria Analítica dos Números como o Teorema dos Números Primos e os Teoremas de Mertens. Boa parte desses resultados estão no Apêndice D. Além disso, recomendamos [2], [18], [26] e [31] como referências.

2 A Conjectura de Artin

2.1 A Origem da Conjectura

Nos artigos 314-317 de sua *Disquisitiones Arithmeticae*, Gauss estudou expansões decimais de frações com denominadores primos e potências de primos. Ele observou que se p é um primo diferente de 2 e de 5 então a mantissa (expansão decimal com a parte inteira excluída) é infinita e periódica. Seja

$$\frac{1}{p} = 0, a_1 a_2 \dots a_k \dots$$

a sua expansão decimal com período de tamanho k. Ele também observou que o tamanho do período $a_1 a_2 \dots a_k$ é o menor inteiro que satisfaz $10^k \equiv 1 \pmod{p}$ (Art. 314). De fato,

$$\frac{1}{p} = \left(\frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_k}{10^k}\right)\left(1 + \frac{1}{10^k} + \ldots + \frac{1}{10^{2k}} + \ldots\right) = \frac{M}{10^k - 1},$$

onde M é algum inteiro. Logo, $10^k - 1 = Mp$, ou seja, $10^k \equiv 1 (\text{mod } p)$.

Se k é o menor inteiro satisfazendo $10^k \equiv 1 (\text{mod } p)$, dizemos que 10 tem *ordem* k (mod p). Pelo pequeno teorema de Fermat,

$$10^{p-1} \equiv 1 (\text{mod } p)$$

o que implica que $0 < k \leq p-1$. Além disso, pelo teorema de Lagrange, $k|(p-1)$. Assim, o maior período de $\frac{1}{p}$ ocorre se, e somente se, 10 tem ordem $p-1$ módulo p. Nesse caso, dizemos que 10 é uma *raiz primitiva* módulo p. Em geral, temos a seguinte

Definição 1. *Seja $p \nmid a$ um primo. Dizemos que a é uma raiz primitiva (mod p) se o menor k tal que $a^k \equiv 1$ (mod p) é $p-1$.*

Vejamos alguns exemplos:

$$\frac{1}{7} = 0, \overline{142857};\ \frac{1}{11} = 0, \overline{09};\ \frac{1}{13} = 0, \overline{076923};\ \frac{1}{17} = 0, \overline{0588235294117647}.$$

Assim, 10 é raiz primitiva (mod 7) e (mod 17) e não é raiz primitiva (mod 11) e (mod 13).

Atribui-se a Gauss a conjectura de que 10 é uma raiz primitiva módulo p para infinitos primos p e também o interesse em saber com que frequência isso ocorre.

Vários matemáticos do século XIX fizeram alusão ao problema, mas a maioria dos resultados era de natureza inconclusiva. Entretanto, destacamos um resultado interessante provado por eles:

Teorema 2.1.1. *2 é uma raiz primitiva mod p se p é da forma $4q+1$, onde q é um primo.*

Demonstração. Primeiro observe que um inteiro a é uma raiz primitiva mod p se, e somente se, para cada primo q,

$$p \equiv 1(\text{mod } q) \implies a^{(p-1)/q} \not\equiv 1(\text{mod } p).$$

Se p é da forma $4q+1$, então $p-1$ tem somente dois divisores primos, a saber, 2 e q. Como q é ímpar, $p = 4q+1 \equiv 5 \pmod 8$ e $\left(\frac{2}{p}\right) = -1$. Por outro lado, pelo critério de Euler $\left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} \pmod p$. Assim,

$$2^{(p-1)/2} \equiv -1(\text{mod } p).$$

Também, se $2^{(p-1)/q} = 2^4 \equiv 1(\text{mod p})$, com q primo, então $p = 3$ ou 5 e nenhum desses é da forma $4q+1$, portanto, pelo critério no começo da demonstração, 2 é uma raiz primitiva (mod p). □

Uma conjectura precisa para determinar os números primos para os quais um inteiro dado é uma raiz primitiva foi formulada em 1927 por Emil Artin.

Conjectura 2.1.2 (Conjectura de Artin para raízes primitivas)**.** *Dado um inteiro $a \neq -1$ e que não é um quadrado perfeito, existem infinitos primos p para os quais a é uma raiz primitiva (mod p). Além disso, se $N_a(x)$ denota o número de tais primos menores ou iguais a x, então*

$$N_a(x) \sim A(a)\frac{x}{\log x}$$

[1] *quando $x \to \infty$, onde $A(a)$ é uma constante que depende de a.*

A seguir, veremos heuristicamente como se obtém a constante $A(a)$.

[1] A notação $f(x) \sim g(x)$, quando $x \to \infty$ significa $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$ e dizemos que $f(x)$ é assintótico a $g(x)$.

2.2 Intuição Elementar

Como já vimos anteriormente, um inteiro a é uma raiz primitiva mod p se, e somente se, para cada primo q,

$$p \equiv 1(\text{mod } q) \implies a^{(p-1)/q} \not\equiv 1(\text{mod } p).$$

Assim, a é uma raiz primitiva se os "eventos "

$$p \equiv 1(\text{mod } q)$$

$$a^{(p-1)/q} \equiv 1(\text{mod } p)$$

não ocorrem simultaneamente. Fixemos um primo q. Vamos calcular a probabilidade de um primo p satisfazer ambas as condições acima. Pelo teorema dos números primos para progressões aritméticas (veja teorema D.9),

$$\pi(x, q, 1) := \sum_{\substack{p \leq x \\ p \equiv 1(\text{mod } q)}} 1 \sim \frac{x}{\varphi(q) \log x} = \frac{x}{(q-1) \log x}.$$

Ou seja, $p \equiv 1 \pmod{q}$ é verdade para primos p com frequência $1/(q-1)$. Agora, calculemos a probabilidade de um primo p satisfazer $a^{(p-1)/q} \equiv 1 \pmod{p}$. Afim de fazer isso, provaremos a seguinte

Proposição 2.2.1. *Tem-se que $a^{(p-1)/q} \equiv 1$ (mod p) se, e somente se, $x^q \equiv a$(mod p) admite solução (mod p).*

Demonstração. De fato, se m é uma solução (mod p) de $x^q \equiv a(\text{mod } p)$, então $m^{p-1} \equiv a^{(p-1)/q} \pmod{p}$. Como p não divide m , $m^{p-1} \equiv 1 \pmod{p}$ pelo pequeno teorema de Fermat. Logo, $a^{(p-1)/q} \equiv 1 \pmod{p}$. Reciprocamente, se $a^{(p-1)/q} \equiv 1 \pmod{p}$, escrevamos $a = \gamma^k$ com γ uma raiz primitiva (mod p). Dessa forma, $\gamma^{k(p-1)/q} \equiv 1 \pmod{p}$, o que implica que $q|k$, já que a potência de uma raiz primitiva é congruente a 1 (mod p) se o expoente for um múltiplo de $p-1$. Assim, $k = bq$ e $(\gamma^b)^q \equiv a \pmod{p}$, o que mostra que $x^q \equiv a(\text{mod } p)$ admite solução. Além disso, se $\alpha_1, \ldots, \alpha_q$ são soluções distintas módulo p de $x^q \equiv 1 \pmod{p}$ então $\alpha_1\gamma^b \ldots \alpha_q\gamma^b$ são todas as soluções distintas de $x^q \equiv a \pmod{p}$. □

Pela proposição 2.2.1, $a^{(p-1)/q} \equiv 1 \pmod{p}$ se, e somente se, $\overline{a} \in (\mathbb{F}_p^*)^q := \{y^q; y \in \mathbb{F}_p^*\}$[2] que tem cardinalidade $\frac{p-1}{q}$. Portanto, $a^{(p-1)/q} \equiv 1 \pmod{p}$ ocorre com probabilidade

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

[2]Aqui usamos $\mathbb{F}_p$ como uma notação para $\mathbb{Z}_p$, o conjunto das classes de congruência módulo p que munido das operações de adição e multiplicação para classes de congruência se torna um corpo.

Se os eventos forem independentes, a probabilidade de eles ocorrerem é $1/q(q-1)$. Para garantir que a seja uma raiz primitiva (mod p), os eventos acima não podem ocorrer para qualquer que seja o q. Isso sugere uma probabilidade de

$$\prod_q \left(1 - \frac{1}{q(q-1)}\right) = A(a)$$

para tais primos.

Em geral, se h é o maior expoente tal que a é uma h-ésima potência perfeita, então para $q \mid h$, temos

$$a^{\frac{p-1}{q}} = b^{\frac{h(p-1)}{q}} \equiv 1 \pmod{p},$$

trivialmente. Com isso, se os eventos fossem independentes, a probabilidade deles ocorrerem simultaneamente é de $\frac{1}{q-1}$ e, portanto, o valor esperado para $A(a)$ seria

$$A(a) = \prod_{q \mid h} \left(1 - \frac{1}{q-1}\right) \prod_{q \nmid h} \left(1 - \frac{1}{q(q-1)}\right).$$

Observação: Na realidade, os eventos acima não são independentes. Por exemplo, se a é livre de quadrados e $a \equiv 1 \pmod 4$ então se p satisfaz $p \equiv 1 \pmod q$ e $a^{\frac{p-1}{q}} \equiv 1 \pmod p$ para cada primo $q \mid a$ então $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. De fato, note que p é quadrado módulo q para cada $q \mid a$. Pela lei de reciprocidade quadrática (ver [2], teorema 9.8) temos

$$\begin{aligned} \left(\frac{a}{p}\right) &= \prod_{q \mid a} \left(\frac{q}{a}\right) = \prod_{q \mid a} \left(\frac{p}{q}\right) (-1)^{\frac{(p-1)(q-1)}{4}} \\ &= (-1)^{\frac{p-1}{2} \sum_{q \mid a} \frac{q-1}{2}}. \end{aligned}$$

Como $a \equiv 1 \pmod 4$, segue que $\sum_{q \mid a} \frac{q-1}{2} \equiv \frac{a-1}{2} \equiv 0 \pmod 2$. Logo, $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) = 1 \pmod p$. Em casos como esse é necessário modificar a constante $A(a)$, o que será feito no capítulo 4. Para saber mais sobre esse assunto, veja, por exemplo, [23], [29] e [34].

2.3 Intuição de Artin

A motivação de Artin teve origem na teoria algébrica dos números. Ele observou que as condições

$$p \equiv 1 (\text{mod } q)$$

$$a^{(p-1)/q} \equiv 1 (\text{mod } p)$$

são satisfeitas se, e somente se, p se decompõe completamente na extensão $L_q = \mathbb{Q}(\zeta_q, a^{1/q})$, onde $\zeta_q = e^{\frac{2\pi i}{q}}$ é uma raiz primitiva da unidade. Para ver isso, lembremos do seguinte

Teorema 2.3.1. *Um primo se ramifica em um corpo de números K se, e somente se, ele*

divide o disc K (discriminante de K).

Demonstração. Ver [26], capítulo 13, teorema 1. □

No caso em que $K = \mathbb{Q}(\zeta_q)$, o anel de inteiros algébricos é $O_K = \mathbb{Z}[\zeta_q]$ (ver [26], seção 5.5), assim,

$$\begin{aligned} \text{disc } K = \text{disc}(1, \zeta_q, \ldots, \zeta_q^{q-2}) &= (-1)^{\frac{(q-1)(q-2)}{2}} N_{K/\mathbb{Q}}(\Phi_q'(\zeta_q)) \\ &= (-1)^{\frac{q-1}{2}} N_{K/\mathbb{Q}}(\Phi_q'(\zeta_q)). \end{aligned}$$

Para calcular $N_{K/\mathbb{Q}}(\Phi_q'(\zeta_q))$, derivamos em ambos lados da igualdade

$$(x-1)\Phi_q(x) = x^q - 1$$

para obter $\Phi_q(x) + (x-1)\Phi_q'(x) = qx^{q-1}$. Calculando em ζ_q e aplicando a norma, temos

$$N_{K/\mathbb{Q}}(\zeta_q - 1) N_{K/\mathbb{Q}}(\Phi_q'(\zeta_q)) = N_{K/\mathbb{Q}}(q\zeta_q^{q-1}) = q^{q-1}.$$

A norma $N_{K/\mathbb{Q}}(\zeta_q - 1)$ é dada por

$$N_{K/\mathbb{Q}}(\zeta_q - 1) = \prod_{j=1}^{q-1}(\zeta_q^j - 1) = \prod_{j=1}^{q-1}(1 - \zeta_q^j) = \Phi_q(1) = q.$$

Logo, $N_{K/\mathbb{Q}}(\Phi_q'(\zeta_q)) = q^{q-2}$ e o discriminante de K é $(-1)^{\frac{q-1}{2}} q^{q-2}$. Já que p não divide o disc K, segue do teorema 2.3.1 que p não se ramifica em K. Por isso,

$$pO_K = \mathfrak{p}_1 \ldots \mathfrak{p}_g,$$

com os graus de inércia todos iguais a f, já que K é uma extensão de Galois (veja teorema D.11). Ou seja, $N(\mathfrak{p}_j) = p^f$, para todo j.

Lema 2.3.2. *Sejam $K = \mathbb{Q}(\zeta_q)$, p um número primo diferente de q e $\mathfrak{p}$ um ideal primo de $\mathbb{Z}[\zeta_q]$ com norma $N(\mathfrak{p}) = p^f$. Então f é a ordem de p (mod q).*

Demonstração. Denotemos a ordem de p módulo q por $\text{ord}_q(p)$. Como $N(\mathfrak{p}) = p^f$, o grupo $(O_K/\mathfrak{p})^*$ é finito e consiste de raízes da unidade (teorema D.14), logo $\overline{1}, \overline{\zeta_q}, \ldots \overline{\zeta_q}^{q-1} \in (O_K/\mathfrak{p})^*$. Se $\overline{\zeta_q}^j = \overline{\zeta_q}^l$ com $j > l$, então $\zeta_q^{j-l} \equiv 1 \bmod \mathfrak{p}$ o que implica que $\mathfrak{p}|(\zeta_q^k - 1)$, onde $k = j - l$. Agora, como $\text{Gal}(K/\mathbb{Q}) = \{\sigma; \sigma : \zeta_q \longmapsto \zeta_q^{m_\sigma}\}$,

$$N((\zeta_q^k - 1)) = N_{K/\mathbb{Q}}(\zeta_q^k - 1) = \prod_{\sigma \in \text{Gal}(K/\mathbb{Q})} \sigma(\zeta_q^k - 1) = \Phi_q(1) = q$$

onde $\Phi_q(x)$ é o q-ésimo polinômio ciclotômico. Daí, segue que $p^f|q$, um absurdo. Logo, $|\langle\overline{\zeta_q}\rangle| = q$ e $q|(N(\mathfrak{p}) - 1)$. Assim, $p^f \equiv 1 \pmod q$ e $\text{ord}_q(p)|f$. Por outro lado, já

que $p^{\mathrm{ord}_q(p)} \equiv 1 \pmod{q}$, segue que $\zeta_q^{p^{\mathrm{ord}_q(p)}} = \zeta_q$. Dessa forma, se $\alpha \in O_K$, então $\alpha = \sum_{m=0}^{q-2} a_m \zeta_q^m$, com $a_m \in \mathbb{Z}$. Daí,

$$\alpha^{p^{\mathrm{ord}_q(p)}} \equiv \sum_{m=0}^{q-2} a_m \zeta_q^m = \alpha \pmod{p},$$

o que implica que

$$\alpha^{p^{\mathrm{ord}_q(p)}} \equiv \alpha \pmod{\mathfrak{p}}.$$

Assim, $O_K/\mathfrak{p} = \{\overline{\alpha};\ \overline{\alpha} \text{ é raiz de } x^{p^{\mathrm{ord}_q(p)}} - x\}$ e, portanto, $p^{\mathrm{ord}_q(p)} \geq N(\mathfrak{p}) = p^f$, donde segue que $\mathrm{ord}_q(p) \geq f$, o que prova o resultado. □

Daí, concluímos que $p \equiv 1 \pmod{q}$, se e somente se, p se decompõe completamente em K.

Teorema 2.3.3 (Kummer-Dedekind)**.** *Sejam K um corpo de números algébricos e $L|K$ uma extensão de grau n; sejam O_K e O_L os anéis de inteiros de K e L, respectivamente. Seja $L = K(\theta)$, com $\theta \in O_L$, e seja $F \in O_K[X]$ o polinômio mínimo de θ sobre K. Suponhamos ainda que uma das seguintes condições é satisfeita:*

(a) *O_K é um domínio de ideais principais.*

(b) *$O_L = O_K[\theta]$.*

Seja $\mathfrak{p}$ um ideal primo não-nulo de O_K, tal que, no caso (a), $\mathfrak{p}$ não divide de αO_K, com $\alpha = \det(c_{ij})$ onde $(c_{ij})_{n\times n}$ é a matriz de mudança entre uma O_K-base de O_L e $\{1, \theta, \ldots \theta^{n-1}\}$. Seja $\overline{F} = \prod_{i=1}^{g} \overline{G_i}^{e_i} \in (O_K/\mathfrak{p})[X]$, onde $G_i \in O_K[X]$, os polinômios $\overline{G_1}, \ldots, \overline{G_g}$ são distintos e irredutíveis sobre $O_K/\mathfrak{p}$, o grau de $\overline{G_i}$ é f_i, para $i = 1, \ldots g$. Então

$$\mathfrak{p}O_L = \prod_{i=1}^{g} \mathcal{Q}_i^{e_i}$$

onde $\mathcal{Q}_1, \ldots, \mathcal{Q}_g$ são ideais primos não-nulos de O_L e $[O_L/\mathcal{Q}_i : O_K/\mathfrak{p}] = f_i$ para todo $i = 1, \ldots, g$. Além disso, $\mathcal{Q}_i \cap O_K[\theta] = \mathfrak{p}O_K[\theta] + G_i(\theta)O_K[\theta]$ para $i = 1, \ldots, g$.

Demonstração. Ver [26], teorema 2 do capítulo 11. □

Seja $L = \mathbb{Q}(a^{1/q})$ e escrevamos $\theta = a^{1/q}$. Temos que O_L e $\mathbb{Z}[\theta]$ são $\mathbb{Z}$-módulos com mesma dimensão e $\mathbb{Z}[\theta] \subset O_L$. Seja $\{\beta_1, \ldots, \beta_q\}$ uma base de O_L e considere a base $\{1, \theta, \ldots, \theta^{q-1}\}$ de $\mathbb{Z}[\theta]$. Se C é a matriz tal que

$$\begin{pmatrix} 1 \\ \theta \\ \vdots \\ \theta^{q-1} \end{pmatrix} = C \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_q \end{pmatrix},$$

então $\mathrm{disc}(1,\theta,\ldots,\theta^{q-1}) = (\det C)^2 \mathrm{disc}(\beta_1,\ldots,\beta_q)$. Por outro lado, existem base $\{\gamma_1,\ldots,\gamma_q\}$ de O_L e inteiros $a_1,\ldots,a_q \in \mathbb{Z}$ tais que $\{a_1\gamma_1,\ldots,a_q\gamma_q\}$ é base de $\mathbb{Z}[\theta]$ (teorema D.15). Desse modo, $\det C = a_1 \ldots a_q = |\mathbb{Z}/a_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/a_q\mathbb{Z}| = [O_L : \mathbb{Z}[\theta]]$. Além disso, se $g(x) = x^q - a$, então temos a seguinte relação

$$\begin{aligned} \mathrm{disc}(1,\theta,\ldots,\theta^{q-1}) = (-1)^{\frac{q(q-1)}{2}} N_{L/\mathbb{Q}}(g'(\theta)) &= (-1)^{\frac{q(q-1)}{2}} N_{L/\mathbb{Q}}(q\theta^{q-1}) \\ &= (-1)^{\frac{q(q-1)}{2}} q^q a^{q-1}. \end{aligned}$$

Assim,

$$[O_L : \mathbb{Z}[\theta]]^2 \mathrm{disc}(\beta_1,\ldots,\beta_q) = (-1)^{\frac{q(q-1)}{2}} q^q a^{q-1}.$$

Como $p \neq q$ e $p \nmid a$, concluímos que $p \nmid [O_L : \mathbb{Z}[\theta]]$.

Teorema 2.3.4. *Sejam K e L corpos de números. Então os primos que dividem o discriminante de KL são os mesmos que dividem o produto $\mathrm{disc}\, K \cdot \mathrm{disc}\, L$.*

Demonstração. Ver [26], seção 13.2, página 253. □

Dos teoremas 2.3.1 e 2.3.4 concluímos que p não se ramifica em L_q. Como $p \equiv 1 \pmod q$ e $a^{\frac{p-1}{q}} \equiv 1 \pmod p$, $x^q \equiv a \bmod p$ possui q raízes (mod p). Logo, para cada ideal primo $\mathfrak{p}$ de O_K que está acima de p, $x^q \equiv a \pmod{\mathfrak{p}}$ tem q soluções e, portanto, pelo teorema 2.3.3, p se decompõe completamente em L_q. Reciprocamente, suponha que p se decompõe completamente em L_q. Pelo teorema 2.3.4, p não se ramifica em K e nem em L. Sejam $\mathfrak{p}$ um ideal de O_K que está acima de p e $\mathfrak{p}O_{L_q}$ o levantamento de $\mathfrak{p}$ a O_{L_q}. Cada divisor primo $\mathcal{B}$ de $\mathfrak{p}O_{L_q}$ é divisor primo de pO_{L_q} e, por isso, está acima de p, assim

$$1 = [O_{L_q}/\mathcal{B} : \mathbb{F}_p] = [O_{L_q}/\mathcal{B} : O_K/\mathfrak{p}] \cdot [O_K/\mathfrak{p} : \mathbb{F}_p],$$

o que implica que $p \equiv 1 \pmod q$. Agora, usando o mesmo argumento para um ideal primo $\mathfrak{q}$ de O_L, obtemos que $x^q \equiv a \pmod p$ tem solução, ou seja, $a^{\frac{p-1}{q}} \equiv 1 \pmod p$. Para concluir, Artin utilizou o teorema de Chebotarev, que enunciaremos a seguir.

Teorema 2.3.5 (Chebotarev)**.** *Seja L/K uma extensão de Galois finita de corpos de números e seja $\mathcal{C}$ uma classe de conjugação de $Gal(L/K)$. Seja*

$$P_{\mathcal{C}} = \left\{ \mathfrak{p} \in P(K); \mathfrak{p} \text{ não se ramifica em } L, \left(\frac{L/K}{\mathfrak{p}}\right) = \mathcal{C} \right\},$$

onde $P(K)$ é o conjunto de todos os ideais primos de O_K e $\left(\frac{L/K}{\mathfrak{p}}\right)$ é o símbolo de Artin em $\mathfrak{p}$. Então a densidade de Dirichlet (resp. natural) existe e é igual a $\frac{\#\mathcal{C}}{\#\mathrm{Gal}(L/K)}$, ou seja,

$$\lim_{s\to 1+} \frac{\sum_{\mathfrak{p}\in P_{\mathcal{C}}} \frac{1}{N(\mathfrak{p})^s}}{\sum_{\mathfrak{p}\in P(K)} \frac{1}{N(\mathfrak{p})^s}} = \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in P_{\mathcal{C}}; N(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{p} \in P(K); N(\mathfrak{p}) \leq x\}} = \frac{\#\mathcal{C}}{\#\mathrm{Gal}(L/K)}.$$

Voltaremos para esse teorema no capítulo 3.

Assim, se p se decompõe em L_q, então $\#(\frac{L_q/\mathbb{Q}}{(p)}) = 1$ e, portanto, pelo teorema de Chebotarev, a densidade dos primos que se decompõe em L_q é

$$\frac{1}{[L_q : \mathbb{Q}]} = \frac{1}{q(q-1)},$$

desde que a não seja uma q-ésima potência. Agora, a é uma raiz primitiva (mod p) se, e somente se, as condições acima não são válidas, ou seja, a é uma raiz primitiva se, e somente se, p não se decompõe completamente em L_q algum. Assim a densidade esperada de tais primos seria

$$\prod_q \left(1 - \frac{1}{q(q-1)}\right).$$

3 A Cota Superior do Crivo de Selberg

Os métodos de crivos tiveram origem nos trabalhos de Viggo Brun sobre a conjectura de Goldbach e a conjectura dos primos gêmeos. Qualquer crivo aritmético se baseia na seguinte ideia: dados um conjunto finito de inteiros $\mathcal{A}$, um conjunto de primos $\mathcal{P}$ e um número $z \geq 2$, se removermos de $\mathcal{A}$ todos aqueles elementos que são divisíveis por primos de $\mathcal{P}$ menores do que z, então os elementos não crivados de $\mathcal{A}$ podem ter divisores primos de $\mathcal{P}$ somente se esses são maiores do que ou iguais a z. O conjunto $\mathcal{A}$ é o conjunto a ser crivado e o conjunto de primos $\mathcal{P}$ é o conjunto de crivação. O objetivo de qualquer teoria de crivos é estimar o número $S(\mathcal{A}, \mathcal{P}, z)$ de elementos não crivados de $\mathcal{A}$. Neste capítulo falaremos de um crivo descoberto por Selberg na década de 1940 em sua pesquisa sobre os zeros da função zeta de Riemann.

3.1 Teorema de Selberg

Sejam $f \in \mathbb{Z}[X]$, M, N números inteiros. Sejam também $\mathcal{A} = \{f(n); 1 \leq n \leq N\}$ e $\mathcal{P} = \{p \in \mathbb{P};\ p \leq M\}$, onde $\mathbb{P}$ é o conjunto de todos os números primos. Nós iremos estimar

$$S(\mathcal{A}, \mathcal{P}, M) = \#\{f(n) \in \mathcal{A};\ p|f(n) \Rightarrow p > M \text{ para } p \in \mathbb{P}\}.$$

Se $P(M) = \prod_{p \leq M} p$, então

$$S(\mathcal{A}, \mathcal{P}, M) = \sum_{\substack{n \leq N \\ (f(n), P(M))=1}} 1 = \sum_{n \leq N} \sum_{d|(f(n), P(M))} \mu(d) = \sum_{d|P(M)} \mu(d) \sum_{\substack{n \leq N \\ d|f(n)}} 1.$$

Escrevendo $S(d) = \sum\limits_{\substack{n \leq N \\ d|f(n)}} 1$, temos $S(\mathcal{A}, \mathcal{P}, M) = \sum_{d|P(M)} \mu(d) S(d)$. Selberg observou que dada qualquer sequência (λ_d) de números reais com $\lambda_1 = 1$ tem-se

$$\sum_{d|k} \mu(d) \leq \left(\sum_{d|k} \lambda_d \right)^2.$$

Em vista disso,

$$\begin{aligned} S(\mathcal{A},\mathcal{P},M) &= \sum_{n\leq N}\sum_{d|(f(n),P(M))}\mu(d) \leq \sum_{n\leq N}\left(\sum_{d|(f(n),P(M))}\lambda_d\right)^2 \\ &= \sum_{n\leq N}\left(\sum_{d_1,d_2|(f(n),P(M))}\lambda_{d_1}\lambda_{d_2}\right) = \sum_{n\leq N}\sum_{d|(f(n),P(M))}\rho(d) \\ &= \sum_{d|P(M)}\rho(d)\sum_{\substack{n\leq N\\ d|f(n)}}1 = \sum_{d|P(M)}\rho(d)S(d), \end{aligned}$$

onde $\rho(d) = \sum_{\substack{[d_1,d_2]=d\\ d_1,d_2|(f(n),P(M))}} \lambda_{d_1}\lambda_{d_2}$ e $[d_1,d_2]$ =mmc(d_1,d_2). Seja

$$s(d) = \#\{f(n); d|f(n), n\leq d\}.$$

Observando que $f(jd+k)\equiv f(k) \pmod d$, $j\in\mathbb{N}$, vemos que

$$S(d) = s(d)\left[\frac{N}{d}\right] + r(d),$$

com $0\leq r(d)\leq s(d)$. Tendo em vista que $\left[\frac{N}{d}\right] = \frac{N}{d}-\epsilon$, com $0\leq\epsilon<1$, obtemos

$$S(d) = N\cdot\frac{s(d)}{d} + r(d) - \epsilon s(d) = Nq(d) + R(d),$$

onde $q(d) = \frac{s(d)}{d}$ e $R(d) = r(d)-\epsilon s(d)$. Temos ainda $|R(d)|\leq(1-\epsilon)s(d)\leq s(d) = dq(d)$.

Teorema 3.1.1. *Sejam f um polinômio com coeficientes inteiros, $m_1, m_2, \ldots, m_r$ inteiros positivos coprimos dois a dois e $m = m_1m_2\cdots m_r$. Então a congruência*

$$f(x)\equiv 0 \ (mod\, m) \tag{3.1}$$

tem uma solução se, e somente se, cada uma das congruências

$$f(x)\equiv 0 \ (mod\, m_i) \qquad (i=1,2,\ldots,r) \tag{3.2}$$

tem uma solução. Além disso, se $\nu(m)$ e $\nu(m_i)$ denotam o número de soluções de (3.1) e (3.2), respectivamente, então

$$\nu(m) = \nu(m_1)\nu(m_2)\cdots\nu(m_r). \tag{3.3}$$

Demonstração. Ver [2], teorema 5.28. □

Lema 3.1.2. *As funções s e q são multiplicativas.*

Demonstração. Sejam d_1, d_2 inteiros positivos relativamente primos. Observe que $s(d_1)$, $s(d_2)$ e $s(d_1d_2)$ são o número de soluções de $f(x) \equiv 0 \pmod{d_1}$, $f(x) \equiv 0 \pmod{d_2}$ e $f(x) \equiv 0 \pmod{d_1d_2}$, respectivamente. Logo, pelo teorema anterior

$$s(d_1d_2) = s(d_1)s(d_2),$$

ou seja, s é multiplicativa. Daí e de $q(d) = \frac{s(d)}{d}$, segue que q é também multiplicativa. □

Assim,

$$S(\mathcal{A}, \mathcal{P}, M) \leq \sum_{d|P(M)} \rho(d)S(d) = N \sum_{d|P(M)} \rho(d)q(d) + \sum_{d|P(M)} \rho(d)R(d).$$

O objetivo é escolher os λ_d $(d \geq 2)$ de forma que

$$\sum_{d|P(M)} \rho(d)q(d) = \sum_{d_1,d_2|P(M)} \lambda_{d_1}\lambda_{d_2}q([d_1, d_2]),$$

que é uma forma quadrática nos $\lambda'_d s$, seja mínima.

Lema 3.1.3. *Seja g uma função multiplicativa e sejam d_1 e d_2 inteiros positivos livres de quadrados. Então*

$$g([d_1, d_2])g((d_1, d_2)) = g(d_1)g(d_2).$$

Demonstração. Como d_1 e d_2 são livres de quadrados, $\frac{d_1}{(d_1,d_2)}$, $\frac{d_2}{(d_1,d_2)}$ e (d_1, d_2) são dois a dois coprimos. E como $[d_1, d_2](d_1, d_2) = d_1d_2$ e g é multiplicativa, segue que

$$g([d_1, d_2])g((d_1, d_2)) = g\left((d_1, d_2)\frac{d_1}{(d_1, d_2)}\frac{d_2}{(d_1, d_2)}\right)g((d_1, d_2)) = g(d_1)g(d_2).$$

□

Como q é multiplicativa, segue do lema 3.1.3 que

$$\sum_{d_1,d_2|P(M)} \lambda_{d_1}\lambda_{d_2}q([d_1, d_2]) = \sum_{d_1,d_2|P(M)} \lambda_{d_1}\lambda_{d_2}q(d_1)q(d_2)\frac{1}{q((d_1, d_2))}. \tag{3.4}$$

Vamos agora introduzir a função aritmética w:

$$w(d) = \frac{1}{q(d)}\prod_{p|d}(1 - q(p))$$

Lema 3.1.4. *w é multiplicativa.*

Demonstração. Sejam d_1 e d_2 relativamente primos. Temos que

$$\begin{aligned} w(d_1d_2) = \frac{1}{q(d_1d_2)} \prod_{p|d_1d_2} (1-q(p)) &= \frac{1}{q(d_1)} \frac{1}{q(d_2)} \prod_{p|d_1}(1-q(p)) \prod_{p|d_2}(1-q(p)) \\ &= w(d_1)w(d_2). \end{aligned}$$

□

Os números $w(d)$ são chamados de *pesos*. Observe que para $w(d)$ esteja bem definido, devemos ter $q(d) \neq 0$. Note ainda que $q(p) = 0$ para algum primo p é equivalente a $s(d) = 0$ que, por sua vez, é equivalente a $(f(n), p) = 1$ para todo $n \in \{1, \ldots, N\}$. Sendo assim, devemos excluir da definição de $P(M)$ esses primos. Também queremos que os pesos sejam não nulos. Para isso, devemos ter $q(p) \neq 1$ para todos os primos que dividem d. Observamos que $q(p) = 1$ é equivalente a $s(p) = p$ que também é equivalente a $p|f(n)$, para todo $n \in \{1, \ldots, N\}$. Com isso, devemos também excluir esses primos na definição de $P(M)$. Fazendo essas correções, temos que

$$P(M) = \prod_{\substack{p \leq M \\ q(p) \neq 0,1}} p.$$

Uma vez que

$$w(d) = \frac{1}{q(d)} \prod_{p|d}(1-q(p)) = \frac{1}{q(d)} \sum_{\delta|d} \mu(\delta)q(\delta) = \sum_{\delta|d} \frac{\mu\left(\frac{d}{\delta}\right)}{q(\delta)},$$

segue da fórmula de inversão de Möbius que $\frac{1}{q(d)} = \sum_{\delta|d} w(\delta)$. Usando isso em (3.4), obtemos

$$\sum_{d_1,d_2|P(M)} \lambda_{d_1}q(d_1)\lambda_{d_2}q(d_2) \sum_{\delta|(d_1,d_2)} w(\delta) = \sum_{\delta|P(M)} w(\delta)v(\delta)^2,$$

onde

$$v(\delta) = \sum_{\substack{d|P(M) \\ \delta|d}} \lambda_d q(d).$$

Novamente, pela fórmula de inversão de Möbius, tem-se

$$\lambda_\delta q(\delta) = \sum_{\substack{\delta|d \\ d|P(M)}} \mu(d/\delta)v(d).$$

Em particular, para $\delta = 1$, temos $1 = \sum_{d|P(M)} \mu(d)v(d)$. Assim, devemos minimizar $\sum_{\delta|P(M)} w(\delta)v(\delta)^2$ sujeita à restrição $\sum_{\delta|P(M)} \mu(\delta)v(\delta) = 1$ (com $v(\delta) = 0$ para $\delta > M$). Pelo método dos multiplicadores de Lagrange,

$$2w(\delta)v(\delta) = c\mu(\delta)$$

para algum escalar c. Assim,

$$v(\delta) = \frac{c\mu(\delta)}{2w(\delta)}$$

de modo que

$$\frac{c}{2}\sum_{\delta|P(M)}\frac{\mu(\delta)^2}{w(\delta)} = 1$$

e

$$c = \frac{2}{\sum_{\delta|P(M)}\frac{1}{w(\delta)}} = \frac{2}{W(M)},$$

com $W(M) = \sum_{\delta|P(M)}\frac{1}{w(\delta)}$. Portanto, o valor mínimo ocorre em $v(\delta) = \frac{\mu(\delta)}{W(M)w(\delta)}$ e é igual a

$$\sum_{\delta|P(M)} w(\delta)\left(\frac{\mu(\delta)}{W(M)w(\delta)}\right)^2 = \frac{1}{W(M)^2}\sum_{\delta|P(M)}\frac{1}{w(\delta)} = \frac{1}{W(M)}.$$

Assim,

$$S(\mathcal{A},\mathcal{P},M) \leq \frac{N}{W(M)} + \sum_{d|P(M)}|\rho(d)R(d)|.$$

Observe que

$$\sum_{d|P(M)}|\rho(d)R(d)| = \sum_{d_1,d_2|P(M)}|\lambda_{d_1}\lambda_{d_2}||R([d_1,d_2])|.$$

Lema 3.1.5. $|R([d_1,d_2])| \leq d_1d_2|q(d_1)q(d_2)|$.

Demonstração. Temos que

$$|R([d_1,d_2])| \leq [d_1,d_2]q([d_1,d_2]) = \frac{d_1d_2}{(d_1,d_2)}\frac{q(d_1)q(d_2)}{q(d_1,d_2)} \leq d_1d_2q(d_1)q(d_2),$$

pois $(d_1,d_2)q((d_1,d_2)) = s((d_1,d_2)) \geq 1$. □

Logo, pelo lema 3.1.5, temos

$$\begin{aligned}\sum_{d_1,d_2|P(M)}|\lambda_{d_1}\lambda_{d_2}||R([d_1,d_2])| &\leq \sum_{d_1,d_2|P(M)}|d_1\lambda_{d_1}q(d_1)||d_2\lambda_{d_2}q(d_2)| \\ &= \left(\sum_{d|P(M)} d|\lambda_d q(d)|\right)^2.\end{aligned}$$

Como $\lambda_d q(d) = \sum_{\substack{\delta | P(M) \\ d|\delta}} \mu(\delta/d)v(\delta)$, segue que

$$\begin{aligned} |\lambda_d q(d)| &\leq \sum_{\substack{\delta | P(M) \\ d|\delta}} |\mu(\delta/d)v(\delta)| \\ &= \sum_{\substack{\delta | P(M) \\ d|\delta}} \frac{1}{W(M)w(\delta)} \\ &= \frac{1}{W(M)w(d)} \sum_{\delta_1 | P(M)} \frac{1}{w(\delta_1)} \\ &= \frac{1}{w(d)}, \end{aligned}$$

onde escrevemos $\delta = d\delta_1$. Portanto,

$$\sum_{d_1, d_2 | P(M)} |\lambda_{d_1}\lambda_{d_2}||R([d_1, d_2])| \leq \left(\sum_{\substack{d|P(M) \\ d\leq M}} \frac{d}{w(d)} \right)^2 \leq (MW(M))^2,$$

uma vez que $v(d) = 0$ para $d > M$. Isso encerra a prova do

Teorema 3.1.6 (Selberg)**.** *Com as notações e hipóteses acima, temos*

$$S(\mathcal{A}, \mathcal{P}, M) \leq \frac{N}{W(M)} + (MW(M))^2,$$

com $W(M) = \sum_{\delta | P(M)} \frac{1}{w(\delta)}$.

3.2 Desigualdade de Brun-Titchmarsh

Nesta seção veremos uma aplicação do crivo de Selberg, a saber, a desigualdade de Brun-Titchmarsh. Seja $\pi(x; q, a) = \sum_{\substack{p \leq x \\ p \equiv a \pmod q}} 1$, ou seja, o número de primos menores ou iguais a x que são congruentes a $a \pmod q$. O teorema a seguir fornece uma estimativa para esse número.

Teorema 3.2.1 (Brun-Titchmarsh)**.** *Sejam a, q números naturais coprimos com $0 < a < q$, $0 < q < x$. Dado $\epsilon > 0$ existe $x_0 = x_0(\epsilon)$ tal que se $x > x_0$ então*

$$\pi(x; q, a) < (2 + \epsilon)\frac{x}{\varphi(q)\log(x/q)}.$$

Demonstração. Vamos aplicar o teorema de Selberg com $f(n) = nq + a$, $N = \left[\frac{x}{q} + 1\right]$ e $M = \left[\left(\frac{x}{q}\right)^{\frac{1}{2}-\epsilon'}\right] + 1$, onde $\epsilon' = \frac{\epsilon}{2(2+\epsilon)}$. Se $p \nmid q$, então existe somente um múltiplo de p

entre $q+a$, $2q+a$, $\ldots$, $pq+a$. De fato, se $iq+a \equiv jq+a \pmod{p}$, com $1 \leq i,j \leq p$, então $(i-j)q \equiv 0 \pmod{p}$ e, por conseguinte, $i \equiv j \pmod{p}$. Assim, $iq+a = jq+a$ e $q+a$, $2q+a$, $\ldots$, $pq+a$ é um sistem completo de resíduos (mod p). Daí, temos que $s(p)=1$, $q(p)=\frac{1}{p}$, $w(p)=\frac{1}{q(p)}(1-q(p))=p(1-\frac{1}{p})=\varphi(p)$ e $w(d)=\varphi(d)$ se $(d,q)=1$. Se $p \mid q$ então $iq+a \equiv a \pmod{p}$ com $1 \leq i \leq p$. Se $p \mid a$ então $p|(q,a)=1$, um absurdo. Assim, $s(p)=0$ e $q(p)=0$. Portanto,

$$P(M) = \prod_{\substack{p \leq M \\ p \nmid q}} p.$$

Temos ainda que

$$W(M) = \sum_{d|P(M)} \frac{1}{w(d)} = \sum_{d|P(M)} \frac{1}{\varphi(d)} = \prod_{\substack{p \leq M \\ p \nmid q}} \left(1 + \frac{1}{\varphi(p)}\right)$$

e

$$\prod_{\substack{p \leq M \\ p \nmid q}} \left(1 + \frac{1}{\varphi(p)}\right) = \prod_{\substack{p \leq M \\ p \nmid q}} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{\substack{p \leq M \\ p \nmid q}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots\right) \geq \sum_{\substack{m \leq M \\ (m,q)=1}} \frac{1}{m}.$$

Como $\varphi(q) = q\prod_{p|q}\left(1-\frac{1}{p}\right)$, segue que

$$\frac{q}{\varphi(q)} W(M) \geq \prod_{p|q} \left(1 - \frac{1}{p}\right)^{-1} \sum_{\substack{m \leq M \\ (m,q)=1}} \frac{1}{m} \geq \sum_{m \leq M} \frac{1}{m} \geq \log M.$$

Daí,

$$\frac{N}{W(M)} \leq \frac{Nq}{\varphi(q)\log M} \leq \frac{x}{\varphi(q)\left(\frac{1}{2}-\epsilon'\right)\log\frac{x}{q}}.$$

Observe que $\frac{1}{1/2-\epsilon'} = 2 + \frac{4\epsilon'}{1-2\epsilon'} = 2+\epsilon$. Assim,

$$\frac{x}{\varphi(q)\left(\frac{1}{2}-\epsilon'\right)\log\left(\frac{x}{q}\right)} = \frac{(2+\epsilon)x}{\varphi(q)\log\left(\frac{x}{q}\right)}.$$

Agora vamos estimar $(MW(M))^2$:

$$W(M) = \sum_{d|P(M)} \frac{1}{\varphi(d)} = \sum_{\substack{d|P(M) \\ (d,q)=1}} \frac{\mu(d)^2}{\varphi(d)} = \prod_{\substack{p \leq M \\ p \nmid q}} \left(1 + \frac{1}{p-1}\right) \leq \prod_{p \leq M} \left(1 - \frac{1}{p}\right)^{-1} \ll \log M,$$

[3] pela fórmula de Mertens (ver [31], página 17, teorema 11). Assim,

$$(MW(M))^2 \ll (M\log M)^2 \ll (x^{1/2-\epsilon'}\log(x/q))^2 = x^{1-2\epsilon'}\log^2\left(\frac{x}{q}\right).$$

Já que

$$\frac{x^{1-2\epsilon'}\log^2(x/q)}{x/\log(x/q)} = \frac{\log^3(x/q)}{x^{2\epsilon'}} \to 0,$$

quando $x \to \infty$, segue que

$$S(\mathcal{A},\mathcal{P},M) \ll \frac{(2+\epsilon)x}{\varphi(q)\log(x/q)},$$

para x suficientemente grande.

Por outro lado,

$$S(\mathcal{A},\mathcal{P},M) \geq \pi(Nq+a;q,a) - \pi(M).$$

Além disso, $\pi(M) \leq M \sim \left(\frac{x}{q}\right)^{1/2-\epsilon'}$. Portanto,

$$\pi(x;q,a) \leq \pi(x+a;q,a) < \frac{(2+\epsilon)x}{\varphi(q)\log\left(\frac{x}{q}\right)}.$$

□

[3] Escrevemos $f(x) \ll g(x)$, ou equivalentemente, $f(x) = O(g(x))$, quando existe uma constante C tal que $|f(x)| \leq Cg(x)$ para todos os valores de x sob consideração. Para mais detalhes veja [2], [5], [6] e [13].

4 A Conjectura de Artin, a Hipótese de Riemann Generalizada e o Teorema de Chebotarev

Em 1922, em sua tese de doutorado, o matemático russo Nikolai Grigor'evich Chebotarev (1894-1947) provou uma conjectura de Frobenius que é conhecida hoje como o teorema de densidade de Chebotarev. Esse teorema é o mesmo que enunciamos no primeiro capítulo: seja L/K uma extensão de Galois finita de corpos de números e seja $\mathcal{C}$ uma classe de conjugação de $\mathrm{Gal}(L/K)$. Seja

$$P_{\mathcal{C}} = \left\{ \mathfrak{p} \in P(K); \mathfrak{p} \text{ não se ramifica em } L, \left(\frac{L/K}{\mathfrak{p}}\right) = \mathcal{C} \right\},$$

onde $P(K)$ é o conjunto de todos os ideais primos de O_K e $\left(\frac{L/K}{\mathfrak{p}}\right)$ é o símbolo de Artin em $\mathfrak{p}$. Então a densidade de Dirichlet (resp. natural) existe e é igual a $\frac{\#\mathcal{C}}{\#\mathrm{Gal}(L/K)}$, ou seja,

$$\lim_{s\to 1+} \frac{\sum_{\mathfrak{p}\in P_{\mathcal{C}}} \frac{1}{N(\mathfrak{p})^s}}{\sum_{\mathfrak{p}\in P(K)} \frac{1}{N(\mathfrak{p})^s}} = \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in P_{\mathcal{C}}; N(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{p} \in P(K); N(\mathfrak{p}) \leq x\}} = \frac{\#\mathcal{C}}{\#\mathrm{Gal}(L/K)}.$$

Uma demonstração desse teorema pode ser encontrada em [17] ou em [33]. A técnica usada por Chebotarev foi fundamental para Artin demonstrar sua lei de reciprocidade, que hoje é considerado o principal resultado da Teoria de Corpos de Classes. Com o desenvolvimento das versões efetivas, o teorema de Chebotarev tem várias aplicações na Teoria dos Números Moderna e Geometria Aritmética. Algumas dessas aplicações podem ser encontradas em [27]. Para mais detalhes sobre o contexto histórico no qual o teorema de Chebotarev foi demonstrado, veja [30].

Neste capítulo veremos uma versão efetiva do teorema de Chebotarev, usando a Hipótese de Riemann Generalizada para certos corpos de números.

4.1 Versão Efetiva do Teorema de Chebotarev para L_k

Teorema 4.1.1. *Seja $P_a(x,k) = \#\{p \leq x; p$ se decompõe completamente em L_q para todo $q \mid k\}$. Então, admitindo a Hipótese de Riemann Generalizada, temos*

$$P_a(x,k) = \frac{Li(x)}{n} + O(\sqrt{x}\log(kx)).$$

A fim de provar este teorema veremos algumas propriedades da função zeta de Dedekind de um corpo de números.

Para um corpo de números K, definimos a função zeta de Dedekind de K por

$$\zeta_K(s) = \sum_{I \subset O_K} \frac{1}{N(I)^s} \tag{4.1}$$

com $\mathrm{Re}(s) > 1$ e $s = \sigma + it$. A seguir provaremos dois resultados sobre a função ζ_K como em [25].

Lema 4.1.2. *Seja f uma função complexa sobre o conjunto de todos os ideais de O_K e suponha que ela seja multiplicativa, isto é, para ideais relativamente primos I e J $(I + J = O_K)$ temos $f(IJ) = f(I)f(J)$. Suponha ainda que a série*

$$G(f,s) = \sum_{I \subset O_K} \frac{f(I)}{N(I)^s}$$

converge absolutamente em um semiplano $\sigma > C$. Então nesse semiplano temos a igualdade

$$G(f,s) = \prod_{\mathfrak{p} \subset O_K} \sum_{m=0}^{\infty} \frac{f(\mathfrak{p}^m)}{N(\mathfrak{p})^{ms}}.$$

Demonstração. Para um número real positivo T, seja A_T o conjunto dos ideais de O_K cujos ideais divisores primos tem suas normas menores ou iguais a T. Então

$$\prod_{\substack{\mathfrak{p} \\ N(\mathfrak{p}) \leq T}} \sum_{m=0}^{\infty} \frac{f(\mathfrak{p}^m)}{N(\mathfrak{p})^{ms}} = \sum_{I \in A_T} \frac{f(I)}{N(I)^s}$$

e

$$\left| \prod_{\substack{\mathfrak{p} \\ N(\mathfrak{p}) \leq T}} \sum_{m=0}^{\infty} \frac{f(\mathfrak{p}^m)}{N(\mathfrak{p})^{ms}} - \sum_{\substack{I \\ N(I) \leq T}} \frac{f(I)}{N(I)^s} \right| \leq \sum_{\substack{I \\ N(I) > T}} \left| \frac{f(I)}{N(I)^s} \right|,$$

que tende a zero quando T tende a infinito, já que $G(f,s)$ é absolutamente convergente com $\sigma > C$. Portanto,

$$\sum_{I \subset O_K} \frac{f(I)}{N(I)^s} = \prod_{\mathfrak{p}} \sum_{m=0}^{\infty} \frac{f(\mathfrak{p}^m)}{N(\mathfrak{p})^{ms}},$$

com $\sigma > C$. □

Proposição 4.1.3. *No semiplano $\sigma > 1$ a série (4.1) converge absolutamente, e a convergência é uniforme em todo subconjunto compacto contido nesse semiplano, e portanto $\zeta_K(s)$ é analítica aí. Além disso, nesse semiplano o produto infinito $P(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}$ converge e $P(s) = \zeta_K(s)$.*

Demonstração. Seja $[K : \mathbb{Q}] = n$. Como existem no máximo n ideais primos em O_K com uma norma dada e essa norma é uma potência de primo, a série $\sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^\sigma}$ é absolutamente convergente para $\sigma > 1$. Além disso, a série é uniformemente convergente em todo conjunto compacto, pois é majorada por

$$\sum_q \frac{n}{q^\sigma},$$

onde q percorre todas as potências de primos em $\mathbb{Z}$. Agora se $T > 0$, então

$$\sum_{\substack{I \\ N(I) \leq T}} \frac{1}{|N(I)|^s} \leq \prod_{\substack{\mathfrak{p} \\ N(\mathfrak{p}) \leq T}} \left(1 + \frac{1}{N(\mathfrak{p})^\sigma} + \frac{1}{N(\mathfrak{p})^{2\sigma}} + \cdots\right).$$

A série no lado direito da desigualdade acima não excede $1 + \frac{3}{N(\mathfrak{p})^\sigma}$, pois é igual a

$$1 + \frac{1}{N(\mathfrak{p})^\sigma - 1}$$

e

$$\frac{1}{N(\mathfrak{p})^\sigma - 1} \leq \frac{3}{N(\mathfrak{p})^\sigma} \Leftrightarrow N(\mathfrak{p})^\sigma \geq \frac{3}{2}.$$

Assim,

$$\sum_{\substack{I \\ N(I) \leq T}} \frac{1}{|N(I)|^s} \leq \prod_{\substack{\mathfrak{p} \\ N(\mathfrak{p}) \leq T}} \left(1 + \frac{3}{N(\mathfrak{p})^\sigma}\right) \leq B,$$

onde B é uma constante, pois a série $3\sum_{\mathfrak{p}} N(\mathfrak{p})^{-\sigma}$ converge uniformemente em todo subconjunto compacto do semiplano $\sigma > 1$. Isso mostra a primeira parte da proposição. A segunda parte segue diretamente do lema 4.1.2. □

Sejam $\sigma_1, \ldots, \sigma_n$ as imersões de K em $\mathbb{C}$. Se $\sigma_i(K) \subset \mathbb{R}$, dizemos que σ_i é uma imersão real; do contrário, dizemos que σ_i é uma imersão complexa. Como o conjugado complexo de uma imersão é uma imersão, podemos fazer uma indexação dos σ_i's de modo que $\sigma_1, \ldots, \sigma_{r_1}$ sejam as imersões reais e $\sigma_{r_1+1}, \ldots \sigma_n$ as imersões complexas onde σ_{r_1+j} e $\sigma_{r_1+r_2+j}$ são conjugados complexos e $j = 1, \ldots, r_2$. Dessa forma, existem $2r_2$ imersões complexas e $r_1 + 2r_2 = n$. Seja ainda $r = r_1 + r_2 - 1$.

Em [12], Erich Hecke demonstrou o seguinte:

Teorema 4.1.4 (Equação funcional para função zeta de Dedekind)**.** *Sejam K um corpo de números e r_1 e r_2 como definidos acima. Então tem-se*

(i) A função zeta de Dedekind $\zeta_K(s)$ admite uma continuação analítica a todo plano complexo com um pólo simples em $s = 1$.

(ii) A função $\zeta_K(s)$ satisfaz a equação funcional

$$A^s\Gamma^{r_1}\left(\frac{s}{2}\right)\Gamma^{r_2}(s)\zeta_K(s) = A^{1-s}\Gamma^{r_1}\left(\frac{1-s}{2}\right)\Gamma^{r_2}(1-s)\zeta_K(1-s),$$

onde $A = 2^{-r_2}\pi^{-\frac{n}{2}}\sqrt{|disc\ K|}$.

Uma demonstração desse teorema pode ser encontrada em [12], [20], teorema 154 e em [21], pág. 254. Voltemos para o caso em que o corpo é da forma $L_k = \mathbb{Q}(b^{\frac{1}{k_1}}, \zeta_k)$. Vamos obter uma cota superior, que é uniforme em relação a k na faixa $-\frac{3}{2} \leq \sigma \leq \frac{11}{2}$. Primeiro, temos que para $\sigma \geq 2$

$$\begin{aligned} |\zeta_{L_k}(s)| &\leq \sum_{I\subset O_{L_k}} \frac{1}{N(I)^\sigma} \leq \zeta_{L_k}(2) = \prod_{\mathfrak{p}\subset O_{L_k}} \left(1 - \frac{1}{N(\mathfrak{p})^2}\right)^{-1} \\ &\leq \prod_p \left(1 - \frac{1}{p^2}\right)^{-n} = \zeta(2)^n = \left(\frac{\pi^2}{6}\right)^n \end{aligned} \tag{4.2}$$

Antes de seguir em frente, vejamos a fórmula de Stirling para uma variável complexa.

Teorema 4.1.5. *Seja $s = \sigma + it$ uma variável complexa. Então tem-se que*

$$\log\Gamma(s) = \left(s - \frac{1}{2}\right)\log s - s + \frac{1}{2}\log 2\pi + O\left(\frac{1}{|s|}\right),$$

quando $|s| \to \infty$, uniformemente com $|arg\ s| \leq \pi - \delta$, com $\delta > 0$ e o ramo do logaritmo é o principal.

Como consequência tem-se para um valor fixo de σ e $|t| \to \infty$ que

$$|\Gamma(\sigma + it)| \sim \sqrt{2\pi}e^{-\frac{\pi|t|}{2}}|t|^{\sigma-\frac{1}{2}}.$$

Para mais detalhes veja [1] e [32].

Dando continuidade, se $\sigma = -\frac{3}{2}$, temos do teorema 4.1.4, item (ii) que

$$|\zeta_{L_k}(s)| = |A|^4 \left|\frac{\Gamma\left(\frac{1-s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)}\right|^{r_1} \left|\frac{\Gamma(1-s)}{\Gamma(s)}\right|^{r_2} |\zeta_{L_k}(1-s)|.$$

Se $s = -\frac{3}{2} + it$, então

$$\left|\frac{\Gamma\left(\frac{1-s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)}\right| = \frac{|\Gamma\left(\frac{5}{4} - i\frac{t}{2}\right)|}{\left|\Gamma\left(-\frac{3}{4} + i\frac{t}{2}\right)\right|} \sim \frac{\sqrt{2\pi}e^{-\frac{\pi|t|}{4}}|t/2|^{\frac{3}{4}}}{\sqrt{2\pi}e^{-\frac{\pi|t|}{4}}|t/2|^{-\frac{5}{4}}} = \frac{|t|^2}{4} \sim \frac{(|t|+2)^2}{4}$$

e

$$\left|\frac{\Gamma(1-s)}{\Gamma(s)}\right| = \frac{\left|\Gamma\left(\frac{5}{2} - it\right)\right|}{\left|\Gamma\left(-\frac{3}{2} + it\right)\right|} \sim \frac{\sqrt{2\pi}e^{-\frac{\pi|t|}{2}}|t|^2}{\sqrt{2\pi}e^{-\frac{\pi|t|}{2}}|t|^{-2}} = |t|^4 \sim (|t|+2)^4.$$

Daí, existe uma constante C_1 tal que

$$|\zeta_{L_k}(s)| \leq |A|^4 C_1^{r_1}(|t|+2)^{2r_1} C_1^{r_2}(|t|+2)^{4r_2}|\zeta_{L_k}(1-s)|.$$

Lembrando que $A = 2^{-r_2}\pi^{-\frac{n}{2}}\sqrt{|\text{disc } L_k|}$, $r_1 + 2r_2 = n$, $\text{Re}(1-s) = \frac{5}{2} > 2$ e usando (4.2), temos

$$|\zeta_{L_k}(s)| \leq |\text{disc } L_k|^2(|t|+2)^{2n}\left(\frac{\pi^2}{6}\right)^n C_1^n. \tag{4.3}$$

Mas,

$$\begin{aligned}
|\text{disc } L_k| &= \left|\text{disc}\left(\prod_{q|k_1}\mathbb{Q}(a^{\frac{1}{q}})\prod_{q|k}\mathbb{Q}(\zeta_q)\right)\right| \\
&\leq \left|\text{disc}\left(\prod_{q|k}\mathbb{Q}(\zeta_q)\right)^{[L_k:\mathbb{Q}(\zeta_k)]} \text{disc}\left(\prod_{q|k_1}\mathbb{Q}(a^{\frac{1}{q}})\right)^{[L_k:\mathbb{Q}(a^{\frac{1}{k_1}})]}\right| \\
&\leq \left|\left(\prod_{q|k}\text{disc}\,\mathbb{Q}(\zeta_q)^{\frac{\varphi(k)}{q}}\right)\right|^{[L_k:\mathbb{Q}(\zeta_k)]}\left|\left(\prod_{q|k_1}\text{disc}\,\mathbb{Q}(a^{\frac{1}{q}})^{\frac{k_1}{q}}\right)\right|^{[L_k:\mathbb{Q}(a^{\frac{1}{k_1}})]} \\
&\leq \left(\prod_{q|k} q^{\frac{(q-2)\varphi(k)}{q}}\right)^{[L_k:\mathbb{Q}(\zeta_k)]}\left(\prod_{q|k_1}|a|^{\frac{(q-1)k_1}{q}}q^{k_1}\right)^{[L_k:\mathbb{Q}(a^{\frac{1}{k_1}})]} \\
&\leq \left(\prod_{q|k} q\prod_{q|k_1}|a|q\right)^n \leq (|a|^{\omega(k)}k^2)^n = (k^{\frac{\log|a|\omega(k)}{\log k}}k^2)^n \leq k^{(\log|a|+2)n} \\
&= k^{C_2 n},
\end{aligned}$$

com $C_2 = \log|a| + 2$. Na igualdade acima usamos a proposição 5.1.4 e proposição D.16 e para as duas desigualdades seguintes usamos os teoremas D.12 e D.13. Assim, para

$\sigma = -\frac{3}{2}$,

$$\begin{aligned} |(s-1)\zeta_{L_k}(s)| &\leq \sqrt{\frac{25}{4}+t^2}k^{2nC_2}(|t|+2)^{2n}\left(\frac{\pi^2}{6}\right)^n C_1^n \\ &\leq (|t|+2)^{3n}k^{2nC_2}k^{n\left(\log\left(\frac{\pi^2}{6}\right)+\log C_1\right)} \\ &\leq (k(|t|+2))^{\left(2C_2+\log\left(\frac{\pi^2}{6}\right)+\log C_1\right)n} \\ &= ((|t|+2)k)^{C_3 n}, \end{aligned} \tag{4.4}$$

onde $C_3 = 2C_2 + \log(\pi^2/6) + \log C_1$. Para $\sigma = \frac{11}{2}$, temos por (4.2), $|\zeta_{L_k}(s)| \leq \left(\frac{\pi^2}{6}\right)^n$. Além disso, temos $|s-1| \leq (|t|+2)^{\frac{3n}{2}}$. Com isso, para $\sigma = \frac{11}{2}$, temos

$$\begin{aligned} |(s-1)\zeta_{L_k}(s)| &\leq \left(\frac{\pi^2}{6}\right)^n (|t|+2)^{\frac{3n}{2}} \\ &\leq k^{n\log\left(\frac{\pi^2}{6}\right)}(|t|+2)^{\frac{3n}{2}} \\ &\leq (k(|t|+2))^{C_3 n}. \end{aligned} \tag{4.5}$$

Seja $C_4 = [C_3] + 1$ e definamos a seguinte função

$$Z(s) = \frac{(s-1)\zeta_{L_k}(s)}{(s+2)^{C_4 n}}.$$

Sobre as retas $\sigma = -\frac{3}{2}$, $\sigma = \frac{11}{2}$, tem-se

$$\begin{aligned} |Z(s)| &= \left|\frac{(s-1)\zeta_{L_k(s)}}{(s+2)^{C_4 n}}\right| \leq \frac{(k(|t|+2))^{C_3 n}}{|s+2|^{C_4 n}} \\ &\leq k^{C_4 n}\frac{(|t|+2)^{C_4 n}}{|s+2|^{C_4 n}}. \end{aligned}$$

Como para $\sigma = -\frac{3}{2}$ e $\sigma = \frac{11}{2}$, $\frac{|t|+2}{|s+2|} \to 1$ quando $|t| \to \infty$, segue que para $|t|$ suficientemente grande, existe uma constante C_5 tal que $\frac{|t|+2}{|s+2|} \leq C_5$. Assim,

$$|Z(s)| \leq (C_5 k)^{C_4 n}. \tag{4.6}$$

Mas $Z(s)$ é uma função analítica para $-\frac{3}{2} \leq \sigma \leq \frac{11}{2}$ e de ordem finita. Logo pelo princípio de Phragmém-Lindelöf (veja teorema D.18), a desigualdade (4.6) permanece válida sobre a faixa $-\frac{3}{2} \leq \sigma \leq \frac{11}{2}$. Portanto,

$$\begin{aligned} |(s-1)\zeta_{L_k}(s)| &= |Z(s)||s+2|^{C_4 n} \leq (C_5 k)^{C_4 n}(|t|+2)^{2C_4 n} \\ &\leq k^{n(\log C_5 + C_4)}(|t|+2)^{2C_4 n} \\ &\leq (k(|t|+2))^{C_6 n}, \end{aligned} \tag{4.7}$$

onde $C_6 = \text{máx}\{\log C_5 + C_4, 2C_4\}$. Agora vamos obter uma cota inferior $|(s-1)\zeta_{L_k}(s)|$ com $\sigma = 2$. Temos que

$$\frac{1}{|\zeta_{L_k}(s)|} = \left|\prod_{\mathfrak{p}}\left(1 - \frac{1}{N(\mathfrak{p})^s}\right)\right| \leq \prod_{\mathfrak{p}}\left(1 + \frac{1}{N(\mathfrak{p})^2}\right) \leq \zeta_{L_k}(2),$$

o que implica para $\sigma = 2$

$$\frac{1}{|(s-1)\zeta_{L_k}(s)|} \leq \frac{1}{|\zeta_{L_k}(s)|} \leq \left(\frac{\pi^2}{6}\right)^n,$$

por (4.2). Assim,

$$|(s-1)\zeta_{L_k}(s)| \geq \left(\frac{\pi^2}{6}\right)^{-n}, \quad \text{com } \sigma = 2. \tag{4.8}$$

Essas cotas foram obtidas com intuito de encontrar informações no que diz respeito à distribuição vertical dos zeros complexos de $\zeta_{L_k}(s)$. Vamos denotar por $\rho = \beta + i\gamma$, com $0 < \beta < 1$, um zero não-trivial complexo de $\zeta_{L_k}(s)$. Denotemos ainda por $N(T)$, para um número real não-negativo T, o número de zeros ρ tais que $0 \leq \gamma \leq T$. Consideremos a função $\xi(s) = (s-1)\zeta_{L_k}(s)$ e definamos por $\nu(y)$ o número de zeros (não necessariamente complexos) de ξ no círculo com centro $2 + iT$ e raio y. Pela de Jensen (teorema D.17),

$$\int_0^{\frac{7}{2}} \frac{\nu(y)}{y} dy = \frac{1}{2\pi}\int_0^{2\pi} \log\left|\xi\left(2 + iT + \frac{7}{2}e^{i\theta}\right)\right| d\theta - \log|\xi(2+iT)|.$$

Por (4.7),

$$\begin{aligned}
\left|\xi\left(2 + iT + \frac{7}{2}e^{i\theta}\right)\right| &\leq \left(k\left(\left|T + \frac{7}{2}\text{sen}\,\theta\right| + 2\right)\right)^{C_6 n} \\
&\leq \left(k\left(T + \frac{11}{2}\right)\right)^{C_6 n} \\
&\leq (k^3(T+2)^3)^{C_6 n} \\
&= (k(T+2))^{3C_6 n}
\end{aligned}$$

e por (4.8), $|\xi(2+iT)| \geq \left(\frac{\pi^2}{6}\right)^{-n}$. Daí, segue que

$$\begin{aligned}
\int_0^{\frac{7}{2}} \frac{\nu(y)}{y} dy &\leq 3C_6 n \log(k(T+2)) + n\log\left(\frac{\pi^2}{6}\right) \\
&\leq C_7 n \log(k(T+2)),
\end{aligned}$$

onde $C_7 = 3C_6 + 1$. Por outro lado, temos

$$\int_0^{\frac{7}{2}} \frac{\nu(y)}{y} dy \geq \int_3^{\frac{7}{2}} \frac{\nu(y)}{y} dy \geq \nu(3)\int_3^{\frac{7}{2}} \frac{dy}{y} \geq \nu(3)\log\frac{7}{6}$$

e

$$\nu(3) \geq N(T+1) - N(T).$$

Logo,

$$N(T+1) - N(T) = O(n \log(k(T+2))). \tag{4.9}$$

A seguir, vamos introduzir uma função que está relacionada com $\zeta_{L_k}(s)$ e seus zeros, a saber,

$$\psi(x) = \psi(x,k) = \sum_{N(\mathfrak{p})^m \leq x} \log N(\mathfrak{p}).$$

Teorema 4.1.6 (A fórmula explícita)**.** *Para $x \geq \frac{3}{2}$, temos*

$$\psi(x) = x - (r \log x + a_0) - \frac{1}{2} r_1 \log\left(1 - \frac{1}{x^2}\right) - r_2 \log\left(1 - \frac{1}{x}\right) - \sum_{\rho} \frac{x^\rho}{\rho},$$

onde

$$a_0 = a_0(k),$$

a série no segundo membro converge uniformemente em qualquer intervalo de x que não contém um número inteiro.

Uma demonstração desse teorema pode ser encontrada em [20], teoremas 197 e 199.

Agora vamos assumir a hipótese de Riemann generalizada, que enunciamos a seguir.

Hipótese de Riemann Generalizada: A parte real β de todo zero complexo não-trivial $\rho = \beta + i\gamma$ da função zeta de Dedekind é igual a $\frac{1}{2}$ para todo corpo da forma L_k.

A fim de estimar $\psi(x)$ através da fórmula explícita, escreveremos ψ na seguinte forma

$$\psi(y) = y - a_0 - \sum_{\rho} \frac{y^\rho}{\rho} + O(n \log y), \tag{4.10}$$

com $y \geq \frac{3}{2}$, uma vez que $r_1, r_2, r \leq n$. Suponha por enquanto que x é da forma $j + \frac{1}{2}$, onde $j \geq 1$ e seja $x \leq y \leq x + \frac{1}{4}$. Como $\rho = \frac{1}{2} + i\gamma$, segue que

$$\left| \sum_{|\gamma| \leq x} \frac{y^\rho}{\rho} \right| \leq y^{\frac{1}{2}} \sum_{|\gamma| \leq x} \frac{1}{|\rho|} = O\left(x^{\frac{1}{2}} \sum_{0 \leq \gamma \leq x} \frac{1}{\gamma + 1} \right).$$

Já que

$$\sum_{0 \leq \gamma \leq x} \frac{1}{\gamma + 1} = \sum_{0 \leq \gamma \leq 1} \frac{1}{\gamma + 1} + \sum_{\mu=1}^{j} \sum_{\mu \leq \gamma \leq \mu+1} \frac{1}{\gamma + 1} \leq N(1) + \sum_{\mu=1}^{j} \frac{N(\mu+1) - N(\mu)}{\mu},$$

segue que

$$x^{\frac{1}{2}} \sum_{0\leq\gamma\leq x} \frac{1}{\gamma+1} = O\left(x^{\frac{1}{2}}\left(N(1) + \sum_{\mu=1}^{j} \frac{N(\mu+1)-N(\mu)}{\mu}\right)\right).$$

Como $\log(k(\mu+2)) = O(\log kx)$, segue por (4.9) que

$$x^{\frac{1}{2}}\left(N(1) + \sum_{\mu=1}^{j} \frac{N(\mu+1)-N(\mu)}{\mu}\right) = O\left(nx^{\frac{1}{2}}\log(kx)\left(1 + \sum_{\mu=1}^{j}\frac{1}{\mu}\right)\right).$$

Por fim, temos

$$1 + \sum_{\mu=1}^{j} \frac{1}{\mu} = O(\log x).$$

Portanto,

$$\left|\sum_{|\gamma|\leq x} \frac{y^\rho}{\rho}\right| \leq O(n\sqrt{x}\log(kx)\log x).$$

Daí e de (4.10),

$$\psi(x) = \psi(y) = y - a_0 - \sum_{|\gamma|>x} \frac{y^\rho}{\rho} + O(n\sqrt{x}\log(kx)\log x).$$

Integrando em relação a y no intervalo $[x, x+\frac{1}{4}]$ obtemos

$$\begin{aligned}
\frac{1}{4}\psi(x) &= \frac{1}{2}\left(x+\frac{1}{2}\right)^2 - \frac{x^2}{2} - \frac{a_0}{4} + \sum_{|\gamma|>x} \frac{x^{\rho+1} - (x+1/4)^{\rho+1}}{\rho(\rho+1)} \\
&+ O(n\sqrt{x}\log(kx)\log x) \\
&= \frac{x}{4} + \frac{1}{32} - \frac{a_0}{4} + \sum_{|\gamma|>x} \frac{x^{\rho+1} - (x+1/4)^{\rho+1}}{\rho(\rho+1)} + O(n\sqrt{x}\log(kx)\log x),
\end{aligned}$$

sendo a integração termo a termo justificada pela última afirmação no teorema 4.1.6. Assim,

$$\begin{aligned}
\psi(x) &= x + \frac{1}{8} - a_0 + 4\sum_{|\gamma|>x} \frac{x^{\rho+1} - (x+1/4)^{\rho+1}}{\rho(\rho+1)} + O(n\sqrt{x}\log(kx)\log x) \\
&= x - a_0 + O(n\sqrt{x}\log(kx)\log x) + O\left(x^{\frac{3}{2}}\sum_{\gamma>x}\frac{1}{\gamma^2}\right).
\end{aligned}$$

Agora, temos por (4.9)

$$\sum_{\gamma>x}\frac{1}{\gamma^2}\leq\sum_{\mu\geq j}\frac{N(\mu+1)-N(\mu)}{\mu^2}=O\left(n\sum_{\mu\geq j}\frac{\log(2k\mu)}{\mu^2}\right)=O\left(\frac{n\log(kx)}{x}\right).$$

Logo,

$$\psi(x)=x-a_0+O(n\sqrt{x}\log(kx)\log x).$$

Assim, para evitar o problema de determinar a magnitude de a_0 diretamente, concluímos que

$$\psi(x)=\psi(x)-\psi\left(\frac{3}{2}\right)=x+O(n\sqrt{x}\log(kx)\log x). \tag{4.11}$$

Observando que $\psi(x)\leq\psi\left(([x]+1)+\frac{1}{2}\right)$ para $x\geq\frac{3}{2}$, concluímos que a fórmula (4.11) permanece válida removendo a restrição $x=j+\frac{1}{2}$.

Seja $\vartheta(x)=\sum_{N(\mathfrak{p})\leq x}\log(N(\mathfrak{p}))$. Temos que

$$\vartheta(x)=\psi(x)+O(n\sqrt{x})=x+O(n\sqrt{x}\log(kx)\log x).$$

Vamos denotar por $\pi(x,k)$ o número de ideais primos $\mathfrak{p}$ de O_{L_k} tais que $N(\mathfrak{p})\leq x$. Pela identidade de Abel (veja teorema D.6),

$$\begin{aligned}\pi(x,k) &= \frac{\vartheta(x)}{\log x}+\int_2^x\frac{\vartheta(t)}{t\log^2 t}dt\\ &= \frac{x}{\log x}+O(nx^{\frac{1}{2}}\log(kx))+\int_2^x\frac{dt}{\log^2 t}+O\left(n\int_2^x\frac{\log(kt)}{\sqrt{t}\log t}dt\right)\\ &= \int_2^x\frac{dt}{\log t}+O(n\sqrt{x}\log(kx))\\ &= \mathrm{Li}(x)+O(n\sqrt{x}\log(kx)).\end{aligned} \tag{4.12}$$

Para concluir a demonstração do teorema 4.1.1, vamos estabelecer uma relação entre $\pi(x,k)$ e $P_a(x,k)$. Escrevamos

$$\pi(x,k)=\Omega(x,k)+\Omega'(x,k),$$

onde $\Omega(x,k)$ conta os ideais primos de O_{L_k} com grau relativo 1 que não dividem ak (isto é, que não contêm $(ak)O_{L_k}$) e $\Omega'(x,k)$ contam os demais ideais primos. Se p é um número primo tal que $(ak,p)=1$, então p não divide o discriminante de L_k e por isso p não se ramifica em L_k. Além disso, como L_k é uma extensão de Galois, os ideais primos que dividem pO_{L_k} têm o mesmo grau relativo, portanto, temos que

$$\Omega(x,k)=nP_a(x,k).$$

Temos ainda que

$$\begin{aligned}\Omega'(x,k) = &\ \# \ (\{\mathfrak{p} \subset O_{L_k};\ N(\mathfrak{p}) = p \leq x,\ (p, ak) = p\} \\ &\cup \ \{\mathfrak{p} \subset O_{L_k};\ N(\mathfrak{p}) = p^f \leq x,\ f \geq 2\}),\end{aligned}$$

logo,

$$\begin{aligned}\Omega'(x,k) &\leq n\omega(ak) + n\#\{p^f \leq x;\ f \geq 2\} \\ &\leq n\omega(ak) + n\sum_{p^2 \leq x} 1.\end{aligned}$$

Das duas relacões acima, obtemos

$$nP_a(x,k) = \pi(x,k) + O(n\omega(k)) + O(n\sqrt{x}).$$

Daí e de (4.12) segue que

$$P_a(x,k) = \frac{1}{n}\mathrm{Li}(x) + O(\sqrt{x}\log(kx)),$$

como queríamos demonstrar.

5 O Teorema de Hooley

Em 1967, Christopher Hooley (ver [14]), assumindo a hipótese de Riemann generalizada para certos corpos de números, demonstrou a conjectura de Artin e uma fórmula assintótica para $N_a(x)$, o número de primos p menores ou iguais a x para os quais a é uma raiz primitiva (mod p). Neste capítulo apresentaremos a demonstração de Hooley para a conjectura de Artin.

5.1 O Teorema e Demonstração

O enunciado do teorema é o seguinte:

Teorema 5.1.1 (Hooley, 1967)**.** *Assuma que a hipótese de Riemann generalizada é verdadeira para a função zeta de Dedekind sobre corpos de Galois da forma $\mathbb{Q}(b^{\frac{1}{k_1}}, \zeta_k)$, onde k é livre de quadrados e $k_1 \mid k$. Então temos:*

(a) Para qualquer inteiro não nulo a diferente de -1 e de um quadrado perfeito, seja $N_a(x)$ o números de primos p menores ou iguais que x para os quais a é uma raiz primitiva (mod p). Seja também a_1 a parte livre de quadrados de a, seja h o maior inteiro com a propriedade que a é uma h-ésima potência e seja

$$C(h) = \prod_{q \mid h} \left(1 - \frac{1}{q-1}\right) \prod_{q \nmid h} \left(1 - \frac{1}{q(q-1)}\right).$$

Então, se $a_1 \not\equiv 1$ (mod 4), temos

$$N_a(x) = C(h)\frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x}\right),$$

quando $x \to \infty$, enquanto, se $a_1 \equiv 1$ (mod 4), temos

$$N_a(x) = C(h)\left(1 - \mu(|a_1|) \prod_{\substack{q \mid h \\ q \mid a_1}} \frac{1}{q-2} \prod_{\substack{q \nmid h \\ q \mid a_1}} \frac{1}{q^2-q-1}\right) \frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x}\right),$$

quando $x \to \infty$.

(b) Se a é diferente de -1 e de um quadrado perfeito, então existem infinitos primos p para os quais a é uma raiz primitiva (mod p).

Vamos denotar as condições

$$p \equiv 1 \pmod{q}, \qquad a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$$

por $R(q,p)$. Assim, a é uma raiz primitiva se, e somente se, $R(q,p)$ for falsa para todo primo q. Tendo em vista que há dois primos variando, vamos definir para $z < x$,

$$N_a(x,z) = \#\{p \leq x; p \nmid a \text{ e } R(q,p) \text{ é falsa, para todo } q \leq z\},$$

$$M_a(x,z_1,z_2) = \#\{p \leq x; p \nmid a \text{ e } R(q,p) \text{ é verdadeira para algum } q \in (z_1,z_2]\}.$$

Agora, se $p \leq x$ é tal que a é uma raiz primitiva (mod p), então em particular $R(q,p)$ não é válida para todo $q \leq z$, logo $N_a(x) \leq N_a(x,z)$. Além disso, se $p \leq x$ é tal que $R(q,p)$ não é válido para $q \leq z$, então ou $R(q,p)$ é falsa para todo primo $q \leq x-1$ ou $R(q,p)$ é verdadeira para algum primo $q \in (z, x-1]$. Assim,

$$N_a(x,z) \leq N_a(x) + M_a(x,z,x-1).$$

Daí, segue que

$$N_a(x) = N_a(x,z) + O(M_a(x,z,x-1)).$$

Na seção 1.3 vimos que $R(q,p)$ é equivalente a p se decompor completamente em L_q. Assim,

$$N_a(x,z) = \#\{p \leq x; p \text{ não se decompõe completamente em } L_q, \forall q \leq z\}.$$

Para qualquer número livre de quadrados k defina

$$P_a(x,k) = \#\{p \leq x; R(q,p) \text{ é verdadeira } \forall q \mid k\}.$$

Pelo princípio de inclusão e exclusão temos para $k = \prod_{q \leq z} q$ que

$$N_a(x,z) = \sum_{d \mid k} \mu(d) P_a(x,d). \tag{5.1}$$

Pela versão efetiva do teorema de Chebotarev aplicada ao corpo L_d temos que

$$P_a(x,d) = \frac{\mathrm{Li}(x)}{n(d)} + O(x^{1/2} \log dx),$$

onde $n(d) = [L_d : \mathbb{Q}]$. Se usássemos isso em (5.1), o termo de erro se tornaria muito

grande. Sendo assim, temos que estimar $N_a(x,z)$ para z muito menor do que x. Iremos escolher $z = \frac{\log x}{6}$. Além disso,

$$M_a(x,z,x-1) \leq M_a(x,z,\frac{\sqrt{x}}{\log^2 x}) + M_a(x,\frac{\sqrt{x}}{\log^2 x},\sqrt{x}\log x) + M_a(x,\sqrt{x}\log x,x-1).$$

Portanto, temos

$$\begin{aligned} N_a(x) &= N_a(x,z) + O(M_a(x,z,\frac{\sqrt{x}}{\log^2 x}) + M_a(x,\frac{\sqrt{x}}{\log^2 x},\sqrt{x}\log x) \\ &+ M_a(x,\sqrt{x}\log x,x-1)). \end{aligned} \tag{5.2}$$

Primeiro vamos estimar $M_a(x,\frac{\sqrt{x}}{\log^2 x},\sqrt{x}\log x)$. Se $p \leq x$ é tal que $R(q,p)$ é verdadeira para algum primo $q \in (\frac{\sqrt{x}}{\log^2 x},\sqrt{x}\log x]$, então p se decompõe completamente em L_q, logo

$$M_a(x,\frac{\sqrt{x}}{\log^2 x},\sqrt{x}\log x) \leq \sum_{\frac{\sqrt{x}}{\log^2 x} < q \leq \sqrt{x}\log x} P_a(x,q).$$

Se $p \leq x$ se decompõe completamente em L_q, então $p \equiv 1 \pmod q$ e, assim

$$P_a(x,q) \leq \sum_{\substack{p \leq x \\ p \equiv 1 \pmod q}} 1 = \pi(x,q,1).$$

Pela desigualdade de Brun-Titchmarsh

$$\pi(x,q,1) \leq \frac{Cx}{\phi(q)\log(x/q)},$$

para alguma constante C. Com isso,

$$M_a(x,\frac{\sqrt{x}}{\log^2 x},\sqrt{x}\log x) \leq \sum_{\frac{\sqrt{x}}{\log^2 x} < q \leq \sqrt{x}\log x} \pi(x,q,1) = O\left(\frac{x}{\log x} \sum_{\frac{\sqrt{x}}{\log^2 x} < q \leq \sqrt{x}\log x} \frac{1}{q}\right).$$

Pelo teorema de Mertens (ver teorema D.7),

$$\sum_{q \leq x} \frac{1}{q} = \log\log x + M + O\left(\frac{1}{\log x}\right),$$

para alguma constante M, logo

$$\begin{aligned}\sum_{\frac{\sqrt{x}}{\log^2 x}<q\leq\sqrt{x}\log x}\frac{1}{q} &= O\left(\log\left(\frac{\log(\sqrt{x}\log x)}{\log\left(\frac{\sqrt{x}}{\log^2 x}\right)}\right)\right)\\ &= O\left(\log\left(\frac{\frac{1}{2}\log x+\log\log x}{\frac{1}{2}\log x-2\log\log x}\right)\right).\end{aligned}$$

Como

$$\begin{aligned}\log\left(\frac{\frac{1}{2}\log x+\log\log x}{\frac{1}{2}\log x-2\log\log x}\right) &= \log\left(1+\frac{3\log\log x}{\frac{1}{2}\log x-2\log\log x}\right)\\ &\leq \frac{3\log\log x}{\frac{1}{2}\log x-2\log\log x}\end{aligned}$$

e

$$\frac{\log x}{\frac{1}{2}\log x-2\log\log x}\to 2$$

quando $x\to\infty$, segue que

$$\sum_{\frac{\sqrt{x}}{\log^2 x}<q\leq\sqrt{x}\log x}\frac{1}{q}=O\left(\frac{\log\log x}{\log x}\right).$$

Portanto,

$$M_a(x,\frac{\sqrt{x}}{\log^2 x},\sqrt{x}\log x)=O\left(\frac{x\log\log x}{\log^2 x}\right). \tag{5.3}$$

Agora vamos estimar $M_a(x,\sqrt{x}\log x,x-1)$. Por $R(q,p)$ ser válida temos que $a^{\frac{p-1}{q}}\equiv 1 \pmod p$ e, com maior razão,

$$a^{\frac{2(p-1)}{q}}\equiv 1 \pmod p.$$

Assim, como $q>\sqrt{x}\log x$ e $p\leq x$, segue que

$$\frac{p-1}{q}<\frac{x}{\sqrt{x}\log x}=\frac{\sqrt{x}}{\log x}.$$

Portanto, os primos p que são contados em $M_a(x,\sqrt{x}\log x,x-1)$ dividem o produto

$$\prod_{m<\sqrt{x}\log^{-1}x}(a^{2m}-1).$$

Por isso,

$$2^{M_a(x,\sqrt{x}\log^{-1}x,x-1)}<\prod_{p\text{ contado por }M_a(x,\sqrt{x}\log^{-1}x,x-1)}p<\prod_{m<\sqrt{x}\log^{-1}x}a^{2m},$$

e

$$\begin{aligned} M_a(x, \sqrt{x}\log^{-1} x, x-1) &< \frac{2\log|a|}{\log 2} \sum_{m<\sqrt{x}\log^{-1} x} m \\ &\leq \frac{2\log|a|}{\log 2} \frac{\sqrt{x}\log^{-1} x \cdot (\sqrt{x}\log^{-1} x + 1)}{2} \\ &= O\left(\frac{x}{\log^2 x}\right). \end{aligned} \tag{5.4}$$

Logo, de (5.2), (5.3) e (5.4) obtem-se

$$N_a(x) = N_a(x,z) + O\left(M_a(x,z,\frac{\sqrt{x}}{\log^2 x})\right) + O\left(\frac{x\log\log x}{\log^2 x}\right). \tag{5.5}$$

Ainda nos resta estimar $N_a(x,z)$ e $M_a(x,z,\frac{\sqrt{x}}{\log^2 x})$, lembrando que $z = \frac{\log x}{6}$. Para isto vamos escrevê-los em termos de $P_a(x,k)$. Em (5.1), vimos que

$$N_a(x,z) = \sum_{d|l} \mu(d) P_a(x,d),$$

com $l = \prod_{q\leq z} q$. E usando o mesmo argumento para obter a desigualdade para $M_a(x, \frac{\sqrt{x}}{\log^2 x}, \sqrt{x}\log x)$, encontramos

$$M_a(x,z,\frac{\sqrt{x}}{\log^2 x}) \leq \sum_{z<q\leq \frac{\sqrt{x}}{\log^2 x}} P_a(x,q). \tag{5.6}$$

Como

$$P_a(x,k) = \frac{\mathrm{Li}(x)}{n(k)} + O(x^{1/2}\log kx),$$

vamos nos empenhar então a calcular o grau $n(k)$ de L_k.

Seja h o maior inteiro positivo tal que a é uma h-ésima potência perfeita. Observamos que a é uma d-ésima potência se, e somente se, $d \mid h$. De fato, se $d \mid h$, então escrevendo $h = ld$ temos $a = b^h = (b^l)^d$. Reciprocamente, supondo que a é uma d-ésima potência, temos, $c^d = a = b^h$. Daí, segue que $c = b^{\frac{h}{d}}$. Se $b = (b')^l$, com $l \in \mathbb{N}$ e $l > 1$, de modo que $\frac{lh}{d} \in \mathbb{N}$, então $a = b^h = (b')^{lh}$, o que contradiz o fato de que h é o maior expoente tal que a é uma h-ésima potência perfeita. Portanto, $d \mid h$. Dessa forma, como a não é um quadrado perfeito, h é um número ímpar. Agora, seja

$$k_1 = \frac{k}{(h,k)}.$$

Como h é ímpar, (h,k) também o é, e por isso, k e k_1 têm a mesma paridade. Note que $p \equiv 1 \pmod q$ para todo $q \mid k$ é equivalente a $p \equiv 1 \pmod k$. Além disso, se $q \mid h$, então

$x^q = a$ admite solução inteira. Sendo assim, basta considerar $x^q \equiv a \pmod{p}$ quando $q \nmid h$.

Lema 5.1.2. *Sejam k_1, k_2 inteiros tais que $(k_1, k_2) = 1$. Se $x^{k_1} \equiv a \pmod{p}$, $x^{k_2} \equiv a \pmod{p}$ admitem solução, então $x^{k_1 k_2} \equiv a \pmod{p}$ admite solução.*

Demonstração. Sejam x_1 e x_2 soluções de $x^{k_1} \equiv a \pmod{p}$ e de $x^{k_2} \equiv a \pmod{p}$, respectivamente. Então, $x_1^{k_1 k_2} \equiv a^{k_2} \pmod{p}$ e $x_2^{k_1 k_2} \equiv a^{k_1} \pmod{p}$. Como $(k_1, k_2) = 1$, existem $r, s \in \mathbb{Z}$, tais que $rk_1 + sk_2 = 1$. Logo,

$$a = a^{rk_1} \cdot a^{sk_2} \equiv (x_2^r)^{k_1 k_2} \cdot (x_1^s)^{k_1 k_2} = (x_1^s x_2^r)^{k_1 k_2} \pmod{p}.$$

□

Assim, do lema 5.1.12 e argumentando indutivamente, concluímos que $x^q \equiv a \pmod{p}$ ser solúvel para todo divisor primo q de k_1 é equivalente a $x^{k_1} \equiv a \pmod{p}$ ter solução. Portanto, $P_a(x, k)$ conta os primos p que são relativamente primos com a que satisfazem as condições:

$$p \equiv 1 \pmod{k}; \quad x^{k_1} \equiv a \pmod{p} \text{ tem solução.} \tag{5.7}$$

Uma vez que os divisores primos q de k_1 não dividem h, a não é uma q-ésima potência e, assim, o polinômio $X^{k_1} - a$ é irredutível em $\mathbb{Q}[X]$(ver Apêndice A). Por isso, a extensão $L = \mathbb{Q}(a^{\frac{1}{k_1}})$ tem grau k_1 sobre $\mathbb{Q}$. Além disso, os fatores primos que dividem o discriminante de L ou dividem a ou dividem k_1. Com isso, p não se ramifica em L. Analogamente, se ζ_k é uma k-ésima raiz primitiva da unidade, então a extensão ciclotômica $K = \mathbb{Q}(\zeta_k)$ tem grau $\varphi(k)$ e tem discriminante que é formado apenas por divisores primos de k. Assim, p não se ramifica em K. Agora, a solubilidade de $x^{k_1} \equiv a \pmod{p}$ e a congruência $p \equiv 1 \pmod{k_1}$ são equivalentes ao fato de que $x^{k_1} \equiv a \pmod{p}$ tem exatamente k_1 soluções. Portanto, pelo teorema de Kummer-Dedekind p se decompõe completamente em L. Da mesma forma, $p \equiv 1 \pmod{k}$ é equivalente a $p \nmid k$ e ao fato de que p se decompõe completamente em K. Assim, (5.7) é equivalente a condição $p \nmid k$ e que p se decompõe completamente na seguinte extensão de Galois

$$L_k = KL = \mathbb{Q}(a^{\frac{1}{k_1}}, \zeta_k).$$

A seguir, vamos calcular o grau

$$n = n(k) = [L_k : \mathbb{Q}] \tag{5.8}$$

de L_k sobre $\mathbb{Q}$. Para isto, basta determinar $[L_k : K]$, pois

$$[L_k : \mathbb{Q}] = [L_k : K][K : \mathbb{Q}] = \varphi(k)[L_k : K]. \tag{5.9}$$

Lema 5.1.3. *Seja K uma extensão de Galois finita de F. Seja L uma extensão arbitrária de F. Suponha que K e L são subcorpos de algum outro corpo. Então $[KL : L]$ divide $[K : F]$.*

Demonstração. Ver [22], teorema 6.1.12 e corolário 6.1.13. □

Assim, como K é de Galois, segue do lema 5.1.3, que $[L_k : L]$ divide $[K : \mathbb{Q}]$ e, portanto, $[L_k : K]$ divide $[L : \mathbb{Q}] = k_1$. Escrevamos

$$k_1 = m[L_k : K]. \tag{5.10}$$

Seja q um fator primo de m e considere a extensão $K(a^{\frac{1}{q}})$ de K. Se $X^q - a$ for irredutível em K, então $[K(a^{\frac{1}{q}}) : K] = q$. Se $X^q - a$ for redutível em K, então $a = b^q$ com $b \in K$ e, assim, $a^{\frac{1}{q}} \in K$. Logo, $[K(a^{\frac{1}{q}}) : K] = 1$ ou q. Além disso, já que $a^{\frac{1}{q}} = (a^{\frac{1}{k_1}})^{\frac{k_1}{q}}$, $K \subseteq K(a^{\frac{1}{q}}) \subseteq L_k$ e, por isso,

$$[K(a^{\frac{1}{q}}) : K] \mid [L_k : K] = \frac{k_1}{m}.$$

Como $(k_1/m, q) = 1$, segue que $[K(a^{\frac{1}{q}}) : K] = 1$ e, consequentemente, $a^{\frac{1}{q}} \in K$. Já que $K/\mathbb{Q}$ é uma extensão abeliana ($\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/k\mathbb{Z})^*$), temos que $\mathbb{Q}(a^{\frac{1}{q}})/\mathbb{Q}$ é também uma extensão abeliana (ver [22], c corolário 6.1.11). Assim,

$$\mathbb{Q}(a^{\frac{1}{q}}) = \mathbb{Q}(a^{\frac{1}{q}}, \zeta_q),$$

o que implica que $q(q-1) = q$, ou seja, $q = 2$. Concluímos que $m = 1$ ou 2, sendo possível $m = 2$ se k_1 (e por sua vez k) for par.

Proposição 5.1.4. *Sejam K um corpo, $a \in K$, l, l_1 e l_2 números inteiros tais que $(l_1, l_2) = 1$ e $l = l_1 l_2$. Então $K(a^{\frac{1}{l}}) = K(a^{\frac{1}{l_1}}, a^{\frac{1}{l_2}})$.*

Demonstração. Como $a^{\frac{1}{l_1}} = (a^{\frac{1}{l}})^{l_2}$ e $a^{\frac{1}{l_2}} = (a^{\frac{1}{l}})^{l_1}$, segue que $K(a^{\frac{1}{l_1}}, a^{\frac{1}{l_2}}) \subseteq K(a^{\frac{1}{l}})$. Por outro lado, como $(l_1, l_2) = 1$, existem $r, s \in \mathbb{Z}$ tais que $rl_1 + sl_2 = 1$. Assim,

$$a^{\frac{1}{l}} = a^{\frac{l_1}{l}r + \frac{l_2}{l}s} = a^{\frac{s}{l_1}} \cdot a^{\frac{r}{l_2}},$$

portanto, $K(a^{\frac{1}{l}}) \subseteq K(a^{\frac{1}{l_1}}, a^{\frac{1}{l_2}})$ e o resultado segue. □

Observe que pela discussão acima, $m = 2$ implica que $\sqrt{a} \in K$. Por outro lado, se $\sqrt{a} \in K$, então $m = 2$. De fato, se $m = 1$, então $[L_k : K] = k_1$. Além disso, da proposição 5.1.4, podemos escrever $L_k = K(\sqrt[\frac{k_1}{2}]{a}, \sqrt{a})$. Como $\sqrt{a} \in K$, temos que $L_k = K(\sqrt[\frac{k_1}{2}]{a})$. Logo, $[L_k : K] \leq k_1/2 < k_1$, um absurdo. Agora seja

$$a = a_1 a_2^2,$$

onde a_1 é livre de quadrados e possivelmente negativo. Com isso, $m = 2$ se, e somente se, $\mathbb{Q}(\sqrt{a_1}) \subseteq K$.

Lema 5.1.5. *Seja p um número primo ímpar. Então o único subcorpo quadrático de $\mathbb{Q}(\zeta_p)$ é*

$$\mathbb{Q}\left(\sqrt{\left(\frac{-1}{p}\right)p}\right).$$

Demonstração. Como $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ é cíclico de ordem $p-1$, ele possui um único subgrupo de ordem $\frac{p-1}{2}$, ou seja, de índice 2. Pelo Teorema de Correspondência de Galois, existe um único subcorpo quadrático de $\mathbb{Q}(\zeta_q)$. Agora, observe que $\sqrt{\left(\frac{-1}{p}\right)p} \notin \mathbb{Q}$. Para concluir a demonstração temos que mostrar que

$$\mathbb{Q}\left(\sqrt{\left(\frac{-1}{p}\right)p}\right) \subseteq \mathbb{Q}(\zeta_p).$$

Para este fim, considere a soma

$$S = \sum_{\nu \in D} \left(\frac{\nu}{p}\right) \zeta_p^{\nu},$$

onde $D = \{\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}\}$. Com isso temos

$$S^2 = \sum_{\nu,\mu \in D} \left(\frac{\nu}{p}\right)\left(\frac{\mu}{p}\right) \zeta_p^{\nu+\mu},$$

pela multiplicatividade do símbolo de Legendre. Quando ν percorre os elementos de D, $\nu\mu$ também o faz para qualquer $\mu \in D$ fixado. Assim, substituindo ν por $\nu\mu$, obtemos

$$\begin{aligned} S^2 &= \sum_{\nu,\mu \in D} \left(\frac{\nu\mu^2}{p}\right) \zeta_p^{\mu(\nu+1)} = \sum_{\nu,\mu \in D} \left(\frac{\nu}{p}\right) \zeta_p^{\mu(\nu+1)} \\ &= \sum_{\mu \in D} \left(\frac{-1}{p}\right) \zeta_p^0 + \sum_{\substack{\nu \in D \\ \nu \neq -1}} \left(\frac{\nu}{p}\right) \sum_{\mu \in D} \zeta_p^{\mu(\nu+1)}. \end{aligned}$$

Como $1 + \zeta_p + \ldots + \zeta_p^{p-1} = 0$, $\sum_{\mu \in D} \zeta_p^{\mu(\nu+1)}$ é igual a -1. Logo,

$$\begin{aligned} S^2 &= \left(\frac{-1}{p}\right)(p-1) + (-1) \sum_{\substack{\nu \in D \\ \nu \neq -1}} \left(\frac{\nu}{p}\right) \\ &= \left(\frac{-1}{p}\right) p - \sum_{\nu \in D} \left(\frac{\nu}{p}\right) \\ &= \left(\frac{-1}{p}\right) p, \end{aligned}$$

pois a quantidade de resíduos quadráticos é igual a quantidade de resíduos não quadráticos. Portanto,

$$\sqrt{\left(\frac{-1}{p}\right)p} \in \mathbb{Q}(\zeta_p)$$

□

Agora, como k é livre de quadrados, disc K é ímpar. Além disso, como disc $\mathbb{Q}(\sqrt{a_1}) \mid$ disc K, devemos ter $a_1 \equiv 1 \pmod 4$ e $a_1 \mid k$. Por outro lado, suponha que $a_1 \equiv 1 \pmod 4$ e $a_1 \mid k$. Escrevamos

$$a_1 = \pm \prod_{i=1}^{r} p_i,$$

onde os p_i's são primos e definamos $q_i = \left(\frac{-1}{p_i}\right) p_i$. Note que $q_i \equiv 1 \pmod 4$ para todo i. Daí e de $a_1 \equiv 1 \pmod 4$, segue que

$$a_1 = \prod_{i=1}^{r} q_i.$$

Pelo lema 5.1.5, $\mathbb{Q}(\sqrt{q_i})$ é subcorpo de $\mathbb{Q}(\zeta_{p_i}) \subseteq K$, ou seja, q_i é um quadrado em K, para todo i. Assim, $a_1 = \prod_{i=1}^{r} q_i$ é também quadrado em $\mathbb{Q}(\zeta_k)$, isto é,

$$\mathbb{Q}(\sqrt{a_1}) \subseteq \mathbb{Q}(\zeta_k).$$

Portanto, $\mathbb{Q}(\sqrt{a_1}) \subseteq \mathbb{Q}(\zeta_k)$ é equivalente a $a_1 \equiv 1 \pmod 4$ e $a_1 \mid k$. Por fim, lembrando que $m = 2$ só é possível se k for par, temos de (5.8), (5.9) e (5.10) que

$$n(k) = \frac{k_1 \varphi(k)}{\varepsilon(k)}, \tag{5.11}$$

onde $\varepsilon(k)$ é dado por

$$\varepsilon(k) = \begin{cases} 2, & \text{se } 2a_1 \mid k \text{ e } a_1 \equiv 1 \pmod 4 \\ 1, & \text{caso contrário.} \end{cases} \tag{5.12}$$

Observação: Note que o caso em que $a_1 = 1$ tem que ser excluído, pois estamos supondo que a não é um quadrado perfeito.

Voltemos agora para o trabalho de estimar $N_a(x, z)$ e $M_a(x, z, \frac{\sqrt{x}}{\log^2 x})$. Por (5.1),

$$N_a(x, z) = \sum_{d \mid l} \mu(d) P_a(x, d).$$

Pela versão efetiva do teorema de Chebotarev, temos

$$\begin{aligned} N_a(x,z) &= \sum_{d|l} \mu(d) \left(\frac{\mathrm{Li}(x)}{n(d)} + O(\sqrt{x}\log x) \right) \\ &= \mathrm{Li}(x) \sum_{d|l} \frac{\mu(d)}{n(d)} + O\left(\sum_{d|l} \sqrt{x}\log x \right). \end{aligned}$$

Agora,

$$l = \prod_{q\leq z} q = e^{\vartheta(z)} \leq e^{2z} = x^{\frac{1}{3}},$$

onde $\vartheta(z) = \sum_{q\leq z} \log q$ é a função ϑ de Chebyshev que satisfaz $\vartheta(z) \leq 2z$. Daí,

$$\begin{aligned} N_a(x,z) &= \mathrm{Li}(x) \sum_{d|l} \frac{\mu(d)}{n(d)} + O\left(\sum_{d\leq x^{\frac{1}{3}}} \sqrt{x}\log x \right) \\ &= \mathrm{Li}(x) \sum_{d|l} \frac{\mu(d)}{n(d)} + O\left(\frac{x}{\log^2 x} \right), \end{aligned}$$

pois

$$\frac{x^{\frac{5}{6}}\log x}{\frac{x}{\log^2 x}} = \frac{\log^3 x}{x^{\frac{1}{6}}} \to 0,$$

quando $x \to \infty$. Como todos os números livre de quadrados k que não excedem z são do tipo d, temos de (5.11)

$$\begin{aligned} N_a(x,z) &= \mathrm{Li}(x) \sum_{k=1}^{\infty} \frac{\varepsilon(k)\mu(k)}{k_1\varphi(k)} + O\left(\mathrm{Li}(x) \sum_{k>z} \frac{1}{k\varphi(k)} \right) + O\left(\frac{x}{\log^2 x} \right) \\ &= \frac{x}{\log x} \sum_{k=1}^{\infty} \frac{\varepsilon(k)\mu(k)}{k_1\varphi(k)} + O\left(\frac{x}{\log^2 x} \right) + O\left(\frac{x}{z\log x} \right), \end{aligned}$$

pois $\mathrm{Li}(x) = O\left(\frac{x}{\log x}\right)$ e

$$\sum_{k>z} \frac{1}{k\varphi(k)} = O\left(\sum_{k>z} \frac{1}{k^2} \right) = O\left(\frac{1}{z} \right),$$

(confira [2], teorema 3.2, (c)). Portanto,

$$N_a(x,z) = \frac{A(a)x}{\log x} + O\left(\frac{x}{\log^2 x} \right), \tag{5.13}$$

onde $A(a) = \sum_{k=1}^{\infty} \frac{\varepsilon(k)\mu(k)}{k_1\varphi(k)}$. Agora vamos calcular $A(a)$. Se $a_1 \not\equiv 1 \pmod 4$, então $\varepsilon(k)$ é igual a 1 por (5.12). Como $\frac{1}{k_1\varphi(k)} = \frac{(h,k)}{k\varphi(k)}$ é uma função multiplicativa, segue da identidade

de Euler (teorema D.10) que

$$\begin{aligned} A(a) = \sum_{k=1}^{\infty} \frac{\mu(k)(h,k)}{k\varphi(k)} &= \prod_{q|h}\left(1-\frac{(h,q)}{q\varphi(q)}\right)\prod_{q\nmid h}\left(1-\frac{(h,q)}{q\varphi(q)}\right) \\ &= \prod_{q|h}\left(1-\frac{1}{q-1}\right)\prod_{q\nmid h}\left(1-\frac{1}{q(q-1)}\right) \\ &=: C(h). \end{aligned} \tag{5.14}$$

Para o caso $a_1 \equiv 1 \pmod 4$, dividiremos a soma $A(a)$ em duas somas, a saber, uma sobre os k's que são divisíveis por $2a_1$ e a outra sobre os que não são. Assim, por (5.12)

$$\begin{aligned} A(a) &= \sum_{k\not\equiv 0 \pmod{2|a_1|}} \frac{\mu(k)}{k_1\varphi(k)} + 2\sum_{k\equiv 0 \pmod{2|a_1|}} \frac{\mu(k)}{k_1\varphi(k)} \\ &= \sum_{k=1}^{\infty} \frac{\mu(k)}{k_1\varphi(k)} + \sum_{k\equiv 0 \pmod{2|a_1|}} \frac{\mu(k)(h,k)}{k\varphi(k)}. \end{aligned} \tag{5.15}$$

A primeira soma é $C(h)$ como vimos em (5.14). Agora, considere a segunda soma. Seja $k' = \frac{k}{2|a_1|}$. Para k livre de quadrados (os k's que não livres de quadrados não contribuem na soma, pois $\mu(k) = 0$), temos que $(k', 2|a_1|) = 1$. Assim, a segunda soma é igual a

$$\sum_{(k',2|a_1|)=1} \frac{\mu(2|a_1|k')(h,2|a_1|k')}{2|a_1|k'\varphi(2|a_1|k')} = \frac{\mu(2|a_1|)(h,2|a_1|)}{2|a_1|\varphi(2|a_1|)} \sum_{(k',2|a_1|)=1} \frac{\mu(k')(h,k')}{k'\varphi(k')}.$$

Agora, de $(k', 2|a_1|) = 1$, segue que $q \mid k'$, se e somente se, $q \nmid 2a_1$, portanto, pela identidade de Euler

$$\begin{aligned} \sum_{(k',2|a_1|)=1} \frac{\mu(k')(h,k')}{k'\varphi(k')} &= \prod_{\substack{q|h \\ q\nmid 2a_1}}\left(1-\frac{1}{q-1}\right)\prod_{\substack{q\nmid h \\ q\nmid 2a_1}}\left(1-\frac{1}{q(q-1)}\right) \\ &= \prod_{\substack{q|h \\ q\nmid 2a_1}}\frac{q-2}{q-1}\prod_{\substack{q\nmid h \\ q\nmid 2a_1}}\frac{q^2-q-1}{q(q-1)} \\ &= C(h)\prod_{\substack{q|h \\ q|2a_1}}\frac{q-1}{q-2}\prod_{\substack{q\nmid h \\ q|2a_1}}\frac{q(q-1)}{q^2-q-1}. \end{aligned}$$

Dessa forma, segue de (5.15) que

$$A(a) = C(h)\left(1 + \frac{\mu(2|a_1|)(h,2|a_1|)}{2|a_1|\varphi(2|a_1|)}\prod_{\substack{q|h \\ q|2a_1}}\frac{q-1}{q-2}\prod_{\substack{q\nmid h \\ q|2a_1}}\frac{q(q-1)}{q^2-q-1}\right)$$

Já que

$$\prod_{\substack{q|h\\ q|2a_1}}(q-1)\prod_{\substack{q\nmid h\\ q|2a_1}}(q-1)=\prod_{q|2a_1}(q-1)=\prod_{q|2a_1}\varphi(q)=\varphi(2|a_1|),$$

obtemos

$$A(a)=C(h)\left(1+\frac{\mu(2|a_1|)(h,2|a_1|)}{2|a_1|}\prod_{\substack{q|h\\ q|2a_1}}\frac{1}{q-2}\prod_{\substack{q\nmid h\\ q|2a_1}}\frac{q}{q^2-q-1}\right).$$

Finalmente, como h é ímpar,

$$\prod_{\substack{q|h\\ q|2a_1}}\frac{1}{q-2}=\prod_{\substack{q|h\\ q|a_1}}\frac{1}{q-2},$$

e

$$\begin{aligned}\prod_{\substack{q\nmid h\\ q|2a_1}}\frac{q}{q^2-q-1} &= \prod_{\substack{q\nmid h\\ q|2a_1}}q\prod_{\substack{q\nmid h\\ q|2a_1}}\frac{1}{q^2-q-1}\\ &= \frac{2|a_1|}{(h,2|a_1|)}\left(\frac{1}{2^2-2-1}\right)\prod_{\substack{q\nmid h\\ q|a_1}}\frac{1}{q^2-q-1}\end{aligned}$$

segue que

$$A(a)=C(h)\left(1-\mu(|a_1|)\prod_{\substack{q|h\\ q|a_1}}\frac{1}{q-2}\prod_{\substack{q\nmid h\\ q|a_1}}\frac{1}{q^2-q-1}\right).$$

Por fim, vamos estimar $M_a(x,z,\frac{\sqrt{x}}{\log^2 x})$. Lembremos que

$$M_a(x,z,\frac{\sqrt{x}}{\log^2 x})\leq\sum_{z<q\leq\frac{\sqrt{x}}{\log^2 x}}P_a(x,q).$$

Pelo teorema de Chebotarev, temos

$$\begin{aligned} M_a(x,z,\frac{\sqrt{x}}{\log^2 x}) &\leq \sum_{z<q\leq \frac{\sqrt{x}}{\log^2 x}} \left(\frac{\mathrm{Li}(x)}{q(q-1)} + O(\sqrt{x}\log x)\right) \\ &= O\left(\frac{x}{\log x}\sum_{q>z}\frac{1}{q^2}\right) + O\left(\sqrt{x}\log x \sum_{q\leq \frac{\sqrt{x}}{\log^2 x}} 1\right) \\ &= O\left(\frac{x}{z\log x}\right) + O\left(\frac{\left(\frac{\sqrt{x}}{\log^2 x}\right)\sqrt{x}\log x}{\log\left(\frac{\sqrt{x}}{\log^2 x}\right)}\right) \\ &= O\left(\frac{x}{\log^2 x}\right), \end{aligned}$$

pois

$$\frac{x\log^{-1} x}{\log\left(\sqrt{x}\log^{-2} x\right)}\frac{\log^2 x}{x} = \frac{\log x}{\log\left(\sqrt{x}\log^{-2} x\right)} \to 2$$

quando $x \to \infty$. Daí e de (5.5), obtemos

$$N_a(x) = \frac{A(a)x}{\log x} + O\left(\frac{x\log\log x}{\log^2 x}\right),$$

concluindo a demonstração do teorema 5.1.1.

Referências

[1] Andrews, G. E., Askey, R., and Roy, R. *Special Functions, volume 71 of Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1999.

[2] Apostol, T. M. *Analytic Number Theory*. Springer, 1976.

[3] Bateman, H. *Higher transcendental functions vol. 1*. Tata-Mcgrawhill Book Company Ltd., Bombay, 1953.

[4] Bilharz, H. Primdivisoren mit vorgegebener primitivwurzel. *Mathematische Annalen 114*, 1 (1937), 476–492.

[5] Cojocaru, A. C., and Murty, M. R. *An introduction to sieve methods and their applications*, vol. 66. Cambridge University Press, 2005.

[6] Davenport, H. *Multiplicative number theory*. No. 74. Springer, 1980.

[7] Dummit, D. S., and Foote, R. M. *Abstract algebra*, vol. 3. Wiley Hoboken, 2004.

[8] Gauss, C. F. *Disquisitiones Arithmeticae, 1801. English translation by Arthur A. Clarke*. Springer-Verlag, New York, 1986.

[9] Gupta, R., and Murty, M. R. A remark on Artin's conjecture. *Inventiones mathematicae 78*, 1 (1984), 127–130.

[10] Hardy, G. H., Riesz, M., et al. *The general theory of Dirichlet's series*. University press,, 1915.

[11] Heath-Brown, D. Artin's conjecture for primitive roots. *The Quarterly Journal of Mathematics 37*, 1 (1986), 27–38.

[12] Hecke, E. Über die zetafunktion beliebiger algebraischer zahlkörper. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse 1917* (1917), 77–89.

[13] Hildebrand, A. J. Asymptotic Analysis, Lectures Notes, Chapter 2, 2009. https://faculty.math.illinois.edu/~hildebr/595ama/ama-ch2.pdf.

[14] Hooley, C. On Artin's conjecture. *J. reine angew. Math 225*, 209-220 (1967), 248.

[15] Ivic, A. *The Riemann zeta-function: theory and applications*. Courier Corporation, 2012.

[16] Jacobson, N. *Basic Algebra, volume I*. Freeman, 1985.

[17] Jarden, M., and Fried, M. *Field arithmetic*. Springer, 2005.

[18] Jones, G. A., and Jones, J. M. *Elementary number theory*. Springer Science & Business Media, 1998.

[19] Karpilovsky, G. *Topics in field theory*, vol. 155. North-Holland, 1989.

[20] Landau, E. *Einführung in die elemetare und analytische Theorie der algebraischen Zahlen und der Ideale*. BG Teubner, 1918.

[21] Lang, S. *Algebraic number theory*. Springer, 1994.

[22] Lang, S. *Algebra revised third edition*, vol. 1. Springer Science and Media, 2002.

[23] Moree, P. Artin's primitive root conjecture–a survey. *Integers 12*, 6 (2012), 1305–1416.

[24] Murty, M. R. Artin's conjecture for primitive roots. *The Mathematical Intelligencer 10*, 4 (1988), 59–67.

[25] Narkiewicz, W. *Elementary and Analytic Theory of Algebraic Numbers*. Springer Science & Business Media, 2004.

[26] Ribenboim, P. *Classical theory of algebraic numbers*. Springer Science & Business Media, 2013.

[27] Serre, J.-P. Quelques applicatmmions du théoreme de densité de chebotarev. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques 54*, 1 (1981), 123–201.

[28] Stein, E. M., and Shakarchi, R. *Complex analysis. Princeton Lectures in Analysis, II*. Princeton University Press, Princeton, NJ, 2003.

[29] Stevenhagen, P. The correction factor in Artin's primitive root conjecture. *J. Théor. Nombres Bordeaux 15*, 1 (2003), 283–391.

[30] Stevenhagen, P., and Lenstra, H. W. Chebotarëv and his density theorem. *The Mathematical Intelligencer 18*, 2 (1996), 26–37.

[31] Tenenbaum, G. *Introduction to analytic and probabilistic number theory.* Cambridge University Press, 1995.

[32] Titchmarsh, E. C. *The theory of functions.* Oxford University Press, USA, 1939.

[33] Triantafillou, N. G. The Chebotarev Density Theorem. `https://math.mit.edu/~ngtriant/notes/chebotarev.pdf`.

[34] Voloch, J. F. Raizes Primitivas e a Conjectura de Artin. *Revista Matemática Universitária Nº 9/10* (1989), 153–158.

Apêndice A - Irredutibilidade de $X^n - a$

Neste capítulo estudaremos a irredutibilidade do polinômio $X^n - a$ em $K[X]$, onde K é um corpo arbitrário. Faremos isso seguindo [19] e [22].

Lema A.1. *Sejam K um corpo, a um elemento de K, e m, n inteiros positivos relativamente primos. Então $X^{mn} - a$ é irredutível sobre K se, e somente se, $X^m - a$ e $X^n - a$ são irredutíveis sobre K.*

Demonstração. Como $X^{mn} - a = (X^n)^m - a = (X^m)^n - a$, segue que se $X^{mn} - a$ é irredutível em $K[X]$, então $X^m - a$ e $X^n - a$ também são irredutíveis em $K[X]$. Reciprocamente, suponha que $X^m - a$ e $X^n - a$ são irredutíveis em $K[X]$. Denotemos por L o corpo de decomposição de $X^{mn} - a$ e seja $\alpha \in L$ uma raiz de $X^{mn} - a$. Então α^m é uma raiz de $X^n - a$ e α^n é uma raiz de $X^m - a$ o que mostra que $[K(\alpha^m) : K] = n$ e $[K(\alpha^n) : K] = m$. Assim, n e m dividem $[K(\alpha) : K]$ e portanto $mn|[K(\alpha) : K]$, pois $(m, n) = 1$. Por outro lado, α é uma raiz de $X^{mn} - a$, por isso, $[K(\alpha) : K] \leq mn$. Portanto, $[K(\alpha) : K] = mn$ e $X^{mn} - a$ é irredutível em $K[X]$. □

Lema A.2. *Sejam p um primo e a um elemento de um corpo K. Então $X^p - a$ é irredutível sobre K se, e somente se, $a \notin K^p$.*

Demonstração. Se $a = \alpha^p$ para algum $\alpha \in K$, então α é uma raiz de $X^p - a$ e, portanto,

$$X^p - a = (X - \alpha)(X^{p-1} + X^{p-2}\alpha + \ldots + \alpha^{p-1}).$$

Logo, $X^p - a$ não é irredutível. Reciprocamente, suponha que $a \notin K^p$. Sejam α uma raiz de $X^p - a$ e N a norma de $K(\alpha)$ a K. Se $[K(\alpha) : K] = d < p$, então como $a = \alpha^p$ segue que

$$N(a) = N(\alpha^p) = N(\alpha)^p.$$

Por outro lado, $N(a) = a^d$. Como $(d, p) = 1$, existem $r, s \in \mathbb{Z}$, tais que $rd + sp = 1$. Assim,

$$a = a^{rd+sp} = (N(\alpha)^r)^p(a^s)^p = (N(\alpha)^r a^s)^p,$$

o que implica que $a \in K^p$, o que é uma contradição. Logo, $[K(\alpha) : K] = p$ e $X^p - a$ é irredutível. □

Lema A.3. *Sejam p um primo, a um elemento de um corpo K e $X^p - a$ irredutível sobre K. Se α é uma raiz de $X^p - a$, então*

(a) Se p é ímpar, ou se $p = 2$ e car $K = 2$, então $\alpha \notin K(\alpha)^p$

(b) Se $p = 2$ e car $K \neq 2$, então $\alpha \in K(\alpha)^2$ se, e somente se, $a \in -4K^4$.

Demonstração. (a) Suponha por contradição que $\alpha = \beta^p$ para algum $\beta \in K(\alpha)$.

- **Caso em que car** $K = p$: Se $\beta \in K(\alpha)$, então

$$\beta = a_0 + a_1\alpha + \ldots + a_{p-1}\alpha^{p-1}$$

e

$$\beta^p = a_0^p + a_1^p\alpha^p + \ldots + a_{p-1}^p\alpha^{p(p-1)} \in K$$

o que implica $a \in K^p$, contradizendo o lema A.2.

- **Caso em que car** $K \neq p$: Se N é a norma de $K(\alpha)$ a K, então $a = N(\alpha^p) = N(\alpha)^p \in K^p$, uma contradição.

(b) Suponha que $\alpha = \beta^2$ com $\beta = b + c\alpha$, $b, c \in K$. De $\alpha = (b + c\alpha)^2$ obtemos

$$b^2 + ac^2 + (2bc - 1)\alpha = 0,$$

donde segue que $b^2 + ac^2 = 0$ e $2bc = 1$. Substituindo $c = \frac{1}{2b}$ em $b^2 + ac^2 = 0$, obtemos $a = -4b^4 \in -4K^4$. Reciprocamente, se $a = -4b^4$, $b \in K$, tome $c = \frac{1}{2b}$. Daí, temos que

$$(b + c\alpha)^2 = (b + \frac{1}{2b}\alpha)^2 = b^2 + \alpha - \frac{4b^4}{4b^2} = \alpha.$$

Portanto, $\alpha \in K(\alpha)^2$. □

Lema A.4. *Sejam K um corpo arbitrário, $n \geq 2$ um inteiro e p um primo. Seja a um elemento arbitrário em K*

(a) Se p é ímpar, ou $p = 2$ e car $K = 2$, então $X^{p^n} - a$ é irredutível sobre K se, e somente se, $a \notin K^p$.

(b) Se $p = 2$ e car $K \neq 2$, então $X^{2^n} - a$ é irredutível sobre K se, e somente se, $a \notin K^2$ e $a \notin -4K^4$.

Demonstração. (a) Se $a = b^p$ para algum $b \in K$, então $X^{p^n} - a = X^{p^n} - b^p$ é divisível por $X^{p^{n-1}} - b$. Reciprocamente, suponha que $a \notin K^p$. Para provar que $X^{p^n} - a$ é irredutível em $K[X]$, usaremos indução em n. Para $n = 1$, o resultado é verdade pelo lema A.2. Agora, seja α uma raiz de $X^{p^n} - a$ e seja $\beta = \alpha^{p^{n-1}}$. Então β é uma raiz de $X^p - a$ e, portanto, pelo lema A.2, $[K(\beta) : K] = p$. Além disso, temos que $\beta \notin K(\beta)^p$ pelo item (a) do lema A.3. Assim, pela hipótese de indução, $X^{p^{n-1}} - \beta$ é irredutível sobre $K(\beta)$ e, portanto, α tem grau p^{n-1} sobre $K(\beta)$. Logo, α tem grau p^n sobre K e $X^{p^n} - a$ é irredutível em $K[X]$.

(b) Se $a \in K^2$, então $X^{2^n} - a$ é redutível. Se $a \in -4K^4$, então $a = -4b^4$, para algum $b \in K$. Escrevendo $Y = X^{2^{n-2}}$, temos

$$X^{2^n} - a = Y^4 + 4b^4 = (Y^2 + 2bY + 2b^2)(Y^2 - 2bY + 2b^2).$$

Reciprocamente, suponha que $a \notin K^2$ e $a \notin 4K^4$. Vamos mostrar que $X^{2^n} - a$ é irredutível. Novamente, sejam α uma raiz de $X^{2^n} - a$ e $\beta = \alpha^{2^{n-1}}$. Como $a \notin K^2$ e β é uma raiz de $X^2 - a$, temos $[K(\beta) : K] = 2$, pelo lema A.2. Temos que mostrar que $[F(\alpha) : F(\beta)] = 2^{n-1}$. Para $n = 2$ isso é verdade, pois β não é um quadrado em $K(\beta)$, já que $a \notin -4K^4$ (ver lema A.3 (b)). Suponha $n > 2$. Novamente, temos que $\beta \notin K(\beta)^2$, pelo lema A.3 (b). Agora se $\beta = -4\gamma^4$ para algum $\gamma \in K(\beta)$, então

$$-a = N(\beta) = 16N(\gamma)^4,$$

donde segue que $\sqrt{-1} \in K(\beta)$ e, portanto, $\beta = (2\sqrt{-1}\gamma^2)^2 \in K(\beta)^2$, uma contradição. Logo, $\beta \notin -4K(\beta)^4$. Assim, por hipótese de indução $X^{2^{n-1}} - \beta$ é irredutível em $K(\beta)$, ou seja, $[K(\alpha) : K(\beta)] = 2^{n-1}$. Portanto, $[K(\alpha) : K] = 2^n$ e $X^{2^n} - a$ é irredutível. □

Teorema A.5. *Seja K um corpo e n um inteiro ≥ 2. Seja $a \in K$, $a \neq 0$. Então, $X^n - a$ é irredutível em $K[X]$ se, e somente se, $a \notin K^p$ para todos os primos p que dividem n e $a \notin -4K^4$ quando $4 \mid n$.*

Demonstração. Seja p^s a maior potência de um primo p que divide n. Se $a \in K^p$, então $X^{p^s} - a$ é redutível pelos lemas A.2 e A.4. Assim, $X^n - a$ é redutível, pelo lema A.1. Se $4|n$ e $a = -4b^4, b \in K$, então

$$X^n - a = X^n + 4b^4 = (X^{n/2} - 2bX^{n/4} + 2b^2)(X^{n/2} + 2bX^{n/4} + 2b^2).$$

Reciprocamente, suponha que $a \notin K^p$ para todos os primos p que dividem n e $a \notin -4K^4$ se $4 \mid n$. Escreva $n = p^s m$. Podemos supor indutivamente que $X^m - a$ é irredutível em $K[X]$. Além disso, pelos lemas A.2 e A.4, $X^{p^s} - a$ é irredutível. Como $(p, m) = 1$, segue do lema A.1 que $X^n - a$ é irredutível. □

Apêndice B - Equação funcional para a função zeta de Riemann

Seja $s = \sigma + it$ uma variável complexa. Definimos a função zeta de Riemann pela série

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

com $\sigma > 1$. A seguir mostraremos que $\zeta(s)$ admite uma continuação analítica a $\mathbb{C}\backslash\{1\}$ e satisfaz uma equação funcional que relaciona o argumento s com o argumento $1 - s$. Para fazer isto, usaremos uma outra função, a saber, a função gama.

A função gama, denotada por $\Gamma(s)$, pode ser definida por uma das seguintes expressões:

(1) $\Gamma(s) = \int_0^{\infty} e^y y^{s-1} dy, \quad \text{Re } s > 0.$

(2) $\Gamma(s) = \lim_{n\to\infty} \frac{n! n^s}{s(s+1)\cdots(s+n)}$, com $s \neq -n$ para n natural.

(3) $\frac{1}{\Gamma(s)} = s e^{\gamma s} \prod_{n=1}^{\infty} [(1+s/n)e^{-\frac{s}{n}}]$ onde $\gamma = \lim_{n\to\infty} \left(\sum_{n=1}^{m} \frac{1}{n} - \log m\right) = 0,5772156649\ldots$ é a constante de Euler-Mascheroni.

Em seguida, mostraremos alguns resultados envolvendo a função gama.

De (2) e (3), segue que a função gama é uma função analítica cujas singularidades finitas são $s = 0, -1, -2, \ldots$. De (1) temos que

$$\Gamma(s) = \int_0^1 e^{-y} y^{s-1}\, dy + \int_1^{\infty} e^{-y} y^{s-1}\, dy = P(s) + Q(s),$$

onde $Q(s)$ é uma função inteira. Expandindo e^{-y} em séries de potências e integrando termo a termo, obtemos

$$P(s) = \sum_{n=0}^{\infty} (-1)^n [n!(s+n)]^{-1}.$$

Por isso, $\frac{(-1)^n}{n!}$ é o resíduo de $\Gamma(s)$ nos pólos simples $s = -n$ $(n = 0, 1, 2, \ldots)$.

Agora, integrando (1) por partes, temos

$$\begin{aligned}\Gamma(s) &= \int_0^\infty e^{-y}y^{s-1}dy = -e^y\frac{y^s}{s}\Big|_0^\infty + \int_0^\infty e^{-y}\frac{y^s}{s}\,dy \\ &= \frac{1}{s}\int_0^\infty e^{-y}y^s dy = \frac{1}{s}\Gamma(s+1),\end{aligned}$$

o que implica

$$\Gamma(s+1) = s\Gamma(s).$$

Se n é um inteiro positivo, então

$$\begin{aligned}\Gamma(s+n) &= \Gamma(s+n-1+1) = (s+n-1)\Gamma(s+n-1) \\ &= s(s+1)\cdots(s+n-1)\Gamma(s).\end{aligned}$$

Além disso, como $\Gamma(1) = \int_0^\infty e^{-y}dy = 1$, segue que $\Gamma(n+1) = n!$. Temos ainda de (3) que

$$\begin{aligned}\Gamma(s)\Gamma(-s) &= \left(se^{\gamma s}\prod_{n=1}^\infty\left[\left(1+\frac{s}{n}\right)e^{-\frac{s}{n}}\right]\right)^{-1} \times \left((-s)e^{-\gamma s}\prod_{n=1}^\infty\left[\left(1-\frac{s}{n}\right)e^{\frac{s}{n}}\right]\right)^{-1} \\ &= -s^{-2}\prod_{n=1}^\infty\left(1-\frac{s^2}{n^2}\right)^{-1}\end{aligned}$$

e já que

$$\operatorname{sen}(\pi s) = \pi s\prod_{n=1}^\infty\left(1-\frac{s^2}{n^2}\right),$$

obtemos

$$\Gamma(s)\Gamma(-s) = -\frac{\pi}{s(\operatorname{sen}(\pi s))}. \tag{B.1}$$

Daí e de $\frac{\Gamma(1-s)}{\Gamma(-s)} = -s$, vem que

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\operatorname{sen}(\pi s)}.$$

Uma outra equação funcional que envolve a função gama é a fórmula de duplicação de Legendre:

$$\Gamma(s)\Gamma\left(s+\frac{1}{2}\right) = \frac{2\sqrt{\pi}}{2^{2s}}\Gamma(2s).$$

Para uma demonstração dessa fórmula veja [3].

Para relacionar a função gama com a função zeta, fazemos a substituição $y \mapsto \pi n^2 y$ para obter

$$\Gamma(s) = \int_0^\infty e^{-y}y^s\frac{dy}{y} = \int_0^\infty e^{-\pi n^2 y}\pi^s n^{2s}y^s\frac{dy}{y},$$

o que implica

$$\pi^{-s}\Gamma(s)\frac{1}{n^{2s}} = \int_0^\infty e^{-\pi n^2 y} y^s \frac{dy}{y}.$$

Agora somamos sobre todo $n \in \mathbb{N}$ para obter

$$\pi^{-s}\Gamma(s)\zeta(2s) = \int_0^\infty \sum_{n=1}^\infty e^{-\pi n^2 y} y^s \frac{dy}{y}.$$

A troca entre a integral e a série é legítima porque

$$\begin{aligned}\sum_{n=1}^\infty \int_0^\infty \left| e^{-\pi n^2 y} y^s \right| \frac{dy}{y} &= \sum_{n=1}^\infty \int_0^\infty e^{-\pi n^2 y} y^{\mathrm{Re}(s)} \frac{dy}{y} \\ &= \pi^{-\mathrm{Re}(s)}\Gamma(\mathrm{Re}(s))\zeta(2\mathrm{Re}(s)) < \infty.\end{aligned}$$

Agora a série sob a integral,

$$g(y) = \sum_{n=1}^\infty e^{-\pi n^2 y},$$

advém da série teta de Jacobi

$$\theta(s) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 s} = 1 + 2\sum_{n=1}^\infty e^{\pi i n^2 s},$$

ou seja,

$$g(y) = \frac{1}{2}(\theta(iy) - 1).$$

A função

$$Z(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

é chamada de função zeta completa. Obtemos assim a

Proposição B.1. *A função zeta completa $Z(s)$, admite a representação integral*

$$Z(s) = \frac{1}{2}\int_0^\infty (\theta(iy) - 1) y^{s/2} \frac{dy}{y}.$$

Seja $f : \mathbb{R}_+^* \to \mathbb{C}$ uma função sobre o grupo $\mathbb{R}_+^*$ de números reais positivos. Definimos a transformada de Mellin como sendo a integral imprópria

$$L(f, s) = \int_0^\infty (f(y) - f(\infty)) y^s \frac{dy}{y},$$

desde que o limite $f(\infty) = \lim_{y\to\infty} f(y)$ e a integral existam.

Teorema B.2 (Princípio de Mellin)**.** *Sejam $f, g : \mathbb{R}_+^* \to \mathbb{C}$ funções contínuas tais que*

$$f(y) = a_0 + O(e^{-cy^\alpha}), \quad g(y) = b_0 + O(e^{-cy^\alpha}),$$

para $y \to \infty$, com constantes positivas c, α. Se essas funções satisfazem a equação

$$f\left(\frac{1}{y}\right) = Cy^k g(y)$$

para algum número real $k > 0$ e algum número complexo $C \neq 0$, então tem-se:

(i) As integrais $L(f,s)$ e $L(g,s)$ converge absoluta e uniformemente se s varia em um domínio compacto arbitrário contido em $\{s \in \mathbb{C}; Re(s) > k\}$. Elas são portanto funções holomorfas sobre $\{s \in \mathbb{C}; Re(s) > k\}$. Elas admitem continuações analíticas a $\mathbb{C}\backslash\{0, k\}$.

(ii) Elas têm pólos simples em $s = 0$ e $s = k$ com resíduos

$$Res_{s=0} L(f,s) = -a_0, \quad Res_{s=k} L(f,s) = Cb_0, \quad respectivamente.$$

$$Res_{s=0} L(g,s) = -b_0, \quad Res_{s=k} L(g,s) = C^{-1}a_0.$$

(iii) Elas satisfazem a equação funcional

$$L(f,s) = L(g, k-s).$$

Demonstração. Se s varia sobre um subconjunto de $\mathbb{C}$, então a função $e^{-cy^\alpha}y^\sigma$, com $\sigma = \mathrm{Re}(s)$, é limitada para $y \geq 1$ por uma constante independente de σ. De $f(y) = a_0 + O(e^{-cy^\alpha})$, vem

$$\left|(f(y) - a_0)y^{s-1}\right| \leq Be^{-cy^\alpha}y^{\sigma+1}y^{-2} \leq \frac{B'}{y^2},$$

para todo $y \geq 1$, com constantes B, B'. A integral $\int_1^\infty (f(y) - a_0)y^{s-1}dy$ é majorada por $\int_1^\infty \frac{B'}{y^2}dy$ que é convergente e é independente de s. Portanto, ela converge absoluta e uniformemente, para todo s no subconjunto compacto. O mesmo vale para $\int_1^\infty (g(y) - b_0)y^{s-1}dy$.

Agora seja $\mathrm{Re}(s) > k$. Dividimos o intervalo de integração $(0, \infty)$ em $(0, 1]$ e $(1, \infty)$ e escrevemos

$$L(f,s) = \int_1^\infty (f(y) - a_0)y^s \frac{dy}{y} + \int_0^1 (f(y) - a_0)y^s \frac{dy}{y}.$$

Para a segunda integral, a substituição $y \mapsto \frac{1}{y}$ e a equação $f\left(\frac{1}{y}\right) = Cy^k g(y)$ nos dão

$$\begin{aligned}
\int_0^1 (f(y) - a_0) y^s \frac{dy}{y} &= -a_0 \frac{y^s}{s}\Big|_0^1 + \int_0^1 f(y) y^s \frac{dy}{y} \\
&= -\frac{a_0}{s} + \int_1^\infty f\left(\frac{1}{y}\right) y^{-s} \frac{dy}{y} \\
&= -\frac{a_0}{s} + C\int_1^\infty (g(y) - b_0) y^{k-s-1} dy + C\int_1^\infty b_0 y^{k-s-1} dy \\
&= -\frac{a_0}{s} + C\int_1^\infty (g(y) - b_0) y^{k-s-1} dy - \frac{Cb_0}{k-s}.
\end{aligned}$$

Por isso, essa integral converge absoluta e uniformemente para $\mathrm{Re}(s) > k$. Portanto, obtemos

$$L(f, s) = -\frac{a_0}{s} + \frac{Cb_0}{s-k} + F(s),$$

onde

$$F(s) = \int_1^\infty [(f(y) - a_0) y^s + C(g(y) - b_0) y^{k-s}] \frac{dy}{y}.$$

De $f\left(\frac{1}{y}\right) = Cy^k g(y)$, vem $g\left(\frac{1}{y}\right) = C^{-1} y^k f(y)$. Assim, de forma similar temos

$$L(g, s) = -\frac{b_0}{s} + \frac{C^{-1} a_0}{s-k} + G(s),$$

onde

$$G(s) = \int_1^\infty [(g(y) - b_0) y^s + C^{-1}(f(y) - a_0) y^{k-s}] \frac{dy}{y}.$$

As integrais $F(s)$ e $G(s)$ convergem absoluta e localmente uniformemente sobre todo plano complexo, como vimos acima. Dessa forma, elas representam funções holomorfas e

$$F(s) = C\left[\int_1^\infty [C^{-1}(f(y) - a_0) y^s + (g(y) - b_0) y^{k-s}] \frac{dy}{y}\right] = CG(k-s).$$

Portanto, $L(f, s)$ e $L(g, s)$ foram continuadas à $\mathbb{C}\backslash\{0, k\}$ e temos

$$\begin{aligned}
L(f, s) &= -\frac{a_0}{s} + \frac{Cb_0}{s-k} + F(s) \\
&= C\left[\frac{b_0}{s-k} - \frac{C^{-1} a_0}{s} + G(k-s)\right] \\
&= C\left[\frac{b_0}{k-s} + \frac{C^{-1} a_0}{(k-s)-k} + G(k-s)\right] \\
&= L(g, k-s),
\end{aligned}$$

e o teorema está provado. □

Pode-se provar que para $s \in \mathbb{H} = \{s \in \mathbb{C};\ \mathrm{Im}(s) > 0\}$ a série $\theta(s)$ satisfaz

$$\theta\left(-\frac{1}{s}\right) = \sqrt{\frac{s}{i}}\theta(s) \tag{B.2}$$

(ver [6], pág. 63).

Teorema B.3. *A função zeta completa*

$$Z(s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

admite uma continuação analítica a $\mathbb{C}\backslash\{0,1\}$ *tem pólos simples em* $s = 0$ *e* $s = 1$ *com resíduos* -1 *e* 1*, respectivamente, e satisfaz a equação funcional*

$$Z(s) = Z(1-s).$$

Demonstração. Temos que

$$Z(2s) = \frac{1}{2}\int_0^\infty (\theta(iy) - 1)y^s\frac{dy}{y},$$

ou seja, $Z(2s)$ é a transformada de Mellin

$$Z(2s) = L(f,s)$$

da função $f(y) = \frac{1}{2}\theta(iy)$. Já que

$$\theta(iy) = 1 + 2e^{-\pi y}\left(1 + \sum_{n=2}^{\infty} e^{-\pi(n^2-1)y}\right)$$

tem-se $f(y) = \frac{1}{2} + O(e^{-\pi y})$. Pela fórmula de transformação (B.2)

$$\begin{aligned} f\left(\frac{1}{y}\right) &= \frac{1}{2}\theta\left(\frac{i}{y}\right) = \frac{1}{2}\theta\left(-\frac{1}{iy}\right) \\ &= \frac{1}{2}y^{\frac{1}{2}}\theta(iy) = y^{\frac{1}{2}}f(y). \end{aligned}$$

Pelo princípio de Mellin, $L(f,s)$ tem uma continuação holomorfa a $\mathbb{C}\backslash\{0,\frac{1}{2}\}$ e pólos simples em $s = 0, \frac{1}{2}$ com resíduos $-\frac{1}{2}$ e $\frac{1}{2}$, respectivamente, e satisfaz a equação funcional

$$L(f,s) = L(f,\frac{1}{2} - s).$$

Consequentemente, $Z(s) = L(f,\frac{s}{2})$ tem uma continuação holomorfa a $\mathbb{C}\backslash\{0,1\}$ e pólos

simples em $s = 0, 1$ com -1 e 1, respectivamente, e satisfaz a equação funcional,

$$Z(s) = L\left(f, \frac{s}{2}\right) = L\left(f, \frac{1}{2} - \frac{s}{2}\right) = Z(1-s).$$

□

Corolário B.4. *A função zeta de Riemann $\zeta(s)$ admite uma continuação analítica a $\mathbb{C}\backslash\{1\}$, tem um pólo simples em $s = 1$ com resíduo 1 e satisfaz a equação funcional*

$$\zeta(1-s) = 2(2\pi)^{-s}\Gamma(s)\cos\left(\frac{\pi s}{2}\right)\zeta(s).$$

Demonstração. $Z(s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)$ tem um pólo simples em $s = 0$, mas $\Gamma\left(\frac{s}{2}\right)$ também tem. Logo $\zeta(s)$ não tem pólos aí. Em $s = 1$, no entanto, $Z(s)$ tem um pólo simples, e $\zeta(s)$ também tem e $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$. O resíduo é

$$Res_{s=1}\zeta(s) = \pi^{\frac{1}{2}}\Gamma\left(\frac{1}{2}\right)^{-1} Res_{s=1}Z(s) = 1.$$

Da equação $Z(1-s) = Z(s)$, temos que

$$\zeta(1-s) = \pi^{\frac{1}{2}-s}\frac{\Gamma\left(\frac{s}{2}\right)}{\Gamma(\frac{1-s}{2})}\zeta(s). \tag{B.3}$$

Substituindo $\frac{1-s}{2}$, respectivamente, $\frac{s}{2}$ na fórmula (B.1) e na fórmula de duplicação de Legendre, obtemos

$$\begin{aligned}
\Gamma\left(\frac{1-s}{2}\right)\Gamma\left(1-\frac{1-s}{2}\right) &= \Gamma\left(\frac{1-s}{2}\right)\Gamma\left(\frac{1+s}{2}\right) \\
&= \frac{\pi}{\operatorname{sen}\left(\pi\left(\frac{1-s}{2}\right)\right)} \\
&= \frac{\pi}{\operatorname{sen}\left(\frac{\pi}{2} - \frac{\pi s}{2}\right)} \\
&= \frac{\pi}{\cos\left(\frac{\pi s}{2}\right)}
\end{aligned}$$

e

$$\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{1+s}{2}\right) = \frac{2\sqrt{\pi}}{2^s}\Gamma(s).$$

Tomando o quociente

$$\frac{\Gamma\left(\frac{s}{2}\right)}{\Gamma\left(\frac{1-s}{2}\right)} = \frac{2}{2^s\sqrt{\pi}}\cos\left(\frac{\pi s}{2}\right)\Gamma(s).$$

Juntando com (B.3), temos

$$\begin{aligned}\zeta(1-s) &= \pi^{\frac{1}{2}-s}\frac{2}{2^s\sqrt{\pi}}\cos\left(\frac{\pi s}{2}\right)\Gamma(s)\zeta(s)\\ &= 2(2\pi)^{-s}\cos\left(\frac{\pi s}{2}\right)\Gamma(s)\zeta(s).\end{aligned}$$

□

Apêndice C - Fórmula Explícita para $\psi(x)$

Para $x > 0$ definimos a função ψ de Chebyshev por

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

onde Λ é a função de von Mangoldt definida por

$$\Lambda(n) = \begin{cases} \log p, & \text{se } n = p^m, \text{ para algum } m \geq 1 \\ 0, & \text{caso contrário.} \end{cases}$$

Com isso, podemos escrever $\psi(x)$ como segue:

$$\psi(x) = \sum_{n \leq x} \Lambda(n) = \sum_{m=1}^{\infty} \sum_{p^m \leq x} \Lambda(p^m) = \sum_{m=1}^{\infty} \sum_{p \leq x^{1/m}} \log p.$$

Na verdade, a soma em m é uma soma finita. De fato, não há termo na soma sobre p quando $x^{1/m} < 2$, ou seja, $\frac{1}{m} \log x < \log 2$, o que implica $m > \frac{\log x}{\log 2} = \log_2 x$. Assim,

$$\psi(x) = \sum_{m \leq \log_2 x} \sum_{p \leq x^{1/m}} \log p.$$

Também pode-se escrever $\psi(x) = \sum_{p^m \leq x} \log p$. A função ψ tem descontinuidades nos pontos onde x é uma potência de primo e para que a fórmula explícita seja também válida nesses pontos é necessário modificar a definição tomando a média dos valores que a função assume à esquerda e à direita desses pontos. Ou seja, definimos

$$\psi_0(x) = \begin{cases} \psi(x), & \text{se } x \text{ não é uma potência de primo} \\ \psi(x) - \frac{1}{2}\Lambda(x), & \text{caso contrário.} \end{cases}$$

Teorema C.1 (Fórmula Explícita)**.** *Para $x > 1$, tem-se*

$$\psi_0(x) = x - \sum_{\rho} \frac{x^\rho}{\rho} - \frac{\zeta'(0)}{\zeta(0)} - \frac{1}{2} \log\left(1 - x^{-2}\right), \tag{C.1}$$

onde a soma sobre os zeros não-triviais $\rho = \beta + i\gamma$ de $\zeta(s)$ é no sentido simétrico como segue

$$\lim_{T\to\infty} \sum_{|\gamma|<T} \frac{x^\rho}{\rho}.$$

Antes de provar o teorema, mostraremos o seguinte lema.

Lema C.2. *Sejam*

$$\delta(y) = \begin{cases} 0, & se\, 0 < y < 1, \\ \frac{1}{2}, & se\, y = 1 \\ 1, & se\, y > 1 \end{cases}$$

e

$$I(y,T) = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{y^s}{s} ds.$$

Então, para $y > 0, c > 0, T > 0$,

$$|I(y,T) - \delta(y)| < \begin{cases} y^c \min(1, T^{-1}|\log y|^{-1}), & se\, y \neq 1 \\ cT^{-1}, & se\, y = 1. \end{cases}$$

Demonstração. Suponha primeiro que $0 < y < 1$. A função $\frac{y^s}{s}$ tende a zero quando $\sigma \to +\infty$, e o faz uniformemente em t. Sejam $b > c$ e C o contorno de um retângulo cujos vértices são $c - iT, c + iT, b + iT$ e $b - iT$. Pelo teorema de Cauchy, temos

$$\int_{c-iT}^{c+iT} \frac{y^s}{s} ds = \int_{b+iT}^{c+iT} \frac{y^s}{s} ds + \int_{b-iT}^{b+iT} \frac{y^s}{s} ds + \int_{c-iT}^{b-iT} \frac{y^s}{s} ds.$$

Daí, fazendo $b \to \infty$, temos

$$I(y,T) = -\frac{1}{2\pi i} \int_{c+iT}^{\infty+iT} \frac{y^s}{s} ds + \frac{1}{2\pi i} \int_{c-iT}^{\infty-iT} \frac{y^s}{s} ds.$$

Agora,

$$\begin{aligned} \left| \int_{c+iT}^{\infty+iT} \frac{y^s}{s} ds \right| &= \lim_{b\to\infty} \left| \int_{c+iT}^{b+iT} \frac{y^s}{s} ds \right| \\ &= \lim_{b\to\infty} \left| \int_c^b \frac{y^{c+iT}}{\sigma + iT} d\sigma \right| \\ &\leq \lim_{b\to\infty} \int_c^b \frac{y^\sigma}{T} d\sigma \\ &= \frac{1}{T} \int_c^\infty y^\sigma d\sigma \\ &= \frac{y^c}{T|\log y|}. \end{aligned}$$

Similarmente, mostramos que

$$\left| \int_{c-iT}^{\infty - iT} \frac{y^s}{s} ds \right| \leq \frac{y^c}{T|\log y|}.$$

Com isso,

$$|I(y,T) - \delta(y)| = |I(y,T)| \leq \frac{y^c}{\pi T|\log y|} < \frac{y^c}{T|\log y|}.$$

Para a outra desigualdade substituimos o segmento de integração por um arco circular com centro 0, raio $R = \sqrt{c^2 + T^2}$, que está à direita do segmento. Assim, sobre o arco $|y^c| \leq y^c$ e $|s| = R$. Daí,

$$|I(y,T)| \leq \frac{y^c \pi R}{2\pi R} < y^c.$$

Para $y > 1$, o argumento é análogo, entretanto, usa-se um retângulo ou um arco circular à esquerda do segmento. A curva então inclui o pólo em $s = 0$, onde o resíduo é 1.

Para o caso $y = 1$, calculamos diretamente:

$$\begin{aligned}
I(1,T) &= \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{ds}{s} = \frac{1}{2\pi} \int_{-T}^{T} \frac{dt}{c+it} \\
&= \frac{1}{2\pi} \int_{-T}^{T} \frac{c-it}{c^2+t^2} dt = \frac{1}{2\pi} \int_{-T}^{T} \frac{c}{c^2+t^2} dt - \frac{i}{2\pi} \int_{-T}^{T} \frac{t}{c^2+t^2} dt \\
&= \frac{1}{\pi} \int_{0}^{T} \frac{c}{c^2+t^2} dt = \frac{1}{\pi} \int_{0}^{\frac{T}{c}} \frac{du}{1+u^2} \\
&= \frac{1}{\pi} \arctan \frac{T}{c} = \frac{1}{\pi} \left(\frac{\pi}{2} - \arctan \frac{c}{T} \right) \\
&= \frac{1}{2} - \frac{1}{\pi} \arctan \frac{c}{T}.
\end{aligned}$$

Já que $\arctan \frac{c}{T} < \frac{c}{T}$, temos que $\left| I(1,T) - \frac{1}{2} \right| < \frac{c}{T}$, concluindo a demonstração. □

Demonstração do teorema C.1. Sabemos que para $\sigma > 1$,

$$\zeta(s) = \prod_p \left(1 - p^{-s}\right)^{-1},$$

onde p percorre todos os primos. Tomando logaritmo de ambos os lados, obtemos

$$\begin{aligned}
\log \zeta(s) &= -\sum_p \log\left(1 - p^{-s}\right) = \sum_p \sum_{m=1}^{\infty} \frac{(p^{-s})^m}{m} \\
&= \sum_p \sum_{m=1}^{\infty} \frac{1}{m p^{ms}}.
\end{aligned}$$

Derivando, encontramos

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_p \sum_{m=1}^{\infty} \frac{\log p}{p^{ms}} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}. \tag{C.2}$$

De

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{y^s}{s} ds = \begin{cases} 0, & \text{se } 0 < y < 1, \\ \frac{1}{2}, & \text{se } y = 1 \\ 1, & \text{se } y > 1, \end{cases}$$

de (C.2) e do fato de que a série $\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$ converge absoluta e uniformemente vem que

$$\psi_0(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \left[-\frac{\zeta'(s)}{\zeta(s)}\right] \frac{x^s}{s} ds.$$

Agora, sejam $c = 1 + \frac{1}{\log x}$ e

$$J(x,T) = \frac{1}{2\pi i}\int_{c-iT}^{c+iT} \left[-\frac{\zeta'(s)}{\zeta(s)}\right] \frac{x^s}{s} ds. \tag{C.3}$$

Pelo lema C.2, temos

$$\begin{aligned} |\psi_0(x) - J(x,T)| &= \left| \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \left[-\frac{\zeta'(s)}{\zeta(s)}\right] \frac{x^s}{s} ds - \frac{1}{2\pi i}\int_{c-iT}^{c+iT} \left[-\frac{\zeta'(s)}{\zeta(s)}\right] \frac{x^s}{s} ds \right| \\ &= \left| \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} \frac{x^s}{s} ds - \frac{1}{2\pi i}\int_{c-iT}^{c+iT} \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} \frac{x^s}{s} ds \right| \\ &= \left| \sum_{n=1}^{\infty} \frac{\Lambda(n)}{2\pi i} \left[\int_{c-i\infty}^{c+i\infty} \frac{(x/n)^s}{s} ds - \int_{c-iT}^{c+iT} \frac{(x/n)^s}{s} ds \right] \right| \\ &< \sum_{\substack{n=1 \\ n\neq x}}^{\infty} \Lambda(n)(x/n)^c \min(1, T^{-1}|\log(x/n)|^{-1}) + cT^{-1}\Lambda(x). \end{aligned} \tag{C.4}$$

A escolha $c = 1 + \frac{1}{\log x}$ nos dará um bom resultado sem muito trabalho e implica que $x^c = ex$. O próximo passo é estimar a série no lado direito de (C.4). Primeiro, tomamos todos os termos para os quais $n \leq \frac{3}{4}x$ ou $n \geq \frac{5}{4}x$. Nesse caso, $\frac{x}{n} \geq \frac{4}{3}$ ou $\frac{x}{n} \leq \frac{4}{5}$ o que implica $\log \frac{x}{n} \geq \log \frac{4}{3}$ ou $\log \frac{x}{n} \leq \log \frac{4}{5} = -\log \frac{5}{4}$. Já que $\log \frac{4}{3} \geq \log \frac{5}{4}$, segue que $\left|\log \frac{x}{n}\right| \geq \log \frac{5}{4}$. Logo,

$$\begin{aligned} \sum_{\substack{n=1 \\ n\leq \frac{3}{4}x \text{ ou } n\geq \frac{5}{4}x}}^{\infty} \Lambda(n)(x/n)^c \min(1, T^{-1}\log|x/n|^{-1}) &\ll xT^{-1}\sum_{n=1}^{\infty} \Lambda(n)n^{-c} = xT^{-1}\left[-\frac{\zeta'(c)}{\zeta(c)}\right] \\ &\ll xT^{-1}\log x, \end{aligned}$$

pois $-\frac{\zeta'(c)}{\zeta(c)} \ll \frac{1}{c-1}$ e $c = 1 + \frac{1}{\log x}$.

Considere agora os termos para os quais $\frac{3}{4}x < n < x$. Seja x_1 a maior potência de primo menor que x. Podemos supor que $\frac{3}{4}x < x_1 < x$, pois do contrário, o termos correspondentes seriam nulos. Para o termo correspondente a $n = x_1$, temos

$$\begin{aligned}\log\frac{x}{n} &= \log\frac{x}{x_1} = -\log\frac{x_1}{x} \\ &= -\log\left(\frac{x_1+x-x}{x}\right) = -\log\left(1-\frac{x-x_1}{x}\right) \\ &\geq \frac{x-x_1}{x},\end{aligned}$$

e portanto a contribuição desse termo é

$$\ll \Lambda(x_1)\min\left[1,\frac{x}{T(x-x_1)}\right] \ll (\log x)\min\left[1,\frac{x}{T(x-x_1)}\right].$$

Para os outros termos, podemos por $n = x_1 - \nu$, onde $0 < \nu < \frac{x}{4}$ e então

$$\begin{aligned}\log\frac{x}{n} \geq \log\frac{x_1}{n} &= -\log\frac{n}{x_1} = -\log\left(\frac{n-x_1+x_1}{x_1}\right) \\ &= -\log\left(1-\frac{\nu}{x_1}\right) \geq \frac{\nu}{x_1}.\end{aligned}$$

Por isso a contribuição desses termos é

$$\ll \sum_{0<\nu<\frac{1}{4}x} \Lambda(x_1-\nu)T^{-1}\frac{x_1}{\nu} \ll xT^{-1}\log x \sum_{0<\nu<\frac{1}{4}x}\frac{1}{\nu} \ll xT^{-1}\log^2 x.$$

Para os termos correspondentes a $x < n < \frac{5}{4}x$ o procedimento é similar, com exceção de que x_1 é substituído por x_2, a menor potência de primo maior do que x.

Para x diferente de uma potência de primo, denotemos por $\langle x\rangle$ a distância de x à potência de primo mais próxima. Juntando as estimativas obtemos

$$|\psi_0(x) - J(x,T)| \ll \frac{x(\log x)^2}{T} + (\log x)\min\left(1,\frac{x}{T\langle x\rangle}\right). \tag{C.5}$$

Agora, vamos substituir o segmento vertical de integração em (C.3) pelos outros lados do retângulo com vértices em

$$c-iT, c+iT, -U+iT, -U-iT,$$

onde U é um inteiro ímpar grande. Dessa forma, a reta vertical à esquerda passa entre dois zeros triviais de $\zeta(s)$. A soma dos resíduos do integrando no seus pólos dentro do

retângulo é

$$x - \sum_{|\gamma|<T} \frac{x^\rho}{\rho} - \frac{\zeta'(0)}{\zeta(0)} - \sum_{0<2m<U} \frac{x^{-2m}}{-2m},$$

onde $x, -\frac{x^\rho}{\rho}, -\frac{\zeta'(0)}{\zeta(0)}$ e $-\frac{x^{-2m}}{-2m}$ são os resíduos do integrando em $s = 1, s = \rho, s = 0$ e $s = -2m$, respectivamente.

Proposição C.3. *Se $\rho = \beta + i\gamma$ percorre os zeros não-triviais de $\zeta(s)$, então para T grande*

$$\sum_\rho \frac{1}{1 + (T - \gamma)^2} = O(\log T).$$

Demonstração. Ver lema do capítulo 15 de [6]. □

Da proposição segue que o número de zeros para os quais $|\gamma - T| < 1$ é $\ll \log T$. Assim a diferença entre as ordenadas desses zeros é $\gg (\log T)^{-1}$. Logo, escolhemos T de modo que

$$|\gamma - T| \gg (\log T)^{-1}$$

para todos os zeros $\beta + i\gamma$. Sabe-se que

$$\frac{\zeta'(s)}{\zeta(s)} = \sum_{\substack{\rho \\ |\gamma - T|<1}} \frac{1}{s - \rho} + O(\log T) \qquad (-1 \le \sigma \le 2)$$

(ver capítulo 1 de [15]). Já que pela escolha de T, temos $|T - \gamma| \gg (\log T)^{-1}$ e o número de termos no somatório acima é $O(\log T)$, segue que

$$\frac{\zeta'(s)}{\zeta(s)} \ll \log^2 T \qquad (-1 \le \sigma \le 2). \tag{C.6}$$

A seguir, vamos estimar $\left|\frac{\zeta'(s)}{\zeta(s)}\right|$ para $\sigma \le -1$. Para isso, usamos a equação funcional de $\zeta(s)$:

$$\zeta(1 - s) = 2(2\pi)^{-s}\Gamma(s)\cos\left(\frac{\pi s}{2}\right)\zeta(s).$$

Em seguida, tomamos o logaritmo e derivamos para obter

$$-\frac{\zeta'(1 - s)}{\zeta(1 - s)} = -\log 2\pi - \frac{\pi}{2}\tan\frac{\pi s}{2} + \frac{\Gamma'(s)}{\Gamma(s)} + \frac{\zeta'(s)}{\zeta(s)}. \tag{C.7}$$

O segundo termo é limitado se $|s - (2m + 1)| \ge \frac{1}{2}$, ou seja, $|(1 - s) + 2m| \ge 2$. O terceiro termo é $\ll \log|s|$ e, por conseguinte, $\ll \log(2|1 - s|)$ para $\sigma \ge 2$ e o último termo é limitado. Portanto,

$$\frac{\Gamma'(s)}{\Gamma(s)} \ll \log(2|s|) \qquad (\sigma \le -1), \tag{C.8}$$

desde que os círculos de raio $\frac{1}{2}$ em torno dos zeros triviais de $\zeta(s)$ sejam excluídos. Usando

(C.6) e (C.8) temos

$$\int_{-U\pm iT}^{c\pm iT}\left[-\frac{\zeta'(s)}{\zeta(s)}\right]\frac{x^s}{s}ds \ll T^{-1}\log^2 T\int_{-\infty}^{c}x^\sigma d\sigma \ll \frac{x\log^2 T}{T\log x}$$

e de (C.8) também temos

$$\int_{-U-iT}^{-U+iT}\left[-\frac{\zeta'(s)}{\zeta(s)}\right]\frac{x^s}{s}ds \ll U^{-1}\log U\int_{-T}^{T}x^{-U}dt \ll \frac{T\log U}{Ux^U},$$

que tende a zero quando $U\to\infty$. Daí e de (C.5), temos

$$\begin{aligned}
\psi_0(x) &= J(x,T)+O\left(\frac{x(\log x)^2}{T}+(\log x)\min\left(1,\frac{x}{T\langle x\rangle}\right)\right)\\
&= \frac{1}{2\pi i}\left[2\pi i\left(x-\sum_{|\gamma|<T}\frac{x^\rho}{\rho}-\frac{\zeta'(0)}{\zeta(0)}-\sum_{0<2m<U}\frac{x^{-2m}}{-2m}\right)\right]\\
&\quad+\frac{1}{2\pi i}\left[\left(\int_{c-iT}^{-U-iT}+\int_{-U-iT}^{-U+iT}+\int_{-U+iT}^{c+iT}\right)\frac{-\zeta'(s)x^s ds}{\zeta(s)s}\right]\\
&\quad+O\left(\frac{x(\log x)^2}{T}+(\log x)\min\left(1,\frac{x}{T\langle x\rangle}\right)\right)\\
&= x-\sum_{|\gamma|<T}\frac{x^\rho}{\rho}-\frac{\zeta'(0)}{\zeta(0)}-\sum_{0<2m<U}\frac{x^{-2m}}{-2m}\\
&\quad+O\left(\frac{x\log^2(xT)}{T}+\frac{T\log U}{Ux^U}+(\log x)\min\left(1,\frac{x}{T\langle x\rangle}\right)\right).
\end{aligned}$$

Fazendo $U\to\infty$, obtemos

$$\begin{aligned}
\psi_0(x) &= x-\sum_{|\gamma|<T}\frac{x^\rho}{\rho}-\frac{\zeta'(0)}{\zeta(0)}-\frac{1}{2}\log\left(1-x^{-2}\right)\\
&\quad+O\left(\frac{x\log^2(xT)}{T}+(\log x)\min\left(1,\frac{x}{T\langle x\rangle}\right)\right).
\end{aligned}$$

Agora, fazendo $T\to\infty$, obtemos

$$\psi_0(x)=x-\sum_{|\gamma|<T}\frac{x^\rho}{\rho}-\frac{\zeta'(0)}{\zeta(0)}-\frac{1}{2}\log\left(1-x^{-2}\right),$$

como queríamos. □

Apêndice D - Lista de Resultados Utilizados

Nesse capítulo listamos alguns resultados que utilizamos ao longo da dissertação.

Teorema D.1 (Pequeno Teorema de Fermat)**.** *Se a é um inteiro e p é um primo tal que $p \nmid a$ então*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Consequentemente, para qualquer inteiro a e qualquer primo p tem-se

$$a^p \equiv a \pmod{p}.$$

Demonstração. Veja [2], teoremas 5.17 e 5.18. □

Teorema D.2. *Sejam a, m inteiros, com $m \geq 1$, $(a, m) = 1$ e $f = \mathrm{ord}_m(a)$. Então temos*

(a) $a^k \equiv a^h \pmod{m}$ *se, e somente se,* $k \equiv h \pmod{f}$.

(b) $a^k \equiv 1 \pmod{1}$ *se, e somente se,* $k \equiv 0 \pmod{f}$. *Em particular,* $f \mid \varphi(m)$

Demonstração. Veja [2], teorema 10.1. □

Definimos a função μ de Möbius por

$$\mu(n) = \begin{cases} 1, & \text{se } n = 1 \\ (-1)^k, & \text{se } n = p_1 \cdots p_k \text{ e } p_i \neq p_j \text{ se } i \neq j \\ 0, & \text{caso contrário.} \end{cases}$$

Teorema D.3. *Se $n \geq 1$ então*

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

Demonstração. Veja [2], teorema 2.1. □

Teorema D.4 (Fórmula de Inversão de Möbius)**.** *Sejam f e g funções multiplicativas. Se*

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

para todo n, então

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

para todo n.

Demonstração. Veja [18], teorema 8.6. □

Teorema D.5. *Para $n \geq 1$ temos*

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

Demonstração. Veja [2], teorema 2.4. □

Teorema D.6 (Identidade de Abel)**.** *Para qualquer função aritmética $a(n)$ seja*

$$A(x) = \sum_{n \leq x} a(n),$$

onde $A(x) = 0$ se $x < 1$. Suponha que f tem uma derivada contínua sobre o intervalo $[y, x]$, onde $0 < y < x$. Então temos

$$\sum_{y < n \leq x} a(n) f(n) = A(x) f(x) - A(y) f(y) - \int_y^x A(t) f(t) dt.$$

Demonstração. Veja [2], teorema 4.2. □

Teorema D.7 (Mertens)**.** *Existe uma constante M tal que*

$$\sum_{p \leq x} \frac{1}{p} = \log\log x + M + O\left(\frac{1}{\log x}\right)$$

para todo $x \geq 2$.

Demonstração. Veja [2], teorema 4.12. □

Teorema D.8 (Fórmula de Mertens)**.** *Para $x \geq 2$, temos*

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log x} \left\{1 + O\left(\frac{1}{\log x}\right)\right\}$$

Demonstração. Veja [31], pág. 17, teorema 11. □

Teorema D.9 (Teorema do Números Primos para Progressões Aritméticas)**.** *Se $k > 0$ e $(h, k) = 1$ temos, para todo $x > 1$,*

$$\sum_{\substack{p \leq x \\ p \equiv h \pmod{k}}} \frac{\log p}{p} = \frac{1}{\varphi(k)} \log x + O(1),$$

onde a soma é sobre os primos $p \leq x$ que são congruentes a h (mod k).

Demonstração. Veja [2], capítulo 7. □

Teorema D.10 (Identidade de Euler)**.** *Seja f uma função aritmética multiplicativa tal que a série $\sum_{n=1}^{\infty} f(n)$ seja absolutamente convergente. Então a soma da série pode ser expressa como um produto absolutamente convergente,*

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} \left(1 + f(p) + f(p^2) + \cdots\right),$$

tomado sobre todos os primos.

Demonstração. Veja [2], teorema 11.6. □

Começaremos falando sobre o símbolo de Artin. Seja L/K uma extensão de Galois de corpos de números. Para qualquer ideal primo $\mathfrak{p}$ de O_K que não se ramifica em L e qualquer ideal primo $\mathfrak{P}$ de O_L que está acima de $\mathfrak{p}$ o **automorfismo de Frobenius** em $\mathfrak{P}$ é o único elemento $\sigma \in \mathrm{Gal}(L/K)$ tal que

$$\sigma(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{P}} \qquad \text{para todo } x \in O_L.$$

Denotamos o automorfismo de Frobenius em $\mathfrak{P}$ por $\left[\frac{L/K}{\mathfrak{P}}\right]$. Se $\tau \in \mathrm{Gal}(L/K)$, então $\left[\frac{L/K}{\tau\mathfrak{P}}\right] = \tau \left[\frac{L/K}{\mathfrak{P}}\right] \tau^{-1}$. Logo, quando $\mathfrak{P}$ percorre sobre todos os ideais primos de O_L que estão acima de $\mathfrak{p}$, o automorfismo de Frobenius percorre sobre alguma classe de conjugação de $\mathrm{Gal}(L/K)$ que depende de $\mathfrak{p}$. Essa classe de conjugação é o símbolo de Artin, $\left(\frac{L/K}{\mathfrak{p}}\right)$. Para mais detalhes, veja [17].

Teorema D.11. *Sejam L/K uma extensão de Galois de grau n, $\mathfrak{p}$ um ideal primo não-nulo de O_K. Se $\mathfrak{p}O_L = \prod_{i=1}^{g} \mathcal{Q}_i^{e_i}$ e se $[O_L/\mathcal{Q}_i : O_K/\mathfrak{p}] = f_i$, então $e_1 = \cdots = e_g$, $f_1 = \cdots = f_g$ e se $O_K/\mathfrak{p}$ é um corpo finito, então cada $O_L/\mathcal{Q}_i$ é isomorfo à extensão de grau f_i de $O_K/\mathfrak{p}$.*

Demonstração. Veja [26], capítulo 11, proposição F. □

Teorema D.12. *Sejam $K \subseteq L \subseteq L'$ corpos de números algébricos. Então*

$$\delta_{L'/K} = (\delta_{L/K})^{[L':L]} \cdot N_{L/K}(\delta_{L'/L})$$

Demonstração. Veja [26], capítulo 13, proposição Q. □

Teorema D.13. *Sejam K_1, K_2 corpos de números algébricos, extensões do corpo K e seja $L = K_1K_2$. Então $N_{K_2/K}(\delta_{L/K_2})$ divide $\delta_{K_1/K}^{[L:K_1]}$ e $N_{K_1/K}(\delta_{L/K_1})$ divide $\delta_{K_2/K}^{[L:K_2]}$.*

Demonstração. Veja [26], capítulo 13, proposição U. □

Teorema D.14. *Seja K um corpo. Se H é um subgrupo finito de K^*, então H é cíclico e, consequentemente, consiste de raízes da unidade.*

Demonstração. Veja [16], teorema 2.18. □

Teorema D.15. *Seja M um módulo livre de posto finito $n \geq 1$ sobre o domínio de ideais principais R, e seja K um submódulo de M. Então existe uma base $\{y_1, \ldots, y_n\}$ para M e elementos não-nulos $a_1, \ldots, a_r \in R$ tal que $r \leq n$, a_i divide a_{i+1} para todo i, e $\{a_1y_1, \ldots, a_ry_r\}$ é uma base para K.*

Demonstração. Veja [7], capítulo 12, teorema 4. □

Proposição D.16. *Se $n, m \geq 1$ com $(n, m) = 1$, então*

$$\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{nm}).$$

Demonstração. Veja a demonstração do corolário 3.2 no capítulo 6 de [22]. □

Teorema D.17 (Formula de Jensen)**.** *Seja Ω um aberto que contém o fecho de um disco D_R e suponha que f é analítica em Ω, $f(0) \neq 0$, e f não se anula no círculo C_R. Se $s_1, \ldots, s_N$ denotam os zeros de f dentro do disco (contando as multiplicidades) então*

$$\log|f(0)| = \sum_{j=1}^{N} \log\left(\frac{|s_j|}{R}\right) + \frac{1}{2\pi}\int_0^{2\pi} \log\left|f(Re^{i\theta})\right| d\theta.$$

Demonstração. Veja [28], capítulo 5, teorema 1.1. □

Teorema D.18 (Princípio de Phragmém-Lindelöf)**.** *Se $f(s)$ é uma função analítica e de ordem finita para $\beta_1 \leq \sigma \leq \beta_2$, $f(s) = O(|t|^{\tau_1})$ para $\sigma = \beta_1$ e $f(s) = O(|t|^{\tau_2})$ para $\sigma = \beta_2$ então*

$$f(s) = O(|t|^{\tau(\sigma)}),$$

uniformemente para $\beta_1 \leq \sigma \leq \beta_2$ e $\tau(x)$ é a função linear de x tal que $\tau(\beta_1) = \tau_1$ e $\tau(\beta_2) = \tau_2$.

Demonstração. Veja [10], capítulo 3, teorema 14. □