MICHELE CORDEIRO GUIMARÃES

SOBRE A CONJECTURA DE GOLDBACH EM ANÉIS POLINOMIAIS

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação em Matemática, para obtenção do título de *Magister Scientiae*.

Orientador: Abílio Lemos Cardoso Júnior
Coorientadora: Sônia Maria Fernandes

VIÇOSA
MINAS GERAIS
2020

Ficha catalográfica elaborada pela Biblioteca Central da Universidade Federal de Viçosa - Campus Viçosa

T
G963a
2020

Guimarães, Michele Cordeiro, 1991-
Sobre a Conjectura de Goldbach em anéis polinomiais / Michele Cordeiro Guimarães. – Viçosa, MG, 2020.
51 f. ; 29 cm.

Orientador: Abílio Lemos Cardoso Júnior.
Dissertação (mestrado) - Universidade Federal de Viçosa.
Referências bibliográficas: f.50-51.

1. Polinômios. 2. Teoria da estimativa - Teoria assintótica. 3. Goldbach, Conjectura de. I. Universidade Federal de Viçosa. Departamento de Matemática. Programa de Pós-Graduação em Matemática. II. Título.

CDD 22. ed. 512.4

MICHELE CORDEIRO GUIMARÃES

SOBRE A CONJECTURA DE GOLDBACH EM ANÉIS POLINOMIAIS

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação em Matemática, para obtenção do título de *Magister Scientiae*.

APROVADA: 29 de setembro de 2020

Assentimento:

Michele Cordeiro Guimarães
Autora

Abílio Lemos Cardoso Júnior
Orientador

Dedico este trabalho à minha família.

Agradecimentos

Agradeço à minha família pelo apoio, pelo incentivo e por ter acreditado em mim desde o início desta longa jornada.

Agradeço aos meus orientadores, o professor Abílio e a professora Sônia, por todos os ensinamentos e pela paciência.

Agradeço ao Alejandro pela amizade, por compartilhar estudos, risadas e por me amparar nos momentos difíceis.

Agradeço também à CAPES pelo apoio financeiro indispensável. O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Resumo

GUIMARÃES, Michele Cordeiro, M.Sc., Universidade Federal de Viçosa, setembro de 2020. **Sobre a Conjectura de Goldbach em anéis polinomiais**. Orientador: Abílio Lemos Cardoso Júnior. Coorientadora: Sônia Maria Fernandes.

A Propriedade de Goldbach estabelece que cada elemento de um anel de polinômios, de grau $n \geq 1$, pode ser escrito como soma de dois elementos do mesmo anel, irredutíveis e cujos graus são n. Apresentamos domínios de integridade gerais tais que seus correspondentes anéis de polinômios satisfazem tal propriedade. Além disso, dado um polinômio mônico $f(x) \in \mathbb{Z}[x]$, apresentamos uma fórmula assintótica para $\mathcal{N}(f,k,t)$, com $k \geq 2$ e quando $t \to \infty$, sendo $\mathcal{N}(f,k,t)$ o número de representações (distintas) de f por somas

$$f(x) = f_1(x) + f_2(x) + \ldots + f_k(x),$$

em que $f_1, f_2, \ldots, f_k$ são polinômios inteiros, mônicos e irredutíveis sobre $\mathbb{Q}$ tais que, para cada $1 \leq i \leq k$, a altura de $f_i(x) := x^{d_i} + y_{i,d_i-1}x^{d_i-1} + \ldots + y_{i,1}x + y_{i,0}$ definida por $H(f_i) := \max_{1\leq j\leq d_i}|y_{i,d_i-j}|$ é no máximo t.

Palavras-chave: Anéis polinomiais. Conjectura de Goldbach. Fórmula assintótica.

Abstract

GUIMARÃES, Michele Cordeiro, M.Sc., Universidade Federal de Viçosa, September 2020. **On Goldbach Conjecture in polynomial rings**. Adviser: Abílio Lemos Cardoso Júnior. Co-adviser: Sônia Maria Fernandes.

The Goldbach Property establishes that each element of a polynomial ring, with degree $n \geq 1$, can be written as the sum of two elements of the same ring, irreducible and whose degrees are n. We present general integral domains such that their corresponding polynomial rings satisfy this property. Furthermore, given a monic polynomial $f(x) \in \mathbb{Z}[x]$, we present an asymptotic formula for $\mathcal{N}(f,k,t)$, with $k \geq 2$ and when $t \to \infty$, being $\mathcal{N}(f,k,t)$ the number of (distinct) representations of f by sums

$$f(x) = f_1(x) + f_2(x) + \ldots + f_k(x),$$

where $f_1, f_2, \ldots, f_k$ are integer, monic and irreducible polynomials (over $\mathbb{Q}$) such that, for each $1 \leq i \leq k$, the height of $f_i(x) := x^{d_i} + y_{i,d_i-1}x^{d_i-1} + \ldots + y_{i,1}x + y_{i,0}$ defined by $H(f_i) := \max_{1\leq j\leq d_i}|y_{i,d_i-j}|$ is at most t.

Keywords: Polynomial rings. Goldbach Conjecture. Asymptotic formula.

Sumário

Introdução

Numa carta datada de 7 de junho de 1742, o matemático prussiano Christian Goldbach escreveu a Leonhard Euler que "qualquer inteiro maior que 2 parecia ser uma soma de três números primos".
Interessando-se pelo problema, Euler observou que, no caso dessa alegação ser verdadeira, seria equivalente à dizer que "todo inteiro par $n \geq 2$ é uma soma de 2 primos" e que "todo inteiro ímpar $n \geq 3$ é uma soma de 3 primos" .

Após a convenção de que 1 não é um número primo, ambas as assertivas foram definidas como **Conjectura de Goldbach**: Todo inteiro par $n > 2$ é uma soma de 2 números primos. **Conjectura Fraca de Goldbach**: Todo inteiro ímpar $n > 5$ é uma soma de 3 números primos.

Em 1900, no Congresso Internacional dos Matemáticos, David Hilbert listou a Conjectura de Goldbach como um dos 23 grandes problemas matemáticos. Muitos desses já foram resolvidos e, em 2013, Harald Andrés Helfgott demosntrou a versão fraca. Veja $https://arxiv.org/pdf/1501.05438.pdf$. Entretanto, a conjectura segue sendo uma das mais antigas questões em aberto da matemática. Diante desses fatos, é de se questionar se existem estruturas diferentes de $\mathbb{Z}$ nas quais alguma variação da Conjectura de Goldbach é verificada. Tal questionamento foi respondido pela primeira vez por David Hayes, em 1965 [6], ao provar que o domínio dos números inteiros $R = \mathbb{Z}$ satisfaz a **Propriedade de Goldbach**, isto é, *cada elemento de* $R[x]$, *de grau* $n \geq 1$, *pode ser escrito como soma de dois elementos de* $R[x]$, *irredutíveis e de grau* n. A demonstração é uma aplicação inteligente do Critério de Irredutibilidade de Eisenstein. Em 1998 [15], o teorema de Hayes e sua prova foram redescobertos por Rattan e Stewart.

Assim como na situação clássica, os resultados esperados são conhecidos para soma de três irredutíveis, como em [7] e [4].

Em 2006 e 2010, respectivamente, Saidak e Kosek consideraram variáveis quantitativas do teorema de Hayes quando o polinômio dado em $\mathbb{Z}[x]$ é mônico.

Para $f(x) \in \mathbb{Z}[x]$ mônico com grau $d \geq 2$ e dois inteiros positivos t e $k \geq 2$, denotamos por $\mathcal{N}(f, k, t)$ o número de representações (distintas) de f por somas

$$f(x) = f_1(x) + f_2(x) + \ldots + f_k(x),$$

em que $f_1, f_2, \ldots, f_k$ são polinômios inteiros, mônicos e irredutíveis sobre $\mathbb{Q}$ tais que, para

cada $1 \leq i \leq k$, a altura de $f_i(x) := x^{d_i} + y_{i,d_i-1}x^{d_i-1} + \ldots + y_{i,1}x + y_{i,0}$, definida por $H(f_i) := \max_{1\leq j\leq d_i}|y_{i,d_i-j}|$, é no máximo t. As notações $\ll, O, \sim$ mencionadas a seguir estão definidas na Seção 1.2.

Saidak descreveu, em 2006 [16], um método de contagem que permitiu deduzir uma estimativa tipo Chebyshev para o número $\mathcal{N}(f, 2, t)$. Ele obteve

$$t^{d-1} \ll \mathcal{N}(f, 2, t) \ll t^{d-1}$$

quando $t \to \infty$, onde as constantes implícitas em $\ll$ dependem apenas do grau e dos coeficientes do polinômio $f(x)$.

Em 2010 [10], Kozek melhorou tal resultado, estabelecendo que

$$\mathcal{N}(f, 2, t) = (2t)^{d-1} + O(t^{d-2}\log t)$$

e, portanto, que

$$\lim_{t\to\infty} \frac{\mathcal{N}(f, 2, t)}{(2t)^{d-1}} = 1.$$

Já em 2011 [13], Paul Pollack realizou um estudo mais geral ao provar que todo domínio Noetheriano R possuindo uma infinidade de ideais maximais satisfaz a Propriedade de Goldbach. Além disso, mostrou que cada elemento de $S[x, y]$ de grau $n \geq 1$ pode ser escrito como soma de dois elementos de $S[x, y]$, irredutíveis e de grau n, para algum domínio S. De modo mais geral, isso significa que o domínio $R := S[x_1, x_2, \cdots, x_m]$ satisfaz a Propriedade de Goldbach, para todo $m \geq 1$.

Também em 2011, Arturas Dubickas generalizou os resultados quantitativos sobre $\mathbb{Z}[x]$ ao apresentar fórmulas assintóticas para $\mathcal{N}(f, k, t)$, com $k \geq 2$. Dado o n-politopo $(\Lambda(n, 1, (n-1)/2)) := \{x = (x_1, \ldots + x_n) \in \mathbb{R}^n \,/\, 0 \leq x_i \leq 1\,,\ x_1 + \ldots + x_n \leq (n-1)/2\}$ (o qual é definido de modo geral na seção 1.3 e é uma interseção limitada de um número finito de semi-espaços fechados de $\mathbb{R}^n$), em [2] Dubickas provou para t suficientemente grande que

$$\mathcal{N}(f, k, t) = \frac{(2^{k-1}(1 - 2V_{k-1}))^{d-1}}{(k-1)!} t^{(k-1)(d-1)} + O(t^{dk-d-k})$$

quando $d \geq 4$,

$$\mathcal{N}(f, k, t) = \frac{(2^{k-1}(1 - 2V_{k-1}))^{2}}{(k-1)!} t^{2(k-1)} + O(t^{2k-3}\log t)$$

quando $d = 3$,

$$\mathcal{N}(f, k, t) = \frac{(2^{k-1}(1 - 2V_{k-1}))}{(k-1)!} t^{k-1} + O(t^{k-3/2})$$

quando $d = 2$, tal que $V_n := \text{vol}\,(\Lambda(n, 1, (n-1)/2))$, para $n \geq 1$. Dubickas também melhorou o resultado de Kosek ao provar que

$$\mathcal{N}(f, 2, t) = (2t)^{d-1} + O(t^{d-2})$$

para $d \geq 4$,

$$t \log t \ll (2t)^2 - \mathcal{N}(f, 2, t) \ll t \log t$$

para $d = 3$,

$$\sqrt{t} \ll 2t - \mathcal{N}(f, 2, t) \ll \sqrt{t}$$

para $d = 2$, e, além disso, obteve o melhor termo de erro possível para $\mathcal{N}(f, 2, t)$, quando $d \geq 4$, mostrando que

$$t^{d-2} < (2t)^{d-1} - \mathcal{N}(f_h, 2, t),$$

para o polinômio $f_h(x) := x^d + x^{d-1} + h(x^{d-2} + \cdots + x + 1)$, em que $h := H(f(x))$.

Em 2017 [11], Lemos e De Araújo realizaram um estudo assintótico da propriedade sobre $\mathbb{Z}[\theta][x]$, com

$$\theta = \begin{cases} \sqrt{-k} & \text{se} \quad -k \not\equiv 1 \pmod 4 \\ \frac{\sqrt{-k}+1}{2} & \text{se} \quad -k \equiv 1 \pmod 4 \end{cases}$$

e $k \geq 2$ um inteiro livre de quadrados, e obtiveram que o número de representações de um polinômio mônico $f(x) \in \mathbb{Z}[\theta][x]$, de grau $d \geq 1$, como uma soma de dois polinômios mônicos irredutíveis $g(x)$ e $h(x)$ em $\mathbb{Z}[\theta][x]$, de alturas no máximo t, é assintoticamente equivalente à $(4t)^{2d-2}$.

Recentemente ([12], 2020), Paran provou que um elemento f do anel $\mathbb{Z}[[x]]$ das séries de potências formais sobre $\mathbb{Z}$ é uma soma de dois elementos irredutíveis de $\mathbb{Z}[[x]]$ se, e somente se, o termo constante de f é da forma $\pm p^k \pm q^l$ ou da forma $\pm p^k$, onde p, q são números primos e k, l são inteiros positivos.

Com o propósito de apresentar o conteúdo do trabalho numa ordem coerente, dividimos seu desenvolvimento em três capítulos.

De modo geral, o Capítulo 1 possui definições e teoremas fundamentais que foram de uso frequente nos capítulos seguintes. Na primeira seção desse capítulo, abordamos conceitos e resultados da Teoria de Anéis que formaram a base necessária para o desenvolvimento do Capítulo 2. Na segunda seção, apresentamos notações pertinentes à Teoria Analítica dos Números que estão presentes no Capítulo 3. Na terceira e última seção do Capítulo 1, exploramos definições, exemplos e proposições sobre politopos que nos permitiram relacionar, para alguns casos, seus números de pontos inteiros e volumes. Tal relação é necessária para provar o Lema 3.1.2, o qual exibe uma fórmula assintótica para o número de soluções em $\mathbb{Z}^n$ de equações lineares da forma $y_1 + \cdots + y_n = b_0$, com $b_0 \in \mathbb{Z}, |y_i| \leq t$ e t um inteiro suficientemente grande. No Capítulo 2, cumprimos o primeiro objetivo do trabalho que é realizar o estudo estabelecido por Pollack no artigo [13], apresentando resultados que determinam casos gerais de domínios de integridade com a Propriedade de Goldbach. O Capítulo 3 apresenta nosso último objetivo: uma abordagem quantitativa de $\mathcal{N}(f, k, t)$ para $k \geq 2$. Nele estabelecemos suas fórmulas assintóticas, apresentadas por Dubickas no artigo [2], em termos de volumes n-dimensionais de determinados politopos.

Capítulo 1

Preliminares

Neste primeiro capítulo, apresentaremos uma série de definições e teoremas que serão de uso frequente no estudo a ser desenvolvido nos capítulos seguintes.

1.1 Conceitos e resultados auxiliares em Teoria de Anéis

Apresentamos, nesta seção, os conceitos e resultados mais específicos e necessários ao desenvolvimento do Capítulo 2, como as definições de elemento irredutível, de ideais comaximais e de anéis Noetherianos, bem como os teoremas que os permeiam. Assumiremos previamente um conhecimento básico da Teoria de Anéis detalhada nos livros [13] e [3].

Definição 1.1.1. *Seja R um domínio de integridade e suponha $r \in R$, um elemento não-nulo e não-unidade.*
Dizemos que r é ***irredutível em*** *R se toda vez que $r = ab$ com $a, b \in R$, tivermos que a ou b é uma unidade em R.*

Apresentamos a versão mais geral do critério de Eisenstein:

Lema 1.1.2. *(Critério de Irredutibilidade de Eisenstein) Seja P um ideal primo de um domínio de integridade R. Suponha que $f(x) = a_0 + a_1x + \ldots + a_nx^n \in R[x]$ é um polinômio não-constante cujos coeficientes satisfazem as seguintes condições:*

(*i*) $a_0, a_1, \ldots, a_{n-1}$ *pertencem à* P;

(*ii*) a_0 *não pertence à* P^2;

(*iii*) a_n *não pertence à* P;

(*iv*) $f(x)$ *é primitivo, isto é,* $\langle a_0, a_1, \cdots, a_n \rangle = R$.

Então f é irredutível sobre R.

Demonstração. Suponhamos $f(x) = g(x)\,h(x)$, tal que $g(x)$, $h(x) \in R[x]$, com $g(x) = b_0 + b_1 x + \cdots b_r x^r$, $h(x) = c_0 + c_1 x + \cdots c_s x^s$, satisfazendo $r \geq 1$, $s \geq 1$ e $r + s = n$.

Tomando a igualdade $f(x) = g(x)\,h(x)$ módulo P, temos

$$\overline{a_0} = \overline{b_0}\;\overline{c_0} \quad \Rightarrow \quad \overline{0} = \overline{b_0}\;\overline{c_0},$$

já que $a_0 \in P$. Como P é ideal primo, temos que R/P é domínio e, portanto, $\overline{b_0}$ ou $\overline{c_0}$ é igual à $\overline{0}$.

Supondo $\overline{b_0} = \overline{0}$ e $\overline{c_0} \neq \overline{0}$, temos $b_0 \in P$ e $c_0 \notin P$.

Note que, para $s \geq r$,

$$\begin{aligned}
a_0 &= b_0\,c_0 \\
a_1 &= b_0\,c_1 + b_1\,c_0 \qquad (1.1)\\
a_2 &= b_0\,c_2 + b_1\,c_1 + b_2\,c_0 \qquad (1.2)\\
&\vdots\ \vdots \\
a_s &= b_0\,c_s + b_1\,c_{s-1} + \cdots + b_r\,c_{s-r} \\
&\vdots\ \vdots \\
a_n &= b_r\,c_s
\end{aligned}$$

Por hipótese, $\{a_0,\, a_1,\, \cdots, a_{n-1}\} \subset P$ e $a_n \notin P$. Como $c_0 \notin P$, por (1.1), $b_1 \in P$. Por (1.2), $b_2 \in P$.

Prosseguindo desta forma, indutivamente, obtemos $b_r \in P$ e, então, $b_r\,c_s = a_n \in P$, o que um é absurdo. Por outro lado, $c_0 \in P$ implica em $b_0\,c_0 = a_0 \in P^2$, o que também é absurdo! Portanto, $f(x)$ não admite decomposição $f(x) = g(x)\,h(x)$, para $g(x)$, $h(x)$ polinômios não-constantes.

Para verificar que se $g(x)$ é uma constante que divide $f(x)$ em $R[x]$ então $g(x)$ é unidade em $R[x]$, usaremos a hipótese de que f é primitivo. Como $g|a_i$ para cada $i \in \{0, \cdots, n\}$, existe $\alpha_i \in R$ tal que $a_i = \alpha_i\,g$, para todo $i \in \{0, \cdots n\}$.

Sabendo que $R = \langle a_0,\, a_1,\, \cdots,\, a_n\rangle$, temos $1 = \beta_0\,a_0 + \beta_1\,a_1 + \cdots + \beta_n\,a_n$ e, então

$$1 = \beta_0\,\alpha_0\,g + \beta_1\,\alpha_1\,g + \cdots + \beta_n\,\alpha_n\,g = \left(\sum_{k=0}^{n} \beta_k\,\alpha_k\right)\,g.$$

Como R é comutativo, temos $1 = x\,g = g\,x$, o que confirma que g é uma unidade em $R[x]$. Portanto, f é irredutível em R. □

Agora, estamos interessados em garantir a existência de uma solução para um sistema de simultâneas congruências. Para isso, começamos com a seguinte definição:

Definição 1.1.3. *Seja R um anel comutativo. Dizemos que dois ideais I_1 e I_2, de R, são* ***comaximais*** *quando $I_1 + I_2 = R$.*

Exemplo 1.1.4. *Os ideais $I_1 = \langle 3 \rangle$ e $I_2 = \langle 5 \rangle$ do anel de inteiros $\mathbb{Z}$ são comaximais. De fato:*

$$1 = 2 \cdot 3 + (-1) \cdot 5 \in I_1 + I_2.$$

Portanto, $\mathbb{Z} = \langle 1 \rangle = I_1 + I_2$.

Aqui, apresentamos o teorema que garante a existência da solução de que falamos anteriormente:

Lema 1.1.5. *(Teorema Chinês dos Restos para anéis comutativos) Seja R um anel comutativo com unidade contendo ideais $I_1, I_2, \cdots, I_k$. Suponha que os ideais I_i, I_j são comaximais sempre que $i \neq j$. Então a aplicação*

$$\begin{array}{rccc} \varphi: & R & \longrightarrow & R/I_1 \times \cdots \times R/I_k \\ & r & \longmapsto & (r \, mod \, I_1, \cdots, r \, mod \, I_k) \end{array}$$

é um epimorfismo de anéis com kernel $I_1 \cap \cdots \cap I_k$. Além disso,

$$R/(I_1 I_2 \cdots I_k) \simeq R/I_1 \times \cdots \times R/I_k.$$

Demonstração. Começamos a prova para $k = 2$. Sejam $A = I_1$, $B = I_2$, ideais de R e $\varphi : R \longrightarrow R/A \times R/B$ tal que

$$\varphi(r) = (r + A,\, r + B).$$

(i) φ é um homomorfismo: dados $r, s \in R$,

$$\begin{aligned} \varphi(r+s) &= (r+s+A,\, r+s+B) = ((r+A)+(s+A), (r+B)+(s+B)) \\ &= (r+A, r+B) + (s+A, s+B) = \varphi(r) + \varphi(s). \\ \varphi(r \cdot s) &= (r \cdot s + A, r \cdot s + B) = ((r+A)\cdot(s+A), (r+B)\cdot(s+B)) \\ &= (r+A, r+B)(s+A, s+B) = \varphi(r) \cdot \varphi(s). \end{aligned}$$

(ii) $\mathrm{Ker}(\varphi) = \{r \in R / \, \varphi(r) = (0 \,\mathrm{mod} A,\, 0 \,\mathrm{mod} B)\} = \{r \in R / \, r \in A \text{ e } r \in B\} = A \cap B$.

(iii) φ é sobrejetor: como $A + B = R$, existem $x \in A$, $y \in B$, tais que $1 = x + y$. Dado $(r_1 + A, r_2 + B) \in R/A \times R/B$, temos $r_2\, x + r_1\, y \in R$. Daí,

$$\begin{aligned} \varphi(r_2\, x + r_1\, y) &= \varphi(r_2)\, \varphi(x) + \varphi(r_1)\, \varphi(y) \\ &= (r_2 + A, r_2 + B)\, \varphi(1-y) + \varphi(r_1 + A, r_1 + B)\, \varphi(1-x) \\ &= (r_2 + A, r_2 + B)(0,1) + (r_1 + A, r_1 + B)(1,0) \\ &= (r_1 + A, r_2 + B), \end{aligned}$$

donde obtemos que $R/A \times R/B = \mathrm{Im}\,(\varphi)$.

(iv) $A \cap B = A\,B$: como A, $B \subset R$ são ideais, dado $a\,b \in A\,B$, temos que $a\,b \in A$ e $a\,b \in B$ pois a, $b \in R$. Então $A\,B \subset A \cap B$. Por outro lado, já que A, B são comaximais, dado $c \in A \cap B$, temos $c = c \cdot 1 = c\,x + c\,y$, com $x \in A$ e $y \in B$. Como $A\,B$ é ideal e $c \in A$, $c \in B$, então $c\,x \in A\,B$, $c\,y \in A\,B$, e $c\,x + c\,y \in A\,B$. Portanto, $A\,B = A \cap B$.

(v) Por último, concluímos que $R/A\,B \simeq R/A \times R/B$, pelo Primeiro Teorema do Isomorfismo de Anéis.

Para o caso geral, escolhemos $A = I_1$ e $B = I_2 \cdots I_k$, ideais de R, com $k \in \mathbb{N}$. Então, basta mostrar que $A + B = R$ para concluirmos a demonstração, já que provamos o teorema para quaisquer dois ideais comaximais de R.

Supondo $A + I_i = R$, para cada $i \in \{2, 3, \cdots, k\}$, existem $x_i \in A$, $y_i \in I_i$, tais que $1 = x_i + y_i$ e $x_i + y_i \equiv y_i \bmod A$. Então,

$$1 = (x_2 + y_2)(x_3 + y_3) \cdots (x_k + y_k) = x + y_2\,y_3 \cdots y_k,$$

onde x é a soma de todos os termos em que aparece x_i, com $i \in \{2, 3, \cdots, k\}$. Como A é um ideal, $x \in A$. Daí,

$$1 = x + y_2\,y_3 \cdots y_k \in A + (I_2 \cdots I_k) = A + B \;\Rightarrow\; R \subset A + B.$$

Portanto, $A = I_1$ e $B = I_2 \cdots I_k$ são comaximais. □

Seguimos com alguns resultados, necessários ao Capítulo 2, que tratam de anéis Noetherianos. Esses anéis são definidos como segue:

Definição 1.1.6. *Seja R um anel comutativo. Dizemos que R é um* ***anel Noetheriano****, ou de Noether, se para toda família $\{I_i\}_{i\in\mathbb{N}}$ de ideais de R ordenada pela inclusão,*

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots,$$

existir $k \in \mathbb{N}$ tal que $I_n = I_k$, para todo $n \geq k$. Neste caso, dizemos que R satisfaz a ***condição de cadeia ascendente*** *e I_k satisfaz a* ***condição maximal****.*

Exemplo 1.1.7. *1. O anel $\mathbb{Z}$ é Noetheriano.*

De fato. Como $\mathbb{Z}$ é DIP, uma cadeia ascendente de ideais de $\mathbb{Z}$ deve ser do tipo

$$\langle x_1\rangle \subseteq \langle x_2\rangle \subseteq \cdots \langle x_n\rangle \subseteq \cdots$$

onde $(x_n)_{n\in\mathbb{N}}$ é uma sequência de inteiros. Note que $\langle x_i\rangle \subseteq \langle x_{i+1}\rangle \Leftrightarrow x_{i+1}$ é um divisor de x_i, para cada $i \in \mathbb{N}$. Como o conjunto de divisores de x_i é finito, para todo $i \in \mathbb{N}$, concluímos que a cadeia é estacionária.

2. *Todo corpo $\mathbb{K}$ é Noetheriano já que só possui dois ideais, o $\langle 0\rangle$ e o próprio $\mathbb{K}$.*

3. *Como aplicação do próximo teorema, temos que o anel $\mathbb{Z}_n$ é Noetheriano, para todo $n \in \mathbb{N}$.*

Teorema 1.1.8. *Se I é um ideal de um anel Noetheriano R, então o quociente R/I é um anel Noetheriano.*

Demonstração. Pelo Terceiro Teorema do Isomorfismo de Anéis, uma cadeia ascendente de ideais de R/I deve ser do tipo

$$J_1/I \subseteq J_2/I \subseteq \cdots \subseteq J_n/I \subseteq \cdots$$

onde cada J_i é um ideal de R que contém I. Como a cadeia $J_1 \subseteq J_2 \subseteq \cdots \subseteq J_n \subseteq \cdots$ é estacionária, a cadeia de ideias de R/I também o é. □

O seguinte teorema é uma caracterização para anéis Noetherianos:

Teorema 1.1.9. *R é um anel Noetheriano se, e somente se, todo ideal de R é finitamente gerado.*

Demonstração. ($\Rightarrow$) Sejam I um ideal de R e Ω o conjunto de todos os ideais finitamente gerados de R. Então Ω é não-vazio, pois $0 \in \Omega$. Seja $I_1 \in \Omega$. Se I_1 satisfaz a condição maximal, acabou. Caso contrário, existe $I_2 \in \Omega$ tal que $I_1 \subset I_2$ e $I_1 \neq I_2$. Se I_2 satisfaz a condição maximal, acabou. Caso contrário, repita o processo. Eventualmente, esse processo termina já que caso contrário obteríamos uma cadeia ascendente $I_1 \subset I_2 \subset I_3 \subset \cdots$ estrita, o que contradiz a hipótese. Então Ω possui um elemento I_k satisfazendo a condição maximal. Supondo $I_k \neq R$, considere o ideal $I_k + \langle r\rangle$, com $r \in R$ e $r \notin I_k$. Esse ideal é finitamente gerado e contém estritamente I_k, o que é uma contradição. Logo, R é finitamente gerado e todo ideal de R também o é.

($\Leftarrow$) Seja $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ uma cadeia ascendente de ideais de R. Temos que $I := \cup_{n=1}^{\infty} I_n$ é um ideal (usando a condição de cadeia) e portanto é finitamente gerado. Sejam $x_1, x_2, \cdots, x_k$ os geradores de I tal que $x_i \in I_{n_i}$ e seja $n = \max_{1\leq i\leq k} n_i$. Então cada x_i pertence à I_n e daí $I = I_n$. Portanto, a cadeia é estacionária. □

Teorema 1.1.10. *(Teorema da Base de Hilbert) Se R é um anel Noetheriano então $R[x]$ também o é.*

Demonstração. Suponhamos que $R[x]$ não é anel Noetheriano e seja $I \subset R[x]$, um ideal que não seja finitamente gerado. Seja $f_1 \in I$, com grau mínimo $n_1 \geq 0$, digamos

$$f_1 = a_1\, x^{n_1} + \Delta_1, \text{ em que } \Delta_1 \text{ é um polinômio de grau menor que } n_1.$$

Já que I não é finitamente gerado, temos $I \neq \langle f_1\rangle$ e então $I - \langle f_1\rangle \neq \varnothing$. Agora, escolhemos f_2 em $I - \langle f_1\rangle$, com grau mínimo $n_2 \geq 0$. Escrevemos

$$f_2 = a_2\, x^{n_2} + \Delta_2, \text{ em que } \Delta_2 \text{ é um polinômio de grau menor que } n_2.$$

Suponhamos que tenha sido escolhido $f_k \in I$ de tal forma que f_{k+1} seja um polinômio de grau mínimo em $I - \langle f_1,\, f_2,\, \cdots,\, f_k\rangle$, com

$$f_{k+1} = a_{k+1}\, x^{n_{k+1}} + \Delta_{k+1}, \text{ em que } \Delta_{k+1} \text{ é um polinômio de grau menor que } n_{k+1}.$$

Para todo $k \in \mathbb{N}$, sejam $n_k = \partial f_k$ e a_k o coeficiente líder de f_k. Pela forma como escolhemos os polinômios, segue que $n_1 \leq n_2 \leq \cdots \leq n_k$ e, além disso, obtemos a cadeia ascendente de ideais

$$\langle a_1\rangle \subset \langle a_1, a_2\rangle \subset \langle a_1, a_2, a_3\rangle \cdots \subset R,$$

que não é estacionária pois, do contrário, existiria algum $k \in \mathbb{N}$ tal que

$$\langle a_1, a_2, \cdots, a_k\rangle = \langle a_1, a_2, \cdots, a_k, a_{k+1}\rangle$$

e daí teríamos $a_{k+1} \in \langle a_1, a_2, \cdots, a_k\rangle$. Então,

$$a_{k+1} = \sum_{i=1}^{k} r_i\, a_i, \text{ com } r_i \in A. \tag{1.3}$$

Definindo o polinômio

$$g := f_{k+1} - \left(\sum_{i=1}^{k} r_i\, x^{n_{k+1}-n_i}\, f_i\right) \in I - \langle f_1,\, f_2,\, \cdots,\, f_k\rangle,$$

observamos que

$$\begin{aligned} g &= a_{k+1}\, x^{n_{k+1}} + \Delta_{k+1} - \left(\sum_{i=1}^{k} r_i\, x^{n_{k+1}-n_i}(a_i\, x^{n_i} + \Delta_i)\right) \\ &= a_{k+1}\, x^{n_{k+1}} + \Delta_{k+1} - \sum_{i=1}^{k} r_i\, a_i\, x^{n_{k+1}} - \sum_{i=1}^{k} r_i\, x^{n_{k+1}-n_i}\, \Delta_i \\ &= \Delta_{k+1} - \sum_{i=1}^{k} r_i\, x^{n_{k+1}-n_i}\, \Delta_i\,, \text{ por (1.3)} \end{aligned}$$

e então $g \in I - \langle f_1,\, f_2,\, \cdots,\, f_k\rangle$ é um polinômio de grau menor que o grau de f_{k+1}, o que é um absurdo. Portanto, $R[x]$ é um anel Noetheriano. □

Proposição 1.1.11. *Se R é um anel Noetheriano e I é um ideal de R, então existem ideais primos (não necessariamente distintos) $P_1, P_2, \ldots, P_k$ tais que*

$$P_1 P_2 \cdots P_k \subset I.$$

Demonstração. Suponha, por absurdo, que o conjunto Ω dos ideais de R que não contém um produto de ideais primos de R seja não-vazio. Considere uma cadeia ascendente de ideais em Ω e seja I_k o ideal que satisfaz a condição maximal para esta cadeia. Esse

ideal não pode ser primo pois se fosse não pertenceria à Ω. Daí, existem $x, y \in R$ tais que $xy \in I_k$ mas $x, y \notin I_k$. Considere os ideais $I_x := I_k + \langle x \rangle$ e $I_y := I_k + \langle y \rangle$. Ambos contêm propriamente o ideal I_k tais que $I_x I_y \subset I_k$. Pela maximalidade de I_k, I_x e I_y não pertencem à Ω e, então, ambos contêm um produto de ideais primos de R. Logo, o produto desses produtos está contido em I_k, o que é uma contradição. □

1.2 Algumas notações em Teoria Analítica dos Números

Para desenvolver um estudo assintótico de determinadas funções, como faremos no Capítulo 3, é preciso ter um breve entendimento sobre comparação da ordem de crescimento entre duas funções. Nesse sentido, usaremos frequentemente os símbolos

$$\ll, \quad O, \quad \sim,$$

cujos significados daremos a seguir. Importantes propriedades podem ser consultadas no livro [8].

Seja t um inteiro positivo, tal que $t \to \infty$ (ou x uma variável contínua que tende ao infinito). Seja $\varphi(t)$ (ou $\varphi(x)$) uma função positiva de t (ou de x) e seja $f(t)$ (ou $f(x)$) uma função qualquer. Se existe uma constante $c > 0$ que não depende de t (ou x) satisfazendo

$$|f| \leq c\varphi,$$

então escrevemos

$$f \ll \varphi.$$

Analogamente, se define $\gg$.

Se existe uma função $g \neq 0$ tal que $f - g \ll \varphi$, é mais conveniente escrevermos

$$f = g + O(\varphi). \tag{1.4}$$

Além disso, $f \sim \varphi$ significa

$$\lim_{t\to\infty} \frac{f(t)}{\varphi(t)} = 1$$

$$\left(\text{ou } \lim_{x\to\infty} \frac{f(x)}{\varphi(x)} = 1. \right)$$

Exemplo 1.2.1. *1.* $x + \dfrac{1}{x} \ll x \ll x + \dfrac{1}{x}$ *pois* $\left| x + \dfrac{1}{x} \right| \leq 2x$;

2. $x + \sin(x) = x + O(1)$ *pois* $x + \sin(x) - x = \sin(x) \ll 1$;

3. $x + \sin(x) \sim x$ *pois*

$$\lim_{x\to\infty} \frac{x+\sin(x)}{x} = 1 + \lim_{x\to\infty} \frac{\sin(x)}{x} = 1$$

1.3 Sobre Politopos e seus volumes

Na Geometria Euclidiana, muitos dos objetos definidos em $\mathbb{R}^2$ e $\mathbb{R}^3$ podem ser estendidos ao $\mathbb{R}^n$ e mensurados (no sentido de Jordan). Um **politopo** n-dimensional, por exemplo, generaliza os termos "polígono" e "poliedro" convexos e possui um **volume** n-dimensional. Neste contexto, definimos formalmente um politopo, exibimos os exemplos relevantes para o trabalho e apresentamos propriedades do volume de um politopo para casos especiais, assim como sua relação com o número de vetores inteiros pertencentes ao politopo em questão.

Esta seção é a base necessária para tratarmos do Lema 3.1.2, o qual estabelecerá uma fórmula assintótica para o número de soluções em $\mathbb{Z}^n$ de determinadas equações lineares, por meio da relação citada.

Consideramos o espaço euclidiano n-dimensional $\mathbb{R}^n$, com $n \geq 2$, munido do produto interno canônico $\langle \cdot, \cdot \rangle$ e da norma euclidiana $| \cdot |$. Denotamos por x um ponto arbitrário $(x_1, \ldots, x_n) \in \mathbb{R}^n_+$.

1.3.1 Definições e exemplos

Definição 1.3.1. *Um conjunto convexo*

$$\{x \,/\, Ax \leq B\},$$

onde $A = (a_{ij})$ *é uma matriz real de ordem* $m \times n$ *e* $B = (b_i)$ *é uma matriz real de ordem* $m \times 1$*, é um* ***politopo*** n*-dimensional (ou* n*-politopo), desde que seja limitado.*

Definição 1.3.2. *Seja* $a = (a_1, \ldots, a_n)$ *um vetor real não-nulo e* b *um número real. Definimos o* ***semi-espaço fechado*** n*-dimensional*

$$G^n_{a,b} := \{x \,/\, \langle a, x \rangle \leq b\}.$$

O correspondente ***hiperplano*** $(n-1)$*-dimensional, normal ao vetor* a*, é dado por*

$$H^{n-1}_{a,b} := \{x \in \mathbb{R}^n \,/\, \langle a, x \rangle = b\}.$$

Em outras palavras, um n-politopo é uma interseção limitada de um número finito de semi-espaços fechados de $\mathbb{R}^n$.

Exemplo 1.3.3. *Vejamos alguns exemplos clássicos:*

1. *O conjunto* $[0,r]^n := \{x \,/\, 0 \leq x_i \leq r,\ para\ 1 \leq i \leq n\}$, *é o* ***hipercubo*** *n-dimensional com arestas de comprimento* r *e um dos vértices sobre a origem.*

2. *Qualquer corpo convexo n-dimensional que possui* $n+1$ *vértices é um politopo chamado* **n-*simplex***. *Formalmente, o conjunto*

$$\Delta_0(n,s) := \{x \,/\, 0 \leq x_i \leq s,\ para\ 1 \leq i \leq n\ \ e\ \ 0 \leq x_1 + \ldots + x_n \leq s\} \tag{1.5}$$

é o simplex com arestas de comprimento s *e um dos vértices sobre a origem. Um simplex também pode ser definido fora da origem, como veremos na Proposição 1.3.7.*

2.1. $\Delta_0(1,s)$ *é o segmento* $[0,s]$.

2.2. $\Delta_0(2,s)$ *é o triângulo com coordenadas* $(0,0)$, $(s,0)$, $(0,s)$.

2.3. $\Delta_0(3,s)$ *é o tetraedro com coordenadas* $(0,0,0)$, $(s,0,0)$, $(0,s,0)$, $(0,0,s)$.

Definimos

$$\Lambda(n,r,s) := \{x \,/\, 0 \leq x_i \leq r\,,\ x_1 + \ldots + x_n \leq s\},\ \text{ para } r,s \in \mathbb{R}_+. \tag{1.6}$$

Observe que o politopo $\Lambda(n,r,s)$ é a interseção do hipercubo $[0,r]^n$ com o semi-espaço fechado $G^n_{1,s}$, em que 1 representa o vetor $(1,\cdots,1) \in \mathbb{R}^n$. Além disso, em alguns casos, essa interseção resulta na estrutura de um simplex:

Exemplo 1.3.4. *Seja* $\Lambda(n,1,(n-1)/2)$.

1. *O polígono* $\Lambda(2,1,1/2) := \{(x_1,x_2) \in [0,1]^2 \,/\, x_1 + x_2 \leq 1/2\}$ *é o* 2*-simplex* $\Delta_0(2,1/2)$.

2. *O poliedro* $\Lambda(3,1,1) := \{(x_1,x_2,x_3) \in [0,1]^3 \,/\, x_1 + x_2 + x_3 \leq 1\}$ *é o* 3*-simplex* $\Delta_0(3,1)$.

1.3.2 Relacionando volumes e número de pontos do reticulado $\mathbb{Z}^n$

Cada corpo convexo $K \subset \mathbb{R}^n$ tem um "volume" no sentido de Jordan (isto é, o corpo K é J-mensurável), assim como todo n-politopo possui volume n-dimensional. Geralmente, o cálculo desse volume leva à inevitável construção de uma triangulação, explícita ou implícita, sobre o politopo (ou seja, uma subdivisão desse objeto geométrico em um conjunto de simplexes satisfazendo algumas propriedades), desde que tais simplexes tenham seus volumes facilmente calculados. Entretanto, tal construção não será abordada neste trabalho e pode ser estudada sob diferentes abordagens, como no Capítulo 17 do livro [5] ou no artigo [9].

Sejam $n \geq 3, u > 0, v \in \mathbb{R}$ e $t \in \mathbb{N}$. Definimos

$$|\Lambda(n-1, 2t, ut+v)| \tag{1.7}$$

como o número de pontos do reticulado $\mathbb{Z}^{n-1}$ que pertencem ao politopo $\Lambda(n-1, 2t, ut+v)$.

Nosso interesse, aqui, é apresentar uma fórmula assintótica para $|\Lambda(n-1, 2t, ut+v)|$ quando $t \to \infty$. Para isso, começamos provando alguns resultados relacionados à volumes de politopos anteriormente definidos:

Proposição 1.3.5. *O volume n-dimensional do n-simplex $\Delta_0(n, s)$ é dado por*

$$vol\,(\Delta_0(n, s)) = \frac{s^n}{n!},$$

para $n \geq 2$.

Demonstração. Provaremos usando a indução sobre $n \geq 2$.

Seja $\Delta_0(2, s) := \{x \,/\, 0 \leq x_1, x_2 \leq s \text{ e } 0 \leq x_1 + x_2 \leq s\}$. Então, seu volume 2-dimensional é dado por

$$vol\,(\Delta_0(2, s)) = \int_0^s \left(\int_0^{s-x_2} 1\, dx_1 \right) dx_2 = \int_0^s (s - x_1)\, dx_1 = s^2 - \frac{s^2}{2} = \frac{s^2}{2}.$$

Agora, suponha $vol\,(\Delta_0(n, s)) = s^n/n!$, para $n \geq 2$. Então, o volume $(n+1)$-dimensional do simplex $\Delta_0(n+1, s)$ é

$$vol\,(\Delta_0(n+1, s)) = \int_0^s \left(\int_0^{s-x_{n+1}} \int_0^{s-x_{n+1}-x_n} \cdots \int_0^{s-\sum_{i=2}^{n+1} x_i} 1\, dx_1 \cdots dx_n \right) dx_{n+1} \tag{1.8}$$

Colocando $b := s - x_{n+1}$, por (1.8) temos

$$\begin{aligned} vol\,(\Delta_0(n+1, s)) &= \int_0^s \left(\int_0^b \int_0^{b-x_n} \cdots \int_0^{b-\sum_{i=2}^{n} x_i} 1\, dx_1 \cdots dx_n \right) dx_{n+1} \\ &= \int_0^s V(\Delta_0(n, b)) dx_{n+1} = \int_0^s \frac{b^n}{n!}\, dx_{n+1} \end{aligned}$$

e com a mudança de variável $X := s - x_{n+1}$, concluímos que

$$vol\,(\Delta_0(n+1, s)) = \int_s^0 -\frac{X^n}{n!}\, dX = \frac{s^{n+1}}{(n+1)!}.$$

□

Caso não haja a necessidade de mencionarmos outros detalhes, escreveremos apenas $vol(K)$ para indicar o volume n-dimensional de um n-politopo K.

Exemplo 1.3.6. *Temos*

$$V_2 = 1/8,\ V_3 = 1/6,\ V_4 = 77/384 \text{ e } V_5 = 9/40,$$

para $V_n := vol\,(\Lambda(n, 1, (n-1)/2))$.

De fato, pelo Exemplo 1.3.4 e pela Proposição 1.3.5, temos

$$V_2 = \frac{(1/2)^2}{2!} = \frac{1}{8},\ \ V_3 = \frac{(1)^3}{3!} = \frac{1}{6}.$$

Para calcular V_4, *observe que* $\Lambda(4, 1, 3/2)$ *pode ser visto como o simplex* $\Delta_0(4, 3/2)$ *subtraído por quatro "simplexes" (a menos de faces em comum com o hipercubo* $[0, 1]^4$*), que possuem arestas medindo* $s = 1/2$. *Cada um desses corpos é uma ponta do* $\Delta_0(4, 3/2)$ *e possui volume igual ao volume do simplex* $\Delta_0(4, 1/2)$, *já que translações preservam volume e uma face* $(n-1)$*-dimensional tem o volume* n*-dimensional nulo. Portanto,*

$$V_4 = \frac{(3/2)^4}{4!} - 4 \cdot \frac{(1/2)^4}{4!} = \frac{81-4}{384} = \frac{77}{384}.$$

Da mesma forma, o volume de $\Lambda(5, 1, 2)$ *é dado pelo volume do simplex* $\Delta_0(5, 2)$ *subtraído dos volumes de cinco "simplexe" que possuem arestas medindo* $s = 1$, *isto é,*

$$V_5 = \frac{2^5}{5!} - 5 \cdot \frac{1^5}{5!} = \frac{27}{120} = \frac{9}{40}.$$

Proposição 1.3.7. *Para* $r < s < nr$ *e* $n \geq 2$, *temos*

$$vol\,(\Lambda(n, r, s)) = vol\,(\Delta_0(n, s)) - n \cdot vol\,(\Delta_0(n, (s-r)).$$

Demonstração. Inicialmente, definimos o n-simplex com arestas de comprimento $s - r$,

$$\Delta_i(n, s-r) := \{x \,/\, 0 \leq x_j \leq s-r \text{ para } j \neq i,\ r \leq x_i \leq s \text{ e } r \leq \textstyle\sum_{k=1}^{n} x_k \leq s\},$$

para cada $i \in \{1, \cdots, n\}$. Afirmamos que

$$\cup_{i=1}^{n} \Delta_i(n, s-r) \cup \Lambda(n, r, s) = \Delta_0(n, s). \tag{1.9}$$

De fato, é claro que $\Delta_i(n, s-r)$ e $\Lambda(n, r, s)$ estão contidos em $\Delta_0(n, s)$, para todo $i \in \{1, \cdots, n\}$, pois $s - r < s$ e $r < s$. Então $(\cup_{i=1}^{n} \Delta_i(n, s-r) \cup \Lambda(n, r, s)) \subset \Delta_0(n, s)$.

Por outro lado, seja $x = (x_1, \cdots, x_n) \in \Delta_0(n, s)$. Se $x_i \leq r$ para todo $1 \leq i \leq n$, então $x \in \Lambda(n, r, s)$. Caso contrário, existe $i \in \{1, \cdots, n\}$ tal que $r < x_i \leq s$. Como $x \in \Delta_0(n, s)$, obtemos

$$r < \textstyle\sum_{k=1}^{n} x_k \leq s.$$

Como $r < x_i$, temos $0 \leq x_j \leq \sum_{j \neq i} x_j < s - r$ para todo $j \neq i$. Portanto, $x \in \Delta_i(n, s-r)$.

Agora, observe que $\Delta_i(n, s-r)$ é congruente à $\Delta_0(n, s-r)$ para cada i, pois ambos são n-simplexes com arestas de comprimento $s-r$ e então possuem mesmo volume. Além disso, para cada $i \in \{1, \cdots, n\}$,

$$\Delta_i(n, s-r) \cap \Lambda(n, r, s) = \{x \,/\, x_i = r,\ 0 \leq x_j \leq s-r \ \text{ para } \ j \neq i \ \text{ e } \ 0 \leq \textstyle\sum_{k \neq i} x_k \leq s-r\},$$

pois $s < nr$ nos fornece $s - r < (n-1)r$, para todo $n \geq 2$, e então $x_j \leq s - r < r$ para todo $j \neq i$. Daí, concluímos que as interseções obtidas acima pertencem à hiperplanos $(n-1)$-dimensionais e então possuem volumes n-dimensionais nulos. Também temos $\Delta_i(n, s-r) \cap \Delta_j(n, s-r) = \emptyset$ para todo $i \neq j$. Portanto, tomando o volume de $\Delta_0(n, s)$, por (1.12) obtemos

$$\begin{aligned}
&vol\,(\cup_{i=1}^{n} \Delta_i(n, s-r) \cup \Lambda(n, r, s)) = \\
&vol\,(\cup_{i=1}^{n} \Delta_i(n, s-r)) + vol\,(\Lambda(n, r, s)) - vol\,(\cup_{i=1}^{n} (\Delta_i(n, s-r) \cap \Lambda(n, r, s))) = \\
&n \cdot vol\,(\Delta_0(n, s-r)) + vol\,(\Lambda(n, r, s)) = vol\,(\Delta_0(n, s)) \Rightarrow \\
&vol\,(\Lambda(n, r, s)) = vol\,(\Delta_0(n, s)) - n \cdot vol\,(\Delta_0(n, (s-r)).
\end{aligned}$$

□

O próximo resultado mostra que, dados $r, s \in \mathbb{R}_+$, o politopo $\Lambda(n, r, s)$ é um corpo expandido do politopo $\Lambda(n, 1, s/r)$, numa escala $r : 1$.

Proposição 1.3.8. *O volume de $\Lambda(n, r, s)$, para $n \geq 2$, é dado por*

$$vol\,(\Lambda(n, r, s)) = r^n\, vol\,(\Lambda(n, 1, s/r)).$$

Demonstração. Tomamos $\mathcal{A} := \Lambda(n, r, s)$ e $\mathcal{B} := \Lambda(n, 1, s/r)$. Se $s \leq r$, temos

$$\begin{aligned}
\mathcal{A} &= \{x \,/\, 0 \leq x_i \leq r\,,\ x_1 + \ldots + x_n \leq s\} \\
&= \{x \,/\, 0 \leq x_i \leq s\,,\ x_1 + \ldots + x_n \leq s\} \\
&= \Delta_0(n, s),
\end{aligned}$$

$$\begin{aligned}
\mathcal{B} &= \{x \,/\, 0 \leq x_i \leq 1\,,\ x_1 + \ldots + x_n \leq s/r\} \\
&= \{x \,/\, 0 \leq x_i \leq s/r\,,\ x_1 + \ldots + x_n \leq s/r\} \\
&= \Delta_0(n, s/r)
\end{aligned}$$

e, pela Proposição 1.3.5, concluímos que

$$vol\,(\mathcal{A}) = \frac{s^n}{n!} = r^n \cdot \frac{(s/r)^n}{n!} = r^n\, vol\,(\mathcal{B}).$$

Para $s > r$, dividimos em dois casos.
Se $s \geq nr$, então $\mathcal{A} = [0, r]^n, B = [0, 1]^n$ e, portanto,

$$vol\,(\mathcal{A}) = r^n = r^n \cdot 1 = r^n\, vol\,(\mathcal{B}).$$

Se $r < s < nr$, usamos as Proposições 1.3.5 e 1.3.7. Daí,

$$\begin{aligned} vol\,(\mathcal{A}) &= vol\,(\Delta_0(n, s)) - n \cdot vol\,(\Delta_0(n, (s - r))) \\ &= \frac{s^n}{n!} - n \cdot \frac{(s - r)^n}{n!}. \end{aligned} \tag{1.10}$$

Como $(s/r) - 1 = (s - r)/r$, temos

$$\begin{aligned} vol\,(\mathcal{B}) &= vol\,(\Delta_0(n, s/r) - n \cdot vol\,(\Delta_0(n, (s - r)/r)) \\ &= \frac{(s/r)^n}{n!} - n \cdot \frac{(\frac{s-r}{r})^n}{n!}. \end{aligned} \tag{1.11}$$

Então, por (1.10) e (1.11) concluímos que

$$vol\,(\mathcal{A}) = \frac{s^n}{n!} - n \cdot \frac{(s - r)^n}{n!} = r^n \cdot \left(\frac{(s/r)^n}{n!} - n \cdot \frac{(\frac{s-r}{r})^n}{n!} \right) = r^n\, vol\,(\mathcal{B}).$$

□

Abaixo, provamos o principal resultado desta seção, necessário para provar o Lema 3.1.2:

Proposição 1.3.9. *Para $n \geq 3$, $u > 0, v \in \mathbb{R}$ fixados e t suficientemente grande, temos*

$$|\Lambda(n - 1, 2t, ut + v)| = 2^{n-1}\, vol(\Lambda(n - 1, 1, u/2))t^{n-1} + O(t^{n-2}).$$

Demonstração. Para $t \to \infty$,

$$\begin{aligned} vol\,(\Lambda(n - 1, 2t, ut + v)) &\to (2t)^{n-1}, \\ |\Lambda(n - 1, 2t, ut + v)| &\to (2t + 1)^{n-1} \end{aligned}$$

já que $\Lambda(n - 1, 2t, ut + v) \to [0, 2t]^{n-1}$. Daí,

$$|\,|\Lambda(n - 1, 2t, ut + v)| - vol\,(\Lambda(n - 1, 2t, ut + v))\,| \to |(2t + 1)^{n-1} - (2t)^{n-1}| \leq Ct^{n-2}$$

para alguma constante $C > 0$ e, então,

$$|\Lambda(n - 1, 2t, ut + v)| = vol\,(\Lambda(n - 1, 2t, ut + v)) + O(t^{d-2}). \tag{1.12}$$

Por outro lado, utilizando a Proposição 1.3.8, obtemos

$$\begin{aligned} vol\left(\Lambda(n-1,2t,ut+v)\right) &= (2t)^{n-1}\left(vol\left(\Lambda(n-1,1,u/2+v/2t)\right)\right) \\ &= (2t)^{n-1}\left(vol\left(\Lambda(n-1,1,u/2)\right)+\frac{c(v,n-1)}{t}\right), \end{aligned}$$

tal que $\dfrac{c(v,n-1)}{t}$ é o volume do corpo limitado pelos hiperplanos $H^{n-1}_{1,u/2}$ e $H^{n-1}_{1,u/2+v/2t}$ e contido no hipercubo $[0,1]^{n-1}$, com $c(v,n)\in\mathbb{R}$. Daí, temos

$$vol\left(\Lambda(n-1,2t,ut+v)\right) = 2^{n-1}\,vol\left(\Lambda(n-1,1,u/2)\right)t^{n-1}+O(t^{n-2}).$$

Portanto, por (1.12), concluímos que

$$|\Lambda(n-1,2t,ut+v)| = 2^{n-1}\,vol\left(\Lambda(n-1,1,u/2)\right)t^{n-1}+O(t^{n-2}).$$

□

A próxima proposição é também necessária para provarmos o Lema 3.1.2:

Proposição 1.3.10. *Para $n\geq 3$, temos*

$$vol\left(\Lambda(n-1,1,n/2)\right)+\ vol\left(\Lambda(n-1,1,n/2-1)\right)=\ vol\,[0,1]^{n-1}=1.$$

Demonstração. Seja

$$\Lambda(n-1,1,n/2-1)=\{(x_1,\cdots,x_{n-1})\in[0,1]^{n-1}\,/\,x_1+\cdots+x_{n-1}\leq n/2-1\}.$$

Considere a reflexão $x_i\mapsto 1-x_i$ sobre os pontos de $\Lambda(n-1,1,n/2-1)$. Definindo $y_i:=1-x_i$, segue que

$$x_i\in[0,1]\Rightarrow y_i\in[0,1] \text{ para todo } i\in\{1,\cdots,n\} \text{ e}$$

$$\begin{aligned} &\sum_{i=1}^{n-1}x_i\leq\frac{n}{2}-1\implies -\sum_{i=1}^{n-1}x_i\geq 1-\frac{n}{2}\implies \\ &(n-1)-\sum_{i=1}^{n-1}x_i\geq 1-\frac{n}{2}+(n-1)\implies \\ &\sum_{i=1}^{n-1}(1-x_i)\geq\frac{n}{2}\implies\sum_{i=1}^{n-1}y_i\geq\frac{n}{2}. \end{aligned}$$

Então

$$\mathcal{R}:=\{(y_1,\cdots,y_{n-1})\in[0,1]^{n-1}\,/\,y_1+\cdots+y_{n-1}\geq n/2\}$$

é o politopo obtido pela reflexão de $\Lambda(n-1,1,n/2-1)$ e, portanto, possuem o mesmo volume. Como

$$\Lambda(n-1,1,n/2) = \{(x_1,\cdots,x_{n-1}) \in [0,1]^{n-1} \,/\, x_1+\cdots+x_{n-1} \leq n/2\},$$

temos

$$\Lambda(n-1,1,n/2) \cup \mathcal{R} = [0,1]^{n-1}.$$

Daí,

$$\begin{aligned} 1 = vol\,([0,1]^{n-1}) = \; & vol\,(\Lambda(n-1,1,n/2) \cup \mathcal{R}) = \\ & vol\,(\Lambda(n-1,1,n/2)) + \; vol\,(\mathcal{R}) - \; vol\,(\Lambda(n-1,1,n/2) \cap \mathcal{R}) = \\ & vol\,(\Lambda(n-1,1,n/2)) + \; vol\,(\mathcal{R}) = \\ & vol\,(\Lambda(n-1,1,n/2)) + \Lambda(n-1,1,n/2-1) \end{aligned} \tag{1.13}$$

De fato, a igualdade (1.13) é válida já que a interseção $\Lambda(n-1,1,n/2) \cap \mathcal{R}$ é o hiperplano $H^{n-1}_{1,n/2} = \{(x_1,\cdots,x_{n-1})/x_1+\cdots+x_{n-1} = n/2\} \subset \mathbb{R}^{n-2}$ e tem volume $(n-1)$-dimensional nulo. □

Capítulo 2

Anéis com a Propriedade de Goldbach

Em 1965 [6], Hayes demonstrou que todo polinômio de grau $n \geq 1$ em $\mathbb{Z}[x]$ é uma soma de dois polinômios em $\mathbb{Z}[x]$, irredutíveis e de grau n. Este resultado foi, em 1998, redescoberto por Rattan e Stewart em [15].

Já em 2011 [14], Pollack buscou generalizar o teorema de Hayes em anéis polinomiais $R[x]$, com R sendo, *a priori*, um domínio arbitrário. Consideremos a seguinte propriedade:

Propriedade 2.0.1. *(Propriedade de Goldbach) Cada elemento de $R[x]$ de grau $n \geq 1$ pode ser escrito como soma de dois elementos de $R[x]$, irredutíveis e de grau n.*

Neste estudo, Pollack provou que qualquer domínio Noetheriano R com uma infinidade de ideais maximais satisfaz a Propriedade de Goldbach e, além disso, demonstrou que $R := S[x]$ satisfaz a Propriedade de Goldbach, para qualquer domínio S.

Neste capítulo nos dedicamos à demonstrar ambos resultados.

2.1 Resultados preliminares

Aqui estão os lemas necessários e mais relevantes ao desenvolvimento da próxima seção, que é a principal do capítulo.

Lema 2.1.1. *Suponha que P e Q são ideais comaximais de um anel comutativo com unidade. Então, para quaisquer inteiros positivos m, n, os ideais P^m e Q^n são comaximais.*

Demonstração. Dados P, Q ideais comaximais de um anel R com unidade, existem $a \in P$, $b \in Q$, tais que $1 = a + b$. Como R é comutativo, para quaisquer $m, n \in \mathbb{Z}_+$, temos:

$$1 = (a+b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} a^k b^{m+n-k} =$$

$$\sum_{k=0}^{m}\binom{m+n}{k}a^k b^{m+n-k}+\sum_{k=m+1}^{m+n}\binom{m+n}{k}a^k b^{m+n-k}.$$

Note que a primeira soma da última igualdade é divisível por $b^n \in Q^n$, e portanto pertence ao ideal Q^n. Da mesma forma, a segunda soma é divisível por $a^m \in P^m$, e portanto pertence ao ideal P^m. Logo, 1 pertence ao ideal $P^m + Q^n$, donde obtemos que $R = P^m + Q^n$. □

Lema 2.1.2. *Se R é um domínio Noetheriano e M é um ideal maximal não-nulo, então $M^2 \neq M$.*

Demonstração. Sendo R um anel Noetheriano e M um ideal maximal de R não-nulo, pelo Teorema 1.1.9 existem $g_1, \ldots, g_k \in R$ não-nulos tais que $M = \langle g_1, \ldots, g_k \rangle$, com $k \in \mathbb{N}$. Supondo $M = M^2$, temos $g_i \in M^2$, isto é, existem $m_i, x_i \in M$, tais que $g_i = m_i x_i$, para cada $i \in \{1, \ldots, k\}$. Como $x_i \in \langle g_1, \ldots, g_k \rangle$, existem $\alpha_{ij} \in R$ tais que:

$$g_i = m_i \cdot \sum_{j=1}^{k} \alpha_{ij} g_j = \sum_{j=1}^{k} (m_i \alpha_{ij}) g_j = \sum_{j=1}^{k} m_{ij} g_j, \tag{2.1}$$

com $m_{ij} = m_i \alpha_{ij} \in M$, para cada $i, j \in \{1, \ldots, k\}$.

Note que a matriz $A := ([m_{ij}] - Id)$ anula o vetor $v := [g_1, \ldots, g_k]^T$. De fato, por (2.1), temos:

$$\begin{bmatrix} (m_{11}-1) & m_{12} & \ldots & m_{1k} \\ m_{21} & (m_{22}-1) & \ldots & m_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ m_{k1} & m_{k2} & \ldots & (m_{kk}-1) \end{bmatrix} \cdot \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^{k} m_{1j} g_j - g_1 \\ \sum_{j=1}^{k} m_{2j} g_j - g_2 \\ \vdots \\ \sum_{j=1}^{k} m_{kj} g_j - g_k \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Portanto, $Av = \vec{0}$. Por outro lado, temos que R/M é corpo e que $\det(A) \neq 0$ em R/M já que, para todo $i, j \in \{1, \ldots, k\}$, $m_{ij} \equiv 0 \bmod M$ e $m_{jj} - 1 \equiv -1 \bmod M$ implica em $\det(A) = (-1)^k = \pm 1 \notin M$. Daí, A é inversível sobre R/M e então admite inversa A^{-1} em R. Mas $A^{-1}Av = \vec{0}$ nos dá que $v = \vec{0}$, o que é uma contradição. Logo, $M \neq M^2$. □

2.2 Resultados principais

Seja S um anel. A ordem (ou número de elementos) de S será denotada por $\#S$.

Lema 2.2.1. *Se R é um domínio Noetheriano, então a família de todos os seus ideais maximais M_i satisfazendo $\#R/M_i = 2$ é finita.*

Demonstração. Considere $\{M_i\}_{i\in I}$ a família de todos ideais maximais M_i de R tais que $\#R/M_i = 2$. Então R/M_i é um corpo de ordem 2, para todo $i \in I$. Daí, para todo $x \in R$, temos $x \in M_i$ ou $x - 1 \in M_i$ e, portanto, $x^2 - x \in M_i$, para todo $i \in I$.

Definindo $J := \bigcap_{i\in I} M_i$ e $S := R/J$, obtemos que $x^2 - x \in J$, para todo $x \in R$. Então, todo elemento de S é idempotente já que $\overline{x^2 - x} = \overline{0}$ nos dá que $\overline{x}^2 = \overline{x}$.

Agora, se P é um ideal primo qualquer de S, então todo elemento do domínio S/P é idempotente, por um argumento análogo ao anterior. Então $S/P \simeq \mathbb{Z}_2$ já que se $x \in S$ é não-nulo então $x(x-1) = 0$ e daí $x = 1$. Portanto, S/P é corpo e P é maximal.

Por outro lado, pelo Teorema 1.1.8, temos que S é anel Noetheriano e, pela Proposição 1.1.11, dado $< 0 >$ ideal próprio de S, existem $P_1, \cdots, P_k$ ideais primos de S distintos e $n_1, \cdots, n_k \in \mathbb{N}^*$ tais que $\langle 0\rangle = P_1^{n_1} P_2^{n_2} \cdots P_k^{n_k}$. Então, $S \simeq S/P_1^{n_1} \cdots P_k^{n_k}$.

Sabendo que cada P_i é maximal, P_i, P_j são comaximais e, pelo Lema 2.1.1, $P_i^{n_i}, P_j^{n_j}$ são também comaximais, para todos i, j distintos. Então, pelo Teorema 1.1.5, obtemos $S \simeq S/P_1^{n_1} \times \cdots \times S/P_k^{n_k}$.

Além disso, temos que $P_i^{n_i} \subseteq P_i$, para cada i. Como $P_i \subset S$, dado $x \in P_i$, temos $x = x^2$ e daí $x = x^{n_i}$ para todo $1 \leq i \leq k$. Portanto, $x \in P_i^{n_i}$. Isso mostra que $P_i = P_i^{n_i}$, para todo $i \in I$. Logo,

$$S \simeq S/P_1 \times \cdots \times S/P_k \simeq \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$$

e S é finito.

Então podemos afirmar que o conjunto de todos os ideais de S é finito e, pelo Teorema da Correspondência Bijetiva para anéis, o conjunto de todos os ideais de R que contém J é finito. Portanto, a família $\{M_i\}_{i\in I}$ é finita. □

Teorema 2.2.2. *Suponha que R é um domínio contendo ideais maximais P e Q, distintos, para os quais as seguintes condições se aplicam:*

(*i*) $\#\, R/P > 2$ *e* $\#\, R/Q > 2$;

(*ii*) $P^2 \neq P$ *e* $Q^2 \neq Q$.

Então R satisfaz a Propriedade de Goldbach.

Demonstração. Seja $f(x) = \sum_{i=0}^{n} a_i x^i$ um polinômio de $R[x]$ de grau $n \geq 1$.
No caso em que $n = 1$, se $a_1 \neq 1$ então podemos escolher a decomposição $f(x) = ((a_1 - 1)x + 1) + (x + a_0 - 1)$. Se $a_1 = 1$, escolhendo $r \notin \{0, 1\}$, temos que $f(x) = (rx + 1) + (1 - r)x + a_0 - 1$ é uma decomposição na forma desejada.

Para o caso em que $n \geq 2$, mostraremos que existem polinômios $g(x) = \sum_{i=0}^{n} b_i x^i$ e $h(x) = \sum_{i=0}^{n} c_i x_i$, ambos pertencentes à $R[X]$ e de grau n, satisfazendo as hipóteses do Lema 1.1.2, tais que $f = g + h$.

Dados P, Q ideais maximais de R, temos $P \subseteq P+Q \subseteq R$ e que P, Q são distintos, por hipótese. Portanto, P, Q são comaximais. Pelo Lema 2.1.1, temos que P^2, Q^2 são comaximais. Pela hipótese (ii), podemos fixar elementos $p \in P$, $q \in Q$ tais que $p \notin P^2$, $q \notin Q^2$. Então, usando a sobrejetividade da aplicação φ do Teorema 1.1.5, existem $b_0, b_1, \ldots, b_n \in R$ tais que

$$\begin{cases} b_i \equiv 0 \pmod{P} \\ b_i \equiv a_i \pmod{Q} \end{cases}, \tag{2.2}$$

para todo $i \in \{1, \ldots, n-1\}$,

$$\begin{cases} b_0 \equiv 0 \pmod{P} \\ b_0 \equiv p \pmod{P^2} \\ b_0 \equiv a_0 \pmod{Q} \\ b_0 \equiv (a_0 - q) \pmod{Q^2} \end{cases} \tag{2.3}$$

e

$$\begin{cases} b_n \not\equiv 0 \pmod{P} \\ b_n \not\equiv a_n \pmod{Q} \end{cases}. \tag{2.4}$$

Daí, definindo $c_i := a_i - b_i$, por esses sistemas de congruências conseguimos obter que $b_0, b_1, \ldots, b_{n-1}$ pertencem à P e $c_0, c_1, \ldots, c_{n-1}$ pertencem à Q, que b_0 não pertence à P^2 e c_0 não pertence à Q^2, e que b_n não pertence à P e c_n não pertence à Q. Isto garante a existência de polinômios g, h em $R[x]$ satisfazendo as três hipóteses do Lema 1.1.2 com respeito à P e à Q, respectivamente, tais que $f = g + h$.

Para garantir que a hipótese (iv) seja satisfeita, fixamos os $b_2, \ldots, b_{n-1}$ obtidos em (2.2) e colocamos condições adicionais para as escolhas de b_0, b_1 e b_n, além daquelas já estabelecidas.

Como $\# R/P > 2$ e $\# R/Q > 2$, é possível escolher b_n, c_n tais que também satisfaçam

$$b_n \not\equiv 0 \pmod{Q} \quad \text{e} \quad c_n \not\equiv 0 \pmod{P}.$$

Agora, escolhemos b_0 satisfazendo o sistema (2.3) com a congruência adicional

$$b_0 \equiv 1 \pmod{b_n}. \tag{2.5}$$

Isto é possível pois $b_n \notin P, Q$, e então os ideais P, Q e $\langle b_n \rangle$ são comaximais. Através do Lema 2.1.1, podemos usar o Teorema 1.1.5 que garante a existência de tal b_0.

Analogamente, é possível escolher b_1 satisfazendo o sistema (2.3) com a congruência adicional $b_1 \equiv a_1 - 1 \pmod{c_n}$. Daí,

$$1 - c_1 \in \langle c_n \rangle. \tag{2.6}$$

Por (2.5), temos $1 \in \langle b_0, b_n \rangle$ e por (2.6), temos $1 \in \langle c_1, c_n \rangle$. Portanto, b_0, b_n geram R, assim como c_1, c_n. Então, pelo Lema 1.1.2, obtemos polinômios $g(x) = \sum_{i=0}^{n} b_i x^i$ e $h(x) = \sum_{i=0}^{n} c_i x_i$ em $R[x]$, irredutíveis de grau n, tais que $f = g + h$. □

Neste momento, apresentamos o principal teorema do capítulo, cuja demonstração segue de forma bem direta dos resultados apresentados:

Teorema 2.2.3. *Suponha que R é um domínio Noetheriano que possui uma infinidade de ideais maximais. Então R satisfaz a Propriedade de Goldbach.*

Demonstração. Seja R um domínio Noetheriano com uma infinidade de ideais maximais M_i. Pelo Lema 2.2.1, há finitos ideais maximais M_i tais que $\# R/M_i = 2$. Então, existem $P \neq Q$ ideais maximais em R tais que $\# R/P > 2$, $\# R/Q > 2$. Daí, R cumpre a hipótese (i) do Teorema 2.2.2. Pelo Lema 2.1.2, $P^2 \neq P$, $Q^2 \neq Q$. Então R cumpre a hipótese (ii) do Teorema 2.2.2 e, portanto, R satisfaz a Propriedade de Goldbach. □

Encerramos o capítulo provando mais um importante teorema:

Teorema 2.2.4. *Se S é um domínio qualquer, então $R := S[x]$ satisfaz a Propriedade de Goldbach.*

Demonstração. Seja S um domínio e seja M um ideal maximal de S. Sabemos que $\mathbb{K} := S/M$ é corpo. Daí, por um análogo ao Teorema de Euclides, garantimos a existência de uma infinidade de polinômios irredutíveis mônicos $\overline{f(x)}$ em $\mathbb{K}[x]$, com $f(x) \in R := S[x]$ sendo mônico.

O ideal $\langle M, f(x) \rangle$ é maximal em R, para cada $\overline{f(x)}$ mônico irredutível em $\mathbb{K}[x]$. De fato, dado $\overline{f(x)} \in \mathbb{K}[x]$ mônico irredutível, a aplicação $\gamma : R \longrightarrow \dfrac{\mathbb{K}[x]}{\langle \overline{f(x)} \rangle}$, que associa cada $h(x) \in R$ à classe $\overline{h(x)} + \langle \overline{f(x)} \rangle$, é um homomorfismo de anéis sobrejetor cujo núcleo é $\langle M, f(x) \rangle$. Então, pelo Teorema do Isomorfismo de Anéis, $\dfrac{R}{\langle M, f(x) \rangle} \simeq \dfrac{\mathbb{K}[x]}{\langle \overline{f(x)} \rangle}$, tal que $\langle \overline{f(x)} \rangle$ é maximal em $\mathbb{K}[x]$. Daí, o ideal $\langle M, f(x) \rangle$ é maximal em R.

Note que o domínio R satisfaz a condição (i) do Teorema 2.2.2. Com efeito, sabemos que $\mathbb{K}[x]$ é um domínio Noetheriano pelo Teorema 1.1.10 e que possui uma infinidade destes ideais maximais $\langle \overline{f(x)} \rangle$. Então, pelo Lema 2.2.1, existem ideais $\langle \overline{f(x)} \rangle \neq \langle \overline{g(x)} \rangle$ maximais em $\mathbb{K}[x]$ tais que $\# \dfrac{\mathbb{K}[x]}{\langle \overline{f(x)} \rangle}, \# \dfrac{\mathbb{K}[x]}{\langle \overline{g(x)} \rangle} > 2$. Consequentemente, obtemos $f(x) \neq g(x) \in R$ mônicos tais que os ideais maximais $P := \langle M, f(x) \rangle, Q := \langle M, g(x) \rangle$ são distintos e satisfazem $\# \dfrac{R}{\langle M, f(x) \rangle}, \# \dfrac{R}{\langle M, g(x) \rangle} > 2$.

Observe também que $P \neq P^2$, $Q \neq Q^2$. De fato, temos $f(x) \notin P^2$ já que, do contrário, teríamos $f(x) = a(x) \cdot M^2 + b(x) \cdot M \cdot f(x) + c(x) \cdot f(x)^2$, com $a(x), b(x), c(x) \in R$ e, então, $\overline{f(x)}^2$ dividiria $\overline{f(x)}$ em $\mathbb{K}[x]$, o que é um absurdo. Analogamente, obtemos $g(x) \notin Q^2$.

Portanto, pelo Teorema 2.2.2, concluímos que R satisfaz a Propriedade de Goldbach. □

Observação 2.2.5. *Sabemos que, para qualquer domínio S, $R := S[x_1, x_2, \cdots, x_n]$ é também um domínio. Então, pelo Teorema 2.2.4, concluímos que R satisfaz a Propriedade de Goldbach, para todo $n \geq 1$.*

Capítulo 3

Uma análise assintótica para $\mathcal{N}(f,k,t)$

Seja $f(x)$ um polinômio mônico em $\mathbb{Z}[x]$ de grau $d \geq 2$, e sejam $k \geq 2, t$ dois números inteiros. Denotamos por $\mathcal{N}(f,k,t)$ o número de representações (distintas) de f por soma de k polinômios inteiros mônicos e irredutíveis sobre $\mathbb{Q}$, $f_1, f_2, \ldots, f_k$,

$$f(x) = f_1(x) + f_2(x) + \ldots + f_k(x),$$

tais que, para cada $1 \leq i \leq k$, a altura de $f_i(x) := x^{d_i} + y_{i,d_i-1}x^{d_i-1} + \ldots + y_{i,1}x + y_{i,0}$ definida por $H(f_i) := \max_{1\leq j\leq d_i}|y_{i,d_i-j}|$ é no máximo t.

Em 2006 [16], Saidak mostrou que, para t suficientemente grande,

$$t^{d-1} \ll \mathcal{N}(f,2,t) \ll t^{d-1}.$$

Em 2010 [10], Kozek melhorou o resultado provando que $\mathcal{N}(f,2,t) \sim (2t)^{d-1}$.

Neste capítulo, mostramos o estudo realizado por Dubickas [2], em 2011, o qual prova uma fórmula assintótica para $\mathcal{N}(f,k,t)$, com $k \geq 2$, e obtém o melhor termo de erro possível para $\mathcal{N}(f,2,t)$, quando $d \geq 4$.

3.1 Resultados preliminares

Nesta seção, provamos lemas auxiliares à próxima seção e apresentamos um lema que assumimos e utilizamos mais adiante.

Lema 3.1.1. *Sejam a, d, t e s inteiros tais que $d \geq 3$ e $t \geq |s| \geq 2$. Então o número de soluções $(h_{d-2}, \ldots, h_0) \in \mathbb{Z}^{d-1}$ da equação linear*

$$s^d + as^{d-1} + h_{d-2}s^{d-2} + \ldots + h_1 s + h_0 = 0,$$

satisfazendo $|h_i| \leq t$, para cada $i \in \{0, 1, \ldots, d-2\}$, não excede $\left(\dfrac{2t}{|s|} + 1\right)^{d-2}$.

Demonstração. É suficiente provarmos o lema para $s > 0$ pois se $s < 0$ podemos trocar s por $-s$ e a por $-a$, se necessário, o que não altera o número de soluções da equação. Já que $s|h_0$, seja $H_0 := h_0/s \in \mathbb{Z}$. Como $t \geq s|H_0|$, H_0 pode assumir no máximo $2\lfloor t/s \rfloor + 1 \leq 2t/s + 1$ valores, onde $\lfloor x \rfloor$ é o maior inteiro menor ou igual à x. Então h_0 assume no máximo $2t/s + 1$ valores inteiros. Por

$$s^{d-1} + as^{d-2} + \ldots + h_2 s + h_1 + h_0/s = 0,$$

obtemos que s divide $h_1 + h_0/s = h_1 + H_0$, tal que $H_1 := (h_1 + H_0)/s \in \mathbb{Z}$. Como $|h_1| \leq t$, para cada h_0 fixado temos

$$t/s \geq |H_1 - H_0/s| = |H_1 - h_0/s^2|,$$

o que nos fornece o máximo de $2\lfloor t/s \rfloor + 1 \leq 2t/s + 1$ valores para H_1 e então h_1 assume no máximo $2t/s + 1$ valores inteiros para cada h_0. Prosseguindo desta maneira, isto é, cada vez dividindo a equação anterior por s e considerando h_j para $h_{j-1}, \ldots, h_0$ fixos, obtemos o fator $2t/s + 1$, para cada $j \leq d - 3$, restando apenas h_{d-2}, o qual fica unicamente determinado pelos $h_{d-3}, \ldots, h_0$. Logo, o número de soluções $(h_{d-2}, \ldots, h_0) \in \mathbb{Z}^{d-1} \cap [-t, t]$ da equação linear não excede $(2t/s + 1)^{d-2}$ para $s > 0$ e $(2t/(-s) + 1)^{d-2}$ para $s < 0$, resultando no máximo de $(2t/|s| + 1)^{d-2}$ soluções. □

Lema 3.1.2. *Dados $b_0 \in \mathbb{Z}$, $n \geq 2$, e $b_1, \ldots, b_n$ inteiros não-nulos, definimos $N(b_1, \ldots, b_n, b_0, t)$ como o número de soluções $(y_1, \ldots, y_n) \in \mathbb{Z}^n$ da equação linear*

$$b_1 y_1 + \ldots + b_n y_n = b_0, \tag{3.1}$$

tais que $|y_i| \leq t$ para cada $1 \leq i \leq n$. Então

$$N(b_1, \ldots, b_n, b_0, t) \leq (2t + 1)^{n-1}, \tag{3.2}$$

para cada $t \in \mathbb{N}$. Além disso,

$$N(1, \ldots, 1, b_0, t) = 2^{n-1}(1 - 2V_{n-1})t^{n-1} + O(t^{n-2}) \text{ para } t \to \infty, \tag{3.3}$$

onde V_n foi definido no Exemplo 1.3.6.

Demonstração. Para provarmos (3.2), observe que y_n é unicamente determinado, a partir da equação (3.1), por cada vetor $(y_1, \ldots, y_{n-1}) \in \mathbb{Z}^{n-1} \cap [-t, t]^{n-1}$ e daí há no máximo $(2t+1)^{n-1}$ de tais vetores, pois cada y_i pode assumir até $2t+1$ valores inteiros. Portanto, existem no máximo $(2t + 1)^{n-1}$ soluções inteiras para a equação linear dada.

Para (3.3), precisamos estimar o número de soluções $(y_1, \cdots, y_{n-1}) \in \mathbb{Z}^{n-1} \cap [-t, t]^{n-1}$ para a equação $y_1 + \cdots + y_n = b_0$. Como $y_n \in [-t, t]$, as soluções de interesse satisfazem

$$-t + b_0 \leq \sum_{i=1}^{n-1} y_i \leq t + b_0. \tag{3.4}$$

Para $n = 2$ temos $y_1 + y_2 = b_0$. Então, quando $t \to \infty$,

$$N(1, 1, b_0, t) = 2t + 1 = 2t + O(1).$$

Consideramos agora $n \geq 3$. Substituindo y_i por $x_i - t$, temos

$$\begin{aligned} &0 \leq x_n \leq 2t \text{ e } b_0 = (\sum_{i=1}^{n} x_i) - nt \Rightarrow \\ &-b_0 \leq nt - \sum_{i=1}^{n-1} x_i \leq 2t - b_0 \Leftrightarrow \\ &-b_0 - nt \leq -\sum_{i=1}^{n-1} x_i \leq (2-n)t - b_0. \end{aligned}$$

Então (3.4) equivale à

$$(n-2)t + b_0 \leq \sum_{i=1}^{n-1} x_i \leq nt + b_0, \text{ com } (x_1, \cdots, x_{n-1}) \in \mathbb{Z}^{n-1} \cap [0, 2t]^{n-1}, \tag{3.5}$$

isto é, $N(1, \cdots, 1, b_0, t)$ é o número de pontos $(x_1, \cdots, x_{n-1})$ satisfazendo (3.5).

Como definido em (1.7), dados $u > 0, v \in \mathbb{R}$, $|\Lambda(n-1, 2t, ut+v)|$ é o número de pontos $(x_1, \cdots, x_{n-1}) \in \mathbb{Z}^{n-1} \cap [0, 2t]^{n-1}$ tais que $\sum_{i=1}^{n-1} x_i \leq ut + v$.
Então, para $t \geq |b_0| + 1$ e $n \geq 3$, temos $(n-2)t + b_0 \geq 0$ e $nt + b_0 \geq 0$ e, portanto, (3.5) implica em

$$N(1, \cdots, 1, b_0, t) = |\Lambda(n-1, 2t, nt + b_0)| - |\Lambda(n-1, 2t, (n-2)t + b_0 - 1)|. \tag{3.6}$$

Usando a Proposição 1.3.9, temos

$$\begin{aligned} &|\Lambda(n-1, 2t, nt + b_0)| = 2^{n-1}\, vol(\Lambda(n-1, 1, n/2))t^{n-1} + O(t^{n-2}), \\ &|\Lambda(n-1, 2t, (n-2)t + b_0 - 1)| = 2^{n-1}\, vol(\Lambda(n-1, 1, n/2-1))t^{n-1} + O(t^{n-2}) \end{aligned}$$

e, por (3.6), o número $N(1, \cdots, 1, b_0, t)$ para t suficientemente grande é

$$2^{n-1}(\, vol(\Lambda(n-1, 1, n/2)) - \, vol(\Lambda(n-1, 1, n/2-1)))t^{n-1} + O(t^{n-2}). \tag{3.7}$$

Pela Proposição 1.3.10, $vol(n-1, 1, n/2) = 1 - vol(n-1, 1, n/2-1)$. Como $V_{n-1} := vol(n-1, 1, n/2-1)$, por (3.7) segue que

$$N(1, \cdots, 1, b_0, t) = 2^{n-1}(1 - 2V_{n-1})t^{n-1} + O(t^{n-2}).$$

□

Assumimos o seguinte resultado de Van Der Waerden e omitimos a demonstração (detalhada em [18]) devido à falta de uma versão traduzida para o inglês:

Lema 3.1.3. *Seja $M_\ell(d,t)$ o conjunto dos polinômios inteiros mônicos de grau $d \geq 2$, altura no máximo t e que possui algum fator de grau ℓ, com $1 \leq \ell \leq d/2$. Então, para $t \to \infty$,*

(i) $t^{d-\ell} \ll |M_\ell(d,t)| \ll t^{d-\ell}$, *para* $\ell < d/2$ *e*

(ii) $t^{d/2} \log t \ll |M_{d/2}(d,t)| \ll t^{d/2} \log t$ *para* d *par e* $\ell = d/2$,

com as constantes em $\ll$ dependendo apenas de d e ℓ.

Denotamos por $M(a,d,t)$ o conjunto de todos os polinômios inteiros mônicos redutíveis de grau d, altura no máximo t e com o coeficiente de x^{d-1} igual à a. Com respeito à cardinalidade do conjunto $M(a,d,t)$, que denotamos por $|M(a,d,t)|$, apresentamos o seguinte resultado:

Lema 3.1.4. *Se $d, t \geq 2$ e a são três inteiros então, para $t \to \infty$, temos*

(i) $t^{d-2} \ll |M(a,d,t)| \ll t^{d-2}$, *para* $d \geq 4$,

(ii) $t \log t \ll |M(a,3,t)| \ll t \log t$,

(iii) $\sqrt{t} \ll |M(a,2,t)| \ll \sqrt{t}$,

onde todas as constantes implícitas em $\ll$ dependem apenas de d.

Demonstração. Começamos por (iii). Precisamos estimar o número de polinômios mônicos redutíveis $x^2 + ax + b \in \mathbb{Z}[x]$, tais que a é um inteiro fixo e $|b| \leq t$. Tal polinômio é redutível se e somente se admite alguma raiz inteira, digamos s. Então devemos ter $b = -s^2 - as$ e, então, $|s^2 + as| \leq t$. Resolvendo a inequação, obtemos

$$|s + a/2| \leq \frac{\sqrt{a^2 + 4t}}{2} \leq |a|/2 + \sqrt{t},$$

isto é, s assume até $1 + |a| + 2\sqrt{t}$ valores inteiros e, como a é fixo, $|M(a,2,t)| \ll \sqrt{t}$. Além disso, note que no máximo dois inteiros distintos, s e s', são raízes do mesmo polinômio $x^2 + ax + b$ que, neste caso, é contado duas vezes em $|M(a,2,t)|$. Daí, obtemos $\sqrt{t} \leq \dfrac{1 + |a| + 2\sqrt{t}}{2} \leq |M(a,2,t)|$ e, portanto,

$$\sqrt{t} \ll |M(a,2,t)| \ll \sqrt{t}.$$

Para encontrar a limitação inferior em (ii), inicialmente fixamos $g(x) := x + a$. Note que qualquer polinômio redutível da forma $f(x) = g(x)x^2 + h_1 x + h_0$, com $|h_1|, |h_0| \leq t$, e $h_1, h_0 \in \mathbb{Z}$, pertence à $M(a,3,t)$.

Consideramos todos os pares $(y_1, y_2) \in \mathbb{Z}^2$ tais que $1 \leq y_1 \leq \lceil t^{1/4} \rceil$, $y_1 < y_2$ e $y_1 y_2 \leq t/2$, onde $\lceil x \rceil$ é o menor inteiro maior ou igual à x. Então

$$\lceil t/(2y_1) \rceil - y_1 \geq t/2y_1 - y_1 \geq y_2 - y_1 > 0$$

e o número de tais pares, para t suficientemente grande, é

$$\sum_{y_1=1}^{\lceil t^{1/4}\rceil} (\lceil t/2y_1\rceil - y_1) > \frac{t}{3}\sum_{y_1=1}^{\lceil t^{1/4}\rceil}\frac{1}{y_1} > \frac{t\log t}{13}. \tag{3.8}$$

Com efeito, sabendo que $\lceil x\rceil < 1+x$, temos $t > 6(1+t^{1/4})^2 > 6\lceil t^{1/4}\rceil^2$, para t suficientemente grande. Assim, $t > 6y_1^2$ e, então, $\lceil t/2y_1\rceil - t/3y_1 > t/2y_1 - t/3y_1 > y_1$, para t suficientemente grande. Isto prova a primeira desigualdade.

Para verificar a segunda, vejamos que vale a seguinte desigualdade, para $t\to\infty$:

$$\int_2^{\lceil t^{1/4}\rceil}\frac{1}{y_1}\,dy_1 = \log\frac{\lceil t^{1/4}\rceil}{2} > \log t^{3/13}. \tag{3.9}$$

Como $1/4 > 3/13$, temos $\lceil t^{1/4}\rceil/2 > \lceil t^{3/13}\rceil > t^{3/13}$, para t suficientemente grande. Isto prova (3.9).

Agora, considere o polinômio $f_{y_1,y_2}(x) := g(x)x^2 - (y_2 + y_1g(y_1))x + y_1y_2 \in \mathbb{Z}[x]$. Vejamos que $f_{y_1,y_2}\in M(a,3,t)$.

Desde que $y_1y_2 \le t/2$, $1\le y_1 < y_2$, e $|g(y_1)| = |y_1+a|$, com a fixo, temos $|y_2|, |y_1||g(y_1)| \le t/2$, para algum t suficientemente grande, e então

$$|y_2 + y_1g(y_1)| \le t/2 + t/2 = t,$$

para t suficientemente grande. Portanto, $H(f_{y_1,y_2}) \le t$. Além disso, $f_{y_1,y_2}(y_1) = 0$, isto é, f_{y_1,y_2} é redutível e assim temos $f_{y_1,y_2}\in M(a,3,t)$.

Mostremos que f_{y_1,y_2} é o mesmo para no máximo 3 pares (y_1,y_2) distintos com as restrições acima pois, combinado com (3.8), resulta que

$$M(a,3,t) > \frac{t\log t}{13\cdot 3} \gg t\log t,$$

para t suficientemente grande. Fixamos um par qualquer de inteiros positivos (s_1,s_2) e assumimos que $f_{s_1,s_2} = f_{y_1,y_2}$, para algum par de inteiros positivos (y_1,y_2). Então

$$s_1s_2 = y_1y_2, \quad s_2 + s_1g(s_1) = y_2 + y_1g(y_1).$$

Defina $\lambda := y_1/s_1 \in \mathbb{Q}$. Pela primeira igualdade acima, temos $y_2 = s_2/\lambda$. Usando isto na segunda igualdade e multiplicando-a por λ, segue que

$$s_1g(\lambda s_1)\lambda^2 - (s_2 + s_1g(s_1))\lambda + s_2 = 0.$$

Assim, obtemos um polinômio em λ de grau 3 e o máximo de 3 números racionais λ distintos satisfazendo $f_{\lambda s_1,\lambda^{-1}s_2} = f_{s_1,s_2}$, isto é, há no máximo 3 pares distintos de inteiros positivos (y_1,y_2) tais que $f_{s_1,s_2} = f_{y_1,y_2}$.

Agora, provemos a limitação superior. Para cada $d \geq 3$, o número de polinômios $x^d + ax^{d-1} + y_{d-2}x^{d-2} + \ldots + y_1 x$ em $M(a,d,t)$, que possui $s = 0$ como raiz, é no máximo $(2t+1)^{d-2}$, pois cada y_i pode assumir até $2t+1$ valores em $\mathbb{Z}$ para cada $i \in \{1, \cdots, d-2\}$. Além disso, o número de soluções $(y_0, \ldots, y_{d-2}) \in \mathbb{Z}^{d-1}$ da equação linear

$$y_0 + y_1 + \ldots + y_{d-2} = -(a+1),$$

com $|y_i| \leq t$ para cada $i \in \{1, \cdots, d-2\}$, é exatamente o número de polinômios em $M(a,d,t)$ que possuem $s = 1$ como raiz e, pelo Lema 3.1.2, este número não excede $(2t+1)^{d-2}$ (o mesmo vale para aqueles que possuem raiz $s = -1$). Então o número de polinômios em $M(a,d,t)$ que possui raiz $s \in \{-1, 0, 1\}$ não excede

$$3\,(2t+1)^{d-2}\,. \tag{3.10}$$

Observe que todo polinômio em $M(a,3,t)$ possui uma raiz $s \in [-t,t]$ (já que possui um fator linear cujo termo constante está limitado em valor absoluto por t e é uma raiz) e, caso $t \geq |s| \geq 2$, pelo Lema 3.1.1 há no máximo

$$(2t/|s|+1) \tag{3.11}$$

destes polinômios, para cada s fixado. Daí, combinando isto com (3.10) para $d = 3$, obtemos

$$\begin{aligned} |M(a,3,t)| \;&\leq\; 3(2t+1) + \sum_{|s|=2}^{t} (2t/|s|+1) \leq\; 6t + 3 + 2\int_1^t (2t/s+1)ds \\ &=\; 8t + 1 + 4t\log t \;\ll\; t\,\log\,t\,, \end{aligned}$$

para t suficientemente grande.

Para o caso (i), suponha $d \geq 4$. Se $|a| \leq t$, então há exatamente $(2t+1)^{d-2}$ polinômios em $M(a,d,t)$ que possuem 0 como raiz. Daí,

$$|M(a,d,t)| \;\geq\; (2t+1)^{d-2} \gg t^{d-2}.$$

Resta provar o limitante superior.

Seja $M_1(a,d,t)$ o subconjunto de $M(a,d,t)$ formado por todos os polinômios que possuem um fator irredutível de grau $d-1$ (isto é, possuem apenas uma raiz inteira) e seja $M_\ell(d,t)$, o conjunto definido no Lema 3.1.3, com $1 \leq \ell \leq \lfloor d/2 \rfloor$.

Se $f(x) = p(x)q(x) \in M(a,d,t) \setminus M_1(a,d,t)$ é sua decomposição em fatores irredutíveis $p(x), q(x) \in \mathbb{Z}[x]$ então $2 \leq \partial\, p(x) \leq \lfloor d/2 \rfloor$ ou $2 \leq \partial\, q(x) \leq \lfloor d/2 \rfloor$, e daí

$$M(a,d,t) \setminus M_1(a,d,t) \subset \bigcup_{\ell=2}^{\lfloor d/2 \rfloor} M_\ell(d,t).$$

Assim,

$$|M(a,d,t) \setminus M_1(a,d,t)| \leq |M_2(d,t)| + \ldots + |M_{\lfloor d/2 \rfloor}(d,t)|.$$

Então, quando $t \to \infty$, pelo Lema 3.1.3 obtemos

$$|M(a,d,t) \setminus M_1(a,d,t)| \ll t^{d-2} + \ldots + t^{d-\lfloor d/2 \rfloor} \ll t^{d-2} \tag{3.12}$$

para $d \geq 5$ e ímpar, pois $\lfloor d/2 \rfloor \geq 2$, e também

$$|M(a,d,t) \setminus M_1(a,d,t)| \ll t^{d-2} + \ldots + t^{d/2} \log t \ll t^{d-2} \tag{3.13}$$

para $d \geq 6$ e par, pois $1 \leq d/2 - 2$ nos dá que $\log t \leq t \leq t^{d/2-2}$ e então $t^{d/2} \log t \leq t^{d-2}$.

Vejamos que também ocorre

$$|M(a,d,t) \setminus M_1(a,d,t)| \ll t^{d-2} \tag{3.14}$$

quando $d = 4$.

Note que todo polinômio em $M(a,4,t) \setminus M_1(a,4,t)$, que não é um produto de dois polinômios quadráticos irredutíveis, possui uma raiz $s \in [-t,t]$. Novamente por (3.10) e (3.11), o número de tais polinômios não excede

$$\begin{aligned} 3(2t+1)^2 + \sum_{|s|=2}^{t} (2t/|s|+1)^2 &\leq 27t^2 + 2\int_1^t (2t/s+1)^2\, ds \\ &\leq 27t^2 + 2(4t^2 + 4t\log t - 3t - 1) \ll t^2, \end{aligned}$$

para t suficientemente grande.

Considere $f(x) = (x^2 + a_1x + b_1)(x^2 + a_2x + b_2) \in M(a,4,t) \setminus M_1(a,4,t)$, com $x^2 + a_1x + b_1, x^2 + a_2x + b_2$ irredutíveis. Note que $a_1 + a_2 = a$ e $b_1, b_2 \neq 0$. Como a altura de f é no máximo t, os coeficientes constantes e de x^2 nos fornecem

$$|b_1b_2| \leq t \quad \text{e} \quad |b_1 + b_2 + a_1a_2| = |b_1 + b_2 + a_1(a - a_1)| \leq t. \tag{3.15}$$

Daí, os pares (b_1, b_2) tais que $b_1b_2 \leq t$ e $1 \leq b_1 \leq b_2$ satisfazem $\lfloor t/b_1 \rfloor - b_1 + 1 > 0$ e totalizam

$$\begin{aligned} \sum_{b_1=1}^{\lfloor \sqrt{t} \rfloor} (\lfloor t/b_1 \rfloor - b_1 + 1) &\leq t + \sum_{b_1=2}^{\sqrt{t}} (t/b_1 - b_1 + 1) \leq t + \int_1^{\sqrt{t}} \frac{t}{b_1} - b_1 + 1\; db_1 \\ &= t\left(\log\sqrt{t} + \frac{\sqrt{t}}{t} - \frac{1}{2t} + \frac{1}{2}\right) \ll t\log t. \end{aligned} \tag{3.16}$$

Então, o número de pares $(b_1, b_2) \in \mathbb{Z}^2$ tais que $|b_1b_2| \leq t$ é também $\ll t\log t$. Além disso, $-t/|b_1| \leq b_2 \leq t/|b_1|$ e $-t \leq b_1 \leq t$. Então $-1-t \leq b_1+b_2 \leq 1+t$, isto é, $|b_1+b_2| \leq t+1$.

Daí, usando a segunda desigualdade de (3.15), obtemos

$$|a_1^2 - aa_1| \leq t + |b_1 + b_2| \leq 2t + 1,$$

para cada par (b_1, b_2) fixado. Portanto, o número de pares (a_1, a_2) satisfazendo esta inequação é $\ll \sqrt{t}$. Isso combinado com (3.16) fornece que o número de polinômios $f(x) = (x^2 + a_1x + b_1)(x^2 + a_2x + b_2) \in M(a, 4, t) \setminus M_1(a, 4, t)$ é

$$\sqrt{t}\,(t \log t) = t^{3/2} \log t \ll t^{3/2}t^{1/2} = t^2,$$

como queríamos.

Agora, observe que todo polinômio em $M_1(a, d, t)$ possui uma raiz $s \in [-t, t]$. Então, utilizando (3.10) e um análogo à (3.11), encontramos que

$$\begin{aligned} |M_1(a, d, t)| \;&\leq\; 3(2t + 1)^{d-2} + 2\sum_{s=2}^{t}(2t/s + 1)^{d-2} \;\leq\; 3(3t)^{d-2} + 3^{d-1}t^{d-2}\sum_{s=2}^{t}(3t/s)^{d-2} \\ &<\; 3^{d-1}t^{d-2} + 3^{d-1}t^{d-2}\sum_{s=2}^{\infty}(1/s^{d-2}) \;\ll\; t^{d-2}, \end{aligned}$$

já que $d - 2 \geq 2$.

Portanto, segue por (3.12), (3.13) e (3.14) que

$$|M(a, d, t)| \;\leq\; |M_1(a, d, t)| + |M(a, d, t) \setminus M_1(a, d, t)| \;\ll t^{d-2} + t^{d-2} \;\ll\; t^{d-2},$$

para todo $d \geq 4$. □

3.2 Resultados principais

Lema 3.2.1. *Sejam $f(x) \in \mathbb{Z}[x]$ um polinômio mônico de grau $d \geq 2, k \geq 2$ e $\mathcal{N}_1(f, k, t)$ o número de representações de f como soma de k polinômios inteiros mônicos irredutíveis $f_1, f_2, \ldots, f_k$ de alturas no máximo t e graus $d, d-1, \ldots, d-1$, respectivamente. Então*

$$0 \;\leq\; \mathcal{N}(f, k, t) - \mathcal{N}_1(f, k, t) \;\ll\; t^{dk-d-k},$$

onde a constante em $\ll$ depende apenas de d e k.

Demonstração. Fixamos $f(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_0 \in \mathbb{Z}[x]$. Cada representação de f como soma de polinômios inteiros mônicos $f_1, f_2, \ldots, f_k$, de alturas no máximo t contém exatamente um polinômio de grau d, digamos f_1, e $k-1$ polinômios cujos graus são no máximo $d-1$. Estimaremos o número de tais representações em que $\partial f_1(x) = d$ e existe $i \in \{2, \ldots, k\}$ tal que $\partial f_i(x) = d - 1$. Assumimos que existem q polinômios $f_i's$ tais que $\partial f_i(x) < d - 1$, para $q \in \{1, \cdots, k-1\}$. Então o coeficiente de x^{d-1} em f_1 é igual à $a_{d-1} - (k - 1 - q) \cdot 1 = a_{d-1} - k + q + 1$.

Denotamos os coeficientes de x^{d-j} em f_i por $y_{i,d-j}$, para cada $i \in \{1, \cdots, k\}, j \in \{2, \cdots, d\}$. Como $f = f_1 + \ldots + f_k$, devemos ter

$$\begin{cases} a_0 &= \sum_{i=1}^{k} y_{i,0} \\ a_1 &= \sum_{i=1}^{k} y_{i,1} \\ \vdots &= \vdots \\ a_{d-2} &= \sum_{i=1}^{k} y_{i,d-2} \end{cases} \tag{3.17}$$

e também $|y_{i,d-j}| \leq t$, para cada $i \in \{1, \cdots, k\}, j \in \{2, \cdots, d\}$.

Se $j = 2$, temos q coeficientes conhecidos na equação $a_{d-2} = \sum_{i=1}^{k} y_{i,d-2}$, já que alguns podem ser 1 e outros podem ser 0. Daí, há no máximo $k - q$ incógnitas. Pelo Lema 3.1.2, o número de soluções $(y_{1,d-2}, \ldots, y_{k,d-2}) \in \mathbb{Z}^k \cap [-t, t]^k$ desta equação não excede $(2t+1)^{k-q-1}$. Além disso, para cada $j \in \{3, \ldots, d\}$, a correspondente equação linear em (3.17) possui no máximo k incógnitas e, novamente pelo Lema 3.1.2, o número de suas soluções não excede $(2t+1)^{k-1}$.

Portanto, para cada $q \in \{1, \ldots, k-1\}$ fixado, o número de soluções inteiras do sistema (3.17), satisfazendo $|y_{i,d-j}| \leq t$, é

$$\leq (2t+1)^{k-q-1}(2t+1)^{(k-1)(d-3+1)} = (2t+1)^{(k-1)(d-1)-q} \leq 3^{(k-1)(d-1)} t^{dk-d-k}. \tag{3.18}$$

Por outro lado, para cada $q \in \{1, \ldots, k-1\}$, existem $\binom{k-1}{q}$ possibilidades para escolher os correspondentes q polinômios f_i, com $2 \leq i \leq k$, cujos graus são estritamente menores que $d - 1$. Então, combinando com (3.18), obtemos que

$$0 \leq \mathcal{N}(f,k,t) - \mathcal{N}_1(f,k,t) \leq 3^{(k-1)(d-1)} \left(\sum_{q=1}^{k-1} \binom{k-1}{q} \right) t^{dk-d-k} \ll t^{dk-d-k}.$$

□

Lema 3.2.2. *Sejam $f(x) \in \mathbb{Z}[x]$ um polinômio mônico de grau $d \geq 2$, um inteiro $k \geq 2$ e $\mathcal{N}_2(f,k,t)$, o número de representações de f como soma de k polinômios inteiros mônicos $f_1, f_2, \ldots, f_k$ de alturas no máximo t e graus $d, d-1, \ldots, d-1$, respectivamente. Então, para $t \to \infty$,*

$$\mathcal{N}_2(f,k,t) = \frac{\left(2^{k-1}(1 - 2V_{k-1})\right)^{d-1}}{(k-1)!} t^{(k-1)(d-1)} + O(t^{dk-d-k}),$$

para cada $d \geq 2$.

Demonstração. Fixamos $f(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_0 \in \mathbb{Z}[x]$. Usando as notações do lema anterior, temos $q = 0$, $a = a_{d-1} - k + 1$,

$$f_1(x) = x^d + ax^{d-1} + \sum_{j=2}^{d} y_{1,d-j} x^{d-j},$$

$$f_i(x) = x^{d-1} + \sum_{j=2}^{d} y_{i,d-j} x^{d-j},$$

para $i \in \{2, \ldots, k\}$. Note que $f = f_1 + \ldots + f_k$ se, e só se, as $k(d-1)$ incógnitas $y_{i,d-j}$ satisfazem o sistema linear (3.17). Então, aplicando a equação (3.3) do Lema 3.1.2 em cada uma das $d-1$ equações do sistema, obtemos que (3.17) tem

$$\left(2^{k-1}(1-2V_{k-1})t^{k-1} + O(t^{k-2})\right)^{d-1} =$$

$$\left(2^{k-1}(1-2V_{k-1})\right)^{d-1} t^{(k-1)(d-1)} + O(t^{dk-d-k}) \tag{3.19}$$

soluções inteiras satisfazendo $|y_{i,d-j}| \leq t$, para t suficientemente grande.

Agora, vejamos que o número destas soluções tais que $f_i = f_l$, para algum $i \neq l$, é $O(t^{dk-d-k})$. De fato, como f_1 é mônico de grau d, $f_1 \neq f_l, \forall\, l > 1$. Se $f_i = f_l$, para alguns índices i, l satisfazendo $2 \leq i < l \leq k$, então $k \geq 3$ e $y_{i,d-j} = y_{l,d-j}$, para cada $j \in \{2, \ldots, d\}$. Portanto, o sistema linear (3.17) possui apenas $(k-1)(d-1)$ incógnitas. Aplicando (3.2) em cada uma das $d-1$ equações lineares, com $n = k-1$, obtemos que o número de soluções inteiras do sistema satisfazendo $|y_{i,d-j}| \leq t$, para t suficientemente grande, não excede

$$(2t+1)^{(k-2)(d-1)} = (2t+1)^{dk-d-k+2-d} = O(t^{dk-d-k})$$

pois $2 - d \leq 0$.

Então podemos assumir que os polinômios $f_1, \ldots, f_k$ de grau $d, d-1, \ldots, d-1$, respectivamente, são distintos. É claro que todas as coleções de polinômios $f_1, f_{\sigma(2)}, \ldots, f_{\sigma(k)}$, com σ percorrendo todas as permutações do conjunto $\{2, \ldots, k\}$, são as mesmas. Portanto, ao contar as soluções de (3.17), em (3.19) levamos em conta cada coleção de polinômios distintos $f_1, \ldots, f_k$ exatamente $(k-1)!$ vezes. Logo,

$$\mathcal{N}_2(f, k, t)(k-1)! = \left(2^{k-1}(1-2V_{k-1})\right)^{d-1} t^{(k-1)(d-1)} + O(t^{dk-d-k}).$$

Isso conclui a prova. □

Seja $M(d,t)$ o conjunto dos polinômios inteiros, mônicos, redutíveis, de grau $d \geq 2$ e altura no máximo t. Dada a função zeta de Riemann ζ e usando o Lema 3.1.3, Chela provou em [1] que

$$|M(d,t)| \sim 2^d(\zeta(d-1) + 1/2 - 2V_{d-1})t^{d-1}, \tag{3.20}$$

para cada $d \geq 3$ e $t \to \infty$, (já que a constante k_d definida em [1] é igual à $2^{d-1}(1-2V_{d-1})$) e para $d = 2$ obteve

$$|M(2,t)| \sim 2t \log t. \tag{3.21}$$

Lema 3.2.3. *Com as notações dos lemas anteriores, temos*

$$0 \leq \mathcal{N}_2(f,k,t) - \mathcal{N}_1(f,k,t) \ll \begin{cases} t^{dk-d-k} \ \textit{para} \ d \geq 4, \\ t^{2k-3}\log t \ \textit{para} \ d = 3, \\ t^{k-3/2} \ \textit{para} \ d = 2, \end{cases}$$

onde as constante em $\ll$ dependem apenas de d e k.

Demonstração. Estimaremos o número de representações $f = f_1 + \ldots + f_k$ tais que $\partial f_1 = d$ e $\partial f_i = d-1$, $\forall\, i \in \{2,\ldots,k\}$, de forma que pelo menos um destes polinômios seja redutível e todos tenham altura no máximo t.

Fixamos $i \in \{1,\ldots,k\}$. Para cada $i \geq 2$, temos $\partial f_i = d-1$, e então o número de possibilidades do f_i ser redutível e de altura no máximo t é $\ll t^{d-2}$ para $d \geq 4$, por (3.20), e $\ll t\log t$ para $d = 3$, por (3.21). (Para $d = 2$, f_i é sempre irredutível.) Agora, para $i = 1$ temos que $\partial f_1 = d$ e que o coeficiente em f_1 de x^{d-1} é um inteiro fixo. Então, pelo Lema 3.1.4, o número de possibilidades para f_1 é $\ll t^{d-2}$ para $d \geq 4$, $\ll t\log t$ para $d = 3$ e $\ll \sqrt{t}$ para $d = 2$. Resumindo, podemos afirmar que, para cada $i \in \{1,\ldots,k\}$, existem $\ll t^{d-2}$ escolhas para polinômios f_i, redutíveis e de altura no máximo t, quando $d \geq 4$, $\ll t\log t$ escolhas quando $d = 3$ e $\ll \sqrt{t}$ quando $d = 2$.

Por outro lado, por (3.2) e por (3.17), o número de representações de $f - f_i$ como soma de $k-1$ polinômios inteiros mônicos $f_1,\ldots,f_{i-1},f_{i+1},\ldots,f_k$, cujas alturas são no máximo t, não excede $(2t+1)^{(d-1)(k-2)}$. Então, segue para $d \geq 4$ que

$$\mathcal{N}_2(f,k,t) - \mathcal{N}_1(f,k,t) \ll (2t+1)^{(k-2)(d-1)}t^{d-2}$$

$$\ll t^{(d-1)(k-2)+d-2} = t^{dk-d-k}.$$

Similarmente, para $d = 3$ temos

$$\mathcal{N}_2(f,k,t) - \mathcal{N}_1(f,k,t) \ll (2t+1)^{2(k-2)}t\log t \ll t^{2k-3}\log t$$

e, para $d = 2$,

$$\mathcal{N}_2(f,k,t) - \mathcal{N}_1(f,k,t) \ll (2t+1)^{(k-2)}\sqrt{t} \ll t^{k-3/2}.$$

□

Apresentamos, a seguir, o principal resultado deste capítulo, que estabelece uma fórmula assintótica para $\mathcal{N}(f,k,t)$, com $k \geq 2$.

Teorema 3.2.4. *Sejam $f(x) \in \mathbb{Z}[x]$, um polinômio mônico de grau $d \geq 2$, e $k \geq 2$, um inteiro. Então, para $t \to \infty$,*

$$\mathcal{N}(f,k,t) = \frac{(2^{k-1}(1-2V_{k-1}))^{d-1}}{(k-1)!}t^{(k-1)(d-1)} + O(t^{dk-d-k})$$

para $d \geq 4$,

$$\mathcal{N}(f,k,t) = \frac{(2^{k-1}(1-2V_{k-1}))^2}{(k-1)!}t^{2(k-1)} + O(t^{2k-3}\log t)$$

para $d = 3$,

$$\mathcal{N}(f,k,t) = \frac{(2^{k-1}(1-2V_{k-1}))}{(k-1)!}t^{k-1} + O(t^{k-3/2})$$

para $d = 2$.

Demonstração. Utilizando os Lemas 3.2.1 e 3.2.3, temos

$$|\mathcal{N}_2(f,k,t) - \mathcal{N}(f,k,t)| \ \leq \ |\mathcal{N}_2(f,k,t) - \mathcal{N}_1(f,k,t)| \ + \ |\mathcal{N}(f,k,t) - \mathcal{N}_1(f,k,t)|$$

$$\ll \begin{cases} t^{dk-d-k} + t^{dk-d-k} \ll t^{dk-d-k} \ \text{ para } \ d \geq 4, \\ t^{3k-3-k} + t^{2k-3}\log t \ \ll \ t^{2k-3}\log t \ \text{ para } \ d = 3, \\ t^{2k-2-k} + t^{k-3/2} \ \ll \ t^{k-3/2} \ \text{ para } \ d = 2. \end{cases} \tag{3.22}$$

Definimos $P_d(t) := \dfrac{(2^{k-1}(1-2V_{k-1}))^{d-1}}{(k-1)!}t^{(k-1)(d-1)}$, para cada $d \geq 2$.

Então, pelo Lema 3.2.2 e por (1.4), existem constantes C_d's tais que

$$|\mathcal{N}_2(f,k,t) - P_d(t)| \ \leq \ C_d t^{dk-d-k}. \tag{3.23}$$

Portanto, por (3.23) e (3.22), obtemos

$$\mathcal{N}(f,k,t) \ = \ \begin{cases} P_d(t) \ + \ O(t^{dk-d-k}) \ \text{ para } \ d \geq 4, \\ P_3(t) \ + \ O(t^{2k-3}\log t) \ \text{ para } \ d = 3, \\ P_2(t) \ + \ O(t^{k-3/2}) \ \text{ para } \ d = 2. \end{cases}$$

□

Teorema 3.2.5. *Seja* $f(x) \in \mathbb{Z}[x]$ *um polinômio mônico de grau* $d \geq 2$. *Então, para* $t \to \infty$,

$$\mathcal{N}(f,2,t) = (2t)^{d-1} + O(t^{d-2}) \tag{3.24}$$

para $d \geq 4$,

$$t\log t \ll (2t^2) - \mathcal{N}(f,2,t) \ll t\log t \tag{3.25}$$

para $d = 3$,

$$\sqrt{t} \ll 2t - \mathcal{N}(f,2,t) \ll \sqrt{t} \tag{3.26}$$

para $d = 2$.

Além disso, o termo de erro para $d \geq 4$ *é o melhor possível.*

Demonstração. Para provarmos (3.26), começamos tomando $f(x) = x^2 + bx + c \in \mathbb{Z}[x]$ e

supondo, sem perda de generalidade,

$$t \geq (|b|+1)+(|c|+1) = |b|+|c|+2 \geq 2.$$

Para que o polinômio f seja soma de dois polinômios mônicos f_1 e f_2, devemos ter os graus dos somandos iguais à 2 e 0 ou iguais à 2 e 1. No primeiro caso, temos $f_1(x) = x^2+bx+(c-1)$ e $f_2(x) = 1$, com $H(f_1), H(f_2) \leq t$, pois $|c-1| \leq |c|+1 \leq t$. Daí, esta representação será contada se, e só se, f_1 for irredutível. Definimos $\delta := 1$ se f_1 é irredutível e $\delta := 0$ para o caso contrário.

No segundo caso, temos $f_1(x) = x^2+(b-1)x+c_1$ e $f_2(x) = x+c_2$, com $c = c_1+c_2$ e f_2 irredutível para qualquer $c_2 \in \mathbb{Z}$. Supondo $|c_1|, |c_2| \leq t$, então $H(f_1), H(f_2) \leq t$ pois $|b-1| \leq t$. Como $c_2 = c-c_1$, temos

$$-t \leq c-c_1 \leq t \Rightarrow c-t \leq c_1 \leq c+t$$

e, portanto,

$$\max\{-t, c-t\} \leq c_1 \leq \min\{t, c+t\}. \tag{3.27}$$

Se $c < 0$, então (3.27) nos dá $-t \leq c_1 \leq c+t$ e nesse intervalo há $2t+1+c$ possíveis valores inteiros para c_1. Se $c \geq 0$, então (3.27) nos dá $c-t \leq c_1 \leq t$ e nesse intervalo há $2t+1-c$ possíveis valores inteiros para c_1. Então o intervalo (3.27) contém exatamente $2t+1-|c|$ inteiros distintos c_1 e, daí, o número de representações inteiras $f = f_1+f_2$ tais que f_1, f_2 são mônicos de altura no máximo t, com $\partial f_1 = 2, \partial f_2 \leq 1$ e $f_1 = x^2+(b-1)x+c_1$ redutível, é exatamente

$$\delta + (2t+1-|c|) - \mathcal{N}(f,2,t).$$

Note que o intervalo (3.27) está contido em $[-(|c|+t), |c|+t]$ e contém $[-(t-|c|), t-|c|]$. De fato, dado $c_1 \in [\max\{-t, c-t\}, \min\{t, c+t\}]$, temos

$$c < 0 \Rightarrow -(-c+t) \leq -t \leq c_1 \leq c+t \leq -c+t,$$

$$c \geq 0 \Rightarrow -(c+t) \leq c-t \leq c_1 \leq t \leq c+t,$$

e dado $c_1 \in [-(t-|c|), t-|c|]$, temos

$$c < 0 \Rightarrow \max\{-t, c-t\} \leq -(t+c) \leq c_1 \leq t+c = \min\{t, c+t\},$$

$$c \geq 0 \Rightarrow \max\{-t, c-t\} = -(t-c) \leq c_1 \leq t-c \leq \min\{t, t+c\}.$$

Então, utilizando a notação do Lema 3.1.4, obtemos

$$|M(b-1,2,t-|c|)| \leq \delta + 2t+1-|c| - \mathcal{N}(f,2,t) \leq |M(b-1,2,t+|c|)| \Rightarrow$$

$$|M(b-1,2,t-|c|)| + |c| - 1 - \delta \leq 2t - \mathcal{N}(f,2,t) \leq |M(b-1,2,t+|c|)| + |c| - 1 - \delta$$

e pelo item (iii) do Lema 3.1.4,

$$\sqrt{t-|c|}|+|c|-1-\delta \ll 2t-\mathcal{N}(f,2,t) \ll \sqrt{t+|c|}+|c|-1-\delta$$

$$\Rightarrow \sqrt{t} \ll 2t-\mathcal{N}(f,2,t) \ll \sqrt{t}.$$

Para provarmos (3.24) e (3.25), assumimos que $f(x) \in \mathbb{Z}[x]$ é um polinômio mônico de grau $d \geq 3$. Se f é soma de dois polinômios mônicos irredutíveis f_1 e f_2, supondo $\partial f_1 = d$, então $\partial f_2 = \ell$, com $\ell \in \{0, 1, \cdots, d-1\}$. Seja $T(f,\ell,t)$ o número de representações de f como soma $f = f_1 + f_2$, para polinômios inteiros mônicos f_1, f_2 com graus d e ℓ, respectivamente, e alturas no máximo t e seja também $T^*(f,\ell,t)$ o número de tais representações em que f_1, f_2 são ambos irredutíveis. Escrevendo

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_{\ell+1}x^{\ell+1} + a_\ell x^\ell + a_{\ell-1}x^{\ell-1} + \cdots + a_1 x + a_0,$$

temos

$$f_1(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_{\ell+1}x^{\ell+1} + (a_\ell - 1)x^\ell + g_1(x), \;\; f_2(x) = x^\ell + g_2(x),$$

para $g_1, g_2 \in \mathbb{Z}[x]$ tal que $\partial g_1, \partial g_2 \leq \ell - 1$. Desde que $H(g_1) \leq t$, existem exatamente $(2t+1)^\ell$ escolhas distintas para g_1 e, para cada escolha de g_1, uma única escolha para g_2, já que

$$g_1(x) + g_2(x) = a_{\ell-1}x^{\ell-1} + \cdots + a_1 x + a_0$$

se $\ell \geq 1$ e $g_2(x) = 0 = g_1(x)$ se $\ell = 0$. Então segue que

$$T(f,\ell,t) \leq (2t+1)^\ell \tag{3.28}$$

para $0 \leq \ell \leq d-1$ e t suficientemente grande.

Agora estimaremos tais representações para $\ell = d-1$ (as quais não levam em conta a redutibilidade). Como $\partial f_1 = d, \partial f_2 = d-1$, temos

$$f_1(x) = x^d + a_{d-1}x^{d-1} + g_1(x), \;\; f_2(x) = x^{d-1} + g_2(x),$$

para $g_1, g_2 \in \mathbb{Z}[x]$ tal que $\partial g_1, \partial g_2 \leq d-2$. Supondo $H(f) = h$, temos que $T(f, d-1, t)$ é pelo menos $(2t-2h+1)^{d-1}$ (pois cada coeficiente de g_1 pode ser escolhido no intervalo $[-t+h, t-h]$). Então, por (3.28), temos

$$(2t-2h+1)^{d-1} \leq T(f,d-1,t) \leq (2t+1)^{d-1}. \tag{3.29}$$

Para um polinômio especial

$$f_h(x) =: x^d + x^{d-1} + h(x^{d-2} + \cdots + x + 1), \tag{3.30}$$

cada coeficiente de $g_1(x)$ pode estar no intervalo $[-t+h, t]$. De fato, se c_1 e c_2 são coeficientes de um mesmo grau arbitrário dos polinômios g_1 e g_2, respectivamente, então $c_1 + c_2 = h$ e

$$c_2 \leq t \Rightarrow c_1 \geq -t + h,$$
$$c_2 \geq -t \Rightarrow c_1 \leq t + h.$$

mas $c_1 \leq t \leq t + h$. Daí, temos

$$T(f_h, d-1, t) = (2t - h + 1)^{d-1}. \tag{3.31}$$

Note que $\mathcal{N}(f, 2, t) = \sum_{\ell=0}^{d-1} T^*(f, \ell, t)$ é o número de representações $f_1 + f_2$, com $\partial f_1 = d, \partial f_2 \leq d-1$ e ambos irredutíveis. Daí,

$$\sum_{\ell=0}^{d-1} T(f, \ell, t) - \mathcal{N}(f, 2, t) = \sum_{\ell=0}^{d-1} T(f, \ell, t) - \sum_{\ell=0}^{d-1} T^*(f, \ell, t) \tag{3.32}$$

é o número dessas representações em que pelo menos um dos polinômios é redutível. Como $|M(a_{d-1} - 1, d, t)|$ é o número de polinômios mônicos, redutíveis, com coeficiente de x^{d-1} igual à $a_{d-1} - 1$, grau d e altura no máximo t, obtemos

$$|M(a_{d-1} - 1, d, t)| \leq \sum_{\ell=0}^{d-1} T(f, \ell, t) - \mathcal{N}(f, 2, t). \tag{3.33}$$

Por outro lado,

$$T(f, \ell, t) - T^*(f, \ell, t) \leq |M(a_{d-1} - 1, d, t)| \cdot 1 + |M(d-1, t)| \cdot 1$$

pois cada $f_1 \in M(a_{d-1}, d, t)$ determina no máximo um $f_2 = f - f_1$ mônico com grau $d-1$, altura t, redutível ou não e, da mesma forma, cada $f_2 \in |M(d-1, t)|$ determina no máximo um $f_1 = f - f_2$ mônico com grau d, altura t, redutível ou não. Então, por (3.32),

$$\sum_{\ell=0}^{d-1} T(f, \ell, t) - \mathcal{N}(f, 2, t) = \sum_{\ell=0}^{d-1} T(f, \ell, t) - \sum_{\ell=0}^{d-1} T^*(f, \ell, t) \leq$$
$$\sum_{\ell=0}^{d-2} T(f, \ell, t) + T(f, d-1, t) - T^*(f, d-1, t) \leq$$
$$\sum_{\ell=0}^{d-2} T(f, \ell, t) + |M(a_{d-1}, d, t)| + |M(d-1, t)| \Rightarrow$$

$$-\mathcal{N}(f, 2, t) \leq |M(a_{d-1}, d, t)| + |M(d-1, t)| - T(f, d-1, t)$$

No caso $d = 3$, por (3.21) temos $\alpha := |M(3-1,t)| = |M(2,t)| \sim 2t\log t$ e se $\beta := |M(a_2 - 1, 3, t)|$, pelo item (ii) do Lema 3.1.4, temos $t\log t \ll \beta \ll t\log t$. Daí, por (3.29),

$$(2t)^2 - \mathcal{N}(f,2,t) \leq (2t)^2 - (2t-2h+1)^2 + \alpha + \beta$$

$$\leq 4(2h-1)t - (2h-1)^2 + \alpha + \beta \leq 4(2h-1)t + \alpha + \beta \ll t\log t.$$

Como $t\log t \ll \beta$, por (3.33) temos $t\log t \ll \beta \leq T(f,0,t) + T(f,1,t) + T(f,2,t) - \mathcal{N}(f,2,t)$ e por (3.29), obtemos

$$t\log t \ll 1 + (2t+1) + (2t+1)^2 - \mathcal{N}(f,2,t) \Rightarrow$$

$$t\log t \ll (2t)^2 + 6t + 3 - \mathcal{N}(f,2,t) \Rightarrow$$

$$(2t)^2 - \mathcal{N}(f,2,t) \gg t\log t.$$

No caso $d \geq 4$, já que $V_1 := vol\,(\Lambda(1,1,0)) = 0$, o Teorema 3.2.4 fornece

$$\mathcal{N}(f,2,t) = (2t)^{d-1} + O(t^{d-2}).$$

Para finalizar a prova do teorema, devemos mostrar que o termo $O(t^{d-2})$ acima é o melhor possível. Consideramos o polinômio f_h definido em (3.30). Por (3.33), temos $\sum_{\ell=0}^{d-1} T(f,\ell,t) - \mathcal{N}(f_h,2,t) \geq 0$. Daí, usando (3.28) e (3.31), obtemos

$$\mathcal{N}(f_h,2,t) \leq \sum_{j=0}^{d-2}(2t+1)^j + (2t+1-h)^{d-1} = \frac{(2t+1)^{d-1}-1}{(2t+1)-1} + (2t+1-h)^{d-1}. \quad (3.34)$$

Fixamos quaisquer $h \geq 2$ e $d \geq 4$. Então, para t suficientemente grande,

$$\left(1+\frac{1}{2t}\right)^{d-1} \leq \frac{3}{2} \Rightarrow (2t+1)^{d-1} \leq \frac{3}{2}(2t)^{d-1} \Rightarrow$$
$$(2t+1)^{d-1} \leq 3\cdot 2^{d-2}t^{d-1} \Rightarrow \frac{(2t+1)^{d-1}}{2t} \leq 3\cdot 2^{d-3}t^{d-2} \Rightarrow$$
$$\frac{(2t+1)^{d-1}-1}{(2t+1)-1} \leq 3\cdot 2^{d-3}t^{d-2}.$$

Então, como $1-h \leq -1$, por (3.34) temos

$$\mathcal{N}(f_h,2,t) \leq 3\cdot 2^{d-3}t^{d-2} + (2t-1)^{d-1}. \quad (3.35)$$

Além disso,

$$(2t-1)^{d-1} < (2t)^{d-1} - (d-2)(2t)^{d-2}, \text{ quando } t \to \infty. \tag{3.36}$$

De fato, para t suficientemente grande, temos

$$\left(1-\frac{1}{2t}\right)^{d-1} + \frac{(d-2)}{2t} < 1 \Rightarrow \left(\frac{2t-1}{2t}\right)^{d-1} + \frac{(d-2)}{2t} < 1 \Rightarrow$$
$$(2t-1)^{d-1} + (d-2)(2t)^{d-2} < (2t)^{d-1}.$$

Então, por (3.35), temos

$$\begin{aligned}\mathcal{N}(f_h, 2, t) &\leq 3 \cdot 2^{d-3} t^{d-2} + (2t)^{d-1} - (d-2)(2t)^{d-2} \\ &= (2t)^{d-1} + (3 - 2(d-2))2^{d-3} t^{d-2} \\ &= (2t)^{d-1} - (2d-7)2^{d-3} t^{d-2} \\ &< (2t)^{d-1} - t^{d-2}.\end{aligned}$$

já que $-(2d-7)2^{d-3} \leq -2 < -1$. Daí, por (3.24), concluímos que $\mathcal{N}(f_h, 2, t) = (2t)^{d-1} + O(t^{d-2})$ e, então, que o termo $O(t^{d-2}) < -t^{d-2}$ não pode ser aumentado.

□

Considerações Finais

Neste trabalho, seguimos uma direção algébrica e uma analítica para abordar um análogo à Conjectura de Goldbach, o qual denominamos por Propriedade de Goldbach e determina que cada elemento de um anel de polinômios $R[x]$ com grau $n \geq 1$ é escrito como soma de dois polinômios de $R[x]$, irredutíveis e de grau n. No Capítulo 1, apresentamos uma série de definições, exemplos e resultados da Teoria de Anéis, da Geometria Euclidiana n-dimensional, assim como notações da Teoria Analítica dos Números, que foram necessárias ao longo da pesquisa.

No Capítulo 2, apresentamos resultados que estabelecem casos gerais de domínios de integridade com tal propriedade. Ao provarmos que um domínio Noetheriano R contendo uma infinidade de ideais maximais satisfaz a Propriedade de Goldbach, observamos que não há como concluir o mesmo para um domínio local, isto é, um domínio que possui um único ideal maximal. Isso ocorre porque o método utilizado pede que R possua pelo menos dois ideais maximais cumprindo algumas hipóteses. Entretanto, estudos mais profundos sobre o Critério de Irredutibilidade de Hilbert [17] mostram que um corpo finitamente gerado satisfaz a Propriedade de Goldbach.

No Capítulo 3, apresentamos uma análise assintótica de $\mathcal{N}(f, k, t)$ por meio de uma técnica que envolve volumes de politopos n-dimensionais. $\mathcal{N}(f, k, t)$ é definido como o número de representações de um polinômio $f(x) \in \mathbb{Z}[x]$ mônico como soma de $k \geq 2$ polinômios inteiros, mônicos, irredutíveis e de alturas no máximo t, para t suficientemente grande. Nada se sabe ainda sobre a possibilidade de utilizar esse método para estudar o comportamento assintótico de $\mathcal{N}(f, 2, t)$ para polinômios $f(x) \in R[x] \neq \mathbb{Z}[x]$, assim como para generalizar os resultados obtidos no artigo [11] sobre o anel $\mathbb{Z}[\theta][x]$, considerando $k \geq 2$.

Referências Bibliográficas

[1] Chela, R., *Reducible polynomials.* Jornal London Mathematic Society, **38** (1963) 183–188.

[2] Dubickas, A., *Polynomials expressible by sums of monic integer irreducible polynomials.* Bull. Math. Soc. Sci. Math. Roumanie, Tome **54** (102) (2011) 65–81.

[3] Dummit, D. S., Foote, R. M., *Abstract algebra.* Third ed., John Wiley & Sons, Hoboken, NJ, 2004.

[4] Effinger, G., Hayes, D. R., *A complete solution to the polynomial 3-primes problem.* Bull. Amer. Math. Soc. (N.S.), **24** (1991) 363–369.

[5] Goodman, J. E., Rourke, J. O., *Handbook of discrete and computational geometry.* Second ed., Chapman & Hall/CRC, 2004.

[6] Hayes, D. R., *A Goldbach theorem for polynomials with integral coeficients.* Amer. Math. Monthly, **72** (1965) 45–46.

[7] Hayes, D. R., *The expression of a polynomial as a sum of three irreducibles.* Acta. Arith., **11** (1966) 461–488.

[8] Keng, H. L., *Introduction to Number Theory.* Springer-Verlag, Berlin Heidelberg New York, 1982.

[9] Kerber, M., Tichy, R., Weitzer, M., *Constrained Triangulations, Volumes of Polytopes, and Unit Equations.* 33rd International Symposium on Computational Geometry (SoCG 2017), **46** (2017) 1–15.

[10] Kozek, M., *An asymptotic formula for Goldbach's conjecture with monic polynomials in* $\mathbb{Z}[x]$. Amer. Math. Monthly, **117** (2010) 365–369.

[11] Lemos, A., De Araújo, A. L. A., *An asymptotic formula for Goldbach's conjecture with monic polynomials in* $\mathbb{Z}[\theta][x]$. Colloquium Mathematicum, **148** (2017) 215–223.

[12] Paran, E., *Twin-prime and Goldbach theorems for* $\mathbb{Z}[[x]]$. Journal Number Theory, (2020) **213** (2020) 453–461.

[13] Polcino, C., *Anéis e Módulos.* Publicações do Instituto de Matemática e Estatística da Universidade de São Paulo, São Paulo, 1972.

[14] Pollack, P., *On Polynomial rings with a Goldbach property.* Amer. Math. Monthly, **118** (2011) 71–77.

[15] Rattan, A., Stewart, C., *Goldbach's conjecture for* $\mathbb{Z}[x]$. C. R. Math. Acad. Sci. Soc. R. Can., **20** (1998) 83–85.

[16] Saidak, F., *On Goldbach's Conjecture for integer polynomials.* Amer. Math. Monthly, **113** (2006) 541–545.

[17] Schinzel, A., Polynomials with special regard to reducibility, Encyclopedia of Mathematics and its Applications, vol. 77, Cambridge University Press, Cambridge, 2000.

[18] Van Der Waerden, B. L., *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt.* Monatsheft fur Matematik und Physik, **43** (1936) 133–147.