Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

A Equação de Ramanujan-Nagell e Algumas de suas Generalizações

por

Matheus Bernardini de Souza

Orientador: Diego Marques Ferreira

Brasília
2013

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

A Equação de Ramanujan-Nagell e Algumas de suas Generalizações

por

Matheus Bernardini de Souza*

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de

MESTRE EM MATEMÁTICA

Brasília, 2013.

Comissão Examinadora:

Prof. Dr. Diego Marques Ferreira - MAT/UnB (Orientador)

Prof. Dr. Hemar Teixeira Godinho - MAT/UnB - Membro

Prof. Dr. José Plinio de Oliveira Santos - MAT/Unicamp - Membro

*O autor foi bolsista da CNPq durante a elaboração deste trabalho.

Aos meus pais e à Rafaela

Agradecimentos

Primeiramente, agradeço a Deus por essa oportunidade.

A minha família, em particular aos meus pais Romulo e Yolanda, por terem me apoiado em todos os momentos, desde que eu escolhi o curso de Matemática. O apoio de vocês sempre será a maior motivação que terei na minha vida. Vocês são meus exemplos e minhas inspirações.

À Rafaela, pelo exemplo de pessoa e de matemática que é para mim. Agradeço pela ajuda nas disciplinas, cobranças e, principalmente, pela paciência que teve nesse período. A força que me deu durante a graduação e o mestrado foi fundamental para que eu conseguisse chegar até aqui.

Ao professor Diego Marques por ter me aceitado como primeiro orientando de mestrado, acreditando em mim nesse desafio. Agradeço por tanto conhecimento compartilhado, pela paciência, pelas sugestões e pelos problemas propostos e resolvidos, inclusive os que são extras a esse trabalho. Sei que formei um amigo nesse período.

Aos demais membros banca examinadora, formada pelos professores Hemar Teixeira Godinho, José Plínio de Oliveira Santos e Leandro Martins Cioletti, por terem aceitado avaliar o meu trabalho.

A todos os professores e funcionários do Departamento de Matemática da UnB. Em particular, gostaria de agradecer ao professor Lineu da Costa Araújo Neto, por ter lecionado o curso de Teoria dos Números no 2/2009, o qual foi espetacular. Esse curso foi de grande influência para a minha escolha no mestrado. Agradeço à professora Cátia Regina Gonçalves, por ter lecionado um dos melhores cursos que assisti na UnB (Introdução a Probabilidade e Aplicações no 2/2011), o qual ocorreu no momento em que mais precisei de algo motivador. Também, agradeço ao professor Mauro Luiz Rabelo, pelo valioso período em que estive no PETMAT.

Aos meus amigos, por me proporcionarem momentos maravilhosos na vida fora da UnB e por acreditarem em mim. Aos novos amigos que fiz na graduação e no mestrado, por todo apoio durante as provas, seminários, apresentações, congressos e exames de qualificação.

Ao CNPq/CAPES pelo apoio financeiro concedido durante a elaboração deste trabalho.

Resumo

O objetivo deste trabalho é mostrar algumas técnicas para resolução de equações diofantinas. Métodos algébricos são ferramentas de grande utilidade para a resolução da equação $x^2 + 7 = y^n$, em que $y = 2$ ou y é ímpar. O uso do método hipergeométrico traz um resultado recente (de 2008) no estudo da equação $x^2 + 7 = 2^n \cdot m$ e técnicas algébricas garantem uma condição necessária para que essa última equação tenha solução.

Palavras-chave: Equação de Ramanujan-Nagell, Método hipergeométrico, Teoria dos números algébricos

Abstract

The objective of this work is to show some techniques for solving Diophantine equations. Algebraic methods are useful tools for solving the equation $x^2 + 7 = y^n$, where $y = 2$ or y is odd. The use of the hypergeometric method brings a recent result (from 2008) in the study of the equation $x^2 + 7 = 2^n \cdot m$ and algebraic techniques ensure a necessary condition for the last equation to have a solution.

Keywords: Ramanujan-Nagell equation, Hypergeometric method, Algebraic number theory

Sumário

Introdução

Neste trabalho, estudaremos a equação diofantina

$$x^2 + c = y^n, \tag{1}$$

em que x, y e n são inteiros positivos e c é uma constante pré-fixada.

Para o caso $n = 1$, temos uma infinidade de soluções da forma $(x, c, x^2 + c)$. Para o caso $n = 2$, conseguimos reescrever a equação como $(y - x)(y + x) = c$ e usando o Teorema Fundamental da Aritmética, temos que $y - x$ e $y + x$ são divisores de c. Logo, há uma quantidade finita de soluções para a equação. Portanto, os casos não triviais ocorrem quando $n \geq 3$.

A primeira referência sobre o estudo dessa equação foi no século XVII, quando P. Fermat mostrou que se $c = 2$ e $n = 3$, então a única solução é $5^2 + 2 = 3^3$. Esse resultado foi publicado por L. Euler [9].

Para $y = 2$ e $c = 7$, S. Ramanujan [18], em 1913, conjecturou que a equação $x^2 + 7 = 2^n$ tem exatamente 5 soluções em inteiros positivos x e n. Em 1960, T. Nagell [17] provou essa afirmação.

O primeiro avanço quando y não está fixado foi dado em 1850 por V. A. Lebesgue* [12]. Ele mostrou que a equação $x^2 + 1 = y^n$ não tem solução. Em 1923, Nagell provou que a equação não tem solução nos casos $c = 3$ e $c = 5$ e tem duas soluções se $c = 4$, dadas por $2^2 + 4 = 2^3$ e $11^2 + 4 = 5^3$. Ele ainda estudou o caso $c = 2$, mas, em 1943, quem conseguiu resolver completamente esse problema foi W. Ljunggren o qual mostrou que essa equação tem apenas a solução $5^2 + 2 = 3^3$ encontrada por Fermat.

Para $c = -1$, temos uma situação interessante, pois é um caso particular da Conjectura de Catalan†. Em 1964, C. Ko [10] mostrou que a única solução é $3^2 - 1 = 2^3$.

Em 1993, J. Cohn [8] resolveu (1) para 77 valores de c entre 1 e 100. Em 1996, M. Mignotte e B. de Weger [15] resolveram (1) para $c = 74$ e $c = 86$ e em 2004, M. Bennett e C. Skinner [6] resolveram (1) para $c = 55$ e $c = 95$.

Faltavam apenas 19 casos para completar as cem primeiras possibilidades para c inteiro positivo e cada caso tinha uma dificuldade particular. A lista completa que

*Não confundir com H. Lebesgue, da integral de Lebesgue.

†Conjectura de Catalan: A única solução da equação $x^m - y^n = 1$ é $3^2 - 2^3 = 1$. A conjectura foi demonstrada em 2002 por Preda Mihailescu.

faltava era

$$c \in \{7, 15, 18, 23, 25, 28, 31, 39, 45, 47, 60, 63, 71, 72, 79, 87, 92, 99, 100\}.$$

Em 2006, Y. Bugeaud, Mignotte e S. Siksek [7] aprimoraram as ideias de Bennett e Skinner e resolveram (1) para os valores de c na lista acima.

Em 2008, Bennett, M. Filaseta e O. Trifonov [5] estudaram uma generalização para (1): a equação $x^2 + 7 = 2^n \cdot m$, em que x, m e n são inteiros positivos. Usando o método hipergeométrico, eles encontraram uma relação entre os números x e m que traz algumas consequências e soluções para essa última equação.

Dividimos o nosso trabalho em 3 capítulos, a saber:

- **Capítulo 1: Preliminares**. Nesse capítulo, enunciaremos resultados de Teoria dos Números e de Álgebra que serão usados no decorrer dos outros capítulos.

- **Capítulo 2: A equação** $x^2 + 7 = y^n$. Um objetivo é entender as técnicas algébricas usadas por Nagell para a resolução da equação, quando $y = 2$. O outro objetivo é entender o métodos usados por Le, quando y um número ímpar. Algo interessante a se observar é que apesar de as duas equações (o caso $y = 2$ e o caso y ímpar) serem relativamente similares, os métodos tem alguma interseção, mas as ideias principais são diferentes.

- **Capítulo 3: A equação** $x^2+7 = 2^n \cdot m$. Algumas ideias encontradas no capítulo 2 reaparecem nesse capítulo e ferramentas novas (os aproximantes de funções analíticas por funções racionais e o método hipergeométrico) são introduzidas para que o resultado de Bennett, Filaseta e Trifonov seja bem compreendido. Eles encontraram uma relação interessante entre as variáveis x, m e n e, com essa relação, resolveremos completamente a equação para m fixado. Conseguimos também uma condição necessária para que a equação tenha solução usando ferramentas de Teoria Elementar dos Números.

Capítulo 1

Preliminares

O objetivo deste capítulo é lembrar de algumas propriedades que servirão de base para o trabalho. Enunciaremos resultados de Teoria dos Números e de Álgebra que serão importantes no decorrer do trabalho.

1.1 Algumas propriedades numéricas

Seja ϕ a função de Euler definida por

$$\phi(n) = \#\{k \in \mathbb{N} : \text{mdc}(n,k) = 1 \text{ e } k \leq n\},$$

em que $n \in \mathbb{N}$. Essa função é multiplicativa, isto é, dados a e b primos entre si, temos que $\phi(ab) = \phi(a)\phi(b)$ e se p é um primo, então $\phi(p^k) = p^k - p^{k-1}$. Com essas duas propriedades e usando o Teorema Fundamental da Aritmética, conseguimos calcular ϕ em todos os números naturais. Um resultado importante é

Teorema 1.1 *(Teorema de Euler) Sejam a e n inteiros positivos. Se* $\text{mdc}(a,n) = 1$*, então* $a^{\phi(n)} \equiv 1 \pmod{n}$.

Demonstração: Consultar [20] nas páginas 43 - 44.

Considere a congruência $x^2 \equiv a \pmod{p}$, em que x e a são inteiros e p é um primo ímpar. Uma pergunta natural é: qual é uma condição para que essa congruência tenha solução? Se a é múltiplo de p, então $x \equiv 0 \pmod{p}$ é solução. Logo podemos restringir o estudo aos casos em que $p \nmid a$. Introduziremos o símbolo de Legendre e enunciaremos alguns resultados importantes a seguir.

Definição 1.1 *Seja p um primo ímpar e a um inteiro com $p \nmid a$. Definimos o símbolo de Legendre* $\left(\frac{a}{p}\right)$ *por*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{ se } x^2 \equiv a \pmod{p} \text{ tem solução} \\ -1, \text{ se } x^2 \equiv a \pmod{p} \text{ não tem solução.} \end{cases}$$

Proposição 1.1 *Sejam a e b inteiros e p um primo ímpar. O símbolo de Legendre tem as seguintes propriedades:*

(i) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

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

Demonstração: Consultar [20] nas páginas 97 - 102.

Teorema 1.2 *(Lei da Reciprocidade Quadrática) Se p e q são primos ímpares distintos, então*

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

Demonstração: Consultar [20] nas páginas 107 - 108.

Um conceito importante na Teoria dos Números é o de valorização p-ádica de um racional não nulo $\frac{a}{b}$. Dado p um primo, definimos $\nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b)$, em que $\nu_p(n) = \max\{k \in \mathbb{N} \cup \{0\} : p^k \mid n\}$ para n inteiro. Para este trabalho, usaremos esse conceito no conjunto $\mathbb{Z}^*$.

Proposição 1.2 *Sejam a e $b \in \mathbb{Z}$ e p um primo. Então*

(i) $\nu_p(ab) = \nu_p(a) + \nu_p(b)$;

(ii) $\nu_p(a \pm b) \geq \min\{\nu_p(a), \nu_p(b)\}$.

Demonstração: Sejam $a = p^\alpha m$ e $b = p^\beta n$, em que $\nu(a) = \alpha$ e $\nu(b) = \beta$.
(i) Note que $ab = p^{\alpha+\beta}mn$ e isso nos mostra que $\nu(ab) = \alpha + \beta = \nu(a) + \nu(b)$.
(ii) Suponha que $\alpha \geq \beta$. Note que $a \pm b = p^\beta(p^{\alpha-\beta}m \pm n)$. Usando **(i)**, obtemos $\nu_p(a+b) = \nu_p(p^\beta) + \nu_p(p^{\alpha-\beta}m \pm n) \geq \nu_p(p^\beta) = \beta$ e $\beta = \min\{\nu_p(a), \nu_p(b)\}$, por hipótese. O caso $\alpha < \beta$ é análogo.

■

Proposição 1.3 *Sejam a e b inteiros não nulos. $a \mid b$ se, e somente se, $\nu_p(a) \leq \nu_p(b)$, para todo primo p.*

Demonstração: Sem perda de generalidade, suponha que a e b são positivos. Pelo Teorema Fundamental da Aritmética, podemos escrever $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ e $b = p_1^{\beta_1} \cdots p_n^{\beta_n}$, em que os p_i's são primos distintos para $i \in \{1, \ldots, n\}$ e α_i e β_i são inteiros não negativos, tais que $\alpha_i + \beta_i \neq 0$. Note que essa escrita implica que $\nu_{p_i}(a) = \alpha_i$ e $\nu_{p_i}(b) = \beta_i$. Observe que $a \mid b \Leftrightarrow \frac{b}{a} = p_1^{\beta_1-\alpha_1} \cdots p_n^{\beta_n-\alpha_n}$ é um inteiro $\Leftrightarrow \beta_i - \alpha_i \geq 0$, para todo $i \in \{1, \ldots, n\} \Leftrightarrow \nu_{p_i}(b) \geq \nu_{p_i}(a)$, para todo p_i. Claramente, se q é um primo que não aparece nas fatorações de a e b, então $\nu_q(a) = \nu_q(b) = 0$.

■

Notação 1.1 *Em alguns casos, escreveremos $p^k \mid\mid a$ para denotar $\nu_p(a) = k$.*

Para finalizar essa seção, enunciaremos um resultado que estima o valor do fatorial de um inteiro positivo.

Teorema 1.3 *(Fórmula de Stirling) Seja n um inteiro positivo. Então*

$$\sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\frac{1}{12n+1}} \leq n! \leq \sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\frac{1}{12n}}.$$

Demonstração: Consultar [21].

1.2 Algumas propriedades algébricas

Considere o corpo $\mathbb{Q}(\sqrt{d}) = \{m + n\sqrt{d} : m, n \in \mathbb{Q}\}$, em que $d \neq 0$ é um número livre de quadrados. Dado $\mu = m + n\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, chamamos de conjugado de μ o número $\bar{\mu} = m - n\sqrt{d}$. Define-se a norma em $\mathbb{Q}(\sqrt{d})$ pela função $\mathcal{N} : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$, tal que $\mathcal{N}(\mu) = m^2 - dn^2 = \mu \cdot \bar{\mu}$.

Proposição 1.4 *A função norma $\mathcal{N}$ é multiplicativa, isto é, dados μ e $\rho \in \mathbb{Q}(\sqrt{d})$, temos que $\mathcal{N}(\mu\rho) = \mathcal{N}(\mu)\mathcal{N}(\rho)$.*

Demonstração: Considere $\mu = m + n\sqrt{d}$ e $\rho = r + s\sqrt{d}$. Então

$$\mu\rho = (m + n\sqrt{d})(r + s\sqrt{d}) = (mr + dns) + (ms + nr)\sqrt{d}$$

e

$$\begin{aligned}
\mathcal{N}(\mu\rho) &= (mr + dns)^2 - d(ms + nr)^2 \\
&= m^2r^2 + 2dmrns + d^2n^2s^2 - dm^2s^2 - 2dmsnr - dn^2r^2 \\
&= m^2(r^2 - ds^2) - dn^2(r^2 - ds^2) \\
&= (m^2 - dn^2)(r^2 - ds^2) = \mathcal{N}(\mu)\mathcal{N}(\rho).
\end{aligned}$$

■

Definição 1.2 *Dizemos que $\mu \in \mathbb{Q}(\sqrt{d})$ é um inteiro algébrico de $\mathbb{Q}(\sqrt{d})$ se é raiz de um polinômio mônico com coeficientes inteiros. Denotaremos o conjunto dos inteiros algébricos de $\mathbb{Q}(\sqrt{d})$ por Ω_d.*

Proposição 1.5 *Se μ é um inteiro algébrico de $\mathbb{Q}(\sqrt{d})$, então $\mathcal{N}(\mu) \in \mathbb{Z}$.*

Demonstração: Como μ é um inteiro algébrico, então existe um polinômio de coeficientes inteiros mônico tal que μ é raiz. Além disso, o polinômio minimal $p(x)$ é de grau 2, pois $\mathbb{Q}(\sqrt{d})$ é uma extensão de grau 2. Note que como μ é raiz de $p(x)$, então seu conjugado $\bar{\mu}$ também é raiz. Pelo Teorema Fundamental da Álgebra, essas são as únicas 2 raízes. Assim, podemos escrever

$$p(x) = (x-\mu)(x-\bar{\mu}) = x^2 - (\mu+\bar{\mu})x + \mu\bar{\mu} = x^2 - (\mu+\bar{\mu})x + \mathcal{N}(\mu).$$

Como os coeficientes de $p(x)$ são inteiros, então $\mathcal{N}(\mu) \in \mathbb{Z}$.

■

Observação 1.1 *A recíproca é falsa. Note que* $\mu = \frac{1+i\sqrt{8}}{3}$ *não é inteiro algébrico (o polinômio minimal de* μ *sobre* $\mathbb{Z}$ *é* $p(x) = 3x^2 - 2x + 3$*), porém* $\mathcal{N}(\mu) = \mu\bar{\mu} = 1$.

Exemplo 1.1 *O conjunto formado pelos inteiros algébricos de* $\mathbb{Q}$ *é exatamente* $\mathbb{Z}$.

Um fato importante é que o conjunto formado pelos inteiros algébricos é um anel. O próximo teorema explicita esse anel.

Teorema 1.4 *Seja* Ω_d *o anel de inteiros algébricos do corpo* $\mathbb{Q}(\sqrt{d})$*. Então*

$$\Omega_d = \begin{cases} \mathbb{Z}[\sqrt{d}], \text{ se } d \equiv 2 \text{ ou } 3 \pmod 4 \\ \mathbb{Z}[\frac{-1+\sqrt{d}}{2}], \text{ se } d \equiv 1 \pmod 4 \end{cases}$$

Demonstração: Consultar [19] nas páginas 97 e 98.

Exemplo 1.2 *Vamos mostrar que se* $d \equiv 1 \pmod 4$*, então o anel de inteiros algébricos é*

$$\Omega_d = \left\{ \frac{a+b\sqrt{d}}{2} \ : \ a, b \in \mathbb{Z}, a \equiv b \pmod 2 \right\}.$$

Pelo Teorema 1.4, temos que

$$\mathbb{Z}\left[\frac{-1+\sqrt{d}}{2}\right] = \left\{ a_0 + b_0\left(\frac{-1+\sqrt{d}}{2}\right) \ : \ a_0, b_0 \in \mathbb{Z} \right\}.$$

Note que

$$a_0 + b_0\left(\frac{-1+\sqrt{d}}{2}\right) = \frac{2a_0 - b_0}{2} + \frac{b_0\sqrt{d}}{2} = \frac{a+b\sqrt{d}}{2},$$

em que $a = 2a_0 - b_0$, $b = b_0$ e $a \equiv 2a_0 - b_0 \equiv b_0 \equiv b \pmod 2$.

Definição 1.3 *Sejam μ e $\rho \in \Omega_d$. Dizemos que μ divide ρ (e denotamos $\mu \mid \rho$) se existe $\theta \in \Omega_d$ tal que $\rho = \mu\theta$.*

Proposição 1.6 *Sejam μ e $\rho \in \Omega_d$. Se $\mu \mid \rho$, então $\mathcal{N}(\mu) \mid \mathcal{N}(\rho)$.*

Demonstração: Como $\mu \mid \rho$, então existe $\theta \in \Omega_d$ tal que $\rho = \mu\theta$. Logo, $\mathcal{N}(\rho) = \mathcal{N}(\mu\theta)$. Pela Proposição 1.4, temos que $\mathcal{N}(\rho) = \mathcal{N}(\mu)\mathcal{N}(\theta)$, o que prova que $\mathcal{N}(\mu) \mid \mathcal{N}(\rho)$.

■

Dizemos que μ é uma unidade em Ω_d se existe $\rho \in \Omega_d$ tal que $\mu\rho = 1$. Como consequência da proposição anterior, obtemos o seguinte.

Corolário 1.1 *Se μ é uma unidade de Ω_d, então $\mathcal{N}(\mu) = \pm 1$.*

Demonstração: Como μ é uma unidade de Ω_d, por definição, existe $\rho \in \Omega_d$ tal que $\mu\rho = 1$. Logo $\mathcal{N}(\mu\rho) = \mathcal{N}(\mu)\mathcal{N}(\rho) = 1$. Como a norma é um número inteiro, então $\mathcal{N}(\mu) \mid 1$, isto é, $\mathcal{N}(\mu) = \pm 1$.

■

Um problema útil na teoria de aneis é determinar as unidades (elementos que possuem inverso multiplicativo) do anel Ω_d.

Teorema 1.5 *Sejam $d < 0$ um inteiro livre de quadrados e $\mathcal{U}_d$ o conjuto formado pelas unidades de Ω_d. Então*

$$\mathcal{U}_d = \begin{cases} \{1, -1, i, -i\}, \text{ se } d = -1 \\ \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}, \text{ se } d = -3 \\ \{1, -1\}, \text{ se } d = -2 \text{ ou } d < -3, \end{cases}$$

em que $i^2 = -1$ e ω é uma raiz cúbica não real da unidade.

Demonstração: Consultar [2] nas páginas 90 -91.

Exemplo 1.3 *Vamos mostrar essa propriedade para o caso em que $d = -7$.*

Seja $\delta = \frac{a+b\sqrt{-7}}{2}$ uma unidade de Ω_{-7}. Lembre-se que a e b são inteiros e $a \equiv b \pmod 2$. Assim, existe $\gamma = \frac{c+d\sqrt{-7}}{2} \in \mathcal{U}_{-7}$ tal que $\delta\gamma = 1$. Logo, $\mathcal{N}(\delta)\mathcal{N}(\gamma) = 1$. Devemos então resolver a equação $\left(\frac{a^2+7b^2}{4}\right)\left(\frac{c^2+7d^2}{4}\right) = 1$, isto é, $(a^2 + 7b^2)(c^2 + 7d^2) = 16$. Sejam $x = a^2 + 7b^2$ e $y = c^2 + 7d^2$. Observe que $x > 0, y > 0$ e x e y são divisores de 16. Vamos verificar as possibilidades para x (e y será igual a $\frac{16}{x}$).

- $a^2 + 7b^2 = 1 \Rightarrow b = 0$ e $a = \pm 1$. Isso é um absurdo, pois $a \not\equiv b \pmod 2$. Observe que isso implica que $a^2 + 7b^2 \neq 16$, pois se pudesse ser igual a 16, $c^2 + 7d^2 = 1$ e teríamos $d = 0$ e $c = \pm 1$.

- $a^2 + 7b^2 = 2 \Rightarrow b = 0$ e $a^2 = 2$. Isso é um absurdo, pois $a \notin \mathbb{Z}$. Observe que isso implica que $a^2 + 7b^2 \neq 8$, pois se pudesse ser igual a 8, $c^2 + 7d^2 = 2$ e teríamos $d = 0$ e $c^2 = 2$.

- $a^2 + 7b^2 = 4 \Rightarrow b = 0$ e $a = \pm 2$.

Assim, as únicas unidades do anel Ω_{-7} são os números ± 1.

Definição 1.4 *O máximo divisor comum de dois inteiros algébricos μ e ρ é o maior (em norma, a menos de unidade) de todos os divisores comuns de μ e ρ. Ele será denotado por* $\mathrm{mdc}(\mu, \rho)$.

Exemplo 1.4 *O* $\mathrm{mdc}\left(\frac{1+\sqrt{-7}}{2}, \frac{1-\sqrt{-7}}{2}\right)$ *é uma unidade em* Ω_{-7}.

Seja $\delta = \mathrm{mdc}\left(\frac{1+\sqrt{-7}}{2}, \frac{1-\sqrt{-7}}{2}\right)$. Por definição, $\delta \mid \frac{1+\sqrt{-7}}{2}$ e $\delta \mid \frac{1-\sqrt{-7}}{2}$. Logo, $\delta \mid \frac{1+\sqrt{-7}}{2} + \frac{1-\sqrt{-7}}{2} = 1$ e então $\mathcal{N}(\delta) \mid \mathcal{N}(1) = 1$. Portanto $\mathcal{N}(\delta) = \pm 1$.

Dizemos que μ e ρ são primos entre si, se $\gamma := \mathrm{mdc}(\mu, \rho)$ é uma unidade do anel, isto é, se $\mathcal{N}(\gamma) = \pm 1$. Pelo exemplo anterior, temos que $\frac{1+\sqrt{-7}}{2}$ e $\frac{1-\sqrt{-7}}{2}$ são primos entre si.

Até o final deste capítulo, considere que R seja um anel, R^* seja o conjunto das unidades de R e 0 seja o elemento neutro para a adição de R.

Um conceito importante é o de Domínio de Fatoração Única.

Definição 1.5 *Dizemos que R é um Domínio de Fatoração Única se R é um domínio de integridade (dados a e $b \in R$, se $a \cdot b = 0$, então $a = 0$ ou $b = 0$) no qual todo elemento que não é nulo ou não é unidade tem uma fatoração única, isto é, tem uma única decomposição em fatores irredutíveis.*

Um problema na teoria de aneis de inteiros algébricos é decidir o seguinte: para que valores de d o anel Ω_d é um Domínio de Fatoração Única (DFU)? Se $d < 0$, então esse problema já está completamente resolvido (por K. Heehner em 1952 e por Stark e A. Baker em 1966, de forma independente). Quando $d > 0$, poucos casos foram resolvidos.

Teorema 1.6 *O anel Ω_d é um DFU, para $d < 0$ livre de quadrados, exatamente quando*

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

Se $d > 0$, então tem-se que Ω_d é um DFU se

$$d \in \{2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 33, 37, 41, 53, 57, 61, 69, 73, 77, 89, 93, 97\}.$$

Observação 1.2 *Se $d > 0$ não pertence ao conjunto acima, então não se pode garantir se Ω_d é um DFU ou não. No entanto, quando $d < 0$, então sempre podemos decidir se Ω_d é um DFU, pelo teorema anterior.*

Os conceitos de primo e irredutivel em um anel R são importantes. Veremos que se R for um DFU, esses conceitos coincidem (assim como acontece em $\mathbb{Z}$).

Definição 1.6 *Um elemento $a \in R - (R^* \cup \{0\})$ diz-se:*

(i) *irredutível se: $a = bc \Rightarrow b \in R^*$ ou $c \in R^*$;*

(ii) *primo se: $a \mid bc \Rightarrow a \mid b$ ou $a \mid c$.*

Teorema 1.7 *Se R é um DFU, então os primos e os irredutíveis coincidem.*

Demonstração: (primo $\Rightarrow$ irredutível) Seja $p \in R$ um primo tal que $p = bc$ (logo $p \mid bc$). Queremos provar que b ou $c \in R^*$. Por definição, $p \mid b$ ou $p \mid c$. Sem perda de generalidade, suponha que $p \mid b$. Assim, existe $d \in R$ tal que $b = p \cdot d$. Multiplicando os lados da última relação por c, obtemos $bc = pdc$, isto é, $p = pdc$. Portanto, $p(1-dc) = 0$. Como $p \neq 0$ e R é um domínio de integridade, então $1 - dc = 0$, ou ainda, $dc = 1$, o que mostra que $c \in R^*$. Portanto, p é irredutível.
(irredutível $\Rightarrow$ primo) Seja $c \in R$ irredutível tal que $c \mid ab$, em que a e $b \in R$. Queremos provar que $c \mid a$ ou $c \mid b$. Por definição, existe $k \in R$ tal que $ab = kc$. Como R é um DFU, existem únicos $\alpha_1, \ldots, \alpha_s$ e $\beta_1, \ldots, \beta_r$ irredutíveis tais que $a = u_1\alpha_1 \cdots \alpha_s$ e $b = u_2\beta_1 \cdots \beta_r$, em que u_1 e u_2 são unidades. Logo, $u_1u_2\alpha_1 \cdots \alpha_s\beta_1 \cdots \beta_r = ab = kc$. Como a fatoração de ab é única e os α_i's, os β_i's e c são irredutíveis, então concluímos que $c = \alpha_i$, para algum $i \in \{1, \ldots, s\}$ (daí, $c \mid a$) ou $c = \beta_j$, para algum $j \in \{1, \ldots, r\}$ (daí, $c \mid b$). Portanto, c é primo.

■

Observação 1.3 *Observe que R ser um domínio de integridade já é suficiente para que (primo $\Rightarrow$ irredutível).*

1.3 Algumas propriedades analíticas

Dada uma função analítica f, queremos encontrar polinômios com coeficientes inteiros que aproximem f em algum sentido. Nesta seção, discutiremos esses aproximantes. Essa teoria será importante no decorrer deste trabalho. Também é importante na prova de irracionalidade de e^a, $a \in \mathbb{Q}^*$, e π, por exemplo. Para mais detalhes, consultar [14].

Definição 1.7 *Seja $f : \Omega \to \mathbb{C}$ uma função analítica, em que $\Omega \subseteq \mathbb{C}$ é um conjunto aberto e conexo e $0 \in \Omega$. Dizemos que $f(z)$ é bem aproximada pela função racional $\frac{P_{r_0}(z)}{Q_{r_1}(z)}$, onde $P_{r_0}(z)$ e $Q_{r_1}(z)$ são polinômios de grau r_0 e r_1, respectivamente, se $Q_{r_1}(z)f(z) - P_{r_0}(z)$ tem um zero de multiplicidade $r_0 + r_1 + 1$ na origem.*

Seja

$$f(z) = \sum_{k=0}^{\infty} a_k z^k$$

a expansão de Taylor de f em torno da origem. Dados r_0 e $r_1 \in \mathbb{N}$, desejamos construir uma outra função analítica g dependendo de f e suas derivadas, de tal forma que os coeficientes de ordens $r_0 + 1, \ldots, r_0 + r_1$ da série de Taylor dessa nova função sejam nulos, isto é, queremos construir uma função g, tal que se

$$g(z) = \sum_{k=0}^{\infty} b_k z^k,$$

então $b_{r_0+1} = \cdots = b_{r_0+r_1} = 0$. Daí, podemos reescrever g como

$$g(z) = \sum_{k=0}^{r_0} b_k z^k + \sum_{k=r_0+r_1+1}^{\infty} b_k z^k = \sum_{k=0}^{r_0} b_k z^k + z^{r_0+r_1+1} \sum_{k=0}^{\infty} c_k z^k,$$

em que $c_k = b_{r_0+r_1+1+k}$.

Vamos exemplificar a construção desses aproximantes para a função exponencial e para isso usaremos operadores diferenciais $D = \frac{d}{dz}$. Como usual, definimos recursivamente, $D^2 = D \circ D$ e $D^m = D^{m-1} \circ D$. Para nossos objetivos o operador $\delta = zD$ será bastante útil.

Proposição 1.7 *Dados k e m inteiros não negativos e $\delta = zD$, em que $D = \frac{d}{dz}$, as seguintes relações são válidas:*

(i) $\delta(z^k) = kz^k$;

(ii) $\delta^m(z^k) = k^m z^k$;

(iii) *Se $T(z)$ é um polinômio com coeficientes complexos, então $T(\delta)z^k = T(k)z^k$.*

Demonstração: (i) Note que $\delta(z^k) = zD(z^k) = z\frac{d}{dz}(z^k) = zkz^{k-1} = kz^k$.
(ii) Provaremos esse item, usando indução sobre m. O item **(i)** é o caso base. A hipótese de indução é: para algum $m \in \mathbb{N}$, temos $\delta^m(z^k) = k^m z^k$. Vamos provar que $\delta^{m+1}(z^k) = k^{m+1} z^k$. Note que $\delta^{m+1}(z^k) = \delta \circ \delta^m(z^k)$. Pela hipótese de indução, temos que $\delta \circ \delta^m(z^k) = \delta(k^m z^k)$. Daí, $\delta^{m+1}(z^k) = z\frac{d}{dz}(k^m z^k) = zk^m kz^{k-1} = k^{m+1} z^k$.

(iii) Seja $T(z) = a_0 + a_1 z + \cdots + a_k z^k \in \mathbb{C}[z]$. Usando os itens **(i)** e **(ii)**, obtemos

$$\begin{aligned} T(\delta)z^k &= a_0 z^k + a_1 \delta(z^k) + \cdots + a_k \delta^k(z^k) \\ &= a_0 z^k + a_1 k z^k + \cdots + a_k k^k z^k \\ &= (a_0 + a_1 k + \cdots + a_k k^k) z^k \\ &= T(k) z^k \end{aligned}$$

■

Usando o item **(iii)** da Proposição 1.7, temos

$$T(\delta)f(z) = \sum_{k=0}^{\infty} a_k T(\delta) z^k = \sum_{k=0}^{\infty} a_k T(k) z^k = \sum_{k=0}^{\infty} b_k z^k.$$

Logo, se tomarmos $T(z) = (z - (r_0 + 1)) \cdots (z - (r_0 + r_1))$, a função $T(\delta)f(z)$ tem os coeficientes de Taylor $b_{r_0+1}, \ldots, b_{r_0+r_1}$ todos nulos. Daí, escolheremos $g(z) = T(\delta)f(z)$. Agora constuiremos os aproximantes (ambos de graus iguais a r) para a função exponencial $f : \mathbb{C} \to \mathbb{C}$ tal que $f(z) = e^z$.

Exemplo 1.5 *A série de Taylor de e^z é*

$$e^z = \sum_{k=0}^{\infty} \frac{1}{k!} z^k.$$

Logo os a_k's satisfazem $a_k = \frac{1}{k!}$. Daí, escolhendo $r_0 = r_1 = r$, temos que

$$T_r(\delta)e^z = \sum_{k=0}^{r} \frac{T_r(k)}{k!} z^k + \sum_{k=2r+1}^{\infty} \frac{T_n(k)}{k!} z^k,$$

onde $T_r(z) = (z - (r + 1)) \cdots (z - 2r)$. Observe que

- *Se $k \leq r$, então*

$$T_r(k) = (-1)(r + 1 - k) \cdots (-1)(2r - k) = (-1)^r \frac{(2r - k)!}{(r - k)!};$$

- *Se $k \geq 2r + 1$, então*

$$T_r(k) = (k - (r + 1)) \cdots (k - 2r) = \frac{(k - r - 1)!}{(k - 2r - 1)!}.$$

Definimos então

$$P_r(z) = \sum_{k=0}^{r} (-1)^r \frac{(2r - k)!}{(r - k)!k!} z^k \text{ e } R_r(z) = \sum_{k=2r+1}^{\infty} \frac{(k - r - 1)!}{(k - 2r - 1)!k!} z^k.$$

Assim, $T_r(\delta)e^z = P_r(z) + R_r(z)$. *Note que os coeficientes de* $P_r(z)$ *e de* $R_r(z)$ *são inteiros, pois* $\frac{(2r-k)!}{(r-k)!} = (k-(r+1))\cdots(k-2r)$ *e* $\frac{(k-r-1)!}{(k-2r-1)!} = (k-(r+1))\cdots(k-2r)$ *são divisíveis por* $r!$ *(ambos são produtos de* r *inteiros consecutivos). Por outro lado, usando o fato que* $\delta^k(e^z) = A_k(z)e^z$, *em que* $A_k(z)$ *é um polinômio de grau* k *com coeficientes inteiros, obtemos* $T_r(\delta)e^z = Q_r(z)e^z$, *em que* $Q_r(z)$ *é um polinômio de grau* r *com coeficientes inteiros. Daí,*

$$Q_r(z)e^z - P_r(z) = R_r(z)$$

e como $R_r(z)$ *tem um zero de multiplicidade de ordem* $2r+1$ *na origem, então* e^z *é bem aproximado por* $\frac{P_r(z)}{Q_r(z)}$.

O próximo resultado, nos fornecerá mais informações sobre $R_r(z)$.

Proposição 1.8 *Dado* $z \in \mathbb{C}$, *então*

$$|R_r(z)| \leq \frac{|z|^{2r+1}}{(r+1)!}e^{|z|}.$$

Em particular, $|R_r(z)|$ *tende a zero, quando* r *tende a infinito.*

Demonstração: Fazendo a mudança de índices $k = \ell + 2r + 1$ na definição de $R_r(z)$, temos

$$R_r(z) = z^{2r+1}\sum_{\ell=0}^{\infty}\frac{(\ell+r)!}{(\ell+2r+1)!}\frac{z^\ell}{\ell!}.$$

Note que

$$\frac{(\ell+2r+1)!}{(\ell+r)!} = (\ell+2r+1)\cdots(\ell+r+1) \geq (r+1)!.$$

Daí,

$$\begin{aligned} R_r(z) &\leq z^{2r+1}\sum_{\ell=0}^{\infty}\frac{1}{(r+1)!}\frac{z^\ell}{\ell!} \\ &= \frac{z^{2r+1}}{(r+1)!}\sum_{\ell=0}^{\infty}\frac{z^\ell}{\ell!} \\ &= \frac{z^{2r+1}}{(r+1)!}e^z. \end{aligned}$$

Portanto,

$$|R_r(z)| \leq \frac{|z|^{2r+1}}{(r+1)!}e^{|z|}.$$

■

Capítulo 2

A Equação $x^2 + 7 = y^n$

O objetivo deste capítulo é estudar a equação $x^2 + 7 = y^n$, em que x, y e n são números naturais. O capítulo será dividido em duas seções e, em cada uma, será explorado um caso particular da equação. Apesar de as equações serem similares, os métodos utilizados são distintos.

2.1 O caso $y = 2$

Nesta seção, estudaremos o caso $y = 2$, isto é, queremos encontrar as soluções para a equação $x^2 + 7 = 2^n$. Em 1913, Ramanujan conjecturou que as únicas soluções para essa equação são $(x, n) \in \{(1, 3), (3, 4), (5, 5), (11, 7), (181, 15)\}$. Em 1948, Nagell [17] provou essa conjectura. O resultado principal desta seção é o seguinte.

Teorema 2.1 *Sejam x e n inteiros positivos tais que*

$$x^2 + 7 = 2^n. \tag{2.1}$$

Então $(x, n) \in \{(1, 3), (3, 4), (5, 5), (11, 7), (181, 15)\}$.

Demonstração: Observe que x é um número ímpar, pois $x^2 + 7$ é par (lembre-se que n é um número natural). Primeiramente, vamos supor que n é um número par, isto é, existe um k natural tal que $n = 2k$. Assim, podemos reescrever (2.1) como $x^2+7 = 2^{2k}$, ou ainda,

$$7 = (2^k + x)(2^k - x).$$

Pelo Teorema Fundamental da Aritmética e usando o fato que $2^k + x > 2^k - x > 0$, obtemos

$$\begin{cases} 2^k + x = 7 \\ 2^k - x = 1. \end{cases}$$

Subtraindo as equações, obtemos $x = 3$. Substituindo esse valor em (2.1), encontramos $3^2 + 7 = 2^n$ e concluímos que $n = 4$. Portanto, se n é par, a única solução é

$$(x, n) = (3, 4).$$

Agora, estamos interessados em estudar a equação quando n é ímpar. Se $n = 1$, então a equação não tem solução. Se $n = 3$, então a única solução é dada por $1^2+7 = 2^3$. Suponha então que $n \geq 5$ é ímpar. Fatorando (2.1) no anel de inteiros algébricos Ω_{-7}, que é um DFU, temos

$$\left(\frac{x + \sqrt{-7}}{2}\right)\left(\frac{x - \sqrt{-7}}{2}\right) = \left(\frac{1 + \sqrt{-7}}{2}\right)^{n-2}\left(\frac{1 - \sqrt{-7}}{2}\right)^{n-2}. \tag{2.2}$$

Como x é ímpar, então cada um dos fatores é um elemento de Ω_{-7}. Seja $\delta = \text{mdc}\left(\frac{x+\sqrt{-7}}{2}, \frac{x-\sqrt{-7}}{2}\right)$. Vamos mostrar que $\mathcal{N}(\delta) = 1$.

Por definição, temos que $\delta \mid \frac{x+\sqrt{-7}}{2}$ e $\delta \mid \frac{x-\sqrt{-7}}{2}$, logo $\delta \mid \frac{x+\sqrt{-7}}{2} - \frac{x-\sqrt{-7}}{2} = \sqrt{-7}$. Assim, $\mathcal{N}(\delta) \mid \mathcal{N}(\sqrt{-7}) = 7$ e então $\mathcal{N}(\delta) \in \{1, 7\}$. Por outro lado, $\mathcal{N}(\delta) \mid \mathcal{N}(\frac{x+\sqrt{-7}}{2}) = \frac{x^2+7}{4} = 2^{n-2}$ e então $\mathcal{N}(\delta)$ é uma potência de 2. Assim, concluímos que $\mathcal{N}(\delta) = 1$.

Vamos mostrar que $\frac{1\pm\sqrt{-7}}{2}$ são primos em Ω_{-7}. Pelo Teorema 1.7, devemos mostrar que esses números são irredutíveis em Ω_{-7}.

Escreva

$$\frac{1 \pm \sqrt{-7}}{2} = \left(\frac{a + b\sqrt{-7}}{2}\right)\left(\frac{c + d\sqrt{-7}}{2}\right).$$

Aplicando a norma na relação acima, obtemos $2 = \frac{(a^2+7b^2)(c^2+7d^2)}{16}$, ou ainda,

$$(a^2 + 7b^2)(c^2 + 7d^2) = 32.$$

Usando a mesma ideia do Exemplo 1.3, temos que $\frac{a+b\sqrt{-7}}{2}$ ou $\frac{c+d\sqrt{-7}}{2}$ é uma unidade em Ω_{-7}. Portanto, $\frac{1+\sqrt{-7}}{2}$ e $\frac{1-\sqrt{-7}}{2}$ são primos.

Pelas observações anteriores, temos que os números $\frac{x+\sqrt{-7}}{2}$ e $\frac{x-\sqrt{-7}}{2}$ são primos entre si e $\frac{1+\sqrt{-7}}{2}$ e $\frac{1-\sqrt{-7}}{2}$ são primos em Ω_{-7}. Por (2.2), deduzimos que

- $\frac{x+\sqrt{-7}}{2} = \pm 1$ e $\frac{x-\sqrt{-7}}{2} = \pm\left(\frac{1+\sqrt{-7}}{2}\right)^{n-2}\left(\frac{1-\sqrt{-7}}{2}\right)^{n-2}$.
- $\frac{x+\sqrt{-7}}{2} = \pm\left(\frac{1+\sqrt{-7}}{2}\right)^{n-2}\left(\frac{1-\sqrt{-7}}{2}\right)^{n-2}$ e $\frac{x-\sqrt{-7}}{2} = \pm 1$.

Essas duas possibilidades não podem ocorrer, pois $\frac{x\pm\sqrt{-7}}{2}$ nunca é um número real, enquanto que ± 1 é real.

- $\frac{x+\sqrt{-7}}{2} = \pm\left(\frac{1+\sqrt{-7}}{2}\right)^{n-2}$ e $\frac{x-\sqrt{-7}}{2} = \pm\left(\frac{1-\sqrt{-7}}{2}\right)^{n-2}$.
- $\frac{x+\sqrt{-7}}{2} = \pm\left(\frac{1-\sqrt{-7}}{2}\right)^{n-2}$ e $\frac{x-\sqrt{-7}}{2} = \pm\left(\frac{1+\sqrt{-7}}{2}\right)^{n-2}$.

Essas duas possibilidades podem ocorrer. Para simplificar a notação, considere $k = n - 2$, ε_1, ε_2, δ_1 e $\delta_2 \in \{\pm 1\}$ tais $\varepsilon_1 \neq \varepsilon_2$ e $\delta_1 = \delta_2$. Então as informações acima podem ser reescritas como

$$\begin{cases} \frac{x+\sqrt{-7}}{2} = \delta_1 \left(\frac{1+\varepsilon_1\sqrt{-7}}{2}\right)^k \\ \frac{x-\sqrt{-7}}{2} = \delta_2 \left(\frac{1+\varepsilon_2\sqrt{-7}}{2}\right)^k. \end{cases}$$

o que implica em

$$\delta_1 \left(\frac{1+\varepsilon_1\sqrt{-7}}{2}\right)^k - \delta_2 \left(\frac{1+\varepsilon_2\sqrt{-7}}{2}\right)^k = \sqrt{-7}.$$

Analisando as possibilidades para ε_1, ε_2, δ_1 e δ_2, concluímos que

$$\left(\frac{1+\sqrt{-7}}{2}\right)^k - \left(\frac{1-\sqrt{-7}}{2}\right)^k = \pm\sqrt{-7}. \tag{2.3}$$

Vamos analisar a identidade (2.3) módulo $\left(\frac{1-\sqrt{-7}}{2}\right)^2 = \frac{-3-\sqrt{-7}}{2} := \beta$. Como n é ímpar e então k também o é. Logo podemos escrever $k = 2j + 1$, para algum $j \in \mathbb{N}$ e então

$$\left(\frac{1-\sqrt{-7}}{2}\right)^k \equiv \left(\frac{1-\sqrt{-7}}{2}\right)\left[\left(\frac{1-\sqrt{-7}}{2}\right)^2\right]^j \equiv 0 \pmod{\beta}.$$

Observe que $\beta = \frac{-3-\sqrt{-7}}{2} \mid \left(\frac{1+\sqrt{-7}}{2}\right)^2 - 1 = \frac{-5+\sqrt{-7}}{2}$. De fato, seja $r = \frac{a+b\sqrt{-7}}{2}$ tal que

$$\left(\frac{a+b\sqrt{-7}}{2}\right)\left(\frac{-3-\sqrt{-7}}{2}\right) = \frac{-5+\sqrt{-7}}{2}.$$

Vamos mostrar que $r \in \Omega_{-7}$, isto é, a e b são inteiros com mesma paridade. Desenvolvendo a relação acima, obtemos

$$\frac{(-3a+7b)+(-a-3b)\sqrt{-7}}{4} = \frac{-5+\sqrt{-7}}{2}.$$

e chegamos ao sistema

$$\begin{cases} \frac{-3a+7b}{2} = -5 \\ \frac{-a-3b}{2} = 1 \end{cases}$$

cuja solução é $(a, b) = (1, -1)$. Assim, $r \in \Omega_{-7}$. Essa divisibilidade é equivalente à congruência

$$\left(\frac{1+\sqrt{-7}}{2}\right)^2 \equiv 1 \pmod{\beta}.$$

Dessa forma, concluímos que

$$\left(\frac{1+\sqrt{-7}}{2}\right)^k \equiv \left(\frac{1+\sqrt{-7}}{2}\right)\left[\left(\frac{1+\sqrt{-7}}{2}\right)^2\right]^j \equiv \left(\frac{1+\sqrt{-7}}{2}\right) \pmod{\beta}.$$

De (2.3) e das observações acima, obtemos

$$\pm\sqrt{-7} \equiv \left(\frac{1+\sqrt{-7}}{2}\right)^k - \left(\frac{1-\sqrt{-7}}{2}\right)^k \equiv \left(\frac{1+\sqrt{-7}}{2}\right) \pmod{\beta}.$$

Note que o número à esquerda da congruência acima não pode ser $\sqrt{-7}$. Se fosse, $\beta = \frac{-3-\sqrt{-7}}{2} \mid \sqrt{-7} - \left(\frac{1+\sqrt{-7}}{2}\right) = \frac{-1+\sqrt{-7}}{2}$. Porém, $\mathcal{N}\left(\frac{-3-\sqrt{-7}}{2}\right) = 4 \nmid 2 = \mathcal{N}\left(\frac{-1+\sqrt{-7}}{2}\right)$. Além disso, o número à esquerda dessa congruência pode ser $-\sqrt{-7}$, pois $\beta = \frac{-3-\sqrt{-7}}{2} \mid -\sqrt{-7} - \left(\frac{1+\sqrt{-7}}{2}\right) = \frac{-1-3\sqrt{-7}}{2}$. De fato, seja $r = \frac{a+b\sqrt{-7}}{2}$ tal que

$$\left(\frac{a+b\sqrt{-7}}{2}\right)\left(\frac{-3-\sqrt{-7}}{2}\right) = \frac{-1-3\sqrt{-7}}{2}.$$

Vamos mostrar que $r \in \Omega_{-7}$, isto é, a e b são inteiros com mesma paridade. Desenvolvendo a relação acima, obtemos

$$\frac{(-3a+7b)+(-a-3b)\sqrt{-7}}{4} = \frac{-1-3\sqrt{-7}}{2}.$$

e chegamos ao sistema

$$\begin{cases} \frac{-3a+7b}{2} = -3 \\ \frac{-a-3b}{2} = -1 \end{cases}$$

cuja solução é $(a, b) = (2, 0)$. Assim, $r \in \Omega_{-7}$.

Assim, concluímos que $\left(\frac{1+\sqrt{-7}}{2}\right) \equiv -\sqrt{-7} \pmod{\beta}$. Voltando a (2.3), temos $\left(\frac{1+\sqrt{-7}}{2}\right)^k - \left(\frac{1-\sqrt{-7}}{2}\right)^k = -\sqrt{-7}$. Usando o Teorema Binomial, obtemos

$$-\sqrt{-7} = \left(\frac{1+\sqrt{-7}}{2}\right)^k - \left(\frac{1-\sqrt{-7}}{2}\right)^k = \sum_{i=0}^{k} \binom{k}{i} \left(\frac{1}{2}\right)^{k-i} \left[\left(\frac{\sqrt{-7}}{2}\right)^i - \left(\frac{-\sqrt{-7}}{2}\right)^i\right].$$

Os casos em que i é par não contribuem para a soma, pois $\left(\frac{\sqrt{-7}}{2}\right)^i - \left(\frac{-\sqrt{-7}}{2}\right)^i = 0$. Para os casos em que i é ímpar (logo $i = 2j+1$, para algum j natural), temos

$$\left(\frac{\sqrt{-7}}{2}\right)^{2j+1} - \left(-\frac{\sqrt{-7}}{2}\right)^{2j+1} = 2 \cdot \left(\frac{\sqrt{-7}}{2}\right)^{2j+1} = 2 \cdot \frac{\sqrt{-7}}{2}\left(-\frac{7}{2^2}\right)^j = \sqrt{-7} \cdot \frac{(-7)^j}{2^{2j}}.$$

Assim,

$$\begin{aligned} -\sqrt{-7} &= \sqrt{-7} \cdot \sum_{j=0}^{\frac{k-1}{2}} \binom{k}{2j+1} \frac{1}{2^{k-2j-1}} \frac{(-7)^j}{2^{2j}} \\ &= \sqrt{-7} \cdot \sum_{j=0}^{\frac{k-1}{2}} \binom{k}{2j+1} \frac{(-7)^j}{2^{k-1}}. \end{aligned}$$

Multiplicando os dois lados da última igualdade por 2^{k-1}, obtemos

$$-2^{k-1} = \sum_{j=0}^{\frac{k-1}{2}} \binom{k}{2j+1} (-7)^j \tag{2.4}$$

Analisando essa igualdade módulo 7, deduzimos que

$$-2^{k-1} \equiv \binom{k}{1} \equiv k \pmod 7. \tag{2.5}$$

Temos que $2^6 \equiv 1 \pmod 7$. Seja $k = 42t + \ell$ com $\ell \in \{1, 2, \ldots, 42\}$ (o número 42 foi escolhido por ser o menor múltiplo comum entre 6 e 7). Observando que $2^{k-1} \equiv 2^{42t+\ell-1} \equiv (2^6)^{7t} \cdot 2^{\ell-1} \equiv 2^{\ell-1} \pmod 7$ e que $k \equiv 42t + \ell \equiv \ell \pmod 7$, obtemos

$$-2^{\ell-1} \equiv \ell \pmod 7.$$

Como ℓ pertence ao conjunto finito $\{1, 2, \ldots, 42\}$, basta verificar para quais ℓ a congruência acima é satisfeita. Usando o programa *Mathematica*®, concluímos que ℓ pertence ao conjunto $\{3, 5, 13, 24, 26, 34\}$. No entanto, pelo fato de k ser ímpar, concluímos que ℓ também o é. Logo $\ell \in \{3, 5, 13\}$. Como $k \equiv \ell \pmod{42}$, então $k \equiv 3, 5$ ou $13 \pmod{42}$.

- Se $k \equiv 3 \pmod{42}$, então podemos ter $k = 3$ ou $k - 3 = 7^z \cdot 6h$, em que $z = \nu_7(k-3) \geq 1$ é a valorização 7-ádica de $k - 3$ e $h \neq 0$.

Se $k = 3$, então $n = 5$ e $x = 5$, fornecendo a solução $5^2 + 7 = 2^5$. Para o outro caso, considere $h \neq 0$.

Afirmação 2.1 *Para todo $j \geq 2$, temos que $7^{z+1} \mid \binom{k}{2j+1} 7^j$.*

Demonstração: Seja $y = \binom{k}{2j+1} 7^j$. Então

$$y = \binom{k}{2j+1} 7^j = \frac{k(k-1)(k-2)(k-3)}{(2j+1)2j(2j-1)(2j-2)} \cdot \binom{k-4}{2j-3} 7^j.$$

Usando a Proposição 1.2, basta provarmos que $\nu_7(7^{z+1}) \leq \nu_7(y)$, pois $\nu_p(7^{z+1}) = 0$ e $\nu_p(y) \geq 0$ para todo primo $p \neq 7$. Por definição, temos que $\nu_7(7^{z+1}) = z + 1$. Como $k - 3 = 7^z \cdot 6h$, com $7 \nmid h$, então $k - 2, k - 1$ e k não são divisíveis por 7. Daí, $\nu_7(k(k-1)(k-2)(k-3)) = z$. Além disso, como $2j + 1 < 7^{j-1}$, para todo $j \geq 2$, então $\nu_7(2j + 1) < j - 1$. Como dentre os números $2j + 1, 2j, 2j - 1$ e $2j - 2$, no máximo um deles é divisível por 7, então temos $\nu_7((2j + 1)2j(2j - 1)(2j - 2)) < j - 1$. Logo,

$$\begin{aligned} \nu_7(y) &= \nu_7(k(k-1)(k-2)(k-3)) + \nu_7\left(\binom{k-4}{2j-3}\right) \\ &\quad + \nu_7(7^j) - \nu_7((2j+1)2j(2j-1)(2j-2)) \\ &\geq z + 0 + j - (j-1) = z + 1. \end{aligned}$$

Portanto, $\nu_7(7^{z+1}) = z + 1 \leq \nu_7(y)$. Assim, $7^{z+1} \mid \binom{k}{2j+1}7^j$.

■

Pela Afirmação 2.1 e por (2.4), deduzimos que

$$-2^{k-1} \equiv \binom{k}{1} - 7 \cdot \binom{k}{3} \equiv k - \frac{7}{6}k(k-1)(k-2) \pmod{7^{z+1}}. \tag{2.6}$$

Por um lado, temos que

$$-2^{k-1} \equiv -2^{7^z \cdot 6 \cdot h + 2} \equiv -(2^{7^z \cdot 6})^h \cdot 2^2 \pmod{7^{z+1}}.$$

Usando o fato que $\phi(7^{z+1}) = 7^{z+1} - 7^z = 7^z \cdot 6$ e o Teorema 1.1, temos que

$$2^{7^z \cdot 6} \equiv 1 \pmod{7^{z+1}}.$$

Assim, concluímos que $-2^{k-1} \equiv -4 \pmod{7^{z+1}}$.

Por outro lado, vamos encontrar um j conveniente tal que

$$k - \frac{7}{6}k(k-1)(k-2) \equiv j \pmod{7^{z+1}}.$$

Como $k - 3 = 7^z \cdot 6h$, então temos que

$$\begin{aligned}
\frac{7}{6}k(k-1)(k-2) &= \frac{7}{6}(7^z \cdot 6h + 3)(7^z \cdot 6h + 2)(7^z \cdot 6h + 1) \\
&= \frac{7}{6}[(7^z \cdot 6h)^2(7^z \cdot 6h + 6) + 7^z \cdot 6h(3 \cdot 2 + 3 \cdot 1 + 2 \cdot 1) + 3 \cdot 2 \cdot 1] \\
&= 7 \cdot [(7^z \cdot 6h)^2(7^z \cdot h + 1) + 7^z \cdot h \cdot 11 + 1] \\
&= 7^{z+1} \cdot [7^z \cdot 36h^2 \cdot (7^z \cdot h + 1 + 11h)] + 7.
\end{aligned}$$

Assim, $k - \frac{7}{6}k(k-1)(k-2) \equiv k - 7 \pmod{7^{z+1}}$. Voltando a (2.6), encontramos a congruência $-4 \equiv k - 7 \pmod{7^{z+1}}$, ou ainda, $k \equiv 3 \pmod{7^{z+1}}$, o que é um absurdo. Portanto, para esse caso temos uma única solução dada por $(x, n) = (5, 5)$.

- Se $k \equiv 5 \pmod{42}$, então podemos ter $k = 5$ ou $k - 5 = 7^z \cdot 6h$, em que $z = \nu_7(k-5)$ e $h \neq 0$.

Se $k = 5$, então $n = 7$ e $x = 11$, fornecendo a solução $11^2 + 7 = 2^7$. Para o outro caso, considere $h \neq 0$.

Afirmação 2.2 *Para todo $j \geq 3$, temos que $7^{z+1} \mid \binom{k}{2j+1} \cdot 7^j$.*

Demonstração: Essa demonstração é análoga à demonstração da Afirmação 2.1 e não será feita neste trabalho.

■

Pela Afirmação 2.2 e por (2.4), deduzimos que

$$-2^{k-1} \equiv \binom{k}{1} - 7 \cdot \binom{k}{3} + 7^2 \cdot \binom{k}{5} \pmod{7^{z+1}}. \tag{2.7}$$

Usando uma ideia similar à usada no caso $k \equiv 3 \pmod{42}$, temos, por um lado, que

$$-2^{k-1} \equiv -2^{7^z \cdot 6 \cdot h + 4} \equiv -(2^{7^z \cdot 6})^h \cdot 2^4 \equiv -16 \pmod{7^{z+1}}$$

e por outro lado

$$\binom{k}{1} - 7 \cdot \binom{k}{3} + 7^2 \cdot \binom{k}{5} \equiv k - 70 + 49 \equiv k - 21 \pmod{7^{z+1}}.$$

Voltando a (2.7), encontramos a congruência $-16 \equiv k - 21 \pmod{7^{z+1}}$, ou ainda, $k \equiv 5 \pmod{7^{z+1}}$, o que é um absurdo. Portanto, para esse caso temos uma única solução dada por $(x, n) = (11, 7)$.

- Se $k \equiv 13 \pmod{42}$, então podemos ter $k = 13$ ou $k - 13 = 7^z \cdot 6h$, em que $z = \nu_7(k - 13)$ e $h \neq 0$.

Se $k = 13$, então $n = 15$ e $x = 181$, fornecendo a solução $181^2 + 7 = 2^{15}$. Para o outro caso, considere $h \neq 0$.

Afirmação 2.3 *Para todo $j \geq 7$, temos que $7^{z+1} \mid \binom{k}{2j+1} \cdot 7^j$.*

Demonstração: Essa demonstração é análoga à demonstração para a Afirmação 2.1 e não será feita neste trabalho.

■

Por (2.4), deduzimos que

$$-2^{k-1} \equiv \sum_{j=0}^{6} \binom{k}{2j+1} \cdot (-7)^j \pmod{7^{z+1}}. \tag{2.8}$$

Usando uma ideia similar à usada no caso $k \equiv 3 \pmod{42}$, temos, por um lado, que

$$-2^{k-1} \equiv -2^{7^z \cdot 6h + 12} \equiv -(2^{7^z \cdot 12})^h \cdot 2^{12} \equiv -4096 \pmod{7^{z+1}}$$

e por outro lado

$$\sum_{j=0}^{6} \binom{k}{2j+1} \cdot (-7)^j \equiv k - 4109 \pmod{7^{z+1}}.$$

Voltando a (2.7), encontramos a congruência $-4096 \equiv k - 4109 \pmod{7^{z+1}}$, ou ainda, $k \equiv 13 \pmod{7^{z+1}}$, o que é um absurdo. Portanto, para esse caso temos uma única solução dada por $(x, n) = (181, 15)$.

Assim, as únicas soluções para (2.1) são $(x, n) = (1, 3), (3, 4), (5, 5), (11, 7), (181, 15)$, o que prova o Teorema 2.1.

■

2.2 O caso y ímpar

Nesta seção, estudaremos a equação $x^2 + 7 = y^n$ em que y é um número ímpar positivo e $n > 1$. Note que se $y = 1$, então a equação não tem solução. Em 1961, D. Lewis [13] provou que a equação tem no máximo duas soluções e se y é um primo ímpar, então a equação não tem solução. O resultado principal desta seção é devido a Le [11] que, em 1997, generalizou o resultado de Lewis.

Teorema 2.2 *A equação*

$$x^2 + 7 = y^n \tag{2.9}$$

não tem soluções em naturais x, y e n, com y ímpar e $n > 2$.

Demonstração: Para iniciar, vamos mostrar que n é ímpar. Suponha, por absurdo, que n seja par, isto é, $n = 2k$, para algum $k \in \mathbb{N}$. Substituindo em (2.9), obtemos

$$x^2 + 7 = y^{2k} \Leftrightarrow 7 = y^{2k} - x^2 \Leftrightarrow 7 = (y^k + x)(y^k - x).$$

Como $y^k + x > y^k - x > 0$ e 7 é primo, então, pelo Teorema Fundamental da Aritmética, concluímos que

$$\begin{cases} y^k + x = 7 \\ y^k - x = 1 \end{cases}$$

Somando as equações, temos $y^k = 4$. Logo, $2 \mid y$, o que é um absurdo, pois, por hipótese, y é ímpar. Portanto, n é ímpar.

Observe que x é par: como y é ímpar, temos $x^2 \equiv y^n - 7 \equiv 0 \pmod 2$. Como x^2 é par, então x é par.

Considere (x, y, n) uma solução para (2.9). Fatorando essa equação no anel Ω_{-7}, obtemos

$$(x + \sqrt{-7})(x - \sqrt{-7}) = y^n. \tag{2.10}$$

Afirmação 2.4 *Seja $\delta = \text{mdc}(x + \sqrt{-7}, x - \sqrt{-7})$. Então δ é uma unidade em Ω_{-7}.*

Demonstração: Basta mostrar que $\mathcal{N}(\delta) = 1$. Por definição, $\delta \mid x + \sqrt{-7}$ e $\delta \mid x - \sqrt{-7}$, logo $\delta \mid (x + \sqrt{-7}) - (x - \sqrt{-7}) = 2\sqrt{-7}$. Daí, $\mathcal{N}(\delta) \mid \mathcal{N}(2\sqrt{-7}) = 28$ e então $\mathcal{N}(\delta) \in \{1, 2, 4, 7, 14, 28\}$. Além disso, temos que $\mathcal{N}(\delta) \mid \mathcal{N}(x + \sqrt{-7}) = x^2 + 7 = y^n$. Como y é ímpar, então $\mathcal{N}(\delta)$ é ímpar. Logo, $\mathcal{N}(\delta) \in \{1, 7\}$. Suponha, por absurdo, que $\mathcal{N}(\delta) = 7$. Como $\mathcal{N}(\delta) \mid x^2 + 7$, concluímos que $7 \mid x^2 + 7$ e então $7 \mid x^2$. Como 7 é primo, então $7 \mid x$ e assim, $7^2 \mid x^2$. Como $\mathcal{N}(\delta) \mid y^n$, então $7^2 \mid y^n$ (pois $n \geq 3$). Portanto, $7^2 \mid x^2 - y^n = 7$, o que é um absurdo. Portanto, $\mathcal{N}(\delta) = 1$.

■

Como Ω_{-7} é um DFU e $x+\sqrt{-7}$ e $x-\sqrt{-7}$ são primos entre si, concluímos que $x+\sqrt{-7}=\delta_1(a+b\sqrt{-7})^n$ e $x-\sqrt{-7}=\delta_2(a_0+b_0\sqrt{-7})^n$, para certos a, a_0, b e $b_0 \in \mathbb{Z}$. Além disso, δ_1 e δ_2 são unidades em Ω_{-7} (δ_1 e $d_2 \in \{\pm 1\}$), com $\delta_1 = d_2$. Observe que

$$y^n = x^2+7 = \mathcal{N}(x+\sqrt{-7}) = \mathcal{N}[\delta_1(a+b\sqrt{-7})^n] = \mathcal{N}(\delta_1)[\mathcal{N}(a+b\sqrt{-7})]^n = (a^2+7b^2)^n.$$

Como n é ímpar e y, a e b são inteiros, então $y = a^2+7b^2$.

Usando o Teorema Binomial para $(a+b\sqrt{-7})^n$ e lembrando que n é ímpar, obtemos

$$\begin{aligned}
\pm(x+\sqrt{-7}) &= (a+b\sqrt{-7})^n \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n-k}(b\sqrt{-7})^k \\
&= \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} a^{n-2k}(b\sqrt{-7})^{2k} + \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k+1} a^{n-2k-1}(b\sqrt{-7})^{2k+1} \\
&= \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} a^{n-2k}(-7b^2)^k + b\sqrt{-7}\cdot \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k+1} a^{n-2k-1}(-7b^2)^k.
\end{aligned}$$

Como x, a e b são inteiros positivos, concluímos que

$$\pm x = \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} a^{n-2k}(-7b^2)^k \tag{2.11}$$

e

$$\pm 1 = b\cdot \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k+1} a^{n-2k-1}(-7b^2)^k. \tag{2.12}$$

Como o somatório que aparece em (2.12) é um número inteiro, então $b \mid 1$. Assim, $b = \pm 1$. Substituindo esse valor em (2.12), obtemos

$$\begin{aligned}
\pm 1 &= \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k+1} a^{n-2k-1}(-7)^k \\
&= \binom{n}{1} a^{n-1} + \binom{n}{3} a^{n-3}(-7) + \cdots + \binom{n}{n}(-7)^{\frac{n-1}{2}}.
\end{aligned}$$

Usando a relação $\binom{n}{k} = \binom{n}{n-k}$, concluímos que

$$\begin{aligned}
\pm 1 &= \binom{n}{n-1} a^{n-1} + \binom{n}{n-3} a^{n-3}(-7) + \cdots + \binom{n}{0}(-7)^{\frac{n-1}{2}} \\
&= \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} a^{2k}(-7)^{\frac{n-1}{2}-k}.
\end{aligned} \tag{2.13}$$

Afirmação 2.5 *O número a é par.*

Demonstração: Suponha, por absurdo, que a seja ímpar. Como $-7 \equiv 1 \pmod 2$ e analisando (2.11) módulo 2, obtemos

$$x \equiv a \left[\sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} a^{n-2k-1} (-7)^k \right] \equiv \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} \pmod 2.$$

Usando o fato que x é par, concluímos que

$$\sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} \equiv 0 \pmod 2. \tag{2.14}$$

Por outro lado, analisando (2.13) módulo 2, temos

$$\pm 1 \equiv \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} a^{2k} (-7)^{\frac{n-1}{2}-k} \equiv \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} \pmod 2.$$

Logo,

$$\sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} \equiv 1 \pmod 2. \tag{2.15}$$

Comparando (2.14) e (2.15), encontramos um absurdo. Portanto, a é par.

■

Afirmação 2.6 *Seja*

$$S = \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} a^{2k} (-7)^{\frac{n-1}{2}-k}.$$

Então, S é igual a 1.

Demonstração: Temos por (2.13) que $S = \pm 1$. Suponha, por absurdo, que $S = -1$. Como $-7 \equiv 1 \pmod 4$ e $a^{2k} \equiv 0 \pmod 4$, para todo $k \geq 1$ (pois a é par), então analisando (2.13) módulo 4, chegamos ao seguinte absurdo:

$$-1 \equiv S \equiv \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} a^{2k} (-7)^{\frac{n-1}{2}-k} \equiv \binom{n}{0} (-7)^{\frac{n-1}{2}} \equiv 1 \pmod 4.$$

■

Seja $\alpha = \nu_2(a)$ a valorização 2-ádica de a. Usando a Notação 1.1, temos que $2^\alpha \mid\mid a$. Dessa forma, $2^{2\alpha} \mid\mid a^2$. Como n é ímpar, faremos dois casos.

- Caso 1: $n \equiv 3 \pmod 4$.

Pelos comentários anteriores, temos

$$2^{2\alpha} \mid\mid \sum_{k=1}^{\frac{n-1}{2}} \binom{n}{2k} a^{2k} (-7)^{\frac{n-1}{2}-k}. \tag{2.16}$$

Usando a Afirmação 2.6 e (2.16), temos que

$$2^{2\alpha} \mid\mid 1 - (-7)^{\frac{n-1}{2}}.$$

Por outro lado, vamos mostrar que $2^3 \mid\mid 1 - (-7)^{\frac{n-1}{2}}$ para todo $n \equiv 3 \pmod 4$. Temos $1 - (-7)^{\frac{n-1}{2}} \equiv 0 \pmod 8$, pois $-7 \equiv 1 \pmod 8$. Para este caso, o número $\frac{n-1}{2}$ é ímpar, isto é, existe $m \in \mathbb{Z}$ tal que $\frac{n-1}{2} = 2m + 1$. Logo,

$$(-7)^{\frac{n-1}{2}} \equiv (-7)^{2m+1} \equiv (-7)^{2m} \cdot (-7) \equiv 49^m \cdot (-7) \equiv 1 \cdot 9 \equiv 9 \pmod{16}.$$

Assim, $2^4 \nmid 1 - (-7)^{\frac{n-1}{2}}$. Portanto,

$$2^3 \mid\mid 1 - (-7)^{\frac{n-1}{2}}.$$

Como $2\alpha \neq 3$, para todo α inteiro, então temos um absurdo para o caso 1. Portanto, $n \not\equiv 3 \pmod 4$.

- Caso 2: $n \equiv 1 \pmod 4$.

Suponha que $2^\beta \mid\mid n - 1$. Então, $\beta \geq 2$ e podemos reescrever essa informação como $\frac{n-1}{2} = 2^{\beta-1} \cdot m$ (com $m \nmid 2$).

Proposição 2.1 *Para este caso, tem-se* $2^{\beta+2} \mid\mid (-7)^{\frac{n-1}{2}} - 1$.

Demonstração: Observe que podemos reescrever a divisibilidade acima como $2^{\beta+2} \mid\mid ((-7)^{2^{\beta-1}})^m - 1$ e assim basta provar que $(-7)^{2^{\beta-1}} \equiv 1 \pmod{2^{\beta+2}}$ e $(-7)^{2^{\beta-1}} \not\equiv 1 \pmod{2^{\beta+3}}$.

Vamos dividir a prova em duas partes. Primeiramente, iremos provar que $(-7)^{2^{\beta-1}} \equiv 1 \pmod{2^{\beta+2}}$, o que é equivalente a provar que $7^{2^{\beta-1}} \equiv 1 \pmod{2^{\beta+2}}$, pois o número $2^{\beta-1}$ é par. Para isso, usaremos indução sobre β. Para o caso base $\beta = 2$, temos

$$7^{2^{2-1}} \equiv 7^2 \equiv 49 \equiv 1 \pmod{16}.$$

A hipótese de indução é que, para algum $\beta \in \mathbb{N}, \beta \geq 2$, a congruência $7^{2^{\beta-1}} \equiv 1 \pmod{2^{\beta+2}}$ é verdadeira, isto é, existe $c \in \mathbb{Z}$ tal que

$$7^{2^{\beta-1}} = 1 + c \cdot 2^{\beta+2}.$$

Elevando os dois termos ao quadrado, obtemos

$$\begin{aligned} 7^{2^\beta} &= 1 + 2c \cdot 2^{\beta+2} + c^2 \cdot 2^{2\beta+4} = 1 + c \cdot 2^{\beta+3} + c^2 \cdot 2^{\beta+1} \cdot 2^{\beta+3} \\ &= 1 + 2^{\beta+3} \cdot (c + c^2 \cdot 2^{\beta+1}). \end{aligned}$$

Portanto, $7^{2^\beta} \equiv 1 \pmod{2^{\beta+3}}$. Agora, resta provar que $((-7)^{2^{\beta-1}})^m \not\equiv 1 \pmod{2^{\beta+3}}$, o que equivale a provar que $(7^{2^{\beta-1}})^m \not\equiv 1 \pmod{2^{\beta+3}}$, pois $2^{\beta-1}$ é par.

Afirmação 2.7 *Temos que* $7^{2^{\beta-1}} \equiv 2^{\beta+2} + 1 \pmod{2^{\beta+3}}$.

Demonstração: Para o caso base $\beta = 2$, temos

$$7^{2^{2-1}} \equiv 7^2 \equiv 49 \equiv 17 \pmod{32}$$

e

$$2^{2+2} + 1 \equiv 16 + 1 \equiv 17 \pmod{32}.$$

A hipótese de indução é que, para algum $\beta \in \mathbb{N}, \beta \geq 2$, seja verdadeira a relação $7^{2^{\beta-1}} \equiv 2^{\beta+2} + 1 \pmod{2^{\beta+3}}$, isto é, existe $c \in \mathbb{Z}$ tal que

$$7^{2^{\beta-1}} = (2^{\beta+2} + 1) + c \cdot 2^{\beta+3}.$$

Usando um procedimento análogo ao anterior, obtemos

$$\begin{aligned} 7^{2^\beta} &= (2^{2\beta+4} + 2 \cdot 2^{\beta+2} + 1) + 2 \cdot (2^{\beta+2} + 1) \cdot c \cdot 2^{\beta+3} + c^2 \cdot 2^{2\beta+6} \\ &= 2^{\beta+4} \cdot 2^\beta + 2^{\beta+3} + 1 + 2^{\beta+4} \cdot (2^{\beta+2} + 1) \cdot c + 2^{\beta+4} \cdot c^2 \cdot 2^{\beta+2} \\ &= 2^{\beta+3} + 1 + 2^{\beta+4} \cdot (2^\beta + (2^{\beta+2} + 1) \cdot c + c^2 \cdot 2^{\beta+2}). \end{aligned}$$

Portanto, $7^{2^\beta} \equiv 2^{\beta+3} + 1 \pmod{2^{\beta+3}}$.

■

Usando a Afirmação 2.7 e o fato que $(\beta + 2) \cdot i > \beta + 3$, para $\beta \geq 2$ e $i \geq 2$, obtemos

$$\begin{aligned} (7^{2^{\beta-1}})^m &\equiv (2^{\beta+2} + 1)^m \pmod{2^{\beta+3}} \\ &\equiv 1 + m \cdot 2^{\beta+2} + \sum_{i=2}^{m} \binom{m}{i} 2^{(\beta+2)\cdot i} \pmod{2^{\beta+3}} \\ &\equiv 1 + m \cdot 2^{\beta+2} \pmod{2^{\beta+3}}. \end{aligned}$$

Como $m \nmid 2$, então $1 + m \cdot 2^{\beta+2} \not\equiv 1 \pmod{2^{\beta+3}}$, o que prova a proposição.

■

Note que

$$2^{2\alpha+\beta-1} \mid\mid \binom{n}{2} a^2 (-7)^{\frac{n-3}{2}} = \frac{n(n-1)}{2}(-7)^{\frac{n-3}{2}} a^2, \tag{2.17}$$

pois $2^{2\alpha} \mid\mid a^2$, $2^{\beta-1} \mid\mid \frac{n-1}{2}$ e n e $(-7)^{\frac{n-3}{2}}$ são ímpares.

Usando a Afirmação 2.6, a Proposição 2.1 e (2.17), concluímos que

$$2^{\gamma} \mid\mid \sum_{k=2}^{\frac{n-1}{2}} \binom{n}{2k} a^{2k} (-7)^{\frac{n-1}{2}-k}, \tag{2.18}$$

em que $\gamma = \min\{\beta+2, 2\alpha+\beta-1\}$.

Afirmação 2.8 *Temos que* $\binom{n}{2k} a^{2k} (-7)^{\frac{n-1}{2}-k} \equiv 0 \pmod{2^{2\alpha+\beta}}$ *para* $k \geq 2$.

Demonstração: Escrevendo $n-1 = 2^{\beta} \cdot p$ (em que p é ímpar, pois $2^{\beta} \mid\mid n-1$) e $a^2 = 2^{2\alpha} \cdot q$ (em que q é ímpar, pois $2^{2\alpha} \mid\mid a^2$), temos

$$\begin{aligned}
\binom{n}{2k} a^{2k} (-7)^{\frac{n-1}{2}-k} &= \frac{n(n-1)}{2k(2k-1)} \binom{n-2}{2k-2} a^2 \cdot a^{2(k-1)} (-7)^{\frac{n-1}{2}-k} \\
&= \frac{n \cdot 2^{\beta} \cdot p}{2k(2k-1)} \binom{n-2}{2k-2} 2^{2\alpha} \cdot q \cdot a^{2(k-1)} (-7)^{\frac{n-1}{2}-k} \\
&= \frac{n \cdot p \cdot q \cdot (-7)^{\frac{n-1}{2}-k}}{2k-1} \binom{n-2}{2k-2} 2^{2\alpha+\beta} \cdot \frac{a^{2(k-1)}}{2k}.
\end{aligned}$$

Seja δ a valorização 2-ádica de $2k$, isto é, $2k = 2^{\delta} \cdot r$, em que $r \geq 1$ é ímpar. Então $2^{\delta} = \frac{2k}{r} \leq 2k$. Assim, $\delta \leq \frac{\log 2k}{\log 2}$. Observe que $\delta \leq \frac{\log 2k}{\log 2} < 2(k-1)$, para todo $k \geq 2$. Como n, p, q e r são ímpares e $2(k-1) - \delta > 0$, concluímos que

$$\begin{aligned}
\nu_2\left(\binom{n}{2k} a^{2k} (-7)^{\frac{n-1}{2}-k}\right) &= \nu_2\left(\frac{n \cdot p \cdot q \cdot (-7)^{\frac{n-1}{2}-k}}{2k-1} \binom{n-2}{2k-2} 2^{2\alpha+\beta} \cdot \frac{a^{2(k-1)}}{2^{\delta} \cdot r}\right). \\
&\geq (2\alpha+\beta) + 2(k-1) - \delta \\
&\geq 2\alpha + \beta
\end{aligned}$$

Portanto, temos que $\binom{n}{2k} a^{2k} (-7)^{\frac{n-1}{2}-k} \equiv 0 \pmod{2^{2\alpha+\beta}}$ para $k \geq 2$.

■

Pela Afirmação 2.8 e por (2.18), temos que

$$2\alpha + \beta \leq \gamma = \begin{cases} \beta+2, \ se\ \beta+2 \leq 2\alpha+\beta-1 \\ 2\alpha+\beta-1, se\ 2\alpha+\beta-1 < \beta+2 \end{cases}$$

A primeira possibilidade é $2\alpha + \beta \leq \beta + 2$ (isto é $\alpha \leq 1$) com a condição $\beta + 2 \leq 2\alpha + \beta - 1$ (isto é $3 \leq 2\alpha$, ou ainda $\alpha \geq 1,5$), o que é um absurdo. A

segunda possibilidade é $2\alpha + \beta \leq 2\alpha + \beta - 1$ (isto é $0 \leq -1$), o que é um absurdo. Assim, concluímos que o Caso 2 também gera um absurdo, ou seja, $n \not\equiv 1 \pmod 4$.

Como n é ímpar e $n \not\equiv 1$ ou $3 \pmod 4$, então temos um absurdo. Portanto, a equação (2.9) não tem solução em naturais x, y e n.

■

Capítulo 3

A Equação $x^2 + 7 = 2^n \cdot m$

O objetivo deste capítulo é estudar a equação $x^2 + 7 = 2^n \cdot m$. Observe que todo número natural pode ser escrito como $2^n \cdot m$, para certos m e n. Dessa forma, resolver a equação completamente, equivaleria a resolver a equação $x^2 + 7 = k$. Já vimos que, para esse caso, temos uma infinidade de soluções. Assim não resolveremos a primeira equação completamente, mas encontraremos uma relação entre os números x e m, quando n é maior que um determinado valor.

O resultado principal deste capítulo é

Teorema 3.1 *Sejam x, m e n inteiros positivos tais que*

$$x^2 + 7 = 2^n \cdot m. \tag{3.1}$$

Então $x \in \{1, 3, 5, 11, 181\}$ ou $m > \sqrt{x}$.

Antes da demonstração, faremos algumas observações.

Observação 3.1 *Pelo Teorema 2.1, se $m = 1$ ou m é uma potência de 2, então a equação (3.1) está completamente resolvida.*

As próximas observações são consequências do Teorema 3.1.

Observação 3.2 *Se $x \in \{1, 3, 5, 11, 181\}$, então temos todas as soluções para (3.1). De fato, bastar usar o Teorema Fundamental da Aritmética para determinar os possíveis valores para n e m. Por exemplo, se $x = 1$, então $2^n \cdot m = 2^3$. Assim, $(m, n) \in \{(1, 3), (2, 2), (4, 1)\}$.*

Observação 3.3 *A condição $m > \sqrt{x}$ é boa no seguinte sentido: dado $m \in \mathbb{N}$, conseguimos limitar os valores de x e de n. De fato,*

$$x < m^2 \text{ e } n < \frac{\log(\frac{m^4+7}{m})}{\log 2},$$

pois $2^n = \frac{x^2+7}{m} < \frac{m^4+7}{m}$. *Dessa forma, escolhemos um dos limitantes e conseguimos determinar todas as soluções para (3.1), para essa escolha de* m.

Vejamos dois exemplos.

Exemplo 3.1 *Se* $m = 3$, *então* $x < 3^2 = 9$ *e* $n < \frac{\log(\frac{3^4+7}{3})}{\log 2} < 4,9$. *É claro que escolheremos o limitante para* n, *pois há menor quantidade de possibilidades para* n, *em relação a quantidade de valores de* x. *Daí verificamos as possibilidades para os valores de* x *na equação* $x^2 + 7 = 2^n \cdot 3$, *em que* $n \in \{1, 2, 3, 4\}$. *Testando esses valores, concluímos que não há soluções neste caso.*

Exemplo 3.2 *Se* $m = 7$, *então* $x < 7^2 = 49$ *e* $n < \frac{\log(\frac{7^4+7}{7})}{\log 2} < 8,5$. *Novamente, escolheremos o limitante para* n. *Daí verificamos as possibilidades para os valores de* x *na equação* $x^2 + 7 = 2^n \cdot 7$, *em que* $n \in \{1, \ldots, 8\}$. *Testando esses valores, obtemos as duas soluções* $(x, n) = (7, 3)$ *e* $(21, 6)$.

A próxima proposição nos dá uma condição necessária para que (3.1) tenha solução.

Proposição 3.1 *Se a equação (3.1) tem solução e* p *é um fator primo ímpar de* m, *então* $p = 7$ *ou* $p \equiv 1, 2$ *ou* $4 \pmod 7$.

Demonstração: Analisando a equação (3.1) módulo p, obtemos $x^2 + 7 \equiv 0 \pmod p$, ou ainda, $x^2 \equiv -7 \pmod p$. Usando a Proposição 1.1 e o Teorema 1.2 para calcular o símbolo de Legendre $\left(\frac{-7}{p}\right)$, obtemos

$$\begin{aligned}\left(\frac{-7}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{7}\right)(-1)^{\frac{7-1}{2}\cdot\frac{p-1}{2}} \\ &= (-1)^{\frac{p-1}{2}}\left(\frac{p}{7}\right)(-1)^{3\cdot\frac{p-1}{2}} = \left(\frac{p}{7}\right)(-1)^{4\cdot\frac{p-1}{2}} \\ &= \left(\frac{p}{7}\right).\end{aligned}$$

Assim, a congruência $x^2 \equiv -7 \pmod p$ tem solução se e somente se $x^2 \equiv p \pmod 7$ tem solução. Testando os casos em que $x \in \{0, \ldots, 6\}$, obtemos $x^2 \equiv 0, 1, 2, 4 \pmod 7$. Portanto, as possibilidades são $p \equiv 0, 1, 2, 4 \pmod 7$. Note que o único primo p tal que $p \equiv 0 \pmod 7$ é $p = 7$. Dessa forma, uma condição necessária para que (3.1) tenha solução é que $p = 7$ ou $p \equiv 1, 2$ ou $4 \pmod 7$.

■

Exemplo 3.3 *A equação* $x^2 + 7 = 2^n \cdot 2013$ *não tem solução, pois* $3 \mid 2013$.

Usando as Observações 3.1 e 3.3 e a Proposição 3.1, temos que a equação (3.1) (com m ímpar fixo) pode ter solução se os primos na fatoração de m são das formas $p = 7$, $p_j = 7j + 1$, $p_k = 7k + 2$ ou $p_\ell = 7\ell + 4$, com j, k e $\ell \in \mathbb{N}$.

Vamos voltar a atenção para o Teorema 3.1. O objetivo inicial é fatorar a equação (3.1) em Ω_{-7}.

3.1 Primeiros passos

Vamos iniciar a demonstração do Teorema 3.1. Note que $x^2 + 7 \equiv 2^n \cdot m \equiv 0 \pmod 2$. Logo x é ímpar. Assim, podemos fatorar (3.1) em Ω_{-7} (que é um DFU) por

$$\left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right) = \left(\frac{1+\sqrt{-7}}{2}\right)^{n-2}\left(\frac{1-\sqrt{-7}}{2}\right)^{n-2} \cdot m. \tag{3.2}$$

Para simplificar a notação, considere $\alpha = \frac{1+\sqrt{-7}}{2}$ (observe que $\mathcal{N}(\alpha) = 2$). Pela equação (3.2), temos que $\alpha^{n-2} \mid \left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right)$. Dessa forma, para $n \geq 3$, concluímos que $\alpha \mid \left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right)$. Além disso, α divide apenas um dos fatores: de fato, se $\alpha \mid \frac{x+\sqrt{-7}}{2}$ e $\alpha \mid \frac{x-\sqrt{-7}}{2}$, então $\alpha \mid \frac{x+\sqrt{-7}}{2} - \frac{x-\sqrt{-7}}{2} = \sqrt{-7}$. Logo, $\mathcal{N}(\alpha) = 2 \mid 7 = \mathcal{N}(\sqrt{-7})$, o que é um absurdo. Analogamente, prova-se que $\bar{\alpha}$ divide apenas um dos fatores. Como $\frac{x+\sqrt{-7}}{2}$ e $\frac{x-\sqrt{-7}}{2}$ são conjugados, temos que se α divide um deles, então $\bar{\alpha}$ divide o outro.

Sem perda de generalidade, suponha que $\alpha \mid \frac{x+\sqrt{-7}}{2}$ e $\bar{\alpha} \mid \frac{x-\sqrt{-7}}{2}$.
Escreva $n-2 := 65j+\ell$, em que $\ell \in \{0, \ldots, 64\}$. Tomando $k := 5j$ podemos reescrever a equação (3.2) como

$$\left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right) = (\alpha^{13})^k(\bar{\alpha}^{13})^k(\alpha\bar{\alpha})^\ell \cdot m = (\alpha^{13})^k(\bar{\alpha}^{13})^k \cdot 2^\ell \cdot m. \tag{3.3}$$

Seja $\beta := \alpha^{13}$. Essa definição e (3.3) implicam que $\beta^k \mid \left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right)$. Como β^k é uma potência de α e $\alpha \nmid \frac{x-\sqrt{-7}}{2}$, então $\beta^k \nmid \frac{x-\sqrt{-7}}{2}$. Assim, $\beta^k \mid \frac{x+\sqrt{-7}}{2}$. Daí, existe um inteiro algébrico μ tal que $\frac{x+\sqrt{-7}}{2} = \beta^k\mu$. Logo, temos que $\frac{x-\sqrt{-7}}{2} = \bar{\beta}^k\bar{\mu}$. Assim, usando (3.3), concluímos que

$$\begin{aligned}\mathcal{N}(\mu) &= \mu\bar{\mu} = |\mu|^2 = \left(\frac{x+\sqrt{-7}}{2\beta^k}\right)\left(\frac{x-\sqrt{-7}}{2\bar{\beta}^k}\right) \\ &= \left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right) \cdot \frac{1}{\beta^k\bar{\beta}^k} = 2^\ell m.\end{aligned}$$

Como $\ell \in \{0, \ldots, 64\}$, então uma estimativa para m é

$$m = \frac{|\mu|^2}{2^\ell} \geq \frac{|\mu|^2}{2^{64}}.$$

Assim, para estimar o valor de m, devemos estimar o valor de $|\mu|$.

Vamos voltar alguns passos anteriores: supondo que $\alpha \mid \frac{x+\sqrt{-7}}{2}$ (daí $\bar{\alpha} \mid \frac{x-\sqrt{-7}}{2}$), vimos que existe um inteiro algébrico μ tal que $\frac{x+\sqrt{-7}}{2} = \beta^k\mu$ e $\frac{x-\sqrt{-7}}{2} = \bar{\beta}^k\bar{\mu}$. Daí concluímos que $\beta^k\mu - \bar{\beta}^k\bar{\mu} = \sqrt{-7}$.

Para o caso em que $\alpha \mid \frac{x-\sqrt{-7}}{2}$ (daí $\bar{\alpha} \mid \frac{x+\sqrt{-7}}{2}$), o procedimento é análogo e a conclusão é que $\beta^k\mu - \bar{\beta}^k\bar{\mu} = -\sqrt{-7}$.

Em qualquer um dos casos, temos que

$$\beta^k\mu - \bar{\beta}^k\bar{\mu} = \pm\sqrt{-7}. \tag{3.4}$$

Observe que (3.4) pode ser reescrita como $\left(\frac{\bar{\beta}}{\beta}\right)^k - \frac{\mu}{\bar{\mu}} = \frac{\pm\sqrt{-7}}{\beta^k\bar{\mu}}$. Logo,

$$\left|\left(\frac{\bar{\beta}}{\beta}\right)^k - \frac{\mu}{\bar{\mu}}\right| = \frac{\sqrt{7}}{|\beta|^k|\bar{\mu}|}. \tag{3.5}$$

Como μ é inteiro algébrico, então $\frac{\mu}{\bar{\mu}}$ é um número algébrico. A relação (3.5) implica que os números $\left(\frac{\bar{\beta}}{\beta}\right)^k$ são bem aproximados por números algébricos.

O objetivo da próxima seção é encontrar aproximantes (funções racionais) para a função $(1-x)^k$ como fizemos na Seção 1.3. Escolheremos $x_0 \in \mathbb{C}$ de tal forma que $1 - x_0 = \frac{\bar{\beta}}{\beta}$, isto é, $x_0 = \frac{\beta-\bar{\beta}}{\beta}$. Para simplificar a notação, considere $\gamma := \beta - \bar{\beta}$. Daí, $x_0 = \frac{\gamma}{\beta}$. Com essas definições, o valor de x_0 é:

$$x_0 = 1 - \frac{\bar{\beta}}{\beta} = \frac{7 + 181\sqrt{-7}}{2^{14}}.$$

3.2 Aproximantes para $(1-x)^k$

Nesta seção, mostraremos alguns resultados que serão importantes na demonstração do Teorema 3.1. O objetivo inicial é encontrar aproximantes para a função $(1-x)^k$, isto é, encontrar polinômios $P_{r,k}(x)$ e $Q_{r,k}(x)$ em $\mathbb{Z}[x]$ que satisfaçam

$$P_{r,k}(x) - (1-x)^k Q_{r,k}(x) = x^{2r+1}E_{r,k}(x) \tag{3.6}$$

e $\partial P_{r,k} = \partial Q_{r,k} = r$. Note que isso implica que $E_{r,k}(x)$ é um polinômio de grau $k-r-1$.

Substituindo $x = x_0$ em (3.6), obtemos

$$\begin{aligned} P_{r,k}(x_0) - (1-x_0)^k Q_{r,k}(x_0) &= x_0^{2r+1}E_{r,k}(x_0) \\ P_{r,k}(x_0) - \left(\frac{\bar{\beta}}{\beta}\right)^k Q_{r,k}(x_0) &= \left(\frac{\gamma}{\beta}\right)^{2r+1} E_{r,k}(x_0). \end{aligned}$$

Multiplicando essa equação por β^k e escrevendo $P' = P_{r,k}(x_0)$, $Q' = Q_{r,k}(x_0)$ e $E' = \gamma^{2r+1}\beta^{k-2r-1}E_{r,k}(x_0)$, obtemos

$$\beta^k P' - \bar{\beta}^k Q' = E'. \tag{3.7}$$

Multiplicando a equação (3.4) por Q', a equação (3.7) por $\bar{\mu}$ e subtraindo as equações, concluímos que

$$\beta^k(Q'\mu - P'\bar{\mu}) = \pm Q'\sqrt{-7} - E'\bar{\mu}. \tag{3.8}$$

Com alguns ajustes, essa será a relação fundamental para conseguirmos estimar o valor de $|\mu|$. De fato, será possível mostrar que $|Q\mu - P\bar{\mu}| \geq 1$, para certos P, Q e E relacionados com P', Q' e E'. Logo $|\beta^k| < |Q\sqrt{-7} - E\bar{\mu}| \leq |Q|\sqrt{7} + |E||\bar{\mu}|$ e daí,

$$|\mu| > \frac{|\beta^k| - |Q|\sqrt{7}}{|E|}. \tag{3.9}$$

Com essa estimativa para $|\mu|$, teremos que estimar $|Q|$ e $|E|$. Para conseguir chegar a isso, vamos voltar as atenções para os aproximantes para $(1-x)^k$.

Sejam k e r inteiros positivos, com $k - r - 1 \geq 0$ (isso é necessário para que $E_{r,k}$ seja um polinômio). Defina as funções $P_{r,k}, Q_{r,k}, E_{r,k} : \mathbb{R} \to \mathbb{R}$ em que

$$P_{r,k}(x) = \frac{(k+r)!}{(k-r-1)!(r!)^2} \int_0^1 t^r (1-t)^{k-r-1}(x-t)^r dt, \tag{3.10}$$

$$Q_{r,k}(x) = \frac{(-1)^r(k+r)!}{(k-r-1)!(r!)^2} \int_0^1 (1-t+xt)^r t^{k-r-1}(1-t)^r dt, \tag{3.11}$$

$$E_{r,k}(x) = \frac{(k+r)!}{(k-r-1)!(r!)^2} \int_0^1 t^r (1-xt)^{k-r-1}(1-t)^r dt. \tag{3.12}$$

Da forma que foram definidas, pode-se concluir que essas funções são polinômios em x, pois são integrais definidas em t de multiplicações de polinômios em x e t. O fator que está multiplicando as integrais aparece para que esses polinômios tenham coeficientes inteiros e veremos a prova disso em breve. Vamos mostrar que $P_{r,k}(x), Q_{r,k}(x)$ e $E_{r,k}(x)$ satisfazem (3.6).

Proposição 3.2 *As funções $P_{r,k}$, $Q_{r,k}$ e $E_{r,k}$ satisfazem*

$$P_{r,k}(x) - (1-x)^k Q_{r,k}(x) = x^{2r+1} E_{r,k}(x)$$

para todo $x \in \mathbb{R}$.

Demonstração: Dado x real, temos

$$\int_0^1 t^r(1-t)^{k-r-1}(x-t)^r dt = \int_0^x t^r(1-t)^{k-r-1}(x-t)^r dt + \int_x^1 t^r(1-t)^{k-r-1}(x-t)^r dt. \tag{3.13}$$

A partir dessa igualdade, o resultado será provado.

Seja $I_1 = \int_0^x t^r(1-t)^{k-r-1}(x-t)^r dt$. Fazendo a mudança de variáveis $t = xu$ $(dt = xdu)$ em I_1 e substituindo u por t posteriormente, obtemos

$$I_1 = \int_0^1 (xt)^r(1-xt)^{k-r-1}(x-xt)^r x dt = \int_0^1 x^r t^r (1-xt)^{k-r-1} x^r (1-t)^r x dt$$

Logo,

$$I_1 = x^{2r+1} \int_0^1 t^r (1-xt)^{k-r-1}(1-t)^r dt.$$

Seja $I_2 = \int_x^1 t^r(1-t)^{k-r-1}(x-t)^r dt$. Fazendo a mudança de variáveis $t = 1-u+xu$ $(dt = (-1+x)du)$ em I_2 e substituindo u por t posteriormente, obtemos

$$\begin{aligned} I_2 &= \int_1^0 (1-t+xt)^r(1-(1-t+xt))^{k-r-1}(x-(1-t+xt)))^r(x-1)dt \\ &= -\int_0^1 (1-t+xt)^r(t(1-x))^{k-r-1}(-(1-x)+t(1-x))^r(-1)(1-x)dt \\ &= \int_0^1 (1-t+xt)^r t^{k-r-1}(1-x)^{k-r-1}((t-1)(1-x))^r(1-x)dt \\ &= \int_0^1 (1-t+xt)^r t^{k-r-1}(1-x)^{k-r-1}(-1)^r(1-t)^r(1-x)^r(1-x)dt. \end{aligned}$$

Logo,

$$I_2 = (1-x)^k(-1)^r \int_0^1 (1-t+xt)^r t^{k-r-1}(1-t)^r dt.$$

Assim, (3.13) pode ser reescrito como

$$\begin{aligned} \int_0^1 t^r(1-t)^{k-r-1}(x-t)^r dt &= x^{2r+1}\int_0^1 t^r(1-xt)^{k-r-1}(1-t)^r dt \\ &+ (1-x)^k(-1)^r \int_0^1 (1-t+xt)^r t^{k-r-1}(1-t)^r dt. \end{aligned}$$

Substituindo os valores encontrados em I_1 e I_2 e multiplicando (3.13) por $\frac{(k+r)!}{(k-r-1)!(r!)^2}$, obtemos

$$P_{r,k}(x) = x^{2r+1}E_{r,k}(x) + (1-x)^k Q_{r,k}(x).$$

Portanto,

$$P_{r,k}(x) - (1-x)^k Q_{r,k}(x) = x^{2r+1}E_{r,k}(x).$$

■

Vamos explicitar as expressões dos polinômios $P_{r,k}(x)$, $Q_{r,k}(x)$ e $E_{r,k}(x)$. Observe que nas três expressões (de $P_{r,k}(x)$, $Q_{r,k}(x)$ e $E_{r,k}(x)$) temos termos do tipo $t^p(1-t)^q$, para certos p e q, no integrando acompanhados por algum fator. Esse último fator pode ser calculado pelo teorema binomial, em que obtemos um somatório envolvendo coeficientes binomiais, potências de x e termos do tipo $t^{p'}(1-t)^{q'}$. Assim, antes de explicitar $P_{r,k}(x)$, $Q_{r,k}(x)$ e $E_{r,k}(x)$, vamos determinar uma fórmula fechada e conveniente para a integral $\int_0^1 t^p(1-t)^q dt$.

Lema 3.1 *Para todos os naturais p e q, temos que*

$$\int_0^1 t^p(1-t)^q dt = \frac{p!q!}{(p+q+1)!}. \tag{3.14}$$

Demonstração: Para provar isso, usaremos indução sobre p e q. Observe que a integral à esquerda de (3.14) é uma função simétrica em p e q. Para ver isso, basta fazer a mudança de variáveis $x = 1 - t$ ($dx = -dt$):

$$\int_0^1 t^p(1-t)^q dt = \int_1^0 (1-x)^p x^q(-1)dx = \int_0^1 (1-x)^p x^q dx.$$

Assim, é suficiente fixar p e usar indução sobre q. Para o caso base $q = 1$, temos

$$\begin{aligned}\int_0^1 t^p(1-t)dt &= \int_0^1 (t^p - t^{p+1})dt = \left(\frac{t^{p+1}}{p+1} - \frac{t^{p+2}}{p+2}\right)\Bigg|_0^1 \\ &= \frac{1}{p+1} - \frac{1}{p+2} = \frac{(p+2)-(p+1)}{(p+1)(p+2)} \\ &= \frac{1}{(p+1)(p+2)} = \frac{p!}{(p+1+1)!}.\end{aligned}$$

A hipótese de indução é que, para algum q natural, seja verdadeira a relação

$$\int_0^1 t^p(1-t)^q dt = \frac{p!q!}{(p+q+1)!}.$$

Vamos mostrar que $\int_0^1 t^p(1-t)^{q+1}dt = \frac{p!(q+1)!}{(p+(q+1)+1)!}$, a partir da hipótese de indução.

$$\begin{aligned}\int_0^1 t^p(1-t)^{q+1}dt &= \int_0^1 t^p(1-t)^q(1-t)dt \\ &= \int_0^1 (t^p(1-t)^q - t^{p+1}(1-t))dt \\ &= \int_0^1 t^p(1-t)^q dt - \int_0^1 t^{p+1}(1-t)^q dt. \qquad (3.15)\end{aligned}$$

Usaremos integração por partes para calcular $\int_0^1 t^{p+1}(1-t)^q dt$. Sejam $u = t^{p+1}$ e $dv = (1-t)^q dt$. Logo, $du = (p+1)t^p dt$ e $v = -\frac{(1-t)^{q+1}}{q+1}$. Assim,

$$\begin{aligned}\int_0^1 t^{p+1}(1-t)^q dt &= t^{p+1}\left[-\frac{(1-t)^{q+1}}{q+1}\right]\Bigg|_0^1 - \int_0^1 \left[-\frac{(p+1)}{(q+1)}t^p(1-t)^{q+1}\right]dt \\ &= \frac{(p+1)}{(q+1)}\int_0^1 t^p(1-t)^{q+1}dt. \qquad (3.16)\end{aligned}$$

Usando (3.15), (3.16) e a hipótese de indução, obtemos

$$\int_0^1 t^p(1-t)^{q+1}dt = \frac{p!q!}{(p+q+1)!} - \frac{(p+1)}{(q+1)}\int_0^1 t^p(1-t)^{q+1}dt.$$

Assim,

$$\left[1 + \frac{(p+1)}{(q+1)}\right]\int_0^1 t^p(1-t)^{q+1}dt = \frac{p!q!}{(p+q+1)!},$$

isto é,

$$\left[\frac{(p+q+2)}{(q+1)}\right]\int_0^1 t^p(1-t)^{q+1}dt = \frac{p!q!}{(p+q+1)!}.$$

Portanto,

$$\int_0^1 t^p(1-t)^{q+1}dt = \frac{(q+1)}{(p+(q+1)+1)}\cdot\frac{p!q!}{(p+q+1)!} = \frac{p!(q+1)!}{(p+(q+1)+1)!}.$$

■

Estamos prontos para obter as expressões para $P_{r,k}(x)$, $Q_{r,k}(x)$ e $E_{r,k}(x)$.

Proposição 3.3 *Os polinômios $P_{r,k}(x)$, $Q_{r,k}(x)$ e $E_{r,k}(x)$ são expressos por*

$$P_{r,k}(x) = (-1)^r\sum_{i=0}^{r}\binom{k+r}{i}\binom{2r-i}{r}(-x)^i,$$
$$Q_{r,k}(x) = (-1)^r\sum_{i=0}^{r}\binom{2r-i}{r}\binom{k-r-1+i}{i}x^i$$

e

$$E_{r,k}(x) = \sum_{i=0}^{k-r-1}\binom{k+r}{2r+i+1}\binom{r+i}{i}(-x)^i,$$

se $x \neq 0$. Além disso, $P_{r,k}(0) = Q_{r,k}(0) = (-1)^r\cdot\binom{2r}{r}$ e $E_{r,k}(0) = \binom{k+r}{2r+1}$.

Demonstração: Primeiramente, vamos determinar $P_{r,k}(0)$, $Q_{r,k}(0)$ e $E_{r,k}(0)$. Usando (3.10), (3.11), (3.12) e o Lema 3.1, temos

$$\begin{aligned}
P_{r,k}(0) &= \frac{(k+r)!}{(k-r-1)!(r!)^2}\int_0^1 t^r(1-t)^{k-r-1}(-t)^r dt \\
&= \frac{(k+r)!}{(k-r-1)!(r!)^2}\cdot(-1)^r\cdot\frac{(2r)!(k-r-1)!}{(2r+k-r-1+1)} \\
&= \frac{(-1)^r(k+r)!}{r!r!}\cdot\frac{(2r)!}{(k+r)!} = (-1)^r\cdot\binom{2r}{r},
\end{aligned}$$

$$\begin{aligned}
Q_{r,k}(0) &= \frac{(-1)^r(k+r)!}{(k-r-1)!(r!)^2}\int_0^1 (1-t)^r t^{k-r-1}(1-t)^r dt \\
&= \frac{(-1)^r(k+r)!}{(k-r-1)!(r!)^2}\cdot\frac{(2r)!(k-r-1)!}{(2r+k-r-1+1)} \\
&= \frac{(-1)^r(k+r)!}{r!r!}\cdot\frac{(2r)!}{(k+r)!} = (-1)^r\cdot\binom{2r}{r},
\end{aligned}$$

e

$$\begin{aligned} E_{r,k}(0) &= \frac{(k+r)!}{(k-r-1)!(r!)^2}\int_0^1 t^r(1-t)^r dt \\ &= \frac{(k+r)!}{(k-r-1)!(r!)^2}\cdot\frac{r!r!}{(r+r+1)} \\ &= \frac{(k+r)!}{(k-r-1)!}\cdot\frac{1}{(2r+1)!} = \binom{k+r}{2r+1}. \end{aligned}$$

Para $x \neq 0$, usamos a definição dada em (3.10)

$$P_{r,k}(x) = \frac{(k+r)!}{(k-r-1)!(r!)^2}\int_0^1 t^r(1-t)^{k-r-1}(x-t)^r dt.$$

Seja $I_P := \int_0^1 t^r(1-t)^{k-r-1}(x-t)^r dt$. Usando o teorema binomial para o termo $(x-t)^r$, o fato que podemos comutar integral e somatório em uma soma finita e o Lema 3.1, temos que

$$\begin{aligned} I_P &= \int_0^1 t^r(1-t)^{k-r-1}\left(\sum_{i=0}^{r}\binom{r}{i}x^i(-t)^{r-i}\right)dt \\ &= \sum_{i=0}^{r}\binom{r}{i}x^i(-1)^{r-i}\int_0^1 t^{2r-i}(1-t)^{k-r-1}dt \\ &= \sum_{i=0}^{r}\frac{r!}{(r-i)!i!}\cdot(-x)^i(-1)^r\cdot\frac{(2r-i)!(k-r-1)!}{(k+r-i)!}. \end{aligned}$$

Logo,

$$\begin{aligned} P_{r,k}(x) &= \frac{(k+r)!}{(k-r-1)!(r!)^2}\cdot\sum_{i=0}^{r}\frac{r!}{(r-i)!i!}\cdot(-x)^i(-1)^r\cdot\frac{(2r-i)!(k-r-1)!}{(k+r-i)!} \\ &= (-1)^r\sum_{i=0}^{r}\frac{(k+r)!}{(k-r-1)!(r!)^2}\cdot\frac{r!}{(r-i)!i!}\cdot\frac{(2r-i)!(k-r-1)!}{(k+r-i)!}\cdot(-x)^i \\ &= (-1)^r\sum_{i=0}^{r}\frac{(k+r)!}{(k+r-i)!i!}\cdot\frac{(2r-i)!}{(r-i)!r!}\cdot(-x)^i \\ &= (-1)^r\sum_{i=0}^{r}\binom{k+r}{i}\binom{2r-i}{r}(-x)^i. \end{aligned}$$

Analogamente, usando (3.11) com o teorema binomial para o termo $((1-t)+xt)^r$ e (3.12) com o teorema binomial para o termo $(1-xt)^{k-r-1}$, provaremos as identidades para $Q_{r,k}(x)$ e $E_{r,k}(x)$, respectivamente no caso $x \neq 0$. Sejam $I_Q := \int_0^1((1-t)+xt)^r t^{k-r-1}(1-t)^r dt$ e $I_E := \int_0^1 t^r(1-xt)^{k-r-1}(1-t)^r dt$. Assim,

$$\begin{aligned} I_Q &= \int_0^1 \left(\sum_{i=0}^{r} \binom{r}{i} (xt)^i (1-t)^{r-i} \right) t^{k-r-1}(1-t)^r dt \\ &= \sum_{i=0}^{r} \binom{r}{i} x^i \int_0^1 t^{k-r-1+i}(1-t)^{2r-i} dt \\ &= \sum_{i=0}^{r} \frac{r!}{(r-i)!i!} \cdot x^i \cdot \frac{(2r-i)!(k-r-1+i)!}{(k+r)!}. \end{aligned}$$

Logo,

$$\begin{aligned} Q_{r,k}(x) &= \frac{(-1)^r(k+r)!}{(k-r-1)!(r!)^2} \cdot \sum_{i=0}^{r} \frac{r!}{(r-i)!i!} \cdot x^i \cdot \frac{(2r-i)!(k-r-1+i)!}{(k+r)!} \\ &= (-1)^r \sum_{i=0}^{r} \frac{(k+r)!}{(k-r-1)!(r!)^2} \cdot \frac{r!}{(r-i)!i!} \cdot \frac{(2r-i)!(k-r-1+i)!}{(k+r)!} x^i \\ &= (-1)^r \sum_{i=0}^{r} \frac{(2r-i)!}{(r-i)!r!} \cdot \frac{(k-r-1+i)!}{(k-r-1)!i!} \cdot x^i \\ &= (-1)^r \sum_{i=0}^{r} \binom{2r-i}{r} \binom{k-r-1+i}{i} x^i. \end{aligned}$$

Também,

$$\begin{aligned} I_E &= \int_0^1 t^r \left(\sum_{i=0}^{k-r-1} \binom{k-r-1}{i} (-xt)^i \right) (1-t)^r dt \\ &= \sum_{i=0}^{k-r-1} \binom{k-r-1}{i} (-x)^i \int_0^1 t^{r+i}(1-t)^r dt \\ &= \sum_{i=0}^{r} \frac{(k-r-1)!}{(k-r-i-1)!i!} \cdot (-x)^i \cdot \frac{(r+i)!r!}{(2r+i+1)!}. \end{aligned}$$

Logo,

$$\begin{aligned} E_{r,k}(x) &= \frac{(k+r)!}{(k-r-1)!(r!)^2} \cdot \sum_{i=0}^{r} \frac{(k-r-1)!}{(k-r-i-1)!i!} \cdot (-x)^i \cdot \frac{(r+i)!r!}{(2r+i+1)!} \\ &= \sum_{i=0}^{r} \frac{(k+r)!}{(k-r-1)!(r!)^2} \cdot \frac{(k-r-1)!}{(k-r-i-1)!i!} \cdot \frac{(r+i)!r!}{(2r+i+1)!} (-x)^i \\ &= \sum_{i=0}^{r} \frac{(k+r)!}{(2r+i+1)!(k-r-i-1)!} \cdot \frac{(r+i)!}{r!i!} (-x)^i \\ &= \sum_{i=0}^{r} \binom{k+r}{2r+i+1} \binom{r+i}{i} (-x)^i. \end{aligned}$$

■

Com essa demonstração, é possível verificar algumas propriedades dos polinômios $P_{r,k}(x), Q_{r,k}(x)$ e $E_{r,k}(x)$.

Corolário 3.1 *Os polinômios $P_{r,k}(x), Q_{r,k}(x)$ e $E_{r,k}(x)$ satisfazem*

$$P_{r,k}(x), Q_{r,k}(x) \text{ e } E_{r,k}(x) \in \mathbb{Z}[x] \text{ e } \partial P_{r,k} = \partial Q_{r,k} = r, \partial E_{r,k} = k - r - 1.$$

Demonstração: Observando a Proposição 3.2, temos que os coeficientes de $P_{r,k}(x)$, $Q_{r,k}(x), E_{r,k}(x)$ são binomiais com sinal (que são números inteiros). Além disso, os termos de maior grau em $P_{r,k}(x), Q_{r,k}(x)$ e $E_{r,k}(x)$ são, respectivamente, r, r e $k-r-1$.

■

Uma relação importante entre esses polinômios é:

Proposição 3.4 *Para todo r natural, temos que*

$$P_{r,k}(x)Q_{r+1,k}(x) - Q_{r,k}(x)P_{r+1,k}(x) = cx^{2r+1},$$

em que c é uma constante não nula.

Demonstração: Usando a identidade (3.6) com r e $r+1$, temos

$$P_{r,k}(x) - (1-x)^k Q_{r,k}(x) = x^{2r+1} E_{r,k}(x) \tag{3.17}$$

e

$$P_{r+1,k}(x) - (1-x)^k Q_{r+1,k}(x) = x^{2r+3} E_{r+1,k}(x). \tag{3.18}$$

Multiplicando (3.17) por $Q_{r+1,k}(x)$, (3.18) por $Q_{r,k}(x)$ e subtraindo as equações, obtemos

$$P_{r,k}(x)Q_{r+1,k}(x) - P_{r+1,k}(x)Q_{r,k}(x) = x^{2r+1}(Q_{r+1,k}(x)E_{r,k}(x) - x^2 Q_{r,k}(x)E_{r+1,k}(x)).$$

Pelo Corolário 3.1, o grau do polinômio à esquerda da igualdade acima é menor do que ou igual a $2r+1$. Suponha que $Q_{r+1,k}(x)E_{r,k}(x) - x^2 Q_{r,k}(x)E_{r+1,k}(x)$ não seja constante. Então o grau do polinômio à direita de da igualdade acima é maior do que $2r+1$. Isso é um absurdo pela igualdade de polinômios. Assim, $Q_{r+1,k}(x)E_{r,k}(x) - x^2 Q_{r,k}(x)E_{r+1,k}(x) = c$, em que c é constante.

Vamos mostrar que $c \neq 0$. Como c é constante, é suficiente escolher $x = 0$ na relação acima. Logo,

$$\begin{aligned} c &= Q_{r+1}(0)E_{r,k}(0) - 0^2 Q_{r,k}(0)E_{r+1}(0) = Q_{r+1}(0)E_{r,k}(0) \\ &= (-1)^{r+1}\binom{2r+2}{r+1}\binom{k+r}{r+1}. \end{aligned}$$

Na definição, temos, por hipótese, que $k \geq r+1$. Logo $k+r \geq 2r+1 > r+1$, para $r > 0$. Além disso, para todo $r > 0$, temos $2r+2 > r+1$. Portanto, $c \neq 0$.

■

3.3 Método hipergeométrico

Como visto no início da Seção 3.2, a equação (3.8) e a estimativa (3.9) serão fundamentais para estimar o valor de $|\mu|$. Queremos encontrar cotas superiores para $|Q_{r,k}(x_0)|$ e $|E_{r,k}(x_0)|$ e usar (3.9) para calcular, em função de x, essa estimativa.

Lembre-se que a variável k está em função de j ($k = 5j$), enquanto que r ainda não está. Vamos definir r em função de j coerentemente. Como $k - r - 1 \geq 0$, então r deve satisfazer $r \leq 5j - 1$. Além disso, colocaremos a condição de r poder assumir "dois"valores consecutivos para j fixado e isso será entendido em breve. Considere $r := 4j - \delta$, em que $\delta \in \{0, 1\}$. Observe que essa escolha é coerente, pois $r = 4j - \delta \leq 4j \leq 5j - 1$. As notações a seguir serão usadas até o final deste capítulo.

Notação 3.1 *Dados $j \in \mathbb{N}$ e $\delta \in \{0, 1\}$, temos*

$$\alpha = \frac{1+\sqrt{-7}}{2},\ \beta = \alpha^{13},\ k = 5j,\ r = 4j - \delta,$$
$$\gamma = \beta - \bar{\beta}\ \text{ e }\ x_0 = \frac{\gamma}{\beta} = \frac{7 + 181\sqrt{-7}}{2^{14}}.$$

Nesse momento, queremos encontrar cotas superiores para $|E_{r,k}(x_0)|$ e $|Q_{r,k}(x_0)|$. Para isso, provaremos algumas desigualdades que serão úteis para encontrá-las.

Lema 3.2 *Sejam a, b e $c \in \mathbb{N}$. Então*

$$\frac{(a+b+c)!}{a!b!c!} < \frac{1}{2\pi}\frac{(a+b+c)^{a+b+c}}{a^a b^b c^c}\sqrt{\frac{a+b+c}{abc}}.$$

Demonstração: Usando o Teorema 1.3, obtemos

$$(a+b+c)! \leq \sqrt{2\pi(a+b+c)}\left(\frac{a+b+c}{e}\right)^{a+b+c} e^{\frac{1}{12(a+b+c)}},$$

$$a! \geq \sqrt{2\pi a}\left(\frac{a}{e}\right)^a e^{\frac{1}{12a+1}},\ b! \geq \sqrt{2\pi b}\left(\frac{b}{e}\right)^b e^{\frac{1}{12b+1}} \text{ e } c! \geq \sqrt{2\pi c}\left(\frac{c}{e}\right)^c e^{\frac{1}{12c+1}}.$$

Assim,

$$\begin{aligned}\frac{(a+b+c)!}{a!b!c!} &\leq \frac{\sqrt{2\pi(a+b+c)}}{\sqrt{2\pi a}\sqrt{2\pi b}\sqrt{2\pi c}} \cdot \frac{\left(\frac{a+b+c}{e}\right)^{a+b+c}}{\left(\frac{a}{e}\right)^a\left(\frac{b}{e}\right)^b\left(\frac{c}{e}\right)^c} \cdot \frac{e^{\frac{1}{12(a+b+c)}}}{e^{\frac{1}{12a+1}}e^{\frac{1}{12b+1}}e^{\frac{1}{12c+1}}} \\ &= \frac{1}{2\pi}\sqrt{\frac{a+b+c}{abc}} \cdot \frac{(a+b+c)^{a+b+c}}{a^a b^b c^c} \cdot e^{\frac{1}{12(a+b+c)} - \frac{1}{12a+1} - \frac{1}{12b+1} - \frac{1}{12c+1}}.\end{aligned}$$

Note que $\frac{1}{12(a+b+c)} - \frac{1}{12a+1} - \frac{1}{12b+1} - \frac{1}{12c+1} < 0$.

De fato, considere $t_y := 12y + 1$, para $y \in \{a, b, c\}$. Observe que

$$\begin{aligned} & \frac{1}{12(a+b+c)} - \frac{1}{t_a} - \frac{1}{t_b} - \frac{1}{t_c} < 0 \\ \Leftrightarrow \quad & \frac{1}{12(a+b+c)} < \frac{1}{t_a} + \frac{1}{t_b} + \frac{1}{t_c} \\ \Leftrightarrow \quad & t_a t_b t_c < 12(a+b+c)[t_a t_b + t_a t_c + t_b t_c] \end{aligned}$$

e essa desigualdade é equivalente a

$$\begin{aligned} & -1 + 24(a+b+c) + 288(a^2+b^2+c^2) + 432(ab+ac+bc) + \\ & +1728(a^2b+ab^2+a^2c+ac^2+b^2c+bc^2) + 3456abc > 0, \end{aligned}$$

que claramente é verdadeira.

Assim, concluímos que $\dfrac{(a+b+c)!}{a!b!c!} < \dfrac{1}{2\pi}\sqrt{\dfrac{a+b+c}{abc}} \cdot \dfrac{(a+b+c)^{a+b+c}}{a^a b^b c^c}$.

■

Com essa última desigualdade, podemos encontrar uma cota superior para $\frac{(k+r)!}{(k-r-1)!(r!)^2}$.

Proposição 3.5 *Se $\delta = 0$, então*

$$\frac{(k+r)!}{(k-r-1)!(r!)^2} = \frac{(9j)!}{(j-1)![(4j)!]^2} < \frac{3}{8\pi}\left(\frac{3^{18}}{2^{16}}\right)^j.$$

Se $\delta = 1$, então

$$\frac{(k+r)!}{(k-r-1)!(r!)^2} = \frac{(9j-1)!}{j![(4j-1)!]^2} < \frac{2}{3\pi}\left(\frac{3^{18}}{2^{16}}\right)^j.$$

Demonstração: Primeiramente, vamos fazer o caso $\delta = 0$. Temos

$$\frac{(9j)!}{(j-1)![(4j)!]^2} = j \cdot \frac{(9j)!}{j![(4j)!]^2}.$$

Fazendo $a = j, b = c = 4j$ e usando o Lema 3.2, temos

$$\begin{aligned} j \cdot \frac{(9j)!}{(j)![(4j)!]^2} &< j \cdot \frac{1}{2\pi} \cdot \frac{(9j)^{9j}}{j^j (4j)^{4j} (4j)^{4j}} \cdot \sqrt{\frac{9j}{j(4j)^2}} \\ &= j \cdot \frac{1}{2\pi} \cdot \frac{3^{18j} \cdot j^{9j}}{j^j \cdot 2^{8j} \cdot j^{4j} \cdot 2^{8j} \cdot j^{4j}} \cdot \frac{3}{4j} \\ &= \frac{j}{4j} \cdot \frac{3}{2\pi} \cdot \left(\frac{3^{18}}{2^{16}}\right)^j \cdot \frac{j^{9j}}{j^{9j}} \\ &= \frac{3}{8\pi} \cdot \left(\frac{3^{18}}{2^{16}}\right)^j. \end{aligned}$$

Agora vamos fazer o caso $\delta = 1$, usando esse último fato:

$$\begin{aligned}\frac{(9j-1)!}{j![(4j-1)!]^2} &= \frac{(9j-1)!}{j![(4j-1)!]^2}\cdot\frac{9j\cdot(4j)^2}{9j\cdot(4j)^2}\\ &= \frac{(9j)!}{j![(4j)!]^2}\cdot\frac{16j^2}{9j} = \frac{16}{9}\cdot j\cdot\frac{(9j)!}{j![(4j)!]^2}\\ &< \frac{16}{9}\cdot\frac{3}{8\pi}\cdot\left(\frac{3^{18}}{2^{16}}\right)^j\\ &= \frac{2}{3\pi}\cdot\left(\frac{3^{18}}{2^{16}}\right)^j.\end{aligned}$$

■

Com isso, pode-se estimar os valores $|Q_{r,k}(x_0)|$ e $|E_{r,k}(x_0)|$.

Proposição 3.6 *Se $\delta = 0$, então*

$$|Q_{r,k}(x_0)| < 0,31\cdot(256,07)^j \text{ e } |E_{r,k}(x_0)| < 0,12\cdot(23,1)^j.$$

Se $\delta = 1$, então

$$|Q_{r,k}(x_0)| < 0,373\cdot(256,07)^j \text{ e } |E_{r,k}(x_0)| < 0,85\cdot(23,1)^j.$$

Assim, se $\delta \in \{0,1\}$, então $|Q_{r,k}(x_0)| < 0,373\cdot(256,07)^j$ e $|E_{r,k}(x_0)| < 0,85\cdot(23,1)^j$.

Demonstração: Para esta prova, usaremos as definições dadas em (3.11) e (3.12). Temos

$$|Q_{r,k}(x_0)| = \left|\frac{(k+r)!}{(k-r-1)!(r!)^2}\right|\cdot\left|\int_0^1 (1-t+x_0t)^r t^{k-r-1}(1-t)^r dt\right|.$$

Usando a Notação 3.1 e definindo $f(t) = 1-(1-x_0)t$, obtemos

$$|Q_{r,k}(x_0)| = \left|\frac{(9j-\delta)!}{(j+\delta-1)![(4j-\delta)!]^2}\right|\cdot\left|\int_0^1 [f(t)]^{4j-\delta}t^{j+\delta-1}(1-t)^{4j-\delta}dt\right|.$$

Pela Proposição 3.5, conseguimos uma estimativa para o primeiro fator. Falta então, uma estimativa para o segundo fator. Usando o fato que $t\in[0,1]$ e $\delta = 0$, obtemos

$$\begin{aligned}\left|\int_0^1 f(t)^{4j}t^{j-1}(1-t)^{4j}dt\right| &\le \int_0^1 |f(t)|^{4j}t^{j-1}(1-t)^{4j}dt\\ &= \int_0^1 [|f(t)|^4t(1-t)^4]^{j-1}\cdot(1-t)^4\cdot|f(t)|^4dt.\end{aligned}$$

Escreva $x_0 = a+bi$, em que $a = \frac{7}{2^{14}}$, $b = \frac{181\sqrt{7}}{2^{14}}$ e $i^2 = -1$. Então

$$\begin{aligned} |f(t)|^2 = |1-(1-x_0)t|^2 &= |1-(1-a)t+bti|^2 = [1-(1-a)t]^2+(bt)^2 \\ &= 1-2(1-a)t+[(1-a)^2+b^2]\cdot t^2. \end{aligned}$$

Substituindo os valores de a e b mencionados anteriormente, concluímos que

$$-2(1-a) = -2\left(1-\frac{7}{2^{14}}\right) = -2\left(\frac{2^{14}-7}{2^{14}}\right) = -\frac{16377}{2^{13}}$$

e

$$(1-2a+a^2+b^2) = \left(1-2\cdot\frac{7}{2^{14}}+\frac{49}{2^{28}}+\frac{181^2\cdot 7}{2^{28}}\right) = 1.$$

Daí,

$$|f(t)|^2 = 1-\frac{16377}{2^{13}}t+t^2.$$

Usando o programa *Mathematica®*, é possível determinar o máximo da função $(1-\frac{16377}{2^{13}}t+t^2)^2t(1-t)^4$, pois t pertence ao conjunto compacto $[0,1]$. Esse máximo é menor do que $0,0433154$. Também, $\int_0^1(1-t)^4(1-\frac{16377}{2^{13}}t+t^2)^2dt = 0,111142$. Logo,

$$\left|\int_0^1 f(t)^{4j}t^{j-1}(1-t)^{4j}dt\right| < (0,0433154)^{j-1}\cdot 0,111142 < (0,0433154)^j\cdot 2,566. \quad (3.19)$$

Pela Proposição 3.5 (para $\delta = 0$) e (3.19), temos

$$\begin{aligned} |Q_{r,k}(x_0)| &< \frac{3}{8\pi}\cdot\left(\frac{3^{18}}{2^{16}}\right)^j\cdot(0,0433154)^j\cdot 2,566 \\ &< 0,30628\cdot(256,07)^j < 0,31\cdot(256,07)^j. \end{aligned}$$

Para o caso $\delta = 1$, temos

$$\begin{aligned} \left|\int_0^1 f(t)^{4j-1}t^j(1-t)^{4j-1}dt\right| &\leq \int_0^1 |f(t)|^{4j-1}t^j(1-t)^{4j-1}dt \\ &= \int_0^1 [|f(t)|^4t(1-t)^4]^{j-1/4}\cdot t^{1/4}dt \\ &< (0,0433154)^{j-1/4}\int_0^1 t^{1/4}dt. \\ &< (0,0433154)^j\cdot(0,0433154)^{-1/4}\cdot\frac{4}{5} \\ &< (0,0433154)^j\cdot 1,754. \end{aligned} \quad (3.20)$$

Pela Proposição 3.5 (para $\delta = 1$) e (3.19), obtemos

$$\begin{aligned} |Q_{r,k}(x_0)| &< \frac{2}{3\pi}\cdot\left(\frac{3^{18}}{2^{16}}\right)^j\cdot 1,754\cdot(0,0433154)^j \\ &< 0,37213\cdot(256,07)^j < 0,373\cdot(256,07)^j. \end{aligned}$$

Assim, concluímos que se $\delta \in \{0,1\}$, então $|Q_{r,k}(x_0)| < 0,373 \cdot (256,07)^j$.

A prova para o caso $E_{r,k}(x)$ é similar à anterior. Temos que

$$E_{r,k}(x_0) = \frac{(k+r)!}{(k-r-1)!(r!)^2} \int_0^1 t^r (1-x_0 t)^{k-r-1} (1-t)^r dt.$$

Usando a Notação 3.1 e definindo $g(t) = 1 - x_0 t$, obtemos

$$E_{r,k}(x_0) = \frac{(9j-\delta)!}{(j+\delta-1)![(4j-\delta)!]^2} \int_0^1 t^{4j-\delta} g(t)^{j+\delta-1} (1-t)^{4j-\delta} dt.$$

Para $\delta \in \{0,1\}$, temos

$$\begin{aligned} \left| \int_0^1 t^{4j-\delta} g(t)^{j+\delta-1} (1-t)^{4j-\delta} dt \right| &\leq \int_0^1 t^{4j-\delta} |g(t)|^{j+\delta-1} (1-t)^{4j-\delta} dt \\ &= \int_0^1 (t(1-t))^{4j-\delta} (|g(t)|^2)^{\frac{j+\delta-1}{2}} dt. \end{aligned}$$

Com a escrita $x_0 = a + bi$, temos

$$\begin{aligned} |g(t)|^2 &= |1 - x_0 t|^2 = |(1-at) + bti|^2 \\ &= (1-at)^2 + b^2 t^2 = 1 - 2at + (a^2+b^2)t^2. \end{aligned}$$

Substituindo os valores de a e b mencionados anteriormente, obtemos

$$-2a = -2 \cdot \frac{7}{2^{14}} = -\frac{7}{2^{13}}$$

$$(a^2+b^2) = \frac{7^2}{2^{28}} + \frac{181^2 \cdot 7}{2^{28}} = \frac{7 \cdot (7+181^2)}{2^{28}} = \frac{7 \cdot 2^{15}}{2^{28}} = \frac{7}{2^{13}}.$$

Logo,

$$|g(t)|^2 = 1 - \frac{7}{2^{13}} t + \frac{7}{2^{13}} t^2 = 1 - \frac{7}{2^{13}} t(1-t).$$

Como $t(1-t) \leq \frac{1}{4}$, para todo $t \in \mathbb{R}$, então $|g(t)|^2 \leq 1$ e

$$\left| \int_0^1 t^{4j-\delta} g(t)^{j+\delta-1} (1-t)^{4j-\delta} dt \right| \leq \int_0^1 \left(\frac{1}{4}\right)^{4j-\delta} dt = 4^{-4j+\delta}.$$

Assim,

$$\left| \int_0^1 t^{4j-\delta} g(t)^{j+\delta-1} (1-t)^{4j-\delta} dt \right| \leq \begin{cases} 256^{-j}, \ se\ \delta = 0 \\ 4 \cdot 256^{-j}, \ se\ \delta = 1. \end{cases} \tag{3.21}$$

Pela Proposição 3.5 e (3.21), obtemos

$$\begin{aligned} |E_{r,k}(x_0)| &< \frac{3}{8\pi} \cdot \left(\frac{3^{18}}{2^{16}}\right)^j \cdot (256)^{-j} \\ &< 0,12 \cdot (23,1)^j. \end{aligned}$$

e

$$\begin{aligned} |E_{r,k}(x_0)| &< \frac{2}{3\pi} \cdot \left(\frac{3^{18}}{2^{16}}\right)^j \cdot 4 \cdot (256)^{-j} \\ &< 0,85 \cdot (23,1)^j. \end{aligned}$$

Assim, concluímos que se $\delta \in \{0,1\}$, então $|E_{r,k}(x_0)| < 0,85 \cdot (23,1)^j$.

■

Defina

$$\mathcal{G}_\delta(j) := \operatorname*{mdc}_{i \in \{0,\ldots,4j-\delta\}} \left(\binom{8j-\delta-i}{4j-\delta} \binom{j+\delta-1+i}{i} \right).$$

Teorema 3.2 *Se $j > 50$ é inteiro e $\delta \in \{0,1\}$, então*

$$\mathcal{G}_\delta(j) > (2,943)^j.$$

Demonstração: Substituir $n = 4j-\delta$, $r = i$, $c = 5$ e $m = j$ em (2.7) de [4]. Na tabela da Proposição 5.1 de [4], há um caso em que $c = 5, d = 4, L_1(c/d) = 1,3098$ e $m_0 = 50$. Usando a desigualdade (2.8) de [4], concluímos que $\mathcal{G}_\delta(j) > (1,0398)^{4j} > (2,943)^j$.

■

Para continuar a demonstração do Teorema 3.1, suponha, por absurdo, que $n > 4000$ e $m \leq \sqrt{x}$. Os outros casos serão realizados após essa parte da demonstração. Pela Observação 3.1, podemos supor que $m \geq 2$.

Como $0 \leq \ell \leq 64$, podemos estimar os valores de j, k e x:

$$j = \frac{n-2-\ell}{65} \geq \frac{4000-2-64}{65} > 60,52, \text{ isto é, } j \geq 61;$$

$$k = 5j \geq 305;$$

$x^2 + 7 = 2^n \cdot m \geq 2^n \cdot 2 > 2^{4001}$. Logo, $x > \sqrt{2^{4001}-7}$. Portanto, $x > 2^{2000}$;

Substituindo k e r, de acordo com a Notação 3.1, nas expressões da Proposição 3.6 e observando que $(-1)^{4j-\delta} = (-1)^\delta$, concluímos que

$$P_{r,k}(x) = (-1)^\delta \sum_{i=0}^{4j-\delta} \binom{9j-\delta}{i} \binom{8j-2\delta-i}{4j-\delta} (-x)^i,$$

$$Q_{r,k}(x) = (-1)^\delta \sum_{i=0}^{4j-\delta} \binom{8j-2\delta-i}{4j-\delta} \binom{j+\delta-1+i}{i} x^i,$$

e

$$E_{r,k}(x) = \sum_{i=0}^{j+\delta} \binom{9j-\delta}{8j-2\delta+i+1} \binom{4j-\delta+i}{i} (-x)^i.$$

Por definição, temos que $\mathcal{G}_\delta(j)$ divide todos os coeficientes do polinômio $Q_{r,k}(x)$, logo $Q^*_{r,k}(x) := \mathcal{G}_\delta(j)^{-1}Q_{r,k}(x) \in \mathbb{Z}[x]$. Multiplicando a equação (3.6) por $\mathcal{G}_\delta(j)^{-1}$, obtemos

$$\mathcal{G}_\delta(j)^{-1}P_{r,k}(x) - \mathcal{G}_\delta(j)^{-1}(1-x)^k Q_{r,k}(x) = \mathcal{G}_\delta(j)^{-1}x^{2r+1}E_{r,k}(x). \tag{3.22}$$

Pelo Corolário 3.1, os termos de graus $0, 1, \ldots, r$ aparecem no polinômio $P^*_{r,k}(x) := \mathcal{G}_\delta(j)^{-1}P_{r,k}(x)$, mesmo que com algum(ns) coeficiente(s) nulo(s). Já para o polinômio $E^{**}_{r,k}(x) := \mathcal{G}_\delta(j)^{-1}x^{2r+1}E_{r,k}(x)$ aparecem os termos de graus $2r+1, \ldots, k+r$, mesmo que com algum(ns) coeficiente(s) nulo(s). Como $r < 2r+1$, para todo $r > 0$, então não existem termos de mesmo grau nos polinômios $P^*_{r,k}(x)$ e $E^{**}_{r,k}(x)$. Por esse motivo e por (3.22), concluímos que $P^*_{r,k}(x)$ e $E^{**}_{r,k}(x) \in \mathbb{Z}[x]$. Observe que $E^*_{r,k}(x) := \mathcal{G}_\delta(j)^{-1}E_{r,k}(x)$ também é um polinômio em $\mathbb{Z}[x]$. De fato, se $E^*_{r,k}(x) \notin \mathbb{Z}[x]$, então $E^{**}_{r,k}(x) \notin \mathbb{Z}[x]$, pois os coeficientes de grau i do polinômio $E^*_{r,k}(x)$ são iguais aos coeficientes de grau $2r+1+i$ do polinômio $E^{**}_{r,k}(x)$ (x^{2r+1} é um monômio).

Observe que os números $P^*_{r,k}(x_0)$, $Q^*_{r,k}(x_0)$ e $E^*_{r,k}(x_0)$ não estão em Ω_{-7}. No entanto, multiplicando esses números por alguma potência conveniente de β, obtemos elementos em Ω_{-7} (em cada caso, a potência de β será o grau do polinômio associado). Assim,

$$\begin{aligned}
\beta^r P^*_{r,k}(x_0) &= \beta^r \mathcal{G}_\delta(j)^{-1}P_{r,k}\left(\frac{\gamma}{\beta}\right) = \beta^r \mathcal{G}_\delta(j)^{-1}\left[a_r\left(\frac{\gamma}{\beta}\right)^r + \cdots + a_1\left(\frac{\gamma}{\beta}\right) + a_0\right] \\
&= A_r\gamma^r + A_{r-1}\gamma^{r-1}\beta + \cdots + A_1\gamma\beta^{r-1} + A_0\beta^r \in \Omega_{-7},
\end{aligned}$$

em que os a_i's ($i = 0, 1, \ldots, r$) são os coeficientes de $P_{r,k}(x)$ e $A_r = \mathcal{G}_\delta(j)^{-1}a_r$.

$$\begin{aligned}
\beta^r Q^*_{r,k}(x_0) &= \beta^r \mathcal{G}_\delta(j)^{-1}Q_{r,k}\left(\frac{\gamma}{\beta}\right) = \beta^r \mathcal{G}_\delta(j)^{-1}\left[b_r\left(\frac{\gamma}{\beta}\right)^r + \cdots + b_1\left(\frac{\gamma}{\beta}\right) + b_0\right] \\
&= B_r\gamma^r + B_{r-1}\gamma^{r-1}\beta + \cdots + B_1\gamma\beta^{r-1} + B_0\beta^r \in \Omega_{-7},
\end{aligned}$$

em que os b_i's ($i = 0, 1, \ldots, r$) são os coeficientes de $Q_{r,k}(x)$ e $B_r = \mathcal{G}_\delta(j)^{-1}b_r$.

$$\begin{aligned}
\beta^{k-r-1}E^*_{r,k}(x_0) &= \beta^{k-r-1}\mathcal{G}_\delta(j)^{-1}E_{r,k}\left(\frac{\gamma}{\beta}\right) \\
&= \beta^{k-r-1}\mathcal{G}_\delta(j)^{-1}\left[c_{k-r-1}\left(\frac{\gamma}{\beta}\right)^{k-r-1} + \cdots + c_1\left(\frac{\gamma}{\beta}\right) + c_0\right] \\
&= C_{k-r-1}\gamma^{k-r-1} + \cdots + C_1\gamma\beta^{k-r-2} + C_0\beta^{k-r-1} \in \Omega_{-7},
\end{aligned}$$

em que os c_i's ($i = 0, 1, \ldots, k-r-1$) são os coeficientes de $E_{r,k}(x)$ e $C_r = \mathcal{G}_\delta(j)^{-1}c_r$.

Fazendo $x = x_0$ na equação (3.22) e multiplicando-a por β^{k+r} (esse fator de correção serve para que todos os elementos pertençam a Ω_{-7}), obtemos

$$\beta^{k+r}\mathcal{G}_\delta(j)^{-1}P_{r,k}(x_0) - \beta^{k+r}\mathcal{G}_\delta(j)^{-1}(1-x_0)^k Q_{r,k}(x_0) = \beta^{k+r}\mathcal{G}_\delta(j)^{-1}x_0^{2r+1}E_{r,k}(x_0).$$

Usando as definições de $P^*_{r,k}(x_0), Q^*_{r,k}(x_0)$ e $E^*_{r,k}(x_0)$, temos

$$\begin{aligned} \beta^k\beta^r P^*_{r,k}(x_0) - \beta^k\beta^r\frac{\bar{\beta}^k}{\beta^k}Q^*_{r,k}(x_0) &= \beta^{k+r}\frac{\gamma^{2r+1}}{\beta^{2r+1}}E^*_{r,k}(x_0). \\ \beta^k\beta^r P^*_{r,k}(x_0) - \bar{\beta}^k\beta^r Q^*_{r,k}(x_0) &= \beta^{k-r-1}\gamma^{2r+1}E^*_{r,k}(x_0). \end{aligned} \tag{3.23}$$

Sejam

$$P = \beta^r P^*_{r,k}(x_0), \quad Q = \beta^r Q^*_{r,k}(x_0), \quad E = \beta^{k-r-1}\gamma^{2r+1}E^*_{r,k}(x_0).$$

Note que P, Q e $E \in \Omega_{-7}$.

Substituindo esses últimos valores em (3.23), obtemos

$$\beta^k P - \bar{\beta}^k Q = E. \tag{3.24}$$

Multiplicando a equação (3.4) por Q, a equação (3.24) por $\bar{\mu}$ e subtraindo as equações, concluímos que

$$\beta^k(Q\mu - P\bar{\mu}) = Q\sqrt{-7} - E\bar{\mu}. \tag{3.25}$$

Proposição 3.7 *Para algum $\delta \in \{0,1\}$, o número $r = 4j - \delta$ é tal que $Q\mu - P\bar{\mu} \neq 0$.*

Demonstração: Das definições de P e Q, deduzimos que

$$\begin{aligned} Q\mu - P\bar{\mu} &= \beta^r\mathcal{G}_\delta(j)^{-1}Q_{r,k}(x_0)\mu - \beta^r\mathcal{G}_\delta(j)^{-1}P_{r,k}(x_0)\bar{\mu} \\ &= \beta^r\mathcal{G}_\delta(j)^{-1}(Q_{r,k}(x_0)\mu - P_{r,k}(x_0)\bar{\mu}). \end{aligned}$$

Como $\beta^r\mathcal{G}_\delta(j)^{-1} \neq 0$, então devemos mostrar que $Q_{r,k}(x_0)\mu - P_{r,k}(x_0)\bar{\mu} \neq 0$ para $r = 4j$ ou $r = 4j - 1$. Seja $s = 4j$. Suponha, por absurdo, que

$$\begin{cases} Q_{s,k}(x_0)\mu - P_{s,k}(x_0)\bar{\mu} = 0 \\ Q_{s-1,k}(x_0)\mu - P_{s-1,k}(x_0)\bar{\mu} = 0 \end{cases}$$

Multiplicando a primeira equação por $P_{s-1,k}(x_0)$, a segunda equação por $P_{s,k}(x_0)$ e subtraindo as equações, obtemos $Q_{s,k}(x_0)P_{s-1,k}(x_0)\mu - Q_{s-1,k}(x_0)P_{s,k}(x_0)\mu = 0$. Como $\mu \neq 0$, então

$$Q_{s,k}(x_0)P_{s-1,k}(x_0) - Q_{s-1,k}(x_0)P_{s,k}(x_0) = 0,$$

o que é um absurdo pela Proposição 3.4.

■

A partir de agora, considere $r = 4j - \delta$ para δ tal que $Q\mu - P\bar{\mu} \neq 0$. Para essa escolha de r, temos que $Q\mu - P\bar{\mu} = \frac{a+b\sqrt{-7}}{2}$, com $a \equiv b \pmod 2$ e a, b não nulos. Logo $|Q\mu - P\bar{\mu}| = \sqrt{\frac{a^2+7b^2}{4}} \geq 1$ (esse mínimo ocorre quando $a = 2$ e $b = 0$).

Aplicando em (3.25) essa última desigualdade e, depois, a desigualdade triangular, obtemos

$$|\beta|^k \cdot 1 \leq |\beta|^k |Q\mu - P\bar{\mu}| = |Q\sqrt{-7} - E\mu| \leq |Q|\sqrt{7} + |E||\mu|. \tag{3.26}$$

Como $|\alpha| = \sqrt{\alpha\bar{\alpha}} = \sqrt{2}$ e $\beta = \alpha^{13}$, então

$$\begin{aligned} |Q|\sqrt{7} &= |\beta|^r |Q_{r,k}(x_0)||\mathcal{G}_\delta(j)^{-1}|\sqrt{7} \\ &< (|\alpha|^{13})^{4j-\delta} \cdot 0,373 \cdot (256,07)^j \cdot (2,943)^{-j} \cdot \sqrt{7} \\ &< 0,99 \cdot 2^{26j} \cdot (87,01)^j < (5,84 \cdot 10^9)^j \end{aligned}$$

e

$$|\beta|^k = (|\alpha|^{13})^{5j} = (2^{32,5})^j > (6,074 \cdot 10^9)^j.$$

Como $j \geq 61$ (de fato, basta que $j \geq 18$), então

$$\frac{|\beta|^k}{|Q|\sqrt{7}} > \left(\frac{6,074 \cdot 10^9}{5,84 \cdot 10^9}\right)^j > (1,04)^j > 2.$$

Logo, $\frac{|\beta|^k}{2} > |Q|\sqrt{7}$. Usando esse fato e (3.26), temos

$$|\beta|^k \leq |Q|\sqrt{7} + |E||\mu| < \frac{|\beta|^k}{2} + |E||\mu|$$

e então

$$\frac{|\beta|^k}{2} \leq |E||\mu| = |\beta|^{k-r-1}|\gamma|^{2r+1}|E^*_{r,k}(x_0)||\mu|.$$

Assim,

$$|\mu| \geq \frac{1}{2} \cdot \frac{|\beta|^{r+1}}{|\gamma|^{2r+1}} \cdot \frac{1}{|E^*_{r,k}(x_0)|}.$$

Para finalizar, devemos estimar $\frac{|\beta|^{r+1}}{|\gamma|^{2r+1}}$ e $|E^*_{r,k}(x_0)|$. Note que $\gamma = \beta - \bar{\beta} = -\sqrt{-7}$. Logo, $|\gamma| = \sqrt{7}$. Lembre-se também que $\beta = \alpha^{13}$ e que $|\alpha| = \sqrt{2}$. Daí,

$$\begin{aligned} \frac{|\beta|^{r+1}}{|\gamma|^{2r+1}} &= \frac{(|\alpha|^{13})^{4j+1-\delta}}{(\sqrt{7})^{8j-2\delta+1}} = \frac{(\sqrt{2})^{52j}(\sqrt{2})^{13(1-\delta)}}{(\sqrt{7})^{8j}(\sqrt{7})^{1-2\delta}} \\ &= \frac{2^{26j}}{7^{4j}} \cdot \frac{(\sqrt{2})^{13(1-\delta)}}{(\sqrt{7})^{1-2\delta}}. \end{aligned}$$

Dessa forma, temos que

$$\frac{|\beta|^{r+1}}{|\gamma|^{2r+1}} = \begin{cases} \left(\frac{2^{26}}{7^4}\right)^j \cdot \frac{(\sqrt{2})^{13}}{\sqrt{7}}, \text{ se } \delta = 0 \\ \left(\frac{2^{26}}{7^4}\right)^j \cdot \sqrt{7}, \text{ se } \delta = 1. \end{cases}$$

Como $\frac{(\sqrt{2})^{13}}{\sqrt{7}} > \sqrt{7}$, temos que

$$\frac{|\beta|^{r+1}}{|\gamma|^{2r+1}} > \sqrt{7} \cdot \left(\frac{2^{26}}{7^4}\right)^j > 2,64 \cdot 27950^j.$$

Também,

$$\begin{aligned} |E^*_{r,k}(x_0)| &= |\mathcal{G}_\delta(j)|^{-1}|E_{r,k}(x_0)| = \frac{|E_{r,k}(x_0)|}{|\mathcal{G}_\delta(j)|} \\ &< \frac{0,85\cdot(23,1)^j}{(2,943)^j} < 0,85\cdot(7,85)^j. \end{aligned}$$

Portanto,

$$|\mu| > \frac{1}{2}\cdot\frac{2,64\cdot 27950^j}{0,85\cdot(7,85)^j} > 1,5\cdot 3560^j. \tag{3.27}$$

Conseguimos finalmente encontrar uma cota inferior para μ, mas essa ainda depende de j. Para encontrarmos uma cota que dependa apenas de x, note que

$$(|\beta|^k)^{0,363} = (|\alpha|^{13\cdot 5^j})^{0,363} = (|\alpha|^{65\cdot 0,363})^j < 3560^j.$$

Isso implica que

$$\frac{(|\beta|^k)^{0,363}}{3560^j} < 1. \tag{3.28}$$

Logo, por (3.27) e (3.28), temos

$$\begin{aligned} |\mu|^{1,363} &= |\mu|\cdot|\mu|^{0,363} > 1,5\cdot 3560^j\cdot\frac{(|\beta|^k)^{0,363}}{3560^j}\cdot|\mu|^{0,363} \\ &> 1,5\cdot(|\beta|^k|\mu|)^{0,363} \end{aligned}$$

Usando os cálculos que foram feitos para encontrar a relação (3.4), temos

$$|\beta|^k|\mu| = |\beta^k\mu| = \left|\frac{x\pm\sqrt{-7}}{2}\right| = \frac{\sqrt{x^2+7}}{2} > \frac{x^2}{2} = 0,5x, \tag{3.29}$$

para todo x positivo. Usando (3.29), obtemos

$$\begin{aligned} |\mu|^{1,363} &> 1,5\cdot(|\beta|^k|\mu|)^{0,363} > 1,5\cdot(0,5x)^{0,363} \\ &> 2,4\cdot x^{0,363} > x^{0,363}. \end{aligned}$$

Assim, concluímos que

$$|\mu|^2 = (|\mu|^{1,363})^{\frac{2}{1,363}} > (x^{0,363})^{\frac{2}{1,363}} > x^{0,532}.$$

Como $|\mu|^2 = \mu\bar{\mu} = 2^\ell\cdot m$, $0\le\ell\le 64$ e $x > 2^{2000}$, então

$$m = \frac{|\mu|^2}{2^\ell} > \frac{x^{0,532}}{2^{64}} > \sqrt{x}. \tag{3.30}$$

Note que a última desigualdade em (3.30) é verdadeira:

$$\frac{x^{0,532}}{2^{64}} > \sqrt{x} \Leftrightarrow \frac{x^{532}}{2^{64000}} > x^{500} \Leftrightarrow x^{532} > 2^{64000}x^{500} \Leftrightarrow x^{532} - 2^{64000}x^{500} > 0 \Leftrightarrow$$

$$\Leftrightarrow x^{500}(x^{32} - 2^{64000}) > 0 \Leftrightarrow x^{32} - 2^{64000} > 0 \Leftrightarrow x^{32} > 2^{64000} \Leftrightarrow x > 2^{2000}.$$

A expressão obtida em (3.30) contradiz a hipótese inicial. Portanto, $n\le 4000$ ou $m > \sqrt{x}$.

3.4 Cálculos finais

Resta mostrar que se $n \leq 4000$ e $x \notin \{1, 3, 5, 11, 181\}$, então $m > \sqrt{x}$. Vamos verificar que esse é um procedimento finito. A ideia principal é analisar a equação $x^2 + 7 = 2^n \cdot m$ módulo 2^n para cada $n \leq 4000$. Note que dado n e encontrado x, temos que $m = \frac{x^2+7}{2^n}$.

Proposição 3.8 *Sejam a e b tais que $a + b \equiv 0 \pmod{2^n}$. Então a é solução para $x^2 + 7 \equiv 0 \pmod{2^n}$ se, e somente se, b também é solução para essa congruência.*

Demonstração: Temos que $a \equiv -b \pmod{2^n}$. Assim, $a^2 \equiv b^2 \pmod{2^n}$ e daí, $a^2 + 7 \equiv b^2 + 7 \pmod{2^n}$. Portanto, a é solução para $x^2 + 7 \equiv 0 \pmod{2^n}$ se, e somente se, b também é solução para essa congruência.

■

Façamos alguns casos de n para encontrarmos um padrão.

Para $n = 1$, a congruência é $x^2 + 7 \equiv 0 \pmod{2}$ cuja única solução incongruente módulo 2 é $x = 1$ e para este caso, tem-se $m = \frac{1^2+7}{2} = 4$. Observe que como 4 é par, então $x = 1$ também será solução para a congruência $x^2 + 7 \equiv 0 \pmod{2^2}$. Além disso, como 0 não é solução para essa congruência, então também não será para nenhuma do tipo $x^2 + 7 \equiv 0 \pmod{2^k}$, em que k é um inteiro positivo.

Para $n = 2$, a congruência é $x^2 + 7 \equiv 0 \pmod{2^2}$. Como observado anteriormente, $x = 1$ é solução para essa congruência e, pela Proposição 3.8, 3 também é solução para essa congruência. Pelo passo anterior, sabe-se 0 não é solução. Além disso, 2 também não é solução para a congruência. Para $x = 1$, tem-se $m = \frac{1^2+7}{2^2} = 2$ e para $x = 3$, tem-se $m = \frac{3^2+7}{2^2} = 4$. Como esses dois valores são pares, então 1 e 3 também serão soluções para a congruência $x^2 + 7 \equiv 0 \pmod{2^3}$.

Para $n = 3$, a congruência é $x^2 + 7 \equiv 0 \pmod{2^3}$. Do passo anterior, temos que 1 e 3 são soluções para essa congruência e 0 e 2 não são. Pela Proposição 3.8, 7 e 5 são soluções e 6 não é solução. Além disso, 4 também não é solução para a congruência. Assim, as únicas 4 soluções incongruentes mod 2^3 são $1, 3, 5$ e 7. A tabela a seguir mostra essas soluções e os respectivos valores de m e aproximações (para cima, com 1 casa decimal) para $\sqrt{x}$.

x	m	$\approx \sqrt{x}$
1	1	1
3	2	1,8
5	4	2,3
7	7	2,7

Com a mesma ideia usada nos passos anteriores, temos que 3 e 5 serão soluções para $x^2+7 \equiv 0 \pmod{2^4}$ (pois os respectivos valores de m são pares) e 1 e 7 não serão (pois os respectivos valores de m são ímpares). Note que se $x \neq 1$, então $m > \sqrt{x}$. Porém, isso ainda não prova o resultado, pois sabemos que há uma infinidade de valores de x satisfazendo a congruência (basta que $x \equiv 1, 3, 5$ ou $7 \pmod{2^3}$).

Façamos o último passo antes de generalizar. Para $n = 4$, a congruência é $x^2+7 \equiv 0 \pmod{2^4}$. Do passo anterior, temos que 3 e 5 são soluções para essa congruência e $0, 1, 2, 4, 6$ e 7 não são. Pela Proposição 3.8, 13 e 11 são soluções e $16, 15, 14, 12, 10$ e 9 não são soluções e assim, as únicas 4 soluções incongruentes mod 2^4 são $3, 5, 11$ e 13. A tabela a seguir mostra essas soluções e os respectivos valores de m e aproximações (para cima, com 1 casa decimal) para $\sqrt{x}$.

x	m	$\approx \sqrt{x}$
3	1	1,8
5	2	2,3
11	8	3,4
13	11	3,7

Note que se $x \neq 3$ ou 5, então $m > \sqrt{x}$.

Estamos preparados para generalizar esses fatos.

Proposição 3.9 *A congruência $x^2 + 7 \equiv 0 \pmod{2^n}$ tem exatamente 4 soluções incongruentes mod 2^n, para cada $n \geq 3$ inteiro positivo. Considerando $x_1(n), x_2(n), x_3(n)$ e $x_4(n)$ essas soluções, temos que duas delas (por exemplo, $x_1(n)$ e $x_2(n)$) são tais que $m_j(n) = \frac{x_j(n)^2+7}{2^n}$ é ímpar, para $j = 1$ ou 2 e as outras duas (por exemplo, $x_3(n)$ e $x_4(n)$) são tais que $m_j(n) = \frac{x_j(n)^2+7}{2^n}$ é par, para $j = 3$ ou 4.*

Demonstração: Faremos indução sobre n. Para o caso base $n = 3$, as soluções são $x_1(3) = 1, x_2(3) = 7, x_3(3) = 3$ e $x_4(3) = 5$.

Vamos dividir a prova em três etapas. Primeiramente, provaremos que há 4 soluções incongruentes mod 2^{n+1} para $x^2+7 \equiv 0 \pmod{2^{n+1}}$. Após, explicitaremos, em função de $x_1(n)$ e $x_2(n)$, as soluções para essa congruência. Por fim, provaremos que duas delas são tais que $m_j(n+1)$ (para $j = 1$ ou 2) é ímpar e as outras duas são tais que $m_j(n+1)$ (para $j = 3$ ou 4) é par. Para simplificar a notação, escreveremos x_j ao invés de $x_j(n)$ e m_j ao invés de $m_j(n)$.

A hipótese de indução é que, dado $n \geq 3$ um inteiro positivo, as únicas soluções incongruentes mod 2^n para $x^2+7 \equiv 0 \pmod{2^n}$ são x_1, x_2, x_3 e x_4 tais que m_1 e m_2 são ímpares e m_3 e m_4 são pares. Sem perda de generalidade, suponha que $x_j \in [0, 2^n - 1]$. Vamos mostrar que há exatamente 4 soluções incongruentes mod 2^{n+1} para $x^2 + 7 \equiv 0 \pmod{2^{n+1}}$, explicitando-as.

Como as únicas soluções para $x^2+7 \equiv 0 \pmod{2^n}$ são x_1, x_2, x_3 e x_4, então qualquer outro número inteiro em $[0, 2^n - 1]$ não é solução para $x^2 + 7 \equiv 0 \pmod{2^{n+1}}$. Pela Proposição 3.8, os únicos números incongruentes mod 2^{n+1} que podem ser solução para a congruência $x^2 + 7 \equiv 0 \pmod{2^{n+1}}$ são x_1, x_2, x_3, x_4, $2^{n+1} - x_1$, $2^{n+1} - x_2$, $2^{n+1} - x_3$ e $2^{n+1} - x_4$. Como m_1 e m_2 são ímpares, então $x_1^2 + 7$ e $x_2^2 + 7$ não são divisíveis por 2^{n+1} e assim x_1, x_2, $2^{n+1} - x_1$ e $2^{n+1} - x_2$ também não são soluções para $x^2 + 7 \equiv 0 \pmod{2^{n+1}}$. Como m_3 e m_4 são pares, então $x_3^2 + 7$ e $x_4^2 + 7$ são divisíveis por 2^{n+1} e assim x_3, x_4, $2^{n+1} - x_3$ e $2^{n+1} - x_4$ também são soluções para $x^2 + 7 \equiv 0 \pmod{2^{n+1}}$. Portanto, as únicas 4 soluções incongruentes mod 2^{n+1} para $x^2+7 \equiv 0 \pmod{2^{n+1}}$ são x_3, x_4, $2^{n+1} - x_3$ e $2^{n+1} - x_4$.

Agora vamos mostrar que

$$y_1 = x_1 + 2^{n-1},\ y_2 = x_1 - 2^{n-1},\ y_3 = x_2 + 2^{n-1},\ y_4 = x_2 - 2^{n-1}$$

são 4 soluções incongruentes mod 2^{n+1} para $x^2+7 \equiv 0 \pmod{2^{n+1}}$, isto é, os conjuntos $\{x_3, x_4, 2^{n+1} - x_3, 2^{n+1} - x_4\}$ e $\{y_1, y_2, y_3, y_4\}$ são iguais. Observe que y_j, com $j \in \{1, 2, 3, 4\}$, não necessariamente está em $[0, 2^{n+1} - 1]$.

$$\begin{aligned} y_1^2 + 7 &\equiv (x_1 + 2^{n-1})^2 + 7 \equiv x_1^2 + 2^n x_1 + 2^{2n-2} + 7 \pmod{2^{n+1}} \\ &\equiv (x_1^2 + 7) + 2^n(x_1 + 2^{n-2}) \equiv 2^n \cdot m_1 + 2^n(x_1 + 2^{n-2}) \pmod{2^{n+1}} \\ &\equiv 2^n(m_1 + x_1 + 2^{n-2}) \pmod{2^{n+1}} \end{aligned}$$

Como $n \geq 3$ e m_1 e x_1 são ímpares, então $(m_1 + x_1 + 2^{n-2})$ é par. Portanto, $y_1^2 + 7 \equiv 0 \pmod{2^{n+1}}$. Analogamente, prova-se que

$$y_2^2 + 7 \equiv 2^n(m_1 - x_1 + 2^{n-2}) \equiv 0 \pmod{2^{n+1}}$$

$$y_3^2 + 7 \equiv 2^n(m_2 + x_2 + 2^{n-2}) \equiv 0 \pmod{2^{n+1}}$$

$$y_4^2 + 7 \equiv 2^n(m_2 - x_2 + 2^{n-2}) \equiv 0 \pmod{2^{n+1}}.$$

Agora vamos mostrar que dentre essas soluções, duas são pares e duas são ímpares. Note que $\frac{(y_1^2+7)-(y_2^2+7)}{2^{n+1}}$ e $\frac{(y_3^2+7)-(y_4^2+7)}{2^{n+1}}$ são ímpares, pois usando os cálculos acima, obtemos

$$\begin{aligned} \frac{(y_1^2 + 7) - (y_2^2 + 7)}{2^{n+1}} &= \frac{2^n(m_1 + x_1 + 2^{n-2}) - 2^n(m_1 - x_1 + 2^{n-2})}{2^{n+1}} \\ &= \frac{2^n \cdot 2x_1}{2^{n+1}} = x_1 \end{aligned}$$

e

$$\begin{aligned} \frac{(y_3^2 + 7) - (y_4^2 + 7)}{2^{n+1}} &= \frac{2^n(m_2 + x_2 + 2^{n-2}) - 2^n(m_2 - x_2 + 2^{n-2})}{2^{n+1}} \\ &= \frac{2^n \cdot 2x_2}{2^{n+1}} = x_2. \end{aligned}$$

Sejam

$$\frac{y_j^2+7}{2^{n+1}} = k_j,$$

para $j \in \{1,2,3,4\}$. Logo $k_1 - k_2 = x_1$ e $k_3 - k_4 = x_2$ e isso mostra que dentre k_1 e k_2, um é par e o outro é ímpar e dentre k_3 e k_4, um é par e o outro é ímpar. Dessa forma, construímos as 4 soluções incongruentes mod 2^{n+1} para $x_1(n+1), x_2(n+1), x_3(n+1)$ e $x_4(n+1)$.

■

Vamos agora mostrar que o procedimento que iremos realizar é finito.

Proposição 3.10 *Considere z_0 uma solução para $x^2+7 \equiv 0 \pmod{2^n}$, isto é, existe m_0 inteiro tal que $\frac{z_0^2+7}{2^n} = m_0$. Se $m_0 > \sqrt{z_0}$ e $z_k = z_0 + k \cdot 2^n$, para k inteiro não negativo, então $m_k > \sqrt{z_k}$, para $m_k = \frac{z_k^2+7}{2^n}$.*

Demonstração: Vamos mostrar que cada número $z_k = z_0 + k \cdot 2^n$ satisfaz a propriedade acima e para isso faremos indução sobre k. Para o caso base $k = 0$, a propriedade é verdadeira.

Suponha que para algum k inteiro com $z_k \equiv z_0 \pmod{2^n}$, tenhamos $m_k > \sqrt{z_k}$, em que $m_k = \frac{z_k^2+7}{2^n}$. Vamos mostrar que $m_{k+1} > \sqrt{z_{k+1}}$.

$$\begin{aligned} m_{k+1} &= \frac{z_{k+1}^2+7}{2^n} = \frac{(z_k+2^n)^2+7}{2^n} = \frac{z_k^2+2^{n+1}z_k+2^{2n}+7}{2^n} \\ &= \frac{z_k^2+7}{2^n} + 2z_k + 2^n = m_k + 2z_k + 2^n \in \mathbb{N} \end{aligned}$$

Assim, usando a hipótese de indução, obtemos

$$m_{k+1} = m_k + 2z_k + 2^n > \sqrt{z_k} + 2^n > \sqrt{z_k + 2^{2n}} > \sqrt{z_k + 2^n} = \sqrt{z_{k+1}}.$$

■

Usado essa proposição, basta que verifiquemos a propriedade $m > \sqrt{x}$ para as soluções entre 0 e $2^n - 1$, desde que $x \notin \{1,3,5,11,181\}$. Caso apareça algum desses valores de x para algum valor de n, então testamos para o próximo número da mesma classe de equivalência. Listaremos os casos em que $n \in \{5,6,7\}$.

Para $n = 5, 6$ e 7, respectivamente, temos:

x	m	$\approx \sqrt{x}$
5	1	2,2
11	4	3,3
21	14	4,6
27	23	5,2
37	43	6,1

x	m	$\approx \sqrt{x}$
11	2	3,3
21	7	4,6
43	29	6,6
53	44	7,3
75	88	8,7

x	m	$\approx \sqrt{x}$
11	1	3,3
53	22	7,3
75	44	8,7
117	107	10,8
139	151	11,8

Observe que para $n = 5$, uma solução é $x = 5$. Assim, acrescentamos na coluna de x o valor 37, pois $37 = 5 + 2^5$. Analogamente, para $n = 6$ e $n = 7$, obtivemos as soluções $x = 11$ e daí acrescentamos na coluna de x os valores 75 e 139, respectivamente, pois $75 = 11 + 2^6$ e $139 = 11 + 2^7$.

O procedimento finito é construir essas tabelas para $n = 1, \ldots, 4000$ e verificar que $m > \sqrt{x}$ em todos os casos, exceto quando $x \in \{1, 3, 5, 11, 181\}$, possivelmente.

Usando o programa *Mathematica*®, fazemos esse teste e verificamos essa propriedade. Isso completa a demonstração do Teorema 3.1.

■

Referências Bibliográficas

[1] ANDREESCU, T., ANDRICA, D., CUCUREZEANU, I., *An Introduction to Diophantine Equations*, Birkhäuser, 2010.

[2] BASTOS, G. G., *Tópicos de Álgebra Abstrata*, 2003.

[3] BENNETT, M. A., *Fractional parts of powers of rational numbers*. Math. Proc. Camb. Phil. Soc. **114** (1993), 191 - 201.

[4] BENNETT, M.A., FILASETA, M., TRIFONOV, O., *On the factorization of consecutive integers*. J. Reine Angew. Math. **629** (2009), 171 - 200.

[5] BENNETT, M. A., FILASETA M., TRIFONOV, O., *Yet another generalization of the Ramanujan-Nagell equation*. Acta Arith. **134**, no. 3 (2008), 211 - 217.

[6] BENNETT, M. A., SKINNER, C. M., *Ternary Diophantine equations via Galois representations and modular forms*. Canad. J. Math. **56** [1] (2004), 23 - 54.

[7] BUGEAUD, Y., MIGNOTTE, M., SIKSEK S., *Classical and modular approaches to exponential and diophantine equations II. The Lebesque-Nagell equation*. Compos. Math. **142** (2006), 31 - 62.

[8] COHN, J. H. E., *The Diophantine equation* $x^2 + C = y^n$. Acta Arith. **65** (1993), 367 - 381.

[9] EULER, L., *Vollständige Einleitung zur Algebra*, Vol. 2., 1770.

[10] KO, C., *On the diophantine equation* $x^2 = y^n + 1, xy \neq 0$. Sci. Sinica (Notes) **14** (1964), 457 - 460.

[11] LE, M., *A note on the diophantine equation* $x^2 + 7 = y^n$. Glasgow Math. J. **39** (1997), 59 - 63.

[12] LEBESGUE, V. A., *Sur l'impossibilite en nombres entiers de l'equation* $x^m = y^2 + 1$. Nouvelles Annales des Mathematiques (1) **9** (1850) 178.

[13] LEWIS, D. J., *Two classes of Diophantine equations*. Pacific J. Math **11** (1961), 1063 - 1076.

[14] MARQUES, D., *Teoria dos Números Transcendentes*, Coleção Textos Universitários, 2013.

[15] MIGNOTTE, M., de Weger, B. M. M., *On the Diophantine equations* $x^2+74 = y^5$ *and* $x^2 + 86 = y^5$. Glasgow Math. J. **38** (1996), 77 - 85.

[16] MURIEFAH, F. S. A., *The Diophantine equation* $x^2 + c = y^n$ *- a brief overview.* Revista Colombiana de Matemáticas **40** (2006), 31 - 37.

[17] NAGELL, T., *The diophantine equation* $x^2 + 7 = 2^n$. Arkiv mathematik **4** (1960), 185 - 187.

[18] RAMANUJAN, S., *Question* 464, J. Indian Math. Soc. **5** (1913), 120.

[19] RIBENBOIM, P., *Classical Theory of Algebraic Numbers*, Springer, 2000.

[20] SANTOS, J. P. O., *Introdução à Teoria dos Números*, Coleção Matemática Universitária, 1998.

[21] STROMBERG, K., *An Introduction to Classical Real Analysis*, Wadsworth International Mathematical Series, 1981.