UNIVERSIDADE DE BRASÍLIA
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA

Formas Lineares em Logaritmos p-ádicos Aplicadas na Resolução de Equações Diofantinas

por

Alessandra Kreutz

Brasília
2016

Alessandra Kreutz

Formas Lineares em Logaritmos p-ádicos Aplicadas na Resolução de Equações Diofantinas

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

Orientador: Prof. Dr. Diego Marques Ferreira.

Brasília

2016

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

KK92f

Kreutz, Alessandra
Formas Lineares em Logaritmos p-ádicos Aplicadas na Resolução de Equações Diofantinas / Alessandra Kreutz; orientador Diego Marques Ferreira. -- Brasília, 2016.
64 p.

Dissertação (Mestrado - Mestrado em Matemática) -- Universidade de Brasília, 2016.

1. Formas lineares em logaritmos p-ádicos. 2. Equações Diofantinas. I. Ferreira, Diego Marques, orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Formas Lineares em Logaritmos p-ádicos Aplicadas na Resolução de Equações Diofantinas

por

Alessandra Kreutz *

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

MESTRE EM MATEMÁTICA

Brasília, 03 de março de 2016.

Comissão Examinadora:

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

Prof. Dr. Hemar Teixeira Godinho – MAT/UnB (Membro)

Profa. Dra. Ana Paula de Araújo Chaves – IME/UFG(Membro)

* O autor foi bolsista do CNPq durante a elaboração desta dissertação.

Agradecimentos

Primeiramente, agradeço à minha família. Em especial, agradeço aos meus pais, Ana Cirlei Kreutz e Vitor José Kreutz, que são meu grande exemplo de vida e estiveram presentes em todas as minhas conquistas. Agradeço também ao meu irmão, Rafael Alessandro Kreutz, por ser exemplo de determinação e coragem.

Agradeço aos meus avós paternos, Bruno e Julita Kreutz (em memória), pelos ensinamentos de fé e pelas bençãos que me proporcionam ao lado de Deus. Agradeço ao meu avô Wilson Portela pelo carinho que sempre demonstrou, e, em especial, agradeço a minha avó Edite Martins, motivo de orgulho para mim por sua força e que esteve presente em todos os momentos da minha vida.

Agradeço ao meu amor e amigo, meu namorado Guilherme Sabino da Silva, que sempre me apoiou em todas as minhas decisões, incentivando e acreditando que nossos sonhos são possíveis. Agradeço pelo seu amor, carinho e respeito que sempre demonstrou comigo e pelo seu bom humor que tornam meus dias mais alegres. Agradeço, também, pela sua compreensão por estarmos tão longes um do outro e por cada momento de felicidade que pudemos compartilhar juntos, todos eles foram únicos. Essa conquista não teria sido possível sem você.

Agradeço à minha melhor amiga e companheira de estudos, Gláucia Lenita Dierings, que embarcou nessa jornada do Mestrado em Brasília junto comigo. Agradeço por sua paciência nos meus dias de mau humor, pela sua amizade sincera e por todas as coisas boas e não tão boas que passamos juntas. Mais que uma amiga, lhe considero como irmã.

Agradeço ao professor Diego Marques pela oportunidade de trabalhar sob sua orientação. Agradeço por sua dedicação, paciência e competência profissional.

Agradeço a todas as pessoas que, de longe ou de perto, torceram pelo meu sucesso e me deram seu apoio. Em especial, aos novos amigos que hoje são minha família aqui em

Brasília. Agradeço, também, a todos os professores que contribuiram na minha formação desde o começo da minha vida escolar e acadêmica.

Agradeço, principalmente, a Deus, que guia meus passos e me fortalece em seu amor, preenchendo minha vida com pessoas maravilhosas.

Agradeço aos professores Diego Marques, Hemar Godinho e Ana Paula Chaves, que compuseram a banca avaliadora, pelas suas contribuições ao trabalho.

Por fim, agradeço ao CNPq, pelo apoio financeiro na realização desta pesquisa.

Resumo

Esta dissertação trata das formas lineares em logaritmos p-ádicos. Além de apresentar alguns dos resultados dados por Bugeaud, Laurent e Yu sobre as formas lineares em logaritmos p-ádicos, o trabalho visa aplicar esses resultados na resolução de algumas equações Diofantinas estudadas por Luca, Marques e Grossman.

Palavras-chave: Formas lineares em logaritmos p-ádicos. Equações Diofantinas.

Abstract

This work treats of linear form in p-adic logarithms. We shall present some results due to Bugeaud, Laurent and Yu about linear form in p-adic logarithms, moreover we shall apply these results for solving some Diophantine equations studied by Luca, Marques and Grossman.

Keywords: Linear form in p-adic logarithms, Diophantine equations.

Sumário

Introdução **1**

1 Preliminares **3**

1.1 Frações contínuas 3

1.2 Equações de Pell 14

1.3 Alguns resultados sobre valorização p-ádica 20

1.4 Um pouco de teoria algébrica dos números 23

1.4.1 Ordem de um ideal com respeito a um ideal primo 25

2 Limitantes para Formas Lineares em Logaritmos **28**

2.1 Formas lineares em logaritmos 28

2.2 Formas lineares em logaritmos p-ádicos 30

3 Aplicações das Formas Lineares em Logaritmos p-ádicos **33**

3.1 Números de Fibonacci que são rep-dígitos 33

3.2 Sequência exponencial fatorial 39

3.3 Somas de fatoriais em sequências recorrentes binárias 47

Referências Bibliográficas **63**

Introdução

A teoria de formas lineares em logaritmos p-ádicos tem uma longa história e seguiu de perto os resultados no domínio complexo. Essa teoria vem sendo aplicada para resolução de equações Diofantinas exponenciais e polinomiais e para sequências recorrentes lineares, como veremos no último capítulo deste trabalho. Além dessas aplicações, existem inúmeras outras como o problema do maior primo divisor de formas binárias ou polinomiais, a teoria do nó e a conjectura *abc*.

No ano de 1966, Baker publicou seus primeiros resultados sobre formas lineares em logaritmos de números algébricos e seus métodos impulsionaram a investigação das formas lineares em logaritmos p-ádicos de números algébricos.

Vários pesquisadores obtiveram resultados análogos aos de Baker para o caso p-ádico, entre eles Coates, van der Poorten, Dong, Yu, Bugeaud e Laurent. Neste trabalho utilizaremos as versões de formas logarítmicas p-ádicas dadas por Bugeaud e Laurent em [3] e por Yu em [20] e [21].

Nesse trabalho, definimos uma forma linear em logaritmos de números algébricos como uma expressão da forma $\Lambda = \sum_{i=1}^{n} b_i \log \alpha_i$, onde estamos considerando $\alpha_1, \ldots, \alpha_n$ números algébricos, $b_1, \ldots, b_n$ inteiros e precisaremos que a forma linear seja não nula. Além disso, também nos referimos como forma linear em logaritmos à forma exponencial de Λ, já que temos $|\Lambda| < e^{|\Lambda|} - 1$.

Os teoremas de formas lineares em logaritmos p-ádicos são utilizados para obter limitantes superiores para ordem de uma forma linear não nula $\Lambda = \alpha_1^{b_1}\alpha_2^{b_2}\cdots\alpha_n^{b_n} - 1$, onde α_i são números algébricos e b_i números inteiros, com relação a um ideal primo P, para então limitar as variáveis envolvidas na equação Diofantina inicial.

Quando utilizamos as formas lineares em logaritmos p-ádicos podemos obter, em alguns casos, uma limitação melhor do que quando utilizamos as formas lineares em loga-

ritmos dada por Baker, o que nos ajuda na hora de computar os casos finitos e verificar quais resultam em solução da equação Diofantina dada.

O objetivo da dissertação é aplicar o método de formas lineares em logaritmos p-ádicos na resolução de três distintas equações Diofantinas. O último capítulo será composto de três seções que tratam dessas equações.

O primeiro problema, estudado por Luca em [10], visa descobrir os números de Fibonacci que são rep-dígitos e para isso, utilizamos a versão das formas logarítmicas p-ádicas dada por Bugeaud e Laurent em [3].

O segundo problema também foi estudado por Luca em conjunto com Marques em [11] e trata da sequência exponencial fatorial dada por $a_1 = 1$ e $a_n = n^{a_{n-1}}$ para $n \geq 2$. Para essa sequência, queremos descobrir quando a soma de seus termos é um quadrado perfeito. Além das formas lineares em logaritmos p-ádicos, usaremos ferramentas de frações contínuas e equações de Pell na resolução do problema.

E ainda, estudaremos o problema de somas fatoriais em sequências recorrentes binárias que Grossman e Luca abordaram em [8].

Cabe ressaltar que usaremos o software *Wolfram Mathematica* como ferramenta auxiliar para o desenvolvimento do trabalho, sendo muito útil no cálculo de frações contínuas, convergentes e limitantes para as variáveis envolvidas nas equações.

Capítulo 1

Preliminares

Nesse capítulo, pretendemos introduzir os pré-requisitos básicos para o bom entendimento do trabalho, listando os principais resultados referentes a frações contínuas, equações de Pell e sequências recorrentes. Além disso, explicitaremos resultados de teoria algébrica dos números que podem ser encontrados em [1], [4] ou [15].

Ainda, serão apresentados alguns resultados sobre números p-ádicos que serão utéis quando estudarmos as formas lineares em logaritmos p-ádicos. Quando necessário, outros resultados e definições poderão ser citados ao longo do texto, para que tudo seja devidamente justificado.

1.1 Frações contínuas

De modo geral, um número real x pode ser representado por mais de uma maneira, por exemplo, $0,5$ também pode ser representado pela fração $1/2$ ou pela fração $3/6$. Nessa seção, estamos interessados em representar um número real pela sua *fração contínua* e estudar as informações que essa representação nos dá sobre o número.

Quando utilizamos a representação de um número real, em particular de um número irracional, por frações contínuas estamos obtendo boas aproximações racionais para este número real. E assim, a definição de frações contínuas torna-se uma ferramenta muito importante frente a dificuldade de se definir um número real quando comparado a definição dos números naturais, inteiros e racionais.

Assim, definimos **frações contínuas** recursivamente. Seja x um número real e consi-

dere

$$\alpha_0 = x,\ a_n = \lfloor \alpha_n \rfloor,$$

onde $\lfloor \alpha_n \rfloor$ é a parte inteira de α_n e se $\alpha_n \notin \mathbb{Z}$, tomamos $\alpha_{n+1} = \dfrac{1}{\alpha_n - a_n}$, para todo $n \in \mathbb{N}$.

Se, para algum n, $\alpha_n = a_n$ temos:

$$x = \alpha_0 = \langle a_0; a_1, a_2, \ldots, a_n \rangle = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}.$$

Caso contrário, denotamos:

$$x = \langle a_0; a_1, a_2, \ldots \rangle = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}.$$

Essa expressão é chamada de *representação por frações contínuas*. Note ainda que $x = \alpha_0 = \langle a_0; \alpha_1 \rangle = \langle a_0; a_1, \alpha_2 \rangle = \cdots = \langle a_0; a_1, \ldots, a_n, \alpha_{n+1} \rangle$.

Vejamos alguns exemplos de números reais escritos como frações contínuas.

Exemplo 1.1.

$$\frac{43}{12} = \langle 3; 1, 1, 2, 2 \rangle,$$

pois

$$\frac{43}{12} = 3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2}}}}.$$

Na prática, para obtermos a representação por frações contínuas do número acima, escrevemos $43/12 = \lfloor 43/12 \rfloor + \{43/12\}$ onde $\lfloor \cdot \rfloor$ é a parte inteira e $\{\cdot\}$ é a parte fracionária de $43/12$. Como $\{43/12\}$ é diferente de zero, consideramos o número $\frac{1}{\{43/12\}}$ e o escrevemos como sua parte inteira mais sua parte fracionária, e seguimos o processo indefinidamente ou, como no exemplo acima, até a parte fracionária ser zero.

Neste exemplo, assim como em todos os casos em que escrevemos um número *racional* por frações contínuas, sempre teremos um processo finito, pois o processo envolvido nada mais é que o algoritmo da divisão.

Exemplo 1.2. $\sqrt{2} = \langle 1; 2, 2, 2, \ldots \rangle$ *pois*

$$\begin{aligned} & 1 + \sqrt{2} = x \\ \Rightarrow \quad & \sqrt{2} = x - 1 \\ \Rightarrow \quad & 2 = (x-1)^2 = x^2 - 2x + 1 \\ \Rightarrow \quad & x^2 = 2x + 1 \\ \Rightarrow \quad & x = 2 + \frac{1}{x}. \end{aligned}$$

Daí temos:

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}.$$

Como observado acima, a representação por frações contínuas do número racional $43/12$ é finita enquanto a representação por frações contínuas do número irracional $\sqrt{2}$ é infinita. Isto não é por acaso, ainda nessa seção veremos que a representação por frações contínuas de um número real x é infinita se, e somente se, x é irracional.

É interessante observar que encontrar a representação por frações contínuas de um número real pode ser bastante trabalhoso, mas existem programas matemáticos que nos fornecem essa representação facilmente. O programa que utilizaremos nesse trabalho é o *Wolfram Mathematica* e, com o comando `ContinuedFraction[x]`, obtemos a representação por fração contínua do número x. Vejamos a utilização do comando nos exemplos acima:

Utilizando `ContinuedFraction[43/12]` obtemos $\{3, 1, 1, 2, 2\}$, e com `ContinuedFraction[Sqrt[2]]` obtemos $\{1, \{2\}\}$. Note que nesse último exemplo o número 2 aparece entre chaves indicando que irá se repetir infinitamente na representação por fração contínua de $\sqrt{2}$ (veremos adiante que chamamos essa representação de *periódica*). Para os irracionais que não fornecem fração contínua periódica é necessário especificar quantos termos da fração contínua desejamos obter, por exemplo, `ContinuedFraction[Pi,15]` nos fornece os 15 primeiros termos da fração contínua de π, que são

$$\{3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1\}.$$

Definição 1.3. *Seja* $x = \langle a_0; a_1, a_2, \ldots \rangle$ *e sejam* $p_n \in \mathbb{Z}$ *e* $q_n \in \mathbb{N}$, $q_n \neq 0$, *primos entre*

si tais que $\frac{p_n}{q_n} = \langle a_0; a_1, \ldots, a_n\rangle, n \geq 0$. *Dizemos que* $\frac{p_n}{q_n}$ *é a* ***n-ésima reduzida*** *ou* ***convergente*** *da fração contínua de* x.

Proposição 1.4. *Dada uma sequência (finita ou infinita)* $a_0, a_1, a_2, \ldots \in \mathbb{R}$ *tal que* $a_k > 0$, *para todo* $k \geq 1$, *definimos as sequências* (x_m) *e* (y_m) *por* $x_0 = a_0,\ y_0 = 1,\ x_1 = a_0a_1 + 1,\ y_1 = a_1,\ x_{m+2} = a_{m+2}x_{m+1} + x_m,\ y_{m+2} = a_{m+2}y_{m+1} + y_m$ *para todo* $m \geq 0$. *Temos então:*

$$\langle a_0; a_1, a_2, \ldots, a_n\rangle = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}} = \frac{x_n}{y_n},\ \forall\ \ n \geq 0.$$

Além disso, $x_{n+1}y_n - x_ny_{n+1} = (-1)^n$ *para todo* $n \geq 0$.

Demonstração. Faremos a prova por indução em n.

Para $n = 0$ temos

$$\langle a_0\rangle = a_0 = \frac{a_0}{1} = \frac{x_0}{y_0}.$$

Para $n = 1$ temos

$$\langle a_0; a_1\rangle = a_0 + \frac{1}{a_1} = \frac{a_0a_1 + 1}{a_1} = \frac{x_1}{y_1}.$$

E, para $n = 2$ temos

$$\begin{aligned}\langle a_0; a_1, a_2\rangle &= a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{a_2}{a_1a_2 + 1} = \frac{a_0a_1a_2 + a_0 + a_2}{a_1a_2 + 1}\\ &= \frac{a_2(a_0a_1 + 1) + a_0}{a_2a_1 + 1} = \frac{a_2x_1 + x_0}{a_2y_1 + y_0} = \frac{x_2}{y_2}.\end{aligned}$$

Suponha que a afirmação seja válida para n, vamos mostrar que a afirmação também é válida para $n + 1$:

$$\begin{aligned}\langle a_0; a_1, \ldots, a_n, a_{n+1}\rangle &= \langle a_0; a_1, \ldots, a_n + {}^1\!/_{a_{n+1}}\rangle\\ &= \frac{(a_n + \frac{1}{a_{n+1}})x_{n-1} + x_{n-2}}{(a_n + \frac{1}{a_{n+1}})y_{n-1} + y_{n-2}}\\ &= \frac{a_{n+1}(a_nx_{n-1} + x_{n-2}) + x_{n-1}}{a_{n+1}(a_ny_{n-1} + y_{n-2}) + y_{n-1}}\\ &= \frac{a_{n+1}x_n + x_{n-1}}{a_{n+1}y_n + y_{n-1}} = \frac{x_{n+1}}{y_{n+1}}.\end{aligned}$$

Agora, resta provar que $x_{n+1}y_n - x_ny_{n+1} = (-1)^n$ para todo $n \geq 0$, e faremos isso usando, novamente, indução em n.

Para $n = 0$ temos $x_1y_0 - x_0y_1 = (a_0a_1 + 1)1 - a_0a_1 = 1 = (-1)^0$.

Agora, supondo verdadeiro para n, temos:

$$\begin{aligned} x_{n+2}y_{n+1} - x_{n+1}y_{n+2} &= (a_{n+2}x_{n+1} + x_n)y_{n+1} - (a_{n+2}y_{n+1} + y_n)x_{n+1} \\ &= -(x_{n+1}y_n - x_ny_{n+1}) = -(-1)^n = (-1)^{n+1}. \end{aligned}$$

Ou seja, a afirmação também é válida para $n + 1$, o que demonstra a proposição. □

Corolário 1.5. *As sequências (p_n) e (q_n), onde $\left(\frac{p_n}{q_n}\right)$ é a sequência dos convergentes da fração contínua de $x = \langle a_0; a_1, a_2, \ldots\rangle$, satisfazem as recorrências:*

$$p_{n+2} = a_{n+2}p_{n+1} + p_n \text{ e } q_{n+2} = a_{n+2}q_{n+1} + q_n$$

para todo $n \geq 0$, com $p_0 = a_0,\ p_1 = a_0a_1 + 1,\ q_0 = 1$ e $q_1 = a_1$.

Observação 1.6. *Frequentemente, é útil considerarmos a sequência acima com os valores iniciais $p_{-1} = 1$ e $q_{-1} = 0$.*

Observe que, mesmo com o corolário anterior, encontrar os convergentes da fração contínua de um número real x pode ser trabalhoso, por isso, a utilização do comando `Convergents[x,a]` no programa *Mathematica* é muito conveniente. Vejamos alguns exemplos:

Exemplo 1.7. *Encontrar os 10 primeiros convergentes da fração contínua de π.*

`Convergents[Pi,10]` *fornece*

$$\frac{p_n}{q_n} \in \left\{3, \frac{22}{7}, \frac{333}{106}, \frac{355}{113}, \frac{103993}{33102}, \frac{104348}{33215}, \frac{208341}{66317}, \frac{312689}{99532}, \frac{833719}{265381}, \frac{1146408}{364913}\right\}.$$

Exemplo 1.8. *Encontrar os 5 primeiros convergentes da fração contínua de $\sqrt{2}$.*

`Convergents[Sqrt[2],5]` *fornece*

$$\frac{p_n}{q_n} \in \left\{1, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}\right\}.$$

Nesses exemplos, já podemos observar que os convergentes da fração contínua são boas aproximações racionais para o número real dado. Cabe ressaltar que sempre que nos referirmos aos *convergentes de x* estamos tratando dos convergentes da representação por frações contínuas do número real x.

Corolário 1.9. *Valem as seguintes propriedades:*

(i) $p_{n+1}q_n - p_nq_{n+1} = (-1)^n,\ \forall\ \ n \geq 0$;

(ii) $p_{n+2}q_n - p_nq_{n+2} = (-1)^n a_{n+2},\ \forall\ \ n \geq 0$

Corolário 1.10. *Para todo $n \in \mathbb{N}$ temos:*

$$x = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}.$$

Demonstração. Note que $x = \langle a_0; a_1, \ldots, a_{n-1}, \alpha_n\rangle$, onde $x = \alpha_0$, $a_n = \lfloor \alpha_n \rfloor$ e $\alpha_{n+1} = \frac{1}{\alpha_n - a_n}$. Pela Proposição 1.4, temos que

$$x = \langle a_0; a_1, \ldots, a_{n-1}, \alpha_n\rangle = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}.$$

□

Proposição 1.11. *Temos, para todo $k \geq 0$,*

$$\frac{p_{2k}}{q_{2k}} < \frac{p_{2k+2}}{q_{2k+2}} < x < \frac{p_{2k+3}}{q_{2k+3}} < \frac{p_{2k+1}}{q_{2k+1}}.$$

Demonstração. Para $n \geq 0$ temos

$$\begin{aligned}\frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n} &= \frac{a_{n+2}p_{n+1} + p_n}{a_{n+2}q_{n+1} + q_n} - \frac{p_n}{q_n} \\ &= \frac{a_{n+2}(p_{n+1}q_n - p_nq_{n+1})}{q_n(a_{n+2}q_{n+1} + q_n)} = \frac{(-1)^n a_{n+2}}{q_{n+2}q_n}\end{aligned}$$

é positivo para n par e negativo para n ímpar.

Daí temos $\frac{p_{2k}}{q_{2k}} < \frac{p_{2k+2}}{q_{2k+2}}$ e $\frac{p_{2k+3}}{q_{2k+3}} < \frac{p_{2k+1}}{q_{2k+1}}$.

Além disso, como $x = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}}$, temos que

$$\begin{aligned}x - \frac{p_n}{q_n} &= \frac{\alpha_{n+1}p_nq_n + p_{n-1}q_n - \alpha_{n+1}q_np_n - q_{n-1}p_n}{(\alpha_{n+1}q_n + q_{n-1})q_n} \\ &= \frac{p_{n-1}q_n - q_{n-1}p_n}{(\alpha_{n+1}q_n + q_{n-1})q_n} \\ &= \frac{-(p_nq_{n-1} - p_{n-1}q_n)}{(\alpha_{n+1}q_n + q_{n-1})q_n} \\ &= \frac{-(-1)^{n-1}}{(\alpha_{n+1}q_n + q_{n-1})q_n} \\ &= \frac{(-1)^n}{(\alpha_{n+1}q_n + q_{n-1})q_n}\end{aligned}$$

é positivo para n par e negativo para n ímpar. Logo, temos o resultado. □

A proposição anterior nos permite concluir que, em particular, temos:

(i) A sequência $\left(\frac{p_{2k+1}}{q_{2k+1}}\right)$ é decrescente e limitada;

(ii) A sequência $\left(\frac{p_{2k}}{q_{2k}}\right)$ é crescente e limitada;

(iii) A sequência $\frac{p_{2k}}{q_{2k}} - \frac{p_{2k+1}}{q_{2k+1}}$ tende a zero.

Os próximos resultados nos permitem concluir que os convergentes da fração contínua de x são "boas aproximações"para x, além disso, a recíproca também é verdadeira, ou seja, "boas aproximações"para x são convergentes da fração contínua de x. Assim, podemos definir $x = \langle a_0; a_1, \ldots \rangle = \lim_{n\to\infty} \frac{p_n}{q_n}$.

Proposição 1.12. *(i) Sejam α um irracional e $\frac{p_k}{q_k}$ os convergentes da fração contínua de α para $k \geq 0$. Se $r, s \in \mathbb{Z}$ com $s > 0$ e k um inteiro positivo tal que*

$$|s\alpha - r| < |q_k\alpha - p_k|$$

então $s \geq q_{k+1}$.

(ii) Se α é um irracional e $\frac{r}{s}$ um número racional com $s > 0$ tal que

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s^2}$$

então $\frac{r}{s}$ é um convergente de α.

Demonstração. (i) Suponha por absurdo que $1 \leq s < q_{k+1}$ e considere o sistema de equações:

$$p_k x + p_{k+1} y = r$$

$$q_k x + q_{k+1} y = s.$$

Temos então, pelo Corolário 1.9,

$$(p_{k+1}q_k - p_k q_{k+1})x = sp_{k+1} - rq_{k+1} \quad \text{e} \quad (p_k q_{k+1} - p_{k+1}q_k)y = sp_k - rq_k,$$

o que nos dá:

$$x = (-1)^k(sp_{k+1} - rq_{k+1}) \quad \text{e} \quad y = (-1)^k(sp_k - rq_k).$$

Vamos provar que x e y são diferentes de zero e com sinais contrários. Se $x = 0$, ${}^{r}/_{s} = {}^{p_{k+1}}/_{q_{k+1}}$ e como p_{k+1} e q_{k+1} são coprimos temos que $q_{k+1}|s$, absurdo pois estamos supondo $1 \leq s < q_{k+1}$. Se $y = 0$, olhando para o sistema de equações temos que $r = p_k x$ e $s = q_k x$, portanto

$$|s\alpha - r| = |x||q_k\alpha - p_k| \geq |q_k\alpha - p_k|,$$

que contradiz a nossa hipótese. Portanto $xy \neq 0$.

Suponha agora que $y < 0$, como $q_k x = s - q_{k+1}y$ temos que $x > 0$. Se $y > 0$ temos $q_{k+1}y \geq q_{k+1} > s$ e portanto $q_k x = s - q_{k+1}y < 0$ implica que $x < 0$. Já sabemos que

$$\frac{p_k}{q_k} < \alpha < \frac{p_{k+1}}{q_{k+1}} \text{ se } k \equiv 0(\text{mod } 2)$$

e

$$\frac{p_{k+1}}{q_{k+1}} < \alpha < \frac{p_k}{q_k} \text{ se } k \equiv 1(\text{mod } 2).$$

Em ambos os casos, $q_k\alpha - p_k$ e $q_{k+1}\alpha - p_{k+1}$ tem sinais opostos e portanto $x(q_k\alpha - p_k)$ e $y(q_{k+1}\alpha - p_{k+1})$ tem o mesmo sinal. Assim:

$$\begin{aligned} |s\alpha - r| &= |(q_k x + q_{k+1}y)\alpha - (p_k x + p_{k+1}y)| \\ &= |x(q_k\alpha - p_k) + y(q_{k+1}\alpha - p_{k+1})| \\ &= |x||q_k\alpha - p_k| + |y||q_{k+1}\alpha - p_{k+1}| \\ &> |x||q_k\alpha - p_k| \geq |q_k\alpha - p_k| \end{aligned}$$

o que é uma contradição. Logo, $s \geq q_{k+1}$.

(ii) Suponha que ${}^{r}/_{s}$ não é um convergente da fração contínua de α, ou seja, ${}^{r}/_{s} \neq {}^{p_k}/_{q_k}$ para todo k. Seja k o maior inteiro não negativo tal que $s \geq q_k$. Como $q_0 = 1$ e (q_k) é crescente, temos que esse inteiro existe. E como $q_k \leq s < q_{k+1}$ implica que

$$|q_k\alpha - p_k| \leq |s\alpha - r| = s\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s}$$

temos

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{2sq_k}.$$

Como $r/s \neq p_k/q_k$, temos $|sp_k - rq_k| \geq 1$ e portanto

$$\frac{1}{sq_k} \leq \frac{|sp_k - rq_k|}{sq_k} = \left|\frac{p_k}{q_k} - \frac{r}{s}\right| \leq \left|\frac{p_k}{q_k} - \alpha\right| + \left|\alpha - \frac{r}{s}\right| < \frac{1}{2sq_k} + \frac{1}{2s^2}$$

o que implica que $\frac{1}{2sq_k} < \frac{1}{2s^2} \Rightarrow q_k > s$, contradição. Logo $\frac{r}{s}$ é convergente da fração contínua de α.

□

Teorema 1.13. *Temos, para todo $n \in \mathbb{N}$,*

$$\left|x - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}.$$

Além disso,

$$\left|x - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2} \ \ ou \ \ \left|x - \frac{p_{n+1}}{q_{n+1}}\right| < \frac{1}{2q_{n+1}^2}.$$

Teorema 1.14 (Hurwitz, Markov)**.** *Para todo α irracional e todo inteiro $n \geq 1$, temos*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}$$

para pelo menos um racional

$$\frac{p}{q} \in \left\{\frac{p_{n-1}}{q_{n-1}}, \frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}\right\}.$$

Em particular, a desigualdade acima tem infinitas soluções racionais $\frac{p}{q}$.

As demonstrações desses últimos resultados podem ser encontradas em [14].

O próximo resultado, devido a Worley [18], nos diz que sob certas condições, podemos obter aproximações para um irracional α que são combinações lineares de convergentes da fração contínua de α.

Teorema 1.15. *Seja α um número irracional e sejam p e q inteiros coprimos satisfazendo a desigualdade*

$$\left|\alpha - \frac{p}{q}\right| < \frac{k}{q^2},$$

onde k é um número real positivo. Então

$$(p, q) = (rp_n \pm sp_{n-1}, rq_n \pm sq_{n-1}),$$

para alguns inteiros não negativos n, r e s tais que $rs < 2k$.

Mais detalhes do Teorema 1.15 podem ser encontrados em [5], [6] e [18].

Observação 1.16. *Do resultado anterior e como $q_0 = 1$ e (q_n) é uma sequência crescente, temos que sempre podemos escolher n o maior índice tal que $q \geq q_n$.*

Agora, mostraremos que se a representação por frações contínuas de x é infinita então x é irracional e a recíproca também é verdadeira.

Teorema 1.17. *O número real x tem representação por frações contínuas infinita se, e somente se, x é irracional.*

Demonstração. ($\Rightarrow$) Seja $x = \langle a_0; a_1, \ldots \rangle$ e suponha, por absurdo, que $x = \frac{p}{q}$, onde p e q são inteiros. Sabemos que

$$\frac{p_{2k}}{q_{2k}} < x < \frac{p_{2k+1}}{q_{2k+1}}.$$

Assim,

$$0 < x - \frac{p_{2k}}{q_{2k}} < \frac{p_{2k+1}}{q_{2k+1}} - \frac{p_{2k}}{q_{2k}}$$

implica que

$$0 < \frac{p}{q} - \frac{p_{2k}}{q_{2k}} < \frac{p_{2k+1}q_{2k} - p_{2k}q_{2k+1}}{q_{2k+1}q_{2k}}.$$

E como $p_{2k+1}q_{2k} - p_{2k}q_{2k+1} = (-1)^{2k}$ temos

$$0 < \frac{pq_{2k} - p_{2k}q}{qq_{2k}} < \frac{(-1)^{2k}}{q_{2k+1}q_{2k}}.$$

Logo,

$$0 < pq_{2k} - p_{2k}q < \frac{q}{q_{2k+1}}.$$

Note que como q é fixo e q_{2k+1} cresce à medida que crescemos o k, temos que para k suficientemente grande $\frac{q}{q_{2k+1}} < 1$ e daí obtemos um absurdo já que $pq_{2k} - p_{2k}q$ seria um inteiro entre 0 e 1. Logo x é irracional.

($\Leftarrow$) É imediato da definição de fração contínua, já que escrevemos $\alpha_{n+1} = \frac{1}{\alpha_n - \lfloor \alpha_n \rfloor}$, $\alpha_n \notin \mathbb{Z}$ para x irracional e $x = \langle a_0; a_1, \ldots, a_n, \alpha_{n+1} \rangle$. □

Veremos que para resolução das equações de Pell $x^2 - dy^2 = N$, onde d é um inteiro positivo que não é um quadrado perfeito, necessitamos encontrar a fração contínua do irracional $\sqrt{d}$. Esse irracional $\sqrt{d}$ é chamado de irracional quadrático pois é raiz da equação $x^2 - d = 0$ e possui propriedades interessantes e úteis quando olhamos sua

representação por frações contínuas. Assim, vejamos agora alguns desses resultados para irracionais quadráticos.

Definição 1.18. *Dizemos que $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ é um* ***irracional quadrático*** *se α é raiz de uma equação da forma $Ax^2 + Bx + C = 0$ com $A, B, C \in \mathbb{Z}$ e $A \neq 0$.*

Assim, podemos escrever $\alpha = \dfrac{a + b\sqrt{e}}{f}$ onde a, b, e, f são inteiros e $e > 0$ não é um quadrado perfeito. Note que

$$\alpha = \frac{af + \sqrt{eb^2f^2}}{f^2} = \frac{P_0 + \sqrt{d}}{Q_0},$$

com $P_0 = af, Q_0 = f^2$ e $d = eb^2f^2$ inteiros, d não é quadrado perfeito e ainda, $Q_0 \mid d - P_0^2$.

Definimos recursivamente, para $k = 0, 1, \ldots$:

$$\alpha_k = \frac{P_k + \sqrt{d}}{Q_k}$$

$$a_k = \lfloor \alpha_k \rfloor$$

$$P_{k+1} = a_kQ_k - P_k$$

$$Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k},$$

e temos que a fração contínua $\langle a_0; a_1, \ldots \rangle$ assim definida é a fração contínua de α.

De fato, seja $k \geq 0$ e assuma que P_k e Q_k são inteiros com $Q_k \mid d - P_k^2$. Então, $P_{k+1} = a_kQ_k - P_k$ é um inteiro e $d - P_{k+1}^2 = (d - P_k^2) + Q_k(2a_kP_k - a_k^2Q_k)$ é divisível por Q_k. Portanto $Q_{k+1} = (d - P_{k+1}^2)/Q_k$ é um inteiro que satisfaz $Q_{k+1} \mid d - P_{k+1}^2$.

Como d não é um quadrado perfeito, temos que as sequências (P_k) e (Q_k) estão bem definidas.

Temos ainda

$$\begin{aligned}
\alpha_k - a_k &= \frac{P_k + \sqrt{d}}{Q_k} - a_k = \frac{\sqrt{d} - (a_kQ_k - P_k)}{Q_k} \\
&= \frac{\sqrt{d} - P_{k+1}}{Q_k} = \frac{d - P_{k+1}^2}{Q_k(\sqrt{d} + P_{k+1})} \\
&= \frac{Q_kQ_{k+1}}{Q_k(\sqrt{d} + P_{k+1})} = \frac{Q_{k+1}}{\sqrt{d} + P_{k+1}} = \frac{1}{\alpha_{k+1}}.
\end{aligned}$$

Em particular, $\alpha_{k+1} > 0$ e $\alpha_k = \langle a_k, \alpha_{k+1} \rangle$. E, portanto, para $k = 0, 1, \ldots$ temos $\alpha = \langle a_0; a_1, \ldots \rangle$.

Definição 1.19. *A fração contínua* $\langle a_0; a_1, a_2, \ldots\rangle$ *é dita* ***periódica*** *se existem* h *e* n *tal que* $a_m = a_{m+h}$ *para todo* $m \geq n$*. Se* h *é o menor número com essa propriedade, escrevemos:*

$$\langle a_0; a_1, \ldots\rangle = \langle a_0; a_1, \ldots, a_{n-1}, \overline{a_n, a_{n+1}, \ldots, a_{n+h-1}}\rangle.$$

E a fração contínua é dita ***puramente periódica*** *se* $a_m = a_{m+h}$ *para todo* $m \geq 0$*.*

Exemplo 1.20. $\sqrt{6} = \langle 2; 2, 4, 2, 4, \ldots\rangle = \langle 2, \overline{2, 4}\rangle$ *é periódica de período* $h = 2$ *e*

$$\frac{1+\sqrt{5}}{2} = \langle 1; 1, 1, \ldots\rangle = \langle \overline{1}\rangle$$

é puramente periódica de período $h = 1$*.*

Proposição 1.21. *Um irracional* α *é quadrático se, e somente se, sua fração contínua é periódica.*

Proposição 1.22. *Seja* $d > 0$ *um inteiro que não é um quadrado perfeito então*

$$\sqrt{d} = \langle a_0; \overline{a_1, a_2, a_3 \ldots, a_2, a_1, 2a_0}\rangle.$$

As demonstrações desses resultados podem ser encontradas em [10].

1.2 Equações de Pell

As equações de Pell são equações em inteiros (x, y) da forma

$$x^2 - dy^2 = N,$$

onde $d > 1$ não é um quadrado perfeito e $N \neq 0$. Note que se (x, y) é solução então $(\pm x, \pm y)$ também é solução da equação e portanto podemos considerar x e y inteiros positivos.

Observação 1.23. *Note que a equação* $x^2 - dy^2 = N$ *quando* d *é um quadrado perfeito pode ser resolvida facilmente pelo método da fatoração para cada* N *dado. E, se* d *é negativo podemos usar o método das desigualdades para resolvê-la. Por isso, é interessante considerarmos o caso em que* $d > 1$ *não é um quadrado perfeito.*

Quando $N \geq 1$, podemos fatorar $x^2 - dy^2 = N$ em fatores positivos, da seguinte forma:

$$\begin{aligned} & (x - \sqrt{d}y)(x + \sqrt{d}y) = N \\ \Rightarrow \quad & (x - \sqrt{d}y)(x + \sqrt{d}y - \sqrt{d}y + \sqrt{d}y) = N \\ \Rightarrow \quad & (x - y\sqrt{d})^2 + (x - y\sqrt{d})(2y\sqrt{d}) = N. \end{aligned}$$

Note que

$$x - \sqrt{d}y > 0 \Rightarrow \frac{x}{y} - \sqrt{d} > 0$$

e como

$$(x - y\sqrt{d})(2y\sqrt{d}) = N - (x - y\sqrt{d})^2$$

temos

$$(x - y\sqrt{d})(2y\sqrt{d}) < N \Rightarrow \frac{x}{y} - \sqrt{d} < \frac{N}{2y^2\sqrt{d}}.$$

Daí:

$$0 < \frac{x}{y} - \sqrt{d} < \frac{N}{2y^2\sqrt{d}}.$$

Quando temos $N < 0$ podemos reescrever a equação de Pell como

$$y^2 - \frac{x^2}{d} = -\frac{N}{d},$$

onde o lado direito é positivo e temos:

$$\left(y - \frac{x}{\sqrt{d}}\right)^2 + \left(y - \frac{x}{\sqrt{d}}\right)\left(\frac{2x}{\sqrt{d}}\right) = -\frac{N}{d}.$$

E ainda,

$$0 < \frac{y}{x} - \frac{1}{\sqrt{d}} < -\frac{N}{2x^2\sqrt{d}}.$$

Em ambos os casos, pela Proposição 1.12, quando $0 < |N| < \sqrt{d}$ temos que x/y é um convergente de $\sqrt{d}$ se $N > 0$ e que y/x é um convergente de $1/\sqrt{d} = \langle 0; \sqrt{d} \rangle$ se $N < 0$, o que é equivalente a x/y ser um convergente de $\sqrt{d}$. Portanto, temos o seguinte resultado:

Teorema 1.24. *Se $0 < |N| < \sqrt{d}$ então todas as soluções em inteiros positivos (x, y) de $x^2 - dy^2 = N$ são tais que x/y é um convergente de $\sqrt{d}$.*

Proposição 1.25. *Se $d > 1$ é um inteiro que não é um quadrado e $\alpha = \alpha_0 = \sqrt{d}$ então $p_{k-1}^2 - dq_{k-1}^2 = (-1)^k Q_k$.*

Demonstração. Como definido anteriormente, $\alpha = \frac{P_0+\sqrt{d}}{Q_0} = \sqrt{d}$ implica que $P_0 = 0$ e $Q_0 = 1$. Além disso, $P_{k+1} = \lfloor\sqrt{d}\rfloor Q_k - P_k$ e $Q_{k+1} = \frac{d-P_{k+1}^2}{Q_k}$ implicam que $P_1 = \lfloor\sqrt{d}\rfloor$ e $Q_1 = d - P_1^2 = d - \lfloor\sqrt{d}\rfloor^2$.

Assim, para $k = 1$, como $p_0 = \lfloor\sqrt{d}\rfloor$ e $q_0 = 1$, temos $p_0^2 - dq_0^2 = \lfloor\sqrt{d}\rfloor^2 - d = -Q_1$.

Agora, vamos considerar $k \geq 2$. Podemos escrever

$$\alpha = \sqrt{d} = \langle a_0; a_1, \ldots, a_{k-1}, \alpha_k\rangle = \frac{\alpha_k p_{k-1} + p_{k-2}}{\alpha_k q_{k-1} + q_{k-2}}.$$

Como $\alpha_k = \dfrac{P_k + \sqrt{d}}{Q_k}$ temos

$$\sqrt{d} = \frac{(P_k + \sqrt{d})p_{k-1} + Q_k p_{k-2}}{(P_k + \sqrt{d})q_{k-1} + Q_k q_{k-2}},$$

o que nos dá

$$dq_{k-1} + \sqrt{d}(P_k q_{k-1} + Q_k q_{k-2}) = P_k p_{k-1} + Q_k p_{k-2} + \sqrt{d}p_{k-1}.$$

Portanto,

$$\begin{aligned} dq_{k-1} &= P_k p_{k-1} + Q_k p_{k-2} \\ p_{k-1} &= P_k q_{k-1} + Q_k q_{k-2}. \end{aligned}$$

Assim, temos que

$$\begin{aligned} p_{k-1}^2 - dq_{k-1}^2 &= (P_k q_{k-1} + Q_k q_{k-2})p_{k-1} - (P_k p_{k-1} + Q_k p_{k-2})q_{k-1} \\ &= Q_k q_{k-2} p_{k-1} - Q_k p_{k-2} q_{k-1} \\ &= Q_k(q_{k-2}p_{k-1} - p_{k-2}q_{k-1}) \\ &= Q_k(-1)^k. \end{aligned}$$

□

Com o resultado seguinte, vamos classificar todas as soluções da equação de Pell quando $N = \pm 1$.

Proposição 1.26. *Seja h o período da fração contínua de $\sqrt{d}$. Então $Q_k = 1$ se, e somente se, $h \mid k$.*

Demonstração. Como h é o período da fração contínua de $\sqrt{d}$ temos que $\alpha_1 = \alpha_{h+1}$ e $\alpha_0, \alpha_1, \ldots, \alpha_{h-1}$ são distintos. Então:

$$\alpha_h = 2a_0 + \frac{1}{\alpha_{h+1}} = 2a_0 + \frac{1}{\alpha_1} = 2a_0 + (\sqrt{d} - a_0) = \sqrt{d} + a_0.$$

Mas $\alpha_h = \frac{P_h + \sqrt{d}}{Q_h}$. Se $Q_h > 1$, então $P_h - a_0 Q_h = (Q_h - 1)\sqrt{d} \notin \mathbb{Q}$, o que é impossível. Então $Q_h = 1$ e o mesmo argumento mostra que $Q_k = 1$ para todos os múltiplos k de h.

Suponha que $Q_k = 1$. Então $\alpha_k = P_k + \sqrt{d}$. Como α_k é puramente periódico (e portanto *reduzido*, ver [10]), $\alpha_k' \in (-1, 0)$, onde α_k' é o conjugado de α_k sobre $\mathbb{Q}[\sqrt{d}]$. Portanto $P_k - \sqrt{d} \in (-1, 0)$. Logo, $P_k = \lfloor \sqrt{d} \rfloor = a_0$. Então $\alpha_k = \alpha_h$ o que implica que k é múltiplo de h. □

Corolário 1.27. *A equação $x^2 - dy^2 = 1$ tem infinitas soluções inteiras (x, y). A equação $x^2 - dy^2 = -1$ tem uma solução inteira (x, y) (e então infinitas) se, e somente se, o período h da fração contínua de $\sqrt{d}$ é ímpar.*

Teorema 1.28. *Seja h o período da fração contínua de $\sqrt{d}$. Então todas as soluções inteiras e positivas (x, y) da equação $x^2 - dy^2 = \pm 1$ são dadas por*

$$x + y\sqrt{d} = (x_1 + y_1\sqrt{d})^l \ \forall \ \ l \geq 1,$$

onde $x_1 + y_1\sqrt{d} = p_{h-1} + q_{h-1}\sqrt{d}$.

Observação 1.29. *A solução minimal em inteiros positivos (x_1, y_1) da equação de Pell $x^2 - dy^2 = \pm 1$ satisfaz $x_1 + \sqrt{d}y_1 < e^{3\sqrt{d}\log d}$ (veja em [9]).*

Outra maneira de analisarmos as soluções da equação de Pell $x^2 - dy^2 = \pm 1$ é observando que toda solução positiva dessa equação pertence a um conjunto finito de sequências binárias recorrentes.

Para isso, vamos primeiramente definir sequência recorrente e sequência recorrente binária, destacando alguns resultados importantes.

Definição 1.30. *Seja $k \geq 1$ um inteiro. Uma sequência $(u_n)_{n \geq 0} \subset \mathbb{C}$ é chamada de* ***linearmente recorrente de ordem*** *k se a recorrência*

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \cdots + a_k u_n$$

vale para todo $n \geq 0$ com alguns coeficientes fixos $a_1, \ldots, a_k \in \mathbb{C}$, $a_k \neq 0$ e onde os k primeiros termos $u_0, u_1, \ldots, u_{k-1}$ são dados.

Se $a_1, \ldots, a_k \in \mathbb{Z}$ e $u_0, \ldots, u_{k-1} \in \mathbb{Z}$, então, por indução em n, temos que u_n é um inteiro para todo $n \geq 0$. O polinômio

$$f(X) = X^k - a_1 X^{k-1} - \cdots - a_k \in \mathbb{C}[X]$$

é chamado de **polinômio característico** de $(u_n)_{n\geq 0}$. Suponha que

$$f(X) = \prod_{i=1}^{s} (X - \alpha_i)^{\sigma_i}$$

onde $\alpha_1, \ldots, \alpha_s$ são raízes distintas de $f(X)$ com multiplicidades $\sigma_1, \ldots, \sigma_s$, respectivamente.

Proposição 1.31. *Suponha que $f(X) \in \mathbb{Z}[X]$ tem raízes distintas, todas com multiplicidade 1. Então existem constantes $c_1, \ldots, c_k \in \mathbb{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ tal que*

$$u_n = \sum_{i=1}^{k} c_i \alpha_i^n$$

vale para todo $n \geq 0$.

Para mais detalhes da proposição acima veja [14].

Definição 1.32. *Se $k = 2$, dizemos que $(u_n)_{n\geq 0}$ é uma **sequência recorrente binária**. Nesse caso, o polinômio característico é da forma*

$$f(X) = X^2 - a_1 X - a_2 = (X - \alpha_1)(X - \alpha_2).$$

Suponha que as raizes α_1 e α_2 sejam distintas, então temos que $u_n = c_1\alpha_1^n + c_2\alpha_2^n$ para todo $n \geq 0$. Se $c_1 c_2 \alpha_1 \alpha_2 \neq 0$ e α_1/α_2 não é uma raiz da unidade, dizemos que a sequência recorrente binária é não degenerada.

Exemplo 1.33. *Um exemplo muito conhecido de sequência recorrente binária é a sequência de Fibonacci dada por $F_0 = 0$, $F_1 = 1$ e $F_{n+2} = F_{n+1} + F_n$ para todo $n \geq 0$. A essa sequência temos associado o polinômio característico $F(X) = X^2 - X - 1$ e a conhecida fórmula de Binet dada por*

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},$$

onde $\alpha = \frac{1+\sqrt{5}}{2}$ e $\beta = \frac{1-\sqrt{5}}{2}$ são as raízes do polinômio característico.

Note ainda que $\beta = -\alpha^{-1}$ *e* $\alpha - \beta = \sqrt{5}$ *assim, podemos reescrever a fórmula de Binet como*

$$F_n = \frac{\alpha^n - (-1)^n \alpha^{-n}}{\sqrt{5}}.$$

Assim, podemos analisar as soluções da equação de Pell como pertencente a um conjunto de sequências binárias através do seguinte teorema.

Teorema 1.34. *Seja* $d > 1$ *um inteiro que não é um quadrado perfeito e seja* $N \neq 0$. *Então toda solução em inteiros positivos* (u, v) *da equação* $u^2 - dv^2 = N$ *pertence a um conjunto de sequências binárias recorrentes. Essas sequências tem a mesma equação característica* $X^2 - 2x_1X + 1$, *onde* (x_1, y_1) *é a solução minimal em inteiros positivos de* $x^2 - dy^2 = 1$.

Demonstração. Primeiramente, note que se existe uma solução (u_0, v_0) de $u^2 - dv^2 = N$ então temos infinitas soluções. De fato, considere (x_1, y_1) solução minimal de $x^2 - dy^2 = 1$, $\zeta = x_1 + \sqrt{d}y_1$ e $\eta = x_1 - \sqrt{d}y_1$. Fazendo

$$u_l + \sqrt{d}v_l = (u_0 + \sqrt{d}v_0)\zeta^l$$

e conjugando, obtemos

$$u_l - \sqrt{d}v_l = (u_0 - \sqrt{d}v_0)\eta^l.$$

Multiplicando essas igualdades obtemos

$$u_l^2 - dv_l^2 = (u_0^2 - dv_0^2)(\zeta\eta)^l = N$$

ou seja, (u_l, v_l) é também solução da equação de Pell.

Observe que

$$u_l = \frac{c_1\zeta^l + c_2\eta^l}{2} \quad \text{e} \quad v_l = \frac{c_1\zeta^l - c_2\eta^l}{2\sqrt{d}}$$

onde $c_1 = u_0 + \sqrt{d}v_0$ e $c_2 = u_0 - \sqrt{d}v_0$. As sequências $(u_l)_{l\geq 0}$ e $(v_l)_{l\geq 0}$ são recorrências binárias e ambas com equação caracterítica dada por

$$f(X) = (X - \zeta)(X - \eta) = X^2 - (\zeta + \eta)X + \zeta\eta = X^2 - 2x_1X + 1.$$

Agora, vamos mostrar que toda solução inteira positiva (u, v) é obtida como descrita acima de alguma solução minimal (u_0, v_0). Seja (u, v) solução inteira positiva de $u^2 - dv^2 =$

N. Se $u+\sqrt{d}v \leq |N|\zeta$, então existem somente finitas possibilidades para (u,v). Suponha agora que $u+\sqrt{d}v \geq |N|\zeta$ e seja $l \geq 1$ o menor inteiro positivo tal que $(u+\sqrt{d}v)\zeta^{-l} \leq N\zeta$. Escrevemos

$$\begin{aligned} u_0+\sqrt{d}v_0 &= (u+\sqrt{d}v)\zeta^{-l} \\ &= ((u+\sqrt{d}v)(x_l-\sqrt{d}y_l) \\ &= (ux_l-dvy_l)+\sqrt{d}(-uy_l+vx_l). \end{aligned}$$

Como u e v são positivos, pela definição de l, temos que $u_0+v_0\sqrt{d} > |N|$, pois caso contrário teríamos $0 < u_0+v_0\sqrt{d} < |N|$, o que implica que

$$(u+\sqrt{d}v)\zeta^{-(l-1)} < (u_0+\sqrt{d}v_0)\zeta < |N|\zeta,$$

mas isso contradiz a escolha de l.

Vamos provar agora que u_0 e v_0 são positivos. É claro que pelo menos um deles é positivo. Desde que $u_0^2-dv_0^2 = N$ temos que $|u_0-\sqrt{d}v_0| = {}^{|N|}/_{(u_0+\sqrt{d}v_0)} < 1$. Se u_0 e v_0 tem sinais contrários, então $1 > |u_0-\sqrt{d}v_0| = |u_0|+\sqrt{d}|v_0|$, o que não é possível. Isso mostra que para toda solução inteira positiva (u,v) existe algum inteiro l não negativo e alguma solução inteira positiva (u_0,v_0) com $u_0+\sqrt{d}v_0 < |N|\zeta$ e tal que $u+\sqrt{d}v < (u_0+\sqrt{d}v_0)\zeta^l$, e portanto, (u,v) pertence a uma união finita de recorrências binárias. □

1.3 Alguns resultados sobre valorização p-ádica

O objetivo dessa seção é tratar de algumas definições e resultados sobre números p-ádicos, a fim de definirmos a valorização p-ádica de um número x que denotaremos por $\nu_p(x)$. Além disso, estenderemos essa definição para valorização ou ordem de um ideal A com respeito a um ideal primo P, denotado por $\mathrm{ord}_P(A)$, que apresentaremos com mais detalhes na próxima seção.

Definição 1.35. *Seja $\mathbb{K}$ um corpo. Um **valor absoluto** $\|\cdot\|$ é uma função de $\mathbb{K}$ para $\mathbb{R}$ que satisfaz:*

(i) $\|x\| \geq 0$ *para todo* $x \in \mathbb{K}$ *e* $\|x\| = 0$ *se, e somente se,* $x = 0$*;*

(ii) $\|xy\| = \|x\|\|y\|$ *para todo* $x, y \in \mathbb{K}$*;*

(iii) Existe $a > 0$ tal que para todo $x, y \in \mathbb{K}$ temos $\|x+y\|^a \leq \|x\|^a + \|y\|^a$.

Se $\mathbb{K} = \mathbb{Q}$ e p é um número primo definimos o valor absoluto, chamado de **valor absoluto p-ádico**, de $\mathbb{Q}$ para $\mathbb{R}$ por: $|0|_p = 0$ e $|x|_p = p^{-\nu_p(x)}$. Onde $\nu_p(x)$ é o expoente de p na decomposição de x em um produto de potências de primos.

Como $\nu_p(x)$ é o expoente de p na decomposição de x em um produto de potências de primos, temos que $\nu_p(x) = m$ se p^m divide x, mas p^{m+1} não divide x. Para qualquer número racional a/b seja $\nu_p(a/b) = \nu_p(a) - \nu_p(b)$, onde $a, b \in \mathbb{Z}, b \neq 0$. Definimos $\nu_p(0) = \infty$. Então as seguintes propriedades são satisfeitas:

(i) $\nu_p(x) = \infty$ se, e somente se, $x = 0$;

(ii) $\nu_p(xy) = \nu_p(x) + \nu_p(y)$;

(iii) $\nu_p(x+y) \geq \min\{\nu_p(x), \nu_p(y)\}$.

Além disso, se $\nu_p(x) < \nu_p(y)$ então $\nu_p(x+y) = \nu_p(x)$.

Teorema 1.36 (De Polignac)**.** *Seja p um número primo e n um inteiro positivo. Então*

$$\nu_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor,$$

onde $\lfloor x \rfloor$ é o maior inteiro menor ou igual que x.

Demonstração. (Esboço:) Existem $\left\lfloor \frac{n}{p} \right\rfloor$ inteiros entre 1 e n que são divisíveis por p, contribuindo com um fator de p. Destes, $\left\lfloor \frac{n}{p^2} \right\rfloor$ contribuem com um segundo fator, e assim por diante. □

Lema 1.37. *Seja p um número primo e seja n um inteiro positivo. Então*

$$\nu_p(n!) < \frac{n}{p-1}.$$

Além disso, se $n \geq p$, então

$$\nu_p(n!) > \frac{n}{2p}.$$

E ainda,

$$\nu_p(n!) \geq \frac{n}{p-1} - \frac{\log(n+1)}{\log p}.$$

Demonstração. Pelo Teorema 1.36, temos que

$$\nu_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^t} \right\rfloor + \cdots .$$

Portanto,

$$\nu_p(n!) < \frac{n}{p} + \frac{n}{p^2} + \cdots + \frac{n}{p^t} + \cdots = n\left(\frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^t} + \cdots\right) = \frac{n}{p-1}.$$

Se $n \geq p$, então $n/p \geq 1$. Como $\lfloor x \rfloor > x/2$ para todo $x \geq 1$ temos

$$\nu_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^t} \right\rfloor + \cdots > \left\lfloor \frac{n}{p} \right\rfloor > \frac{n}{2p}.$$

A última desigualdade é o Lema 1 em [3].

□

Definição 1.38. *Dizemos que um valor absoluto $\|\cdot\|$ é **Arquimediano** se o corpo tem característica zero e se existe $m \in \mathbb{Z}$ tal que $\|m\| > 1$. Caso contrário, dizemos que é **não Arquimediano**.*

Lema 1.39. *Um valor absoluto $\|\cdot\|$ em um corpo $\mathbb{K}$ é não Arquimediano se, e somente se, satisfaz*

$$\|x + y\| \leq \max(\|x\|, \|y\|).$$

Chamamos a desigualdade do lema anterior de **ultramétrica** e vamos nos referir ao valor absoluto não Arquimediano como valor absoluto ultramétrico.

O valor absoluto p-ádico é um valor absoluto ultramétrico. De fato, $|x+y|_p = p^{-\nu_p(x+y)}$ e $\nu_p(x+y) \geq \min(\nu_p(x), \nu_p(y))$ nos dá $|x+y|_p \leq p^{-\min(\nu_p(x),\nu_p(y))}$. Por outro lado, $\max(|x|_p, |y|_p) = \max(p^{-\nu_p(x)}, p^{-\nu_p(y)}) \geq p^{-\min(\nu_p(x),\nu_p(y))}$. Logo $|x+y|_p \leq \max(|x|_p, |y|_p)$.

Se $\mathbb{K}$ é um corpo e P é um ideal primo não nulo de $\mathcal{O}_\mathbb{K}$, podemos introduzir um **valor absoluto P-ádico** de maneira similar: para $x \in \mathbb{K}^*$ seja $\nu_P(x) = \mathrm{ord}_P(x)$ o expoente de P na decomposição do ideal principal $\langle x \rangle$ em produto de potências de ideais primos, e seja $|x|_P = C^{-\nu_P(x)}$ para algum $C > 1$ (e $|0|_P = 0$).

Por se tratar de uma ferramenta fundamental no estudo das formas lineares em logaritmos p-ádicos, faremos um estudo mais preciso da ordem de um ideal com respeito a um ideal primo na seção seguinte.

1.4 Um pouco de teoria algébrica dos números

Nessa seção, apresentaremos definições e resultados de teoria algébrica dos números que podem ser encontrados em [1], [4] ou [15]. Não temos por objetivo dar detalhes da teoria, apenas desejamos dar noções que possibilitem o entendimento do restante do trabalho.

Definição 1.40. *Um número complexo é dito um* ***número algébrico*** *se satisfaz uma equação polinomial*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0,$$

onde $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}$.

Caso $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$ *então esse número é dito um* ***inteiro algébrico****.*

Dado um corpo de números algébricos $\mathbb{K}$ definimos $\mathcal{O}_{\mathbb{K}}$ como o **anel dos inteiros algébricos de** $\mathbb{K}$. Observe que se $\mathbb{L}$ e $\mathbb{K}$ são corpos de números algébricos tais que $\mathbb{L} \subseteq \mathbb{K}$ então $\mathcal{O}_{\mathbb{L}} \subseteq \mathcal{O}_{\mathbb{K}}$.

Definição 1.41. *Dizemos que* D *é um* ***domínio de Dedekind*** *se* D *é um domínio Noetheriano (toda cadeia de ideais ascendente é finita),* D *é integralmente fechado e se todo ideal primo de* D *é um ideal maximal.*

É possível mostrar que o anel dos inteiros algébricos de um corpo $\mathbb{K}$, $\mathcal{O}_{\mathbb{K}}$, é um domínio de Dedekind.

Teorema 1.42. *Se* D *é um domínio de Dedekind então todo ideal não nulo de* D *pode ser escrito de maneira única como produto de ideais primos.*

Seja $\mathbb{K}$ um corpo de números algébricos de grau n, ou seja, $[\mathbb{K} : \mathbb{Q}] = n$, e sejam $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ os $\mathbb{K}$-conjugados de α, definimos a **norma de** α por

$$N(\alpha) = \alpha_1\alpha_2 \cdots \alpha_n.$$

Se $\alpha \in \mathbb{Q}$ temos que $N(\alpha) = \alpha^n$. Além disso, temos que a norma é multiplicativa, isto é, $N(\alpha\beta) = N(\alpha)N(\beta)$ para α e β em $\mathbb{K}$.

Teorema 1.43. *Seja* $\mathbb{K}$ *um corpo de números algébricos de grau* n*. Então:*

(i) Se α *é unidade de* $\mathcal{O}_{\mathbb{K}}$ *então* $N(\alpha) = \pm 1$*;*

(ii) Se $\alpha \in \mathcal{O}_{\mathbb{K}}$ e $N(\alpha) = \pm 1$ então α é unidade de $\mathcal{O}_{\mathbb{K}}$;

(iii) Se $\alpha \in \mathcal{O}_{\mathbb{K}}$ e $N(\alpha) = \pm p$, onde p é um primo racional, então α é irredutível;

(iv) Se $\alpha \in \mathcal{O}_{\mathbb{K}}$ então $N(\langle\alpha\rangle) = |N(\alpha)|$.

Dado um ideal I de $\mathcal{O}_{\mathbb{K}}$ definimos a **norma de** I por

$$N(I) = \text{card}(\mathcal{O}_{\mathbb{K}}/I),$$

onde $\mathcal{O}_{\mathbb{K}}/I$ é o anel quociente de $\mathcal{O}_{\mathbb{K}}$ por I. E vale $N(IJ) = N(I)N(J)$ para I e J ideais de $\mathcal{O}_{\mathbb{K}}$.

Teorema 1.44. *Seja I ideal de $\mathcal{O}_{\mathbb{K}}$. Então:*

(i) Se $N(I) = p$ então I é ideal primo de $\mathcal{O}_{\mathbb{K}}$;

(ii) $N(I) \in I$.

Considere agora A um domínio de Dedekind com corpo quociente $\mathbb{K}$. Seja $\mathbb{L}$ uma extensão separável de $\mathbb{K}$ de grau finito n e seja B o fecho inteiro de A em $\mathbb{L}$. Note que B é também um domínio de Dedekind.

Seja P um ideal primo de A, então o *lifting* ou a *extensão* de P para B é o ideal de B gerado por P, que denotaremos por PB ou $\langle P\rangle_B$. Cabe ressaltar que o ideal $\langle P\rangle_B$ pode não ser ideal primo em B.

Como B é domínio de Dedekind, podemos escrever o ideal $\langle P\rangle_B$ como produto de ideais primos de B:

$$\langle P\rangle_B = \prod_{i=1}^{g} Q_i^{e_i},$$

onde Q_i são ideais primos de B e e_i são inteiros positivos.

Por outro lado, podemos começar com um ideal Q de B e obter um ideal primo de A da seguinte forma: $P = Q \cap A$. Nesse caso, dizemos que Q *encontra-se sobre* P ou que P é uma *contração* de Q para A.

Suponha agora que temos um ideal primo não nulo P de A que se estende para B. A próxima proposição nos diz que os ideais $Q_1, Q_2, \ldots, Q_g$ que aparecem na fatoração de $\langle P\rangle_B$ são precisamente os ideais primos de B que encontram-se sobre P.

Proposição 1.45. *Seja Q um ideal primo de B. Então Q aparece na fatoração prima de $\langle P\rangle_B$ se, e somente se, $Q \cap A = P$.*

Assumindo

$$\langle P\rangle_B = \prod_{i=1}^{g} Q_i^{e_i}$$

temos que g é o *número de decomposição* de P na extensão $\mathbb{L}|\mathbb{K}$, $e_i = e(Q_i|P)$ é o *índice de ramificação* de Q_i em $\mathbb{L}|\mathbb{K}$ e definimos o *grau de inércia* de Q_i, $f_i = f(Q_i|P)$, como a dimensão de B/Q_i sobre A/P.

Considere ainda uma extensão separável $\mathbb{E}|\mathbb{L}$ de grau finito e C o fecho inteiro de B em $\mathbb{E}$. Assim, dado um ideal primo J de C e sejam $Q = J \cap B$ e $P = Q \cap A$ com $P \neq 0$. Então:

$$e(J|P) = e(J|Q) \cdot e(Q|P),$$

$$f(J|P) = f(J|Q) \cdot f(Q|P).$$

Seja $\mathbb{K}$ um corpo de números algébricos sobre $\mathbb{Q}$. Seja θ um número algébrico tal que $\mathbb{K} = \mathbb{Q}(\theta)$ e sejam $\theta_1 = \theta, \theta_2, \ldots, \theta_n$ os conjugados de θ sobre $\mathbb{Q}$. Então os corpos

$$\mathbb{Q}(\theta_1) = \mathbb{Q}(\theta) = \mathbb{K}, \mathbb{Q}(\theta_2), \ldots, \mathbb{Q}(\theta_n)$$

são chamados os corpos conjugados de K.

Enunciaremos agora o Teorema das Unidades de Dirichlet que utilizaremos no terceiro capítulo. A demonstração desse teorema pode ser encontrado em [1] ou [15].

Teorema 1.46 (Teorema das Unidades de Dirichlet)**.** *Seja $\mathbb{K}$ um corpo de números algébricos de grau n. Seja r o número de conjugados reais do corpo $\mathbb{K}$ e seja $2s$ o número de conjugados complexos do corpo $\mathbb{K}$, assim $n = r + 2s$. Então $\mathcal{O}_\mathbb{K}$ contêm $r + s - 1$ unidades $\varepsilon_1, \ldots, \varepsilon_{r+s-1}$ tais que cada unidade de $\mathcal{O}_\mathbb{K}$ pode ser expressa unicamente da forma $\rho\varepsilon_1^{n_1} \cdots \varepsilon_{r+s-1}^{n_{r+s-1}}$, onde ρ é uma raiz da unidade em $\mathcal{O}_\mathbb{K}$ e $n_1, \ldots, n_{r+s-1}$ são inteiros.*

1.4.1 Ordem de um ideal com respeito a um ideal primo

Seja A um ideal não nulo de um domínio de Dedekind D, então A pode ser escrito de forma única como $A = \prod_{i=1}^{n} P_i^{a_i}$, onde P_i são ideais primos distintos e a_i são inteiros. Dizemos então que $a_i = \mathrm{ord}_{P_i}(A)$ é a ordem do ideal A com respeito ao ideal primo P_i, $i = 1, \ldots, n$.

Assim, se P é ideal primo diferente de P_i para todo i, dizemos que $\mathrm{ord}_P(A) = 0$. Além disso, temos $\mathrm{ord}_P(\langle 1\rangle) = 0$ e $\mathrm{ord}_P(P^k) = k$.

Claramente, dados A e B ideais não nulos de um domínio de Dedekind D, temos que $A \mid B$, ou seja, existe um ideal C de D tal que $B = AC$, se, e somente se, $\mathrm{ord}_P(A) \leq \mathrm{ord}_P(B)$, para todo ideal primo P.

Teorema 1.47. *Sejam A e B ideais não nulos de um domínio de Dedekind D. Então*

$$A \mid B \Leftrightarrow B \subseteq A.$$

Teorema 1.48. *Sejam A e B ideais não nulos de um domínio de Dedekind D e P um ideal primo de D. Então:*

(i) $ord_P(AB) = ord_P(A) + ord_P(B)$

(ii) $ord_P(A + B) = \min\{ord_P(A), ord_P(B)\}$.

Analogamente à definição de ordem de um ideal com respeito a um ideal primo, podemos definir a ordem de um elemento não nulo com relação a um ideal primo. Seja D um domínio de Dedekind e $\mathbb{K}$ seu corpo quociente. Para $\alpha \in \mathbb{K}$, $\alpha \neq 0$, definimos $\mathrm{ord}_P(\alpha) = \mathrm{ord}_P(\langle\alpha\rangle)$, para qualquer ideal primo P de D. Daí, se A for um ideal de D temos que $\alpha \in A$ se, e somente se, $\mathrm{ord}_P(\alpha) \geq \mathrm{ord}_P(A)$, para todo ideal primo P de D.

Teorema 1.49. *Seja D um domínio de Dedekind e $\mathbb{K}$ seu corpo quociente. Seja P um ideal primo de D, então*

(i) Para α, $\beta \in \mathbb{K}^*$ temos

$$ord_P(\alpha\beta) = ord_P(\alpha) + ord_P(\beta);$$

(ii) Para α, $\beta, \alpha + \beta \in \mathbb{K}^*$ temos

$$ord_P(\alpha + \beta) \geq \min\{ord_P(\alpha), ord_P(\beta)\}.$$

Além disso, se $ord_P(\alpha) \neq ord_P(\beta)$ então

$$ord_P(\alpha + \beta) = \min\{ord_P(\alpha), ord_P(\beta)\}.$$

Teorema 1.50. *Sejam $\mathbb{L}$ um corpo de números algébricos e P um ideal primo em $\mathcal{O}_{\mathbb{L}}$. Então existe um único primo $p \in \mathbb{Z}$ tal que $P \mid \langle p \rangle$.*

Teorema 1.51. *Sejam $\mathbb{L}$ um corpo de números algébricos de grau D sobre $\mathbb{Q}$ e P um ideal primo em $\mathcal{O}_{\mathbb{L}}$. Se $p \in \mathbb{Z}$ é o primo que está em P então $N(P) = p^f$, para algum $f \in \{1, \ldots, D\}$, onde $N(P)$ é a norma de P.*

As demonstrações de todos esses resultados podem ser encontradas em [1].

O número f dado pelo teorema acima é chamado de **grau de inércia** de P em $\mathcal{O}_{\mathbb{L}}$ e é a dimensão de P sobre o corpo $\mathbb{Z}/p\mathbb{Z}$, ou seja, $\mathcal{O}_{\mathbb{L}}/P$ é um corpo finito com p^f elementos.

Além disso, se $\langle p \rangle = P_1^{e_1} \ldots P_g^{e_g}$, onde $P_1, \ldots, P_g$ são ideais primos distintos de $\mathcal{O}_{\mathbb{L}}$ e $e_1, \ldots, e_g$ são inteiros positivos temos que $\sum_{i=1}^{g} e_i f_i = D$. Chamamos g de **número de decomposição** e temos que $g \leq D$. E ainda, se e é tal que $P^e \mid \langle p \rangle$ e $P^{e+1} \nmid \langle p \rangle$ então e é dito o **índice de ramificação** de P.

Considerando e o índice de ramificação de P, onde P é um ideal primo que divide p, temos que $\nu_p(x) = \mathrm{ord}_P(x)e^{-1}$.

Para o caso particular em que $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ é um corpo quadrático temos a seguinte classificação:

Teorema 1.52. *Seja p um primo ímpar. Então*

(i) p é ramificado em $\mathbb{Q}(\sqrt{d}) \Leftrightarrow p$ divide d,

(ii) p é inerte em $\mathbb{Q}(\sqrt{d})$ (ou seja, $\langle p \rangle = P$) $\Leftrightarrow \left(\frac{d}{p}\right) = -1$,

(iii) p é totalmente decomposto em $\mathbb{Q}(\sqrt{d}) \Leftrightarrow \left(\frac{d}{p}\right) = 1$,

onde $\left(\frac{d}{p}\right)$ é o símbolo de Legendre.

Capítulo 2

Limitantes para Formas Lineares em Logaritmos

2.1 Formas lineares em logaritmos

Uma forma linear em logaritmos de números algébricos é uma expressão da forma

$$\Lambda = \sum_{i=1}^{n} b_i \log \alpha_i,$$

onde estamos considerando $\alpha_1, \ldots, \alpha_n$ números algébricos, $b_1, \ldots, b_n$ inteiros e precisaremos que a forma linear seja não nula.

Sabendo que $|\Lambda| < e^{|\Lambda|} - 1$, por vezes chamaremos de forma linear em logaritmos a expressão $\Lambda = \alpha_1^{b_1}\alpha_2^{b_2}\cdots\alpha_n^{b_n} - 1$ que é a forma exponencial da nossa forma linear em logaritmos de números algébricos.

Em 1966, Alan Baker deu um limitante para o valor absoluto de uma forma linear em logaritmos, o que possibilitou a resolução de alguns tipos de equações Diofantinas, por exemplo, equações Diofantinas onde as variáveis desconhecidas estão no expoente (chamadas equações Diofantinas exponenciais).

Inicialmente, vamos fazer algumas considerações sobre números algébricos. Seja α um número algébrico de grau d e seja $f(x) = \sum_{i=0}^{d} a_i x^{d-i} \in \mathbb{Z}[x]$ seu polinômio minimal, com $a_0 > 0$ e $\text{mdc}(a_0, \ldots, a_d) = 1$. Definimos $\mathcal{H}(\alpha) = \max\{|a_0|, \ldots, |a_d|\}$ como a **altura clássica** de α e escrevendo $f(x) = a_0 \prod_{i=1}^{d}(x - \alpha^{(i)})$, onde $\alpha = \alpha^{(1)}$ e $\alpha^{(i)}$ são os conjugados

de α, definimos a **altura logarítmica de** α como

$$h(\alpha) = \frac{1}{d}\left(\log|a_0| + \sum_{i=1}^{d} \log \max\{1, |\alpha^{(i)}|\}\right).$$

Como estamos tratando de limitantes para as formas lineares em logaritmos de números algébricos, muitas vezes basta estimar a altura logarítmica do número algébrico α em vez de calculá-la efetivamente. Para isso, podemos utilizar as seguintes propriedades que podem ser encontradas em [17, Propriedade 3.3].

Sejam x e y números algébricos, então valem:

(i) $h(x^{-1}) = h(x)$;

(ii) $h(x/y) \leq h(x) + h(y)$;

(iii) $h(xy) \leq h(x) + h(y)$;

(iv) $h(x+y) \leq h(x) + h(y) + \log 2$.

Ainda, dizemos que dois números reais x e y são **multiplicativamente independentes** se a única solução da equação $x^a y^b = 1$, em inteiros a e b, é $a = b = 0$. Caso contrário, dizemos que x e y são **multiplicativamente dependentes**.

O seguinte resultado foi provado por Baker e Wüstholz, em 1993, para uma quantidade arbitrária n de números algébricos.

Teorema 2.1 (Baker e Wüstholz)**.** *Sejam $\alpha_1, \ldots, \alpha_n$ números algébricos não nulos e $b_1, \ldots, b_n$ inteiros, $D = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}]$, $B = \max\{|b_1|, \ldots, |b_n|, e\}$ e para $i = 1, \ldots n$, $A_i = \max\{\mathcal{H}(\alpha_i), e\}$. Se $\Lambda = \sum_{i=1}^{n} b_i \log \alpha_i \neq 0$ então*

$$|\Lambda| > \exp\left(-(16nd)^{2n+2} \log A_1 \cdots \log A_n \log B\right).$$

Usando o fato que $|\Lambda| < e^{|\Lambda|} - 1$ temos o seguinte corolário:

Corolário 2.2. *Se $\alpha_1^{b_1} \cdots \alpha_n^{b_n} \neq 1$ então*

$$|\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1| > \exp(-(17(n+1)D)^{2n+7} \log A_1 \cdots \log A_n \log B).$$

Em geral, buscamos resolver equações Diofantinas de duas ou três variáveis, por isso é interessante questionarmos se é possível melhorar os limitantes das formas lineares em logaritmos quando trabalhamos com dois ou três logaritmos. E é exatamente isso que Laurent, Mignotte e Nesterenko obtiveram para formas lineares em dois logaritmos:

Teorema 2.3 (Laurent, Mignotte e Nesterenko)**.** *Sejam b_1 e b_2 inteiros positivos e α_1, α_2 números algébricos reais positivos multiplicativamente independentes. Sejam $\Lambda = b_1 \log \alpha_1 - b_2 \log \alpha_2$, $D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]$ e A_1, A_2 tais que*

$$\log A_i \geq \max \left\{ h(\alpha_i), \frac{|\log \alpha_i|}{D}, \frac{1}{D} \right\}, \ i = 1, 2.$$

Além disso, defina

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}.$$

Então

$$\log |\Lambda| \geq -24,34 \cdot D^4 \left(\max \left\{ \log b' + 0,14, \frac{21}{D}, \frac{1}{2} \right\} \right)^2 \log A_1 \log A_2.$$

Um exemplo simples da aplicação desse teorema pode ser encontrado em [13].

Muitas vezes, quando utilizamos os resultados acima para resolução de equações diofantinas obtemos limitantes muito grandes para as variáveis envolvidas na equação e mesmo com o auxílio do computador, não é viável computar os casos finitos. Assim, precisamos utilizar estratégias que reduzam os limitantes das variáveis, o que podemos fazer em alguns casos com a ajuda do seguinte lema devido a Dujella e Pethö [7].

Lema 2.4 (Dujella e Pethö)**.** *Seja M um inteiro positivo e p/q um convergente da fração contínua do irracional γ tal que $q > 6M$ e seja μ um número real. Seja $\varepsilon = \|\mu q\| - M\|\gamma q\|$, onde $\|\cdot\|$ é a distância até o inteiro mais próximo. Se $\varepsilon > 0$, então não existe solução para*

$$0 < m\gamma - n + \mu < A \cdot B^{-m}$$

em inteiros positivos m e n com

$$\frac{\log Aq/\varepsilon}{\log B} \leq m \leq M.$$

2.2 Formas lineares em logaritmos p-ádicos

Nessa seção, veremos os teoremas de formas lineares em logaritmos p-ádicos dados por Yu, Bugeaud e Laurent. Esses teoremas são utilizados para obter limitantes superiores para ordem de uma forma linear não nula $\Lambda = \alpha_1^{b_1} \alpha_2^{b_2} \cdots \alpha_n^{b_n} - 1$ com relação a um ideal primo P.

Os resultados de formas lineares em logaritmos p-ádicos, assim como os de formas lineares em logaritmos dados por Baker, são utilizados para obter limitantes para as variáveis envolvidas em uma equação Diofantina. Em alguns casos, as formas lineares em logaritmos p-ádicos nos dão uma limitação melhor do que quando utilizamos as formas lineares em logaritmos vistas na seção anterior, o que nos auxilia na hora de computar os casos finitos e verificar quais resultam em solução da equação Diofantina dada.

Sejam $\mathbb{L}$ um corpo de números algébricos de grau D sobre $\mathbb{Q}$ e P um ideal primo em $\mathcal{O}_{\mathbb{L}}$. Sejam e_P e f_P os índices de ramificação e inércia, respectivamente. Sabemos que se $p \in \mathbb{Z}$ é o único número primo tal que $P \mid p$, então

$$\langle p \rangle = \prod_{i=1}^{k} P_i^{e_i},$$

onde $P_1, \ldots, P_k$ são ideais primos de $\mathcal{O}_{\mathbb{L}}$. Temos que o ideal primo P é um dos ideais primos P_i, digamos $P = P_1$ e daí $e_P = e_1$.

Teorema 2.5. *Nas condições acima, sejam $\alpha_1, \ldots, \alpha_n$ números algébricos e $b_1, \ldots, b_n$ inteiros. Sejam $H_j \geq \max\{h(\alpha_j), \log p\}$, para todo $j = 1, \ldots, n$ e $B = \max\{|b_1|, \ldots, |b_n|\}$. Se $\Lambda = \prod_{i=1}^{n} \alpha_i^{b_i} - 1$ é diferente de zero então*

$$ord_P(\Lambda) \leq 19(20\sqrt{n+1}D)^{2(n+1)} e_P^{n-1} \frac{p^{f_P}}{(f_P \log p)^2} \log(e^5 nD) H_1 \cdots H_n \log B.$$

Essa versão de limitantes para formas lineares em logaritmos p-ádicos foi dada por Kunrui Yu em [21] como consequência de um teorema mais geral. Outras versões dadas por Yu podem ser encontradas em [20], ou ainda no trabalho de Grossman e Luca em [8], onde encontra-se a seguinte versão para limitantes de formas lineares em logaritmos p-ádicos.

Teorema 2.6. *Suponha $\alpha_1, \ldots, \alpha_n$ números algébricos, diferentes de zero e um, com alturas não excedendo $A_1, \ldots, A_n$. Vamos assumir, $A_i \geq e$. Seja D o grau de $\mathbb{L} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ sobre $\mathbb{Q}$. Sejam $b_1, \ldots, b_n$ números inteiros e $B \geq \max\{|b_1|, \ldots, |b_n|, e\}$. Seja P um ideal primo de $\mathcal{O}_{\mathbb{L}}$ dividindo o primo p. Se $ord_P(\alpha_i) = 0$ para todo $i = 1, 2, \ldots, n$ e se $\Lambda = \alpha_1^{b_1} \alpha_2^{b_2} \ldots \alpha_n^{b_n} - 1 \neq 0$, então existem constantes computáveis C_1 e C_2 tais que*

$$ord_P(\Lambda) < (C_1 nD)^{C_2 n} \frac{p^D}{\log^2 p} \log A_1 \cdots \log A_n \log(D^2 B).$$

Da mesma forma que no caso complexo, temos que é útil conhecer a forma linear em dois logaritmos p-ádicos. O resultado que enunciaremos abaixo, dado por Bugeaud e Laurent, é originalmente uma estimativa da valorização p-ádica do número Λ, $v_p(\Lambda)$, mas que por definição está relacionada com a ordem do ideal gerado por Λ com relação ao ideal primo P que divide p pela seguinte definição:

$$v_p(\Lambda) = e_P^{-1}\mathrm{ord}_P(\Lambda).$$

Assim, a estimativa encontrada para $\mathrm{ord}_P(\Lambda)$ é a estimativa de $v_p(\Lambda)$ vezes o índice de ramificação e_P.

Teorema 2.7 (Bugeaud e Laurent)**.** *Seja $\mathbb{L}$ um corpo de números algébricos de grau D sobre $\mathbb{Q}$. Sejam P um ideal primo em $\mathcal{O}_\mathbb{L}$ e p um primo racional tal que $P \mid p$. Suponha $\log A_j \geq \max\left\{h(\alpha_j), \dfrac{f_P \log p}{D}\right\}$ e sejam $\Lambda = \alpha_1^{b_1}\alpha_2^{b_2} - 1$ e $b' = \dfrac{|b_1|}{D\log A_2} + \dfrac{|b_2|}{D\log A_1}$. Se α_1 e α_2 são multiplicativamente independentes, então*

$$ord_P(\Lambda) \leq \frac{24p(p^{f_P}-1)D^5}{f_P^5(p-1)(\log p)^4}(\max\{\log b' + \log\log p + 0,4; 10 f_P \log p/D; 10\})^2 \log A_1 \log A_2.$$

Assim como para formas lineares em logaritmos, existem outras versões dos teoremas de formas lineares em logaritmos p-ádicos. No entanto, optamos por enunciar os teoremas que utilizaremos na resolução das equações Diofantinas do próximo capítulo.

Capítulo 3

Aplicações das Formas Lineares em Logaritmos p-ádicos

Neste capítulo, pretendemos dar sentido ao que foi exposto acima resolvendo três equações Diofantinas utilizando o método de formas lineares em logaritmos p-ádicos.

3.1 Números de Fibonacci que são rep-dígitos

Um **rep-dígito** é um inteiro positivo que tem um único dígito repetido quando escrito na base 10 e podemos generalizar essa definição para qualquer base $b > 1$ chamando de **rep-dígito na base b**.

Exemplo 3.1. *O número*

$$77777 = 7 \cdot 10^4 + 7 \cdot 10^3 + 7 \cdot 10^2 + 7 \cdot 10 + 7 = 7 \cdot \frac{10^5 - 1}{10 - 1}$$

é um rep-dígito.

Exemplo 3.2. *Os números de Mersenne, que são números da forma $M_n = 2^n - 1$ onde n é número natural, são rep-dígitos na base 2, pois $M_n = \overline{111\ldots1}_{(2)}$ quando escrito na base 2.*

Queremos encontrar os números de Fibonacci que são rep-dígitos, o que nos leva ao seguinte teorema estudado por Luca em [10].

Teorema 3.3. *O maior número de Fibonacci que é um rep-dígito é $F_{10} = 55$.*

Demonstração. Inicialmente vamos assumir que F_n possua m dígitos e que d é o dígito repetido. Queremos então encontrar todas as soluções da seguinte equação Diofantina.

$$F_n = \overline{ddd\ldots d}_{(10)} = d \cdot 10^{m-1} + d \cdot 10^{m-2} + \cdots + d \cdot 10 + d = d \cdot \frac{10^m - 1}{10 - 1},$$

com $d \in \{1, 2, \ldots, 9\}$.

Seja $\alpha = \frac{1+\sqrt{5}}{2}$ então podemos reescrever a equação usando a fórmula de Binet:

$$\frac{\alpha^n - \varepsilon\alpha^{-n}}{\sqrt{5}} = F_n = d \cdot \frac{10^m - 1}{9},$$

onde $\varepsilon = (-1)^n \in \{\pm 1\}$.

Escrevendo de forma conveniente temos

$$\alpha^n + \frac{d\sqrt{5}}{9} - \varepsilon\alpha^{-n} = \frac{d10^m\sqrt{5}}{9},$$

ou seja,

$$\alpha^{-n}\left(\alpha^{2n} + \frac{d\sqrt{5}}{9}\alpha^n - \varepsilon\right) = \frac{d2^m(\sqrt{5})^{2m+1}}{9}.$$

Ou ainda,

$$\alpha^{-n}(\alpha^n - z_1)(\alpha^n - z_2) = \frac{d2^m(\sqrt{5})^{2m+1}}{9} \tag{3.1}$$

onde z_1 e z_2 são soluções da equação quadrática

$$X^2 + \frac{d\sqrt{5}}{9}X - \varepsilon = 0,$$

ou seja,

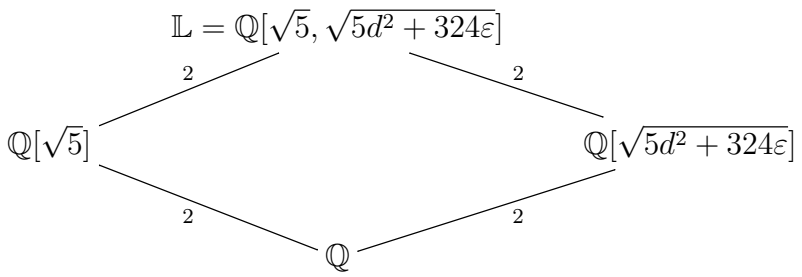
$$z_{1,2} = \frac{-d\sqrt{5} \pm \sqrt{5d^2 + 324\varepsilon}}{18}.$$

Queremos aplicar o Teorema 2.7, devido a Bugeaud e Laurent, para resolver a equação Diofantina acima. Para isso, precisamos verificar todas as hipóteses.

Inicialmente, note que (3.1) é diferente de zero e assuma que $d \neq 9$. Vamos mostrar que $z_{1,2}$ e α são multiplicativamente independentes.

Note que $\alpha \in \mathbb{Q}[\sqrt{5}]$ e se $\varepsilon = -1$ temos que $5d^2 + 324\varepsilon < 5 \cdot 8^2 - 324 = -4 < 0$, daí $z_{1,2}$ é complexo com parte real diferente de zero, e portanto multiplicativamente independente com α. Agora, se $\varepsilon = 1$, temos que $5d^2 + 324\varepsilon$ é coprimo com 5, pois $5 \nmid 324$, e não é um quadrado perfeito para todo $d \in \{1, \ldots, 8\}$. Logo, $z_{1,2} = x_1\sqrt{5} \pm x_2\sqrt{c}$ com $x_1, x_2 \in \mathbb{Q}^*$ e $c \neq 0, 1, 5$ um inteiro livre de quadrados. Assim, α e $z_{1,2}$ são multiplicativamente independentes também nesse caso, já que nenhuma potência de $z_{1,2}$ está em $\mathbb{Q}[\sqrt{5}]$.

Seja $\mathbb{L} = \mathbb{Q}[z_1, z_2] = \mathbb{Q}[\sqrt{5}, \sqrt{5d^2 + 324\varepsilon}]$ e observe no diagrama abaixo que o grau da extensão de $\mathbb{L}$ sobre $\mathbb{Q}$ é $D = 4$.



Considere agora P um ideal primo em $\mathcal{O}_{\mathbb{L}}$ que divide $\sqrt{5}$, ou seja, $\langle\sqrt{5}\rangle \subseteq P$. Queremos estimar a ordem com relação ao ideal P da igualdade (3.1).

Por um lado temos que

$$\mathrm{ord}_P(\alpha^{-n}(\alpha^n - z_1)(\alpha^n - z_2)) = \mathrm{ord}_P(\alpha^{-n}) + \mathrm{ord}_P(\alpha^n - z_1) + \mathrm{ord}_P(\alpha^n - z_2).$$

Note que α^{-n} é uma unidade em $\mathcal{O}_{\mathbb{L}}$, pois

$$N(\alpha^{-n}) = N(\alpha)^{-n} = \left[\left(\frac{1+\sqrt{5}}{2}\right)^2\left(\frac{1-\sqrt{5}}{2}\right)^2\right]^{-n} = 1.$$

Logo, temos $\mathrm{ord}_P(\alpha^{-n}) = 0$.

Por outro lado,

$$\mathrm{ord}_P\left(\frac{d2^m(\sqrt{5})^{2m+1}}{9}\right) \geq 2m+1,$$

pois como P divide $\sqrt{5}$ temos $\langle\sqrt{5}\rangle = PA$ para algum ideal A e daí $\langle\sqrt{5}\rangle^{2m+1} = P^{2m+1}A^{2m+1}$. Logo, a ordem de $\frac{d2^m(\sqrt{5})^{2m+1}}{9}$ com relação ao ideal primo P é pelo menos $2m+1$.

Assim, temos

$$2m+1 \leq \mathrm{ord}_P(\alpha^n - z_1) + \mathrm{ord}_P(\alpha^n - z_2). \tag{3.2}$$

Queremos estimar

$$\mathrm{ord}_P(\alpha^n - z_{1,2}) = \mathrm{ord}_P(z_{1,2}(\alpha^n z_{1,2}^{-1} - 1)) = \mathrm{ord}_P(z_{1,2}) + \mathrm{ord}_P(\alpha^n z_{1,2}^{-1} - 1).$$

Portanto, precisamos estimar $\mathrm{ord}_P(z_{1,2})$ e $\mathrm{ord}_P(\alpha^n z_{1,2}^{-1} - 1)$.

Mas, temos que $\mathrm{ord}_P(z_{1,2}) = 0$ pois P não divide $z_{1,2}$. De fato, se dividisse teríamos

$$z_{1,2}^2 + \frac{-d\sqrt{5}}{9}z_{1,2} + \varepsilon \equiv 0(\mathrm{mod}\ P) \Rightarrow \varepsilon \equiv 0(\mathrm{mod}\ P),$$

o que é um absurdo.

E, para $\mathrm{ord}_P(\alpha^n z_{1,2}^{-1} - 1)$ utilizaremos o Teorema 2.7 com $\Lambda = \alpha^n z_{1,2}^{-1} - 1$.

Note inicialmente que P não pode dividir ambos $\alpha^n - z_1$ e $\alpha^n - z_2$, pois daí dividiria a diferença $z_1 - z_2 = \frac{\sqrt{5d^2+324\varepsilon}}{9}$ que é um número algébrico cuja norma é um número racional, sendo o numerador e o denominador coprimos com 5. Logo temos que para um dos índices $i = 1$ ou $i = 2$, $\mathrm{ord}_P(\alpha^n - z_i) = 0$. Suponha que $\mathrm{ord}_P(\alpha^n - z_2) = 0$ e vamos estimar $\mathrm{ord}_P(\Lambda)$ com $\Lambda = \alpha^n z_1^{-1} - 1$.

Precisamos estimar as alturas logarítmicas de α e z_1. Como $X^2 - X - 1$ é o polinômio minimal de α em $\mathbb{Z}[X]$ temos que $h(\alpha) = \dfrac{1}{2}(\log 1 + \log \alpha + \log 1) < 0,25$. Agora, note que os conjugados de z_1 são da forma

$$\frac{\pm d\sqrt{5} \pm \sqrt{5d^2 + 324\varepsilon}}{18}$$

e seus valores absolutos são menores ou iguais que

$$\frac{8\sqrt{5} + \sqrt{5 \cdot 64 + 324}}{18} < 2,41.$$

Note ainda que o polinômio minimal de z_1 divide o polinômio

$$81\left(X^2 - \frac{d\sqrt{5}}{9}X - \varepsilon\right)\left(X^2 + \frac{d\sqrt{5}}{9}X - \varepsilon\right) = 81(X^2 - \varepsilon)^2 - 5d^2X^2 \in \mathbb{Z}[X]$$

portanto $h(z_1) < \dfrac{1}{4}(\log 81 + 4\log(2,41)) < 2$.

É interessante observarmos que o ideal gerado por $\sqrt{5}$ é um ideal primo em $\mathcal{O}_{\mathbb{Q}[\sqrt{5}]} \subseteq \mathcal{O}_{\mathbb{L}}$ pelo Teorema 1.44, e que 5 é um quadrado perfeito nesse corpo pois $5 = (\sqrt{5})^2$. Logo, o índice de ramificação é $e(\langle\sqrt{5}\rangle|\langle 5\rangle) = 2$.

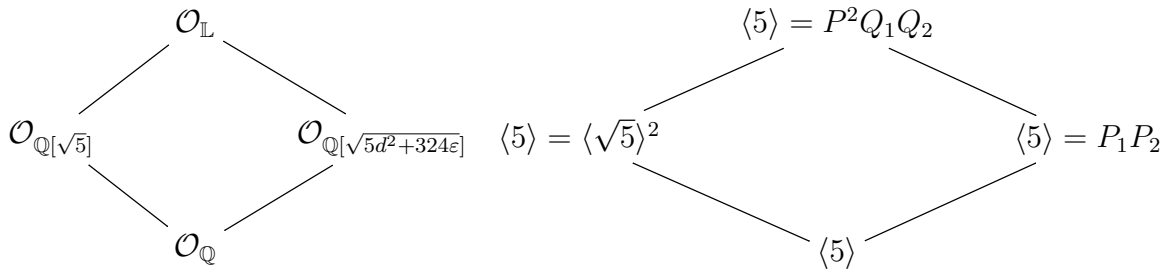
Temos ainda, pelo Teorema 1.52, que como $5d^2 + 324\varepsilon$ é livre de quadrados e

$$\left(\frac{5d^2 + 324\varepsilon}{5}\right) = \left(\frac{324\varepsilon}{5}\right) = \left(\frac{18^2}{5}\right)\left(\frac{\pm 1}{5}\right) = 1,$$

5 se divide em dois ideais primos distintos em $\mathcal{O}_{\mathbb{Q}[\sqrt{5d^2+324\varepsilon}]} \subseteq \mathcal{O}_{\mathbb{L}}$, ou seja, $\langle 5\rangle = P_1P_2$ com $P_1 \neq P_2$.

Como $e_P = e(P|5) = e(P|\langle\sqrt{5}\rangle) \cdot e(\langle\sqrt{5}\rangle|5) = 2 \cdot e(P|\langle\sqrt{5}\rangle)$ temos que $e_P = 2$ ou $e_P = 4$.

Suponha que $e_P = 4$. Logo, $\langle 5\rangle = P^4$ em $\mathcal{O}_{\mathbb{L}}$. Mas nesse caso, pela Proposição 1.45 teríamos $P_1 = P_2$ em $\mathcal{O}_{\mathbb{Q}[\sqrt{5d^2+324\varepsilon}]}$, o que é um absurdo.



Portanto, temos $e_P = 2$, $f_P = 1$ e $D = 4$.

Cabe ressaltar que, como o índice de ramificação é limitado pelo grau da extensão, poderíamos utilizar $e_P \leq 4$ no nosso problema. No entanto, já que foi possível determinar exatamente que $e_P = 2$, fazemos uso desse valor, obtendo assim uma limitação melhor para nossa forma linear em logaritmos.

Tomando $\alpha_1 = \alpha$, $\alpha_2 = z_1$, $b_1 = n$ e $b_2 = -1$, podemos considerar

$$\log A_1 = 1 > \max\left\{h(\alpha), \frac{\log 5}{4}\right\},$$

$$\log A_2 = 2 > \max\left\{h(z_1), \frac{\log 5}{4}\right\}$$

$$\text{e} \quad b' \leq \frac{n}{8} + \frac{1}{4} = \frac{n+2}{8}.$$

Perceba que nesse momento podemos aplicar o Teorema 2.7 e limitar $\text{ord}_P(\alpha^n - z_1)$. No entanto pela desigualdade (3.2) obteríamos uma limitação para m em função de n, que não é suficiente para resolvermos a equação Diofantina inicial. Logo, precisamos de outros artifícios para obter o resultado.

Por indução em n podemos verificar que

$$\alpha^{n-2} < F_n < \alpha^{n-1}$$

para todo $n \geq 3$. Assim temos

$$\begin{aligned} & \alpha^{n-2} < F_n = \frac{d}{9}(10^m - 1) < 10^m \\ \Rightarrow \quad & (n-2)\log\alpha < m\log 10 \\ \Rightarrow \quad & n - 2 < m\frac{\log 10}{\log\alpha} \\ \Rightarrow \quad & n < 4,8m + 2. \end{aligned}$$

Assim, $b' < \frac{n+2}{8} < 0,6m + 0,5$ e temos pela equação (3.2):

$$\begin{aligned} 2m+1 &< \frac{24 \cdot 5 \cdot (5-1) \cdot 4^5}{(5-1) \cdot (\log 5)^4} \cdot 1 \cdot 2 \\ &\cdot \quad (\max\{\log(0,6m+0,5) + \log\log 5 + 0,4; (10\log 5)/4; 10\})^2 \\ &< 3,7 \cdot 10^4 \cdot (\max\{\log(0,6m+0,5) + \log\log 5 + 0,4; (10\log 5)/4; 10\})^2 \end{aligned}$$

Como $(10 \log 5)/4 < 10$ temos:

$$2m + 1 < 3,7 \cdot 10^4 \cdot (\max\{\log(0,6m+0,5) + \log\log 5 + 0,4; 10\})^2.$$

Se o máximo da expressão acima é 10 temos que $2m+1 < 3,7 \cdot 10^4 \cdot 10^2 \Rightarrow m < 1,9 \cdot 10^6$. No outro caso, podemos utilizar o *Mathematica* para encontrar a limitação para o m através do comando:

```
Reduce[2*m+1<3.7*10^4*(Log[0.6*m+0.5]+Log[Log[5]]+0.4)^2,m,Integers]
```

Obtendo assim $m < 4,6 \cdot 10^6$.

Logo, $m < 4,6 \cdot 10^6$ e $n < 2,3 \cdot 10^7$.

Para analisarmos essa quantidade finita de casos, recorremos ao *Mathematica*. Existe mais de uma maneira de fazermos isso, e aqui, daremos uma delas. Inicialmente buscamos artifícios matemáticos que otimizem o tempo que o programa levará para encontrar as soluções. Por exemplo, podemos procurar soluções congruentes módulo 10^8, com $m = 8$ e se obtivermos alguma solução, aumentamos as casas decimais para verificar se continua sendo solução da nossa equação inicial.

```
Timing[Catch[Do[{n, d};If[Mod[Fibonacci[n] - d*(10^8 - 1)/9, 10^8] == 0,
Print[{n, d}]], {n, 11, 2.3*10^7}, {d, 1, 8}]]]
```

É interessante observar que se considerarmos $n < 10^5$ o comando

```
Timing[Catch[Do[{n, d};If[Mod[Fibonacci[n] - d*(10^8 - 1)/9, 10^8] == 0,
Print[{n, d}]], {n, 11, 10^5}, {d, 1, 8}]]]
```

retorna $\{273.937756, \text{Null}\}$, o que significa que demorou menos que 5 minutos para retornar que não existe nenhuma solução. No entanto, quando consideramos o comando com $n < 2,3 \cdot 10^7$, o programa pode demorar dias para retornar se existe alguma solução. De modo geral, não haverá soluções.

Para finalizar, resta analisar o caso em que $d = 9$, ou seja, queremos resolver a equação Diofantina $F_n = 10^m - 1$.

Para isso, usaremos o *Teorema do Divisor Primitivo de Carmichael* que diz que se $n > 12$ então existe p primo tal que $p \mid F_n$ e $p \nmid F_1 \cdots F_{n-1}$. Tal primo p é chamado de *divisor primitivo.*

Sabendo que para todo inteiro positivo k valem

$$\begin{aligned} F_{4k} + 1 &= F_{2k-1}L_{2k+1} \\ F_{4k+1} + 1 &= F_{2k+1}L_{2k} \\ F_{4k+2} + 1 &= F_{2k+2}L_{2k} \\ F_{4k+3} + 1 &= F_{2k+1}L_{2k+2} \end{aligned}$$

onde L_n é um termo da sequência de Lucas dada por $L_0 = 2$, $L_1 = 1$ e $L_n = L_{n-1} + L_{n-2}$, temos que $10^m = F_n + 1 = F_{(n-\delta)/2}L_{(n+\delta)/2}$ onde $\delta \in \{\pm 1, \pm 2\}$ e $n \equiv \delta (\bmod\ 2)$. Portanto, se $n > 26$ temos $(n - \delta)/2 > 12$ e $F_{(n-\delta)/2}$ tem um divisor primitivo $p > 12$, mas isso é um absurdo pois p dividiria 10^m. Logo, não temos solução para $d = 9$ e $n > 26$.

Utilizando o *Mathematica* para computar F_n quando $n \leq 26$ temos que a maior solução é $F_{10} = 55$.

`Table[Fibonacci[n], {n, 0, 26}]` nos dá

$$\{0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \mathbf{55}, 89, 144, 233, 377, 610, 987, 1597,$$
$$2584, 4181, 6765, 10946, 17711, 28657, 46368, 75025, 121393\}.$$

□

3.2 Sequência exponencial fatorial

Definição 3.4. *Seja $(a_n)_{n\geq 1}$ a sequência definida por $a_1 = 1$ e $a_n = n^{a_{n-1}}$ para $n \geq 2$. Essa sequência é chamada de* ***exponencial fatorial.***

Observe que os primeiros termos da sequência exponencial fatorial são $a_1 = 1$, $a_2 = 2^1 = 2$, $a_3 = 3^{2^1} = 9$, $a_4 = 4^{3^{2^1}} = 262144$ e $a_5 = 5^{262144}$ tem 183231 dígitos decimais (ver [16]).

Teorema 3.5. *A única solução da equação*

$$a_1 + \cdots + a_n = m^2$$

em inteiros positivos m e n é $m = n = 1$.

O problema de encontrar as soluções para a equação $a_1 + \cdots + a_n = m^l$, com $l > 1$, foi estudado por Luca e Marques em [11] e aqui, estamos interessados no caso em que $l = 2$, já que utilizaremos as formas lineares em logaritmos p-ádicos para encontrar as soluções.

Além disso, a sequência exponencial fatorial (a_n) aparece como A049384 em [16]. Uma propriedade interessante dessa sequência é que o número $\sum_{n\geq 1} 1/a_n$ é um número de Liouville e portanto transcendente. Outra curiosidade é que

$$\sum_{n\geq 1} 1/a_n = 1,611114925808376736\underbrace{1111\ldots111}_{183213}272243\ldots.$$

Vamos então à prova do teorema:

Demonstração. Começaremos com algumas observações que valem em geral.

Observe que se $b_n := \sum_{1\leq k\leq n} a_k$ temos:

$$\begin{aligned} b_1 &= a_1 = 1, \text{ que é um quadrado perfeito.} \\ b_2 &= a_1 + a_2 = 1 + 2^1 = 3, \\ b_3 &= a_1 + a_2 + a_3 = 2^2 \times 3 \text{ e} \\ b_4 &= a_1 + \cdots + a_4 = 2^2 \times 65539, \text{ que não são quadrados perfeitos.} \end{aligned}$$

Agora note que se $b_5 = m^2$ e $p \mid m^2$ então $p^2 \mid m^2$.

Com a ajuda do computador, vemos que $17 \mid b_5$ mas $b_5 \equiv 17 \times 5 \pmod{17^2}$, ou seja, $17^2 \nmid b_5$. Logo, b_5 não é um quadrado perfeito. O mesmo argumento usamos para mostrar que b_6, b_7 e b_8 não são quadrados perfeitos. De fato, $7 \mid b_6$ mas $b_6 \equiv 7 \times 2 \pmod{7^2}$, $2 \mid b_7$ mas $b_7 \equiv 2 \pmod{2^2}$ e $2 \mid b_8$ mas $b_8 \equiv 2 \pmod{2^2}$.

Logo, vamos considerar $n \geq 9$.

Observe que $a_n = n^{a_{n-1}} > e^{a_{n-1}}$ para $n \geq 3$ então $\log a_n > a_{n-1}$. Além disso, $a_n \geq 2a_{n-1}$ para todo $n \geq 2$. De fato, já que $x > 2\log x$ para todo $x \geq 1$ temos $a_n > 2\log a_n > 2a_{n-1}$, para $n \geq 3$ e, para $n = 2$ temos $a_2 = 2 = 2a_1$. Logo, $a_n \geq 2a_{n-1}$ para $n \geq 2$.

Usando essas desigualdades, temos que:

$$\begin{aligned}
0 < m^2 - a_n &= m^2 - n^{a_{n-1}} = a_{n-1} + a_{n-2} + \cdots + a_1 \\
&\leq a_{n-1} + \frac{a_{n-1}}{2} + \frac{a_{n-2}}{2} + \cdots + \frac{a_2}{2} \\
&\leq a_{n-1} + \frac{a_{n-1}}{2} + \frac{a_{n-1}}{2^2} + \cdots + \frac{a_{n-1}}{2^{n-2}} \\
&= a_{n-1}\left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^{n-2}}\right) \\
&< 2a_{n-1} < 2\log a_n.
\end{aligned}$$

Ou seja,

$$0 < m^2 - n^{a_{n-1}} < 2\log a_n \tag{3.3}$$

Primeiramente, note que se n é ímpar então $a_{n-1} = (n-1)^{a_{n-2}}$ é par, e portanto $a_n = n^{a_{n-1}}$ é um quadrado perfeito. Daí, dividindo a desigualdade $0 < m^2 - a_n < 2\log a_n$ por $m + \sqrt{a_n}$ temos:

$$\begin{aligned}
& 0 < m^2 - a_n = (m - \sqrt{a_n})(m + \sqrt{a_n}) < 2\log a_n \\
\Rightarrow\ & 0 < m - \sqrt{a_n} < \frac{2\log a_n}{m + \sqrt{a_n}} \\
\Rightarrow\ & 0 < m - \sqrt{a_n} < \frac{2\log a_n}{\sqrt{a_n}} < 1.
\end{aligned}$$

Note que na última desigualdade usamos o fato de que $2\log x < \sqrt{x}$ para $x \geq 75$.

Mas aí, temos

$$0 < m - \sqrt{a_n} < 1$$

o que é uma contradição, já que $m - \sqrt{a_n}$ é um inteiro quando a_n é um quadrado perfeito.

Se considerarmos n par e quadrado perfeito, temos novamente que a_n é um quadrado perfeito e obtemos a mesma contradição acima.

Logo, vamos assumir que n é par mas n não é um quadrado perfeito. Então $n \geq 10$ e temos:

$$0 < m - \sqrt{a_n} < \frac{2\log a_n}{\sqrt{a_n}}.$$

Portanto,

$$0 < m - \sqrt{n} \times n^{(a_{n-1}-1)/2} < \frac{2\log a_n}{n^{a_{n-1}/2}} = \frac{2a_{n-1}\log n}{n^{a_{n-1}/2}}.$$

Dividindo as desigualdades acima por $n^{(a_{n-1}-1)/2}$ e tomando o módulo obtemos:

$$\left|\sqrt{n} - \frac{m}{n^{(a_{n-1}-1)/2}}\right| < \frac{2a_{n-1}\log n}{n^{a_{n-1}-0{,}5}}.$$

Pelo Teorema 1.15, devido a Worley, temos que se α é um irracional e

$$\left|\alpha - \frac{p}{q}\right| < \frac{\kappa}{q^2},$$

então existem inteiros k, r e s com $|r| < 2\kappa$, $|s| < 2\kappa$, $p = rp_k + sp_{k-1}$ e $q = rq_k + sq_{k-1}$, onde p_k/q_k é o k-ésimo convergente de α. Além disso, podemos escolher k de maneira que k seja máximo na condição $q_k \leq q$.

Na nossa situação, como

$$\left|\sqrt{n} - \frac{m}{n^{(a_{n-1}-1)/2}}\right| < \frac{2a_{n-1}\log n}{n^{a_{n-1}-0,5}}$$

temos que $\alpha = \sqrt{n}$, $p = m$, $q = n^{(a_{n-1}-1)/2} = rq_k + sq_{k-1}$, $\kappa = \frac{2a_{n-1}\log n}{\sqrt{n}}$ e ainda $\max\{|r|, |s|\} < \frac{4a_{n-1}\log n}{\sqrt{n}}$.

Observe que $q = n^{(a_{n-1}-1)/2}$ é inteiro já que n é par e portanto a_{n-1} é ímpar, implicando que $(a_{n-1} - 1)/2$ é um inteiro.

Definimos o numerador e o denominador dos convergentes da fração contínua como sequências recorrentes no Corolário 1.5. Como os convergentes da fração contínua de $\sqrt{n}$ nos dão as soluções da equação de Pell $X^2 - nY^2 = 1$ e $(1, 0)$ também é solução dessa equação de Pell, podemos fazer uma pequena mudança de variável e definir as sequências recorrentes do numerador e denominador dos convergentes da seguinte maneira: considerando $\sqrt{n} = \langle u_0, \overline{u_1, \ldots, u_h}\rangle$, onde h é o menor período par da fração contínua de $\sqrt{n}$, definimos

$$\begin{aligned} p_0 &= 1 & q_0 &= 0 \\ p_1 &= u_0 & q_1 &= 1 \\ p_k &= u_{k-1}p_{k-1} + p_{k-2}, & q_k &= u_{k-1}q_{k-1} + q_{k-2}, \quad \forall \quad k \geq 2. \end{aligned}$$

Com essa nova definição temos que a solução minimal da equação de Pell $X^2 - nY^2 = 1$ é (p_h, q_h). Para ver isso, basta utilizarmos as proposições 1.25 e 1.26.

Usando a definição podemos obter

$$q_k \geq F_k \geq \left(\frac{1+\sqrt{5}}{2}\right)^{k-2},$$

onde F_k é o k-ésimo número de Fibonacci. Assim, como escolhemos k tal que $q_k < q = n^{(a_{n-1}-1)/2}$ temos

$$(k-2)\log\left(\frac{1+\sqrt{5}}{2}\right) < \frac{a_{n-1}-1}{2}\log n.$$

O que nos dá

$$\begin{aligned} k &< \frac{(a_{n-1}-1)\log n}{2\log\left(\frac{1+\sqrt{5}}{2}\right)} + 2 \\ &< 2[(a_{n-1}-1)\log n + \log n] \\ &< 2a_{n-1}\log n. \end{aligned}$$

Agora, para cada $l \in \{0, \ldots, h-1\}$ considere a recorrência binária $(q_{h\lambda+l})_{\lambda\geq 0}$ com valores iniciais $q_l \leq q_h$ e $q_{h+l} \leq q_{2h}$ e equação característica $X^2 - 2p_hX + 1$. Chamaremos de

$$\zeta = p_h + \sqrt{n}q_h \quad \text{e} \quad \zeta^{-1} = p_h - \sqrt{n}q_h$$

as raízes da equação característica. Assim, podemos escrever

$$q_{h\lambda+l} = c_1\zeta^{\lambda} + c_2\zeta^{-\lambda},$$

onde $q_l = c_1 + c_2$ e $q_{h+l} = c_1\zeta + c_2\zeta^{-1}$. Assim, obtemos

$$c_1 = \frac{q_{h+l} - \zeta^{-1}q_l}{\zeta - \zeta^{-1}} \quad \text{e} \quad c_2 = \frac{q_l\zeta - q_{h+l}}{\zeta - \zeta^{-1}}.$$

Escrevendo $k = h\lambda + l$ para algum $l \in \{1, \ldots, h\}$ temos $q_k = c_1\zeta^{\lambda} + c_2\zeta^{-\lambda}$ e $q_{k-1} = d_1\zeta^{\lambda} + d_2\zeta^{-\lambda}$, com $q_{l-1} = d_1 + d_2$ e $q_{h+(l-1)} = d_1\zeta + d_2\zeta^{-1}$, obtendo assim

$$d_1 = \frac{q_{h+(l-1)} - \zeta^{-1}q_{l-1}}{\zeta - \zeta^{-1}} \quad \text{e} \quad d_2 = \frac{q_{l-1}\zeta - q_{h+(l-1)}}{\zeta - \zeta^{-1}}.$$

Portanto $q = n^{(a_{n-1}-1)/2} = rq_k + sq_{k-1} = (rc_1 + sd_1)\zeta^{\lambda} + (rc_2 + sd_2)\zeta^{-\lambda}$, ou seja

$$n^{(a_{n-1}-1)/2} = \alpha_1\zeta^{\lambda} + \alpha_2\zeta^{-\lambda},$$

onde $\alpha_i = rc_i + sd_i,\ i = 1, 2$.

Como estamos considerando n par, temos que $2^{(a_{n-1}-1)/2}$ divide o lado esquerdo na igualdade acima. Queremos estudar o expoente de 2 no lado direito.

Inicialmente, observe que $\beta_i = (\zeta - \zeta^{-1})\alpha_i$ é um inteiro algébrico para $i = 1, 2$. Seja $\beta_1 = 2^t\gamma_1$, onde $t \geq 0$ e γ_1 não é múltiplo de 2. Observe que β_2 é o conjugado de β_1 com o sinal trocado e que portanto $\beta_2 = 2^t\gamma_2$ e γ_2 não é múltiplo de 2.

Além disso,

$$\begin{aligned} |\beta_1| &= |(\zeta - \zeta^{-1})\alpha_1| = |\zeta - \zeta^{-1}| \left| \left(\frac{q_{h+l} - \zeta^{-1}q_l}{\zeta - \zeta^{-1}}\right) r + \left(\frac{q_{h+(l-1)} - \zeta^{-1}q_{l-1}}{\zeta - \zeta^{-1}}\right) s \right| \\ &\leq (q_{2h} + \zeta q_h)|r| + (q_{2h} + \zeta q_h)|s| \\ &= (|r| + |s|)(q_{2h} + \zeta q_h). \end{aligned}$$

Logo, como $|\beta_1\beta_2| = 2^{2t}|\gamma_1\gamma_2| \geq 2^{2t}$ pois $|\gamma_1\gamma_2| \geq 1$ já que γ_1 e γ_2 são inteiros algébricos, temos:

$$2^{2t} \leq |\beta_1||\beta_2| = |\beta_1|^2 \leq (|r| + |s|)^2(q_{2h} + \zeta q_h)^2.$$

E assim,

$$2^t \leq (|r| + |s|)(q_{2h} + \zeta q_h) \leq \frac{8a_{n-1}\log n}{\sqrt{n}}(q_{2h} + \zeta q_h).$$

Sabendo que $\zeta < e^{3\sqrt{n}\log n}$,

$$q_h = c_1\zeta + c_2\zeta^{-1} = \frac{\zeta - \zeta^{-1}}{2\sqrt{n}} < \zeta$$

e

$$q_{2h} = c_1\zeta^2 + c_2\zeta^{-2} = \frac{\zeta^2 - \zeta^{-2}}{2\sqrt{n}} < \zeta^2,$$

então

$$\begin{aligned} t\log 2 &\leq \log\left(\frac{8a_{n-1}\log n}{\sqrt{n}}\right) + \log\left(q_{2h} + \zeta q_h\right) \\ &< \log\left(\frac{8a_{n-1}\log n}{\sqrt{n}}\right) + \log\left(2\zeta^2\right), \end{aligned}$$

o que nos dá $t < 3a_{n-2}\log(n-1)$.

Como $2^{(a_{n-1}-1)/2}$ divide $\alpha_1\zeta^{\lambda} + \alpha_2\zeta^{-\lambda}$ então divide $\beta_1\zeta^{\lambda} + \beta_2\zeta^{-\lambda} = 2^t(\gamma_1\zeta^{\lambda} + \gamma_2\zeta^{-\lambda})$. Além disso, $(a_{n-1}-1)/2 - t > 0$ e portanto $2^{(a_{n-1}-1)/2-t}$ divide

$$\gamma_1\zeta^{\lambda} + \gamma_2\zeta^{-\lambda} = -\gamma_2\zeta^{-\lambda}\left(\left(\frac{-\gamma_1}{\gamma_2}\right)\zeta^{2\lambda} - 1\right).$$

Considere P ideal primo dividindo $p = 2$. Queremos estimar

$$\mathrm{ord}_P\left(-\gamma_2\zeta^{-\lambda}\left(\left(\frac{-\gamma_1}{\gamma_2}\right)\zeta^{2\lambda} - 1\right)\right).$$

Mas, note que, $\mathrm{ord}_P(-\gamma_2) = \mathrm{ord}_P(\zeta^{-\lambda}) = 0$ pois ζ é unidade ($\zeta\zeta^{-1} = 1$) e P não divide γ_2 (pois se dividisse, 2 dividiria γ_1 ou γ_2, o que não ocorre).

Queremos portanto estimar a ordem de 2 que pode aparecer em $\Lambda = \left(\frac{-\gamma_1}{\gamma_2}\right)\zeta^{2\lambda} - 1$ utilizando formas lineares em logaritmos p-ádicos.

Por um lado, como

$$t < 3a_{n-2}\log(n-1) \ \text{ e } \ 2^{(a_{n-1}-1)/2-t} \mid -\gamma_2\zeta^{-\lambda}\Lambda,$$

temos que

$$\mathrm{ord}_P(\Lambda) \geq \frac{a_{n-1}-1}{2} - 3a_{n-2}\log(n-1) > \frac{a_{n-1}}{4}.$$

Para obter uma estimativa superior para $\mathrm{ord}_P(\Lambda)$ usaremos o Teorema 2.7. Assim, considere $\alpha_1 = -\dfrac{\gamma_1}{\gamma_2}$, $\alpha_2 = \zeta$, $b_1 = 1$ e $b_2 = 2\lambda$. Note que $\mathbb{K} = \mathbb{Q}[\sqrt{n}]$ e portanto $D = 2$. Consideramos $p = 2$ e P um ideal primo dividindo 2, e vamos considerar que α_1 e α_2 são multiplicativamente independentes.

Precisamos determinar A_1 e A_2, para isso vamos estimar a altura logarítmica de α_1 e α_2. Como $|\gamma_1\gamma_2| \geq 1$, $|\gamma_1| \leq (|r|+|s|)(q_{h+l}+\zeta q_l)$ e

$$2(|r|+|s|)\zeta^2 < 2\frac{8a_{n-1}\log n}{\sqrt{n}}e^{6\sqrt{n}\log n} < 16a_{n-1}e^{6\sqrt{n}\log n}$$

temos

$$\begin{aligned} h(\alpha_1) &\leq \frac{\log|\gamma_1/\gamma_2|}{2} = \frac{\log\left(\dfrac{|\gamma_1|^2}{|\gamma_1\gamma_2|}\right)}{2} \leq \frac{\log|\gamma_1|^2}{2} = \log|\gamma_1| \\ &\leq \log\left((|r|+|s|)(q_{h+l}+\zeta q_l)\right) < \log\left((|r|+|s|)(q_{2h}+\zeta q_h)\right) \\ &< \log\left(2(|r|+|s|)\zeta^2\right) < \log 16a_{n-1} + 6\sqrt{n}\log n. \end{aligned}$$

E ainda,

$$h(\alpha_2) = h(\zeta) = \frac{\log\zeta}{2} < \frac{3\sqrt{n}\log n}{2} = 1,5\sqrt{n}\log n.$$

Logo, podemos escolher

$$\log A_1 = 2\log a_{n-1} > \log 16a_{n-1} + 6\sqrt{n}\log n$$

e

$$\log A_2 = \log a_{n-1} > 1,5\sqrt{n}\log n.$$

Resta determinar b' para termos satisfeitas todas as hipóteses do Teorema 2.7. Note que $2\lambda \leq 2(h\lambda + l) = 2k < 4a_{n-1}\log n$ pois vimos que $k < 2a_{n-1}\log n$. Assim

$$b' = \frac{1}{2\log a_{n-1}} + \frac{2\lambda}{4\log a_{n-1}} < \frac{a_{n-1}}{2}.$$

Lembrando que f é o índice de inércia e portanto $f \leq 2$, temos que $\dfrac{p^f-1}{f^5} \leq 1$ e obtemos que

$$\mathrm{ord}_P(\Lambda) \leq \frac{24\cdot 2\cdot 2^5}{(2-1)(\log 2)^4}\cdot(\log a_{n-1})^2\cdot 2\log a_{n-1}\log a_{n-1} < 14000\cdot(\log a_{n-1})^4.$$

Comparando com a limitação inferior obtida anteriormente temos

$$a_{n-1} < 56000(\log a_{n-1})^4$$

e usando o *Mathematica* obtemos $a_{n-1} < 10^{11}$, que é falso para $n \geq 10$.

O comando que utilizamos no *Mathematica* para obter a limitação do a_{n-1} é o seguinte: `Reduce[x<56000*(Log[x])^4,x,Integers]`.

Logo, não existe solução para o caso em que $n \geq 10$ e α_1 e α_2 são multiplicativamente independentes.

Basta analisarmos o caso em que α_1 e α_2 são multiplicativamente dependentes.

Inicialmente, note que $\zeta = p_h + \sqrt{n}q_h$ é uma unidade em $\mathcal{O}_{\mathbb{K}}$ pois $N(\zeta) = \zeta\zeta^{-1} = 1$, e como $\zeta > 1$ temos que ζ pode ser o gerador da parte livre de torção do grupo das unidades de $\mathcal{O}_{\mathbb{K}}$. Se ζ não for o gerador, existe $\zeta_1 > 1$ unidade que é gerador com $\zeta = \zeta_1^2$ e tal que a norma de ζ_1 é -1. De fato, se $\zeta_1 = a + \sqrt{n}b$ temos que $N(\zeta_1) = a^2 - nb^2 = \pm 1$, mas se $N(\zeta_1) = 1$ teríamos que (a, b) é solução da equação de Pell $X^2 - nY^2 = 1$ com $\zeta = \zeta_1^2 > \zeta_1$, contrariando o fato de (p_h, q_h) ser a solução minimal. Logo $N(\zeta_1) = -1$.

Logo, para considerarmos os dois casos, vamos escrever $\zeta = \zeta_1^{\delta}$ com $\delta \in \{1, 2\}$. Além disso, como $\frac{\gamma_1}{\gamma_2}$ é unidade, pelo Teorema das Unidades de Dirichlet 1.46, temos $\frac{\gamma_1}{\gamma_2} = \varepsilon\zeta_1^{\sigma}$, onde $\varepsilon = \pm 1$.

Como vimos,

$$2\log a_{n-1} > h(\alpha_1) = h\left(-\frac{\gamma_1}{\gamma_2}\right) = h(\varepsilon\zeta_1^{\sigma}) = \frac{|\sigma|\log\zeta_1}{2} > \frac{|\sigma|\log\left(\frac{1+\sqrt{5}}{2}\right)}{2},$$

onde a última desigualdade vem do fato que $\zeta = p_h + q_h\sqrt{n} \geq 1 + \sqrt{10}$, pois $n \geq 10$ e p_h, q_h são inteiros positivos. Daí, se $\zeta_1 = \zeta \geq 1 + \sqrt{10} > \frac{1+\sqrt{5}}{2}$ e se $\zeta_1 = \sqrt{\zeta} \geq \sqrt{1 + \sqrt{10}} > \frac{1+\sqrt{5}}{2}$. Obtendo assim uma limitação para $|\sigma|$, isto é, $|\sigma| < 9\log a_{n-1}$.

Observe que

$$\Lambda = \left(-\frac{\gamma_1}{\gamma_2}\right)\zeta^{2\lambda} - 1 = -\varepsilon\zeta_1^{\sigma}(\zeta_1^{\delta})^{2\lambda} - 1 = -\varepsilon\zeta_1^{2\delta\lambda+\sigma} - 1,$$

e portanto, Λ divide

$$\zeta_1^{4\delta\lambda+2\sigma} - 1 = (\zeta_1^{2\delta\lambda+\sigma} - 1)(\zeta_1^{2\delta\lambda+\sigma} + 1),$$

que divide

$$\zeta^{4\delta\lambda+2\sigma} - 1 = \zeta_1^{\delta(4\delta\lambda+2\sigma)} - 1, \quad \delta \in \{1, 2\}.$$

Logo, $\mathrm{ord}_P(\Lambda) \leq \mathrm{ord}_P(\zeta^{4\delta\lambda+2\sigma} - 1)$. E agora, usaremos o Teorema 2.5 com um logaritmo para limitar superiormente $\mathrm{ord}_P(\zeta^{4\delta\lambda+2\sigma} - 1)$. Já vimos que $h(\zeta) < 1,5\sqrt{n}\log n$. Temos ainda que $p = 2$, $f_P \leq 2$, $H_1 = 2\log a_{n-1}$, $B = |4\delta\lambda + 2\sigma|$ e $D = 2$. Portanto

$$\begin{aligned}\mathrm{ord}_P(\zeta^{4\delta\lambda+2\sigma} - 1) &\leq 19(20\sqrt{2}\cdot 2)^4 \frac{2}{(\log 2)^2}\log(2e^5)2\log a_{n-1}\log|4\delta\lambda + 2\sigma| \\ &< 9,3\cdot 10^9 \log a_{n-1}\log(8\lambda + 2|\sigma|).\end{aligned}$$

Note que, como $\lambda < 2a_{n-1}\log n$ e $|\sigma| < 9\log a_{n-1}$, temos $8\lambda + 2|\sigma| < a_{n-1}^2$. Logo,

$$\begin{aligned}\mathrm{ord}_P(\zeta^{4\delta\lambda+2\sigma} - 1) &< 9,3\cdot 10^9 \log a_{n-1}\log a_{n-1}^2 \\ &< 18,6\cdot 10^9(\log a_{n-1})^2.\end{aligned}$$

Assim, comparando com o limite inferior obtido para $\mathrm{ord}_P(\Lambda)$ temos

$$\frac{a_{n-1}}{4} < 18,6\cdot 10^9(\log a_{n-1})^2$$

e usando no *Mathematica* o comando

```
Reduce[x<4*18.6*10^9*(Log[x])^2,x,Integers]
```

obtemos $a_{n-1} < 7,7\cdot 10^{13}$, o que é um absurdo para $n \geq 10$.

Portanto, a única solução da equação $a_1 + \cdots + a_n = m^2$ é $m = n = 1$. □

A solução do problema para $l > 2$, ou seja, quando $a_1 + a_2 + \cdots + a_n = m^l$, pode ser encontrada em [11] e, da mesma forma que no caso $l = 2$, a única solução é $m = n = 1$.

3.3 Somas de fatoriais em sequências recorrentes binárias

Nessa seção, vamos considerar o problema de expressar um termo de uma sequência recorrente binária não degenerada como a soma de fatoriais. Esse problema foi estudado por Grossman e Luca em [8].

Como vimos no primeiro capítulo, uma sequência recorrente binária $(u_n)_{n\geq 0}$ é uma sequência de inteiros tal que

$$u_{n+2} = ru_{n+1} + su_n, \quad \forall \ \ n \geq 0.$$

Vamos considerar r e s inteiros não nulos tais que $r^2 + 4s \neq 0$.

Sejam α e β as duas raízes da equação caractetística $X^2 - rX - s = 0$. Sabemos que existem duas constantes a e b tais que $u_n = a\alpha^n + b\beta^n, \ \forall \ n \geq 0$ (veja [14]). Considerando u_0 e u_1 os valores iniciais da sequência recorrente temos o seguinte sistema

$$\begin{cases} u_0 = a + b \\ u_1 = a\alpha + b\beta \end{cases}$$

o que nos dá

$$a = \frac{u_1 - \beta u_0}{\alpha - \beta} \ \text{ e } \ b = \frac{\alpha u_0 - u_1}{\alpha - \beta}.$$

Consideramos ainda $(u_n)_{n\geq 0}$ como uma sequência não degenerada, ou seja, $ab\alpha\beta \neq 0$ e α/β não é raiz da unidade.

Antes de enunciar o teorema principal desta seção, veremos alguns lemas importantes que serão utilizados na demonstração do teorema mais adiante.

Lema 3.6. *Seja $A > 0$ um número real dado. Então a equação*

$$\sum_{i=1}^{k} a_i n_i! = 0, \qquad a_i \in \mathbb{Z}, \ \ |a_i| < A \ \ \textit{para} \ \ i = 1, 2, \ldots, k \ \ \textit{e} \ \ n_1 < n_2 < \ldots < n_k,$$

onde nem todos os a_i's são zero, tem somente um número finito de soluções efetivamente computáveis.

Demonstração. Seja

$$B_n = \frac{1}{n} + \frac{1}{n(n-1)} + \cdots + \frac{1}{n!}, \ \ \text{para} \ \ n \geq 1.$$

Note que $B_1 = B_2 = 1$ e $B_3 = 2/3$. Em particular temos que $B_n \leq 2/n$ para $n \leq 3$. Vamos mostrar por indução em n que $B_n < 2/n$ para $n \geq 4$.

$$\begin{aligned} & B_{n-1} = \frac{1}{n-1} + \frac{1}{(n-1)(n-2)} + \cdots + \frac{1}{(n-1)!} \\ \Rightarrow \ & \frac{B_{n-1}}{n} = \frac{1}{n(n-1)} + \frac{1}{n(n-1)(n-2)} + \cdots + \frac{1}{n(n-1)!} \\ \Rightarrow \ & \frac{B_{n-1}}{n} + \frac{1}{n} = \frac{1}{n} + \frac{1}{n(n-1)} + \cdots + \frac{1}{n!} \\ \Rightarrow \ & \frac{1}{n}(1 + B_{n-1}) = B_n. \end{aligned}$$

Portanto,

$$B_n = \frac{1}{n}(1 + B_{n-1}) \leq \frac{1}{n}\left(1 + \frac{2}{n-1}\right).$$

Note que $1 + \dfrac{2}{n-1} < 2 \Leftrightarrow \dfrac{2}{n-1} < 1 \Leftrightarrow n-1 > 2 \Leftrightarrow n > 3$. Como $n \geq 4$ temos que $B_n < \dfrac{2}{n}$.

Assuma agora que $\sum_{i=1}^{k} a_i n_i! = 0$ vale para alguns $n_1 < \cdots < n_k$. Podemos assumir que nenhum dos a_i's é nulo. Vamos mostrar que $n_k < 2A$. Suponha, por contradição, que $n \geq 2A$. Então

$$\left|\sum_{i=1}^{k} a_i n_i!\right| \geq |a_k| n_k! - \left|\sum_{i=1}^{k-1} a_i n_i!\right| > n_k! - A\sum_{i=1}^{n_{k-1}} i! = n_k!\left(1 - A\sum_{i=1}^{n_{k-1}} \frac{i!}{n_k!}\right).$$

Note que $B_{n_k} = \sum_{i=1}^{n_{k-1}} \dfrac{i!}{n_k!}$, logo

$$\left|\sum_{i=1}^{k} a_i n_i!\right| > n_k!(1 - AB_{n_k}) \geq n_k!\left(1 - \frac{2A}{n_k}\right) \geq 0, \quad \text{para} \quad n_k \geq 2A.$$

Portanto,

$$\left|\sum_{i=1}^{k} a_i n_i!\right| > 0.$$

O que é um contradição com a hipótese, portanto $n_k < 2A$ e assim tem somente um número finito de soluções computáveis. □

Lema 3.7. *Seja $(u_n)_{n\geq 0}$ uma sequência recorrente binária não degenerada. Sejam α e β as raízes da equação característica e assuma que $|\alpha| > |\beta|$. Então, existem duas constantes C_1 e C_2 efetivamente computáveis, dependendo somente da sequência $(u_n)_{n\geq 0}$, tais que*

$$|u_n| > |\alpha|^{n - C_1 \log n} \quad \textit{para} \quad n > C_2.$$

Demonstração. Temos que

$$|u_n| = |a\alpha^n + b\beta^n| = |-a\alpha^n| \left|\frac{-b}{a}\left(\frac{\beta}{\alpha}\right)^n - 1\right|.$$

Note que $\frac{-b}{a}\left(\frac{\beta}{\alpha}\right)^n \neq 1$ para n suficientemente grande, caso contrário $u_n = 0$ para infinitos n.

Usando o corolário do Teorema 2.1 para formas lineares em logaritmos com $\alpha_1 = \frac{-b}{a}$, $\alpha_2 = \frac{\beta}{\alpha}$, $b_1 = 1$ e $b_2 = n$ temos

$$\left|\frac{-b}{a}\left(\frac{\beta}{\alpha}\right)^n - 1\right| > e^{-C\log n}.$$

Logo, para $n > C_2$,

$$|u_n| > |a||\alpha|^n e^{-C\log n}.$$

Escolhendo uma constante C_1 adequada temos que

$$|u_n| > |\alpha|^{n-C_1\log n}$$

para $n > C_2$.

□

Lema 3.8. *Seja $(u_n)_{n\geq 0}$ uma sequência recorrente binária não degenerada e seja p um número primo tal que $p \nmid s$ onde r e s são inteiros não nulos dados na recorrência $u_{n+2} = ru_{n+1} + su_n, \ \ \forall \ \ n \geq 0$ e tais que $r^2 + 4s \neq 0$. Então, existem duas constantes C_1 e C_2 efetivamente computáveis, dependendo de p e da sequência $(u_n)_{n\geq 0}$, tais que*

$$\nu_p(u_n) < C_1 \log^2 n, \quad \textit{para} \ \ n > C_2.$$

Demonstração. Considere P o ideal primo dividindo p. Como $\nu_p(u_n) = \mathrm{ord}_P(u_n)e_P^{-1}$, onde e_P é o índice de ramificação de P, temos $\nu_p(u_n) \leq \mathrm{ord}_P(u_n)$. Além disso, temos que $u_n = a\alpha^n + b\beta^n$. Assim,

$$\begin{aligned}\nu_p(u_n) &\leq \mathrm{ord}_P(u_n) = \mathrm{ord}_P(a\alpha^n + b\beta^n) = \mathrm{ord}_P\left(-b\beta^n\left(\frac{-a}{b}\left(\frac{\alpha}{\beta}\right)^n - 1\right)\right) \\ &= \mathrm{ord}_P(-b) + \mathrm{ord}_P(\beta^n) + \mathrm{ord}_P\left(\frac{-a}{b}\left(\frac{\alpha}{\beta}\right)^n - 1\right).\end{aligned}$$

Note que como α e β são as raízes da equação característica $X^2 - rX - s = 0$ temos $-s = \alpha\beta$. E como $p \nmid s$ temos que $p \nmid \alpha$ e $p \nmid \beta$.

Além disso, temos que $P \nmid \alpha$ e $P \nmid \beta$. De fato, se $P \mid \alpha$ então $N(P) \mid N(\alpha)$, onde N é a norma em $\mathbb{Q}(\alpha)$ que sabemos ser multiplicativa. Logo, $p^{f_P} \mid N(\alpha) = \alpha\beta$, onde f_P é o índice de inércia, e daí $p \mid \alpha$ ou $p \mid \beta$, contradição. Logo, $P \nmid \alpha$. Analogamente, $P \nmid \beta$.

Portanto $\mathrm{ord}_P(\alpha) = \mathrm{ord}_P(\beta) = 0$. Considere ainda $\mathrm{ord}_P(-b) < c_1$, onde c_1 é uma constante positiva. Resta estimar $\mathrm{ord}_P\left(\frac{-a}{b}\left(\frac{\alpha}{\beta}\right)^n - 1\right)$.

Vamos considerar dois casos:

Caso 1: $\frac{-a}{b}$ e $\frac{\alpha}{\beta}$ são multiplicativamente independentes. Neste caso utilizaremos o Teorema 2.7 com $\alpha_1 = \frac{-a}{b}$, $\alpha_2 = \frac{\alpha}{\beta}$, $b_1 = 1$ e $b_2 = n$. Temos que $b' \leq c_2 n$, onde c_2 é uma constante que depende de (u_n). Assim,

$$\mathrm{ord}_P\left(\frac{-a}{b}\left(\frac{\alpha}{\beta}\right)^n - 1\right) < c_4(\max\{c_3\log n, c_5\})^2 < c_6\log^2 n, \quad \text{para} \ \ n > C_2,$$

onde c_3, c_4, c_5 e c_6 dependem de (u_n) e p. E portanto,

$$\nu_p(u_n) \leq \mathrm{ord}_P(u_n) < c_1 + c_6 \log^2 n, \quad \text{para} \quad n > C_2$$

ou seja,

$$\nu_p(u_n) < C_1 \log^2 n, \quad \text{para} \quad n > C_2,$$

com C_1 e C_2 dependendo somente de (u_n) e p.

Caso 2: $\frac{-a}{b}$ e $\frac{\alpha}{\beta}$ são multiplicativamente dependentes. Assim, existem x e y inteiros não nulos tais que

$$\left(\frac{-a}{b}\right)^x = \left(\frac{\alpha}{\beta}\right)^y.$$

Assim, aplicando a ordem com relação ao ideal primo P temos

$$x \cdot \mathrm{ord}_P(-a/b) = y \cdot \mathrm{ord}_P(\alpha/\beta) = y(\mathrm{ord}_P(\alpha) - \mathrm{ord}_P(\beta)) = 0,$$

já que P não divide α nem β.

Logo, como $x \neq 0$ e $y \neq 0$ temos que $\mathrm{ord}_P(-a/b) = 0$ e $\mathrm{ord}_P(\alpha/\beta) = 0$. E assim, estamos nas condições para aplicar o Teorema 2.6 com $B = n$. Ou seja,

$$\mathrm{ord}_P\left(\frac{-a}{b}\left(\frac{\alpha}{\beta}\right)^n - 1\right) < (2k_1 D)^{2k_2} \frac{p^D}{\log^2 p} \log A_1 \log A_2 \log(D^2 n) < k_3 \log^2 n,$$

para $n > C_3$. Portanto

$$\nu_p(u_n) \leq \mathrm{ord}_P(u_n) < c_1 + k_3 \log^2 n, \quad \text{para} \quad n > C_3$$

o que nos dá

$$\nu_p(u_n) < C_4 \log^2 n \quad \text{para} \quad n > C_3.$$

□

Lema 3.9. *Seja $(u_n)_{n\geq 0}$ uma sequência recorrente binária não degenerada e seja p um número primo tal que $p \mid mdc(r, s)$. Então*

$$\nu_p(u_n) \geq \left\lfloor \frac{n}{2} \right\rfloor \quad \forall \quad n \geq 3.$$

Demonstração. Usaremos indução sobre n e o fato de $u_n = ru_{n-1} + su_{n-2}$.

Seja $d = \mathrm{mdc}(r, s)$.

Para $n = 3$ temos, como $p \mid d$,

$$\nu_p(u_3) = \nu_p(ru_2 + su_1) = \nu_p(d) + \nu_p(r_1u_2 + s_1u_1) \geq 1 = \lfloor \tfrac{3}{2} \rfloor.$$

Supondo verdadeiro para todo $k \leq n-1$, temos:

$$\begin{aligned}
\nu_p(u_n) &= \nu_p(ru_{n-1} + su_{n-2}) \\
&= \nu_p(d) + \nu_p(r_1u_{n-1} + s_1u_{n-2}) \\
&\geq 1 + \min\{\nu_p(r_1) + \nu_p(u_{n-1}), \nu_p(s_1) + \nu_p(u_{n-2})\} \\
&\geq 1 + \min\{\lfloor \tfrac{n-1}{2} \rfloor, \lfloor \tfrac{n-2}{2} \rfloor\} \\
&\geq 1 + \lfloor \tfrac{n-2}{2} \rfloor \\
&= \lfloor 1 + \tfrac{n-2}{2} \rfloor \\
&= \lfloor \tfrac{n}{2} \rfloor.
\end{aligned}$$

Logo, $\nu_p(u_n) \geq \lfloor \frac{n}{2} \rfloor$ para todo $n \geq 3$. □

Agora estamos aptos a demonstrar o teorema principal.

Teorema 3.10. *Seja $A > 1$ um número real, k um inteiro positivo fixado e $(u_n)_{n\geq 0}$ uma dada sequência recorrente binária não degenerada, como acima. Então, existe uma constante C efetivamente computável dependendo de A, k e da sequência $(u_n)_{n\geq 0}$, tal que se*

$$u_m = a_1 n_1! + \cdots + a_k n_k!, \quad a_i \in \mathbb{Z},\ |a_i| < A \quad \text{para } i = 1, \ldots, k,$$

onde n_i são inteiros não nulos arbitrários para $i = 1, 2, \ldots, k$, então $m < C$.

Demonstração. Para demonstrar o teorema usaremos indução em k. Note que quando $k = 0$ temos $u_m = 0$ e pelo Lema 3.7, tem somente um número finito de soluções computáveis.

Se $k = 1$ temos $u_m = an!$, para algum inteiro a com $|a| < A$. Nesse caso, considere p um primo menor ou igual que s que não divide s.

Se $n < s$ obtemos uma limitação também para m e o teorema está provado.

Seja então $n \geq s$.

Pelo Lema 3.8 temos $\nu_p(u_m) < C_1 \log^2 m$ para $m > C_2$. Por outro lado, como $u_m = an!$ temos $\nu_p(u_m) = \nu_p(an!) = \nu_p(a) + \nu_p(n!)$ e pelo Lema 1.37 temos $\nu_p(n!) > n/2p$. Assim

$$\frac{n}{2p} < \nu_p(n!) \leq \nu_p(a) + \nu_p(n!) = \nu_p(u_m) < C_1 \log^2 m,$$

para $m > C_2$.

Portanto, $n < 2pC_1 \log^2 m < 2sC_1 \log^2 m$ para $m > C_2$.

Agora, pelo Lema 3.7 temos $|\alpha|^{m-C_3 \log m} < |u_m| = |an!| < An^n$, para $m > C_4$. Logo

$$\frac{m}{2} < m - C_3 \log m < \frac{\log A}{\log |\alpha|} + \frac{n \log n}{\log |\alpha|} < C_5 n \log n,$$

para $m > C_6$.

Tomando $m > \max\{C_2, C_6\}$ temos

$$n < 2sC_1 \log^2 (2C_5 n \log n).$$

Logo, obtemos $n < C_7$ e assim u_m é limitada e portanto m também é limitado, provando o teorema.

Note que no caso $k = 1$ tomamos $p \leq s$ e $p \nmid s$, mas quando $s = 2$ tal primo não existe. Mas, caso $s = 2$ basta tomar $p = 3$ e teremos $n < 2 \cdot 3C_1 \log^2 m < 2 \cdot 3C_1 \log^2 (2C_5 n \log n)$ e da mesma forma o teorema está provado.

Vamos supor agora $k \geq 2$.

Observe que podemos assumir que $n_1 < n_2 < \cdots < n_k$. De fato, se tivermos $n_i = n_j$ para alguns índices $i \neq j$, colocamos em evidência esses n_i e substituímos a constante A por kA.

Observe também que, pelo Lema 3.6 e por indução, se $\sum_{j \in J} a_j n_j! = 0$ para algum conjunto de índices não vazio J, temos que existe um número finito de soluções computáveis, e portanto podemos assumir que $\sum_{j \in J} a_j n_j! \neq 0$.

Vamos denotar por $C_1, C_2, \ldots$ as constantes (maiores que 1) que dependem somente de k, A e da sequência $(u_n)_{n \geq 0}$.

Inicialmente, observe que, pelo Lema 3.7, temos

$$|\alpha|^{m-C_2 \log m} < |u_m| \quad \text{para} \quad m > C_1. \tag{3.4}$$

Por outro lado,

$$|u_m| = \left| \sum_{i=1}^{k} a_i n_i! \right| < \sum_{i=1}^{k} An_k! = kAn_k! < kAn_k^{n_k} = kAe^{n_k \log n_k}, \tag{3.5}$$

onde a última desigualdade segue do fato que $n! \leq n^n$ para todo $n \geq 1$.

Assim, por (3.4) e (3.5), temos $|\alpha|^{m-C_2 \log m} < kAe^{n_k \log n_k}$ para $m > C_1$.

Afirmação:

$$n_k > C_3 \frac{m}{\log m}, \quad \text{para} \quad m > C_1. \tag{3.6}$$

De fato, sejam l_1 e l_2 constantes maiores que 1 tais que $|\alpha|^{l_1} > kA$ e $|\alpha|^{l_2} > e$. Logo, para $m > C_1$,

$$\begin{aligned}
& |\alpha|^{m - C_2 \log m} < kAe^{n_k \log n_k} < |\alpha|^{l_1 + l_2 n_k \log n_k} \\
\Rightarrow \quad & m - C_2 \log m < l_1 + l_2 n_k \log n_k \\
\Rightarrow \quad & \frac{m}{\log m} - C_2 < \frac{l_1}{\log m} + l_2 n_k \frac{\log n_k}{\log m} \leq l_1 + l_2 n_k \frac{\log n_k}{\log m} \\
\Rightarrow \quad & \frac{m}{2 \log m} < \frac{m}{\log m} - C_2 - l_1 < l_2 n_k \frac{\log n_k}{\log m}
\end{aligned} \tag{3.7}$$

Além disso, como $u_m = a\alpha^m + b\beta^m$ e $|\alpha| > |\beta|$ temos $|u_m| \leq l_3 |\alpha|^m < |\alpha|^{2m}$ para $m > C_1$.

Por outro lado, $u_m = a_1 n_1! + \cdots + \alpha_k n_k!$ implica que

$$|u_m| \geq |a_k| n_k! - |a_1 n_1! + \cdots + a_{k-1} n_{k-1}!| > |a_k| n_k! - A(k-1) n_{k-1}! > l_4 n_k!,$$

para uma constante l_4.

Portanto,

$$|\alpha|^{2m} > |u_m| > l_4 n_k! > |\alpha|^{2n_k} \Rightarrow m > n_k \Rightarrow \log m > \log n_k.$$

Voltando em (3.7) temos

$$n_k > C_3 \frac{m}{\log m}$$

para $m > C_1$ e a afirmação está provada.

Note que se limitarmos n_k por cima por um polinômio em $\log m$ será possível encontrar uma constante C tal que $m < C$ e o teorema estará provado. Para fazer isso, encontraremos um limitante superior para n_1, que será nossa base de indução, e então usaremos indução em j para limitar superiormente n_j, para $1 \leq j \leq k$.

Então, vamos começar limitando n_1. Para isso, escolha q o menor primo maior que s, onde s é dado na equação característica da recorrência $(u_m)_{m \geq 0}$.

Pelo Lema 3.8, como $q \nmid s$ já que $q > s$, temos $\nu_q(u_m) < C_4 \log^2 m$ para $m > C_5$. Além disso, pelo Lema 1.37 dado no primeiro capítulo, ou $n_1 < q$ (e aí já teríamos

uma limitação para n_1, pois pelo Postulado de Bertrand existe um primo q entre s e $2s$, portanto $n_1 < q < 2s$), ou

$$\nu_q(n_1!) > \frac{n_1}{2q}.$$

Note que, como estamos supondo $n_1 < n_2 < \cdots < n_k$ e $u_m = \sum_{i=1}^{k} a_i n_i!$ temos que $n_1! \mid n_i!$ para todo $i = 1, \ldots, k$ e portanto $n_1! \mid u_m$. Logo,

$$\frac{n_1}{2q} < \nu_q(n_1!) \leq \nu_q(u_m) < C_4 \log^2 m \ \text{ para } \ m > C_5.$$

Portanto,

$$n_1 < 2qC_4 \log^2 m \ \text{ para } \ m > C_5. \tag{3.8}$$

Podemos assumir $C_5 > \max\{e, C_1\}$ e $C_4 > 1$. Seja $C_6 = \max\{C_5, e^{2qC_4}\}$. Assim, se $m > C_6$ então $m > C_5$ e $m > e^{2qC_4}$. De $m > C_5$ temos que vale (3.8) e de $m > e^{2qC_4}$ temos que $\log m > 2qC_4$. Portanto,

$$n_1 < 2qC_4 \log^2 m < \log^3 m \ \text{ para } \ m > C_6. \tag{3.9}$$

Para concluir a prova do teorema, precisamos analisar três casos.

Caso 1: $\text{mdc}(r, s) \neq 1$.

Como $\text{mdc}(r, s) \neq 1$, seja p um primo divisor de $\text{mdc}(r, s)$. Vamos usar indução para mostrar que $n_j < \log^{j+2} m$, para m suficientemente grande.

O caso $j = 1$ é dado pela desigualdade (3.9). Assuma que $n_i < \log^{i+2} m$ para $i = 1, \ldots, j$, onde $1 \leq j \leq k$.

Suponha que

$$N_j = \sum_{i=1}^{j} a_i n_i! = p^x y,$$

onde $p \nmid y$.

Note que nesse caso $x = \nu_p(N_j)$.

Assim,

$$\log_p \left| \sum_{i=1}^{j} a_i n_i! \right| = x + \log_p |y| \geq x,$$

pois $\log_p |y| \geq 0$ já que $y \in \mathbb{Z}$.

Como

$$|N_j| = \left| \sum_{i=1}^{j} a_i n_i! \right| < kAn_j! < kAn_j^{n_j},$$

segue que

$$x \leq \log_p \left| \sum_{i=1}^{j} a_i n_i! \right| < \log_p(kA) + n_j \log_p(n_j),$$

ou seja

$$\nu_p(|N_j|) = \nu_p \left(\left| \sum_{i=1}^{j} a_i n_i! \right| \right) < \frac{n_j \log n_j + \log kA}{\log p}.$$

Usando a hipótese de indução para n_j temos

$$\begin{aligned} \nu_p \left(\left| \sum_{i=1}^{j} a_i n_i! \right| \right) &< \frac{\log^{j+2} m \log\log^{j+2} m}{\log p} + \frac{\log kA}{\log p} \\ &= C_7 + \frac{j+2}{\log p} \log^{j+2} m \log\log m \\ &= C_7 + C_8 \log^{j+2} m \log\log m, \end{aligned}$$

onde $C_7 = \frac{\log kA}{\log p}$ e $C_8 = \frac{j+2}{\log p}$.

Considere $C_9 = C_7 + C_8$ e assuma $m > e^e$. Portanto, temos

$$\nu_p(N_j) = \nu_p \left(\sum_{i=1}^{j} a_i n_i! \right) < C_9 \log^{j+2} m \log\log m. \tag{3.10}$$

Agora, note que pelo Lema 3.9 temos

$$\nu_p(u_m) \geq \left\lfloor \frac{m}{2} \right\rfloor \geq \frac{m-1}{2}.$$

Se

$$\frac{m-1}{2} \leq C_9 \log^{j+2} m \log\log m < C_9 \log^{k+2} m \log\log m,$$

então obtemos $m < C_{10}$ e o teorema está provado.

Vamos considerar então o caso em que

$$\frac{m-1}{2} > C_9 \log^{j+2} m \log\log m.$$

Assim,

$$\nu_p(u_m) \geq \frac{m-1}{2} > C_9 \log^{j+2} m \log\log m > \nu_p \left(\sum_{i=1}^{j} a_i n_i! \right),$$

ou seja,

$$\nu_p(u_m) > \nu_p \left(\sum_{i=1}^{j} a_i n_i! \right). \tag{3.11}$$

Note que

$$u_m - \left(\sum_{i=1}^{j} a_i n_i! \right) = \sum_{i=j+1}^{k} a_i n_i!$$

e portanto

$$n_{j+1}! \mid u_m - \left(\sum_{i=1}^{j} a_i n_i! \right).$$

Assim,

$$\nu_p(n_{j+1}!) \leq \nu_p \left(u_m - \left(\sum_{i=1}^{j} a_i n_i! \right) \right) = \nu_p \left(\sum_{i=1}^{j} a_i n_i! \right),$$

onde a última igualdade vem da desigualdade (3.11) e do fato que se $\nu_p(x) < \nu_p(y)$ então $\nu_p(x+y) = \nu_p(x)$.

Logo, de (3.10) temos $\nu_p(n_{j+1}!) < C_9 \log^{j+2} m \log\log m$, e como $\nu_p(n_{j+1}!) > \frac{n_{j+1}}{2p}$ temos

$$n_{j+1} < 2pC_9 \log^{j+2} m \log\log m. \tag{3.12}$$

Observe que queremos mostrar que $n_{j+1} < \log^{j+3} m$ para m suficientemente grande. Logo, devemos ter na desigualdade (3.12) $2pC_9 \log\log m < \log m$. Para isso, basta escolhermos $C_{11} = \max\{C_6, (4pC_9)^{4pC_9}\}$. Assim, para $m > C_{11}$ temos que

$$n_{j+1} < \log^{j+3} m.$$

Assim, temos completa a indução e vale $n_k < \log^{k+2} m$ e de (3.6) obtemos um limitante superior para m, provando o Teorema.

Caso 2: $s \neq \pm 1$.

Inicialmente, note que pelo caso 1 podemos supor que r e s são coprimos. Além disso, como α e β são raízes de $X^2 - rX - s = 0$ temos que $\alpha\beta = -s \neq \pm 1$, portanto α e β não são unidades, já que $N(\alpha) = N(\beta) = \alpha\beta \neq \pm 1$, onde $N(x)$ é a norma de x em $\mathbb{Q}(\alpha)$.

Considere P um ideal primo de norma p em $\mathbb{Q}(\alpha)$ dividindo o ideal gerado por α.

Vamos provar por indução que $n_j < \log^{3j} m$ para m suficientemente grande. O caso $j = 1$ vale pela desigualdade (3.9) para $m > C_6$. Assuma agora que $n_i < \log^{3i} m$ para $i = 1, 2, \ldots, j$ e $1 \leq j < k$.

Considere $u_m = a\alpha^m + b\beta^m$ e $N_j = \sum_{i=1}^{j} a_i n_i!$.

Já vimos que $|N_j| < kAn_j^{n_j}$, logo

$$\log |N_j| < n_j \log n_j + \log kA,$$

e pela hipótese de indução temos

$$\begin{aligned}\log|N_j| &< \log^{3j} m \log\log^{3j} m + \log kA \\ &= 3j \log^{3j} m \log\log m + \log kA \\ &< C_{12} \log^{3j} m \log\log m, \end{aligned} \tag{3.13}$$

onde $C_{12} = 2 \cdot \max\{3k, \log kA\}$.

Assuma novamente que $m > e^e$. Como $u_m = a_1 n_1! + \cdots + a_k n_k!$, podemos reescrever essa equação como

$$a\alpha^m + b\beta^m - N_j = \sum_{i=j+1}^{k} a_i n_i!.$$

Observe que, como α e β são raízes de $X^2 - rX - s = 0$ temos $\alpha - \beta = \pm\sqrt{r^2 + 4s}$ e o ideal primo P não divide $\alpha - \beta$.

De fato, se P dividisse $\alpha - \beta$ então P dividiria $(\alpha - \beta)^2 = r^2 + 4s$ e, como a norma é multiplicativa, teríamos que $N(P) \mid N(r^2 + 4s) = (r^2 + 4s)^2$, pois $r^2 + 4s \in \mathbb{Z}$. Logo, $p \mid (r^2 + 4s)^2 \Rightarrow p \mid r^2 + 4s$.

Além disso, P divide α e portanto divide $s = -\alpha\beta$. Assim, $N(P)|N(s) \Rightarrow p \mid s^2 \Rightarrow p \mid s$.

Logo, como p divide $r^2 + 4s$ e p divide s, temos que p divide r^2 e portanto p divide r. O que é um absurdo pois r e s são coprimos.

Assim, P não divide o denominador de a e b e portanto

$$\mathrm{ord}_P(a\alpha^m) \geq m. \tag{3.14}$$

Observe que o fato de P não dividir o denominador de a é fundamental para que $\mathrm{ord}_P(a\alpha^m) \geq m$, pois se P dividisse o denominador de a a ordem de $a\alpha^m$ com respeito ao ideal P poderia ser menor que m.

Queremos estimar $\mathrm{ord}_P(a\alpha^m + b\beta^m - N_j) \geq \min\{\mathrm{ord}_P(a\alpha^m), \mathrm{ord}_P(b\beta^m - N_j)\}$. Logo, precisamos estimar $\mathrm{ord}_P(b\beta^m - N_j)$.

Note que

$$\mathrm{ord}_P(b\beta^m - N_j) = \mathrm{ord}_P\left(N_j\left(\frac{b}{N_j}\beta^m - 1\right)\right) = \mathrm{ord}_P(N_j) + \mathrm{ord}_P\left(\frac{b}{N_j}\beta^m - 1\right).$$

Assim, se $\frac{b}{N_j}$ e β são multiplicativamente independentes usamos o Teorema 2.7 para formas lineares p-ádicas em dois logaritmos com $\alpha_1 = \frac{b}{N_j}$, $\alpha_2 = \beta$, $b_1 = 1$ e $b_2 = m$. Note

que $h(\alpha_1) \leq h(b) + h(N_j) = \overline{c_1} \log |N_j|$, onde $\overline{c_1}$ é uma constante que depende de u_m. Além disso, $b' < \overline{c_2} m$, onde $\overline{c_2}$ depende de u_m também. Logo, aplicando o Teorema 2.7 temos

$$\mathrm{ord}_P \left(\frac{b}{N_j} \beta^m - 1 \right) < \overline{c_3} \log^2 m \log |N_j|,$$

onde $\overline{c_3}$ depende apenas de u_m.

Caso $\frac{b}{N_j}$ e β são multiplicativamente dependentes então existem inteiros não nulos x e y tais que

$$\left(\frac{b}{N_j} \right)^x = \beta^y.$$

Daí

$$x \cdot \mathrm{ord}_P \left(\frac{b}{N_j} \right) = y \cdot \mathrm{ord}_P(\beta) = 0,$$

pois P não divide β (pois se dividisse, como divide α, dividiria $\alpha - \beta$, absurdo).

Logo,

$$\mathrm{ord}_P \left(\frac{b}{N_j} \right) = \mathrm{ord}_P(\beta) = 0$$

e podemos usar o Teorema 2.6 com $\alpha_1 = \frac{b}{N_j}$, $\alpha_2 = \beta$, $b_1 = 1$, $b_2 = m$ e $B \geq m$ obtendo

$$\mathrm{ord}_P \left(\frac{b}{N_j} \beta^m - 1 \right) < \overline{c_4} \log^2 m \log |N_j|,$$

onde $\overline{c_4}$ depende apenas de u_m.

Em qualquer caso, temos

$$\mathrm{ord}_P(b\beta^m - N_j) < C_{13} \log^2 m \log |N_j|.$$

Além disso, por (3.13) temos

$$\begin{aligned} \mathrm{ord}_P(b\beta^m - N_j) &< C_{13} \log^2 m C_{12} \log^{3j} m \log \log m \\ &= C_{14} \log^{3j+2} m \log \log m, \end{aligned} \tag{3.15}$$

onde $C_{14} = C_{12} \cdot C_{13}$.

Agora, se $m \leq C_{14} \log^{3j+2} m \log \log m \leq C_{14} \log^{3k+2} m \log \log m$ então é possível limitar m e o Teorema está provado.

Logo, podemos assumir $m > C_{14} \log^{3j+2} m \log \log m$.

Assim, temos

$$\mathrm{ord}_P(a\alpha^m) \geq m > C_{14} \log^{3j+2} m \log \log m > \mathrm{ord}_P(b\beta^m - N_j).$$

E, como $n_{j+1}! \mid u_m - N_j$, pelo mesmo argumento usado no caso 1 temos

$$\begin{aligned} \mathrm{ord}_P(n_{j+1}!) &\leq \mathrm{ord}_P(u_m - N_j) \\ &= \mathrm{ord}_P(a\alpha^m + (b\beta^m - N_J)) \\ &= \mathrm{ord}_P(b\beta^m - N_j) \\ &< C_{14} \log^{3j+2} m \log\log m. \end{aligned}$$

Como, $\nu_p(n_{j+1}!) \leq \mathrm{ord}_P(n_{j+1}!)$ e $\nu_p(n_{j+1}!) > \frac{n_{j+1}}{2p}$ temos

$$n_{j+1} < 2pC_{14} \log^{3j+2} m \log\log m.$$

Portanto, escolhendo $C_{15} = \max\{C_6, (4pC_{14})^{4pC_{14}}\}$ segue que

$$n_{j+1} < \log^{3(j+1)} m \quad \text{para} \quad m > C_{15}.$$

Logo, vale $n_k < \log^{3k} m$ e de (3.6) obtemos um limitante superior para m, provando o teorema.

Caso 3: $s = \pm 1$

Vamos analisar o caso em que $s = -1$ e o caso em que $s = 1$ é análogo. Como $\alpha\beta = -s = 1$ temos que $\beta = \alpha^{-1}$.

Seja p um número primo que não divide o numerador do número racional $N(ab)$ onde a norma é dada em $\mathbb{Q}(\alpha)$.

Vamos mostrar por indução que $n_j < \log^{3j} m$ para m suficientemente grande. Novamente, o caso $j = 1$ é dado pela desigualdade (3.9). Assuma então que $n_i < \log^{3i} m$ para $i = 1, 2, \ldots, j$ e $1 \leq j < k$.

Considerando a mesma notação do caso 2, temos $N_j = \sum_{i=1}^{j} a_i n_i!$ e assim

$$u_m - N_j = a\alpha^m + b\beta^m - N_j = a\beta^m \left(\alpha^{2m} - \frac{N_j}{a}\alpha^m + \frac{b}{a} \right).$$

Logo, podemos escrever

$$u_m - N_j = a\beta^m(\alpha^m - z_1)(\alpha^m - z_2),$$

onde z_1 e z_2 são raízes da equação

$$X^2 - \frac{N_j}{a}X + \frac{b}{a} = 0.$$

Seja P um ideal primo dividindo p em $\mathbb{L} = \mathbb{Q}(\alpha, z_1)$. Queremos estimar

$$\mathrm{ord}_P(u_m - N_j) = \mathrm{ord}_P(a\beta^m) + \mathrm{ord}_P(\alpha^m - z_1) + \mathrm{ord}_P(\alpha^m - z_2).$$

Note que $\mathrm{ord}_P(a\beta^m) = \mathrm{ord}_P(a) + \mathrm{ord}_P(\beta^m)$ e $\mathrm{ord}_P(\beta^m) = 0$ pois β é unidade, já que $N(\beta) = \alpha\beta = 1$.

Além disso, $P \nmid a$, pois se dividisse então $N(P) = p^{f_P}$ dividiria $N(a)$, o que implica que p divide $N(a)$ e portanto p divide $N(ab) = N(a)N(b)$, absurdo. Logo, $\mathrm{ord}_P(a) = 0$.

Resta estimar $\mathrm{ord}_P(\alpha^m - z_i)$ para $i = 1, 2$.

Observe que

$$\mathrm{ord}_P(\alpha^m - z_i) = \mathrm{ord}_P(z_i(\alpha^m z_i^{-1} - 1)) = \mathrm{ord}_P(z_i) + \mathrm{ord}_P(\alpha^m z_i^{-1} - 1).$$

Se α e z_i são multiplicativamente independentes, usamos o Teorema 2.7 com $\alpha_1 = \alpha$, $\alpha_2 = z_i$, $b_1 = m$ e $b_2 = -1$.

E se α e z_i são multiplicativamente dependentes temos que existem constantes não nulas x e y tais que

$$\alpha^x = z_i^y \Rightarrow x \cdot \mathrm{ord}_P(\alpha) = y \cdot \mathrm{ord}_P(z_i) \Rightarrow \mathrm{ord}_P(z_i) = 0,$$

já que α é unidade e $\mathrm{ord}_P(\alpha) = 0$.

Logo, podemos usar o Teorema 2.6.

Em ambos os casos, obtemos

$$\mathrm{ord}_P(\alpha^m z_i^{-1} - 1) < C_{16} \log^2 m \log |N_j|.$$

E portanto,

$$\mathrm{ord}_P(u_m - N_j) < 2C_{16} \log^2 m \log |N_j|.$$

Usando a desigualdade (3.13) temos

$$\mathrm{ord}_P(u_m - N_j) < C_{17} \log^{3j+2} m \log\log m,$$

onde $C_{17} = 2C_{12}C_{16}$.

Analogamente ao caso 2, como $n_{j+1} \mid u_m - N_j$ e $\frac{n_{j+1}}{2p} < \nu_p(n_{j+1}!) < \mathrm{ord}_P(n_{j+1}!)$ temos

$$n_{j+1} < 2pC_{17} \log^{3j+2} m \log\log m.$$

E escolhendo $C_{18} = \max\{C_6, (4pC_{17})^{4pC_{17}}\}$ temos

$$n_{j+1} < \log^{3(j+1)} m \quad \text{para} \quad m > C_{18}.$$

Logo, completamos a indução e $n_k < \log^{3k} m$. Por fim, comparando com (3.6) encontramos um limitante superior para m e temos demonstrado o teorema.

□

Grossman e Luca ainda analisaram as sequências de Fibonacci e de Lucas como soma de fatoriais e obtiveram o seguinte resultado que pode ser encontrado em [8].

Teorema 3.11. *Sejam $(F_n)_{n\geq 0}$ e $(L_n)_{n\geq 0}$ as sequências de Fibonacci e Lucas respectivamente. essas sequências são dadas por $F_0 = 0,\ F_1 = 1,\ L_0 = 2,\ L_1 = 1$ e ambos satisfazem a recorrência $u_{n+2} = u_{n+1} + u_n$. Então, a maior solução da equação*

$$F_m = n_1! \pm n_2!$$

é $F_{12} = 5! + 4!$.

E a maior solução da equação

$$L_m = n_1! \pm n_2!$$

é $L_6 = 4! - 3!$.

Referências Bibliográficas

[1] ALACA, S., WILLIAMS, K. S., *Introductory Algebraic Number Theory*, Cambridge University Press, 2004.

[2] BORWEIN, J., der POORTEN, A., SHALLIT, J., ZUDILIN, W., *Neverending Fractions. An Introduction to Continued Fractions*, 1 ed., 2014.

[3] BUGEAUD, Y.,LAURENT, M., *Minoration effective de la distance p-adique entre puissances de nombres algébriques*, J. Number Theory **61** (1996), 31-42.

[4] COHEN, H., *Number Theory*, Vol. 1, Springer.

[5] DUJELLA, A., *Continued fractions and RSA with small secret exponents*, Tatra Mt. Math. Publ. **29** (2004), 101-112.

[6] DUJELLA, A., IBRAHIMPASIC, B., *On Worley's theorem in Diophantine approximations*, Annales Mathematicae et Informaticae **35** (2008), 61-73.

[7] DUJELLA, A., PETHÖ, A., *A Generalization of a Theorem of Baker and Davenport*, Quart. J. Math. Oxford **49** (1998), no. 3, 291-306.

[8] GROSSMAN, G., LUCA, F., *Sums of Factorials in Binary Recurrence Sequences*, Journal of Number Theory, **93** (2002), 87-107.

[9] HUA, L. K., *Introduction to number theory*, Springer-Verlag, 1982.

[10] LUCA, F., *Effective methods for Diophantine equations*. Disponível em: https://math.dartmouth.edu/archive/m105f12/public_html/lucaHungary1.pdf. Acesso em 01 dez. 2015.

[11] LUCA, F., MARQUES, D., *Perfect powers in the summatory function of the power tower*, J. de Théorie des Nombres de Bordeaux **22** (2010), 581-596.

[12] LUCA, F., *Products of factorials in binary recurrence sequences*, Rocky Mountain J. Math. **29** (1999), No 4, 1387-1411.

[13] MARQUES, D., *Teoria dos Números Transcendentes*, 1 ed., Rio de Janeiro: SBM, 2013.

[14] MARTINEZ, F. B., MOREIRA, C. G., SALDANHA, N., TENGAN, E., *Teoria dos números - um passeio com primos e outros números familiares pelo mundo inteiro*, 2 ed., Rio de Janeiro: IMPA, 2011.

[15] RIBENBOIM, P., *Classical Theory of Algebraic Numbers*, 1 ed., Universitext, 2000.

[16] SLOANE, N. J. A., *The On-Line Encyclopedia of Integers Sequences*, http://www.research.att.com/ njas/sequences/.

[17] WALDSCHMIDT, M., *Diophantine approximation on linear algebraic groups: transcendence properties of the exponential function in several variables*, 1 ed., Grundlehren der mathematischen Wissenschaften, 2000.

[18] WORLEY, R. T., *Estimating* $|\alpha - p/q|$, J. Austral. Math. Soc. Ser. A **31** (1981), 202-206.

[19] WÜSTHOLZ, G., *A Panorama of Number Theory or The View from Baker's Garden*, Cambridge University Press, 2002.

[20] YU, K., *Linear forms in p-adic logarithms III*, Compositio Math. **91** (1994), No 3, 241-276.

[21] YU, K., *p-adic logarithmic forms and group varieties II*, Acta Arith. **89** (1999), 337-378.