Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Sobre Problemas Envolvendo Números de k-bonacci e Coeficientes Fibonomiais

por

Gérsica Valesca Lima de Freitas

Orientador: Diego Marques

Brasília
2017

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

Fs

Freitas, Gérsica
Sobre problemas envolvendo números de k-bonacci e coeficientes fibonomiais / Gérsica Freitas; orientador Diego Marques. -- Brasília, 2017.
67 p.

Tese (Doutorado - Doutorado em Matemática) -- Universidade de Brasília, 2017.

1. sequência de Fibonacci. 2. equações diofantinas. 3. coeficiente fibonomial. 4. período de Pisano. 5. formas Lineares em logaritmos. I. Marques, Diego , orient. II. Título.

Aos meus avós,

Antônia de Lima Moura, Lenilda Paiva de Freitas, Salomão Barbosa de Freitas

e a meus pais, Gilvanusa de Lima Moura e Leomax Paiva de Freitas.

Sobre problemas envolvendo números de k-bonacci e coeficientes fibonomiais

por

Gersica Valesca Lima de Freitas

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

DOUTOR EM MATEMÁTICA

Brasília, 20 de setembro de 2017.

Comissão Examinadora:

Prof. Dr. Diego Marques Ferreira (Orientador)

Prof. Dr. Hemar Teixeira Godinho– MAT/UnB

Prof. Dr. José Plínio de Oliveira — UNICAMP

Profa. Dra. Ana Paula de Araújo Chaves — UFG

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

Agradecimentos

Inicialmente a Deus, por esta grande oportunidade de evoluir e por nas horas difíceis me carregar em seus braços.

Aos meus avôs que sempre cuidaram de mim e me deram a melhor educação possível. Se não fosse por eles, acreditando em mim, nunca teria apostado em mim mesma. Aos meus pais que do jeito deles sempre me apoiaram.

Aos professores da banca que aceitaram e enriqueceram meu trabalho com suas orientações. Ao professor "Gugu"que me recepcionou maravilhosamente no IMPA e me ajudou em um lema.

Aos meus professores que sempre estiveram prontamente e pacientemente me auxiliando nessa caminhada. Em especial aos professores que tive oportunidade de fazer disciplina na UNB, isto é, aos professores Luíz Miranda, Ziazheng Zhou, Hemar Gondinho e Diego Marques. Ao professor Hemar eu deixo meu agradecimento mais especial, nunca vou esquecer a recepção feita por ele. Me fez sentir que a teoria dos números aqui é uma família.

Ao meu orientador Professor Doutor Diego Marque segue um agradecimento exclusivo. Ele foi de uma importância singular no meu amadurecimento na pesquisa matemática. Agradeço por todas oportunidades de aprender e pesquisar. Além dos vários ensinamentos não matemáticos na praia de Copacabana. Após tanta convivência no último ano já o

considero um amigo.

Aos amigos adquiridos durante essa jornada, Alex, Marcelo, Ricardo, Emerson, Jacqueline, Paulo Henrique, Filipe, Yerko, Joel, Alan, Lais, Cid, Dióscoro, Martino, Juliana, Yuri, Antônio, Henrique, Michael e Alessandra. Em especial aos irmãozinhos da área Daiane, Elaine, Josimar, Carol e Bruno. Em particular à Lucimeire e Jean irmãozinhos sempre presentes e preocupados comigo.

A minha família pedregal que sempre estive comigo, mesmo com toda essa distância, Eudes Mendes, Renato, Lily, Rafinha, Nacib, Mariana, Tony, Mônica, Mylenna e Wanderson. Essas pessoas e algumas outras foram anjos que Deus me mandou para preencher meu coração. Elas fizeram melhor e tomaram conta de tudo.

Aos meu amigos de infância que sempre me apoiam em tudo que faço, Many, Gyl Dayana, Gilmar, Jessica, Priscila e Ricardo. Aos meus amigos de Campina Grande, Mel, Ewerton e Larissa.

A Luan Diego, se não fosse por você nunca teria vindo fazer doutorado aqui. Muito obrigada por me induzir a isso e por me ajudar na adaptação.

Por fim, as pessoas que foram muito importantes em fazer Brasília uma casa pra mim. Toda a galera das 23:00 da "smart"em especial a um anjo chamado Mônica e a minha "esposa" Camila que eu sempre soube que eramos almas irmãs só tinha detalhes nos separando. Se eu gosto hoje dessa cidade é graças a vocês.

Ao CNPq e CAPES pelo apoio financeiro concedido durante a realização desta Tese.

"Um problema que vale a pena ser atacado
prova seu valor contra-atacando."

Piet Hein

Resumo

Os números de Fibonacci possui várias generalizações, entre elas temos a sequência $(F_n^{(k)})_n$ que é chamada de sequência de Fibonacci k-generalizada. Observando a identidade $F_n^2 + F_{n+1}^2 = F_{2n+1}$, Chaves e Marques, em 2014, provaram que a equação Diofantina $(F_n^{(k)})^2 + (F_{n+1}^{(k)})^2 = F_m^{(k)}$ não possui soluções em inteiros positivos n, m e k, com $n > 1$ e $k \geq 3$. Nesse trabalho, mostramos que a equação Diofantina $(F_n^{(k)})^2 + (F_{n+1}^{(k)})^2 = F_m^{(l)}$, não possui solução para $2 \leq k < l$ e $n > k + 1$. Outra generalização da sequência de Fibonacci são os coeficientes fibonomiais. Em 2015, Marques e Trojovský provaram que se $p \equiv \pm 1 \pmod 5$, então $p \nmid \begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F$, para todo $a \geq 1$. Nesse trabalho, encontramos as classe de resíduos de $\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F$ módulo p, p^2, p^3 e p^4, quando $p \equiv \pm 1 \pmod 5$ e sobre uma condição mais fraca. Em particular, provamos que se p é um número primo tal que $p \equiv \pm 1 \pmod 5$, então $\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 \pmod p$.

Palavras-chave: sequência de Fibonacci, formas Lineares em logaritmos, método de redução, equações diofantinas, coeficiente fibonomial, período de Pisano.

Abstract

The Fibonacci numbers have several generalizations, between them we have the sequence $(F_n^{(k)})_n$ which is called the generalized Fibonacci sequence. Regarding the identity $F_n^2 + F_{n+1}^2 = F_{2n+1}$, Chaves and Marques, in 2014, proved that $(F_n^{(k)})^2 + (F_{n+1}^{(k)})^2 = F_m^{(k)}$, does not have solution for integers n, m and k, with $n > 1$ and $k \geq 3$. In this work, we show that $(F_n^{(k)})^2 + (F_{n+1}^{(k)})^2 = F_m^{(l)}$ does not have solutions for $2 \leq k < l$ and $n > k + 1$. Another generalization of the Fibonacci sequence is the Fibonomial coefficients. In 2015, Marques and Trojovský proved that if $p \equiv \pm 1 \pmod 5$, then $p \nmid \begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F$, for all $a \geq 1$. In this work, we also find the residue class of $\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F$ modulo p, p^2, p^3 and p^4, when $p \equiv \pm 1 \pmod 5$, under some weak hypothesis. In particular, we proved that if p is a prime number such that $p \equiv \pm 1 \pmod 5$, then $\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 \pmod p$.

Keywords: Fibonacci sequence, linear forms in logarithms, reduction method, Diophantine equations, Fibonomial coefficients, Pisano period

Sumário

Introdução **1**

1 Preliminares **6**

1.1 Sequências recorrentes 6

1.2 Generalizações da sequência de Fibonacci 10

1.2.1 Sequência de Fibonacci k-generalizada 10

1.2.2 Coeficiente fibonomial 12

1.3 Formas lineares em logaritmos 13

1.4 Método de redução 14

1.5 Outras definições e resultados auxiliares 14

1.5.1 Congruência em $\mathbb{Q}$ 14

1.5.2 Funções simétricas 15

1.5.3 Lemas chaves 16

2 Quando a Soma de Quadrados de Dois Números Consecutivos de k-bonacci é Um Número de l-bonacci **19**

2.1 Uma limitação superior para m e n em termos de l 20

2.2 O caso l grande 24

2.2.1 O caso $n < 2^{k/2}$ 26

2.2.2 O caso $2^{k/2} < n$ 28
2.3 Prova do teorema principal 30

3 Resto da divisão de $\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F$ por p^k para $k = 1, 2, 3$ e 4 **33**
3.1 Resto do coeficiente fibonomial módulo p 33
3.2 Resto do coeficiente fibonomial módulo p^2 36
3.3 Resto do coeficiente fibonomial módulo p^3 38
3.4 Resto do coeficiente fibonomial módulo p^4 45

Referências **54**

Introdução

Um importante matemático grego do século III a.C. foi Diofanto de Alexandria. Considerado por muitos estudiosos como o "pai da álgebra", Diofanto está para a Aritmética como Euclides está para a Geometria, ou Ptolomeu para a Astronomia. Ele escreveu vários outros livros além de Arithmetica, mas muito poucos resistiram ao tempo. O mesmo se refere a um trabalho que consiste de uma coleção de lemas chamado *The Porisms (ou Porismata)*, mas este livro foi inteiramente perdido. Embora o "The Porisms" está perdido, sabemos de três lemas contidos lá, uma vez que seu autor se refere a eles em Arithmetica.

Diofanto ficou famoso pelas suas coleções de problemas envolvendo equações com soluções geniais. Por esse motivo, as equações onde buscamos soluções inteiras são chamadas de *equações Diofantinas*. Mais precisamente, uma equação Diofantina é uma equação do tipo $f(x_1, x_2, \ldots, x_n) = 0$, onde f é uma função em n variáveis e procuramos soluções $(x_1, \ldots, x_n) \in \mathbb{Z}^n$. Uma das equações Diofantinas mais famosas é $x^n + y^n = z^n$, que é conhecida como *equação de Fermat* e foi considerada pelo mesmo quando ele lia o livro Arithmetica, onde o autor discutia as soluções da equação $x^2 + y^2 = z^2$(conhecida como *equação de Pitágoras*). Existem infinitos números inteiros que satisfazem esta equação (caso $n = 2$ da equação de Fermat), por exemplo $(3k, 4k, 5k)$, para todo $k \geq 1$. Fer-

mat sugeriu que não existem soluções em inteiros não nulos, para $n > 2$. A prova dessa afirmação (chamado "O Último Teorema de Fermat") foi dada por Andrew Wiles no ano de 1994.

No ocidente, a sequência de Fibonacci apareceu pela primeira vez no livro *Liber Abaci* (1202) de Leonardo Fibonacci, embora ela já tivesse sido descrita por gregos e indianos. Fibonacci considerou o crescimento de uma população idealizada (não realista biologicamente) de coelhos. Os números descrevem o número de casais na população de coelhos depois de n meses se for suposto que:

- No primeiro mês temos apenas um casal e casais amadurecem sexualmente (e reproduzem-se) apenas após o segundo mês de vida.
- Não há problemas genéticos no cruzamento consanguíneo.
- Todos os meses, cada casal fértil dá a luz a um novo casal, e os coelhos nunca morrem.

Logo, cada F_n vai contabilizar o número de casais no mês n, para cada $n \in \mathbb{N}$. Formalmente, a sequência de Fibonacci, $(F_n)_n$, é definida por $F_{n+2} = F_{n+1} + F_n$, para todo $n \geq 1$, e com valores iniciais $F_1 = 1$ e $F_2 = 1$. Os primeiros números da sequência são:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, \ldots.$$

Os números de Fibonacci são conhecidos por satisfazerem várias identidades, alguns exemplos são $F_n^2 - F_{n-2}^2 = F_{2n-2}$ e $F_{n+1}^2 - F_n^2 = F_{n-1}F_{n+2}$. Temos interesse na seguinte identidade

$$F_n^2 + F_{n+1}^2 = F_{2n+1}, \tag{1}$$

para todo $n \geq 0$. Em particular essa identidade, que pode ser provada por indução, nos diz que a soma do quadrados de dois números de Fibonacci consecutivos ainda é um número de Fibonacci.

Em 2010, Marques e Togbé, em [18], mostraram que para um s fixo, se $F_n^s + F_{n+1}^s$ é um número de Fibonacci para infinitos n, então $s = 1$ ou 2. No ano seguinte, Luca e Oyono, em [16], resolveram o problema completamente mostrando que a equação Diofantina

$$F_n^s + F_{n+1}^s = F_m,$$

não tem solução (n, m, s) com $n \geq 2$ e $s \geq 3$.

Uma generalização dos números de fibonacci é dada pela seguinte definição.

Definição 0.1. *Para cada inteiro $k \geq 2$ a sequência de Fibonacci k-generalizada ou sequência k-Fibonacci, $F^{(k)} := (F_n^{(k)})_{n \geq 2-k}$, é dada pela recorrência*

$$F_n^{(k)} = F_{n-1}^{(k)} + \cdots + F_{n-k}^{(k)},$$

para todo $n \geq 2$ e com valores iniciais $F_{-(k-2)}^{(k)} = F_{-(k-3)}^{(k)} = \cdots = F_0^{(k)} = 0$ e $F_1^{(k)} = 1$.

Em 2014, Chaves e Marques, em [7], estudaram uma generalização da equação (1) e mostraram que a equação Diofatina

$$(F_n^{(k)})^2 + (F_{n+1}^{(k)})^2 = F_m^{(k)}, \tag{2}$$

não possui soluções em inteiros positivos n, m e k, com $n > 1$ e $k \geq 3$. No mesmo ano, Luca e Gómez, em [32], mostraram que a equação

$$(F_n^{(k)})^s + (F_{n+1}^{(k)})^s = F_m^{(k)},$$

não possui soluções em inteiros positivos quando $k \geq 3$, $n \geq 2$ e $s \geq 2$.

Um dos focos de nosso trabalho é determinar os números da forma $(F_n^{(k)})^2 + (F_{n+1}^{(k)})^2$ que são números de l-bonacci. Com essa generalização da equação (2) conseguimos observar que, mesmo adicionando esse grau de liberdade vale:

Teorema 0.1. *A equação Diofantina*

$$(F_n^{(k)})^2 + (F_{n+1}^{(k)})^2 = F_m^{(l)},$$

não possui solução para $2 \leq k < l$ e $n > k + 1$.

Em 1975, Erdös conjecturou que 2^k nunca é a soma de potências distintas de 3, para todo $k > 8$. Por exemplo, $2^8 = 3^5 + 3^2 + 3 + 1$. Se isso for verdade, então $3 \mid \binom{2^{k+1}}{2^k}$, para $k \geq 9$.

Em 1915, Fontené publicou uma nota de uma página, em [11], sugerindo uma generalização dos coeficientes binomiais que é feita substituindo cada número natural por termos de uma sequência (A_n) arbitrária de números reais ou complexos.

Desde 1960, existe muito interesse em estudar essa generalização quando a sequência é a de números de Fibonacci. Mais precisamente,

Definição 0.2. *O coeficiente Fibonomial é definido como*

$$\begin{bmatrix} m \\ k \end{bmatrix}_F = \frac{F_{m-k+1} \cdots F_{m-1} F_m}{F_1 \cdots F_k},$$

para todo $1 \leq k \leq m$ *e quando* $k > m$ *definimos* $\begin{bmatrix} m \\ k \end{bmatrix}_F = 0$.

Observe que $p \mid \binom{p^{a+1}}{p^a}$, para todo primo p. Isso decorre claramente do fato de que

$$\binom{p^{a+1}}{p^a} = p\binom{p^{a+1}-1}{p^a-1}.$$

Nesse espírito, em 2012, Marques e Trojovský estudaram a generalização deste fato no caso fibonomial. Eles provaram, em [25] e [26], que $p \mid \begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F$ para todo $a \geq 1$ e $p \in \{2, 3\}$. Posteriormente, Marques, Sellers e Trojovský, em [27], provaram que o número $\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F$ é divisível por p para todo primo p tal que $p \equiv \pm 2 \pmod 5$ e para todo inteiro $a \geq 1$. Marques e Trojovský, em [28], também provaram que se $p \equiv \pm 1 \pmod 5$, então $p \nmid \begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F$ para todo inteiro $a \geq 1$. Além disso, no mesmo artigo eles encontraram o maior expoente de p que divide $\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}$ quando $p \equiv \pm 2 \pmod 5$.

O outro objetivo desse trabalho é encontrar a classe de resíduos de $\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F$ módulo p, p^2, p^3 e p^4 quando $p \equiv \pm 1 \pmod 5$. Provaremos os seguintes resultados:

Teorema 0.2. *Seja* p *um primo tal que* $p \equiv \pm 1 \pmod 5$. *Então*

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 \pmod p,$$

para todo $a \geq 0$.

Provaremos ainda que

Teorema 0.3. *Seja* p *um primo tal que* $z(p) = p - 1$, *onde* $z(p) = \min\{k \in \mathbb{N};\ p \mid F_k\}$. *Então para* $k \in \{2, 3, 4\}$, *temos*

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 + p + \cdots + p^{k-1} \pmod{p^k},$$

para todo $a \geq k$.

Na demonstração do teorema anterior, o leitor vai observar que para cada k vão aparecer novas dificuldades que foram contornadas a partir de ferramentas diferentes da matemática.

Por fim, deixamos uma conjectura relacionada ao teorema anterior

Conjectura 0.1. *Seja p um primo tal que $z(p) = p - 1$. Então*

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 + p + \cdots + p^{k-1} \pmod{p^k}.$$

para todo $a,\ k \in \mathbb{N}$ tais que $a \geq k$.

CAPÍTULO 1

Preliminares

1.1 Sequências recorrentes

Sequências recorrentes são sequências $(u_n)_n$ nas quais cada termo é determinado em função de termos anteriores. Particularmente trabalhamos com as que são lineares e com coeficientes inteiros, isto é, quando existem $c_1, \ldots, c_k \in \mathbb{Z}$ tais que

$$u_{n+k} = c_1 u_{n+k-1} + \cdots + c_k u_n, \ \forall \ n \geq 0. \tag{1.1}$$

Note que esse tipo de sequência fica unicamente determinada pela escolha dos k valores iniciais $u_1, \ldots, u_k$. Nesse caso dizemos que $(u_n)_n$ é uma *sequência recorrente linear de ordem k* (supondo que $c_k \neq 0$). Exemplos dessas sequências são as *progressões geométricas* e as *progressões aritméticas*.

Dois exemplos muito importantes dessas sequências são: A sequência de Fibonacci, $(F_n)_n$, que é uma sequência recorrente linear de ordem 2, e satisfaz $F_{n+2} = F_{n+1} + F_n$ para todo $n \geq 0$, onde $F_0 = 0$ e $F_1 = 1$. Outro exemplo é a sequência de Lucas, $(L_n)_n$,

que é uma sequência recorrente linear cuja relação de recorrência é a mesma da sequência de Fibonacci, ou seja, $L_{n+2} = L_{n+1} + L_n$, para todo $n \geq 0$, onde $L_0 = 2$ e $L_1 = 1$.

Um fato interessante sobre essas sequências é que existe uma forma fechada explícita para o seu n-ésimo termo, mas primeiro vamos exibir algumas definições necessárias.

Definição 1.1. *O polinômio característico de uma sequência $(u_n)_n$, satisfazendo (1.1) é dado por*

$$P(x) = x^k - c_1 x^{k-1} - \cdots - c_{k-1}x - c_k,$$

onde denotamos por $\lambda_1, \lambda_2, \ldots, \lambda_r$ suas raízes complexas com multiplicidades $a_1, a_2, \ldots, a_r$, respectivamente.

Por exemplo, o polinômio característico da sequência de Fibonacci é $P(x) = x^2 - x - 1$ cujas raízes são $(1 + \sqrt{5})/2$ e $(1 - \sqrt{5})/2$.

Um importante resultado sobre sequências recorrentes lineares, que pode ser encontrado em [29], afirma que para todo $n \in \mathbb{N}$, temos

$$u_n = Q_1(n)\lambda_1^n + Q_2(n)\lambda_2^n + \cdots + Q_r(n)\lambda_r^n,$$

onde $Q_1, \ldots, Q_r$ são polinômios sobre o corpo $\mathbb{Q}(\lambda_1, \ldots, \lambda_r)$ com grau $\deg(Q_i) < a_i$, para todo $i \in [1, r]$. Note que, a partir daqui denotaremos o conjunto $\{a, a+1, \ldots, b\}$ por $[a, b]$, com $a, b \in \mathbb{Z}$ e $a < b$.

No caso da sequência de Fibonacci temos que

$$F_n = c_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + c_2 \left(\frac{1-\sqrt{5}}{2}\right)^n,$$

onde $c_i = (-1)^{i+1}/\sqrt{5}$. A fórmula anterior é conhecida como *fórmula de Binet* (apesar de ser um resultado já conhecido por Euler, D. Bernoulli, e De Moivre mais de um século antes).

Enunciaremos abaixo algumas propriedades da sequência de Fibonacci e que serão primordiais para as demonstrações do terceiro capítulo.

Lema 1.1.1. *Temos,*

(a) (Fórmula da Adição) $F_{m+n} = F_{m-1}F_n + F_m F_{n+1}$.

(b) (Fórmula de múltiplos ângulos) $F_{kn+c} = \sum_{i=0}^{k} \binom{k}{i} F_{c-i} F_n^i F_{n+1}^{k-i}$.

(c) $F_n \mid F_m$ *se, e somente se,* $n \mid m$.

(d) (Identidade de d'Ocagne) $(-1)^n F_{m-n} = F_m F_{n+1} - F_n F_{m+1}$.

(e) Para todo p *primo,* $F_{p-(5/p)} \equiv 0 \pmod{p}$*, onde* $(\frac{a}{q})$ *denota o símbolo de Legendre de* a *com respeito a um primo* $q > 2$.

Para uma demonstração dos itens (c), (d) e (e) do lema anterior veja [27, Lemma 2.1].

Em 1774, Lagrange observou que para qualquer inteiro n, a sequência de números de Fibonacci módulo n é periódica.

Definição 1.2. *O período de Pisano, denotado por* $\pi(n)$*, é o menor período da sequência de Fibonacci módulo* n.

Alguns valores do período de Pisano são:

$$1, 3, 8, 6, 20, 24, 16, 12, 24, 60, \ldots$$

Propriedade 1.1. *Temos,*

(1) Com exceção de $\pi(2) = 3$*, o período de Pisano é sempre par.*

(2) Se $(m, n) = 1$*, então* $\pi(m \cdot n) = mmc(\pi(m), \pi(n))$ *(pelo teorema do resto chinês).*

(3) Se p *é primo, então* $\pi(p^k)$ *divide* $p^{k-1}\pi(p)$*. É conjecturado que* $\pi(p^k) = p^{k-1}\pi(p)$ *para todo* p *primo e* $k > 1$.

(4) Se $n = 2k$*, então* $\pi(n) = 3 \cdot 2^{k-1} = 3n/2$*. Se* $n = 5^k$*, então* $\pi(n) = 20 \cdot 5^{k-1} = 4n$*. Daí, se* $n = 2 \cdot 5^k$*, então* $\pi(n) = 6n$.

(5) Se $n \equiv a \pmod{\pi(p)}$*, então* $F_n \equiv F_a \pmod{p}$.

(6) Seja $p \neq 2$ *e* 5 *primo. Se* $p \equiv \pm 1 \pmod{10}$*, então* $\pi(p)$ *divide* $p - 1$*. Se* $p \equiv \pm 3 \pmod{10}$*, então* $\pi(p)$ *divide* $2(p + 1)$.

Definição 1.3. *A ordem de aparição de* n *na sequência de Fibonacci, denotada por* $z(n)$*, é definida como o menor inteiro positivo* k*, tal que* $n \mid F_k$.

Existem vários resultados sobre $z(n)$ na literatura. Por exemplo, Marques, em [19, 20, 21, 22, 23], encontrou todos os pontos fixos de $z(n)$ e também fórmulas fechadas para essa função em alguns inteiros relacionados à sequência de Fibonacci.

Lema 1.1.2. *Se $n \mid F_m$, então $z(n) \mid m$.*

Uma demonstração do lema anterior pode ser encontrada em [19, Lemma 2.2].

Observação 1.1.1. *Note que o Lema 1.1.1 (e) junto com o Lema 1.1.2 implica que $z(p) \mid p - (5/p)$ para todo primo $p \neq 5$. Logo, $z(5) = 5$ e*

- *$z(p) \mid p + 1$ se $p \equiv \pm 2 \pmod 5$,*
- *$z(p) \mid p - 1$ se $p \equiv \pm 1 \pmod 5$.*

Lema 1.1.3. *Para todo primo $p \neq 5$, temos que $(z(p), p) = 1$.*

Uma demonstração do lema pode ser encontrada em [20, Lemma 2.3].

Na próxima definição apresentamos uma ferramenta matemática crucial para nosso segundo problema.

Definição 1.4. *A valorização p-ádica (ou a ordem) de a, $\nu_p(a)$, é o expoente da maior potência do primo p que divide a.*

Agora vamos enunciar algumas propriedades sobre valorização p-ádica.

Propriedade 1.2. *Sejam $a, b \in \mathbb{Z}^*$. Temos*

(1) $\nu_p(ab) = \nu_p(a) + \nu_p(b)$,

(2) $\nu_p(a/b) = \nu_p(a) - \nu_p(b)$,

(3) $\nu_p(a + b) \geq \min\{\nu_p(a), \nu_p(b)\}$ *e vale a igualdade se* $\nu_p(a) \neq \nu_p(b)$.

O lema a seguir mostra algumas fórmulas de valorização p-ádica e sua prova pode ser encontrada em [9, p. 263].

Lema 1.1.4. *Escreva* $n_0 + n_1 p + n_2 p^2 + \cdots$ *para a expansão p-ádica de um inteiro* $n \geq 1$. *Então,*

(a) (Fórmula de De Polignac) $\nu_p(n!) = \sum_{k\geq 1} \lfloor \frac{n}{p^k} \rfloor = \frac{n-(n_0+n_1+n_2+\cdots)}{p-1}$,

(b) $\nu_p\left(\binom{p^n}{k}\right) = n - \nu_p(k)$, *para todo* $k \geq 1$.

A proposição abaixo apresenta o valor da valorização p-ádica de cada termo da sequência de Fibonacci. Uma prova de um resultado mais geral pode ser encontrada em [15, p. $236 - 237$ e section 5].

Proposição 1.1.1. *Se* $n \geq 1$ *e* $p \neq 2$ *e* 5, *então*

$$\nu_2(F_n) = \begin{cases} 0, & se \quad n \equiv 1, 2 \pmod 3 \\ 1, & se \quad n \equiv 3 \pmod 6 \\ 3, & se \quad n \equiv 6 \pmod{12} \\ \nu_2(n) + 2, & se \quad n \equiv 0 \pmod{12} \end{cases}$$

$\nu_5(F_n) = \nu_5(n)$, *e se o primo* $p \neq 2, 5$, *então*

$$\nu_p(F_n) = \begin{cases} \nu_p(n) + e(p), & se \quad n \equiv 0 \pmod{z(p)} \\ 0, & se \quad n \not\equiv 0 \pmod{z(p)}, \end{cases}$$

onde $e(p) = \nu_p(F_{z(p)})$.

Uma consequência da proposição anterior é que, se p é primo e $z(p) \mid m$, então $p \mid F_m$.

1.2 Generalizações da sequência de Fibonacci

Ao decorrer do tempo várias generalizações dos números de Fibonacci foram dadas. Nesse trabalho temos interesse nas seguintes.

1.2.1 Sequência de Fibonacci k-generalizada

Para cada inteiro $k \geq 2$ a sequência de Fibonacci k-generalizada ou sequência k-bonacci, $F^{(k)} := (F_n^{(k)})_{n \geq 2-k}$, é dada pela recorrência

$$F_n^{(k)} = F_{n-1}^{(k)} + \cdots + F_{n-k}^{(k)}, \tag{1.2}$$

para todo $n \geq 2$ e com valores iniciais $F_{-(k-2)}^{(k)} = F_{-(k-3)}^{(k)} = \cdots = F_0^{(k)} = 0$ e $F_1^{(k)} = 1$.

Note que essa generalização é de fato uma família de sequências, onde cada escolha de k produz uma sequência distinta. Por exemplo, a usual sequência de Fibonacci, $(F_n)_n$, é obtida para $k = 2$ e para os valores posteriores de k essas sequências são chamadas de Tribonacci, Tetranacci, Pentanacci, Hexanacci, Heptanacci, Octanacci e assim por diante.

Em 2012, Bravo e Luca estudaram a equação Diofantina $F_n^{(k)} = 2^m$, em [1], e mostraram que as únicas potências de dois nessa sequência são os primeiros $k+1$ termos não nulos, isto é,

$$F_1^{(k)} = 1,\ F_2^{(k)} = 1,\ F_3^{(k)} = 2,\ F_4^{(k)} = 4, \ldots, F_{k+1}^{(k)} = 2^{k-1},$$

enquanto que o próximo termo da sequência é $F_{k+2}^{(k)} = 2^k - 1$.

Outra informação importante sobre essa sequência é o seu polinômio característico. À saber, o polinômio característico de $F_n^{(k)}$ é

$$\phi_k(x) = x^k - x^{k-1} - x^{k-2} - \cdots - x - 1,$$

e é irredutível sobre $\mathbb{Q}[x]$. Como foi observado, em [34, Corollary 3.5], esse polinômio possui uma única raiz, α, fora do círculo unitário. Ao longo desse trabalho, α será a raiz dominante de $\phi_k(x)$, que é um número de Pisot de grau k. Além disso, conhecemos o seguinte fato sobre essa raiz, descoberto pelo Wolfram em [34, Lemma 3.6].

Fato 1.2.1. (Lema de Wolfram) *Para todo $k \geq 2$, temos*

$$2(1 - 2^{-k}) < \alpha < 2.$$

Agora, consideramos para um inteiro $k \geq 2$, a função

$$g(x, k) = \frac{x - 1}{2 + (k+1)(x-2)}, \tag{1.3}$$

para todo $x > 2(1-2^{-k})$. Com essa notação Dresden e Du, em [8, Theorem 1], obtiveram a seguinte fórmula, chamada de "Binet-like formula",

$$F_n^{(k)} = \sum_{i=1}^{k} g(\alpha_i, k)\alpha_i^{n-1}, \tag{1.4}$$

onde $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_k$ são os zeros de $\phi_k(x)$. Nesse mesmo artigo foi mostrado que a contribuição dos zeros que estão dentro do círculo unitário, para a fórmula (1.4), é muito pequena, mais precisamente,

$$|F_n^{(k)} - g(\alpha_i, k)\alpha_i^{n-1}| < \frac{1}{2}, \tag{1.5}$$

para todo $n > k - 1$.

Outro fato importante foi provado por Bravo e Luca, em [4, Lemma 1], e nos dá a seguinte estimativa para o $F_n^{(k)}$.

Fato 1.2.2. (Lema Bravo-Luca) *Para todo $k \geq 2$ temos que*

$$\alpha^{n-2} \leq F_n^{(k)} \leq \alpha^{n-1},$$

para todo $n \geq 1$.

1.2.2 Coeficiente fibonomial

Nessa seção introduzimos uma generalização dos coeficientes binomiais, sugerida em 1915 por Fontené, ver [11]. Essa generalização se baseia em substituir cada número natural por termos da sequência de Fibonacci. Desde 1960, existe muito interesse em estudar essa generalização. Mais precisamente,

Definição 1.5. *O coeficiente fibonomial é definido como*

$$\begin{bmatrix} m \\ k \end{bmatrix}_F = \frac{F_{m-k+1} \ldots F_{m-1} F_m}{F_1 \ldots F_k},$$

para todo $1 \leq k \leq m$ e para $k > m$, definimos $\begin{bmatrix} m \\ k \end{bmatrix}_F = 0$.

Observação 1.2.1. *Podemos provar por indução que $\begin{bmatrix} m \\ k \end{bmatrix}_F \in \mathbb{Z}$. Para isso usamos a seguinte identidade*

$$\begin{bmatrix} m \\ k \end{bmatrix}_F = F_{k+1} \begin{bmatrix} m-1 \\ k \end{bmatrix}_F + F_{m-k-1} \begin{bmatrix} m-1 \\ k-1 \end{bmatrix}_F,$$

que é uma consequência de $F_m = F_{k+1}F_{m-k} + F_k F_{m-k-1}$.

1.3 Formas lineares em logaritmos

Seja η um número algébrico de grau d com polinômio primitivo minimal sobre os inteiros

$$a_0x^d + a_1x^{d-1} + \cdots + a_d = a_0\prod_{i=1}^{d}(x - \eta^{(i)}),$$

onde o coeficiente líder a_0 é positivo e os $\eta^{(i)}$'s são os conjugados algébricos de η. Então a altura logaritmica de η é dada por

$$\mathsf{h}(\eta) = \frac{1}{d}\Big(\log a_0 + \sum_{i=1}^{d}\log(\max\{|\eta^{(i)}|, 1\}\Big).$$

Em particular, se $\eta = p/q$ é um número racional irredutível, então $\mathsf{h}(\eta) = \log\max\{|p|, |q|\}$. A função altura logaritmica possui as seguintes propriedades. Sejam η e γ números algébricos, então

- $\mathsf{h}(\eta \pm \gamma) \leq \mathsf{h}(\eta) + \mathsf{h}(\gamma) + \log 2$,
- $\mathsf{h}(\eta\gamma^{\pm 1}) \leq \mathsf{h}(\eta) + \mathsf{h}(\gamma)$,
- $\mathsf{h}(\eta^s) = |s|\mathsf{h}(\eta)$, *para todo* $s \in \mathbb{Z}$.

O próximo lema nos dá uma estimativa de $g(\alpha, k)$, sua demonstração pode ser encontrada em [5, Lemma 2].

Lema 1.3.1. *Para todo $k \geq 2$, seja α a raiz dominante de $F_n^{(k)}$, e considere a função definida anteriormente $g(x, k)$. Então*

(a) Se $i \in [2, k]$, então $1/2 < g(\alpha, k) < 3/4$ e $|g(\alpha_i, k)| < 1$.

(b) Temos que $\mathsf{h}(g(\alpha, k)) < 4\log k$.

Uma ferramenta muito importante que vamos utilizar em nosso primeiro problema é uma limitação inferior para formas lineares logaritmicas *à la Baker*. O próximo teorema nos dá uma limitação assim e é devido a Matveev.

Teorema 1.1. (Matveev) *Suponha que $\gamma_1, \ldots, \gamma_t$ são números algébricos reais positivos em um corpo de números algébricos $\mathbb{K}$ de grau D, e $b_1, \ldots, b_t \in \mathbb{Z}$ tais que $\Lambda := \gamma_1^{b_1} \ldots \gamma_t^{b_t} - 1$ é não nulo. Então*

$$|\Lambda| > \exp(-1.4 \times 30^{t+3} \times t^{4.5} \times D^2(1 + \log D)(1 + \log B)A_1 \cdots A_t),$$

onde $B \geq \max\{|b_1|, \ldots, |b_t|\}$, e $A_i \geq \max\{D\mathsf{h}(\gamma_i), |\gamma_i|, 0.16\}$, para todo $i \in [1, t]$.

Para uma demonstração desse teorema ver [30] ou [6, Theorem 9.4].

1.4 Método de redução

Em 1998, Dujella e Pethö, em [10, Lemma 5 (a)], apresentam uma versão do método de redução baseado no Lema de Baker-Davenport. Apresentamos o lema seguinte, que é uma variação imediata do resultado devido a Dujella e Pethö, que será uma ferramenta chave no nosso trabalho desempenhando a função de diminuir drasticamente os limitantes das variáveis da equação Diofantina trabalhada aqui.

Lema 1.4.1. *Seja M um inteiro positivo e seja p/q um convergente da fração contínua do número irracional γ tal que $q > 6M$. Sejam A, B, μ números reais com $A > 0$ e $B > 1$. Defina $\epsilon = \|\mu q\| - M\|\gamma q\|$ (onde $\|x\|$ denota a distância de x ao inteiro mais próximo). Se $\epsilon > 0$, então não existe solução da desigualdade*

$$0 < |u\gamma - v + \mu| < AB^{-w} \tag{1.6}$$

em inteiros positivos u, v e w com

$$u \leq M \text{ e } w \geq \frac{\log(Aq/\epsilon)}{\log B}.$$

1.5 Outras definições e resultados auxiliares

1.5.1 Congruência em $\mathbb{Q}$

Agora, para uma maior conveniência do leitor, definiremos congruência para números racionais.

Definição 1.6. *Sejam $a/b, c/d \in \mathbb{Q}$. Dizemos que $a/b \equiv c/d \pmod{p^k}$ se $p \nmid bd$ e $\nu_p(a/b - c/d) \geq k$.*

Por exemplo,

$$\tfrac{1}{2} \equiv 4 \quad \tfrac{1}{4} \equiv 2 \quad \tfrac{1}{6} \equiv 6 \pmod{7}.$$

Proposição 1.5.1. *Sejam $a, b, c \in \mathbb{Z}$, $k \in \mathbb{N}$ e p um número primo ímpar. Se $a \equiv bc \pmod{p^k}$ e $(b, p) = 1$, então $\frac{a}{b} \equiv c \pmod{p^k}$.*

Demonstração. Note que

$$\nu_p\Big(\frac{a}{b} - c\Big) = \nu_p\Big(\frac{a - cb}{b}\Big) = \nu_p(a - cb) - \nu_p(b) \geq k,$$

pois $a \equiv bc \pmod{p^k}$ e $(b, p) = 1$. □

Proposição 1.5.2. *Sejam $\frac{a}{b} \equiv \frac{c}{d} \pmod{p^k}$ e $\frac{e}{f} \equiv \frac{g}{h} \pmod{p^k}$, com $(bdfh, p) = 1$. Então*

$$\frac{ae}{bf} \equiv \frac{cg}{dh} \pmod{p^k}.$$

Demonstração. Por hipótese, $\nu_p(ad - bc) \geq k$ e $\nu_p(eh - gf) \geq k$. Logo,

$$\nu_p(aedh - bfcg) = \nu_p((eh - gf)ad + (ad - bc)gf) \geq k.$$

Como $(bfdh, p) = 1$ chegamos a congruência desejada. □

1.5.2 Funções simétricas

Um polinômio $P(x_1, \ldots, x_n) \in \mathbb{A}[x_1, \ldots, x_n]$ (onde $\mathbb{A}$ é um anel) é chamado *simétrico* se

$$P(x_{\alpha(1)}, \ldots, x_{\alpha(n)}) = P(x_1, \ldots, x_n),$$

para toda permutação $\alpha \in S_n$, onde S_n é o conjunto das permutações do conjunto $[1, n]$. Para cada, $k \in [1, n]$, o polinômio

$$\sigma_k(x_1, \ldots, x_n) = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k}$$

é simétrico em $x_1, \ldots, x_n$ e é chamado de $k-$ésima função simétrica elementar.

Fato 1.5.1. *Defina $S = \prod_{t=1}^{r}(\lambda - x_t)$. Então podemos reescrever S da seguinte forma*

$$S = \lambda^r + \sigma_1(\overline{x})\lambda^{r-1} + \cdots + (-1)^r \sigma_r(\overline{x}), \tag{1.7}$$

onde $\overline{x} = (x_1, \ldots, x_k)$. A prova da fato acima pode ser obtida por indução.

1.5.3 Lemas chaves

Lema 1.5.1. *Seja p um primo ímpar tal que $p \equiv \pm 1 \pmod{10}$. Então existem inteiros $j \geq 0$ e s tais que para todo $m \in \mathbb{N}$ temos*

$$F_{p^m(p-1)} \equiv sp^{j+m+1} \pmod{p^{j+m+3}},$$

com $(s,p) = 1$.

Demonstração. Como $p \equiv \pm 1 \pmod{10}$ temos pelas Propriedades 1.1 item (6) que $\pi(p^2) \mid p(p-1)$. Daí,

$$F_{p(p-1)} \equiv 0 \pmod{p^2} \text{ e } F_{p(p-1)+1} \equiv 1 \pmod{p^2}.$$

Logo, existem $s,\ t \in \mathbb{Z}$ tais que

$$F_{p(p-1)} = sp^{j+2} \text{ e } F_{p(p-1)+1} = 1 + tp^2,$$

onde $(s,p) = 1$ e $j \geq 0$. Segue do Lema 1.1.1, item (b), para $k = p^{m-1}$, $n = p(p-1)$ e $c = 0$ que

$$\begin{aligned} F_{p^m(p-1)} &= \sum_{i=1}^{p^{m-1}} \binom{p^{m-1}}{i} F_{-i} F_{p(p-1)}^{i} F_{p(p-1)+1}^{p^{m-1}-i} \\ &= \sum_{i=1}^{p^{m-1}} \binom{p^{m-1}}{i} F_{-i} (sp^{j+2})^i (1+tp^2)^{p^{m-1}-i}. \end{aligned}$$

Usamos o binômio de Newton e chegamos que

$$F_{p^m(p-1)} = \sum_{i=1}^{p^{m-1}} \binom{p^{m-1}}{i} F_{-i} s^i \sum_{k=0}^{p^{m-1}-i} \binom{p^{m-1}-i}{k} t^k p^{2k+i(j+2)}. \tag{1.8}$$

Note que

$$\nu_p\Big(\binom{p^{m-1}}{i}\binom{p^{m-1}-i}{k} p^{2k+i(j+2)}\Big) \geq j+m+3,$$

onde $i \geq 2$ e $k \geq 1$. De fato, pelo Lema 1.1.4 e por $\nu_p(i) \leq i$ temos

$$\begin{aligned} \nu_p\Big(\binom{p^{m-1}}{i}\binom{p^{m-1}-i}{k} p^{2k+i(j+2)}\Big) &\geq m-1-\nu_p(i)+2k+ij+2i \\ &\geq m+ij+2k+i-1 \geq m+j+3, \end{aligned}$$

onde $i \geq 2$ e $k \geq 1$. Com a afirmação acima voltamos para a equação (1.8) e concluímos que

$$F_{p^m(p-1)} \equiv p^{m-1} s p^{j+2} \equiv s p^{m+j+1} \pmod{p^{m+j+3}},$$

onde $(s,p) = 1$ e $m \in \mathbb{N}$. □

Agora notamos que existe uma propriedade semelhante quando consideramos números de Fibonacci que possuem índices múltiplos de $p^m(p-1)$.

Lema 1.5.2. *Seja p um primo ímpar tal que $p \equiv \pm 1 \pmod{10}$. Então, para todo $m \geq 3$ e todo $k \in \mathbb{N}$ vale a seguinte propriedade*

$$F_{kp^m(p-1)} \equiv k s p^{j+m+1} \pmod{p^{j+m+3}},$$

onde $(s,p) = 1$.

Demonstração. Pelo lema anterior existe $s \in \mathbb{N}$ de modo que

$$F_{p^m(p-1)} \equiv s p^{j+m+1} \pmod{p^{j+m+3}},$$

onde $(s,p) = 1$ e $j \geq 0$, isto é, existem $s,\ t \in \mathbb{Z}$ tais que $F_{p^m(p-1)} = s p^{j+m+1} + t p^{j+m+3}$. Pela fórmula de múltiplos ângulos com $k = k$, $n = p^m(p-1)$ e $c = 0$ temos

$$\begin{aligned} F_{kp^m(p-1)} &= \sum_{i=1}^{k} \binom{k}{i} F_{-i} F_{p^m(p-1)}^{i} F_{p^m(p-1)+1}^{k-i} \\ &= \sum_{i=1}^{k} \binom{k}{i} F_{-i} (s p^{j+m+1} + t p^{j+m+3})^{i} F_{p^m(p-1)+1}^{k-i}. \end{aligned} \tag{1.9}$$

Particularmente,

$$(s p^{j+m+1} + t p^{j+m+3})^{i} = \sum_{l=0}^{i} \binom{i}{l} (s p^{j+m+1})^{l} (t p^{j+m+3})^{i-l}$$

$$= (t p^{j+m+3})^{i} + \sum_{l=1}^{i-1} \binom{i}{l} (s p^{j+m+1})^{l} (t p^{j+m+3})^{i-l} + (s p^{j+m+1})^{i}.$$

Note que $i(j+m+1) \geq j+m+3$, para $i \geq 2$. Logo,

$$(s p^{j+m+1} + t p^{j+m+3})^{i} \equiv 0 \pmod{p^{j+m+3}},$$

para $i \geq 2$.

Além disso, Como $F_{p^m(p-1)+1} \equiv 1 \pmod{p^2}$ temos que existe $u \in \mathbb{Z}$ tal que $F_{p^m(p-1)+1} = 1 + up^2$. Por fim, retornamos a equação (1.9) e concluímos que

$$\begin{aligned} F_{kp^m(p-1)} &\equiv k(sp^{j+m+1} + tp^{j+m+3})F^{k-1}_{p^m(p-1)+1} \pmod{p^{j+m+3}} \\ &\equiv ksp^{j+m+1}F^{k-1}_{p^m(p-1)+1} \pmod{p^{j+m+3}} \\ &\equiv ksp^{j+m+1}(1+up^2)^{k-1} \pmod{p^{j+m+3}} \\ &\equiv ksp^{j+m+1}\sum_{v=0}^{k-1}\binom{k-1}{v}(up^2)^v \pmod{p^{j+m+3}} \\ &\equiv ksp^{j+m+1} \pmod{p^{j+m+3}}. \end{aligned}$$

□

CAPÍTULO 2

Quando a Soma de Quadrados de Dois Números Consecutivos de k-bonacci é Um Número de l-bonacci

Os números de Fibonacci satisfazem a seguinte identidade

$$F_n^2 + F_{n+1}^2 = F_{2n+1}, \tag{2.1}$$

para todo $n \geq 0$. Mais precisamente, essa identidade nos diz que a soma do quadrados de dois números de Fibonacci consecutivos ainda é um número de Fibonacci.

Em 2010, Marques e Togbé, em [18], mostraram que para um s fixo, se $F_n^s + F_{n+1}^s$ é um número de Fibonacci para infinitos n, então $s = 1$ ou 2. No ano seguinte, Luca e Oyono, em [16], resolveram o problema completamente mostrando que a equação Diofantina

$$F_n^s + F_{n+1}^s = F_m,$$

não tem solução (n, m, s) com $n \geq 2$ e $s \geq 3$.

Em 2014, Chaves e Marques, em [7], estudaram uma generalização da equação (2.1) e mostraram que a equação Diofatina

$$(F_n^{(k)})^2 + (F_{n+1}^{(k)})^2 = F_m^{(k)}, \tag{2.2}$$

não possui suluções em inteiros positivos n, m e k, com $n > 1$ e $k \geq 3$. No mesmo ano, Luca e Gómez, em [32], mostraram que a equação

$$(F_n^{(k)})^s + (F_{n+1}^{(k)})^s = F_m^{(k)},$$

não possui soluções em inteiros positivos quando $k \geq 3$, $n \geq 2$ e $s \geq 2$.

Nosso interesse nesse capítulo é observar quais números da forma $(F_n^{(k)})^2 + (F_{n+1}^{(k)})^2$ são números de l-bonacci. Observaremos que, mesmo adicionando esse grau de liberdade obtemos o seguinte resultado.

Teorema 2.1. *A equação Diofantina*

$$(F_n^{(k)})^2 + (F_{n+1}^{(k)})^2 = F_m^{(l)}, \tag{2.3}$$

não possui solução para $2 \leq k < l$ *e* $n > k + 1$.

Vejamos uma breve ideia da nossa demonstração. Primeiro, usamos a fórmula de Dresden, veja [8, Formula (2)], e assim obtemos uma limitação superior para a forma linear em três logaritmos relacionada à equação (2.1). Em seguida usamos uma limitação inferior dada por Matveev para obtermos uma limitação para $n,\ m$ em função de l. Bravo e Luca usaram, em [1, p. 77 e 78], um argumento combinando algumas estimativas junto com o Teorema do Valor Médio. No nosso caso usamos esse argumento duas vezes e conseguimos limitantes superiores para nossas formas lineares em três logaritmos. Agora, combinando esses resultados conseguimos limitantes efetivos para nossas variáveis. Como os limitantes são "astronômicos", usamos um argumento de redução, devido a Dujella e Pethö, que reduz drasticamente os limitantes. Finalmente colocamos no software Mathematica e chegamos no resultado.

O primeiro passo da nossa demonstração é conseguir relações entre as variáveis. Na seção a seguir relacionaremos as variáveis m e n com l.

2.1 Uma limitação superior para m e n em termos de l

Denote por α e β as raízes reais (que denominamos anteriormente de dominantes) de $F_n^{(k)}$ e $F_m^{(l)}$, respectivamente. Note que $\alpha < \beta$. De fato, suponha por absurdo que $\alpha > \beta$, então existe $n_0 \in \mathbb{N}$ tal que $(\alpha/\beta)^{n-2} > \beta$, para todo $n \geq n_0$. Logo, $F_n^{(k)} \geq \alpha^{n-2} > \beta^{n-1} \geq F_n^{(l)}$, para todo $n \geq n_0$. Absurdo, pois $l > k$.

Segue do Fato 1.2.2 que

$$F_m^{(l)} = (F_n^{(k)})^2 + (F_{n+1}^{(k)})^2 \geq \alpha^{2n-4} + \alpha^{2n-2} = \alpha^{2n-4}(1+\alpha^2) > \alpha^{2n-2}$$

e

$$F_m^{(l)} = (F_n^{(k)})^2 + (F_{n+1}^{(k)})^2 \leq \alpha^{2n-2} + \alpha^{2n} = \alpha^{2n-2}(1+\alpha^2) < \alpha^{2n+1},$$

onde usamos que $1 + \alpha^2 < \alpha^3$, para $k \geq 2$. Usamos as estimativas $\beta^{m-2} \leq F_m^{(k)} \leq \beta^{m-1}$ e $\alpha < \beta$, junto com as desigualdades anteriores e concluímos que

$$\alpha^{m-2} < \alpha^{2n+1} \Rightarrow m < 2n+3 \tag{2.4}$$

e

$$(\sqrt{2})^{2n-2} < \alpha^{2n-2} < \beta^{m-1} < 2^{m-1} \Rightarrow n < m. \tag{2.5}$$

Aqui usamos que $\sqrt{2} < (1+\sqrt{5})/2 \leq \alpha$, para todo $k \geq 2$, pois $(1+\sqrt{5})/2$ é a raiz dominante da sequência de Fibonacci. Logo,

$$n < m < 2n+3. \tag{2.6}$$

Nessa seção provaremos o seguinte resultado

Lema 2.1.1. *Se (n, m, k, l) é um uma solução inteira da equação Diofantina (2.3), com $l > k$ e $m > l + 1$, então*

$$n < 3 \cdot 10^{15} l^9 \log^3 l \quad \textit{and} \quad m < 6.1 \cdot 10^{15} l^9 \log^3 l.$$

Demonstração. Sejam $F_n^{(k)} = g(\alpha, k)\alpha^{n-1} + E_n(k)$ *e* $F_m^{(l)} = g(\beta, l)\beta^{m-1} + E_m(l)$. Então segue da equação (2.3) que

$$g(\beta, l)\beta^{m-1} + E_m(l) = (g(\alpha, k)\alpha^{n-1} + E_n(k))^2 + (g(\alpha, k)\alpha^n + E_{n+1}(k))^2,$$

expandimos os quadrados e obtemos,

$$g(\beta, l)\beta^{m-1} + E_m(l) = g(\alpha, k)^2(1+\alpha^2)\alpha^{2n-2} + 2g(\alpha, k)(E_n(k) + \alpha E_{n+1}(k)\alpha^{n-1} + E_n(k)^2 + E_{n+1}(k)^2.$$

Agora, organizamos os termos de maior ordem de um lado. Logo,

$$g(\alpha,k)^2(1+\alpha^2)\alpha^{2n-2}-g(\beta,l)\beta^{m-1} = -2g(\alpha,k)(E_n(k)+\alpha E_{n+1}(k)\alpha^{n-1}-(E_n(k)^2+E_{n+1}(k^2)+E_m(l).$$

Assim,

$$\begin{aligned} |g^2(1+\alpha^2)\alpha^{2n-2} - h\beta^{m-1}| &< |2g(E_n(k)+\alpha E_{n+1}(k))\alpha^{n-1}| + |(E_n^2(k)+E_{n+1}^2(k))| + |E_m(l)| \\ &< 2\cdot\frac{3}{4}\alpha^{n-1}(\frac{1}{2}+1)+1 \\ &< 2.5\alpha^{n-1}+1, \end{aligned}$$

onde denotamos por $g := g(\alpha,k)$ e $h := g(\beta,l)$, e usamos as limitações, vistas no primeiro capítulo, para os E_n's e g junto com o Fato 1.2.1. Portanto,

$$|g^2(1+\alpha^2)\alpha^{2n-2} - h\beta^{m-1}| < 3\alpha^{n-1}. \tag{2.7}$$

Dividimos ambos os lados pelo termo $g^2(1+\alpha^2)\alpha^{2n-2}$ e usamos as estimativas novamente para obter a seguinte limitação

$$\left|1 - \frac{h\beta^{m-1}}{g^2(1+\alpha^2)\alpha^{2n-2}}\right| < \frac{4}{\alpha^{n-1}} < \frac{8}{(1.6)^n}. \tag{2.8}$$

Visando usar o Lema 1.1, tomamos $t = 3$,

$$\gamma_1 := \alpha,\ \gamma_2 := \beta,\ \gamma_3 := \frac{h}{g^2(1+\alpha^2)}$$

e

$$b_1 := -2n+2,\ b_2 := m-1,\ b_3 := 1.$$

Para essa escolha, temos $D = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}] \leq kl < l^2$. Note que $\mathsf{h}(\gamma_1) = \log\alpha/k < 0.7/k$ e da mesma forma $\mathsf{h}(\gamma_2) < 0.7/l$. Pelo Lema 1.3.1 temos que $\mathsf{h}(g) < 4\log k$ e $\mathsf{h}(h) < 4\log l$. Daí,

$$\begin{aligned} \mathsf{h}(\gamma_3) &\leq \mathsf{h}(h) + 2\mathsf{h}(g) + 2\mathsf{h}(\alpha) + \log 2 \\ &\leq 12\log l + \frac{1.4}{k} + \log 2, \end{aligned}$$

pois $k < l$. Assim, podemos pegar $A_1 := 0.7l^2, A_2 := 0.7l$ e $A_3 := 15l^2\log l$, pois $12l^2\log l + 3l^2 < 15l^2\log l$, para todo $l \geq 3$. Pela desigualdade (2.6) podemos considerar $B = 2n+2$.

Nos resta apenas provar que $\frac{g(\beta,l)\beta^{m-1}}{g(\alpha,k)^2(1+\alpha^2)\alpha^{2n-2}} \neq 1$. Suponha ao contrário, i.e.,

$$g(\beta,l)\beta^{m-1} = g(\alpha,k)^2(1+\alpha^2)\alpha^{2n-2}.$$

Seja $\mathbb{L} = \mathbb{Q}(\alpha_1,\ldots,\alpha_k,\beta_1,\ldots,\beta_l)$ o fecho normal de $\mathbb{Q}(\alpha,\beta)$ e $\phi_1,\ldots,\phi_l$ os elementos de $Gal(\mathbb{L}/\mathbb{Q})$ tal que $\phi_i(\beta) = \beta_i$. Como $l > k$, existe $i \neq j \in \{1,\ldots,l\}$ tal que $\phi_i(\alpha) = \phi_j(\alpha)$. Aplicamos $\phi_j^{-1}\phi_i$ na relação anterior e obtemos que $\phi_j^{-1}(\alpha_1) = \alpha_s$. Então $s \neq 1$ (pois $\phi_j(\alpha_i) = \alpha_j \neq \alpha_i$) e além disso

$$\left(\frac{7}{4}\right)^{m-1} < \beta^{m-1} = \left|\frac{g(\alpha_s,k)}{g(\beta,l)}\right||1+\alpha_s^2||\alpha_s|^{2n-2} < 4,$$

onde usamos $\beta > 7/4$, $|g(\alpha_s,l)| < 1 < 2|g(\beta,l)|$ e $|\alpha_s| < 1$, para $s > 1$. Contudo a desigualdade $(7/4)^{m-1} < 4$ acontece apenas para $m \in [1,3]$. Absurdo, pois $m > l+1 \geq 4$.

Logo, podemos aplicar o Teorema 1.1 e assim,

$$\left|1 - \frac{h\beta^{m-1}}{g^2(1+\alpha^2)\alpha^{2n-2}}\right| > \exp(-1.7\times 10^{13} l^9 \log^2 l \log n), \tag{2.9}$$

onde usamos que $1 + 2\log l < 4\log l$ e $1 + \log(2n+2) < 4\log n$, para $l \geq 3$ e $n \geq 3$, respectivamente.

Como a função $x \mapsto x/\log x$ é crescente para $x > e$ temos que

$$\frac{x}{\log x} < A \Rightarrow x < 2A\log A. \tag{2.10}$$

De fato, suponha por absurdo que $x \geq 2A\log A$, então

$$A = \frac{2A\log A}{2\log A} < \frac{2A\log A}{\log(2A\log A)} \leq \frac{x}{\log x},$$

onde usamos que $A > 2\log A$, para todo $A \geq 3$. Contradizendo assim nossa hipótese.

Combinamos (2.8) e (2.9) e obtemos que

$$\exp(-1.7\times 10^{13} l^9 \log^2 l \log n) < \frac{8}{(1.6)^n}.$$

Então,

$$\frac{n}{\log n} < 3.7\cdot 10^{13} l^9 \log^2 l.$$

Assim, usamos (2.10), com $x := n$ e $A := 3.7\cdot 10^{13} l^9 \log^2 l$ e concluímos que

$$n < 2(3.7\cdot 10^{13} l^9 \log^2 l)\log(3.7\cdot 10^{13} l^9 \log^2 l).$$

Portanto,

$$n < 3 \cdot 10^{15} l^9 \log^3 l,$$

pois $\log(3.7) + 13 \log 10 + 9 \log l + 2 \log \log l < 40 \log l$, para todo $l \geq 3$. Por fim, usamos a estimativa (2.6) e chegamos que

$$m < 6.1 \cdot 10^{15} l^9 \log^3 l.$$

□

2.2 O caso l grande

Nessa seção vamos assumir que $l > 1026$. Temos

$$m < 6.1 \cdot 10^{15} l^9 \log^3 l < 2^{l/2}.$$

Usaremos um argumento chave devido a Bravo e Luca. Contudo, apresentaremos esse argumento aqui para que nosso trabalho fique mais completo. Defina $\lambda = 2 - \beta$, deduzimos que $0 < \lambda < 1/2^{l-1}$ (pois $2(1 - 2^{-l}) < \beta < 2$). Então

$$\beta^{m-1} > (2 - \lambda)^{m-1} = 2^{m-1}(1 - \frac{\lambda}{2})^{m-1} > 2^{m-1}(1 - (m-1)\lambda),$$

pois vale a desigualdade $(1 - x)^m > 1 - 2mx$, para todo $m \geq 1$ e $0 < x < 1$. Além disso, $(m-1)\lambda < 2^{l/2}/2^{l-1} = 2/2^{l/2}$ e assim

$$2^{m-1} - \frac{2^m}{2^{l/2}} < \beta^{m-1} < 2^{m-1} + \frac{2^m}{2^{l/2}}.$$

Portanto,

$$|\beta^{m-1} - 2^{m-1}| < \frac{2^m}{2^{l/2}}. \tag{2.11}$$

Agora, definimos para $x > 2(1 - 2^{-l})$ a função $f_1(x) := g(x, l)$ que é diferenciável no intervalo $[\beta, 2]$. Pelo Teorema do Valor Médio existe $\xi \in (\beta, 2)$ tal que $f_1(\beta) - f_1(2) = f_1'(\xi)(\beta - 2)$. Assim,

$$|f_1(\beta) - f_1(2)| < \frac{2l}{2^l}, \tag{2.12}$$

onde usamos que $|\beta - 2| < 1/2^{l-1}$ e $|f_1'(\xi)| < l$ (note que a desigualdade $x^2 - 5x + 6 > 0$, vale para $1 < x < 2$, e que $2 + (l+1)(\xi - 2) > 2 - (l+1)/2^{(l-1)} \geq 1$, para todo $l \geq 3$.

Além disso, $f_1'(\xi) = (1-l)/(2+(l+1)(\xi-2))^2$. Daí, $|f_1'(\xi)| < l$). Por simplicidade, denotamos $\delta_1 = \beta^{m-1} - 2^{m-1}$ e $\eta_1 = f_1(\beta) - f_1(2) = f_1(\beta) - 1/2$. Após alguns cálculos chegamos a seguinte relação

$$2^{m-2} = h\beta^{m-1} - 2^{m-1}\eta_1 - \frac{\delta_1}{2} - \delta_1\eta_1, \tag{2.13}$$

onde lembramos que $h = f_1(\beta)$. O fato a seguir vai nos permitir usar o argumento de Bravo e Luca no nosso problema.

Lema 2.2.1. *Temos que*

$$3\alpha^{n-1} < 2^{5/2}\frac{2^{m-2}}{2^{l/2}}.$$

Demonstração. Com efeito, primeiro concluímos de (2.5) que

$$\alpha^{2n-2} < 2^{m-1} \Rightarrow \alpha^{n-1} < 2^{(m-1)/2} \Rightarrow 3\alpha^{n-1} < 2^{\frac{m-1}{2}+2} = 2^{(m+3)/2}. \tag{2.14}$$

Por outro lado, as seguinte implicações são verdadeiras

$$m \geq l+2 \Leftrightarrow m-l+1 \geq 3 \Leftrightarrow 2m-l+5-4 \geq m+3.$$

Logo,

$$\frac{m+3}{2} \leq m - \frac{l-5}{2} - 2 \Leftrightarrow 2^{\frac{m+3}{2}} \leq 2^{m-\frac{l-5}{2}-2} \Leftrightarrow 2^{\frac{m+3}{2}} \leq 2^{5/2}\cdot\frac{2^{m-2}}{2^{l/2}}. \tag{2.15}$$

Por fim, combinamos (2.14) e (2.15) chegando assim no resultado desejado. □

Segue da relação (2.13) que

$$|2^{m-2} - g^2(1+\alpha^2)\alpha^{2n-2}| < |h\beta^{m-1} - g^2(1+\alpha^2)\alpha^{2n-2}| + 2^{m-1}|\eta_1| + \left|\frac{\delta_1}{2}\right| + |\delta_1\eta_1|,$$

e da limitação (2.7) que

$$|2^{m-2} - g^2(1+\alpha^2)\alpha^{2n-2}| < 3\alpha^{n-1} + 2^{m-1}|\eta_1| + \left|\frac{\delta_1}{2}\right| + |\delta_1\eta_1|.$$

Assim, pelo Lema 2.2.1 e as limitações (2.11) e (2.12) temos que

$$|2^{m-2} - g^2(1+\alpha^2)\alpha^{2n-2}| < 2^{5/2}\cdot\frac{2^{m-2}}{2^{l/2}} + 2^{m-1}\frac{2l}{2^l} + \frac{2^{m-1}}{2^{l/2}} + \frac{4l}{2^l}\frac{2^{m-1}}{2^{l/2}}.$$

Dividimos ambos os lado por 2^{m-2} e notamos que a seguinte cadeia de desigualdades $4l < 8l < 2^{l/2} < 2^l$ é válida, para todo $l > 14$, então

$$\left|1 - \frac{g^2(1+\alpha^2)\alpha^{2n-2}}{2^{m-2}}\right| < 2^{5/2} \cdot \frac{1}{2^{l/2}} + 2\frac{2l}{2^l} + \frac{2}{2^{l/2}} + \frac{4l}{2^l}\frac{2}{2^{l/2}}.$$

Portanto, para todo $l > 1026$ obtemos que

$$\left|1 - \frac{g^2(1+\alpha^2)\alpha^{2n-2}}{2^{m-2}}\right| < \frac{10}{2^{l/2}}. \tag{2.16}$$

Para concluir nosso resultado, para l grande, precisaremos subdividir nossa prova em dois casos. A saber, quando $n < 2^{k/2}$ e $n > 2^{k/2}$.

2.2.1 O caso $n < 2^{k/2}$

Aplicamos novamente o argumento devido a Bravo e Luca. Entretanto, agora usamos a raiz dominante de $F_n^{(k)}$ e observamos que tudo que for feito para n é também válido para $n+1$. Vamos repetir o argumento para conveniência do leitor. Seja $\lambda = 2 - \alpha$, deduzimos que $0 < \lambda < 1/2^{k-1}$, pois $2(1 - 2^{-k}) < \alpha < 2$. Então,

$$\alpha^{n-1} > (2-\lambda)^{n-1} = 2^{n-1}(1 - \frac{\lambda}{2})^{n-1} > 2^{n-1}(1 - (n-1)\lambda),$$

onde usamos o fato de que $(1-x)^n > 1 - 2nx$ para todo $n \geq 1$ e $0 < x < 1$. Além disso, $(n-1)\lambda < 2^{k/2}/2^{k-1} = 2/2^{k/2}$. Portanto,

$$2^{n-1} - \frac{2^n}{2^{k/2}} < \alpha^{n-1} < 2^{n-1} + \frac{2^n}{2^{k/2}}$$

e assim,

$$|\alpha^{n-1} - 2^{n-1}| < \frac{2^n}{2^{k/2}}.$$

Usamos o mesmo argumento para $n+1$ e obtemos

$$|\alpha^n - 2^n| < \frac{2^{n+1}}{2^{k/2}}.$$

Considere a função $f_2(x) := g(x,k)$ para $x > 2(1-2^{-k})$. Essa função é diferenciável em $[\alpha, 2]$. Usamos o Teorema do valor Médio e constatamos que existe algum $\xi \in (\alpha, 2)$ tal que $f_2(\alpha) - f_2(2) = f_2'(\xi)(\alpha - 2)$. Assim,

$$|f_2(\alpha) - f_2(2)| < \frac{2k}{2^k},$$

onde usamos o fato de $|\alpha-2| < \frac{1}{2^{k-1}}$ e $|f_2'(\xi)| < k$. Definimos $\delta = \alpha^{n-1} - 2^{n-1}$, $\tilde{\delta} = \alpha^n - 2^n$ e $\eta = f_2(\alpha) - f_2(2) = f_2(\alpha) - 1/2$ e após alguns cálculos concluímos que

$$f_2(\alpha)\alpha^{n-1} = 2^{n-2} + 2^{n-1}\eta + \frac{\delta}{2} + \delta\eta$$

e

$$f_2(\alpha)\alpha^n = 2^{n-1} + 2^n\eta + \frac{\tilde{\delta}}{2} + \tilde{\delta}\eta.$$

Elevamos $f_2(\alpha)\alpha^{n-1} - 2^{n-2}$ e $f_2(\alpha)\alpha^n - 2^{n-1}$ ao quadrado e obtemos que

$$2^{2n-4} = f_2^2(\alpha)\alpha^{2n-2} - \left(\delta\eta 2^n + \delta 2^{n-2} + \delta^2\eta + \eta^2 2^{2n-2} + 2^n\eta^2\delta + \frac{\delta^2}{4} + (\delta\eta)^2 + 2^{2n-2}\eta\right)$$

e

$$2^{2n-2} = f_2^2(\alpha)\alpha^{2n} - \left(\tilde{\delta}\eta 2^{n+1} + \tilde{\delta}2^{n-1} + \tilde{\delta}^2\eta + \eta^2 2^{2n} + 2^{n+1}\eta^2\tilde{\delta} + \frac{\tilde{\delta}^2}{4} + (\tilde{\delta}\eta)^2 + 2^{2n}\eta\right).$$

Novamente fazemos alguns cálculos e concluímos que

$$\begin{aligned}
\left|2^{2n-4}\cdot 5 - h\beta^{m-1}\right| &= \left|2^{2n-2} + 2^{2n-4} - h\beta^{m-1}\right| \\
&< 3\cdot\alpha^{n-1} + 527\cdot\frac{2^{2n-4}}{2^{k/2}} \\
&\leq 6\cdot\frac{2^{2n-4}}{2^{k/2}} + 527\cdot\frac{2^{2n-4}}{2^{k/2}} \\
&= 533\cdot\frac{2^{2n-4}}{2^{k/2}}, \qquad (2.17)
\end{aligned}$$

para todo $k \geq 2$. Usamos (2.16), (2.17) e chegamos em

$$\begin{aligned}
\left|2^{2n-4}\cdot 5 - 2^{m-2}\right| &< \left|2^{2n-4}\cdot 5 - h\beta^{m-1}\right| + |2^{m-2} - g^2(1+\alpha^2)\alpha^{2n-2}| \\
&\quad + |g^2(1+\alpha^2)\alpha^{2n-2} - h\beta^{m-1}| \\
&< 533\cdot\frac{2^{2n-4}}{2^{k/2}} + 10\cdot\frac{2^{m-2}}{2^{l/2}} + 3\cdot\alpha^{n-1} \\
&\leq 533\cdot\frac{2^{2n-4}}{2^{k/2}} + 160\cdot\frac{2^{2n-4}}{2^{k/2}} + 6\cdot\frac{2^{2n-4}}{2^{k/2}} = 699\cdot\frac{2^{2n-4}}{2^{k/2}}.
\end{aligned}$$

Logo,

$$\left|1 - \frac{2^{m-2}}{2^{2n-4}\cdot 5}\right| = \left|1 - \frac{2^{m+2-2n}}{5}\right| < \frac{140}{2^{k/2}}.$$

Lembramos que $m \leq 2n+2$ e então $m - 2n - 2 \leq 0$. Daí, $m + 2 - 2n \leq 4$. Assim,

$$\frac{1}{5} < \left|1 - \frac{2^{m+2-2n}}{5}\right| < \frac{140}{2^{k/2}}.$$

Portanto, $k \leq 18$. Como estamos tratando o caso $n < 2^{k/2}$, temos a estimativa $n < 512$ e $m < 1027$. Contradizendo assim a hipótese de $l > 1026$, pois supomos desde o princípio que $m > l + 1$.

2.2.2 O caso $2^{k/2} < n$

Nosso plano agora é considerar a desigualdade (2.16) e depois encontrar uma limitação superior para n. O passo seguinte é usar métodos computacionais para encontrar limitações para k, l, m e n.

Lema 2.2.2. *Se (n, m, k, l) é uma solução inteira não trivial da equação (2.3) com $l > 1026$, $2^{k/2} < n$ e $m > l + 1$, então*

$$n < m < 3.8 \cdot 10^{307},\ l < 6.3 \cdot 10^{31}\ e\ k \leq 2091.$$

Demonstração. Note que o Lema 2.1.1 junto com o fato de $l > 1026$ implica na seguinte cadeia de desigualdade

$$2^{k/2} < n < 3 \cdot 10^{15} l^9 \log^3 l < l^{15}. \tag{2.18}$$

Em particular, temos que

$$k < 44 \log l. \tag{2.19}$$

Provaremos agora que $\frac{g^2(1+\alpha^2)\alpha^{2n-2}}{2^{m-2}} \neq 1$. De fato, seja $\mathbb{L} = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ o fecho normal e $\psi_1, \ldots, \psi_k$ os elementos de $Gal(\mathbb{L}/\mathbb{Q})$ tais que $\psi_i(\alpha) = \alpha_i$. Aplicamos o automorfismo ψ_i, para qualquer $i \in [2, k]$, e auferimos o seguinte absurdo

$$1 > g(\alpha_i, k)^2(1 + \alpha_i^2)\alpha_i^{2n-2} = 2^{m-2} > 1.$$

Logo, $\frac{g^2(1+\alpha^2)\alpha^{2n-2}}{2^{m-2}} \neq 1$. Com intuito de aplicar o Lema 1.1, tomamos $t := 3$,

$$\lambda_1 := \alpha,\ \lambda_2 := 2,\ \lambda_3 := g^2(1 + \alpha^2)$$

e

$$b_1 := 2n - 2,\ b_2 := -m + 2,\ b_3 := 1.$$

Para essa escolha, temos $D = [\mathbb{Q}(\alpha) : \mathbb{Q}] = k$ e por (2.4) escolhemos $B = 2n$. Além disso, como ja foi feito na seção 2.1, podemos considerar $A_1 = 0.7$, $A_2 = 0.7k$ e $A_3 = 9k \log k$. Então segue do Lema de Matveev que

$$\left|1 - \frac{g^2(1+\alpha^2)\alpha^{2n-2}}{2^{m-2}}\right| \geq \exp(-Qk^4(1+\log k)(1+\log 2n)\log k),$$

onde $Q = 1.4 \cdot 30^6 \cdot 3^{4.5} \cdot 0.7^2 \cdot 9 < 6.4 \cdot 10^{11}$. Mais ainda,

$$\left|1 - \frac{g^2(1+\alpha^2)\alpha^{2n-2}}{2^{m-2}}\right| \geq \exp(-5.7 \cdot 10^{12}k^4 \log^2 k \log n), \tag{2.20}$$

pois $1 + \log k < 3 \log k$ e $1 + \log 2n < 3 \log n$, para todo $k \geq 2$ e $n \geq 3$, respectivamente. Combinamos (2.16) e (2.20) para concluir que

$$l < 1.8 \cdot 10^{13} k^4 \log^2 k \log n.$$

Sabemos que $\log n < 15 \log l$, para todo $l > 1026$. Então

$$\frac{l}{\log l} < 2.8 \cdot 10^{14} k^4 \log^2 k.$$

Pela desigualdade (2.10) chegamos que

$$l < 2.9 \cdot 10^{16} k^4 \log^3 k, \tag{2.21}$$

pois $\log(2.8) + 14 \log 10 + 4 \log k + 2 \log \log k < 51 \log k$, para $k \geq 2$. Então por (2.18) obtemos,

$$\begin{aligned} n &< 3 \cdot 10^{15}(2.9 \cdot 10^{16}k^4 \log^3 k)^9 \log^3(2.9 \cdot 10^{16}k^4 \log^3 k) \\ &< 3 \cdot 10^{15} \cdot 5.9 \cdot 10^{142} k^{36} (\log k)^{27} \log^3(2.9 \cdot 10^{16}k^4 \log^3 k) \\ &< 3 \cdot 10^{15} \cdot 5.9 \cdot 10^{142} k^{36} (\log k)^{27} (56 \log k)^3. \end{aligned}$$

Assim,

$$n < 8.5 \cdot 10^{168} k^{36} (\log k)^{30}. \tag{2.22}$$

Como $k < 2 \log n / \log 2$, temos

$$k < \frac{2}{\log 2} \log(8.5 \cdot 10^{168} k^{36} (\log k)^{30}).$$

Usamos o software *Mathematica* e obtemos $l < 6.3 \cdot 10^{31}$. Portanto,

$$n < 1.9 \cdot 10^{307},\ m < 3.8 \cdot 10^{307}\ e\ 2 \leq k \leq 2091. \tag{2.23}$$

□

2.3 Prova do teorema principal

Seja $\Lambda_2 = (2n-2)\log\alpha - (m-2)\log 2 + \log[g^2(1+\alpha^2)]$, então por (2.16),

$$|1 - e^{\Lambda_2}| < \frac{10}{2^{l/2}}. \tag{2.24}$$

Se $\Lambda_2 > 0$, então segue de (2.24) que

$$0 < \Lambda_2 \leq e^{\Lambda_2} - 1 < \frac{10}{2^{l/2}}.$$

Logo,

$$0 < (2n-2)\frac{\log\alpha}{\log 2} - m + \Big[2 + \frac{\log(g^2(1+\alpha^2))}{\log 2}\Big] < 14.5 \cdot (1.42)^{-l}.$$

Por outro lado, se $\Lambda_2 < 0$, então $|1 - e^{\Lambda_2}| < 4$ e $e^{|\Lambda_2|} < 5$. Assim,

$$0 < |\Lambda_2| \leq e^{|\Lambda_2|} - 1 = e^{|\Lambda_2|}|e^{\Lambda_2} - 1| < 5.1 \cdot 10/2^{l/2} < 51/2^{l/2}.$$

Consequentemente

$$0 < |\Lambda_2| < 5.1 \cdot 10/2^{l/2} < 51/2^{l/2}$$

e assim,

$$0 < (m-2)\frac{\log 2}{\log\alpha} - 2n + \Big[2 + \frac{\log[g^2(1+\alpha^2)]}{\log\alpha}\Big] < 126 \cdot (1.42)^{-l}.$$

O argumento de trabalho para $\Lambda_2 > 0$ e $\Lambda_2 < 0$ são análogos. Logo, para evitarmos repetições desnecessárias, consideramos apenas o caso $\Lambda_2 > 0$. Então

$$0 < (2n-2)\gamma_k - m + \mu_k < 14.5 \cdot (1.42)^{-l}, \tag{2.25}$$

onde $\gamma_k := \frac{\log\alpha}{\log 2}$ e $\mu_k := 2 + \frac{\log(g^2(1+\alpha^2))}{\log 2}$.

Usando o mesmo argumento que o usado na prova de que $\frac{h\beta^{m-1}}{g^2(1+\alpha^2)\alpha^{2n-2}} \neq 1$, concluímos que $\gamma_k = \log\alpha/\log 2$ é irracional, para qualquer inteiro $k \geq 2$. Seja $q_{m,k}$ o denominador do m-ésimo convergente da fração contínua de γ_k. Consideramos $M_k := 1.3 \cdot 10^{169} k^{36} \log^{30} k < M_{2091}$ e usamos o software *Mathematica* para obtermos que

$$\min_{2\leq k\leq 2091}(q_{600,k}) > 6M_k \quad e \quad \max_{2\leq k\leq 2091}(q_{600,k}) < 6.6 \cdot 10^{1123}.$$

Definimos $\epsilon_k := \|\mu_k q_{600}\| - M_k\|\gamma_k q_{600}\|$, para $2 \leq k \leq 2091$, e obtemos que

$$\min_{2\leq k\leq 2091} \epsilon_k > 1.2 \cdot 10^{-105}.$$

Note que as hipóteses para usar o Lema 1.4.1 são satisfeitas para $A = 14.5$ e $B = 1.42$. Portanto não existe solução para desigualdade (2.25) (e então não tem solução para a equação Diofantina (2.3)) para n e l satisfazendo

$$2n - 2 < M_k \;\; e \;\; l \geq \frac{\log(Aq/\epsilon)}{\log B}.$$

Como $2n - 2 < M_k$, para todo $2 \leq k \leq 2091$, por (2.23) temos que

$$l < \frac{\log(Aq_{600,k}/\epsilon_k)}{\log B} < 8076.$$

Observe que nesse ponto estamos sobre a hipótese de $2^{k/2} < n$. Logo, obtemos da relação (2.19) que $k \leq 395$. Repetimos o argumento anterior três vezes e conseguimos que

$$l \leq 1621 \; e \; k \leq 325.$$

Observação 2.3.1. *Os próximos passos não dependem da hipótese de que $l > 1026$. Portanto, estaremos resolvendo os casos em que l é pequeno também, isto é, quando $l \leq 1026$.*

Suponha que $l \leq 1621$. Segue do Lema 2.1.1 que

$$n < 9.4 \cdot 10^{46} \; e \; m < 2 \cdot 10^{47}.$$

Agora, definimos a seguinte forma linear logarítmica

$$\Lambda_1 = (m-1)\log\beta - (2n-2)\log\alpha + \log\Big[\frac{h}{g^2(1+\alpha^2)}\Big].$$

Se $\Lambda_1 > 0$,então por (2.8),

$$0 < \Lambda_1 \leq e^{\Lambda_1} - 1 < \frac{8}{1.6^n}$$

e

$$0 < (m-1)\gamma'_{l,k} - 2n + \mu'_{l,k} < 16.7 \cdot (1.6)^{-n}.$$

onde $\gamma'_{l,k} := \frac{\log\beta}{\log\alpha}$ e $\mu'_{l,k} := 2 + \frac{\log(h/g^2(\alpha^2+1))}{\log\alpha}$.

Usando o mesmo argumento que o usado na prova de que $\frac{h\beta^{m-1}}{g^2(1+\alpha^2)\alpha^{2n-2}} \neq 1$, concluímos que $\gamma_{k,l} = \frac{\log\beta}{\log\alpha}$ é irracional, para todo $l > k \geq 2$. Tomamos $M_l := 6.1 \cdot 10^{15} l^9 \log^3 l$ e usamos o software *Mathematica* para obter que

$$\min_{2\leq k<l\leq 1621}(q_{1000,k,l}) - 6M_l > 0 \; e \; \max_{2\leq k<l\leq 1621}(q_{1000,k,l}) < 3.2 \cdot 10^{3210}.$$

Definindo $\epsilon_{l,k} := \|\mu'_{k,l} q_{1000}\| - M_l \|\gamma'_{k,l} q_{1000}\|$. Então

$$\min_{2\leq k<l\leq 1621}(\epsilon_{l,k}) > 1.2 \cdot 10^{-2110},$$

Agora, podemos aplicar o Lemma 1.1 para $A = 16.7$ e $B = 1.6$. Como $m-1 < M_l$, temos

$$n < \frac{\log(16.7 \cdot q_{1000,k,l}/\epsilon_{k,l})}{\log 1.6} < 26072.$$

Portanto, por (2.6) concluímos que $m < 52144$.

Finalmente usamos um algoritmo no software Mathematica que confirma que a equação (2.3) não possui solução para $2 \leq k < l \leq 1621$, $k+1 < n < 26072$ e $l+1 < m < 52144$.

□

CAPÍTULO 3

Resto da divisão de $\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F$ por p^k para $k = 1, 2, 3$ e 4

Em 2012, Marques e Trojovský provaram, em [25] e [26], que $p \mid \begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F$, para todo $a \geq 1$ e $p \in \{2, 3\}$. Posteriormente, Marques, Sellers e Trojovský em [27] provaram que o número $\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F$ é divisível por p para todo primo p tal que $p \equiv \pm 2 \pmod 5$ e para todo inteiro $a \geq 1$. Marques e Trojovský também provaram, em [28], que se $p \equiv \pm 1 \pmod 5$, então $p \nmid \begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F$ para todo inteiro $a \geq 1$.

Nosso objetivo, nesse capítulo, é encontrar a classe de resíduos de $\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F$ módulo p, p^2, p^3 e p^4.

3.1 Resto do coeficiente fibonomial módulo p

Vamos relembrar que, pela definição de coeficiente fibonomial, temos

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F = \prod_{j=1}^{p^a} \frac{F_{p^a(p-1)+j}}{F_j}$$

e que definimos anteriormente $e(p) = \nu_p(F_{z(p)})$.

Antes de provarmos o nosso primeiro teorema vamos provar um lema técnico que vai ser bastante utilizado durante esse capítulo.

Lema 3.1.1. *Seja p um primo tal que $p \equiv \pm 1 \pmod 5$, então*

$$\frac{F_{p^a(p-1)+tz(p)}}{F_{tz(p)}} \equiv 1 \pmod p,$$

para todo $t \in [1, \lfloor \frac{p^a}{z(p)} \rfloor]$.

Demonstração. Pela fórmula da adição temos

$$F_{p^a(p-1)+tz(p)} = F_{p^a(p-1)-1}F_{tz(p)} + F_{p^a(p-1)}F_{tz(p)+1}$$

e portanto,

$$\frac{F_{p^a(p-1)+tz(p)}}{F_{tz(p)}} = F_{p^a(p-1)-1} + \frac{F_{p^a(p-1)}}{F_{tz(p)}}F_{tz(p)+1}.$$

As propriedades de valorização p-ádica e o Lema 1.1.1 implicam que

$$\nu_p\Big(\frac{F_{p^a(p-1)}}{F_{tz(p)}}\Big) = \nu_p(F_{p^a(p-1)}) - \nu_p(F_{tz(p)}) = a - \nu_p(t) > 0,$$

pois $(p, z(p)) = 1$ e $t < p^a$. Assim, $\frac{F_{p^a(p-1)}}{F_{tz(p)}} \equiv 0 \pmod p$. Além disso, como $p \equiv \pm 1 \pmod 5$, temos $p^a(p-1) - 1 \equiv -1 \pmod{\pi(p)}$ (pela propriedade (6) do período de Pisano). Logo, $F_{p^a(p-1)-1} \equiv 1 \pmod p$. Assim,

$$\frac{F_{p^a(p-1)+tz(p)}}{F_{tz(p)}} \equiv 1 \pmod p,$$

para todo $t \in [1, \lfloor \frac{p^a}{z(p)} \rfloor]$. □

Teorema 3.1. *Seja p um primo tal que $p \equiv \pm 1 \pmod 5$. Então*

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 \pmod p,$$

para todo $a \geq 0$.

Demonstração. Observe que

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix} - 1 = \frac{\prod_{k=1}^{\lfloor p^a/z(p) \rfloor} F_{kz(p)}}{F_1 \dots F_{p^a}} \Big(\prod_{k=1}^{\lfloor p^a/z(p) \rfloor} \frac{F_{p^a(p-1)+kz(p)}}{F_{kz(p)}} S_1 - S_2 \Big),$$

onde $S_1 = \prod_{j\in\mathcal{M}} F_{p^a(p-1)+j}$, $S_2 = \prod_{j\in\mathcal{M}} F_j$ e $\mathcal{M} = \{j \in [1, p^a] : z(p) \nmid j\}$.

Como $p \equiv \pm 1 \pmod 5$, temos que $\pi(p) \mid p-1$. Logo, $p^a(p-1)+j \equiv j \pmod{\pi(p)}$ e (pela propriedade (5)) temos que

$$F_{p^a(p-1)+j} \equiv F_j \pmod p.$$

Em particular, $S_1 \equiv S_2 \pmod p$. Concluímos pelo Lema 3.1.1 que

$$\prod_{k=1}^{\lfloor p^a/z(p)\rfloor} \frac{F_{p^a(p-1)+kz(p)}}{F_{kz(p)}} S_1 \equiv S_2 \pmod p.$$

Por outro lado, a hipótese $p \equiv \pm 1 \pmod 5$ implica que $z(p) \mid p-1$. Então pelo Lema 1.1.1 observamos que

$$\nu_p\Big(\prod_{k=1}^{\lfloor p^a/z(p)\rfloor} F_{kz(p)}\Big) = \nu_p(F_1 \dots F_{p^a}),$$

pois $\nu_p(F_j) = 0$ quando $z(p) \nmid j$. Portanto, $\nu_p(\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F - 1) > 0$. □

Agora, usamos o mesmo raciocínio para efetuarmos uma pequena generalização no teorema anterior. Para isso provamos um lema semelhante ao Lema 3.1.1. Salientamos que o próximo lema independe do primo módulo 5.

Lema 3.1.2. *Seja $a \geq 0$, $k \geq 1$ e $p \neq 2, 5$. Temos*

$$\frac{F_{p^a(p^{2k}-1)+tz(p)}}{F_{tz(p)}} \equiv 1 \pmod p,$$

para todo $t \in [1, \lfloor \frac{p^a}{z(p)} \rfloor]$ e $k \in \mathbb{Z}$.

Demonstração. Novamente pela fórmula da adição

$$\frac{F_{p^a(p^{2k}-1)+tz(p)}}{F_{tz(p)}} = F_{p^a(p^{2k}-1)-1} + \frac{F_{p^a(p^{2k}-1)}}{F_{tz(p)}} F_{tz(p)+1}.$$

Pelas propriedades de valorização p-ádica temos

$$\nu_p\Big(\frac{F_{p^a(p^{2k}-1)}}{F_{tz(p)}}\Big) = \nu_p(F_{p^a(p^{2k}-1)}) - \nu_p(F_{tz(p)}) = a - \nu_p(t) > 0,$$

pois $(p, z(p)) = 1$ e $t < p^a$. Por outro lado, note que

$$p^{2k} - 1 = (p^2)^k - 1 = (p^2-1)((p^2)^{k-1} + \cdots + 1) = (p+1)(p-1)(p^{2k-2} + \cdots + 1)$$

$$= (p+1)(p-1)(p^{2k-2} + p^{2k-4} + \cdots + 1).$$

O período de Pisano é tal que $\pi(p) \mid p-1$ ou $\pi(p) \mid 2(p+1)$. Logo, $p^a(p^{2k}-1) + j \equiv j \pmod{\pi(p)}$ e (pela propriedade (5)) temos que $F_{p^a(p^{2k}-1)+j} \equiv F_j \pmod p$. Decorre que $F_{p^a(p^{2k}-1)-1} \equiv 1 \pmod p$, pois $p^a(p^{2k}-1) - 1 \equiv -1 \pmod{\pi(p)}$. Assim,

$$\frac{F_{p^a(p^{2k}-1)+tz(p)}}{F_{tz(p)}} \equiv 1 \pmod p,$$

para todo $t \in [1, \lfloor \frac{p^a}{z(p)} \rfloor]$. □

De posse do lema anterior, observamos que mesmo adicionando uma quantidade par de potências do primo p continuamos com o mesmo resto módulo p. Assim conseguimos uma sutil generalização do Teorema 3.1. Vejamos a seguir.

Teorema 3.2. *Seja $a \geq 0$, $k \geq 1$ e $p \neq 2, 5$ primo, então*

$$\begin{bmatrix} p^{a+2k} \\ p^a \end{bmatrix}_F \equiv 1 \pmod p.$$

Demonstração. Observe que

$$\begin{bmatrix} p^{a+2k} \\ p^a \end{bmatrix}_F - 1 = \frac{\prod_{k=1}^{\lfloor p^a/z(p) \rfloor} F_{kz(p)}}{F_1 \ldots F_{p^a}} \Big(\prod_{k=1}^{\lfloor p^a/z(p) \rfloor} \frac{F_{p^a(p^{2k}-1)+kz(p)}}{F_{kz(p)}} S_1 - S_2 \Big),$$

onde $S_1 = \prod_{j \in \mathcal{M}} F_{p^a(p^{2k}-1)+j}$, $S_2 = \prod_{j \in \mathcal{M}} F_j$ e $\mathcal{M} = \{j \in [1, p^a] : z(p) \nmid j\}$.

Particularmente, pelo Lema 3.1.2 temos que $S_1 \equiv S_2 \pmod p$. Além disso, pelo Lema 1.1.1 temos que, $p \mid F_{p^a(p^{2k}-1)+j}$ se, e somente se, $z(p) \mid j$. Como vimos anteriormente, $\nu_p\Big(\frac{\prod_{k=1}^{\lfloor p^a/z(p) \rfloor} F_{kz(p)}}{F_1 \ldots F_{p^a}}\Big) = 0$ e

$$\prod_{k=1}^{\lfloor p^a/z(p) \rfloor} \frac{F_{p^a(p^{2k}-1)+kz(p)}}{F_{kz(p)}} S_1 \equiv S_2 \pmod p,$$

Assim, $\nu_p(\begin{bmatrix} p^{a+2k} \\ p^a \end{bmatrix} - 1) > 0$. □

3.2 Resto do coeficiente fibonomial módulo p^2

Nessa seção precisaremos exigir um pouco mais da função ordem de aparição. Observamos, a partir do software *Mathematica*, que não existe padrão aparente para o resto da divisão quando aumentamos a potência de p. De fato, os primos 29 e 41 tem a propriedade de $z(p) = (p-1)/2$, e

$$\begin{bmatrix} p^2 \\ p \end{bmatrix}_F \equiv 88, 124 \equiv 1 + 3p \pmod{p^2},$$

respectivamente. Já os primos 11 e 19, que satisfazem $z(p) = p-1$, são da seguinte forma

$$\begin{bmatrix} p^2 \\ p \end{bmatrix}_F \equiv 12, 20 \equiv 1 + p \pmod{p^2}.$$

Conjecturamos que $\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 + 3p \pmod{p^2}$, e $\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 + p \pmod{p^2}$, quando $z(p) = (p-1)/2$ e $z(p) = p-1$, respectivamente. Acreditamos que a demonstração da conjectura, quando $z(p) = (p-1)/2$, é similar ao caso que estudaremos nessa seção.

Vejamos no teorema a seguir que quando $z(p) = p-1$ e $k = 2$ nossa conjectura é verdadeira.

Teorema 3.3. *Seja p um primo tal que $z(p) = p-1$. Então*

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 + p \pmod{p^2},$$

para todo $a \geq 2$.

Demonstração. Denotamos por $\mathcal{M}$ o conjunto dos $j \in [1, p^a]$ tais que $p-1 \nmid j$. Pelas propriedades do período de Pisano vale a seguinte cadeia $\pi(p^2) \mid p(p-1) \mid p^a(p-1)$. Então, $F_{p^a(p-1)+j} \equiv F_j \pmod{p^2}$, pois $p^a(p-1) + j \equiv j \pmod{\pi(p^2)}$, para todo $j \in \mathcal{M}$. Assim,

$$\prod_{j \in \mathcal{M}} \frac{F_{p^a(p-1)+j}}{F_j} \equiv 1 \pmod{p^2},$$

pois $(\prod_{j \in \mathcal{M}} F_j, p^2) = 1$. Logo, nosso coeficiente fibonomial se reduz módulo p^2 à

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv \prod_{j=1}^{p^{a-1}+\cdots+1} \frac{F_{p^a(p-1)+j(p-1)}}{F_{j(p-1)}} \pmod{p^2}.$$

Aqui usamos que $p^a - 1 = (p-1)(p^{a-1} + \cdots + 1)$.

Por outro lado, pela fórmula da adição

$$\frac{F_{p^a(p-1)+j(p-1)}}{F_{j(p-1)}} = F_{p^a(p-1)-1} + \frac{F_{p^a(p-1)}F_{j(p-1)+1}}{F_{j(p-1)}}.$$

Sendo $j \in [1, p^{a-1} + \cdots + 1] \setminus \{p^{a-1}\}$, temos

$$\begin{aligned}\nu_p\Big(\frac{F_{p^a(p-1)}F_{j(p-1)+1}}{F_{j(p-1)}}\Big) &= \nu_p(F_{p^a(p-1)}F_{j(p-1)+1}) - \nu_p(F_{j(p-1)}) \\ &\geq a + e(p) - (a - 2 + e(p)) = 2,\end{aligned}$$

pois $\nu_p(j) \leq a-2$ e $p^{a-1} + \cdots + 1 < 2p^{a-1}$. Assim, $\frac{F_{p^a(p-1)}F_{j(p-1)+1}}{F_{j(p-1)}} \equiv 0 \pmod{p^2}$. Usamos o fato de $F_{p^a(p-1)-1} \equiv 1 \pmod{p^a}$ e concluímos que $\frac{F_{p^a(p-1)+j(p-1)}}{F_{j(p-1)}} \equiv 1 \pmod{p^2}$, para $j \in [1, p^{a-1} + \cdots + 1] \setminus \{p^{a-1}\}$.

Logo, precisamos analisar o caso em que $j = p^{a-1}$. Pela fórmula da adição

$$\frac{F_{p^a(p-1)+p^{a-1}(p-1)}}{F_{p^{a-1}(p-1)}} = F_{p^a(p-1)-1} + \frac{F_{p^a(p-1)}F_{p^{a-1}(p-1)+1}}{F_{p^{a-1}(p-1)}}.$$

Utilizamos a fórmula de múltiplos ângulos com $k = p$, $n = p^{a-1}(p-1)$ e $c = 0$ para obter

$$\frac{F_{p^a(p-1)}}{F_{p^{a-1}(p-1)}} = \sum_{i=1}^{p} \binom{p}{i} F_{-i} F^{i-1}_{p^{a-1}(p-1)} F^{p-i}_{p^a(p-1)+1}.$$

Note que $p \mid \binom{p}{i}$ quando $i \in [2, p]$ e $p \mid F_{p^{a-1}(p-1)}$. Logo,

$$\frac{F_{p^a(p-1)}F_{p^a(p-1)+1}}{F_{p^{a-1}(p-1)}} \equiv pF^p_{p^a(p-1)+1} \pmod{p^2}.$$

Além disso, sendo $F^p_{p^a(p-1)+1} \equiv 1 \pmod{p^2}$, temos

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 + p \pmod{p^2}.$$

□

3.3 Resto do coeficiente fibonomial módulo p^3

Para módulo p^3 temos o seguinte resultado.

Teorema 3.4. *Seja p um primo tal que $z(p) = p - 1$. Então*

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 + p + p^2 \pmod{p^3},$$

para todo $a \geq 3$.

Demonstração. Pela definição de coeficiente fibonomial, temos

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F = \prod_{j=1}^{p^a} \frac{F_{p^a(p-1)+j}}{F_j}.$$

Primeiro vamos definir o conjunto $\mathcal{M}$ como o conjunto dos $j \in [1, p^a]$ tais que $p - 1 \nmid j$. Pela propriedade do período de Pisano $\pi(p^a)$ divide $p^{a-1}\pi(p) = p^{a-1}(p-1)$. Então, $p^a(p-1) + j \equiv j \pmod{\pi(p^3)}$, onde $j \in \mathcal{M}$. Temos

$$\prod_{j \in \mathcal{M}} \frac{F_{p^a(p-1)+j}}{F_j} \equiv 1 \pmod{p^3}.$$

pois $(\prod_{j\in\mathcal{M}} F_j, p^3) = 1$. Logo, nosso coeficiente fibonomial se reduz módulo p^3 à

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv \prod_{j=1}^{p^{a-1}+\cdots+1} \frac{F_{p^a(p-1)+j(p-1)}}{F_{j(p-1)}} \pmod{p^3}.$$

Nossa primeira afirmação será colocada de forma mais geral para que nosso estudo fique o mais completo possível.

Afirmação 3.3.1. *Se $p \nmid j$, então $\frac{F_{p^a(p-1)+j(p-1)}}{F_{j(p-1)}} \equiv 1 \pmod{p^a}$.*

Demonstração. Pela fórmula da adição

$$\frac{F_{p^a(p-1)+j(p-1)}}{F_{j(p-1)}} = F_{p^a(p-1)-1} + \frac{F_{p^a(p-1)}F_{j(p-1)+1}}{F_{j(p-1)}}.$$

Note que

$$\begin{aligned} \nu_p\Big(\frac{F_{p^a(p-1)}F_{j(p-1)+1}}{F_{j(p-1)}}\Big) &= \nu_p(F_{p^a(p-1)}F_{j(p-1)+1}) - \nu_p(F_{j(p-1)}) \\ &= \nu_p(p^a(p-1)) - \nu_p(j) = a \end{aligned}$$

e assim, $\frac{F_{p^a(p-1)}F_{j(p-1)+1}}{F_{j(p-1)}} \equiv 0 \pmod{p^a}$. Portanto, $\frac{F_{p^a(p-1)+j(p-1)}}{F_{j(p-1)}} \equiv 1 \pmod{p^a}$, onde usamos que $F_{p^a(p-1)-1} \equiv 1 \pmod{p^a}$. □

Logo, precisamos analisar os quocientes da seguinte forma

$$\frac{F_{p^a(p-1)+jp(p-1)}}{F_{jp(p-1)}},$$

e segue de $\lfloor \frac{p^a-1}{p(p-1)} \rfloor = \lfloor \frac{p^{a-1}+\cdots+1}{p} \rfloor = p^{a-2}+\cdots+1$ que $j \in [1, p^{a-2}+\cdots+1]$. Com isso reduzimos nosso problema a mostrar que

$$S := \prod_{j=1}^{r} \frac{F_{p^a(p-1)+jp(p-1)}}{F_{jp(p-1)}} \equiv 1+p+p^2 \pmod{p^3},$$

onde $r := p^{a-2}+\cdots+1$. Note que podemos escrever S da seguinte forma

$$\prod_{j=1}^{r} \frac{F_{p^a(p-1)+jp(p-1)}}{F_{jp(p-1)}} = \prod_{j=1}^{r} \Big(F_{p^a(p-1)-1} + \frac{F_{p^a(p-1)}F_{jp(p-1)+1}}{F_{jp(p-1)}} \Big) = \prod_{j=1}^{r} (\lambda - y(j)),$$

onde $\lambda = F_{p^a(p-1)-1}$ *e* $y(j) = -\frac{F_{p^a(p-1)}F_{jp(p-1)+1}}{F_{jp(p-1)}}$. Pela Proposição 1.5.1, citada nas preliminares sobre funções simétricas, podemos reescrever S da seguinte forma

$$S = \lambda^r - \sigma_1(\overline{y})\lambda^{r-1} + \cdots + (-1)^r \sigma_r(\overline{y}), \tag{3.1}$$

onde $\sigma_{j's}(\overline{y})$ são as funções simétricas elementares e $\overline{y} = (y(1), \ldots, y(r))$. Como $\lambda \equiv 1 \pmod{p^3}$, temos que

$$\prod_{j=1}^{r} \frac{F_{p^a(p-1)+jp(p-1)}}{F_{jp(p-1)}} \equiv 1 + \sigma_1(\overline{x}) + \cdots + \sigma_r(\overline{x}) \pmod{p^3},$$

onde $\overline{x} = (x(1), \ldots, x(r))$ e $x(j) = -y(j)$.

Observamos agora que a partir de um certo k as funções simétricas elementares são congruentes a zero módulo p^3. Vejamos:

Afirmação 3.3.2. *Se $k \in [2, r]$, então $\sigma_k(\overline{x}) \equiv 0 \pmod{p^3}$.*

Demonstração. Lembre que

$$\sigma_j(\overline{x}) = \sum_{1 \le i_1 < \cdots < i_k \le r} x(i_1) \cdots x(i_k).$$

Logo, a valorização p-ádica de cada termo do somatório é

$$\begin{aligned} \nu_p(x(i_1)\cdots x(i_k)) &= \sum_{j=1}^{k} \nu_p\Big(\frac{F_{p^a(p-1)}F_{i_j p(p-1)+1}}{F_{i_j p(p-1)}} \Big) \\ &= \sum_{j=1}^{k} \nu_p(p^a(p-1)) + e(p) - \nu_p(i_j) - 1 - e(p) \\ &= k(a-1) - \sum_{j=1}^{k} \nu_p(i_j). \end{aligned}$$

Por outro lado, $i_j \leq r < 2p^{a-2}$. De fato, $r < \frac{p^a-1}{p(p-1)} < \frac{p^a}{p\cdot p/2} = 2p^{a-2}$. Daí,

$$\nu_p(x(i_1)\cdots x(i_k)) \geq k(a-1) - (a-2) - (k-1)(a-3) = 2k-1 \geq 3,$$

pois $k \geq 2$. Assim, $\nu_p(\sigma_k(\overline{x})) \geq 3$. Portanto, $\sigma_k(\overline{x}) \equiv 0 \pmod{p^3}$, para todo $k \geq 2$. □

Com isso nosso problema fica reduzido a

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 + \sigma_1(\overline{x}) \equiv 1 + x(1) + \cdots + x(r) \pmod{p^3}.$$

Afirmação 3.3.3. *Se $j \in [1,r] \setminus \{ip^{a-3} : i \in [1,p+1]\}$, então $x(j) \equiv 0 \pmod{p^3}$.*

Demonstração. Seja

$$x(j) = \frac{F_{p^a(p-1)+jp(p-1)}}{F_{jp(p-1)}},$$

com $j \in [1,r] \setminus \{ip^{a-3} : i \in [1,p+1]\}$. Novamente vamos analisar a valorização p-ádica de $x(j)$. Temos

$$\nu_p(x(j)) = \nu_p(F_{p^a(p-1)}F_{jp(p-1)+1}) - \nu_p(F_{jp(p-1)}) = a - 1 - \nu_p(j).$$

Observe que $(p+2)p^{a-3} > r$. De fato,

$$p^{a-3} + \cdots + 1 = \frac{p^{a-2}-1}{p-1} < \frac{p^{a-2}}{p/2} = 2p^{a-3} \Rightarrow p^{a-2} + \cdots + 1 < (p+2)p^{a-3}.$$

Logo, $\nu_p(j) \leq a-4$ e assim, $\nu_p(x(j)) \geq a-1-(a-4) = 3$. Portanto, $x(j) \equiv 0 \pmod{p^3}$, para todo $j \in [1,r] \setminus \{ip^{a-3} : i \in [1,p+1]\}$. □

Temos por consequência da afirmação acima que a primeira função simétrica fica mais simples módulo p^3, isto é,

$$\sigma_1(\overline{x}) \equiv \sum_{i=1}^{p+1} x(ip^{a-3}) \pmod{p^3}.$$

Logo, nosso coeficiente fibonomial tem a seguinte forma módulo p^3

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 + \sum_{i=1}^{p+1} x(ip^{a-3}) \pmod{p^3}.$$

No próximo passo vamos analisar o que acontece com algumas combinações dos $x(ip^{a-3})$ para $i \in [1,p+1]$.

Afirmação 3.3.4. *Sejam $i, j \in [1, p-1]$, com $i + j = p$. Então $x(ip^{a-3}) + x(jp^{a-3}) \equiv 0 \pmod{p^3}$.*

Demonstração. Sejam $i, j \in [1, p-1]$. Então

$$x(ip^{a-3}) + x(jp^{a-3}) = \frac{F_{p^a(p-1)}F_{ip^{a-2}(p-1)+1}}{F_{ip^{a-2}(p-1)}} + \frac{F_{p^a(p-1)}F_{jp^{a-2}(p-1)+1}}{F_{jp^{a-2}(p-1)}}$$

$$= \frac{F_{p^a(p-1)}}{F_{ip^{a-2}(p-1)}F_{jp^{a-2}(p-1)}}\Big[F_{jp^{a-2}(p-1)}F_{ip^{a-2}(p-1)+1} + F_{ip^{a-2}(p-1)}F_{jp^{a-2}(p-1)+1}\Big].$$

Agora, usamos a definição da sequência de Fibonacci e obtemos

$$\frac{F_{p^a(p-1)}}{F_{ip^{a-2}(p-1)}F_{jp^{a-2}(p-1)}}\Big[F_{jp^{a-2}(p-1)}F_{ip^{a-2}(p-1)}+F_{jp^{a-2}(p-1)}F_{ip^{a-2}(p-1)-1}+F_{ip^{a-2}(p-1)}F_{jp^{a-2}(p-1)+1}\Big].$$

Observamos que pela fórmula aditiva de números de Fibonacci

$$\frac{F_{p^a(p-1)}}{F_{ip^{a-2}(p-1)}F_{jp^{a-2}(p-1)}}\Big[F_{jp^{a-2}(p-1)}F_{ip^{a-2}(p-1)} + F_{jp^{a-2}(p-1)+ip^{a-2}(p-1)}\Big].$$

Por fim, usamos a hipótese de $i + j = p$ e chegamos em

$$\frac{F_{p^a(p-1)}}{F_{ip^{a-2}(p-1)}F_{jp^{a-2}(p-1)}}\Big[F_{jp^{a-2}(p-1)}F_{ip^{a-2}(p-1)} + F_{p^{a-1}(p-1)}\Big].$$

Note que

$$\nu_p(F_{jp^{a-2}(p-1)}F_{ip^{a-2}(p-1)}) = \nu_p(i) + \nu_p(j) + 2a - 4 + 2e(p) = 2a - 4 + 2e(p)$$

e

$$\nu_p(F_{p^a(p-1)}) = a - 1 + e(p).$$

Como $2a - 4 + 2e(p) > a - 1 + e(p)$, para $a \geq 3$, temos que

$$\nu_p(F_{jp^{a-2}(p-1)}F_{ip^{a-2}(p-1)} + F_{p^{a-1}(p-1)}) = a - 1 + e(p),$$

onde usamos o fato de que $\nu_p(m + n) = \min\{\nu_p(m), \nu_p(n)\}$ se $\nu_p(m) \neq \nu_p(n)$. Logo,

$$\nu_p(x(ip^{a-3}) + x(jp^{a-3})) = a + e(p) + a - 1 + e(p) - (2(a-2) + e(p)) = 3.$$

Portanto, $x(ip^{a-3}) + x(jp^{a-3}) \equiv 0 \pmod{p^3}$, quando $i + j = p$. □

Aplicamos a afirmação anterior para os pares $(i,j) = (k+1, p-1-k)$ para $k \in [0,(p-3)/2]$. Concluímos que

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 + x(p^{a-2}) + x((p+1)p^{a-3}) \pmod{p^3}.$$

Afirmação 3.3.5. *Temos que* $x(p^{a-2}) \equiv p \pmod{p^3}$.

Demonstração. Usamos a fórmula de múltiplos ângulos para $k = p$, $n = p^{a-1}(p-1)$ e $c = 0$. Logo,

$$x(p^{a-2}) = \frac{F_{p^a(p-1)}F_{p^a(p-1)+1}}{F_{p^{a-1}(p-1)}} = \sum_{i=1}^{p} \binom{p}{i} F_{-i} F^{i-1}_{p^{a-1}(p-1)} F^{p-i+1}_{p^a(p-1)+1}.$$

Observe que

$$\nu_p\left(\binom{p}{i} F^{i-1}_{p^{a-1}(p-1)}\right) = \begin{cases} 1 + (i-1)(a-1+e(p)), & i \in [2, p-1] \\ (p-1)(a-1+e(p)), & i = p. \end{cases}$$

Logo, $\nu_p(\binom{p}{i} F^{i-1}_{p^{a-1}(p-1)}) \geq 3$, para todo $i \in [2,p]$. Assim,

$$\frac{F_{p^a(p-1)}F_{p^{a-1}(p-1)+1}}{F_{p^{a-1}(p-1)}} \equiv pF^p_{p^{a-1}(p-1)+1} \pmod{p^3}$$

e consequentemente,

$$x(p^{a-2}) \equiv p \pmod{p^3},$$

pois $F_{p^{a-1}(p-1)+1} \equiv 1 \pmod{p^3}$. □

Então,

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 + p + x((p+1)p^{a-3}) \pmod{p^3}.$$

Afirmação 3.3.6. *Temos que* $x((p+1)p^{a-3}) \equiv p^2 \pmod{p^3}$.

Demonstração. Lembre que

$$x((p+1)p^{a-3}) = \frac{F_{p^a(p-1)}F_{p^{a-2}(p-1)(p+1)+1}}{F_{p^{a-2}(p-1)(p+1)}} = \frac{F_{p^a(p-1)}F_{p^{a-2}(p^2-1)+1}}{F_{p^{a-2}(p^2-1)}}.$$

Agora, usamos a fórmula de múltiplos ângulos para $k = p^2$, $n = p^{a-2}(p-1)$ e $c = 0$. Temos,

$$\frac{F_{p^a(p-1)}F_{p^{a-2}(p^2-1)+1}}{F_{p^{a-2}(p^2-1)}} = \sum_{i=1}^{p^2} \binom{p^2}{i} F_{-i} \frac{F^i_{p^{a-2}(p-1)}}{F_{p^{a-2}(p^2-1)}} F^{p^2-i+1}_{p^{a-2}(p-1)+1}.$$

Note que

$$\nu_p\Big(\binom{p^2}{i}\frac{F^i_{p^{a-2}(p-1)}}{F_{p^{a-2}(p^2-1)}}\Big) \geq \begin{cases} 1+(i-1)(a-2+e(p)), & i\in[2,p^2-1] \\ (p^2-1)(a-2+e(p)), & i=p^2. \end{cases}$$

Portanto, $\nu_p\Big(\binom{p^2}{i}\frac{F^i_{p^{a-2}(p-1)}}{F_{p^{a-2}(p^2-1)}}\Big) \geq 3$ e assim,

$$\frac{F_{p^a(p-1))}}{F_{p^{a-2}(p^2-1)}} \equiv p^2\frac{F_{p^{a-2}(p-1)}}{F_{p^{a-2}(p^2-1)}}F^{p^2-1}_{p^{a-2}(p-1)+1} \pmod{p^3}. \tag{3.2}$$

Agora, afirmamos que

$$\frac{F_{p^{a-2}(p^2-1)}}{F_{p^{a-2}(p-1)}} \equiv p+1 \pmod{p^3}.$$

De fato, usamos novamente a fórmula de múltiplos ângulos para $k=p+1$, $n=p^{a-2}(p-1)$ e $c=0$ e obtemos

$$\frac{F_{p^a(p^2-1)}}{F_{p^{a-2}(p-1)}} = \sum_{i=1}^{p+1}\binom{p+1}{i}F_{-i}F^{i-1}_{p^{a-2}(p-1)}F^{p+1-i}_{p^{a-2}(p-1)+1}.$$

Note que a valorização p-ádica é

$$\nu_p\Big(\binom{p+1}{i}F^{i-1}_{p^{a-2}(p-1)}\Big) \geq \begin{cases} 1+(i-1)(a-2+e(p)), & i\in[2,p-1] \\ (p-1)(a-2+e(p)), & i\in\{p,p+1\}. \end{cases}$$

Consequentemente, $\nu_p(\binom{p+1}{i}F^{i-1}_{p^{a-2}(p-1)}) \geq 3$, para $i\in[2,p+1]$. Assim,

$$\frac{F_{p^{a-2}(p^2-1)}}{F_{p^{a-2}(p-1)}} \equiv p+1 \pmod{p^3}, \tag{3.3}$$

pois $F^p_{p^{a-2}(p-1)+1} \equiv 1 \pmod{p^3}$ e $p \mid \binom{p+1}{i}$, para $i\in[1,p]$.

Além disso, mostramos que

$$\frac{F_{p^{a-2}(p-1)}}{F_{p^{a-2}(p^2-1)}} \equiv p^2-p+1 \pmod{p^3}.$$

De fato, observe que

$$p^3+1=(p+1)(p^2-p+1)$$

Pela equação (3.3) obtemos

$$1 \equiv p^3+1 \equiv \frac{F_{p^{a-2}(p^2-1)}}{F_{p^{a-2}(p-1)}}(p^2-p+1) \pmod{p^3}.$$

Como $\nu_p(\frac{F_{p^{a-2}(p-1)}}{F_{p^{a-2}(p^2-1)}}) = 0$, temos das propriedades de congruência para números racionais que

$$\frac{F_{p^{a-2}(p-1)}}{F_{p^{a-2}(p^2-1)}} \equiv p^2 - p + 1 \pmod{p^3}$$

como desejávamos. Portanto, voltamos para a equação (3.2) e concluímos que

$$\frac{F_{p^a(p-1)}}{F_{p^{a-2}(p^2-1)}} \equiv p^2(p^2 - p + 1) \pmod{p^3}$$

e por conseguinte

$$x((p+1)p^{a-3}) \equiv p^2 \pmod{p^3},$$

pois $F_{p^{a-2}(p^2-1)+1} \equiv 1 \pmod{p^3}$. □

Finalmente chegamos no resultado desejado, isto é,

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 + p + p^2 \pmod{p^3}.$$

□

3.4 Resto do coeficiente fibonomial módulo p^4

Por fim, conseguimos mostrar que esse padrão se mantém quando aumentamos a congruência para p^4.

Teorema 3.5. *Seja p um primo tal que $z(p) = p - 1$. Então*

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 + p + p^2 + p^3 \pmod{p^4},$$

para todo $a \geq 4$.

Demonstração. Por definição temos que

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F = \prod_{j=1}^{p^a} \frac{F_{p^a(p-1)+j}}{F_j}.$$

Como $\pi(p^a) \mid p^a(p-1)$, temos $p^a(p-1) + j \equiv j \pmod{\pi(p^4)}$, para todo $j \in M$, onde $M = \{j \in [1, p^a] : p - 1 \nmid j\}$. Logo,

$$\prod_{j \in M} F_{p^a(p-1)+j} \equiv \prod_{j \in M} F_j \pmod{p^4}.$$

Note que $(\prod_{j\in M} F_j, p^4) = 1$. Então,

$$\prod_{j\in M} \frac{F_{p^a(p-1)+j}}{F_j} \equiv 1 \pmod{p^4}.$$

Assim, pelas propriedades de congruência para racionais temos

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv \prod_{j=1}^{p^{a-1}+\cdots+1} \frac{F_{p^a(p-1)+j(p-1)}}{F_{j(p-1)}} \pmod{p^4}.$$

Dividimos nossa prova em pequenas afirmações com o objetivo de tornar nossa exposição mais clara.

Afirmação 3.4.1. *Se $p \nmid j$, então $\frac{F_{p^a(p-1)+j(p-1)}}{F_{j(p-1)}} \equiv 1 \pmod{p^4}$.*

Demonstração. De fato, pela fórmula da adição

$$\frac{F_{p^a(p-1)+j(p-1)}}{F_{j(p-1)}} = F_{p^a(p-1)-1} + \frac{F_{p^a(p-1)}F_{j(p-1)+1}}{F_{j(p-1)}}.$$

Note que $F_{p^a(p-1)-1} \equiv 1 \pmod{p^4}$ e

$$\nu_p\Big(\frac{F_{p^a(p-1)}F_{j(p-1)+1}}{F_{j(p-1)}}\Big) = \nu_p(p^a(p-1)) + e(p) - (\nu_p(j) + e(p)) = a - \nu_p(j) = a \geq 4.$$

Segue então o resultado. □

Sendo assim

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv \prod_{j=1}^{r} \frac{F_{p^a(p-1)+jp(p-1)}}{F_{jp(p-1)}} \pmod{p^4},$$

onde $r := p^{a-2} + \cdots + 1$. Escrevemos a congruência acima da seguinte forma

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F == \prod_{j=1}^{r} \Big(F_{p^a(p-1)-1} + \frac{F_{p^a(p-1)}F_{jp(p-1)+1}}{F_{jp(p-1)}}\Big) = \prod_{j=1}^{r}(\lambda - y(j)),$$

onde $\lambda = F_{p^a(p-1)-1}$ e $y(j) := -\frac{F_{p^a(p-1)}F_{jp(p-1)+1}}{F_{jp(p-1)}}$. Novamente, usaremos que

$$\prod_{j=1}^{r}(\lambda - y(j)) = \lambda^r - \sigma_1(\overline{y})\lambda^{r-1} + \cdots + (-1)^r\sigma_r(\overline{y}),$$

onde σ_j é a j-ésima função simétrica e $\overline{y} = (y(1), \ldots, y(r))$. Assim,

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv \prod_{j=1}^{r} \frac{F_{p^a(p-1)+jp(p-1)}}{F_{jp(p-1)}} \equiv 1 + \sigma_1(\overline{x}) + \cdots + \sigma_r(\overline{x}) \pmod{p^4}$$

onde $\overline{x} := (x(1), \ldots, x(r))$, $x(j) = -y(j)$ e $\lambda \equiv 1 \pmod{p^4}$.

Observamos que as funções simétricas elementares são zeros módulo p^4 quando o grau é maior do que ou igual a 3.

Afirmação 3.4.2. *Se $k \in [3, r]$, então $\sigma_k(\overline{x}) \equiv 0 \pmod{p^4}$.*

Demonstração. Com efeito, seja

$$\sigma_k(\overline{x}) = \sum_{1 \leq i_1 < \cdots < i_k \leq r} x(i_1) \cdots x(i_k).$$

Então cada termo do somatório é da seguinte forma

$$x(i_1) \cdots x(i_k) = (F_{p^a(p-1)})^k \prod_{j=1}^{k} \frac{F_{i_j p(p-1)+1}}{F_{i_j p(p-1)}}.$$

Daí, $\nu_p(x(i_1) \cdots x(i_k)) = ak - k - \sum_{j=1}^{k} \nu_p(i_j)$. Contudo $i_k \leq r < 2p^{a-2}$. Logo sem perda de generalidade, $\nu_p(i_k) \leq a-2$ e $\nu_p(i_j) \leq a-3$, para todo $j \in [1, k-1]$. Consequentemente,

$$\nu_p(x(i_1) \cdots x(i_k)) \geq ak - k - (k-1)(a-3) - (a-2) = 2k - 1 \geq 5,$$

para $k \geq 3$. Portanto

$$x(i_1) \cdots x(i_k) \equiv 0 \pmod{p^4},$$

e assim auferimos a afirmação. □

Desse modo, o coeficiente fibonomial módulo p^4 se restringe à

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 + \sigma_1(\overline{x}) + \sigma_2(\overline{x}) \pmod{p^4}.$$

Continuamos nossa averiguação no comportamento das funções simétricas elementares módulo p^4. Visamos agora suas componentes $x(i)$'s e concluímos que a menos de um subconjunto, a ser determinado, elas são nulas módulo p^4.

Afirmação 3.4.3. *Seja $j \in [1, r] \setminus N$, com $N := \{ip^{a-4} : i \in [1, p^2 + p + 1]\}$, então*

$$x(j) \equiv 0 \pmod{p^4}.$$

Demonstração. Note que $\nu_p(x(j)) = a - 1 - \nu_p(j)$. Como $j \in [1, r] \setminus \{ip^{a-4} : i \in [1, p^2 + p + 1]\}$, temos que $\nu_p(j) \leq a - 5$. Logo, $\nu_p(x(j)) \geq a - 1 - a + 5 = 4$ e chegamos no resultado. □

Pela afirmação anterior reduzimos a segunda função simétrica elementar módulo p^4 à

$$\sigma_2(\overline{x}) \equiv \sum_{1\leq i<j\leq p^2+p+1} x(ip^{a-4})x(jp^{a-4}) \pmod{p^4}.$$

Observamos que estudando a valorização p-ádica de alguns de seus termos podemos simplifica-la ainda mais. Efetivamente,

Afirmação 3.4.4. *Seja $i, j \in [1, p^2+p+1] \setminus \{p^2\}$, com $i \neq j$. Então*

$$x(ip^{a-4})x(jp^{a-4}) \equiv 0 \pmod{p^4}.$$

Demonstração. Sabemos que

$$x(ip^{a-4})x(jp^{a-4}) = \frac{F^2_{p^a(p-1)}F_{ip^{a-3}(p-1)+1}F_{jp^{a-3}(p-1)+1}}{F_{ip^{a-3}(p-1)}F_{jp^{a-3}(p-1)}}.$$

Então $\nu_p(x(ip^{a-4})x(jp^{a-4})) = 2a - \nu_p(i) - \nu_p(j) - 2(a-3) = 6 - \nu_p(i) - \nu_p(j)$. Como $i, j \in [1, p^2+p+1] \setminus \{p^2\}$, temos $\nu_p(i),\ \nu_p(j) \leq 1$. Daí, $\nu_p(x(ip^{a-4})x(jp^{a-4})) \geq 4$ e chegamos assim no resultado. □

Agora, notamos que pelo fato de $i < j$ podemos reescrever $\sigma_2(\overline{x})$. Segue da Afirmação 3.4.4 que

$$\sigma_2(\overline{x}) \equiv x(p^{a-2})(\sigma_1(\overline{x}) - x(p^{a-2})) \pmod{p^4}.$$

Observamos que nosso problema foi reduzido a analisar a primeira função simétrica, ou seja,

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 + \sigma_1(\overline{x}) + x(p^{a-2})(\sigma_1(\overline{x}) - x(p^{a-2})) \pmod{p^4}.$$

Pela Afirmação 3.4.3 sabemos que

$$\sigma_1(\overline{x}) \equiv \sum_{i=1}^{p^2+p+1} x(ip^{a-4}) \pmod{p^4}.$$

Definimos anteriormente o seguinte conjunto

$$N := \{ip^{a-4} : i \in [1, p^2+p+1]\}.$$

Agora consideramos os seguintes subconjuntos de $[1, p^2+p+1]$. Denote $N_1 = [1, p-1]$, $N_2 = [p+2, p^2-p-2] \setminus \{tp : t \in [2, p-2]\}$ e $N_3 = [p^2-p-1, p^2+p+1] \setminus \{p^2-p, p, p^2+p\}$.

Afirmação 3.4.5. *Seja $i, j \in N_1$ tais que $i + j = p$. então*

$$x(ip^{a-4}) + x(jp^{a-4}) \equiv 0 \pmod{p^4}.$$

Demonstração. Pela definição temos que

$$x(ip^{a-4}) + x(jp^{a-4}) = \frac{F_{p^a(p-1)}}{F_{ip^{a-3}(p-1)}F_{jp^{a-3}(p-1)}}[F_{ip^{a-3}(p-1)}F_{jp^{a-3}(p-1)} + F_{(i+j)p^{a-3}(p-1)}].$$

Note que,

$$\nu_p(F_{ip^{a-3}(p-1)}F_{jp^{a-3}(p-1)}) = \nu_p(i) + \nu_p(j) + 2a - 6 + 2e(p)$$

e

$$\nu_p(F_{(i+j)p^{a-3}(p-1)}) = \nu_p(i + j) + a - 3 + e(p).$$

Logo, sendo $i, j \in N_1$ e $i + j = p$ temos

$$\begin{aligned}\nu_p(F_{ip^{a-3}(p-1)}F_{jp^{a-3}(p-1)}) &= \nu_p(i) + \nu_p(j) + 2a - 6 + 2e(p) = 2a - 6 + 2e(p)\\ &= 2a - 6 + 2e(p) = a - 3 + e(p) + a - 3 + e(p)\\ &> a - 3 + e(p) + 1 = a - 2 + e(p) = \nu_p(F_{(i+j)p^{a-3}(p-1)}).\end{aligned}$$

Assim,

$$\begin{aligned}\nu_p(x(ip^{a-4}) + x(jp^{a-4})) &\geq a + e(p) - \nu_p(i) - \nu_p(j) - 2a + 6 - 2e(p)\\ &\quad + \min\{(\nu_p(i) + \nu_p(j) + 2a - 6 + 2e(p), \nu_p(i + j) + a - 3 + e(p)\}\\ &\geq a + e(p) + a - 2 + e(p) - 2(a - 3) - 2e(p) = 4,\end{aligned}$$

onde usamos o fato de que $\nu_p(m + n) = \min\{\nu_p(m), \nu_p(n)\}$ se $\nu_p(m) \neq \nu_p(n)$. Portanto, $x(ip^{a-4}) + x(jp^{a-4}) \equiv 0 \pmod{p^4}$ para $i, j \in N_1$ e $i + j = p$. □

Afirmação 3.4.6. *Seja $i, j \in N_2$ tais que $i + j = p^2$. Então*

$$x(ip^{a-4}) + x(jp^{a-4}) \equiv 0 \pmod{p^4}.$$

Demonstração. Como na afirmação anterior observamos que nesse caso $\nu_p(i) = \nu_p(j) = 0$, já que $i, j \in N_2$ e

$$\begin{aligned}\nu_p(F_{ip^{a-3}(p-1)}F_{jp^{a-3}(p-1)}) &= 2a - 6 + 2e(p) = a - 1 + e(p) + a - 4 + e(p)\\ &\geq a - 1 + e(p) = \nu_p(F_{(i+j)p^{a-3}(p-1)}).\end{aligned}$$

Daí, $\nu_p(x(ip^{a-4}) + x(jp^{a-4})) \geq a + e(p) + a - 1 + e(p) - 2a + 6 - 2e(p) = 5$ e chegamos assim no resultado. □

Afirmação 3.4.7. *Seja $i, j \in N_3$ tais que $i + j = 2p^2$. Então*

$$x(ip^{a-4}) + x(jp^{a-4}) \equiv 0 \pmod{p^4}.$$

A demonstração é completamente análoga a afirmação anterior.

De posse dessas afirmações chegamos no seguinte resultado

$$\sigma_1(\overline{x}) \equiv \sum_{k=1}^{p+1} x(kp^{a-3}) + x((p+1)p^{a-4}) \pmod{p^4}.$$

Afirmação 3.4.8. *Note que*

$$\sum_{k=1}^{p-1} x(kp^{a-3}) \equiv 0 \pmod{p^4}.$$

Demonstração. Lembramos que $x(kp^{a-3}) = \frac{F_{p^a(p-1)}F_{kp^{a-2}(p-1)+1}}{F_{kp^{a-2}(p-1)}}$. Foi provado anteriormente, no Lema 1.5.2, que existem $j,\ s \in \mathbb{Z}$ com $(p, s) = 1$ tais que

$$F_{p^a(p-1)} \equiv sp^{a+j+1} \pmod{p^{a+j+3}},$$

$$F_{kp^{a-2}(p-1)} \equiv ksp^{a+j-1} \pmod{p^{a+j+1}}$$

e

$$F_{kp^{a-2}(p-1)+1} \equiv 1 \pmod{p^{a-2}}.$$

Então existem $r_1, r_2, r_3 \in \mathbb{Z}$ tais que

$$x(kp^{a-3}) = \frac{(sp^{a+j+1} + r_1p^{a+j+3})(1 + r_3p^{a-2})}{ksp^{a+j-1} + r_2p^{a+j+1}}.$$

Daí,

$$(ks + p^2)x(kp^{a-3}) = p^2(s + sr_3p^{a-2} + r_1p^2 + r_1r_3p^a).$$

Note que $\nu_p(x(kp^{a-3})) = a - (a-2) = 2$, pois $\nu_p(k) = 0$. Logo,

$$ksx(kp^{a-3}) \equiv sp^2 \pmod{p^4},$$

e portanto,

$$x(kp^{a-3}) \equiv \frac{p^2}{k} \pmod{p^4},$$

pois $(p, s) = 1$. Logo, concluímos que

$$\begin{aligned}\sum_{k=1}^{p-1} x(kp^{a-3}) &= \frac{1}{2}\sum_{k=1}^{p-1} x(kp^{a-3}) + x((p-k)p^{a-3}) \\ &\equiv \frac{1}{2}\sum_{k=1}^{p-1} p^2\Big(\frac{1}{k} + \frac{1}{p-k}\Big) \pmod{p^4} \\ &\equiv \sum_{k=1}^{p-1} \frac{p^3}{2k(p-k)} \pmod{p^4}.\end{aligned}$$

Uma vez que $\frac{p^3}{k(p-k)} \equiv -\frac{p^3}{k^2} \pmod{p^4}$, temos

$$\sum_{k=1}^{p-1} x(kp^{a-3}) \equiv \frac{p^3}{2}\sum_{k=1}^{p-1} \frac{-1}{k^2} \pmod{p^4}. \tag{3.4}$$

Por outro lado, como $\mathbb{Z}_p$ é corpo temos que todo elemento não nulo possui inverso. Além disso,

$$k^{-1} \equiv \frac{1}{k} \pmod{p} \Leftrightarrow kk^{-1} \equiv 1 \pmod{p}.$$

Logo,

$$\sum_{k=1}^{p-1} \frac{1}{k^2} \equiv \sum_{k=1}^{p-1} (k^{-1})^2 \equiv \sum_{k=1}^{p-1} m^2 \equiv \frac{p(p-1)(2p-1)}{6} \equiv 0 \pmod{p},$$

pois $p \neq 2, 3$. Daí, $\nu_p(\sum_{k=1}^{p-1} \frac{1}{k^2}) > 0$. Portanto, retornamos para (3.4) e concluímos que

$$\sum_{k=1}^{p-1} x(kp^{a-3}) \equiv 0 \pmod{p^4}.$$

□

Assim,

$$\sigma_1(\overline{x}) \equiv x(p^{a-2}) + x((p+1)p^{a-4}) + x((p+1)p^{a-3}) \pmod{p^4}.$$

Nas próximas afirmações encontraremos as congruências que vão caracterizar $\sigma_1(\overline{x})$ módulo p^4.

Afirmação 3.4.9. *Note que*

$$x(p^{a-2}) \equiv p \pmod{p^4}.$$

Demonstração. Seja

$$x(p^{a-2}) = \frac{F_{p^a(p-1)}F_{p^{a-1}(p-1)+1}}{F_{p^{a-1}(p-1)}}.$$

Pela fórmula de múltiplos ângulos para $k = p$, $n = p^{a-1}(p-1)$ e $c = 0$ temos

$$x(p^{a-2}) = \sum_{i=1}^{p} \binom{p}{i} F_{-i} F^{i-1}_{p^{a-1}(p-1)} F^{p-i+1}_{p^{a-1}(p-1)+1}.$$

Observe que

$$\nu_p\Big(\binom{p}{i} F^{i-1}_{p^{a-1}(p-1)}\Big) = \begin{cases} 1 + (i-1)(a-1+e(p)), & i \in [2, p-1], \\ (p-1)(a-1+e(p)), & i = p. \end{cases}$$

Daí, $\nu_p(\binom{p}{i} F^{i-1}_{p^{a-1}(p-1)}) \geq a + e(p) > 4$, com $i \geq 2$. Logo,

$$x(p^{a-2}) \equiv pF^p_{p^{a-1}(p-1)+1} \pmod{p^4}.$$

Assim,

$$x(p^{a-2}) \equiv p \pmod{p^4},$$

pois $F_{p^{a-1}(p-1)+1} \equiv 1 \pmod{p^4}$. □

Afirmação 3.4.10. *Note que*

$$x((p+1)p^{a-4}) + x((p+1)p^{a-3}) \equiv p^2 \pmod{p^4}.$$

Demonstração. Seja

$$x((p+1)p^t) = \frac{F_{p^a(p-1)}F_{(p+1)p^{t+1}(p-1)+1}}{F_{(p+1)p^{t+1}(p-1)}},$$

com $t \in \{a-4, a-3\}$. Foi provado que existem $s_1, l_1, l_2, l_3 \in \mathbb{Z}$ e $j \geq 0$ tais que

$$F_{p^a(p-1)} = sp^{a+j+1} + l_1 p^{a+j+3},$$

$$F_{(p+1)p^{t+1}(p-1)} = (p+1)sp^{t+j+2} + l_2 p^{t+j+4}$$

e

$$F_{(p+1)p^{t+1}(p-1)+1} = 1 + l_3 p^2.$$

Então,

$$((p+1)sp^{t+j+2} + l_2 p^{t+j+4})x((p+1)p^t) = (sp^{a+j+1} + l_1 p^{a+j+3})(1 + l_3 p^2).$$

Sendo $t \in \{a-4, a-3\}$, temos

$$\nu_p(l_2 p^{t+j+4} x((p+1)p^t)) \geq a+j+4+2 = a+j+6.$$

Logo,

$$(p+1)sp^{t+j+2}x((p+1)p^t) \equiv sp^{a+j+1} \pmod{p^{a+j+3}},$$

com $t \in \{a-4, a-3\}$. Seja $t = a-3$, então

$$(p+1)sp^{a+j-1}x((p+1)p^{a-3}) \equiv sp^{a+j+1} \pmod{p^{a+j+3}}$$

$$x((p+1)p^{a-3}) \equiv \frac{p^2}{p+1} \pmod{p^4} \tag{3.5}$$

Agora, seja $t = a-4$. Então

$$(p+1)sp^{a+j-2}x((p+1)p^{a-4}) \equiv sp^{a+j+1} \pmod{p^{a+j+3}},$$

e assim,

$$x((p+1)p^{a-4}) \equiv \frac{p^3}{p+1} \pmod{p^4}. \tag{3.6}$$

Por (3.5) e (3.6) temos

$$x((p+1)p^{a-4}) + x((p+1)p^{a-3}) \equiv \frac{p^2}{p+1} + \frac{p^3}{p+1} \pmod{p^4}$$

$$\equiv p^2 \pmod{p^4}.$$

□

Retornamos ao problema e chegamos que

$$\sigma_1(\overline{x}) \equiv p + p^2 \pmod{p^4}.$$

Assim,

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 + (p+p^2) + p(p+p^2-p) \pmod{p^4}.$$

$$\equiv 1 + p + p^2 + p^3 \pmod{p^4}$$

como queríamos. □

A partir dos nossos estudos nos sentimos aptos a conjecturar o seguinte resultado.

Conjectura 3.1. *Seja p um primo tal que $z(p) = p - 1$. Então*

$$\begin{bmatrix} p^{a+1} \\ p^a \end{bmatrix}_F \equiv 1 + \cdots + p^{k-1} \pmod{p^k}.$$

para todo $a,\ k \in \mathbb{N}$ tais que $a \geq k$.

Quando tentamos provar nossa conjectura notamos que os argumentos utilizados aqui não são suficientes para tal. Por exemplo, no caso $k = 5$ o conjunto N definido na seção 3.4 se torna muito complexo. Isso torna a partição de N, feita nessa mesma seção, inviável.

Referências

[1] J. J. Bravo, F. Luca, Powers of two in generalized Fibonacci sequences, *Rev. Colombiana Mat.* **46** (2012), 67–79.

[2] J. J. Bravo, F. Luca, Coincidences in generalized Fibonacci sequences, *J. Number Theory.* **133** (2013), 2121–2137.

[3] J. J. Bravo, F. Luca, On the largest prime factor of the k-Fibonacci numbers. *Int. J. Number Theory* **9** (2013), 1351–1366.

[4] J. J. Bravo, F. Luca, On a conjecture about repdigits in k-generalized Fibonacci sequences, *Publ. Math. Debrecen* **82** Fasc. 3–4 (2013).

[5] J. J. Bravo, C. A. Gómez, F. Luca, Powers of two as sums of two k-Fibonacci numbers, *Miskolc Mathematical Notes.* **17** (2014).

[6] Y. Bugeaud, M. Mignotte, S. Siksek, Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas powers, *Annals of Math* **163** (2006), 969–1018.

[7] A. P. Chaves, D. Marques, A Diophantine equation related to the sum of squares of consecutive k-generalized Fibonacci numbers, *The Fibonacci Quarterly* **52** (2014), 70–74.

[8] G. P. Dresden, Z. Du, A simplified Binet formula for k-generalized Fibonacci numbers, *Journal of Integer Sequences*, **17** (4) (2014).

[9] L. E. Dickson, *History of the Theory of Numbers.* Carnegie Institution of Washington, Volume 1, (1919).

[10] A. Dujella, A. Pethő, A generalization of a theorem of Baker and Davenport, *Quart. J. Math. Oxford Ser.* (2) **49** (1998), 291–306.

[11] G. Fontené, Généralisation d'une formule connue, *Nouv. Ann. Math* **4** (1915), 112.

[12] H. W. Gould, Generalization of Hermite's divisibility theorems and the Mann-Shanks primality criterion for s-Fibonomial arrays, *Fibonacci Quart* **12** (1974), 157-166.

[13] H. Hasse, Number theory, Classics in Mathematics, Springer-Verlag (2002).

[14] D. Kalman, R. Mena, The Fibonacci numbers exposed, *Math. Mag.* **76** (2003), no. 3, 167–181.

[15] T. Lengyel, The order of the Fibonacci and Lucas numbers. *Fibonacci Quart.* **33** (1995), 234–239.

[16] F. Luca, R. Oyono, An exponential Diophantine equation related to powers of two consecutive Fibonacci numbers. *Proc. Japan Acad. Ser.* **87** (2011) p. 45–50.

[17] T. Koshy, *Fibonacci and Lucas Numbers with Applications*, Wiley, New York, 2001.

[18] D. Marques, A. Togbé, On the sum of powers of two consecutive Fibonacci numbers. *Proc. Japan Acad. Ser. A,* **86** (2010), 174–176.

[19] D. Marques, On the order of appearance of integers at most one away from Fibonacci numbers, *Fibonacci Quart.* **50** (2012), 36–43.

[20] D. Marques, Fixed points of the order of appearance in the Fibonnacci sequence, *Fibonacci Quart.* **51** (2013), 346–351.

[21] D. Marques, On integer numbers with locally smallest order of appearance in the Fibonacci sequence, *Internat. J. Math. Sci.*, Article ID 407643 (2011), 4 páginas.

[22] D. Marques, The order of appearance of product of consecutive Fibonacci numbers, *Fibonacci Quart.* **50** 2 (2012), 132–139.

[23] D. Marques, The order of appearance of powers Fibonacci and Lucas numbers, *Fibonacci Quart.* **50** 3 (2012), 239–245.

[24] D. Marques, The proof of a conjecture concerning the intersection of k-generalized Fibonacci sequences, *Bull. Brazilian Math. Soc.* **44** (3) (2013), 455–468.

[25] D. Marques and P. Trojovský, On parity of Fibonomial coeffiecients , *Utilitas Math.* **97** (2015), 129–135.

[26] D. Marques and P. Trojovský, On divisibility properties of Fibonomial coefficients by 3, *J. Integer Seq.* **15** (2012), Article 12.6.4.

[27] D. Marques, J. Sellers, and P. Trojovský, On divisibility properties of certain Fibonomial coefficients by p, *Fibonacci Quart* **51** (2013), 78–83.

[28] D. Marques and P. Trojovský, The p-adic of some Fibonomial coefficients, *J. Integer Seq.* **18** (2015), Article 15.3.1.

[29] F. B. Martinez, C. G. Moreira, N. Saldanha, E. Tengan *Teoria dos Números: Um Passeio com Primos e Outros números Familiares pelo Mundo Inteiro.* Projeto Euclides, Associação Instituto Nacional de Matemática Pura e Aplicada. ed. **1**. (2010)

[30] E. M. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers, II, *Izv. Ross. Akad. Nauk Ser. Mat.* **64** (2000), 125–180. English translation in *Izv. Math.* **64** (2000), 1217–1269.

[31] T. D. Noe and J. V. Post, Primes in Fibonacci n-step and Lucas n-step sequences, *J. Integer Seq.*, **8** (2005), Article 05.4.4.

[32] C. A. G. Ruiz, F. Luca, An exponential Diophantine equation related to the sum of powers of two consecutive k-generalized Fibonacci numbers, *Colloquium Mathematicum* **137** (2014), 171–188.

[33] Wolfram Research, Inc., Mathematica, Version 7.0, Champaign, IL (2008).

[34] A. Wolfram, Solving generalized Fibonacci recurrences, *Fibonacci Quart.* **36** (1998), 129–145.