

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Equações Diofantinas Envolvendo Sequências de Fibonacci Generalizadas

Vinícius Facó Ventura Vieira

Orientado por
Prof. Dr. Diego MARQUES

Março de 2016

Gostaria de dedicar esse trabalho à memória de quem sempre terei orgulho de chamar de irmão, Rodrigo Ottoni de Brito.

E também a meus avós, todos acadêmicos e que são minha grande inspiração a seguir na carreira, Edith Vieira (in memorian), Aglaêda Facó Ventura (in memorian), Oldegar Franco Vieira (in memorian) e Manuel Mateus Ventura.

Agradecimentos

- Primeiramente gostaria de agradecer imensamente ao meu orientador, Diego Marques. Nada desse trabalho seria realizado sem sua orientação, seu companheirismo e sua disposição. Devo toda realização desse trabalho, tudo que aprendi no desenvolvimento desse e todas as experiências nesses últimos quatro anos a ele;
- Também gostaria de agradecer ao meu orientador de mestrado e membro da banca da minha defesa, Hemar Godinho, por ser o primeiro a acreditar na minha capacidade e a me introduzir no desenvolvimento de trabalhos acadêmicos;
- Ao Professor Yuri Bilu por ter me recebido em Bordeaux e pela ótima orientação em meu período na França;
- Aos professores José Othon Lopes, José Plínio Santos, Paulo Henrique Rodrigues e Noraí Rocco por concordarem em participar da banca examinadora da tese e pelas correções precisas no trabalho;
- À minha família por sempre estar ao meu lado e ofertar constante apoio psicológico, emocional e financeiro. Em especial aos meus pais, Mônica Facó e Fernando Tolentino;
- Aos meus amigos por serem meu norte de felicidade e apoio nos momentos de dificuldade, Marina, Bárbara, Heluiza, Jaqueline, Ismael, Livea, Laura, Paloma, Braz, Gustavo, Alvaro;
- A Disley José, pelo companheirismo, dedicação, disposição, preocupação e por me dar forças quando eu mais precisei;
- Aos colegas alunos de Teoria dos Números, Ana Paula Chaves, Luciana Ventura, Thiago Porto, Daiane Soares, Lucimeire Carvalho, Elaine Cristine, Gérsica Freitas, Bruno de Paula, Filipe Augusto, Josimar Aguirre, Jean Lelis, Carol Lafeté e Alessandra Kreutz;
- Aos vários professores que contribuíram à minha formação, Lineu Neto (o responsável por eu estar na Teoria dos Números), Nigel Pitt, Cátia Gonçalves, Pavel Zaleski, Elves Barros, Noraí Rocco, entre muitos outros;
- Aos colegas da turma de língua japonesa: arigatou gozaimasu;
- Aos colegas de voleibol pela compreensão e companheirismo nesse trajeto;
- E, finalmente, a todos que prestigiam esse trabalho.

Resumo

A famosa e amplamente estudada sequência de Fibonacci é determinada pela recorrência $F_n = F_{n-1} + F_{n-2}$, onde $F_0 = 0$ e $F_1 = 1$. Podemos estender essa sequência para sequências recorrentes de ordem maior. Logo, para $k \geq 2$ e $n \geq -(k-2)$, seja $F_n^{(k)} = F_{n-1}^{(k)} + \dots + F_{n-k}^{(k)}$, onde $F_{-(k-2)}^{(k)} = \dots = F_{-1}^{(k)} = F_0^{(k)} = 0$ e $F_1 = 1$. Vamos estudar algumas equações Diofantinas envolvendo tais sequências. Num primeiro momento, lembramos que um número perfeito é um natural que é soma de seus divisores próprios. Então, vamos aplicar formas lineares em logaritmo para achar números perfeitos pares em sequências de Fibonacci generalizadas. Em outras palavras, vamos estudar a equação $F_n^{(k)} = 2^{p-1}(2^p - 1)$. Em outro problema, vamos estudar a valorização 2-ádica de $F_n^{(k)}$, quando $k = 4$, a fim de procurar fatoriais nessa sequência, ou seja, vamos estudar a equação $Q_n = m!$. Também, vamos usar técnicas parecidas para resolver um caso particular da equação de Brocard-Ramanujan, $n^2 = m! + 1$, quando o inteiro n é um número da sequência mencionada previamente.

Palavras-chave: Equações Diofantinas; Sequências de Fibonacci Generalizadas; Números de k -bonacci; Números Perfeitos; Formas Lineares em Logaritmo, Valorização p -ádica; Fatorial; Equação de Brocard-Ramanujan.

Abstract

The famous and widely studied Fibonacci sequence is determined by the recurrence $F_n = F_{n-1} + F_{n-2}$, where $F_0 = 0$ and $F_1 = 1$. We can extend this sequence for higher order recurrences. So, for $k \geq 2$ and $n \geq -(k-2)$, let $F_n^{(k)} = F_{n-1}^{(k)} + \cdots + F_{n-k}^{(k)}$, where $F_{-(k-2)}^{(k)} = \cdots = F_{-1}^{(k)} = F_0^{(k)} = 0$ and $F_1 = 1$. We shall study some Diophantine equations involving such sequences. First, we recall that a perfect number is a natural number which equals the sum of all its proper divisors. Then, we shall apply linear forms in logarithms to find even perfect numbers in generalized Fibonacci sequences. In other words, we shall study the Diophantine equation $F_n^{(k)} = 2^{p-1}(2^p - 1)$. In another problem, we shall study the 2-adic valuation of $F_n^{(k)}$, when $k = 4$, in order to find factorials in that sequence, i.e., we shall study the equation $Q_n = m!$. Also, we shall use similar techniques to solve a particular case of the Brocard-Ramanujan equation, $n^2 = m! + 1$, when the integer n is a number of the previously mentioned sequence.

Key Words: Diophantine Equations; Generalized Fibonacci Sequence; K -bonacci Numbers; Perfect Numbers; Linear Forms in Logarithms, P -adic Valuation; Factorial, Brocard-Ramanujan Equation.

Índice

Introdução	1
1 Preliminares	6
1.1 Sequências de Fibonacci k -generalizadas	6
1.2 Formas lineares em logaritmo	14
1.3 Método de redução	15
1.4 Outros resultados auxiliares	16
2 Números Perfeitos Pares na Sequência de Fibonacci Generalizada	20
2.1 A equação $F_n^{(k)} = 2^{p-1}(2^p - 1)$	20
2.2 Um limitante para n e p em termos de k	21
2.3 Os casos pequenos: $3 \leq k \leq 167$	24
2.4 $n \neq 2p + 1$	26
2.5 $n = 2p + 1$ e a conclusão do Teorema 2.1	28
3 A Valorização 2-ádica de Q_n e a Equação $Q_n = m!$	30
3.1 Alguns lemas preliminares	30
3.2 A valorização 2-ádica de Q_n	39
3.3 A equação $Q_n = m!$	46
4 Um Caso Particular da Equação de Brocard-Ramanujan	48
4.1 $T_n^2 = m! + 1$	48
4.1.1 A valorização 2-ádica de $T_n - 1$	49
4.1.2 A valorização 2-ádica de $T_n + 1$	50

4.1.3	Resolvendo $T_n^2 = m! + 1$	53
4.2	$Q_n^2 = m! + 1$	54
4.2.1	A valorização 2-ádica de $Q_n + 1$	54
4.2.2	A valorização 2-ádica de $Q_n - 1$	55
4.2.3	Resolvendo $Q_n^2 = m! + 1$	57
Referências Bibliográficas		58

Introdução

Poucos historiadores sabem ao certo em que época viveu Diofanto de Alexandria. Alguns sustentam a hipótese de que ele viveu no século III D. C., outros que ele foi contemporâneo a Herão e pouco se sabe sobre sua história pessoal. O que é amplamente conhecido é a herança que esse deixou para o estudo da Álgebra e da Teoria dos Números ao estabelecer o estudo de equações com soluções nos inteiros, conhecidas em sua homenagem como equações Diofantinas. Em aspectos mais formais, dada uma função f , uma equação Diofantina é uma equação do tipo

$$f(x_1, x_2, \dots, x_n) = 0,$$

onde procuramos soluções $(x_1, \dots, x_n) \in \mathbb{Z}^n$.

Historicamente, as equações Diofantinas têm sido parte central do estudo em Teoria dos Números. Várias dessas foram objeto de estudos, como as equações de Pell, os triplos pitagóricos e como exemplo mais famoso, a equação do Último Teorema de Fermat.

Como consequência do estudo em torno de diferentes tipo de equações Diofantinas, surgiram também vários procedimentos e técnicas diferenciadas para resolvê-las. Podemos destacar o método algébrico e o método modular (utilizado por A. Wiles na solução do Último Teorema de Fermat). Em nossos estudos utilizaremos o método das formas lineares em logaritmo, o mais indicado e adequado para a resolução de equações Diofantinas exponenciais.

O método das formas lineares em logaritmo será útil para a resolução da primeira equação apresentada neste trabalho, mas será conveniente para a resolução das equações restantes. Para essas, técnicas diferentes serão introduzidas para resolver equações Diofantinas envolvendo fatoriais, a utilizar-se uma consequência da Fórmula de *de Polignac*. Em todos os casos, entretanto, estaremos estudando equações Diofantinas envolvendo números da sequência de k -bonacci (ou simplesmente números de k -bonacci), uma generalização importante da sequência de Fibonacci.

Em 1202, o matemático Leonardo de Pisa, conhecido como *Fibonacci*, estabeleu em seu livro *Liber Abaci* um problema sobre o crescimento em uma população de coelhos, seguindo as seguintes regras:

- Um casal (uma fêmea e um macho) recém-nascido de coelhos é colocado em um campo;

- Esses coelhos são capazes de reproduzir com um mês de idade de forma que a fêmea dá a luz a um novo casal (uma fêmea e um macho) no final do segundo mês;
- os coelhos nunca morrem;
- cada casal sempre vai se reproduzir e gerar um novo casal com um macho e uma fêmea a partir do segundo mês.

Note que no primeiro mês temos apenas um casal de coelhos. Um novo casal será gerado apenas no final do segundo mês, logo teremos dois casais no terceiro mês. O novo casal, vai gerar um próximo casal apenas no final do quarto mês, enquanto o primeiro vai produzir mais um. Portanto teremos 3 casais no quarto mês, 5 no quinto mês, etc... Logo, teremos a seguinte sequência

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

Em termos formais, essa sequência pode ser definida pela recorrência $F_n = F_{n-1} + F_{n-2}$, com termos iniciais $F_0 = 0$ e $F_1 = 1$. Essa sequência ficou conhecida como sequência de Fibonacci (esse nome foi utilizado primeiramente por Édouard Lucas no século 19).

Seja $k \geq 2$, vamos denotar por $F_n^{(k)} = (F_n^{(k)})_{n \geq -(k-2)}$, a sequência de Fibonacci k -generalizada, cujos termos satisfazem

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

onde $F_{-(k-2)}^{(k)} = F_{-(k-2)+1}^{(k)} = \dots = F_0 = 0$ e $F_1 = 1$. Tal sequência também é conhecida por sequência de Fibonacci generalizada de ordem k ou sequência de k -bonacci. Para $k = 2$ temos a sequência de Fibonacci, para $k = 3$ a sequência de Tribonacci, para $k = 4$ a sequência de Tetranacci, etc...

Dado um número natural n , seja $\sigma(n)$ a soma de todos os divisores de n , então n é dito *perfeito* quando $\sigma(n) = 2n$. Os números perfeitos possuem uma extensa história na matemática, de todos os resultados os envolvendo talvez o mais conhecido seja o teorema de Euclides-Euler, o qual caracteriza todos os números perfeitos pares.

Teorema (Euclides-Euler) *Um natural n par é perfeito se, e somente se, existe um primo p tal que $2^p - 1$ também é primo e $n = 2^{p-1}(2^p - 1)$.*

Ainda não é conhecida a existência de números perfeitos ímpares ou a existência de infinitos números perfeitos (sequer pares, pois esse problema está relacionado com a existência de infinitos primos de Mersenne), mas sabe-se que, se um número perfeito n é ímpar, então $n = p^a x^2$, onde p é um primo que satisfaz $p \equiv a \equiv 1 \pmod{4}$. Luca, em [36], provou que não existem números perfeitos na sequência de Fibonacci e mais tarde provou junto com Huguet, em [37], que não existe número perfeito da forma F_{mk}/F_k . O mesmo resultado foi obtido por Phong, em [54], de forma independente. Se torna imediatamente natural se perguntar sobre a existência de números perfeitos nas sequências de k -bonacci. Aqui, vamos responder em parte essa pergunta. Mais precisamente, vamos provar a não existência de números perfeitos pares em sequências de k -bonacci quando $k \not\equiv 3 \pmod{4}$. Então, temos o seguinte resultado:

Teorema. *A equação Diofantina*

$$F_n^{(k)} = 2^{p-1}(2^p - 1) \quad (2)$$

não apresenta soluções para inteiros positivos n, k e p , onde p e $2^p - 1$ são primos, se ao menos uma das seguintes condições for satisfeita:

1. $2 \leq k \leq 167$;
2. $n \neq 2p + 1$;
3. $n = 2p + 1$ e $p \geq k$;
4. $n = 2p + 1, p < k$ e $k \not\equiv 3 \pmod{4}$;
5. $n = 2p + 1, p < k, k \equiv 3 \pmod{4}$ e $2p - k + 1 \neq 2^{k-p+1}$.

Em particular, não há nenhum número perfeito par em $(F_n^{(k)})_{n \geq -(k-2)}$ quando $k \not\equiv 3 \pmod{4}$.

Para obter tal resultado, vamos utilizar um eficiente método para resolver equações Diofantinas, o método das formas lineares em logaritmo, combinado com um método de redução e um método adicional desenvolvido por Bravo e Luca. Tal método foi utilizado para a resolução de diversas equações Diofantinas envolvendo números de k -bonacci. Por exemplo, Bravo e Luca resolveram, em [7], o problema de achar potências de 2 que são números de k -bonacci. Em 2013, duas conjecturas envolvendo $F_n^{(k)}$ foram provadas. A primeira foi provada por Bravo e Luca, em [9], e envolve achar números com apenas um dígito distinto em sequências de k -bonacci e a segunda envolve uma conjectura de Noe e Post, em [51], sobre coincidências em termos dessas sequências, provada de forma independente por Marques em [44] e por Bravo e Luca em [8].

Tal método entretanto pode não ser efetivo para a resolução de equações Diofantinas não exponenciais, como por exemplo as que envolvem fatoriais. Erdős e Selfridge, em [19], provaram que $n!$ é uma potência perfeita, apenas quando $n = 1$. No caso Fibonacci, Luca provou, em [35], que F_n é um produto de fatoriais apenas quando $n = 1, 2, 3, 6, 12$, e que o maior produto de números de Fibonacci que é um fatorial é $F_1 F_2 F_3 F_4 F_5 F_6 F_8 F_{10} F_{12} = 11!$ em [39], juntamente com Stănică. Para tais, ele utilizou o Teorema do Divisor Primitivo, mas tal resultado é inexistente para recorrências de ordem maior, como $F_n^{(k)}$. Logo, teremos que usar algum outro método.

Como, para cada $k \geq 2$, cada sequência possui características muito específicas parece bem difícil obter uma fórmula geral para a valorização 2-ádica de $F_n^{(k)}$. Em 2014, Marques e Lengyel, em [47], forneceram uma fórmula fechada para a valorização 2-ádica para os números de Tribonacci, T_n . Eles provaram que, para $n \geq 1$,

$$\nu_2(T_n) = \begin{cases} 0, & \text{se } n \equiv 1, 2 \pmod{4}; \\ 1, & \text{se } n \equiv 3, 11 \pmod{16}; \\ 2, & \text{se } n \equiv 4, 8 \pmod{16}; \\ 3, & \text{se } n \equiv 7 \pmod{16}; \\ \nu_2(n) - 1, & \text{se } n \equiv 0 \pmod{16}; \\ \nu_2(n+4) - 1, & \text{se } n \equiv 12 \pmod{16}; \\ \nu_2((n+1)(n+17)) - 3, & \text{se } n \equiv 15 \pmod{16}. \end{cases}$$

E utilizaram esse resultado para demonstrar que os únicos resultados para a equação Diofantina $T_n = m!$ são $(n, m) \in \{(1, 1), (2, 1), (3, 2), (7, 4)\}$.

Aqui vamos proceder de forma similar para resolver a equação $F_n^{(4)} = Q_n = m!$, quando $n \not\equiv 75 \pmod{80}$. Vamos obter o seguinte resultado:

Teorema. Para $n \geq 1, n \not\equiv 75 \pmod{80}$, temos que

$$\nu_2(Q_n) = \begin{cases} 17, & \text{se } n = 78 \\ 0, & \text{se } n \equiv 1, 2 \pmod{5}; \\ 1, & \text{se } n \equiv 3 \pmod{10}; \\ 2, & \text{se } n \equiv 4, 9 \pmod{20}; \\ 3, & \text{se } n \equiv 5, 8 \pmod{20}; \\ \nu_2(n) + 2, & \text{se } n \equiv 0 \pmod{20}; \\ \nu_2(n+10) + 2, & \text{se } n \equiv 10 \pmod{20}; \\ \nu_2(n+6) + 1, & \text{se } n \equiv 14 \pmod{20}; \\ \nu_2(n+1) + 1, & \text{se } n \equiv 19 \pmod{20}; \\ \nu_2((n+5)^2) + 1, & \text{se } n \equiv 15, 35, 55 \pmod{80}; \\ \nu_2((n+2)^2) + 1, & \text{se } n \equiv 18, 38, 58 \pmod{80}; \\ \nu_2((n+2)(n-78)) + 1, & \text{se } n \equiv 78 \pmod{80}, n > 78. \end{cases}$$

Para então provar o seguinte teorema:

Teorema. As únicas soluções para a equação Diofantina

$$Q_n = m! \tag{3}$$

em inteiros positivos $m, n \not\equiv 75 \pmod{80}$ são

$$(n, m) \in \{(1, 1), (2, 1), (3, 2)\}.$$

A mais famosa equação Diofantina envolvendo fatoriais foi proposta por Brocard em [11], em 1876, e independentemente por Ramanujan em [55], [56, p. 327], em 1913. A equação Diofantina

$$m! + 1 = n^2 \tag{4}$$

é então conhecida como a *equação Diofantina de Brocard-Ramanujan*, ou simplesmente *equação de Brocard-Ramanujan*.

Recentemente, Berndt e Galway, em [4], não acharam nenhuma solução da equação Diofantina de Brocard-Ramanujan para números até $m = 10^9$ e diferentes das soluções triviais $m = 4, 5$ e 7 . Entretanto, a equação ainda é um problema em aberto.

Em 2012, Marques, em [43], provou que $(m, n) = (4, 5)$ é a única solução dessa equação quando n é um número de Fibonacci. Mais uma vez, a prova depende do Teorema do Divisor Primitivo e também de algumas propriedades algébricas de $F_n \pm 1$.

Aqui, vamos procurar soluções (m, n) da equação de Brocard-Ramanujan onde n é um número de Tribonacci. Com efeito, vamos mostrar que

Teorema. *Não existem soluções $(m, n) \in \mathbb{Z}^2$ para a equação*

$$T_n^2 = m! + 1. \quad (5)$$

Além disso, vamos também achar as soluções da equação para o caso Tetranacci. De fato, temos o seguinte resultado:

Teorema. *A equação*

$$Q_n^2 = m! + 1 \quad (6)$$

não possui nenhuma solução em $(m, n) \in \mathbb{Z}^2$.

Capítulo 1

Preliminares

Antes de desenvolver os resultados principais apresentados aqui, vamos precisar de alguns resultados envolvendo sequências de Fibonacci k -generalizadas, formas lineares em logaritmo e valorização p -ádica de fatoriais.

1.1 Sequências de Fibonacci k -generalizadas

Em 1202 o matemático Leonardo de Pisa estabeleceu, pela primeira vez, uma sequência recorrente relacionada com um problema envolvendo a quantidade populacional de coelhos. No século 19, o teórico dos números Édouard Lucas estudou tal sequência pela primeira vez de forma detalhada. Tal sequência ficou conhecida como sequência de Fibonacci e é definida pela recorrência

$$F_n = F_{n-1} + F_{n-2},$$

onde $F_0 = 0$ e $F_1 = 1$. Como já dito anteriormente, a sequência de Fibonacci já foi amplamente estudada e possui inúmeras propriedades já conhecidas. Dentre as quais, destacamos a Fórmula de Binet:

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}},$$

onde α, β são as raízes do polinômio característico $\Psi(x) = x^2 - x - 1$ e, portanto,

$$\alpha = \frac{1 + \sqrt{5}}{2}$$

e

$$\beta = -\frac{1}{\alpha} = 1 - \alpha = \frac{1 - \sqrt{5}}{2}.$$

Observação: Note que, como $\alpha - 1 = 1/\alpha$, então

$$\alpha = 1 + \frac{1}{1 + \frac{1}{1 + \dots}}$$

e

$$|\beta| = \frac{1}{1 + \frac{1}{1 + \frac{1}{\dots}}} < 1,$$

e então α e β possuem exatamente a mesma parte fracionária.

Aqui, trabalharemos com uma determinada generalização da sequência de Fibonacci. No caso, dado $k \geq 2$, sejam $F_0^{(k)} = F_{-1}^{(k)} = \dots = F_{-(k-2)}^{(k)} = 0$ e $F_1^{(k)} = 1$ e a sequência definida pela seguinte recorrência, para $n \geq 2$:

$$F_n^{(k)} = F_{n-1}^{(k)} + F_{n-2}^{(k)} + \dots + F_{n-k}^{(k)}. \quad (1.1)$$

Tal sequência é definida, para cada $k \geq 2$, como a sequência de Fibonacci generalizada de ordem k , sequência de Fibonacci k -generalizada ou sequência de k -bonacci. Além disso, os números pertencentes a tal sequência são conhecidos como *números de k -bonacci*. Temos que o polinômio característico da sequência é $p_k(x) = x^k - x^{k-1} - \dots - 1$. Note que, pela Lei dos Sinais de Descartes, $p_k(x)$ tem no máximo uma raiz real positiva. Chamaremos tal raiz de $\alpha^{(k)}$ (aqui, escrevemos o índice sobrescrito para enfatizar a dependência em k , mas podemos denotar, quando não existem ambiguidades, apenas por α). Observe que

$$p_{k+1}(x) = x \left(x^k - \frac{x^k - 1}{x - 1} \right) - 1,$$

e logo $p_{k+1}(\alpha^{(k)}) = -1$. Assim $\alpha^{(k+1)} > \alpha^{(k)}$, para todo k . E como $p_k(2) = 1$ para todo k , temos que à medida que k tende a infinito, $\alpha^{(k)}$ se aproxima de 2. Note também que, quando $x = 2(1 - 2^{-k})$,

$$\begin{aligned} x^k - \dots - 1 &= x^k - \frac{x^k - 1}{x - 1} \\ &= 2^k(1 - 2^{-k})^k - \frac{2^{2k}(1 - 2^{-k})^k - 2^k}{2^k - 1} \\ &= \frac{(2^k - 1)2^k(1 - 2^{-k})^k - 2^{2k}(1 - 2^{-k})^k - 2^k}{2^k - 1} \\ &= \frac{2^k(1 - 2^{-k})^k(-2^k)}{2^k - 1} \\ &< 0. \end{aligned}$$

Assim, $\alpha^{(k)}$ está entre $2(1 - 2^{-k})$ e 2 para todo k .

As outras raízes de $p_k(x)$ estarão todas dentro do círculo unitário, pelo seguinte Teorema provado por Miller, em [50]:

Teorema 1.1. *Toda raiz $\beta \neq \alpha$ de $p_k(x)$ satisfaz*

$$|\beta| < 1.$$

Como consequência direta, temos que $p_k(x)$ é irredutível sobre \mathbb{Q} e suas raízes são todas irracionais. Além disso, note que $(x - 1)p_k(x) = r_{k+1}(x) = x^{k+1} - 2x^k + 1$. Assim,

denotando as raízes de $p_k(x)$ por $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$, onde $\alpha_1 = \alpha$ sempre denotará a raiz real positiva fora do círculo unitário, temos que as raízes de $r_{k+1}(x)$ serão $1, \alpha_1, \alpha_2, \dots, \alpha_k$. Portanto, $r'_{k+1}(x) = x^{k-1}((k+1)x - 2k)$. Note que $r'_{k+1}(x)$ se anula apenas em $x = 0$ (que não é raiz de $p_k(x)$) e $x = 2k/(k+1)$. Mas, como

$$\begin{aligned} \left(\frac{2k}{k+1}\right)^{k+1} - 2\left(\frac{2k}{k+1}\right)^k + 1 &= \frac{(2k)^{k+1} - 2^{k+1}k^k(k+1) + (k+1)^{k+1}}{(k+1)^{k+1}} \\ &= \frac{2^{k+1}k^k(-1) + (k+1)^{k+1}}{(k+1)^{k+1}}, \end{aligned}$$

e, para todo $k \geq 2$,

$$k \neq \left(\frac{2k}{k+1}\right)^{k+1}$$

(pois $2k/(k+1) \notin \mathbb{Z}$), então, $2^{k+1}k^k(-1) + (k+1)^{k+1} \neq 0$ e todas as raízes de $p_k(x)$ são simples. Finalmente, note que α é raiz de $p_k(x)$ se, e somente se, $1/\alpha$ é raiz de $q_k(x) := 1 - x - x^2 - \dots - x^k$.

Vamos agora procurar uma forma similar à formula de Binet exposta acima para seqüências de Fibonacci. Primeiro, note que

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}} = \frac{\alpha - 1}{2 + 3(\alpha - 2)}\alpha^{n-1} + \frac{\beta - 1}{2 + 3(\beta - 2)}\beta^{n-1}. \quad (1.2)$$

Seja $f(x) = \sum_{i=1}^{\infty} F_n^{(k)} x^i$ a função geradora de $F_n^{(k)}$. Assim, temos que

$$\begin{aligned} \left(1 - \sum_{j=1}^k x^j\right) f(x) &= 1 \\ \implies f(x) &= \frac{1}{1 - \sum_{j=1}^k x^j} = \frac{1}{\prod_{j=1}^k (1 - \alpha_j x)} = \frac{1}{q_k(x)}. \end{aligned}$$

Escrevendo $f(x)$ por meio de frações parciais, como todas as raízes de $p_k(x)$ são simples, temos que

$$f(x) = \frac{1}{\prod_{j=1}^k (1 - \alpha_j x)} = \sum_{j=1}^k \frac{A_j}{1 - \alpha_j x},$$

onde

$$A_j = \frac{1}{\prod_{m=1, m \neq j}^k \left[1 - \alpha_m \left(\frac{1}{\alpha_j}\right)\right]}.$$

Temos que $A_j = \alpha_j / q'_k(1/\alpha_j)$, logo

$$f(x) = \sum_{j=1}^k \frac{-\alpha_j}{q'_k\left(\frac{1}{\alpha_j}\right)} \cdot \frac{1}{1 - \alpha_j x} = \sum_{i=0}^{\infty} \left[\sum_{j=1}^k \frac{-\alpha_j}{q'_k\left(\frac{1}{\alpha_j}\right)} \right] \alpha_j^{i-1} x^i.$$

Assim,

$$F_n^{(k)} = \sum_{j=1}^k \frac{-\alpha_j (\alpha_j)^{n-1}}{q'_k \left(\frac{1}{\alpha_j} \right)}.$$

Como $q'_k \left(\frac{1}{\alpha_j} \right) = - \sum_{m=1}^k m \left(\frac{1}{\alpha_j} \right)^{m-1}$ e

$$\left[1 - \sum_{m=1}^k \left(\frac{1}{\alpha_j} \right)^m \right], \text{ quando } 1 \leq j \leq k,$$

e então

$$- \left(1 - \frac{1}{\alpha_j} \right) q'_k \left(\frac{1}{\alpha_j} \right) = 2 - (k+1) \left(\frac{1}{\alpha_j} \right)^k,$$

e assim

$$F_n^{(k)} = \sum_{j=1}^k \frac{\alpha_j (\alpha_j)^{n-1} \left(1 - \frac{1}{\alpha_j} \right)}{2 - (k+1) \left(\frac{1}{\alpha_j} \right)^k}.$$

Como visto anteriormente,

$$x^k - \dots - 1 = x^k - \frac{x^k - 1}{x - 1}.$$

E assim, $\alpha_j^{k+1} - 2\alpha_j^k = -1$. Portanto $\alpha_j - 2 = -1 \cdot 1/\alpha_j^k$. Então, temos que

$$\frac{\alpha_j \left(1 - \frac{1}{\alpha_j} \right)}{2 - (k+1) \left(\frac{1}{\alpha_j} \right)^k} = \frac{\alpha_j - 1}{2 + (k+1)(\alpha_j - 2)}.$$

E assim provamos o seguinte teorema:

Teorema 1.2. *Seja $F_n^{(k)}$ o n -ésimo número de k -bonacci. Temos que*

$$F_n^{(k)} = \sum_{i=1}^k \frac{\alpha_i - 1}{2 + (k+1)(\alpha_i - 2)} \alpha_i^{n-1}, \quad (1.3)$$

onde $\alpha_1, \dots, \alpha_k$ são as raízes de $p_k(x) = x^k - x^{k-1} - \dots - 1$.

Note que, para $k = 2$ a equação dada acima coincide com a equação (1.2). Observe também que, como existe apenas uma raiz α de $p_k(x)$ que está fora do círculo unitário, a contribuição das outras que tem módulo menor do que 1 deve se aproximar de 0 à medida que n vai para infinito. De forma que

$$F_n^{(k)} \approx g(\alpha, k) \alpha^{n-1},$$

onde

$$g(x, k) := \frac{x - 1}{2 + (k + 1)(x - 2)}. \quad (1.4)$$

O Lema a seguir expõe, para $k \geq 2$ dado, algumas propriedades da função $g(x, k)$ (como função de x).

Lema 1.3. *Seja $k \geq 2$, então*

1. $g(2 - 1/k, k) = 1$;
2. $g(2, k) = \frac{1}{2}$;
3. $g(x, k)$ é contínua e decrescente no intervalo $[1 - 1/k, \infty)$;
4. $g(x, k) > \frac{1}{x}$ no intervalo $(2 - 1/k, 2)$.

Demonstração. 1. Temos que

$$g(2 - 1/k, k) = \frac{2 - \frac{1}{k} - 1}{2 + (k + 1)(2 - \frac{1}{k} - 2)} = \frac{k - 1}{2k - k - 1} = 1.$$

2. Também temos que

$$g(2, k) = \frac{2 - 1}{2 + (k + 1)(2 - 2)} = \frac{1}{2}.$$

3. Aqui, vamos reescrever $g(x, k)$ da seguinte forma

$$g(x, k) = \frac{1}{k + 1} \left(1 + \frac{1 - \frac{2}{k+1}}{x - (2 - \frac{2}{k+1})} \right).$$

Então, note que, $g(x, k)$ é um escalar de uma translação de $1/x$. E como

$$\lim_{x \rightarrow 2 - \frac{2}{k+1}} g(x, k) = +\infty,$$

$x = 2 - 2/k + 2$ é uma assíntota vertical de $g(x, k)$ e usando os itens anteriores, temos o resultado.

4. Note que,

$$\begin{aligned} \frac{x - 1}{2 + (k + 1)(x - 2)} &= \frac{1}{x} \\ \implies x^2 - x &= 2 + (k + 1)(x - 2) \\ \implies x^2 - (k + 2)x + 2k &= 0 \\ \implies x = 2, x = k &\geq 2. \end{aligned}$$

Assim, $g(x, k)$ e $1/x$ se interceptam em $x = 2$ e $x = k$, e como $1/x < g(x, k)$ em $x = 2 - 2/k + 1$ e as duas são contínuas, então $g(x, k) > \frac{1}{x}$ em $(2 - 1/k, 2)$.

□

Lema 1.4. *Seja, para cada $k \geq 2$ dado, $E_k(n)$ definido como*

$$\begin{aligned} E_k(n) &= F_n^{(k)} - \frac{\alpha - 1}{2 + (k+1)(\alpha - 2)} \alpha^{n-1} \\ &= F_n^{(k)} - g(\alpha, k) \alpha^{n-1}, \end{aligned}$$

onde α é a raiz real positiva de $x^k - x^{k-1} - \dots - 1 = 0$. Então, temos que $E_k(n)$ satisfaz, para $n \geq 2$

$$E_k(n) = E_k(n-1) + E_k(n-2) + \dots + E_k(n-k).$$

Demonstração. Por definição, temos que

$$F_n^{(k)} = F_{n-1}^{(k)} + \dots + F_{n-k}^{(k)}.$$

Além disso, $\alpha^k = \alpha^{k-1} + \dots + \alpha + 1$ e portanto

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

Logo

$$\begin{aligned} E_k(n) &= F_n^{(k)} - g(\alpha, k) \alpha^{n-1} \\ &= F_{n-1}^{(k)} + \dots + F_{n-k}^{(k)} - g(\alpha, k) \alpha^{n-2} - \dots - g(\alpha, k) \alpha^{n-(k+1)} \\ &= g(\alpha, k) \alpha^{n-2} + E_k(n-1) + \dots + g(\alpha, k) \alpha^{n-(k+1)} + E_k(n-k) \\ &\quad - g(\alpha, k) \alpha^{n-2} - \dots - g(\alpha, k) \alpha^{n-(k+1)} \\ &= E_k(n-1) + E_k(n-2) + \dots + E_k(n-k). \end{aligned}$$

□

Teorema 1.5. *Seja $F_n^{(k)}$ o n -ésimo número de k -bonacci, $n \geq -(k-2)$ e α a única raiz real positiva de $x^k - x^{k-1} - \dots - 1 = 0$ de forma que*

$$F_n^{(k)} = g(\alpha, k) \alpha^{n-1} + E_k(n),$$

então, temos que

$$|E_k(n)| < \frac{1}{2}.$$

Demonstração. Primeiramente vamos provar o teorema para $n = -1, -2, \dots, -(k-2)$, depois para $n = 0$. E finalmente faremos para $n \geq 1$. Pela definição de $F_n^{(k)}$, temos que $F_0^{(k)} = 0 = F_{-1}^{(k)} = \dots = F_{-(k-2)}^{(k)}$, logo, para esses casos, é suficiente provar que $|g(\alpha, k) \alpha^{n-1}| < 1/2$. Para $-(k-2) \leq n \leq -1$, note que, como $\alpha^{-1} < 1$ e

$$\alpha > 2(1 - 2^{-k}) \implies \frac{1}{\alpha^2} < \frac{1}{4(1 - 2^{-k})^2} < \frac{1}{2},$$

então, pelo Lema 1.3, $|g(\alpha, k)|$ e

$$|g(\alpha, k) \alpha^{n-1}| < \frac{1}{2}.$$

Para $n = 0$, não é difícil mostrar que $g(\alpha, k)\alpha^{-1} < 1/2$ para $k = 2$ ou $k = 3$. Note que, para $k \geq 4$, temos que

$$2 - \frac{1}{3k} < 2 - \frac{2}{2^k} < \alpha, \quad (1.5)$$

e então

$$\alpha^{-1} < \frac{3k}{6k-1}. \quad (1.6)$$

Pelo Lema 1.3 e pela equação (1.5),

$$g(\alpha, k) < g(2 - 1/3k) = \frac{3k-1}{5k-1}. \quad (1.7)$$

Assim, pelas equações (1.6) e (1.7),

$$g(\alpha, k)\alpha^{-1} < \frac{3k-1}{5k-1} \cdot \frac{3k}{6k-1} < \frac{(3k) \cdot 1}{(5k-1) \cdot 2} < \frac{1}{2}.$$

Para $n = 1$, temos que $E_k(1) = F_1^{(k)} - g(\alpha, k)\alpha^{1-1} = 1 - g(\alpha, k)$. Mas pelo Lema 1.3, temos que $g(\alpha, k) > g(2, k) = 1/2$. E assim

$$|E_k(1)| < \frac{1}{2}.$$

Suponha, por absurdo, que para algum $n \geq 2$, $|E_k(n)| \geq 1/2$. Seja n_0 o menor inteiro tal que isso aconteça. Subtraindo as duas equações

$$\begin{aligned} E_k(n_0 + 1) &= E_k(n_0) + \dots + E_k(n_0 - (k-1)) \\ E_k(n_0) &= E_k(n_0 - 1) + \dots + E_k(n_0 - k), \end{aligned}$$

obtemos

$$E_k(n_0 + 1) = 2E_k(n_0) - E_k(n_0 - k).$$

Como $n_0 - k < n_0$, então $|E_k(n_0 - k)| < 1/2$ e $|E_k(n_0)| > |E_k(n_0 - k)|$. E assim $0 < E_k(n_0) - E_k(n_0 - k) = E_k(n_0 + 1) - E_k(n_0)$. Portanto, podemos concluir indutivamente que $|E_k(n_0 + i)| > \dots > |E_k(n_0 + 1)| > |E_k(n_0)|$ o que contraria o fato da contribuição das raízes de $x^k - x^{k-1} - \dots - 1 = 0$ que estão dentro do círculo unitário ser trivial. Logo,

$$|E_k(n)| < \frac{1}{2},$$

para todo $n \geq 2$.

□

Vamos expor mais alguns resultados necessários sobre números de k -bonacci.

Lema 1.6. Para $2 \leq n \leq k+1$,

$$F_n^{(k)} = 2^{n-2}. \quad (1.8)$$

Para $2 \leq j \leq k+1$,

$$F_{k+j}^{(k)} = 2^{k+j-2} - i2^{j-3}. \quad (1.9)$$

Demonstração. Primeiramente, pela definição de $F_n^{(k)}$, temos que $F_{n-1}^{(k)} = F_{n-2}^{(k)} + \dots + F_{n-(k+1)}^{(k)}$. Assim

$$\begin{aligned} F_n^{(k)} - F_{n-1}^{(k)} &= F_{n-1}^{(k)} + \dots + F_{n-k}^{(k)} - F_{n-2}^{(k)} - \dots - F_{n-1}^{(k)} - F_{n-(k+1)}^{(k)} \\ &= F_{n-1}^{(k)} - F_{n-(k+1)}^{(k)}. \end{aligned}$$

Logo,

$$F_n^{(k)} = 2F_{n-1}^{(k)} - F_{n-(k+1)}^{(k)}. \quad (1.10)$$

Agora, para $2 \leq n \leq k+1$, temos que $F_{n-(k+1)}^{(k)} = 0$ e, portanto,

$$F_n^{(k)} = 2F_{n-1}^{(k)} = 2^2 F_{n-2}^{(k)} = \dots = 2^{n-2} F_{n-(n-2)}^{(k)} = 2^{n-2} F_2^{(k)} = 2^{n-2},$$

provando a primeira parte do teorema.

Agora, se $2 \leq j \leq k+1$, queremos mostrar que $F_{k+j}^{(k)} = 2^{k+j-2} - j2^{j-3}$. Vamos proceder por indução em j . Primeiramente, note que

$$F_{k+2}^{(k)} = 2F_{k+1}^{(k)} - F_1 = 2(2^{k+1}) - 1 = 2^{k+2} - 1.$$

Agora, suponha que a equação (1.9) seja verdadeira para $F_{k+j-1}^{(k)}$. Note que $j-1 \leq k$, logo $F_{j-1}^{(k)} = 2^{j-3}$. Portanto,

$$\begin{aligned} F_{k+j}^{(k)} &= 2F_{k+j-1}^{(k)} - F_{j-1}^{(k)} \\ &= 2(2^{k+j-3} - (j-1)2^{j-4}) - 2^{j-3} \\ &= 2^{k+j-2} - (j-1)2^{j-3} - 2^{j-3} \\ &= 2^{k+j-2} - j2^{j-3}, \end{aligned}$$

e o teorema está provado. □

Teorema 1.7. *Seja $F_n^{(k)}$ o n -ésimo número de k -bonacci e α a única raiz real positiva de $x^k - x^{k-1} - \dots - 1 = 0$, então*

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

Demonstração. Vamos proceder por indução em $n \geq 2$, para um $k \geq 2$ dado. Note que, pelo Lema 1.6, para $2 \leq n \leq k+1$, $F_n^{(k)} = 2^{n-2}$ e o resultado segue para esses casos. Suponha, então, que o resultado seja verdadeiro para todo inteiro menor que $n \geq k+2$, logo

$$\begin{aligned} \alpha^{n-3} &\leq F_{n-1}^{(k)} \leq \alpha^{n-2} \\ \alpha^{n-4} &\leq F_{n-2}^{(k)} \leq \alpha^{n-3} \end{aligned}$$

$$\begin{aligned} & \vdots \\ \alpha^{n-k-2} & \leq F_{n-k}^{(k)} \leq \alpha^{n-k-1}. \end{aligned}$$

Como $\alpha^k = \alpha^{k-1} + \dots + \alpha + 1$, então

$$\begin{aligned} \alpha^{n-2} &= \alpha^{n-3} + \dots + \alpha^{n-k-2} \\ \alpha^{n-1} &= \alpha^{n-2} + \dots + \alpha^{n-k-1}. \end{aligned}$$

Portanto, somando as equações na hipótese de indução acima, temos que

$$\begin{aligned} \alpha^{n-3} + \alpha^{n-4} + \dots + \alpha^{n-k-2} &\leq F_{n-1}^{(k)} + F_{n-2}^{(k)} + \dots + F_{n-k}^{(k)} \leq \alpha^{n-1} + \alpha^{n-2} + \dots + \alpha^{n-k-1} \\ \implies \alpha^{n-2} &\leq F_n^{(k)} \leq \alpha^{n-1}. \end{aligned}$$

□

1.2 Formas lineares em logaritmo

Nesta seção vamos explicar um pouco como utilizar formas lineares em logaritmo para resolver equações Diofantinas exponenciais. Em 1966, Baker estabeleceu o seguinte importante resultado:

Teorema 1.8. *Sejam $\alpha_1, \alpha_2, \dots, \alpha_n$ números algébricos sobre \mathbb{C} , diferentes de 0 e 1 tais que $\log \alpha_1, \log \alpha_2, \dots, \log \alpha_n$ são linearmente independentes sobre \mathbb{Q} . Então, para todos $(\beta_0, \beta_1, \beta_2, \dots, \beta_n) \in \overline{\mathbb{Q}} \setminus \{(0, 0, \dots, 0)\}$, temos que*

$$\beta_0 + \beta_1 \log \alpha_1 + \dots + \beta_n \log \alpha_n \neq 0.$$

Mas o resultado mais importante de Baker veio 9 anos mais tarde, o qual fornece uma cota inferior para formas lineares em logaritmo de algébricos:

Teorema 1.9. *Sejam $\alpha_1, \alpha_2, \dots, \alpha_n$ números algébricos sobre \mathbb{C} , diferentes de 0 e 1. Além disso, sejam b_1, b_2, \dots, b_n inteiros tais que*

$$b_1 \log \alpha_1 + \dots + b_n \log \alpha_n \neq 0.$$

Então

$$|b_1 \log \alpha_1 + \dots + b_n \log \alpha_n| \geq (eB)^{-C},$$

onde $B := \max\{|b_1|, \dots, |b_n|\}$ e C é uma constante efetivamente computável dependente apenas de n e $\alpha_1, \alpha_2, \dots, \alpha_n$.

Seja, agora, γ um algébrico de grau s . Vamos denotar por $h(\gamma)$ a *altura logarítmica* definida por

$$h(\gamma) := \frac{1}{s} \left(\log |a| + \sum_{j=1}^s \log \max\{1, |\gamma^{(j)}|\} \right),$$

onde a é o coeficiente líder do polinômio minimal de γ sobre \mathbb{Z} e $(\gamma^{(j)})_{1 \leq j \leq s}$ são os conjugados de γ sobre \mathbb{Q} .

O próximo resultado foi fornecido por Matveev em [49] e será essencial em nossos procedimentos futuros.

Teorema 1.10. *Sejam $\gamma_1, \dots, \gamma_n$ números algébricos reais e b_1, \dots, b_n inteiros. Seja D o grau da extensão finita $\mathbb{Q}(\gamma_1, \dots, \gamma_n)$ sobre \mathbb{Q} e, finalmente, sejam A_j números reais que satisfazem*

$$A_j \geq \max \{ Dh(\gamma_j), |\gamma_j|, 0.16 \}, \text{ para todo } j = 1, \dots, n.$$

Suponha que

$$B \geq \max \{ |b_1|, \dots, |b_n| \}.$$

Se $\gamma_1^{b_1} \cdots \gamma_t^{b_n} \neq 1$, então

$$|\gamma_1^{b_1} \cdots \gamma_t^{b_n} - 1| \geq \exp(-1.4 \cdot 30^{t+3} \cdot t^{4.5} \cdots D^2(1 + \log D)(1 + \log B)A_1 \cdots A_n).$$

Então, se queremos resolver uma equação Diofantina exponencial $G(m_1, m_2, \dots, m_n) = 0$ em inteiros positivos, podemos usar o teorema acima para transformar essa equação em uma inequação do tipo $|b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n| > \exp(-C \log m_n)$. Além disso, podemos usar algumas ferramentas para transformar a equação em outra desigualdade da forma $|b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n| < k^{-m_n}$. Combinando as duas inequações, temos

$$\frac{m_n}{\log m_n} < \frac{C}{\log k},$$

e como C e k são constantes e $m_n / \log m_n$ tende a infinito à medida que m_n cresce, então nossa equação possui um número finito de soluções. Ou seja, $\max \{m_1, \dots, m_n\} < K$. Assim, podemos usar algum método computacional para calcular essas soluções mecanicamente.

1.3 Método de redução

Se a constante K mencionada no final da seção anterior for muito grande, talvez não seja tão simples e talvez até não seja possível calcular as soluções da equação Diofantina exponencial $G(m_1, \dots, m_n) = 0$. Para tal, podemos utilizar algum método para reduzir essa constante de forma a facilitar a resolução do nosso problema. Aqui, vamos precisar do seguinte resultado de Dujella e Pethö([18]):

Teorema 1.11. *Suponha que M seja um inteiro positivo. Seja p/q um convergente da fração contínua do número irracional γ tal que $q > 6M$ e sejam A, B números reais com $A > 0$ e $B > 1$. Seja $\epsilon = \|\mu q\| - M \|\gamma q\|$, onde $\mu \in \mathbb{R}$ e $|a|$ denota o inteiro mais próximo de um número real a . Se $\epsilon > 0$, então não há soluções para o inequação*

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

em inteiros positivos m, n e k com

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

1.4 Outros resultados auxiliares

O método de formas lineares em logaritmo é extremamente eficiente para equações Diofantinas exponenciais (ou que possam ser expressadas de forma exponencial), mas pode não ser eficiente no caso de outros tipos de equações Diofantinas, como uma equação envolvendo fatoriais, por exemplo.

Aqui, vamos expor alguns resultados auxiliares que nos ajudarão na resolução de equações Diofantinas envolvendo fatoriais. Primeiramente, vamos definir formalmente o conceito de valorização (ou ordem) de um racional.

Seja $p \in \mathbb{Z}$ primo. Todo inteiro $a \in \mathbb{Z}$ pode ser escrito como $a = p^{\nu_p(a)} a'$, onde p não divide a' e tal representação é única. Assim, podemos definir:

Definição 1. *Seja um primo $p \in \mathbb{N}$. A valorização p -ádica em \mathbb{Z} é a função*

$$\nu_p : \mathbb{N} \cup \{0\} \longrightarrow \mathbb{R},$$

definida da seguinte forma: para cada $a \in \mathbb{Z}$ não-nulo, seja $\nu_p(a)$ o único inteiro positivo que satisfaz

$$a = p^{\nu_p(a)} a',$$

onde p e a' são primos entre si.

Vamos estender ν_p para os racionais da seguinte forma: se $x = a/b \in \mathbb{Q}$, então,

$$\nu_p(x) = \nu_p(a) - \nu_p(b).$$

Por conveniência, a partir deste momento, vamos estabelecer que $\nu_p(0) = +\infty$. Vamos também observar que a valorização p -ádica de $x \in \mathbb{Q}$ também é determinada pela fórmula

$$x = \frac{a}{b} p^{\nu_p(x)},$$

onde p não divide ab .

Temos as seguintes propriedades da valorização p -ádica:

Lema 1.12. *Para todo $x, y \in \mathbb{Q}$, temos que*

1. $\nu_p(xy) = \nu_p(x) + \nu_p(y)$
2. $\nu_p(x + y) \geq \min\{\nu_p(x), \nu_p(y)\}$.

Demonstração. 1. Temos que $x = p^{\nu_p(x)}a/b$, $y = p^{\nu_p(y)}c/d$ e $xy = p^{\nu_p(xy)}e/f$, onde p não divide ab , cd e ef . Portanto,

$$p^{\nu_p(xy)}\frac{e}{f} = xy = p^{\nu_p(x)}\frac{a}{b}p^{\nu_p(y)}\frac{c}{d} = p^{\nu_p(x)+\nu_p(y)}\frac{ac}{bd},$$

e, como a valorização é única, temos

$$\nu_p(xy) = \nu_p(x) + \nu_p(y).$$

2. Temos que

$$x + y = p^{\nu_p(x+y)}\frac{g}{h} = p^{\nu_p(x)}\frac{a}{b} + p^{\nu_p(y)}\frac{c}{d}.$$

Seja $\nu = \min\{\nu_p(x), \nu_p(y)\}$, logo:

$$\begin{aligned} x + y &= p^{\nu_p(x+y)}\frac{g}{h} = p^{\nu_p(x)}\frac{a}{b} + p^{\nu_p(y)}\frac{c}{d} \\ &= p^\nu(p^{\nu_p(x)-\nu}\frac{a}{b} + p^{\nu_p(y)-\nu}\frac{c}{d}), \end{aligned}$$

como $\nu_p(x) - \nu \geq 0$ e $\nu_p(y) - \nu \geq 0$, então

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

□

Agora, vamos proceder à fórmula de *de Polignac*, a fim de achar um limitante para fatoriais em termos de sua valorização p -ádica.

Vamos denotar por $[a]$ a parte inteira de um real a .

Lema 1.13. *Sejam $a, b, c \in \mathbb{N}$. Temos que*

$$\left\lfloor \frac{\left\lfloor \frac{a}{b} \right\rfloor}{c} \right\rfloor = \left\lfloor \frac{a}{bc} \right\rfloor.$$

Demonstração. Sejam

$$q_1 = \left\lfloor \frac{a}{b} \right\rfloor \quad q_2 = \left\lfloor \frac{\left\lfloor \frac{a}{b} \right\rfloor}{c} \right\rfloor.$$

Logo,

$$a = bq_1 + r_1, \text{ com } r_1 \leq b - 1,$$

e

$$\left\lfloor \frac{a}{b} \right\rfloor = q_1 = cq_2 + r_2, \text{ com } r_2 \leq c - 1.$$

Portanto,

$$a = bq_1 + r_1 = b(cq_2 + r_2) + r_1 = bcq_2 + br_2 + r_1.$$

Como

$$br_2 + r_1 \leq b(c-1) + b - 1 = bc - 1,$$

então

$$q_2 = \left\lfloor \frac{a}{bc} \right\rfloor.$$

□

Teorema 1.14. (Fórmula de de Polignac) *Sejam n um número natural, p um número primo e $\nu_p(n)$ a valorização p -ádica de n . Temos então que*

$$\nu_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^{\lfloor \log_p(n) \rfloor}} \right\rfloor.$$

Demonstração. Vamos proceder por indução sobre $n \geq 1$. Para $n = 1$, o resultado segue diretamente. Logo, suponha que seja válido para todo $m < n$, assim, temos que os múltiplos de p entre 1 e n são

$$p, 2p, 3p, \dots, \left\lfloor \frac{n}{p} \right\rfloor p.$$

Portanto,

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

Pela hipótese de indução e pelo Lema 1.13, temos que

$$\begin{aligned} \nu_p \left(\left\lfloor \frac{n}{p} \right\rfloor! \right) &= \left\lfloor \frac{\left\lfloor \frac{n}{p} \right\rfloor}{p} \right\rfloor + \left\lfloor \frac{\left\lfloor \frac{n}{p} \right\rfloor}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{\left\lfloor \frac{n}{p} \right\rfloor}{p^{\lfloor \log_p n \rfloor - 1}} \right\rfloor \\ &= \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^{\lfloor \log_p n \rfloor}} \right\rfloor, \end{aligned}$$

e o resultado segue. □

Note que, como $a - 1 < \lfloor a \rfloor \leq a$, então

$$\begin{aligned} \nu_p(n!) &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^{\lfloor \log_p(n) \rfloor}} \right\rfloor \\ &= \sum_{j=1}^{\lfloor \log_p n \rfloor} \left\lfloor \frac{n}{p^j} \right\rfloor \\ &\leq \sum_{j=1}^{\infty} \frac{n}{p^j} \\ &= \frac{n}{p-1}. \end{aligned}$$

Além disso,

$$\begin{aligned}\nu_p(n!) &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^{\lfloor \log_p(n) \rfloor}} \right\rfloor \\ &> \left(\frac{n}{p} - 1 \right) + \left(\frac{n}{p^2} - 1 \right) + \cdots + \left(\frac{n}{p^{\lfloor \log_p n \rfloor}} - 1 \right) \\ &= \frac{n}{p-1} - \lfloor \log_p n \rfloor.\end{aligned}$$

Assim, temos que

Lema 1.15. *Para todo inteiro $n \geq 1$ e p primo, temos que*

$$\frac{n}{p-1} - \left\lfloor \frac{\log n}{\log p} \right\rfloor - 1 \leq \nu_p(n!) \leq \frac{n-1}{p-1}.$$

Capítulo 2

Números Perfeitos Pares na Sequência de Fibonacci Generalizada

2.1 A equação $F_n^{(k)} = 2^{p-1}(2^p - 1)$

Conforme mencionado previamente, estamos direcionando nossos estudos para sequências de Fibonacci generalizadas de ordem $k \geq 3$. Neste capítulo, vamos procurar números perfeitos pares em tais sequências. Por agora, vamos estabelecer que p denota um número primo, tal que $2^p - 1$ também é primo. Como sabemos, um número inteiro n é dito *perfeito* quando $\sigma(n) = 2n$, onde $\sigma(n)$ é a soma de todos os divisores positivos de n . Também sabemos que, pelo Teorema de Euclides-Euler, todo número perfeito par é da forma $2^{p-1}(2^p - 1)$. Com isso, queremos achar as soluções (se existirem) da equação Diofantina

$$F_n^{(k)} = 2^{p-1}(2^p - 1). \quad (2.1)$$

Assim, neste capítulo, vamos provar o seguinte teorema:

Teorema 2.1. *A equação Diofantina (2.1) não apresenta soluções para inteiros positivos n, k e p , onde p e $2^p - 1$ são primos, se ao menos uma das seguintes condições for satisfeita:*

1. $2 \leq k \leq 167$;
2. $n \neq 2p + 1$;
3. $n = 2p + 1$ e $p \geq k$;
4. $n = 2p + 1, p < k$ e $k \not\equiv 3 \pmod{4}$;
5. $n = 2p + 1, p < k, k \equiv 3 \pmod{4}$ e $2p - k + 1 \neq 2^{k-p+1}$.

Em particular, não há nenhum número perfeito par em $(F_n^{(k)})_{n \geq -(k-2)}$ quando $k \not\equiv 3 \pmod{4}$.

Observação: É importante mencionar que, apesar da restrição $k \not\equiv 3 \pmod{4}$, acredita-se que todas as soluções da equação (2.1) estão caracterizadas. Uma justificativa intuitiva para tal, se deve ao fato de todas essas soluções acontecerem se, e somente se,

$$2p - k + 1 = 2^{k-p+1}. \quad (2.2)$$

Pois, se $p < k$ e (2.2) é válida, podemos escrever $t = k - p$, e obter

$$2p - k + 1 = p + p - k + 1 = p + t + 1 = 2^{t+1} = 2^{k-p+1}.$$

Assim, não só temos que ter p e $2^p - 1$ primos, como temos também que $p = 2^{t+1} - t - 1$ e $2^{2^{t+1}-t-1} - 1$ devem ser números primos. Lembrando que o conjunto dos números primos tem densidade nula nos naturais pelo Teorema do Número Primo e acredita-se que o conjunto dos primos de Mersenne também tem densidade nula no conjunto dos números primos pela Conjectura de Wagstaff.

Tal observação vai ao encontro da revisão do artigo [20] feita por Florian Luca ao site MathSciNet.

Disponível em: <www.ams.org/mathscinet>. Acesso em: 21 de Janeiro de 2016.

2.2 Um limitante para n e p em termos de k

Primeiramente, note que $F_n^{(k)}$ é uma potência de 2 para todo $1 \leq n \leq k + 1$, logo podemos supor que $n > k + 1$. Aqui, iremos estabelecer um limitante para n e p em termos de k . Iremos provar o seguinte resultado:

Lema 2.2. *Se (n, k, p) é uma solução inteira da equação Diofantina (2.1) com $n > k + 1$, então*

$$n < 1.7 \cdot 10^{14} k^4 \log^3 k \quad e \quad p < 1.2 \cdot 10^{14} k^4 \log^3 k. \quad (2.3)$$

Demonstração. Usando a equação (2.1) e o Teorema 1.2, temos que:

$$F_n^{(k)} = \sum_{i=1}^k g(\alpha_i, k) \alpha_i^{n-1} = g(\alpha, k) \alpha^{n-1} + E_k(n) = 2^{p-1}(2^p - 1) = 2^{2p-1} - 2^{p-1}.$$

Logo,

$$g(\alpha, k) \alpha^{n-1} - 2^{2p-1} = -2^{p-1} - E_k(n) < 0. \quad (2.4)$$

Portanto, dividindo os dois lados por 2^{2p-1} e usando o Teorema 1.5, temos que:

$$\left| \frac{g(\alpha, k) \alpha^{n-1}}{2^{2p-1}} - 1 \right| = \left| \frac{2^{p-1}}{2^{2p-1}} + \frac{E_k(n)}{2^{2p-1}} \right| < \left| \frac{1}{2^p} + \frac{1}{2^{2p}} \right| = \frac{1}{2^p} \left| 1 + \frac{1}{2^p} \right| < \frac{1}{2^{p-1}}. \quad (2.5)$$

Agora, a fim de podermos usar o Teorema 1.10, vamos definir $t := 3$,

$$\gamma_1 := g(\alpha, k), \gamma_2 := 2, \gamma_3 := \alpha$$

e

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

Para tal escolha, temos que $D = [\mathbb{Q}(\alpha) : \mathbb{Q}] = k$. Também temos que $h(\gamma_2) = \log 2$. Além disso, temos que os conjugados $\alpha_2, \dots, \alpha_k$ de α estão dentro do círculo unitário, logo $\log(\max\{1, |\alpha_i|\}) = \log 1 = 0$, para todo $2 \leq i \leq k$. Portanto,

$$h(\gamma_3) = h(\alpha) = \frac{\log(\alpha)}{k} < \frac{\log 2}{k} < \frac{0.7}{k}.$$

Vamos então achar uma estimativa para $h(\gamma_1)$. Primeiramente, temos que:

$$h(\gamma_1) = h(g(\alpha, k)) = h\left(\frac{\alpha - 1}{2 + (k + 1)(\alpha - 2)}\right).$$

Escrevendo o polinômio característico de γ_1 ,

$$f_{\gamma_1}(x) = \prod_{i=1}^k \left(x - \frac{\alpha_i}{2 + (k + 1)(\alpha_i - 2)}\right),$$

temos, como consequência direta do Teorema Fundamental das Funções Simétricas (utilizando as funções simétricas elementares e as relações de Girard), que $f_{\gamma_1}(x) \in \mathbb{Q}[x]$. Portanto, o coeficiente líder a_0 do polinômio minimal de γ_1 sobre \mathbb{Z} divide $\prod_{i=1}^k (2 + (k + 1)(\alpha_i - 2))$. Escrevendo $\Psi_k(y) := \prod_{i=1}^k (y - \alpha_i)$, observe que

$$|\Psi_k(y)| < \max\{y^k, 1 + y + \dots + y^{k-1}\} < 2^k, \text{ para todo } 0 < y < 2.$$

Assim, temos que

$$\begin{aligned} a_0 &\leq \left| \prod_{i=1}^k (2 + (k + 1)(\alpha_i - 2)) \right| \\ &= (k + 1)^k \left| \prod_{i=1}^k \left(2 - \frac{2}{k + 1} - \alpha_i\right) \right| \\ &= (k + 1)^k \left| \Psi_k\left(2 - \frac{2}{k + 1}\right) \right| \\ &< 2^k (k + 1)^k. \end{aligned}$$

Além disso, usando desigualdade triangular, temos que

$$|2 + (k + 1)(\alpha_i - 2)| = |(k + 1)(\alpha_1 - 2) - (-2)| \geq (k + 1)|\alpha_i - 2| - 2 > k - 1 > 1,$$

e que $2 + (k + 1)(\alpha - 2) > 1/2$, pois $2(1 - 2^{-k}) < \alpha < 2$ e $k > 2$.

Portanto,

$$\left| \frac{\alpha_i - 1}{2 + (k + 1)(\alpha_i - 2)} \right| < 2, \text{ para todo } 1 \leq i \leq k. \quad (2.6)$$

Logo,

$$\begin{aligned}
h(\gamma_1) &= h\left(\frac{\alpha - 1}{2 + (k + 1)(\alpha - 2)}\right) \\
&= \frac{1}{k} \left(\log a_0 + \sum_{i=1}^k \log \max \left\{ \left| \frac{\alpha_i - 1}{2 + (k + 1)(\alpha_i - 2)} \right|, 1 \right\} \right) \\
&< \frac{1}{k} (k \log 2 + k \log(k + 1) + k \log 2) \\
&= \log(k + 1) + \log 4 \\
&= \log(4k + 4).
\end{aligned}$$

Assim, podemos tomar $A_1 := k \log(4k + 4)$, $A_2 := k \log 2$ e $A_3 := 0.7$.

Note que $|-2p + 1|$ e $|n - 1|$ são ambos maiores do que 1, logo $\max\{|b_1|, |b_2|, |b_3|\} = \max\{2p - 1, n - 1\}$. Usando a equação (2.1), o Teorema 1.7 e o fato de que $2^p - 1 > 2^{p/2}$ para todo $p \geq 2$, temos que

$$2^{n-1} \geq F_n^{(k)} = 2^{p-1}(2^p - 1) > 2^{3p/2-1} \Rightarrow n > \frac{3p}{2}. \quad (2.7)$$

Assim, podemos escolher $B := 2n - 3$. Além disso, pela equação (2.4), temos que $g(\alpha, k)\alpha^{n-1}2^{-2p+1} < 1$. Logo, estamos prontos para utilizar o Teorema 1.10.

Portanto, usando que $1 + \log k < 2 \log k$ e $\log(4k + 4) < 2.6 \log k$, quando $k \geq 3$,

$$\begin{aligned}
\left| \frac{g(\alpha, k)\alpha^{n-1}}{2^{2p-1}} - 1 \right| &\geq \exp(-0.98 \cdot 30^6 \cdot 3^{4.5} \cdot k^4(1 + \log k)(1 + \log(2n - 3)) \log(4k + 4) \log 2) \\
&> \exp(-3.7 \cdot 10^{11} k^4 \log^2 k(1 + \log(2n - 3))).
\end{aligned}$$

Usando esse fato, a desigualdade (2.5) e que $1 + \log(2n - 3) < 2 \log n$ para $n \geq 2$, temos que

$$\begin{aligned}
&\exp(-3.7 \cdot 10^{11} k^4 \log^2 k(1 + \log(2n - 3))) < \frac{1}{2^{p-1}} \\
&\Rightarrow 2^{p-1} < \exp(3.7 \cdot 10^{11} k^4 \log^2 k(1 + \log(2n - 3))) \\
&\Rightarrow \log 2^{p-1} < 3.7 \cdot 10^{11} k^4 \log^2 k(1 + \log(2n - 3)) < 7.4 \cdot 10^{11} k^4 \log^2 k \log n \\
&\quad \Rightarrow \log 2^{p-1} < 7.4 \cdot 10^{11} k^4 \log^2 k \log n \\
&\quad \Rightarrow p - 1 < 10.6759 \cdot 10^{11} k^4 \log^2 k \log n.
\end{aligned}$$

Agora, note que $\alpha^{n-2} \leq F_n^{(k)} = 2^{p-1}(2^p - 1) = 2^{2p-1} - 2^{p-1} < 2^{2p-1}$. Portanto,

$$2p - 1 > 0.8n - 1.7, \quad (2.8)$$

assim $2p - 2 > 0.8n - 2.7 \Rightarrow p - 1 > 0.4n - 1.35$.

Logo,

$$\begin{aligned} p - 1 &< 10.6759 \cdot 10^{11} k^4 \log^2 k \log n \\ \Rightarrow 0.4n &< 10.676 \cdot 10^{11} k^4 \log^2 k \log n. \end{aligned}$$

Portanto,

$$\frac{n}{\log n} < 2.7 \cdot 10^{12} k^4 \log^2 k. \quad (2.9)$$

Agora, note que, para $x > e$, a função $x/\log x$ é crescente. Suponha que, para $A \geq 3$,

$$\frac{x}{\log x} < A \Rightarrow x > 2A \log A > e,$$

logo, como $2 \log A < A$ para $A \geq 3$, temos que

$$\frac{x}{\log x} > \frac{2A \log A}{\log(2A \log A)} > \frac{2A \log A}{\log A^2} = A,$$

que é uma contradição. Portanto,

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

Assim, colocando $x := n$ e $A := 2.7 \cdot 10^{12} k^4 \log^2 k$, temos que

$$n < 1.7 \cdot 10^{14} k^4 \log^3 k. \quad (2.10)$$

Além disso, usando a desigualdade (2.7), temos que

$$p < 1.2 \cdot 10^{12} k^4 \log^3 k.$$

Isso conclui a prova do lema. □

2.3 Os casos pequenos: $3 \leq k \leq 167$

Na seção passada, estabelecemos uma primeira cota de n e p em função de k . Neste momento, vamos estudar os casos onde $3 \leq k \leq 167$. Mais precisamente, vamos provar o seguinte lema:

Lema 2.3. *A equação (2.1) não apresenta soluções para $n > k + 1$ e $3 \leq k \leq 167$.*

Demonstração. Primeiramente, podemos usar o programa *Mathematica* para verificar em tempo hábil que não há soluções da equação (2.1) para $p \leq 23$. Assim, vamos assumir que $p > 23$. Aplicado o logaritmo e usando as equações (2.4) e (2.5) temos que

$$0 < (2p - 1) \log 2 - (n - 1) \log \alpha + \log(1/g(\alpha, k)) < 1.001 \cdot 2^{-p+1}.$$

Dividindo a equação acima por $\log \alpha$, obtemos

$$0 < (2p - 1)\gamma_k - (n - 1) + \mu_k < 3.6 \cdot 2^{-p}, \quad (2.11)$$

onde $\gamma_k = \log 2 / \log \alpha^{(k)}$, $\mu_k = \log(1/g(\alpha^{(k)}, k)) / \log \alpha^{(k)}$ e $\alpha^{(k)}$ é a raiz real positiva de $x^k - x^{k-1} - \dots - 1 = 0$.

Note que, se γ_k for racional, então $\gamma_k = p/q$ para inteiros positivos p e q . Assim $p/q = \log 2 / \log \alpha^{(k)} \Rightarrow 2^q = (\alpha^{(k)})^p$. Conjugando essa relação por algum automorfismo do grupo de Galois do polinômio característico da sequência sobre \mathbb{Q} e usando o fato de que tal automorfismo deixa \mathbb{Q} fixo, temos que $2^q = |(\alpha_i^{(k)})^q| < 1$, para $i > 1$, o que é absurdo, pois $q \geq 1$. Logo, γ_k é irracional e, portanto, possui fração contínua infinita. Seja $q_{m,k}$ o denominador do m -ésimo convergente da fração contínua de γ_k . Tomando $M_k := 2.41 \cdot 10^{14} k^4 \log^3 k \leq M_{167} < 2.6 \cdot 10^{25}$ para todo $3 \leq k \leq 167$, usamos o *Mathematica* para obter

$$\min_{3 \leq k \leq 167} q_{90,k} > 7 \cdot 10^{38} > 6M_{167}$$

e

$$\max_{3 \leq k \leq 167} q_{90,k} < 4.4 \cdot 10^{102}.$$

Agora, vamos definir $\epsilon_k := \|\mu_k q_{90,k}\| - M_k \|\gamma_k q_{90,k}\|$ e assim

$$\min_{3 \leq k \leq 167} \epsilon_k = 0.0000571469 \dots$$

Temos, pelo Lema 2.2, que $2p - 1 < M_k$. Assim, colocando $A = 3.6$ e $B = 2$, pelo Teorema 1.11, a equação (2.11) não tem solução para p satisfazendo

$$p \geq \frac{\log(Aq_{90,k}/\epsilon_k)}{\log B}.$$

Logo, se a equação (2.1) tem solução,

$$p < \frac{\log(Aq_{90,k}/\epsilon_k)}{\log B} \leq \frac{\log(3.6 \cdot 4.4 \cdot 10^{102}/0.000057146)}{\log 2} = 356.917 \dots$$

Então, pela equação (2.8), temos que $n \leq 890$, e como $2^p - 1$ é primo, então

$$p \in \{2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127\}.$$

Basta verificar pelo *Mathematica* que a equação (2.1) não tem solução para nenhum desses casos e o lema está provado. \square

2.4 $n \neq 2p + 1$

Note que o lema da seção anterior prova a primeira parte do Teorema 2.1. Vamos agora direcionar os estudos à prova dos itens restantes. Mais precisamente, aqui, para o caso quando $n \neq 2p + 1$.

Pelo Lema 2.3, podemos considerar $k \geq 168$. Assim, usando o Lema 2.2, temos que

$$n < 1.7 \cdot 10^{14} k^4 \log^3 k < 2^{k/2}.$$

Seja, agora, $\lambda := 2 - \alpha > 0$. Como $2(1 - 2^{-k}) < \alpha < 2$, então $\lambda < 2 - 2(1 - 2^{-k}) = 1/2^{k-1}$. Ou seja, $\lambda \in (0, 1/2^{k-1})$. Além disso,

$$\begin{aligned} \alpha^{n-1} &= (2 - \lambda)^{n-1} \\ &= 2^{n-1} \left(1 - \frac{\lambda}{2}\right)^{n-1} \\ &= 2^{n-1} e^{(n-1) \log(1-\lambda/2)} \\ &\geq 2^{n-1} e^{-\lambda(n-1)}, \end{aligned}$$

onde usamos o fato de que $\log(1 - x) \geq -2x$ para todo $x < 1/2$. Também temos que $e^{-x} \geq 1 - x$ para todo $x \in \mathbb{R}$. Logo,

$$\alpha^{n-1} \geq 2^{n-1}(1 - \lambda(n-1)).$$

Note que $\lambda(n-1) < (n-1)/2^{k-1} < 2^{k/2}/2^{k-1} = 2/2^{k/2}$. Logo

$$\alpha^{n-1} > 2^{n-1}(1 - 2/2^{k/2}).$$

Portanto,

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

ou

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

Note agora que $g(\alpha, k) = (\alpha - 1)/(2 + (k + 1)(\alpha - 2))$ como uma função de α é uma função contínua (pois $\alpha \neq 2$). Portanto

$$\frac{\partial g}{\partial \alpha}(\alpha, k) = \frac{1 - k}{(2 + (k + 1)(\alpha - 2))^2}.$$

Usando o Teorema do Valor Médio, existe $\theta \in (\alpha, 2)$ tal que

$$g(\alpha, k) = g(2, k) + (\alpha - 2) \frac{\partial g}{\partial \alpha}(\theta, k).$$

Para $k \geq 3$ temos que $|\partial g / \partial \alpha(\theta)| = (k - 1)/(2 + (k + 1)(\theta - 2))^2 < k$.

Portanto,

$$|g(\alpha, k) - g(2, k)| = |\alpha - 2| \left| \frac{\partial g}{\partial \alpha}(\theta, k) \right| = \lambda \left| \frac{\partial g}{\partial \alpha}(\theta, k) \right| < \frac{2k}{2^k}.$$

Escrevendo

$$\alpha^{n-1} = 2^{n-1} + \delta \quad e \quad g(\alpha, k) = g(2, k) + \eta,$$

então temos que

$$|\delta| < \frac{2^n}{2^{k/2}} \quad e \quad |\eta| < \frac{2k}{2^k}.$$

Além disso, como $g(2, k) = 1/2$,

$$g(\alpha, k)\alpha^{n-1} = 2^{n-2} + \frac{\delta}{2} + 2^{n-1}\eta + \eta\delta.$$

Observe que

$$\left| \frac{g(\alpha, k)\alpha^{n-1}}{2^{2p-1}} - 1 \right| < \frac{1}{2^{p-1}} \implies |2^{2p-1} - g(\alpha, k)\alpha^{n-1}| < \frac{2^{2p-1}}{2^{p-1}} = 2^p.$$

Assim

$$\begin{aligned} |2^{2p-1} - 2^{n-2}| &= \left| (2^{2p-1} - g(\alpha, k)\alpha^{n-1}) + \frac{\delta}{2} + 2^{n-1}\eta + \eta\delta \right| \\ &< 2^p + \frac{2^{n-1}}{2^{k/2}} + \frac{2^n k}{2^k} + \frac{2^{n+1}k}{2^{3k/2}}. \end{aligned}$$

Usando os fatos de que $4k/2^k < 1/2^{k/2}$ e $8k/2^{3k/2} < 1/2^{k/2}$, temos que

$$|2^{n-2} - 2^{2p-1}| < 2^p + \frac{5 \cdot 2^{n-2}}{2^{k/2}},$$

ou equivalentemente

$$|1 - 2^{2p-n+1}| < 2^{p-n+2} + \frac{5}{2^{k/2}}.$$

Pela equação (2.7), temos que $p < 2n/3$. Assim,

$$|1 - 2^{2p-n+1}| < \frac{4}{2^{n/3}} + \frac{5}{2^{k/2}} < \frac{9}{(\sqrt[3]{2})^k},$$

pois $n > k$.

Temos que $n \neq 2p + 1$, logo $2p \geq n$ ou $n \geq 2p + 2$. No primeiro caso, $2p - n + 1 \geq 1$, logo

$$|1 - 2^{2p-n+1}| > \frac{1}{2}.$$

No segundo caso, $2p - n + 1 \leq 0$, logo $n - 2p - 1 \geq 1$. Portanto,

$$|1 - 2^{2p-n+1}| = \left|1 - \frac{1}{2^{n-2p-1}}\right| \geq 1 - \frac{1}{2^{n-2p-1}} \geq 1 - \frac{1}{2} = \frac{1}{2}.$$

Portanto, $(\sqrt[3]{2})^k < 18 \Rightarrow k \leq 13$, que é absurdo. Assim, a equação (2.1) não tem solução quando $n \neq 2p + 1$.

2.5 $n = 2p + 1$ e a conclusão do Teorema 2.1

Observe que, pelos cálculos executados nas seções anteriores deste capítulo, conseguimos demonstrar os dois primeiros itens do Teorema 2.1. Aqui, vamos considerar os casos restantes, nos quais $n = 2p + 1$. Assim, podemos considerar uma nova versão da equação Diofantina (2.1), com uma variável a menos:

$$F_{2p+1}^{(k)} = 2^{p-1}(2^p - 1). \quad (2.12)$$

Demonstraremos agora que a equação (2.12) não tem solução. Para tal, vamos considerar dois casos.

Caso 1: $p \geq k$.

Nesse caso, vamos mostrar de fato que

$$F_{2p+1}^{(k)} < 2^{p-1}(2^p - 1),$$

para todo $p \geq k$. Com efeito, vamos mostrar que a relação acima vale independente da primalidade de p e para tal, vamos proceder por indução em $p \geq k$. Na base de indução, $p = k$, temos, pelo Lema 1.6, que

$$\begin{aligned} 2^{k-1}(2^k - 1) - F_{2k+1}^{(k)} &= 2^{k-1}(2^k - 1) - 2^{2k-1} + (k+1)2^{k-1} \\ &= (k+1)2^{k-2} - 2^{k-1} \\ &> 0. \end{aligned}$$

Como $n = 2p + 1$, temos que $n \geq 2k + 1$. Logo

$$\begin{aligned} F_{n-k}^{(k)} &\geq 1 \\ \implies F_n^{(k)} + F_{n-1}^{(k)} + \dots + F_{n-k+1}^{(k)} &\leq F_{n-1}^{(k)} + \dots + F_{n-k+1}^{(k)} + F_{n-k}^{(k)} + F_n^{(k)} \\ \implies F_{n+1}^{(k)} &\leq 2F_n^{(k)}. \end{aligned}$$

Suponha agora que $F_{2p+1}^{(k)} < 2^{p-1}(2^p - 1)$. Assim

$$\begin{aligned} F_{2p+3}^{(k)} &\leq 4F_{2p+1}^{(k)} \\ &< 2^p(2^{p+1} - 2) \\ &< 2^p(2^{p+1} - 1). \end{aligned}$$

O que conclui nossa indução e, conseqüentemente, esse caso. Logo, a equação (2.12) não tem solução quando $p \geq k$.

Caso 2: $p < k$.

Neste caso, como supomos que $n = 2p + 1 > k + 1$, então $k/2 < p < k \Rightarrow 2 \leq 2p + 1 - k \leq k$. Usando o Lema 1.6, temos que

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

Juntando essa relação com a equação (2.12), temos que

$$2p + 1 - k = 2^{k-p+1}.$$

Note que, se k é par, então $2p - k + 1$ é ímpar, logo $k - p + 1 = 0$ e $2p + 1 - k = 1 \Rightarrow 2p = k$ e $k = p - 1$, o que é absurdo. Portanto, k é ímpar. Se $k \equiv 1 \pmod{4}$, então, com $l \in \mathbb{Z}$,

$$2p + 1 - k = 2p + 1 - 4l - 1 = 2(p - 2l),$$

e como $p - 2l$ é ímpar, então a valorização 2-ádica de $2p + 1 - k$ é 1. Logo, $k - p + 1 = 1 \Rightarrow k = p$, que é absurdo.

Assim, juntando as seções anteriores, concluímos a demonstração do Teorema 2.1. \square

Capítulo 3

A Valorização 2-ádica de Q_n e a Equação $Q_n = m!$

Neste capítulo vamos direcionar nossos estudos para a resolução da equação Diofantina

$$Q_n = m!. \quad (3.1)$$

Observe que, diferentemente da equação (2.1), não podemos proceder aqui da mesma forma, uma vez que geralmente o método das formas lineares em logaritmo *à la Baker* não se aplica nesse caso. Por outro lado, como dito anteriormente, Luca resolveu a equação $F_n = F_n^{(2)} = m!$ tendo como base o Teorema do Divisor Primitivo. Mais uma vez, não temos tal propriedade para sequências de k -bonacci. Vamos aqui seguir um processo análogo ao feito por D. Marques e T. Lengyel para resolver a equação $T_n = m!$ para obter

Teorema 3.1. *As únicas soluções para a equação Diofantina*

$$Q_n = m! \quad (3.2)$$

em inteiros positivos m e $n \not\equiv 75 \pmod{80}$ são

$$(n, m) \in \{(1, 1), (2, 1), (3, 2)\}.$$

3.1 Alguns lemas preliminares

Num primeiro momento, vamos estabelecer alguns lemas preliminares.

Lema 3.2. *Para inteiros n, m com $n \geq 0$ e $m \geq 4$, temos que*

$$Q_{n+m} = Q_{m-3}Q_n + (Q_{m-3} + Q_{m-4})Q_{n+1} + (Q_{m-3} + Q_{m-4} + Q_{m-5})Q_{n+2} + Q_{m-2}Q_{n+3}.$$

Demonstração. Queremos achar $\alpha_1, \alpha_2, \alpha_3$ e α_4 tais que

$$Q_{n+m} = \alpha_1 Q_n + \alpha_2 Q_{n+1} + \alpha_3 Q_{n+2} + \alpha_4 Q_{n+3}.$$

Note que, $Q_{n+m+1} = \alpha_1 Q_{n+1} + \alpha_2 Q_{n+2} + \alpha_3 Q_{n+3} + \alpha_4 Q_{n+4}$, $Q_{n+m+2} = \alpha_1 Q_{n+2} + \alpha_2 Q_{n+3} + \alpha_3 Q_{n+4} + \alpha_4 Q_{n+5}$ e $Q_{n+m+3} = \alpha_1 Q_{n+3} + \alpha_2 Q_{n+4} + \alpha_3 Q_{n+5} + \alpha_4 Q_{n+6}$. Portanto, desejamos resolver o seguinte sistema linear

$$\begin{cases} Q_{n+m} = \alpha_1 Q_n + \alpha_2 Q_{n+1} + \alpha_3 Q_{n+2} + \alpha_4 Q_{n+3} \\ Q_{n+m+1} = \alpha_1 Q_{n+1} + \alpha_2 Q_{n+2} + \alpha_3 Q_{n+3} + \alpha_4 Q_{n+4} \\ Q_{n+m+2} = \alpha_1 Q_{n+2} + \alpha_2 Q_{n+3} + \alpha_3 Q_{n+4} + \alpha_4 Q_{n+5} \\ Q_{n+m+3} = \alpha_1 Q_{n+3} + \alpha_2 Q_{n+4} + \alpha_3 Q_{n+5} + \alpha_4 Q_{n+6} \end{cases}$$

Reescrevendo o sistema linear acima em forma matricial, temos que

$$\begin{bmatrix} Q_n & Q_{n+1} & Q_{n+2} & Q_{n+3} \\ Q_{n+1} & Q_{n+2} & Q_{n+3} & Q_{n+4} \\ Q_{n+2} & Q_{n+3} & Q_{n+4} & Q_{n+5} \\ Q_{n+3} & Q_{n+4} & Q_{n+5} & Q_{n+6} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{bmatrix} = \begin{bmatrix} Q_{n+m} \\ Q_{n+m+1} \\ Q_{n+m+2} \\ Q_{n+m+3} \end{bmatrix}$$

Para $n = 0$, temos que

$$\begin{bmatrix} Q_0 & Q_1 & Q_2 & Q_3 \\ Q_1 & Q_2 & Q_3 & Q_4 \\ Q_2 & Q_3 & Q_4 & Q_5 \\ Q_3 & Q_4 & Q_5 & Q_6 \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{bmatrix} = \begin{bmatrix} Q_m \\ Q_{m+1} \\ Q_{m+2} \\ Q_{m+3} \end{bmatrix}$$

e, assim, a matriz aumentada é

$$\left[\begin{array}{cccc|c} 0 & 1 & 1 & 2 & Q_m \\ 1 & 1 & 2 & 4 & Q_{m+1} \\ 1 & 2 & 4 & 8 & Q_{m+2} \\ 2 & 4 & 8 & 15 & Q_{m+3} \end{array} \right].$$

Note que, pela equação (1.10) para $k = 4$, temos que $2Q_{m+2} - Q_{m+3} = Q_{m-2}$, $2Q_{m+1} - Q_{m+2} = Q_{m-3}$, $2Q_m - Q_{m+1} = Q_{m-4}$ e $Q_m - Q_{m-3} - Q_{m-4} - 2Q_{m-2} = Q_{m-1} - Q_{m-2} = Q_{m-3} + Q_{m-4} + Q_{m-5}$.

Assim, podemos fazer algumas operações elementares para obter

$$\begin{aligned} & \left[\begin{array}{cccc|c} 0 & 1 & 1 & 2 & Q_m \\ 1 & 1 & 2 & 4 & Q_{m+1} \\ 1 & 2 & 4 & 8 & Q_{m+2} \\ 2 & 4 & 8 & 15 & Q_{m+3} \end{array} \right] \rightarrow \left[\begin{array}{cccc|c} 0 & 1 & 1 & 2 & Q_m \\ 1 & 1 & 2 & 4 & Q_{m+1} \\ 1 & 2 & 4 & 8 & Q_{m+2} \\ 0 & 0 & 0 & 1 & Q_{m-2} \end{array} \right] \rightarrow \left[\begin{array}{cccc|c} 0 & 1 & 1 & 2 & Q_m \\ 1 & 1 & 2 & 4 & Q_{m+1} \\ 1 & 0 & 0 & 0 & Q_{m-3} \\ 0 & 0 & 0 & 1 & Q_{m-2} \end{array} \right] \rightarrow \\ & \rightarrow \left[\begin{array}{cccc|c} 0 & 1 & 1 & 2 & Q_m \\ 0 & 1 & 0 & 0 & Q_{m-3} + Q_{m-4} \\ 1 & 0 & 0 & 0 & Q_{m-3} \\ 0 & 0 & 0 & 1 & Q_{m-2} \end{array} \right] \rightarrow \left[\begin{array}{cccc|c} 0 & 0 & 1 & 0 & Q_{m-3} + Q_{m-4} + Q_{m-5} \\ 0 & 1 & 0 & 0 & Q_{m-3} + Q_{m-4} \\ 1 & 0 & 0 & 0 & Q_{m-3} \\ 0 & 0 & 0 & 1 & Q_{m-2} \end{array} \right]. \end{aligned}$$

Logo, obtemos

$$\begin{aligned}\alpha_1 &= Q_{m-3}; \\ \alpha_2 &= Q_{m-3} + Q_{m-4}; \\ \alpha_3 &= Q_{m-3} + Q_{m-4} + Q_{m-5}; \\ \alpha_4 &= Q_{m-2},\end{aligned}$$

e o lema está provado. □

Lema 3.3. *Para todo $s \geq 1$ ímpar e $t \geq 7$, vale que*

$$Q_{2^{t-5} \cdot 5s} \equiv 2^{t-3} \pmod{2^{t-2}}.$$

Demonstração. Procederemos por indução em t simultaneamente nas congruências abaixo

$$\begin{aligned}Q_{2^{t-5} \cdot 5s-2} &\equiv 0 \pmod{2^{t-2}}; \\ Q_{2^{t-5} \cdot 5s-1} &\equiv 2^{t-4} \delta \pmod{2^{t-2}}; \\ Q_{2^{t-5} \cdot 5s} &\equiv 2^{t-3} \pmod{2^{t-2}}; \\ Q_{2^{t-5} \cdot 5s+1} &\equiv 2^{t-3} + 1 \pmod{2^{t-2}},\end{aligned} \tag{3.3}$$

onde $s = 2r + 1$, e $\delta = 1$ ou 3 se r é par ou ímpar, respectivamente.

Primeiramente, para a base de indução $t = 7$, temos

$$\begin{aligned}Q_{20s-2} &\equiv 0 \pmod{32}; \\ Q_{20s-1} &\equiv 8\delta \pmod{32}; \\ Q_{20s} &\equiv 16 \pmod{32}; \\ Q_{20s+1} &\equiv 17 \pmod{32},\end{aligned} \tag{3.4}$$

e então, fazemos indução em $s \geq 1$ simultaneamente nas congruências acima. Todas as congruências seguem a mesma ideia, e note que todas são válidas para $s = 1$. Suponha que sejam válidas para s ímpar. Assim, pelo Lema 3.2 para a primeira congruência, temos que

$$\begin{aligned}Q_{20(s+2)-2} &= Q_{20s+38} \\ &= Q_{20s-3}Q_{38} + (Q_{20s-3} + Q_{20s-4})Q_{39} + (Q_{20s-3} + Q_{20s-4} + Q_{20s-5})Q_{40} \\ &\quad + Q_{20s-2}Q_{41} \\ &\equiv 0 + 16(Q_{20s-3} + Q_{20s-4}) + 0 + 0 \pmod{32} \\ &\equiv 0 \pmod{32},\end{aligned}$$

onde usamos que Q_{20s-3}, Q_{20s-4} são ímpares pela equação (1.10) para $k = 4$ e $Q_{38} \equiv Q_{40} \equiv 0 \pmod{32}$.

Para a segunda congruência da base de indução, temos que

$$\begin{aligned}
Q_{20(s+2)-1} &= Q_{(20s+2)+37} \\
&= Q_{20s-1}Q_{37} + (Q_{20s-1} + Q_{20s-2})Q_{38} + (Q_{20s-1} + Q_{20s-2} + Q_{20s-3})Q_{39} \\
&\quad + Q_{20s}Q_{40} \\
&\equiv 8\delta + 0 + 16 + 0 \pmod{32} \\
&\equiv 8(\delta + 2) \pmod{32},
\end{aligned}$$

onde usamos que $Q_{20s-3} \equiv 1 - 8\delta \pmod{32}$ pela recorrência de Q_n .

Agora, suponha que a terceira congruência seja verdade para s ímpar. Logo, pelo Lema 3.2, temos, para $s + 2$, que

$$\begin{aligned}
Q_{20(s+2)} &= Q_{20s+40} = Q_{(20s+3)+37} \\
&= Q_{20s}Q_{37} + (Q_{20s} + Q_{20s-1})Q_{38} + (Q_{20s} + Q_{20s-1} + Q_{20s-2})Q_{39} + Q_{20s+1}Q_{40} \\
&\equiv Q_{20s} + 16(Q_{20s-1} + Q_{20s-2}) \pmod{32} \\
&\equiv 16 \pmod{32}.
\end{aligned}$$

Para a última congruência, temos que

$$\begin{aligned}
Q_{20(s+2)+1} &= Q_{20s+41} = Q_{(20s+3)+38} \\
&= Q_{20s}Q_{38} + (Q_{20s} + Q_{20s-1})Q_{39} + (Q_{20s} + Q_{20s-1} + Q_{20s-2})Q_{40} + Q_{20s+1}Q_{41} \\
&\equiv 0 + 16(Q_{20s} + Q_{20s-1}) + 0 + 17 \pmod{32} \\
&\equiv 17 \pmod{32}.
\end{aligned}$$

Vamos agora prosseguir para a indução em $t \geq 7$. Para tal, vamos, primeiramente, executá-la para $Q_{2^{t-5}.5s-2} \equiv 0 \pmod{2^{t-2}}$. As outras congruências de (3.3) seguirão os mesmos passos. Note que, pela definição de Q_n , temos que $Q_{2^{t-3}.5s-3} \equiv 1 - 2^{t-4}\delta \pmod{2^{t-2}}$ e $Q_{2^{t-3}.5s-4} \equiv 2^{t-3} - 1 \pmod{2^{t-2}}$. Podemos reescrever essas relações e (3.3) da seguinte forma

$$\begin{aligned}
Q_{2^{t-5}.5s-2} &= a_1 2^{t-2}; \\
Q_{2^{t-5}.5s-1} &= a_2 2^{t-2} + 2^{t-4}\delta; \\
Q_{2^{t-5}.5s} &= a_3 2^{t-2} + 2^{t-3}; \\
Q_{2^{t-5}.5s+1} &= a_4 2^{t-2} + 2^{t-3} + 1; \\
Q_{2^{t-5}.5s-3} &= a_5 2^{t-2} + 1 - 2^{t-4}\delta; \\
Q_{2^{t-3}.5s-4} &= a_6 2^{t-2} + 2^{t-3} - 1,
\end{aligned} \tag{3.5}$$

para $a_1, a_2, a_3, a_4, a_5, a_6 \in \mathbb{Z}$.

Portanto, temos que

$$\begin{aligned}
Q_{2^{t-4}5s-2} &= Q_{(2^{t-5}5s+1)+(2^{t-5}5s-3)} \\
&= Q_{2^{t-5}5s-2}Q_{2^{t-5}5s-3} + (Q_{2^{t-5}5s-2} + Q_{2^{t-5}5s-3})Q_{2^{t-5}5s-2} \\
&\quad + (Q_{2^{t-5}5s-2} + Q_{2^{t-5}5s-3} + Q_{2^{t-5}5s-4})Q_{2^{t-5}5s-1} + Q_{2^{t-5}5s}Q_{2^{t-5}5s-1} \\
&= (a_52^{t-2} + 1 - 2^{t-4}\delta)(a_12^{t-2}) \\
&\quad + (a_52^{t-2} + 1 - 2^{t-4}\delta + a_12^{t-2})a_12^{t-2} \\
&\quad + (a_52^{t-2} + 1 - 2^{t-4}\delta + a_12^{t-2} + a_62^{t-2} + 2^{t-3} - 1)(a_22^{t-2} + 2^{t-4}\delta) \\
&\quad + (a_32^{t-2} + 2^{t-3})(a_22^{t-2} + 2^{t-4}\delta) \\
&\equiv 0 \pmod{2^{t-1}},
\end{aligned}$$

onde usamos o fato de que $2t - 4 \geq t - 1$ para $t \geq 7$.

Para a segunda congruência, temos que

$$\begin{aligned}
Q_{2^{t-4}5s-1} &= Q_{(2^{t-5}5s+2)+(2^{t-5}5s-3)} \\
&= Q_{2^{t-5}5s-1}Q_{2^{t-5}5s-3} + (Q_{2^{t-5}5s-1} + Q_{2^{t-5}5s-2})Q_{2^{t-5}5s-2} \\
&\quad + (Q_{2^{t-5}5s-1} + Q_{2^{t-5}5s-2} + Q_{2^{t-5}5s-3})Q_{2^{t-5}5s-1} + Q_{2^{t-5}5s}Q_{2^{t-5}5s} \\
&= (a_22^{t-2} + 2^{t-4})(a_52^{t-2} + 1 - 2^{t-4}\delta) \\
&\quad + (a_22^{t-2} + 2^{t-4} + a_12^{t-2})(a_12^{t-2}) \\
&\quad + (a_22^{t-2} + 2^{t-4} + a_12^{t-2} + a_52^{t-2} + 1 - 2^{t-4})(a_22^{t-2} + 2^{t-4}\delta) \\
&\quad + (a_32^{t-2} + 2^{t-3})(a_32^{t-2} + 2^{t-3}) \\
&\equiv a_22^{t-2} + 2^{t-4}\delta + a_22^{t-2} + 2^{t-4}\delta \pmod{2^{t-1}} \\
&\equiv 2^{t-3}\delta \pmod{2^{t-1}}.
\end{aligned}$$

Para a terceira congruência de (3.3), temos que

$$\begin{aligned}
Q_{2^{t-4}5s} &= Q_{(2^{t-5}5s+2)+(2^{t-5}5s-2)} \\
&= Q_{2^{t-5}5s-1}Q_{2^{t-5}5s-2} + (Q_{2^{t-5}5s-1} + Q_{2^{t-5}5s-2})Q_{2^{t-5}5s-1} \\
&\quad + (Q_{2^{t-5}5s-1} + Q_{2^{t-5}5s-2} + Q_{2^{t-5}5s-3})Q_{2^{t-5}5s} + Q_{2^{t-5}5s}Q_{2^{t-5}5s+1} \\
&= (a_22^{t-2} + 2^{t-4})(a_12^{t-2}) \\
&\quad + (a_22^{t-2} + 2^{t-4} + a_12^{t-2})a_12^{t-2} \\
&\quad + (a_22^{t-2} + 2^{t-4} + a_12^{t-2} + a_52^{t-2} + 1 - 2^{t-4})(a_32^{t-2} + 2^{t-3}) \\
&\quad + (a_32^{t-2} + 2^{t-3})(a_42^{t-2} + 2^{t-3} + 1) \\
&\equiv 2^{t-2} \pmod{2^{t-1}},
\end{aligned}$$

onde usamos o fato de que $2t - 6 \geq t - 1$ para $t \geq 7$.

Vamos, então, partir para a quarta e última congruência de (3.3). Então, temos que

$$\begin{aligned}
Q_{2^{t-4}5s+1} &= Q_{(2^{t-5}5s+3)+(2^{t-5}5s-2)} \\
&= Q_{2^{t-5}5s}Q_{2^{t-5}5s-2} + (Q_{2^{t-5}5s} + Q_{2^{t-5}5s-1})Q_{2^{t-5}5s-1} \\
&\quad + (Q_{2^{t-5}5s} + Q_{2^{t-5}5s-1} + Q_{2^{t-5}5s-2})Q_{2^{t-5}5s} + Q_{2^{t-5}5s+1}Q_{2^{t-5}5s+1} \\
&= (a_32^{t-2} + 2^{t-3})(a_12^{t-2}) \\
&\quad + (a_32^{t-2} + 2^{t-3} + a_22^{t-2} + 2^{t-4}\delta)(a_22^{t-2} + 2^{t-4}\delta) \\
&\quad + (a_32^{t-2} + 2^{t-3} + a_22^{t-2} + 2^{t-4}\delta + a_12^{t-2})(a_32^{t-2} + 2^{t-3}) \\
&\quad + (a_42^{t-2} + 2^{t-3} + 1)(a_42^{t-2} + 2^{t-3} + 1) \\
&\equiv a_42^{t-2} + 2^{t-3} + 1a_42^{t-2} + 2^{t-3} \pmod{2^{t-1}} \\
&\equiv 2^{t-2} + 1 \pmod{2^{t-1}},
\end{aligned}$$

o que conclui nossa indução e o lema está provado. □

Ainda temos mais um lema a provar antes de seguirmos em frente.

Lema 3.4. *Para todo $s \geq 1$ ímpar e $t \geq 8$, vale que*

$$Q_{2^{t-3}5s-2} \equiv 2^{t+2} \pmod{2^{t+3}}.$$

Demonstração. O procedimento para a demonstração é análogo àquele do lema anterior, mas agora iremos executar indução simultaneamente nas seguintes congruências

$$\begin{aligned}
Q_{2^{t-3}5s-2} &\equiv 2^{t+2} \pmod{2^{t+3}}; \\
Q_{2^{t-3}5s-1} &\equiv 2^{t-2}5s \pmod{2^{t+3}}; \\
Q_{2^{t-3}5s} &\equiv 2^{t-1}13s \pmod{2^{t+3}}; \\
Q_{2^{t-3}5s+1} &\equiv 2^{t-1}9s + 1 \pmod{2^{t+3}}.
\end{aligned} \tag{3.6}$$

Usando a definição de Q_n , temos que $Q_{2^{t-3}5s-3} \equiv 1 + 2^{t+2} - 2^{t-2} \cdot 13s \pmod{2^{t+3}}$ e $Q_{2^{t-3}5s-4} \equiv 2^{t-2} \cdot 34s - 1 \pmod{2^{t+3}}$. Reescrevendo as relações acima e (3.6) da mesma forma que fizemos no lema anterior, temos, para $b_1, \dots, b_6 \in \mathbb{Z}$, que

$$\begin{aligned}
Q_{2^{t-5}5s-2} &= b_12^{t+3} + 2^{t+2}; \\
Q_{2^{t-5}5s-1} &= b_22^{t+3} + 2^{t-2} \cdot 5s; \\
Q_{2^{t-5}5s} &= b_32^{t+3} + 2^{t-1} \cdot 13s; \\
Q_{2^{t-5}5s+1} &= b_42^{t+3} + 2^{t-1} \cdot 9s + 1; \\
Q_{2^{t-5}5s-3} &= b_52^{t+3} + 1 + 2^{t+2} - 2^{t-2} \cdot 13s; \\
Q_{2^{t-5}5s-4} &= b_62^{t+3} + 2^{t-2} \cdot 34s - 1;
\end{aligned} \tag{3.7}$$

Vamos primeiramente fazer a base de indução $s = 1$ e executar a indução em $t \geq 7$. Como no lema anterior, o procedimento segue os mesmos passos para as quatro congruências acima. Primeiramente, vamos executar a indução no caso $s = 1$ para $Q_{2^{t-3}5s-2} \equiv 2^{t+2} \pmod{2^{t+3}}$.

Para $t = 7$, temos que $Q_{2^{t-3}5-2} = Q_{2^{4}5-2} = Q_{78} \equiv 512 \pmod{1024}$. Vamos então supor que o lema seja verdade para t . Logo, temos que

$$\begin{aligned}
Q_{2^{t-2}5-2} &= Q_{(2^{t-3}5+1)+(2^{t-3}5-3)} \\
&= Q_{2^{t-3}5-2} \cdot Q_{2^{t-3}5-3} + (Q_{2^{t-3}5-2} + Q_{2^{t-3}5-3})Q_{2^{t-3}5-2} \\
&\quad + (Q_{2^{t-3}5-2} + Q_{2^{t-3}5-3} + Q_{2^{t-3}5-4})Q_{2^{t-3}5-1} + Q_{2^{t-3}5-1}Q_{2^{t-3}5} \\
&= (b_1 2^{t+3} + 2^{t+2})(b_5 2^{t+3} + 1 + 2^{t+2} - 2^{t-2} \cdot 13) \\
&\quad + (b_1 2^{t+3} + 2^{t+2} + b_5 2^{t+3} + 1 + 2^{t+2} - 2^{t-2} \cdot 13)(b_1 2^{t+3} + 2^{t+2}) \\
&\quad + (b_1 2^{t+3} + 2^{t+2} + b_5 2^{t+3} + 1 + 2^{t+2} - 2^{t-2} \cdot 13 + b_6 2^{t+3} + 2^{t-2} \cdot 33) \\
&\quad \times (b_2 2^{t+3} + 2^{t-2} \cdot 5) \\
&\quad + (b_2 2^{t+3} + 2^{t-2} \cdot 5)(b_3 2^{t+3} + 2^{t-1} \cdot 13) \\
&\equiv 2^{t+2} + 2^{t+2} \pmod{2^{t+4}} \\
&\equiv 2^{t+3} \pmod{2^{t+4}},
\end{aligned}$$

o que conclui a indução em t e por consequência a base da indução em s . Sigamos assim à segunda parte da indução, para $s \geq 1$. Nesse caso, vamos supor então que $Q_{2^{t-3}5s-2} \equiv 2^{t+2} \pmod{2^{t+3}}$. Dessa forma, temos que

$$\begin{aligned}
Q_{2^{t-3}5(s+1)-2} &= Q_{2^{t-3}5+1+2^{t-3}5s-3} \\
&= Q_{2^{t-3}5-2} \cdot Q_{2^{t-3}5s-3} + (Q_{2^{t-3}5-2} + Q_{2^{t-3}5-3})Q_{2^{t-3}5s-2} \\
&\quad + (Q_{2^{t-3}5-2} + Q_{2^{t-3}5-3} + Q_{2^{t-3}5-4})Q_{2^{t-3}5s-1} + Q_{2^{t-3}5-1}Q_{2^{t-3}5s} \\
&= (b_1 2^{t+3} + 2^{t+2})(b_5 2^{t+3} + 1 + 2^{t+2} - 2^{t-2} \cdot 13s) \\
&\quad + (b_1 2^{t+3} + 2^{t+2} + b_5 2^{t+3} + 1 + 2^{t+2} - 2^{t-2} \cdot 13)(b_1 2^{t+3} + 2^{t+2}) \\
&\quad + (b_1 2^{t+3} + 2^{t+2} + b_5 2^{t+3} + 1 + 2^{t+2} - 2^{t-2} \cdot 13 + b_6 2^{t+3} + 2^{t-2} \cdot 33) \\
&\quad \times (b_2 2^{t+3} + 2^{t-2} \cdot 5s) \\
&\quad + (b_2 2^{t+3} + 2^{t-2} \cdot 5)(b_3 2^{t+3} + 2^{t-1} \cdot 13s) \\
&\equiv 2^{t+2} + 2^{t+2} \pmod{2^{t+4}} \\
&\equiv 2^{t+3} \pmod{2^{t+4}},
\end{aligned}$$

o que conclui a indução em s para essa primeira congruência.

Partiremos agora para a congruência $Q_{2^{t-3}5s-1} \equiv 2^{t-2}5s \pmod{2^{t+3}}$. Então, vamos mostrar aqui que $Q_{2^{t-3}5s-1} \equiv 2^{t-2} \cdot 5s \pmod{2^{t+3}}$. Para a base de indução $s = 1$, vamos fazer indução sobre $t \geq 7$ para mostrar que $Q_{2^{t-3}5-1} \equiv 2^{t-2} \cdot 5 \pmod{2^{t+3}}$. Para $t = 7$, é facilmente verificável. Suponhamos então que a congruência seja válida para t , e assim

$$\begin{aligned}
Q_{2^{t-2}5-1} &= Q_{(2^{t-3}5+1)+(2^{t-3}5-2)} \\
&= Q_{2^{t-3}5-2} \cdot Q_{2^{t-3}5-2} + (Q_{2^{t-3}5-2} + Q_{2^{t-3}5-3})Q_{2^{t-3}5-1} \\
&\quad + (Q_{2^{t-3}5-2} + Q_{2^{t-3}5-3} + Q_{2^{t-3}5-4})Q_{2^{t-3}5} + Q_{2^{t-3}5-1}Q_{2^{t-3}5+1}
\end{aligned}$$

$$\begin{aligned}
&= (b_1 2^{t+3} + 2^{t+2})(b_1 2^{t+3} + 2^{t+2}) \\
&\quad + (b_1 2^{t+3} + 2^{t+2} + b_5 2^{t+3} + 1 + 2^{t+2} - 2^{t-2} \cdot 13)(b_2 2^{t+3} + 2^{t-2} \cdot 5) \\
&\quad + (b_1 2^{t+3} + 2^{t+2} + b_5 2^{t+3} + 1 + 2^{t+2} - 2^{t-2} \cdot 13 + b_6 2^{t+3} + 2^{t-2} \cdot 33) \\
&\quad \times (b_3 2^{t+3} + 2^{t-1} \cdot 13) \\
&\quad + (b_2 2^{t+3} + 2^{t-2} \cdot 5)(b_4 2^{t+3} + 2^{t-1} \cdot 9 + 1) \\
&\equiv b_2 2^{t+3} + 2^{t+2} \cdot 5 + b_2 2^{t+3} + 2^{t-2} \cdot 5 \pmod{2^{t+4}} \\
&\equiv 2^{t-1} \cdot 5 \pmod{2^{t+4}},
\end{aligned}$$

concluindo a base de indução. Suponha então que essa relação vale para s , com isso, temos que

$$\begin{aligned}
Q_{2^{t-3} \cdot 5(s+1)-1} &= Q_{(2^{t-3} \cdot 5s-2)+(2^{t-3} \cdot 5+1)} \\
&= Q_{2^{t-3} \cdot 5-2} Q_{2^{t-3} \cdot 5s-2} + (Q_{2^{t-3} \cdot 5-2} + Q_{2^{t-3} \cdot 5-3}) Q_{2^{t-3} \cdot 5s-1} \\
&\quad + (Q_{2^{t-3} \cdot 5-2} + Q_{2^{t-3} \cdot 5-3} + Q_{2^{t-3} \cdot 5-4}) Q_{2^{t-3} \cdot 5s} + Q_{2^{t-3} \cdot 5-1} Q_{2^{t-3} \cdot 5s+1} \\
&= (b_1 2^{t+3} + 2^{t+2})(b_1 2^{t+3} + 2^{t+2}) \\
&\quad + (b_1 2^{t+3} + 2^{t+2} + b_5 2^{t+3} + 1 + 2^{t+2} - 2^{t-2} \cdot 13)(b_2 2^{t+3} + 2^{t-2} \cdot 5s) \\
&\quad + (b_1 2^{t+3} + 2^{t+2} + b_5 2^{t+3} + 1 + 2^{t+2} - 2^{t-2} \cdot 13 + b_6 2^{t+3} + 2^{t-2} \cdot 33) \\
&\quad \times (b_3 2^{t+3} + 2^{t-1} \cdot 13s) \\
&\quad + (b_2 2^{t+3} + 2^{t-2} \cdot 5)(b_4 2^{t+3} + 2^{t-1} \cdot 9s + 1) \\
&\equiv 2^{t-2} \cdot 5s + 2^{t-2} \cdot 5 \pmod{2^{t+3}} \\
&\equiv 2^{t-2} \cdot 5(s+1) \pmod{2^{t+3}}.
\end{aligned}$$

E a indução para a segunda congruência está terminada. Para a terceira congruência $Q_{2^{t-3} \cdot 5s} \equiv 2^{t-1} \cdot 13s \pmod{2^{t+3}}$, vamos proceder da mesma forma. Para $s = 1$, vamos provar por indução que $Q_{2^{t-3} \cdot 5} \equiv 2^{t-1} \cdot 13 \pmod{2^{t+3}}$. Para $t = 7$, é simples computar que $Q_{80} \equiv 832 \pmod{1024}$. Supondo então que a congruência para $s = 1$ seja válida para t , temos que

$$\begin{aligned}
Q_{2^{t-2} \cdot 5} &= Q_{(2^{t-3} \cdot 5+2)+(2^{t-3} \cdot 5-2)} \\
&= Q_{2^{t-3} \cdot 5-1} \cdot Q_{2^{t-3} \cdot 5-2} + (Q_{2^{t-3} \cdot 5-1} + Q_{2^{t-3} \cdot 5-2}) Q_{2^{t-3} \cdot 5-1} \\
&\quad + (Q_{2^{t-3} \cdot 5-1} + Q_{2^{t-3} \cdot 5-2} + Q_{2^{t-3} \cdot 5-3}) Q_{2^{t-3} \cdot 5} + Q_{2^{t-3} \cdot 5} Q_{2^{t-3} \cdot 5+1} \\
&= (b_2 2^{t+3} + 2^{t-2} \cdot 5)(b_1 2^{t+3} + 2^{t+2}) \\
&\quad + (b_2 2^{t+3} + 2^{t-2} \cdot 5 + b_1 2^{t+3} + 2^{t+2})(b_2 2^{t+3} + 2^{t-2} \cdot 5) \\
&\quad + (b_2 2^{t+3} + 2^{t-2} \cdot 5 + b_1 2^{t+3} + 2^{t+2} + b_5 2^{t+3} + 1 + 2^{t+2} - 2^{t-2} \cdot 13) \\
&\quad \times (b_3 2^{t+3} + 2^{t-1} \cdot 13) \\
&\quad + (b_3 2^{t+3} + 2^{t-1} \cdot 13)(b_4 2^{t+3} + 2^{t-1} \cdot 9 + 1) \\
&\equiv 0 + 0 + b_3 2^{t+3} + 2^{t-1} \cdot 13 + b_3 2^{t+3} + 2^{t-1} \cdot 13 \pmod{2^{t+4}} \\
&\equiv 2^t \cdot 13 \pmod{2^{t+4}}.
\end{aligned}$$

Com a base de indução $s = 1$ completa, suponha que $Q_{2^{t-3}5s} \equiv 2^{t-1}13s \pmod{2^{t+3}}$ seja verdade. Assim,

$$\begin{aligned}
Q_{2^{t-2} \cdot 5(s+1)} &= Q_{(2^{t-3} \cdot 5+2)+(2^{t-3} \cdot 5s-2)} \\
&= Q_{2^{t-3} \cdot 5-1} \cdot Q_{2^{t-3} \cdot 5s-2} + (Q_{2^{t-3} \cdot 5-1} + Q_{2^{t-3} \cdot 5-2})Q_{2^{t-3} \cdot 5s-1} \\
&\quad + (Q_{2^{t-3} \cdot 5-1} + Q_{2^{t-3} \cdot 5-2} + Q_{2^{t-3} \cdot 5-3})Q_{2^{t-3} \cdot 5s} + Q_{2^{t-3} \cdot 5}Q_{2^{t-3} \cdot 5s+1} \\
&= (b_2 2^{t+3} + 2^{t-2} \cdot 5)(b_1 2^{t+3} + 2^{t+2}) \\
&\quad + (b_2 2^{t+3} + 2^{t-2} \cdot 5 + b_1 2^{t+3} + 2^{t+2})(b_2 2^{t+3} + 2^{t-2} \cdot 5s) \\
&\quad + (b_2 2^{t+3} + 2^{t-2} \cdot 5 + b_1 2^{t+3} + 2^{t+2} + b_5 2^{t+3} + 1 + 2^{t+2} - 2^{t-2} \cdot 13) \\
&\quad \times (b_3 2^{t+3} + 2^{t-1} \cdot 13s) \\
&\quad + (b_3 2^{t+3} + 2^{t-1} \cdot 13)(b_4 2^{t+3} + 2^{t-1} \cdot 9s + 1) \\
&\equiv 0 + 2^{t-1} \cdot 13s + 0 + 2^{t-1} \cdot 13 \pmod{2^{t+3}} \\
&\equiv 2^{t-1} \cdot 13(s+1) \pmod{2^{t+3}},
\end{aligned}$$

e a indução da terceira congruência de (3.6) está completa.

Partiremos agora para a indução da quarta e última congruência. Mais uma vez, colocando $s = 1$ para realizar indução sobre $t \geq 7$. Como antes, o caso $t = 7$ é facilmente computável, então vamos supor que $Q_{2^{t-3}5+1} \equiv 2^{t-1}9 + 1 \pmod{2^{t+3}}$. Portanto, temos que

$$\begin{aligned}
Q_{2^{t-2} \cdot 5+1} &= Q_{(2^{t-3} \cdot 5+3)+(2^{t-3} \cdot 5-2)} \\
&= Q_{2^{t-3} \cdot 5} \cdot Q_{2^{t-3} \cdot 5-2} + (Q_{2^{t-3} \cdot 5-1} + Q_{2^{t-3} \cdot 5})Q_{2^{t-3} \cdot 5-1} \\
&\quad + (Q_{2^{t-3} \cdot 5-1} + Q_{2^{t-3} \cdot 5} + Q_{2^{t-3} \cdot 5-2})Q_{2^{t-3} \cdot 5} + Q_{2^{t-3} \cdot 5+1}Q_{2^{t-3} \cdot 5+1} \\
&= (b_3 2^{t+3} + 2^{t-1} \cdot 13)(b_1 2^{t+3} + 2^{t+2}) \\
&\quad + (b_3 2^{t+3} + 2^{t-1} \cdot 13 + b_2 2^{t+3} + 2^{t-2} \cdot 5)(b_2 2^{t+3} + 2^{t-2} \cdot 5) \\
&\quad + (b_3 2^{t+3} + 2^{t-1} \cdot 13 + b_2 2^{t+3} + 2^{t-2} \cdot 5 + b_1 2^{t+3} + 2^{t+2}) \\
&\quad \times (b_3 2^{t+3} + 2^{t-1} \cdot 13) \\
&\quad + (b_4 2^{t+3} + 2^{t-1} \cdot 9 + 1)(b_4 2^{t+3} + 2^{t-1} \cdot 9 + 1) \\
&\equiv b_4 2^{t+3} + 2^{t-1} \cdot 9 + b_4 2^{t+3} + 2^{t-1} \cdot 9 + 1 \pmod{2^{t+4}} \\
&\equiv 2^t \cdot 9 + 1 \pmod{2^{t+4}}.
\end{aligned}$$

Com a base da indução terminada, vamos supor que $Q_{2^{t-3}5s+1} \equiv 2^{t-1}9s+1 \pmod{2^{t+3}}$. Logo, temos que

$$\begin{aligned}
Q_{2^{t-2} \cdot 5(s+1)+1} &= Q_{(2^{t-3} \cdot 5+3)+(2^{t-3} \cdot 5s-2)} \\
&= Q_{2^{t-3} \cdot 5} \cdot Q_{2^{t-3} \cdot 5s-2} + (Q_{2^{t-3} \cdot 5-1} + Q_{2^{t-3} \cdot 5})Q_{2^{t-3} \cdot 5s-1} \\
&\quad + (Q_{2^{t-3} \cdot 5-1} + Q_{2^{t-3} \cdot 5} + Q_{2^{t-3} \cdot 5-2})Q_{2^{t-3} \cdot 5s} + Q_{2^{t-3} \cdot 5+1}Q_{2^{t-3} \cdot 5s+1} \\
&= (b_3 2^{t+3} + 2^{t-1} \cdot 13)(b_1 2^{t+3} + 2^{t+2}) \\
&\quad + (b_3 2^{t+3} + 2^{t-1} \cdot 13 + b_2 2^{t+3} + 2^{t-2} \cdot 5)(b_2 2^{t+3} + 2^{t-2} \cdot 5s) \\
&\quad + (b_3 2^{t+3} + 2^{t-1} \cdot 13 + b_2 2^{t+3} + 2^{t-2} \cdot 5 + b_1 2^{t+3} + 2^{t+2}) \\
&\quad \times (b_3 2^{t+3} + 2^{t-1} \cdot 13s) \\
&\quad + (b_4 2^{t+3} + 2^{t-1} \cdot 9 + 1)(b_4 2^{t+3} + 2^{t-1} \cdot 9s + 1)
\end{aligned}$$

$$\begin{aligned}
&\equiv 0 + 0 + 0 + 2^{t-1} \cdot 9 + 2^{t-1} \cdot 9s + 1 \pmod{2^{t+4}} \\
&\equiv 2^{t-1} \cdot 9(s+1) + 1 \pmod{2^{t+4}}.
\end{aligned}$$

O que conclui a indução da quarta congruência de (3.6) e a demonstração do lema. \square

3.2 A valorização 2-ádica de Q_n

Antes de direcionar nossa atenção à solução da equação (3.1), ainda precisamos calcular a valorização 2-ádica de Q_n . Essa nos fornecerá a ferramenta fundamental para solucionarmos a equação em questão. Em outras palavras, vamos, nesta seção, demonstrar o seguinte resultado:

Teorema 3.5. *Para $n \geq 1, n \not\equiv 75 \pmod{80}$, temos que*

$$\nu_2(Q_n) = \begin{cases} 17, & \text{se } n = 78 \\ 0, & \text{se } n \equiv 1, 2 \pmod{5}; \\ 1, & \text{se } n \equiv 3 \pmod{10}; \\ 2, & \text{se } n \equiv 4, 9 \pmod{20}; \\ 3, & \text{se } n \equiv 5, 8 \pmod{20}; \\ \nu_2(n) + 2, & \text{se } n \equiv 0 \pmod{20}; \\ \nu_2(n+10) + 2, & \text{se } n \equiv 10 \pmod{20}; \\ \nu_2(n+6) + 1, & \text{se } n \equiv 14 \pmod{20}; \\ \nu_2(n+1) + 1, & \text{se } n \equiv 19 \pmod{20}; \\ \nu_2((n+5)^2) + 1, & \text{se } n \equiv 15, 35, 55 \pmod{80}; \\ \nu_2((n+2)^2) + 1, & \text{se } n \equiv 18, 38, 58 \pmod{80}; \\ \nu_2((n+2)(n-78)) + 1, & \text{se } n \equiv 78 \pmod{80}, n > 78. \end{cases}$$

Demonstração. Vamos dividir essa demonstração nos 11 casos apresentados acima (note que o caso $n = 78$ é trivial).

Caso 1: $n \equiv 1, 2 \pmod{5}$.

Note que, pela equação (1.10) para $k = 4$, temos que $Q_n - Q_{n-5}$ é par. Portanto,

$$Q_n \text{ é ímpar} \iff Q_{n-5} \text{ é ímpar},$$

logo, como $Q_1 = Q_2 = 1$, temos que

$$\nu_2(Q_n) = 0, \text{ se } n \equiv 1, 2 \pmod{5},$$

e esse caso está provado.

Caso 2: $n \equiv 3 \pmod{10}$.

Observe que, para provar esse caso, é suficiente provar que

$$Q_n \equiv 2 \pmod{4}, \text{ se } n \equiv 3 \pmod{10}.$$

Sendo assim, vamos proceder por indução na congruência acima, onde $n = 10l + 3$, $l \geq 0$.

Temos que $l = 0 \Rightarrow Q_3 = 2 \equiv 2 \pmod{4}$. Suponha agora que a congruência seja verdade para l . Assim, pelo Lema 3.2, temos que

$$\begin{aligned} Q_{10(l+1)+3} &= Q_{(10l+5)+8} \\ &= Q_8 Q_{10l+2} + (Q_{20l+2} + Q_{20l+1})Q_9 + (Q_{10l+2} + Q_{10l+1} + Q_{10l})Q_{10} + Q_{11}Q_{10l+3} \\ &= 56Q_{10l+2} + 108(Q_{10l+2} + Q_{10l+1}) + 208(Q_{10l+2} + Q_{10l+1} + Q_{10l}) + 401Q_{10l+3} \\ &\equiv 0 + 0 + 0 + 401 \cdot 2 \pmod{4} \\ &\equiv 2 \pmod{4}, \end{aligned}$$

e esse caso está provado.

Caso 3: $n \equiv 4, 9 \pmod{20}$.

Para esse caso a congruência correspondente será

$$Q_n \equiv 4 \pmod{8}, \text{ se } n \equiv 4, 9 \pmod{20}.$$

Vamos fazer, primeiramente, o caso $n \equiv 4 \pmod{20}$, o caso $n \equiv 9 \pmod{20}$ seguirá praticamente os mesmos cálculos. Assim, temos que $n = 20l + 4$ e já temos o que precisamos para fazer a indução sobre $l \geq 0$. Para $l = 0$, $Q_4 = 4 \equiv 4 \pmod{8}$. Suponha agora que a congruência seja válida para l . Logo, temos que

$$\begin{aligned} Q_{20(l+1)+4} &= Q_{(20l+6)+18} \\ &= Q_{18}Q_{20l+3} + (Q_{20l+3} + Q_{20l+2})Q_{19} + (Q_{20l+3} + Q_{20l+2} + Q_{20l+1})Q_{20} \\ &\quad + Q_{21}Q_{20l+4} \\ &= 39648Q_{20l+3} + 76424(Q_{20l+3} + Q_{20l+2}) + 147312(Q_{20l+3} + Q_{20l+2} + Q_{20l+1}) \\ &\quad + 283953Q_{20l+4} \\ &\equiv 0 + 0 + 0 + 283953 \cdot 4 \pmod{8} \\ &\equiv 4 \pmod{8}, \end{aligned}$$

o que finaliza a primeira indução.

Agora, vamos fazer a indução para o caso $n \equiv 9 \pmod{20}$. Assim, temos que $n = 20l + 9$ e já temos o que precisamos para fazer a indução sobre $l \geq 0$. Para $l = 0$, $Q_9 = 108 \equiv 4 \pmod{8}$. Suponha agora que a congruência seja válida para l . Logo, temos

que

$$\begin{aligned}
Q_{20(l+1)+9} &= Q_{(20l+11)+18} \\
&= Q_{18}Q_{20l+8} + (Q_{20l+8} + Q_{20l+7})Q_{19} + (Q_{20l+8} + Q_{20l+7} + Q_{20l+6})Q_{20} \\
&\quad + Q_{21}Q_{20l+9} \\
&= 39648Q_{20l+8} + 76424(Q_{20l+8} + Q_{20l+7}) + 147312(Q_{20l+8} + Q_{20l+7} + Q_{20l+6}) \\
&\quad + 283953Q_{20l+9} \\
&\equiv 0 + 0 + 0 + 283953 \cdot 4 \pmod{8} \\
&\equiv 4 \pmod{8},
\end{aligned}$$

e esse caso também está provado.

Caso 4: $n \equiv 5, 8 \pmod{20}$.

Para esse caso, vamos provar a congruência correspondente,

$$Q_n \equiv 8 \pmod{16}, \text{ se } n \equiv 5, 8 \pmod{20}.$$

Vamos, primeiramente, fazer o caso $n \equiv 5 \pmod{20}$, mais uma vez, o caso $n \equiv 8 \pmod{20}$ seguirá praticamente os mesmos cálculos.

Assim, temos que $n = 20l + 5$. Para $l = 0$, $Q_5 = 8 \equiv 8 \pmod{16}$. Suponha agora que a congruência seja válida para l . Logo, temos que

$$\begin{aligned}
Q_{20(l+1)+5} &= Q_{(20l+7)+18} \\
&= Q_{18}Q_{20l+4} + (Q_{20l+4} + Q_{20l+3})Q_{19} + (Q_{20l+4} + Q_{20l+3} + Q_{20l+2})Q_{20} \\
&\quad + Q_{21}Q_{20l+5} \\
&= 39648Q_{20l+4} + 76424(Q_{20l+4} + Q_{20l+3}) + 147312(Q_{20l+4} + Q_{20l+3} + Q_{20l+2}) \\
&\quad + 283953Q_{20l+5} \\
&\equiv 0 + 0 + 0 + 283953 \cdot 8 \pmod{16} \\
&\equiv 8 \pmod{16},
\end{aligned}$$

onde usamos que $Q_{20l+7} + Q_{20l+6}$ é par, pois, pelo Caso 1, é a soma de dois ímpares. O que finaliza a indução.

Agora, temos que $n = 20l + 8$. Para $l = 0$, $Q_8 = 56 \equiv 8 \pmod{16}$. Suponha agora que a congruência seja válida para l . Logo, temos que

$$\begin{aligned}
Q_{20(l+1)+8} &= Q_{(20l+10)+18} \\
&= Q_{18}Q_{20l+7} + (Q_{20l+7} + Q_{20l+6})Q_{19} + (Q_{20l+7} + Q_{20l+6} + Q_{20l+5})Q_{20} \\
&\quad + Q_{21}Q_{20l+8} \\
&= 39648Q_{20l+7} + 76424(Q_{20l+7} + Q_{20l+6}) + 147312(Q_{20l+7} + Q_{20l+6} + Q_{20l+5}) \\
&\quad + 283953Q_{20l+8} \\
&\equiv 0 + 0 + 0 + 283953 \cdot 8 \pmod{16} \\
&\equiv 8 \pmod{16},
\end{aligned}$$

onde usamos mais uma vez que $Q_{20l+7} + Q_{20l+6}$ é par devido ao Caso 1. E então esse caso também está provado.

Caso 5: $n \equiv 0 \pmod{20}$.

Note que, nesse caso, temos que $n = 2^{t-5} \cdot 5s$, com $s \geq 1$ ímpar e $t \geq 7$. Portanto, pelo Lema 3.3, temos que $\nu_2(Q_n) = t - 3$. Por outro lado,

$$\nu_2(n) + 2 = \nu_2(2^{t-5}5s) + 2 = t - 5 + 2 = t - 3 = \nu_2(Q_n).$$

Caso 6: $n \equiv 10 \pmod{20}$.

Agora, usamos as congruências apresentadas na demonstração do Lema 3.3 juntamente com a definição da sequência de Tetranacci para mostrar que $Q_{2^{t-5}5s-10} \equiv 2^{t-3}(\delta - 2) \pmod{2^{t-2}}$. Então, como nesse caso $n = 2^{t-5} \cdot 5s - 10$, com $s \geq 1$ ímpar e $t \geq 7$,

$$\nu_2(n + 10) + 2 = \nu_2(2^{t-5}5s) + 2 = t - 3 = \nu_2(Q_n).$$

Caso 7: $n \equiv 14 \pmod{20}$.

Procedendo como no Caso 6, ou seja, usando as congruências apresentadas na demonstração do Lema 3.3, temos que $Q_{2^{t-5}5s-6} \equiv 2^{t-4}\delta \pmod{2^{t-2}}$. Portanto, como nesse caso $n = 2^{t-5} \cdot 5s - 6$, com $s \geq 1$ ímpar e $t \geq 7$,

$$\nu_2(n + 6) + 1 = \nu_2(2^{t-5}5s) + 1 = t - 4 = \nu_2(Q_n).$$

Caso 8: $n \equiv 19 \pmod{20}$.

Aqui, temos que $n = 2^{t-5} \cdot 5s - 1$, com $s \geq 1$ ímpar e $t \geq 7$. Segue diretamente das congruências apresentadas na demonstração do Lema 3.3 que $Q_{2^{t-5}5s-1} \equiv 2^{t-4}\delta \pmod{2^{t-2}}$. Logo,

$$\nu_2(n + 1) + 1 = \nu_2(2^{t-5}5s) + 1 = t - 4 = \nu_2(Q_n).$$

Caso 9: $n \equiv 15, 35, 55 \pmod{80}$.

Note que, se $n \equiv 15 \pmod{80}$, então $n = 80l + 15$. Assim, temos que

$$\nu_2((n + 5)^2) + 1 = 2\nu_2(80l + 20) + 1 = 2\nu_2(20(4l + 1)) + 1 = 5.$$

Assim, queremos provar que $\nu_2(Q_n) = 5$ quando $n = 80l + 15$. Para tal, vamos executar uma indução sobre $l \geq 0$ análoga às feitas nos Casos 1 e 2. Assim, nossa congruência correspondente será

$$Q_n \equiv 2^5 \pmod{2^6} \text{ se } n \equiv 15 \pmod{80}.$$

Para a base de indução $l = 0$, temos que

$$n = 15 \implies Q_n = Q_{15} = 5536 \equiv 32 \pmod{64}.$$

Suponha então que a congruência seja válida para l e, portanto, temos que

$$\begin{aligned} Q_{80(l+1)+15} &= Q_{(80l+17)+78} \\ &= Q_{78}Q_{80l+14} + (Q_{80l+14} + Q_{20l+13})Q_{79} \\ &\quad + (Q_{80l+14} + Q_{80l+13} + Q_{80l+12})Q_{80} + Q_{81}Q_{80l+15} \\ &\equiv 0 + 0 + 0 + 2^5 \pmod{2^6} \\ &\equiv 2^5 \pmod{2^6}, \end{aligned}$$

onde usamos que $Q_{78} \equiv Q_{80} \equiv 0 \pmod{64}$, $Q_{81} \equiv 1 \pmod{64}$, $Q_{79} \equiv 32 \pmod{64}$ e $(Q_{80l+14} + Q_{20l+13})$ é par pelos Casos 2 e 7. O que conclui a indução.

O caso $n \equiv 55 \pmod{80}$ segue exatamente os mesmos cálculos, pois

$$\nu_2((n+5)^2) + 1 = 2\nu_2(80l+60) + 1 = 2\nu_2(20(4l+3)) + 1 = 5.$$

Assim, queremos provar que $\nu_2(Q_n) = 5$ quando $n = 80l + 55$. Para tal, vamos executar uma indução sobre $l \geq 0$ também análoga às feitas nos Casos 1 e 2. Assim, nossa congruência correspondente será

$$Q_n \equiv 2^5 \pmod{2^6} \text{ se } n \equiv 55 \pmod{80}.$$

Para a base de indução $l = 0$, é fácil computar que $Q_n = Q_{55} \equiv 32 \pmod{64}$. Suponha então que a congruência seja válida para l e, portanto, temos que

$$\begin{aligned} Q_{80(l+1)+55} &= Q_{(80l+57)+78} \\ &= Q_{78}Q_{80l+54} + (Q_{80l+54} + Q_{20l+53})Q_{79} \\ &\quad + (Q_{80l+54} + Q_{80l+53} + Q_{80l+52})Q_{80} + Q_{81}Q_{80l+55} \\ &\equiv 0 + 0 + 0 + 2^5 \pmod{2^6} \\ &\equiv 2^5 \pmod{2^6}, \end{aligned}$$

onde usamos mais uma vez que $Q_{78} \equiv Q_{80} \equiv 0 \pmod{64}$, $Q_{81} \equiv 1 \pmod{64}$, $Q_{79} \equiv 32 \pmod{64}$ e que $(Q_{80l+54} + Q_{20l+53})$ é par pelos Casos 2 e 7. E da mesma forma, concluímos a indução.

Para o caso $n \equiv 35 \pmod{80}$, temos que

$$\nu_2((n+5)^2) + 1 = 2\nu_2(80l+40) + 1 = 2\nu_2(40(2l+1)) + 1 = 7.$$

Assim, queremos provar, nesse caso, que $\nu_2(Q_n) = 7$. Que traz a congruência correspondente

$$Q_n \equiv 2^7 \pmod{2^8} \text{ se } n \equiv 35 \pmod{80}, \quad (3.8)$$

ou seja, $n = 80l + 35$. Para $l = 0$, segue que $Q_{35} = 2775641472 \equiv 128 \pmod{256}$.

Agora, pela equação (1.10) para $k = 4$, temos que $Q_{80l+38} = 2Q_{80l+42} - Q_{80l+43}$, e pela definição de Q_n , temos que $Q_{80l+37} + Q_{80l+36} = Q_{80l+38} - Q_{80l+35} - Q_{80l+34}$ e $Q_{76} + Q_{77} = Q_{78} - Q_{75} - Q_{74}$. Além disso, note que $Q_{78} \equiv Q_{75} \equiv 0 \pmod{2^8}$, $Q_{74} = 2^6 s_1$, como s_1 ímpar, e que, pelo Caso 7, $Q_{74}Q_{80l+34} \equiv 0 \pmod{2^8}$. Finalmente, observe que, pelo Caso 2, $Q_{80l+43} = 2s_2$, que $Q_{80l+42} = s_3$, com s_2, s_3 ímpares, e que Q_{76} é ímpar, logo, pela hipótese da indução, $Q_{76}Q_{80l+35} \equiv 2^7 \pmod{2^8}$.

Agora, suponha que a congruência (3.8) seja verdade para l . Assim, temos que

$$\begin{aligned} Q_{80(l+1)+35} &= Q_{(80l+40)+75} \\ &= Q_{75}Q_{80l+37} + (Q_{80l+37} + Q_{20l+36})Q_{76} \\ &\quad + (Q_{80l+37} + Q_{80l+36} + Q_{80l+35})Q_{77} + Q_{78}Q_{80l+38} \\ &= Q_{75}Q_{80l+37} + (Q_{80l+38} - Q_{20l+35} - Q_{80l+34})Q_{76} \\ &\quad + (Q_{80l+38} - Q_{80l+34})Q_{77} + Q_{78}Q_{80l+38} \\ &= Q_{75}Q_{80l+37} + (Q_{80l+38} - Q_{80l+34})(Q_{77} + Q_{76}) - Q_{80l+35}Q_{76} + Q_{78}Q_{80l+38} \\ &\equiv 0 + (Q_{80l+38} - Q_{80l+34})(Q_{78} - Q_{75} - Q_{74}) + 2^7 + 0 \pmod{2^8} \\ &\equiv 2^7 - Q_{80l+38}Q_{74} \pmod{2^8} \\ &\equiv 2^7 + 2^6 s_1(Q_{80l+43} - 2Q_{80l+42}) \pmod{2^8} \\ &\equiv 2^7 + 2^7 s_1(s_2 + s_3) \pmod{2^8} \\ &\equiv 2^7 \pmod{2^8}, \end{aligned}$$

pois $s_2 + s_3$ é par. Assim, a indução está completa.

Caso 10: $n \equiv 18, 38, 58 \pmod{80}$.

Esse caso é análogo ao Caso 9. Note que, se $n \equiv 18 \pmod{80}$, então $n = 80l + 18$ e assim

$$\nu_2((n+2)^2) + 1 = 2\nu_2(80l+20) + 1 = 2\nu_2(20(4l+1)) + 1 = 5.$$

Com isso, chegamos à congruência correspondente

$$Q_n \equiv 2^5 \pmod{2^6} \text{ se } n \equiv 18 \pmod{80},$$

e exatamente como no caso anterior, procedemos por indução sobre l . Para $l = 0$, temos

$Q_{18} = 39648 \equiv 32 \pmod{64}$. Supondo então que a congruência é válida para l , temos que

$$\begin{aligned}
Q_{80(l+1)+18} &= Q_{(80l+20)+78} \\
&= Q_{78}Q_{80l+17} + (Q_{80l+17} + Q_{20l+16})Q_{79} \\
&\quad + (Q_{80l+17} + Q_{80l+16} + Q_{80l+15})Q_{80} + Q_{81}Q_{80l+18} \\
&\equiv 0 + 0 + 0 + 2^5 \pmod{2^6} \\
&\equiv 2^5 \pmod{2^6}.
\end{aligned}$$

Os cálculos para $n \equiv 58 \pmod{80}$ são praticamente os mesmos. Assim, nesse caso, $n = 80l + 58$ e

$$\nu_2((n+2)^2) + 1 = 2\nu_2(80l+60) + 1 = 2\nu_2(20(4l+3)) + 1 = 5.$$

Com isso, chegamos à congruência correspondente

$$Q_n \equiv 2^5 \pmod{2^6} \text{ se } n \equiv 58 \pmod{80},$$

e exatamente como no caso anterior, procedemos por indução sobre l . Para $l = 0$, é simples computar que $Q_{58} \equiv 32 \pmod{64}$. Supondo então que a congruência é válida para l , temos que

$$\begin{aligned}
Q_{80(l+1)+58} &= Q_{(80l+60)+78} \\
&= Q_{78}Q_{80l+57} + (Q_{80l+57} + Q_{20l+56})Q_{79} \\
&\quad + (Q_{80l+57} + Q_{80l+56} + Q_{80l+55})Q_{80} + Q_{81}Q_{80l+58} \\
&\equiv 0 + 0 + 0 + 2^5 \pmod{2^6} \\
&\equiv 2^5 \pmod{2^6}.
\end{aligned}$$

Para $n \equiv 38 \pmod{80}$, temos que $n = 80l + 38$, e fazemos indução análoga ao caso $n = 80l + 35$. Para $l = 0$, temos que $Q_{38} = 19878720128 \equiv 128 \pmod{256}$. Supondo que é verdade para l , temos que

$$\begin{aligned}
Q_{80(l+1)+38} &= Q_{(80l+40)+78} \\
&= Q_{78}Q_{80l+37} + (Q_{80l+37} + Q_{20l+36})Q_{79} \\
&\quad + (Q_{80l+37} + Q_{80l+36} + Q_{80l+35})Q_{80} + Q_{81}Q_{80l+38} \\
&= Q_{75}Q_{80l+37} + (Q_{80l+38} - Q_{20l+35} - Q_{80l+34})Q_{76} \\
&\quad + (Q_{80l+38} - Q_{80l+34})Q_{77} + Q_{78}Q_{80l+38} \\
&\equiv 0 + 0 + 0 + 2^7 \pmod{2^8} \\
&\equiv 2^7 \pmod{2^8},
\end{aligned}$$

onde usamos o Caso 9.

Caso 11: $n \equiv 78 \pmod{80}, n > 78$.

Neste caso, sabemos que 160 divide exatamente um entre $n + 2$ e $n - 78$. Vamos supor que $160 \mid n + a$, para algum $a \in \{2, -78\}$. Assim $\nu_2(n + b) = 4$, para $b \in \{2, -78\} \setminus \{a\}$, e então, queremos provar que

$$\nu_2(Q_n) = \nu_2(n + a) + 5.$$

Mas, pelo Lema 3.4,

$$Q_{2^t-35s-a} \equiv 2^{t+2} \pmod{2^{t+3}}.$$

Portanto

$$\nu_2(Q_n) = \nu_2(Q_{2^t-35s-a}) = t + 2 = \nu_2(n + a) + 5.$$

Isso completa esse caso e conseqüentemente a prova do teorema. \square

Observação: O caso $n \equiv 75 \pmod{80}$ é bastante complicado. Nesse caso, o comportamento de $\nu_2(Q_n)$ é bastante similar ao caso $n \equiv 78 \pmod{80}$, o que sugere que $\nu_2(Q_n) = \nu_2((n + 5)(n + 75)) + 1$, quando $n \equiv 75 \pmod{80}$. Mas esses valores diferem dos esperados quando $n \equiv 555 \pmod{640}$.

De fato, é possível (e não muito complicado) mostrar que a valorização nesse caso não pode ter a forma $\nu_2(P(n)) + k$, onde $P(n)$ é um polinômio em n e k é uma constante inteira. Assim, as técnicas utilizadas para os outros casos se tornam ineficazes quando $n \equiv 75 \pmod{80}$. O que torna necessária uma nova forma de lidar com o problema.

3.3 A equação $Q_n = m!$

Nesta seção, vamos usar o Teorema 3.5 para resolver a equação (3.1) quando $n \not\equiv 75 \pmod{80}$. Assim, vamos demonstrar o seguinte resultado:

Teorema 3.6. *As únicas soluções para a equação Diofantina*

$$Q_n = m! \tag{3.9}$$

em inteiros positivos m e $n \not\equiv 75 \pmod{80}$ são

$$(n, m) \in \{(1, 1), (2, 1), (3, 2)\}.$$

Demonstração. Se $m \leq 22$, é fácil ver que as únicas soluções para a equação (3.1) são as já listadas no enunciado do teorema. Então, vamos supor que $m \geq 23$, então $(1.93)^{n-1} > Q_n = m! \geq 23!$ e, logo, $n > 80$. Usando o Lema 1.15 (para $p = 2$) juntamente com o Teorema 3.5, temos que

$$\begin{aligned} m - \left\lfloor \frac{\log m}{\log 2} \right\rfloor - 1 &\leq \nu_2(m!) = \nu_2(Q_n) \\ &< \nu_2(n(n + 10)(n + 6)(n + 1)(n + 5)^2(n + 2)^3(n - 78)) + 15 \\ &\leq 10\nu_2(n + \omega) + 15, \end{aligned}$$

para $\omega \in \{0, 1, 2, 5, 6, 10, -78\}$. Então $\nu_2(n + \omega) \geq (m - \lfloor \log m / \log 2 \rfloor - 16)/10$ e então, $2^{\lfloor (m - \lfloor \log m / \log 2 \rfloor - 16)/10 \rfloor}$ divide $n + \omega$. Em particular, $2^{\lfloor (m - \lfloor \log m / \log 2 \rfloor - 16)/10 \rfloor} \leq |n + \omega| \leq n + 78$ e aplicando a função \log , obtemos

$$\left\lfloor \frac{1}{10} \left(m - \left\lfloor \frac{\log m}{\log 2} \right\rfloor - 16 \right) \right\rfloor \leq \frac{\log(n + 78)}{\log 2}. \quad (3.10)$$

Por outro lado, pelo Teorema 1.7, $(1.92)^{n-2} < Q_n = m! < (m/2)^m$ e $\log n < 1.6m \log(m/2) + 2$. Substituindo isso em (3.10), chegamos em

$$\left\lfloor \frac{1}{10} \left(m - \left\lfloor \frac{\log m}{\log 2} \right\rfloor - 16 \right) \right\rfloor \leq \frac{\log(1.6m \log(m/2) + 80)}{\log 2}.$$

Essa desigualdade implica em $m \leq 121$ e então $n < 1.6 \cdot 121 \log(130/2) + 2 = 796, 272 \dots$. Agora, usando o *Mathematica*, não obtemos nenhuma solução para a equação (3.1) com $23 \leq m \leq 121$ e $81 \leq n \leq 796$. Com isso, a prova do teorema está completa. \square

Capítulo 4

Um Caso Particular da Equação de Brocard-Ramanujan

Já conhecemos a equação de Brocard-Ramanujan, $m! + 1 = n^2$. Aqui, vamos trabalhar com um caso particular dessa equação, onde n é um número de Tribonacci ou Tetranacci. Com efeito, usaremos aqui as técnicas e resultados obtidos no capítulo anterior e procuraremos as soluções de

$$(F_n^{(k)})^2 = m! + 1, \quad (4.1)$$

quando $k = 3$ ou $k = 4$.

4.1 $T_n^2 = m! + 1$

Primeiramente, vamos estudar a equação (4.1) quando $k = 3$. Vamos precisar de alguns resultados preliminares desenvolvidos por D. Marques e T. Lengyel [47] análogos aos da seção 3.1.

Lema 4.1. *Para todos inteiros n, m , com $n \geq 0$ e $m \geq 2$, temos que*

$$T_{n+m} = T_{m-2}T_n + (T_{m-3} + T_{m-2})T_{n+1} + T_{m-1}T_{n+2}.$$

Lema 4.2. *Para todo $s \geq 1$ e $t \geq 6$, temos que $T_{2^{t-3}s} \equiv s2^{t-4} \pmod{2^{t-3}}$.*

Demonstração. Iremos proceder por indução em s para provar simultaneamente as seguintes congruências

$$T_{2^{t-3}s} \equiv s2^{t-4} \pmod{2^{t-3}}, T_{2^{t-3}s-1} \equiv 0 \pmod{2^{t-3}}, T_{2^{t-3}s+1} \equiv 1 \pmod{2^{t-3}}. \quad (4.2)$$

Primeiramente, vamos lidar com a base de indução $s = 1$. Então, queremos provar que, para todo $t \geq 6$, vale

$$T_{2^{t-3}} \equiv 2^{t-4} \pmod{2^{t-3}}, T_{2^{t-3}-1} \equiv 0 \pmod{2^{t-3}}, T_{2^{t-3}+1} \equiv 1 \pmod{2^{t-3}}.$$

Vamos proceder por indução em t . Claramente as congruências valem para $t = 6$. Portanto, suponha que elas sejam válidas para t . Então usamos o lema 4.1 para $T_{2^{t-2}} = T_{(2^{t-3}-1)+(2^{t-3}+1)}$ a fim de obter

$$T_{2^{t-2}} = T_{2^{t-3}-1}^2 + (T_{2^{t-3}-2} + T_{2^{t-3}-1})T_{2^{t-3}} + T_{2^{t-3}}T_{2^{t-3}+1}. \quad (4.3)$$

Usando a relação de recorrência da definição de Tribonacci, obtemos $T_{2^{t-3}-2} \equiv 2^{t-4} + 1 \pmod{2^{t-3}}$. Agora, escrevemos $T_{2^{t-3}-2} = 1 + 2^{t-4} + a2^{t-3}$, $T_{2^{t-3}-1} = b2^{t-3}$, $T_{2^{t-3}} = 2^{t-4} + c2^{t-3}$ e $T_{2^{t-3}+1} = 1 + d2^{t-3}$. Assim, obtemos

$$\begin{aligned} T_{2^{t-2}} &= b^2 2^{2t-6} + (1 + 2^{t-4} + (a+b)2^{t-3})(2^{t-4} + c2^{t-3}) + (2^{t-4} + c2^{t-3})(1 + d2^{t-3}) \\ &\equiv 2^{t-4} + c2^{t-3} + 2^{t-4} + c2^{t-3} \pmod{2^{t-2}} \\ &\equiv 2^{t-3} \pmod{2^{t-2}}, \end{aligned}$$

como desejado. Aqui usamos o fato de que $2t-8 \geq t-2$, pois $t \geq 6$. Procedemos de forma similar para provar as outras congruências de (4.3). Agora, por hipótese de indução, vamos supor que as congruências em (4.2) valem para s . Então, usamos o mesmo procedimento (e o Lema 4.1) para $T_{2^{t-3}(s+1)} = T_{(2^{t-3}s-1)+(2^{t-3}+1)}$ e obtemos o resultado. \square

Procedendo à equação (4.1), vamos primeiramente calcular as valorizações de $T_n - 1$ e $T_n + 1$.

4.1.1 A valorização 2-ádica de $T_n - 1$

Nesse caso, temos que

Teorema 4.3. *Para $n \geq 5$, temos que*

$$\nu_2(T_n - 1) = \begin{cases} 0, & \text{se } n \equiv 0, 3 \pmod{4}; \\ 1, & \text{se } n \equiv 5 \pmod{8}; \\ \nu_2(n-2) - 1, & \text{se } n \equiv 2 \pmod{8}; \\ \nu_2(n+2) - 1, & \text{se } n \equiv 6 \pmod{8}; \\ \nu_2((n-1)(n+7)) - 3, & \text{se } n \equiv 1 \pmod{8}. \end{cases}$$

Demonstração. Primeiramente, note que, pela equação (1.10) para $k = 3$, temos que $T_n - 1$ é ímpar para todo $n \equiv 0, 3 \pmod{4}$, o que prova o primeiro caso. Agora note que, a fim de provar o segundo caso, é suficiente provar que $T_n \equiv 3 \pmod{4}$. Nesse caso, temos que $n = 8k + 5$, $k \geq 0$. Então procederemos por indução sobre k . Para $k = 0$ segue trivialmente, pois $T_5 - 1 = 7 - 1 = 6 = 2 \cdot 3$. Logo, vamos supor que $T_{8k+5} \equiv 3 \pmod{4}$. Usando o Lema 4.1, temos que

$$\begin{aligned} T_{8(k+1)+5} &= T_{(8k+5)+8} \\ &= T_6 T_{8k+5} + (T_6 + T_5) T_{8k+6} + T_7 T_{8k+7} \\ &= 13T_{8k+5} + 20T_{8k+6} + 24T_{8k+7} \\ &\equiv 3 \pmod{4}. \end{aligned}$$

No terceiro caso, para $t \geq 6$ e $s \geq 1$ ímpar, escrevemos $n = 2^{t-3}s + 2$. Agora, pelo Lema 4.2, temos que

$$\begin{aligned} T_{2^{t-3}s+2} &= T_{2^{t-3}s+1} + T_{2^{t-3}s} + T_{2^{t-3}s-1} \\ &\equiv 1 + 2^{t-4} + 0 \pmod{2^{t-3}} \\ &\equiv 1 + 2^{t-4} \pmod{2^{t-3}}. \end{aligned}$$

Logo

$$\nu_2(T_n - 1) = t - 4 = \nu_2(2^{t-3}s) - 1 = \nu_2(n - 2) - 1.$$

Vamos proceder da mesma forma no quarto caso. Para $t \geq 6$ e $s \geq 1$ ímpar, escrevemos $n = 2^{t-3}s - 2$. Então, pelo Lema 4.2, temos que

$$\begin{aligned} T_{2^{t-3}s-2} &= T_{2^{t-3}s+1} - T_{2^{t-3}s} - T_{2^{t-3}s-1} \\ &\equiv 1 - 2^{t-4} - 0 \pmod{2^{t-3}} \\ &\equiv 1 + 2^{t-4} \pmod{2^{t-3}}. \end{aligned}$$

Portanto

$$\nu_2(T_n - 1) = t - 4 = \nu_2(2^{t-3}s) - 1 = \nu_2(n + 2) - 1.$$

Para o quinto e último caso, $n \equiv 1 \pmod{8}$. Sabemos que 16 divide exatamente um entre $n-1$ e $n+7$. Suponhamos que $16|n+a$, para algum $a \in \{-1, 7\}$. Então $\nu_2(n+b) = 3$ para $b \in \{-1, 7\} \setminus \{a\}$, e logo, queremos provar que

$$\nu_2(T_n - 1) = \nu_2(n + a).$$

Para tal, escrevemos $n = 2^{t-2}s - a$, para $t \geq 5$ e $s \geq 1$ ímpar, e procedemos como no Lema 4.2 para provar que

$$T_{2^{t-2}s-a} - 1 \equiv 2^{t-2} \pmod{2^{t-1}}.$$

Portanto

$$\nu_2(T_n - 1) = t - 2 = \nu_2(n + a) + 1,$$

e a demonstração está completa. □

4.1.2 A valorização 2-ádica de $T_n + 1$

Agora, vamos proceder à prova do seguinte teorema:

Teorema 4.4. *Para $n \geq 1$, temos que*

$$\nu_2(T_n + 1) = \begin{cases} 15, & \text{se } n = 61; \\ 0, & \text{se } n \equiv 0, 3 \pmod{4}; \\ 1, & \text{se } n \equiv 1, 2, 6 \pmod{8}; \\ 3, & \text{se } n \equiv 5 \pmod{16}; \\ \nu_2((n+3)^2) - 3, & \text{se } n \equiv 13, 29, 45 \pmod{64}; \\ \nu_2((n-61)(n+3)) - 3, & \text{se } n \equiv 61 \pmod{64}, n > 61. \end{cases}$$

Demonstração. Os dois primeiros casos são triviais. O terceiro e o quarto seguem os mesmos passos. Note que, para prová-los, é suficiente provar que $T_n \equiv 1 \pmod{4}$ quando $n \equiv 1, 2, 6 \pmod{8}$ e $T_n \equiv 7 \pmod{16}$ quando $n \equiv 5 \pmod{16}$.

Logo, primeiramente, vamos escrever $n = 8l + 1$ e proceder por indução sobre $l \geq 0$. Para a base de indução $n = 0$ o resultado segue trivialmente, pois $T_1 + 1 = 2$. Suponhamos, então, que $T_{8l+1} \equiv 1 \pmod{4}$. Assim

$$\begin{aligned} T_{8(l+1)+1} &= T_{(8l+1)+8} \\ &= T_6 T_{8l+1} + (T_6 + T_5) T_{8l+2} + T_7 T_{8l+3} \\ &= 13T_{8l+1} + (13 + 7)T_{8l+2} + 24T_{8l+3} \\ &\equiv 1 \pmod{4}. \end{aligned}$$

Para o caso $n \equiv 2 \pmod{8}$, vamos escrever $n = 8l + 2$ e proceder por indução sobre $l \geq 0$. Para a base de indução $n = 0$ o resultado segue trivialmente, pois $T_2 + 1 = 2$. Suponhamos, então, que $T_{8l+2} \equiv 1 \pmod{4}$. Assim

$$\begin{aligned} T_{8(l+1)+2} &= T_{(8l+2)+8} \\ &= T_6 T_{8l+2} + (T_6 + T_5) T_{8l+3} + T_7 T_{8l+4} \\ &= 13T_{8l+2} + (13 + 7)T_{8l+3} + 24T_{8l+4} \\ &\equiv 1 \pmod{4}. \end{aligned}$$

Agora, vamos escrever $n = 8k + 6$ e proceder por indução sobre $k \geq 0$. Para $k = 0$, segue diretamente, pois $T_6 + 1 = 13 + 1 = 14 = 2 \cdot 7$. Agora, temos que

$$\begin{aligned} T_{8(l+1)+6} &= T_{(8l+6)+8} \\ &= T_6 T_{8l+6} + (T_6 + T_5) T_{8l+7} + T_7 T_{8l+8} \\ &= 13T_{8l+6} + 20T_{8l+7} + 24T_{8l+8} \\ &\equiv 1 \pmod{4}. \end{aligned}$$

Para o caso $n \equiv 5 \pmod{16}$, vamos escrever $n = 16l + 5$ e proceder por indução sobre $l \geq 0$. Para a base de indução $n = 0$ o resultado segue trivialmente, pois $T_5 + 1 = 8$. Suponhamos, então, que $T_{16l+5} \equiv 7 \pmod{16}$. Como mostramos acima, temos que $T_{16l+6} \equiv 1 \pmod{4}$, logo $T_{16l+5} = 4r + 1$, onde $r \in \mathbb{N}$. Assim

$$\begin{aligned} T_{16(l+1)+5} &= T_{(16l+5)+16} \\ &= T_{14} T_{8l+5} + (T_{14} + T_{13}) T_{8l+6} + T_{15} T_{8l+7} \\ &= 1705T_{8l+5} + (1705 + 927)T_{8l+6} + 3136T_{8l+7} \\ &\equiv 15 + 8T_{16l+6} \pmod{16} \\ &\equiv 15 + 8(4r + 1) \pmod{16} \\ &\equiv 7 \pmod{16}. \end{aligned}$$

Agora, note que, se $n \equiv 13 \pmod{64}$,

$$\begin{aligned}\nu_2((n+3)^2) - 3 &= 2\nu_2(n+3) - 3 \\ &= 2\nu_2(64k+13+3) - 3 = 2\nu_2(16(4k+1)) - 3 = 2 \cdot 4 - 3 \\ &= 5.\end{aligned}$$

Então, é suficiente provar que $T_n \equiv 31 \pmod{64}$. Mais uma vez, procederemos por indução. Primeiramente, note que $T_{13} = 927 \equiv 31 \pmod{64}$. Agora, temos que

$$\begin{aligned}T_{64(k+1)+13} &= T_{(64k+13)+64} \\ &= T_{62}T_{64k+13} + (T_{62} + T_{61})T_{64k+14} + T_{63}T_{64k+15} \\ &\equiv -1 + 32T_{64k+14} \pmod{64}.\end{aligned}$$

Mas, pelo caso anterior, temos que $T_{64k+14} \equiv 1 \pmod{4}$. Logo,

$$\begin{aligned}T_{64(k+1)+13} &\equiv -1 + 32T_{64k+14} \pmod{64} \\ &\equiv 32 - 1 \pmod{64} \\ &\equiv 31 \pmod{64}.\end{aligned}$$

Antes de partir para o próximo caso, vamos mostrar que $T_{64l+30} \equiv 1 \pmod{8}$. Para tal, vamos também proceder por indução. É trivial para a base de indução $l = 0$. Agora, temos que

$$\begin{aligned}T_{64(l+1)+30} &= T_{(64l+30)+64} \\ &= T_{62}T_{64l+30} + (T_{62} + T_{61})T_{64l+31} + T_{63}T_{64l+32} \\ &\equiv 1 \pmod{8},\end{aligned}$$

logo, $T_{64l+32} = 8l + 1$.

Agora, quando $n \equiv 29 \pmod{64}$, temos que

$$\begin{aligned}\nu_2((n+3)^2) - 3 &= 2\nu_2(n+3) - 3 \\ &= 2\nu_2(64k+29+3) - 3 = 2\nu_2(32(2k+1)) - 3 = 2 \cdot 5 - 3 \\ &= 7.\end{aligned}$$

Então, é suficiente provar que $T_n \equiv 127 \pmod{256}$. Mais uma vez, procederemos por indução. Primeiramente, é fácil mostrar que $T_{29} \equiv 127 \pmod{256}$. Agora, temos que

$$\begin{aligned}T_{64(l+1)+29} &= T_{(64l+29)+64} \\ &= T_{62}T_{64l+29} + (T_{62} + T_{61})T_{64l+30} + T_{63}T_{64l+31} \\ &\equiv 95 + 32T_{64l+30} \pmod{256} \\ &\equiv 95 + 32(8r+1) \pmod{256} \\ &\equiv 127 \pmod{256}.\end{aligned}$$

Agora, note que, se $n \equiv 45 \pmod{64}$,

$$\begin{aligned}\nu_2((n+3)^2) - 3 &= 2\nu_2(n+3) - 3 \\ &= 2\nu_2(64k+45+3) - 3 = 2\nu_2(16(4k+3)) - 3 = 2 \cdot 4 - 3 \\ &= 5.\end{aligned}$$

Então, é suficiente provar que $T_n \equiv 31 \pmod{64}$. Mais uma vez, procederemos por indução. Primeiramente, note que é trivial mostrar que $T_{45} \equiv 31 \pmod{64}$. Agora, temos que

$$\begin{aligned}T_{64(k+1)+45} &= T_{(64k+45)+64} \\ &= T_{62}T_{64k+45} + (T_{62} + T_{61})T_{64k+46} + T_{63}T_{64k+47} \\ &\equiv -1 + 32T_{64k+14} \pmod{64}.\end{aligned}$$

Mas, pelo caso anterior, temos que $T_{64k+46} \equiv 1 \pmod{4}$. Logo,

$$\begin{aligned}T_{64(k+1)+45} &\equiv -1 + 32T_{64k+14} \pmod{64} \\ &\equiv 32 - 1 \pmod{64} \\ &\equiv 31 \pmod{64}.\end{aligned}$$

Para o último caso, o procedimento é o mesmo feito no último caso do Teorema 4.3. Note que, como $n \equiv 61 \pmod{64}$, 128 divide exatamente um entre $n - 61$ e $n + 3$. Suponhamos que $128|n + a$, para algum $a \in \{-61, 3\}$. Então $\nu_2(n + b) = 6$ para $b \in \{-61, 3\} \setminus \{a\}$, e logo, queremos provar que

$$\nu_2(T_n + 1) = \nu_2(n + a) + 3.$$

Para tal, escrevemos $n = 2^{t-2}s - a$, para $t \geq 8$ and $s \geq 1$ ímpar, e realizamos o mesmo procedimento realizado no Lema 4.2 para provar que

$$T_{2^{t-2}s-a} + 1 \equiv 2^{t+1} \pmod{2^{t+2}}.$$

Portanto

$$\nu_2(T_n + 1) = t + 1 = \nu_2(n + a) + 3,$$

e a demonstração está completa. □

4.1.3 Resolvendo $T_n^2 = m! + 1$

Agora, vamos proceder de forma similar ao Teorema 3.6 para resolver a equação de Brocard-Ramanujan para números de k -bonacci.

Teorema 4.5. *Não existem soluções $(m, n) \in \mathbb{Z}^2$ para a equação*

$$T_n^2 = m! + 1. \tag{4.4}$$

Demonstração. Se $n \leq 61$, uma busca direta mostra que não há soluções para a equação (5). Logo, podemos supor que $n > 61$ e então $m \geq 30$. Usando o Lema 1.15 e os Teoremas 4.3 e 4.4, deduzimos que

$$\begin{aligned} m - \left\lfloor \frac{\log m}{\log 2} \right\rfloor - 1 &\leq \nu_2(m!) = \nu_2(T_n - 1) + \nu_2(T_n + 1) \\ &< \nu_2((n+2)(n-2)(n-1)(n+7)(n+3)^3(n-61)) + 5 \\ &\leq 8\nu_2(n+\omega) + 5, \end{aligned}$$

para algum $\omega \in \{-61, -2, -1, 2, 3, 7\}$. Então $\nu_2(n+\omega) \geq (m - \lfloor \log m / \log 2 \rfloor - 6)/8$ e então, $2^{\lfloor (m - \lfloor \log m / \log 2 \rfloor - 6)/8 \rfloor}$ divide $n+\omega$. Em particular, $2^{\lfloor (m - \lfloor \log m / \log 2 \rfloor - 6)/8 \rfloor} \leq |n+\omega| \leq n+61$ (pois $n+\omega \neq 0$) e aplicando a função \log , obtemos

$$\left\lfloor \frac{1}{8} \left(m - \left\lfloor \frac{\log m}{\log 2} \right\rfloor - 6 \right) \right\rfloor \leq \frac{\log(n+61)}{\log 2}. \quad (4.5)$$

Por outro lado, pelo Lema 1.7, temos que $(1.83)^{2n-4} < T_n^2 = m! + 1 < 2(m/2)^m$ e portanto $n < 0.9m \log(m/2) + 2.6$. Substituindo isso em (4.5), obtemos

$$\left\lfloor \frac{1}{8} \left(m - \left\lfloor \frac{\log m}{\log 2} \right\rfloor - 6 \right) \right\rfloor \leq \frac{\log(0.9m \log(m/2) + 63.6)}{\log 2}.$$

Essa desigualdade traz $m \leq 78$ e então $n < 0.9 \cdot 78 \log(78/2) + 2.6 = 259.782 \dots$. Agora, usando um procedimento no *Mathematica* não obtemos nenhuma solução para a equação (5) com $30 \leq m \leq 78$ e $62 \leq n \leq 259$. \square

4.2 $Q_n^2 = m! + 1$

Agora, vamos proceder da mesma forma para resolver a equação $(F_n^{(k)})^2 - 1 = m!$, quando $k = 4$. Primeiramente, vamos estabelecer as valorizações 2-ádicas de $Q_n + 1$ e $Q_n - 1$.

4.2.1 A valorização 2-ádica de $Q_n + 1$

Teorema 4.6. *Para $n \geq 1$, temos que*

$$\nu_2(Q_n + 1) = \begin{cases} 0, & \text{se } n \not\equiv 1, 2 \pmod{5}; \\ 1, & \text{se } n \equiv 1, 2, 7 \pmod{10}; \\ \nu_2((n+4)(n+14)) + 1, & \text{se } n \equiv 6 \pmod{10}. \end{cases}$$

Demonstração. Primeiramente, note que, pela equação (1.10) para $k = 4$, temos que $Q_n - 1$ é ímpar para todo $n \equiv 0, 3, 4 \pmod{4}$, o que prova trivialmente o primeiro caso. O

restante da demonstração seguirá os mesmos passos do caso $k = 3$, ou seja, procederemos por indução nos três primeiros casos. Assim, no caso onde $n \equiv 1 \pmod{10}$, temos que $n = 10l + 1$. Para o caso $n = 1$ é trivial, pois $Q_1 + 1 = 2$. Vamos supor que $Q_n + 1 \equiv 2 \pmod{4}$ ou $Q_n \equiv 1 \pmod{4}$. Logo, usando o Lema 3.2 e o Teorema 3.5, temos que

$$\begin{aligned} Q_{10(l+1)+1} &= Q_{(10l+3)+8} \\ &= Q_8 Q_{10l} + Q_9(Q_{10l} + Q_{10l-1}) + Q_{10}(Q_{10l} + Q_{10l-1} + Q_{10l-2}) + Q_{11}Q_{10l+1} \\ &\equiv 0 + 0 + 0 + 1 \pmod{4} \\ &\equiv 1 \pmod{4}. \end{aligned}$$

Para os casos, $n \equiv 2, 7 \pmod{10}$, temos que $n \equiv 2 \pmod{5}$. Logo, $n = 5l + 2$. Com isso, vamos fazer nossa indução. Para $n = 2$, $Q_2 + 1 = 2$ e o resultado se segue. Vamos supor que $Q_{5l+2} + 1 \equiv 2 \pmod{4}$. Portanto

$$\begin{aligned} Q_{5(l+1)+2} &= Q_{(5l+4)+3} \\ &= Q_3 Q_{5l+1} + Q_4(Q_{5l+1} + Q_{5l}) + Q_5(Q_{5l+1} + Q_{5l} + Q_{5l-1}) + Q_6 Q_{5l+2} \\ &\equiv 1 \pmod{4}. \end{aligned}$$

Para o caso onde $n \equiv 6 \pmod{10}$, note que 20 divide exatamente um entre $n + 4$ e $n + 14$. Suponhamos que $20|n + a$, para algum $a \in \{4, 14\}$. Então $\nu_2(n + b) = 1$ para $b \in \{4, 14\} \setminus \{a\}$, e logo, queremos provar que

$$\nu_2(Q_n + 1) = \nu_2(n + a) + 2.$$

Mas, para $t \geq 6$, pela demonstração do Lema 3.3, temos que

$$\begin{aligned} Q_{2^{t-5} \cdot 5s-4} &= Q_{2^{t-5} \cdot 5s} - Q_{2^{t-5} \cdot 5s-1} - Q_{2^{t-5} \cdot 5s-2} - Q_{2^{t-5} \cdot 5s-3} \\ &\equiv 2^{t-3} - 2^{t-4}\delta - 1 + 2^{t-4}\delta \pmod{2^{t-2}} \\ &\equiv 2^{t-3} - 1 \pmod{2^{t-2}}, \end{aligned}$$

e o resultado segue. □

4.2.2 A valorização 2-ádica de $Q_n - 1$

Teorema 4.7. *Para $n \geq 3$, temos que*

$$\nu_2(Q_n - 1) = \begin{cases} 0, & \text{se } n \not\equiv 1, 2 \pmod{5}; \\ 1, & \text{se } n \equiv 6 \pmod{10}; \\ \nu_2((n-1)(n+9)) + 1, & \text{se } n \equiv 1 \pmod{10}; \\ \nu_2((n-2)(n+3)) + 1, & \text{se } n \equiv 2 \pmod{5}. \end{cases}$$

Demonstração. Primeiramente, note que, pela equação (1.10), temos que $Q_n - 1$ é ímpar para todo $n \equiv 0, 3, 4 \pmod{4}$, o que prova trivialmente o primeiro caso. Para o segundo caso, note que podemos escrever $n = 10l + 6$ e proceder por indução sobre $l \geq 0$. Para $l = 0$, temos que $\nu_2(Q_n - 1) = \nu_2(Q_6 - 1) = \nu_2(14) = 1$. Vamos então supor que $\nu_2(Q_{10l+6} - 1) = 1$, em outras palavras, que $Q_{10l+6} \equiv 3 \pmod{4}$.

Assim, usando o Lema 3.2, temos que

$$\begin{aligned}
Q_{10(l+1)+6} &= Q_{(10l+8)+8} \\
&= Q_8 Q_{10l+5} + Q_9(Q_{10l+5} + Q_{10l+4}) + Q_{10}(Q_{10l+5} + Q_{10l+4} + Q_{10l+3}) \\
&\quad + Q_{11} Q_{10l+6} \\
&= 56Q_{10l+5} + 108(Q_{10l+5} + Q_{10l+4}) + 208(Q_{10l+5} + Q_{10l+4} + Q_{10l+3}) \\
&\quad + 401Q_{10l+6} \\
&\equiv 0 + 0 + 0 + 1 \cdot 3 \pmod{4} \\
&\equiv 3 \pmod{4},
\end{aligned}$$

e a indução está completa.

Para o caso onde $n \equiv 1 \pmod{10}$, note que 20 divide exatamente um entre $n - 1$ e $n + 9$. Suponhamos que $20|n + a$, para algum $a \in \{-1, 9\}$. Então $\nu_2(n + b) = 1$ para $b \in \{-1, 9\} \setminus \{a\}$, e logo, queremos provar que

$$\nu_2(Q_n + 1) = \nu_2(n + a) + 2.$$

Mas, para $t \geq 7$, pela demonstração do Lema 3.3, temos que

$$Q_{2^{t-5} \cdot 5s+1} \equiv 2^{t-3} + 1 \pmod{2^{t-2}},$$

e o resultado se segue.

Vamos agora estudar o caso onde $n \equiv 12 \pmod{20}$. Nesse caso, $n = 20l + 12$ e vamos mostrar por indução que $\nu_2(Q_n - 1) = 2$. Primeiramente, para $l = 0$ temos que $\nu_2(Q_n - 1) = \nu_2(Q_{12} - 1) = \nu_2(772) = 2$. Vamos então supor que $\nu_2(Q_{20l+12} - 1) = 2$, ou $Q_{20l+12} \equiv 5 \pmod{8}$. Assim, usando o Lema 3.2, temos que

$$\begin{aligned}
Q_{20(l+1)+12} &= Q_{(20l+14)+18} \\
&= Q_{18} Q_{20l+11} + Q_{19}(Q_{20l+11} + Q_{20l+10}) + Q_{20}(Q_{20l+11} + Q_{20l+10} + Q_{20l+9}) \\
&\quad + Q_{21} Q_{20l+12} \\
&= 39648Q_{10l+11} + 76424(Q_{10l+11} + Q_{10l+10}) \\
&\quad + 147312(Q_{10l+11} + Q_{10l+10} + Q_{10l+9}) + 283953Q_{10l+12} \\
&\equiv 0 + 0 + 0 + 1 \cdot 5 \pmod{8} \\
&\equiv 5 \pmod{8},
\end{aligned}$$

o que termina a indução.

Quando $n \equiv 2 \pmod{20}$, podemos escrever, para $t \geq 7$ e $s \geq 1$ ímpar, $n = 2^{t-5} \cdot 5s + 2$. Agora, note que, pelo Lema 3.3, temos que $Q_{2^{t-5} \cdot 5s + 2} \equiv 2^{t-4} \delta + 1 \pmod{2^{t-3}}$. Mas por outro lado temos que

$$\nu_2(n - 2) + 1 = \nu_2(2^{t-5} \cdot 5s) + 1 = t - 4,$$

e com isso então, nesse caso, $\nu_2(Q_n - 1) = \nu_2(n - 2) + 1$.

Observe que, quando $n \equiv 12 \pmod{20}$, então $\nu_2(n - 2) + 1 = \nu_2(20l + 12 - 2) + 1 = \nu_2(10(2l + 1)) + 1 = 2$. Portanto, podemos concluir que $\nu_2(Q_n - 1) = \nu_2(n - 2) + 1$, quando $n \equiv 2 \pmod{10}$.

No caso onde $n \equiv 7 \pmod{20}$, temos que $n = 20l + 7$. Vamos mostrar por indução que $\nu_2(Q_n - 1) = 2$. Primeiramente, para $l = 0$, temos que $\nu_2(Q_n - 1) = \nu_2(Q_7 - 1) = \nu_2(28) = 2$. Vamos então supor que $\nu_2(Q_{20l+7} - 1) = 2$, ou $Q_{20l+7} \equiv 5 \pmod{8}$. Assim, usando o Lema 3.2, temos que

$$\begin{aligned} Q_{20(l+1)+7} &= Q_{(20l+9)+18} \\ &= Q_{18}Q_{20l+6} + Q_{19}(Q_{20l+6} + Q_{20l+5}) + Q_{20}(Q_{20l+6} + Q_{20l+5} + Q_{20l+4}) \\ &\quad + Q_{21}Q_{20l+7} \\ &= 39648Q_{10l+6} + 76424(Q_{10l+6} + Q_{10l+5}) + 147312(Q_{10l+6} + Q_{10l+5} + Q_{10l+4}) \\ &\quad + 283953Q_{10l+7} \\ &\equiv 0 + 0 + 0 + 1 \cdot 5 \pmod{8} \\ &\equiv 5 \pmod{8}, \end{aligned}$$

o que termina a indução. Observe que nesse caso $\nu_2(n + 3) + 1 = \nu_2(20l + 7 + 3) + 1 = \nu_2(10(2l + 1)) + 1 = 2$, portanto, quando $n \equiv 7 \pmod{20}$, $\nu_2(Q_n - 1) = \nu_2(n + 3) + 1$.

Quando $n \equiv 17 \pmod{20}$, podemos escrever, para $t \geq 7$ e $s \geq 1$ ímpar, $n = 2^{t-5} \cdot 5s - 3$. Agora, note que, pelo Lema 3.3, temos que $Q_{2^{t-5} \cdot 5s - 3} \equiv 1 - 2^{t-4} \delta \pmod{2^{t-3}}$. Mas por outro lado temos que

$$\nu_2(n + 3) + 1 = \nu_2(2^{t-5} \cdot 5s) + 1 = t - 4,$$

e com isso então, nesse caso, $\nu_2(Q_n - 1) = \nu_2(n + 3) + 1$. Portanto, temos que $\nu_2(Q_n - 1) = \nu_2(n + 3) + 1$, quando $n \equiv 7 \pmod{10}$.

Como $\nu_2(n + 3) = 0$ quando $n \equiv 2 \pmod{10}$ e $\nu_2(n - 2) = 0$ quando $n \equiv 7 \pmod{10}$, então provamos que $\nu_2(Q_n - 1) = \nu_2((n + 3)(n - 2)) + 1$ quando $n \equiv 2 \pmod{5}$. E assim, completamos a demonstração do teorema. \square

4.2.3 Resolvendo $Q_n^2 = m! + 1$

Teorema 4.8. *A equação*

$$Q_n^2 = m! + 1 \tag{4.6}$$

não possui nenhuma solução em $(m, n) \in \mathbb{Z}^2$.

Demonstração. Observe que, $n \geq 3$ e usando o Lema 1.15 e os Teoremas 4.7 e 4.6, deduzimos que

$$\begin{aligned} m - \left\lfloor \frac{\log m}{\log 2} \right\rfloor - 1 &\leq \nu_2(m!) = \nu_2(Q_n - 1) + \nu_2(Q_n + 1) \\ &< \nu_2((n-2)(n-1)(n+3)(n+4)(n+9)(n+14)) + 5 \\ &\leq 6\nu_2(n+\omega) + 5, \end{aligned}$$

para algum $\omega \in \{-2, -1, 3, 4, 9, 14\}$. Então $\nu_2(n+\omega) \geq (m - \lfloor \log m / \log 2 \rfloor - 6)/6$ e então, $2^{\lfloor (m - \lfloor \log m / \log 2 \rfloor - 6)/6 \rfloor}$ divide $n+\omega$. Em particular, $2^{\lfloor (m - \lfloor \log m / \log 2 \rfloor - 6)/8 \rfloor} \leq |n+\omega| \leq n+14$ (pois $n+\omega \neq 0$) e aplicando a função \log , obtemos

$$\left\lfloor \frac{1}{6} \left(m - \left\lfloor \frac{\log m}{\log 2} \right\rfloor - 6 \right) \right\rfloor \leq \frac{\log(n+14)}{\log 2}. \quad (4.7)$$

Por outro lado, pelo Lema 1.7, temos que $(1.92)^{2n-4} < Q_n^2 = m! + 1 < 2(m/2)^m$ e portanto $n < 0.8m \log(m/2) + 2.6$. Substituindo isso em (4.7), obtemos

$$\left\lfloor \frac{1}{6} \left(m - \left\lfloor \frac{\log m}{\log 2} \right\rfloor - 6 \right) \right\rfloor \leq \frac{\log(0.8m \log(m/2) + 16.6)}{\log 2}.$$

Essa desigualdade traz $m \leq 55$ e então $n < 0.8 \cdot 55 \log(55/2) + 2.6 = 162.424\dots$. Agora, usando um procedimento no *Mathematica* não obtemos nenhuma solução para a equação (6) e a demonstração está completa. □

Referências Bibliográficas

- [1] M. Agronomof, Sur une suite récurrente, *Mathesis* **4** (1914), 125-126.
- [2] G. Back, M. Caragiu, The greatest prime factor and recurrent sequences. *Fibonacci Quart.* **48** (2010) 358-362.
- [3] G. Berman, K. D. Fryer, *Introduction to Combinatorics*, Academic Press, New York, 1972.
- [4] B. C. Berndt, W. Galway, The Brocard–Ramanujan diophantine equation $n! + 1 = m^2$, *The Ramanujan J.* **4** (2000), 41–42.
- [5] Y. Bilu, G. Hanrot and P. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers (with an appendix by M. Mignotte), *J. reine angew. Math.* **539** (2001), 75–122.
- [6] M. Bollman, H. S. Hernández, F. Luca, Fibonacci numbers which are sums of three factorials. *Publ. Math. Debrecen* **77** (2010), no. 1-2, 211–224.
- [7] J. Bravo, F. Luca, Power of two in generalized Fibonacci sequences, *Rev. Colomb. Mat.* **46** (2012), 67–79.
- [8] J. Bravo, F. Luca, Coincidences in generalized Fibonacci sequences, *J. Number Theory* **133** (2013), 2121–2137.
- [9] J. Bravo, F. Luca, On a conjecture about repdigits in k -generalized Fibonacci sequences, *Publ. Math. Debrecen* **82** Fasc. 3-4 (2013), 623-639.
- [10] J. Bravo, F. Luca, On the largest prime factor of the k -Fibonacci numbers, *Int. J. Number Theory* **9** (2013), 1351–1366.
- [11] H. Brocard, Question 166, *Nouv. Corresp. Math.* **2** (1876), 287.
- [12] Y. Bugeaud, M. Mignotte, S. Siksek, Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas Powers, *Ann. Math.* **163** (2006), 969–1018.
- [13] Y. Bugeaud, M. Mignotte, F. Luca, S. Siksek, Fibonacci numbers at most one away from a perfect power, *Elem. Math.* **63** (2008), 65–75.

- [14] M. Cipu, F. Luca, On the Galois group of the generalized Fibonacci polynomial, *An. Stiint. Univ. Ovidius Constanta Ser. Mat.* **9** (2001), 27–38.
- [15] C. Cooper, F.T. Howard, Some identities for r -Fibonacci numbers, *Fibonacci Q.* **49**(3) (2011), 231–243.
- [16] L.E. Dickson, History of the Theory of Numbers. Divisibility and Primality, vol. 1, *Chelsea Publishing Co.*, New York (1966).
- [17] G.P. Dresden, Z. Du, A simplified Binet formula for k -generalized Fibonacci numbers, *J. Integer Seq.* **17** (2014), 1–9.
- [18] A. Dujella, A. Pethó, A generalization of a theorem of Baker and Davenport, *Q.J. Math. Oxf. Ser. (2)* **49** (1998), 291–306.
- [19] P. Erdős, J. L. Selfridge, The product of consecutive integers is never a power. *Illinois J. Math.* **19** (1975), 292–301.
- [20] V. Facó and D. Marques, *Even Perfect Numbers among Generalized Fibonacci Sequences*, *Rendiconti Del Circolo Matematico di Palermo* **63** (2014) 363 - 370.
- [21] M. Feinberg, Fibonacci-Tribonacci, *Fibonacci Quart.* **1** (1963), 71-74.
- [22] J. Feng, More identities on the tribonacci numbers, *Ars Comb.* **100** (2011), 73-78.
- [23] G. Grossman, F. Luca, Sums of factorials in binary recurrence sequences, *J. Number Theory* **93** (2002), no. 2, 87–107.
- [24] J. H. Halton, On the divisibility properties of Fibonacci numbers. *The Fibonacci Quarterly* **4.3** (1966) 217-240.
- [25] E. Jacobson. Distribution of the Fibonacci numbers mod 2^k . *The Fibonacci Quarterly* **30.3** (1992) 211-15.
- [26] J. Klaška, A search for Tribonacci-Wieferich primes, *Acta Math. Univ. Ostrav.* **16** (2008), 15-20.
- [27] J. Klaška, On Tribonacci-Wieferich primes. *Fibonacci Quart.* **46/47** (2008/09), 290-297.
- [28] J. Klaška, Tribonacci partition formulas modulo m . *Acta Math. Sin. (Engl. Ser.)* **26** (2010) 465-476.
- [29] J. Klaška, L. Skula, The cubic character of the Tribonacci roots. *Fibonacci Quart.* **48** (2010) 21-28.
- [30] J. Klaška, L. Skula, Periods of the Tribonacci sequence modulo a prime $p \equiv 1 \pmod{3}$. *Fibonacci Quart.* **48** (2010) 228-235.
- [31] J. Klaška, L. Skula, A note on the cubic characters of Tribonacci roots. *Fibonacci Quart.* **48** (2010) 324-326.

- [32] T. Koshy, *Fibonacci and Lucas Numbers with Applications*, Wiley, New York (2001).
- [33] T. Lengyel, *The order of the Fibonacci and Lucas numbers*. *The Fibonacci Quarterly* **33**. 3 (1995), 234-239.
- [34] P. Y. Lin, De Moivre-type identities for the Tribonacci numbers. *Fibonacci Quart.* **26** (1988), 131-134.
- [35] F. Luca, Products of factorials in binary recurrence sequences. *Rocky Mountain J. Math.* **29** (1999), no. 4, 1387–1411.
- [36] F. Luca, Perfect Fibonacci and Lucas numbers, *Rend. Circ. Mat. Palermo Ser. II* **49** (2000), 313–318.
- [37] F. Luca, V. J. Mejjia Huguet, On perfect numbers which are ratios of two Fibonacci numbers, *Ann. Math. Inf.* **37** (2010), 107–124.
- [38] F. Luca, S. Siksek, Factorials expressible as sums of at most three Fibonacci numbers, *Proc. of the Edinburgh Math. Soc.* **53** (2010), no. 3, 679–729.
- [39] F. Luca, P. Stănică, $F_1 F_2 F_3 F_4 F_5 F_6 F_8 F_{10} F_{12} = 11!$, *Port. Math.* **63** (2006), 251–260.
- [40] D. Marques, The Fibonacci version of the Brocard-Ramanujan Diophantine equation, *Port. Math.* **68**, (2011) 185–189.
- [41] D. Marques, The order of appearance of product of consecutive Fibonacci numbers, *Fibonacci Quart.* **50**. 2 (2012) 132-139.
- [42] D. Marques, On the intersection of two distinct k -generalized Fibonacci sequences. *Mathematica Bohemica*, **137** (2012) 403-413.
- [43] D. Marques, Fibonacci numbers at most one away from the product of factorials. *Notes on Number Theory and Discrete Mathematics* **18** (2012), 13–19.
- [44] D. Marques, The proof of a conjecture concerning the intersection of k -generalized Fibonacci sequences, *Bull. Braz. Math Soc.* **44**(3) (2013), 455–468.
- [45] D. Marques, On the spacing between terms of generalized Fibonacci sequences, *Coll. Math.* **134** (2014), 267–280.
- [46] D. Marques, On k -generalized Fibonacci numbers with only one distinct digit, *Util. Math.*(preprint)
- [47] D. Marques, T. Lengyel, The 2-adic order of Tribonacci numbers and the equation $T_n = m!$. *Journal of Integer Sequences*, **17** (2014) , p. 14.10.1.
- [48] D. Marques, A. Togbé, Perfect powers among Fibonomial coefficients, *C. R. Acad. Sci. Paris, Ser. I* **348** (2010) 717–720.

- [49] 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.
- [50] M. D. Miller, On generalized Fibonacci numbers, *Amer. Math. Monthly* **78** (1971), 1108–1109.
- [51] T. D. Noe, J. V. Post, Primes in Fibonacci n -step and Lucas n -step sequences, *J. Integer Seq.* **8** (2005), 1–12.
- [52] M. Overholt, The Diophantine Equation $n! + 1 = m^2$, *Bulletin London Math. Soc.*, **25** (1993), 104.
- [53] A. Pethö, Fifteen problems in number theory. *Acta Univ. Sapientiae Math.* **2** (2010), 72–83.
- [54] B. Phong, Perfect numbers concerning Fibonacci sequence, *Acta Acad. Paed. Agriensis Sectio Math.* **26** (1999), 3–8.
- [55] S. Ramanujan, Question 469, *J. Indian Math. Soc.* **5** (1913), 59.
- [56] S. Ramanujan, *Collected Papers*, Chelsea, New York, 1962.
- [57] D. W. Robinson, *The Fibonacci matrix modulo m* , *The Fibonacci Quarterly*, **1.2** (1963) 29–36.
- [58] W. R. Spickerman, Binet’s formula for the Tribonacci sequence, *Fibonacci Quart.* **20** (1982), 118–120.
- [59] W. R. Spickerman, R. N. Joyner, Binet’s formula for the recursive sequence of order k , *Fibonacci Q.* **22** (1984) 327–331.
- [60] Z. W. Sun, Mixed sums of primes and other terms, arXiv:0901.3075v3
- [61] J. Vinson, *The relation of the period modulo m to the rank of apparition of m in the Fibonacci sequence.* *The Fibonacci Quarterly* **1.2** (1963) 37–45.
- [62] E. M. Waddill, Some properties of a generalized Fibonacci sequence modulo m . *Fibonacci Quart.* **16** (1978), 344–353.
- [63] Wolfram Research Inc. Mathematica, Version 7.0, Champaign (2008).
- [64] A. Wolfram, Solving generalized Fibonacci recurrences, *Fibonacci Q.* **36** (1998), 129–145.