REVISEM

Revista Sergipana de Matemática e Educação Matemática

https://doi.org/10.34179/revisem.v8i3.18391

UMA GENERALIZAÇÃO DO PEQUENO TEOREMA DE FERMAT VIA SISTEMAS DINÂMICOS E A SOLUÇÃO DE UM PROBLEMA DE L. LEVINE

Arlane Manoel Silva Vieira
Universidade Federal do Maranhão
arlane.silva@ufma.br
Lucas Bispo Cruz
Universidade Federal do Maranhão
lb.cruz@discente.ufma.br

Resumo

Fixado um inteiro $k \geq 1$, Levine [10] considera o sistema dinâmico definido pela função $f(z) = z^k$ no círculo unitário $\mathbb{S}^1$ e prova que $\sum_{m|n} \mu(n/m)\mathcal{N}_m$ é divisível por n, generalizando assim o pequeno teorema de Fermat. A notação $\mathcal{N}_m$ indica o número de pontos fixos de f^m em $\mathbb{S}^1$ e μ é a função de Möbius. Ao mesmo tempo o autor deixa em aberto uma pergunta: dada uma sequência de inteiros $(p_m)_m$ não-negativos, existe alguma função f que realiza essa sequência, ou seja, $p_m = \mathcal{N}_m$ e satisfaz o critério de divisibilidade? Neste artigo revisitamos o conhecido teorema de Euler usando polinômios de Chebyshev, seguindo Carrillo e Guzmán [3] e Frame *et al* [7], e respondemos negativamente à pergunta de Levine com um argumento baseado no teorema de Sharkovsky.
Palavras-Chave: Órbitas periódicas; teorema de Euler; polinômios de Chebyshev.

Abstract

Given an integer $k \geq 1$, Levine [10] considers the dynamical system defined by the function $f(z) = z^k$ on the unit circle $\mathbb{S}^1$ and proves that $\sum_{m|n} \mu(n/m)\mathcal{N}_m$ is divisible by n, thus generalizing Fermat's little theorem. The notation $\mathcal{N}_m$ indicates the number of fixed points of f^m in $\mathbb{S}^1$ and μ is the Möbius function. At the same time, the author leaves an open question: given a sequence of non-negative integers $(p_m)_m$, is there any function f that performs this sequence, that is, $p_m = \mathcal{N}_m$ and does it satisfy the divisibility criterion? In this article we revisit Euler's well-known theorem using Chebyshev's polynomials, following Carrillo and Guzmán [3] and Frame *et al* [7], and answer Levine's question in the negative with an argument based on Sharkovsky's theorem .
Keywords: Periodic orbits; Euler's theorem; Chebyshev polynomials.

1 Introdução

Múltiplos e divisores de números inteiros são temas apresentados aos estudantes desde o ensino fundamental e dentre as habilidades que se busca desenvolver no ensino de aritmética básica podemos citar a capacidade de elaborar e resolver problemas que envolvam critérios de divisibilidade, um tema intrinsecamente relacionado aos testes de primalidade e aplicações à criptografia [4], dentre eles o conhecido pequeno teorema de Fermat [1].

Tal resultado diz que dado um número primo p e um inteiro a, se $\text{mdc}(p, a) = 1$ então $a^{p-1} - 1$ é divisível por p. Na literatura é apresentada uma generalização desse teorema retirando-se a hipótese de que a e p são primos entre si, e neste caso verifica-se que p divide $a^p - a$, para qualquer inteiro positivo a. Existem diversas demonstrações desse resultado, até mesmo usando técnicas de sistemas dinâmicos problematizadas em [10], [5] e [7], por exemplo.

Com o objetivo de revisitar o pequeno teorema de Fermat e suas generalizações, escolhemos uma abordagem induzida via sistemas dinâmicos utilizando a iteração de polinômios de Chebyshev do tipo 1.

De modo geral, dados um conjunto S não-vazio e uma função $f : S \to S$, dizemos que o par (f, S) é um *sistema dinâmico*, e quando não há risco de confusão, dizemos apenas que f é um sistema dinâmico. A *órbita* de um ponto $x \in S$ pela ação de f é a sequência $(f^n(x))_n$, onde f^n é o n-ésimo iterado de f definido recursivamente por $f^0 = \text{Id}_S$ e $f^{k+1} = f \circ f^k$, para $k \geq 0$, e Id_S é a *função identidade* de S.

A órbita de um ponto $x \in S$ é *periódica* se existe $k \geq 1$ tal que $f^k(x) = x$, neste caso dizemos que x é periódico de *período* k, e que $\{x, f(x), f^2(x), \ldots, f^{k-1}(x)\}$ é um *k-ciclo*. Observe que se x é ponto periódico de período $k \geq 1$ de f então $f^{k\ell}(x) = x$ para qualquer $\ell \geq 1$ inteiro. Isto significa que qualquer múltiplo inteiro do período de um ponto periódico também é um período desse ponto. O menor desses períodos é chamado *período mínimal*, e o ciclo correspondente é chamado *ciclo minimal*. Quando $k = 1$, dizemos que x é um ponto fixo de f. A coleção dos pontos periódicos de f de período k será indicada por $P_k(f)$ e, sua cardinalidade será denotada por $\mathcal{N}_k(f)$.

O conjunto dos pontos periódicos de período minimal k será denotado por $P_k^*(f)$, e sua cardinalidade por $\mathcal{N}_k^*(f)$, ou simplesmente $\mathcal{N}_k^*$ quando não houver perigo de confusão.

Essencialmente, as abordagens via sistemas dinâmicos que encontramos na literatura para demonstrar o pequeno teorema de Fermat envolvem contar órbitas periódicas de um sistema dinâmico (f, S) no qual o número $\mathcal{N}_n(f)$ é finito, para todo $n \geq 1$. Levine [10] considera a função $f(z) = z^k$, para $z \in \mathbb{S}^1$, enquanto que Iga [8] discute a dinâmica de $T_n(x) := \{nx\}$ para $0 \leq x < 1$, com $T_n(1) := 1$. O símbolo $\{x\}$ denota a parte

fracionária de $x \in \mathbb{R}$. Posteriormente, e sem citar o artigo de Levine [10], Frame *et al* [7] analisa as órbitas de $g_a(x) \equiv ax \,(\mathrm{mod}\, 1)$, para cada inteiro $a \geq 1$, no intervalo $[0, 1]$. Mais recentemente, observando-se que os polinômios de Chebyshev possuem as mesmas propriedades de composição que aquelas funções estudadas em [10, 8, 7], Dragovic [5] apresentou uma nova demonstração do pequeno teorema de Fermat.

Seguindo Dragovic [5], consideremos o polinômio $T_n : [-1, 1] \to [-1, 1]$ de grau n definido por $T_n(x) = \cos(n \arccos(x))$. De modo equivalente, para cada $0 \leq \theta \leq \pi$, temos

$$T_n(\cos(\theta)) = \cos(n\theta). \tag{1.1}$$

Esta relação define os polinômios de Chebyshev de grau n (Veja a Figura 1[1]) e a relação de recorrência definida em $(\mathbf{P}_3)$, nos mostra como encontrar a expressão para cada um destes polinômios. Os cinco primeiros polinômios desta família estão listados abaixo:

$$\begin{aligned} T_0(x) &= 0; \\ T_1(x) &= x; \\ T_2(x) &= 2x^2 - 1; \\ T_3(x) &= 4x^3 - 3x, \\ T_4(x) &= 8x^4 - 8x^2 + 1 \end{aligned}$$

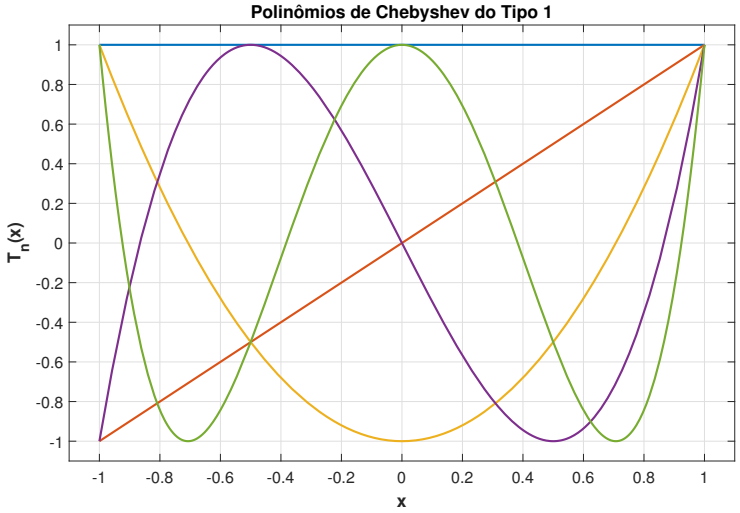

Figura 1: Gráfico de T_n, para $n = 0, 1, 2, 3, 4$.

[1]Produzida pelos autores

Cada função T_n é um sistema dinâmico no intervalo $[-1, 1]$, e estamos interessados na contagem das órbitas periódicas de cada uma dessas funções. O artigo de Dragovic [5] contém um único lema, que apesar de elementar é fundamental para o resultado pretendido, sem demonstração. Na Seção 3, discutimos as propriedades básicas de T_n e a demonstração detalhada desse lema, inclusive da contagem de pontos fixos de T_n.

Ainda neste contexto demonstramos na Seção 3 que, para quaisquer inteiros $a > 1$ e $n \geq 1$, tem-se

$$a^n = \sum_{m|n} \mathcal{N}_m^*(T_a) \tag{1.2}$$

Seguindo Frame [7] e Iga [8], apresentamos uma prova detalhada do conhecido teorema de Euler, uma generalização do pequeno teorema de Fermat, na Seção 4. É importante destacar que o Lema 3.4 foi apresentado em Frame [7], mas a nossa prova é diferente. Da mesma forma, o Teorema 4.2 foi enunciado sem demonstração por Frame [7], e neste trabalho usamos indução finita para demonstrá-lo.

Teorema 1.1 (Euler)**.** *Sejam a e n dois inteiros positivos, primos entre si. Então $a^{\phi(n)} - 1$ é divisível por n, onde ϕ é a função de Euler.*

Como consequência, demonstraremos também o seguinte resultado.

Teorema 1.2 (Forma generalizada do pequeno teorema de Fermat)**.** *Para quaisquer inteiros positivos a e n, temos*

$$n \mid \sum_{d|n} \mu\left(\frac{n}{d}\right) a^d, \tag{1.3}$$

onde μ é a função de Möbius.

A partir do Teorema 1.2 e da relação (1.2) concluímos que

$$n \mid \sum_{d|n} \mu\left(\frac{n}{d}\right) \mathcal{N}_d(T_a), \tag{1.4}$$

para quaisquer inteiros positivos a e n.

Nossa contribuição original, até onde sabemos, trata-se da pergunta de Levine [10], que responderemos negativamente na seção 5 e está relacionada à recíproca do Teorema 1.2, no seguinte sentido. Dado um inteiro $a > 1$, o polinômio de Chebyshev T_a define a sequência $(\mathcal{N}_m(T_a))_m$ que satisfaz a relação (1.4), para todo inteiro $m \geq 1$. Neste caso dizemos que a sequência $(\mathcal{N}_m(T_a))_m$ é *realizável*. Em outras palavras, dizer que uma sequência $(p_m)_m$ de inteiros positivos é realizável significa que existe um sistema dinâmico f tal que $\mathcal{N}_m(f) = p_m$, para cada $m \geq 1$, e $(\mathcal{N}_m)_m$ satisfaz a relação (1.4). Levine pergunta se qualquer sequência $(p_m)_m$ de inteiros positivos é realizável. Com um argumento baseado no teorema de Sharkovsky [6], apresentamos na seção 5 um contra-exemplo para esta questão.

2 Preliminares: as funções de Euler e de Möbius

Para cada inteiro positivo n, a cardinalidade do conjunto

$$\{m \in \mathbb{N} | m \leq n \text{ e } \text{mdc}(m,n) = 1\}$$

é denotada por $\phi(n)$. Esta é a função ϕ de Euler. Também é um exemplo de uma *função multiplicativa* [12, p. 72], ou seja, $\phi(mn) = \phi(m)\phi(n)$ sempre que m e n forem inteiros positivos relativamente primos. Abaixo deixamos exemplos da imagem da função em alguns números inteiros.

Exemplo 2.1. De acordo com a definição da função ϕ de Euler, temos:

$$\begin{aligned}
\phi(5) &= |\{m \in \mathbb{N} | m \leq 5 \text{ e } \text{mdc}(m,5) = 1\}| = |\{1,2,3,4\}| = 4 \\
\phi(9) &= |\{m \in \mathbb{N} | m \leq 9 \text{ e } \text{mdc}(m,9) = 1\}| = |\{1,2,4,5,7,8\}| = 6 \\
\phi(p) &= |\{m \in \mathbb{N} | m \leq p \text{ e } \text{mdc}(m,p) = 1\}| = |\{1,\ldots,p-2,p-1\}| = p-1
\end{aligned}$$

Ao longo do texto usaremos duas propriedades importantes da função ϕ, cujas provas podem ser encontradas em [12, seção 4.2].

(E_1) Se p é um número primo e $r \geq 1$ é um número inteiro então

$$\phi(p^r) = p^r - p^{r-1}. \tag{2.1}$$

(E_2) Se $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, onde $p_1, p_2, \ldots, p_k$ são primos distintos e $r_j \geq 1$ é inteiro, para cada $j = 1, 2, \ldots, k$, então

$$\phi(n) = \phi(p_1^{r_1})\phi(p_2^{r_2}) \cdots \phi(p_k^{r_k}). \tag{2.2}$$

A *função de Möbius* é a função μ definida sobre os inteiros $n \geq 1$ da seguinte forma: $\mu(1) := 1$ e para $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, onde $p_1, p_2, \ldots, p_k$ são primos distintos e $r_j \geq 1$ é inteiro, para cada $j = 1, 2, \ldots, k$,

$$\mu(n) := \begin{cases} (-1)^k, & \text{se } r_1 = r_2 = \cdots = r_k = 1; \\ 0, & \text{se } r_j > 1 \text{ para algum } j \in \{1,2,\ldots,k\}. \end{cases}$$

Exemplo 2.2. Vejamos alguns exemplos de valores da função de Möbius:

$$\begin{aligned}
\mu(7) &= -1, \text{pois 7 é primo;} \\
\mu(12) &= \mu(2^2 \cdot 3) = 0, \text{pois existe uma potência prima diferente de 1,} \\
\mu(50) &= \mu(2 \cdot 5^2) = 0, \text{pois existe uma potência prima diferente de 1,} \\
\mu(210) &= \mu(2 \cdot 3 \cdot 5 \cdot 7) = (-1)^4 = 1, \text{pois só existem potências com expoente unitário.}
\end{aligned}$$

Usaremos as seguintes propriedades da função de Möbius (veja em [9, p. 192] ou [12]):

($\mathbf{M}_1$) A função de μ de Möbius também é multiplicativa, isto é, $\mu(mn) = \mu(m)\mu(n)$ para quaisquer $m, n \geq 1$ inteiros primos entre si;

($\mathbf{M}_2$) Para qualquer $n \geq 1$ inteiro,

$$F(n) := \sum_{d|n} \mu(d) = \begin{cases} 1, & \text{se } n = 1; \\ 0, & \text{se } n > 1. \end{cases}$$

($\mathbf{M}_3$) (**Fórmula da inversão de Möbius**) Dadas duas sequências de números inteiros positivos $(a_n)_n$ e $(b_n)_n$ tais que

$$a_n = \sum_{d|n} b_d,$$

temos que

$$b_n = \sum_{d|n} \mu\left(\frac{n}{d}\right) a_d. \tag{2.3}$$

3 Um lema geral e os polinômios de Chebyshev

Considere um sistema dinâmico $f : S \to S$. O resultado a seguir mostra que o conjunto $P_m^*(f)$ pode ser particionado em ciclos minimais disjuntos.

Lema 3.1. *(i) Se x_0 é um ponto periódico de período n com período minimal igual a m, então $m|n$.*

(ii) Dois m-ciclos minimais são disjuntos ou idênticos.

(iii) Para todo $m \geq 1$, $m|\mathcal{N}_m^*$ sempre que $\mathcal{N}_m^*$ for finito.

Demonstração. (i) Como x_0 é periódico com período n e período minimal m, temos que $m \leq n$. Pelo algoritmo da divisão de Euclides, existem q e r inteiros positivos, tais que $n = qm + r$ e $0 \leq r < m$. Portanto

$$x_0 = f^n(x_0) = f^{qm+r}(x_0) = f^r(f^{qm}(x_0)) = f^r(x_0)$$

Como m é o menor inteiro positivo para o qual se tem $f^m(x_0) = x_0$, segue-se que $r = 0$, ou seja, $m|n$.

(ii) Consideremos dois m-ciclos minimais

$$C_1 := \{x_0, f(x_0), \ldots, f^{m-1}(x_0)\} \text{ e } C_2 := \{y_0, f(y_0), \ldots, f^{m-1}(y_0)\}$$

e suponha que existam $0 \leq i, j < m$ tais que $f^i(x_0) = f^j(y_0)$. Não há perda de generalidade ao supormos que $i \leq j$. Assim, $x_0 = f^{j-i}(y_0)$ e portanto, $f^\ell(x_0) \in C_2$ para cada $\ell = 0, 1, \ldots, m-1$, e provamos que $C_1 \subseteq C_2$. Por outro lado, existe um único $0 \leq \ell < m$ tal que $j - i + \ell = m$. Logo,

$$f^\ell(x_0) = f^{j-i+\ell}(y_0) = f^m(y_0) = y_0,$$

e isto prova que $C_2 \subseteq C_1$.

(iii) De fato, pelo item (ii), o conjunto $P_m^*(f)$ está particionado em órbitas periódicas de período m, duas a duas disjuntas com m elementos cada. Sejam $O_1, O_2, \ldots, O_k$ essas órbitas periódicas. Em particular,

$$P_m^*(f) = \bigcup_{j=1}^{k} O_j.$$

Como $|O_j| = m$ temos que

$$|P_m^*(f)| = \sum_{j=1}^{k} |O_j| = k \cdot m,$$

e portanto, m divide $\mathcal{N}_m^*(f) := |P_m^*(f)|$. □

Mais especificamente, consideremos os polinômios T_n definidos por (1.1). Temos as seguintes propriedades:

($\mathbf{P}_1$) Composição: $T_n \circ T_m = T_{n \cdot m}$.

Demonstração. De fato, dado $x \in [-1, 1]$ podemos escrever $x = \cos\theta$, para algum $\theta \in [0, \pi]$, e portanto

$$(T_n \circ T_m)(\cos(\theta)) = T_n(T_m(\cos(\theta))) = T_n(\cos(m\theta)) = \cos(nm\theta) = T_{n \cdot m}(\cos(\theta)).$$

□

($\mathbf{P}_2$) Extremos do domínio: $T_n(1) = 1$ e $T_n(-1) = (-1)^n$.

Demonstração. Basta ver que $T_n(1) = T_n(\cos(0)) = \cos(n \cdot 0) = 1$ e, $T_n(-1) = T_n(\cos(\pi)) = \cos(n\pi) = (-1)^n$. □

($\mathbf{P}_3$) Recorrência: $T_0(x) = 1$, $T_1(x) = x$, $T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$, para cada $n \geq 1$.

Demonstração. Observe que, para cada $n \geq 1$,

$$\begin{aligned} T_{n+1}(\cos(\theta)) + T_{n-1}(\cos(\theta)) &= \cos((n+1)\theta) + \cos((n-1)\theta) \\ &= 2\cos(\theta)\cos(n\theta). \end{aligned}$$

Subsituindo-se $x = \cos(\theta)$ na relação acima obtemos

$$T_{n+1}(x) + T_{n-1}(x) = 2xT_n(x),$$

e segue a conclusão. □

O resultado a seguir é fundamental para a contagem de pontos periódicos e foi apresentado por Dragovic [5], sem demonstração. Para a conveniência do leitor incluímos uma prova completa.

Lema 3.2. *Para $\theta \in [0, \pi]$, as afirmações abaixo são equivalentes:*

(i) $T_n(\cos(\theta)) = \cos(\theta)$*;*

(ii) $\operatorname{sen}\left(\frac{n-1}{2}\theta\right)\operatorname{sen}\left(\frac{n+1}{2}\theta\right) = 0$*;*

(iii) $\frac{n-1}{2}\theta = l\pi$ *ou* $\frac{n+1}{2}\theta = k\pi$*, para* $l, k \geq 0$ *inteiros;*

(iv) $0 \leq \theta = \frac{2l\pi}{n-1} \leq \pi$ *ou* $0 \leq \theta = \frac{2k\pi}{n+1} \leq \pi$*, para* $l, k \geq 0$ *inteiros.*

Demonstração. (i)⇔ (ii):

$$\begin{aligned} T_n(\cos\theta) = \cos(n\theta) &\Leftrightarrow \cos(n\theta) = \cos\theta \\ &\Leftrightarrow \cos(n\theta) - \cos\theta = 0 \\ &\Leftrightarrow -2\operatorname{sen}\left(\frac{n-1}{2}\theta\right)\operatorname{sen}\left(\frac{n+1}{2}\theta\right) = 0 \\ &\Leftrightarrow \operatorname{sen}\left(\frac{n-1}{2}\theta\right)\operatorname{sen}\left(\frac{n+1}{2}\theta\right) = 0. \end{aligned}$$

(ii)⇔ (iii):

$$\operatorname{sen}\left(\frac{n-1}{2}\theta\right)\operatorname{sen}\left(\frac{n+1}{2}\theta\right)=0 \Leftrightarrow \frac{n-1}{2}\theta = l\pi \quad \text{ou} \quad \frac{n+1}{2}\theta = k\pi,$$

para $l, k \geq 0$ inteiros.

(iii)⇔(iv): Veja que $0 \leq \theta = \dfrac{2l\pi}{n-1} \leq \pi$ ou $0 \leq \theta = \dfrac{2k\pi}{n+1} \leq \pi$, para $l, k \geq 0$ inteiros se, e somente se,

$$n\theta = 2\ell\pi + \theta \ \text{ ou } \ n\theta = 2k\pi - \theta,$$

o que é equivalente a $\cos(n\theta) = \cos(\theta)$, isto é, $T_n(\cos\theta) = \cos\theta$. □

O Lema 3.2 é fundamental para a contagem de pontos fixos dos polinômios T_n, definidos pela relação (1.1).

Teorema 3.3. *Para cada $n \geq 2$ inteiro, a função T_n possui exatamente n pontos fixos em seu domínio.*

Demonstração. No caso $n \geq 2$, usaremos o Lema 3.2 para verificar que T_n possui exatamente n pontos fixos. Para tanto, note que $\theta \mapsto \cos\theta$ é uma função bijetora entre os intervalos $[0, \pi]$ e $[-1, 1]$, e portanto, segue do item (iv) do Lema 3.2, que é suficiente verificar que existem exatamente n frações da forma

$$x_l := \frac{2l}{n-1} \quad \text{e} \quad y_k := \frac{2k}{n+1}, \tag{3.1}$$

no intervalo $[0, 1]$, para $l, k \geq 0$ inteiros. Inicialmente vamos verificar em quais casos ocorre $x_l = y_k$. Note que $x_l = y_k$ se, e somente se,

$$(k-l)n = k + l \tag{3.2}$$

e isto implica que $n|(k+l)$ e $k \geq l$. Consideremos os seguintes casos:

Caso 1. Para $k = l$ temos que $k + l = 0$ e portanto, $k = l = 0$.

Caso 2. Agora, suponha que $k > l$. Como $0 \leq 2l \leq n-1$ e $0 \leq 2k \leq n+1$ concluímos que $0 \leq k + l \leq n$. Lembrando que $n|(k+l)$, só pode ocorrer $k + l = 0$ ou $k + l = n$. O primeiro caso implica em $k = l = 0$ como antes. Já o segundo conduz à relação $k - l = 1$, pois $(k-l)n = k + l$. E como $k + l = n$ devemos ter $2k = n + 1$ e $l = k - 1$, de modo que esta relação impõe a restrição de que n seja ímpar.

Em resumo, se n é par então $x_0 = y_0$ e todas as outras frações em (3.1) são distintas e caso seja n ímpar temos $x_0 = y_0$ e, $x_{(n-1)/2} = y_{(n+1)/2} = 1$ e as demais frações

são distintas. Para determinar a quantidade de frações x_l e y_k no intervalo $[0,1]$, analisaremos por caso de acordo com a paridade de n.

Suponha que $n = 2m$ para algum $m \geq 1$ inteiro. Então $0 \leq l \leq m-1$ e $0 \leq k \leq m$, totalizando $m+(m+1) = 2m+1 = n+1$ frações, e como $x_0 = y_0 = 0$, concluímos que existem n frações distintas da forma (3.1) no intervalo $[0,1]$.

Considere agora que $n = 2m+1$, para um certo $m \geq 1$ inteiro. Da mesma forma que antes, $0 \leq l \leq m$ e $0 \leq k \leq m+1$, contabilizando $(m+1)+(m+2) = (2m+1)+2 = n+2$ frações. Observando que existem duas repetições neste caso, segue a mesma conclusão. □

O resultado a seguir também foi demonstrado em [7] em um contexto semelhante.

Lema 3.4. *Seja $a > 1$ um inteiro.*

(i) A função T_a possui a^n pontos periódicos de período n, para todo $n \geq 1$.

(ii) Dado um inteiro $n \geq 1$,

$$a^n = \sum_{m|n} \mathcal{N}_m^*(T_a).$$

Demonstração. (i) Como $T_a^n = T_{a^n}$, pela propriedade ($\mathbf{P}_1$), segue a conclusão.
(ii) Pelo item (i) do Lema 3.1, um ponto é periódico de período n se, e somente se, for periódico de período minimal m, para algum $m|n$. Portanto, (ii) segue de (i). □

4 O pequeno teorema de Fermat e generalizações

A apresentação da prova do pequeno teorema de Fermat segue as mesmas linhas de [5] que incluímos aqui para deixar o texto mais completo.

Teorema 4.1 (Pequeno Teorema de Fermat). *Seja $a \geq 2$ um número inteiro. Se $p \geq 2$ é primo então*

$$p|(a^p - a).$$

Demonstração. Fixemos um inteiro $a \geq 2$ e um primo p. Pelo item (ii) do Lema 3.4,

$$a^p = \sum_{m|p} \mathcal{N}_m^*(T_a) = \mathcal{N}_1^*(T_a) + \mathcal{N}_p^*(T_a).$$

Como $\mathcal{N}_1^*(T_a) = a$, concluímos que $\mathcal{N}_p^*(T_a) = a^p - a$. Pelo item (iii) do Lema 3.1, segue que $p|\mathcal{N}_p^*$, isto é, $p|(a^p - a)$. □

4.1 O teorema de Euler

Observe que o teorema de Euler (Teorema 1.1) é uma generalização do pequeno teorema de Fermat (Teorema 4.1). De fato, sejam p primo e $a \geq 2$ um inteiro, então $\phi(p) = p-1$ e portanto, $a^{p-1} - 1$ é divisível por p.

Para provar o Teorema 1.1 desenvolveremos alguns resultados preliminares, que podem ser encontrados em [7] e em [8], mas sem demonstração.

Teorema 4.2. *Sejam p e q dois primos distintos e, $a \geq 2$ e $k \geq 1$ inteiros, então:*

(i) $pq|(a^{pq} - a^p - a^q + a)$

(ii) p^k *divide* $a^{p^k} - a^{p^{k-1}}$ *para todo* $k \geq 1$.

Demonstração. (i) Sejam p e q primos distintos e $a \geq 2$ inteiro. Pelo item (ii) do Lema 3.4,

$$a^{pq} = \sum_{m|pq} \mathcal{N}_m^*(T_a) = \mathcal{N}_1^* + \mathcal{N}_p^* + \mathcal{N}_q^* + \mathcal{N}_{pq}^*.$$

Portanto,

$$a^{pq} = a + (a^p - a) + (a^q - a) + \mathcal{N}_{pq}^*,$$

de onde segue que

$$\mathcal{N}_{pq}^* = a^{pq} - a^p - a^q + a.$$

Pelo item (iii) do Lema 3.1 concluímos que $pq|(a^{pq} - a^p - a^q + a)$.

(ii) Sejam p um primo e $a \geq 2$ inteiro. Inicialmente, vamos provar por indução em $k \geq 1$ que

$$\mathcal{N}_{p^k}^* = a^{p^k} - a^{p^{k-1}}. \tag{4.1}$$

Na demonstração do pequeno teorema de Fermat (Teorema 4.1) vimos que $\mathcal{N}_p^* = a^p - a$, e portanto a relação (4.1) é verdadeira para $k = 1$. Agora fixemos $k \geq 2$ e suponha que a afirmação (4.1) seja verdadeira para $j = 1, 2, \ldots, k-1$. Novamente pelo item (ii) Lema 3.4,

$$a^{p^k} = \sum_{m|p^k} \mathcal{N}_m^*(T_a) = \mathcal{N}_1^* + \mathcal{N}_p^* + \mathcal{N}_{p^2}^* + \cdots + \mathcal{N}_{p^{k-1}}^* + \mathcal{N}_{p^k}^*. \tag{4.2}$$

Mas, por hipótese,

$$\begin{aligned} a^{p^k} &= a + (a^p - a) + (a^{p^2} - a^p) + \cdots + (a^{p^{k-1}} - a^{p^{k-2}}) + \mathcal{N}_{p^k}^* \\ &= a^{p^{k-1}} + \mathcal{N}_{p^k}^*, \end{aligned}$$

e portanto, $\mathcal{N}^*_{p^k} = a^{p^k} - a^{p^{k-1}}$.

Pelo Segundo Princípio da Indução [11, Teorema 9], segue que (4.1) é verdadeira para todo $k \geq 1$. Para finalizar a prova basta observar que $p^k | \mathcal{N}^*_{p^k}$, pelo item (iii) do Lema 3.1. Logo, $p^k | (a^{p^k} - a^{p^{k-1}})$ para todo $k \geq 1$. □

Com o Teorema 4.2 podemos demonstrar o Teorema de Euler, seguindo a mesma estratégia de Frame *et al* [7].

Demonstração do Teorema 1.1. Fixemos um inteiro $n \geq 1$, e seja $a \geq 2$ um inteiro relativamente primo com n. Já vimos que, se n é primo o Teorema de Euler se reduz ao pequeno teorema de Fermat. Assim, podemos supor que n não é primo e escrevemos $n = \prod_{i=1}^{k} p_i^{r_i}$, onde $p_1, p_2, \ldots, p_k$ são primos distintos e $r_j \geq 1$ é inteiro, para cada $j = 1, 2, \ldots, k$. Pelo Teorema 4.2,

$$p_i^{r_i} \left| \left(a^{p_i^{r_i}} - a^{p_i^{r_i - 1}} \right) = a^{p_i^{r_i - 1}} \left(a^{p_i^{r_i} - p_i^{r_i - 1}} - 1 \right), \right.$$

para $i = 1, 2, \ldots, k$. Como a e n são relativamente primos, então a e cada $p_i^{r_i}$ também são relativamente primos. Assim,

$$p_i^{r_i} \mid \left(a^{p_i^{r_i} - p_i^{r_i - 1}} - 1 \right),$$

para $i = 1, 2, \ldots, k$. Em particular, para cada $i = 1, 2, \ldots, k$, existe um inteiro positivo q_i tal que

$$a^{\phi(p_i^{r_i})} = a^{p_i^{r_i} - p_i^{r_i - 1}} = q_i p_i^{r_i} + 1.$$

Seja

$$s = \prod_{j=1, j \neq i}^{k} \phi(p_j^{r_j}).$$

Então

$$\begin{aligned} a^{\phi(n)} &= a^{\prod_{j=1}^{k} \phi(p_j^{r_j})} \\ &= a^{\phi(p_i^{r_i}) \prod_{j=1, j \neq i}^{k} \phi(p_j^{r_j})} \\ &= a^{\phi(p_i^{r_i}) \cdot s} \\ &= (q_i p_i^{r_i} + 1)^s \\ &= \sum_{j=0}^{s} \binom{s}{j} (q_i p_i^{r_i})^j \end{aligned}$$

$$
\begin{aligned}
&= 1 + \sum_{j=1}^{s} \binom{s}{j} (q_i p_i^{r_i})^j \\
&= 1 + p_i^{r_i} \sum_{j=1}^{s} \binom{s}{j} (q_i)^j (p_i^{r_i})^{j-1}.
\end{aligned}
$$

Definindo-se $q = \sum_{j=1}^{s} \binom{s}{j} (q_i)^j (p_i^{r_i})^{j-1}$, obtemos

$$a^{\phi(n)} - 1 = q p_i^{r_i},$$

e portanto, $p_i^{r_i}$ divide $a^{\phi(n)} - 1$ para cada $i = 1, 2, \ldots, k$. Como $p_i^{r_i}$ e $p_j^{r_j}$ são relativamente primos para todo $i \neq j$ com $i, j = 1, 2, \ldots, k$, tem-se:

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k} \Big| \left(a^{\phi(n)} - 1\right).$$

□

4.2 Demonstração do Teorema 1.2

Demonstração do Teorema 1.2. Tomando-se $a_n = a^n$ e $b_n = \mathcal{N}_n^*$, com $n \geq 1$ inteiro, segue-se do Lema 3.4 que

$$a_n = \sum_{d|n} b_d,$$

e pela propriedade $(\mathbf{M}_3)$,

$$\mathcal{N}_n^* = b_n = \sum_{d|n} \mu\left(\frac{n}{d}\right) a_d = \sum_{d|n} \mu\left(\frac{n}{d}\right) a^d.$$

A conclusão segue agora do Lema 3.1. □

Em particular, mostramos que se $\mathcal{N}_n$ é o número de pontos fixos de T_a^n, então

$$n \Big| \sum_{d|n} \mu\left(\frac{n}{d}\right) \mathcal{N}_d \tag{4.3}$$

para todo inteiro $n \geq 1$.

5 O problema de Levine e as sequências realizáveis

Antes de apresentar a discussão para a pergunta de Levine [10], que iniciamos na Introdução, faremos uma breve exposição do conhecido Teorema de Sharkovsky. Veja Du [6] para uma prova elementar e elegante.

Primeiro consideramos uma ordem especial no conjunto dos números inteiros positivos, chamada *ordem de Sharkovsky*, da seguinte forma:

$$\begin{array}{ccccccccccc}
 & 3 & \succ & 5 & \succ & \cdots & \succ & 2n+1 & \succ & \cdots \\
\succ & 2\cdot 3 & \succ & 2\cdot 5 & \succ & \cdots & \succ & 2\cdot(2n+1) & \succ & \cdots \\
\succ & 2^2\cdot 3 & \succ & 2^2\cdot 5 & \succ & \cdots & \succ & 2^2\cdot(2n+1) & \succ & \cdots \\
 & \vdots & & \vdots & & \ddots & & \vdots & & \vdots \\
\succ & 2^m\cdot 3 & \succ & 2^m\cdot 5 & \succ & \cdots & \succ & 2^m\cdot(2n+1) & \succ & \cdots \\
\succ & 2^m & \succ & 2^{m-1} & \succ & \cdots & \succ & 2 & \succ & 1
\end{array}$$

Teorema 5.1 (Sharkovsky)**.** *Sejam $I \subset \mathbb{R}$ um intervalo compacto e $f : I \to I$ uma função contínua. Se f possui um ponto periódico de período minimal $n \geq 1$ e $n \succ m$ na ordem de Sarkovsky então f também possui um ponto periódico de período minimal m.*

O Teorema de Sharkovsky (vide [6]) é o principal resultado na construção de uma sequência que servirá como contraexemplo para a pergunta Levine [10]. Assim, fixemos um inteiro $k > 1$, e considere a sequência $(a_d)_d$ definida por:

$$a_d = \begin{cases} k, & \text{se } k \mid d; \\ 0, & \text{caso contrário.} \end{cases} \tag{5.1}$$

Exemplo 5.2. Mais precisamente $(a_d)_d$ é uma família de sequências com parâmetro $k > 1$. Vejamos alguns exemplos:

(a) Para $k = 3$, $(a_d)_d = (0, 0, 3, 0, 0, 3, 0, \dots)$.

(b) Para $k = 4$, $(a_d)_d = (0, 0, 0, 4, 0, 0, 0, 4, 0, 0, 0, 4, \dots)$.

(c) Para $k = 5$, $(a_d)_d = (0, 0, 0, 0, 5, 0, 0, 0, 0, 5, 0, \dots)$.

Vamos provar inicialmente que, para qualquer $n \geq 1$,

$$n \Big| \sum_{d|n} \mu\left(\frac{n}{d}\right) a_d. \tag{5.2}$$

De fato, o resultado é imediato se $n = 1$, de modo que podemos assumir que $n > 1$. Além disso, se n não é múltiplo de k, então qualquer divisor de n também não pode ser múltiplo de k, e portanto, segue da definição de a_d que

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) a_d = 0.$$

Suponha agora que n é múltiplo de k. Isto significa que existe $m \geq 1$ inteiro tal que $n = mk$, para algum inteiro $m \geq 1$. Então,

$$\begin{aligned}
\sum_{d|n} \mu\left(\frac{n}{d}\right) a_d &= \sum_{d|n,\, k|d} \mu\left(\frac{n}{d}\right) a_d + \sum_{d|n,\, k\nmid d} \mu\left(\frac{n}{d}\right) a_d \\
&= \sum_{d|n,\, k|d} \mu\left(\frac{n}{d}\right) \cdot k + \sum_{d|n,\, k\nmid d} \mu\left(\frac{n}{d}\right) \cdot 0 \\
&= k \sum_{d|n,\, k|d} \mu\left(\frac{n}{d}\right).
\end{aligned}$$

Em particular, se $k = n$ então a afirmação (5.2) é verdadeira. Assim, para concluir a discussão vamos provar que

$$\sum_{d|n,\, k|d} \mu\left(\frac{n}{d}\right) = 0,$$

com $m > 1$, uma vez que $n = mk$. Para isto, como $k \mid d$ existe um único $\ell = \ell(d) \geq 1$ inteiro tal que $d = k\ell$. Como $n = km$, obtemos

$$\sum_{d|n,\, k|d} \mu\left(\frac{n}{d}\right) = \sum_{\ell|m} \mu\left(\frac{m}{\ell}\right) = 0,$$

pela propriedade $(\mathbf{M}_2)$. Assim, provamos que vale a afirmação (5.2) para a sequência $(a_d)_d$ dada, seja qual for o parâmetro $k > 1$.

Por fim, suponha (por absurdo!) que exista um sistema dinâmico $f : I \to I$, onde $I \subset \mathbb{R}$ é um intervalo compacto, em que $a_d = \mathcal{N}_d(f)$ (definido de acordo com a expressão (5.1)) seja a quantidade de pontos periódicos de período $d \geq 1$ de f em I. Tomando-se $k = 3$, assim como no exemplo dado, obtemos a sequência $(a_d)_d = (0, 0, 3, 0, 0, 3, 0, \dots)$ e concluímos que f possui três pontos periódicos de período 3, e portanto formam um ciclo minimal de comprimento 3. Entretanto, como $a_4 = \mathcal{N}_4(f) = 0$, não existem pontos periódicos de período 4 para f, e em particular, não existem pontos periódicos de período minimal 2. Isto contradiz o Teorema de Sharkovsky, uma vez que $3 \succ 2$ na ordem de Sharkovsky.

Portanto, encontramos uma família de sequências que satisfazem o critério de divisibilidade exposto na equação (5.2) mas não se realizam por um sistema dinâmico, o que responde negativamente o problema levantado por Levine [10] e abre um leque grande no estudo da contagem de órbitas periódicas de sistemas dinâmicos.

6 Considerações finais

Usando técnicas conhecidas de sistemas dinâmicos em conjunto com boas propriedades da família de polinômios de Chebyshev apresentadas em [5], revisitamos o pequeno teorema de Fermat e algumas generalizações, como o teorema de Euler. Uma dessas generalizações já foi discutida por Levine [10], e resolvemos o problema proposto pelo autor no mesmo artigo, por meio de um contraexemplo para afirmar que: Toda seqüência das quantidades de pontos fixos de um sistema dinâmico compacto satisfaz a relação de divisilidade (5.2) mas nem toda sequência relacionada a esta divisibilidade está ligada a um sistema dinâmico.

As sequências que satisfazem a relação (5.2) são conhecidas como *sequências de Dold* ou *sequências realizáveis* e têm papel importante em topologia e na contagem de órbitas periódicas de sistemas dinâmicos, como visto neste artigo. Entretanto, sua contribuição não se limita a apenas esta contagem, tendo em vista que podemos relacionar a este tipo de sequência outros objetos de dimensão maior, como vetores e matrizes (para um tratado sobre o assunto com aplicações recomendamos Byszewski *et al* [2] e as referências nele contidas).

Com a finalidade de desenvolver a fundo o estudo das sequências de Dold, busca-se a possibilidade de construir uma caracterização mais completa utilizando a família de sequências definidas em (5.1) juntamente com a função de Möbius e suas propriedades, em especial a fórmula da inversão de Möbius, para estabelecer uma relação entre uma sequência de Dold qualquer e combinações de sequências do tipo (5.1). [2]

Referências

[1] Burn, B., *Fermat's little theorem: Proofs that Fermat might have used*, The Mathematical Gazette, vol. **86**, no. 507, pp. 415–422, 2002.

[2]Este artigo é um recorte do trabalho de conclusão de curso da Especialização em Matemática Computacional do Centro de Ciências de Codó (CCCO/UFMA)

[2] Byszewski, J., Graff, G. and Ward, T., *Dold sequences, periodic points, and dynamics*, Bulletin of the London Mathematical Society, vol. **53**, no. 5, pp. 1263 – 1298, 2021.

[3] Carrillo, H., Guzmán, J. R. *A dynamical systems proof of Euler's generalization of the little Theorem of Fermat*, Aportaciones Matemáticas, Serie Comunicaciones, vol. **25**, pp. 199–202, 1999.

[4] Coutinho, S. C. *Números inteiros e criptografia RSA*. Segunda edição, Rio de Janeiro: IMPA, 2014.

[5] Dragović, V., *Polynomial dynamics and a proof of the Fermat little theorem*, The American Mathematical Monthly, vol. **120**, no. 2, pp. 171–173, 2013.

[6] Du, B.-S., *A simple proof of Sharkovsky's theorem*, The American Mathematical Monthly, vol. **111**, no. 7, pp. 595–599, 2004.

[7] Frame, M., Johnson, B. and Sauerberg, J., *Fixed points and Fermat: a dynamical systems approach to number theory*, The American Mathematical Monthly, vol. **107**, no. 5, pp. 422–428, 2000.

[8] Iga, K. *A dynamical systems proof of Fermat's little theorem*, Mathematics Magazine, vol. **76**, no. 1, pp. 48–51, 2003.

[9] LeVeque, W.J., *Fundamentals of number theory*. Addison-Wesley Reading, Mass, 1977.

[10] Levine, L., *Fermat's little theorem: A proof by function iteration*, Mathematics Magazine, vol. **72**, no. 4, pp. 308 – 309, 1999.

[11] Lima, E.L. *O princípio da indução*, Revista Eureka, no. 3, pp. 26–43, 1998.

[12] Santos, J. P. O., *Introdução à teoria dos números*. 3a. Edição, Rio de Janeiro: IMPA, 2020.

Submetido em 15 de Dezembro de 2022.
Revisado em 03 de Junho de 2023.
Aceito em 04 de Setembro de 2023.