Uma generalização do pequeno teorema de Fermat via sistemas dinâmicos e a solução de um problema de L. Levine

A. M. S. Vieira,* F. G. S. Alves† & L. B. Cruz‡

June 12, 2022

Resumo. Fixado um inteiro $k \geq 1$, Em [1], Levine considera a dinâmica induzida pela função $f(z) = z^k$ no círculo unitário $\mathbb{S}^1$ e provou que $\sum_{m|n} \mu(n/m)\mathcal{N}_m$ é divisível por n, portanto, generalizando 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 $(\mathcal{N}_m)_m$ não-negativos, existe alguma função f que realiza essa sequência e satisfaz o critério de divisibilidade? Neste artigo revisitamos o conhecido teorema de Euler usando polinômios de Chebyshev e respondemos negativamente à pergunta de Levine com um argumento baseado no teorema de Sharkovsky.

Palavras-chave. divisibilidade, órbitas periódicas, polinômios de Chebyshev, teorema de Sharkovsky.

1. Introdução

Múltiplos e divisores são temas apresentados aos estudantes desde o ensino fundamental e dentre as habilidades que se busca desenvolver podemos citar a capacidade de elaborar e resolver problemas que envolvam critérios de divisibilidade, um tema intrinsecamente relacionado aos testes de primalidade [2], dentre eles o conhecido pequeno teorema de Fermat [3].

*Centro de Ciências de Codó, Universidade Federal do Maranhão, Av. Dr. José Anselmo, 2008, 1654000-00, Codó, MA, Brasil – E-mail: arlane.silva@ufma.br - - cyanhttps://orcid.org/0000-0002-1198-2957

†Centro de Ciências de Codó, Universidade Federal do Maranhão, Av. Dr. José Anselmo, 2008, 1654000-00, Codó, MA, Brasil – E-mail: fabricio.alves@discente.ufma.br - -cyanhttp://lattes.cnpq.br/3945451724964287

‡Centro de Ciências de Codó, Universidade Federal do Maranhão, Av. Dr. José Anselmo, 2008, 1654000-00, Codó, MA, Brasil – E-mail: dacruzlucas09@gmail.com - - cyanhttp://lattes.cnpq.br/2547900722103969

Succisamente, esse resultado diz que dado um número primo p, se $mdc(p, a) = 1$ então que $a^{p-1} - 1$ 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 [1], [4] e [5], por exemplo.

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

De modo geral, dado 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 $f^0 = \mathrm{Id}_S$ 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 indicado 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.

Seguindo Dragovic [4], 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).

Cada função T_n induz um sistema dinâmico no intervalo $[-1, 1]$, e estamos interessados na contagem das órbitas periódicas de cada uma dessas funções. Neste sentido demonstraremos 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 [5], apresentamos uma prova do conhecido teorema de Euler, uma generalização do pequeno teorema de Fermat.

Teorema 1.1. *(Teorema de Euler) Dado um inteiro $n \geq 1$, seja a um inteiro positivo relativamente primo com n, então $a^{\phi(n)} - 1$ é divisível por n, onde ϕ é a função de Euler.*

Como consequência, demonstraremos também o seguinte resultado.

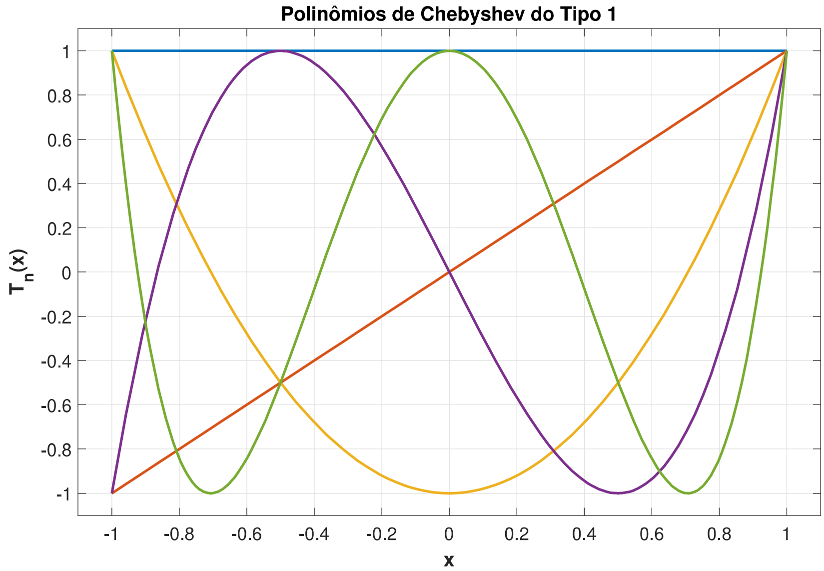

Figura 1: Gráfico de T_n, para $n = 0, 1, 2, 3, 4$.

Teorema 1.2. *(Forma generalizada do pequeno teorema de Fermat) Para quaisquer inteiros positivios n e a, 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 n e a. A pergunta de Levine [1], que responderemos negativamente na seção 5 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 $n \geq 1$. Neste caso dizemos que a sequência $(\mathcal{N}_m(T_a))_m$ é *realizável*. Em outras palavras, dizer que uma sequência $(\mathcal{N}_m)_m$ de inteiros positivos é realizável significa que existe um sistema dinâmico f tal que $\mathcal{N}_m := \mathcal{N}_m(f)$, para cada $m \geq 1$, e $(\mathcal{N}_m)_m$ satisfaz a relação (1.4). Levine pergunta se qualquer sequência $(\mathcal{N}_m)_m$ de inteiros positivos é realizável. Com um argumento baseado no teorema de Sharkovsky, apresentamos um contra-exemplo para esta questão.

2. Um lema geral

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.

Lema 2.1. *Sobre os pontos períodicos e órbitas de um sistema dinâmico, podemos afirmar que:*

(i) Se x_0 é um ponto 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 tem período n e período minimal m, temos que $m \leq n$. Pelo algoritmo da divisão de Euclides, existem q e r inteiros positivos, com $0 \leq r < m$, tais que $n = qm + r$. 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 $j - i + \ell = m$. Portanto,

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

e isto prova que $C_2 \subseteq C_1$.

(iii) Note que o conjunto dos pontos periódicos de período minimal m está particionado em m-ciclos disjuntos por (ii). Como m-ciclos mínimais contêm exatamente m pontos, e o número de ciclos é um número inteiro, devemos ter $m|\mathcal{N}_m^*$. $\square$

3. Polinômios de Chebyshev do tipo 1

Nesta seção resumiremos algumas propriedades dos polinômios T_n, definido por (1.1) e apresentadas em [4]. Para a comodidade do leitor apresentaremos as demonstrações.

(P1) 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

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

□

(P2) 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, $T_n(-1) = T_n(\cos(-1)) = \cos(n\pi) = (-1)^n$. □

(P3) 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

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

Com $x = \cos(\theta)$, a propriedade está provada. □

O resultado a seguir é fundamental para a contagem de pontos periódicos e foi apresentado em [4], sem demonstração. Para a conveniência do leitor incluímos uma prova completa.

Lema 3.1. *Para um número $\theta \in [0,\pi]$, as afirmações abaixo são equivalentes:*

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

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

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

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

Demonstração. (i)⇔ (ii): Como $T_n(\cos\theta) = \cos(n\theta)$, segue-se de (i) que $\cos(n\theta) = \cos\theta$. Mas

$$\cos(n\theta) - \cos\theta = -2\sin\left(\frac{n-1}{2}\theta\right)\sin\left(\frac{n+1}{2}\theta\right),$$

e portanto,

$$\sin\left(\frac{n-1}{2}\theta\right)\sin\left(\frac{n+1}{2}\theta\right) = 0.$$

(ii)⇔(iii): De (ii) segue-se imediatamente que

$$\frac{n-1}{2}\theta = l\pi \quad \text{ou} \quad \frac{n+1}{2}\theta = k\pi,$$

para $l, k \geq 0$ inteiros.
(iii)⇔(iv): Como $0 \leq \dfrac{\theta}{\pi} \leq 1$, o item (iii) implica imediatamente (iv), e vice-versa. □

Observando-se que $\theta \mapsto \cos\theta$ é uma função bijetora entre os intervalos $[0, \pi]$ e $[-1, 1]$, segue-se do Lema 3.1, que T_n possui n pontos fixos, para cada $n \geq 0$. O resultado a seguir também foi demonstrado por [5] em um contexto semelhante.

Lema 3.2. *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 **P1**, segue-se a conclusão.
(ii) Pelo Lema 2.1, 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 [4] que incluímos aqui para a conveniência do leitor.

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 Lema 3.2,

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

Como $\mathcal{N}_1^*(T_a) = a$, concluímos que $\mathcal{N}_p^*(T_a) = a^p - a$. Pelo Lema 2.1, segue-se que $p|\mathcal{N}_p^*$. □

4.1. O teorema de Euler

A função ϕ de Euler é uma *função multiplicativa* definida para $n \geq 1$ inteiro e conta a quantidade de números de inteiros até n relativamente primos com n (para mais detalhes veja [6] ou [7]).

Observe que o Teorema de Euler (Teorema 1.1) é uma generalização do pequeno Teorema de Fermat. De fato, para $n = p$ primo temos que $\phi(p) = p - 1$ e portanto, $a^{p-1} - 1$ é divisível por p. No caso em que $mdc(a, p) = 1$ segue-se que $p|(a^p - a)$.

Para provar o Teorema 1.1 succisamos de alguns resultados preliminares, que discutiremos a seguir e podem ser encontrados em [5] e em [8], sem demonstração.

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

(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 Lema 3.2,

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

Portanto,
$$a^{pq} = a + (a^p - a) + (a^q - a) + \mathcal{N}_{pq}^*,$$
de onde segue-se que
$$\mathcal{N}_{pq}^* = a^{pq} - a^p - a^q + a.$$
Pelo Lema 2.1, $pq|(a^{pq} - a^p - a^q + a)$.
(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 Lema 3.2,

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

para todo $k \geq 1$ inteiro. 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 princípio de indução forte [9], segue-se que (4.1) é verdadeira para todo $k \geq 1$. Para finalizar a prova basta observar que $p^k|\mathcal{N}_{p^k}^*$, pelo Lema 2.1. Logo, $p^k|(a^{p^k} - a^{p^{k-1}})$ para todo $k \geq 1$. □

Com o resultado anterior podemos demonstrar o Teorema de Euler, seguindo a mesma linha de [5].

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, de modo que podemos escrever $n = \prod_{i=1}^{k} p_i^{r_i}$, 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,

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

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 $i = 1, 2, \ldots, k$. Como consequência,

$$p_i^{r_i} \Big| \left(a^{\prod_{j=1}^{k} p_j^{r_j} - p_j^{r_j - 1}} - 1\right),$$

para $i = 1, 2, \ldots, k$. Note ainda que

$$\phi(n) = \prod_{i=1}^{k} \phi(p_i^{r_i}) = \prod_{i=1}^{k} (p_i^{r_i} - p_i^{r_i - 1}),$$

e portanto,

$$p_i^{r_i} \Big| \left(a^{\phi(n)} - 1\right),$$

para $i = 1, 2, \ldots, k$. 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:

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

□

Antes de demonstrar o Teorema 1.2, apresentaremos a função μ de Möbius e algumas de suas propriedades básicas (veja em [6, p. 192] ou [7]).

4.2. A função de Möbius e prova do Teorema 1.2

A *função de Möbius* é a função μ definida sobre os inteiros $n \geq 1$ da seguinte forma: $\mu(1) = 1$ e para $n = \prod_{j=1}^{k} p_j^{a_j}$, representado em sua forma fatorada em produto de potências de primos distintos,

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

Para maior comodidade do leitor, resumimos a seguir algumas propriedades da função μ que usaremos daqui por diante.

($\mu 1$) A função de μ de Möbius é multiplicativa, isto é, $\mu(mn) = \mu(m)\mu(n)$ para quaisquer $m, n \geq 1$ inteiros e relativamente primos.

($\mu 2$) Para qualquer $n \geq 1$ inteiro,

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

($\mu 3$) Dadas duas sequências de números inteiro positivos $(a_n)_n$ e $(b_n)_n$ tais que

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

segue-se da fórmula da inversão de Möbius diz que

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

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 3.2 que

$$b_n = \sum_{d|n} a_d,$$

e pela propriedade ($\mu 3$),

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

A conclusão segue agora do Lema 2.1. □

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 um contra-exemplo para a pergunta de Levine [1], que discutimos na Introdução, faremos uma breve exposição do conhecido Teorema de Sharkovsky. Veja Du [10] 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.*

Para justificar a discussão iniciada por Levine [1], a seguir definimos uma sequência especial que será usada no contra-exemplo de nossa afirmação. Assim, para todo $n \in \mathbb{N}^*$ considere a sequência $(a_n)_{n\in\mathbb{N}^*}$ da seguinte forma:

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

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_n 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 basta provar que

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

com $m > 1$. Para isto, como $k \mid d$ existe um único $\ell = \ell(d) \geq 1$ inteiro tal que $d = k\ell$. Logo,

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

pela propriedade ($\mu 2$). De qualquer forma, provamos que vale a afirmação (5.2) para a sequência $(a_n)_n$ dada.

Para finalizar, suponha que exista um sistema dinâmico $f : I \to I$, onde $I \subset \mathbb{R}$ é um intervalo compacto, em que $a_n = \mathcal{N}_n(f)$ seja a quantidade de pontos periódicos de período $n \geq 1$ de f em I. Tomando-se $k = 3$ concluímos que f possui 3 pontos periódicos de período 3, e portanto formam um ciclo minimal de comprimento 3. Entretanto, como $\mathcal{N}_4(f) = 0$ 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.

6. Considerações finais

Usando técnicas conhecidas de sistemas dinâmicos em conjunto com boas propriedades da família de polinômios de Chebyshev apresentada em [4], revisitamos o pequeno teorema de Fermat e algumas generalizações, como o teorema de Euler. Uma dessas generalizações já foi discutida por Levine [1], e resolvemos o problema proposto pelo autor no mesmo artigo, por meio de um contraexemplo.

As sequências que satisfazem a relação (5.2) são conhecidas como *sequências de Dold*, apesar de não haver unanimidade em sua nomenclatura, e têm papel importante em topologia e na contagem de órbitas periódicas de sistemas dinâmicos, como visto neste artigo. Entretanto, a caracterização completa dessas sequências ainda é um problema em aberto. Para um tratado sobre o assunto com aplicações recomendamos Byszewski *et al* [11] e as referências nele contidas.

Referências

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

[2] A. Andrade, M. coelho, W. oliveira, R. oliveira, A. Lessa, and L. Quintino, “Fundamentos e conceitos do teste de primalidade derteministico através do algorítmo agrawal-kayal-saxena,” *Revista Acadêmica Drummond*, vol. 8, p. 113, 05 2017.

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

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

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

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

[7] J. P. de Oliveira Santos, *Introdução à teoria dos números.* Instituto de Matemática Pura e Aplicada, 1998.

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

[9] A. Reid, "The principle of mathematical induction: A viable proof technique for high school students," *Retrieved from pub. ist. ac. at*, 2014.

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

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