Trabalho apresentado no XLI CNMAC, Unicamp - Campinas - SP, 2022.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics
Preprint

Polinômios de Chebyshev e uma prova para o teorema de Euler

Arlane M.S. Vieira[1], Fabrício G.S. Alves [2], Lucas B. da Cruz[3]
Centro de Ciências de Codó, UFMA

No estudo de Teoria dos números, encontramos propriedades belíssimas e bastante curiosas, em especial relacionadas aos números primos como o Pequeno Teorema de Fermat e em seu caso mais geral, o Teorema de Euler. Aqui, utilizamos alguns conceitos de Dinâmica como pontos fixos e pontos periódicos juntamente com a iteração de uma família especial de polinômios (os polinômios de Chebyshev) para expressar uma prova para alguns destes teoremas importantes.

1 Polinômios de Chebyshev do Tipo 1

Definição 1.1. *[1] Seja $n \in \mathbb{N}_0$ e $\theta \in [0, \pi]$, têm-se*

$$T_n(\cos(\theta)) = \cos(n\theta) \tag{1}$$

A relação acima define os polinômios de Chebyshev de grau n para $x \in [-1, 1]$, onde

$$T_n(x) = \cos(n \arccos(x)) \tag{2}$$

Abaixo, enunciamos o lema que nos auxilia a contar os pontos fixos dos polinômios de Chebyshev.

Lema 1.1. . *[2] Seja T_a o a-ésimo polinômio de Chebyshev do Tipo 1, tem-se:*

(i) *A função T_a possui a^n pontos de período n no intervalo $[-1, 1]$.*

(ii) *Para todo inteiro $a > 1$ e todo inteiro $n \geq 1$, $a^n = \sum_{m|n} \mathcal{N}_m(T_a)$.*

Prova: ***(i)*** *Note que os pontos de período n da função T_a são os pontos fixos da função T_a^n. Com efeito, usando a propriedade da composição, temos:*

$$T_a^n(x) = T_a^n(\cos(\theta)) = \cos(a^n\theta) \tag{3}$$

E a equação $\cos(\theta) = \cos(a^n\theta)$ possui a^n soluções no intervalo $[0, \pi]$. Portanto T_a^n possui a^n pontos fixos, isto é, T_a possui a^n pontos de período n.
(ii) *Note que, os pontos de período n são pontos de período mínimo m para algum $m|n$ e* ***(ii)*** *segue de* ***(i)****.*

Agora, com o auxílio da propriedade dos pontos fixos, podemos provar o pequeno teorema de fermat: Para todo inteiro $a \geq 2$ e e todo primo p, tem-se $a^p \equiv a(mod\, p)$. De fato, tome o polinômio $T_a : [-1, 1] \to [-1, 1]$ definido por $T_a(x) = \cos(a \arccos(x))$. Itera-se tal função p-vezes retornando a função

$$\underbrace{T_a \circ T_a \circ \cdots \circ T_a}_{\text{p-iterações}} = T_a^p \tag{4}$$

[1] arlane.silva@ufma.br
[2] fabricio$_g$sa@yahoo.com.br
[3] dacruzlucas09@gmail.com

O número de pontos fixos de T_a^p é exatamente igual ao número de pontos p-periodicos de T_a e $a^p = \sum_{m|p} \mathcal{N}_m(T_a)$. Portanto, $\mathcal{N}_p = a^p - a$. Por fim, seja x_0 um ponto de período minimal m, consideramos o m-ciclo minimal $\{x_0, x_1, \ldots, x_{m-1}\}$. A sequencia $\{x_i, f(x_i), f^2(x_i), \ldots, f^{m-1}(x_i)\}$ é completamente determinada por qualquer x_i pertencente ao m-ciclo e é uma reordenação dos elementos do m-ciclo original. Ainda mais, dois m-ciclos minimais são disjuntos ou idênticos. E, note que os pontos de ordem mínima m são particionados em m-ciclos disjuntos. Como m-ciclos mínimos contêm exatamente m pontos, e o numero de ciclos é um número inteiro, nós temos $m|\mathcal{N}_m$.

Portanto, temos que $p|\mathcal{N}_p$,isto é, $p|(a^p - a)$ e está provado o Pequeno Teorema de Fermat.

Agora, generalizando o teorema para um p não primo, necessitamos de mais alguns resultados enunciados no teorema abaixo.

Teorema 1.1. *.[3] Generalizando o resultado do Pequeno Teorema de Fermat para primos e potência de primos, temos:*

(i) *Dados p e q primos distintos e $a \geq 2$. Então $pq|(a^{pq} - a^p - a^q + a)$.*

(ii) *Seja p primo e $a \geq 2$ inteiro. Então p^k divide $a^{p^k} - a^{p^{k-1}}$ para todo $k \geq 1$*

Para demonstrar os resultados citados, basta analisar as iterações de T_a pq-vezes para **i** e $p^k - vezes$ para **ii** e o resultado segue. Agora, podemos discutir sobre o toerema de Euler, enunciado e mostrado abaixo.

Teorema 1.2 (Teorema de Euler)**.** *Seja n um número inteiro positivo e a é um inteiro relativamente primo a n, então*

$$a^{\phi(n)} \equiv 1 \, (mod \, n) \tag{5}$$

onde $\phi(n) := \{j \in \mathbb{N} \, | 1 \leq j \leq n \wedge (j, n) = 1\}$

Dem. *Tome $n = \prod_{i=1}^{k} p_i^{r_i}$. Para todo $i = 1, 2, \ldots, k$ e $a \geq 2$, tome a função $T_a^{p_i^{r_i}}$, i.e., T_a iterada $p_i^{r_i}$.*

*Pelo **Lema 1.1**, $a^{p_i^{r_i}} = \sum_{m|p_i^{r_i}} \mathcal{N}_m(T_a)$ e **Teorema 1.1**, $p_i^{r_i} \mid \left(a^{p_i^{r_i}} - a^{p_i^{r_i - 1}}\right)$ e como a e $n = \prod_{i=1}^{k} p_i^{r_i}$ são relativamente primos, então a e $p_i^{r_i}$ são relativamente primos para todo $i = 1, 2, \ldots, k$. Assim, temos:*

$$p_i^{r_i} \mid \left(a^{\prod_{i=1}^{k} p_i^{r_i} - p_i^{r_i - 1}} - 1\right) \tag{6}$$

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:

$$p_1^{r_1} \cdot p_2^{r_2} \cdot \cdots \cdot p_k^{r_k} \mid \left(a^{\phi(n)} - 1\right) \tag{7}$$

Portanto, o resultado segue.

Referências

[1] Vladimir Dragović. "Polynomial Dynamics and a Proof of the Fermat Little Theorem". Em: **The American Mathematical Monthly** 120.2 (2013), pp. 171–173.

[2] Michael Frame, Brenda Johnson e Jim Sauerberg. "Fixed points and Fermat: a dynamical systems approach to number theory". Em: **The American Mathematical Monthly** 107.5 (2000), pp. 422–428.

[3] Lionel Levine. "Fermat's Little Theorem: A Proof by Function Iteration". Em: **Mathematics Magazine** 72.4 (1999), pp. 308–309.