Rotações e números naturais: uma introdução aos sistemas dinâmicos

Felipe César F. Monteiro*

Instituto de Ciências Matemáticas e de Computação
Universidade de São Paulo
felipe.cesar.monteiro@usp.br

Resumo

Utilizaremos sistemas dinâmicos e rotações num círculo para provar que seu número natural favorito está no começo de uma potência de 2.

1. Introdução

O ponto onde queremos chegar é o seguinte: Fixado um k natural (que não seja uma potência de 10), para qualquer p natural, existe uma potência de k, digamos k^n que começa com este número. Por exemplo: para $k = 2$, $p = 81$, temos o natural $n = 13$, tal que $2^{13} = 8192$, onde os dois primeiros digitos é o 81.

Tabela 1: *Exemplos de k's e p's, associados a menor potência n tal que k^n comece com p*

k	p	n	k^n
2	81	13	8192
2	7	46	70368744177664
2	666	800	666801443287...77376
5	14	26	1490116119384765625
7	6	14	678223072849

Para isso, usaremos ferramentas de sistemas dinâmicos discretos, área da matemática que estuda o comportamento de funções quando aplicadas repetidamente em conjuntos. Estudaremos uma classe especial de funções definidas neste: as rotações de ângulo irracional. Estaremos usando, dessa forma, sistemas dinâmicos para resolver nosso problema inicial, um problema de teoria dos números. É interessante observar duas áreas que parecem distantes da matemática se relacionando.

*Agradecimentos a Amanda Figur, pela direção de arte, Vinícius Novelli, pela paciência, Thaís Jordão, pelo encorajamento, e aos pareceristas pelas sugestões e ajuda na produção deste texto.

2. Colando o intervalo em forma de círculo

Considere o intervalo $[0, 1)$, e vá deformando ele até colar o ponto 0 no buraco onde deveria estar o ponto 1. Veja nesta imagem que este é um jeito bastante interessante (e prático) de visualizarmos o círculo.

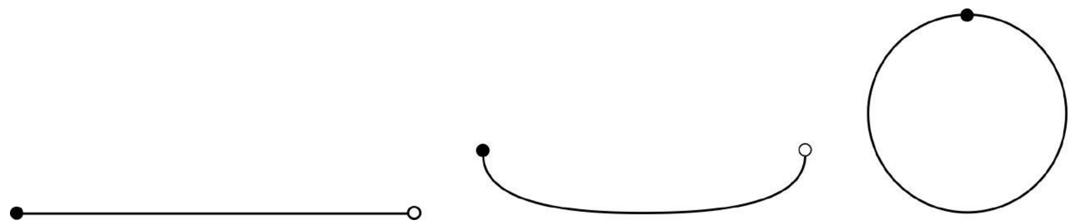

Figura 1: *Mostrando como transformar o intervalo num circulo*

Note que em nenhum momento esticamos o segmento, então as distâncias entre os pontos ainda estão preservadas, só que meio tortas. Distâncias agora são medidas com arcos de circunferências ao invés de retas. Isso não é uma demonstração! É só uma intuição do fato. Demonstração completa pode ser encontrada em [1].

Vamos definir uma maneira diferente de somar números em $[0, 1)$. A nossa motivação é a seguinte: Somando os números 0.8 e 0.9, conseguimos o número 1.7, que está fora do nosso intervalo. O ideal seria que, com a soma nova, sempre que somamos dois números de $[0, 1)$, obtemos um número também de $[0, 1)$. Definiremos da seguinte maneira:

Definição 2.1. *Considere $x, y \in [0, 1)$. Definiremos a Soma Nova da seguinte forma:*

$$x +_n y = \begin{cases} x + y & , se(x + y) < 1 \\ 1 - (x + y), & se(x + y) \geq 1 \end{cases}$$

Intuitivamente, estamos tirando a parte inteira do número. Por exemplo, nessa nova soma, $0.8 + 0.9 = 1.7 \rightarrow 0.7$.

Já fazemos isso com ângulos! Lembre-se que aconteciam coisas como $1080^o = 0^o$, ou $415^o = 45^o$, só que no nosso caso, ao invés de tirarmos múltiplos de 360, tiramos múltiplos de 1. é como se, ao somar números, estamos rodando os pontos correspondentes no círculo.

Veja que somarmos um número por 0.1 vai ser equivalente a caminhar o número por 36^o (basta fazer a regra de 3, agora dar uma volta completa pelo círculo é a mesma coisa que somar 1). Agora, assim como ângulos no círculo, teremos várias formas de escrever o mesmo número. Por exemplo, o número 0.5 (ou o equivalente a 180^o), pode ser escrito como $1.5 = 1 + 0.5$, $0.5 - 2 = -2.5$, etc.

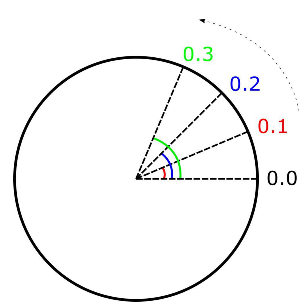

Figura 2: *Somando dois números (ou rodando um número)*

Quando dois pontos são iguais no círculo, dizemos que: $x = y \pmod 1$ (isso só quer dizer que podemos somar ou subtrair o número 1 várias vezes em x até obtermos y). Para evitarmos essas redundâncias, tomaremos sempre como *representante* [1] deste ponto um valor entre $[0, 1)$.

[1]Essa palavra não é por acaso. Se você já ouviu falar em classes de equivalência, é exatamente o que estamos fazendo

Outra característica interessante que podemos definir é uma forma medir distância entre dois pontos, que chamaremos de $d(x, y)$, usando os ângulos (ou arcos): $d(x, y) = |y - x \pmod 1|$. Ou seja, basta tomarmos o módulo do representante da diferença entre os dois pontos. Esta distância, além de ser sempre positiva, possui as propriedade do módulo da reta que conhecemos, como:

1. A desigualdade triangular: Dados $x, y, z \in \mathbb{R}$, $|x - z| = |x - y| + |y - z|$

2. A simetria: Dados $x, y \in \mathbb{R}$, $|x - y| = |y - x|$.

Note mais uma propriedade, agora diferente de $\mathbb{R}$: Essa distância é *limitada*. De fato, para quaisquer $x, y \in [0, 1)$, $|y - x \pmod 1| < 1$, é só notar que $y - x \pmod 1$ é escolhido como elemento de $[0, 1)$.

Agora, nosso $[0, 1)$ pode ser visto como um círculo, e a nossa soma nova definida é a mesma coisa que rotacionar pontos no circulo. Podemos nos referir a pontos em [0,1) como ângulos. Para tornarmos a rotação um conceito melhor formalizado, dado $\alpha \in [0, 1)$ podemos definir a seguinte função:

$$R_\alpha : [0,1) \longrightarrow [0,1)$$
$$x \mapsto \alpha + x \pmod 1,$$

que é uma rotação de ângulo α. Para funcionar, precisamos aplicar a função primeiro e depois "consertar"o ângulo para voltar para a nossa forma entre 0 e 1. Note que R_α definida assim é bijetora e que a inversa é a seguinte $R_{-\alpha}$.

Teorema 2.0.1. *Rotação é uma função que preserva distâncias. Mais precisamente, dados $x, y \in [0, 1)$, $d(y, x) = d(R_\alpha(y), R_\alpha(x))$.*

Demonstração. Basta abrir as definições:

$$|R_\alpha(y) - R_\alpha(x) \pmod 1| = |(\alpha + y) - (\alpha + x) \pmod 1| = |\alpha - \alpha + y - x \pmod 1| = |y - x \pmod 1|$$

□

3. Rotações

3.1 Rápida introdução a sistemas dinâmicos

Antes de estudarmos o comportamento das funções de rotação no círculo, discutiremos um pouco sobre algumas ferramentas usadas na área de sistemas dinâmicos discretos e fixaremos algumas notações.

A primeira coisa a se explicar é: o que exatamente essa área da matemática estuda? Primeiro, temos um conjunto X e uma função $f : X \longrightarrow X$, que é aplicada repetidamente em pontos do conjunto. A intuição desta observação é a seguinte: Queremos olhar o "futuro" de um ponto qualquer e pensar que cada aplicação da função é uma unidade de tempo.

Ou seja, analisando o ponto $f(x)$ e o ponto $f(f(x)) = (f \circ f)(x)$, e assim sucessivamente, nos dá a nossa noção de tempo da seguinte maneira: podemos pensar como um tempo discreto, onde o primeiro estado do nosso ponto x seria $f(x)$, e o segundo estado $(f \circ f)(x)$.

Se nossa função f possuir uma função inversa, podemos ainda "voltar no tempo" da seguinte forma: analisando os pontos $f^{-1}(x)$, ou $(f^{-1} \circ f^{-1})(x)$. Neste caso, estariamos estudando os estados que precederam o inicial do nosso ponto x.

Considere o seguinte exemplo:

$$f : \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \mapsto x^2.$$

Podemos estudar, por exemplo, o *comportamento* do ponto 2. Ou seja, analisarmos cada aplicação da função na imagem do ponto anterior:$f(2) = 4$, $(f \circ f)(2) = f(4) = 16$, $(f \circ f \circ f)(2) = f(16) = 256$, etc... Vemos que estes números crescem bastante e nunca param de crescer (tendem a infinito). Já se estudarmos o comportamento do ponto 1, ele é bem mais sem graça: $f(1) = 1$, $(f \circ f)(1) = 1$, $(f \circ f \circ f)(1) = 1$ [2].

Como vimos, a quantidade de parênteses ao estudar esse tipo de comportamento aumenta bastante. Então, vamos fixar a seguinte notação: Dado $x \in X$, definiremos:

$$f^n(x) = \overbrace{f \circ f \circ ... \circ f}^{n}(x) \ \ , \ \ f^{-n}(x) = \overbrace{f^{-1} \circ f^{-1} \circ ... \circ f^{-1}}^{n}(x) \ \text{ e } \ f^0(x) = x$$

Agora, vamos a uma definição que será o principal conjunto que estudaremos neste texto:

Definição 3.1. *Se tivermos um cojunto X qualquer e uma função $f : X \longrightarrow X$ bijetora, definimos a órbita da função num ponto $x \in X$ como o conjunto:*

$$\mathbb{O}_f(x) = \{f^n(x) : n \in \mathbb{Z}\} = \{..., f^{-n}(x), ..., f^{-3}(x), f^{-2}(x), f^{-1}(x), x, f(x), f^2(x), f^3(x), ..., f^n(x), ...\}$$

Definimos também a semiórbita positiva e a semiórbita negativa como, respectivamente:

$$\mathbb{O}^+_f(x) = \{f^n(x) : n \in \mathbb{Z} \text{ } e \text{ } n \geq 0\}$$

e

$$\mathbb{O}^-_f(x) = \{f^n(x) : n \in \mathbb{Z} \text{ } e \text{ } n \leq 0\}.$$

Assim, $\mathbb{O}_f(x) = \mathbb{O}^+_f(x) \cup \mathbb{O}^-_f(x)$

A intuição destas definições é a seguinte: A órbita de um ponto x é toda a história dele (seguindo a comparação com o tempo). Ou seja, são todas as aplicações de $f^n(x)$ e $f^{-n}(x)$ possiveis nele. Considerar a semiórbita positiva é considerar apenas o futuro do ponto e a semiórbita negativa é considerar o passado. No caso das rotações, a notação $R^n_\alpha = (R_\alpha \circ ... \circ R_\alpha)(x) = |\alpha + ... + \alpha + x \text{ (mod 1)}| = |n\alpha + x \text{ (mod 1)}| = R_{n \cdot \alpha}(x)$.

3.2 Comportamento de rotações

As rotações no círculo possuem um comportamento interessante. Primeiro, provaremos que, se rotacionarmos um ponto por um ângulo irracional, nunca voltamos ao ponto inicial. Note que isso é a mesma coisa que dizer que a órbita é infinita.

[2] Pontos que possuem esse comportamento, ou seja, que f(p) = p são chamados de pontos fixos e são bem importantes!

Teorema 3.2.1. *A órbita de um ponto em $[0,1)$ por uma rotação de ângulo irracional é sempre infinita.*

Demonstração. Seja $x \in [0,1)$ ponto inicial e $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ Suponhamos que a semiórbita positiva desta função em x seja finita. Então, vai existir $n \in \mathbb{N}$ tal que $R_\alpha^n(x) = x$. O que significa que:

$$n \cdot \alpha + x = x \text{ (mod 1)} \Rightarrow n \cdot \alpha = 0$$

Mas isso significa que $n \cdot \alpha$ é multiplo de 1 (inteiro). Então, existe $m \in \mathbb{Z}$ tal que $n \cdot \alpha = m$ ou seja $\alpha = m/n$. Mas α é irracional, e conseguimos escrever ele em forma de fração. Conseguimos, assim, um absurdo. Logo, a órbita não pode ser finita. □

Veja que, seguindo o mesmo raciocínio, é possivel mostrar que se α for racional, a órbita da rotação é finita.

Agora, precisamos provar um lema antes de seguirmos para o próximo teorema sobre rotações. Ele é uma versão um pouco diferente do famoso princípio da casa dos pombos.

A versão usual é a seguinte: Se eu tenho um número n de pombos devem ser colocados em m casas e se $n > m$, ou seja, o número de pombos é maior que o número de casas, então pelo menos uma casa irá conter mais de um pombo. De fato, não temos espaço para tantos pombos assim.

O Teorema abaixo segue a mesma linha: Eu não consigo um número grande o suficiente de espaçamentos de tamanho $\varepsilon > 0$ de um conjunto limitado da reta, pois não há espaço para isso. Ou seja, os espaçamentos devem estar contidos no conjunto (casa dos pombos) e não vão caber no conjunto se o número de espaçamentos (pombos) for muito grande.

Antes, definiremos a função "piso". Dado um número $x \in \mathbb{R}$, definimos $\lfloor x \rfloor$ como o maior inteiro que é menor ou igual a x. Alguns exemplos: $\lfloor 2 \rfloor = 2$, $\lfloor 2.1 \rfloor = 2$, $\lfloor -2.9 \rfloor = -2$.

Teorema 3.2.2 (Princípio da casa dos pombos)**.** *Dado $\varepsilon > 0$ e um conjunto $\{x_1, \ldots, x_k\}$ de k pontos em $[0,1)$, com $k \geq \lfloor \frac{1}{\varepsilon} \rfloor + 2$, então existem $i \neq j$ em $\{1, \ldots, k\}$ tais que $d(x_i, x_j) = |x_i - x_j \text{ (mod 1)}| < \varepsilon$.*

Demonstração. Dado $\varepsilon > 0$ e um conjunto de k pontos em $[0,1)$, com $k \geq \lfloor \frac{1}{\varepsilon} \rfloor + 2$. Suponha, por hipótese de absurdo, que $d(x_i, x_j) \geq \varepsilon$ para todo $i \neq j$ em $\{1, \ldots, k\}$. Isto é, que eles estão bem espaçados um do outro.

Podemos reescrever este conjunto ordenando os elementos, da seguinte maneira:

$0 \leq x_1 < \ldots < x_k < 1$. Como sabemos que a distância de dois elementos do círculo (ou do intervalo $[0,1)$) é limitada por 1 e que $d(x_k, x_1) = x_k - x_1$ (pois estão ordenados) e

$$d(x_k, x_1) = x_k - x_{k-1} + x_{k-1} - x_{k-2} + ... - x_2 + x_2 - x_1 = \sum_{i=1}^{k-1} x_{i+1} - x_i.$$

Conseguimos a igualdade anterior apenas somando e subtraindo termos iguais na expressão. E então, aplicando que a distância é limitada, temos:

$$1 > d(x_k, x_1) = \sum_{i=1}^{k-1} x_{i+1} - x_i = \sum_{i=1}^{k-1} d(x_{i+1}, x_i) \geq (k-1)\varepsilon.$$

Esta ultima desigualdade seguindo do fato da hipótese de que cada $d(x_{i+1}, x_i) \geq \varepsilon$. Agora, como $(k-1)\varepsilon < 1$, ou seja:

$$k < 1 + \frac{1}{\varepsilon} \underbrace{\Longrightarrow}_{k \in \mathbb{Z}} k \leq 1 + \left\lfloor \frac{1}{\varepsilon} \right\rfloor,$$

contradizendo a hipótese sobre a limitação de k. Ou seja, conseguimos um absurdo. Se tivermos conjuntos com este espaçamento, teriamos que ter uma quantidade menor de conjuntos. para conseguir fazer com que estes "caibam"no intervalo. □

Agora, chegamos no teorema mais importante do nosso texto, e a chave para provarmos o fato inicial do texto. Provarmos que as órbitas irracionais são densas em [0,1).

Dizemos que um subconjunto $A \subset \mathbb{R}$ é *denso* se para todo $z \in \mathbb{R}$, $\varepsilon > 0$, existe $a \in A$ tal que $a \in I_{(z,\varepsilon)}$, onde $I_{(z,\varepsilon)} = (z-\varepsilon, z+\varepsilon)$. Um exemplo é o conjunto dos números racionais nos reais. Podemos considerar conjuntos densos em $[0,1)$ ao invés de na reta inteira, substituindo por: A é denso em $[0,1)$ se para todo $z \in [0,1)$, $\varepsilon > 0$, existe $a \in A$ tal que $z \in (z-\varepsilon, z+\varepsilon)$.

A intuição desta definição de denso é que, qualquer vizinhança de um ponto do conjunto (no caso, um intervalinho em volta dele), existe um ponto do meu denso que está nessa vizinhança.

O fato que queremos provar significa que, dado um ponto z do círculo, eu consigo sair do meu ponto favorito do círculo x rotacionando com um ângulo irracional qualquer, e consigo chegar tão próximo quanto eu queira deste ponto. Outra maneira de pensar é que estes pontos estão bem distribuidos pelo círculo.

Teorema 3.2.3 (Órbitas irracionais são densas em [0,1))**.** *Seja $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ um número irracional. Então, para qualquer $x \in [0,1)$, a semiórbita positiva de R_α em x é densa em $[0,1)$.*

Demonstração. Fixe $\varepsilon > 0$ e $z \in [0,1)$. Vamos mostrar que existe um ponto na semiórbita positiva de x que dista menos de ε de z. Note como isso é o que precisamos provar: este ponto da semiórbita positiva estará no intervalo $(z-\varepsilon, z+\varepsilon)$. Como α é irracional, esta semiórbita é infinita.

Escolha um conjunto de pontos nesta órbita com cardinalidade (que chamaremos de k) maior do que ou igual a $\lfloor \frac{1}{\varepsilon} \rfloor + 2$. Podemos supor que este conjunto é da forma $\{x, R_\alpha(x), ..., R_\alpha^k(x)\}$, pois caso este seja da forma $\{R_\alpha^{n_1}(x), ..., R_\alpha^{n_k}(x)\}$, apenas o completamos até obter $\{x, R_\alpha(x), ..., R_\alpha^{n_k}(x)\}$, e a quantidade de pontos distintos neste trecho da órbita não diminui.

Pelo **Teorema 3.2.2**, existem $j < i$ em $\{1, \ldots, k\}$ tais que $d(R_\alpha^i(x), R_\alpha^j(x)) < \varepsilon$. Aplicando R_α^{-j} (que preserva distâncias), obtemos

$$d(R_\alpha^{i-j}(x), x) < \varepsilon.$$

Incrivelmente, esta desigualdade não depende de $x \in [0,1)$! De fato, se $y \in [0,1)$, então $y = |(y-x)+x| = R_{y-x}(x)$. Temos, dessa forma:

$$\begin{aligned} d(R_\alpha^{i-j}(y), y) &= d(R_\alpha^{i-j} \circ R_{y-x}(x), R_{y-x}(x)) \\ &= d(R_{(i-j)\alpha} \circ R_{y-x}(x), R_{y-x}(x)) \\ &= d(R_{(i-j)\alpha+y-x}(x), R_{y-x}(x)) \\ &= d(R_{y-x} \circ R_\alpha^{i-j}(x), R_{y-x}(x)) \\ &= d(R_\alpha^{i-j}(x), x). \end{aligned}$$

Para conseguirmos esta última sequência de igualdades, basta escrevermos a definição das rotações e das distâncias, por exemplo:

$$d(R_\alpha^{n_i-n_j} \circ R_{y-x}(x), R_{y-x}(x)) = |((n_i-n_j)\alpha + y - x + x) - (y - x + x) \text{ (mod 1)}|$$

Ou seja, até agora, temos que existem i, j tais que aplicar a rotação $i-j$ vezes em qualquer ponto dista menos que ε do ponto x. (Ou seja, eu conseguimos aplicar rotações até chegar tão perto quanto eu queira do meu ponto inicial).[3] Observe que podemos escolher um representante (que chamaremos de θ) para $(i-j)\alpha \in [0,1)$ que esteja em $[-1/2, 1/2)$, basta somar ou subtrair 1 de maneira conveniente. Defina $\rho = |\theta|$.

[3] Isso faz sentido, inclusive. Tente desenhar ;)

Temos $|\theta| < \varepsilon$ pelo seguinte motivo:

$$\begin{aligned}|\theta| = |\theta - 0 \pmod 1| = |(i-j)\alpha - 0 \pmod 1| = |(i-j)\alpha + x - x \pmod 1| &= d((i-j)\alpha + x, x)\\ &= d(R_\alpha^{i-j}(x), x)\\ &< \varepsilon,\end{aligned}$$

onde o segundo sinal de igualdade acima ocorre pois $(i-j)\alpha \equiv \theta \bmod 1$. Ainda, dado $w \in [0,1)$ qualquer, $\theta + w = (i-j)\alpha + w \pmod 1$, ou seja, $R_\alpha^{i-j} = R_\theta$.

Escreva $N = \lfloor \frac{1}{\rho} \rfloor + 1$ (observe que esta escolha de N depende apenas de $i-j$ e de α, portanto independe de x) e considere o seguinte subconjunto:

$$\{R_{l\cdot\theta}(x);\, l = 0, 1, \ldots, N\} = \{x, R_\theta(x), R_{2\theta}(x), ..., R_{(l-1)\theta(x)}, R_{l\cdot\theta}(x)\} \subset \{R_\alpha^m(x);\, m \in \mathbb{N}\}.$$

Provemos que esta reunião de N subintervalos de $[0,1)$ cobre o conjunto $[0,1)$. Isto é,

$$[0,1) \subset \bigcup_{l=0}^{N-1} [R_{l\theta}(x), R_{(l+1)\theta}(x)).$$

De fato, cada intervalo deste é equivalente a somar θ. Ou seja, conseguimos os conjuntos: $(x, x+\theta)$, $(x+\theta, x+2\theta)$, ..., $(x+(N-1)\theta, x+N\theta)$, todos de mesmo comprimento. Em algum momento, porém, estes intervalos irão "dar a volta"[4] no intervalo $[0,1)$. Como, por definição:

$$\left\lfloor \frac{1}{\rho} \right\rfloor + 1 \geq \frac{1}{\rho}$$

então:

$$N\rho = \left(\left\lfloor \frac{1}{\rho} \right\rfloor + 1 \right) \rho \geq 1.$$

Logo, a soma total dos comprimentos é maior ou igual que 1, o comprimento de $[0,1)$. Logo, no mínimo, estes intervalos conseguem voltar ao ponto x novamente, no caso em que o comprimento é igual a 1. Caso os intervalos continuem, já conseguimos o que queriamos.

Vejamos na imagem [5]:

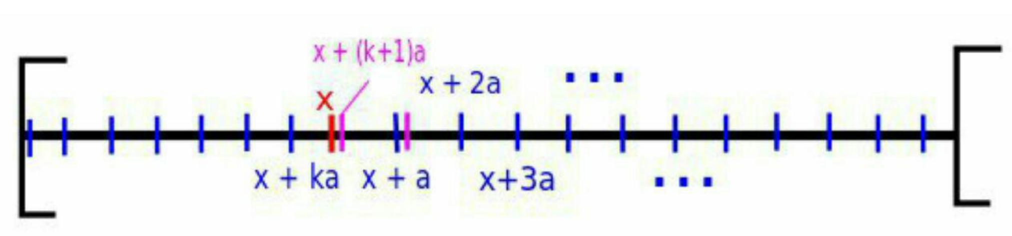

Figura 3: *Uma ilustração dessa cobertura e como ela funciona*

[4]Formalmente, isto é novamente do fato de qualquer intervalo de $\mathbb{R}$ de comprimento maior ou igual a 1 possuir um representante nesta soma (mod 1)

[5]Utilizando a imaginação para imaginar intervalos igualmente espaçados e relevando a capacidade do autor de fazer imagens.

Assim, o ponto $z \in [0,1)$ fixado no início pertencerá algum destes subintervalos, ou seja, existe $0 \le n \le N$ tal que

$$d(R_{n\theta}(x), z) < \rho < \varepsilon.$$

No entanto, $R_{n\theta}(x) = R_{\alpha}^{n(i-j)}(x)$. Então:

$$d(R_{\alpha}^{n(i-j)}(x), z) < \varepsilon,$$

concluíndo a prova do teorema.

□

4. Aplicação final

4.1 Sobre os números naturais

Finalmente, chegamos no resultado final. O que queremos provar é o seguinte:

Teorema 4.1.1. *Dado um número natural k fixado (que não seja uma potência de 10) , para todo outro número p natural, existe uma potência de k que começa com esse número.*

Demonstração. Queremos provar que, fixado $k \in \mathbb{N}$, $k \neq 10^m$ $\forall$ $m \in \mathbb{N}$, para todo $p \in \mathbb{N}$, existe $n \in \mathbb{N}$ tal que existe $l \in \mathbb{N}$ $k^n = 10^l p + q$ para algum $q \in \mathbb{N}$, onde $0 \le q < 10^l$. idéia da demonstração é traduzir este problema em termos de densos e abertos intervalos em $[0,1)$, manipulando as inequações, para aplicarmos o teorema que provamos sobre o círculo. A afirmação do teorema é equivalente a:

$$10^l p \le k^n < 10^l(p+1)$$

A primeira parte da inequação segue do fato de existir $q \ge 0$ tal que $k^n = 10^l p + q$. A segunda, do fato de que $q < 10^l$, logo $10^l + q < 10^l + 10^l$. Agora, como $\log_{10}$ é uma função crescente, ela não muda as inequações:

$$\log_{10}(10^l p) \le \log_{10}(k^n) < \log_{10}(10^l(p+1))$$

que é equivalente a:

$$l + \log_{10}(p) \le n \cdot \log_{10} k < l + \log_{10}(p+1)$$

Seja $m \doteq \lfloor \log_{10}(p) \rfloor + 1$ que é exatamente o número de digitos de p. Para mostrar isto, basta escrever como a expansão decimal de p e notar que a parte inteira é referente a potência de 10 do último número desta expansão. Logo:

$$0 \le \log_{10}(p) - (m-1) \le n \cdot \log_{10} k - (m-1) - l < \log_{10}(p+1) - (m-1) \le 1$$

Conseguimos isso somando o termo $-m - l - 1$ em todas as desigualdades. A idéia por trás é conseguirmos trazer estes termos para o intervalo $[0,1)$. Provemos a última destas desigualdades. Observe que ela é equivalente a

$$\log_{10}(p+1) \le 1 + \lfloor \log_{10} p \rfloor,$$

que por sua vez, é equivalente a

$$p + 1 \le 10^{1 + \lfloor \log_{10} p \rfloor} = 10^{\text{número de dígitos de p}}.$$

Mas se p tem k dígitos, então $p \leq \underbrace{99\ldots9}_{k}$ e $p+1 \leq 10^k$, como queríamos. Podemos reescrever a inequação acima desse modo:

$$\log_{10}\left(\frac{p}{10^{m-1}}\right) \leq \left\{n \cdot \log_{10} k\right\} \leq \log_{10}\left(\frac{p+1}{10^{m-1}}\right)$$

No meio, temos a função parte fracionária $\{\cdot\}$. De fato, sabemos que $m+l+1$ é inteiro, subtraímos de um inteiro k^n, e conseguimos um número entre 0 e 1. Isto só acontecerá quando o resultado desta é exatamente a parte fracionária de k^n.

Assim, conseguimos traduzir o problema de achar p tal que $10^l p \leq k^n < 10^l(p+1)$, para achar $n\log_{10} k$ que satisfaça isso para todo p.

Para o último passo, precisamos provar que $\left(n\log_{10} k\right)_{n\in\mathbb{N}}$ é uma sequência de números irracionais. Note que $\log_{10} k$ é irracional, pois, caso contrário, existiram $p, q \in \mathbb{Z}$ tais que:

$$\log_{10} k = \frac{p}{q} \Rightarrow k = 10^{p/q} \Rightarrow k^q = 10^p$$

Como $k \in \mathbb{N}$, isto implica que existe $m \in \mathbb{N}$ tal que $k = 10^m$, contradizendo a hipótese do inicio.

Veja que $\left(n\log_{10} k\right)_{n\in\mathbb{N}}$ é a órbita de rotações de ângulo α. De fato,

$$R^n_{\log_{10} k}(0) = \overbrace{\log_{10} k + \log_{10} k + \log_{10} k + \ldots + \log_{10} k}^{n} + 0 = n\log_{10} k$$

Ou seja, é densa no círculo. Para cada aberto em $[0,1)$, existe um elemento desta sequência neste aberto e existe $n \in \mathbb{N}$ tal que $n \cdot \log_{10} k$ está no intervalo $\left(\log_{10}\left(\frac{p}{10^{m-1}}\right), \log_{10}\left(\frac{p+1}{10^{m-1}}\right)\right)$. Assim, o resultado vale de fato (como tudo que fizemos foram equivalências, podemos agora voltar as equivalências com este n que provamos que existe), e conseguimos nossa potência de k. $\square$

Um outro resultado relacionado a este teorema que é interessante também (mas assunto para outro texto) é que fixado k (k= 2 por exemplo) então a frequência das potências de 2 começadas com o digito 1 é maior que as potências de 2 começadas com o digito 2, que é maior que as começadas com 3, etc. Neste caso, existe uma demonstração matemática para um conceito um pouco mais geral, e que não foi totalmente explicado/demonstrado matemáticamente: a Lei de Benford.

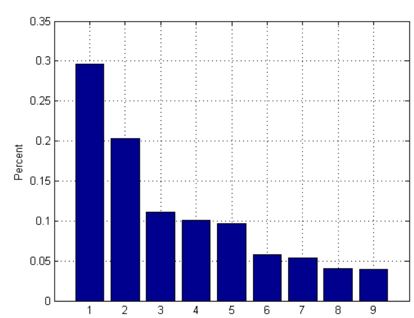

Figura 4: *Previsão de probabilidade de cada digito pela Lei de Benford*

A lei de Benford é um conceito que foi criado por Frank Benford, em 1939, e refere-se à distribuição de frequência dos primeiros digitos de números. Mais precisamente, é observado (dados experimentais) que em vários casos onde os dados variam bastante em termos de ordem de grandeza, a quantidade de números nestes dados que começam com 1 é maior dos que começam com 2 e assim sucessivamente.

Esse conceito é bem contraintuitivo. O resultado esperado seria que todos os digitos tivessem a mesma distribuição nos dados. Existe um site para gastar bastante tempo livre olhando a lei de Benford em ação: `http://www.testingbenfordslaw.com/`. Eles possuem vários bancos de dados variados que mostram como a lei de benford funciona.

A área dos sistêmas dinâmicos que estuda conceitos relacionados a probabilidade e distribuição chama-se teoria ergódica. Este e outros resultados interessantes envolvendo sistemas dinâmicos e teoria dos números pode ser encontrado em [3].

5. Conclusão

Usamos este exemplo como uma forma de introduzir este conteúdo e algumas ferramentas deste para alguém com pouca familiaridade, e para os já familiares com o assunto, oferecemos um fato divertido. Também é um pouco surpreendente como conseguimos traduzir um problema de teoria dos números em estudar o comportamento de rotaçõs no círculo. A dinâmica vai muito além disso, e se você se interessou a aprender mais sobre o assunto, recomendo [2] como um bom livro introdutório (só requer conhecimentos de cálculo).

Todo o conteúdo deste texto, realizado com mais detalhes e mais rigor, está presente no livro de Katok, Hasselblatt [1] (p. 96-98, p,111). A demonstração do fato do começo do texto, onde eu identifico o círculo colando o intervalo $[0, 1)$ e que esta colagem preserva distâncias é feita com detalhes também neste livro.

Referências

[1] Boris Hasselblatt Anatole Katok. *Introduction to the Modern Theory of Dynamical Systems (Encyclopedia of Mathematics and its Applications)*. Cambridge University Press, 1996.

[2] Robert L. Devaney. *An Introduction to Chaotic Dynamical Systems, 2nd Edition*. Westview Press, 2003.

[3] Thomas Ward Manfred Eisiedler. *Ergodic Theory with a view towards Number Theory*. Springer, 2011.