Variações sobre o Teorema de Recorrência de Poincaré

Etienne Ghys

UMPA ENS-Lyon

Tradução de ***Paulo Sad (IMPA)*** [1]

Henri Poincaré é o fundador da teoria dos sistemas dinâmicos[2]. Face à impossibilidade de resolver explicitamente as equações diferenciais que governam as trajetórias dos planetas, ele desenvolveu um ambicioso programa que procurava descrever *qualitativamente* o movimento dos corpos celestes. Em sua famosa memória de 1890 ([8]), *Sobre o problema dos três corpos e as equações da dinâmica* [3], ele demonstrou um teorema surpreendente. Mais adiante daremos um enunciado preciso desse teorema, mas preferimos citar diretamente a análise que H. Poincaré faz dos seus próprios trabalhos ([11]):

> "Não me foi possível resolver rigorosa e completamente o problema da estabilidade do sistema solar, entendendo essa palavra num sentido estritamente matemático. O emprego de invariantes integrais permitiu-me, no entanto, obter certos resultados parciais, sobretudo quando aplicados ao problema conhecido como restrito, em que os dois corpos principais evoluem em órbitas sem excentricidade e influenciam o movimento de um terceiro corpo de massa negligenciável. Neste caso, deixando de lado certas trajetórias excepcionais, cujo aparecimento é infinitamente pouco provável, pode-se demonstrar que *o sistema voltará uma infinidade de vezes tão próximo quanto desejarmos da sua posição inicial*. Trata-se do que chamei estabilidade segundo Poisson."

Dois artigos de divulgação que apareceram em *Pour la Science* ([5]) e *Science et Vie* ([3]) descrevem esse teorema por meio de um exemplo onde *se enxerga* uma recorrência de modo impressionante. No exemplo, aplica-se uma determinada transformação a uma reprodução fotográfica de H. Poincaré e itera-se o procedimento. Pouco resta do grande homem a partir da terceira iteração mas, de modo miraculoso, depois de 241 iterações, temos H. Poincaré de volta sem que falte um só fio de sua barba! Nós reproduzimos esse resultado no fim deste artigo[4].

Trataremos de explicar aqui por que tal exemplo, mesmo tão inesperado, *de modo algum* ilustra o teorema de Poincaré! O fenômeno é, na verdade, o resultado de uma série de pequenos "milagres" de natureza aritmética que analisaremos. Esperamos assim ter uma melhor compreensão do *verdadeiro* teorema de Poincaré e de suas limitações. De passagem, encontraremos algumas questões abertas que talvez alguns leitores tenham prazer em atacar.

O Teorema de Recorrência de Poincaré

Na prática, lidaremos com um caso bastante particular do teorema, suficiente para nossos propósitos.

Seja C o quadrado $[0,1] \times [0,1]$ (o qual em breve será a tela de um computador...). Colando os lados opostos de C obtém-se um toro T. Dito de outro modo, T é obtido a partir de C quando se identifica, para cada $t \in [0,1]$, os pontos $(0,t)$ e $(1,t)$, bem como $(t,0)$ e $(t,1)$. Pode-se também pensar em T como o quociente do plano $\mathbb{R}^2$ pela rede $\mathbb{Z}^2$ dos pontos de coordenadas inteiras, isto é, identificamos (x,y) com (x',y') se a sua diferença possuir coordenadas inteiras. O toro T torna-

[1] *N. do E.* Este artigo foi originalmente publicado no *Le journal de maths des élèves de l'École normale supérieure de Lyon*, em 1994, publicação encerrada cujo conteúdo pode ser encontrado no endereço *www.umpa.ens-lyon.fr/JME/*.

[2] Entre outros...

[3] Agraciada com o prêmio de Sua Majestade o Rei Oscar II da Suécia.

[4] Sem a amável permissão das mencionadas revistas.

se um espaço métrico de forma natural, definindo-se a distância entre dois pontos como o mínimo das distâncias entre os diversos pontos de $\mathbb{R}^2$ que os representam.

Seja $F : \mathbb{R}^2 \to \mathbb{R}^2$ um homeomorfismo que preserva área, isto é, a área de qualquer domínio $\Omega \subset \mathbb{R}^2$ é igual àquela de $F(\Omega)$. Quando F é um difeomorfismo, isto é o mesmo que dizer que o determinante de sua matriz jacobiana é igual a ± 1 em cada ponto. Suponhamos também que F passa ao quociente como um homeomorfismo de T. Dito de outro modo, F e sua inversa levam pontos de $\mathbb{R}^2$ que diferem por um elemento da rede $\mathbb{Z}^2$ em pontos que também diferem por um elemento da mesma rede. Obtém-se, deste modo, um homeomorfismo f do toro T que preserva área de modo mais ou menos evidente.

Sendo k um inteiro positivo, denotamos por f^k a composição $f \circ \cdots \circ f$, k vezes, do homeomorfismo f. A *órbita* de um ponto $a \in T$ é a sequência $(a_k)_{k\geq 0}$ definida por $a_k = f^k(a)$. Estudar a dinâmica de f significa descrever o comportamento assintótico dessas órbitas quando o "tempo" k tende a infinito. Diz-se que $a \in T$ é *recorrente* quando é ponto de acumulação de sua órbita.

Teorema (Poincaré, 1890)**.** *O conjunto de pontos recorrentes de um homeomorfismo do toro que preserva área é denso no toro.*

Demonstração. Se n é um inteiro positivo, diremos que um ponto $a \in T$ é $1/n$*-recorrente* se existe um inteiro k estritamente positivo de modo que a distância (em T) entre a e $f^k(a)$ é estritamente inferior a $1/n$. O conjunto de pontos $1/n$-recorrentes é um aberto $R_n \subset T$ e sua intersecção infinita é o conjunto de pontos recorrentes de f. Pelo teorema de Baire, é suficiente mostrar que R_n é um aberto denso para todo n.

A ideia da prova é muito simples. Seja Ω uma bola aberta de T de raio inferior a $1/(2n)$ e consideremos a sequência $f^k(\Omega)$ de abertos com $k \geq 0$. Todos esses abertos iterados possuem a mesma área, de modo que não podem ser dois a dois disjuntos devido à finitude da área total de T. Existem, portanto, dois inteiros k_1 e k_2 com $0 \leq k_1 < k_2$ de modo que $f^{k_1}(\Omega)$ e $f^{k_2}(\Omega)$ não são disjuntos. Tomando $k = k_2 - k_1$, temos então que $\Omega \cap f^k(\Omega)$ não é vazio. Isto significa precisamente que a bola Ω, qualquer que seja ela, contém ao menos um ponto $1/n$-recorrente e, portanto, R_n é denso em T. Isto demonstra o teorema. □

Algumas observações devem ser feitas.

- Utilizamos o teorema de Baire, uma dezena de anos mais novo que o de Poincaré! Sugerimos ao leitor que leia os artigos de Poincaré ([8, 10]) para encontrar o enunciado original.

- Seria fácil mostrar que o conjunto de pontos não recorrentes é de medida de Lebesgue nula (ver, por exemplo, [6]). Poincaré não tinha a teoria geral de medida à disposição, mas suas ideias eram claras! Ele escreve em [9]: "(...) pode-se dizer que as [trajetórias não recorrentes] são a exceção e que as [trajetórias recorrentes] são a regra, do mesmo modo que os números racionais são a exceção e os irracionais, a regra. Demonstro, com efeito, que a probabilidade de selecionar as condições iniciais do movimento que resultem em uma solução instável [não recorrente] é nula. Dita deste modo, a afirmativa talvez não faça muito sentido: em minha Memória, apresento uma definição precisa[5]".

- Ser f um homeomorfismo do toro não tem nenhuma importância. Em geral, dispomos de um espaço X, que pode ser o espaço de fases de um sistema mecânico, e de um homeomorfismo f de X que envia cada posição inicial na posição um segundo mais tarde, por exemplo. A mecânica clássica nos ensina que, em numerosos casos, X é uma "variedade simplética", mas para nós o que interessa é que existe uma noção de volume em X e que o homeomorfismo f preserva esse volume (teorema de Liouville). O teorema de Poincaré se generaliza nesse contexto, uma vez que a hipótese crucial (mas bastante geral) é verificada: a finitude do volume total de X. Para outras informações, ver [1].

[5] A "precisão" de que se trata aqui é certamente a de Poincaré e não tem muito a ver com aquela de Bourbaki.

O exemplo de *Pour la Science* e *Science et Vie*

Seja Φ a aplicação linear de $\mathbb{R}^2$ cuja matriz é

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Trata-se de um difeomorfismo que preserva área pois o determinante da matriz é -1. Por outro lado, Φ leva injetivamente a rede de pontos de coordenadas inteiras em si mesma, visto que os coeficientes de Φ e de sua inversa são inteiros. Por passagem ao quociente, Φ define um difeomorfismo de T que preserva área, o qual continuaremos a denotar por Φ, sem grande perigo de confusão.

Esse exemplo é de grande importância na teoria de sistemas dinâmicos, apesar da extrema simplicidade da sua definição. Em certo sentido, é muito mais que um exemplo.

Teorema (Anosov, 1967)**.** *Seja Ψ um difeomorfismo de T próximo de Φ na topologia C^1.* [6] *Existe, então, um homeomorfismo h do toro T tal que*

$$\Psi = h \circ \Psi \circ h^{-1}.$$

Para uma demonstração, consultar [2].

Isto significa que os difeomorfismos próximos de Φ são "os mesmos" que Φ, a menos de uma mudança de coordenadas por um homeomorfismo. Se compreendemos a estrutura de Φ, compreendemos também, de imediato, a estrutura de um aberto do grupo de difeomorfismos de T. Trata-se da famosa *estabilidade estrutural*, presente em tantos trabalhos nos últimos 30 anos. O leitor provavelmente adivinhou que o resultado é bem mais geral que o enunciado apresentado acima; em particular, ele continuará válido se trocarmos Φ por outra matriz 2×2, com coeficientes inteiros e de determinante ± 1, contanto que não haja autovalores de módulo 1.

Apliquemos o teorema de recorrência de Poincaré a Φ: quase todos os pontos de T são recorrentes. Nos artigos de *Pour la Science* e *Science et Vie* toma-se uma reprodução do rosto de Poincaré dentro do quadrado $[0,1] \times [0,1]$ utilizado na construção[7] do toro T, depois itera-se essa imagem por Φ. Após 241 iterações, produz-se o milagre: Poincaré está de volta! Será que este comportamento está previsto pelo teorema de recorrência?

Por que o exemplo surpreende?

É certamente a rapidez do retorno de Poincaré que é surpreendente. O teorema de recorrência não indica o valor provável do tempo de retorno, mas podemos estimá-lo heuristicamente de modo simples. Se Ω é um aberto não vazio de T, vimos que o argumento essencial da prova consiste na impossibilidade de todos os $\Phi^k(\Omega)$ serem disjuntos. De fato, não podemos encontrar em T senão um número inferior a $\acute{a}rea(T)/\acute{a}rea(\Omega)$ de abertos disjuntos de área igual a $\acute{a}rea(\Omega)$. Portanto, podemos esperar um tempo de retorno da ordem de $\acute{a}rea(T)/\acute{a}rea(\Omega)$. Isto é de fato um teorema, sob uma hipótese técnica, a ergodicidade[8], que é satisfeita em nosso caso:

Teorema (Kač, 1947)**.** *Seja f um homeomorfismo do toro T que preserva área e é ergódico. Seja $\Omega \neq \emptyset$ um aberto não vazio e denotemos, para cada $a \in \Omega$, $u(a)$ como sendo o menor inteiro não nulo k tal que $f^k(a) \in \Omega$. Então o valor médio de u em Ω é*

$$\frac{1}{\acute{a}rea(\Omega)} \int u(a)d(a) = \frac{\acute{a}rea(T)}{\acute{a}rea(\Omega)}.$$

Apliquemos esse teorema ao rosto de Poincaré. Claro, foi preciso discretizar a imagem e substituí-la por um número finito de pontos (os "pixels"), e foram esses os pontos iterados. Suponhamos, então, o quadrado substituído pelo conjunto finito de N^2 elementos formados pelos pontos $(i/N, j/N)$, com $1 \leq i \leq N$ e $1 \leq j \leq N$. Cada pixel corresponde a um pequeno quadrado que recobre uma proporção de $1/N^2$ do grande quadrado $[0,1] \times [0,1]$. Segundo o teorema precedente, esperamos que um pixel retorne a seu lugar após um

[6] Os difeomorfismos f_1 e f_2 do toro são C^1-próximos se provêm de dois difeomorfismos F_1 e F_2 de $\mathbb{R}^2$ tais que $F_1 - F_2$ é pequeno juntamente com suas derivadas parciais de primeira ordem.

[7] No exemplo, a origem do sistema de coordenadas está no centro da tela do computador: o nariz de Poincaré é um ponto fixo.

[8] Diz-se que um homeomorfismo do toro é ergódico se todo conjunto boreliano invariante ou possui medida de Lebesgue nula ou seu complemento possui medida de Lebesgue nula. O leitor corajoso poderá mostrar que Φ é ergódico, de modo que o teorema se aplica (bem, em caso de pane, consultar [2] e [7]).

número de iterações da ordem de N^2. Se tomarmos, por exemplo, $N = 1000$, o tempo de retorno de um pixel será próximo de um milhão, bastante maior do que 241!

E isto não é tudo! Se cada pixel retorna mais ou menos depois de um milhão de iterações, os tempos de retorno variam provavelmente de um pixel a outro. O tempo de retorno da imagem completa é, portanto, o M.M.C. de um milhão de inteiros. Estes, por sua vez, são também da ordem de um milhão. Logo, a imagem deveria requerer um tempo muito grande antes de retornar...

Para ilustrar esse fenômeno, citaremos alguns resultados combinatórios a respeito das permutações de um conjunto finito E_M com M elementos (mais tarde faremos $M = N^2$). O número de permutações de tal conjunto é $M!$, e é bem conhecido que uma permutação σ é um produto de ciclos disjuntos. Se um ponto a pertence a E_M, o período de a sob a ação de σ é o comprimento do ciclo de σ que contém a. O período da permutação, isto é, sua ordem dentro do grupo simétrico de todas as permutações, é o M.M.C. dos comprimentos dos ciclos que a constituem. Pode-se, então, tentar estimar as médias aritméticas dessas quantidades sobre o conjunto das $M!$ permutações de E_M. Seguem-se os resultados (consulte [4], onde se encontram também muitas referências e complementos):

Teorema. *Quando M tende a infinito,*

1. *o valor médio do período de uma permutação de um conjunto com M elementos é equivalente a $M^{\log M/2}$, e*
2. *o valor médio do comprimento do maior ciclo de uma permutação de um conjunto com M elementos é equivalente a $0,62432965\ldots M$.*

Quando M é igual a um milhão, o teorema precedente fornece um valor tão grande para a média da ordem de uma permutação que perdemos a esperança de recuperar Poincaré!

Ainda pior: quando discretizamos um homeomorfismo f em um conjunto finito E_M com M elementos, obtemos uma aplicação $\bar{f}_M$ de E_M em si mesmo que não é, necessariamente, uma bijeção. Dois pixels a e b podem ser diferentes, mas suas imagens por f podem estar de tal modo próximas que acabam identificadas em E_M. Assim o computador itera, de fato, uma aplicação não necessariamente bijetiva de um conjunto finito em si mesmo.

Vamos introduzir, agora, algumas noções elementares relativas à estrutura de uma aplicação $\bar{f}$ de um conjunto finito E em si mesmo. Para cada inteiro positivo k, seja $E(k)$ a imagem $\bar{f}^k(E)$. Definimos, assim, uma sequência decrescente de partes de E, a qual, portanto, se torna estacionária porque E é finito. Seja R a intersecção dos $E(k)$: é um subconjunto invariante por $\bar{f}$ e a restrição de $\bar{f}$ a R é uma bijeção. Diremos que R é a *parte recorrente* de E e o complemento de R em E é a *parte errante*. Afirmar que um ponto $a \in E$ está na parte recorrente ou errante depende de que sua órbita $\bar{f}^k(a)$ passe ou não novamente por a. Definimos o *grau de recorrência* de $\bar{f}$ como o quociente entre os cardinais da parte recorrente e de E. Em [4] encontramos o teorema seguinte:

Teorema. *Quando M tende a infinito,*

1. *a média do grau de recorrência entre as M^M aplicações de um conjunto com M elementos em si mesmo é igual a $\sqrt{\frac{\pi}{2M}}$, e*
2. *o número médio de ciclos da restrição à parte recorrente é igual a $\log M$.*

Em outras palavras, uma aplicação "aleatória" de um conjunto com um milhão de elementos tem, em média, uma parte recorrente contendo pouco mais de um milhar de elementos distribuídos em uma dezena de ciclos. A vasta maioria dos pontos não volta jamais à sua posição original quando iteramos a aplicação. Mais uma razão para duvidarmos do retorno do rosto de Poincaré...

Porque o exemplo é muito particular

Primeiro milagre. *O conjunto finito E_{N^2}, formado pelos pontos $(i/N, j/N)$, com $1 \leq i \leq N$ e $1 \leq j \leq N$, e utilizado na discretização, é um conjunto invariante por Φ.*

De fato, a aplicação linear Φ preserva tanto a rede $\mathbb{Z}^2$ como também todas as redes $\frac{1}{N}\mathbb{Z}^2$. A discretização de Φ é, portanto, uma bijeção de E_{N^2}, e já observamos que se trata de uma propriedade muito particular.

Se conjugarmos Φ por um homeomorfismo do toro escolhido ao acaso, o novo homeomorfismo assim obtido em geral não preserva mais o conjunto E_{N^2}, e a discretização deixa de ser bijetiva.

Segundo milagre. *A permutação induzida por Φ no conjunto E_{N^2} é muito particular e sua ordem é bem menor que a ordem $(N^2)^{\log N}$ esperada (por exemplo, para $N^2 = 10^6$ esperamos algo como 10^{41}).*

Antes de justificar essa afirmativa, introduziremos uma notação. Sendo $\mathcal{A}$ um anel comutativo com unidade, denotemos por $GL(2, \mathcal{A})$ o grupo de matrizes 2×2 com coeficientes em $\mathcal{A}$ e de determinante inversível. Esse grupo age naturalmente por aplicações "lineares" em $\mathcal{A} \times \mathcal{A}$.

Em particular, podemos considerar $GL(2, \mathbb{Z})$ e $GL(2, \mathbb{Z}/N\mathbb{Z})$, com o consequente homomorfismo induzido pela redução módulo N:

$$\rho_N : GL(2, \mathbb{Z}) \to GL(2, \mathbb{Z}/N\mathbb{Z}) .$$

O conjunto E_{N^2} de discretização certamente se identifica com $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ e a ação de Φ sobre esse conjunto é simplesmente aquela de $\rho_N(\Phi)$ agindo em $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ (identificamos o difeomorfismo Φ com a matriz 2×2 que o define). A ordem da restrição de Φ a E_{N^2} é, portanto, a ordem de Φ dentro do grupo finito $GL(2, \mathbb{Z}/N\mathbb{Z})$. Assim obtemos uma estimativa, grosseira mas eficaz, dessa ordem; ela é majorada pelo cardinal desse grupo finito, o qual é evidentemente inferior a N^4. Ainda não compreendemos por que o número 241 é tão pequeno. No entanto, pelo menos agora temos uma cota superior da ordem de 10^{12}, mais razoável do que 10^{41}.

Terceiro milagre. *A ordem dos elementos de $GL(2, \mathbb{Z}/N\mathbb{Z})$ é, de fato, bem menor que a cota anterior N^4.*

Para simplificar, trabalharemos no subgrupo $SL(2, \mathbb{Z}/N\mathbb{Z})$ das matrizes de determinante 1. Observemos que a matriz Φ não está nesse grupo, e sim o seu quadrado.

Teorema. *A ordem de um elemento de $SL(2, \mathbb{Z}/N\mathbb{Z})$ é inferior ou igual a $3N$.*

A demonstração seguinte é, talvez, um pouco técnica. O leitor assustado pode simplesmente ignorá-la, sem prejuízo da compreensão do que se segue.

Demonstração. Seja A um elemento do grupo $SL(2, \mathbb{Z}/N\mathbb{Z})$. Vamos distinguir vários casos.

Primeiro caso. Suponhamos inicialmente N primo (denotando-o, obviamente, por p). Os dois autovalores de A ou estão em $\mathbb{Z}/p\mathbb{Z}$ ou em um corpo F_{p^2} que é uma extensão quadrática[9] de $\mathbb{Z}/p\mathbb{Z}$.

1. Suponhamos que A seja diagonalizável sobre o corpo finito $\mathbb{Z}/p\mathbb{Z}$ de p elementos. Como os dois autovalores são inversos um do outro, a ordem de A como elemento de $SL(2, \mathbb{Z}/p\mathbb{Z})$ é, portanto, igual à ordem de um desses autovalores no grupo multiplicativo constituído pelos elementos não nulos de $\mathbb{Z}/p\mathbb{Z}$. É um divisor de $p - 1$ e, claro, inferior a $3p$.

2. Suponhamos agora que os autovalores de A estejam não mais em $\mathbb{Z}/p\mathbb{Z}$, mas em F_{p^2}. Os dois autovalores λ_1 e λ_2 de A são intercambiados pelo automorfismo de Frobenius

$$x \in F_{p^2} \mapsto x^p \in F_{p^2} .$$

   Portanto, $\lambda_2 = \lambda_1^p$ e $\lambda_1^{p+1} = 1$, pois o determinante de A vale 1. Resulta que a ordem de A divide $p + 1$ e é, em particular, inferior a $3p$.

3. Se a matriz A não é diagonalizável em $\mathbb{Z}/p\mathbb{Z}$ nem em F_{p^2}, então os dois autovalores de A são iguais e valem ± 1.

   - Se a matriz A é unipotente (isto é, se os dois autovalores são iguais a 1), então ela é conjugada a uma matriz da forma

$$\begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix} ,$$

     com $v \in \mathbb{Z}/p\mathbb{Z}$. A ordem de tal matriz é 1 ou p, portanto inferior a $3p$.
   - Se os dois autovalores de A são iguais a -1, então $-A$ é unipotente e a ordem de A divide $2p$, logo é inferior a $3p$.

[9] Em caso de necessidade, consulte [12].

Segundo caso. Suponhamos agora que N seja uma potência p^n de um número primo e demonstremos o teorema por indução em n. O caso $n = 1$ acaba de ser verificado; suponhamos o teorema demonstrado até n. Por redução módulo p^n, temos um homomorfismo

$$\rho : SL(2, \mathbb{Z}/p^{n+1}\mathbb{Z}) \to SL(2, \mathbb{Z}/p^n\mathbb{Z}) .$$

Devido à hipótese de indução, sabemos que a ordem de um elemento de $SL(2, \mathbb{Z}/p^n\mathbb{Z})$ é inferior a $3p^n$ e, portanto, é suficiente mostrar que a ordem de um elemento do núcleo de ρ é 1 ou p. Esse núcleo é constituído por matrizes da forma

$$Id + p^n B ,$$

de modo que sua p-ésima potência é a identidade em $SL(2, \mathbb{Z}/p^{n+1}\mathbb{Z})$.

Terceiro caso. Resta-nos agora mostrar que, sendo o teorema válido para os inteiros $p_1^{n_1}, \ldots, p_\ell^{n_\ell}$ dois a dois primos entre si, então também é válido para o produto $N = p_1^{n_1} \ldots p_\ell^{n_\ell}$. Utilizando as reduções módulo $p_1^{n_1}, \ldots, p_\ell^{n_\ell}$, definimos um homomorfismo de $SL(2, \mathbb{Z}/N\mathbb{Z})$ no produto dos $SL(2, \mathbb{Z}/p_i^{n_i}\mathbb{Z})$; o "Teorema Chinês dos Restos" garante que se trata de um isomorfismo. Portanto, a ordem de um elemento de $SL(2, \mathbb{Z}/N\mathbb{Z})$ é o M.M.C. das ordens das componentes de sua imagem no produto dos $SL(2, \mathbb{Z}/p_i^{n_i}\mathbb{Z})$. O *segundo caso* nos mostra que a ordem de um elemento de $SL(2, \mathbb{Z}/p^n\mathbb{Z})$ é, de fato, de uma das formas seguintes:

- αp^β, em que α divide $(p-1)$ e $0 \leq \beta \leq n-1$,
- αp^β, em que α divide $(p+1)$ e $0 \leq \beta \leq n-1$,
- p^β, em que $\beta \leq n$,
- $2p^\beta$, em que $\beta \leq n$.

Se p é um número ímpar, $p+1$ é par! Se $p \neq 2$ essa ordem é inferior ou igual a p^n ou é o dobro de um inteiro inferior ou igual a p^n. Segue-se facilmente que, se N é ímpar, isto é, se todos os p_i são diferentes de 2, então o M.M.C. das diversas ordens módulo os $p_i^{n_i}$ é menor ou igual a $2N$.

Se $N = 2^n$, a ordem é inferior ou igual a $3 \times 2^{n-1}$, ou seja, $\frac{3N}{2}$ (verifique por que a quarta possibilidade acima foi excluída).

No caso geral, N é o produto de uma potência de 2 e de um número ímpar, de modo que a ordem módulo N é majorada por $(\frac{3}{2} \times 2)N = 3N$, e o teorema está demonstrado.

Observemos que a cota obtida é optimal. Por exemplo, pode-se encontrar um elemento de $SL(2, \mathbb{Z}/10\mathbb{Z})$ que é de ordem 3 módulo 2 e de ordem $10 = (2 \times 5)$ módulo 5, portanto de ordem $30 = (3 \times 10)$ módulo 10. □

Observação 1. Fixemos uma matriz $A \in SL(2, \mathbb{Z})$ e um número primo p. Não é difícil convencer-se de que existem inteiros α e β tais que, *para todo n suficientemente grande*, a ordem da projeção de A em $SL(2, \mathbb{Z}/p^n\,\mathbb{Z})$ é exatamente $\alpha\, p^{n-\beta}$. Assim, quando n tende a infinito, a ordem de A módulo p^n é comparável a p^n. Para a "maioria" dos inteiros N (não necessariamente potências de um número primo), pode-se pensar que a ordem de A módulo N tem a mesma ordem de grandeza que N. Deixamos ao leitor a tarefa de dar sentido claro a esta afirmação e verificar se ela é exata! De qualquer modo, se $N \sim 1000$, temos agora uma cota de 3000 para a ordem de um elemento de $\mathbb{Z}/N\mathbb{Z}$ e, em casos numerosos, essa cota é excessiva. Portanto, o nosso número 241 começa a parecer razoável!

Quarto milagre. *Existe uma sequência de inteiros $(\phi)_{k\geq 0}$, tendendo a infinito (exponencialmente) quando k tende a infinito, tal que se discretizarmos o monitor do computador em $\phi_k \times \phi_k$ pontos, então o retorno de H. Poincaré se produz* exatamente *após* $2k$ *iterações...*

É claro que escolher a discretização em função do tempo de retorno desejado é um pouco de trapaça. Mas isto mostra bem o caráter ilusório dessas recorrências. A qualidade de tais discretizações é excelente pois, como veremos, para retornos após 106, 238, 240, 242 ou 246 iterações:

$$\begin{aligned}
\phi_{53} &= 119218851371 \\
\phi_{119} &= 740507036646495126456359 9 \\
\phi_{120} &= 535835925499096664087184 0 \\
\phi_{121} &= 193867259084898819397956 01 \\
\phi_{132} &= 507551073590046945548232 04 .
\end{aligned}$$

Constatamos, em particular, que esses números são bem superiores à precisão dos melhores monitores de computador (que são da ordem de 1000×1000).

Para justificar tais afirmações, introduzimos duas sequências de Fibonacci a_k e b_k definidas por

$$a_0 = 0\,,\ a_1 = 1\,,\ a_{k+2} = a_{k+1} + a_k$$
$$b_0 = 2\,,\ b_1 = 1\,,\ b_{k+2} = b_{k+1} + b_k$$

para $k \geq 0$, e definimos a sequência ϕ_k por

$$\phi_{2k} = a_{2k} \qquad \phi_{2k+1} = b_{2k+1}\,.$$

É facil ver que ϕ_k tende exponencialmente a infinito quando k tende a infinito.

Teorema. *A $2k$-ésima potência de Φ é congruente à identidade módulo ϕ_k.*

Demonstração. Pelo Teorema de Hamilton-Cayley (para matrizes 2×2!) temos que

$$\Phi^2 = \Phi + \mathrm{Id}\,.$$

Resulta que

$$\Phi^{-2} = -\Phi^{-1} + \mathrm{Id}\,.$$

Logo, para todo inteiro k,

$$\Phi^{k+2} = \Phi^{k+1} + \Phi^k$$

e

$$\Phi^{-(k+2)} = -\Phi^{-(k+1)} + \Phi^{-k}\,.$$

Para cada k, façamos

$$A_k = \Phi^k - (-1)^k\,\Phi^{-k}\,,\ B_k = \Phi^k + (-1)^k\,\Phi^{-k}\,.$$

Portanto, para todo inteiro k,

$$A_{k+2} = A_{k+1} + A_k\,,\ B_{k+2} = B_{k+1} + B_k\,.$$

Por outro lodo, obtemos facilmente

$$A_0 = 0\,,\ A_1 = \Phi + \Phi^{-1}\,,$$
$$B_0 = 2\,\mathrm{Id}\,,\ B_1 = \Phi - \Phi^{-1} = \mathrm{Id}\,.$$

Assim, por recorrência, chegamos às expressões

$$A_k = a_k\,(\Phi + \Phi^{-1})\,,\ B_k = b_k\,\mathrm{Id}\,.$$

Finalmente,

$$\Phi^{4k} - \mathrm{Id} = (\Phi^{2\,k} - \Phi^{-2\,k})\Phi^{2\,k} = a_{2\,k}\,(\Phi + \Phi^{-1})\Phi^{2\,k}$$
$$\Phi^{4k+2} - \mathrm{Id} = (\Phi^{2\,k+1} - \Phi^{-2\,k-1})\Phi^{2\,k+1} = b_{2\,k+1}\,\Phi^{2k+1}\,.$$

Mostramos então que $\Phi^{2\,k} - \mathrm{Id}$ é divisível por ϕ_k. □

Observação 2. As potências ímpares de Φ não apresentam esse fenômeno de alta recorrência encontrado para as potências pares. A matriz Φ, por ter determinante -1, reverte orientação[10]. Torna-se necessário elevar Φ a uma potência par para obter um "retorno orientado"! Mais precisamente, se a matriz inteira Φ^{2k+1} é igual a Id módulo um certo inteiro ℓ, comparando os determinantes obtemos que $\ell = \pm 1$ ou $\ell = \pm 2$. É por este motivo que pensamos que a recorrência apresentada em *Pour la Science* e em *Science et Vie* não se produz após 241 iterações e que possivelmente existe um erro de uma unidade na contagem dos iterados (a primeira figura correspondendo à iteração de ordem zero). A recorrência se produz certamente na 240-ésima iteração!

Resta compreender o valor 240, mesmo tendo claro agora que ele é necessariamente artificial. Uma explicação possível vem da constatação seguinte. Quando decompomos os inteiros ϕ_k em fatores primos (usando MAPLE por exemplo), observamos que aparecem números primos quase todos extremamente grandes, com a notável exceção de ϕ_{120}. Por exemplo, nos casos escolhidos anteriormente:

$$\begin{aligned}
\phi_{53} &= 119218851371\\
\phi_{119} &= 29 \times 239 \times 10711 \times 3571 \times 27932732439809\\
\phi_{120} &= 2^5 \times 3^2 \times 5 \times 7 \times 11 \times 23 \times 31\\
&\quad \times 41 \times 61 \times 241 \times 2161 \times 2521 \times 20641\\
\phi_{121} &= 199 \times 97420733208491869044199\\
\phi_{123} &= 2^2 \times 4767481 \times 370248451 \times 7188487771\,.
\end{aligned}$$

Os fabricantes de computadores têm a tendência natural a escolher os tamanhos dos monitores utilizando inteiros que são produtos de pequenos inteiros como 2, 3 ou 5, e parece, finalmente, ser esta propriedade de ϕ_{120} que está por trás do fenômeno de retorno após 120 iterações... Por outro lado, não se trata de uma surpresa realmente. O polinômio $X^{2k} - 1$ é o produto de polinômios ciclotômicos indexados pelos divisores de $2k$, de modo que, se $2k$ tem muitos divisores (como 120), então é o caso também de $A^{2k} - \mathrm{Id}$.

Terminamos este parágrafo com uma observação. Se examinarmos atentamente a fotocópia ruim anexada ao fim deste artigo, constatamos um estranho fenômeno:

[10] Na fotografia inicial, vemos a orelha *esquerda* do Mestre, ao passo que em sua transformação por Φ o que vemos é uma orelha *direita*, mesmo que deformada.

após 48 iterados vemos aparecer 5 faces de H. Poincaré deslocadas entre si. Deixamos ao leitor o prazer de procurar a explicação. Simplesmente observamos que:

- $240 = 5 \times 48$.
- $\phi_{24} = 43368 = 2^5 \times 3^2 \times 7 \times 23$ (portanto 5 divide ϕ_{120}, mas não ϕ_{24}).
- o discriminante do polinômio $X^2 - X - 1$ é 5, de modo que a redução módulo 5 de ϕ tem um autovalor duplo (e 5 é o único primo com tal propriedade).

Uma questão

O espaço de todos os homeomorfismos do toro que preservam área pode ser munido (por exemplo) da topologia da convergência uniforme. Diremos que uma propriedade de um homeomorfismo é *genérica* se o conjunto de homeomorfismos que a satisfazem é residual no sentido de Baire (isto é, uma intersecção enumerável de abertos densos). O problema que propomos agora ao leitor é o de saber em que medida um computador é capaz de detectar a dinâmica genérica de um homeomorfismo. Precisemos a questão.

Se N é um inteiro positivo, tomemos novamente E_{N^2} como o conjunto de pontos do toro de coordenadas $(i/N, j/N)$, com $1 \leq i \leq N$ e $1 \leq j \leq N$. Sejam f um homeomorfismo do toro que preserva área e

$$\bar{f}_N : E_{N^2} \to E_{N^2}$$

a *discretização de ordem* N, isto é, a aplicação que leva um ponto de E_{N^2} no ponto de E_{N^2} mais próximo de sua imagem por f (genericamente único). Seja $r_N(f)$ o grau de recorrência de $\bar{f}_N$.

Problema. *Podemos descrever o comportamento assintótico da sequência $r_N(f)$, quando N tende a infinito, para um homeomorfismo genérico do toro que preserva área?*

Na verdade, a discretização de um homeomorfismo genérico não é uma aplicação qualquer de um conjunto de N^2 elementos em si mesmo: a continuidade de f provoca uma "espécie de continuidade fraca para $\bar{f}_N$ no conjunto E_{N^2}". Portanto, não é claro que a estimativa do grau de recorrência que descrevemos anteriormente, do tipo $\frac{\sqrt{\pi/2}}{N}$, seja válida para $r_N(f)$. Se essa estimativa (ou alguma outra um pouco pior) fosse válida para um homeomorfismo genérico, poderíamos nos colocar questões sobre o uso da informática em sistemas dinâmicos...

A mistura

Para terminar, citaremos um resultado que liquida a esperança de haver recorrência quando substituímos pontos por figuras (veja [7] para mais informações). De fato, enquanto quase todos os pontos são recorrentes, as figuras possuem uma tendência à mistura.

Teorema. *Sejam Ω_1 e Ω_2 dois borelianos do toro T. Então a área da intersecção $\Phi^k(\Omega_1) \cap \Omega_2$ tende ao produto das áreas de Ω_1 e Ω_2 quando o inteiro k tende a infinito.*

Demonstração. Sejam u_1 e u_2 as funções indicadoras de Ω_1 e Ω_2, respectivamente. Trata-se de mostrar que

$$\begin{aligned} lim_{k\to\infty} \int_T u_1 \circ \Phi^{-k}(x,y)\, u_2(x,y) dx\, dy \\ = \int_T u_1(x,y) dx\, dy \int_T u_2(x,y) dx\, dy\,. \end{aligned}$$

A fortiori, é suficiente demonstrar esse fato para os pares (u_1, u_2) de funções de T com quadrado integrável. Desenvolvendo u_1 e u_2 em séries de Fourier, recaímos no caso em que u_1 e u_2 são da forma

$$\begin{aligned} u_1(x,y) &= \exp\{2\pi i(m_1\, x + n_1\, y)\} \\ u_2(x,y) &= \exp\{2\pi i(m_2\, x + n_2\, y)\}\,, \end{aligned}$$

em que x e y são elementos de $\mathbb{R}/\mathbb{Z}$ e m_1, m_2, n_1, n_2 são inteiros.

Quando calculamos $u_1 \circ \Phi^{-k}$, obtemos

$$u_1 \circ \Phi^{-k}(x,y) = \exp\{2\pi i\,(m(k)\, x + n(k)\, y)\}$$

com

$$\begin{pmatrix} m(k) \\ n(k) \end{pmatrix} = \left(\Phi^{-k}\right)^t \begin{pmatrix} m_1 \\ n_1 \end{pmatrix}.$$

Se (m_1, n_1) ou (m_2, n_2) é $(0,0)$ então o produto das integrais de $u_1 \circ \phi^{-k}$ e u_2 é certamente constante e a convergência desse produto não é muito difícil...

Se (m_1, n_1) e (m_2, n_2) são diferentes de $(0,0)$, verificamos facilmente para k suficientemente grande que

$(m(k), n(k)) \neq (m_2, n_2)$, de modo que $u_1 \circ \Phi^{-k}$ e u_2 são ortogonais para o produto hermitiano do espaço de Hilbert formado pelas funções de quadrado integrável e, claro, cada uma dessas funções possui integral nula. Aqui também a convergência é simples.... Terminamos assim a prova do teorema. □

O teorema significa que, se iterarmos um pequeno domínio Ω_1 por Φ, ele vai "se distribuir" no toro de maneira uniforme: assintoticamente, a proporção de $\Phi^k(\Omega_1)$ em Ω_2 é a mesma que a de Ω_1 em T. Tudo se embaralha e se turva...

Avec le temps...
Avec le temps, va, tout s'en va
On oublie le visage et l'on oublie la voix
Le cœur quand ça bat plus, c'est pas la peine d'aller
Chercher plus loin, faut laisser faire et c'est très bien
Avec le temps...
Avec le temps, va, tout s'en va
L'autre qu'on adorait, qu'on cherchait sous la pluie
L'autre qu'on devinait au détour d'un regard
Entre les mots, entre les lignes et sous le fard
D'un serment maquillé qui s'en va faire sa nuit
Avec le temps tout s'évanouit.

LÉO FERRÉ[11]

Agradecimentos. Tenho o prazer de agradecer a Christophe Bavard, Patrick Iglesias, Bruno Sevennec e minha filha Elise por suas preciosas ajudas na preparação deste texto.

Referências

[1] ARNOLD, V. *Les méthodes mathématiques de la mécanique classique*. Traduit du russe par Djilali Emaraek. Moscou: Mir, 1976.

[2] ARNOLD, V. *Chapitres supplémentaires de la théorie des équations différentielles ordinaires*. Traduit du russe par Djilali Emaraek. Moscou: Mir, 1980.

[3] BERGER, M. Maths 89: l´école française 3ème du monde. *Science et Vie (hors série): 200 ans de science (1789–1989)*, n. 166, p. 274–283, mars, 1989.

[4] BOLLOBÁS, B. *Random Graphs*. London: Academic Press, 1985.

[5] CRUTCHFIELD, J.; FARMER, D.; PACKARD, N.; SHAW, R. Le Chaos. *Pour la Science*, février, p. 26–50, 1987.

[6] OXTOBY, J.-C. *Measure and Category. A survey of the analogies between topological and measure spaces*. New York: Springer Verlag, 1971. (Graduate Texts in Mathematics, 2)

[7] PETERSEN, K. *Ergodic Theory*. Cambridge: Cambridge University Press, 1983. (Cambridge Studies in Advanced Mathematics, 2)

[8] POINCARÉ, H. Sur le problème des trois corps et les équations de la dynamique. *Acta Mathematica*, v. 13, p. 1–270, 1890.

[9] POINCARÉ, H. Sur le problème des trois corps. *Bulletin Astronomique*, v. 8, p. 12–24, 1891.

[10] POINCARÉ, H. *Les méthodes nouvelles de la mécanique céleste*. Paris: Gauthier-Villars, 1899. Tome 3.

[11] POINCARÉ, H. Analyse des travaux scientifiques. *Oeuvres de Henri Poincaré*. Paris: Gauthier-Villars, 1952. Tome 7.

[12] SERRE, J.-P. *Cours d´arithmétique*. Paris: Presses Universitaires de France, 1970.

Etienne Ghys (ghys@umpa.ens-lyon.fr)
UMPA ENS-Lyon
46, allée d'Italie
69364 Lyon cedex 7

[11] *N. do T.* Poeta e músico franco-monegasco. Deixamos para o leitor a tradução desse trecho da canção "Avec le temps".


0
1
2
3
4
5
7
10
19
47
48
237
239
240
241