RMU

REVISTA MATEMÁTICA UNIVERSITÁRIA

ISSN: 2675-5254

Ano 2021, Volume 2

Índice

SBM

SOCIEDADE BRASILEIRA DE MATEMÁTICA

SOBRE A RMU

A Matemática Universitária é uma publicação da Sociedade Brasileira de Matemática semestral de divulgação de ideias e estímulos ao estudo e à curiosidade intelectual, dirigida a todos que se interessam pelo ensino e estudo da Matemática em nível Superior. É direcionada a professores, pesquisadores, alunos de graduação e pós graduação, promovendo e fortalecendo o intercâmbio entre os membros dessa comunidade.

ISSN
2675–5254l

Periodicidade
Semestral

Contato

Endereço:
Sociedade Brasileira de Matemática
Estrada Dona Castorina, 110 sala 109
Jardim Botânico
22460-320 Rio de Janeiro – RJ
Email: `rmu@sbm.org.br`
Página web: `https://rmu.sbm.org.br/`

RMU
REVISTA MATEMÁTICA UNIVERSITÁRIA

SBM
SOCIEDADE BRASILEIRA DE MATEMÁTICA

RMU
REVISTA MATEMÁTICA UNIVERSITÁRIA

SBM
SOCIEDADE BRASILEIRA DE MATEMÁTICA

Revista Matemática Universitária, vol. 2, 2021
ISSN: 2675-5254 — **DOI:** 10.21711/26755254/rmu20216

A ESPIRAL LOGARÍTMICA E O LOGO DA SBM

MICHEL SPIRA

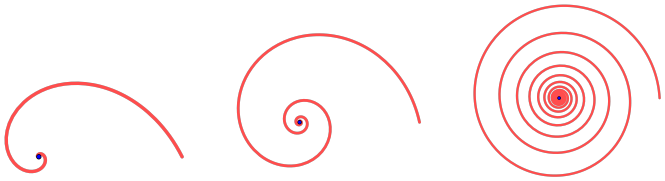
Resumo. A espiral logarítmica é uma das mais fascinantes curvas da Matemática, devido a suas maravilhosas propriedades e sua ubiquidade em fenômenos naturais e científicos. Ela foi objeto de estudo de, entre outros, Descartes, Torricelli e Jacob Bernoulli. Aqui apresentamos a família de espirais logarítmicas e algumas de suas propriedades, mostramos como gerar espirais logarítmicas a partir de retângulos e triângulos isósceles, e determinamos quando as espirais assim geradas são tangentes aos lados da figura geradora. Ao final, discutimos o logo da SBM.

1. A espiral logarítmica

Uma curva dada em um sistema de coordenadas polares de origem O por uma equação da forma

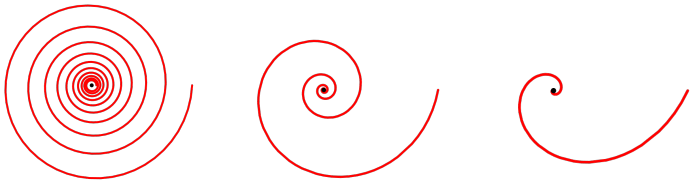
$$r(\theta) = ap^{\theta} \tag{1}$$

onde $a, p \in \mathbb{R}^+$ é dita uma *espiral logarítmica de centro* O. Essa equação determina uma família $\mathcal{L}$ de curvas a dois parâmetros; $a = r(0)$ é apenas um fator de escalonamento e não tem influência no comportamento assintótico de uma espiral logarítmica, que é determinado por p. Quando $p < 1$ temos $\lim_{\theta\to\infty} r(\theta) = 0$ e quando $p > 1$ temos $p < 1$ temos $\lim_{\theta\to-\infty} r(\theta) = 0$; em ambos os casos, podemos considerar O como uma representação do infinito.



$p = 0,6$ $p = 0,8$ $p = 0,95$

Data de aceitação: Junho de 2021.
Palavras chave. Espiral logarítmica, logo da SBM.



$p = 1,05$ $p = 1,2$ $p = 1,6$

Definimos acima uma família de curvas, mas mesmo assim vamos ocasionalmente referir-nos "à"espiral logarítmica. Esse abuso de linguagem já é consagrado e seu uso indica que discurso está sendo feito de modo genérico.

O centro O e dois pontos distintos (b, β) e (c, γ) em coordenadas polares com $b, c \in \mathbb{R}^+$ determinam uma única espiral logarítmica. De fato, definindo

$$p = \left(\frac{b}{c}\right)^{\frac{1}{\beta-\gamma}}$$

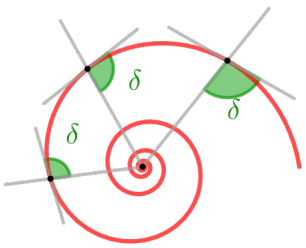
e

$$a := \frac{b}{p^\beta} = \frac{c}{p^\gamma} \ .$$

temos que a espiral logarítmica dada por $r = ap^\theta$ passa pelos pontos dados. Reciprocamente, quando conhecidos o centro e dois pontos (também em coordenadas polares) de uma mesma espiral logarítmica, os parâmetros a e p podem ser recuperados como acima.

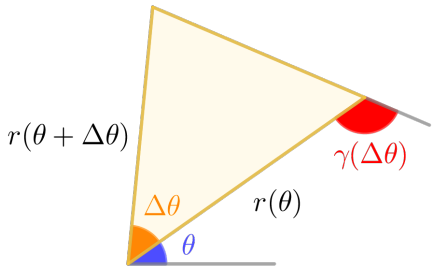
Para finalizar essa introdução, observamos que as funções r como em (1) levam progressões aritméticas em progressões geométricas e são as únicas funções com essa propriedade; equivalentemente, suas inversas são as únicas funções que levam progressões geométricas em progressões aritméticas ([1], capítulo 8). Dessa maneira, as ideias de raios igualmente espaçados angularmente e raios em progressão geométrica são equivalentes em uma espiral logarítmica.

1.1. **A propriedade equiangular.** Uma linda propriedade de $\mathcal{L}$ é que o ângulo entre o raio vetor e a tangente em qualquer ponto de uma espiral logarítmica dada é constante; vamos denotar esse ângulo por δ a partir de agora.



Do ponto de vista qualitativo, isso decorre imediatamente do fato apontado anteriormente de que r como em (1) leva progressões aritméticas em progressões geométricas; para nossos propósitos, no entanto, é importante caracterizar δ quantitativamente,

o que vamos fazer mostrando que $\operatorname{ctg}\delta \equiv \ln p$. Para isso, consideremos a figura abaixo, onde supomos por um momento que r é uma função diferenciável qualquer[1].



A lei dos senos nos dá a primeira igualdade abaixo

$$\frac{r(\theta+\Delta\theta)}{\operatorname{sen}\gamma(\Delta\theta)} = \frac{r(\theta)}{\operatorname{sen}[\gamma(\Delta\theta)-\Delta\theta]} = \frac{r(\theta+\Delta\theta)-r(\theta)}{\operatorname{sen}\gamma(\Delta\theta)-\operatorname{sen}[\gamma(\Delta\theta)-\Delta\theta]}$$

e a segunda segue de propriedades elementares de proporções. Reescrevendo essa última igualdade como

$$\frac{r(\theta+\Delta\theta)-r(\theta)}{\Delta\theta}\cdot\frac{1}{r(\theta)} = \frac{\operatorname{sen}\gamma(\Delta\theta)-\operatorname{sen}[\gamma(\Delta\theta)-\Delta\theta]}{\Delta\theta}\cdot\frac{1}{\operatorname{sen}[\gamma(\Delta\theta)-\Delta\theta]}\ ,$$

fazendo $\Delta\theta \to 0$ e observando que $\lim_{\Delta\theta\to 0}\gamma(\Delta\theta) = \delta(\theta)$ obtemos

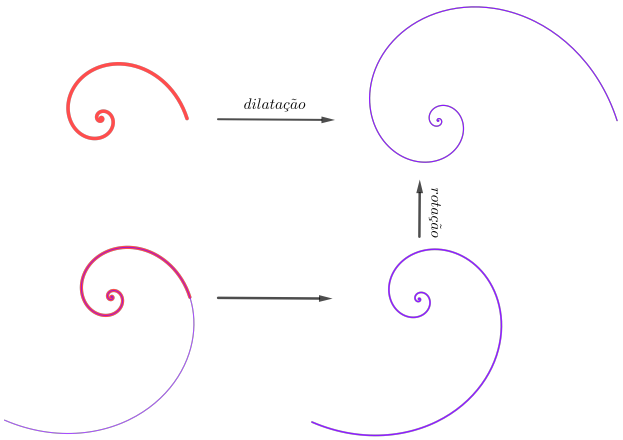
$$\frac{r'(\theta)}{r(\theta)} = \operatorname{ctg}\delta(\theta)\ . \tag{2}$$

Quando $r(\theta) = ap^\theta$ temos $\operatorname{ctg}\delta(\theta) = \ln p$ para todo θ, como anunciado. A equação (1) costuma ser apresentada na forma $r(\theta) = ae^{b\theta}$ para deixar em evidência o parâmetro $b = \ln p$.

Reciprocamente, (2) mostra que a propriedade equiangular é característica de $\mathcal{L}$; por esse motivo, uma espiral logarítmica também atende pelo nome de *espiral equiangular*.

1.2. **Autosimilaridade.** Outra bela propriedade de $\mathcal{L}$ é a *autosimilaridade por rotação*, que diz que uma rotação com centro O e ângulo α e uma dilatação de centro O e razão p^α têm o mesmo efeito sobre uma espiral logarítmica. Para ver isso, basta escrever $r(\theta+\alpha) = ap^{\theta+\alpha} = p^\alpha r(\theta)$ para todo θ.

[1] A redação original do argumento que segue foi corrigida e simplificada com sugestões dos relatores.



A autosimilaridade por rotação é uma propriedade característica de $\mathcal{L}$. De fato[2], seja r uma curva contínua dada em coordenadas polares tal que para todo α existe $\lambda(\alpha)$ tal que

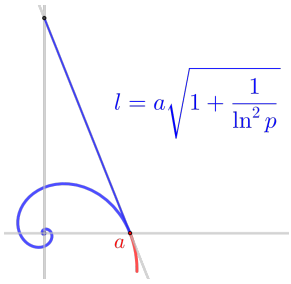
$$\lambda(\alpha)r(\theta) = r(\theta + \alpha) \tag{3}$$

para todo θ; sem perda de generalidade, podemos supor $r(0) = 1$. Colocando $\theta = 0$ em (3) obtemos $\lambda(\alpha) = r(\alpha)$ para todo α; em particular, λ é contínua. Segue também de (3) que $\lambda(\alpha+\beta) = r(\alpha+\beta) = \lambda(\alpha)\lambda(\beta)$ para todos α, β e logo $\lambda(\alpha) = e^{c\alpha}$ para algum c ([1], capítulo 8). Colocando $p = e^c$ temos $r(\theta) = \lambda(\theta) = e^{c\theta} = p^\theta$ e recuperamos uma espiral logarítmica.

1.3. **Um mínimo de História.** Vamos agora apresentar alguns aspectos históricos da espiral logarítmica.

René Descartes (1596-1650) descobriu a espiral logarítmica a partir da propriedade equiangular; devemos a ele a terminologia *espiral equiangular*. A primeira menção a essa curva aparece em uma de suas cartas, enviada para Marin Mersenne (1588-1648) em 1638 [2].

Evangelista Torricelli (1608-1647) determinou em 1645 o comprimento da espiral logarítmica de $\theta = 0$ a $\theta = \infty$ usando o método de exaustão ([2],[3] capítulo 9). Essa foi a segunda retificação de uma curva na história da Matemática, a primeira sendo a da circunferência. O resultado de Torricelli aparece na figura abaixo.



[2]Argumento sugerido por Marco Moriconi.

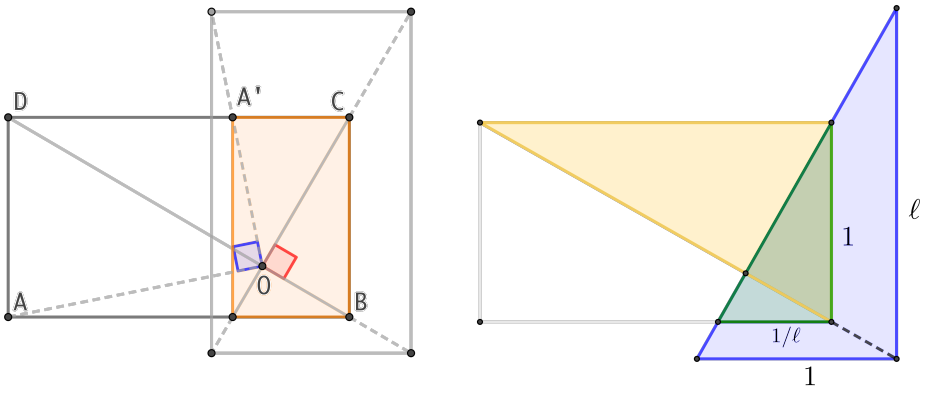
Jacob Bernoulli (1654-1705) estudou profundamente a espiral logarítmica e descobriu muitas de suas maravilhosas propriedades, que o levaram a chamá-la de *spira mirabilis*. Descrever as contribuições de Bernoulli foge ao escopo desse artigo; observamos apenas que a terminologia *espiral logarítmica* foi introduzida por ele em 1691 [2].

Mencionamos também que Isaac Newton (1642-1726) mostrou nos *Principia* que se um corpo percorre uma espiral logarítmica sob a ação de uma força central então essa força varia com o inverso do cubo da distância ao centro ([4],[5]).

Encerramos aqui nossa breve apresentação da espiral logarítmica. Recomendamos ([2],[3] capítulo 9) para exposições históricas mais completas, ([6],[7]) para detalhes sobre as propriedades que tanto encantaram Bernoulli, ([8],[9],[10]) para suas manifestações em outras áreas de conhecimento, ([11],[12],[13]) para informações adicionais e lindas figuras, e [14] para os interessados em seus aspectos místicos.

2. A espiral associada a um retângulo

A figura abaixo, à esquerda, mostra um retângulo $ABCD$ de dimensões $\ell \times 1$ com $\ell > 1$; o ponto O é a interseção da diagonal BD com a perpendicular por C.

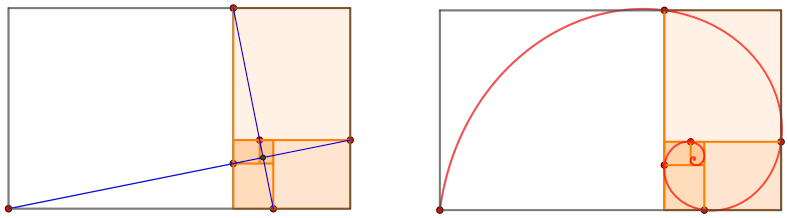


O retângulo sombreado é obtido do retângulo original por uma rotação de $\frac{\pi}{2}$ em torno de O no sentido horário seguida de uma contração de $\frac{1}{\ell}$ com centro O; o ponto A' é a imagem de A por esse processo e OA é perpendicular a OA'. Para justificar essas afirmativas[3] basta observar a figura à direita, onde notamos que todos os triângulos que aparecem são semelhantes. O triângulo azul é a imagem do triângulo amarelo pela rotação e o triângulo verde, a imagem desse último pela contração. Como a imagem do retângulo original por essas transformações é um retângulo e já temos as imagens de três de seus vértices, a correção da figura à esquerda fica estabelecida.

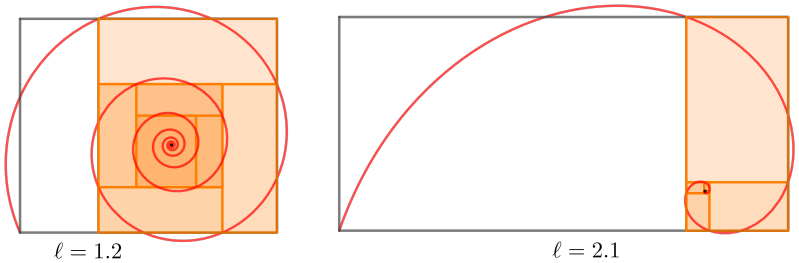
Como o retângulo sombreado é semelhante ao retângulo original, podemos iterar essa construção e obter a figura a seguir, à esquerda, onde exibimos cinco iterações, as sucessivas imagens de A e os raios por elas determinados. Esses raios formam uma progressão geométrica de razão $\frac{1}{\ell}$ e estão angularmente espaçados de $\frac{\pi}{2}$, de

[3]Agradecemos a um dos relatores por insistir na inclusão de uma justificativa.

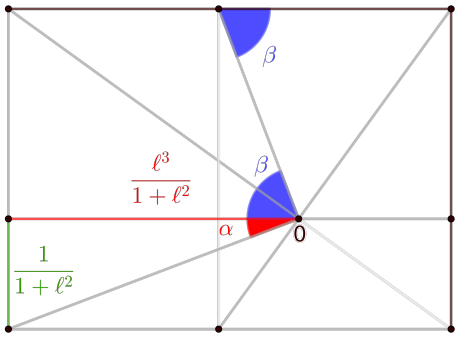
modo que seus extremos estão em uma espiral de centro O, como à direita. Dizemos que essa é a *espiral associada ao retângulo*; para ela temos $p = \ell^{\frac{2}{\pi}}$.



A figura a seguir



e o teorema do valor intermediário mostram que existe um único retângulo $\ell_0 \times 1$ tal que a espiral associada é tangente ao lado CD (e logo também tangente a BC e AB). Para determinar ℓ_0, consideramos o retângulo $\ell \times 1$ da figura abaixo

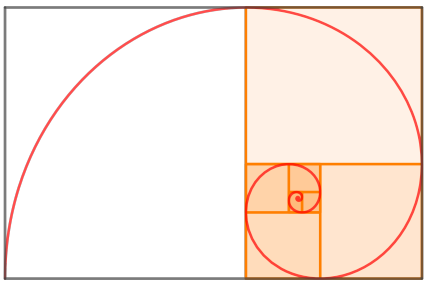


onde vemos que $\operatorname{ctg}\beta = \operatorname{tg}\alpha = \frac{1}{\ell^3}$. A condição de tangência é $\beta = \delta$; como $\operatorname{ctg}\delta = \ln p$ temos, nesse caso,

$$\frac{1}{\ell^3} = \frac{2}{\pi}\ln \ell$$

e segue que ℓ_0 é o (único) zero de $f(x) = x^3 \ln x - \frac{\pi}{2}$. O comando `Root` do *Geogebra* fornece $\ell_0 = 1,5388620467\ldots$[4]; aqui temos $\delta_0 = 74°39'18''\ldots$. Segue para contemplação a figura correspondente.

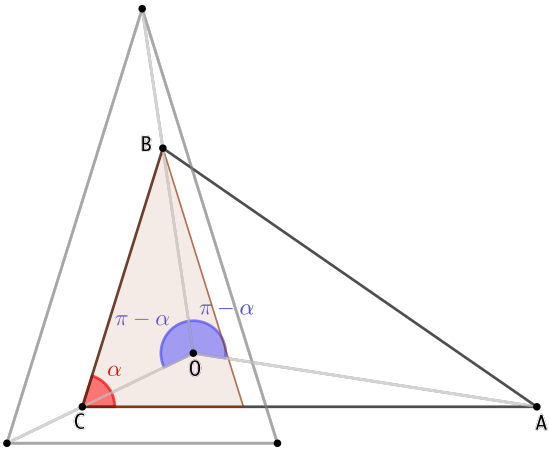
[4] O *Mathematica* fornece o mesmo valor, como informa um dos relatores.



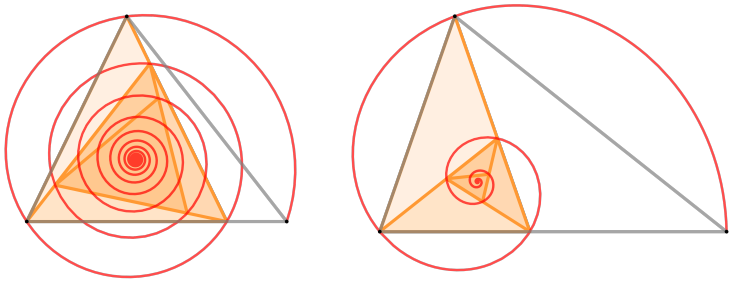
3. A espiral associada a um triângulo isósceles

Espirais logarítmicas também aparecem associadas a triângulos isósceles, em particular ao assim dito *triângulo áureo* ([15],[16]). Vamos aqui analisar brevemente essas espirais, de modo análogo ao que fizemos na seção anterior.

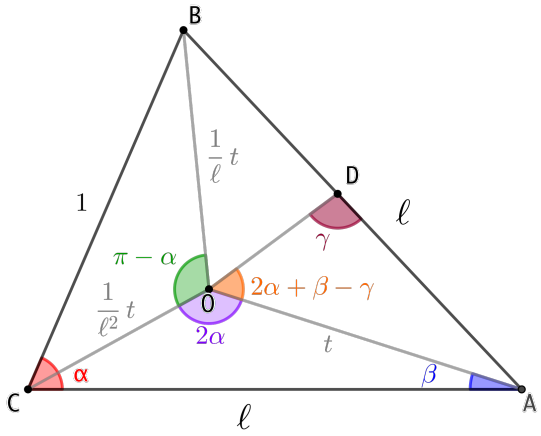
Consideremos um triângulo isósceles ABC de base $BC = 1$ e lados $AB = AC = \ell$, com $\widehat{ABC} = \widehat{ACB} = \alpha$; nele determinamos o ponto O como a interseção de arcos capazes de $\pi - \alpha$ dos segmentos AB e BC.



O triângulo sombreado é obtido a partir do triângulo original por uma rotação de $\pi - \alpha$ em torno de O no sentido anti-horário seguida de uma contração de $\frac{1}{\ell}$ com centro O; a iteração desse processo leva a uma espiral logarítmica de centro O que passa pelas sucessivas imagens de A.



Para essa espiral temos $p = \left(\frac{1}{\ell}\right)^{\frac{1}{\pi-\alpha}}$. Como na seção anterior, existe um único triângulo isósceles cuja espiral associada é tangente a seus lados. Para determiná-lo, consideremos a seguinte figura.



Aqui D é o primeiro ponto (quando existe) onde a espiral associada intercepta o lado AB; a diferença angular entre A e D é $2\pi + 2\alpha + \beta - \gamma$. Temos

$$\alpha = \arccos \frac{1}{2\ell}$$

$$t = \ell^2 \sqrt{\frac{1}{\ell^2+2}} \text{ (lei dos cossenos no triângulo } ACO)$$

$$\beta = \operatorname{arcsen} \frac{t \operatorname{sen} 2\alpha}{\ell^3} \text{ (lei dos senos no triângulo } ACO)$$

$$OD = tp^{2\pi+2\alpha+\beta-\gamma}$$

e lembramos que

$$\delta = \operatorname{arcctg} \ln p = \arccos \frac{\ln p}{\sqrt{1+\ln^2 p}} \, .$$

A espiral é tangente em D quando $\gamma = \delta$; nesse caso, a lei dos senos no triângulo ADO nos dá

$$\frac{t}{\operatorname{sen}\delta} = \frac{tp^{2\pi+2\alpha+\beta-\delta}}{\operatorname{sen}(2\alpha+\beta)}$$

ou seja

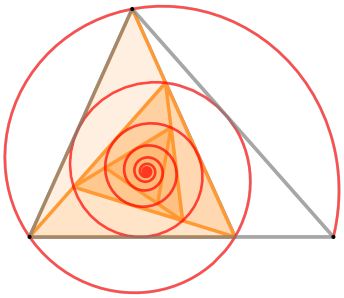
$$\operatorname{sen}(2\alpha+\beta) = p^{2\pi+2\alpha+\beta-\delta} \operatorname{sen}\delta$$

e segue que a tangência ocorre quando ℓ é o (único) zero da função

$$g(x) = \operatorname{sen}[2\alpha(x)+\beta(x)] - p(x)^{2\pi+2\alpha(x)+\beta(x)-\delta(x)} \operatorname{sen}\delta(x) \, .$$

O comando `Root` fornece o zero $\ell_1 = 1,2162407940\ldots$[5], que corresponde a um triângulo isósceles com ângulo da base $65°43'33''\ldots$ e a $\delta_1 = 96°10'21''\ldots$. Segue, também para contemplação, a figura pertinente.

[5] Já o *Mathematica* fornece $\ell_1 = 1,21624079\,42\ldots$, como apontado pelo mesmo relator.

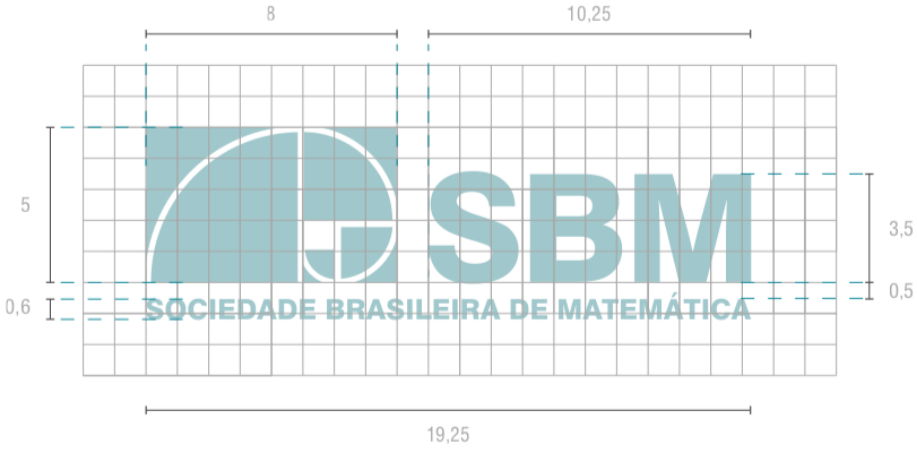


4. O logo da SBM

Nessa seção vamos considerar alguns aspectos do logo da SBM, começando por sua história.

Um concurso para a escolha do logo foi divulgado no *Noticiário da SBM* em outubro de 1977. Em reunião do Conselho Diretor de maio de 1978 não houve consenso sobre nenhuma das propostas, o que se repetiu em em reuniões de março e outubro de 1980, bem como de junho de 1981; a partir daí não se encontram mais menções a esse assunto no *Noticiários* [17][6]. Em comunicação pessoal, o professor César Camacho informa que o logo foi escolhido em um concurso realizado pela diretoria da SBM durante seu mandato como presidente no período 1987-89; a proposta vencedora foi de Rodolfo Capeto, na época o *designer* gráfico do IMPA.

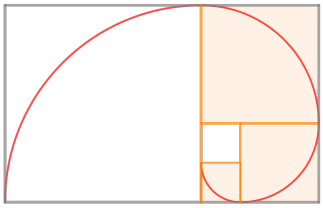
A descrição do logo aparece no *Manual da marca e identidade visual* da SBM [18]



e vemos que ele é a conhecida *espiral de Fibonacci* ([19],[20]) em um retângulo 8×5. A partir do quadrado branco, os lados dos quadrados são 1, 1, 2, 3 e 5 que, com o lado 8 do retângulo, são os primeiros termos da *sequência de Fibonacci*. Essa espiral é formada por quartos de círculo[7], de modo a fazê-la tangente aos lados do retângulo.

[6]Referência indicada por Paulo Cézar Carvalho.

[7]O *Manual* não especifica a espessura dos arcos de círculo e dos segmentos que delimitam os quadrados; em uma grade apropriada, observa-se que ela é aproximadamente $\frac{1}{5}$.



Como $\frac{8}{5\Phi} = 0,9888\ldots$, o retângulo $\frac{8}{5} \times 1$ é uma boa aproximação do retângulo $\Phi \times 1$, onde $\Phi = \frac{1+\sqrt{5}}{2}$ é o *número de ouro*. Retângulos semelhantes a esse último, conhecidos como *retângulos áureos*, são os únicos retângulos que deixam quadrados em seu caminho no processo de rotação e contração descrito na seção 2.

Podemos assim visualizar no logo as ideias de quadrado, círculo, tangência e números de Fibonacci e, de modo aproximado, do número de ouro e do retângulo áureo. Ressaltamos também a simplicidade de seus elementos, que resulta em grande facilidade para sua descrição e composição gráfica.

Por outro lado, a gênese da espiral de Fibonacci através de arcos de círculo e números de Fibonacci faz com que ela não seja sequer de classe C^2 e exclui qualquer sugestão das ideias de autosimilaridade, equiangularidade e representação do infinito. Notamos que, com exceção da referência a números de Fibonacci, ela não tem relação com a História da Matemática, e observamos ainda que, às vezes apresentada como uma espiral logarítmica, ela ilustra o uso incorreto e autoritário de linguagem matemática em pseudociência, misticismo, culto do número de ouro, arte e outras manifestações culturais ([14],[21],[22],[23],[24]).

A construção de uma espiral por meio de quartos de círculo pode ser realizada no retângulo áureo ([16],[25]) e é originalmente devida a Albrecht Dürer (1471-1528) [20]. Aqui aplicam-se os mesmos comentários feitos no parágrafo anterior em relação à espiral de Fibonacci, com exceção da possibilidade de representação do infinito.

Notamos, finalmente, que essa não é a primeira vez que o logo de uma sociedade matemática é criticado[8]. Em [26] (ver também [27]) aponta-se que o logo da MAA anterior a 1972 apresentava uma projeção em perspectiva incorreta do icosaedro, que foi devidamente corrigida.

5. Duas propostas

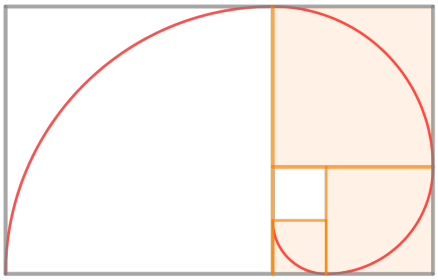
O logo da SBM acompanhou boa parte da história da Matemática brasileira, tendo assim inegável valor simbólico e afetivo. Por outro lado, de acordo com o exposto na seção anterior, consideramos que ele não possui características adequadas para representar nossa Sociedade. Desse modo, apresentamos duas propostas para eventual consideração por parte do Conselho Diretor e dos membros da SBM.

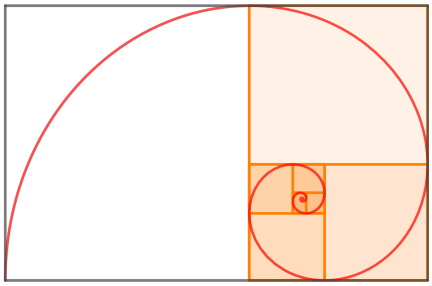
I. Substituir o logo pela espiral tangente no retângulo $\ell_0 \times 1$.

II. Substituir o logo pela espiral tangente na página e nas publicações digitais da SBM como uma animação explorando as propriedades da espiral logarítmica[9].

[8] Observação devida a Humberto Bortolossi.

[9] Ideia sugerida por Paulo Cézar Carvalho.





Agradecimentos

O autor agradece a generosa colaboração de César Camacho, Humberto Bortolossi, Marco Moriconi e Paulo Cézar Carvalho, bem como a dos dois relatores.

Referências

[1] Elon Lages Lima, Paulo Cézar Pinto Carvalho, Eduardo Wagner e Augusto César Morgado: *A Matemática do Ensino Médio*. Coleção do Professor de Matemática, SBM, 1996

[2] Raymond Claire Archibald: *Notes on the logarithmic spiral, golden section and the Fibonacci series*. Note V *in* Jay Hambidge: *Dynamic symmetry*. Yale University Press, 1920.

[3] Øyvind Hammer: *The Perfect Shape: Spiral Stories*. Copernicus, 2016.

[4] Herman Erlichson: *Newton's Solution to the Equiangular Spiral Problem and a New Solution Using Only the Equiangular Property*. Historia Mathematica 19 (1992), pp.420-413.

[5] Curtis Wilson: *Newton on the Equiangular Spiral. An Addendum to Erlichson's Account*. Historia Mathematica 21 (1994), pp.196-203.

[6] Sérgio Alves: *A espiral equiangular*. Notas de minicurso, I Bienal da SBM, 2002.

[7] Eli Maor: *The logarithmic spiral*. The Mathematics Teacher, vol. 67(4), 1974, pp. 321-327.

[8] Kinko Tsuji, Stefan Müller (eds): *Spirals and vortices in Culture, Nature and Science*. Springer Verlag, 2019.

[9] Jay Kappraff: *The Logarithmic Spiral in Geometry, Nature, Architecture, Design and Music*. https://directorymathsed.net/public/CataniaConferenceDocuments&Papers/Proceedings/All%20PapersInPDF/KAPPRAFF.pdf

[10] Khristo Boyadzhiev: *Spirals and Conchospirals in the Flight of Insects*. The College Mathematics Journal 30(1), 1999, pp. 23-31.

[11] Jim Wilson: *Equiangular Spiral (or Logarithmic Spiral) and Its Related Curves*. http://jwilson.coe.uga.edu/EMT668/EMAT6680.F99/Erbas/KURSATgeometrypro/related%20curves/related%20curves.html

[12] https://mathcurve.com/courbes2d.gb//logarithmic/logarithmic.shtml

[13] http://xahlee.info/SpecialPlaneCurves_dir/EquiangularSpiral_dir/equiangularSpiral.html

[14] http://www.spirasolaris.ca

[15] Arthur Lee Loeb & William Varney: *Does the golden spiral exist, and if not, where is its center? In* István Hargittai & Clifford Alan Pickover (eds.): *Spiral Symmetry*, World Scientific, 1992.

[16] John Sharp: *Spirals and the golden section*. Nexus Network Journal, vol. 4(1), 2002, pp. 59-82.

[17] Viviane de Oliveira Santos: *Uma história da Sociedade Brasileira de Matemática durante o período de 1969 a 1989: criação e desenvolvimento*. Tese de doutorado, Unesp - Rio Claro, 2016.

[18] *Manual da marca e identidade visual*. SBM, 2017. https://www.sbm.org.br/wp-content/uploads/2017/03/SBM_Manual_Marca_ver20170223.pdf

[19] https://en.wikipedia.org/wiki/Fibonacci_number
[20] Andrey Polezhaev: *Spirals, Their Types and Peculiarities. In* Kinko Tsuji, Stefan Müller (eds): *Spirals and vortices in Culture, Nature and Science.*
[21] *The Fibonacci Sequence in Nature.* https://insteading.com/blog/fibonacci-sequence-in-nature/
[22] *The Fibonacci Sequence Is Everywhere – Even the Troubled Stock Market.* https://www.smithsonianmag.com/science-nature/fibonacci-sequence-stock-market-180974487/
[23] *The Fibonacci Sequence In Artistic Composition.* https://www.markmitchellpaintings.com/blog/the-fibonacci-sequence-in-artistic-composition/
[24] *Nature's proof of inteligent design: sacred geometry, phi, the Fibonacci spiral, & self-reflective designs.* https://newearthknowledge.com/2019/11/22/proof-intelligent-design/
[25] https://en.wikipedia.org/wiki/Golden_spiral
[26] Branko Grunbaum: *Geometry strikes again.* Mathematics Magazine 58(1) (Jan.1985), pp. 12-17.
[27] Doris Schattschneider: *The mistery of the MAA logo.* Mathematics Magazine 58(1) (Jan.1985), p. 18

Rua da Nascente 136, Distrito de São Gonçalo do Rio das Pedras, Serro, MG
Email address: michelspira@gmail.com

RMU
REVISTA MATEMÁTICA UNIVERSITÁRIA

SBM
SOCIEDADE BRASILEIRA DE MATEMÁTICA

Revista Matemática Universitária, vol. 2, 2021
ISSN: 2675-5254 — **DOI:** 10.21711/26755254/rmu20217

UM INCANSÁVEL COMBATENTE NA DEFESA DA INVESTIGAÇÃO MATEMÁTICA: ANTÓNIO ANICETO MONTEIRO (1907-1980)

LUÍS MANUEL RIBEIRO SARAIVA

Uma perspectiva mais completa da acção de qualquer pessoa implica ter-se em conta o contexto em que viveu, as restrições que teve de enfrentar ou, pelo contrário, o ambiente favorável que encontrou. Neste sentido podemos dizer que o matemático António Aniceto Monteiro foi um verdadeiro gigante na ciência do século XX, e mais especificamente na matemática. Viveu a época conturbada do pós Primeira Guerra Mundial, com a ascensão do fascismo e do nazismo na Europa, que culminaram na Guerra Civil de Espanha (1936-1939) e na 2ª Guerra Mundial (1939-1945). No seu país suportou a época inicial de uma ditadura que se estendeu de 1926 até 1974, um regime retrógrado que colocava o povo sob intensa vigilância e repressão. Mesmo quando partiu para o Brasil para aí viver, Monteiro continuou a ser vigiado pela polícia política portuguesa.

Foi educado num sistema universitário que tinha como única finalidade a transmissão de conhecimento aos futuros quadros da administração pública e aos futuros professores. O currículo universitário no que diz respeito à matemática era antiquado, tinha imensas falhas, e a investigação matemática praticamente não existia enquanto actividade organizada.

No primeiro relatório trimestral que enviou de Paris, onde estava a fazer um estágio que o havia de conduzir ao doutorado, dirigido à Junta de Educação Nacional, a entidade que subsidiava a sua estada e a quem tinha de prestar contas periodicamente, caracterizou de forma preocupante o conhecimento recebido por um licenciado em Ciências Matemáticas no Ensino Superior em Portugal:

"ignorância de uma enormidade de conhecimentos basilares; educação enciclopédica, de que resulta o conhecimento superficial de todas as matérias estudadas; ausência quase completa de espírito crítico; ausência de iniciação aos métodos de investigação, de que resulta um interesse nulo pela investigação científica."

Data de aceitação: Setembro de 2021.
Palavras chave. Matemática portuguesa do século XX; António Monteiro; investigação matemática no Brasil e na Argentina no século XX; revistas matemáticas.

É este grave estado de coisas que Monteiro queria mudar quando completasse a sua formação em Paris (1931-1936) e regressasse a Portugal, o que aconteceu após concluir o seu doutorado sob a orientação do matemático francês Maurice Fréchet [1].

FIGURA 1. Maurice Fréchet em Portugal em 1942. Foto na Faculdade de Ciências de Lisboa (hoje Museu Nacional de História Natural e da Ciência) com a grande maioria dos matemáticos da chamada geração de 40. Da esquerda para a direita: Hugo Ribeiro, Armando Gibert, António Monteiro, Manuel Zaluar Nunes, Bento de Jesus Caraça, Maurice Fréchet, José Sebastião e Silva, Ruy Luis Gomes, José Ribeiro de Albuquerque e Augusto Sá da Costa. Monteiro foi para o Brasil em 1945, e os restantes, com excepção de Sebastião e Silva e Ribeiro de Albuquerque, seriam excluídos da Universidade na grande purga feita pelo regime em 1946/47.

No regresso a Portugal Monteiro foi o dinamizador principal daquela que ficou conhecida por "Geração de 40" [2], que em dez anos (1936-1945) mudou o panorama matemático português, criando em 1937 um jornal de investigação matemática internacional, a Portugaliae Mathematica, que ainda hoje existe, iniciando um jornal de divulgação matemática em 1940, a Gazeta de Matemática, que igualmente continua a ser publicada [3], e fundando a Sociedade Portuguesa de Matemática (SPM) em 1940. Esse grupo de matemáticos teve uma actividade constante na organização de diversos Seminários sobre temas da actualidade matemática e fundaram diversos centros de pesquisa, criando condições para, de um modo continuado, se poder desenvolver investigação matemática em Portugal sobre temas então actuais [4].

Monteiro considerava que o renascimento da matemática no seu país só seria possível se se criasse uma corrente de fundo entre os estudantes do Ensino Secundário e da Universidade de interesse pela Matemática. Nesse sentido, e igualmente como tentativa de ultrapassar o bloqueamento que era feito na Universidade às propostas de renovação curricular dos matemáticos da nova geração, e seguindo o exemplo dos Estados Unidos para mobilizar a juventude e levá-la a uma prática em que desenvolvesse um espírito crítico virado para a pesquisa, foram criados os Clubes de

Matemática em 1942. De começo a iniciativa teve muito sucesso, foram fundados clubes em várias universidades e faculdades, mas pouca duração tiveram, pois o Governo, receoso de tudo o que fosse adquirir espírito crítico, fez espalhar o boato que neles só participavam comunistas, o que bastou para em poucos anos fazê-los desaparecer.

A Ditadura queria manter um controle estrito sobre a população, e com a vitória da Frente Popular nas eleições espanholas de Fevereiro de 1936 o regime entrou em pânico, sentindo-se ameaçado por haver em Espanha uma aliança progressista no poder, que incluía os socialistas. Apertou então o seu controle, e fez entrar em vigor um decreto que obrigava todos os que queriam ter emprego no Estado a assinar uma declaração que essencialmente exprimia o apoio ao regime. Monteiro recusou assinar essa declaração, e em consequência ficou impossibilitado de trabalhar para o Estado, nomeadamente não podia ser docente universitário. Deste modo, para ganhar a vida, Monteiro deu explicações particulares. Mas a situação estava muito longe de ser ideal, e Monteiro a partir de certa altura começou a procurar hipóteses de trabalho fora de Portugal, no que foi ajudado por matemáticos estrangeiros.

Acabou por aparecer um convite do Brasil em Setembro de 1943 que ele aceitou, mas as burocracias da ditadura atrasaram cerca de ano e meio a sua partida. Deixou então Portugal, na companhia de sua esposa Lídia, e dos dois filhos, António e Luiz. Teve a cátedra de Análise Superior na Faculdade Nacional de Filosofia da Universidade do Brasil (FNFi), no Rio de Janeiro, futura UFRJ. Nessa altura o seu

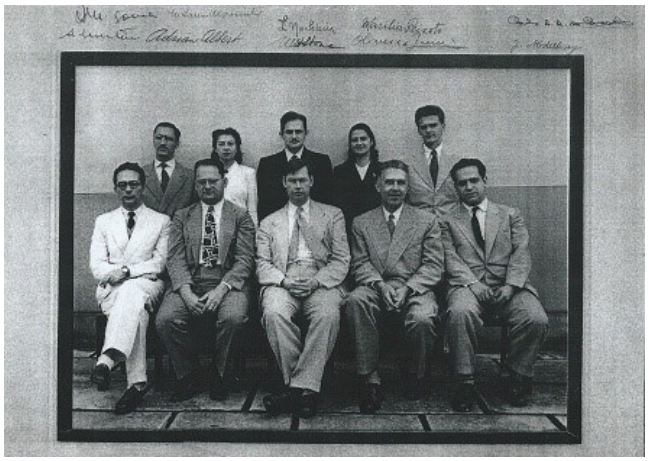


FIGURA 2. Elementos do Departamento de Matemática da FNFi em 1948. Entre parêntesis está a idade de cada um na altura da foto: De pé: Alvércio Moreira Gomes (32), Maria Laura Mousinho (31), Leopoldo Nachbin (26), Marília Peixoto (27), Carlos Alberto Aragão Carvalho (24). Sentados: António Monteiro (41), Abraham Adrien Albert (43), Marshall Harvey Stone (45), Ernesto Luiz de Oliveira Junior (47), José Abdelhay (31). Foto do espólio de António Monteiro, gentilmente cedida por Jorge Rezende.

Departamento de Matemática era o segundo melhor centro de matemática do Brasil,

estando o primeiro na Faculdade de Filosofia, Ciências e Letras da Universidade de S. Paulo (FFCL). Assinou um contrato de quatro anos, renovável. O Departamento de Matemática da FNFi teve visitantes estrangeiros importantes, como Abraham Adrien Albert (1905-1972), Professor Catedrático em Chicago e futuro Presidente da American Mathematical Society no biénio 1965/66, e Marshall Harvey Stone (1903-1989), Professor Catedrático em Harvard, Presidente da American Mathematical Society em 1943/44, e futuro Presidente da International Mathematical Union no período 1952-54. O Presidente do Departamento de Matemática, e responsável pela contratação de Monteiro, bem como da viabilização das visitas de Albert e de Stone, era Ernesto Luiz de Oliveira Junior (1901-?), que tinha sido assistente dos matemáticos italianos Luigi Fantappié (1901-1956) e Giacomo Albanese (1890-1948) na FFCL entre 1934 e 1936. Monteiro deu vários cursos e seminários sobre temas como Topologia Geral, Espaços de Hilbert, Análise Funcional, Álgebras de Boole e Reticulados. Contactou importantes matemáticos, entretanto chegados à FFCL, alguns já conhecidos de Paris, como André Weil (1906-1998) e Jean Dieudonné, (1906-1992) dois elementos fundamentais do grupo Bourbaki.

Monteiro orientou alguns alunos nos anos que esteve no Rio de Janeiro: Maria Laura Mouzinho (mais tarde Maria Laura Leite Lopes) (1917-2013) teve Monteiro por supervisor do seu doutorado, sendo a segunda mulher a obter o doutorado em matemática no Brasil (1949). A primeira tinha sido Marília Peixoto (1921-1961), ao ser aprovada em concurso para livre docente na Escola Nacional de Engenharia [5] em 1948. Além disso teve influência decisiva em Leopoldo Nachbin (1922-1993), contratado em 1947 para docente da FNFi, Maurício Peixoto (1921-2019), da Escola Nacional de Engenharia, o único matemático brasileiro com o qual Monteiro tem um artigo em comum publicado na Portugaliae Mathematica, e Paulo Ribenboim (1928-), também contratado para a FNFi em 1948. Nachbin foi um dos maiores matemáticos brasileiros do século XX, estando na fundação do Centro Brasileiro de Pesquisas Físicas em 1949, na do CNPq e da CAPES em 1951. Foram alunos de Monteiro os dois primeiros matemáticos brasileiros a darem conferências plenárias nos Congressos Internacional de Matemáticos: Leopoldo Nachbin em Estocolmo, 1962, e Maurício Peixoto em Vancouver, em 1974. Os dois, conjuntamente com Lélio Gama, foram co-fundadores do Instituto de Matemática Pura e Aplicada (IMPA) em 1952. Peixoto foi presidente do CNPq, da Academia Brasileira de Ciências e da Sociedade Brasileira de Matemática. Já na Argentina, Monteiro orientou o doutorado de Mário Tourasse Teixeira (1925-1993) que defendeu a sua tese na FFCL da Universidade de S. Paulo em 1965.

Em 1945 e 46 Monteiro foi igualmente investigador no Núcleo Técnico Científico da Fundação Getúlio Vargas, e com Lélio Gama (1892-1981) coordenou o seu Núcleo de Matemática. Participou da fundação da revista de pesquisa matemática Summa Brasiliensis Mathematicae, da qual sairam 2 volumes entre 1946 e 1951: o primeiro diz respeito ao período 1945/46, o segundo é relativo aos anos 1947/51. Estes dois primeiros números têm artigos de Monteiro (com Hugo Ribeiro), Nachbin, Maria Laura, Paulo Ribenboim, Maurício Peixoto e Lélio Gama, mas igualmente de Paul Halmos (1916-2006), Jean Dieudonné (2), Abraham Albert (2), André Weil, Paul Erdös (1913-1996), Jacques Dixmier (1924-) e Oscar Zariski (1899-1986). Depois da

partida de Monteiro para a Argentina ainda foram publicados mais dois números, o nº 3, com artigos de 1952 a 1956, e o nº4, relativo ao período de 1957 a 1960.

Em 1948 iniciou a publicação das Notas de Matemática, sendo o editor dos seis primeiros volumes (1948/49), que incluem dois trabalhos seus, dois de Nachbin, um de Maurício Peixoto e um de José Abdelhay (1917-1996), colega de Monteiro no Departamento de Matemática da FNFi. Do nº7, já com Monteiro na Argentina, até ao nº 47, em 1972, foi Nachbin o editor. A partir daí a North Holland Publishing Company tomou conta das Notas, se bem que Nachbin ainda tenha sido o editor dos primeiros números.

Havia (e continua a haver) no Brasil uma numerosa comunidade portuguesa, e uma parte muito significativa estava declaradamente contra a ditadura em Portugal. Por essa razão o governo português destacou para o Brasil numerosos agentes da sua polícia política para vigiarem os movimentos da comunidade portuguesa e informarem o governo das iniciativas contrárias ao regime que fossem aí organizadas. Monteiro também tomou parte activa em sessões antifascistas. Por isso era pessoa non grata do regime, que procurou dificultar-lhe a vida, fazendo pressão para o seu contrato na Universidade não ser renovado. Outro problema surgiu pelo facto da Universidade, a partir de certa altura, ter começado a pagar-lhe os ordenados com cada vez maior atraso. Monteiro ficou com a sua vida bastante dificultada e começou a estudar as possibilidades de ir trabalhar para outro país. No fim de 1948, por meio do matemático espanhol Pedro Pi Calleja (1907-1986) [6], chegou-lhe uma oferta de emprego na Universidade de Cuyo, em S. Juan, na Argentina.

Em 1949 tornou-se investigador do Centro Brasileiro de Pesquisas Físicas (CBPF) que passou a distribuir o Summa Brasiliensis Mathematicae. O CBPF era uma alternativa ao ambiente conservador da FNFi. A pressão feita sobre a Universidade acabou por ter efeito, e o contrato de Monteiro, depois de vários atrasos, não foi renovado, o que o deixou sem meios de subsistência. Para ter um ordenado regular, passou a trabalhar na Companhia de Aviação Transcontinental, onde fez cálculos estatísticos, utilizou a programação linear para optimizar a procura de lugares, e elaborou roteiros de voo. Mas era claramente uma solução provisória, até ser possível a sua saída para uma universidade noutro país.

Finalmente parte para a Argentina, onde chega a 5 de Dezembro. Aqui vai ter uma acção importante na modernização da matemática deste país. Ficou em S. Juan de 1950 a 1956, leccionando na Universidade de Cuyo, tendo igualmente dinamizado a criação em 1951 de um Departamento de Investigações Científicas, sediado em Mendoza, que incluía um Instituto de Matemática. Em 1955 colaborou na criação da Revista Matemática Cuyana. A partir de 1957 mudou-se para Bahia Blanca, contratado pela Universidad del Sur (UNS). Organizou a licenciatura em Matemática e o Instituto de Matemática, estruturou e organizou a sua biblioteca, que passou a ser a mais completa da América do Sul, e criou duas séries de publicações da UNS, que incluiam preprints e apontamentos de seminários avançados de pesquisa: Notas de Lógica Matemática em 1964, e Notas de Álgebra e Análise em 1966. Estabeleceu um regime de permutas com outras instituições. A qualidade e o quantidade dos artigos incluídos nos números destas duas publicações eram tais que se conseguiram desse modo alguns dos mais caros e reputados jornais estrangeiros. Em 1970, das 453

publicações que a Biblioteca do Instituto de Matemática recebia, cerca de metade era obtida por troca com publicações criadas pelo matemático português.

Monteiro tinha dito que nunca regressaria a Portugal enquanto ele estivesse sob o domínio da ditadura. Esta foi derrubada na revolução de 1974, pelo que a partir daí passou a ser viável a Monteiro visitar o seu país. Foi o que fez em 1977, ficando em Portugal dois anos como investigador do Centro de Matemática e Aplicações Fundamentais. Escreveu um artigo, "Sur les Algèbres de Heyting Symmétriques", que obteve em 1978 o Prémio Gulbenkian de Ciência e Tecnologia. Regressou em 1979 à Argentina, e faleceu pouco depois, a 29 de Outubro de 1980, em Bahia Blanca.

Em reconhecimento do muito que fez pela matemática argentina e pela sua modernização, e em particular pela sua universidade, a UNS deu o seu nome à Biblioteca do Instituto de Matemática. Desde 1991 que a UNS organiza, de dois em dois anos, um congresso com o nome Dr António Monteiro. Em cada Encontro é colocado ênfase num ramo diferente da matemática, para assim se ir percorrendo a matemática na sua variedade.

Em 2006, na sessão Ibero-American mathematics in the 19th and 20th centuries, no Congresso Internacional dos Matemáticos de Madrid, foi feita uma homenagem a Monteiro, e simultaneamente foram lançadas as suas obras em livro (número limitado de exemplares) e em CD-ROM [7], numa edição conjunta da Fundação Calouste Gulbenkian e da Humboldt Press de Londres. O CD ROM só ficou comercialmente disponível em 2008.

Podemos terminar com duas citações, uma de um seu aluno argentino, outra de um aluno brasileiro. Ambas dão conta não só da grande influência matemática de Monteiro, respectivamente na Argentina e no Brasil, mas igualmente revelam o carisma deste matemático que se dedicava por completo à missão que se tinha atribuído, e que, pelo seu empenho e atitude, modificava a vida daqueles que com ele trabalhavam.

Roberto Cignoli (1938-2018), um dos alunos argentinos de Monteiro, escreveu no prefácio da excelente Fotobiografia que a Sociedade Portuguesa de Matemática publicou em 2007 [8], na celebração dos cem anos do nascimento de António Monteiro:

> "António Aniceto Monteiro dejó profundas huellas de su paso por los tres países en los que actuó: Portugal, Brasil y Argentina. En los tres debió afrontar penurias morales y económicas, que no consiguieron doblegar su espiritú de luchador incansable en pro de la investigación matemática, la que consideraba un aporte esencial para el desarollo científico de los países."

Igualmente é muito significativo o depoimento prestado por Paulo Ribenboim nos Anais do Encontro Internacional realizado em 2007 em Lisboa para celebrar os cem anos do nascimento de António Monteiro e publicados como número especial do Boletim da SPM [9]. Por questões de saúde não foi possível a Ribenboim viajar para participar no Encontro, mas não quis deixar de marcar presença e enviou um texto para ser lido no seu início, intitulado "Lembrando Monteiro", que conclui deste modo:

> "Aos jovens, o carisma e a honestidade intelectual de Monteiro eram exemplares e um modelo que não me abandonou.[...] O Monteiro foi o primeiro – como (não) se diz em inglês "the first but not the least" - de uma trindade

FIGURA 3. António Monteiro (à esquerda) e sua esposa, Lídia Monteiro, no casamento de seu aluno Roberto Cignoli (à direita), aqui com a esposa, Carmen Cignoli. Foto de Maio de 1965. Foto do espólio de António Monteiro, gentilmente cedida por Jorge Rezende.

> de matemáticos que me formaram, juntamente com o Dieudonné e o Krull, a quem devo uma grande parte do que me tornei. Minha opinião sobre os "grandes homens" é clara: não são os generais, nem os politicos, mas os cientistas, artistas e os matemáticos, que são os cientistas-artistas. Monteiro foi um grande homem."

António Aniceto Monteiro foi de facto uma figura notável da história científica do século XX, deixando profundamente gravada a sua acção em Portugal, no Brasil e na Argentina.

Notas

[1] A sua tese intitula-se "Sur l'aditivité des noyaux de Fredholm".

[2] Nesta geração pontificaram, entre outros, Hugo Ribeiro (1910-1988), Ruy Luis Gomes (1905-1984), Bento de Jesus Caraça (1901-1948), Armando Gibert (1914-1985), Manuel Zaluar Nunes (1907-1967), João Remy Freire (1917-1992), José Sebastião e Silva (1914-1972) e José da Silva Paulo (1905-1976).

[3] Embora a publicação não tenha sido continua.

[4] "Núcleo de Matemática, Física e Química" (1936), "Centro de Estudos Matemáticos Aplicados à Economia" (1938), "Seminário de Análise Geral" (1939), "Centro de Estudos Matemáticos de Lisboa" (1940), "Centro de Estudos Matemáticos do Porto" (1942). Igualmente começaram a ser publicados em 1943 os Cadernos de Análise Geral com trabalhos deste grupo de matemáticos em cinco séries: ´Álgebra Moderna, Topologia Geral, Teoria da Medida e Integração, Geometria das Distâncias, e Teoria das Estruturas e Problemas de Fundamentos.

[5] Na época o grau de livre-docente era equivalente ao de doutor. Agradeço esta informação ao Professor Clóvis Pereira da Silva.

[6] Matemático espanhol que abandonou a Espanha no fim da Guerra Civil e emigrou, primeiro para França, onde trabalhou no Instituto Henri Poincaré, e depois,

devido ao começo da 2ª Guerra Mundial, para a América do Sul. Esteve primeiro em Cuba e depois fixou-se na Argentina em 1942, onde permaneceu até 1956, tendo então regressado a Espanha.

[7] The Works of António A. Monteiro (editores: E. Ortiz, A. Pereira Gomes e J P Kahane), Fundação Calouste Gulbenkian, Lisbon- The Humboldt Press, London, 2008.

[8] António Aniceto Monteiro Uma fotobiografia a várias vozes/una fotobiografía a varias voces (coordenadores: J. Rezende, L. Monteiro e E. Amaral), Sociedade Portuguesa de Matemática, Lisboa, 2007. Jorge Rezende tem neste momento um artigo muito desenvolvido sobre a passagem de Monteiro no Brasil, intitulado "O Estrangeiro Indesejável: O Brasil e António Aniceto Monteiro (lutas, tramas, diplomacias e polícias)" a sair brevemente no número 39 de Cultura, Revista de História e Teoria de Ideias, publicação do CHAM, Centro de Humanidades.

[9] Actas do Colóquio do Centenário de António Aniceto Monteiro (1907-1980), Editor: Luis Saraiva, Boletim da Sociedade Portuguesa de Matemática, Número Especial, Lisboa, 2008. Estes Anais incluiem o artigo de António Videira "António Monteiro no Brasil (1945-1949): uma breve passagem com resultados duradouros", pp. 183-211. O número 19 da Portugaliae Mathematica, de 1980, de homenagem a Monteiro, inclui o artigo de Leopoldo Nachbin "The Influence of António A. Ribeiro Monteiro in the Development of Mathematics in Brazil", pp. XV-XVII.

Luís Saraiva é Professor Associado do Departamento de Matemática da Faculdade de Ciências da Universidade de Lisboa e investigador do Centro Interuniversitário de História da Ciência e da Tecnologia (CIUHCT).

Email address: lmsaraiva@fc.ul.pt

RMU
REVISTA MATEMÁTICA UNIVERSITÁRIA

SBM
SOCIEDADE BRASILEIRA DE MATEMÁTICA

Revista Matemática Universitária, vol. 2, 2021
ISSN: 2675-5254 — **DOI:** 10.21711/26755254/rmu20218

SOBRE MATRIZES DE TRANSFERÊNCIA E O TEOREMA DE PERRON-FROBENIUS

EVERTON ARTUSO

Resumo. Nesse trabalho introduzimos o formalismo das matrizes de transferência e sua aplicabilidade, via Teorema de Perron-Frobenius, na teoria de transições de fase. Apresentamos dois modelos estatísticos unidimensionais, dentre os quais um de interesse biológico proposto por Kittel e que exibe o fenômeno de transição de fases.

1. Introdução

Em 1907, Oskar Perron publicou em [13] resultados sobre o espectro de matrizes positivas irredutíveis, dentre os quais, mostra que tal matriz possui um autovalor maximal, simples e estritamente positivo, cujo módulo é o raio espectral e não há nenhum outro autovalor com mesmo módulo, com autovetor associado cujas componentes também são estritamente positivas. Em 1912, Ferdinand Georg Frobenius estende em [6] alguns dos resultados de Perron, agora válidos para matrizes não negativas. Uma demonstração muito elegante do Teorema de Perron-Frobenius pode ser encontrada em [14], a qual será reproduzida em detalhes no Apêndice A. O Teorema de Perron-Frobenius tem aplicação nas mais variadas áreas, como por exemplo Equações Diferenciais Ordinárias e Parciais (Método numérico dos três pontos [10]), Economia (Modelo Econômico de Leontiev e Estabilidade de Mercados Competitivos [19]), Física (Mecânica Estatística [17]), Probabilidade e Estatística (Cadeias de Markov [4] e Modelos populacionais [8]), Saúde Pública (Epidemiologia [3]) entre outras.

O fato do Teorema de Perron-Frobenius garantir que o autovalor maximal de matrizes primitivas é simples e estritamente positivo gera consequências muito importantes na teoria da termodinâmica de sistemas físicos, por exemplo, de modo que em muitos sistemas de spins unidimensionais, a pressão - função analítica que depende da temperatura - coincide, a menos de uma constante multiplicativa, com o logaritmo natural de tal autovalor. Por definição, a *pressão* é dada como uma

Data de aceitação: Fevereiro de 2021.
Palavras chave. Matriz de Perron-Frobenius, autovalor maximal, transição de fase.

média do logaritmo da função de partição, uma quantidade que normaliza a distribuição de probabilidade de estado estacionário de configurações microscópicas, no limite termodinâmico. Já uma *transição de fase* é geralmente definida como uma singularidade da pressão em alguma das suas variáveis.

Do ponto de vista experimental, é possível distinguir entre dois tipos de transição de fase: as transições de primeira ordem, nas quais ocorre a coexistência de fases, como por exemplo um sólido de alta densidade e um fluido de baixa densidade; e as transições contínuas (de segunda ordem) nas quais flutuações e correlações crescem a tal ponto que seja macroscopicamente observável. De uma perspectiva termodinâmica, a compreensão de transições de primeira ordem se dá associando a cada fase uma *energia livre* (o que estamos denominando como pressão). A fase escolhida pelo sistema, dados certos parâmetros externos, é aquela com a menor energia livre de modo que uma transição de fase ocorre quando as energias livres de duas (ou mais) fases são iguais. Mudanças repentinas em quantidades macroscopicamente mensuráveis que ocorrem em transições de primeira ordem são descritas matematicamente como descontinuidades na primeira derivada da energia livre. Já as descontinuidades em derivadas de ordem superior estão relacionadas a transições de fase contínuas (de ordem superior). [1]

Um dos modelos que tradicionalmente introduz o método da matriz de transferência é o conhecido modelo de Ising, que em uma dimensão não apresenta transição de fase, mas em maiores dimensões tais transições ocorrem [5], [17]. Em particular, a técnica da matriz de transferência foi utilizada por Onsager em [12] na solução original do modelo de Ising em duas dimensões.

Outro exemplo é o modelo de Kittel resolvido via matriz de transferência (conforme [2]), cuja solução original utilizou séries geométricas, em [9]. Aplicar a técnica da matriz de transferência nesse modelo se caracteriza como um recurso didático, uma vez que tal recurso é rico em detalhes. Este modelo unidimensional não se encaixa completamente nas hipóteses do Teorema de Perron-Frobenius (fato este apontado pelo próprio Kittel em [9]), o que enriquece a discussão, uma vez que apresenta transição de fase conforme o número de configurações do seu espaço de estados; a saber, se o espaço de estados (ou seja, o conjunto de estados que um sítio da rede unidimensional pode assumir) tiver apenas dois estados (fechado e aberto), o modelo não apresenta transição de fase, todavia a transição ocorre se houver mais estados (diferentes estados para distintas forma de abertura, por exemplo). A técnica da matriz de transferência será utilizada a fim de mostrar que a transição de fase está associada à degenerescência do seu autovalor máximo.

Inicialmente enunciamos o Teorema de Perron-Frobenius e um Teorema auxiliar e depois os aplicamos, juntamente com o formalismo da matriz de transferência, aos modelos de Ising e de Kittel. Por fim, demonstramos o Teorema de Perron-Frobenius no Apêndice A.

2. Matriz de Perron-Frobenius

Uma matriz $M = (m_{i,j})_{0 \leq i,j \leq s-1}$ é dita *não negativa* se cada uma das suas entradas for não negativa. Em outros termos, para todo $i, j \in \{0, \ldots, s-1\}$, $m_{ij} \geq 0$. Uma matriz não negativa M é dita *irredutível* se, para todo i, j existe algum $k \geq 1$ tal

que $m_{ij}^{(k)} > 0$, denotando por $(m_{ij}^{(k)})$ as entradas da k-ésima potência de M, a saber, M^k. Ela é dita *primitiva* se M^k é positiva para algum $k \geq 1$, isto é, todos os $m_{ij}^{(k)} > 0$ para o mesmo k, e o menor k tal que isso acontece é chamado de *índice de primitividade* de M.

Teorema 2.1 (Perron-Frobenius)**.** [14] *Seja M uma matriz primitiva. Então*

(i) *M admite um autovalor θ tal que $|\lambda| < \theta$ para quaisquer outros autovalores λ de M.*

(ii) *Existe um autovetor com todas as entradas positivas associado ao autovalor θ.*

(iii) *θ é um autovalor simples, ou seja, tem multiplicidade algébrica um.*

Demonstração. Apresentaremos a demonstração do teorema no apêndice A.

O Teorema de Perron-Frobenius apresenta várias aplicações, muitas das quais apresentadas em [11], onde também encontramos diversas demonstrações do referido Teorema.

2.1. **Transição de Fase.** Muitas vezes, transições de fase podem ser detectadas por meio de singularidades na energia livre no limite termodinâmico, ou seja, a quebra de analiticidade da pressão topológica. A pressão, por sua vez, coincide com o maior autovalor (também dependente da temperatura e do campo magnético) da matriz de transferência. As ferramentas essenciais para a execução dessa análise são o Teorema de Perron-Frobenius e outro teorema que garante a analiticidade dos autovalores da matriz de transferência.

Embora fundamental, o Teorema de Perron-Frobenius não é suficiente para mostrar se há ou não transição de fase quando as entradas da matriz de transferência dependem do parâmetro $\beta = 1/kT$, associado ao inverso da temperatura. Nesse caso temos uma família de matrizes dependendo da temperatura, $M(\beta)$, e precisamos de outro resultado válido para matrizes analíticas em β (ou seja, todos os seus elementos são funções analíticas de β).

Teorema 2.2. [2] *Para todo β em um conjunto simplesmente conexo $D \subset \mathbb{C}$, seja $M(\beta)$ um operador linear em um espaço vetorial X n-dimensional ($M(\beta)$ é uma matrix complexa $n \times n$). Se $M(\beta)$ for analítica em D então cada um dos s autovalores de $M(\beta)$ têm multiplicidade constante e cada um deles pode ser expresso como uma função analítica em D, $\lambda_j(\beta)$, $j \in \{1, \ldots, s\}$.*

Demonstração. A demonstração deste resultado exige conhecimentos prévios em assuntos como conexidade, singularidades, polos removíveis, entre outros, fugindo do escopo do trabalho. Tal demonstração encontra-se em [7], Capítulo II, Teorema 1.8. ■

Assim, para uma matriz de transferência não negativa irredutível $M(\beta)$ - caso mais geral do que o que demonstramos (matriz primitiva) - cujos elementos são funções analíticas em uma vizinhança do eixo real positivo, $\beta > 0$, os Teoremas 2.1 e 2.2 garantem que o autovalor maximal (portanto a pressão) é uma função analítica de β, para todo $\beta > 0$. Para matrizes não negativas irredutíveis, o Teorema pode ser encontrado em [18].

3. Modelo de Ising

Consideremos uma amostra de algum material cujos átomos estão arranjados em uma estrutura regular cristalina. Suponhamos que cada um desses átomos carrega um momento magnético (algo como um ímã ligado a cada átomo) chamado de *spin*. Assumamos que cada spin tem a tendência de se alinhar com seus vizinhos e que, inicialmente, esteja orientados aleatoriamente, como na Figura 1. Nessa seção, nos baseamos em [5].

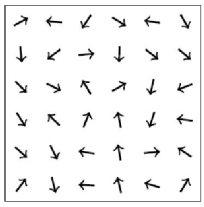


Figura 1. [5] Estado inicial.

Se o material é exposto a um campo magnético externo apontando numa direção específica, então um tipo de ordem aparece: os spins tendem a se alinhar com o campo, e assim apontam na mesma direção. Se diminuímos devagar a intensidade do campo externo até zero, dois casos podem ocorrer.

Na Figura 2, a ordem global é progressivamente perdida conforme o campo decresce, chegando a zero, quando os spins tornam-se desordenados novamente, como no seu estado inicial. Tal comportamento é chamado *paramagnético*.

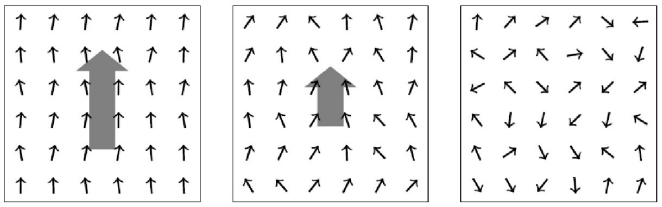


Figura 2. [5] Campo magnético decrescente.

Esse fenômeno pode ser medido quantitativamente ao se introduzir a *magnetização*, que é a média dos spins, projetada na direção do campo magnético. Para o paramagneto, conforme o campo decresce de um valor positivo para zero (mantendo a direção fixada), ou similarmente, se ele cresce de um valor negativo para zero, a magnetização tende a zero, como na Figura 3.

Ainda outro cenário é possível: como o campo externo decresce, a ordem global decresce, mas a interação local entre os spins é forte o suficiente para manter o material em estado de magnetização global mesmo depois que o campo externo tenha alcançado zero. Tal comportamento é chamado *ferromagnetismo*, representado na Figura 4.

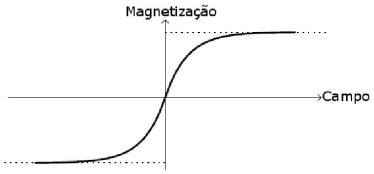


FIGURA 3. [5]

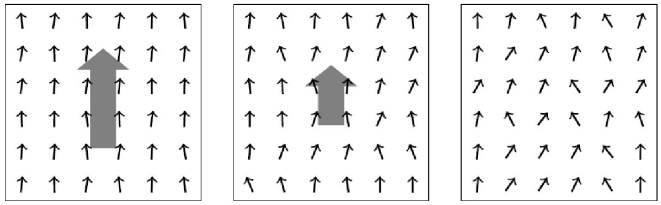


FIGURA 4. [5] Ferromagnetismo.

Um ferromagneto exibe, portanto, *magnetização espontânea*, que é uma ordem global produzida mesmo com a ausência de um campo magnético externo. O valor da magnetização espontânea, $\pm m^*$, depende da forma em que o campo externo se aproxima de zero (de > 0 ou < 0), representado na Figura 5.

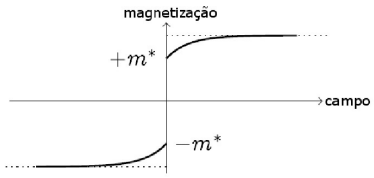


FIGURA 5. [5] Magnetização espontânea.

Usando o processo descrito, pode-se, a princípio, preparar um material ferromagnético com magnetização espontânea em uma direção arbitrária aplicando o campo magnético nessa direção, e fazê-lo decrescer lentamente a zero. Pode-se observar ainda que, na Figura 5, quando o campo vai para zero, a magnetização tem uma descontinuidade e salta de um valor estritamente positivo para uma valor estritamente negativo, o que representa uma *transição de fase* de primeira ordem.

O modelo de Ising é um modelo simples que busca reproduzir as propriedades descritas acima. A principal simplificação é assumir que os spins são restritos a uma direção particular, apontando para cima ou para baixo. Apesar de ser um modelo simples, é útil na descrição de outros sistemas (tais como um gás) que, com as devidas simplificações, pode ser mapeado pelo modelo de Ising. Para mais detalhes, veja [5].

3.1. **Sistema de spins de Ising.** Os spins podem ser encontrados em dois estados, tradicionalmente denotados por $+1$ ("para cima") e -1 ("para baixo"), e interagem

com cada outro spin e com o campo magnético externo. Esses spins serão identificados com os nós (vértices) de um grafo, que será o modelo da estrutura cristalina.

Considere um conjunto finito de pontos V com a estrutura de grafo não orientado sem loops e com no máximo uma aresta entre cada par de pontos. Quando $\{i, j\}$ é uma aresta do grafo, diremos que $j \in V$ é um *vizinho* de $i \in V$. Em cada sítio $i \in V$ encontra-se uma variável ς_i tomando dois possíveis valores, ± 1. Um estado microscópico do sistema, geralmente chamado de *configuração*, é dado pelo estado específico dos spins em cada vértice, isto é, por um elemento $\omega \in \Omega_V := \{-1, 1\}^V$. A variável aleatória $\varsigma_i : \Omega_V \to \{-1, 1\}$ definida por $\varsigma_i(\omega) := \omega_i$ dá o valor do spin no vértice i, e a configuração ω é também geralmente chamada de spin em i.

As interações entre os spins são definidas de tal forma que:

- *Os spins interagem somente com os spins localizados em sua vizinhança* (no sentido de grafos). Assumindo que os spins em dois sítios distintos $i, j \in V$ interagem se, e só se, o par $\{i, j\}$ é uma aresta do grafo, que denotamos por $i \sim j$.
- *A interação deve favorecer a concordância entre os valores dos spins.* Na forma mais simples do modelo, a qual é tratada aqui, isto é feito da seguinte forma: um par de spins nos vértices i e j de uma aresta *diminui* a energia global das configurações se elas concordam ($\varsigma_i = \varsigma_j$), e *aumenta* a energia global se elas diferem. Mais precisamente, os spins nos vértices das arestas $\{i, j\}$ contribuem para a energia total por uma quantidade $-\beta\varsigma_i\varsigma_j$, onde $\beta \geq 0$ mede a força da interação, e também interpreta o inverso da temperatura. Assim, em baixas temperaturas, configurações nas quais a maioria dos pares de vizinhos estão alinhados tem menor energia.
- *Cada spin pode interagir com um campo magnético externo.* No caso de um campo magnético externo constante $h \in \mathbb{R}$ agindo sobre o sistema, sua interação com o spin no sítio i contribui para a energia total pela quantidade $-h\varsigma_i$. Isto é, quando o campo magnético é positivo, as configurações com maioria dos seus spins iguais a $+1$ tem menor energia.

A *energia* de uma configuração ω é obtida através da soma das interações sobre todos os pares, e pela adição da interação de cada spin com o campo magnético:

$$H := -\beta \sum_{i \sim j} \varsigma_i \varsigma_j - h \sum_i \varsigma_i. \tag{1}$$

A função H é também conhecida como o *Hamiltoniano*. De acordo com a Mecânica Estatística, a probabilidade de observação do sistema na configuração ω é dada por

$$\mu(\omega) := \frac{1}{Z} \exp(-H(\omega)), \tag{2}$$

onde $e^{-H(\omega)}$ é conhecido como *peso de Boltzmann*. A constante de normalização

$$Z := \sum_{\omega \in \Omega_V} \exp(-H(\omega)) \tag{3}$$

desempenha um importante papel na teoria, e é conhecida como *função de partição*.

Dois pontos $i, j \in \mathbb{Z}$ são *vizinhos próximos* se $|j-i| = 1$, que denotamos por $i \sim j$. Denotamos por V_N uma *caixa de tamanho linear* N unidimensional,

$$V_N := \{x \in \mathbb{Z} : 0 \leq x < N\}. \tag{4}$$

Para mais detalhes, veja [5].

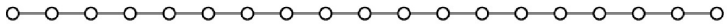


FIGURA 6. [5] Caixa unidimensional.

O objetivo é estudar o modelo de Ising em uma caixa grande V_N. Assim, iremos considerar o modelo através de uma sequência de caixas crescentes $V_1, V_2, \ldots, V_N, \ldots$, e descrever o seu comportamento no *limite termodinâmico*, isto é, quando $N \to \infty$. A *pressão* é dada pelo limite (quando este existir)

$$\psi(\beta, h) := \lim_{N\to\infty} \frac{1}{|V_N|} \log Z_{V_N,\beta,h}. \tag{5}$$

Uma *transição de fase* é geralmente definida como uma singularidade da pressão em alguma das suas variáveis.

Seja T_N o grafo obtido por ligar $N-1$ com 0 em $V_N = \{0, 1, \ldots, N-1\}$ como um toro (Figura 7). Formalmente, T_N é obtido de V_N adicionando-lhe uma aresta entre $N-1$ e 0.

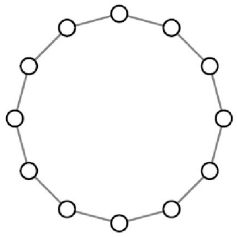


FIGURA 7. [5] Envolvendo V_N em um toro T_N.

Iremos calcular $\psi_\beta(h)$ usando o toro T_N ao invés de V_N. A saber, como o grafo T_N pode ser obtido e V_N adicionando-lhe uma aresta (conectando $N-1$ a 0), temos

$$-\beta \leq H_{V_N,\beta,h}(\omega) - H_{T_N,\beta,h}(\omega) \leq \beta.$$

Por consequência, $e^{-\beta} Z_{T_N,\beta,h} \leq Z_{V_N,\beta,h} \leq e^{\beta} Z_{T_N,\beta,h}$. Assim, se existe, o limite é

$$\lim_{N\to\infty} \frac{1}{|V_N|} \log Z_{T_N,\beta,h} = \psi_\beta(h). \tag{6}$$

A vantagem de se trabalhar com T_N ao invés de V_N é que $Z_{T_N,\beta,h}$ pode ser escrito como o traço de uma matriz 2×2. De fato, definindo $\omega_N = \omega_0$,

(7)

$$Z_{T_N,\beta,h} = \sum_{\omega\in\Omega_{V_N}} e^{-H_{V_N,\beta,h}(\omega)} = \sum_{\substack{\omega_j=\pm 1 \\ j\in\{0,\ldots,N-1\}}} \prod_{i=0}^{N-1} e^{\beta\omega_i\omega_{i+1}+h\omega_i} = \sum_{\substack{\omega_j=\pm 1 \\ j\in\{0,\ldots,N-1\}}} \prod_{i=0}^{N-1} A_{\omega_i,\omega_{i+1}},$$

onde os números $A_{+,+} = e^{\beta+h}$, $A_{+,-} = e^{-\beta+h}$, $A_{-,+} = e^{-\beta-h}$ e $A_{-,-} = e^{\beta-h}$ podem ser colocados na forma de uma matriz, chamada de *matriz de transferência*:

$$A = \begin{pmatrix} e^{\beta+h} & e^{-\beta+h} \\ e^{-\beta-h} & e^{\beta-h} \end{pmatrix}. \tag{8}$$

Uma observação útil é que $Z_{T_N,\beta,h}$ pode ser interpretado com o traço da N-ésima potência de A:

$$Z_{T_N,\beta,h} = \sum_{\omega_0=\pm 1} (A^N)_{\omega_0,\omega_0} := tr(A^N). \tag{9}$$

Tal fato pode ser provado utilizando o princípio da indução forte. Usando a condição de contorno $\omega_{N+1} = \omega_0$, para $N = 2$, temos

$$\begin{aligned} \sum_{\substack{w_j=\pm 1 \\ j=0,1}} \prod_{i=0}^{1} A_{\omega_i,\omega_{i+1}} &= \sum_{\substack{w_j=\pm 1 \\ j=0,1}} A_{\omega_0,\omega_1} A_{\omega_1,\omega_0} \\ &= A_{+,+}A_{+,+} + A_{+,-}A_{-,+} + A_{-,+}A_{+,-} + A_{-,-}A_{-,-} \\ &= (A_{1,1}A_{1,1} + A_{1,2}A_{2,1}) + (A_{2,1}A_{1,2} + A_{1,1}A_{1,1}) \\ &= \left(A^2\right)_{1,1} + \left(A^2\right)_{2,2} = tr\left(A^2\right). \end{aligned}$$

Faremos o caso $N = 3$ para clarear o raciocínio:

$$\begin{aligned} \sum_{\substack{w_j=\pm 1 \\ j=0,1,2}} \prod_{i=0}^{2} A_{\omega_i,\omega_{i+1}} &= \sum_{\substack{w_j=\pm 1 \\ j=0,1,2}} A_{\omega_0,\omega_1} A_{\omega_1,\omega_2} A_{\omega_2,\omega_0} \\ &= A_{1,1}A_{1,1}A_{1,1} + A_{1,1}A_{1,2}A_{2,1} + A_{1,2}A_{2,1}A_{1,1} + A_{1,2}A_{2,2}A_{2,1} \\ &+ A_{2,1}A_{1,1}A_{1,2} + A_{2,1}A_{1,2}A_{2,2} + A_{2,2}A_{2,1}A_{1,2} + A_{2,2}A_{2,2}A_{2,2} \\ &= A_{1,1}\left(A^2\right)_{1,1} + A_{1,2}\left(A_{2,1}A_{1,1} + A_{2,2}A_{2,1}\right) \\ &+ A_{2,1}\left(A_{1,2}A_{2,2} + A_{1,1}A_{1,2}\right) + A_{2,2}\left(A^2\right)_{2,2} \\ &= A_{1,1}\left(A^2\right)_{1,1} + A_{1,2}\left(A^2\right)_{2,1} + A_{2,1}\left(A^2\right)_{1,2} + A_{2,2}\left(A^2\right)_{2,2} \\ &= \left(A^3\right)_{1,1} + \left(A^3\right)_{2,2} = tr\left(A^3\right). \end{aligned}$$

Note que, para $s \geq 0$,

$$tr\left(A^N\right) = \sum_{i=1,2} \left(A^{N-s}A^s\right)_{i,i} = \sum_{i=1,2}\sum_{k=1,2} \left(A^{N-1}\right)_{i,k} \left(A^s\right)_{k,i}. \tag{10}$$

Supondo que a igualdade (9) seja válida para qualquer $t \leq N$, $t \in \mathbb{N}$, vamos provar para $N+1$: De fato, como $\sum_{w_N=\pm 1} A_{\omega_{N-1},\omega_N} A_{\omega_N,\omega_0} = \left(A^2\right)_{\omega_{N-1},\omega_0}$, temos

$$\begin{aligned}
\sum_{\substack{w_j=\pm 1 \\ j\in\{0,\ldots,N\}}} \prod_{i=0}^{N} A_{\omega_i,\omega_{i+1}} &= \sum_{\substack{w_j=\pm 1 \\ j\in\{0,\ldots,N\}}} A_{\omega_0,\omega_1} A_{\omega_1,\omega_2} \ldots A_{\omega_{N-1},\omega_N} A_{\omega_N,\omega_0} \\
&= \sum_{w_N=\pm 1} \left(\sum_{\substack{w_j=\pm 1 \\ j\in\{0,\ldots,N-1\}}} A_{\omega_0,\omega_1} \ldots A_{\omega_{N-2},\omega_{N-1}} \right) A_{\omega_{N-1},\omega_N} A_{\omega_N,\omega_0} \\
&= \sum_{\substack{w_j=\pm 1 \\ j\in\{0,N-1\}}} \left(A^{N-1}\right)_{\omega_0,\omega_{N-1}} \left(A^2\right)_{\omega_{N-1},\omega_0} \\
&= \sum_{w_0=\pm 1} \left(A^{N+1}\right)_{\omega_0,\omega_0} = tr\left(A^{N+1}\right).
\end{aligned}$$

Assim, reduzimos o problema de encontrar a função de partição ao de encontrar a soma dos elementos diagonais (traço) da N-ésima potência da matriz de transferência. Por outro lado, o traço de matriz, na base conveniente, é simplesmente a soma de seus autovalores, e os autovalores de A^N são $\lambda_\pm^N$, uma vez que $\lambda_\pm$ são os autovalores de A determinados pelo polinômio característico resultante de

$$\begin{vmatrix} e^{\beta+h} - \lambda & e^{-\beta+h} \\ e^{-\beta-h} & e^{\beta-h} - \lambda \end{vmatrix} = 0, \tag{11}$$

dado por

$$\lambda^2 - \lambda e^{\beta}\left(e^h + e^{-h}\right) + \left(e^{2\beta} - e^{-2\beta}\right) = 0, \tag{12}$$

cujas soluções são

$$\begin{aligned}
\lambda_\pm &= \frac{1}{2}\left[e^{\beta}\left(e^h + e^{-h}\right) \pm \sqrt{e^{2\beta}\left(e^h + e^{-h}\right)^2 - 4\left(e^{2\beta} - e^{-2\beta}\right)}\right] \\
&= \frac{1}{2}\left[e^{\beta}\left(2\cosh(h)\right) \pm \sqrt{e^{2\beta}\left(2\sinh(h)\right)^2 - 4(2\sinh(2\beta))}\right] \\
&= e^{\beta}\cosh(h) \pm \sqrt{e^{2\beta}\cosh^2(h) - 2\sinh(2\beta)}, \qquad (13)
\end{aligned}$$

em que utilizamos as identidades $e^x - e^{-x} = 2\sinh(x)$ e $e^x + e^{-x} = 2\cosh(x)$. Assim A tem dois dois autovalores $\lambda_+ > \lambda_-$ dados por

$$\lambda_\pm = e^{\beta}\cosh(h) \pm \sqrt{e^{2\beta}\cosh^2(h) - 2\sinh(2\beta)}. \tag{14}$$

Como A pode ser diagonalizado, $A = BDB^{-1}$ onde D é uma matriz diagonal cujos elementos da diagonal são λ_+ e λ_-, e como o traço satisfaz $tr(GH) = tr(HG)$, temos

$$Z_{T_N,\beta,h} = tr(A^N) = tr(BD^NB^{-1}) = tr(D^N) = \lambda_+^N + \lambda_-^N, \tag{15}$$

o que pode ser escrito como

$$Z_{T_N,\beta,h} = \lambda_+^N \left(1 + \frac{\lambda_-^N}{\lambda_+^N}\right), \tag{16}$$

e como $\lambda_+ > \lambda_-$, tomando o limite termodinâmico temos

$$\psi_\beta(h) = \lim_{N\to\infty} \frac{1}{|V_N|} \log Z_{T_N,\beta,h} = \lim_{N\to\infty} \frac{1}{|V_N|} \log\left(\lambda_+^N \left(1 + \frac{\lambda_-^N}{\lambda_+^N}\right)\right) = \log \lambda_+. \tag{17}$$

Ou seja, $\psi_\beta(h) = \log \lambda_+$, e para todo $\beta \geq 0$, e todo $h \in \mathbb{R}$, a pressão $\psi_\beta(h)$ existe e é igual a

$$\psi_\beta(h) = \log\left\{e^\beta \cosh(h) + \sqrt{e^{2\beta}\cosh^2(h) - 2\sinh(2\beta)}\right\}, \tag{18}$$

que é uma função analítica.

Em outros termos, tratamos de um modelo simples, pois o fato da pressão não apresentar nenhuma quebra de analiticidade garante que o modelo de Ising unidimensional não apresenta coexistência de fases, não havendo, portanto, nenhuma transição de fase. Note que não precisamos utilizar os Teoremas 2.1 e 2.2 nessa abordagem. Todavia se, ao invés de realizarmos todos os cálculos para mostrar a analiticidade da pressão, aplicássemos diretamente os Teoremas 2.1 e 2.2 na Matriz de Transferência do modelo, uma vez que essa satisfaz suas hipóteses, garantiríamos a existência de um único autovalor simples e maximal $\lambda(\beta)$ e a analiticidade da função $\log(\lambda(\beta))$.

Em geral, o comportamento assintótico (quando $N \to \infty$) do sistema descrito pela distribuição de Gibbs em uma caixa suficientemente grande pode ser relacionado com as propriedades analíticas da pressão em h. Assumindo que o limite e as derivadas podem ser intercambiados (o que acontece sob certas circunstâncias, veja [15]),

$$\frac{\partial \psi_\beta(h)}{\partial h} = \lim_{N\to\infty} \frac{1}{|V_N|} \frac{\partial}{\partial h} \log Z_{V_N,\beta,h} = \lim_{N\to\infty} \left\langle \frac{M_N}{|V_N|} \right\rangle_{V_N,\beta,h} = m_\beta(h), \tag{19}$$

e portanto, a magnetização média está relacionada com a derivada da pressão.

A pressão $\psi_\beta(h)$ do Modelo de Ising unidimensional é analítica em h em todas as temperaturas. De fato, temos, pela equação (18),

$$\begin{aligned} m_\beta(h) = \frac{\partial \psi_\beta(h)}{\partial h} &= \frac{\frac{e^{2\beta}\cosh(h)\sinh(h)}{\sqrt{e^{2\beta}\cosh^2(h) - 2\sinh(2\beta)}} + e^\beta \sinh(h)}{\sqrt{e^{2\beta}\cosh^2(h) - 2\sinh(2\beta)} + e^\beta \cosh(h)} \\ &= \frac{\frac{e^{\beta}\cosh(h)\sinh(h)}{\sqrt{\cosh^2(h) - 2e^{-2\beta}\sinh(2\beta)}} + e^\beta \sinh(h)}{e^\beta\sqrt{\cosh^2(h) - 2e^{-2\beta}\sinh(2\beta)} + e^\beta \cosh(h)} \\ &= \frac{\frac{\cosh(h)\sinh(h)}{\sqrt{\cosh^2(h) - 2e^{-2\beta}\sinh(2\beta)}} + \sinh(h)}{\sqrt{\cosh^2(h) - 2e^{-2\beta}\sinh(2\beta)} + \cosh(h)}. \end{aligned} \tag{20}$$

Em particular, $\frac{\partial \psi_\beta}{\partial h}(0) = 0$. Somente no limite $\beta \to \infty$ a função $\psi_\beta(h)$ se torna não diferenciável em $h = 0$, pois

$$\lim_{\beta\to\infty} \frac{\partial \psi_\beta(h)}{\partial h} = \lim_{\beta\to\infty} \frac{\frac{\cosh(h)\sinh(h)}{\sqrt{\cosh^2(h)-2e^{-2\beta}\sinh(2\beta)}} + \sinh(h)}{\sqrt{\cosh^2(h) - 2e^{-2\beta}\sinh(2\beta)} + \cosh(h)}$$

$$= \frac{\frac{\cosh(h)\sinh(h)}{\sqrt{\cosh^2(h)-1}} + \sinh(h)}{\sqrt{\cosh^2(h) - 1} + \cosh(h)} = \begin{cases} 1 & \text{se } h > 0 \\ -1 & \text{se } h < 0 \end{cases}, \tag{21}$$

e o limite $\lim_{h\to 0}\lim_{\beta\to\infty} \frac{\partial \psi_\beta(h)}{\partial h}$ não existe. De fato, para qualquer $\beta > 0$, temos $m_\beta(h) = 1$ quando $h \to +\infty$, pois

$$\lim_{h\to\infty} m_\beta(h) = \lim_{h\to\infty} \frac{\frac{\cosh(h)\sinh(h)}{\sqrt{\cosh^2(h)-2e^{-2\beta}\sinh(2\beta)}} + \sinh(h)}{\sqrt{\cosh^2(h) - 2e^{-2\beta}\sinh(2\beta)} + \cosh(h)}$$

$$= \lim_{h\to\infty} \frac{\frac{(e^h+e^{-h})(e^h-e^{-h})}{\sqrt{(e^h+e^{-h})^2-4e^{-2\beta}(e^{2\beta}-e^{-2\beta})}} + e^h - e^{-h}}{\sqrt{(e^h+e^{-h})^2 - 4e^{-2\beta}(e^{2\beta}-e^{-2\beta})} + e^h + e^{-h}}$$

$$= \lim_{h\to\infty} \frac{\frac{e^h-e^{-3h}}{\sqrt{1+2e^{-h}+e^{-3h}-4e^{-2(\beta+h)}(e^{2\beta}-e^{-2\beta})}} + e^h - e^{-h}}{e^h\left(\sqrt{1+2e^{-h}+e^{-2h}-4e^{-2(\beta+h)}(e^{2\beta}-e^{-2\beta})} + 1 + e^{-2h}\right)}$$

$$= \lim_{h\to\infty} \frac{\frac{1-e^{-4h}}{\sqrt{1+2e^{-h}+e^{-3h}-4e^{-2(\beta+h)}(e^{2\beta}-e^{-2\beta})}} + 1 - e^{-2h}}{\sqrt{1+2e^{-h}+e^{-2h}-4e^{-2(\beta+h)}(e^{2\beta}-e^{-2\beta})} + 1 + e^{-2h}} = 1, \tag{22}$$

e, de modo similar, $m_\beta(h) = -1$ quando $h \to -\infty$. Portanto,

$$\lim_{\beta\to\infty} m_\beta(h) = \begin{cases} 1 & \text{se } h > 0 \\ -1 & \text{se } h < 0 \end{cases}, \tag{23}$$

a derivada da pressão não é contínua em 0 e ψ_β não é analítica no limite $\beta \to \infty$.

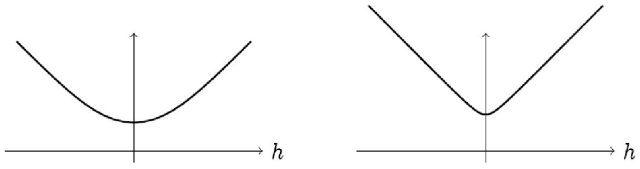


FIGURA 8. [5] A pressão $\psi_\beta(h)$ para $\beta = 0.8$ a esquerda e $\beta = 2$ a direita.

Pela expressão explicitada em (18) a aplicação $h \to \psi_\beta(h)$ é analítica e assim, diferenciável com respeito a h. Como mencionado anteriormente, a derivada da pressão representa a densidade de magnetização média $m_\beta(h) = \frac{\partial \psi_\beta(h)}{\partial h}$, que no caso do Modelo de Ising unidimensional, é representado na Figura 9.

Para mais detalhes, consulte [5] e [17].

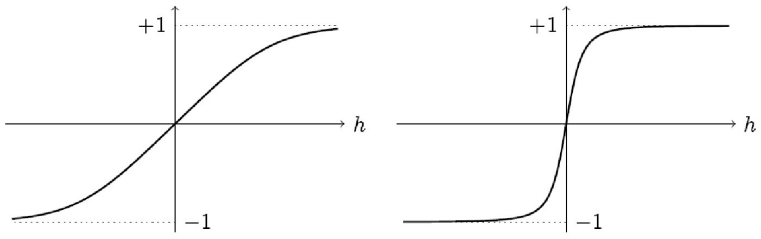


FIGURA 9. [5] $m_\beta(h)$ para $\beta = 0.8$ e $\beta = 2$.

4. Modelo de Kittel via matriz de transferência

O modelo de Kittel é de fato um modelo de 'zíper' (fecho de correr) de extremidade única, discutido "como uma boa maneira de introduzir um exemplo de biofísica em um curso de física estatística", e inspirado em modelos de 'zíper' duplo de polipeptídeo ou moléculas de DNA - Figura 10.

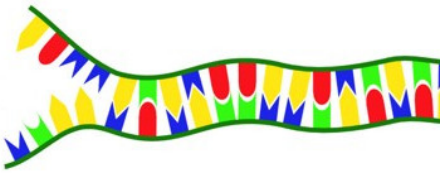


FIGURA 10. [20] O modelo de zíper de Kittel foi baseado em ligações de moléculas de DNA.

Conforme [9], vamos considerar um 'zíper' de N ligações que podem ser abertas apenas por uma extremidade. Se as ligações $1, 2, \ldots, n$ estão todas abertas, a energia necessária para abrir a ligação $n+1$ é ε; no entanto, se nem todas as ligações anteriores estiverem abertas, a energia necessária para abrir a ligação $n+1$ será infinita. A ligação N (a última) não pode ser aberta, e diz-se que o 'zíper' está aberto quando as primeiras $N-1$ ligações estiverem. Kittel supôs que existem G orientações que cada ligação aberta pode assumir, isto é, o estado aberto de uma ligação é *G-fold* degenerado, correspondendo a liberdade rotacional de uma ligação (esta pode assumir valores de 1 a G quando aberta). Não haverá transição de fase para $G = 1$ (neste caso temos $0 \leftrightarrow$ fechada e $1 \leftrightarrow$ aberta), como mostra [9]. A energia requerida para abrir as primeiras p ligações é $p\varepsilon$; se p ligações estiverem abertas, a degenerecência é G^p.

Para introduzir o contexto do formalismo do operador de transferência, conforme [2], vamos resolver o modelo de Kittel em termos de uma matriz de transferência (o caminho de Kittel envolve séries geométricas, é muito mais simples e rápido, veja [9], todavia, devido as suas particularidades, não é um procedimento facilmente aplicável a outros modelos para os quais a matriz de transferência funciona bem).

Para esse fim, vamos escrever o modelo Hamiltoniano como

$$H_N = \varepsilon\left(1-\delta_{s_1,0}\right) + \sum_{i=2}^{N-1}\left(\varepsilon + V_0\delta_{s_{i-1},0}\right)\left(1-\delta_{s_i,0}\right) \tag{24}$$

onde $s_i = 0$ significa que a ligação i está fechada, $s_i = 1, 2, \ldots, G$ significa que a ligação está aberta em um dos G possíveis estados, e $\delta_{s,s'}$ é o delta de Kronecker dado por

$$\delta_{s,s'} = \begin{cases} 1 & \text{se} \quad s = s' \\ 0 & \text{se} \quad s \neq s' \end{cases} . \tag{25}$$

A energia necessária para abrir a ligação s_i é dada por $\varepsilon + V_0\delta_{s_{i-1},0}$, de modo que se a ligação s_{i-1} estiver aberta, então $\delta_{s_{i-1},0} = 0$, e caso esteja fechada, uma das restrições de Kittel na elaboração do modelo é que, nesse caso, a energia para a abertura da ligação i seja infinita, de onde $V_0 = \infty$. Além disso, impusemos a condição de contorno $s_N = 0$ (a extremidade mais à direita do zíper está sempre fechada). A função de partição será dada por

$$Z_N = \sum_{conf.} \exp\left(-\beta H_N\right), \tag{26}$$

com $\beta = 1/kT$ sendo o inverso da temperatura e a soma é tomada sobre todas as configurações das variáveis s_i, para $i = 1, \ldots, N-1$.

Reescreveremos a função de partição (26) usando o fato que, para todo $i = 1, \ldots, N-1$, vale

$$1 + \left(e^{-\beta V_0} - 1\right)\delta_{s_i,0}\left(1-\delta_{s_{i+1},0}\right) = \begin{cases} e^{-\beta V_0} & \text{se} \quad s_{i+1} \neq 0 \\ 1 & \text{se} \quad s_{i+1} = 0 \end{cases} = e^{-\beta V_0 \delta_{s_i,0}\left(1-\delta_{s_{i+1},0}\right)}; \tag{27}$$

com efeito, se $s_i \neq 0$, o produto $\delta_{s_i,0}\left(1-\delta_{s_{i+1},0}\right)$ sempre se anula e a igualdade também ocorre, o que demonstra a igualdade (27). Aplicando a equação (24) na

equação (26), temos

$$\begin{aligned}
Z_N &= \sum_{conf.} \exp\left(-\beta H_N\right) = \sum_{conf.} \exp\left(-\beta\left[\varepsilon\left(1-\delta_{s_1,0}\right)+\sum_{i=2}^{N-1}\left(\varepsilon+V_0\delta_{s_{i-1},0}\right)\left(1-\delta_{s_i,0}\right)\right]\right)\\
&= \sum_{conf.} \exp\left(-\beta\varepsilon\left(1-\delta_{s_1,0}\right)\right)\exp\left(-\beta\sum_{i=2}^{N-1}\left(\varepsilon+V_0\delta_{s_{i-1},0}\right)\left(1-\delta_{s_i,0}\right)\right)\\
&= \sum_{conf.} \exp\left(-\beta\varepsilon\left(1-\delta_{s_1,0}\right)\right)\prod_{i=2}^{N-1}\exp\left(-\beta\left(\varepsilon+V_0\delta_{s_{i-1},0}\right)\left(1-\delta_{s_i,0}\right)\right)\\
&= \sum_{conf.} \exp\left(-\beta\varepsilon\left(1-\delta_{s_1,0}\right)\right)\prod_{i=1}^{N-2}\exp\left(-\beta\varepsilon-\beta\varepsilon\delta_{s_{i+1},0}-\beta V_0\delta_{s_i,0}+\beta V_0\delta_{s_i,0}\delta_{s_{i+1},0}\right)\\
&= \sum_{conf.} \exp\left(-\beta\varepsilon\left(1-\delta_{s_1,0}\right)\right)\prod_{i=1}^{N-2}e^{-\beta\varepsilon\left(1-\delta_{s_{i+1},0}\right)}e^{-\beta V_0\delta_{s_i,0}\left(1-\delta_{s_{i+1},0}\right)}\\
&\overset{(27)}{=}\overset{(28)}{=} \sum_{conf.} \exp\left(-\beta\varepsilon\left(1-\delta_{s_1,0}\right)\right)\prod_{i=1}^{N-2}e^{-\beta\varepsilon\left(1-\delta_{s_{i+1},0}\right)}\left[1+\left(e^{-\beta V_0}-1\right)\delta_{s_i,0}\left(1-\delta_{s_{i+1},0}\right)\right]
\end{aligned}$$

e portanto

$$Z_N = \sum_{conf.} e^{-\beta\varepsilon\left(1-\delta_{s_1,0}\right)}\prod_{i=1}^{N-2}e^{-\beta\varepsilon\left(1-\delta_{s_{i+1},0}\right)}\left[1+\left(e^{-\beta V_0}-1\right)\delta_{s_i,0}\left(1-\delta_{s_{i+1},0}\right)\right]. \tag{29}$$

A partir de agora, supomos que $V_0=\infty$, logo $e^{-\beta V_0}=0$. Considere a matriz de transferência $\mathcal{T}_{(G+1)\times(G+1)}=(t_{s,s'})$ definida como

$$t_{s,s'} = e^{-\beta\varepsilon\left(1-\delta_{s',0}\right)}\left[1-\delta_{s,0}\left(1-\delta_{s',0}\right)\right], \tag{30}$$

com $s,s'\in\{0,1,\ldots,G\}$, ou seja,

$$\mathcal{T} = \begin{pmatrix} 1 & 0 & \cdots & 0\\ 1 & e^{-\beta\varepsilon} & \cdots & e^{-\beta\varepsilon}\\ \vdots & \vdots & & \vdots\\ 1 & e^{-\beta\varepsilon} & \cdots & e^{-\beta\varepsilon}\end{pmatrix}. \tag{31}$$

A função de partição pode ser escrita como

$$Z_N = \sum_{\substack{s_i\in\{0,1,\ldots,G\}\\ i\in\{1,\ldots,N-1\}}} e^{-\beta\varepsilon\left(1-\delta_{s_1,0}\right)}\prod_{i=1}^{N-2}t_{s_i,s_{i+1}}. \tag{32}$$

É importante respeitar a restrição de Kittel na qual a ligação s_{i+1} não seja aberta (não pode tomar os valores 1 ou 2) se a ligação s_i for fechada ($s_i=0$) - a restrição diz que a energia para abrir a ligação s_i é infinita caso s_{i-1} esteja fechada. Isso produz entradas nulas na primeira linha da matriz.

A função de partição pode ser reescrita na forma

$$Z_N = \langle \psi, \mathcal{T}^{N-2}\phi \rangle \,. \tag{33}$$

para certos ψ e ϕ em $\mathbb{R}^{G+1}$ satisfazendo $\langle \psi, x\rangle > 0$ e $\langle \phi, x\rangle > 0$ para $x > 0$. Assim, para $\psi = \begin{pmatrix} 1 & e^{-\beta\varepsilon} & \cdots & e^{-\beta\varepsilon}\end{pmatrix}$ e $\phi^t = \begin{pmatrix} 1 & 1 & \dots & 1\end{pmatrix}$, temos

$$Z_N = \begin{pmatrix} 1 & e^{-\beta\varepsilon} & \cdots & e^{-\beta\varepsilon}\end{pmatrix} \mathcal{T}^{N-2} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} . \tag{34}$$

Inicialmente, vamos explorar a equação (34) para valores baixos. Para $N = 2$, temos

$$\begin{aligned} Z_2 &= \sum_{s_1\in\{0,1,\dots,G\}} e^{-\beta\varepsilon\left(1-\delta_{s_1,0}\right)} = e^{-\beta\varepsilon(1-\delta_{0,0})} + \sum_{s_1\in\{1,\dots,G\}} e^{-\beta\varepsilon\left(1-\delta_{s_1,0}\right)} \\ &= 1 + Ge^{-\beta\varepsilon} = \begin{pmatrix} 1 & e^{-\beta\varepsilon} & \cdots & e^{-\beta\varepsilon}\end{pmatrix} I_{G+1} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}, \end{aligned}$$

uma vez que $\delta_{s_1,0} = 1$ se $s_1 = 0$ e $\delta_{s_1,0} = 0$ se $s_1 \neq 0$, além de que $\mathcal{T}^{2-2} = \mathcal{T}^0 = I_{G+1}$. Para $N = 3$, temos

$$\begin{aligned} Z_3 &= \sum_{\substack{s_1\in\{0,1,\dots,G\}\\ s_2\in\{0,1,\dots,G\}}} e^{-\beta\varepsilon\left(1-\delta_{s_1,0}\right)} t_{s_1,s_2} = \sum_{s_2\in\{0,1,\dots,G\}} t_{0,s_2} + e^{-\beta\varepsilon} \sum_{\substack{s_1\in\{1,\dots,G\}\\ s_2\in\{0,1,\dots,G\}}} t_{s_1,s_2} \\ &= \begin{pmatrix} t_{0,0} & t_{0,1} & \cdots & t_{0,G}\end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} + e^{-\beta\varepsilon} \begin{pmatrix} t_{1,0} & t_{1,1} & \cdots & t_{1,G} \\ \vdots & \vdots & \ddots & \vdots \\ t_{G,0} & t_{G,1} & \cdots & t_{G,G}\end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \\ &\overset{(31)}{=} \begin{pmatrix} 1 & e^{-\beta\varepsilon} & \cdots & e^{-\beta\varepsilon}\end{pmatrix} \mathcal{T} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} . \end{aligned} \tag{35}$$

Mostremos a validade da equação (34) para todo $N \geq 2$. Pela equação (32), temos

$$\begin{aligned}
Z_N &= \sum_{\substack{s_i\in\{0,1,\ldots,G\}\\ i\in\{1,\ldots,N-1\}}} e^{-\beta\varepsilon\left(1-\delta_{s_1,0}\right)} \prod_{i=1}^{N-2} t_{s_i,s_{i+1}} \\
&= \sum_{\substack{s_i\in\{0,1,\ldots,G\}\\ i\in\{2,\ldots,N-1\}}} t_{0,s_2}\ldots t_{s_{N-2},s_{N-1}} + e^{-\beta\varepsilon} \sum_{\substack{s_i\in\{0,1,\ldots,G\}\\ i\in\{2,\ldots,N-1\}\\ s_1\in\{1,\ldots,G\}}} t_{s_1,s_2}\ldots t_{s_{N-2},s_{N-1}} \\
&\overset{(37)}{=} \sum_{s_{N-1}\in\{0,1,\ldots,G\}} t^{(N-2)}_{0,s_{N-1}} + e^{-\beta\varepsilon} \sum_{\substack{s_1\in\{1,\ldots,G\}\\ s_{N-1}\in\{0,1,\ldots,G\}}} t^{(N-2)}_{s_1,s_{N-1}} \\
&= \begin{pmatrix} t^{(N-2)}_{0,0} & t^{(N-2)}_{0,1} & \cdots & t^{(N-2)}_{0,G} \end{pmatrix} \begin{pmatrix} 1\\1\\\vdots\\1 \end{pmatrix} + e^{-\beta\varepsilon} \begin{pmatrix} t^{(N-2)}_{1,0} & t^{(N-2)}_{1,1} & \cdots & t^{(N-2)}_{1,G}\\ \vdots & \vdots & \ddots & \vdots\\ t^{(N-2)}_{G,0} & t^{(N-2)}_{G,1} & \cdots & t^{(N-2)}_{G,G} \end{pmatrix} \begin{pmatrix} 1\\1\\\vdots\\1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & e^{-\beta\varepsilon} & \cdots & e^{-\beta\varepsilon} \end{pmatrix} \begin{pmatrix} t^{(N-2)}_{0,0} & t^{(N-2)}_{0,1} & \cdots & t^{(N-2)}_{0,G}\\ t^{(N-2)}_{1,0} & t^{(N-2)}_{1,1} & \cdots & t^{(N-2)}_{1,G}\\ \vdots & \vdots & \ddots & \vdots\\ t^{(N-2)}_{G,0} & t^{(N-2)}_{G,1} & \cdots & t^{(N-2)}_{G,G} \end{pmatrix} \begin{pmatrix} 1\\1\\\vdots\\1 \end{pmatrix} \\
&\overset{(36)}{=} \begin{pmatrix} 1 & e^{-\beta\varepsilon} & \cdots & e^{-\beta\varepsilon} \end{pmatrix} \mathcal{T}^{N-2} \begin{pmatrix} 1\\1\\\vdots\\1 \end{pmatrix},
\end{aligned}$$

em que usamos, na terceira igualdade, que para todo $k \geq 2$, vale

$$t^{(k)}_{s_1,s_{k+1}} = \sum_{\substack{s_i\in\{0,1,\ldots,G\}\\ i\in\{2,\ldots,k\}}} t_{s_1,s_2}\ldots t_{s_k,s_{k+1}}. \tag{37}$$

A matriz $\mathcal{T}$ tem três autovalores distintos, a saber $\lambda_1 = Ge^{-\beta\varepsilon}$, $\lambda_2 = 1$ e $\lambda_3 = 0$, calculados via núcleo da matriz $\mathcal{T} - \lambda I$. Os autovetores dos dois autovalores não nulos são v_1 e v_2 dados, respectivamente, por

$$v_1 = \begin{pmatrix} 0\\1\\\vdots\\1 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 1-Ge^{-\beta\varepsilon}\\1\\\vdots\\1 \end{pmatrix}. \tag{38}$$

Os vetores $\begin{pmatrix}1 & e^{-\beta\varepsilon} & \cdots & e^{-\beta\varepsilon}\end{pmatrix}$ e $\begin{pmatrix}1 & 1 & \cdots & 1\end{pmatrix}$ podem ser escritos na base de autovetores $\{v_1, v_2\}$, a saber

$$\begin{pmatrix}1\\ e^{-\beta\varepsilon}\\ \vdots\\ e^{-\beta\varepsilon}\end{pmatrix} = \frac{e^{-\beta\varepsilon}\left(1-Ge^{-\beta\varepsilon}\right)-1}{1-Ge^{-\beta\varepsilon}}v_1 + \frac{1}{1-Ge^{-\beta\varepsilon}}v_2, \tag{39}$$

$$\begin{pmatrix}1\\ 1\\ \vdots\\ 1\end{pmatrix} = \frac{-Ge^{-\beta\varepsilon}}{1-Ge^{-\beta\varepsilon}}v_1 + \frac{1}{1-Ge^{-\beta\varepsilon}}v_2, \tag{40}$$

e como $\langle v_1, v_1\rangle = \langle v_1, v_2\rangle = \langle v_2, v_1\rangle = G$ e $\langle v_2, v_2\rangle = \left(1-Ge^{-\beta\varepsilon}\right)^2 + G$, temos

$$\begin{aligned}
Z_N &\overset{(34)}{=} \begin{pmatrix}1 & e^{-\beta\varepsilon} & \cdots & e^{-\beta\varepsilon}\end{pmatrix}\mathcal{T}^{N-2}\begin{pmatrix}1\\ 1\\ \vdots\\ 1\end{pmatrix}\\
&\overset{(39),(40)}{=} \left\langle \frac{e^{-\beta\varepsilon}\left(1-Ge^{-\beta\varepsilon}\right)-1}{1-Ge^{-\beta\varepsilon}}v_1 + \frac{1}{1-Ge^{-\beta\varepsilon}}v_2, \mathcal{T}^{N-2}\left(\frac{-Ge^{-\beta\varepsilon}}{1-Ge^{-\beta\varepsilon}}v_1 + \frac{1}{1-Ge^{-\beta\varepsilon}}v_2\right)\right\rangle\\
&= \left\langle \frac{e^{-\beta\varepsilon}\left(1-Ge^{-\beta\varepsilon}\right)-1}{1-Ge^{-\beta\varepsilon}}v_1 + \frac{1}{1-Ge^{-\beta\varepsilon}}v_2, \frac{-Ge^{-\beta\varepsilon}}{1-Ge^{-\beta\varepsilon}}\mathcal{T}^{N-2}(v_1) + \frac{1}{1-Ge^{-\beta\varepsilon}}\mathcal{T}^{N-2}(v_2)\right\rangle\\
&= \left\langle \frac{e^{-\beta\varepsilon}\left(1-Ge^{-\beta\varepsilon}\right)-1}{1-Ge^{-\beta\varepsilon}}v_1 + \frac{1}{1-Ge^{-\beta\varepsilon}}v_2, \frac{-Ge^{-\beta\varepsilon}}{1-Ge^{-\beta\varepsilon}}\lambda_1^{N-2}v_1 + \frac{1}{1-Ge^{-\beta\varepsilon}}\lambda_2^{N-2}v_2\right\rangle\\
&= \left\langle \frac{e^{-\beta\varepsilon}\left(1-Ge^{-\beta\varepsilon}\right)-1}{1-Ge^{-\beta\varepsilon}}v_1 + \frac{1}{1-Ge^{-\beta\varepsilon}}v_2, \frac{\left(-Ge^{-\beta\varepsilon}\right)\left(Ge^{-\beta\varepsilon}\right)^{N-2}}{1-Ge^{-\beta\varepsilon}}v_1 + \frac{1}{1-Ge^{-\beta\varepsilon}}v_2\right\rangle\\
&= \frac{-\left(Ge^{-\beta\varepsilon}\right)^{N-1}\left(1-Ge^{-\beta\varepsilon}\right)e^{-\beta\varepsilon} + \left(Ge^{-\beta\varepsilon}\right)^{N-1}}{\left(1-Ge^{-\beta\varepsilon}\right)^2}\langle v_1, v_1\rangle + \frac{e^{-\beta\varepsilon}\left(1-Ge^{-\beta\varepsilon}\right)-1}{\left(1-Ge^{-\beta\varepsilon}\right)^2}\langle v_1, v_2\rangle\\
&- \frac{\left(Ge^{-\beta\varepsilon}\right)^{N-1}}{\left(1-Ge^{-\beta\varepsilon}\right)^2}\langle v_2, v_1\rangle + \frac{1}{\left(1-Ge^{-\beta\varepsilon}\right)^2}\langle v_2, v_2\rangle\\
&= \frac{-\left(Ge^{-\beta\varepsilon}\right)^{N} + \left(Ge^{-\beta\varepsilon}\right)^{N+1} + Ge^{-\beta\varepsilon} - \left(Ge^{-\beta\varepsilon}\right)^2 + \left(1-Ge^{-\beta\varepsilon}\right)^2}{\left(1-Ge^{-\beta\varepsilon}\right)^2}\\
&= \frac{\left(1-\left(Ge^{-\beta\varepsilon}\right)^{N}\right)\left(1-Ge^{-\beta\varepsilon}\right)}{\left(1-Ge^{-\beta\varepsilon}\right)^2} = \frac{1-\left(Ge^{-\beta\varepsilon}\right)^{N}}{1-Ge^{-\beta\varepsilon}}.
\end{aligned} \tag{41}$$

Ou seja,

$$Z_N = \frac{1-\left(Ge^{-\beta\varepsilon}\right)^{N}}{1-Ge^{-\beta\varepsilon}}, \tag{42}$$

ou de modo alternativo,

$$Z_N = \frac{1}{1 - Ge^{-\beta\varepsilon}} \left(-\lambda_1^N + \lambda_2^N\right), \tag{43}$$

o que mostra que a função de partição pode ser escrita como uma combinação linear da N-ésima potência dos autovalores da matriz de transferência. No limite termodinâmico, resta somente o maior autovalor e, para $N \to \infty$, a pressão é dada por

$$f \equiv \frac{1}{N} F \equiv -\frac{1}{\beta N} \log Z_N = -\frac{1}{\beta} \log \max\left(\lambda_1, \lambda_2\right) \tag{44}$$

onde o logaritmo tem base natural. Para termos uma transição de fase, o que significa que a pressão, dado que os autovalores são positivos e funções analíticas de β, é não analítica em algum ponto, devemos ter dois autovalores se cruzando em certo β_c. Neste caso basta comparar λ_1 e λ_2 e descobrir que eles se cruzam em uma temperatura dada por $\beta_c = \frac{\log G}{\varepsilon}$ ou, de modo equivalente, $T_c = \frac{\varepsilon}{k \log G}$ (veja Figura 11). Em T_c, a derivada da energia livre é descontínua, implicando que temos uma transição de fase de primeira ordem. Note que $T_c = \frac{\varepsilon}{k \log G}$ é finito enquanto $G > 1$; para o caso não degenerado $G = 1$ (somente um estado aberto) a transição ocorre em $T = \infty$ ou, em outras palavras, não existe transição de fase.

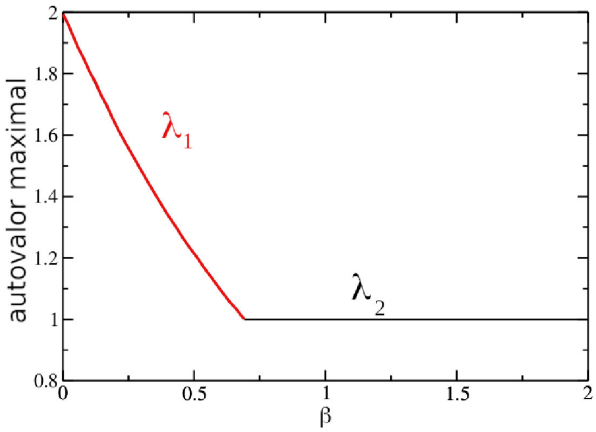


FIGURA 11. [2] Autovalores $\lambda_1 = Ge^{-\beta\varepsilon}$ e $\lambda_2 = 1$ em função de β, quando $G = 2$ e $\varepsilon = 1$; λ_1 e λ_2 se cruzam em $\beta_c = \log 2$, havendo, portanto, transição de fase de primeira ordem.

A matriz de transferência que encontramos no modelo de Ising unidimensional, composta por fatores de Boltzmann (exponenciais), é sempre estritamente positiva e, consequentemente, primitiva e analítica em β. Nessas condições, pelos Teoremas 2.1 e 2.2, não teremos uma transição de fase para qualquer $\beta > 0$. Conforme [2], a única maneira de escaparmos da hipótese do teorema de Perron-Frobenius é atribuindo uma energia infinita a algumas configurações, dando origem a entradas nulas na matriz, que podem ou não ser irredutíveis. Este é exatamente o caso no modelo de Kittel.

É importante perceber que a quebra da hipótese de irredutibilidade não garante o cruzamento de autovalores: de fato, a matriz de transferência do modelo de Kittel para o caso não degenerado, $G = 1$, também é redutível, uma vez que $t_{1,2}^{(k)} = 0$ para qualquer $k \geq 1$, e o cruzamento de autovalores ocorre apenas em $\beta = 0$ (ou temperatura infinita), como já explicado, produzindo a analiticidade do autovalor maximal (daí a pressão) para qualquer temperatura finita.

5. Discussão e Considerações Finais

Apresentamos resultados sobre o tratamento de transições de fase utilizando matrizes de transferência e o Teorema de Perron-Frobenius, exemplificando tal técnica com o modelo de Ising, e mostrando porque não há transição de fase, e com o modelo de Kittel, no qual há transição de fase em geral.

Uma vez que modelo de Kittel não satisfaz completamente nas hipóteses do Teorema de Perron-Frobenius - o que acontece pois a n-ésima potência de sua matriz de transferência ainda conta com entradas nulas, seja qual for o n - este apresenta transição de fase conforme o número de configurações do seu espaço de estados, a saber, se o espaço de estados tiver apenas dois estados (fechado e aberto), o modelo não apresenta transição de fase, todavia se houver mais estados (diferentes estados para distintas forma de abertura, por exemplo), o modelo apresenta transição de fase. Em outros termos, como a n-ésima potência de sua matriz de transferência tem entradas nulas, para qualquer que seja o n, não há garantias de um único autovalor maximal por parte do Teorema de Perron-Frobenius.

Apêndice A. Teorema de Perron-Frobenius

Nesse apêndice apresentaremos a demonstração do Teorema de Perron-Frobenius (Teorema 2.1) baseada em [14]. No Lema seguinte provamos um argumento que se faz necessário na demonstração do Teorema 2.1.

Lema A.1. *Dados $z_1, \ldots, z_s \in \mathbb{C} \setminus \{0\}$, se*

$$\left| \sum_{j=1}^{s} z_j \right| = \sum_{j=1}^{s} |z_j|, \tag{45}$$

então os argumentos desses números complexos são iguais, isto é,

$$\arg z_1 = \arg z_2 = \cdots = \arg z_s. \tag{46}$$

Demonstração. O lema nada mais é do que a condição de igualdade na desigualdade triangular generalizada para um número qualquer de argumentos. Mostraremos por indução sobre s. Para $s = 2$ o lema é a desigualdade triangular conhecida: se $z, w \in \mathbb{C}$ são não nulos então $|z + w| \leq |z| + |w|$, com igualdade realizada se, e somente se, $\arg z = \arg w$, ou seja, $w = \lambda z$ com $\lambda > 0$.

Para $s \geq 3$ segue de (45) que

$$\sum_{j=1}^{s} |z_j| = \left| \sum_{j=1}^{s} z_j \right| \leq \left| \sum_{j=1}^{s-1} z_j \right| + |z_s| \leq \sum_{j=1}^{s} |z_j|, \tag{47}$$

de modo que

$$\sum_{j=1}^{s} |z_j| = \left| \sum_{j=1}^{s-1} z_j \right| + |z_s|, \tag{48}$$

e então

$$\sum_{j=1}^{s-1} |z_j| = \left| \sum_{j=1}^{s-1} z_j \right|. \tag{49}$$

Assumamos como hipótese de indução que $\arg z_1 = \arg z_2 = \cdots = \arg z_{s-1}$ e provemos que a igualdade vale também para $\arg z_s$. Pela hipótese de indução, existem $w \in \mathbb{C}$ e $\lambda_1, \lambda_2, \ldots, \lambda_{s-1} > 0$ tais que $z_j = \lambda_j w$ para $1 \leq j \leq s-1$. Pondo $\lambda = \lambda_1 + \lambda_2 + \cdots + \lambda_{s-1}$, podemos reescrever (45) como

$$\left| \sum_{j=1}^{s} z_j \right| = |\lambda w + z_s| = |\lambda w| + |z_s|, \tag{50}$$

e a desigualdade triangular para $s = 2$ fornece $\arg z_s = \arg \lambda w = \arg w = \arg z_j$ para $1 \leq j \leq s-1$, já que $\lambda > 0$. ■

Uma vez provado o Lema, podemos prosseguir para a demonstração do Teorema 2.1. A notação utilizada para vetores não negativos será $x \geq 0$, o que significa que $x_j \geq 0$ em cada componente do vetor x. Ainda, a notação $|x|$ para um vetor x se refere ao vetor $(|x_1|, \ldots, |x_s|)$.

Demonstração do Teorema 2.1. (i) Seja $\tau \in \mathbb{C}$ um autovalor de M cujo módulo é maximal, isto é, $|\lambda| \leq |\tau|$ para qualquer autovalor λ de M. Se $y \in \mathbb{C}^s$ é o autovetor associado a τ então como $My = \tau y$ temos $\tau y_i = \sum_{j=1}^{s} m_{ij} y_j$ para todo i e $|\tau||y_i| \leq \sum_{j=1}^{s} m_{ij}|y_j|$ uma vez que as entradas da matriz M são não-negativas. Assim

$$|\tau| \leq \min_{\{i:y_i \neq 0\}} \frac{\sum_{j=1}^{s} m_{ij}|y_j|}{|y_i|}.$$

Considere agora a função r, definida para vetores não-negativos de $\mathbb{R}^s$ e dada por

$$r(x) = \min_{\{i:x_i \neq 0\}} \frac{\sum_{j=1}^{s} m_{ij} x_j}{x_i}$$

para $x \in \mathbb{R}^s$ com $x \neq 0$. Esta função r é semi-contínua superiormente e homogênea no conjunto $\{x \in \mathbb{R}^s \setminus \{0\}, x \geq 0\}$ de modo que o supremo

$$\theta = \sup_{\substack{x \geq 0 \\ x \neq 0}} r(x) = \sup_{\substack{x \geq 0 \\ \|x\| = 1}} r(x)$$

existe e é realizado, uma vez que $\{x \geq 0 : \|x\| = 1\}$ é compacto (veja Exercício 21 do Capítulo II de [16]). Como

$$\min_{\{i:x_i \neq 0\}} \frac{\sum_{j=1}^{s} m_{ij} x_j}{x_i} \leq \theta$$

para todo $x \geq 0$, temos $\theta \geq |\tau| > 0$. Vamos provar que θ é um autovalor. Escrevendo

$$\theta = \min_{\{i:y_i \neq 0\}} \frac{\sum_{j=1}^{s} m_{ij} y_j}{y_i}$$

para algum $y \geq 0$ com $\|y\| = 1$, se $z = My - \theta y$ for não nulo, temos

$$M(M^k y) - \theta M^k y = M^k z > 0$$

onde $M^k > 0$ por ser M primitiva. Assim, pondo $x = M^k y$, teremos $\theta x < Mx$ e portanto $\theta x_i < \sum_{j=1}^{s} m_{ij} x_j$ para todo i, o que contradiz a nossa hipótese. Dessa forma, $My = \theta y$ e θ é um autovalor positivo tal que $|\lambda| \leq \theta$ para qualquer outro autovalor λ de M. Suponha agora que λ é um autovalor de M com $|\lambda| = \theta$. Se $My = \lambda y$ então $\theta|y| = |My| \leq M|y|$ e os argumentos anteriores garantem que $M|y| = \theta|y|$, de onde vem

$$M^k|y| = \theta^k|y| = |M^k y|$$

e, para todo i,

$$\left| \sum_{j=1}^{s} m_{ij}^{(k)} y_j \right| = \sum_{j=1}^{s} m_{ij}^{(k)} |y_j|.$$

Pelo Lema A.1, as componentes y_j de y tem todas o mesmo argumento, $e^{i\phi}$ digamos, teremos $y = |y|e^{i\phi}$, logo se multiplicarmos o vetor y por $e^{-i\phi}$ vem $ye^{-i\phi} = |y|e^{i\phi}e^{-i\phi} = |y|$, ou seja, o resultado é um autovetor positivo correspondente a λ, e assim λ é positivo e $\lambda = \theta$.

(ii) Mostramos em (i), para o autovalor dominante θ e um vetor qualquer y não negativo tal que $My \geq \theta y$, que o vetor $|y|$ é um autovetor positivo associado a θ.

(iii) Começaremos mostrando que a multiplicidade geométrica de θ é um, ou seja, que $\dim \ker(M - \theta I) = 1$. Supondo que haja dois vetores, x e y, linearmente independentes em $\ker(M - \theta I)$, pelo item (ii) temos que x e y são vetores positivos, ou seja, ambos não têm nenhuma componente nula e pondo $z = y_1 x - x_1 y$ onde x_1 e y_1 são a primeira componente de x e y respectivamente, temos que a primeira componente de z é nula pois $z_1 = y_1 x_1 - x_1 y_1 = 0$. Logo por (ii) ou z é autovetor positivo de M ou $z = 0$; como $z_1 = 0$ segue que z não pode ser positivo, assim $z = 0$, o que mostra que existe uma combinação linear nula não trivial de x e y, uma vez que $x_1 > 0$ e $y_1 > 0$, e daí segue que x e y são linearmente dependentes, uma contradição com a hipótese. Assim, a dimensão do núcleo de $M - \theta I$ é um.

Ainda devemos mostrar que a multiplicidade algébrica de θ é um. Para isso, vamos provar que $\ker(M - \theta I) = \ker(M - \theta I)^2$. Claramente $\ker(M - \theta I) \subset \ker(M - \theta I)^2$ pois se $Mx = \theta x$ para algum x então

$$M^2 x = M(Mx) = M(\theta x) = \theta Mx = \theta^2 x. \tag{51}$$

Para mostrar que a igualdade é válida, vamos supor que existe $y \in \ker(M - \theta I)^2 \setminus \ker(M - \theta I)$ e mostrar que isto não é possível. Nessas condições,

$M^2y = \theta^2 y$ mas $My \neq \theta y$, logo

$$(M-\theta I)^2 y = (M-\theta I)\left[(M-\theta I)y\right] = 0 \tag{52}$$

e daí $(M-\theta I)y \in \ker(M-\theta I)$. Como $\dim\ker(M-\theta I) = 1$, temos que $(M-\theta I)y$ é múltiplo de algum vetor $x \in \ker(M-\theta I)$, ou seja, $(M-\theta I)y = tx$ para algum $t \neq 0$ que por simplicidade tomaremos como sendo um (a rigor, basta escolher $\frac{y}{t}$ ao invés de y), logo

$$My = \theta y + x \tag{53}$$

e para todo $n \geq 1$, vale

$$M^n y = \theta^n y + n\theta^{n-1}x. \tag{54}$$

Vamos provar a equação (54) por indução. Uma vez que já temos o resultado para $n = 1$ na equação (53), supomos para $n = k$, ou seja, $M^k y = \theta^k y + k\theta^{k-1}x$, e vamos mostrar para $n = k+1$. De fato,

$$\begin{aligned} M^{k+1}y &= M(M^k y) \overset{(HI)}{=} M(\theta^k y + k\theta^{k-1}x) \\ &= \theta^k My + k\theta^{k-1}Mx \\ &\overset{(53)}{=} \theta^k(\theta y + x) + k\theta^{k-1}\theta x \\ &= \theta^{k+1}y + (k+1)\theta^k x. \end{aligned}$$

Assim, para qualquer $n \geq 2$ temos

$$M^n|y| = |M^n y)| = |\theta^n y + n\theta^{n-1}x| \geq \theta^{n-1}(n|x| - \theta|y|). \tag{55}$$

Como $|x| \in \ker(M-\theta I)$ é autovetor positivo de M, existe um n_0 suficientemente grande tal que $n_0|x| - \theta|y| \geq \theta|y|$, e por (55), temos

$$M^{n_0}|y| \geq \theta^{n-1}(n|x| - \theta|y|) \geq \theta^{n_0}|y|. \tag{56}$$

Mas M^{n_0}, por sua vez, é uma matrix primitiva com θ^{n_0} sendo seu autovalor positivo dominante. Usando outra vez os itens (i) e (ii) temos $M^{n_0}|y| = \theta^{n_0}|y|$, logo

$$M^{n_0}y = \theta^{n_0}y. \tag{57}$$

Por hipótese, tínhamos $My \neq \theta y$, uma vez que $y \in \ker(M-\theta I)^2 \backslash \ker(M-\theta I)$, logo $My > \theta y$ ou $My < \theta y$. Suponha, sem perda de generalidade, que $My > \theta y$, e por indução supomos válida $M^n y > \theta^n y$, logo

$$M^{n+1}y = M(M^n y) \overset{HI}{>} \theta^n M(y) > \theta^{n+1}y,$$

e portanto, $M^n y \neq \theta^n y$ para todo $n \in \mathbb{N}$, o que contradiz a equação (57). Assim $\ker(M-\theta I)^2 \setminus \ker(M-\theta I) = \emptyset$ e $\ker(M-\theta I)^2 = \ker(M-\theta I)$, o que mostra o resultado. ■

Agradecimentos

O autor agradece ao revisor anônimo pelos diversos apontamentos que ajudaram a qualificar o trabalho e ao professor Michel Spira que indicou uma prova mais direta e contundente para o Lema A.1.

Referências

[1] Blythe, R. A. e Evans, M. R., The Lee-Yang theory of equilibrium and nonequilibrium phase transitions, *Brazilian Journal of Physics*, **33** (2003), p. 464-475.

[2] Cuesta, J.A. and Sánchez, A., General non-existence theorem for phase transitions in one-dimensional systems with short range interactions, and physical examples of such transitions, in *Journal of Statistical Physics*, **115** (2004), p. 869-893.

[3] Daley, D. J., Gani, J., A deterministic general epidemic model in a stratified population, in *Probability, Statistics and Optimization*, (Wiley, 1994)), p. 117-132.

[4] Feller, W., *An Introduction to Probability Theory and Its Applications*, Vol. 1, (Wiley, 1950).

[5] Friedli, S. and Velenik, Y. *Statistical Mechanics of Lattice Systems: A Concrete Mathematical Introduction*, (Cambridge University Press, 2017).

[6] Frobenius, F. G., Über Matrizen aus nicht negativen Elementen, in *S. B. Preuss Acad. Wiss. Berlin*, **25** (1912), p. 456-477.

[7] Kato, S., *Perturbation Theory for Linear Operators*, vol. 132 of *Grundlehren der mathematischen Wissenschaften*. (Springer-Verlag, 1980).

[8] Keyfitz, N., *Applied Mathematical Demography*, 2nd ed., (Springer-Verlag, 1977).

[9] Kittel, C., Phase Transition of a Molecular Zipper, in *American Journal of Physics*, **37**, (1969), p. 917-920.

[10] MacCluer, C. R., *Boundary Value Problems and Orthogonal Expansions*. (IEEE Press, 1994).

[11] MacCluer, C. R., The Many Proofs and Applications of Perron's Theorem, *SIAM Review*, **42** n. 3 (2000) p. 487-498.

[12] Onsager, L., Crystal Statistics I. A Two-Dimensional Model with an Order-Disorder Transition, in *Physical Review*, **65** (1944), p. 117-149.

[13] Perron, O., Zur Theorie der Matrices, *Math. Ann. 64*, **25** (1907), p. 248-263.

[14] Queffelec, M., *Substitution Dynamical Systems - Spectral Analysis*, (Springer-Verlag, Berlin-Heidelberg, 2010).

[15] Rudin, W., *Principle of Mathematical Analysis*, 3 ed. (McGraw-Hill, 1976).

[16] Rudin, W., *Real and Complex Analysis*, 3 ed. (McGraw-Hill, 1986).

[17] Salinas, S., *Introdução a Física Estatística*, 2 ed. (Edusp, 2018).

[18] Seneta, E., *Nonnegative Matrices and Markov Chains*, 2 ed. (Springer-Verlag, 1981).

[19] Takayama, A., *Mathematical Economics*. (Dryden Press, 1974).

[20] Trapp, C., Schenkelberger, M. and Ott, A., Stability of double-stranded oligonucleotide DNA with a bulged loop: a microarray study, *BMC Biophysics*, **4** n. 20 (2011).

Universidade Federal da Fronteira Sul
Avenida Edmundo Gaievisky, SN
Realeza, PR

Email address: everton.artuso@uffs.edu.br

RMU
REVISTA MATEMÁTICA UNIVERSITÁRIA

SBM
SOCIEDADE BRASILEIRA DE MATEMÁTICA

Revista Matemática Universitária, vol. 2, 2021
ISSN: 2675-5254 — **DOI:** 10.21711/26755254/rmu20219

RETICULADOS E NÚMEROS BINÁRIOS: UM ATAQUE À CRIPTOGRAFIA RSA

JOSÉ LAUDELINO DE M. NETO

Resumo. Descrevemos um ataque ao criptosistema RSA, desenvolvido por May e Ritzenhofen em [1], que consiste em fatorar simultaneamente, utilizando teoria de reticulados, dois números inteiros positivos $N_1 = p_1q_1$ e $N_2 = p_2q_2$, onde p_1, p_2, q_1 e q_2 são números primos ímpares. Mas, para tal feito é necessário ter duas dicas a respeito destes números N_1 e N_2, a saber: p_1 e p_2 devem ter alguns bits finais em comum e q_1 e q_2 devem ter a mesma quantidade de bits.

1. Introdução

Nos dias atuais, a criptografia se encontra em voga, pois basta reparar que ao iniciar uma conversa no aplicativo de mensagens *WhatsApp*, somos surpreendidos com um aviso alertando que *"As mensagens e as chamadas são protegidas com a criptografia de ponta a ponta (...)"*. E o que é criptografia? Podemos dizer que é a arte de codificar uma mensagem, transformando um texto legível e entendível em um texto que fique não compreensível para leitores não autorizados. Apenas leitores autorizados terão acesso ao texto original.

Exemplificando o que foi dito no parágrafo acima: o seguinte texto original *"BOM"* é cifrado, por algum método criptográfico, no texto *"ABBDLG"*. Então, somente pessoas autorizadas terão como descriptografar o texto cifrado e recuperar a mensagem original. Os leitores não autorizados, terão acesso apenas ao texto cifrado e não compreensível.

Um dos métodos criptográficos mais famosos é o RSA, criado por Rivest, Shamir e Adleman. Sua segurança consiste na dificuldade em fatorar um número como um produto de primos, pois o cerne do RSA é um número N positivo, produto de dois números primos ímpares, p e q [4]. Este número $N = pq$ é chamado de *RSA moduli*.

Desde o surgimento de técnicas criptográficas, pesquisam-se maneiras de quebrar a criptografia e desvendar o texto cifrado. Não é diferente com o RSA e é isso que apresentaremos neste texto, um ataque a criptografia RSA, desenvolvida por May e

Data de aceitação: Agosto de 2021.
Palavras chave. Álgebra Linear; Teoria dos Números; Congruência.

Ritzenhofen [1], na tentativa de fatorar um *RSA moduli* $N = pq$ utilizando números binários e teoria de reticulados.

2. Reticulados

Ressaltamos que, na literatura matemática, o termo reticulado é usado em duas situações distintas. Numa delas, um assunto se refere a conjuntos parcialmente ordenados [5], que não é o do nosso interesse, e na outra se refere a subconjuntos de um espaço vetorial real [3]. Portanto, para entender reticulados no contexto de álgebra linear, é necessário ter conhecimento prévio sobre: conjunto de vetores Linearmente Independentes (LI), espaço vetorial, base de um espaço vetorial, norma de um vetor etc.

Um reticulado inteiro L é um subgrupo discreto e adititivo de $\mathbb{Z}^n$. Equivalentemente, sejam $d, n \in \mathbb{N}$ e $\mathbf{b}_1, \ldots, \mathbf{b}_d \in \mathbb{Z}^n$ vetores LI, um reticulado inteiro L é o conjunto de todas as combinações lineares inteiras dos vetores $\mathbf{b}_i$, ou seja,

$$L = \{a_1\mathbf{b}_1 + \ldots + a_d\mathbf{b}_d; a_i \in \mathbb{Z}\}.$$

Neste caso, dizemos que o conjunto $\{\mathbf{b}_1, \ldots, \mathbf{b}_d\}$ é uma base do reticulado L.

O Problema do Menor Vetor, em inglês *Shortest Vector Problem*, é uma das pesquisas na área [2] e consiste em determinar o vetor de menor comprimento de um reticulado. Ou seja, denotamos $\|\mathbf{v}\|$ como a norma euclidiana do vetor $\mathbf{v}$, e o Problema do Menor Vetor consiste em determinar $\mathbf{0} \neq \mathbf{a} \in L$ tal que $\|\mathbf{a}\| \leq \|\mathbf{v}\|$ para qualquer vetor $\mathbf{v}$ de L. Adotamos a norma tradicional euclidiana, porém o problema também pode ser proposto para outras normas usuais. Se $\mathbf{a}$ é o menor vetor do reticulado L, então escrevemos $\|\mathbf{a}\| = \lambda_1(L)$.

Para um caso de dimensão n qualquer, resolver o Problema do Menor Vetor não é uma tarefa fácil. Entretanto, para um reticulado bidimensional L, no caso em que $n = 2$, é possível utilizar um algoritmo chamado de Redução de Gauss, o qual resolve o Problema do Menor Vetor.

O Algoritmo da Redução de Gauss funciona calculando uma sequência de bases $\{\mathbf{a}, \mathbf{b}\}$ de um reticulado bidimensional L, que satisfaz a propriedade

$$\|\mathbf{a}\| \leq \|\mathbf{a} - \mathbf{b}\| < \|\mathbf{b}\|,$$

e, ao final de uma quantidade finita de iterações, retorna uma base $\{\mathbf{a}, \mathbf{b}\}$ tal que $\|\mathbf{a}\| = \lambda_1(L)$.

Algoritmo da Redução de Gauss
Entrada: Base de um reticulado bidimensional L, $\{\mathbf{a}, \mathbf{b}\}$.
Saída: Base $\{\mathbf{a}, \mathbf{b}\}$ do reticulado L satisfazendo $\|\mathbf{a}\| = \lambda_1(L)$.

(1) Se $\|\mathbf{a}\| > \|\mathbf{b}\|$, então troque $\mathbf{a}$ por $\mathbf{b}$ e vá para (2). Caso contrário, vá para (2).
(2) Se $\|\mathbf{a} - \mathbf{b}\| > \|\mathbf{a} + \mathbf{b}\|$, então $\mathbf{b} := -\mathbf{b}$ e vá para (3). Caso contrário, vá para (3).
(3) Se $\|\mathbf{b}\| \leq \|\mathbf{a} - \mathbf{b}\|$, então pare e retorne $\{\mathbf{a}, \mathbf{b}\}$. Caso contrário, vá para (4).
(4) Se $\|\mathbf{a}\| \leq \|\mathbf{a} - \mathbf{b}\|$, então vá para (6). Caso contrário, vá para (5).
(5) Se $\|\mathbf{a}\| = \|\mathbf{b}\|$, então pare e retorne $\{\mathbf{a}, \mathbf{a} - \mathbf{b}\}$. Caso contrário, vá para (6).

(6) Determine $\mu \in \mathbb{Z}$ tal que $\|\mathbf{b} - \mu\mathbf{a}\|$ é o menor possível, faça $\mathbf{a} := \mathbf{b} - \mu\mathbf{a}$, $\mathbf{b} := \mathbf{a}$. Se $\|\mathbf{a}-\mathbf{b}\| > \|\mathbf{a}+\mathbf{b}\|$, faça $\mathbf{b} := -\mathbf{b}$. Se $\{\mathbf{a}, \mathbf{b}\}$ satisfizer $\|\mathbf{a}\|, \|\mathbf{b}\| < \|\mathbf{a}-\mathbf{b}\|, \|\mathbf{a}+\mathbf{b}\|$, então pare e retorne $\{\mathbf{a}, \mathbf{b}\}$. Caso contrário, refaça (6).

A etapa (6) é um loop, pois é necessário tornar a repetir o procedimento em (6), até chegarmos ao objetivo. O medo seria o da etapa (6) entrar em um loop infinito, porém isso não ocorre, pois o valor de $\|\mathbf{a}\|$ ou $\|\mathbf{b}\|$ diminui a cada iteração e, como existe uma quantidade finita de vetores de L menores que $\|\mathbf{a}\| + \|\mathbf{b}\|$, então o algoritmo irá finalizar após uma quantidade finita de iterações [2]. Além disso, o problema para determinar μ na etapa (6) é contornado ao considerarmos a Proposição abaixo, pois garante um intervalo de números inteiros positivos para μ. É justo por isso que μ pode ser calculado de modo eficiente, pois vamos testando todos os valores de μ deste intervalo garantido pela Proposição, até encontrarmos um $\mu \in \mathbb{Z}$ tal que $\|\mathbf{b} - \mu\mathbf{a}\|$ é o menor possível.

Proposição: *Sejam* $\mathbf{a}, \mathbf{b}$ *vetores tais que* $\|\mathbf{b}\| > \|\mathbf{b} - \mathbf{a}\|$. *Então, podemos calcular de modo eficiente um inteiro* μ *tal que* $\|\mathbf{b} - \mu\mathbf{a}\|$ *é o menor possível. Além disso,* $1 \leq \mu \leq 2\frac{\|\mathbf{b}\|}{\|\mathbf{a}\|}$.
Demonstração: A demonstração detalhada desta Proposição é encontrada na referência [2]. ■

3. Fatorando dois *RSA moduli* simultaneamente

Apresentamos o tema principal deste texto, descrito no Teorema abaixo, que foi a técnica desenvolvida por May e Ritzenhofen [1], a fatoração simultânea de dois *RSA moduli*, onde duas dicas são dadas. No caso, sejam $N_1 = p_1q_1$ e $N_2 = p_2q_2$ dois *RSA moduli* e a primeira dica dada é que p_1 e p_2 na sua forma binária possuem alguns dígitos finais em comum, ou seja, alguns bits finais iguais. A segunda dica é que q_1 e q_2 tem a mesma quantidade de dígitos na sua escrita em binário, o que equivale a dizer que q_1 e q_2 tem a mesma quantidade de bits.

Com o intuito de apresentar a prova do Teorema, lembramos a construção do anel de inteiros módulo n, onde n é um número inteiro positivo. Dizemos que dois números inteiros a e b são congruentes módulo n se e somente se n divide $a - b$. Neste caso, escrevemos $a \equiv b (\text{mod } n)$. A relação $\equiv$ é de equivalência e o conjunto das classes de equivalência é denotado por $\mathbb{Z}_n$. As operações de soma e multiplicação induzidas de $\mathbb{Z}$ em $\mathbb{Z}_n$ o tornam um anel comutativo. Verifica-se que uma classe de equivalência $\bar{a} \in \mathbb{Z}_n$ tem inverso multiplicativo se e somente se $\text{mdc}(a, n) = 1$.

Teorema: *Sejam* $N_1 = p_1q_1$ *e* $N_2 = p_2q_2$ *dois RSA moduli distintos, onde* q_i *tem* α *bits. Suponhamos que* p_i *possuem* $t > 2(\alpha + 1)$ *bits finais em comum. Então,* N_1 *e* N_2 *podem ser fatorados simultaneamente.*
Demonstração: Como p_1, p_2 possuem t bits finais em comum, temos

$$p_1 = 2^t\widetilde{p_1} + p \quad \text{e} \quad p_2 = 2^t\widetilde{p_2} + p.$$

Assim, $N_i = (p + 2^t\widetilde{p_i})q_i$, implicando que $pq_i \equiv N_i (\text{mod } 2^t), i = 1, 2$. Sendo q_i primos ímpares, então possuem inversos multiplicativos em $\mathbb{Z}_{2^t}$. Logo,

$$N_1q_1^{-1} \equiv N_2q_2^{-1} (\text{mod } 2^t) \Rightarrow (N_1^{-1}N_2)q_1 - q_2 \equiv 0 (\text{mod } 2^t). \tag{1}$$

O conjunto de soluções

$$L = \left\{(x_1, x_2) \in \mathbb{Z}^2; (N_1^{-1}N_2)x_1 - x_2 \equiv 0 (\text{mod } 2^t)\right\}$$

forma um grupo aditivo e discreto de $\mathbb{Z}^2$. Isto é, L é um reticulado bidimensional.

Afirmamos que L possui os vetores $\mathbf{b}_1 = (1, N_1^{-1}N_2)$ e $\mathbf{b}_2 = (0, 2^t)$ como base. Com efeito, $\mathbf{b}_1, \mathbf{b}_2 \in L$ e são LI. Por outro lado, seja $(x_1, x_2) \in L$. Então, $x_2 = (N_1^{-1}N_2)x_1 - k2^t$, para algum $k \in \mathbb{Z}$. Assim, $(x_1, x_2) = x_1\mathbf{b}_1 - k\mathbf{b}_2$.

Pela Equação (1), vemos que $\mathbf{q} = (q_1, q_2) \in L$. Entretanto, $\mathbf{q}$ ainda está indeterminado. Para deteminar explicitamente quem é $\mathbf{q}$, utilizamos o Algoritmo da Redução de Gauss nos vetores $\mathbf{b}_1$ e $\mathbf{b}_2$. Após aplicarmos o referido algoritmo, obtemos como retorno que $\mathbf{q}$ é o menor vetor de L, ou seja, $\|\mathbf{q}\| = \lambda_1(L)$ (para maiores detalhes desta passagem, ver [1]). Consequentemente, temos material suficiente para fatorar N_1 e N_2 simultaneamente. ■

O Teorema acima nos garante o algoritmo a seguir:
Entrada: dois RSA moduli N_1 e N_2 satisfazendo as hipóteses do Teorema.
Saída: q_1 e q_2, onde $N_1 = p_1q_1$ e $N_2 = p_2q_2$.

(1) Calcule $N_1^{-1}N_2 \in \mathbb{Z}_{2^t}$.
(2) Considere L o reticulado gerado por $\mathbf{a} = (1, N_1^{-1}N_2)$ e $\mathbf{b} = (0, 2^t)$.
(3) Utilize o Algoritmo da Redução de Gauss para determinar o menor vetor $\mathbf{q} = (q_1, q_2)$ do reticulado L.

Para visualizarmos melhor, consideremos um caso prático. Sejam $N_1 = p_1q_1 = 372581$ e $N_2 = p_2q_2 = 493571$ dois *RSA moduli* tais que p_1 e p_2 possuem 12 bits finais em comum e q_1 e q_2 possuem 4 bits, ou seja, N_1 e N_2 satisfazem as condições do Teorema. Sendo assim, estamos aptos para utilizar o algoritmo apresentado acima. Primeiro, calculamos $N_1^{-1}N_2$ módulo $2^{12} = 4096$,

$$N_1^{-1}N_2 \equiv 1863 (\text{mod } 4096).$$

Seja L o reticulado gerado pelos vetores $\mathbf{a} = (1, 1863)$ e $\mathbf{b} = (0, 4096)$. Então, chegamos na etapa de aplicar o Algoritmo da Redução de Gauss. Observamos que os vetores $\mathbf{a}$ e $\mathbf{b}$ satisfazem as etapas (1) a (4) do Algoritmo da Redução de Gauss e, da etapa (4), vamos para a etapa (6), que, como mencionado antes, funciona como um loop até chegarmos a base procurada do reticulado.

Para o loop da etapa (6), vamos iniciar a primeira iteração com $\mathbf{a}_0 = \mathbf{a}$ e $\mathbf{b}_0 = \mathbf{b}$. Utilizando a Proposição, obtemos que

$$1 \leq \mu \leq 2\frac{\|\mathbf{b}_0\|}{\|\mathbf{a}_0\|} \approx 4.$$

Assim, para $\mu \in \{1, 2, 3, 4\}$, testando caso a caso, concluimos que o menor valor possível para $\|\mathbf{b}_0 - \mu\mathbf{a}_0\|$ é quando $\mu = 2$. Logo,

$$\mathbf{a}_1 = \mathbf{b}_0 - 2\mathbf{a}_0 = (-2, 370), \quad \mathbf{b}_1 = \mathbf{a}_0 = (1, 1863).$$

Como $\|\mathbf{b}_1\|$ não é menor que $\|\mathbf{a}_1 - \mathbf{b}_1\|$, repetimos o procedimento e, para $\mu \in \{1, 2, \ldots, 10\}$, analisando caso a caso, temos que o menor valor possível para $\|\mathbf{b}_1 - \mu\mathbf{a}_1\|$ é quando $\mu = 5$. Então,

$$\mathbf{a}_2 = \mathbf{b}_1 - 5\mathbf{a}_1 = (11, 13), \quad \mathbf{b}_2 = \mathbf{a}_1 = (-2, 370).$$

Mais uma vez, como $\|\mathbf{b}_2\|$ não é menor que $\|\mathbf{a}_2 - \mathbf{b}_2\|$, fazemos o procedimento e, para $\mu \in \{1, 2, \ldots, 42\}$, calculando todas as opções disponíveis, temos que o menor valor possível para $\|\mathbf{b}_2 - \mu\mathbf{a}_2\|$ é quando $\mu = 17$. Logo,

$$\mathbf{a}_3 = \mathbf{b}_2 - 17\mathbf{a}_2 = (-189, 149), \quad \mathbf{b}_3 = \mathbf{a}_2 = (11, 13).$$

Neste caso, temos que $\|\mathbf{a}_3\|$ e $\|\mathbf{b}_3\|$ são menores que $\|\mathbf{a}_3 - \mathbf{b}_3\|$ e $\|\mathbf{a}_3 + \mathbf{b}_3\|$. Então, temos que $\mathbf{q} = (11, 13)$ e $(-189, 149)$ é uma base do reticulado L que satisfaz $\|\mathbf{q}\| = \lambda_1(L)$. Portanto,

$$N_1 = 372581 = p_1 q_1 \quad \text{e} \quad N_2 = 493571 = p_2 q_2,$$

onde $q_1 = 11, q_2 = 13$ e, consequentemente, $p_1 = 33871$ e $p_2 = 37967$.

Em binário, temos

$$\begin{aligned} p_1 &= (1000010001001111)_2, \\ p_2 &= (1001010001001111)_2 \\ q_1 &= (1011)_2, \\ q_2 &= (1101)_2. \end{aligned}$$

Referências

[1] Alexander May & Maike Ritzenhofen, *Implicit Factoring: On Polynomial Time Factoring Given Only an Implicit Hint*, In Stanislaw Jarecki and Gene Tsudik, editores, Public Key Cryptography, volume 5443 of Lecture Notes in Computer Science, p. 1-14. Springer, 2009.

[2] Daniele Micciancio & Shafi Goldwasser, *Complexity of lattice problems: a cryptographic perspective*, Kluwer Academic Publishers, 2002.

[3] Fernando Daniel Moreira Coelho, *O Algoritmo LLL e Aplicações*, Dissertação de Mestrado, Faculdade de Ciências e Tecnologia, Universidade de Coimbra, 2007.
<http://www.mat.uc.pt/~jsoares/research/mest_Fernando_Coelho.pdf>
Acesso em: 12/05/2021.

[4] Manoel Lemos, *Criptografia, Números Primos e Algoritmos*, IMPA, 2010.
<https://impa.br/wp-content/uploads/2017/04/PM_04.pdf> Acesso em: 13/06/2021.

[5] Michell Lucena Dias, *Introdução à Teoria dos Reticulados e Reticulados de Subgrupos*, Trabalho de Conclusão de Curso, Unidade Acadêmica de Matemática, Universidade Federal de Campina Grande, 2013.
<http://mat.ufcg.edu.br/pgmat2/wp-content/uploads/sites/2/2015/06/TCC-Michell.pdf>
Acesso em: 12/05/2021.

Departamento de Ciências Exatas
Centro de Ciências Aplicadas e Educação (CCAE)
Universidade Federal da Paraíba (UFPB)
Rio Tinto, PB
Email address: laudelino@dcx.ufpb.br

RMU
REVISTA MATEMÁTICA UNIVERSITÁRIA

SBM
SOCIEDADE BRASILEIRA DE MATEMÁTICA

Revista Matemática Universitária, vol. 2, 2021
ISSN: 2675-5254 — **DOI:** 10.21711/26755254/rmu202110

UM AGRADECIMENTO A SOPHIE GERMAIN

RIELI TAINÁ GOMES DOS SANTOS

Resumo. O artigo tem como objetivo relatar a história de uma jovem matemática inserida em uma sociedade extremamente patriarcal e suas tentativas em fazer parte do meio científico da época.

1. Introdução

É primavera na França, as flores estão desabrochando, as árvores recuperam suas folhagens. Juntamente ao clima agradável e quente, o clima revolucionário aflora. No poder está o monarca absoluto Luís XVI, este decidido a manter a sociedade francesa em camadas distintas e distantes: os privilegiados e o povo. A crise econômica permeia a França e o descontentamento com os gastos exacerbados por parte da nobreza é grande.

Além disso, o Iluminismo influencia as decisões, incitando a racionalidade, a importância do intelecto, o debate e as críticas. Na sociedade científica da época, o empirismo ganha forma e lugar. No entanto, as mulheres não eram permitidas nesse meio, tendo como função natural cuidar da casa e dos filhos.

Esse é o contexto do fim do século XVIII, mais especificamente do dia 1 de abril de 1776. Nesse dia nasce Sophie Germain em Paris. Mas o que há de tão especial nessa mulher?

2. A Matemática

Filha de pai burguês, um próspero comerciante, deputado e amigo de filósofos da época, Sophie vivenciou diversos debates políticos, ainda que não pudesse participar. À medida que se tornava adolescente, o encanto pelos números crescia. A sociedade

Data de aceitação: Setembro 2021.
Palavras chave. Sophie Germain, Mulheres na Ciência, História da Matemática.
A autora deste artigo gostaria de prestar agradecimento à professora Nincia Cecília Ribas Borges Teixeira (UNICENTRO) pela revisão ortográfica deste trabalho e ao corpo editorial, assim como aos pareceristas, pelas sugestões que possibilitaram uma melhora considerável deste artigo.

patriarcal da época a proibia de se aprofundar nos assuntos da Rainha das Ciências. Ainda assim, ao anoitecer ia, escondida, para a extensa biblioteca do pai para ler.

O episódio que mais intrigou Sophie foi a morte de Arquimedes, retratada no livro *Essais Historiques sur la Mathématique de Montucla*, em que ele fora morto por um soldado romano por estar imerso em um problema de geometria. "O que há de tão interessante nessa área que valia mais que sua própria vida?", perguntou-se a menina. Posteriormente, esse evento a influenciaria na escolha da área matemática a seguir.

3. A Revolução

Quando Sophie estava com 13 anos, a Revolução Francesa eclodiu. Dessa maneira, a rotina dos franceses foi drasticamente perturbada, assim como a da menina, que fora proibida de sair de casa. O ano de 1789 ficou conhecido como "O Grande Medo", com invasões frequentes a propriedades da aristocracia e o medo dos camponeses de ataques da nobreza. Como Sophie vinha de uma família burguesa, o medo se instalou.

Apesar da participação efetiva das mulheres na Revolução Francesa, foram lhes concedidos apenas direitos civis e nenhum direito político. Assim, a situação feminina na época continuava tensa e as mulheres ainda sofriam preconceito de gênero em certos ambientes tidos como masculinos.

A fim de entender melhor o contexto pós-revolução, Michelle Perrot afirma que:

> A Revolução Francesa é, também, contraditória. O universalismo da Declaração dos direitos do homem e do cidadão não concerne verdadeiramente às mulheres: elas não são indivíduos. A Revolução lhes concede, no entanto, direitos civis, mas nenhum direito político. (Perrot, 2007, p. 142)

Restava, então, para Sophie, planejar um modo de se inserir na sociedade científica da época a fim de aprofundar ainda mais seus conhecimentos na Matemática, já que era proibida de frequentar as academias.

4. O Plano

Para que pudesse receber cópias das anotações das aulas ministradas na *École Polytechnique* em Paris, Germain adotou o codinome de um ex-aluno: Antoine-Auguste Le Blanc. Sophie estava particularmente interessada nas aulas de análise ministradas por Joseph-Louis Lagrange. Dessa maneira, ela poderia estudar os assuntos tratados nas aulas sem revelar sua verdadeira identidade.

O uso de codinomes masculinos apropriados por mulheres para adentrarem em ambientes masculinos era frequente até meados do século XX, quando os movimentos feministas ganharam força e as mulheres conquistaram o direito de serem ouvidas. Então, no século XVIII, suas vozes ainda eram silenciadas e, para que fossem ouvidas, deveriam usar como meio as vozes masculinas, como retrata Londa Schiebingir: *"Mesmo a grande feminista inglesa Mary Wollstone-craft, em seus esforços para criar igualdade entre os sexos, encorajava as mulheres a tornarem-se 'mais masculinas e respeitáveis'."* (Schienbinger, 2001, p. 138)

5. A Revelação

Os professores da *École Polytechnique* tinham por costume motivar os alunos a enviarem observações escritas sobre os conteúdos tratados nas aulas expositivas. Germain, então, enviou suas anotações a Lagrange que, desconfiado da rápida melhora acadêmica de Antoine-Auguste Le Blanc, solicitou uma entrevista com o ex-aluno e Sophie obrigou-se a revelar sua verdadeira identidade. Devido a sua genialidade na área, o professor a incentivou a dar continuidade em seus estudos e começou a orientá-la.

A figura marcante de Sophie no cenário matemático da época, devido à constatação feita por Lagrange de que seus trabalhos eram de alta qualidade, atraiu a curiosidade de diversos estudiosos, ansiosos para enviarem seus estudos para a cientista e conversarem sobre suas pesquisas. Germain estava inserida direta e indiretamente no campo científico parisiense e tendo como importantes mentores Lagrange e Legendre.

Quando Legendre, em 1798, publicou um resumo sobre sua pesquisa intitulado *Essai sur la théorie des nombres*, a cientista leu e veio a se interessar pela Teoria dos Números. Decidiu, portanto, enviar uma carta ao grande matemático dessa área, C. F Gauss, com suas observações pessoais, em especial acerca o Último Teorema de Fermat. É claro que o medo de ser julgada por seu gênero a fez assinar as cartas com seu codinome. Ao perceber a determinação e talento de Germain, Gauss respondeu à matemática. A troca de cartas entre os cientistas ficou cada vez mais frequente.

As cartas entre os cientistas perduraram por anos sem que Gauss soubesse a verdadeira identidade de Germain. No entanto, em 1806, o imperador Napoleão Bonaparte invadiu a Prússia e Sophie, temendo pela morte de Gauss, pediu ao General Pernety, amigo próximo da família, que garantisse a segurança do cientista. O general disse a Gauss que agradecesse a "Mademoiselle Germain". Mas quem seria ela? Nunca havia escutado esse nome antes.

Posteriormente, Germain enviou uma carta ao matemático revelando sua identidade e aquele a respondeu com uma magnífica carta a agradecendo e reconhecendo seu trabalho e determinação. Essa carta está presente em Germain and Stupuy, 1896.

Em meados de 1830, Gauss convenceu a Universidade de Göttingen a homenagear Germain com um título honorário, feito inédito para uma mulher, no entanto, Sophie faleceu antes de aceitar o título devido a um câncer nas mamas.

6. Contribuições Científicas

Sophie foi de extrema importância para a Física. Na Alemanha, Chladni havia feito experimentos sobre as vibrações de membranas elásticas, os quais tiveram resultados muito curiosos. Dessa forma, o cientista visitou Paris, em 1808, a fim de reproduzir tais experimentos. Seu método consistia em despejar areia fina sobre uma placa que vibrava e, à vista disso, padrões eram formados de acordo com as vibrações produzidas. Durante esse período, a teoria matemática acerca dos movimentos de vibração unidimensionais estava completa, mas surgia a necessidade de estender os estudos para as vibrações em superfícies elásticas. Napoleão, líder militar da época,

instigou a Academia de Ciências a abrir uma competição para incentivar a procura de uma explicação matemática para esse problema.

Sophie decidiu participar da competição e submeteu anonimamente sua teoria matemática acerca das vibrações das membranas elásticas, em 21 de setembro de 1811. No entanto, devido ao fato de Germain não possuir um curso formal em Análise, a equação das superfícies elásticas fornecida por ela estava com imprecisões e a questão ainda estava em aberto. A Academia, então, abriu pela segunda vez a competição e Sophie estudou mais profundamente sobre o assunto e, em 23 de setembro de 1813, submeteu novamente seu trabalho, ainda com imprecisões, como relata Legendre em uma carta enviada a Sophie em 4 de dezembro de 1813:

> Não entendo nada, na análise que você está me enviando, certamente, há um erro de redação ou de raciocínio. [...] Se a comissão do Instituto fosse dessa opinião, você poderia ser mencionada com honra; mas temo que a análise fracassada prejudique seriamente a dissertação, apesar do que ela pode conter de bom. (Laubenbacher and Pengelley, 2010)

E foi o que realmente ocorreu, Sophie recebeu apenas uma menção honrosa.

A competição foi estendida novamente e, com mais confiança, Germain abandonou o anonimato. Dessa vez, o trabalho da cientista foi premiado, apesar de ainda ser criticado como incompleto. Sophie, com sua personalidade reservada, não compareceu a premiação pública, onde o prêmio foi anunciado.

Com o conhecimento vasto acerca dessas áreas da Física, auxiliou nos cálculos para a construção da Torre Eiffel. No entanto, a cientista não recebeu o reconhecimento merecido por esse feito. Na lista de agradecimento aos matemáticos que ajudaram na construção da Torre, o nome de Sophie não aparece dentre os 72 nomes incluídos na lista, todos masculinos.

Além disso, Germain contribuiu fortemente para a área de Teoria dos Números. A Academia de Ciências abriu uma nova competição para a prova do Último Teorema de Fermat (UTF) e, apesar da cientista nunca ter publicado sobre esse assunto, é conhecido que ela estudou os teoremas não demonstrados por Fermat devido aos créditos dados a ela em uma segunda edição do ensaio de *Théorie des Nombres* de Legendre. Porém, o resultado creditado a cientista nesse ensaio, conhecido hoje como Teorema de Germain, é uma pequena parte do trabalho de Sophie na tentativa de provar o UTF. Ademais, estudou sobre certos números com propriedades especiais, denominados, posteriormente, de Primos de Germain. Mas o que têm de tão especiais?

Primeiramente, vamos enunciar o Último Teorema de Fermat. Este afirma que não existem $x, y, z \in \mathbb{N}$, todos não-nulos, que satisfaçam a seguinte equação:

$$x^n + y^n = z^n$$

em que $n > 2$ e $n \in \mathbb{N}$.

O Primeiro Caso do UTF afirma que:

$$x^n + y^n = z^n$$

é impossível em inteiros não divisíveis por n.

Um número primo de Germain p é assim chamado quando $2p+1$ é também primo. Temos, como exemplos, os números 2, 3, 5, 11, 23, 29, etc. A infinitude desses números é até hoje desconhecida, sendo titulada como uma conjectura. Os Primos de Germain conquistaram tamanha notoriedade, pois o Primeiro Caso do UTF é válido para $n = p$, onde p é um primo de Germain. Nesse momento, havia apenas provas para $n = 4$, demonstrada pelo próprio Fermat, e para $n = 3$, demonstrada por Euler.

Teorema 6.1 (Teorema de Germain)**.** *Seja p um primo ímpar. Se existe um primo auxiliar q com as seguintes propriedades:*

(1) $x^p + y^p + z^p \equiv 0 \pmod q$ *implica* $x = 0$ *ou* $y = 0$ *ou* $z = 0 \pmod q$ *e*
(2) $a^p \equiv p \pmod q$ *é impossível para qualquer inteiro* a*,*

então o Caso 1 do Último Teorema de Fermat é válido para p.

Uma prova para esse teorema pode ser encontrada em Martinez et al. 2018.

Em 1823, Sophie compartilhou esse teorema com Legendre. Ela havia encontrado primos auxiliares para todos os primos menores que 100, exceto para o 2. Legendre extendeu o teorema de Germain para primos auxiliares das formas $q = 4p + 1, 8p + 1, 10p+1, 14p+1$ ou $16p+1$. Além disso, o cientista provou que o teorema não seria válido quando $q = (mn + 1)$ se m fosse divisível por 3. Assim, foram encontrados primos auxiliares q para todos os primos menores que 197, provando, portanto o Caso 1 do UTF para todos esses primos. Ademais, todas essas descobertas foram feitas antes mesmo da prova para o caso em que $n = 5$.

Os Primos de Germain são de grande importância, pois contribuíram fortemente para diversos avanços nas provas do Primeiro Caso do UTF. Em 1908, Leonard Dickson, generalizando o Teorema de Germain, provou o Primeiro Caso do UTF para todos os primos menores que 7.000 e J. Rosser, em 1940, utilizando também a generalização, provou o Primeiro Caso para todos os primos menores que 41.000.000.

7. A Filósofa

Além do encanto da cientista pelas ciências exatas, sua infância, situada no fervor dos ideais revolucionários do século XVIII, influenciou no seu futuro interesse pela filosofia científica, ao ouvir diversos debates em que seu pai participava. Ademais, Sophie era uma leitora ávida de poemas e era encantada pela música.

Sophie escreveu dois trabalhos filosóficos: *Pensées Diverses*, o qual é uma coleção de breves reflexões acerca de diversos assuntos e *Considérations générales sur l'état des sciences et des lettres aux différentes époques de leur culture*, no qual a filósofa trata das conexões existentes entre a arte e a ciência por meio da história do desenvolvimento intelectual humano. Germain apresenta, nessa última obra, as similaridades entre trabalhos científicos e artísticos, os quais devem seguir certas regras para que sejam considerados belos.

Por exemplo, a uma primeira vista, cálculo e poesia parecem distintos em todos os aspectos, mas perceba que ambos são inspirados por uma ideia de proporção e ordem e suas escritas necessitam de certo estilo para que a mensagem seja devidamente transmitida. De acordo com Germain, ciência e arte são ambas inspiradas pela procura de uma verdade universal por meio da ordem e da simplicidade. Além

disso, Sophie discute sobre o início da atividade intelectual humana e discorre acerca da linguagem, a qual foi inventada para comunicação, mas no decorrer do desenvolvimento humano, foi utilizada para discutir ideias abstratas e novas palavras foram criadas, sem uma definição precisa. É por esse motivo, segundo ela, que uma mesma frase possui uma infinidade de interpretações diferentes. Assim, para Sophie, a Matemática era a única linguagem que não causava essa confusão e apresentava ao ser humano uma realização da verdade.

A escola filosófica de Diderot, ao procurar explicar as similaridades entre ciência e arte, deixou de focar apenas nas causas do fenômeno, isto é, nos "porquês"e passou a se perguntar "como?". Nos escritos de Sophie, é possível perceber a relação próxima de suas reflexões com a escola de Diderot e, também, de Condorcet.

Suas obras não foram publicadas enquanto estava viva e certamente não foram escritas para tal fim, pois tratavam-se, em sua maioria, de notas e reflexões isoladas. Seu sobrinho, Armand-Jacques Lherbette, como forma de homenagem a memória de Sophie, em 1833, compilou e imprimiu suas reflexões filosóficas. Em 1879, esses escritos foram republicados em uma obra titulada *Oeuvres philosophiques de Sophie Germain* (Germain and Stupuy 1896), contendo também correspondências da cientista e sua bibliografia por Hippolyte Stupuy. A obra *Considérations* foi elogiada por Auguste Comte, fundador da filosofia positivista, e influenciou posteriormente em suas reflexões.

8. Agradecimento

Dessa maneira, pode-se perceber o preconceito gritante que havia na época quanto aos lugares ocupados pelas mulheres. Sabendo das dificuldades enfrentadas pela matemática, venho agradecer a persistência dessa incrível mulher em estudar e aprofundar-se em assuntos tão inalcançáveis para as mulheres de sua época. Com toda certeza, seus progressos na Matemática e na Física impactam a ciência como um todo nos dias de hoje. Seus estudos acerca da elasticidade permitiram avanços em grandes construções na engenharia e seus estudos em Teoria dos Números auxiliaram diversos matemáticos.

Além disso, agradeço a Germain pela inspiração para encontrar a voz feminina em um mundo tão masculino. As estatísticas quanto à participação feminina nas ciências exatas melhorou muito, mas ainda é preocupante. Precisamos conhecer mais mulheres como Germain, que deram o primeiro passo para uma equidade de gênero no meio científico, assim como no meio social.

Referências

A. D. Centina and A. Fiocca. The correspondence between Sophie Germain and Carl Friedrich Gauss. *Archive for History of Exact Sciences*, 66(6):585–700, nov 2012. ISSN 1432-0657. doi: 10.1007/s00407-012-0105-x. URL https://doi.org/10.1007/s00407-012-0105-x.

S. Germain and H. Stupuy. *Oeuvres philosophiques de Sophie Germain ; suivies de pensées et de lettres inédites. Et précédées d'une notice sur sa vie et ses oeuvres (Nouv. éd.) / par Hte Stupuy.* 1896. URL https://gallica.bnf.fr/ark:/12148/bpt6k2032890.

A. Granville and M. B. Monagan. The first case of fermat's last theorem is true for all prime exponents up to 714,591,416,091,389. *Transactions of the American Mathematical Society*, 306(1):329–359, 1988. ISSN 00029947. URL http://www.jstor.org/stable/2000841.

N. Hall, M. Jones, and G. Jones. A Vida e o Trabalho de Sophie Germain. pages 32–35, jan 2004. URL <http://gazeta.spm.pt/getArtigo?gid=89.

A. M. Hill. Sophie Germain: a mathematical biography. University of Oregon, 1995.

L. Kelley. Why Were So Few Mathematicians Female? *The Mathematics Teacher*, 89(7):592–596, 1996. ISSN 0025-5769. URL https://www.jstor.org/stable/27969922. Publisher: National Council of Teachers of Mathematics.

R. Laubenbacher and D. Pengelley. "Voici ce que j'ai trouvé:" Sophie Germain's grand plan to prove Fermat's Last Theorem. *Historia Mathematica*, 37(4):641–692, Nov. 2010. ISSN 0315-0860. doi: 10.1016/j.hm.2009.12.002. URL https://www.sciencedirect.com/science/article/pii/S0315086009001347.

F. Martinez, C. G. Moreira, N. Saldanha, and E. Tengan. *Teoria dos Números - um passeio com primos e outros números familiares pelo mundo inteiro*. IMPA - Instituto de Matemática Pura e Aplicada, 5rd edition, 2018. ISBN 978-85-244-0447-4.

M. Perrot. *As mulheres ou os silêncios da história*. EDUSC, Bauru, SP, 2005. ISBN 85-7460-251-5. Tradução: Viviane Ribeiro.

M. Perrot. *Minha historia das mulheres*. Contexto, São Paulo, 2007. ISBN 978-85-7244-348-7. Translation: Angela M. S. Côrrea.

L. Saya. O Clima Revolucionário na França do Século XVIII: politização, descristianização e o impacto nas instituições sociais. pages 1–13, 2016.

L. Schienbinger. *O feminismo mudou a ciência?* EDUSC, Bauru, SP, 2001. ISBN 85-7460-063-6. Tradução: e Raul Fiker.

I. Stewart and D. Tall. *Algebraic Number Theory and Fermat's Last Theorem*. 3rd edition, 1945. ISBN 1568811195. doi: 10.1201/b19331.

Universidade Estadual do Centro-Oeste - PR
Email address: rielitaina@outlook.com