Mathematica

Revista eletrônica de divulgação matemática

Universidade Estadual do Oeste do Paraná - UNIOESTE
Centro de Ciências Exatas e Tecnológicas

Mathematica

Revista eletrônica de divulgação matemática

Cascavel - Paraná

Apresentação

A Revista Mathematica surgiu no final de 2019, com uma conversa informal entre alguns professores do curso de Matemática da Unioeste. Desejávamos inicialmente abrir um espaço para divulgação dos resultados obtidos em projetos de iniciação científica, monografias de conclusão de curso, dissertações de mestrado e pesquisas individuais de professores. Muitos destes trabalhos produzem belos textos de matemática que acabam por serem conhecidos por um número reduzido de pessoas. Surgiu então a ideia de criar uma revista que pudesse divulgar estes resultados na forma de textos curtos, didáticos e com conteúdo matemático que pudesse interessar aos alunos de graduação. Neste contexto, uma revista poderia também atrair a atenção de professores, pesquisadores e acadêmicos de instituições de todo o país.

A nossa intenção era publicar o primeiro número no ano de 2020. Contudo o ano de 2020 iniciou e com ele a pandemia causada pelo Coronavírus. Assim como todas as demais atividades, as atividades universitárias ficaram prejudicadas neste momento. As aulas foram suspensas e os projetos de pesquisa e de iniciação científica foram reestruturados. Não conseguimos no ano de 2020 divulgar a revista de forma satisfatória. Acreditamos ainda que mesmo chegando ao conhecimento de alguns professores e acadêmicos a existência da revista, havia outras preocupações maiores do que enviar um texto para uma revista nova e desconhecida.

Neste ano de 2023, a Revista Mathematica recebeu três textos que foram avaliados e considerados aptos para publicação. O conselho editorial agradece aos autores pelo envio dos trabalhos e também à comissão científica pelas contribuições feitas durante o processo de avaliação e correção dos trabalhos.

O conselho editorial.

Cascavel, 20 de Dezembro de 2023.

Índice de trabalhos

Um estudo sobre a Criptografia RSA

Dafne Moraes Deparis Teixeira - Universidade Federal da Fronteira Sul
Raquel Lehrer - Universidade Estadual do Oeste do Paraná

(*Recebido em 06/11/2023. Aceito em 30/11/2023. Publicado em 20/12/2023*)

Resumo: A necessidade da escrita secreta para o homem é um ponto indiscutível; desde a antiguidade até os dias atuais, o sigilo na comunicação deve ser tão velho quanto o surgimento da escrita. No decorrer do tempo, é possível perceber a evolução de códigos e cifras, que foram impulsionados pela ameaça de informações secretas acabarem nas mãos de inimigos, e também devido aos decifradores que ao descobrirem o funcionamento de uma cifra, obrigavam os cifradores a inventarem uma nova cifra desconhecida e mais segura. Apresentamos aqui alguns aspectos da Criptografia RSA, como sua história, método de funcionamento e os conceitos de matemática envolvidos. Finalizamos com um exemplo de como a Criptografia RSA funciona.

Palavras-chave: Criptografia RSA; números primos; Pequeno Teorema de Fermat.

1 Introdução

Por anos, reis e rainhas necessitavam da comunicação secreta para assuntos de disputa de território; manutenção de segredos de estado; transações militares com seus exércitos. No decorrer da história da Criptografia, é possível perceber a evolução de códigos e cifras. Isso trouxe avanços tecnológicos, que começaram com a invenção de instrumentos criptográficos que facilitavam a cifragem; e posteriormente, a invenção do telégrafo, do rádio e de máquinas que evoluíram até chegarem ao ilustre computador.

Conforme Carneiro (2017, p.4), a palavra criptografia tem origem grega, *kryptos* significa oculto, escondido, secreto, e *graphein*, escrita. Apenas ocultar a mensagem, trata-se do método chamado esteganografia, já a criptografia esconde o significado da mensagem, tornando um texto legível em um texto ilegível, para isso utiliza-se códigos ou cifras, de modo que apenas a pessoa (remetente e destinatário) que possuir a chave transformará o texto ilegível em legível novamente. As cifras podem ser classificadas em cifras de transposição e cifras de substituição. Na cifra de transposição, as letras da mensagem são reordenadas. A cifra de substituição consiste em trocar palavras, frases, sentenças ou até mesmo códigos, por outras palavras, frases, sentenças, ou códigos. Para cifrar o transmissor aplica um algoritmo, composto por uma chave, na mensagem original transformando-a no texto cifrado, o receptor da mensagem fará o caminho inverso para decifra-lá, mas para isso precisa conhecer o algoritmo e a chave, que podem ser combinados previamente. A chave é um elemento confidencial que cifra e decifra a mensagem, ela pode ser simétrica ou assimétrica. Nas cifras que usam chave simétrica, geralmente, no processo de decifragem é aplicado o oposto da chave de cifragem, ou ainda, se sabemos a chave para cifrar

obtemos, facilmente, a chave para decifrar. Já na cifra com chave assimétrica temos uma chave para cifragem e outra diferente para decifragem.

É possível observar, ao longo da história da criptografia, que a distribuição de chaves para a codificação e decodificação de mensagens sempre foi um ponto crítico, pois os criptógrafos conviviam com o risco da chave parar em mãos erradas. Além disso, o crescente uso dos computadores para cifrar comunicações importantes, implicou no aumento da demanda por distribuição de chaves, o que tornou-se impraticável tanto logisticamente quanto pelos custos exorbitantes.

Segundo Singh (2020, p. 277-279), o criptógrafo Whitfield Diffie tinha grande interesse pelo problema da distribuição de chaves. Nascido em 1944, graduou-se em matemática no Massachusetts Institute of Technology, em 1965. Ele possuía uma visão de mundo conectado, onde pessoas comuns com seus computadores interligados por linhas telefônicas nas suas casas pudessem trocar informações através de e-mails, comprar produtos pela internet, realizar transações bancárias, mas isso implicaria na necessidade de privacidade digital. Diffie teve sua visão de mundo concretizada com a ARPANet em 1969, evoluindo para Internet em 1982. Diffie conheceu Hellman e Merkle, e os três vislumbravam resolver o problema da distribuição de chaves. De acordo com Singh (2020, p. 280-281), Martin Hellman, nascido em 1945, era professor da Universidade de Stanford na Califórnia, e Ralph Merkle um refugiado intelectual. Juntos concluíram que a solução para o problema da distribuição de chaves era uma função matemática de mão única, ou seja, difícil de reverter. Após uma busca incessante, Hellman conseguiu chegar a um esquema, usando a função modular $Y^x (\text{mod } P)$, na qual não era necessária a troca de chaves, o receptor e o emissor apenas precisavam decidir juntos os valores de Y e P, sendo Y menor que P, podendo fazer isso por telefone, pois esses valores não eram a chave, portanto não eram sigilosos.

Entretanto, Diffie foi além do conquistado pelos três, chegando ao conceito de chave assimétrica. Até o momento, todas as cifras eram formadas por chaves simétricas, ou seja, para o processo de decifragem era aplicado o oposto da chave de cifragem. Já na cifra com chave assimétrica seria uma chave para cifragem e outra diferente para decifragem. Em 1975, Diffie publicou seu trabalho sobre o sistema de chaves assimétricas, porém ele ainda não havia descoberto uma cifra que preenchesse os requisitos do seu sistema.

A descoberta da função matemática que satisfazia os requisitos do sistema de chaves assimétricas foi realizada, em 1977, por Ron Rivest, Leonard Adleman e Adi Shamir, dois cientistas da computação e um matemático, respectivamente. Eles eram pesquisadores do Laboratório de Ciência da Computação do MIT, Estados Unidos. Por isso, o método de cifra de chave pública mais influente da criptografia moderna ficou conhecido como RSA. Conforme descreveu Singh (2020, p. 300), a RSA é baseada em uma função modular, na qual é colocado um número, que corresponde a mensagem a ser cifrada, o resultado disso é um texto cifrado, ou seja, outro número. Um aspecto importante dessa função de mão única é a possibilidade de escolha do valor de N, cada pessoa para personalizar sua função pode escolher um valor de N diferente. A flexibilidade de N é o que torna-a uma função de mão única reversível sob certas circunstâncias. O valor de N é obtido através da multiplicação de dois números primos p e q, o número N é a

chave pública de uma pessoa, e os números p e q correspondem à chave particular dela. A pessoa pode divulgar sua chave pública, por exemplo, colocá-la em um lista pública de chaves, onde constem as chaves de diversas pessoas. Para cifrar uma mensagem, obtemos a chave pública N do destinatário e colocamos na forma geral da função de mão única, então temos a função de mão única do destinatário. O destinatário receberá o resultado da aplicação da mensagem na sua função personalizada, ele usará sua chave particular p e q para decifrá-la.

A segurança da RSA reside no fato que os valores de p e q não são públicos, e apenas eles revertem a função de mão única utilizada. E a força da RSA reside na escolha de p e q suficientemente grandes, gerando N ainda maior, para que seja virtualmente impossível fatorar N para chegar na chave particular p e q, capaz de decifrar as mensagens. "O único problema para a segurança da criptografia de chave pública RSA é que, em alguma época no futuro, alguém possa encontrar um modo rápido de fatorar N" (Singh, 2020, p. 303).

O método de criptografia RSA que aqui apresentaremos garante, conforme Carneiro (2017, p. 97), "a transmissão de informações confidenciais através de redes inseguras e ainda a autenticação do usuário extremamente necessária em transações bancárias". Em outras palavras, ele tornou viável a comunicação através da Internet e, possibilitou o desenvolvimento da assinatura digital.

O RSA é um método de criptografia de chave pública bastante utilizado, devido a segurança que ele fornece. Esse fato, conforme já escrevemos nesse trabalho, reside na inexistência de uma forma rápida para fatorar números muito grandes. Sendo assim, na próxima seção faremos uma revisão de alguns conceitos matemáticos necessários para a descrição e fundamentação do método de Criptografia RSA, apresentados na seção 3. Na seção 4 explicaremos por que a Criptografia RSA é segura e na seção 5 apresentaremos um exemplo de como a criptografia RSA é efetivamente aplicada numa mensagem.

2 Preliminares

Nesta seção, apresentaremos os conceitos e resultados necessários para a demonstração da validade do método da criptografia RSA. Algumas demonstrações foram omitidas para uma maior fluidez da leitura, mas sempre foram indicadas referências onde tais demonstrações podem ser encontradas.

Os conjuntos numéricos utilizados serão os seguintes: $\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$, o conjunto dos números naturais; $\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$, o conjunto dos números inteiros. Denotaremos por $\mathbb{N}^*$, quando $\mathbb{N} \setminus \{0\}$, e também $\mathbb{Z}^*$, quando for $\mathbb{Z} \setminus \{0\}$.

Definição 1. Sejam a, $b \in \mathbb{Z}$. Dizemos que b *divide* a se existir algum $q \in \mathbb{Z}$ tal que $a = b \cdot q$. Utilizamos a notação $b \mid a$. Caso b não divide a, denotamos por $b \nmid a$.

Definição 2. Um número inteiro p é chamado *número primo* se as seguintes condições se verificam: $p \neq 0$, $p \neq \pm 1$ e os únicos divisores de p são ± 1, $\pm p$.

Se um número inteiro $n \neq \{0, \pm 1\}$ não é primo, então dizemos que n é *composto*. Nesse caso, n não possui apenas os divisores ± 1 e $\pm n$. Dessa maneira, devem existir números inteiros u e v tais que $1 < u < n$ e $1 < v < n$ e $n = u \cdot v$.

Definição 3. Sejam a e b dois números inteiros, $a \neq 0$ ou $b \neq 0$. Dizemos que $d \in \mathbb{Z}$ é o *máximo divisor comum* de a e b se cumpre as seguintes condições:

i) $d > 0$;

ii) $d \mid a$ e $d \mid b$;

iii) se d' é um inteiro tal que $d' \mid a$ e $d' \mid b$, então $d' \mid d$ (ou seja, todo divisor comum de a e b também é divisor de d).

Definição 4. Sejam a e b dois inteiros, $a \neq 0$ ou $b \neq 0$. Dizemos que a e b são *primos entre si (ou coprimos)* quando $mdc(a, b) = 1$.

Definição 5. Sejam a e b inteiros quaisquer e m um inteiro maior que 1. Dizemos que *a é congruente a b módulo m* se $m \mid (a - b)$. Denotamos isto por $a \equiv b (\text{mod } m)$. Se $m \nmid (a - b)$ dizemos que *a é incongruente a b módulo m* e denotamos $a \not\equiv b (\text{mod } m)$.

Segue diretamente das definições acima a seguinte proposição:

Proposição 6. *Se a, b e m são inteiros, com $m > 1$, temos que $a \equiv b (mod\ m)$ se, e somente se, existir um inteiro k tal que $a = b + k \cdot m$.*

Proposição 7. *Seja m um número inteiro tal que $m > 1$.*

(a) Se a e b são inteiros tais que $a \equiv b (mod\ m)$, então $a - b \equiv 0 (mod\ m)$.

(b) Se a, b, c e d são inteiros tais que $a \equiv b (mod\ m)$ e $c \equiv d (mod\ m)$, então $a + c \equiv b + d (mod\ m)$.

(c) Se a, b, c e d são inteiros tais que $a \equiv b (mod\ m)$ e $c \equiv d (mod\ m)$, então $a - c \equiv b - d (mod\ m)$.

(d) Se a, b, c e d são inteiros tais que $a \equiv b (mod\ m)$ e $c \equiv d (mod\ m)$, então $a \cdot c \equiv b \cdot d (mod\ m)$.

(e) Se a e b são inteiros tais que $a \equiv b (mod\ m)$, então $a \cdot x \equiv b \cdot x (mod\ m)$, para todo inteiro x.

(f) Seja d um inteiro tal que $mdc(d, m) = 1$. Se a e b são inteiros tais que $a \cdot d \equiv b \cdot d (mod\ m)$, então $a \equiv b (mod\ m)$.

(g) Se a, b e d são inteiros, com $d \neq 0$, tais que $a \cdot d \equiv b \cdot d (mod\ m \cdot d)$, então $a \equiv b (mod\ m)$.

(h) Se a e b são inteiros tais que $a \equiv b (mod\ m)$, então $a^x \equiv b^x (mod\ m)$ para todo natural x.

A demonstração desta proprosição pode ser encontrada em Silva e Gomes (2018, p. 167 - 169).

Definição 8. Sejam a, r e m números inteiros, com $m > 1$. Dizemos que r é um *resíduo de a módulo m* se $a \equiv r(\text{mod } m)$.

Definição 9. Seja $m \in \mathbb{Z}$ tal que $m > 1$. Dizemos que o conjunto de números inteiros $\{r_1, r_2, \ldots, r_m\}$ é um *sistema completo de resíduos módulo m* se

(1) $r_i \not\equiv r_j(\text{mod } m)$ para $i \neq j$;

(2) para todo inteiro n existe um r_i tal que $n \equiv r_i(\text{mod } m)$.

Exemplo 1. Os conjuntos $\{0, 1, 2, 3, 4\}$ e $\{5, 16, 17, 28, 29\}$ são sistemas completos de resíduos módulo 5.

A demonstração da proposição a seguir pode ser encontrada em Santos (2020, p. 34).

Proposição 10. *Se k inteiros $r_1, r_2, \ldots, r_k$ formam um sistema completo de resíduos módulo m então $k = m$.*

Definição 11. Sejam $a \in \mathbb{Z}$ e m um inteiro maior que 1. Uma solução de $a \cdot x \equiv 1(\text{mod } m)$ é chamado de *inverso de a módulo m.*

Proposição 12. *Seja m um inteiro maior que 1. O número inteiro a possui inverso módulo m se, e somente se, $mdc(a, m) = 1$.*

Tal resultado pode ser encontrado em Coutinho (2009, p. 82-83).

Demonstraremos agora dois importantes teoremas em Teoria dos Números e com aplicabilidade no método RSA. Conforme Boyer (2012, p. 310), o Pequeno Teorema de Fermat foi uma conjetura de Fermat, sendo Euler o primeiro a publicar uma demonstração dela. E, a partir disso, Euler demonstrou uma afirmação um pouco mais geral, que trata-se do Teorema de Euler.

Teorema 13. *(Pequeno Teorema de Fermat) Seja p primo. Se $p \nmid a$ então $a^{p-1} \equiv 1(mod\ p)$.*

Prova. Sabemos que o conjunto formado pelos p números $0, 1, 2, \ldots, p-1$ constitui um sistema completo de resíduos módulo p. Isto significa que qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado em correspondência biunívoca com um subconjunto de $\{0, 1, 2, \ldots, p-1\}$. Vamos agora considerar os números $a, 2 \cdot a, 3 \cdot a, \ldots, (p-1) \cdot a$. Como $mdc(a, p) = 1$, nenhum destes números $i \cdot a$, $1 \leq i \leq p-1$ é divisível por p, ou seja, nenhum é congruente a zero módulo p. Quaisquer dois deles são incongruentes módulo p, pois $a \cdot j \equiv a \cdot k(\text{mod } p)$ implica $j \equiv k(\text{mod } p)$ e isto só possível se $j = k$, uma vez que ambos j e k são positivos e menores que p e não divisíveis por p. Temos, portanto, um conjunto de $p-1$ elementos incongruentes módulo p e não divisíveis por p. Logo, cada um deles é congruente a exatamente um dentre os elementos $0, 1, 2, \ldots, p-1$. Se multiplicarmos estas congruências, membro a membro, teremos:

$$a \cdot (2 \cdot a) \cdot (3 \cdot a) \ldots (p-1) \cdot a \equiv 1 \cdot 2 \cdot 3 \ldots (p-1)(\text{mod } p)$$

ou seja, $a^{p-1} \cdot (p-1)! \equiv (p-1)!(\text{mod } p)$. Mas como, $mdc((p-1)!, p) = 1$, podemos cancelar o fator $(p-1)!$ em ambos os lados, obtendo

$$a^{p-1} \equiv 1(\text{mod } p),$$

o que conclui a demonstração. □

Definição 14. Se m é um inteiro positivo, a *função ϕ de Euler*, denotada por $\phi(m)$, é definida como sendo o número de inteiros positivos menores do que ou iguais a m que são coprimos com m.

Definição 15. Um *sistema reduzido de resíduos módulo m* é um conjunto de $\phi(m)$ inteiros $r_1, r_2, \ldots, r_{\phi(m)}$, tais que cada elemento do conjunto é coprimo com m, e se $i \neq j$, então $r_i \not\equiv r_j(\text{mod } m)$.

Exemplo 2. O conjunto $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ é um sistema completo de resíduos módulo 9, portanto $\{1, 2, 4, 5, 7, 8\}$ é sistema reduzido de resíduos módulo 9, ou seja, $\phi(9) = 6$. A fim de obter um sistema reduzido de resíduos de um sistema completo módulo m, basta retirar os elementos do sistema completo que não são coprimos com m.

É possível observar que $\phi(m) \leq m - 1$ para $m \geq 2$. Também para $m \geq 2$, temos que $\phi(m) = m - 1$ se, e somente se, m é um número primo, veja Burton (1980, p.136 - 137). Realmente, m é primo se, e somente se, $\{1, 2, \ldots, m-1\}$ é um sistema reduzido de resíduos módulo m, o que significa $\phi(m) = m - 1$.

Teorema 16. *Sejam a um inteiro positivo tal que $mdc(a, m) = 1$. Se $r_1, r_2, \ldots, r_{\phi(m)}$ é um sistema reduzido de resíduos módulo m, então $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\phi(m)}$ é, também, um sistema reduzido de resíduos módulo m.*

Prova. Na sequência $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\phi(m)}$ temos $\phi(m)$ elementos, é necessário mostrar que todos eles são coprimos com m e, dois a dois, incongruentes módulo m. Como $mdc(a, m) = 1$ e $mdc(r_i, m) = 1$, temos que $mdc(a \cdot r_i, m) = 1$ (Hefez (2016), p. 71). Logo, nos resta mostrar que $a \cdot r_i \not\equiv a \cdot r_j(\text{mod } m)$ se $i \neq j$. Mas, como $mdc(a, m) = 1$, pelo item (f) da Proposição 7, de $a \cdot r_i \equiv a \cdot r_j(\text{mod } m)$ temos $r_i \equiv r_j(\text{mod } m)$, o que implica $i = j$, uma vez que $r_1, r_2, \ldots, r_{\phi(m)}$ é um sistema reduzido de resíduos módulo m, o que conclui a demonstração. □

Proposição 17. *As seguinte propriedades da função ϕ de Euler são válidas:*

i) Sejam p um número primo e k um natural não nulo. Então $\phi(p^k) = p^k - p^{k-1}$.

ii) $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$, sempre que $m, n \in \mathbb{N}^*$ e $mdc(m, n) = 1$.

iii) Se $n = p_1^{a_1} \cdot p_2^{a_2} \ldots p_t^{a_t}$ é a fatoração de n em números primos, onde $n > 1$, então

$$\phi(n) = (p_1^{a_1} - p_1^{a_1-1}) \cdot (p_2^{a_2} - p_2^{a_2-1}) \ldots (p_t^{a^t} - p_t^{a_t-1}).$$

A demonstração de tal proposição pode ser encontrada em Silva e Gomes (2018, p. 212 - 214).

Teorema 18. *(Euler) Sejam m, $a \in \mathbb{Z}$ com $m > 1$ e $mdc(a, m) = 1$, então*

$$a^{\phi(m)} \equiv 1(mod\ m).$$

Prova. O Teorema 16 mostra que os elementos $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\phi(m)}$ constituem um sistema reduzido de resíduos módulo m se $mdc(a, m) = 1$ e $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ for um sistema reduzido de resíduos módulo m. Isto significa que $a \cdot r_i$ é congruente a exatamente um dos r_j, $1 \leq j \leq \phi(m)$, e portanto o produto dos $a \cdot r_i$ deve ser congruente ao produto dos r_j módulo m, isto é,

$$a \cdot r_1 \cdot a \cdot r_2 \cdots a \cdot r_{\phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\phi(m)} (\text{mod } m),$$

ou seja,

$$a^{\phi(m)} \cdot r_1 \cdot r_2 \cdots r_{\phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\phi(m)} (\text{mod } m).$$

Como

$$mdc\left(\prod_{i=1}^{\phi(m)} r_i, m\right) = 1,$$

pelo item (f) da Proposição 7, podemos cancelar

$$\prod_{i=1}^{\phi(m)} r_i$$

em ambos os lados para obter $a^{\phi(m)} \equiv 1(\text{mod } m)$. □

Como para p primo, $\phi(p) = p - 1$, o Teorema de Euler é uma generalização do Pequeno Teorema de Fermat.

3 Codificação e Decodificação

A primeira etapa para conseguirmos aplicar o método de criptografia RSA trata-se de uma pré-codificação, que consiste na substituição das letras da mensagem por números, o que transforma a mensagem em uma sequência numérica. A substituição é realizada usando a seguinte tabela:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Os espaços entre as palavras serão substituídos pelo número 36.

Observamos que a escolha desses números para substituir as letras em vez de 1, 2, 3, ..., e assim sucessivamente, é para evitar ambiguidades. Por exemplo, ao corresponderemos A e B aos números 1 e 2, respectivamente, no decorrer do texto, o número 12 resultaria na dúvida, é A e B ou é L?

Posteriormente, determinamos os parâmetros do método de criptografia RSA, escolhendo dois números primos p e q. O par (n, e) é a chave de codificação do sistema RSA, sendo $n = p \cdot q$ e e um número inteiro, tal que e é inversível módulo $\phi(n)$. Como vimos na seção anterior, a função ϕ é conceituada pela Definição 14, e os cálculos de $\phi(n)$ podem ser realizados usando a Proposição 17, isto é, $\phi(n) = (p_1^{a_1} - p_1^{a_1-1}) \cdot (p_2^{a_2} - p_2^{a_2-1}) = (p^1 - p^0) \cdot (q^1 - q^0) = (p-1) \cdot (q-1)$. Já o número e para ser inversível módulo $\phi(n)$ precisa seguir o disposto na Proposição 12, ou seja, $mdc(e, \phi(n)) = 1$.

Para finalizar a pré-codificação, a sequência numérica será dividida em blocos, sendo cada bloco denotado por b. A divisão em blocos seguirá regras, os blocos não podem iniciar com o número 0 e deverão ser menores que n, para evitar problemas na decodificação; e para maior segurança, não corresponder a palavras ou letras, o que torna impossível a análise de frequência.

O bloco b codificado será $C(b) = a$, que é igual ao resto da divisão de b^e por n, ou ainda,

$$b^e \equiv a (\text{mod } n), \text{ com } 0 < a < n. \tag{1}$$

Cada bloco b passará pela etapa de codificação separadamente. A mensagem codificada é uma sequência blocos codificados $(C(b_1), C(b_2), \ldots, C(b_n))$. Vale salientar que os blocos codificados devem ser mantidos separados, para não tornar impossível a decodificação da mensagem.

A chave de decodificação do sistema RSA é o par (n, d), onde d é o inverso de e módulo $\phi(n)$. Assim como acontece com e, o $mdc(d, \phi(n)) = 1$. É possível obter d pelo método das divisões sucessivas, resolvendo a equação diofantina que resulta da equação de congruência linear $e \cdot d \equiv 1 (\text{mod } \phi(n))$ (Definição 11).

A decodificação trata-se de encontrar o bloco da mensagem original. O bloco da mensagem decodificado será $D(a) = l$, que é igual ao resto da divisão de a^d por n, ou seja,

$$a^d \equiv l (\text{mod } n) \text{ com } 0 < l < n. \tag{2}$$

Para calcularmos as congruências (1) e (2), é possível aplicar os Teoremas de Fermat e de Euler e também a Proposição 7.

4 Por que o método de Criptografia RSA funciona e é seguro?

O método funciona se, decodificando um bloco codificado, conseguimos obter o bloco correspondente da mensagem original. Considerando as notações adotadas anteriormente, temos um sistema de Criptografia RSA de parâmetros p e q, $n = p \cdot q$, a chave de codificação (n, e) e a chave de decodificação (n, d), e queremos mostrar que se b é um inteiro e $1 \leq b \leq n - 1$, então

$D(C(b)) \equiv b(\text{mod } n)$. Com a orientação de dividirmos a mensagem original em blocos menores do que n, temos b e $D(C(b))$ estão entre 1 e $n-1$, ou seja, só podem ser congruentes módulo n se são iguais. Sendo assim, precisamos provar apenas que $D(C(b)) \equiv b(\text{mod } n)$. De (1) e (2), contamos com $C(b) \equiv b^e \equiv a(\text{mod } n)$ e $D(a) \equiv a^d \equiv l(\text{mod } n)$, o que resulta em

$$D(C(b)) \equiv (b^e)^d \equiv b^{e \cdot d}(\text{mod } n). \tag{3}$$

Dessa forma, e retomando o fato que $n = p \cdot q$, onde p e q são números primos distintos, calcularemos, separadamente,

$$b^{e \cdot d} \equiv b(\text{mod } p) \tag{4}$$

e

$$b^{e \cdot d} \equiv b(\text{mod } q). \tag{5}$$

Sabemos que d é o inverso de e módulo $\phi(n)$, logo, pela Definição 11, $e \cdot d \equiv 1(\text{mod } \phi(n))$, o que corresponde a $e \cdot d = 1 + k \cdot \phi(n)$ pela Proposição 6. Usando a Proposição 17,

$$e \cdot d = 1 + k \cdot (p-1) \cdot (q-1), \text{ para algum inteiro } k. \tag{6}$$

Substituindo (6) em (4) e (5),

$$b^{e \cdot d} \equiv b^{1+k \cdot (p-1) \cdot (q-1)} \equiv b \cdot b^{k \cdot (p-1) \cdot (q-1)}(\text{mod } p). \tag{7}$$

e

$$b^{e \cdot d} \equiv b^{1+k \cdot (p-1) \cdot (q-1)} \equiv b \cdot b^{k \cdot (p-1) \cdot (q-1)}(\text{mod } q). \tag{8}$$

Primeiramente, mostraremos que $b^{e \cdot d} \equiv b(\text{mod } p)$. Supondo que $p \mid b$, logo $b = 0 + k \cdot p$, para algum k inteiro, o que resulta em, pela Proposição 6, $b \equiv 0(\text{mod } p)$, e também $b^{e \cdot d} \equiv 0(\text{mod } p)$. Logo,

$$b^{e \cdot d} \equiv b(\text{mod } p). \tag{9}$$

Agora, supondo que $p \nmid b$, pelo Pequeno Teorema de Fermat,

$$b^{p-1} \equiv 1(\text{mod } p).$$

Assim, dos itens (h) e (e) da Proposição 7, obtemos, respectivamente,

$$(b^{(p-1)})^{k \cdot (q-1)} \equiv 1^{k \cdot (q-1)} \equiv 1(\text{mod } p)$$

e

$$(b^{(p-1)})^{k \cdot (q-1)} \cdot b \equiv 1 \cdot b \equiv b(\text{mod } p) \tag{10}$$

De, (7) e (10), $b^{e \cdot d} \equiv b(\text{mod } p)$. Portanto, $b^{e \cdot d} \equiv b(\text{mod } p)$ para qualquer b inteiro. Analogamente, $b^{e \cdot d} \equiv b(\text{mod } q)$ para qualquer b inteiro.

Acabamos de mostrar as congruências $b^{e \cdot d} \equiv b(\text{mod } p)$ e $b^{e \cdot d} \equiv b(\text{mod } q)$ para qualquer b inteiro. A Definição 5 de congruência nos permite dizer que p e q dividem $b^{e \cdot d} - b$. Como

$mdc(p, q) = 1$, segue que $n = p \cdot q$ divide $b^{e \cdot d} - b$ (vide Hefez (2016, p. 71)). Portanto, podemos concluir que $b^{e \cdot d} \equiv b (\text{mod } n)$. Isto encerra a demonstração de que o método RSA funciona.

Como vimos anteriormente, a criptografia RSA é um método de chave pública, considerando os parâmetros do sistema adotados anteriormente, sendo eles os números primos p e q, e $n = p \cdot q$. A chave de codificação ou chave pública (n, e) é acessível a qualquer usuário, já a chave de decodificação (n, d) é privada. Por isso, o método RSA só será seguro se for difícil de calcular d, quando conhecemos apenas n e e.

Para calcular d aplicamos o método das divisões sucessivas a $\phi(n)$ e e. No entanto, para calcular $\phi(n)$ é necessário fatorar n para obter p e q. Se n for um número grande, fatorá-lo torna-se muito difícil por não existirem algoritmos rápidos para fatoração.

Então, acredita-se que quebrar o código RSA é equivalente a fatorar n. Por isso é importante a escolha de primos suficientemente grandes.

5 Exemplo

Para ilustrar o método de criptografia RSA descrito acima, faremos um exemplo, codificando a mensagem **"PIERRE DE FERMAT"**.

Primeiramente, faremos a etapa de pré-codificação usando a tabela da seção 3, o que nos dá a seguinte sequência numérica:

2518142727143613143615142722 1029

Os parâmetros escolhidos são $p = 5$ e $q = 17$, então temos $n = p \cdot q = 5 \cdot 17 = 85$ e $\phi(n) = (p-1) \cdot (q-1) = 4 \cdot 16 = 64$. O número 3 é inversível módulo $\phi(85) = 64$, então tomaremos $e = 3$. Lembrando que os blocos devem ser menores que $n = 85$, obtemos os seguintes blocos da sequência numérica acima:

2-51-81-42-72-71-43-61-31-43-61-51-42-72-2-10-2-9

Seja $(85, 3)$ a chave de codificação e $C(b) \equiv b^e (\text{mod } n)$ a fórmula, iniciemos a codificação dos blocos:

1. $b_1 = 2$: Como $2^3 = 8$ e $8 \equiv 8 (\text{mod } 85)$. Logo $C(2) = 8$.

2. $b_2 = 51$: Como $51^3 = 132651$ e $132651 \equiv 51 (\text{mod } 85)$. Logo $C(51) = 51$.

3. $b_3 = 81$: Como $81 \equiv -4 (\text{mod } 85)$, então $81^3 \equiv (-4)^3 \equiv -64 \equiv 21 (\text{mod } 85)$. Logo $C(81) = 21$.

4. $b_4 = 42$: Como $42^3 = 74088$ e $42^3 \equiv 53 (\text{mod } 85)$. Logo $C(42) = 53$.

5. $b_5 = 72$: Como $72^3 = 373248$ e $72^3 \equiv 13 (\text{mod } 85)$. Logo $C(72) = 13$.

6. $b_6 = 71$: Como $71^3 = 357911$ e $71^3 \equiv 61(\text{mod } 85)$. Logo $C(71) = 61$.

7. $b_7 = 43$: Como $43^3 = 79507$ e $43^3 \equiv 32(\text{mod } 85)$. Logo $C(43) = 32$.

8. $b_8 = 61$: Como $61^3 = 226981$ e $61^3 \equiv 31(\text{mod } 85)$. Logo $C(61) = 31$.

9. $b_9 = 31$: Como $31^3 = 29791$ e $31^3 \equiv 41(\text{mod } 85)$. Logo $C(31) = 41$.

10. $b_{10} = 43$: Como $43^3 = 79507$ e $43^3 \equiv 32(\text{mod } 85)$. Logo $C(43) = 32$.

11. $b_{11} = 61$: Como $61^3 = 226981$ e $61^3 \equiv 31(\text{mod } 85)$. Logo $C(61) = 31$.

12. $b_{12} = 51$: Como $51^3 = 132651$ e $132651 \equiv 51(\text{mod } 85)$. Logo $C(51) = 51$.

13. $b_{13} = 42$: Como $42^3 = 74088$ e $42^3 \equiv 53(\text{mod } 85)$. Logo $C(42) = 53$.

14. $b_{14} = 72$: Como $72^3 = 373248$ e $72^3 \equiv 13(\text{mod } 85)$. Logo $C(72) = 13$.

15. $b_{15} = 2$: Como $2^3 = 8$ e $8 \equiv 8(\text{mod } 85)$. Logo $C(2) = 8$.

16. $b_{16} = 10$: Como $10^3 = 10^2 \cdot 10$, $10 \equiv 10(\text{mod } 85)$ e $10^2 \equiv 15(\text{mod } 85)$, então $10^3 \equiv 15 \cdot 10 \equiv 65(\text{mod } 85)$. Logo $C(10) = 65$.

17. $b_{17} = 2$: Como $2^3 = 8$ e $8 \equiv 8(\text{mod } 85)$. Logo $C(2) = 8$.

18. $b_{18} = 9$: Como $9^3 = 9^2 \cdot 9 = 81 \cdot 9$ e $81 \equiv (-4)(\text{mod } 85)$, então $9^3 \equiv (-4) \cdot 9 \equiv -36 \equiv 49(\text{mod } 85)$. Logo $C(9) = 49$.

Portanto, a mensagem codificada é

8-51-21-53-13-61-32-31-41-32-31-51-53-13-8-65-8-49

Agora, o objetivo é decodificar, então será necessário a chave de decodificação $(85, d)$, mas ainda não conhecemos o d. O que sabemos é que d é o inverso de e módulo $\phi(n)$, logo $3 \cdot d \equiv 1(\text{mod } 64)$, o que implica, $64 \cdot k + 3 \cdot (-d) = 1$. Aplicando o método das divisões sucessivas de 64 por 3, temos que $1 = 64 + 3 \cdot (-21)$. Logo, o inverso de 3 módulo 64 é -21, mas precisamos de d positivo, pois usaremos como expoente de potências, então $d = 64 - 21 = 43$ que é o menor inteiro positivo congruente a -21 módulo 64. Agora, já possuímos a chave de decodificação (85, 43) e a fórmula $D(a) \equiv a^d(\text{mod } n)$, então podemos ilustrar o processo de decodificação dos blocos:

1. $a_1 = 8$: Como $8^3 = 512$, $512 \equiv 2(\text{mod } 85)$ e $43 = 3 \cdot 14 + 1$, temos

$$\begin{aligned} 8^3 &\equiv 2(\text{mod } 85) \\ (8^3)^{14} &\equiv 2^{14} \equiv 16384 \equiv 64(\text{mod } 85) \\ 8^{42} \cdot 8 &\equiv 64 \cdot 8(\text{mod } 85) \\ 8^{43} &\equiv 2(\text{mod } 85). \end{aligned}$$

Logo $D(8) = 2$.

2. $a_2 = 51$: Como $51^3 = 132651$, $132651 \equiv 51(\text{mod } 85)$ e $43 = 3 \cdot 14 + 1$, temos

$$\begin{aligned} 51^3 &\equiv 51(\text{mod } 85) \\ (51^3)^{14} &\equiv 51^{14} \equiv 51^3 \cdot 51^3 \cdot 51^3 \cdot 51^3 \cdot 51^2 \equiv 51 \cdot 51 \cdot 51 \cdot 51 \cdot 51^2(\text{mod } 85) \\ 51^{42} &\equiv 51^3 \cdot 51^3 \equiv 51 \cdot 51(\text{mod } 85) \\ 51^{42} \cdot 51 &\equiv 51 \cdot 51 \cdot 51 \equiv 51^3 \equiv 51(\text{mod } 85) \\ 51^{43} &\equiv 51(\text{mod } 85). \end{aligned}$$

Logo $D(51) = 51$.

3. $a_3 = 21$: Como $21^4 = 194481$, $194481 \equiv 1(\text{mod } 85)$ e $43 = 4 \cdot 10 + 3$, temos

$$\begin{aligned} 21^4 &\equiv 1(\text{mod } 85) \\ (21^4)^{10} &\equiv 1^{10} \equiv 1(\text{mod } 85) \\ 21^{40} &\equiv 1(\text{mod } 85) \\ 21^{40} \cdot 21^3 &\equiv 1 \cdot 21^3 \equiv 9261 \equiv 81(\text{mod } 85) \\ 21^{43} &\equiv 81(\text{mod } 85). \end{aligned}$$

Logo $D(21) = 81$.

4. $a_4 = 53$: Como $53^4 = 7890481$, $7890481 \equiv 16(\text{mod } 85)$, $16^2 = 256 \equiv 1(\text{mod } 85)$ e $43 = 4 \cdot 10 + 3$, temos

$$\begin{aligned} 53^4 &\equiv 16(\text{mod } 85) \\ (53^4)^{10} &\equiv 16^{10} \equiv (16^2)^5 \equiv 1^5 \equiv 1(\text{mod } 85) \\ 53^{40} &\equiv 1(\text{mod } 85) \\ 53^{40} \cdot 53^3 &\equiv 1 \cdot 53^3 \equiv 148877 \equiv 42(\text{mod } 85) \\ 53^{43} &\equiv 42(\text{mod } 85). \end{aligned}$$

Logo $D(53) = 42$.

5. $a_5 = 13$: Como $13^2 = 169$, $169 \equiv -1(\text{mod } 85)$ e $43 = 2 \cdot 21 + 1$, temos

$$\begin{aligned} 13^2 &\equiv -1(\text{mod } 85) \\ (13^2)^{21} &\equiv (-1)^{21} \equiv -1(\text{mod } 85) \\ 13^{42} &\equiv -1(\text{mod } 85) \\ 13^{42} \cdot 13 &\equiv -1 \cdot 13 \equiv -13 \equiv 72(\text{mod } 85) \\ 13^{43} &\equiv 72(\text{mod } 85). \end{aligned}$$

Logo $D(13) = 72$.

6. $a_6 = 61$: Como $61^4 = 13845841$, $13845841 \equiv 21(\text{mod } 85)$, $21^4 \equiv 1(\text{mod } 85)$ e $43 = 4 \cdot 10 + 3$, temos

$$61^4 \equiv 21(\text{mod } 85)$$

$$\begin{aligned}(61^4)^{10} &\equiv (21)^{10} \equiv (21^4)^2 \cdot 21^2 \equiv 1^2 \cdot 441 \equiv 16(\text{mod } 85)\\ 61^{40} &\equiv 16(\text{mod } 85)\\ 61^{40} \cdot 61^3 &\equiv 16 \cdot 226981 \equiv 16 \cdot 31 \equiv 496 \equiv 71(\text{mod } 85)\\ 61^{43} &\equiv 71(\text{mod } 85).\end{aligned}$$

Logo $D(61) = 71$.

7. $a_7 = 32$: Como $32^2 = 1024$, $1024 \equiv 4(\text{mod } 85)$, $43 = 2 \cdot 20 + 3$, temos

$$\begin{aligned}32^2 &\equiv 4(\text{mod } 85)\\ (32^2)^{20} &\equiv 4^{20} \equiv 2^{40} \equiv (2^8)^5 \equiv 1^5 \equiv 1(\text{mod } 85)\\ 32^{40} \cdot 32^3 &\equiv 1 \cdot 32^2 \cdot 32 \equiv 4 \cdot 32 \equiv 128 \equiv 43(\text{mod } 85)\\ 32^{43} &\equiv 43(\text{mod } 85).\end{aligned}$$

Logo $D(32) = 43$.

8. $a_8 = 31$: Como $31^4 = 923521$, $923521 \equiv 81 \equiv -4(\text{mod } 85)$, $43 = 4 \cdot 10 + 3$, temos

$$\begin{aligned}31^4 &\equiv -4(\text{mod } 85)\\ (31^4)^{10} &\equiv (-4)^{10} \equiv 2^{20} \equiv (2^8)^2 \cdot 2^4 \equiv 1^2 \cdot 16 \equiv 16(\text{mod } 85)\\ 31^{40} \cdot 31^3 &\equiv 16 \cdot 29791 \equiv 16 \cdot 41 \equiv 61(\text{mod } 85)\\ 31^{43} &\equiv 61(\text{mod } 85).\end{aligned}$$

Logo $D(31) = 61$.

9. $a_9 = 41$: Como $41^4 = 2825761$, $2825761 \equiv 21(\text{mod } 85)$, $21^4 \equiv 1(\text{mod } 85)$ e $43 = 4 \cdot 10 + 3$, temos

$$\begin{aligned}41^4 &\equiv 21(\text{mod } 85)\\ (41^4)^{10} &\equiv (21)^{10} \equiv (21^4)^2 \cdot 21^2 \equiv (1)^2 \cdot 441 \equiv 1 \cdot 16 \equiv 16(\text{mod } 85)\\ 41^{40} \cdot 41^3 &\equiv 16 \cdot 68921 \equiv 16 \cdot 71 \equiv 1136 \equiv 31(\text{mod } 85)\\ 41^{43} &\equiv 31(\text{mod } 85).\end{aligned}$$

Logo $D(41) = 31$.

10. $a_{10} = 32$: Como $32^2 = 1024$, $1024 \equiv 4(\text{mod } 85)$, $43 = 2 \cdot 20 + 3$, temos

$$\begin{aligned}32^2 &\equiv 4(\text{mod } 85)\\ (32^2)^{20} &\equiv 4^{20} \equiv 2^{40} \equiv (2^8)^5 \equiv 1^5 \equiv 1(\text{mod } 85)\\ 32^{40} \cdot 32^3 &\equiv 1 \cdot 32^2 \cdot 32 \equiv 4 \cdot 32 \equiv 128 \equiv 43(\text{mod } 85)\\ 32^{43} &\equiv 43(\text{mod } 85).\end{aligned}$$

Logo $D(32) = 43$.

11. $a_{11} = 31$: Como $31^4 = 923521$, $923521 \equiv 81 \equiv -4(\text{mod } 85)$, $43 = 4 \cdot 10 + 3$, temos

$$31^4 \equiv -4(\text{mod } 85)$$

$$\begin{aligned}(31^4)^{10} &\equiv (-4)^{10} \equiv 2^{20} \equiv (2^8)^2 \cdot 2^4 \equiv 1^2 \cdot 16 \equiv 16(\text{mod } 85)\\ 31^{40} \cdot 31^3 &\equiv 16 \cdot 29791 \equiv 16 \cdot 41 \equiv 61(\text{mod } 85)\\ 31^{43} &\equiv 61(\text{mod } 85).\end{aligned}$$

Logo $D(31) = 61$.

12. $a_{12} = 51$: Como $51^3 = 132651$, $132651 \equiv 51(\text{mod } 85)$ e $43 = 3 \cdot 14 + 1$, temos

$$\begin{aligned}51^3 &\equiv 51(\text{mod } 85)\\ (51^3)^{14} &\equiv 51^{14} \equiv 51^3 \cdot 51^3 \cdot 51^3 \cdot 51^3 \cdot 51^2 \equiv 51 \cdot 51 \cdot 51 \cdot 51 \cdot 51^2(\text{mod } 85)\\ 51^{42} &\equiv 51^3 \cdot 51^3 \equiv 51 \cdot 51(\text{mod } 85)\\ 51^{42} \cdot 51 &\equiv 51 \cdot 51 \cdot 51 \equiv 51^3 \equiv 51(\text{mod } 85)\\ 51^{43} &\equiv 51(\text{mod } 85).\end{aligned}$$

Logo $D(51) = 51$.

13. $a_{13} = 53$: Como $53^4 = 7890481$, $7890481 \equiv 16(\text{mod } 85)$, $16^2 = 256 \equiv 1(\text{mod } 85)$ e $43 = 4 \cdot 10 + 3$, temos

$$\begin{aligned}53^4 &\equiv 16(\text{mod } 85)\\ (53^4)^{10} &\equiv 16^{10} \equiv (16^2)^5 \equiv 1^5 \equiv 1(\text{mod } 85)\\ 53^{40} &\equiv 1(\text{mod } 85)\\ 53^{40} \cdot 53^3 &\equiv 1 \cdot 53^3 \equiv 148877 \equiv 42(\text{mod } 85)\\ 53^{43} &\equiv 42(\text{mod } 85).\end{aligned}$$

Logo $D(53) = 42$.

14. $a_{14} = 13$: Como $13^2 = 169$, $169 \equiv -1(\text{mod } 85)$ e $43 = 2 \cdot 21 + 1$, temos

$$\begin{aligned}13^2 &\equiv -1(\text{mod } 85)\\ (13^2)^{21} &\equiv (-1)^{21} \equiv -1(\text{mod } 85)\\ 13^{42} &\equiv -1(\text{mod } 85)\\ 13^{42} \cdot 13 &\equiv -1 \cdot 13 \equiv -13 \equiv 72(\text{mod } 85)\\ 13^{43} &\equiv 72(\text{mod } 85).\end{aligned}$$

Logo $D(13) = 72$.

15. $a_{15} = 8$: Como $8^3 = 512$, $512 \equiv 2(\text{mod } 85)$ e $43 = 3 \cdot 14 + 1$, temos

$$\begin{aligned}8^3 &\equiv 2(\text{mod } 85)\\ (8^3)^{14} &\equiv 2^{14} \equiv 16384 \equiv 64(\text{mod } 85)\\ 8^{42} \cdot 8 &\equiv 64 \cdot 8(\text{mod } 85)\\ 8^{43} &\equiv 2(\text{mod } 85).\end{aligned}$$

Logo $D(8) = 2$.

16. $a_{16} = 65$: Como $65^3 = 274625$, $274625 \equiv 75 \equiv -10(\text{mod } 85)$, $10^2 \equiv 100 \equiv 15(\text{mod } 85)$, $15^5 \equiv 759375 \equiv 70(\text{mod } 85)$ e $43 = 3 \cdot 14 + 1$, temos

$$\begin{aligned} 65^3 &\equiv -10(\text{mod } 85) \\ (65^3)^{14} &\equiv (-10)^{14} \equiv (10^2)^7 \equiv 15^7 \equiv 15^5 \cdot 15^2 \equiv 70 \cdot 225 \equiv 70 \cdot 55 \equiv 3850 \equiv 25(\text{mod } 85) \\ 65^{42} \cdot 65 &\equiv 25 \cdot 65 \equiv 1625 \equiv 10(\text{mod } 85) \\ 65^{43} &\equiv 10(\text{mod } 85). \end{aligned}$$

Logo $D(65) = 10$.

17. $a_{17} = 8$: Como $8^3 = 512$, $512 \equiv 2(\text{mod } 85)$ e $43 = 3 \cdot 14 + 1$, temos

$$\begin{aligned} 8^3 &\equiv 2(\text{mod } 85) \\ (8^3)^{14} &\equiv 2^{14} \equiv 16384 \equiv 64(\text{mod } 85) \\ 8^{42} \cdot 8 &\equiv 64 \cdot 8(\text{mod } 85) \\ 8^{43} &\equiv 2(\text{mod } 85). \end{aligned}$$

Logo $D(8) = 2$.

18. $a_{18} = 49$: Como $49^2 = 2401$, $2401 \equiv 21(\text{mod } 85)$, $21^4 \equiv 1(\text{mod } 85)$ e $43 = 2 \cdot 21 + 1$, temos

$$\begin{aligned} 49^2 &\equiv 21(\text{mod } 85) \\ (49^2)^{21} &\equiv 21^{21} \equiv (21^4)^5 \cdot 21 \equiv 1^5 \cdot 21 \equiv 21(\text{mod } 85) \\ 49^{42} \cdot 49 &\equiv 21 \cdot 49 \equiv 1029 \equiv 9(\text{mod } 85) \\ 49^{43} &\equiv 9(\text{mod } 85). \end{aligned}$$

Logo $D(49) = 9$.

Logo, a sequência decodificada será

2-51-81-42-72-71-43-61-31-43-61-51-42-72-2-10-2-9,

reescrevendo a sequência temos

25-18-14-27-27-14-36-13-14-36-15-14-27-22-10-29.

Agora, já podemos fazer a conversão para letras usando a tabela da seção 3.1:

P-I-E-R-R-E–D-E–F-E-R-M-A-T.

Portanto, a mensagem é PIERRE DE FERMAT, assim concluindo a decodificação e o nosso exemplo do método.

Referências

BOYER, C. B. *História da matemática*, 3 ed. - São Paulo: Blucher, 2012.

BURTON, D. M. *Elementary Number Theory*, revised printing, Boston: Allyn and Bacon, 1980.

CARNEIRO, F. J. F. *Criptografia e Teoria dos Números.* Rio de Janeiro: Editora Ciência Moderna Ltda., 2017.

COUTINHO, S. C. *Números Inteiros e Criptografia RSA*, Rio de Janeiro: IMPA, 2009.

HEFEZ, A. *Exercícios resolvidos de Aritmética.* 1ª ed. Rio de Janeiro: SBM, 2016.

SANTOS, J. P. O. *Introdução à Teoria do Números.* 3ª ed. Rio de Janeiro: IMPA, 2020.

SILVA, J. C.; GOMES, O. R. *Estruturas Algébricas para Licenciatura: Elementos de Aritmética Superior.* V. 2. São Paulo: Blucher, 2018.

SINGH, S. *O livro dos códigos.* 5ª ed. Rio de Janeiro: Record, 2005.

Construção axiomática do conjunto dos Números Naturais

Sandro Marcos Guzzo - UNIOESTE - Universidade Estadual do Oeste do Paraná

(*Recebido em 13/11/2023. Aceito em 07/12/2023. Publicado em 20/12/2023*)

Resumo: A construção dos conjuntos numéricos é um assunto clássico na matemática, bem como o estudo das propriedades das operações definidas sobre estes conjuntos. Em geral, em um primeiro curso de álgebra e/ou de análise real, comumento oferecido aos alunos dos cursos de graduação em matemática, os estudantes se familiarizam com a construção dos conjuntos dos números inteiros, dos números racionais e dos números reais. Mas a construção dos números naturais, normalmente não é apresentada. Nosso trabalho consiste em definir ou construir o conjunto dos números naturais. Tal construção será feita a partir dos axiomas de Peano. Nosso trabalho é definir um conjunto denotado por $\mathbb{N}$, duas operações (adição e multiplicação), uma relação de ordem, e provar as principais propriedades destas operações e desta relação, neste conjunto.

Palavras-chave: Axiomas de Peano; Conjunto dos números naturais.

1 Introdução

A construção dos conjuntos numéricos $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ é parte da ementa das disciplinas de álgebra e/ou análise real de muitos cursos de graduação em matemática. Assumindo a existência do conjunto dos números naturais, pode-se construir o conjunto dos números inteiros, e verificar que este novo conjunto é um anel de integridade sob as operações de adição e multiplicação nele definidas. De posse do conjunto dos números inteiros pode-se construir o conjunto dos números racionais, e verificar que este novo conjunto é um corpo sob as operações de adição e multiplicação. A abordagem clássica para estas duas construções é o uso de classes de equivalência.

O conjunto dos números reais por sua vez, pode ser construído a partir dos números racionais. Uma das mais tradicionais abordagens é o método dos cortes de Dedekind. Nesta abordagem recomendamos Guidorizzi (2001). Outra abordagem bastante comum é o método das sequências de Cauchy. Nesta abordagem recomendamos Monteiro (1978). Os números reais ainda podem ser construídos diretamente do conjunto dos números inteiros pelo método dos quase-homomorfismos. Nesta abordagem recomendamos Street (1985).

Como mencionado anteriormente, estas construções partem de um ponto em comum que é o conhecimento de um conjunto primitivo, o conunto dos números naturais, o qual deseja-se melhorar a estrutura. O conjunto dos números naturais por sua vez também pode ser "construído".

Este é o objetivo deste trabalho: axiomatizar o conjunto dos números naturais. Pretendemos ainda definir em tal conjunto as operações de adição e multiplicação, bem como uma relação de ordem e demonstrar propriedades importantes envolvendo essas operações e a relação.

Propriedades estas que acabam por embasar a construção dos demais conjuntos numéricos anteriormente citados. O procedimento que adotaremos neste texto é o sugerido por Sah (1967).

2 Construção de $\mathbb{N}$

Começamos nosso trabalho postulando a existência de um conjunto que satisfaz certas propriedades axiomáticas. Tais axiomas são conhecidos como axiomas de Peano.

Postulado 1. Postulamos a existência de um conjunto $\mathcal{P}$, e de uma aplicação $s : \mathcal{P} \to \mathcal{P}$, que satisfazem os seguintes axiomas:

$\mathbf{P_i}$ (axioma da infinidade) A aplicação s é injetiva mas não sobrejetiva.

$\mathbf{P_{ii}}$ (axioma da indução) Se $S \subset \mathcal{P}$ com $S \not\subset s(\mathcal{P})$ e $s(S) \subset S$, então $S = \mathcal{P}$.

Observe que da não sobrejetividade de s segue que existe (pelo menos) um elemento em $\mathcal{P}$ que não está em $s(\mathcal{P})$. Isto significa que $\mathcal{P} - s(\mathcal{P})$ é não vazio, e portanto o próprio conjunto $\mathcal{P}$ é não vazio. Também, da injetividade de s, temos uma bijeção entre $\mathcal{P}$ e $s(\mathcal{P}) \subsetneq \mathcal{P}$. Levando em conta que não pode haver bijeção entre um conjunto finito e uma parte própria dele, isto acarreta que o conjunto $\mathcal{P}$ é infinito. Daí o fato de o axioma $\mathbf{P_i}$ ser conhecido como axioma da infinidade.

A aplicação s associada a $\mathcal{P}$ é chamada aplicação sucessor, e o elemento $s(x) \in \mathcal{P}$ é dito elemento sucessor do elemento $x \in \mathcal{P}$. Como $\mathcal{P} - s(\mathcal{P})$ é não vazio existe $x \in \mathcal{P}$ de forma que $x \notin s(\mathcal{P})$, isto é, existe uma elemento de $\mathcal{P}$ que não é sucessor de elemento algum de $\mathcal{P}$. Na Proposição que segue, vamos demonstrar que tal elemento é único.

Proposição 1. *O conjunto $\mathcal{P} - s(\mathcal{P})$ possui um único elemento.*

Prova. Seja $e \in \mathcal{P} - s(\mathcal{P})$, isto é, $e \in \mathcal{P}$ e $e \notin s(\mathcal{P})$, e consideremos o conjunto

$$S = \{e\} \cup s(\mathcal{P}).$$

Assim, como $e \in \mathcal{P}$ e $s(\mathcal{P}) \subset \mathcal{P}$, temos que $S \subset \mathcal{P}$. Por outro lado, $S \not\subset s(\mathcal{P})$ já que $e \in S$ e $e \notin s(\mathcal{P})$. Vamos mostrar que $s(S) \subset S$ e, para isto, seja $y = s(x) \in s(S)$ para algum $x \in S$. Como $x \in S$, então $x = e$ ou $x \in s(\mathcal{P})$. Se $x = e$ então $x \in \mathcal{P}$ e $y = s(x) \in s(\mathcal{P}) \subset S$. Por outro lado, se $x \in s(\mathcal{P}) \subset \mathcal{P}$, então também $s(x) \in s(\mathcal{P}) \subset S$. Segue que $s(S) \subset S$ e do axioma $\mathbf{P_{ii}}$ temos $S = \mathcal{P}$, isto é, $\mathcal{P} = \{e\} \cup s(\mathcal{P})$ e portanto existe um único elemento que está em $\mathcal{P}$ e que não está em $s(\mathcal{P})$, o elemento e. □

O elemento e da proposição anterior, será deste ponto em diante chamado de zero de $\mathcal{P}$, e denotado por 0. É o único elemento que não é sucessor de nenhum elemento de $\mathcal{P}$, isto é, o único elemento que pertence ao conjunto $\mathcal{P} - s(\mathcal{P})$.

Os axiomas $\mathbf{P_i}$ e $\mathbf{P_{ii}}$ podem ser substituídos por axiomas alternativos (mas equivalentes), para agora contemplar a existência (e unicidade) do elemento $0 \in \mathcal{P} - s(\mathcal{P})$.

Postulado 2. Postulamos a existência de um conjunto $\mathcal{P}$, com um elemento $0 \in \mathcal{P}$, e uma aplicação $s : \mathcal{P} \to \mathcal{P}$, satisfazendo

$\mathbf{P_1}$) $0 \notin s(\mathcal{P})$.

$\mathbf{P_2}$) s é injetiva.

$\mathbf{P_3}$) Se $S \subset \mathcal{P}$ com $0 \in S$ e $s(S) \subset S$, então $S = \mathcal{P}$.

A Proposição 2 demonstra a equivalência entre os postulados 1 e 2.

Proposição 2. *Os postulados 1 e 2 são equivalentes.*

Prova. Suponha então válidos $\mathbf{P_i}$ e $\mathbf{P_{ii}}$. $\mathbf{P_2}$ é consequência imediata de $\mathbf{P_i}$. A proposição 1 garante $\mathbf{P_1}$. Para mostrar $\mathbf{P_3}$, seja $S \subset \mathcal{P}$ tal que $0 \in S$ e $s(S) \subset S$. Então como $0 \in S$ e $0 \notin s(\mathcal{P})$ então $S \not\subset s(\mathcal{P})$. Então temos $S \subset \mathcal{P}$ com $S \not\subset s(\mathcal{P})$ e $s(S) \subset S$, e do axioma $\mathbf{P_{ii}}$ temos que $S = \mathcal{P}$, o que prova $\mathbf{P_3}$.

Suponha agora $\mathbf{P_1}$, $\mathbf{P_2}$ e $\mathbf{P_3}$ válidos. De $\mathbf{P_2}$, s é injetiva e como $0 \in \mathcal{P}$ com $0 \notin s(\mathcal{P})$ temos que $\mathcal{P} \not\subset s(\mathcal{P})$ donde s não é sobrejetiva, e isto garante $\mathbf{P_i}$. Para mostrar $\mathbf{P_{ii}}$, seja $S \subset \mathcal{P}$ com $S \not\subset s(\mathcal{P})$ e $s(S) \subset S$. Como $S \not\subset s(\mathcal{P})$ então existe $x \in S \subset \mathcal{P}$ com $x \notin s(\mathcal{P})$ e assim, $x \in \mathcal{P} - s(\mathcal{P})$. Mas o único elemento de $\mathcal{P}$ que não está em $s(\mathcal{P})$ é 0, donde $x = 0$. Assim, $S \subset \mathcal{P}$, com $x = 0 \in S$ e $s(S) \subset S$. De $\mathbf{P_3}$ temos que $S = \mathcal{P}$, o que prova $\mathbf{P_{ii}}$. □

Um fato importante é que não são únicos o conjunto $\mathcal{P}$ e a aplicação s, satisfazendo o postulado 2, e consequentemente o postulado 1. Como exemplo citamos os pares de conjuntos $\mathcal{P}$ e aplicações s,

$$\begin{cases} \mathcal{P} = \{0, 2, 4, 6, 8, 10, \dots\} \\ s(n) = n + 2, \quad n \in \mathcal{P}, \end{cases}$$

e também

$$\begin{cases} \mathcal{P} = \{1, 10, 100, 1000, 10000, \dots\} \\ s(n) = 10 \cdot n, \quad n \in \mathcal{P}. \end{cases}$$

Claro que estes exemplos são apenas sugestivos pois ainda não definimos a adição de números naturais, usada na definição de s no primeiro exemplo, e nem a multiplicação usada na definição de s no segundo exemplo. Observe que, no segundo exemplo, $0 \notin \mathcal{P}$ mas isto não é um problema, porque por nossa convenção, 0 é o elemento que não é sucessor de ninguém. Neste caso, este elemento ainda existe porém é o elemento 1.

Dentre todos os conjuntos e aplicações que satisfazem os axiomas de Peano, escolhemos um destes conjuntos e uma destas aplicações e deste ponto em diante os citaremos como o conjunto dos números naturais $\mathbb{N}$ e a aplicação sucessor s. O conjunto $\mathbb{N}^* = s(\mathbb{N})$ é chamado de conjunto dos números naturais positivos. O número 0 é o (único) número natural que satisfaz $0 \in \mathbb{N} - s(\mathbb{N})$.

3 Adição em $\mathbb{N}$ e suas propriedades

Vamos agora dotar este conjunto de uma operação, que chamaremos de adição em $\mathbb{N}$, e provar algumas de suas importantes propriedades. Como $\mathbb{N} = \{0\} \cup s(\mathbb{N})$ então vamos definir a adição sobre $\mathbb{N}$ definindo indutivamente, primeiro sobre $\{0\}$ e depois sobre elementos de $s(\mathbb{N})$.

Definição 3. A adição em $\mathbb{N}$ é a operação $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, sendo que escrevemos $m + n$ para designar $+(m, n)$, que satisfaz

$i)$ $0 + n = n$,

$ii)$ $s(m) + n = s(m + n)$

para todos $m, n \in \mathbb{N}$.

O elemento $m+n = +(m, n) \in \mathbb{N}$ é chamado de soma de m com n. Nos resultados que se seguem, mostraremos que, embora $\mathbb{N}$ não seja um grupo, a adição possui elemento neutro, é comutativa, associativa e vale a lei do cancelamento.

Teorema 4. *A adição em* $\mathbb{N}$ *admite elemento neutro, isto é, existe* $e \in \mathbb{N}$*, tal que* $e+a = a = a+e$ *para qualquer* $a \in \mathbb{N}$*.*

Prova. O elemento neutro x da adição, se existir deve ser único, e deve satisfazer $x+a = a = a+x$ para qualquer $a \in \mathbb{N}$. Desta forma, o item (i) da definição da adição, nos diz que se algum elemento neutro existir, este elemento deve ser 0. Vamos então mostrar que 0 satisfaz as duas igualdades.

Claramente o próprio item (i) da definição da adição garante que $0 + a = a$, para todo $a \in \mathbb{N}$, e então vamos mostrar a segunda igualdade. Seja $S = \{m \in \mathbb{N}; \quad m = m + 0\}$.

Naturalmente $S \subset \mathbb{N}$ com $0 \in S$. Seja agora $y = s(x) \in s(S)$ para algum $x \in S$. Como $x \in S$, temos $x = x + 0$ e disto decorre que $y + 0 = s(x) + 0 = s(x + 0) = s(x) = y$, donde $y \in S$ também. Assim $s(S) \subset S$, e do axioma $\mathbf{P_3}$ segue que $S = \mathbb{N}$. Logo, $0 + m = m = m + 0$ para todo $m \in \mathbb{N}$, e então 0 é o elemento neutro da adição em $\mathbb{N}$. □

Observe que tradicionalmente seríamos levados a provar primeiro a comutatividade da adição para não precisar provar as duas igualdades no teorema anterior. Entretanto como veremos adiante, para provar a comutatividade da adição, precisaremos da existência do elemento neutro bem como da associatividade da adição.

Teorema 5. *A adição em* $\mathbb{N}$ *é associativa, isto é,* $(x + y) + z = x + (y + z)$*, para quaisquer* $x, y, z \in \mathbb{N}$*.*

Prova. Seja $S = \{m \in \mathbb{N}; \quad m + (a + b) = (m + a) + b \quad \text{para todos} \quad a, b \in \mathbb{N}\}$. Temos que $S \subset \mathbb{N}$ e $0 \in S$ já que $0 + (a + b) = a + b = (0 + a) + b$ para quaisquer $a, b \in \mathbb{N}$. Seja agora $y = s(x) \in s(S)$ para algum $x \in S$. Então para quaisquer $a, b \in \mathbb{N}$ temos $x+(a+b) = (x+a)+b$ e também

$$y + (a + b) = s(x) + (a + b) = s(x + (a + b))$$

$$= s((x+a)+b) = s(x+a)+b = (s(x)+a)+b = (y+a)+b.$$

Segue que $y \in S$, o que mostra que $s(S) \subset S$. Do axioma $\mathbf{P_3}$ temos que $S = \mathbb{N}$ e portanto todo $m \in \mathbb{N}$ satisfaz $m+(a+b) = (m+a)+b$ para quaisquer $a, b \in \mathbb{N}$. Fica mostrada a associatividade da adição. □

Sendo válida a associatividade da adição em $\mathbb{N}$, a partir de agora escreveremos simplesmente $m+a+b$, para indicar $m+(a+b)$ ou $(m+a)+b$.

Lema 6. *Para qualquer $n \in \mathbb{N}$ tem-se $s(n) = n + s(0)$.*

Prova. Seja $S = \{n \in \mathbb{N}; \quad s(n) = n + s(0)\}$. Então $S \subset \mathbb{N}$ e, como $0 + s(0) = s(0)$, temos $0 \in S$. Dado agora $y = s(x) \in s(S)$, para $x \in S$, temos que $s(x) = x + s(0)$, e disto obtemos

$$s(y) = s(s(x)) = s(x + s(0)) = s(x) + s(0) = y + s(0),$$

e assim, $y = s(x) \in S$, donde $s(S) \subset S$. Segue de $\mathbf{P_3}$ que $S = \mathbb{N}$, e portanto $s(n) = n + s(0)$ para qualquer $n \in \mathbb{N}$. □

Teorema 7. *A adição em $\mathbb{N}$ é comutativa, isto é, $m + n = n + m$ para quaisquer $m, n \in \mathbb{N}$.*

Prova. Seja $S = \{m \in \mathbb{N}; \quad m + a = a + m \quad \text{para todo} \quad a \in \mathbb{N}\}$. Claramente $S \subset \mathbb{N}$ e pelo Teorema 4 temos $0 \in S$. Dado $y = s(x) \in s(S)$ para algum $x \in S$, então $x + a = a + x$ para todo $a \in \mathbb{N}$, e usando o lema 6, temos

$$\begin{aligned} y + a &= s(x) + a = s(x + a) \\ &= s(a + x) = s(a) + x \\ &= a + s(0) + x = a + s(0 + x) = a + s(x) = a + y. \end{aligned}$$

Então $y \in S$, o que mostra que $s(S) \subset S$ e pelo axioma $\mathbf{P_3}$ temos que $S = \mathbb{N}$. Portanto a adição é comutativa em $\mathbb{N}$. □

Mostraremos agora a validade da lei do cancelamento para a adição em $\mathbb{N}$.

Teorema 8. *Para quaisquer $x, y, m \in \mathbb{N}$, se $x + m = y + m$ então $x = y$.*

Prova. Consideremos o conjunto

$$S = \{m \in \mathbb{N}; \quad a + m = b + m \quad \Rightarrow \quad a = b, \quad \text{para quaisquer} \quad a, b \in \mathbb{N}\}.$$

Temos $S \subset \mathbb{N}$ com $0 \in S$ já que, se $a + 0 = b + 0$ então $a = b$ para quaisquer $a, b \in \mathbb{N}$. Agora, tomemos $y = s(x) \in s(S)$ para $x \in S$. Queremos mostrar que $y = s(x) \in S$ e para isto suponhamos que $a + s(x) = b + s(x)$ para $a, b \in \mathbb{N}$ arbitrários. Então disto decorre que

$$s(x + a) = s(x) + a = a + s(x) = b + s(x) = s(x) + b = s(x + b).$$

Da injetividade de s segue que $x + a = x + b$ e como $x \in S$ então segue que $a = b$. Desta forma $y = s(x) \in S$, e do axioma $\mathbf{P_3}$ temos que $S = \mathbb{N}$, o que significa que para qualquer $m \in \mathbb{N}$, se $a + m = b + m$ então $a = b$, quaisquer que sejam $a, b \in \mathbb{N}$. □

4 Multiplicação em $\mathbb{N}$ e suas propriedades

Definiremos agora uma outra operação em $\mathbb{N}$, que chamaremos de multiplicação, e provaremos algumas de suas propriedades. Novamente, como $\mathbb{N} = \{0\} \cup s(\mathbb{N})$ então definiremos a multiplicação em $\mathbb{N}$ indutivamente, definindo-a primeiro sobre $\{0\}$ e depois sobre os elementos de $s(\mathbb{N})$.

Definição 9. A multiplicação é a operação $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, sendo que escrevemos $m \cdot n$ ou simplesmente mn para indicar $\cdot(m, n)$, que satisfaz

i) $0 \cdot n = 0$,

ii) $s(m) \cdot n = (m \cdot n) + n$

para todos $m, n \in \mathbb{N}$.

O elemento $mn = \cdot(m, n) \in \mathbb{N}$ é chamado de produto de m com n. Para o item (ii) vamos supor, deste ponto em diante, que a multiplicação tem preferência sobre a adição, e então escreveremos simplesmente $mn + n$ em vez de $(mn) + n$.

A multiplicação possui propriedades similares às da adição. Entretanto, as demonstrações destas propriedades para a multiplicação são mais extensas. A multiplicação possui elemento neutro, é comutativa, associativa e vale a lei do cancelamento (com restrições). A prova da existência do elemento neutro precisará de um lema auxiliar.

Lema 10. *Dados $m, n \in \mathbb{N}$, se $mn = 0$, então $m = 0$ ou $n = 0$.*

Prova. Procederemos pela contrapositiva. Suponha que $m \neq 0$ e $n \neq 0$, ou ainda, $m, n \in s(\mathbb{N})$. Existem então $x, y \in \mathbb{N}$ tais que $m = s(x)$ e $n = s(y)$. Assim, das definições de multiplicação e de adição,

$$mn = s(x)s(y) = xs(y) + s(y) = s(y) + xs(y) = s(y + xs(y)),$$

e então, $mn \in s(\mathbb{N})$ o que garante que $mn \neq 0$. □

O próximo Teorema trata da busca por um elemnto neutro $e \in \mathbb{N}$ para a multiplicação. Um elemento que deve satisfazer $en = n = ne$ para todo $n \in \mathbb{N}$. Vamos tecer alguns comentários na tentativa de intuir quem deveria ser este elemento e. Sabemos que $0 \cdot n = 0$, e portanto na procura por um elemento $e \in \mathbb{N}$ que satisfaz $en = n$ para todo $n \in \mathbb{N}$, vemos que e não pode ser o elemento 0. Então $e \in s(\mathbb{N})$, e desta forma $e = s(x)$ para algum $x \in \mathbb{N}$. Sendo assim, x deverá satisfazer $s(x)n = n$, ou ainda $xn + n = n = 0 + n$. Mas pela lei do cancelamento para a adição, x deve satisfazer $xn = 0$ para todo $n \in \mathbb{N}$. Do lema anterior, o único $x \in \mathbb{N}$ que satisfaz essa igualdade deve ser $x = 0$, e desta forma $e = s(x) = s(0)$.

Teorema 11. *Existe $e \in \mathbb{N}$ tal que $en = n = ne$ para todos $n \in \mathbb{N}$;*

Prova. Mostraremos que $e = s(0)$ satisfaz as duas igualdades desejadas. De fato, $s(0)n = 0 \cdot n + n = 0 + n = n$ para qualquer $n \in \mathbb{N}$. Agora, para mostrar a segunda igualdade, seja $S = \{m \in \mathbb{N}; \quad ms(0) = m\}$.

Desta forma, $S \subset \mathbb{N}$ e também $0 \in S$, pois $0 \cdot s(0) = 0$. Dado $y = s(x) \in s(S)$, para algum $x \in S$, temos então $xs(0) = x$ e usando também o Lema 6 decorre que,

$$ys(0) = s(x)s(0) = xs(0) + s(0) = x + s(0) = s(x) = y.$$

Então temos que $y \in S$, o que mostra que $s(S) \subset S$ e do Axioma $\mathbf{P_3}$, $S = \mathbb{N}$. Temos assim que $ms(0) = m$ para todo $m \in \mathbb{N}$. □

O elemento $s(0) \in \mathbb{N}$ é então o elemento neutro da multiplicação, e naturalmente este é o elemento sucessor do elemento $0 \in \mathbb{N}$. Chamaremos o elemento $s(0)$ de unidade do conjunto $\mathbb{N}$ e representaremos este elemento de agora em diante por 1. Desta forma, temos $1 = s(0)$ e também $1 \cdot a = a = a \cdot 1$ para qualquer $a \in \mathbb{N}$.

Com a notação $s(0) = 1$ e o Lema 6 temos imediatamente que $s(x) = x + s(0) = x + 1$, para qualquer $x \in \mathbb{N}$. De outra forma, o sucessor de um número natural x é o número natural $x + 1$.

Queremos agora mostrar que a multiplicação é associativa e comutativa. Para provar isto, precisaremos primeiro da distributividade da multiplicação em relação à adição. Esta por sua vez utilizará um lema auxiliar. Este lema refere-se ao produto por 0 pela esquerda. A definição de multiplicação já garante em seu item (i) que $0 \cdot a = 0$ para qualquer $a \in \mathbb{N}$. Mas como ainda não mostramos a comutatividade da multiplicação, precisaremos provar também que $a \cdot 0 = 0$ para todo $a \in \mathbb{N}$.

Lema 12. *Para todo $n \in \mathbb{N}$, temos $n \cdot 0 = 0$.*

Prova. Consideremos o conjunto $S = \{m \in \mathbb{N}; \quad m \cdot 0 = 0\}$.

Temos que $S \subset \mathbb{N}$ e como $0 \cdot 0 = 0$ então $0 \in S$. Também seja $y = s(x) \in s(S)$ para $x \in S$. Então $x \cdot 0 = 0$ e decorre disto que $y \cdot 0 = s(x) \cdot 0 = x \cdot 0 + 0 = 0 + 0 = 0$. Segue que $y \in S$ e que $s(S) \subset S$. Pelo Axioma $\mathbf{P_3}$ temos $S = \mathbb{N}$, donde $m \cdot 0 = 0$ para todo $m \in \mathbb{N}$. □

Teorema 13. *Para quaisquer $x, y, z \in \mathbb{N}$, temos $x(y+z) = xy+xz$ e também $(y+z)x = yx+zx$, isto é, a operação multiplicação é distributiva com relação à operação adição em $\mathbb{N}$.*

Prova. Consideremos o conjunto $S = \{m \in \mathbb{N}; \quad m(a+b) = ma + mb, \quad \text{para todos} \quad a, b \in \mathbb{N}\}$.

Claro que $S \subset \mathbb{N}$ e que $0 \in S$ já que $0 \cdot (a+b) = 0 = 0+0 = 0 \cdot a + 0 \cdot b$ para quaisquer $a, b \in \mathbb{N}$. Agora suponha $y = s(x) \in s(S)$, para $x \in S$. Então $x(a+b) = xa + xb$, e assim temos

$$\begin{aligned} y(a+b) = s(x)(a+b) &= x(a+b) + (a+b) \\ &= xa + xb + a + b \\ &= xa + a + xb + b \\ &= s(x)a + s(x)b = ya + yb. \end{aligned}$$

Segue que $y \in S$ e então $s(S) \subset S$. Do axioma $\mathbf{P_3}$ temos $S = \mathbb{N}$ e a distributividade à esquerda da multiplicação em relação à adição. Para provar a distributividade à direita, consideremos o conjunto $T = \{m \in \mathbb{N}; \quad (a+b)m = am + bm, \quad \text{para todos} \quad a, b \in \mathbb{N}\}$.

Então $T \subset \mathbb{N}$ e usando o Lema 12 temos que $(a+b) \cdot 0 = 0 = 0 + 0 = a \cdot 0 + b \cdot 0$ para quaisquer $a, b \in \mathbb{N}$, e então $0 \in T$. Agora suponha $y = s(x) \in s(T)$ para $x \in T$. Então $(a+b)x = ax + bx$ e usando o fato que $y = s(x) = x + 1$ e a distributividade pela esquerda já provada, temos

$$\begin{aligned}(a+b)y = (a+b)s(x) &= (a+b)(x+1)\\ &= (a+b)x + (a+b) \cdot 1\\ &= ax + bx + (a+b)\\ &= ax + a + bx + b\\ &= ax + a \cdot 1 + bx + b \cdot 1\\ &= a(x+1) + b(x+1) = ay + by.\end{aligned}$$

Temos então que $y \in T$, e por conseguinte $s(T) \subset T$. Do axioma $\mathbf{P_3}$ temos $T = \mathbb{N}$. A multiplicação é portanto distributiva também à direita em relação à adição. □

Teorema 14. *Para quaisquer $x, y, z \in \mathbb{N}$, temos $x(yz) = (xy)z$.*

Prova. Seja $S = \{m \in \mathbb{N}; \quad m(ab) = (ma)b, \quad \text{para todos} \quad a, b \in \mathbb{N}\}$.

Temos que $S \subset \mathbb{N}$ e também $0 \in S$ pois $0 \cdot (ab) = 0 = 0 \cdot b = (0 \cdot a) \cdot b$ para quaisquer $a, b \in \mathbb{N}$. Seja agora $y = s(x) \in s(S)$ com $x \in S$. Então para quaisquer $a, b \in \mathbb{N}$ temos $x(ab) = (xa)b$ e disto temos

$$\begin{aligned}y(ab) = s(x)(ab) &= x(ab) + ab\\ &= (xa)b + ab = (xa + a)b = (s(x)a)b = (ya)b.\end{aligned}$$

Então $y \in S$ e $s(S) \subset S$. Do axioma $\mathbf{P_3}$ temos que $S = \mathbb{N}$ e fica provada a associatividade da multiplicação. □

Teorema 15. *Para quaisquer $m, n \in \mathbb{N}$, temos $mn = nm$.*

Prova. Considerando $S = \{m \in \mathbb{N}; \quad ma = am, \quad \text{para todos} \quad a \in \mathbb{N}\}$, temos $S \subset \mathbb{N}$. Também, usando a definição da multiplicação e o lema 12, temos $a \cdot 0 = 0 = 0 \cdot a$ para todo $a \in \mathbb{N}$, o que garante que $0 \in S$. Suponha agora $y = s(x) \in s(S)$ para $x \in S$. Então para todo $a \in \mathbb{N}$ temos $xa = ax$ e também

$$\begin{aligned}ya = s(x)a &= xa + a\\ &= ax + a \cdot 1 = a(x+1) = as(x) = ay.\end{aligned}$$

Segue que $y \in S$ e então $s(S) \subset S$. O axioma $\mathbf{P_3}$ garante que $S = \mathbb{N}$ e portanto $ma = am$ para todos $a, m \in \mathbb{N}$. □

5 Relação de ordem em $\mathbb{N}$

Conhecida a adição em $\mathbb{N}$ é possível definir em $\mathbb{N}$ uma relação de ordem (total). Definimos em $\mathbb{N}$, a relação $\leq$ dada por,

$$a \leq b, \quad \text{se e somente se,} \quad \text{existe} \quad n \in \mathbb{N} \quad \text{tal que} \quad a + n = b.$$

Observe que na definição da relação $\leq$, usamos a existência de um elemento $n \in \mathbb{N}$. Como $\mathbb{N} = \{0\} \cup s(\mathbb{N})$ então pode ocorrer que $n \in \{0\}$ ou $n \in s(\mathbb{N})$. Mas note que não podemos ter simultaneamente $n \in \{0\}$ e $n \in s(\mathbb{N})$ já que a união $\{0\} \cup s(\mathbb{N})$ é disjunta. Se $n = 0$ então claramente $a = b$. Se por outro lado tivermos $n \in s(\mathbb{N})$ então escrevemos $a < b$. Resumindo,

$$a < b, \quad \text{se e somente se,} \quad \text{existe} \quad n \in s(\mathbb{N}) \quad \text{tal que} \quad a + n = b.$$

Claramente podemos dizer que $a \leq b$, se e somente se, $a = b$ ou $a < b$, sendo que $a = b$ e $a < b$ são condições exclusivas uma da outra. A expressão $b \geq a$ é equivalente a $a \leq b$, e da mesma forma, a expressão $b > a$ é equivalente a $a < b$.

Vamos verificar primeiro que $\leq$ é de fato uma relação de ordem.

Proposição 16. *A relação $\leq$ é uma relação de ordem (parcial) em $\mathbb{N}$.*

Prova. Dado qualquer $a \in \mathbb{N}$, temos $a \leq a$, uma vez que $a + 0 = a$. Desta forma $\leq$ é reflexiva.

Dados $a, b \in \mathbb{N}$ tais que $a \leq b$ e $b \leq a$, então temos que existem $m, n \in \mathbb{N}$, que satisfazem $a + m = b$ e $b + n = a$. Assim, $a + m + n = b + n = a = a + 0$, e da lei do cancelamento em $\mathbb{N}$ (Teorema 8), segue que $m + n = 0$, donde $m + n \notin s(\mathbb{N})$. Vamos mostrar que $m \notin s(\mathbb{N})$. De fato, procedendo contrapositivamente se $m \in s(\mathbb{N})$ então $m = s(x)$ para algum $x \in \mathbb{N}$ e segue que $m + n = s(x) + n = s(x + n) \in s(\mathbb{N})$. Isto prova que $m \notin s(\mathbb{N})$ e como o único elemento de $\mathbb{N}$ que não pertence a $s(\mathbb{N})$ é 0, temos que $m = 0$. Desta forma, $b = a + m = a + 0 = a$, e a relação é anti-simétrica.

Dados agora $a, b, c \in \mathbb{N}$ tais que $a \leq b$ e $b \leq c$, então existem $m, n \in \mathbb{N}$ tais que $a+m = b$ e $b + n = c$. Assim, $a + (m + n) = (a + m) + n = b + n = c$, e então $a \leq c$ já que $(m + n) \in \mathbb{N}$. Temos portanto a transitividade da relação $\leq$. □

Queremos provar agora que esta ordem é total. Para isto usaremos um lema auxiliar.

Lema 17. *Para qualquer $n \in \mathbb{N}$ temos que $n \leq s(n)$.*

Prova. Naturalmente, para qualquer $n \in \mathbb{N}$,

$$n + s(0) = s(0) + n = s(0 + n) = s(n),$$

e como $s(0) \in s(\mathbb{N}) \subset \mathbb{N}$, então $n \leq s(n)$. □

Proposição 18. *A relação de ordem $\leq$ é total em $\mathbb{N}$.*

Prova. Seja $a \in \mathbb{N}$ arbitrário, e considere o conjunto

$$S_a = \{n \in \mathbb{N}; \quad a \leq n \quad \text{ou} \quad n \leq a\}.$$

Então $S_a \subset \mathbb{N}$. Como $0 + a = a$ então $0 \leq a$ e com isto $0 \in S_a$. Mostraremos que $s(S_a) \subset S_a$. Seja $y = s(x) \in s(S_a)$ para algum $x \in S_a$. Desta forma, $x \leq a$ ou $a \leq x$.

Se $a \leq x$, como $x \leq s(x)$ então da transitividade de $\leq$ segue que $a \leq s(x)$ donde $s(x) \in S_a$, isto é, $y \in S_a$.

Se $x \leq a$ então $x + k = a$ para algum $k \in \mathbb{N}$. Se $k = 0$ então não há o que mostrar pois daí $a = x$ e podemos utilizar o caso $a \leq x$. Se $k \neq 0$ então $k \in s(\mathbb{N})$, donde $k = s(m)$ para algum $m \in \mathbb{N}$. Então $s(x) + m = s(x + m) = s(m + x) = s(m) + x = k + x = a$. Segue que $s(x) \leq a$ e então $s(x) \in S_a$, ou ainda, $y \in S_a$.

Em qualquer caso, temos $s(S_a) \subset S_a$. Segue do axioma $\mathbf{P_3}$ que $S_a = \mathbb{N}$. Assim, dados $m, n \in \mathbb{N}$ arbitrários, temos que $m \in S_n$ e da definição de S_n, temos que $m \leq n$ ou $n \leq m$, e o conjunto $\mathbb{N}$ é totalmente ordenado. □

Nestes termos, dados $a, b \in \mathbb{N}$, temos $a \leq b$ ou $b \leq a$. Se considerarmos separadamente a possibilidade $a = b$, temos então a propriedade tricotômica da relação de ordem, isto é, dados $a, b \in \mathbb{N}$, ou $a = b$, ou $a < b$, ou $b < a$.

Neste ponto podemos revisitar o Lema 17, onde provamos que $n \leq s(n)$ para todo $n \in \mathbb{N}$. Como já mencionado anteriormente, $n + 1 = s(n)$ para todo $n \in \mathbb{N}$ e $1 = s(0) \in s(\mathbb{N})$. Segue portanto da definição da relação $<$, que $n < s(n)$ para todo $n \in \mathbb{N}$. Como consequência disso, o conjunto dos números naturais não possui um elemento máximo. De fato, dado qualquer número natural n sempre existe outro número natural (o sucessor de n) maior do que n.

A lei do cancelamento também é válida para a multiplicação, com uma certa restrição, como dito antes. Como sabemos que $0 \cdot x = 0 = 0 \cdot y$ para quaisquer $x, y \in \mathbb{N}$, isto nos diz que $ax = ay$ não pode garantir que $x = y$ no caso em que $a = 0$. Entretanto se $a \neq 0$ então podemos garantir este cancelamento. Este Teorema não pôde ser mencionado na seção anterior pois faz uso da relação de ordem.

Teorema 19. *Para quaisquer $a, x, y \in \mathbb{N}$, se $a \neq 0$ e $ax = ay$, então $x = y$.*

Prova. Supondo $a \neq 0$, então temos que $a \in s(\mathbb{N})$ e $a = s(m)$ para algum $m \in \mathbb{N}$. Sejam também $x, y \in \mathbb{N}$ tais que $ax = ay$. Como a relação de ordem em $\mathbb{N}$ é total, então temos $x \leq y$ ou $y \leq x$. Vamos analisar cada um dos casos.

Se $x \leq y$ então existe $k \in \mathbb{N}$ tal que $x + k = y$. Assim,

$$\begin{aligned} s(m) \cdot x = ax = ay &= a(x + k) \\ &= ax + ak = s(m) \cdot x + s(m) \cdot k. \end{aligned}$$

Da lei do cancelamento para a adição, temos que $s(m) \cdot k = 0$, e do lema 10, temos que obrigatoriamente $k = 0$, uma vez que $s(m) \neq 0$. Sendo assim, $y = x + k = x + 0 = x$.

Analogamente, se $y \leq x$ então existe $l \in \mathbb{N}$ tal que $y + l = x$. Então também

$$s(m) \cdot y = ay = ax = a(y + l) = s(m) \cdot y + s(m) \cdot l,$$

donde segue que $s(m) \cdot l = 0$ e como $s(m) \neq 0$ então $l = 0$. Logo, $x = y + l = y + 0 = y$, e isto encerra esta demonstração. □

Para finalizar esta seção mostraremos agora a compatibilidade das operações de adição e multiplicação para com a relação de ordem em $\mathbb{N}$. Isto significa que dados $a, b \in \mathbb{N}$ arbitrários, se $a \leq b$ então $a + m \leq b + m$, e também $am \leq bm$ para qualquer $m \in \mathbb{N}$.

Teorema 20. *Dados $a, b \in \mathbb{N}$ com $a \leq b$ então, $a + m \leq b + m$ e $am \leq bm$, qualquer que seja $m \in \mathbb{N}$.*

Prova. Sejam então $a, b \in \mathbb{N}$ com $a \leq b$. Então existe $k \in \mathbb{N}$ tal que $a + k = b$. Dado $m \in \mathbb{N}$ arbitrário, usando a comutatividade e a associatividade da adição em $\mathbb{N}$, temos

$$(a + m) + k = (a + k) + m = b + m,$$

o que garante que $a + m \leq b + m$.

Também, usando a distributividade da multiplicação com relação à adição em $\mathbb{N}$, temos

$$am + km = (a + k)m = bm,$$

o que garante que $am \leq bm$ já que $km \in \mathbb{N}$. □

Conclusões

Como prentendido, construímos o conjunto dos números naturais usando os Axiomas de Peano. Definimos a adição, a multiplicação e uma relação de ordem total em $\mathbb{N}$, além de provarmos as principais propriedades das operações de adição e multiplicação e da relação $\leq$.

Embora tenhamos considerado o número natural 0, é importante observar ao leitor, que alguns autores não consideram o número 0 como sendo um número natural. Isso não invalida a nossa construção. Entretanto, para os casos em que não se deseja incluir 0 como número natural, ajustes deste texto devem ser feitos. Neste caso, o número natural que não pertence ao conjunto $s(\mathbb{N})$ deve ser representado por 1. A adição e a multiplicação devem ser redefinidas colocando respectivamente $1 + n = s(n)$ e $1 \cdot n = n$. Cabe observar que neste caso, a adição não terá elemento neutro. O Lema 6 deve ser adaptado para provar que $s(n) = n + 1$ para todo $n \in \mathbb{N}$, e os Teoremas 5, 7 e 8 continuam válidos bastando substituir 0 por 1 nas demonstrações. O Lema 10 fica sem efeito. No Teorema 11 basta colocar diretamente $e = 1$ na demonstração. O Lema 12 deve ser adaptado para provar que $n \cdot 1 = n$ para todo $n \in \mathbb{N}$, e os Teoremas 13, 14 e 15 bastando praticamente substituir 0 por 1.

Referências

Guidorizzi, Hamilton L. *Um curso de cálculo.* Volume 1, 5^a edição, Rio de Janeiro: Livros Técnicos e Científicos, 2001.

Monteiro, L. H. Jacy. *Elementos de Álgebra.* 2^a edição, Rio de Janeiro: Livros Técnicos e Científicos, 1978.

Street, Ross. *An efficient construction of the real numbers.* Gazette of the Australian Mathematical Society **12** (1985) 57–58.

Sah, Chih-Han. *Abstract algebra.* New York: Academic Press, 1967.

Caracterização dos conjuntos compactos da reta real

Edson Carlos Licurgo Santos - Universidade Estadual do Oeste do Paraná - Toledo

(*Recebido em 15/11/2023. Aceito em 29/11/2023. Publicado em 20/12/2023*)

Resumo: Muitas das propriedades e aplicações das funções reais contínuas são obtidas em conjuntos compactos. Nosso objetivo aqui é caracterizar os conjuntos compactos da reta real. Inicialmente faremos uma apresentação dos conceitos topológicos da reta real, entre eles, as definições de conjunto aberto, conjunto fechado e conjunto compacto. O nosso resultado principal apresentará uma equivalência de quatro definições distintas de conjunto compacto da reta real.

Palavras-chave: Conjuntos compactos; Compacidade da reta real.

1 Noções preliminares

Vamos iniciar com algumas noções preliminares que também vão permitir fixar algumas notações. Em alguns casos apresentaremos os conceitos de forma bem sucinta e rápida. Mais detalhes ou mais resultados sobre os temas abordados neste texto podem ser encontrados em Lima (1976) e Figueiredo (1975).

Definição 1. Seja $X \subset \mathbb{R}$. Dizemos que $a \in \mathbb{R}$ é supremo do conjunto X, e escrevemos $a = \sup X$, se
i) $x \leq a$, para todo $x \in X$;
ii) Dado $\varepsilon > 0$, existe $b \in X$ tal que $a - \varepsilon < b$.

Definição 2. Seja $X \subset \mathbb{R}$. Dizemos que $a \in \mathbb{R}$ é ínfimo do conjunto X, e escrevemos $a = \inf X$, se
i) $a \leq x$, para todo $x \in X$;
ii) Dado $\varepsilon > 0$, existe $b \in X$ tal que $b < a + \varepsilon$.

Definição 3. Seja $X \subset \mathbb{R}$. Dizemos que X é enumerável se X é finito ou se existe uma bijeção $f : \mathbb{N} \to X$.

Definição 4. Seja (x_n) uma sequência de números reais. Dizemos que $a \in \mathbb{R}$ é o limite da sequência (x_n), e escrevemos $a = \lim x_n$ se, dado $\varepsilon > 0$ existe $n_0 \in \mathbb{N}$ tal que

$$|x_n - a| < \varepsilon, \quad \text{para todo} \quad n > n_0.$$

Neste caso também dizemos que (x_n) converge para a e escrevemos $x_n \to a$.

2 Conjuntos abertos

Definição 5. Seja $X \subset \mathbb{R}$. Dizemos que x é um ponto interior de X se existe $\varepsilon > 0$ tal que $(a-\varepsilon; a+\varepsilon) \subset X$. O Conjunto dos pontos interiores de X é chamado de interior de X e é denotado por $int(X)$. Dizemos que o conjunto X é aberto se $int(X) = X$.

Podemos observar que $int(X) \subset X$, qualquer que seja $X \subset \mathbb{R}$. Mais ainda, se $int(X) \neq \emptyset$, então X contém um intervalo da reta e portanto X é não-enumerável. Outro resultado útil a respeito do interior de um conjunto é que se $X \subset Y$, então $int(X) \subset int(Y)$.

Exemplo 1. *a*) Os exemplos triviais de conjuntos aberto da reta são $\mathbb{R}$ e $\emptyset$. De fato, $\emptyset$ é aberto pois se não o fosse deveríamos apresentar um elemento no conjunto vazio que não está no seu interior, o que é um absurdo. $\mathbb{R}$ por sua vez, é aberto pois dado qualquer $x \in \mathbb{R}$, temos claramente $(x-\varepsilon, x+\varepsilon) \subset \mathbb{R}$ qualquer que seja $\varepsilon > 0$ dado.

b) Os intervalos abertos são exemplos canônicos de conjuntos abertos da reta real. Consideramos o intervalo aberto (a,b). Dado $x \in (a,b)$, escolhemos $\varepsilon = \min\{x-a, b-x\}$. Logo $(x-\varepsilon, x+\varepsilon) \subset (a,b)$ e $(a,b) \subset int((a,b))$. Portanto (a,b) é um conjunto aberto. Já para o intervalo fechado $[a,b]$, como $(a,b) \subset [a,b]$, então temos que $(a,b) = int((a,b)) \subset int([a,b]) \subset [a,b]$. Podemos ver claramente que $(a-\varepsilon, a+\varepsilon) \not\subset [a,b]$ qualquer que seja $\varepsilon > 0$ e por este motivo $a \notin int([a,b])$. Pelo mesmo motivo $b \notin int([a,b])$. Assim, $int([a,b]) = (a,b)$. De modo análogo podemos mostrar que $int((a,b]) = int([a,b)) = (a,b)$.

c) Temos que $int(\mathbb{Q}) = \emptyset$, pois $\mathbb{Q}$ é enumerável. Também temos que $int(\mathbb{R} - \mathbb{Q}) = \emptyset$, mesmo sendo $\mathbb{R} - \mathbb{Q}$ não-enumerável.

Teorema 6. *a) Se $A_1, A_2, \ldots, A_n$ são conjuntos abertos, então $A = \bigcap_{j=1}^{n} A_j$ é um conjunto aberto.*
b) Se $(A_\lambda)_{\lambda \in L}$ é uma família arbitrária de conjuntos abertos, então $A = \bigcup_{\lambda \in L} A_\lambda$ é um conjunto aberto.

Demonstração. a) Dado $x \in A = \bigcap_{j=1}^{n} A_j$, $x \in A_j$, para todo $j = 1, \ldots, n$, por hipótese, existem $\varepsilon_j > 0$ tais que $(x-\varepsilon_j, x+\varepsilon_j) \subset A_j$. Seja $\varepsilon = \min\{\varepsilon_j; j = 1, \ldots, n\}$. Logo $(x-\varepsilon, x+\varepsilon) \subset (x-\varepsilon_j, x+\varepsilon_j) \subset A_j$, para todo $j = 1, \ldots, n$. Portanto $(x-\varepsilon, x+\varepsilon) \subset A$ e A é aberto.

b) Dado $x \in A = \bigcup_{\lambda \in L} A_\lambda$, então $x \in A_\lambda$ para algum $\lambda \in L$. Logo, como A_λ é aberto, existe $\varepsilon > 0$ tal que $(x-\varepsilon, x+\varepsilon) \subset A_\lambda$. Portanto $(x-\varepsilon, x+\varepsilon) \subset A_\lambda \subset \bigcup_{\lambda \in L} A_\lambda = A$ e A é aberto. □

Exemplo 2. *a*) A interseção infinita, mesmo que enumerável, de conjunto abertos pode não ser um conjunto aberto. De fato, se pomos $A_n = \left(-\frac{1}{n}, \frac{1}{n}\right)$, então cada A_n é um conjunto aberto, mas $\bigcap_{j=1}^{\infty} A_j = \{0\}$, que não é conjunto aberto.

b) Como $int(X)$ pode ser representado como a reunião de todos os conjuntos abertos contidos em X, então $int(X)$ é um conjunto aberto e $int(int(X)) = int(X)$.

Queremos agora caracterizar os subconjuntos abertos de $\mathbb{R}$ em termos de intervalos abertos.

Lema 7. *Seja $(I_\lambda)_{\lambda\in L}$ uma família arbitrária de intervalos abertos, tal que $p \in I_\lambda$, para todo $\lambda \in L$. Então $A = \bigcup_{\lambda\in L} I_\lambda$ é um intervalo aberto.*

Demonstração. Para cada $\lambda \in L$, escrevemos $I_\lambda = (a_\lambda, b_\lambda)$. Pode ocorrer $a_\lambda = -\infty$ ou $b_\lambda = +\infty$, para algum $\lambda \in L$. Como $a_\lambda < p < b_\mu$, temos que $a_\lambda < b_\mu$, para todos $\lambda, \mu \in L$. Sejam $a = \inf\{a_\lambda, \lambda \in L\}$ e $b = \sup\{b_\lambda, \lambda \in L\}$. Pode ocorrer $a = -\infty$ ou $b = +\infty$. Queremos provar que $(a, b) = A = \bigcup_{\lambda\in L} I_\lambda$. Claro que $A \subset (a, b)$. Dado $x \in (a, b)$, pelas definições de supremo e ínfimo, ou pelas propriedades de conjuntos ilimitados, temos que existem $\lambda, \mu \in L$ tais que $a_\lambda < x$ e $x < b_\mu$. Se $x < b_\lambda$, então $x \in I_\lambda \subset A$. Se $x > b_\lambda$, então temos $a_\mu < b_\lambda \leq x$ e $x \in I_\mu \subset A$. Isto conclui a demonstração. □

Teorema 8. *Se $A \subset \mathbb{R}$ é um conjunto aberto, então existe uma única família enumerável de intervalos abertos, dois a dois disjuntos, $(I_j)_{j\in M\subset\mathbb{N}}$ tal que $A = \bigcup_{j\in M} I_j$.*

Demonstração. Para cada $x \in A$, seja I_x a reunião de todos os intervalos abertos contendo x e contidos em A. Pelo lema anterior, I_x é um intervalo aberto. Dados $x, y \in A$, queremos mostrar que $I_x \cap I_y = \emptyset$ ou $I_x = I_y$. Se $z \in I_x \cap I_y$, então $I = I_x \cup I_y$ é um intervalo aberto contendo x e contido em A. Logo $I \subset I_x$ e $I_y \subset I_x$. De modo análogo, $I_x \subset I_y$. Portanto $I_x = I_y$. Podemos afirmar que A é a reunião de intervalos abertos, dois a dois disjuntos.

Vamos mostrar que esta reunião é enumerável. Para cada I_x, com $x \in A$, escolhemos um número racional $r(I_x) \in I_x$. A função $I_x \mapsto r(I_x)$ é injetiva, pois se $I_x \neq I_y$, então $I_x \cap I_y = \emptyset$ e $r(I_x) \neq r(I_y)$. Como o conjunto $\mathbb{Q}$ dos números racionais é enumerável, então a família $(I_x)_{x\in A}$ é enumerável.

Falta provar a unicidade. Vamos supor que $A = \bigcup_m J_m$, onde os intervalos J_m são abertos e dois a dois disjuntos. Escrevemos $J_m = (a_m, b_m)$. Vamos provar que $a_m \notin A$. Para isso, suponha por contradição que $a_m \in A$. Então $a_m \in J_p = (a_p, b_p)$, para algum $J_p \neq J_m$. Seja $b = \min\{b_m, b_p\}$. Logo $(a_m, b) \subset J_m \cap J_p$ contradizendo o fato de que J_m e J_p são dois a dois disjuntos. Segue que $a_m \notin A$ e do mesmo modo mostra-se que $b_m \notin A$. Isto mostra que para todo m e $x \in J_m$, J_m é o maior, no sentido de inclusão, intervalo contendo x e contido em A. Logo $J_m = I_x$, provando a unicidade. □

Corolário 9. *Seja I um intervalo aberto tal que $I = A \cup B$, onde A e B são abertos e disjuntos, então ($A = \emptyset$ e $B = I$) ou ($A = I$ e $B = \emptyset$).*

Demonstração. Basta aplicar a unicidade do teorema aos conjuntos A e B, se ambos são não-vazios. □

3 Conjuntos fechados

Definição 10. Dizemos que um ponto a é aderente ao conjunto X se a é o limite de uma sequência (x_n) de pontos de X. O conjunto dos pontos aderentes ao conjunto X é chamado fecho de X e é denotado $\overline{X}$. Dizemos que X é fechado se $\overline{X} = X$.

Podemos observar que $X \subset \overline{X}$, pois para todo $x \in X$, podemos tomar a sequência constante convergindo para x.

Teorema 11. *São equivalentes:*
i) $a \in \overline{X}$*;*
ii) para todo $\varepsilon > 0$, $(a-\varepsilon, a+\varepsilon) \cap X \neq \emptyset$*;*
iii) Se I *é um intervalo aberto contendo* a*, então* $I \cap X \neq \emptyset$*.*

Demonstração. i) $\Rightarrow$ *ii).* Vamos supor que $a = \lim x_n$, onde $x_n \in X$, para todo $n \in \mathbb{N}$. Dado $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que $x_n \in (a-\varepsilon, a+\varepsilon)$ ($\Leftrightarrow |x_n - a| < \varepsilon$), para todo $n > n_0$. Logo, $x_n \in (a-\varepsilon, a+\varepsilon) \cap X$, para todo $n > n_0$.

ii) $\Rightarrow$ *iii).* Dado um intervalo aberto I contendo a, como I é um conjunto aberto, existe $\varepsilon > 0$ tal que $(a-\varepsilon, a+\varepsilon) \subset I$. Por hipótese $(a-\varepsilon, a+\varepsilon) \cap X \neq \emptyset$. Logo $I \cap X \neq \emptyset$.

iii) $\Rightarrow$ *ii).* É claro.

ii) $\Rightarrow$ *i).* Dado $\varepsilon_n = \frac{1}{n}$, por hipótese, obtemos $x_n \in \left(a - \frac{1}{n}, a + \frac{1}{n}\right) \cap X$. Logo, (x_n) é uma sequência de pontos de X e $\lim x_n = a$. De fato, dado $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que $\frac{1}{n_0} < \varepsilon$. Portanto, se $n > n_0$, $\frac{1}{n} < \frac{1}{n_0} < \varepsilon$ e $x_n \in \left(a - \frac{1}{n}, a + \frac{1}{n}\right) \subset \left(a - \frac{1}{n_0}, a + \frac{1}{n_0}\right) \subset (a-\varepsilon, a+\varepsilon)$, como queríamos. □

Exemplo 3. *a)* Se X é limitado superiormente (resp. inferiormente), então $\sup X \in \overline{X}$ (resp. $\inf X \in \overline{X}$).

b) $\overline{(a,b)} = [a,b]$. De fato, $a = \inf(a,b) \in \overline{(a,b)}$, e dado qualquer $c < a$ tomamos $\varepsilon = (a-c) > 0$ e temos que $(c-\varepsilon, c+\varepsilon) \cap (a,b) = \emptyset$ mostrando que $c \notin \overline{(a,b)}$. De outra forma $\overline{(a,b)}$ não contém nenhum número menor do que a. Da mesma forma $b = \sup(a,b) \in \overline{(a,b)}$, e também, dado qualquer $c > b$, então com $\varepsilon = (c-b) > 0$ temos que $(c-\varepsilon, c+\varepsilon) \cap (a,b) = \emptyset$. Assim, nenhum número maior do que b pode pertencer a $\overline{(a,b)}$.

c) De modo análogo ao item anterior podemos mostrar que $\overline{[a,b]} = \overline{(a,b]} = \overline{[a,b)} = [a,b]$.

d) $\overline{\mathbb{Q}} = \mathbb{R}$.

Podemos observar que existem conjuntos que não são abertos e nem fechados. Por exemplo, $\mathbb{Q}$, $\mathbb{R} - \mathbb{Q}$, $[a,b)$. Por outro lado, os únicos conjuntos que são abertos e fechados são $\mathbb{R}$ e $\emptyset$. Esta é uma conclusão que vamos tirar do próximo Teorema.

Teorema 12. $X \subset \mathbb{R}$ *é fechado se, e somente se, seu complentar* $\mathbb{R} - X$ *é aberto.*

Demonstração. Vamos supor que X é fechado. Dado $x \in \mathbb{R} - X$, então $x \notin X = \overline{X}$. Logo, existe $\varepsilon > 0$ tal que $(x-\varepsilon, x+\varepsilon) \cap X = \emptyset$. Logo $(x-\varepsilon, x+\varepsilon) \subset \mathbb{R} - X$ e $\mathbb{R} - X$ é aberto. Para a recíproca supomos que $\mathbb{R} - X$ é aberto. Se X não é fechado, existe $x \in \overline{X}$, tal que $x \notin X$. Logo $x \in \mathbb{R} - X = int(\mathbb{R} - X)$. Isto significa que existe $\varepsilon > 0$ tal que $(x-\varepsilon, x+\varepsilon) \subset \mathbb{R} - X$. Portanto $(x-\varepsilon, x+\varepsilon) \cap X = \emptyset$ e $x \notin \overline{X}$, o que é uma contradição. □

Corolário 13. *a)* $\emptyset$ *e* $\mathbb{R}$ *são conjuntos fechados;*

b) Se $F_1, F_2, \ldots, F_n$ *são conjuntos fechados, então* $F = \bigcup_{j=1}^{n} F_j$ *é um conjunto fechado;*

c) Se $(F_\lambda)_{\lambda \in L}$ *é uma família de arbitrária de conjuntos fechados, então* $F = \bigcap_{\lambda \in L} F_\lambda$ *é um conjunto fechado.*

Demonstração. a) $\emptyset$ e $\mathbb{R}$ são conjuntos fechados pois seus respectivos complementares $\mathbb{R}$ e $\emptyset$ são conjuntos abertos.

b) Sejam $A_j = \mathbb{R} - F_j$, $1 \leq j \leq n$. Pelo Teorema anterior A_j é uma conjunto aberto, para todo $1 \leq j \leq n$. Logo $A = \bigcap_{j=1}^{n} A_j$ é um conjunto aberto. Portanto

$$\mathbb{R} - A = \mathbb{R} - \bigcap_{j=1}^{n} A_j = \bigcup_{j=1}^{n} (\mathbb{R} - A_j) = \bigcup_{j=1}^{n} F_j = F$$

é fechado.

c) Sejam $A_\lambda = \mathbb{R} - F_\lambda$, $\lambda \in L$. Logo A_λ é aberto e $A = \bigcup_{\lambda \in L} A_\lambda$ é aberto. Portanto

$$\mathbb{R} - A = \mathbb{R} - \bigcup_{\lambda \in L} A_\lambda = \bigcap_{\lambda \in L} (\mathbb{R} - A_\lambda) = \bigcap_{\lambda \in L} F_\lambda = F$$

é fechado. □

Podemos observar que a reunião infinita, mesmo que enumerável, de conjuntos fechados pode não ser um conjunto fechado. Por exemplo, $\mathbb{Q} = \bigcup_{x \in \mathbb{Q}} \{x\}$, $\{x\}$ é um conjunto fechado, para cada $x \in \mathbb{R}$, mas $\overline{\mathbb{Q}} = \mathbb{R}$.

Corolário 14. *Se* $A \subset \mathbb{R}$ *é aberto e fechado, então* $A = \emptyset$ *ou* $A = \mathbb{R}$.

Demonstração. Temos que A e $\mathbb{R} - A$ são abertos. Como $\mathbb{R} = A \cup (\mathbb{R} - A)$, pelo Corolário 9, $A = \emptyset$ ou $A = \mathbb{R}$. □

Teorema 15. *Seja* $X \subset \mathbb{R}$. *Então* $\overline{\overline{X}} = \overline{X}$, *ou seja,* $\overline{X}$ *é um conjunto fechado.*

Demonstração. Vamos mostrar que $\mathbb{R} - \overline{X}$ é um conjunto aberto. Dado $x \in \mathbb{R} - \overline{X}$, então $x \notin \overline{X}$ e existe $\varepsilon > 0$ tal que $(x-\varepsilon, x+\varepsilon) \cap X = \emptyset$. Logo, se $y \in (x-\varepsilon, x+\varepsilon)$, então $y \notin \overline{X}$. Portanto $(x-\varepsilon, x+\varepsilon) \cap \overline{X} = \emptyset$ e $(x-\varepsilon, x+\varepsilon) \subset \mathbb{R} - \overline{X}$, mostrando que $\mathbb{R} - \overline{X}$ é aberto e que $\overline{X}$ é fechado, como queríamos. □

4 Ponto de acumulação

Definição 16. Seja $X \subset \mathbb{R}$. Dizemos que a é um ponto de acumulação de X se, para todo $\varepsilon > 0$ existe $x \in X$ tal que $0 < |x - a| < \varepsilon$. Isto significa que todo intervalo aberto contendo a, contém algum ponto de X, diferente de a. O conjunto dos pontos de acumulação de X é chamado de derivado de X e é denotado X'. Um ponto $a \in X$ que não é ponto de acumulação de X é chamado de ponto isolado.

Teorema 17. *São equivalentes:*
i) $a \in X'$*;*
ii) $a = \lim x_n$*, onde* (x_n) *é uma sequência de pontos de* X*, dois a dois distintos;*
iii) Todo intervalo aberto contendo a*, contém uma infinidade de pontos de* X*.*

Demonstração. i) $\Rightarrow$ *ii).* Dado $\varepsilon_1 = 1$, por hipótese, existe $x_1 \in X$ tal que $0 < |x_1 - a| < \varepsilon_1$. Dado $\varepsilon_2 = \min\{\frac{|x_1 - a|}{2}, \frac{1}{2}\}$, existe $x_2 \in X$ tal que $0 < |x_2 - a| < \varepsilon_2$. Procedendo desta forma obtemos uma sequência (x_n) de pontos de X, dois a dois distintos, tal que $a = \lim x_n$.

ii) $\Rightarrow$ *iii).* Dado um intervalo aberto I contendo a, por hipótese, existe $n_0 \in \mathbb{N}$ tal que se $n > n_0$, então $x_n \in I$. Como a sequência (x_n) é formada por pontos de X, dois a dois distintos, então $Y = \{x_{n_0}, x_{n_0+1}, \dots\}$ é um conjunto infinito contido em I e $Y \subset X$.

iii) $\Rightarrow$ *i).* Dado $\varepsilon > 0$, da hipótese, $(a - \varepsilon, a + \varepsilon)$ contém uma infinidade de pontos de X. Logo, existe $x \in X$, com $x \neq a$ tal que $x \in (a - \varepsilon, a + \varepsilon)$. Portanto $0 < |x - a| < \varepsilon$, como queríamos. □

Exemplo 4. Temos que $\mathbb{Q}' = \mathbb{R}$, $\mathbb{Z}' = \mathbb{N}' = \emptyset$ e $(a, b)' = [a, b]$. Também, se $X = \left\{\frac{1}{n}; n \in \mathbb{N}\right\}$, então $X' = \{0\}$.

Teorema 18. *Seja* $X \subset \mathbb{R}$*. Então* $\overline{X} = X \cup X'$*.*

Demonstração. Claro que, pelas definições dadas, $X \cup X' \subset \overline{X}$. Seja $x \in \overline{X}$, tal que $x \notin X$. Dado $\varepsilon > 0$ temos que $(x - \varepsilon, x + \varepsilon) \cap X \neq \emptyset$. Como $x \notin X$, então existe $y \in (a - \varepsilon, a + \varepsilon) \cap X$, com $y \neq x$, ou seja, $0 < |y - x| < \varepsilon$. Portanto $x \in X'$ e $\overline{X} \subset X \cup X'$. □

5 Conjuntos compactos

Definição 19. Uma cobertura de um conjunto $X \subset \mathbb{R}$ é uma família $(C_\lambda)_{\lambda \in L}$ de subconjuntos de $\mathbb{R}$ tal que $X \subset \bigcup_{\lambda \in L} C_\lambda$. Uma subcobertura é uma subfamília $(C_\lambda)_{\lambda \in L_1}$, $L_1 \subset L$, para a qual ainda vale $X \subset \bigcup_{\lambda \in L_1} C_\lambda$.

Podemos agora enunciar o teorema que vai nos permitir definir conjuntos compactos na reta.

Teorema 20. *As seguintes afirmações sobre* $K \subset \mathbb{R}$ *são equivalentes:*
a) K *é limitado e fechado;*

b) Toda cobertura por abertos de K possui uma subcobertura finita;

c) Todo subconjunto infinito de K possui um ponto de acumulação $a \in K$;

d) Toda sequência de pontos de K possui uma subsequência que converge para algum ponto de K.

Demonstração. *a)* $\Rightarrow$ *b).* Primeiramente vamos supor que $K = [a, b]$. Dada uma cobertura $[a, b] \subset \bigcup_{\lambda \in L} C_\lambda$ de $[a, b]$ por conjuntos abertos, vamos supor que não existe uma subcobertura finita. O ponto médio do intervalo $[a, b]$, $\frac{a+b}{2}$, o divide em dois intervalos de comprimento $\frac{b-a}{2}$. Pelo menos um deles não pode ser coberto por um número finito dos C_λ. Digamos $[a_1, b_1]$. Começando agora com $[a_1, b_1]$ repetimos o processo infinitas vezes e obtemos $[a, b] \supset [a_1, b_1] \supset [a_2, b_2] \supset \cdots$, onde o comprimento de $[a_n, b_n]$ é $\frac{a+b}{2^n}$ e nenhum deles pode ser coberto por um número finito dos C_λ. Afirmamos que existe $c \in [a_n, b_n]$, para todo $n \in \mathbb{N}$. De fato, temos que $a_1 \leq a_2 \leq \cdots \leq \cdots \leq b_2 \leq b_1$. O conjunto $A = \{a_j, \quad j \in \mathbb{N}\}$ é limitado superiormente. Seja $c = \sup A$. Temos que $a_n \leq c$, para todo $n \in \mathbb{N}$. Por outro lado, $c \leq b_n$, para todo $n \in \mathbb{N}$, pois cada b_n é cota superior de A. Logo $c \in [a_n, b_n]$, para todo $n \in \mathbb{N}$. Em particular $c \in [a, b]$. Logo, existe $\lambda \in L$ tal que $c \in C_\lambda$. Seja $m \in \mathbb{N}$ tal que $\frac{a+b}{2^m} < \varepsilon$. Segue que $c \in [a_m, b_m] \subset (c - \varepsilon, c + \varepsilon) \subset C_\lambda$ e $[a_m, b_m]$ pode ser coberto por um único C_λ, o que é uma contradição. No caso geral $K \subset \bigcup_{\lambda \in L} C_\lambda$. Seja $[a, b]$ um intervalo limitado e fechado contendo K. Isto é possível pois K é limitado. Seja $A = \mathbb{R} - K$. Temos que $[a, b] \subset \left(\bigcup_{\lambda \in L} C_\lambda \cup A \right)$ é uma cobertura por aberto de $[a, b]$, pois K é fechado. Pelo que já foi visto, existem $\lambda_1, \lambda_2, \ldots, \lambda_n$ tais que $[a, b] \subset (C_{\lambda_1} \cup C_{\lambda_2} \cup \cdots \cup C_{\lambda_n} \cup A)$. Portanto $K \subset (C_{\lambda_1} \cup C_{\lambda_2} \cup \cdots \cup C_{\lambda_n} \cup A)$ é uma cobertura finita de K.

b) $\Rightarrow$ *c).* Seja $X \subset K$ um conjunto que não possui pontos de acumulação em K. Dado $x \in K$, existe um intervalo aberto I_x, tal que, $I_x \cap X = \{x\}$ se $x \in X$, ou $I_x \cap X = \emptyset$ se $x \notin X$. Logo, $K \subset \bigcup_{x \in K} I_x$. Por hipótese, existem $x_1, x_2, \ldots, x_n$ tais que $K \subset (I_{x_1} \cup I_{x_2} \cup \cdots \cup I_{x_n})$. Em particular $X \subset (I_{x_1} \cup I_{x_2} \cup \cdots \cup I_{x_n})$. Como cada I_{x_j} contém no máximo um elemento de X, então X é finito. Isto prova *c).*

c) $\Rightarrow$ *d).* Seja (x_n) uma sequência de pontos de K. Se o conjunto $X = \{x_j, \quad j \in \mathbb{N}\}$ é finito, então existe $n_0 \in \mathbb{N}$ tal que $x_n = x_{n_0}$, para todo $n > n_0$. Obtemos $(x_{n_0}, x_{n_0+1}, \ldots)$ uma subsequência constante e portanto convergente para $x_{n_0} \in K$. Se X é infinito, então por hipótese, X possui um ponto de acumulação $a \in K$. Logo, para todo $\varepsilon > 0$, $(a - \varepsilon, a + \varepsilon)$ contém uma infinidade de pontos de X e portanto contém termos x_n de índices arbitrariamente grandes. Dado $\varepsilon = 1$ escolhemos $x_{n_1} \in (a-1, a+1)$. Dado $\varepsilon = \frac{1}{2}$ escolhemos $x_{n_2} \in (a - \frac{1}{2}, a + \frac{1}{2})$ com $n_2 > n_1$. Isto é possível pois $(a - \frac{1}{2}, a + \frac{1}{2})$ contém termos x_n de índices arbitrariamente grandes. Procedendo desta forma obtemos uma subsequêcia (x_{n_i}) que converge para $a \in K$, pois $|x_{n_i} - a| < \frac{1}{i}$ para todo $i \in \mathbb{N}$.

d) $\Rightarrow$ *a).* Se K não é limitado, existem $x_1, x_2 \in K$, com $x_2 > x_1 + 1$. Também existe $x_3 \in K$ tal que $x_3 > x_2 + 1$. Procedendo desta forma obtemos uma sequeência (x_n) que não possui subsequência convergente, pois qualquer subsequência é ilimitada. Se K não é fechado, existe

$x \in \overline{K}$ com $x \notin K$. Logo, existe uma sequência (x_n) de pontos de K tal que $\lim x_n = x$. Toda subsequência desta sequência deve convergir para x e $x \notin K$. Com esta contradição completamos a demonstração. □

Definição 21. Seja $K \subset \mathbb{R}$. Dizemos que K é compacto se for satisfeita uma das condições do Teorema 4.2 sobre K.

No Teorema 20, as implicações $a) \Rightarrow b)$ e $a) \Rightarrow c)$ são conhecidas, respectivamente, por Teorema de Borel-Lebesgue e Teorema de Bolzano-Weierstrass.

Exemplo 5. *a*) Todo conjunto infinito e limitado X possui um ponto de acumulação. De fato, $X \subset [a, b]$ e $[a, b]$ é compacto.

b) O conjunto $X = \{0, 1, \frac{1}{2}, \dots, \frac{1}{n}, \dots\}$ é compacto, pois é limitado e fechado. Por outro lado, $Y = X - \{0\} = \{1, \frac{1}{2}, \dots, \frac{1}{n}, \dots\}$ não é compacto. De fato, se para cada $n \in \mathbb{N}$ pomos $I_n = \left(\frac{1}{n} - \frac{1}{2}\left[\frac{1}{n} - \frac{1}{n+1}\right], \frac{1}{n} + \frac{1}{2}\left[\frac{1}{n} - \frac{1}{n+1}\right]\right)$, então $Y \subset \bigcup_{n\in\mathbb{N}} I_n$ é uma cobertura por aberto de Y que não possui subcobertura finita, pois $I_n \cap Y = \left\{\frac{1}{n}\right\}$.

c) Os conjuntos $\mathbb{R}$, $\mathbb{Q}$ e $\mathbb{R} - \mathbb{Q}$, não são compactos.

d) Um exemplo importante de conjunto compacto não-enumerável é o conjunto de Cantor. Dado o intervalo $[0, 1]$ retiramos deste o seu terço médio aberto $\left(\frac{1}{3}, \frac{2}{3}\right)$. Em seguida, retiramos de $\left[0, \frac{1}{3}\right]$ o seu terço médio aberto $\left(\frac{1}{9}, \frac{2}{9}\right)$ e de $\left[\frac{2}{3}, 1\right]$ o seu terço médio aberto $\left(\frac{7}{9}, \frac{8}{9}\right)$. Ficamos então com $\left[0, \frac{1}{9}\right] \cup \left[\frac{2}{9}, \frac{1}{3}\right] \cup \left[\frac{2}{3}, \frac{7}{9}\right] \cup \left[\frac{8}{9}, 1\right]$. O próximo passo é retirar deses intervalos os seus respectivos terços médios abertos. Repete-se o processo indefinidamente. O conjunto K dos pontos não retirados é o conjunto de Cantor. Se indicamos por $I_1, I_2, \dots$ os intervalos retirados, então $K = [0, 1] - \bigcup_{n=1}^{\infty} I_n = [0, 1] \cap \left(\mathbb{R} - \bigcup_{n=1}^{\infty} I_n\right)$ é fechado e, como é limitado, K é compacto.

Em espaços métricos pode ocorrer de um conjunto X ser limitado e fechado sem que toda cobertura por abertos de X possua subcobertura finita. Consideramos, por Exemplo l^2, o conjunto de todas as sequências $x = (x_1, x_2, \dots)$ de números reais tais que $\sum_{i=1}^{\infty} x_i^2 < \infty$. Dados $x, y \in l^2$, definimos $|x| = \sqrt{\sum_{i=1}^{\infty} x_i^2}$ e a distância $d(x, y)$ como sendo $d(x, y) = |x - y|$. Desta forma, definimos o análogo ao intervalo aberto da reta como sendo $B(x, r) = \{y \in l^2; |y - x| < r\}$, a bola aberta e centro x e raio r. A definição de conjunto aberto é análoga ao caso real, considerando agora as bolas abertas. Seja $X = \{e_1, e_2, \dots\} \subset l^2$, onde $e_i = (0, 0, \dots, 0, 1, 0, \dots)$ (1 na i-ésima posição). Se $m \neq n$, então $|e_m - e_n| = \sqrt{1^2 + (-1)^2} = \sqrt{2}$. Isto significa que X é limitado. Mais ainda, como todos os pontos de X são isolados, então X é fechado. Mas, sendo discreto (sem pontos de acumulação) e infinito, X não é compacto.

6 Considerações finais

Conjuntos compactos constituem uma importante classe de conjuntos na análise real (ou em $\mathbb{R}^n$ ou mesmo na análise funcional). Destacamos por exemplo o Teorema de Weierstrass, que afirma que toda função contínua $f : X \to \mathbb{R}$ definida em um compacto $X \subset \mathbb{R}$, admite ponto de máximo e de mínimo.

Nestes termos, ressaltamos a importância do estudo dos conjuntos compactos. O Teorema 20 reúne quatro modos distintos de afirmar que um subconjunto da reta real é compacto.

Agradecimento

O autor agradece aos revisores pelo apontamento de erros e as correções que proporcionaram a melhoria deste texto.

Referências

Lima, Elon Lages. *Curso de análise, volume I.* Rio de Janeiro, Instituto de Matemática Pura e Aplicada, 1976.

Figueiredo, Djairo Guedes de. *Análise I.* Rio de Janeiro, LTC, 1975.

Créditos

Este volume foi gerado em código LaTeX, editado no TeXstudio[1] versão 4.3.6 (64 bits, Qt 6.5.2 R), e compilado pelo MiKTeX[2] versão 2.9.6000 (32 bit). Para esta edição foram utilizados os seguintes pacotes LaTeX:

This issue was created in LaTeX code, edited on TeXstudio[1] version 4.3.6 (64 bits, Qt 6.5.2 R), and compiled by MiKTeX[2] version 2.9.6000 (32 bit). This issue uses the following LaTeX packages:

`amssymb`	`makeidx`	`float`
`amsfonts`	`babel`	`graphicx`
`amsmath`	`inputenc`	`indentfirst`
`latexsym`	`multicol`	`enumerate`
`amsthm`	`color`	`fancyhdr.`

[1] https://www.texstudio.org/
[2] https://miktex.org/

Índice de autores