Estruturas Algébricas

Valnira Aparecida Alves de Oliveira

INFORMAÇÕES SOBRE O AUTOR

Valnira Aparecida Alves de Oliveira

- Formada em Matemática pela FAFIMAN.
- Mestre em Desenvolvimento da Tecnologia pela UFPR.
- Pedagoga pela Fapan.
- Psicopedagoga pela FAFIMAN.
- Socioterapeuta pela PUC Curitiba.
- Mediadora do PEI (Programa de Enriquecimento Instrumental) pelo Centro Cognitivo do Paraná-Israel.
- Professora de Cálculo I e II, Estatística e Geometria Analítica pela Faculdade Uningá.
- Professora de Métodos Quantitativos Matemáticos, Estatística e Matemática Financeira pela faculdade UNIFCV.
- Professora de Matemática e Psicopedagogia pela Fainsep.

Sobre o Autor

A professora Valnira Aparecida Alves de Oliveira nasceu em Apucarana, Paraná; é casada e possui duas filhas. Mestre em Desenvolvimento da Tecnologia pela UFPR, licenciada em Matemática e Psicopedagogia pela FAFIMAN, com mais de 30 anos de vida acadêmica, sua vida profissional se caracterizou no ensino e dedicação à sala de aula. Professora de Matemática, desde 1989, exerceu docência nos mais diferentes níveis - Alfabetização, Ensino fundamental e médio (Colégio Marista) e Ensino superior. Atualmente, a autora possui um espaço de atendimentos a adolescentes com dificuldades em Matemática, além de lecionar Cálculo I e II, Estatística e Geometria Analítica pelas Faculdades Uningá e FCV.

INTRODUÇÃO DO LIVRO

A experiência adquirida nestes mais de 30 anos de vida acadêmica motivou-me a apresentar um trabalho, cuja ênfase é no aspecto didático. Procurei de modo objetivo organizar um texto, no qual o estudante possa absorver ao máximo todos os conteúdos apresentados.

Um bom livro-texto e um bom professor são certamente uma grande vantagem em um curso de ensino superior, mas o aprendizado depende de você, caro(a) aluno(a). Pensando nisso, o livro-texto foi estruturado em quatro unidades.

Na Unidade 1, apresentam-se dois grandes e importantes assuntos da Matemática, Indução e Boa ordenação. Na parte inicial desta unidade, abordou-se os mais variados tipos de números, bem como a maneira correta de trabalhar-se com eles, além de exemplificar toda a teoria dos conjuntos numéricos. Já na segunda parte, apresentou-se princípios e formas da Indução e Boa ordenação matemática, assim como importantes algoritmos matemáticos, preparando o aluno para a sequência da obra.

A Unidade 2 trata dos Divisores e Múltiplos. No início dela, ensina-se o graduando a como encontrar e trabalhar com o MDC (Máximo Divisor Comum) e o MMC (Mínimo Múltiplo Comum) de diversos números, como também traz algumas aplicações no dia a dia. Já na parte final, o aluno será capaz de compreender e resolver equações diofantinas, sendo essas de extrema importância na matemática, auxiliando-o na resolução de variados problemas.

Na Unidade 3, expõe-se em um primeiro momento o que são Congruências e Anéis, assuntos importantíssimos, que darão suporte ao graduando na construção de um raciocínio sólido e bem estruturado na solução de diversos exercícios. Em sua parte final, trata de Corpos e Ideais, sendo complementos dos primeiros assuntos abordados.

Por fim, a Unidade 4 exibe os dois últimos assuntos: Polinômios e Grupos. Assim, primeiramente, o graduando mergulhará no universo dos polinômios e observará como muitas coisas presentes no cotidiano existem graças a eles. Finalizando a obra, o aluno aprenderá sobre Grupos, suas propriedades e teoremas de extrema importância para a graduação.

UNIDADE I

Indução e Boa Ordenação

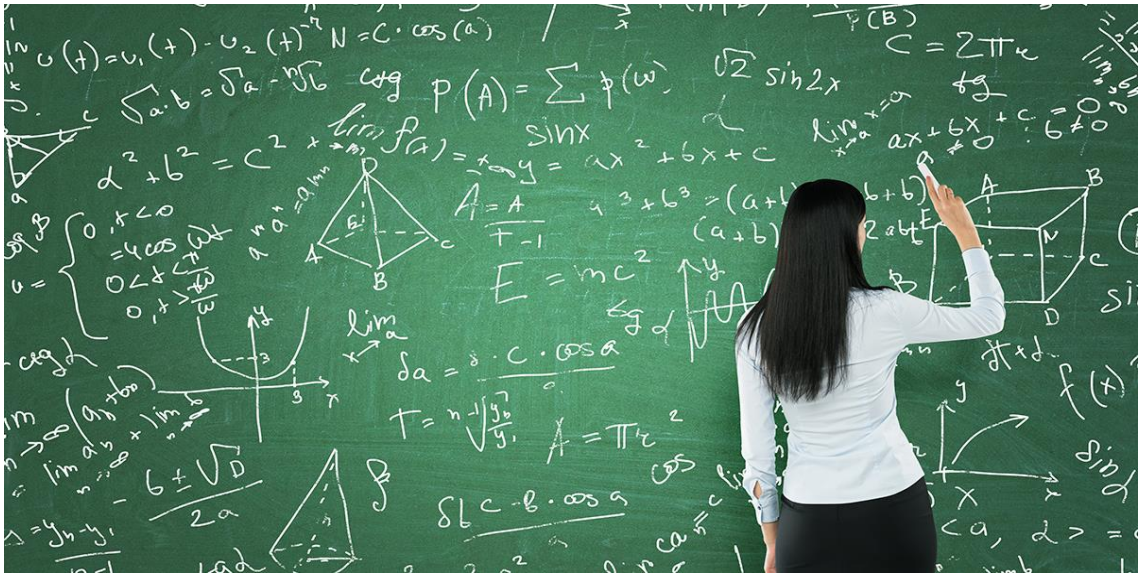
Valnira Oliveira

Introdução

Adquirir o conhecimento da ciência matemática é, para muitos, um processo complicado e traumático, visto que a álgebra é uma das matérias mais temidas pelos alunos, fundamentalmente, para os que frequentam o ensino fundamental, que ao se depararem com fórmulas, contas, e o aprofundamento matemático, se assustam, pois estavam acostumados com uma linguagem numérica diferente e mais figurativa. Para Garcia (2003), esse contato introdutório com a álgebra causa uma grande separação entre a matemática "concreta" da aritmética, e envolve o aluno em uma matemática "abstrata" da álgebra. No processo educacional, as crianças que frequentam as escolas, em sua grande maioria, não estão prontas para essa nova abordagem no estudo da álgebra e os professores não se atentam ao processo de transição de conhecimento e abordagem e acabam, assim, pulando etapas, espalhando os conteúdos e, dessa forma, os alunos não só perdem o interesse pela matemática, como, muitas vezes, ficam assustados, passando a temer pelo resto da caminhada escolar a matéria.

O âmbito algébrico, ou o linguajar matemático, são apresentados inúmeras vezes sem conexão e com ausência de sentido. Como uma ciência, a matemática deve ser compreendida e precisa ser o mais cativante possível para o estudante se apaixonar e a decifrar sem medo, sem ser obrigado a apenas tirar sua nota para passar de ano letivo, mas para carregá-la pela vida e sentir cada experiência prática que a álgebra pode explicar e promover.

O objetivo central deste guia visa exemplificar conceitos aritméticos de forma mais contundente e eficaz no sentido de criar uma relação mais aprofundada e íntima do aluno com os números.



Fonte: Denis Ismagilov / 123RF.

UM POUCO DE HISTÓRIA

Os números estão presentes na história da humanidade desde os tempos mais remotos. Segundo Caraça (1998), existem evidências arqueológicas de que o homem, há 50.000 anos, era capaz de contar.

A humanidade cresceu e se desenvolveu juntamente com a ciência matemática, pois a necessidade do ser humano de contar objetos fez com que as civilizações criassem seus próprios símbolos para a representação dos números e para realizar operações.

Com o passar do tempo, o homem foi sendo desafiado a desenvolver contagens mais complexas, dessa forma, foi se desenvolvendo sistemas numéricos, que podem ser conceituados como métodos de se realizar grandes contagens seguindo uma forma sistematizada.

Essencialmente, estes métodos de contagem se baseavam em definir um determinado algarismo, N, e, a partir dele, atribuir nomes aos seguintes (1,2,3,4..., N). Os números formados nada mais eram do que uma combinação com a base N. Por exemplo, atualmente utilizamos o conjunto numérico decimal (0,1,2,3,4,5,6,7,8,9) sendo que esses algarismos são conhecidos como indo-arábicos. Observa-se que, este sistema de numeração é composto por 10 números. O número 1 representa simplesmente ele mesmo multiplicado por 100 que resulta em uma unidade. Já o número 111 é dado a partir de uma multiplicação de (1X102) +(1X101) + (1X100) = (1X100) + (1X10) + (1X1) = 111.

Dessa forma, cada povo desenvolveu seu próprio sistema de contagem. Os egípcios apresentavam diversos complexos numéricos, entre eles o chamado sistema de base 10. Os babilônios já se firmaram no sistema sexagesimal, de base 60. Os gregos utilizavam um sistema baseado na representação alfabética. Na Índia utilizava-se um sistema muito bem estruturado com figurações para os mais variados dígitos, incluindo o zero.

Com o passar dos anos, o homem desenvolveu equações matemáticas e foi aos poucos percebendo a existência de outros tipos de número. Na Babilônia já existia um algoritmo que realizava o cálculo de raízes quadradas. Os gregos perceberam que a existência dos números irracionais, embora não tenha criado esses “novos números”, criou uma teoria para tentar explicá-los.

Tempos depois, o escocês John Napier inventou os logaritmos, que desenvolveu bastante a compreensão numérica. Assim, com o passar dos séculos, o homem foi descobrindo sua própria personalidade e junto a isso, desvendou a essência dos algarismos até compreendê-los e enxergá-los da maneira que conhecemos em nossa época, favorecendo nossa compreensão numérica.

NÚMEROS RELATIVOS

Números relativos são aqueles que estão acompanhados de um sinal + (mais) ou de - (menos). A única exceção é o zero, pois não é acompanhado de sinal algum, denominado número neutro.

Exemplificando: (+8), (-4), (-100), 0.

REPRESENTAÇÃO GEOMÉTRICA

Toma-se uma reta qualquer orientada em um determinado sentido, no qual denomina-se eixo orientado. Assim, em um ponto aleatório dessa reta, coloca-se o número zero, ponto este que é chamado de origem.

_____|0_____>

A partir do zero no sentido da flecha, coloca-se os números acompanhados do sinal de +, ou seja, os números positivos.

_____|0___|+1__|+2__|+3__|+4___|+5____>

Obs.: Os números que não estão acompanhados com o sinal de mais subentendem-se que são positivos também 8 = +8.

A partir do zero, escreve-se, no sentido oposto da flecha, os números acompanhados do sinal de – (negativos).

_____-4|__-3_|_-2|_-1__|0___|+1__|+2__|+3__|+4___|+5____>

Obs.: Os números sempre crescem no sentido da flecha.

Assim: 1>-12

-9>-20

4<8

Isto é, os números positivos crescem conforme se afastam da origem e os números negativos decrescem conforme se afastam da origem.

MÓDULO OU VALOR ABSOLUTO

Módulo, ou valor absoluto, é o valor do número sem considerar seu sinal.

Exemplo: módulo de +8 é 8 e o módulo de -8 é 8. Geralmente representa-se o módulo através de duas barras.

Exemplificando:

O módulo de -2 representa-se por |-2| = 2.

NÚMEROS SIMÉTRICOS OU OPOSTOS

Números simétricos não são apenas os iguais ou parecidos. Esse conceito se estende também aos que são opostos um do outro, ou seja, são números que em uma reta possuem a mesma distância do ponto zero, o ponto inicial. O aparecimento desses números opostos está ligado de modo direto ao desenvolvimento dos números inteiros. No conjunto dos inteiros, cada elemento positivo também possui um valor correspondente negativo, sendo, portanto, simétricos. Quando são ordenados a partir da reta numérica, os números inteiros são designados da seguinte forma:

Exemplo: +2 e -2 têm o mesmo módulo |+2|=|-2|=2, porém apresentam sinais opostos.

Se quisermos simplificar este conceito, podemos identificar o oposto ou simétrico de qualquer número apenas colocando o sinal de – (negativo) antes do número. Observe os exemplos:

O contrário do número + 24 é dado por: – (+24) → – 24

O contrário do número – 2 é dado por: – (– 2) → + 2

O contrário de – 16 é dado por: – (– 16) → + 16.

O contrário de + 443 é: – (+ 443) → – 443

O contrário de – 25 é: – (–25) → +25

O contrário de + 2320 é: – (+2320) → – 2320

TIPOS DE NÚMEROS

Na matemática existem diferentes grupos representando os diferentes tipos de números que se tem conhecimento, aos quais chamamos de Conjuntos Numéricos. Cada conjunto é como se fosse uma comunidade única de algarismos, que foram, então, separadas de acordo com suas características em comum, conforme listado a seguir:

a) Números Naturais

Os números naturais são aqueles que usamos cotidianamente para realizar contagens. Seu objetivo foi justamente esse. Atualmente, além de realizar contas, utiliza-se esse conjunto de algarismos para compor dígitos, por exemplo, identificar os números do celular de uma pessoa, ou demonstrar o horário em um relógio digital.

Os números naturais são representados pela letra N, como mostrado abaixo:

N = {0,1,2,3,4,5,6,7, ...}

Quando a representação excluir o número zero, então adiciona-se um asterisco (*) e é dada por:

N*= {1,2,3,4,5,6,7...}

b) Números Inteiros

Acrescentando os números negativos aos números naturais, forma-se o conjunto dos inteiros. Sendo, então, todos os naturais positivos e os negativos e o zero.

O conjunto dos números inteiros é representado por:

Z= {..., -2, -1,0,1,2,3...}

Ao excluir o zero deste conjunto, obtém-se:

Z* = {..., -2, -1,1,2,3,4,5...}

c) Números Racionais

Neste conjunto, qualquer algarismo que pode ser descrito no formato de razão do tipo a/b , com a Є (pertence) ao conjunto Z e b Є Z*, fazem parte do conjunto dos números racionais.

Exemplos: $\frac{8}{25}$; $-2 = -\frac{2}{1}$; $0{,}3333 = \frac{1}{3}$

Nota: Q*, assim como nos exemplos anteriores, aparece com o símbolo (*), que denota a ausência do zero.

Q+ é a representação do conjunto dos números racionais não-negativos.

Q- é a representação do conjunto dos números racionais não-positivos.

d) Números Irracionais

Aqueles elementos os quais sua escrita não pode ser feita como divisão entre dois inteiros, pois são infinitos e não periódicos, chamam-se de números irracionais. Este conjunto representa-se pela letra I.

Exemplo: I = {...$\sqrt{2}$, π= 3,141592, ϕ = 1,618033, **e=2,718281,...**}

Todas as raízes não exatas são exemplos de número irracional. No exemplo acima, respectivamente, aparecem: a raiz quadrada de 2, o número Pi, o número de Ouro e o número de Euler.

e) Números Reais

Os números reais são aqueles compostos pela junção dos conjuntos dos números racionais e dos irracionais, sendo que os números naturais, inteiros são subconjuntos dos números reais. A representação dos reais se dá por:

R = {...-10, - π, -2, -1.12, 0, 1,2.45, 5...}

R* é a representação dos números reais com exceção do zero.

R+ representa, evidentemente, todos os reais não-negativos.

R- é a representação dos números reais com não-positivos.

A grosso modo, os números reais são todos aqueles que conhecemos, exceto os números complexos.

RELAÇÕES ENTRE OS CONJUNTOS

Quando se relaciona um elemento qualquer a um conjunto utiliza-se o símbolo de pertence (Є).

Exemplificando:

O número 2 Є R, ou seja, o número 2 faz parte e está inserido no conjunto dos números reais.

Quando se relaciona um conjunto com outro utiliza-se o símbolo de contido (C). Partindo dessa premissa, concluímos que o conjunto dos Racionais (Q) está contido nos números reais (R)

Nota: Os símbolos ⊄ e ∉, significam, respectivamente, não contido e não pertence.

Assim, para termos a dimensão dessas inclusões de um conjunto para o outro, é mostrado conforme a Figura 1.1

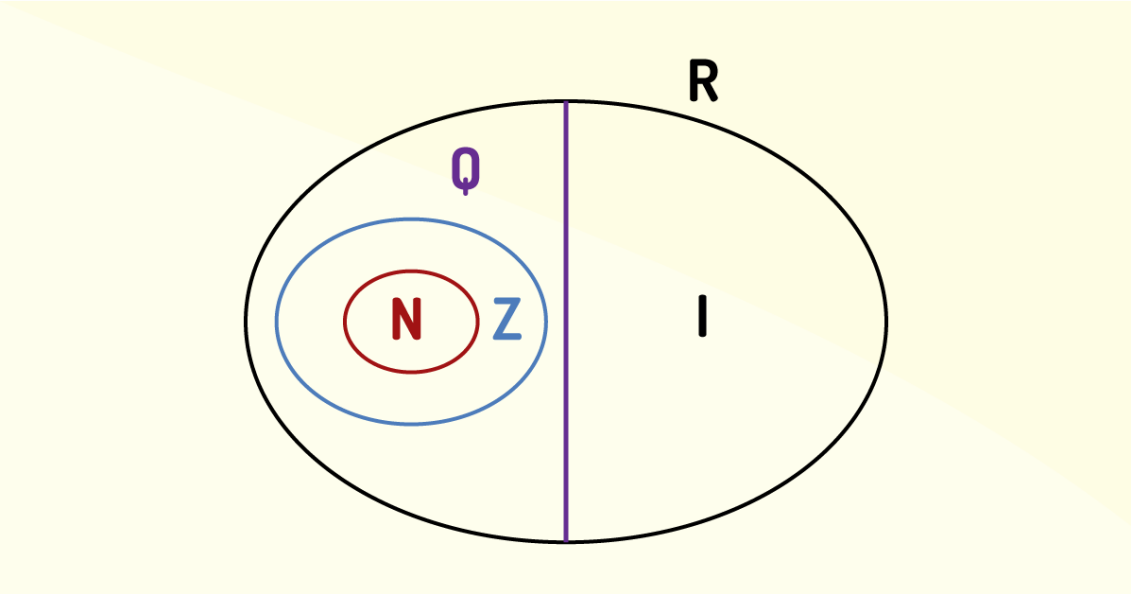


Figura 1.1 – Relação de conjuntos
Fonte: Elaborada pela autora.

Note que ao unir os conjuntos de números racionais e irracionais, o resultado obtido é, na verdade, o conjunto dos números reais.

MÚLTIPLOS

Considerando o conjunto dos números naturais visto anteriormente, sendo ele:

N = {0,1,2,3,4,5,6,7, ...}

Multiplica-se o número 5 por todos os elementos que pertencem aos naturais, como demonstrado abaixo:

5 x 0 = 0

5 x 1 = 5

5 x 2 = 10

5 x 3 = 15

Representemos por M5 o grupo dos números múltiplos de 5.

Assim, M5 = {0,5,10,15,20,25,30...}

Dessa maneira, conclui-se que para se encontrar os múltiplos de um determinado número, basta multiplicá-lo por um conjunto qualquer, seja ele, o conjunto dos números naturais, racionais, irracionais, inteiros, reais ou complexos.

Outros exemplos:

M6 = {0,6,12,18,24, 30...}

M8 = {0,8,16,24, 32,}

Nos exemplos analisados acima, vemos que os múltiplos de um número podem ser infinitos. Também se sabe que o múltiplo de um elemento é o produto deste com um outro número qualquer.

Nota: O zero só tem um múltiplo que é ele mesmo. O zero, portanto, é múltiplo de qualquer número.

Também, qualquer algarismo é múltiplo de 1. Sendo que todos os números são além de tudo, múltiplos deles mesmos.

Observa-se abaixo, um conjunto de elementos múltiplos de 5.

M5 = {0,5,10,15,20,25, ...}

Veja que 20 é múltiplo de 5, logo 5 é divisor de 20.

Quando um número é múltiplo do outro, denomina-se então de divisor do primeiro. Portanto 5 é divisor, submúltiplo ou fator de 20.

Exemplificando: Encontre os divisores de 20:

20 -> 1x 20 = 20

20 -> 2 x 10 = 20

20 -> 4 x 5 = 20

D20 = {1,2,4,5,10,20}

Mais exemplos:

D8 = {1,2,4,8}

D10= {1,2,5,10}

D30= {1,2,3,5,6,10,15,30}

Dos exemplos acima, pode-se observar que o 1 é divisor em comum de qualquer número.

0:1 = 0; 1:1 = 1; 2:1 = 2.

Todo número (diferente de zero) é divisível por si mesmo.

Exemplo: 4:4 = 1; 6:6 = 1; 10:10 = 1.

Nenhum número é divisível por zero.

Exemplo: 2:0 = impossível.

Nota: O conjunto dos divisores de um número é finito.

Veja que:

M6 = {1,2,3,6}

M10 = {1,2,5,10}

Estes dois conjuntos acimas são finitos.

MÚLTIPLOS COMUNS

Se considerarmos um conjunto A, tendo seus elementos os múltiplos de 2, teremos este conjunto representado por:

A = {0,2,4,6,8,10,12,14,16,18,20, ...}

Agora, colocando um conjunto, B, como sendo o conjunto de números múltiplos de 3, teremos:

B = {0,3,6,9,12,15,18,21...}

Colocando estes conjuntos de múltiplos de 2 e 3 acionamos um novo conjunto C.

C = {0,6,12, ...}

Exemplo: Determinemos o conjunto dos múltiplos comuns de 2 e de 5.

A = {0,2,4,6,8,10,12,14,16,18,20...}

B = {0,5,10,15,20,25,30, ...}

C = {0, 10, 20...}

DIVISORES COMUNS

Seja A o grupo algébrico dos divisores de 36, dado por:

A = {1,2,3,4,6,9,12,18, 36}

B sendo o conjunto dos divisores de 54.

B = {1,2,3,6,9,18,27, 54}

C é o conjunto dos divisores comuns de 36 e de 54.

C é o conjunto intersecção de A e B.

Assim, os números que dividem ao mesmo tempo tanto 36 como 54 são:

C = {1,2,3,6,9,18}

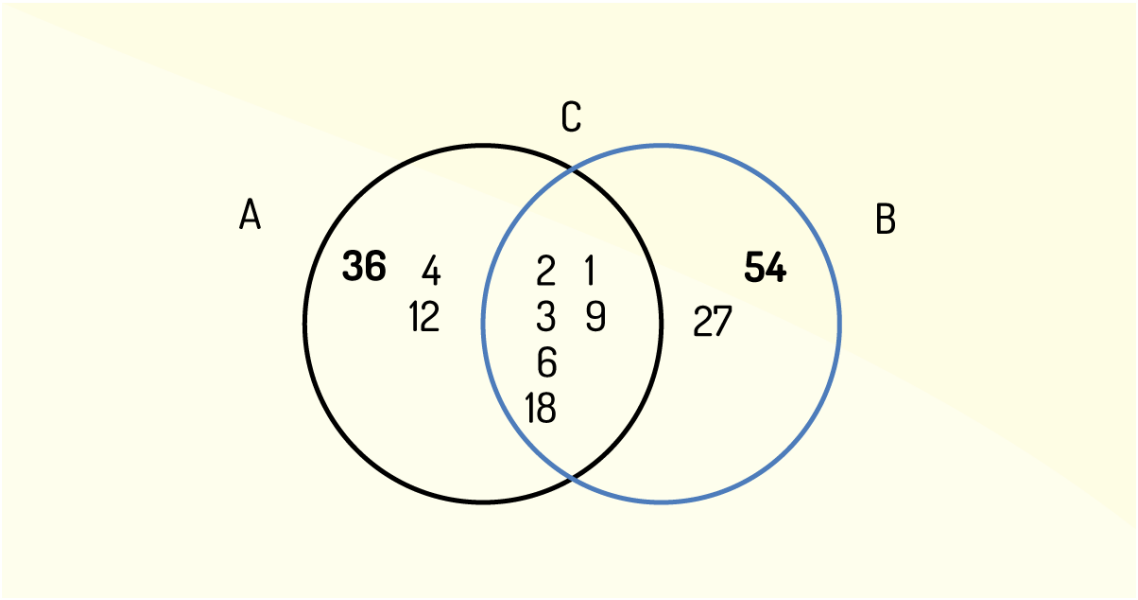


Figura 1.2 – Divisores em Comum

Fonte: Elaborada pela autora.

Nota: Conforme a Figura 1.2 conclui-se que o divisor em comum entre 36 e 54 são {1,2,3,6,9,18}.

ATIVIDADE

1- Um matemático, ao mencionar a Teoria dos Conjuntos, em uma certa turma, realizou uma pesquisa sobre as preferências das pessoas por seleções de vôlei, de seus n alunos, obtido o seguinte resultado:

- 40 alunos admiram o Brasil;
- 40 alunos admiram a Alemanha;
- 20 alunos admiram a França;
- 5 alunos admiram o Brasil e a França;
- 2 alunos admiram a França e a Alemanha.

Se designarmos por A o conjunto dos admiradores do Brasil, por B o conjunto dos admiradores da Alemanha e por C o conjunto dos admiradores da França, todos da referida turma, teremos, evidentemente, $A \cap B = \emptyset$. Concluímos que o número n de alunos dessa turma é:

a) 95.
b) 93.
c) 86.
d) 92.
e) 83

PRINCÍPIO DA INDUÇÃO E DA BOA ORDENAÇÃO

Todos os tipos de estudos ou ciências naturais lidam em seus processos com um procedimento denominado de indução empírica. Essa indução, serve, primordialmente, para a formulação de regras ou leis que apontam fenômenos, baseados em uma quantidade de observações exclusivas, selecionadas atentamente pelos estudiosos. Esse processo não é pelo ponto de vista da lógica o mais correto a ser utilizado, entretanto, seus resultados são altamente satisfatórios. Por exemplo, não há como duvidar do fato de que quando um corpo é solto no vácuo, considerando seu próprio peso, cairá na posição vertical local.

Porém um teorema matemático, para ser válido, deve se estabelecer de modo totalmente diferente. Basicamente se for verificado que certo fato ou afirmação é verdadeiro em uma grande quantidade de casos, no ramo matemático, ainda não seria possível concluir que tal fato é verdadeiro em todos os casos. Por esse motivo, o princípio da indução no âmbito da matemática é definido como uma metodologia de demonstração baseado no princípio da indução finita, que é muito utilizado quando se tem que provar que certos elementos são válidos para todos os números naturais.

Considerando todos os algarismos já criados pelo ser humano até os dias atuais, os números naturais foram os primeiros a serem descobertos, no primeiro momento, com o objetivo principal e único de se contar as coisas, principalmente, elementos da natureza. Mesmo sendo os mais simples, o conjunto dos números naturais não são compreendidos em sua totalidade, existindo ainda um campo de descoberta a ser desvendado.

Visto isso, podemos nos perguntar, afinal de contas, o que realmente são os números naturais representados pelo conjunto N? Por já termos adquirido um conhecimento primário, podemos descrever seus algarismos em forma de números reais, como segue abaixo:

$1, 2 = 1+ 1, 3 = 2+ 1 = (1+ 1) + 1, 4 = 3+ 1 = (1+ 1+ 1) + 1, \cdots$

A grande dificuldade, entretanto, se dá quando temos que provar as propriedades elementares destes números. Nesse ponto, não podemos mais apenas contar com essa descrição simplista, pois apesar de termos consciência de quais são esses algarismos, ainda assim, teríamos grandes problemas em descrevê-los de modo mais abrangente e explícito. Uma saída para tal problema seria dar a esses números propriedades que faça as suas características se tornarem mais inequívocas ao conjunto dos números naturais, isso, já o vendo dentro dos reais. De modo inicial, consideraremos um subconjunto S dos números reais, que possuem as propriedades a seguir:

(1) O conjunto S possui o número 1.

(2) Todas as vezes que S tiver um número n, necessariamente, terá também o número n + 1.

(3) Não existe qualquer subconjunto próprio de S que satisfaça as condições anteriores.

Em suma, podemos explicar as propriedades acima, dizendo que o item (3) coloca o fato de que S possui efetivamente as propriedades anteriores, e se o subconjunto S 0 pertence a S, este último, obrigatoriamente, contém as propriedades (1) e (2), então, S 0 é igual ao S.

Provaremos que, se existe de fato um subconjunto S dos números reais, aos quais satisfaça exatamente as três condições postas acima, então, este conjunto será único. Se S1 e S2 são, na verdade, dois subconjuntos, temos que S1 ∩ S2, contemplam as propriedades (1) e (2), e pela terceira segue que:

$$S1 = S1 \cap S2 = S2$$

Neste estágio inicial ainda não é possível provar que o conjunto S de fato existe. Porém admitamos a existência do seguinte axioma: há um subconjunto dos números reais o qual possui todas as três propriedades listadas. A este subconjunto excepcional, denominaremos de conjunto dos números naturais e será representado pela letra N. A terceira propriedade é o que chamamos de Princípio da Indução matemática, que se define mais precisamente a partir do conceito em que um subconjunto S dos números naturais é dado de tal modo que o número 1 pertence a S e de acordo com as propriedades sempre que o 1 pertencer a S o n+1 também pertencerá, tendo por indução S = N.

A propriedade, então, nos traz um dos mais fortes e poderosos métodos matemáticos, a de demonstração por indução.

Suponhamos que seja apresentada uma sentença matemática chamada de P (n), a qual se necessite de uma variável natural n, podendo ser confirmada ou desmentida dependendo de qual elemento n a substituímos. Estas sentenças serão chamadas de sentenças abertas, definidas apenas sobre os conjuntos dos números naturais. (N).

Abaixo, daremos alguns exemplos sobre as sentenças abertas, todas definidas sobre N:

a) P (n): n é par.

Aqui, obviamente a afirmação P (1) não é verdadeira, já que coloca o número 1 como par. A partir disso, os elementos P (3), P (5) e P (9) também são falsos, já que afirmam que 3, 5 e 9 são números pares também. Entretanto fica evidente que P (2), P (4), P (8) e P (22) são autênticos, pois 2, 4, 8 e 22 são sim pares.

b) P (n) : n é múltiplo de 3.

Nesse item, teremos, por exemplo, P (1), P (2), P (4) e P (5) sendo falsos, em contrapartida P (3) e P (6) são confiáveis, seguindo a mesma lógica do item a).

c) P (n): $1 + 3 + 5 + 7 + \cdots + (2n - 1) = n\,2$.

Agora, os elementos, P (1), P (2), P (3), P (4), . . ., P (10) são autênticos. Define-se aqui de forma precisa o significado do axioma aberto P (n). Ela representa o valor total dos n primeiros números ímpares que são iguais a n 2. Você consegue enxergar algum número natural m de modo que P (m) seja falso? Pois bem, se prosseguirmos a busca e realizarmos algumas outras tentativas, você se certificará de que esta fórmula tem enormes probabilidades de ser correta para todo o conjunto dos números naturais n; ou seja, P (n) é aplicável para todo $n \in N$.

d) P (n): $n\,2 - n + 41$ é um primo, para todo $n \in N$.

De forma simples, é possível verificar que os elementos P (1), P (2), P (3) são autênticos. Se formos prolongar um pouco, com algum trabalho, será possível ir mais adiante, comprovando também que P (4), P (5), . . ., P (35) são igualmente corretas. Portanto é de se considerar que tenhamos encontrado um polinômio os quais seus valores nos números inteiros serão sempre números primos.

Por fim, podemos aplicar mais testes e confirmar as suspeitas? Evidentemente sim. Os elementos P (36), P (37), P (38) e P (40) são legítimos.

Podemos encerrar as hipóteses e finalizar satisfeitos por nossa descoberta? Para aqueles que ainda insistirem em contrariar essa teoria, realizaremos um último teste com a proporção n = 41.

Perceba que $412 - 41 + 41 = 412$ não é primo. Assim, para a nossa decepção, P (41) é ilegítima! Para saber se é possível provar que não há qualquer polinômio em uma variável com coeficientes inteiros cujos valores nos naturais representam sempre algarismos primos, não havia, então, a princípio qualquer probabilidade de P (n) ser autêntico para todo número natural n.

Como justificar, portanto, que um axioma aberto que se define sobre os naturais é sempre legítimo? Primeiramente, você entra de acordo com o fato de ser impossível testar um por um os elementos, ou seja, todos os números naturais, já que são infinitos. Desse modo, será preciso buscar algum método alternativo.

Iremos, abaixo, exibir esse método, demonstrando por indução matemática a forma que resolverá a nossa questão.

Considerando P (n) uma sentença aberta em relação aos naturais e denotado pela letra V o seu conjunto verdade em N, ou seja, um subconjunto de N, que se expressa como:

$V = \{n \in N; P(n) \text{ é verdadeira}\}$.

Para se comprovar que P (n) é legítima para todo caso $n \in N$, é necessário demonstrar que $V = N$. Isso pode ser executado usando o Princípio de Indução Matemática.

Considere, para isto, demonstrar que o número 1 pertence a V e que n + 1 está em V, sempre que n pertence a V. Assim, nós provamos o seguinte teorema, descrito abaixo:

Teorema (Prova por Indução Matemática). Seja P (n) um axioma aberto sobre N. Presuma que:

(i) P (1) é autêntico;

(ii) Independentemente do n ∈ N, todas as vezes que P (n) é legítima, assim seguirá para P (n + 1) também ser legítima.

Portanto P (n) é sim autêntico em todo n ∈ N. Utilizaremos agora, esta estratégia para demonstrar que é válido em todo conjunto natural n, da seguinte expressão:

$1 + 3 + \cdots + (2n - 1) = n\,2.$

Veja que P (1) é legítima, pois a fórmula é corriqueiramente válida para n = 1. Imagine agora que, para qualquer n natural, P (n) seja autêntico. Esperamos provar que P (n+ 1) é legítima. Se somarmos 2n+ 1, sendo ele o elemento ímpar mais próximo depois de 2n−1, nos dois lados da igualdade acima, teremos essa igualdade também aceita:

$1 + 3 + \cdots + (2n - 1) + (2n + 1) = n\,2 + (2n + 1) = (n + 1)2.$

Isso evidencia que, de fato P (n+ 1) é autêntica, sempre que P (n) também for. De acordo com o teorema, essa fórmula é aceita para qualquer algarismo natural n.

Historicamente, essa demonstração realizada foi elaborada pela primeira vez em 1575, de acordo com os registros do estudioso Francesco Maurolycos. Perceba que nesta demonstração, pode-se dar a impressão de que estamos utilizando o argumento de P (n) ser sempre verdadeira para impor e concluir que a expressão P (n + 1) também seja autêntica. Mas na prática, o que realmente está acontecendo? Estamos utilizando essa tese para provar o teorema?

Na verdade, não! Preste bem atenção, pois esse estágio é o mais delicado de todo o teorema. Tendo um número natural n, haverá duas possibilidades:

(a) P (n) é autêntica, ou
(b) P (n) é falsa.

A segunda hipótese do Teorema coloca que não é necessário assumirmos de maneira absoluta que P (n) é autêntico nos casos de n ∈ N, podendo em algumas circunstâncias ser falsa em determinados valores de n, ou quem sabe até, para todos os valores de n. O que esse item está exigindo é que todas as vezes em que n pertença ao item (a) acima, n + 1 também possa se enquadrar a essa mesma categoria; não exigindo nada quando n pertencer à categoria (b).

De forma exemplificada, o axioma aberto P (n): n = n + 1 cumpre (por vacuidade) a segunda hipótese do Teorema, já que nenhum n ∈ N está na categoria (a). O que causa uma imperfeição, no sentido que o Teorema já não nos garanta que P (n) é legítima para todo n, e, portanto, a primeira hipótese não é verificada, já que P (1): 1 = 2 é falsa!

É necessário ter a percepção de que o princípio da Indução Matemática é distinto da indução empírica das ciências naturais, onde se é comum, depois de um razoável número, finito, por necessidade, de testes, já considerar leis gerais que predominaram e reinaram aquele campo de estudo. Tais leis são tomadas como verdades absolutas, até que algum outro estudioso, prove ao contrário. Na aritmética não existe espaço para se lidar com informações verdadeiras até que se prove outra coisa. A Prova por Indução Matemática visa justamente comprovar e estabelecer que aquele determinado axioma aberto, sobre os elementos naturais, será sempre autêntico, em todos os casos, sem haver margem para oposição.

ELEMENTOS DA LÓGICA MATEMÁTICA

Para se ter uma compreensão completa sobre as definições e os teoremas que circundam todas as teorias da aritmética, é preciso, primordialmente, se habituar na utilização de uma linguagem diferenciada, mais rigorosa e técnica em relação a que usamos em nosso cotidiano. Adquirir este costume pode ser tornar mais fácil quando se utiliza os recursos de alguns símbolos e noções da lógica matemática, dos quais falaremos um pouco neste item. Entretanto é importante destacar que a lógica matemática possui atualmente aplicações diversas e de extrema importância nas mais diferentes áreas, sendo uma das principais e com mais destaque, o ramo tecnológico.

TERMOS E PROPOSIÇÕES: LINGUAGEM MATEMÁTICA

A linguagem utilizada na aritmética, assim como qualquer outra, possui suas designações, seus termos próprios e nomes, além, claro, das proposições características dessa área. Essa especificação serve, principalmente, para indicar aspectos matemáticos: algarismos, pontos, funções, conjuntos, operações, figuras geométricas etc. No caso das proposições, é essencialmente usada para determinar se as afirmações são verdadeiras ou não. Para exemplificar essas designações específicas podemos citar a seguinte:

1: 7, 3 + 4, 2 − √ π 7, 2 + 3i, N, R.

Veja que nessas duas primeiras designações, existe um mesmo objeto em comum, ou seja, são equivalentes. Portanto o símbolo que se usa para salientar que as designações a e b são sinônimas é o sinal de igual (=), deste modo, teríamos no linguajar matemático a = b. Em relação às proposições (verdadeira ou falsa) indica-se:

7 = 3 + 4, 4 ≤ 4, 2 + 3i = 3 + 2i, 2 + 1 < 1 + 2.

Sendo uma proposição, precisa ser obrigatoriamente verdadeira ou falsa, porém, jamais uma coisa e outra. Na primeira hipótese, deverá ter um valor lógico de 1 e consequentemente na segunda o valor de 0. Assim, os símbolos (1 e 0) servem para classificar verdade ou falsidade.

No caso de ambas as proposições obtiverem um mesmo valor lógico, serão, então, chamadas de equivalentes:

7 ≤ 0 e (−2)5 = 2 x (-5)

Neste caso, a indicação se dá pelos símbolos p e q. Na linguagem matemática escreve-se p ⇐⇒ q.

Quando temos duas proposições demarcadas, como visto antes pelos símbolos p e q, escrevemos p∧q (ler “p e q”), que serão consideradas verdadeiras ou autênticas quando ambas assim forem, e se tornarão falsas, no caso de pelo menos uma delas ser falsa.

Por exemplo, se considerarmos duas proposições, sendo a primeira “4 é um número par” e a segunda “4 é um divisor de 10”, teremos uma proposição falsa, pois a hipótese número 2 não é verdadeira.

Oposto a isso, temos a disjunção, ou comumente escrita na linguagem matemática p ∨ q, (“p ou q”), que se baseia em constatar o fato de ao menos uma das proposições ser verdade. Nessa regra, p v q só será considerada falsa quando as duas forem falsas, e não apenas uma como no exemplo acima.

Nota: A conjunção e a disjunção podem ser definidas de forma completamente parecidas, caso se tenha mais de duas proposições. Para exemplificar isso, podemos considerar um conjunto de proposições p, q e r. Se afirmarmos que todas são autênticas, ela por completo será verdadeira. Se tornará falsa se uma delas, e apenas uma, também for falsa.

Agora se p é uma proposição, a negação de p, se tornaria uma nova, sendo escrita pelo símbolo ~ p ou simplesmente dizendo não p. Teríamos, então, que a proposição ~ p é autêntica e 2p falsa. Se somarmos ambos os valores lógicos dessas proposições, serão iguais a unidade, portanto se evidencia que toda proposição p, teremos:

$\sim (\sim p) \Longleftrightarrow p.$

De forma mais simples, são verificadas as propriedades a seguir, conhecidas como as primeiras leis de De Morgan, se relacionando às três operações lógicas, representadas pelos símbolos ∨, ∧ e ~:

$\sim (p \wedge q) \Longleftrightarrow (\sim p) \vee (\sim q)$

$\sim (p \vee q) \Longleftrightarrow (\sim p) \wedge (\sim q)$

Podemos descrever essa linguagem dizendo que as proposições p e q estão sendo negadas, ou seja, não são legítimas, o que é similar a dizer que no mínimo uma delas é falsa. Outro ponto importante é a implicação, que se designa pelo símbolo p =⇒ q (que pode ler-se “p implica q” ou “se p, então q”) uma nova proposição que permite dizer, se p é legítima, q também será. Essa implicação p =⇒ q só será, então, falsa, no caso de p ser verdadeira e

q falsa, ou seja, se o valor lógico de p for superior. Como no exemplo das proposições abaixo:

$2 \geq 2 \Longrightarrow 3 > 2 + 1$,

$3 = 2 \Longrightarrow 5 < 0$,

$3 = 2 \Longrightarrow 5 \geq 0$,

$(1000!)2 > 2\ 20000 \Longrightarrow 1000! > 2\ 1000$

Apenas a primeira não é verdadeira. É evidente que quando se analisa essas implicações de forma conjunta $p \Longrightarrow q$ e $q \Longrightarrow p$, as proposições p e q são equivalentes; simbolicamente:

$[\ (p \Longrightarrow q) \wedge (q \Longrightarrow p)\ ] \Longleftrightarrow (p \Longleftrightarrow q)$.

EXPRESSÕES COM VARIÁVEIS

Além desses termos e das proposições que consideramos no tópico anterior, a linguagem matemática utiliza diversas vezes expressões que fazem mediações com variáveis, ou seja, adiciona em seu vocabulário diversos símbolos, a maioria das vezes, letras que podem substituir designações a partir de regras determinadas. Como na expressão abaixo:

$x, (x - y)\ 2\ , x\ 2 - 2xy + y\ 2$

Essas designações se converterão de letras para números reais, isso se forem substituídas de acordo com as regras estabelecidas. Por exemplo, se trocarmos as letras x pelo algarismo 1 e o y por 0, teremos a expressão acima convertida em designação do número 1. Já as expressões que possuírem variáveis, também se transformarão quando as suas figuras e símbolos forem adequadamente substituídos de forma conveniente a elas. Essas chamaremos de expressões designatórias, como a que se segue abaixo:

$\sqrt{}\ x - 1$, cotg x, y x.

É preciso frisar, no entanto, que para as últimas expressões se converterem em números é preciso mais que simples substituições destas variáveis. De forma prática, por exemplo, de nada adiantaria substituir o x pelo 0, já que não iria resultar em nenhum número real, independentemente do valor que fosse posto ao y, portanto duas expressões designatórias que estiverem em uma mesma variável x, serão equivalentes se no caso os valores de todos os x se convertam a uma designação e a partir dela, converta a outra também. Nesse sentido, as expressões x e √3 x 3, por exemplo, são equivalentes, pois uma converte a outra, diferentemente das expressões p |x| e √ x, que se trocarmos o x por −1, por exemplo, a primeira se transformará em uma designação do número 1 e a segunda ficará sendo um símbolo sem significado. Obviamente, essa definição de equivalência é similar no caso de se ter expressões designatórias com mais de uma variável. Assim, torna-se equivalentes as expressões designatórias:

(x − y) 2 e x 2 − 2xy + y 2

Suponhamos que x e y têm em seu domínio o conjunto R. Consideremos agora a seguinte expressão:

x 2 > 0, 2 x = x 2 , x 2 − y 2 = 0, x − y > y − z.

Em ambos os casos, se formos trocar todas as variáveis por designações de números reais, teremos, a partir daí, não mais designações, mas sim proposições e como já visto, terão que ser classificadas em autênticas ou falsas.

Nesse caso, quando podem se tornar proposição, as expressões chamam-se de proposicionais ou de condições. Elas podem também se combinar por meio de operações lógicas, similares ao que consideramos nas proposições. Por exemplo, p (x) e q (x), expressões proposicionais que possuem uma variável apenas. A conjunção p (x) ∧ q (x) se converte para proposição legítima no caso de serem atribuídos valores a x que a torne verdadeira em ambas condições. P (x) e q (x).

Agora, a disjunção p (x) ∨ q (x) é uma condição que será falsa para os valores da variável que tornam p (x) e q (x) ambas falsas.

A negação de p (x) é a condição ~ p (x), que apenas se tornará verdadeira para os valores de x que se converterão p (x) em uma proposição falsa.

Em relação a implicação, p (x) =⇒ q (x), também se converterá em uma proposição falsa, no caso de atribuição a x os valores nos quais p (x) forem verdadeiros e em contrapartida, q (x) falsa. Por fim, a equivalência p (x) ⇐⇒ q (x) é o conjunto das implicações p (x) =⇒ q (x) e q (x) =⇒ p (x).

Abaixo, alguns exemplos de equivalências verdadeiras, independentemente dos valores reais que forem atribuídos às variáveis.

[(x > 3) ∨ (x = 3)] ⇐⇒ x ≥ 3,

[(x < 3) ∧ (x ≥ 2)] ⇐⇒ 2 ≤ x < 3,

~ (x < 1) ⇐⇒ x ≥ 1, x 2 > 0 ⇐⇒ x 6= 0.

Serão, também, verdadeiras em todos os casos:

x < 1 =⇒ x < 3,

[(x < y) ∧ (y < z)] =⇒ x < z,

Se formos supor que x se designa agora a uma variável ao qual o domínio é o conjunto N, dos números naturais, temos:

~ (x é par) ⇐⇒ x é ímpar

x é múltiplo de 6 =⇒ x é múltiplo de 3,

[(x é múltiplo de 2) ∧ (x é múltiplo de 3)] ⇐⇒ (x é múltiplo de 6).

QUANTIFICADORES

Se no caso for dada uma condição p (x), e nela for atribuída a variável x, valores referentes ao seu domínio, teremos como visto, uma conversão para proposição. Contudo em aritmética, tem-se outra forma de extrema relevância para se obter proposições através desta condição p (x). Chama-se quantificadores e são descritos na linguagem própria da matemática pelos símbolos, ∀x ou ∃x.

Essa proposição ∀x p (x) pode ser lida da seguinte forma “qualquer que seja x, p (x) ” ou então “para todo o x, tem-se p (x) ”. Além disso, será verdadeira ao atribuir qualquer valor de x do seu domínio. Já a proposição ∃x p (x), que se lê “existe um x tal que p (x) ” ou “para algum x, tem-se p (x) ”, não é legítima, portanto é falsa, isso também se converter seus valores atribuídos a x, com um valor de seu domínio, da mesma forma que o anterior.

Por exemplo, considerando x uma variável real, são verdadeiras as proposições:

∀x x 2 + 1 > 0, ∃x x 4 ≤ 0 e ∃x x 2 − 3 = 0.

No caso das proposições que tiverem mais de uma variável, o uso de quantificadores torna-se bem similar. Se considerarmos, por exemplo, variáveis x e y a proposição ∀x∃y y < x poderá ser interpretada como “qualquer que seja x existe um y tal que y < x” e se assemelha, a dizer que “não existe um número real que seja menor do que todos os outros”. Obviamente, essa proposição é legítima, mas não seria caso o domínio de x e y fosse o conjunto dos reais ao invés dos naturais. Como não é o caso, então torna-se verdadeira.

A proposição ∃y∀x y < x, que traz à tona a existência de um número real ser menor do que os outros quaisquer é evidentemente falsa. É interessante ressaltar também que, ao trocar a posição dos quantificadores se obterá, a partir daí, uma proposição não equivalente. Entretanto os quantificadores do mesmo tipo inclinarão sempre para uma proposição equivalente, como é fácil de se imaginar a essa altura, como os exemplos abaixo, de proposições equivalentes.

∀x∀y [x 3 = y 3 ⇐⇒ x = y]

∀y∀x [x 3 = y 3 ⇐⇒ x = y]

De forma abreviada, tornam-se:

∀x, y [x 3 = y 3 ⇐⇒ x = y].

Se formos dar duas condições — p (x, y) e q (x, y) por exemplo — diremos que a primeira implicará formalmente a segunda, se é verdadeira a proposição:

$\forall x, y\ p(x, y) \Longrightarrow q(x, y)$

Por exemplo, no conjunto dos reais, x = y 2 implica formalmente x 2 = y 4, mas já a implicação:

x > y =⇒ x 2 > y 2 não é formal.

Veja que na linguagem da aritmética utiliza-se apenas a palavra "implica", no sentido formal, ou até mesmo pode-se utilizar o recurso dos símbolos da forma p (x) =⇒ q (x), em lugar de ∀x p (x) =⇒ q (x). São nada mais do que "abusos de linguagem", ou o popular "gastar vocabulário", onde geralmente não influencia e não traz nenhum inconveniente para o contexto matemático, visto que tanto uma forma como outra, ainda permite reconhecer e identificar os quantificadores.

De forma parecida, dizemos que as condições p (x, y) e q (x, y) são formalmente equivalentes (ou apenas equivalentes) se tiver:

$\forall x, y\ p(x, y) \Longleftrightarrow q(x, y)$,

É importante ressaltar que a implicação formal p (x, y) =⇒ q (x, y) pode também se manifestar dizendo que "p (x, y) é condição suficiente para q (x, y) " ou que "q (x, y) é condição indispensável para p (x, y) ". Já no caso de equivalência formal, é comum também dizer-se que "p (x, y) é condição necessária e suficiente para q (x, y) ".

É de suma e fundamental relevância as seguintes leis, que foram também designadas a partir de De Morgan, que indicam o processo de se negar proposições com quantificadores:

$\sim \forall x\ p(x) \Longleftrightarrow \exists x \sim p(x)$,

$\sim \exists x\ p(x) \Longleftrightarrow \forall x \sim p(x)$.

Para declarar esta última, podemos dizer que “não havendo qualquer valor de x que faça com que p (x) seja verdadeira, todos os valores de x farão essa proposição falsa, e reciprocamente”. Por exemplo:

$\sim \forall x\ x\ 2 > 0 \Longleftrightarrow \exists x\ x\ 2 \leq 0,$

$\sim \forall x,y \exists z\ x = yz \Longleftrightarrow \exists x,y \forall z\ x\ 6= yz$

INDUÇÃO E DEDUÇÃO

O conceito de raciocínio é que tal ação faz o cérebro partir de um estado de premissa, ou suposição, até uma conclusão, uma definição sobre algo. Com esse embasamento podemos argumentar que o raciocínio é um tipo de conhecimento indireto e mediato, isto é, não depende apenas de nós mesmos, e nem de um ou outro fator, mas é intermediado por uma série de questões. Portanto raciocínio é o oposto de intuição.

Raciocinar, ou argumentar, é quando colocamos as informações de modo organizado e as evidenciamos de uma maneira que nos faça chegar a alguma conclusão sobre determinado assunto. Esse processo nos faz ter uma ligação entre aquilo que já conhecemos e aquilo que ainda desconhecemos, que através do raciocínio bem elaborado passaremos a desbravar. Em suma, portanto, são meios de se construir novos conhecimentos, a partir de uma prévia que já existia. Resumidamente, existem dois processos aos quais organizamos nosso modo de pensar e raciocinar que são a dedução e a indução.

a) Deduzir

Deduzir significa alcançar a verdade específica, com base em outra que geralmente é maior e mais abrangente. Deste modo, quando colocamos um fato específico dentro de outro mais generalizado, estamos raciocinando por meio da dedução, como no exemplo a seguir:

1) A é similar a B (fato abrangente, também chamada de premissa maior);
2) existe um X que é semelhante a A (caso particular ou premissa menor);

2) dessa forma, este X será igual a B (conclusão).

Partimos agora para um exemplo que envolva e se aplica no âmbito da matemática:

1) todo algarismo ímpar pode ser escrito como 2n + 1, para qualquer n inteiro;
2) o elemento 325 é um número ímpar;
3) logo, 325 pode ser escrito como 2n + 1, se n for igual a 162.

Ou seja, 2 x 162 + 1 = 325.

b) Induzir

No processo da indução, fazemos o oposto da dedução. Ao induzir, buscamos situações isoladas, particulares e entre elas procuramos algo em comum, algum padrão ou norma geral que possa se aplicar a todos os casos isolados ou parecidos observados, como se segue no exemplo:

1) todos os As vistos são iguais a B (observação de dados ou fatos isolados);
2) portanto todo A é igual a B (indução).

Partimos para uma exemplificação numérica:

1) todo número que apresenta o algarismo das unidades igual a 4 é um número par;
2) portanto 64 é um número par.

c) A indução na matemática

No âmbito das ciências experimentais, induzir é um processo natural, como a biologia e a química. Mesmo não sendo o padrão da matemática, que se compreende muito mais como uma ciência de exatidão, alguns ramos que estão em desenvolvimento baseiam suas respostas por meio do método de indução.

É preciso considerar que, os resultados alcançados sob essa técnica, necessitam ser postos à prova, se deparando com outros critérios mais independentes, já que o processo de indução pode acarretar conclusões erradas, pois obter premissas verdadeiras não significa que as conclusões também serão verdadeiras.

Analisamos dois exemplos:

1) o elemento 64 é par;
2) portanto todo número que tiver dois algarismos será par.

Aqui, a generalização da premissa verdadeira resultou em uma conclusão falsa ou incorreta.

Seguimos para um outro exemplo:

1) A expressão f (n) = n^2- n + 41 produz, para n = 1, um resultado primo (verdadeiro: f (1) = 41);
2) A expressão f (n) = n^2- n + 41 produz, para n = 2, um resultado primo (verdadeiro: f (2) = 43);
3) A expressão f (n) = n^2 - n + 41 produz, para n = 3, um resultado primo (verdadeiro: f (2) = 47);
4) logo, a expressão f (n) = n² - n + 41, nEN, produz números primos.

Analisando esse exemplo, podemos encontrar conclusões autênticas para ≤n ?? 40; entretanto, a expressão, f (41) = ⟦41⟧ ^2- ⟦41⟧ ^ + 41 = ⟦41⟧ ^2, não é primo!

Resumidamente, podemos dizer que o fato de se generalizar as 41 premissas, resultaram em uma conclusão equivocada.

d) Garantia de validade

Esses exemplos trazem à tona um pensamento relevante. Afinal, até que ponto deve-se testar a validade de uma hipótese? Uma outra questão é: como assegurar essa conclusão alcançada?

Há, na verdade, dois métodos para resolver essas questões. A primeira é uma abordagem experimental, onde o cientista buscaria a resolução do problema, na base do experimento em si, e após testar inúmeras possibilidades, descobriria e concluiria que a fórmula fracassa quando chega no n = 41. A questão é que a hipótese poderia cair apenas em um n muito grande, o que levaria muito tempo para descobrir e seria descoberto após muito trabalho, isso ainda considerando a fórmula que poderia ser verdadeira. Após algumas centenas de testes, o cientista concluiria que há inúmeras evidências para que a expressão realmente gere todos os primos superiores a 40. Entretanto jamais teria absoluta certeza de que isto é autêntico, pois poderia existir algum elemento não testado que derrubaria sua tese, afinal, existem infinitos números naturais e só é possível explorar uma pequena parte deles, então, neste método, o pesquisador teria que conviver com o fato de que sua tese poderia ser quebrada a qualquer momento.

Um segundo método é a abordagem matemática, onde o cientista buscará resolver esses problemas a partir de um raciocínio sistemático e lógico, a qual a solução seria única, indiscutível, correta e permaneceria pela eternidade.

Raciocínio dedutivo Raciocínio indutivo

Na dedução, a conclusão apenas explicita eu ratifica o que já havia sido dado a conhecer pelas premissas. A conclusão enuncia uma verdade que ultrapassa o conhecimento dado pelas premissas.

Se todas as premissas são verdadeiras, então as conclusões são verdadeiras. Se todas as premissas são verdadeiras, então a conclusão, provavelmente (mas não necessariamente) será verdadeira.

Quadro 1.1 – Dedução x Indução

Raciocínio Dedutivo	**Raciocínio Indutivo**
Na dedução, a conclusão apenas explicita eu ratifica o que já havia sido dado a conhecer pelas premissas.	A conclusão enuncia uma verdade que ultrapassa o conhecimento dado pelas premissas
Se todas as premissas são verdadeiras, então as conclusões são verdadeiras.	Se todas as premissas são verdadeiras, então a conclusão, provavelmente (mas não necessariamente) será verdadeira.

Fonte: Ângela Maria (2011).

No quadro acima, comparamos as duas formas de raciocínio, apontando duas diferenças relevantes, a respeito das características de cada uma, tanto na forma dedutiva como indutiva. Visualizamos, então, as diferenças básicas destas formas de pensamento, aos quais estamos em constante contato.

AS DUAS FORMAS DE INDUÇÃO

Voltando um pouco, o método da indução finita corresponde a um processo aritmético criado para provar proposições que são autênticas em uma determinada sequência de objetos. Esse conceito é muito usado em áreas da matemática como a teoria dos números, geometria, análise combinatória etc. Entretanto a indução pode também aparecer em qualquer outro ramo da aritmética e por essa razão existem duas formas de se descrever esse princípio.

a) Princípio da Indução Finita - 1ª forma

Consideramos P (n) como um enunciado que descreve uma propriedade sobre um algarismo natural n maior ou igual a um número natural n0 fixado.

Definição (PIF 1ª forma). Caso precisemos provar que as duas condições abaixo são válidas:

C1: P (n0) é autêntica (ou seja, vale a propriedade para n0);

C2: é autêntica a implicação P (n) → P (n + 1) isso para todo n ≥ n0.

Portanto podemos dizer que a propriedade P (n) é verdadeira e autêntica para todo n ≥ n0.

Na prática, para conseguirmos confirmar um teorema por indução finita, precisamos demonstrar que essas duas condições dadas pelo princípio estão sendo satisfeitas. Isso é fundamental, pois é o que vai basear nossa garantia da propriedade em toda a infinidade de casos existentes. Especificamente na segunda condição, como apenas uma única implicação será falsa, se a sua premissa for autêntica e a conclusão falsa, só é preciso eliminar essa possibilidade para termos, então, a validação da implicação que deseja.

Dessa forma, o que se faz comumente é tornar um k qualquer valor maior ou igual a n0, isso admitindo que P (k) seja legítimo, e provar que essencialmente P (k + 1) também precisa ser autêntico. Além de tudo isso, é realizada também a prova de que é válida a propriedade para n0 (primeiro natural), a indução nos garante em todas as afirmações a validação da propriedade.

Exemplificando:

Considerando que 2^4 = 16 e 4! = 4.3.2.1 = 24, logo vale que 2^4 < 4! E dessa maneira, a (C1), primeira condição do P IF, foi alcançada. Assumindo que 2?k = k! (∗) para um k genérico maior do que 4, como:

• 2 k+1 = 2.2 k • (k + 1)! = (k + 1) k! • (k + 1) > 2, se k > 4

A partir da desigualdade (*) teremos:

2 k+1 = 2.2 k < 2.k! < (k + 1). k! = (k + 1)!

Fica, então, consolidada a validação de (C2), a segunda condição do P IF. Desse modo, o princípio da indução finita garante que vale 2? n < n!, para todo n > 4.

b) Princípio da Indução Finita - 2ª forma

Considerando P (n) uma pronúncia que descreve uma propriedade sobre um número natural n maior ou igual a um número natural n0 fixado.

Definição (PIF 2ª forma). Se conseguirmos provar que valem as duas condições abaixo:

CC1: P (n0) é autêntica (ou seja, vale a propriedade para n0);

CC2: para todo $n \geq n0$, é verdadeira a implicação $P(n0) \wedge P(n0 + 1) \wedge ... \wedge P(n - 1) \wedge P(n) \rightarrow P(n + 1)$.

Podemos concluir, a partir dessas condições, que a propriedade P (n) é autêntica para todo $n \geq n0$.

Na execução, para se provar uma propriedade, baseado na segunda forma de indução, é preciso provar que esta propriedade P tenha validade para n0, e em seguida, seja dado um n aleatório superior ao n0 admitindo que P vale para todos os elementos entre o n0 e ele mesmo (n), é preciso provar também que P valerá para n + 1. Ou resumidamente, comprovar a seguinte afirmação:

P (k) verdadeira para $n0 \leq k \leq n \rightarrow$ P (n) verdadeira.

Esta forma pode ser fundamental e essencial em algumas oportunidades, como no Teorema fundamental da Aritmética, que veremos a seguir.

Exemplificando:

O primeiro algarismo é o 2, que é número primo. Como 2 é igual a 2, concluímos que 2 admite uma "fatoração"/ única em primos. E, desse modo (CC1) está satisfeita. Assumimos agora que todos os números entre 2 e n, incluindo eles mesmos, permitem uma fatoração em números primos, única a menos da ordem dos fatores. Consideremos o número n + 1, haverá duas opções:

a) +1 é primo, e nesse caso a sua "fatoração" é certamente única, tendo como único "fator" o próprio primo n + 1, assim como no caso do número 2.

b) n + 1 é composto, ou seja, n + 1 = p.q, onde p e q são números naturais inferiores aos n e superiores ou iguais a 2. Sendo assim, supomos (logo acima), que a também chamada de hipótese de indução, tanto p como q admitem decomposição em fatores primos. Multiplicando todos os fatores de p pelos fatores de q obviamente obtemos o número n + 1.

Já que as fatorações de p e q são exclusivas a menos da ordem dos fatores, é preciso ainda provar que, no caso de haver outro elementos primos que realizassem a fatoração encontrada, teríamos também fatorações diversas para p e q, o que é impossível por hipótese.

PRINCÍPIO DA BOA ORDEM

Existem na matemática clássica alguns axiomas que consideram objetos que não podem ser desenvolvidos, nem como algoritmo finito, nem infinito. Podemos ver isso como um lado mais abstrato da aritmética, mas de toda forma, essa abstração toda não traz muitas consequências produtivas ao desenvolvimento matemático. Não se tem nenhum relato de existência de algum resultado verdadeiramente prático e relevante, decorrente dessas práticas e teorias que envolvem o abstrato. A matemática construtiva, portanto, não faz parte e não contribui para esse método.

Um dos exemplos mais clássicos que se tem desse modo de enxergar a aritmética é o princípio da Boa ordem. Juntamente com outros exemplos, esses princípios podem ser nomeados de teoremas sem serem admitidos também como axiomas. Se fossem axiomas, passariam a reger o que é e o que não é uma verdade absoluta e exata, o que complicaria muito a matemática.

Em suma, o Princípio da Boa ordem, diz que todo conjunto aritmético pode ser bem ordenado, ou seja, cada conjunto x, por exemplo, possui uma relação de ordem, representado por R (pode-se pensar na relação de ordem <= da aritmética dos números inteiros, como exemplo) de modo que (X, R) é completamente ordenado (i.e., para todos x, y em X, xRy ou yRx) e todo subconjunto Y de X contém um elemento minimizante b (i.e., bRx para todo elemento x de Y).

Podemos ver isso na prática, se colocarmos, por exemplo, o conjunto dos números naturais N= {0,1,2,3, …}. Ele é extremamente bem ordenado pela relação de ordem <=, menor ou igual. O conjunto N é limitado inferiormente, então todo subconjunto de N terá elemento mínimo, que é, então, um elemento minimizante.

Em conjuntos com cardinalidade elevada, é interessante observar como se concentra a relação de ordem. Em alguns casos, pode acontecer de não existir algoritmo ou algarismo finito ou não para estabelecer essa relação ordenada, além disso se considerarmos conjuntos dos números inteiros Z, com cardinalidade alefe 0, e o operador P, construía-se o conjunto P (Z) com cardinalidade alefe um, o conjunto P (P (Z)) com cardinalidade alefe dois, o conjunto P (P (… (P (Z)) …), n vezes, com cardinalidade alefe n, e assim sucessivamente.

PRINCÍPIO DO MENOR INTEIRO

Consideramos S um subconjunto de N, podemos afirmar que um número natural a é o elemento mais inferior de S, isso no caso de possuírem as propriedades que seguem: i) $a \in S$, ii) $a \leq n$, para todo $n \in S$. Logo de cara, verificamos que se o conjunto S possui um elemento menor, se torna único. Concluímos isso, pela lógica em que se o elemento a e a0 são os menores de S, então, $a \leq a\ 0$, ou seja, $a = a0$. Essa denotação quando ocorre é dada por minS. Essa informação é importante, pois nem sempre é fácil provar aquilo que é óbvio, muitas vezes, quando afirmamos isso, dá-se a impressão de que qualquer um poderia resolver sem grande esforço.

Mas iremos agora, de forma efetiva, mostrar o que parece óbvio, isto é, todo subconjunto não vazio N, possui um elemento menor.

Exemplificando:

Considere S sendo um subconjunto não vazio de N. Imaginemos que este conjunto S não tenha nenhum menor elemento. Demonstraremos que S é vazio, levando a uma contradição. Imagine um conjunto T, que seja um complementar de S em N, isto é, o

conjunto dos naturais pertencentes a S. Queremos demonstrar, portanto, que T = N, ou para se utilizar outra linguagem simbólica S = ∅. Defina o conjunto:

$I_n = \{k \in N; k \leq n\}$, e considere a sentença aberta

P (n): $I_n \subset T$.

Já que $1 \leq n$, para todo $n \in N$, tem-se, portanto, que $1 \in T$, pois, se fosse o oposto, 1 seria um menor elemento de S. Desse modo, P (1) é verdadeira.

Considere agora que P (n) seja autêntico, para qualquer n. Se $n + 1 \in S$, como não há elemento de I_n pertencente a em S, obteríamos n + 1 que é um menor elemento de S, fato, como visto, que não é permitido. Assim, $n + 1 \in T$, onde se segue que $I_{n+1} = I_n \cup \{n + 1\} \subset T$, provando que, para todo n, temos que $I_n \subset T$; portanto, $N \subset T \subset N$ e, consequentemente, T = N.

ATIVIDADE

2 - Tendo em vista o raciocínio dedutivo e suas especificidades na matemática, assinale V para verdadeiro e F para falso, em relação às afirmações a seguir.

I. É uma técnica de raciocínio dedutivo, usada para provar alguma ideia obtida com um raciocínio indutivo.
II. Ao utilizar a indução para provar resultados, podemos assumir que “P(k) é V” para forçar o resultado esperado, tranquilamente.
III. Todo subconjunto não-vazio do conjunto dos inteiros positivos tem um elemento mínimo.
IV. Indução matemática é um método de prova matemática utilizado para demonstrar a verdade de um número finito de proposições.

Está correto o que se afirma em:

a) I apenas.
b) II apenas.
c) I e II apenas.
d) I e III apenas.
e) II, III e IV apenas.

DESCRIÇÃO DO ALGORITMO

No entendimento dos gregos sobre matemática, os algarismos eram magnitudes geométricas. Assim, este termo, para eles, pode ser compreendido como uma sequência finita e ordenada de regras ou passos, em um esquema de processamento, que possibilita a realização de uma determinada função - resolução de problemas, cálculos etc.

Algoritmo, então, é uma palavra latinizada, que tem origem do nome Al Khowarizmi, que foi um matemático árabe do século nono. Surgiu, a partir, de uma necessidade em se realizar cálculos sem o auxílio de recursos como os dedos ou os ábacos. Antes disso, a estruturação de cálculo era muito associada às ferramentas que se dispunham à mão, como pedras, varetas, calculadora à manivela etc. Os utensílios que temos à disposição, atualmente, levaram séculos para se desenvolverem e foram criados a partir de muito estudo.

ALGORITMO DA DIVISÃO

Após a realização de cálculos mais práticos, foi possível se criar operações. A divisão juntamente com adição, subtração e multiplicação correspondem ao que chamamos de quatro operações básicas. A divisão é muito temida, principalmente entre os alunos das séries iniciais, do ensino fundamental e é tida como a mais difícil por muitos, entretanto, o diferencial da divisão é que possui um algoritmo diferenciado em relação às outras três.

Para entendermos bem este algoritmo é preciso que relembremos todos os elementos que de fato compõem uma operação de divisão, e consequentemente comporão seu algoritmo. Abaixo segue a descrição de cada um:

Dividendo (D): *número que será dividido*

Divisor (d): *número que se divide*

Quociente (q): *resultado da divisão*

Resto (r): *diversas vezes, ao finalizar a divisão, sobra uma quantidade que não pode ser dividida mais. Essa quantidade recebe o nome de resto.*

Seguindo esses elementos, a operação da divisão define-se dentro da seguinte fórmula: D= d.q+r.

A resolução da divisão se dá então em D: d, em que procuraremos um número q, que será multiplicado por d, e aí será encontrado D como resultado ou, no mínimo, muito próximo a ele. O resto r se formará, quando de fato sobrar, na subtração D – d.q. Se esse resultado for 0, então não há resto evidente.

Essa técnica é usada para se dividir algarismos próximos aos presentes nas tabuadas de 1 ao 10. Por exemplo, ao se dividir 80:9, procura-se um número q, que ao ser multiplicado por 9, tenha como resultado 80 ou, no mínimo, próximo a isso. Sabemos que 9.8 = 72, assim, podemos realizar a subtração 80-72 = 8, portanto temos todos os elementos encontrados.

D= d.q+r

80= 9.8 + 8

Este algoritmo da divisão compreende um método fácil e prático na realização das divisões de algarismos a algarismos, da mesma maneira que as outras operações. Na linguagem escolar, esse algoritmo tem sido chamado de forma geral como “método chave”, pois é representado da seguinte forma:

D | d

r q

Da mesma maneira, é preciso encontrar um número q, que ao ser multiplicado por d, tenha o resultado D. Caso não seja possível o resultado exato, deve-se encontrar um valor aproximado e anotar as sobras nas posições descritas acima. O método chave auxilia nessa visualização.

Exemplificando:

Exemplo 1: Veja como é feita a divisão de 9 por 3:

9 | 3

-9 3

0

Nesse exemplo, percebemos que: dividendo = 9, divisor = 3, quociente = 3 e resto = 0. Se o resultado (r) foi 0, portanto, não há resto. (r).

Exemplo 2 – Analise agora a divisão de 92 por 2. Em um primeiro passo, divida 9 por 2 e anote o resto 1. Perceba que 4·2 +1 = 9, então colocaremos 4 no quociente, o resultado de 4·2 abaixo do 9 (que é o algarismo o qual estamos dividindo nessa primeira etapa) e subtraímos 9 por esse resultado. Temos, então, que o resto é 1.

 92 | 2

-8   4

1

Ao lado do resto 1, “puxe” o próximo algarismo do dividendo:

92 | 2

-8   4

12

Em seguida, repita o procedimento para o número 12, composto agora pelo resto e pelo próximo número do dividendo inicial:

92 | 2

-8 46

12

-12

0

Enfim, chegamos ao resultado da divisão: 46. Escrevemos, portanto, a expressão que segue:

$r + q \cdot d = D$

$0 + 46 \cdot 2 = 92$

ALGORITMO DE EUCLIDES

Em aritmética, o Algoritmo de Euclides corresponde a um processo simples e muito eficaz para se encontrar o máximo divisor comum entre dois ou mais números inteiros, isso, se forem diferentes de zero. Este algoritmo é um dos mais antigos da história da matemática, sendo conhecido desde o surgimento nos livros VII e X da grande obra "Elementos de Euclides", aproximadamente nos anos 300 a.C. Este algoritmo não exige que se fatore os elementos.

O máximo divisor comum, ou MDC corresponde ao maior número inteiro que se possa dividir ambos elementos, sem deixar nenhum resto. Podemos citar de exemplo o número 21, que é o MDC de 252 e 105. (252 = 21x12; 105= 21x5). Agora observe que 252 – 105 = 147, por essa razão o MDC de 147 e 105 também será 21 e assim sucessivamente, os números diminuirão até se alcançar o zero.

Se formos fazer o oposto e reverter os passos do algoritmo de Euclides, o MDC passará a ser expresso como a soma dos dois algarismos originais, onde cada um deles será multiplicado por um valor inteiro, positivo ou negativo, por exemplo, 21 = 5x105 + (-2) x 252. Essa propriedade é denominada de Bézout.

O algoritmo original de Euclides foi elaborado apenas para números naturais e comprimentos geométricos, entretanto, no século XIX, foi generalizado para diversas outras classes matemáticas como os inteiros gaussianos e os polinômios.

CÁLCULO DO ALGORITMO DE EUCLIDES

O cálculo do algoritmo baseia-se na ideia de que dois números naturais sempre terão divisores em comum. Por exemplo, os números 12 e 18 possuem 1,2,3 e 6 como divisores iguais, sendo que o 6 é o maior. Então, neste caso, o 6 será chamado de máximo divisor comum de 12 e 18, e indicado como m.d.c (12,18) = 6

Exemplificando:

mdc(6,12)=6

mdc(12,20)=4

mdc(20,24)=4

mdc(12,20,24)=4

mdc (6,12,15) = 3

Uma das maneiras de se aplicar o algoritmo de Euclides e calculá-lo a fim de se encontrar o m.d.c, é utilizando a decomposição em fatores primos. Acompanhe, por exemplo, o cálculo do m.d.c entre os elementos 36 e 90:

36 = 2 x 2 x 3 x 3

90 = 2 x 3 x 3 x 5

O m.d.c. será sempre o produto dos fatores primos em comuns, que nesse caso se dará por:

m.d.c.(36,90)= 2x3x3

Enfim, m.d.c.(36,90) = 18.

Se escrevêssemos essa fatoração em forma de potência, teríamos os seguintes números:

36=2^2 x 3^2

90= 2 x 3^2 x 5

Ou seja, m.d.c.(36,90) = 2 x 3^2 = 18

DIVISÃO SUCESSIVA

Um outro método que pode ser utilizado na resolução do m.d.c é o processo da divisão sucessiva. Esse método consiste basicamente em dividir dois ou mais números simultaneamente pelo menor fator primo que se encontre. Caso o número ainda não seja divisível pelo menor primo, então deverá ser repetido.

Ao final das divisões, o m.d.c se tornará o produto dos diferentes fatores primos encontrados.

Exemplificando:

Encontre o MDC entre 90 e 54.

Primeiro, monta-se uma tabela contendo os números, depois realiza-se a divisão dos números pelo menor fator primo e em seguida multiplica-se pelos fatores primos diferentes encontrados. Esses passos estão devidamente exemplificados na imagem abaixo:

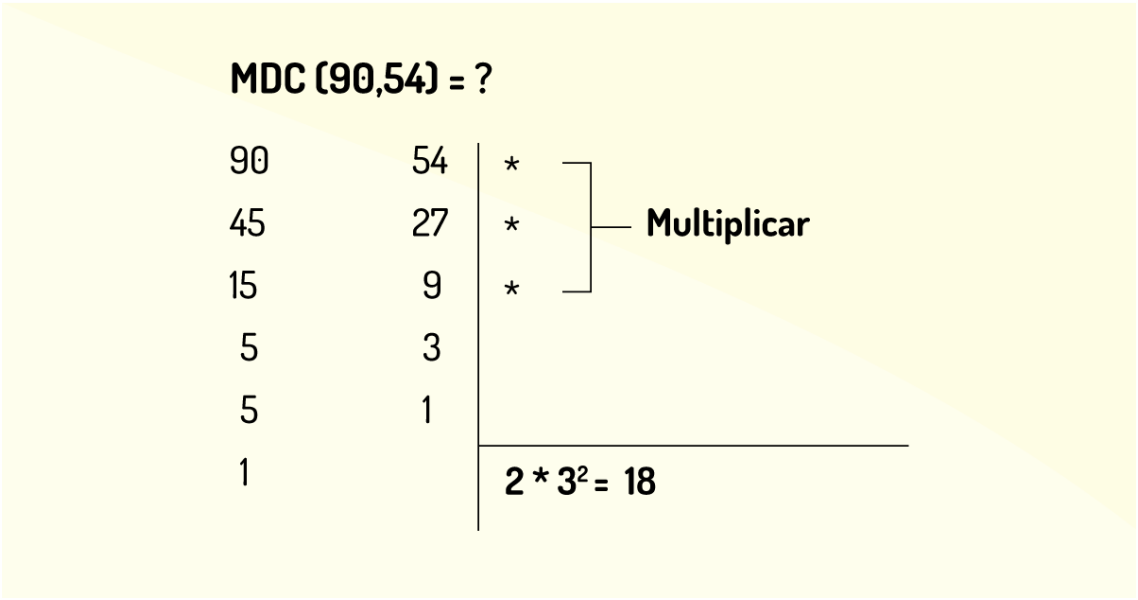


Figura 1.3 – MDC entre 90 e 54

Fonte: Elaborada pela autora.

Portanto temos:

MDC (90, 54) = 2 x 32 = 18.

Observação: Veja que 2 e 3 foram os menores fatores primos que dividiram simultaneamente os algarismos 90 e 54. Portanto o produto entre eles é o m.d.c entre os números em questão.

NÚMEROS PRIMOS

Os números considerados primos são aqueles naturais que possuem apenas dois divisores diferentes, e não mais que isso. Esses divisores são o 1 e eles próprios.

Exemplificando:

1) O 2 possui unicamente os divisores 1 e 2, portanto 2 é um número primo.
2) O 17 possui apenas os divisores 1 e 17, portanto 17 é um número primo.
3) O 10 tem os seguintes divisores: 1, 2, 5 e 10, portanto 10 não é um número primo.

Curiosamente o número 1 não é primo, pois possui, nesse caso, apenas um divisor, ele próprio.

Já o número 2 é o único número primo que é par.

Todos os números naturais que possuírem mais de dois divisores não são primos e são chamados de compostos, por exemplo, o número 15, que tem mais do que apenas dois divisores. Assim, 15 é um número composto. Para se comprovar e conferir que um número é primo, basta executarmos a divisão dele por outros primos 2, 3, 5, 7, 11 etc., até que nós tenhamos:

- ou uma divisão com resto zero (e neste caso o número não é primo);
- ou uma divisão com quociente menor que o divisor e o resto diferente de zero. Neste caso o número é primo.

Outra maneira é multiplicar dois números primos. O resultado será um número composto, ou seja, um número composto é resultado do produto de dois números primos, conforme: 2 x 5 = 10, 2 e 5 são primos e o produto entre eles é o número composto: 10.

Exemplificando:

1) O número 203:

- não é par, então não é divisível por 2;
- 2+0+3 = 5, portanto não é divisível por 3;
- não termina em 0 nem em 5, portanto não é divisível por 5;
- por 7: 203 / 7 = 29, com resto zero, logo 203 é divisível por 7, e portanto não é um número primo.

2) O número 137:

- não é par, portanto não é divisível por 2;
- 1+3+7 = 11, portanto não é divisível por 3;
- não termina em 0 nem em 5, portanto não é divisível por 5;
- por 7: 137 / 7 = 19, com resto 4. O quociente (19) ainda é maior que o divisor (7).

- por 11: 137 / 11 = 12, com resto 5. O quociente (12) é maior que o divisor (11).
- por 13: 137/13 = 10, com resto 7. O quociente (10) é menor que o divisor 13, e além disso o resto é diferente de zero (o resto vale 7), portanto 137 é um número primo.

Um cientista da aritmética chamado Eratóstenes (285-194 a.C) desenvolveu um simples sistema, de forma objetiva para desvendar se um número é ou não primo. Esse conceito foi denominado crivo de Eratóstenes. Para fazer a representação do crivo, consideremos uma tabela simples, com os 100 primeiros números naturais de 1 a 100:

1º passo: identificar o primeiro número primo da tabela, que é o 2;

2º passo: demarcar todos os múltiplos desse número;

3º passo: localizar o segundo número primo (3) e também marcar todos os seus múltiplos;

4º passo: repetir a operação até o último número, que na tabela é o 97.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Figura 1.4 – Números Primos

Fonte: Eves (1995, p. 195).

Na tabela representada pela Figura 1.5, destaca-se a lista dos 100 primeiros números naturais, com ênfase em roxo nos números primos entre 1 e 100. São eles: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

ATIVIDADE

3 – Como foi visto, o número primo é um tipo de número que é divisível por 1 ou por ele mesmo. Então, tendo como base a unidade estudada, qual das opções abaixo representa um número primo?

a) 2002
b) 1950
c) 1943
d) 1917
e) 647

TEOREMA FUNDAMENTAL DA MATEMÁTICA

Sabemos que toda matéria é composta e formada por pequenas partículas chamadas de átomos. Os primeiros a saberem de tal afirmação foram os gregos antigos, especificamente, o filósofo Demócrito (que viveu entre 546 a 460 a.C.), que deu o nome dessas partículas de átomos (do grego a: não; tomo: divisão), pois de fato se acreditava que não poderiam ser divididas, ou seja, um átomo seria indivisível. Entretanto, nos dias atuais, sabe-se que cada partícula de átomo pode sim ser dividida em outras mais pequenas, porém, a ideia em que a matéria exista em mínimas unidades ainda persiste.

Na aritmética também existe esse conceito de unidades mínimas, mas no lugar dos átomos, essa função é realizada pelos números primos.

Aqui se baseia o teorema fundamental da matemática, ou da aritmética, o TFA. Os descendentes de Pitágoras (Pitagóricos, 500 a 300 a.C.) foram os primeiros a tentarem desmistificar as propriedades gerais desses números, mas diferentemente das partículas atômicas, os números primos seguem em pleno funcionamento, como um conjunto numérico de extrema relevância, sendo atribuída a eles, até mesmo a responsabilidade em se criar absolutamente todos os números naturais diferentes de 0 e 1.

O TFA garante que um número natural que seja diferente de 0 e de 1, é sim, um número primo ou, no mínimo pode ser escrito como um produto de números primos, conforme mostra a Figura 1.5.

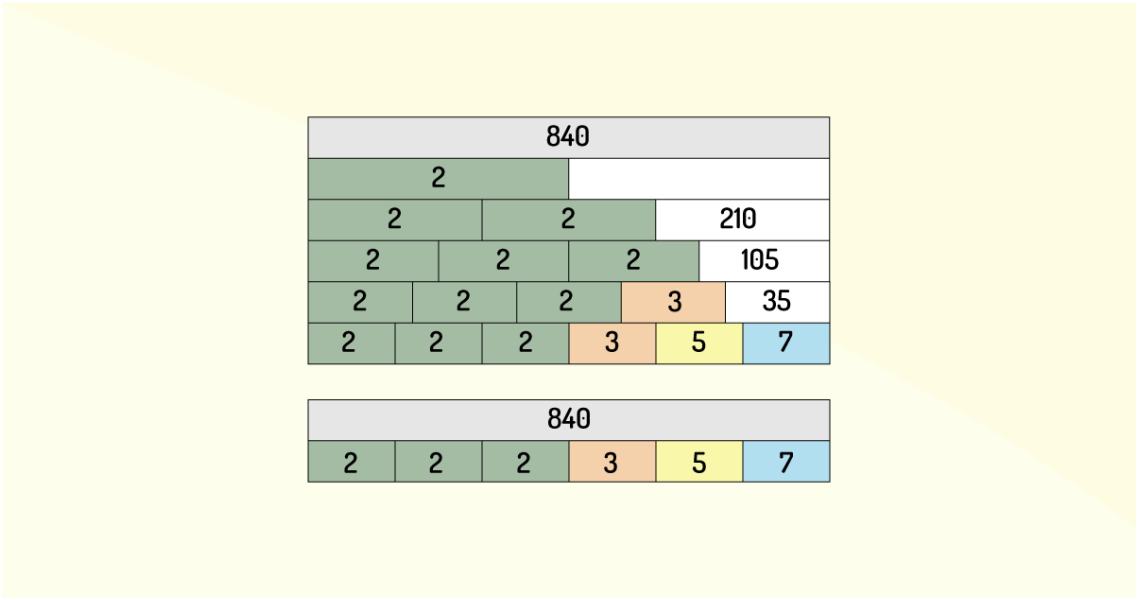


Figura 1.5 – Números primos e suas derivações (840 = 2 × 2 × 2 × 3 × 5 × 7)
Fonte: Garcia (2003, p. 242).

No exemplo acima percebe-se que o valor 840 não é primo, ou seja, é divisível por outros valores que não 1 ou ele mesmo, porém, quando se faz a fatoração, aparece em seu produto números primos, nisto é que se baseia o TFA.

SIGNIFICADO DE DIVISOR, DIVIDE E DIVISÍVEL

Na linguagem matemática, especificamente no meio dos números naturais, as palavras divisor, divide e divisível são similares. Em termos gerais, podemos explicá-las como a e b números naturais sendo que: "a é um divisor de b" significando que há um número c, de modo ac = b; "a divide b" já mostra que "existe um número natural c tal que ac = b; Se dissermos que "b é divisível por a", significa, neste caso, que "existe um número natural c tal que ac = b;

Como este teorema garante que todo algarismo natural superior a 1 (n > 1) pode ser escrito como um produto de números primos e essa decomposição de primos é única, isso permite que se use uma notação para a fatoração.

Exemplo: 1512 = 2×2×2×2×3×3×7 = Fatoração de (1512) = 2 3×3 2×7.

Como já vimos no tópico anterior, este segundo método de se escrever, por meio da fatoração, é um exemplo de escrita exponencial da decomposição em primos. É preferível que se descreva sempre a decomposição em primos na ordem crescente, pois permite uma referência aos expoentes mais facilmente. No caso do exemplo acima, os expoentes seriam 3, 2 e 1.

Para se fatorar um número natural n, n>1, existem alguns passos que podem ser seguidos formalmente, sendo os seguintes:

- **Passo 1:** fazer uma listagem com todos os algarismos primos menores ou no mínimo iguais a n, deixando-os em ordem crescente;
- **Passo 2:** dividir n de maneira sucessiva por esses elementos primos, até se encontrar um primeiro divisor primo p1 de n. sucessivamente por esses primos, até encontrar um primeiro divisor primo p1 de n. Se esse divisor p1 não for encontrado, então n é primo e a fatoração está terminada. Encontrado o divisor primo p1 de n, poderá ir para o próximo Passo;
- **Passo 3:** como p1|np, existe a1∈N tal que n=p1·a1;
- **Passo 4:** novamente fazer uma lista com todos os primos menores ou no mínimo iguais a a1−√a1, distribuindo-os em ordem crescente;
- **Passo 5:** dividir a1 de forma sucessiva pelos mesmos primos apontados no Passo 4, até encontrar um primeiro divisor p2 de a1. Se esse divisor p2 não for encontrado, então a1 é primo e a fatoração está terminada: n=p1·a1. Encontrado o divisor primo p2p2 de a1a1, ir para o próximo Passo;
- **Passo 6:** como p2|a1, existe a2∈N tal que a1=p2·a2. Assim, n=p1·p2·a2;
- **Passo 7:** mais uma vez listar todos os elementos primos menores ou iguais a a2−−√a2, escrevendo-os em ordem crescente;
- **Passo 8:** dividir a2 sucessivamente pelos primos listados no Passo 7, até encontrar um primeiro divisor p3 de a2. Se esse divisor p3 não for encontrado, então a2 é primo e a fatoração está terminada: n=p1·p2·a2. Encontrado o divisor primo p3 de a2, ir para o próximo Passo;

- **Passo 9:** como p3|a2, existe a3∈N tal que a2=p3·a3. Assim, n=p1·p2·p3·a3;
- **Passo 10:** listar todos os primos menores ou iguais a a3−−√a3, escrevendo-os em ordem crescente;
- **Passo 11:** dividir a3 sucessivamente pelos primos listados no Passo 10, até encontrar um primeiro divisor p4 de a3. Se esse divisor p4 não for encontrado, então a3 é primo e a fatoração está terminada: n=p1·p2·a2·a3.

Exemplificando:

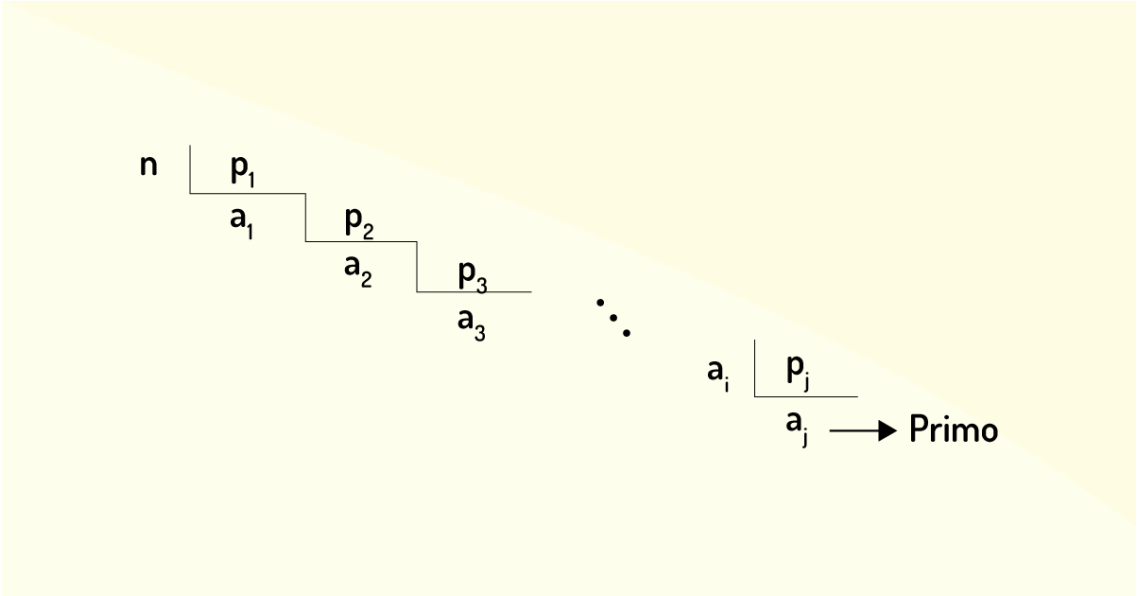


Figura 1.6 – Fatoração, método escadinha
Fonte: Garcia (2003, p. 243).

Observa-se que todas as vezes que um fator primo pj é achado, a partir de um divisor aj de n, um novo procedimento se abre e novos passos são executados. Este processo abre uma sequência decrescente, a1>a2>a3>⋯ de divisores de n. Por essa sequência, ter um número finito de termos, podemos concluir que o processo terá um fim, em algum momento. Muito provavelmente, este final se dará quando se encontrar um número primo.

O processo sucessivo por primos, quando aplicada no processo de fatoração ou decomposição, podem ser representadas, ou escritas das mais variadas maneiras. Para ficar no âmbito numérico, vejamos a decomposição de 60 em três maneiras diferentes:

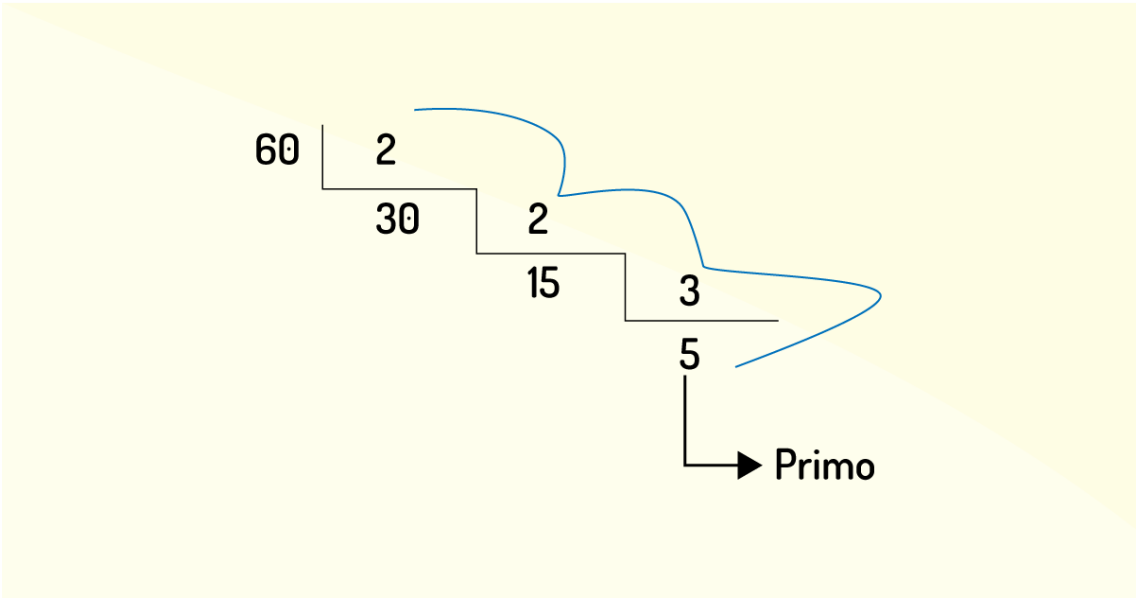


Figura 1.7 – Decomposição
Fonte: Mello (2009, p. 561).

Baseando-se nessa lógica, é necessário conhecer os números primos menores ou iguais a n√n, se quisermos realizar a decomposição de um número natural n, superior a 1.

FORMAS DO TFA

O TFA aparece vinculado à obra Elementos de Euclides, entretanto, sua primeira demonstração correta foi feita por Gauss e publicada em 1801, na obra *Disquisitiones Arithmeticae.*

Podemos conceituar o teorema a partir de duas abordagens. A primeira, conceitua que qualquer número natural maior que 1 ou é primo ou poderá ser escrito como fator de primo, como citado já anteriormente.

Para este conceito, existe uma justificativa que se segue:

Justificativa - Se n é um número natural, ou seja, n>1, ele sendo um número primo, já não haverá nada para ser demonstrado. Partimos então, de que n seja um número composto. Como n tem divisores diferentes de 1, chama-se p1 o menor dentre esses divisores distintos de 1. Assim, existe um número natural n1 tal que: $n=p1 \cdot n1$. (i)

Se na primeira forma, a regra coloca que todo número maior que 1 pode ser primo ou produto primo, nesta segunda forma de se ver o teorema os algarismos maiores que 1 ou são primos, podem ser escritos de forma única.

Aqui, baseia-se de forma teórica o exemplo visto acima, portanto, o TFA defende essa ideia central de que qualquer número pode ser fatorado e seus produtos serem transformados em números primos, ou que ele próprio seja primo, sendo divisível apenas por 1 ou ele mesmo.

Assim, o teorema aritmético apresenta um resultado que além de assegurar a representatividade de um número natural maior do que 1, como produto de seus divisores primos, também confirma que essa representação será única. Além de outros benefícios, este resultado nos faz iniciar um processo de divisores de forma segura, pelo primo que nos for mais conveniente, dependendo da situação que apareça.

Já a segunda maneira é mais simbólica. Se n representa um número natural, n>1, então existirão números primos, p1, p2, p3...pr, com $r \geq 1$, sendo que n=p1, p2, p3…pr…., essa representação também é única.

ATIVIDADE

4- Um dos princípios do teorema fundamental da aritmética é sobre os restos da divisão. Se considerarmos o número 62015 e o dividirmos por 10, qual seria o valor correspondente ao seu resto?

a) 4.
b) 5.
c) 6.
d) 8.
e) 9.

FIQUE POR DENTRO

Em nosso cotidiano, quando estamos em alguma situação relacionada à matemática, dificilmente lembramos das aulas que vimos e dos assuntos que lemos. Porém a matemática elementar, como vimos nesta unidade, se faz presente em diversas tarefas do nosso dia a dia. É preciso estar atento e compreender que a matemática envolve interação com o mundo a nossa volta.

Para aprofundar seus conhecimentos leia o artigo: Múltiplos e divisores: importantes ferramentas no ensino médio, disponível em: <http://uenf.br/posgraduacao/matematica/wp-content/uploads/sites/14/2017/09/11072014Bruno-Franca-Marques-da-Silva.pdf> e o site: <https://pt.khanacademy.org/math/pre-algebra/pre-algebra-factors-multiples/pre-algebra-factors-mult/a/factors-and-multiples-review>.

REFLITA

Estou vendo a matemática como fonte de estudo primordial para minha vida? Ou a quero simplesmente como meio de tirar nota? Que importância eu dou a ela?

INDICAÇÕES DE LEITURA

Livro: Manual da Indução matemática

Editora: Interciência; Edição: 1ª (1 de janeiro de 1999)

Autor: Luis Lopes

ISBN: 8571930139

Comentário: Este livro possui uma sistematização muito bem ordenada sobre a indução matemática e outros conteúdos algébricos. Sua grande vantagem é que possui muitas fórmulas, explicações e diversos exemplos e exercícios muito úteis para o aprendizado.

Filme: PI

Gênero: Suspense, Ficção científica

Ano: 1998

Elenco Principal: Sean Gullette, Mark Margolis, Ben Shenkman

Comentário: O filme PI conta a história de Max, que construiu um supercomputador capaz de descobrir o número completo do Pi e compreender a existência da vida na Terra, adivinhando, dessa forma, os acontecimentos no mercado da bolsa de valores e, por isso, ser requisitado por representantes de Wall Street e também por uma seita que busca decifrar os mistérios da matemática. Vale a pena assisti-lo!

UNIDADE II

Divisores e Múltiplos Comuns

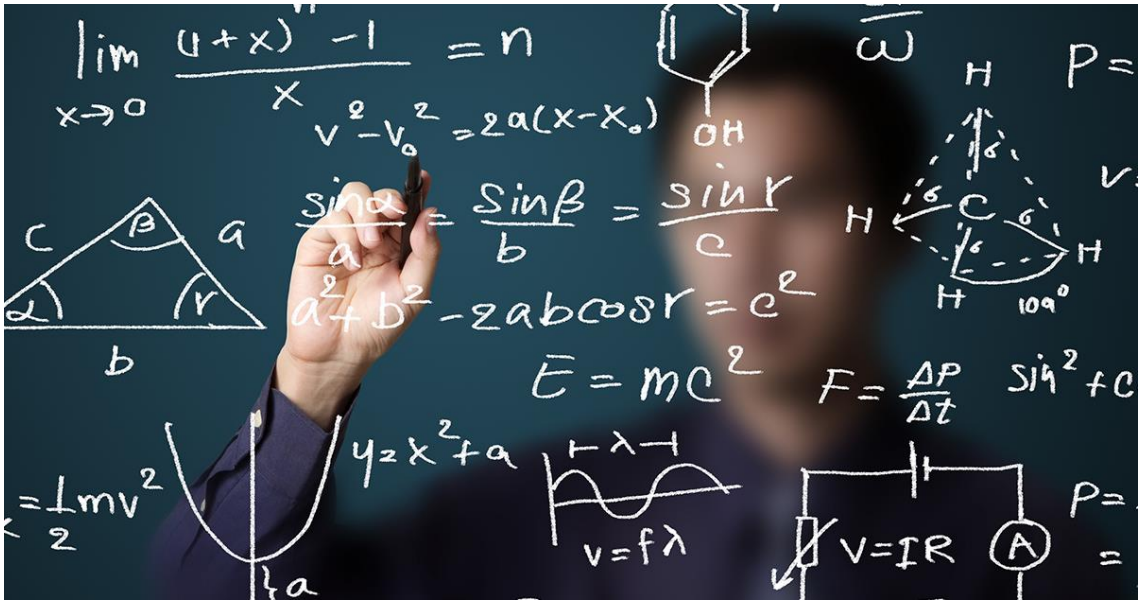
Valnira Oliveira

Introdução

Como visto na unidade anterior, é possível encontrar divisores em comum entre dois ou até mais números. Chamamos de máximo divisor comum aquele número que for o maior dos divisores entre os dois números naturais comparados.

É isso que veremos nesta unidade intitulada de Divisores e Múltiplos Comuns nos tópicos Máximo Divisor Comum (MDC), Mínimo Múltiplo Comum (MMC), Equações diofantinas lineares e Aplicações da teoria dos números no ensino básico.

Vamos lá, então?



Fonte: Dusit Panyakhom / 123RF.

MÁXIMO DIVISOR COMUM (MDC)

A fórmula e o procedimento para realizar essa determinação de encontrar o máximo divisor comum é muito simples, como veremos a seguir:

Nota: dois números naturais possuem sempre divisores em comum.

Na unidade anterior, vimos a decomposição por fatores primos e por meio dela podemos calcular o MDC entre dois números. Para a realização deste cálculo são necessárias três etapas descritas abaixo:

1ª etapa: decompõe-se o número em fatores primos;

2ª etapa: seleciona-se os fatores primos de **menores** expoentes que se repetem em ambos os casos;

3ª etapa: realiza-se a multiplicação dos fatores primos.

Exemplificando:

Encontre o MDC entre 36 e 90.

1ª etapa: é preciso decompor 36 e 90, a partir dos fatores primos, podendo escrevê-los em forma exponencial também.

$36 = \quad 2 \times 2 \times 3 \times 3 = 2^2 \times 3^2$

$90 = \quad 2 \times 3 \times 3 \times 5 = 2 \times 3^2 \times 5$

2ª etapa: entre eles, selecionamos os fatores primos de **menores** expoentes que se repetem em ambos os casos.

Neste exemplo, os números 2 e 3^2 se repetem nos dois casos e possuem **menores** expoentes.

3ª etapa: realiza-se a multiplicação dos fatores primos, e encontra-se o resultado final.

Portanto o MDC entre 36 e 90 que é igual MDC (36,90) = 3^2 x 2 = 18.

ATIVIDADE

1- Utilizando os conhecimentos adquiridos até o presente momento desta unidade, calcule o MDC entre os números 12 e 32.

a) (32, 12) = 2 * 2 = 4
b) (32, 12) = 2 * 2 = 7
c) (32, 12) = 2 * 2 = 8
d) (32, 12) = 2 * 2 = 3

MÍNIMO MÚLTIPLO COMUM (MMC)

O mínimo múltiplo comum (MMC) corresponde à operação para encontrar o menor múltiplo que seja diferente de zero, visto que é múltiplo comum entre todos os números fornecidos.

Pode ser bem observado em situações em que encontramos o denominador comum entre frações, por exemplo, e para encontrá-lo, assim como o MDC, também é muito simples e pode-se repetir o processo da decomposição por fatores primos, ou a decomposição simultânea.

Vale ressaltar que para se localizar os múltiplos de determinado número, basta multiplicá-lo pela sequência dos naturais. O zero, por exemplo, será múltiplo de todos os números, já que a sequência dos naturais parte dele.

Agora, como saber se números são ou não múltiplo um do outro? Para responder essa pergunta, é primordial descobrir se este número é divisível pelo outro. Como exemplo, podemos afirmar que 25 é múltiplo de 5, já que é divisível por 5.

Nesse sentido, podemos afirmar que o cálculo do MMC pode ser realizado pela comparação da tabuada desses números.

Exemplificando:

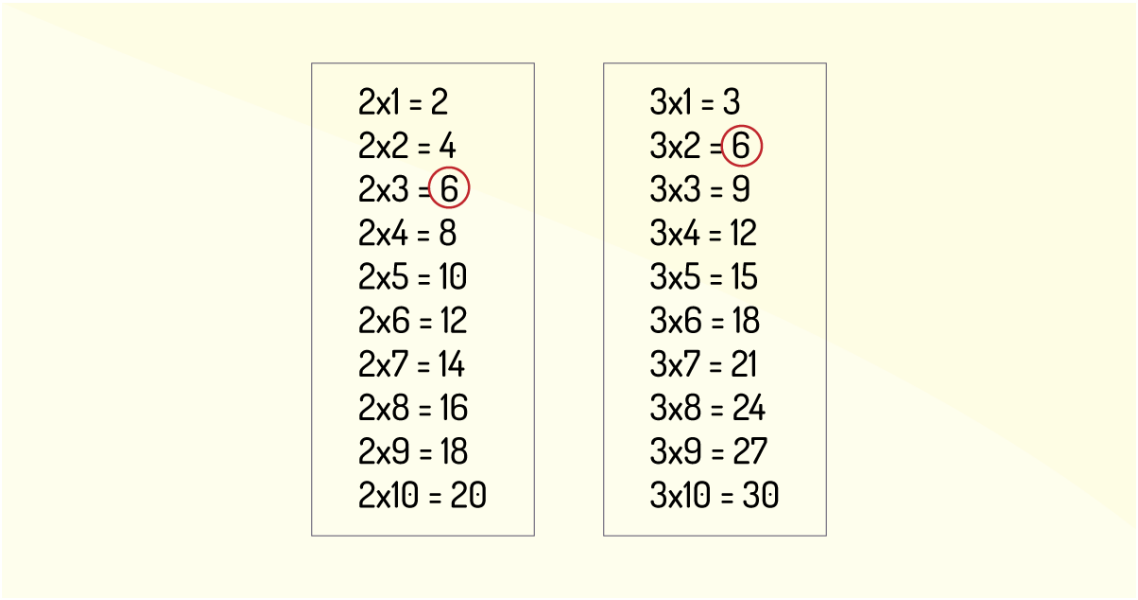


Figura 2.1 – Comparação de tabuadas

Fonte: Elaborada pela autora.

Para termos clareza com relação a este exemplo, descobriremos qual o MMC de 2 e 3. Veja na imagem da tabuada, que o menor valor que multiplica estes dois números é 6, portanto, de forma fácil, sem contas, e apenas na visualização da tabuada, encontramos o mínimo múltiplo comum entre esses dois elementos, que é o número 6.

O único problema dessa fórmula prática e direta é quando nos deparamos com números maiores. Nesse caso, essa técnica não será tão eficiente, já que é mais difícil se ter uma tabuada com números extensos. Nesses casos, a dica será utilizar o método da fatoração, isto é, decompor os números em fatores primos. Por esse método, já conhecido por nós, veja como acontece o cálculo do MMC entre 12 e 45.

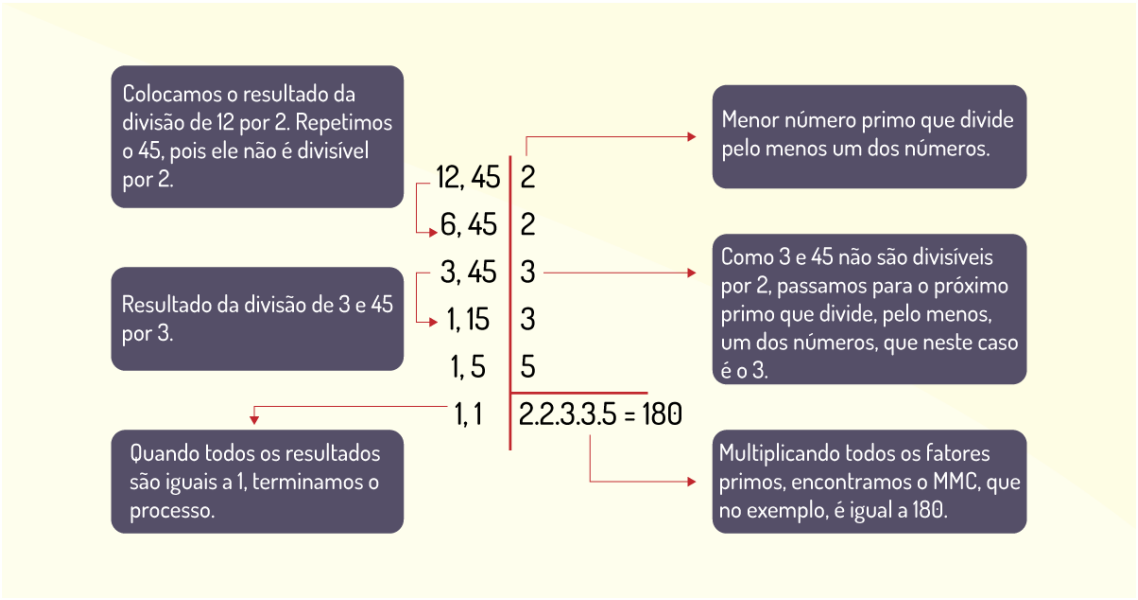


Figura 2.2 – Método da decomposição por fatores primos

Fonte: Tabuada (on-line).

Perceba que nesse sistema, vamos dividindo os dois elementos por números primos, ou seja, os números naturais que são divisíveis por 1 e eles mesmos apenas. Ao fim da decomposição multiplica-se esses números primos, encontrando, assim, o mínimo múltiplo comum, que no exemplo acima é 180. Daremos abaixo um exemplo contendo três elementos, veja:

Exemplificando:

Calcule o MMC entre os números 4, 6 e 12.

Observe que os números 4, 6 e 12 podem ser escritos como fatores de números primos. Desse modo, realizamos as três etapas, já conhecidas por nós:

1ª etapa: fatora-se o número em fatores primos.

$4 = 2 \times 2 = 2^2$

$6 = 2 \times 3$

$12 = 2 \times 2 \times 3 = 2^2 \times 3$

2ª etapa: entre todos os números primos do exemplo acima, seleciona-se apenas os fatores primos distintos de **maiores** expoentes.

Neste caso, os fatores primos distintos de **maiores** expoentes são o 2^2 e o 3^1.

3ª etapa: realiza-se a multiplicação dos fatores primos.

Logo, $2^2 \times 3 = 4 \times 3 = 12$.

Logo, o MMC entre 2,6 e 12 ou o MMC (2;6;12) é 12.

M.M.C E FRAÇÕES

O processo de se encontrar o MMC também é muito utilizado em operações com frações, que para a grande maioria dos alunos, é motivo de medo e complicação, porém, mostraremos que é mais simples do que se pensa.

Pela matemática básica, ainda nas séries iniciais, aprendemos que para somar ou subtrair frações, é necessário que ambas tenham denominadores em comum. Desse modo, entre frações, podemos calcular o MMC entre os denominadores, e, a partir daí, o resultado passará a ser o novo denominador das frações.

Exemplificando: 2/5+ 2/6

Aqui vemos que os denominadores são distintos, 5 e 6, portanto o primeiro passo é encontrar o MMC entre eles. Assim temos:

Agora que encontramos o MMC entre 5 e 6, que é 30, podemos realizar a soma das frações, pois agora o 30 passará a ser o denominador em comum. Essa adição se dá através do esquema abaixo:

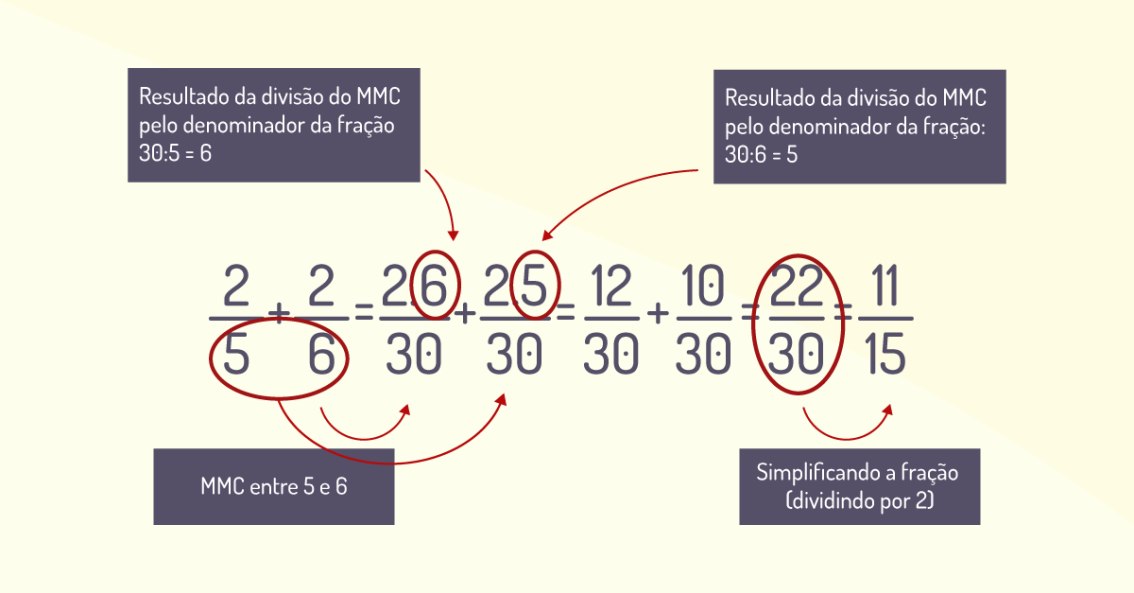


Figura 2.3 – Adição de frações.

Fonte: Lessa (on-line).

Soma-se as frações conforme o esquema acima, igualando os denominadores encontrados pelo MMC e depois dividindo o resultado pelo denominador, simplificando, então, a fração e executando a soma. No caso de subtração, realiza-se o mesmo procedimento.

DECOMPOSIÇÃO SIMULTÂNEA

Um outro método, muito simples e útil para o cálculo do MMC, é a decomposição simultânea.

Essa técnica consiste em realizar a divisão de todos os números encontrados na questão pelo menor fator primo correspondente a eles. A partir daí, o MMC será encontrado pela multiplicação de todos esses fatores usados na decomposição.

Exemplificando: Calcule o MMC entre 80, 60 e 30.

Para isso, a exemplo do MDC, montaremos uma tabela contendo os números e realizaremos a divisão em fatores primos, para assim, multiplicarmos e encontrarmos o MMC entre esses valores, conforme a Figura 2.4:

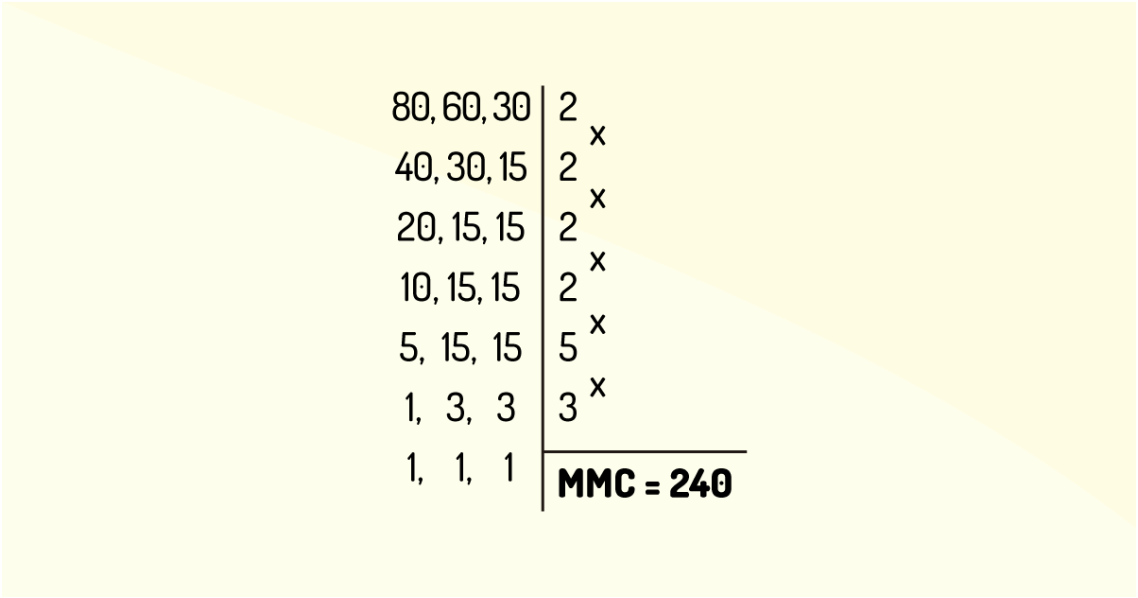


Figura 2.4 – Cálculo de MMC
Fonte: Calcular... (on-line).

O resultado, então, é o MMC (80,60 e 30) = 2 x 2 x 2 x 2 x 5 x 3 = 240.

Essa técnica é a melhor entre todas, quando se tem muitos elementos.

PROPRIEDADES DO MMC

O mínimo múltiplo comum possui duas propriedades as quais descreveremos abaixo:

1ª propriedade: o MMC entre dois algarismos primos entre si será o produto entre esses dois.

Ex: como já foi visto, 4 e 15, por exemplo, são primos entre si, então o MMC entre eles será 4 x 15 = 60.

2ª propriedade: se for dado dois ou até mais números e se um deles for múltiplo de todos os outros, então também será o m.m.c. dos números dados.

Ex: perceba que 30 é múltiplo de 6 e consequentemente múltiplo de 3. Assim, o MMC (3;6;30) = 30.

ATIVIDADE

2 – Considere os números 30, 60 e 90. Baseado no aprendizado sobre MDC e MMC, assinale a partir das afirmações a alternativa correta.

I. 3 é o único divisor positivo ímpar de 60.
II. A soma dos números primos positivos que são simultaneamente divisores de 30 e de 60 é igual a 5.
III. A soma dos divisores positivos primos do número 30 é igual a 10.
IV. O mínimo múltiplo comum entre 30 e 60 é 2700.
V. O máximo divisor comum entre 30, 60 e 90 é 6.

Qual das afirmações é verdadeira? Assinale a alternativa correta.

a) III e V.
b) II, III e IV.
c) I e V.
d) I e II.
e) Todas estão corretas.

EQUAÇÕES DIOFANTINAS LINEARES

O matemático Diofanto foi um dos responsáveis pelo grande crescimento e evolução da álgebra no mundo, e a partir deles, outros inúmeros matemáticos se inspiraram e se dedicaram aos estudos da teoria dos números. A maioria dos historiadores colocam Diofanto como pertencente ao século III d. C. Além do fato de que seus estudos e carreira terem sidos baseados na região de Alexandria, nada mais se sabe de grande relevância sobre o grego.

Entre seus principais trabalhos, Diofanto foi cultor da aritmética, números poligonais e Porisma. Entre eles, porém, o que mais destaca-se é a aritmética, já que é a obra mais intacta e mais completa do matemático, sendo seis livros de todos os treze que já escreveu.

Nesta obra da aritmética citada, Diofanto faz uma abordagem complexa em relação à teoria dos números, se dedicando, principalmente, na resolução de 130 problemas que ocorrem entre as equações. A obra possui tanta importância no meio matemático que os problemas algébricos que tem resultados indeterminados, encontrando-se apenas soluções racionais, foram batizados como “problemas diofantinos”, e esse termo designa até hoje as soluções que não são inteiras.

FORMA DE SINCOPAÇÃO DE DIOFANTO

Uma das técnicas de Diofanto era de realizar simplificações, por meio de abreviações. A palavra aritmética em si é uma conjunção entre *arithmos* (número) e *techne* (ciência). O autor utilizou essa palavra em grego para denotar alguns de seus símbolos e abreviações como no caso *arithmos*, em que colocou α e ρ, e com o passar dos anos se desenvolveu para um sinal sigma grego ς.

Existe também uma teoria, apesar de ainda haver dúvidas quanto a ela, de que a notação para potência se indicaria pelas letras da palavra grega dunamis (NAMI∑) que na tradução significa “potência” e “incógnita ao cubo”.

Compreendendo isso facilmente, podemos explicar os símbolos das potências seguintes da incógnita (quadrado-quadrado), (quadrado-cubo) e (cubo-cubo).

Para a expressão “menos”, Diofanto utiliza um símbolo que se assemelha a um V inverso com a bissetriz traçada nele. Também teria se originado a partir da palavra grega *leipis* (ΛΕΙΨΙ∑), que significa “menos”. Todos os elementos negativos eram associados e antes de se escreverem eram denotados com o sinal de menos.

UM POUCO DE HISTÓRIA

As equações Diofantinas compõem uma teoria em que estão inseridas na teoria dos números e tem como objetivo central investigar se as soluções das equações são inteiras ou racionais, por exemplo, a equação, $2x + 4y = 5$, $y^2 - x^3 = -2$ ou $x^2 + y^2 = z^2$. Em relação a nomenclatura, obviamente, equações Diofantinas, faz uma homenagem a um dos maiores estudiosos de álgebra que já existiu, Diophantus de Alexandria, que foi o responsável por descobrir, desenvolver e formular inúmeras equações. Como já citado, serviu de grande inspiração para outros matemáticos brilhantes, como o francês Pierre de Fermat (1601-1665).

Fermat tinha um cargo, na época, de conselheiro, e uma de suas responsabilidades estava interligada com a condenação de pessoas para serem mortas na fogueira, por essa razão, não devia ter muitas amizades. Quando tinha tempo livre, Pierre se dedicava ao estudo da aritmética e ganhou até um apelido de “Príncipe dos Amadores”, pois nesses momentos de estudo acabou descobrindo os conceitos de probabilidade, fundamentos do cálculo e complexos teoremas sobre os números inteiros. Fermat, porém, ganhou interesse pela matemática graças a uma obra de um escritor chamado Bachet, *Arithmetica* de *Diophantus*, livro que consolidou as ideias de Diofanto.

A partir daí, Fermat iniciou um novo ciclo da área da teoria dos números, tendo entre elas a análise diofantina, sendo responsável por formular os mais famosos problemas da matemática, desafiando estudiosos por diversas gerações. Podemos afirmar que Pierre Fermat influenciou praticamente todas as áreas da aritmética, afirmando até mesmo que possuía demonstrações para as Ternas Pitagóricas: se $n \geq 3$, a equação $x^n + y^n = z^n$, não admite soluções inteiras não-nulas.

Foi nessa demonstração que criou a conhecida “demonstração de Fermat”, que por muitos anos foi considerada o desafio mais complicado e famoso da matemática, justamente por parecer muito simples, mas nenhum matemático antes de 1994 conseguiu desvendar.

Fermat adorava provocar situações embaraçosas com outros matemáticos, principalmente os ingleses, porém, o destino fez com que justamente um inglês chamado Andrew Wiles fosse o iluminado para desvendar o “último teorema de Fermat”. Na época (1994), tal feito chegou a ser comparado com a descoberta dos átomos e o descobrimento das estruturas do DNA.

Wiles conta que desde criança tinha obsessão por esse teorema e se propôs de todas as maneiras tentar resolvê-lo. É considerado uma das conquistas mais importantes da história da matemática, e tudo se originou das ideias de Diofanto, ainda no século III. Podemos perceber assim, a importância e relevância que o matemático possui em toda a história.

EQUAÇÃO DIOFANTINA

As equações diofantinas costumam aparecer em problemas, cuja característica principal é de agrupamento, como nos casos abaixo:

Exemplo 1: Um laboratório médico tem a seu dispor 2 máquinas de raio x. Uma delas examina 15 imagens por vez, já a outra 25 imagens. Quantas vezes essas máquinas devem ser ligadas para examinar 2 mil imagens?

Exemplo 2: Quantos campos de futebol e quantos campos de queimada são necessários para que 80 alunos joguem simultaneamente? E se forem 77 alunos?

Exemplo 3: Para agrupar 13 aviões em filas de 3 ou de 5, quantas filas serão formadas de cada tipo?

Para se resolver esses problemas, precisamos buscar soluções inteiras e positivas, sendo assim, não se permite números negativos nesses casos. Dessa forma, podemos organizar o raciocínio pela equação diofantina:

$$ax + by = c$$

Observando os casos acima descritos e entendendo a fórmula dada, o problema do laboratório médico pode ser descrito através de: 15x+25y = 2000.

Na questão dos campos, uma equação é 10l0x+12y=80, que demonstra 2 soluções x = 2 e y = 5 ou x = 8 e y = 0, enquanto a outra questão baseia-se no mesmo método e é representada pela equação l0x + 12y = 77, não possuindo soluções (que sejam pares de números inteiros).

Em relação aos aviões (que pode ser usado como figura de linguagem e ser, portanto, apresentado desde as fases iniciais da escola), a equação 3x+5y=13 apresenta uma única solução (pares de números inteiros e positivos) x = 1 , y=2.

Ao se elaborar e colocar em prática qualquer um dos problemas, é preciso zelar na escolha dos coeficientes a, b e c, pois não determinarão apenas o nível de dificuldade do problema, mas também controlarão a quantidade de soluções possíveis que existirá, desde que sejam, como visto, inteiros ou inteiros positivos.

Quando estudamos qualquer problema matemático, é interessante termos algum processo para seguir, pois assim, para qualquer problema, teremos já na cabeça a forma de resolução e também identificaremos se possui ou não soluções, e se possui, saber quantas são.

Podemos citar como exemplo a equação de segundo grau abaixo:

$$ax^2 + bx + c = 0 ,$$

Essa equação só terá soluções reais se os seus elementos forem maiores que zero.

$$b^2 - 4ac \quad 0 .$$

Quando isso ocorrer,vas soluções reais x1 e x2 serão dadas por:

$$x_1 = \left(-b + \sqrt{b^2 - 4ac}\right)/2a \qquad \text{e} \qquad x_2 = \left(-b - \sqrt{b^2 - 4ac}\right)/2a$$

Quando estudamos as equações Diofantinas, $ax + by = c$, com a,b e c sendo números inteiros, é necessário saber se existe um critério predeterminado que permita afirmar que aquela equação, originada de um problema, possui solução e também um método para achar tais soluções, caso existam de fato. No caso das diofantinas, nosso único interesse é colocar soluções inteiras de $ax + by = c$.

Há, realmente, um critério único, que nos faz decidir se a equação padrão de $ax + by = c$ possui ou não soluções inteiras. Esse critério está descrito a seguir:

1. um critério de existência de solução, que já tem como subproduto um processo para encontrarmos uma solução particular;

2. um algoritmo para buscar essa solução particular;

3. a expressão que já propõe todas as soluções inteiras a partir de uma particular.

A EXISTÊNCIA DA SOLUÇÃO

Tendo, portanto, identificado a resolução da equação diofantina sendo ela:

$$ax + by = c,$$

Ou seja, sendo a, b e c como números inteiros, devemos, então, procurar as soluções x e y, para que se forme um par ordenado de números inteiros.

Para isso, deveremos usar propriedades de divisibilidade, que descreveremos abaixo, sendo que as duas primeiras possuem conotação de verificação imediata e a terceira sendo responsável por prova. Essas propriedades foram retiradas da Revista Professor de Matematica (RPM):

Propriedade 1 - Se d divide a, então dividirá am, para qualquer inteiro m;

Propriedade 2 - Se d divide a e divide b, então dividirá a + b;

Propriedade 3 - Se d é o máximo divisor comum de a e b, então existem inteiros r e s tais que

$$ar + bs = d.$$

Vemos que, com base nas duas primeiras propriedades, caso o problema apareça da forma ax + by = c, e, a partir dele, houver solução com x0 e y0 inteiros, sendo d um divisor comum, de a e b, então deverá dividir o elemento c. Portanto temos já, uma condição para que se exista uma solução inteira na equação.

Segundo a terceira propriedade, essa condição já é suficiente para comprovar que há solução, não precisando de outros elementos. Entretanto no caso de d, além de divisor comum, for o máximo divisor, então c = dm, a partir daí, segundo essa propriedade três, existirão inteiros r e s tais que ar + bs = d. Assim, multiplicando-se os membros desta igualdade pelo inteiro m, teremos a (rm) + b (sm) = c, sendo que x = rm e y = sm será a solução procurada.

Concluímos dessa forma, que uma equação diofantina ax + by = c, possui solução inteira, se o MDC de a e b puder dividir c.

Exemplificando:

Aplicando-se o teorema 1, podemos perceber que uma equação diofantina com os elementos 4x + 6y = 9, não possui solução, pois o máximo divisor comum (4 e 6) é 2 e o número 2 não pode dividir 9. O número 4x + 6y, com x e y, sendo inteiros, sempre serão pares, evidentemente, que jamais chegaram a ser 9, não importando a divisão que se faça.

De todo modo, se formos pensar na expressão 8x + 12y = 36, haverá solução, já que o MDC entre 8 e 12 é 4, e 4 divide 36.

Nota: Se o MDC entre o elemento a e b forem primos, então, pode-se afirmar que a equação diofantina sempre tem soluções inteiras, independentemente de qual seja o valor de c.

CÁLCULO DE UMA SOLUÇÃO PARTICULAR

Observamos, então, no tópico anterior, que para a busca de soluções inteiras de uma equação diofantina, podemos tomar o MDC de a e b como algum elemento primo, preferencialmente o 1, e que ao encontrar as soluções inteiras também se compara com encontrar valores inteiros para r e s tais que ar + bs = 1. Entretanto não é construtiva a prova que temos para se chegar a esses elementos r e s.

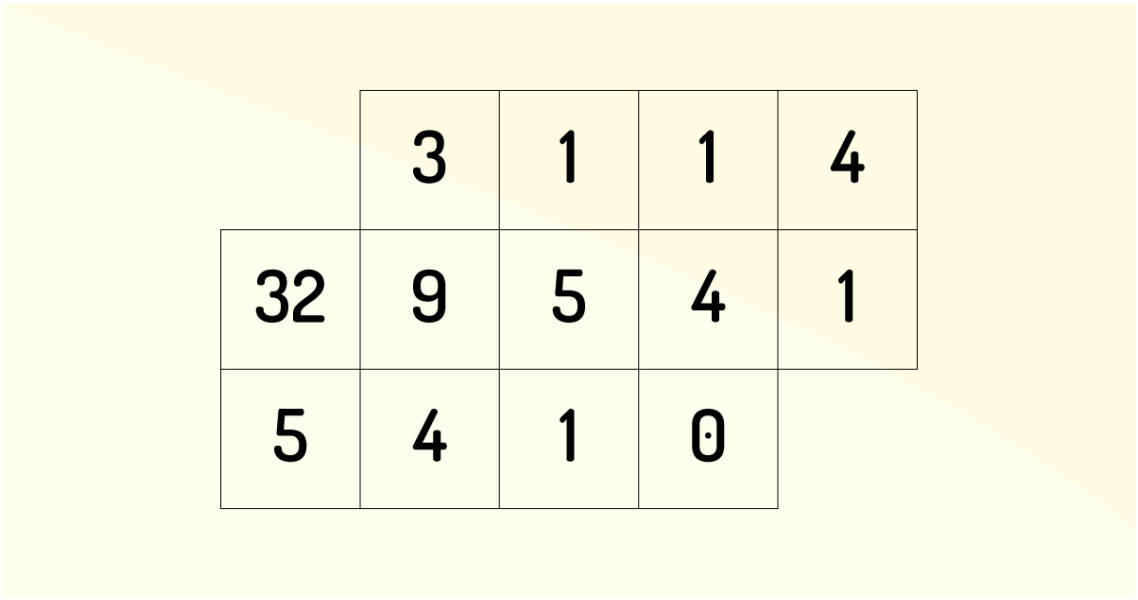
Um dos métodos que podemos utilizar, para se alcançar tais números, é aplicar o algoritmo de Euclides, que já conhecemos, ou então realizar o processo das divisões sucessivas para calcular o MDC de a e b. Esse algoritmo será autêntico quando estiver de acordo com as observações abaixo:

a) Caso os elementos a e b sejam inteiros, sendo o b > 0, existem inteiros q e r, com 0 r < b, únicos, de forma que a = bq + r (esse é o algoritmo da divisão).

b) Caso a e b sejam também inteiros, considerando o b > 0, e, dessa vez a = bq + r, contendo, 0 r < b. Então o mdc(a,b)=mdc(b,r). Dessa forma, veremos que o conjunto dos divisores comuns de a e b é similar aos divisores comuns de b e r. Concluímos, então, de modo forçado, que o máximo divisor comum de a e b é igual ao de b e r. E, finalmente, se a = bq + r e g for um divisor comum de a e b (isto é, g divide a e g divide b), então, de a bq = r, segue-se que g divide b e g divide r. Por fim, g é um divisor comum de b e r.

O oposto também é válido, se o elemento g divide b e r, como a = bq + r, segue-se que g divide a e b.

Agora, demonstraremos, através de exemplo, como encontrar os inteiros r e s, sendo eles ar + bs = 1, citado anteriormente. Para que isso aconteça, consideremos dois números, 32 e 9. Ao aplicarmos o algoritmo de Euclides, no cálculo do máximo divisor comum entre eles, teremos o seguinte resultado:



	3	1	1	4
32	9	5	4	1
5	4	1	0	

Figura 2.5 - O algoritmo de Euclides no cálculo máximo divisor entre os números 32 e 9.

Fonte: Elaborada pela autora.

Pelo algoritmo, podemos resumir as divisões, a partir do esquema abaixo:

32	=	3	x	9	+	5	(A)
9	=	1	x	5	+	4	(B)
5	=	1	x	4	+	1	(C)

e, a partir, da análise da segunda tabela, concluímos que:

$$mdc\ (32,9) = mdc\ (9,5) = mdc\ (5,4) = mdc\ (4,1) = 1.$$

O próximo passo é combinar de forma que fique conveniente as três expressões (A), (B), (C) e aí, encontraremos os inteiros r e s, sendo que teremos 32r + 9s = 1. Desse modo, nós tiramos da expressão (C), a afirmação 5 1 x 4=1. De (B), resultou o axioma 4 = 9 1 x 5 que, se jogarmos na expressão acima, ficaria:

5 l x (9 l x 5) = l ou 5 1 x 9 + 1 x 5 = 1

ou, ainda, de forma mais direta, 2 x 5 1 x 9 = 1.

Por fim, da expressão (A), obtemos 5 = 32 3 x 9 que, assim como na (B), incluiremos na expressão acima, chegando então a:

2 x (32 3 x 9) 1 x 9 =1 ou 2 x 32 7 x 9 = 1

Finalmente, os números que procuramos se fazem presentes, e são o 2 e o 7.

CONSTRUÇÃO DE TODAS AS SOLUÇÕES A PARTIR DE UMA

Tendo os coeficientes (x_0, y_0), obteremos uma solução inteira a partir da equação diofantina se a e b forem relativamente inteiros. Portanto a expressão deverá ficar ax_0+by_0 = c. Veja agora que, se, no primeiro elemento, somarmos e subtrairmos o mesmo número, essa igualdade continuará em vigor. Se quisermos colocar a e b em evidência, deveremos exigir que o número a ser acrescentado seja múltiplo de ab, ou seja teríamos uma escrita na forma abk, sendo o k um elemento inteiro. A partir daí, teríamos que:

Essa expressão, prova que o par ($x_0 + bk, y_0 ak$) continua sendo uma equação diofantina. Perceba também que até este momento ainda não utilizamos a hipótese de o máximo divisor comum a e b ser igual a 1.

A pergunta fundamental agora é: será que estas opções são todas as soluções inteiras existentes? Ou poderão existir outras? Para responder isso, faremos uma suposição de que (x0, y0) e (x1, y1) são soluções inteiras da equação, agora sim incluindo o MDC de a e b = 1. Assim teremos:

$$ax_0 + by_0 = c \qquad e \qquad ax_1 + by_1 = c.$$

O que resulta em:

$$a\ (x_1 \quad x_0) = b(y_0 \quad y_1).$$

Primeiro caso: Se o a = 1, chamaremos de k; o inteiro que resultar em y0 y1 e teremos $x_0 \quad x_1 = bk$, isto é, $x_1 = x0 + bk$, sendo que $y_0 \quad y_1 = k$, ou seja, $y_1 = y_0 \quad k$, que é igual a y1 = y0 ak, pois a = 1. Então, neste caso, qualquer solução (x_1,y_1) é da forma $(x_0 + bk, y_0 \ ak)$, com k inteiro.

Segundo caso: Se o a 1, a não dividirá *b*, isso porque a e *b* são primos. Então, a divide $y_0 \quad y_1$, ou seja, existe k; inteiro tal que $y_0 \quad y_1 = ak$, sendo que $y_1 = y_0$ ak. Mas então a($x_1 \ x_0$) = bak, e, como a 0, vem que $x_1 \quad x_0 = bk$, ou seja, $x_1 = x_0 + bk$.

Assim, exibimos um teorema que diz se o par ordenado (x_0, y_0) de fato for uma solução da equação diofantina ax + by = c, com regra mdc (a, b) = 1, então (x_1, y_1) será consequentemente solução da equação se, e somente se, existir um inteiro k tal que $x_1 = x_0 + bk \quad e \quad y_1 = y_0 \ ak$.

Preste atenção que a condição de a e b serem primos, não é necessária aqui, para que o x_1 *e* y_1 tornem-se soluções da equação diofantina, entretanto, essa regra ainda é importante para garantir que essas sejam todas as soluções da equação proposta.

Exemplificando:

Dada a equação diofantina 143x + 17y = 132, buscaremos as soluções inteiras para ela. De início, colocamos o máximo divisor comum entre (143,17) = 1, portanto, já podemos estabelecer que essa equação terá soluções inteiras. Para se achar, ao menos uma delas, veja que:

143 = 8 x 17 + 7, 17 = 2 x 7 + 3, 7 = 2 x 3 + 1. Logo temos:

l = 7 2 x 3 = 7 2 x [17 2 x 7] = 5 x 7 2 x 17 =

= 5 x [143 8 x 17] 2 x 17 = 5 x 143 42 x 17.

Em que descrevemos:

143 x [5 x 132] + 17 x [42 x 132] = 132,

Isto é a solução da equação que se dá por: (x0, y0) = (660, 5544), portanto, todas as demais soluções ainda não encontradas, se darão da mesma forma: x = 660 + 17k e y = 5544 143k , em que k é um inteiro arbitrário.

AS DIFERENTES FORMAS DE RESOLVER UMA EQUAÇÃO DIOFANTINA

De forma conceitual, para se resolver uma equação diofantina, é necessário encontrar valores correspondentes para as variáveis x e y, que precisam necessariamente ser números inteiros. Uma solução padrão é mais fácil de ser encontrada do que uma integral, exigindo, de quem faz, um processo de inúmeras etapas. Antes de tudo, é preciso encontrar o MDC dos coeficientes dados no problema. Se, caso, conseguir encontrar uma solução integral, de uma equação linear, será mais fácil aplicar a ela um padrão e, assim, identificar inúmeras outras soluções possíveis. A seguir, colocaremos três métodos de resolução das equações, dando a cada um deles, o passo a passo necessário.

- **Método 1:** Preparando a Equação

a) Escreva-a em formato padrão – para uma equação ser linear, não deve ter nenhum expoente maior que 1, em qualquer uma de suas variáveis. O primeiro passo para solucioná-la é escrevê-la de forma padronizada, representada no estilo diofantino ax + bx = c, sendo que a, b e c sempre serão valores inteiros. Em muitos problemas, a equação já estará neste padrão, porém, caso não esteja, é preciso utilizar-se das regras de álgebra para executar essa ordenação, ou partir para uma combinação de termos. Se o problema der, por exemplo, 23x + 4y – 7x = -3y + 15, você pode simplificar essa equação combinando elementos similares até chegar em 16x + 7y = 15.

b) Se possível reduza a equação – após sua equação estar dentro do formato padrão, observe bem os termos de a, b e c. Caso haja, entre eles, algum fator comum, busque uni-los a fim de reduzir a equação. Após reduzir igualmente os três termos, as soluções encontradas também serão válidas para a descrição original. Se os três forem elementos pares, por exemplo, poderá dividi-los e simplificá-los por 2, como segue a demonstração abaixo:

- 42x + 36y = 48 (todos os termos são divisíveis por {\displaystyle 2}2), e depois,

- 21x + 18y = 24 (todos os termos são divisíveis por {\displaystyle 2}3)

- 7x + 6y = 8 (a equação chegou ao formato mais reduzido possível)

c) Determine a impossibilidade de uma solução – para algumas equações, será possível determinar se existe ou não solução possível. Se houver, algum múltiplo comum do lado esquerdo da expressão que não convém com o lado direito, pode ser, neste caso, que a solução não exista. Se a e b forem pares, a soma de ambos os lados também precisa ser par, se não for, é possível também que não se tenha resultados. Por outro lado, se o elemento c for ímpar, aí não existirá solução inteira.

- 2x + 4y = 21 - não possui solução inteira.

- 5x + 10y = 17 - não pode ter solução inteira, uma vez que o lado esquerdo da equação é divisível por 5 {\displaystyle 5}, mas não o lado direito.

- **Método 2** – Utilizando o algoritmo euclidiano

a) Reaprenda o algoritmo euclidiano – esse sistema consiste em divisões repetidas, em que será usado cada resto como divisor de uma nova conta. O último divisor utilizado será o MDC entre os valores analisados. Os passos, descritos abaixo, demonstram o uso do algoritmo euclidiano na determinação do MDC entre 272 e 36:

- 272 = 7 x 36 + 20 – divida o número maior (272) pelo menor (36) e anote o resto (20);

- 36 = 1 x 20 + 16 – divida o divisor prévio (36) pelo resto (20) e anote o novo resto (16);

- 20 = 1 x 16 + 4 – repita o procedimento, dividindo o divisor (20) pelo resto prévio (16) e anote o novo resto (4);

- 16 = 4 x 4 = 0, Repita o procedimento, dividindo o divisor (16) pelo resto prévio (4), uma vez que o resto agora é 0, conclua que 4 é o MDC dos números originais 272 e 36.

b) Aplique o algoritmo euclidiano aos coeficientes a{\displaystyle {\text{a}}} e b{\displaystyle {\text{b}}} – se a equação já estiver em formato padrão, identifique os coeficientes a e b e realize o cálculo do MDC, pelo algoritmo euclidiano entre esses elementos. A partir daí, determine soluções integrais para a equação linear. Por exemplo 87x + 64y = 3. Os passos a seguir mostrarão como isso ocorre:

87 = 1 x 64 + 23

64 = 2 x 23 + 18

23 = 1 x 18 + 5

18 = 3 x 5 + 3

5 = 1 x 3 + 2

3 = 1 x 2 + 1

2 = 2 x 1 + 0

c) Identifique o máximo divisor comum (MDC) – se o algoritmo euclidiano se suceder para esse par ordenado até a divisão chegar a 1, então, concluiremos, que o MDC entre 87 e 64 é 1. Ou simplesmente dizemos que ambos os números são primos entre si mesmos.

d) Interprete o resultado – após o complemento do algoritmo e a determinação do MDC entre a e b, deveremos comparar os resultados com o valor de c, dado na equação. Se o MDC entre esses dois valores também for divisor, então, essa equação linear terá uma solução integral. Se não for, então, não haverá solução possível. Voltando ao 87x + 64y =3, essa equação terá solução integral, já que seu MDC pode ser igualmente dividido pelo elemento c (3). Se supormos que o MDC fosse 5, aí não poderia haver essa divisão, então, não obteríamos soluções integrais, evidentemente.

- Método 3 – Renomeando o MDC para encontrar a solução.

a) Rotule os passos da redução do MDC – neste método, para se encontrar a solução de uma equação linear, será preciso utilizar o trabalho feito no algoritmo euclidiano como suporte em um processo de repetição, sendo que o objetivo é renomear e simplificar os valores. De início, numere os passos da redução do algoritmo para ter um caminho referencial, após isso terá a lógica que se exemplifica abaixo:

Passo 1: 87 = (1 x 64) + 23

Passo 2: 64 = (2 x 23) + 18

Passo 3: 23 = (1 x 18) + 5

Passo 4: 18 = (3 x 5) + 3

Passo 5: 5 = (1 x 3) + 2

Passo 6: 3 = (1 x 2) + 1

Passo 7: 2 = (2 x 1) + 0

{\displaystyle 87x-64y=3}

b) Comece com o último passo contendo um resto – reescreva a equação, para que siga o restante das informações dadas na expressão. Nesse problema, o passo 6 é o último a ter um resto que é o próprio 1. Nesse caso, poderá ser reescrito da seguinte forma:

$$1 = 3 – (1 \times 2).$$

c) Isole o resto do passo anterior – esse processo pode ser considerado um passo a passo de como ir elevando cada etapa. Todas as vezes, você deverá rever o lado direito da equação e focar nos valores da etapa acima. É possível reavaliar o passo 5, para isolar o resto que se segue, como demonstrado abaixo:

$$2 = 5 – (1 \times 3) \text{ ou } 2 = 5 - 3$$

d) Faça uma substituição e simplifique – observe que a revisão do sexto passo possui o número 2, e a revisão do quinto passo também é igual a 2. Então teremos que substituir ?a igual? dado do passo 5 para que entre no lugar do 2 no passo 6, como abaixo:

$1 = 3 – (1 \times 2)$ – Essa é a revisão do passo 6.

$1 = 3 – (5 \times 3)$ – Faça a substituição no lugar do valor 2.

$1 = 3 – (5 + 3)$ – Distribuição do sinal negativo.

$1 = 2 (3) – 5$ – Simplifique.

e) Repita o processo de substituição e simplificação – caminhando pelos passos do algoritmo euclidiano, inverte-se a forma e repete-se o mesmo procedimento. Após cada etapa, reveja a anterior e substitua o valor do último resultado encontrado. Se a última foi o passo 5, agora refaça o quarto passo, e siga isolando o resto:

$3 = 18 – (3 \times 5)$

Substitua o valor no lugar do 3{\displaystyle 3} na última etapa e simplifique:

1= 2 (18 – 3 x 5) – 5

1= 2 (18) – 6(5) – 5

1= 2 (18) – 7(5)

f) Continue repetindo os passos de substituição e simplificação – esse procedimento seguirá se repetindo, até que se chegue novamente a etapa original do algoritmo euclidiano. O objetivo central, deste processo, é determinar uma equação que seja baseada nos termos 87 e 64, que são os coeficientes originais do problema que estamos exemplificando.

Esse processo se repetirá, passo a passo, até chegar novamente à etapa original do algoritmo euclidiano. A finalidade desse procedimento é determinar uma equação que seja escrita em termos de {\displaystyle 87} 87 e 64{\displaystyle 64}, os coeficientes originais do problema a serem resolvidos. Desse modo, os próximos passos a se seguir são:

1 = 2(18) – 7(5)

1 = 2(18) – 7(23 – 18) – Substituição do passo 3

1 = 2(18) – 7(23) + 7(18)

1 = 9(18) – 7(23)

1= 9(64 – 2 x 23) – 7(23) – Substituição do passo 2

1= 9(64) – 18(23) – 7(23)

1= 9(64) – 25(23)

1= 9(64) – 25(87 – 64) – Substituição do passo 1

1= 9(64) – 25(87) + 25(64)

1= 34(64) – 25(87)

g) Reescreva o resultado em termos dos coeficientes originais – ao voltar para o início, no primeiro passo, do algoritmo euclidiano, perceba que os coeficientes do problema original também retornam. Então, recoloque os números para que se alinhem junto com a primeira equação. Desse modo, a expressão inicial para se resolver é 87x – 64y = 3. Assim, é possível remarcar a última etapa do processo a fim de deixar todos os termos padronizados. É preciso aqui, ter uma atenção especial, principalmente ao 64. Veja que na equação original, é subtraído, entretanto, o algoritmo euclidiano o trata como sendo positivo. Só será possível considerar a subtração, transformando o 34 em um valor negativo. Ficando, então, da seguinte forma nossa equação:

$$87\ \ -25) – 64(-34) = 1$$

h) Multiplique o fator necessário para determinar as soluções – veja que o MDC do problema era 1, de tal forma que essa foi a solução exigida. Mas essa solução não representa a real solução do problema proposto, pois originalmente a equação é 87x – 64y = 3. É preciso então, uma multiplicação dos termos da última equação por esse termo, para se chegar a uma real solução, ficando:

87 (-25 x 3) – 64(-34x 3) = 1 x 3

87(-75) – 64(-102) = 3

i) Identifique a solução integral da equação – os elementos que serão multiplicados pelos coeficientes originais representam a solução x e y do nosso problema. Podemos identificar como um par ordenado, (x,y) = (-75, -102).

ATIVIDADE

3 - Tendo como base nossos estudos acerca das Equações Diofantinas, analise as assertivas a seguir:

I. Antes de se resolver uma equação diofantina, é preciso ordenar e padronizar os elementos da equação, mas não se faz necessário tirar o MDC dos coeficientes.
II. Uma equação diofantina possui apenas um padrão e todas possuem uma ou mais soluções.
III. Para se resolver uma equação diofantina, é necessário encontrar valores correspondentes para as variáveis x e y.
IV. As Equações Diofantinas são equações algébricas que apresentam solução no conjunto dos números inteiros.

Está correto o que se afirma em:

a) I apenas.
b) II apenas.
c) I, II e III apenas.
d) II e IV apenas.
e) III e IV apenas.

APLICAÇÕES DA TEORIA DOS NÚMEROS NO ENSINO BÁSICO

Chama-se de teoria dos números o ramo de estudos sobre todos os números naturais ou inteiros positivos (1,2,3,4 ...), considerando todas as suas propriedades. O matemático Leopold Kronecker disse certa vez que, em relação aos números, Deus criou todos os naturais, e suas derivações foram criadas pelo homem que se evoluiu e desenvolveu. Entretanto os inteiros positivos foram, sem dúvida, a primeira criação matemática dos seres humanos e é até impossível pensar a humanidade sem o contato com os números, mesmo que de forma inconsciente e sem o domínio total, pode-se concluir que em toda história o homem possuía uma relação com os algarismos.

Apesar de o conjunto dos números naturais formar o principal sistema da matemática, estudar suas propriedades e derivações tem chamado muita atenção dos matemáticos desde sempre.

No antigo Egito, guardado junto ao enorme tesouro ali pertencente, foi encontrou o papiro *Rhind*, que descreve a aritmética praticada ali, há pelo menos 2000 anos a.C., provando que essas curiosidades e relações numéricas não vem de hoje. No fim do terceiro milênio a. C., tábuas cuneiformes da Mesopotâmia já mostravam uma matemática avançada e bem aplicada desses povos.

Desde a antiguidade, os números são utilizados em transações comerciais, e desde desse período, já se tem pensado em aprofundar os estudos sobre eles. A princípio, se tem notícia de uma primeira teoria oficial dos números no ano 600 a. C. com Pitágoras e seus discípulos, que foram responsáveis por classificar os inteiros das mais diversas maneiras, como pares, ímpares, primos e assim por diante.

A teoria dos números, a partir daí, foi se desenvolvendo e é a área da matemática que tem o objetivo de descobrir e aprofundar as relações dos números entre si. Por exemplo, consideremos um conjunto dos quadrados de 1, 4, 9, 16, 25,... Se pegarmos a somatória de dois desses quadrados, eventualmente, teremos como resultado um outro número quadrado.

Outro fascínio que envolve os números inteiros são as ternas de Pitágoras, como (3, 4, 5), (5, 12, 13), (20, 21, 29). Veja que $2^2+4^2= 5^2$, o mesmo acontece para: $5^2+12^2= 13^2$ e $20^2+ 21^2 = 29^2$. Em contrapartida, se colocarmos por exemplo (2,3,4) ao quadrado $2^2+3^2 = 4^2$, não dará um resultado quadrado. Então, será que existiram ou não ternas infinitas? E se existir, há uma fórmula padrão para descrevê-las? Estas questões são exemplos sobre em que se baseia a teoria dos números.

Dentro dessa teoria, há uma grande variedade de objetos investigados: primos, quadrados, ímpares, conjuntos, números racionais, algébricos, funções, códigos e muitos outros.

APLICAÇÃO PRÁTICA

Já na antiguidade, Pitágoras mencionava que os números são quem, na verdade, governam e ditam o ritmo do mundo. O significado dessa frase é grandiosa e impactante e coloca a matemática como o centro de nossa vida cotidiana.

Ao longo da história, o ser humano administrou a matemática como uma ferramenta de organização de processos e estruturação de várias atividades, desde contar frutos colhidos no campo, até calcular distâncias e dimensões e assim se localizar melhor no planeta Terra.

A matemática sustenta-se, portanto, pelas relações que fazemos dela com as coisas. O sistema decimal, por exemplo, foi concebido a partir da condição em que temos dez dedos nas mãos e nos pés, o que comprova que usamos essa ciência como relacionamentos a nossa volta. A aplicação matemática se dá também em provar a existência ou não de alguma situação, como se comprovar ou não a existência de um triângulo, em que suas medidas não podem ser aleatórias e que cada parte deve ter o mesmo tamanho sendo que um dos lados deve ser maior que a diferença dos outros dois.

Assim como em outras ciências exatas, para que um argumento matemático seja autêntico, é preciso que seja provado. Esse questionamento será comprovado ou não a partir de axiomas, teoremas, hipóteses, testes, observações e deduções.

Atualmente, outra importância da aplicação fundamental da matemática é a respeito do indivíduo, pois aquele que a domina e a compreende é considerado muito mais capaz de planejar e executar as funções sociais do que aquele que tem dificuldade. Portanto podemos concluir que a matemática é um meio de inclusão nos grupos sociais e pessoais, possuindo os seguintes objetivos:

- transformar a realidade de um indivíduo, tornando-o capaz;
- desenvolver sua capacidade de resolução de problemas;
- alimentar o interesse, a curiosidade e a criatividade;
- desenvolver diversas habilidades quantitativas e qualitativas;
- identificar, planejar, raciocinar sobre diversas situações e a partir da análise tomar melhores decisões;
- realizar uma comunicação matemática, através das ferramentas e meios que essa ciência disponibiliza.

Além dessas qualificações, muitas outras podem ser apontadas, como benefícios do conhecimento e domínio matemático.

Na parte teórica, de conteúdos em si, a aritmética pode apresentar, inúmeras divisões distintas, sendo classificada, principalmente, a partir de quatro grandes grupos, listados a seguir:

1 - Espaço e forma: Estuda-se e analisa-se diversas formas e estruturas geométricas, aprendendo a realizar os cálculos de tamanho e distâncias, por exemplo. Podemos nomeá-los como:

- localização, figuras bidimensionais e tridimensionais;
- propriedade dos triângulos;
- relações dos quadriláteros;
- cálculo da área e do perímetro de figuras geométricas;
- identificação e operações com ângulos;
- propriedade dos polígonos;
- coordenadas cartesianas;
- relações métricas do triângulo, do círculo e da circunferência;
- relações trigonométricas.

2 - Grandezas e medidas: Essa área da matemática é utilizada para descrever padrões como velocidade, tempo, capacidade, densidade, volume, entre outros. Nesse sentido, temos os seguintes conteúdos abrangidos:

- cálculo do perímetro de figuras planas;
- problemas relacionados com o cálculo de área;
- noções de unidades de medida;
- transformações de unidades de medida;
- relações entre as unidades de medida.

3 - Número e operações / álgebra e funções: a matemática se relaciona de forma mais direta com a álgebra, os cálculos e os números em si. Destaca-se os seguintes conteúdos:

- contagem;
- conjuntos;
- todas as classes de números e suas operações;
- frações e seus tipos;
- polinômios;
- potenciação;
- radicais e suas operações;
- porcentagem;
- matemática financeira;
- grandezas direta e inversamente proporcionais;
- progressões numéricas;
- expressão numérica;
- expressão algébrica;
- equações;
- inequações;
- sistemas;
- funções.

4 - Tratamento da informação: Usa-se o tratamento da informação para fazer padrões de análise e compará-los a outros ou não. Os conteúdos deste grupo são os seguintes:

- tipos de tabelas;
- tipos de gráficos;
- confecção de tabelas;
- confecção de gráficos;
- interpretação de tabelas e de gráficos;
- análise dos dados contidos em tabelas e gráficos.

JOGOS MATEMÁTICOS

Uma das metodologias de ensino e aprendizagem para a teoria dos números é a aplicação de jogos matemáticos, que estimulem o pensamento e a criação. Se o jogo for proposto com argumentos e objetivos bem explícitos, que quando posto em prática, realmente fará o educando aplicar seus conhecimentos matemáticos, então, é uma ótima opção.

Em um primeiro momento, os jogos devem ser apresentados e depois relacionados com os conhecimentos já pré-adquiridos, sempre com relação à teoria dos números. Ao final, é feita uma conexão entre a prática elaborada e executada e a teoria estudada. A seguir, colocaremos dois exemplos de jogos, retirados do livro Os desafios das escolas públicas paranaenses, de Nunes (2014, p. 12-13) referenciado no final desta apostila.

Quadro 2.1: Exemplos de jogos

a) A moeda falsa **Situação 1:** Em uma bolsinha estão 9 moedas idênticas, sendo que 8 delas têm o mesmo peso e uma moeda é mais leve que as demais, portanto, é falsa. Utilizando uma balança de dois pratos e sem pesos, quantas pesagens são suficientes para descobrir a moeda falsa? **Situação 2:** Um garoto possui 4 moedas idênticas, onde 3 têm o mesmo peso e uma é falsa, e assim pesa menos que as demais. Utilizando uma balança de dois pratos e sem pesos, quantas pesagens são suficientes para descobrir a moeda falsa? **Situação 3:** Uma menina possui 8 moedas de ouro idênticas, das quais sete têm o mesmo peso e uma pesa menos que as demais por ser falsa. Utilizando uma balança de dois pratos e sem pesos, quantas pesagens são suficientes para descobrir a moeda falsa? **Situação 4:** Um morador de rua pedindo esmolas, contabilizou ao final do dia 27 moedas idênticas de um real. Porém ficou sabendo que alguém de propósito lhe deu uma moeda falsa de um real e, por ser honesto, não queria passar esta moeda falsa para outra pessoa e assim tentou descobrir a sua procedência. Caso tivesse à disposição uma balança de dois pratos e sem pesos, quantas pesagens seriam suficientes para descobrir a moeda falsa?

Situação 5: Adriano tem sete moedas idênticas, porém, duas delas são falsas e pesam menos que as demais. Utilizando uma balança de dois pratos e sem pesos, quantas pesagens são suficientes para descobrir as duas moedas falsas?

b) Envolvendo operações básicas

Utilizando as peças de um dominó é possível fazer uma brincadeira interessante, que pode ser feita pelo professor em sala de aula com seus alunos, ou por alguém que queira impressionar os amigos. Bem, comece colocando todas as peças com as faces numeradas voltadas para baixo, e em seguida, embaralhe-as. Peça a um colega que escolha uma das peças sem que você veja quais são os algarismos da mesma. É possível com o auxílio de algumas continhas descobrir a peça que seu colega pegou. Para isto, peça a ele que escolha um dos algarismos da peça escolhida e multiplique por cinco, em seguida some três ao resultado da multiplicação.

Depois peça que multiplique o resultado obtido anteriormente por dois. Agora peça que some o outro algarismo da peça do dominó com o resultado da multiplicação anterior. Por fim, peça para seu colega dizer o resultado final. Deste resultado basta subtrair seis para descobrir os algarismos da peça escolhida pelo colega, já que o resultado desta subtração apresenta exatamente os dois algarismos que compõem a peça. Por exemplo, se o resultado final for 26, você faz a seguinte subtração $26 - 6 = 20$, isto significa que a peça escolhida tem os algarismos dois e zero.

Fonte: Nunes (2014, p. 12-13).

Como visto, os jogos matemáticos são uma forma de estimular o pensamento lógico, a criatividade e o raciocínio. Vale a pena sua utilização para aplicar conhecimentos matemáticos adquiridos!

ATIVIDADE

4 - Sobre a teoria dos Números, assinale qual alternativa está correta.

a) Possui três grandes áreas de estudo.
b) Tem se desenvolvido a partir dos tempos modernos.
c) Foi inventada por Pitágoras.
d) Sua aplicação pode se dar em qualquer área de nossas vidas.
e) Os jogos matemáticos não podem se relacionar de forma direta, no estudo da teoria dos números.

.

FIQUE POR DENTRO

Nesta unidade, vivenciamos diversas evoluções de pensamento. A jornada de uma ideia, desde a sua percepção até seus ajustes finais deve ser modelada de acordo com a realidade em que se vive. O aumento das necessidades do ser humano faz com que o conhecimento abra cada vez mais as portas. Por mais que inúmeras vezes, as propriedades trabalhadas aqui, como os múltiplos, os divisores, as equações, as teorias, entre outras áreas, sejam assustadoras vistas de longe, é preciso ter cautela e determinação, já que sem seus estudos e vivências não teríamos um chão seguro para pisar.

Para aprofundar seus conhecimentos, acesse o artigo: Equações Diofantinas Lineares: Um desafio motivador para os alunos do ensino médio. Disponível em: <https://sapientia.pucsp.br/bitstream/handle/11292/1/Wagner%20Marcelo%20Pommer.pdf>. Veja mais pelo site: <https://www.somatematica.com.br/coluna/gisele/25052001.php>.

REFLITA

Estou completamente envolvido com minha formação educacional? Em que esses conhecimentos podem me ajudar? Pense a respeito!

INDICAÇÕES DE LEITURA

Nome do livro: Princípios da Matemática para concursos vol 1: Múltiplos e divisores

Nome do autor: Jamerson Fernando Confort Martins

Editora: Ciência Moderna

ISBN: 9788539904556

Comentário: Para aqueles que pensam em prestar concurso, fica a indicação dos princípios da matemática. Mesmo que você não realize concursos, mas quer se aprofundar em múltiplos e divisores, este livro, possui uma aprendizagem sólida, organizado de forma clara e precisa.

Filme: O quarto de Fermat

Gênero: Suspense

Ano: 2007

Elenco Principal: Alejo Sauras, Elena Ballesteros, Lluís Homar e Pascal Santi Millán

Sinopse: A obra O quarto de Fermat apresenta uma história sobre quatro matemáticos que vão passar um fim de semana em um lugar da Espanha tentando solucionar desafios intelectuais, mas aos poucos o enigma fica ainda mais difícil, e coisas estranhas começam a acontecer, como paredes que começam a se mexer, a porta que é trancada e a sala encolhendo-se pouco a pouco.

UNIDADE III

Congruências

Valnira Oliveira

Introdução

Olá, aluno(a)! Bem-vindo(a) à terceira unidade de nosso material. A partir de agora estudaremos a respeito da congruência ou congruência módulo m, que é uma importante ferramenta da teoria elementar dos números. Esse fundamental conceito matemático tem diversas aplicações e foi desenvolvida, essencialmente, pelo matemático alemão Carl Friedrich Gauss (1777-1855). O matemático nomeou m como congruência, com base no fato de que o elemento a daria sempre o mesmo resto de b, quando dividido pelo m.

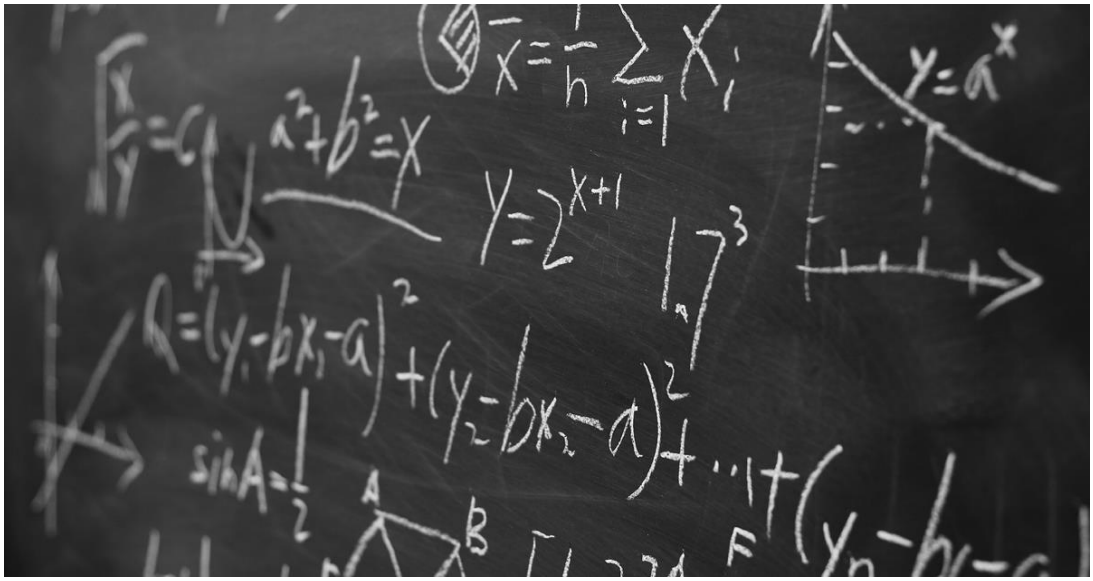
Quando estudamos alguns aspectos do conjunto dos números inteiros, deparamo-nos com o problema da divisão euclidiana (divisão com restos), conforme discutimos nas unidades anteriores. Tais conteúdos devem ser introduzidos já no Ensino Fundamental, assim como a congruência. Buscaremos apresentar algumas aplicações e propriedades básicas dessa área aritmética.

Exemplificando:

Dada a expressão:

27 31 (mod 4),

teremos o (mod 4), pois, se utilizarmos os princípios da teoria euclidiana de divisibilidade, nesse contexto, teremos tanto o 27 quanto o 31 deixando em suas divisões um resto 3, quando divididos por 4.



Fonte: Denis Ismagilov / 123RF.

PROPRIEDADES

O conteúdo relativo à álgebra modular pode ser estudado introduzindo relações de congruências a partir do conjunto dos números inteiros, que se encaixam, também, nas operações do anel dos inteiros, abrangendo três das operações básicas da matemática: a adição, subtração e multiplicação. De forma mais concreta, dizemos que um inteiro positivo chamado *n* terá dois elementos, que denominaremos *a* e *b*, ditos aqui como congruentes ou côngruos, escrito como módulo *n* ou em uma formula organizada:

a = b (mod n)

Quando a diferença entre *a* - *b* for um inteiro múltiplo de *n*, chamaremos o elemento *n* de modelo da congruência. Observe o exemplo abaixo:

Exemplificando:

38 = 2 (mod 12), pois 38 - 2 = 36, que é múltiplo de 12.

Podemos aplicar essa mesma regra, em relação aos números negativos:

-8 = 7 (mod 5)

2 = -3 (mod 5)

-3 = -8 (mod 5)

Caso os elementos *a* e *b* sejam ambos positivos ou ambos negativos, teremos *a* = *b* (mod *n*). Essa afirmação pode ser considerada se *a*/*n* e *b*/*n* possuir o mesmo resto. Colocando em números poderemos observar melhor, por exemplo, 38 = 14 (mod 12), em que os dois valores 38/12 e 14/12, possuem o mesmo resto, isto é, 2.

Veja, também, que 38 - 14 = 24, portanto, o resultado é um inteiro múltiplo de 12, o que entra em concordância com a definição inicial de relação em congruência.

Vale destacar que é muito comum a congruência possuir várias relações simultâneas com diferentes módulos e esses módulos são incorporados na notação. Mesmo se essa notação tiver quatro elementos, ainda assim a relação será fixada como binária. Isso precisa estar esclarecido se a notação $a \equiv_n b$ for utilizada, ao invés da tradicional.

As propriedades existentes nessa relação de congruência são as seguintes:

se, $a_1 = b_1 \pmod n$ e $a_2 = b_2 \pmod n$

então:

$a_1 + a_2 = b_1 + b_2 \pmod n$

$a_1 - a_2 = b_1 - b_2 \pmod n$

Observe que as propriedades descritas acima serão válidas se expandirmos a teoria e incluir nela os números reais.

Você deve estar se perguntando, mas onde está a operação de divisão, em todo esse processo da congruência? Pois bem, em congruências não se aplica divisões. Em seu lugar realiza-se uma multiplicação, em ambos os elementos, por algum número que não seja conveniente. Como qualquer número, na divisão por 1 deve restar 0, então, não é interessante, nem recomendado, utilizar o módulo 1, já que para qualquer *a* e *b* inteiro sempre existirá $a = b = 0 \pmod 1$.

CLASSES DE CONGRUÊNCIA

Todas as vezes em que houver uma relação de equivalência em um conjunto X, será possível definir uma parte P sobre esse mesmo X. Várias partes de P, que podemos chamar de subconjuntos X, é denominada (a coleção) de partição de X, evidentemente, se todos os elementos dessa coleção participarem de ambos conjuntos X e P. Os elementos de P são postos em pares e quando se unem formam, novamente, o conjunto X.

Já para se elaborar uma partição de Z, utilizando o método da congruência de módulo *m*, primeiramente será preciso definir para cada número inteiro a sua classe de equivalência, como se dá na expressão abaixo:

$$[a]_m = \{x \text{ e } Z;\ x = a \pmod m\}$$

Em casos que o número inteiro *m* já estiver subentendido sua presença, na expressão será utilizado apenas [a], que denota $[a]_m$. Com esses termos, o quociente do conjunto Z se dará pela relação $= \pmod m$ e a partição escrita por:

$Z/_{=(\text{mod } m)} = \{[a]_m; a \in Z\}$

Simplificando a expressão, podemos descrever $Z/_{=(\text{mod } m)}$ apenas como Z_m. Para conseguirmos enxergar essa partição de Z, podemos visualizar uma linha, em que são marcados todos os números inteiros, separando-os pela mesma distância. Logo após, para se ter a representação de Z_m, imagine essa linha sendo enrolada em volta de uma circunferência (infinitas vezes, já que esse é um exercício de imaginação, pois os números inteiros são infinitos). O zero será posto de forma que ocupe a mesma posição dos inteiros: … -2n, -n, n, 2n, 3n, ... Posteriormente à conclusão, poderemos pensar nos elementos Z_n como sendo os *n* pontos distribuídos sobre a circunferência que se formou. Veja o esquema a seguir, que ajuda nessa visualização:

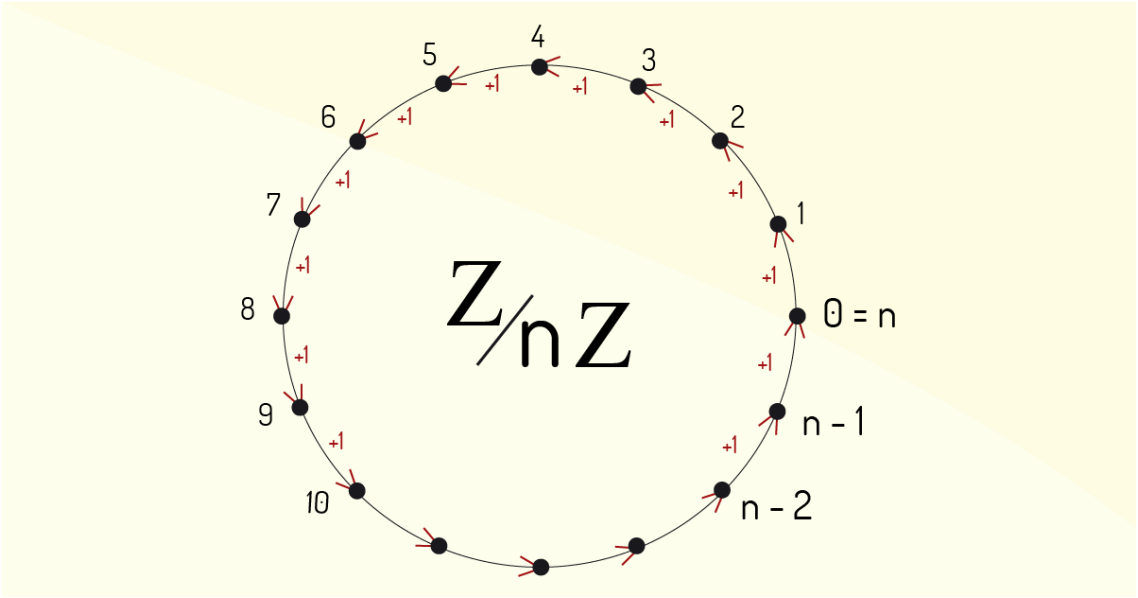


Figura 3.1 – Circunferência Z_n

Fonte: Elaborada pela autora.

Conforme representado anteriormente, cada ponto da circunferência representa uma equivalência de módulo *n*, isto é, são classes que ilustram o conjunto dos inteiros que estão sobrepostos naqueles pontos, dentro da circunferência criada. Agora, o que há de tão atrativo na participação dos números inteiros?

Bem, a grande vantagem de se dividir os números inteiros em classes de congruência que se tem, é a consequência que essas classes terão em ser mais compatíveis com as operações de adição e de multiplicação. Se essas classes forem compatíveis será possível definirmos em cada Z_m ainda mais operações de adição e multiplicação, ou seja, criar mais e novas operações. Para isso, devemos seguir o procedimento a seguir:

Quando fixado um inteiro *m* e dadas as classes [a] e [b], definimos:

[a] + [b] = [a + b]

[a] x [b] = [a x b] ou, para simplificar, ([a] [b] = [ab]).

Em outras palavras, temos a soma do produto das classes de congruência, elementos inteiros *a* e *b*, que é a classe da sua própria soma dos produtos. É essencial notar, também, de que forma a compatibilidade da congruência com as operações nos subconjuntos Z é usada. Podemos dar duas classes de equivalência: A = [a] = [a´] e B = [b] = [b´], que será similar a expressão [A] + [B], resultando em [a + b], [a´ + b], [a + b´] ou [a´ + b´]. Nesse caso, todas essas classes são equivalentes. Mais do que isso, definindo essas operações, os elementos (z_m, +, x) também se tornam um anel com unidade, ou seja, passam a valer as propriedades a seguir:

Z = {0, + ou - 1, + ou - 2, + ou - 3...} e Z_m = {mZ + 0, mZ + 1, ..., mZ + (m - 1) }

ATIVIDADE

1 - Com base nos estudos desta unidade e de seus conhecimentos adquiridos ao longo dessa trajetória, faça o que se pede:

A partir da propriedade MOD, ao observar três números que, somados a 16, tornam o resultado divisível por 6, podemos dizer que:

a) Os três números são 4, 10 e 20.
b) Os três números são 2, 8 e 14.
c) Os três números são 4, 6 e 8.
d) Os três números são 2, 10 e 12.
e) Os três números são 4, 8 e 10.

TEORIA DOS ANÉIS

Nos estudos voltados para a matemática do último século, as questões algébricas e numéricas, que tanto a marcavam, diminuíram, passando a se dedicar mais, de forma tendenciosa, para aquilo que é abstrato. Entre essa área, denominada de álgebra moderna, chama-se a atenção para a teoria dos anéis e dos ideais, pois são completamente abstratas, desde a sua origem. Trata-se de um conteúdo impensável na antiguidade, já que é totalmente moderno. Se pesquisarmos a fundo, encontraremos a maior parte dos estudos que se relacionam com os anéis desenvolvidos nos últimos 80 e 90 anos. Portanto, essa é, de fato, uma área que vem se desenvolvendo muito recentemente.

Em contrapartida, a teoria dos anéis teve sua origem em meados do século XIX, tendo, na verdade, poucos autores dedicados em estudar essa teoria moderna. O primeiro a iniciar os estudos foi Richard Dedekind (1831-1916), que foi o responsável por introduzir, em 1871, as noções de ideais, a fim de generalizar o teorema fundamental da matemática a um patamar mais abstrato. Em seguida, David Hilbert (1862-1945), Edmund Lasker (1868-1941) e Francis Sowerby Macaulay (1862-1927) contribuíram para o desenvolvimento de anéis e polinômios.

No entanto, quem, de fato, criou a teoria dos anéis foi Adolf Fraenkel (1891-1965), em seu trabalho, denominado “On the divisors of zero and the decomposition of rings” (Divisores de zero e a decomposição dos anéis). Nesse estudo, Fraenkel desenvolveu a primeira caracterização para as noções de anel que conhecemos e estudamos atualmente. Vale ressaltar que essas noções postas por ele, hoje servem apenas como critério histórico e não são mais estudadas, no entanto, naquele momento, foram muito importantes para o desenvolvimento dessa teoria. Seu real objetivo era de generalizar e amplificar os estudos dos corpos, a fim de obter uma teoria para ser aplicada aos módulos inteiros n e a desenvolver os sistemas conhecidos como números hipercomplexos.

A definição de anéis que embasa os estudos atuais teria surgido no século XX, mais precisamente em 1917, com o matemático japonês Masazo Sono, em sua obra “On congruences” (Em congruências).

Se falarmos em contribuição, quem mais fez pelo avanço das questões abstratas da matemática e da teoria dos anéis foi Emmy Noether (1882-1935). Seu artigo, “Ideal theory in rings” (Teoria ideal em Anéis), publicado em 1921, deu origem a teoria abstrata dos anéis. Nesse trabalho, a autora e matemática estende ainda mais os trabalhos de Hilbert, Lasker e Macaulay sobre os anéis de polinômios e, na sequência, ainda evolui conceitos de anel abstrato que Dedekind havia realizado para anéis de números algébricos.

Essa revolução em trabalhar com os modos abstratos da aritmética nas áreas dos anéis e ideais levou a um contexto de estudo da fatoração prima e acabou, por consequência, criando o que hoje chamamos de álgebra comutativa. Na década de 30, todas essas ideias foram organizadas e postas à disposição da nova geração de pesquisadores, estudiosos e matemáticos que vinham pela frente, a fim de desvendarem e evoluírem esse lado abstrato.

Questões fundamentais como, por que (-1) + (-1) = 1 e $a \cdot 0 = 0$, são pontos relevantes e objetos centrais de estudo que fazem parte da justificação dessas áreas abstratas de estudo, conduzindo aos conceitos de anel e domínio de integridade.

ANÉIS

Quando pensamos na teoria dos números vemos que a matemática faz parte de toda nossa vida e está ligada diretamente ao nosso cotidiano, seja ele qual for, desde o início dos tempos. Recorremos aos números para descrevermos e planejarmos boa parte das ocorrências de nosso dia.

Quando realizamos uma conta simples, utilizamo-nos, por exemplo, de números naturais. Quando cortamos um bolo fazemos uso de frações ou números racionais, medimos distâncias, tamanhos, contabilizamos prejuízos, enfim, se prestarmos atenção estamos mais que familiarizados com os diversos conjuntos numéricos existentes. Podemos então, relacionar os conjuntos, da seguinte maneira:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Enfatizamos que, conforme vimos anteriormente, já estamos acostumados, em nosso dia a dia, a lidar com esses números e conjuntos. Ainda que não saibamos seus conceitos, não são estranhos para nós e temos condições de perceber que cada um desses conjuntos numéricos estão inseridas em operações de adição e de multiplicação, possuindo diversas propriedades.

Diante disso, no próximo tópico introduziremos o estudo de estruturas algébricas, baseando-se nos conceitos sobre a teoria dos anéis e seus domínios.

CONCEITO DE ANEL

Podemos definir anel $(A, +, \cdot)$, como um conjunto A, que tem duas operações binárias, em que as denotaremos de + e $\cdot$, sendo que esse anel pode ser descrito da seguinte forma:

(1) (A, +) é um grupo abeliano

(2) é associativa; isto é,

$$(a \cdot b) \cdot c = a \cdot (b \cdot c), \text{ para quaisquer } a, b, c \in A$$

(3) é distributiva relativamente a +; ou seja,

$$a \cdot (b + c) = a \cdot b + a \cdot c, \text{ e,}$$

$$(b + c) \cdot a = b \cdot a + c \cdot a, \text{ para quaisquer } a, b, c \in A.$$

Utilizaremos a denotação A, simplesmente para falar sobre um anel arbitrário $(A, +, \cdot)$. Se observarmos esse anel A, considerando-o como comutativo, então, juntamente com o elemento $\cdot$, devemos chamá-lo de anel com identidade ou, também, de anel unitário. Mostraremos no quadro a seguir algumas notações adicionais:

Quadro 3.1 – Notações de anéis

Designação	**Notação**	**O que representa**
Zero do anel	0	Neutro de +

Simétrico de a ∈ A	-a	inverso de a no grupo (A, +)
Múltiplo de a ∈ A	na	a + a + · · · + a (n ∈ Z parcelas)
Identidade do anel	1	neutro de ·, caso exista
Inverso de a ∈ A	a^{-1}	inverso de a em (A, ·), caso exista
Potência de a ∈ A	a n a - n	a · a · · · · · a (n ∈ Z + fatores) $a^{-1} \cdot a^{-1} \cdot \cdot \cdot \cdot \cdot a^{-1}$ (n ∈ Z + fatores)

Fonte: Adaptado de Waerden (1931).

Apresentaremos, a partir de agora, a composição algébrica de anel e, também, a exemplificaremos.

Temos conhecimento de diversos tipos de conjuntos, todos variáveis, certo? Internamente a cada conjunto, estão definidas as operações de adição e de multiplicação entre seus membros. Essas operações apresentam, também, propriedades únicas. Vamos relembrar algumas delas a seguir:

- os n´números naturais N = {0, 1, 2, 3, . . .};
- os polinômios com coeficientes reais, denotados por R[x];
- as matrizes Mn×n ®;
- os números inteiros Z = {. . ., −3, −2, −1, 0, 1, 2, 3, . . .};
- os números racionais Q = {m| n, m ∈ Z e n 6 diferente de 0};
    - N
- os números reais R;
- os números complexos C = {a + bi | a, b ∈ R e $i^2 = -1$}.

Os conjuntos dos números inteiros, racionais e reais podem ser equiparados, também, com uma relação com ordem ≤. Observemos que nas operações de adição e de multiplicação, a ordenação e suas propriedades relacionam-se com as características gerais dos números inteiros.

Retomando a definição que fizemos no início deste tópico, um anel A é um conjunto que tem operações de adição (+) e de multiplicação (·). Essas operações apresentam as seguintes propriedades:

A1 (Associativa). Para qualquer a, b, c ∈ A, teremos (a + b) + c = a + (b + c).

A2 (Comutativa). Para qualquer a, b ∈ A, teremos a + b = b + a.

A3 (Existência de um elemento neutro para a adição). Existe, então, θ ∈ A, tal que a + θ = θ + a = a, para todo a ∈ A.

A4 (Existência de simétrico). Em cada a ∈ A, que houver a ′ ∈ A, tal que a + a ′ = a ′ + a = θ.

M1 (Associativa). Para qualquer a, b, c ∈ A, teremos (a · b) · c = a · (b · c).

AM (Distributiva). Para qualquer a, b, c ∈ A, teremos a · (b + c) = a · b + a · c e (a + b) · c = a · c + b · c.

Exemplificando:

Consideremos um intervalo I = (-1, 1), sendo F (I) o conjunto de todas as funções de I em R, ou seja:

$$F(I) = \{f: I \to R \mid f \text{ é uma função}\}$$

Para qualquer elemento de f, g ∈ F (I), as operações comuns de adição e de multiplicação de funções são determinadas por:

$$(f + g)(x) = f(x) + g(x), \text{ para todo } x \in I \text{ e}$$
$$(f \cdot g)(x) = f(x) \cdot g(x), \text{ para todo } x \in I$$

Dadas essas operações, podemos concluir que F (I) é um anel.

PROPRIEDADES ELEMENTARES

Como algumas propriedades elementares dos anéis, tem-se a unicidade de um elemento neutro aditivo, além do simétrico e, também, casos em que se tenha o elemento neutro multiplicativo.

Então, considerando um anel A, teremos as opções:

(i) O elemento neutro aditivo é único.

(ii) O elemento neutro multiplicativo, se existe, é único.

(iii) O simétrico é único.

Exemplificando:

(i) No primeiro caso, consideramos θ e θ' como elementos neutros aditivos do anel A. Portanto, descreveremos:

$$\theta = \theta' + \theta = \theta'$$

Observamos a primeira igualdade originada do fato de θ' ser um elemento neutro da adição e, na sequência, a segunda proveniente de θ ser um neutro da adição. Desse modo, temos a conclusão de que $\theta = \theta'$ e o elemento neutro aditivo é único.

(ii) No segundo caso, daremos um anel A, com unidades *e* e *e′*. Teremos, então:

$$e = e' \cdot e = e'$$

Aqui, a primeira igualdade deve-se ao fato de *e´* ser uma unidade, assim como a segunda. Temos, portanto, $e = e'$ e o elemento neutro multiplicativo é único.

(iii) No terceiro caso, veremos $a' \in A$ e $a'' \in A$ simétricos de $a \in A$. Assim, teremos:

$(\theta = a + a'', \theta = a' + a)$ e $(a' = a' + \theta = a' + (a + a'') = (a' + a) + a'' = \theta + a'' = a'')$

Com isso, a terceira igualdade terá uma associação da adição. Então, a simetria dessa expressão será única.

Desse modo, a partir da unicidade do elemento neutro aditivo, do simétrico e do neutro multiplicativo, quando ele aparece, denotaremos daqui pra frente um anel A, com propriedades elementares, sendo:

- o elemento neutro da adição pelo símbolo 0;
- o simétrico de *a* pelo símbolo -*a*;
- a unidade ou elemento neutro multiplicativo, se existe, pelo símbolo 1.

Além disso, devemos descrever a expressão, a - b = a + (-b) e a nomearemos de subtração.

DOMÍNIO DE INTEGRIDADE

Podemos definir domínio de integridade como um próprio anel de integridade ou comutativo, com unidade e sem divisores de zero. Um anel Z tem propriedades que, de maneira geral, um anel comum não tem.

Considerando um elemento não nulo “a”, em um anel comutativo A, é chamado um divisor de zero caso exista um elemento não nulo “b” em A, de modo que ab = 0.

Dessa maneira, quanto tiver um anel comutativo, com unidade, será chamado de domínio integral ou, de forma mais simples, apenas de domínio, caso não tenha nenhum divisor de zero. Assim, um domínio integral pode ser representado pela expressão: ab = 0 $\Leftrightarrow$ a = 0 ou b = 0.

ATIVIDADE

2 - Após o estudo da Teoria dos Anéis e os conhecimentos adquiridos ao longo dessa trajetória, analise as alternativas e julgue a única correta.

a) O conjunto dos números inteiros **(Z)** não é Anel.
b) O conjunto dos números inteiros **(Z)** é Anel.
c) $12 \equiv 5 (mod 3)$, pois 12 - 5 = 7. Então, dizemos que 12 é côngruo a 5.
d) $11 \equiv 5 (mod 3)$, pois 11 - 5 = 6 = 2*3. Então, dizemos que 11 não é côngruo a 5.
e) $7 \equiv 15 (mod 2)$, pois 7 - 15 = -8 = 2*-4. Então, dizemos que 7 não é côngruo a 15.

CORPOS

Podemos definir os anéis Z e Q como domínios de integridade ou anéis de integridade. Entretanto, enquanto no anel dos inteiros apenas os elementos 1 e -1 são simétricos e multiplicativos, nos anéis de números racionais todos os elementos que não sejam nulos podem admitir a simetria e a multiplicação. Portanto, podemos definir um anel K, comutativo com unidade, como corpo, isso se todos os elementos não nulos desse conjunto K também admitirem ser simétricos multiplicativos, isto é:

$$\forall\ a \in K,\ a \neq 0,\ \exists\ b \in K;\ a * b = 1$$

Nota: O *b* que aparece na definição de corpo também é chamado de oposto de *a* e descrito como a^{-1}. Em um anel com unidade, indicaremos a denotação U (A) como subconjunto de A, elaborado pelos membros que possuem simétrico multiplicativo (inverso). Damos o nome a esses elementos de invisíveis. Desse modo, um corpo definido por K é, de fato, um anel comutativo com unidade, de modo que $U(K) = K* = K - \{0K\}$.

Exemplificando:

As letras Q, R e C são os exemplos mais conhecidos de corpos. O teorema que explicitaremos diz que, se for finito, corpos e domínios passam a ser os mesmos, ou seja, se D for um domínio do tipo finito, D também se tornará um corpo.

Se D é um domínio, logo D será um anel comutativo com unidade. Dessa forma, só resta provar que todos os elementos não nulos também podem ser invertidos. Portanto, seja a ≠ 0 um dos elementos de D, sendo esse conjunto finito, a sequência de a, a2, a3, a4... irá se repetir, ou seja, existe um i > j, tal que a i = a j. Assim, pela lei do cancelamento, a j (a i - j - 1) = 0 e como a ≠ 0, temos que a i - j = 1. Se i - j = 1, a = 1 e, portanto, se inverte.

PROPRIEDADES DOS CORPOS

Consideramos K como um conjunto qualquer e, nele estão definidas operações binárias, adição e multiplicação, denotadas com os símbolos ++ e xx, respectivamente. Dizemos que KK, inserida a essas operações, constituirá um corpo quando se tiver as seguintes propriedades:

(1) Propriedades da adição:

(a) Propriedade comutativa: $\forall \alpha, \beta \in K: \alpha + \beta = \beta + \alpha \forall \alpha, \beta \in K: \alpha + \beta = \beta + \alpha$

(b) Propriedade associativa: $\forall \alpha, \beta, \gamma \in K: (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ $\forall \alpha, \beta, \gamma \in K: (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$

(c) Existência de elemento neutro: $\exists 0 \in K: 0 + \alpha = \alpha, \forall \alpha \in K \exists 0 \in K: 0 + \alpha = \alpha, \forall \alpha \in K$

(d) Existência de simétricos: $\forall \alpha \in K, \exists - \alpha \in K: \alpha + (-\alpha) = 0$

(2) Propriedades da multiplicação:

(a) Propriedade comutativa: $\forall \alpha, \beta \in K: \alpha\beta = \beta\alpha \forall \alpha, \beta \in K: \alpha\beta = \beta\alpha$

(b) Propriedade associativa: $\forall \alpha, \beta, \gamma \in K: (\alpha\beta)\ \gamma = \alpha\ (\beta\gamma)$ $\forall \alpha, \beta, \gamma \in K: (\alpha\beta)\ \gamma = \alpha\ (\beta\gamma)$

(c) Existência de elemento neutro: $\exists 1 \in K \setminus \{0\}: 1\alpha = \alpha, \forall \alpha \in K \exists 1 \in K \setminus \{0\}: 1\alpha = \alpha, \forall \alpha \in K$

(3) Propriedade (distributiva) de ligação:

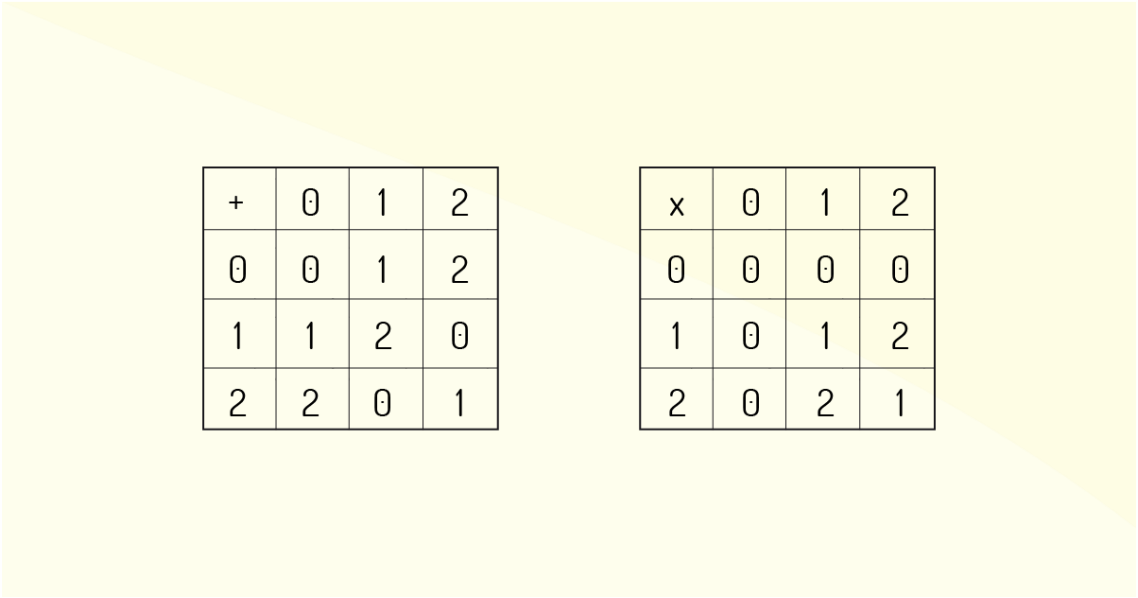
$\forall \alpha, \beta, \gamma \in K: (\alpha + \beta)\ \gamma = \alpha\gamma + \beta\gamma$

Exemplificando:

Um dos exemplos mais comuns de corpos é o conjunto RR, dos números reais, com as operações comuns de adição e de multiplicação. Também é um corpo o conjunto QQ, dos números racionais, com operações habituais. E, por fim, o conjunto CC, dos números complexos, com operações habituais.

Quando dizemos que serão considerados corpos apenas os números reais, subentende-se que serão observadas somente as operações usuais, mas nelas se incluem os números racionais e complexos, já que estamos falando dos reais.

Porém, é possível definir inúmeros outros corpos. Poderíamos elaborar um corpo, por exemplo, a partir do conjunto K = {0, 1, 2} K = {0, 1, 2}, estabelecendo as duas operações de adição e de multiplicação, a partir das figuras apresentadas:



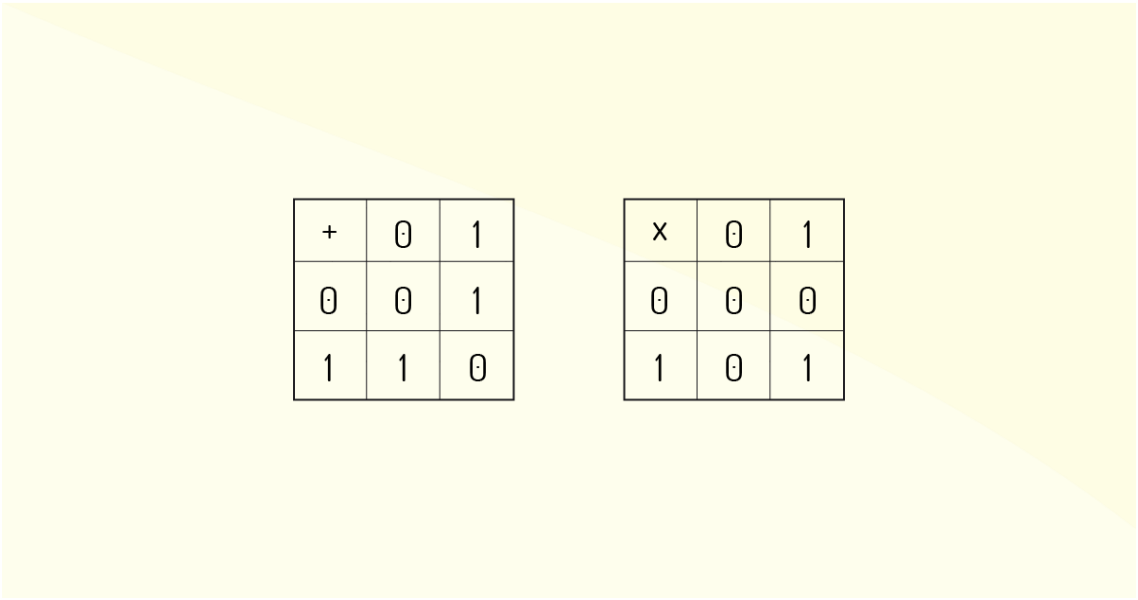
+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Figura 3.2 – Operações de adição e de multiplicação

Fonte: Garcia (2003, p. 65).

A propriedade 2 - c, conforme definição vista anteriormente, demonstra que um corpo só será, de fato, corpo, se tiver, no mínimo, dois elementos diferentes. Mas, vemos que, mesmo com um conjunto simples de dois elementos, será possível a construção de um corpo, sendo K = {0, 1} K = {0, 1}. Para esse exemplo, observemos as seguintes figuras:



+	0	1
0	0	1
1	1	0

x	0	1
0	0	0
1	0	1

Figura 3.3 – Corpos com dois elementos
Fonte: Garcia (2003, p. 66).

Veja que na figura 3.3 temos a construção do corpo, primeiramente, pela propriedade da adição e, em seguida, pela propriedade da multiplicação. Observe que ambas as propriedades apresentam dois elementos distintos, ou seja, encontramos nas duas figuras os números zero e um.

A seguir, veremos os subanéis.

SUBANÉIS

Resumidamente, podemos definir um subanel (de acordo com o nome sub) como um subconjunto não vazio denominado S, baseado em um anel (R, +, ·). Dizemos que R pode ser um subanel se nas operações induzidas pelas operações de R (restrições) existir o subanel S que, nesse caso, seria um anel também.

Em suma, a partir desse teorema, um subconjunto $S \neq \emptyset$ de um anel (R, +, ·) será um subanel de R se as seguintes afirmações forem contempladas:

(i) Para todo a, $b \in S \rightarrow a - b + (-b) \in S$

(ii) Para todo a, $b \in S \rightarrow a \cdot b \in S$

(→) Se S ⊆ R é um subanel, logo em todos os elementos a, b ϵ S, teremos -b ϵ S e a ϵ S. Então, a - b ϵ S, pois + é uma operação binária em S e, a · b ϵ S, pois · é uma operação em S.

(←) Sejam + |S: S × S → R e · |S: S × S → R, como restrições de + e · à S, a condição (ii) implica que → · |S: S ×S → S, i · é, · | S é uma operação em S., porém, ainda teria:

• 0 ϵ S, pois S ≠ Ø → ∃ a ϵ S (i) → = 0 = a - a ϵ S.

• para todo b ϵ S → -b ϵ S, pois para b ϵ S, como 0 ϵ S

Como a associação de +, a comutação de + e a associação e distribuição valem em R, teremos, também, essas propriedades ativas em S, que é seu subconjunto. Desse modo, (S, +, ·) torna-se um anel, provando que S é subanel de R.

Exemplificando:

• Em termos numéricos, o conjunto dos múltiplos de 2, 2Z é um subanel de Z, valendo-se da mesma regra, com as operações de adição e de multiplicação de inteiros usuais.
• Em geral, (nZ, +, ·) é um subanel de (Z, +, ·) para qualquer inteiro positivo n.
• 2Z será um subanel de Z. Embora, comumente, n Z ⊆ Z são subanéis, para todo n ≥ 0.

É certo que, para todo a, b ϵ n Z → a = nk1, b = nk2, com k1, k2 ϵ Z. Assim, a - b = n (k1 - k2) ϵ n Z e a · b = n (k1 k2 n) ϵ n Z. Se analisarmos R = Z6, teremos:

S1 = {0, 2, 4} e S2 = {0, 3} são subanéis de Z6, pois 2 · 4 = 2, -2 = 4;

3 = -3, 3 · 3 = 3.

Veja que 1R = 1, 1S1 = 4, 1S2 = 3. Dessa forma, Si ⊆ R são subanéis com 1, tais que:

1Si ≠ 1R, para i = 1, 2.

{0} e R são sempre subanéis de R, denominados como subanéis **triviais**.

Z ⊆ Q ⊆ R⊆ C é, portanto, uma fileira de subanéis.

Outra propriedade dos subanéis é que a unidade de um anel não necessariamente é a do subanel. Vejamos, por exemplo, o anel Z12 e seu subconjunto B = {0; 3; 6; 9}. Verificamos, de forma simples, que para cada x ϵ B e cada y ϵ B, tem-se um x - y ϵ B e um x. y ϵ B. Portanto, B é um subanel de Z12.
Veja, agora, que 9 . 3 = 3, 9 . 6 = 6 e 9 . 9 = 9. Então, se denotarmos 1B = 9, teremos 1B . x = x, ∀ x ϵ B. Como esse caso é comutativo, teremos que 1B = 9 é um elemento de unidade da multiplicação em B. Assim, B torna-se um subanel comutativo com unidade, mesmo que seu elemento unidade não seja a mesma que o anel Z12.
Considerando (A, +, ·) e S, ∅ um subconjunto de A, S será um subanel de A somente se S for fechado com relação a subtração e a multiplicação de A. Ou seja, somente se x - y ∈ S e x · y ∈ S para quaisquer x, y ∈ S .

OS AXIOMAS

Dentro da teoria dos anéis e dos subanéis é possível identificarmos sete axiomas. A seguir, demonstraremos a definição de cada um deles:

A1. Como na operação de adição há uma associação entre A, $S \subset A$ e consideramos S como fechado para a operação de adição, então, A continuará associando-se com S. Basicamente, podemos dizer que o S herda a adição de A.

A2. De maneira parecida, *S* herda, também, a comutatividade da adição de *A*.

A3. O elemento zero está em *S*. As propriedades do zero, então, são naturalmente herdadas de *A*.

A4. O elemento de simetria está em *S*. Logo, as propriedades dele também são herdadas de *A*.

A5. Como *S* é fechado com respeito à multiplicação, *S* herda a associatividade da multiplicação de *A*.

A6. Da mesma forma, *S* herda de *A* a comutatividade da multiplicação.

A7. Já que *S* é fechado pelas duas operações, então, *S* herdará a propriedade distributiva de *A*.

ATIVIDADE

3) Em relação aos grupos, corpos e subanéis, assinale a alternativa correta.

a) um grupo tem duas propriedades fundamentais, Associatividade e Elemento Neutro.
   Justificativa: Falsa. Entre outras propriedades, um grupo tem três propriedades fundamentais, Associatividade, Elemento Neutro e Inversos.

b) Podemos definir subanel como um subconjunto vazio denominado S.
   Justificativa: Falsa. Podemos definir subanel como um subconjunto não vazio denominado S.

c) A essência por trás da Teoria dos Grupos é tomar dois elementos de um conjunto, combinar eles de alguma maneira e retornar um terceiro elemento do mesmo conjunto e é esse o papel das operações binárias.
   Justificativa: Falsa. O objetivo principal dessa teoria é fazer com que dois elementos de um conjunto combinem-se.

d) As letras Q, R e S são os exemplos mais conhecidos de corpos.
   Justificativa: Falsa. Os exemplos mais conhecidos são Q, R e C, ao invés de S.

e) Na teoria dos anéis e subanéis existem até sete axiomas.
   Justificativa: Verdadeira. Dentro da teoria existem sete axiomas.

IDEAIS

Os ideais foram propostos, primeiramente, por Dedekind, em 1876, de forma generalizada, pois, um matemático chamado Ernst Kummer, já havia contemplado algo sobre essa área. Alguns anos mais tarde, essa teoria foi ainda mais expandida por David Hilbert e Emmy Noether.

Na teoria dos anéis, ramo já abordado nos tópicos anteriores, um ideal é, na verdade, um subconjunto diferenciado de um anel. O conceito amplia, de forma apropriada, algumas propriedades muito importantes dos números inteiros, como “número par” e “múltiplo de 3”.

Por exemplo, na teoria dos anéis, os ideais são estudados como primos. Ao invés de números primos, em que se definem ideais coprimos como uma generalização dos algarismos coprimos e, também, pode-se provar um teorema de resto para ideais. Dedekind criou seus domínios e foi considerado uma importante classe dos anéis. Os ideais poderiam até mesmo imitar esses domínios, originando uma versão atualizada do teorema fundamental da aritmética. Nesses anéis, todos os ideais não nulos, podendo ser descritos como produtos únicos de ideais primos.

Um ideal também pode ser utilizado na construção de um anel quociente, da mesma maneira que um subgrupo normal é utilizado na elaboração de um grupo quociente.

Assim, podemos definir ideal a partir da lógica em que seja o conjunto R um anel com $(R, +)$ e, sendo o grupo abeliano desse anel um subconjunto I de R, é chamado ideal à direita se cumprirem tais afirmações:

- $(I, +)$ é um subgrupo de $(R, +)$
- xr está em I para todo x em I e todo r em R

Igualmente, será reconhecido e nomeado como ideal **à esquerda** se:

- $(I, +)$ é um subgrupo de $(R, +)$
- rx está em I para todo x em I e todo r em R

Se observarmos, os ideais que estão à esquerda em R são os mesmos que estão à direita do anel oposto R^{op} e vice-versa. Concluímos, desse modo, que quando R for um anel comutativo, as noções de ideal à esquerda e à direita coincidirão e, se o ideal for bilateral, não precisaremos nomeá-lo esquerda ou direita, apenas chamá-lo de ideal.

Os subconjuntos {0} e *R* de um anel *R* são ideais.

Chamamos de ideal próprio, se o conjunto de R também for próprio. Por sua vez, será chamado de Ideal gerado, caso A seja um conjunto qualquer de R.
O ideal estará bem definido quando a interseção dele com os conjuntos (não vazia, porque {\displaystyle A\subset R\,}) de todos os ideais que estão em *A* (que na interseção seja descrito por <A> ou (A)), for compreendido com todas as somatórias finitas da forma apresentada a seguir:

$$r_1a_1 + \cdots + r_na_n$$

com cada r_i em *R* respectivamente e cada a_i em *A*.

TIPOS DE IDEAIS

Os ideais são importantes, pois aparecem como centros dos homomorfismos (que veremos mais à frente) e, também, permitem definir os anéis quocientes. Existem diversos tipos de ideais analisados, uma vez que cada tipo gera distintos anéis quocientes. A seguir, veremos alguns deles:

- **Ideal maximal**: um ideal *I* será denominado de **ideal maximal** quando não existir outro ideal próprio *J*, tal que *I* é um subconjunto de *J*. O anel quociente dele será um corpo.
- **Ideal primo**: um ideal *I* será denominado de **ideal primo** quando, para qualquer *a* e *b* em *R* e *ab* em *I*, ao menos um (*a* ou *b*) estiver em *I*. O anel quociente de um ideal primo será um domínio de integridade.
- **Ideal primário**: um ideal *I* é chamado **ideal primário** caso, para qualquer *a* e *b* em *R* e *ab* em *I*, ao menos um (*a* ou b^n) estiver em *I*, para algum número natural *n*. Todo ideal primo é primário.

- **Ideal principal**: será chamado de ideal principal quando ele for gerado por algum elemento.
- **Ideal primitivo**: é o ideal que anula um módulo simples à esquerda. Um ideal primitivo à direita também é definido de forma similar. Perceba que, apesar do nome, ideais primitivos à direita e à esquerda serão sempre ideais bilaterais. Anéis quocientes construídos com ideais primitivos são anéis primitivos.
- Veremos, na sequência, um pouco mais sobre alguns deles.

Ideal Maximal

Dado um ideal M 6 = A, o anel A denomina-se maximal se, em qualquer ideal I de A, a propriedade M ⊆ I implicar I = M ou I = A.

Exemplificando:

Aplicado no anel dos inteiros Z, (0) e (10) não são maximais:

(0) ⊂ (10) ⊂ (5) ⊂ Z.

Em contrapartida, (5) é maximal:

(5) ⊆ (m) ⊆ Z ⇔ m|5 ⇒ m = 1 ou m = 5 ⇔ (m) = Z ou (m) = (5).

Por fim, teremos: o elemento A como um anel comutativo com identidade e I um ideal de A.

Logo:

(a) A/I é um domínio de integridade se e, só se, I for primo.

(b) A/I é um corpo se e, só se, I for maximal.

(c) Todo o ideal maximal de A é primo.

Ideal Primo

O ideal primo define-se por ser um subconjunto de um anel que tem inúmeras propriedades em comum com as de um valor primo dos anéis inteiros. Para esses anéis inteiros, os ideais primos são conjuntos que apresentam todos os múltiplos de qualquer elemento primo dado, juntamente com o nulo.

Em suma, podemos afirmar que os ideais primitivos são primos e ideais primos são simultaneamente primários, além de se enquadrarem como semiprimos.

Exemplificando:

- Se R descreve o anel C [X, Y] dos polinômios em dupla variável com coeficientes complexos, então, o ideal gerado pelo polinômio $Y^2 - X^3 - X - 1$ é um primo.
- No anel Z [X] dos polinômios com coeficientes inteiros o ideal criado por 2 e X é, também, um ideal primo. Ele baseia-se em todos os polinômios cujo termo constante é par.
- Em qualquer anel R um ideal maximal é um ideal M, que é classificado assim no conjunto de todos os ideais próprios de R, ou seja, M está embutido em exatamente dois ideais de R, sendo eles o próprio M e o anel completo R. Na prática, todo ideal maximal é primo, também. Em um domínio de ideais principais, todo ideal primo não nulo é maximal, mas, de forma geral, isso não é autêntico.
- Se M é uma variedade suave, R é o anel de funções reais suaves sobre M e x é um ponto de M. Com isso, o conjunto de todas as funções suaves f forma um ideal primo (e, também, um ideal maximal) em R.

Cabe informar, também, que a utilidade prática dos ideais primos dá-se na área da geometria algébrica, em que as variedades são determinadas como conjuntos nulos de ideais em anéis de polinômios.

Em uma abordagem moderna, que se prega o abstratismo, inicia-se com um anel comutativo arbitrário e, a partir dele, transforma-se em um conjunto de seus ideais primos, também denominado de seu espectro. A partir disso, define-se uma série de generalizações e de variações, que são chamadas de esquemas, sendo aplicadas não somente na geometria ou nesses conteúdos abstratos, mas, também, na teoria dos números.

A entrada desses ideais primos, na teoria da álgebra, foi um avanço grandioso. Naquele momento, percebeu-se que a propriedade da fatoração única expressada no teorema fundamental da matemática não se aplicava em todo anel de inteiros algébricos, mas foi encontrado seu substituto à altura, quando Dedekind trocou elementos por esses ideais primos.

Ideal Principal

Podemos definir um ideal principal como aquele que é gerado por um elemento. Esse ideal apresenta três denominações distintas:

- ideal principal à esquerda: {\displaystyle Ra = {ra|r\in R}\,} Ra = ra / r E R
- ideal principal à direita: {\displaystyle aR = {ar|r\in R}\,} aR = aR / r E R
- ideal principal bilateral: {\displaystyle I = {e_{1}ad_{1}+e_{2}ad_{2} + \ldots +e_{n}ad_{n}|e_{1},d_{1},e_{2},d_{2},\ldots ,e_{n},d_{n}\in R}\,}I = e1 ad1 + e2 ad2 + ... + en adn ...

No caso comutativo, o principal dá-se por um conjunto na representação aR = aR / r E R. Em Z, é simples demonstrar que todo ideal, na verdade, também é principal, mas isso não se valida em todos os casos. Podemos perceber isso ao analisar quando um ideal é criado por {2, *x*} no domínio de integridade {\displaystyle \mathbb {Z} [x]\,}Z [x] dos polinômios de coeficientes inteiros.

HOMOMORFISMO DE ANÉIS

A partir de agora, estudaremos a definição de homomorfismos. Esse conceito matemático diz respeito a aplicações, com o intuito de fazer comparações de estruturas algébricas de mesma origem. Os termos utilizados no homomorfismo são, em sua base, muito parecidos com os utilizados na teoria dos grupos. Tem-se um núcleo, uma imagem, além dos teoremas de isomorfismos, entre outras propriedades.

Podemos descobrir muitas informações e dados sobre anéis observando sua interação com outros anéis. No entanto, isso só é possível através dos homomorfismos. O homomorfismo é, portanto, uma ferramenta que preserva as operações soma e multiplicação dos anéis.

Definição: um homomorfismo representado por φ, de um anel R, em um anel S, é uma aplicação de R em S, que preserva, como dito, as operações de um anel. Ou seja:

$$\Phi (a + b) = \varphi (a) + \varphi (b)$$

$$\Phi (ab) = \varphi (a) \cdot \varphi (b)$$

Quando se tem um homomorfismo de anéis injetivo e sobrejetivo, ele passa a ser denominado isomorfismo de anéis. Nesse caso, podemos dizer que R e S são isomorfos. Veja que na definição apresentada anteriormente, as operações do lado esquerdo do sinal igualitário são as de R, já as do lado direito são de S. Quando se tem um isomorfismo $\varphi : R \rightarrow S$ isso mostra que R e S são, em linguagem algébrica, idênticos e similares.

Exemplificando:

De forma geral, se I é um ideal de um anel R, a ferramenta que faz a associação para cada elemento r de R a sua classe r + I, chama-se homomorfismo de anéis ou, nesse caso, homomorfismo canônico.

Seja φ: R [x] → R, que se associa a f (x) 7- → f (1), então φ é um homomorfismo sobrejetivo, já que:

$$\Phi (f + g) = (f + g) (1) = f (1) + g (1) = \varphi (f) + \varphi (g)$$

$$\Phi (f \cdot g) = (f \cdot g) (1) = f(1) \cdot g (1) = \varphi (f) \cdot \varphi (g)$$

Para todo $a \in R$, a = f (1), em que f (x) = $a \in R$ [x]. Isso prova, definitivamente, que φ é sobrejetivo.

PROPRIEDADES DOS HOMOMORFISMOS

Considerando φ um homomorfismo de um anel R sobre um anel S, então, teremos as seguintes propriedades:

1. φ (0) = 0
2. Φ (-r) = -φ(r) para todo r em R.
3. Para todo r em R e todo inteiro positivo n, φ (nr) = nφ (r) e φ(r n) = φ(r) n
4. Se A for um subanel de R, então, φ (A) será um subanel de S.
5. Se I for um ideal de R e φ é sobrejetivo, então, φ (I) será um ideal de S.
6. Se J for um ideal de S, então, φ -1 (J) será um ideal de R.
7. Se R for comutativo, então, φ (R) será comutativo.
8. Se R tiver unidade 1 e φ é sobrejetivo, então, φ (1) será a unidade de S, se S for não nulo.
9. φ será um isomorfismo somente se φ for sobrejetivo e ker φ = {r ∈ R|φ(r) = 0} = {0}.
10. Se φ for um isomorfismo de R sobre S, então, φ -1 será um isomorfismo de S sobre R.

Exemplificando:

1. Aplicando φ a expressão 0 + 0 = 0 teremos φ(0 + 0) = φ(0) e, assim, φ(0) + φ(0) = φ(0). Isto é, 2φ(0) - φ(0) = 0 e, finalmente, φ(0) = 0.
2. Aplicando φ a expressão r + (-r) = 0 teremos que φ(r) + φ(-r) = φ(0) = 0. Juntando os dois lados -φ(r) teremos que φ(-r) = -φ(r), conforme procuramos comprovar.
3. φ(nr) = φ(r + r + r +...r) = nφ(r) e φ(rn) = φ(rr...r) = φ(r) n, pela definição de homomorfismo.
4. Sejam x, y ∈ φ(A), então, x = φ(a1) e y = φ(a2), de modo que a1 e a2 estão em A. Pela prova, basta demonstrar que x - y ∈ φ(A) e xy ∈ φ(A). Mas x - y = φ(a1) - φ(a2) = φ(a1 - a2) ∈ φ(A), pois A é um subanel. Por motivo semelhante, xy = φ(a1) φ(a2) = φ(a1a2) ∈ φ(A).

5. Como I é um subanel, com base no item anterior, φ(I) já é um subanel de S. Só falta provar que S . φ(I) ⊂ φ(I). Como φ é sobre todo s, em S, é da forma s = φ(r) para algum r, em R. Assim, sφ(a) = φ(r) · φ(a) = φ(ra) ∈ φ(I) para todo a ∈ I.
6. Aplicando o teste para saber se é um ideal, sejam x, y ∈ φ -1 (J), existem j1 e j2 em J, tais que φ(x) = j1 e φ(y) = j2. Como φ(x - y) = φ(x) - φ(y) = j1 - j2 ∈ J, temos que x - y ∈ φ -1 (J). Também, para todo r ∈ R e x ∈ φ -1 (J), temos φ(rx) = φ(r) φ(x) ∈ J, o que demonstra que rx ∈ φ -1 (J).
7. Basta olhar que φ(r1) φ(r2) = φ(r1r2) = φ(r2r1) = φ(r2) φ (r1) para todo r1 e r2 em R.
8. Para todo s ∈ S, s = φ(r) para algum r em R porque φ é sobre. Assim φ (1) = φ(r)φ(1) = φ(r1) = φ(r) = s. Analogamente φ(1)s = s.
9. Se φ é isomorfismo, então, φ é sobre e injetiva, isto é, se φ(r1) = φ(r2) então r1 = r2. Se r ∈ ker φ, então, φ(r) = φ(0) = 0 e, desse modo, r = 0. Assim, ker φ = {0}. Reciprocamente, suponha que φ é sobre e ker φ = {0}. Provaremos, com isso, que φ é injetiva. Para tanto, suponha que φ(r1) = φ(r2), então, φ(r1 - r2) = 0, o que mostra que r1 - r2 = 0, porque ker φ = {0}. Assim, φ é injetivo e sobre e, sendo assim, um isomorfismo.
10. Temos de provar que φ -1 (s1 + s2) = φ -1 (s1) + φ -1 (s2) e φ -1 (s1. s2) = φ -1 (s1) . φ -1 s2. Suponhamos que φ -1 (s1) = r1 e φ -1 (s2) = r2. Logo, φ(r1) = s1, φ(r2) = s2 e φ(r1 + r2) = φ(r1) + φ(r2) = s1 + s2. Isso mostra que φ -1 (s1 + s2) = r1 + r2 = φ -1 (s1) + φ -1 (s2).

ISOMORFISMOS

Na área da álgebra abstrata, a definição de isomorfismo apresenta-se como um homomorfismo bijetivo. Ou seja, duas estruturas algébricas são denominadas isomorfos, se houver, entre elas, um mapeamento bijetivo.

Outra maneira de se conceituar isomorfismo é pensar em dois objetos que, essencialmente, devem ser indistinguíveis, isto é, que não podem ser distinguidos. Essa área algébrica realizará o levantamento sobre esses elementos, mostrando, assim, um relacionamento entre as propriedades ou as operações.

Os isomorfismos são estudados para que se possa estender os conhecimentos a respeito de uns fenômenos para outros. Por exemplo, se dois objetos forem isomorfos, então, todas as propriedades deles podem ser mantidas por um isomorfismo e o que for válido para um dos objetos também será válido para o outro.

Caso um dos isomorfismos seja encontrado em alguma área ou parte do ensino matemático (em que inúmeros teoremas já foram desbravados e muitos processos estão disponíveis para encontrar a resolução), a função isomorfa pode ser utilizada para mapear as questões dessa área desconhecida, para um ambiente em que os problemas serão melhor entendidos e, dessa forma, para melhor trabalhar com eles.

Na álgebra abstrata, dois isomorfismos principais e básicos são considerados. Definimos cada um deles a seguir:

- Isomorfismo de grupos: um isomorfismo entre grupos distintos.
- Isomorfismo de anéis: um isomorfismo entre anéis. (Perceba que isomorfismos entre campos comuns, são, na verdade, isomorfismos de anéis).

Do mesmo modo que os automorfismos de uma sustentação algébrica formam um grupo, os isomorfismos entre dois elementos que partilham entre si a mesma estrutura também formam uma unidade.

Existem diversos exemplos de isomorfismo entre os teoremas e teorias algébricas. A teoria de Laplace é um isomorfismo que mapeia e transforma equações complicadas em equações mais fáceis. Na teoria das categorias, se considerarmos uma categoria C, em que se consiste em duas classes, uma de objetos distintos e outra de morfismos, passaremos a ter uma definição geral de isomorfismo que ultrapassa a anterior, sendo todo isomorfismo um morfismo.

Dessa forma, temos: $f\colon a \to b$, que tem uma inversa i.e., existindo um morfismo $g\colon b \to a$, com $g\colon b \to a$ e $gf = 1_a$. Como exemplo, podemos citar um mapa linear bijetor, que corresponde a um isomorfismo constituído a partir de espaços vetoriais, de maneira que a função seguirá bijetora, uma vez que a inversa é, também, contínua. Trata-se, portanto, de um isomorfismo sob espaços topológicos, chamada homeomorfismo.

Já no teorema dos grafos, um isomorfismo sob dois grafos, *G* e *H*, é um mapa bijetor *f* de um vértice de *G* para um vértice de *H*, que sustenta os “pilares de arestas”, no sentido de que há uma aresta de um vértice *u* para outro *v* em *G*, se houver uma aresta de f (*u*) para f (*v*) em *H*.

Em análise aritmética, um isomorfismo entre dois espaços de Hilbert é uma bijeção que mantém a adição, a multiplicação escalar e o produto interno. Logo, nas teorias primárias do atomismo lógico, o convívio formal entre fatos e proposições legítimas foi desenvolvido por Bertrand Russel e Ludwig Wittgenstein para ser isomórfico. Um modelo dessa forma de pensar pode ser visto na Introdução à Filosofia da Matemática de Russell.

ATIVIDADES

4) A partir da função f: G → J, assinale a alternativa que apresenta expressões que correspondem a um homomorfismo.

a) G = (Z, +), J = (Z, +), f (x) = 7x.

b) G = (Z, +), J = (Z, +), f (x) = 7x + 1.

c) G = (Z, +), J = (Z, +), f (x) = 7 x 2.

d) G = (R, +), J = (Z, +), f (x) = IxI.

e) G = (Z, +), J = (Z, +), f (x) = 8x + 1.

FIQUE POR DENTRO

Essa terceira unidade distanciou-se um pouco da álgebra tradicional e trouxe estudos relacionado ao abstrato. Trata-se de uma área mais recente na matemática, que enaltece conceitos como anéis e homomorfismos, relativamente mais complexos que os estudos tradicionais, pois não possuem uma lógica tão concreta quanto aos números em si. É interessante observar a importância de se adquirir novos conhecimentos e sair de nossa zona de conforto, estimulando nossa mente para o novo e buscando raciocínios diferentes, para sabermos resolver os mais diversos e complexos tipos de problemas.

Para aprofundar seus conhecimentos, recomendamos a leitura do artigo: "Aneis Euclidianos no contexto das Equações Diofantinas", disponível em: <https://www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/yuri.pdf> e do site: <http://www.uel.br/projetos/matessencial/superior/algebra/corpos.htm>.

REFLITA

"A Matemática apresenta invenções tão sutis que poderão servir não só para satisfazer os curiosos como, também para auxiliar as artes e poupar trabalho aos homens" (DESCARTES, século XVII).

INDICAÇÕES DE LEITURA

Nome do Livro: Álgebra Moderna

Editora: Saraiva

Edição: 5ª (8 de dezembro de 2017)

Autor: Hygino H. Domingues

ISBN: 8547223053

Comentário: Neste livro, o autor apresenta os principais elementos da álgebra moderna e descreve, de forma simples, e com uma linguagem acessível, as teorias e os teoremas, fundamentais para ampliar nosso horizonte matemático.

Filme: Quebrando a banca

Gênero: Policial

Ano: 2008

Elenco Principal; Kevin Spacey, Jim Sturgess, Kate Bosworth, Jeff Ma, Laurence Fishburne

Sinopse: O filme *Quebrando a banca* apresenta a história de Ben Campbell, um jovem que, para custear a faculdade, participa de jogos de cartas, em Las Vegas, com uma identidade falsa, todos os fins de semana. O grupo que ele integra é liderado por um professor de matemática e gênio em estatística, com quem consegue montar um código infalível. Contando cartas e usando um complexo sistema de sinais, eles conseguem quebrar diversos cassinos. Vale a pena assistir!

UNIDADE IV

Polinômios

Valnira Oliveira

Introdução

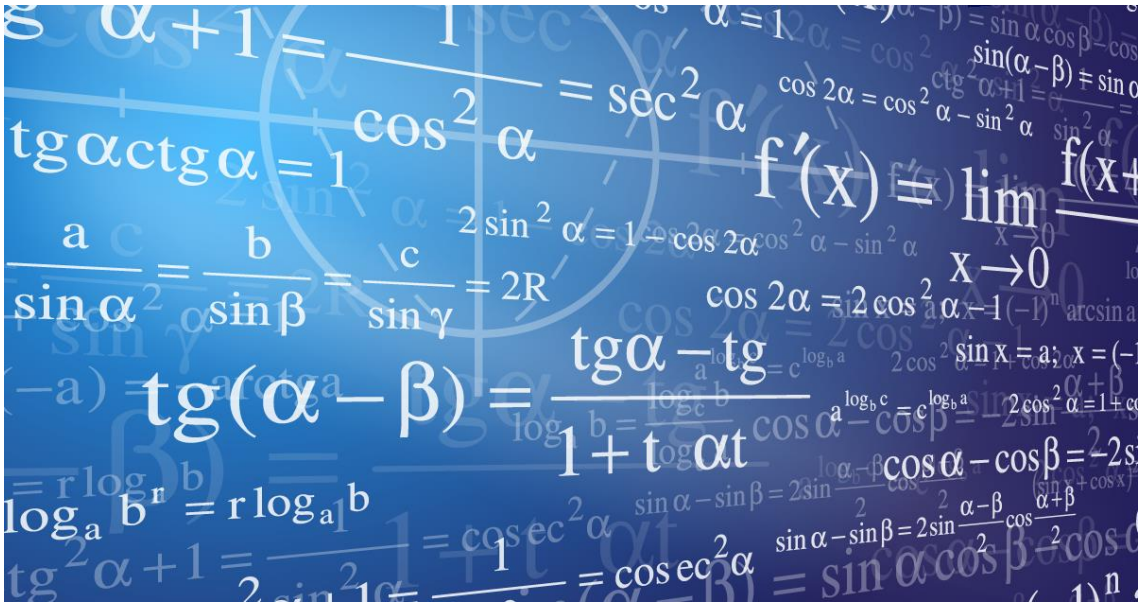
Uma das grandes constatações no sistema de ensino vigente atual é que a maior parte dos alunos tem dificuldade para compreender os conceitos matemáticos. Eles até aprendem a realizar operações matemáticas, porém acabam executando estes processos de forma mecânica, decorando as fórmulas. Ou seja, os alunos conhecem o algoritmo, entretanto, não conseguem entender os conceitos envolvidos por trás dos números e, como consequência, não estabelecem uma ligação entre a teoria matemática e a prática do mundo real que os circunda. Percebe-se, ainda, que toda a revisão dos conteúdos básicos feita no começo de cada ano não traz qualquer resultado adicional.

Vale considerar que o ensino da matemática se encaixa no processo de educação ao qual nos situamos: aquele em que o docente apresenta o conteúdo e, em seguida, os alunos simplesmente resolvem uma sequência de exercícios. No entanto, tal método é ineficaz e pouco produtivo, já que nele não se constrói um conhecimento verdadeiro sobre o que a aritmética trata.

Sendo assim, esta unidade visa fazer essa ponte entre os conceitos teóricos e a prática em si, unindo os dois aprendizados e trazendo à tona os grandes estudiosos da matemática, além de suas descobertas. Dessa forma, será possível ter um conhecimento mais aprofundado sobre os fundamentos da aritmética. Tudo isso para que o aprendizado seja mais eficaz e proveitoso.

As equações polinomiais, também conhecidas como “equações algébricas”, são indispensáveis em nosso dia a dia, principalmente para a modelagem e resolução de problemas. Dada a sua importância, é comum que nos perguntemos sobre a existência de fórmulas capazes de resolver equações de grau maior do que 2.

Desde o século XIX, sabe-se que, além das equações de 2°grau, apenas as de 3° e 4° graus podem ser resolvidas por fórmulas que envolvem os radicais e os coeficientes das equações. No entanto, isso não quer dizer que seja impossível conhecer as raízes de equações algébricas de grau maior do que 4.



Fonte: Denis Ismagilov / 123RF.

MONÔMIOS

Definem-se como monômios as expressões algébricas representadas por apenas um só termo. Por exemplo, a sentença: 2x; 10y; 25ab;√2x, etc.

A parte numérica dos monômios é denominada “coeficiente”. Na unidade 2x2, por exemplo, o algarismo 2 é o coeficiente, ou seja, todas as representações numéricas.

Em algumas situações, ou problemas, o coeficiente aparecerá em forma de letras, como no caso de ax^2, sendo que o elemento “a” pode ser considerado coeficiente de x^2. A parte composta por letras em um monômio é denominada “parte literal”.

Exemplificando:

10 k^3corresponde à parte literal.

Em80m^{100}, m^{100} corresponde à parte literal.

Dadas essas informações, podemos nos perguntar: afinal qual é a definição de polinômio?

POLINÔMIOS

Um polinômio, ou função polinomial, pode ser definido de várias maneiras. Para nossos propósitos, vamos nos concentrar em apenas uma delas. Chama-se “polinômio” a soma algébrica de vários monômios, ou “função polinomial”, na variável complexa x, toda função definida por:

$$P(x)=anx^n + an\text{-}1x^{n-1} + an\text{-}2x^{n-2} +...+a2x^2 + a1x^1+a0$$

Esta é a expressão para todo x C, sendo n N, e an, an-1,an-2,...,a2,a1 e a0 sendo os coeficientes do polinômio P(X). Os monômios anx^n, $an\text{-}1x^{n-1\wedge}$, $an\text{-}2x^{n-2}$, $a2x^2$ e $a1x^1$ são os termos do polinômio, sendo que a0 é o termo independente de *x*.

Exemplificando:

P(x)= 5x^4+3x^2-10ix +4

Os elementos 5, 3, -10i e 4 são os coeficientes de P(x), considerando que 4 é o termo independente deste polinômio.

Agora veja:

$Q(x)=-x^5+x+10$

Veja que os termos x^4,x^3 e x^2 não constam no polinômio Q(x). Isso mostra que os coeficientes desses elementos são todos iguais a zero. Assim, teremos:

$Q(x)=-5x^5+0x^4+0x^3+0x^2+x+10$

Ao tirar seus coeficientes, fica: -5, 0, 0, 0, 1 e 10.

H(x) = 100

Perceba que o polinômio H(x) é denominado “polinômio constante”, pois ele é formado por apenas um número complexo (em particular, um número real).

R(x) = 0

O polinômio R(x) também é constante, porém todos os seus coeficientes são iguais a zero. Dessa forma, R(x) é chamado de polinômio nulo e pode ser representado por:

R(x)= 0x^n+ 0x^(n-1)+0x^(n-2)+...+0x^2+0x^1+0

GRAU DE POLINÔMIO

Considere o polinômio $P(x)=anx^n + an\text{-}1x^{n-1} + an\text{-}2x^{n-2}+...+a2x^2+a1x^1+a0$ sendo um polinômio não nulo. O grau de P(x) é o maior valor numérico do expoente que acompanha a variável x dentre todos os monômios com coeficientes diferentes de zero.

Exemplificando:

$Q(x)= 2400x^2+2000x+1100$tem grau 2.

$H(x)= 10x^{10}+5x^7+x^5$ tem grau 10

$P(x)=0x^3+0x^2+10x$ tem grau 1.

Nota: Todo polinômio constante tem grau 0.

Vale ressaltar que não se define grau para o polinômio nulo. Esta é uma observação que precisamos ficar atentos.

VALOR NUMÉRICO DE UM POLINÔMIO

O valor numérico de um polinômio nada mais é do que o valor que ele irá assumir em um ponto específico de seu domínio.

Como a função $P(x)=anx^n + na - 1x^{n-1} + na - 2x^{n-2}+...+a2x^2+a1x^1+a0$ assume valores em quaisquer pontos de seu domínio C, neste caso, tem-se:

P(z)= anz^n+ an〖-1z〗^(n-1)+an〖-2z〗^(n-2)+...+a2z^2+a1z^1+a0 , para todo z E C.

Exemplificando:

Para o polinômio P(x) =10x^2- 20x^1-50, calcule P (1).

P (1) = 10 *(1) ² - 20 *(1) -50 = 10-20 -50 = -60.

P (i) = 10 (i) ²-20 (i) -50.

RAIZ DE UM POLINÔMIO

Dado um número z E C, tal que P(z) = 0, sendo que, para um polinômio qualquer P: C -> C, dizemos que z é a raiz do polinômio P(x).

Exemplificando:

P(x)= 10x^10+ 5x^7+x^5.

Veja que, se x = 0, temos:

P(0) = 10〖(0)〗^10+ 5〖(0)〗^7+〖(0)〗^5= 0.

Assim, dizemos que x = 0 é raiz do polinômio P(x).

Agora, observe que x = 1, sendo:

P(1) = 10〖(1)〗^10+ 5〖(1)〗^7+〖(1)〗^5= 10+5+1=16

Ou seja, x = 1 não é raiz de P(x).

Q(x) = x^3+ 2x^2-x^1-2.

Para x = -2, tem-se:

Q(-2) =〖(-2)〗^3+ 2〖(-2)〗^2-〖(2)〗^1-2 = 0.

Ou seja, x = -2 é raiz do polinômio Q(x).

IDENTIDADE DE POLINÔMIOS

Considere dois polinômios P, Q: C -> C. Eles são similares em caso de assumirem valores numéricos semelhantes para quaisquer valores em comum designados à variável. Ou seja, P(x) = Q (x), x E C. Assim, denota-se que P(x) ≡ Q(x).

Nota: Para que P(x) e Q(x) sejam iguais, basta que os coeficientes de P(x) e Q(x) sejam iguais.

Exemplo:

Para que P(x) = ax^3+ bx^2+〖cx〗^1+d e Q(x)= 100x^3- 2x^2+〖20x〗^1+400 sejam iguais, basta que: a = 100, b = -2, c =20 e d= 400.

OPERAÇÕES ENTRE POLINÔMIOS

Em um primeiro momento, vamos efetuar as operações conhecidas entre polinômios, como adição, subtração e multiplicação. Logo em seguida, estudaremos detalhadamente a divisão entre polinômios.

Adição e subtração de polinômios

Dado dois polinômios P(x) e H(x), obtemos a soma adicionando os coeficientes dos termos correspondentes de P(x) e H(x).

Exemplo:

Sendo P(x)= 〖10x〗^3+ 5x^2+ 〖4x〗^1+1 e H(x)= 6x^2- 〖3x〗^1+9, temos que:

P(x)+ H(x)= (〖10x〗^3+ 5x^2+ 〖4x〗^1+1) +(0x^3+6x^2- 〖3x〗^1+9) =

〖(10+0)x〗^3+(5+6)x^2+ 〖(4-3)x〗^1+(1+9) = 〖10x〗^3+ 11x^2+ 〖1x〗^1+10

Já a subtração entre os polinômios P(x) e H(x) é realizada de modo similar à adição entre eles, porém fazemos a adição do primeiro com o oposto do segundo, ou seja, P(x) + (- Q (x)) = P(x) – Q(x).

Exemplo:

P(x) - Q(x) = (〖10x〗^3+ 5x^2+ 〖4x〗^1+1) - (0x^3+6x^2- 〖3x〗^1+9) =

〖(10- 0)x〗^3+(5-6)x^2+ 〖(4+3)x〗^1+(1- 9) = 〖10x〗^3- 1x^2+ 〖7x〗^1- 8

Nota: De forma geral, o grau do polinômio P(x) + Q(x) é, no máximo, igual ao maior dos graus entre P(x) e Q(x) e, no mínimo, zero.

Multiplicação de polinômios

O produto de dois polinômios P(x) e Q(x) é feito por meio da multiplicação de cada termo de P(x) por todos os termos de Q(x), diminuindo os termos semelhantes.

Exemplo:

Para P1(x) = 2x^2+4 e P2(x)= 5x^1+10, obtém-se:

C(x)= P1(x) · P2(x)

C(x) = (2x^2+4)· (5x^1+10)

C(x) = 10x^3+20x^2+20x^1+40

Para P1(x) = 2x^2+4, obtém-se:

D(x)= P1(x) · P1(x)

D(x) = (2x^2+4)· (2x^2+4)

D(x) = 4x^4+8x^2+8x^2 +16

D(x) = 4x^4+16x^2 +16

Nota: O grau do polinômio P(x) · Q(x) é dado pela soma do grau de P(x) com o grau de Q(x). Desse modo, gr(P·Q) = gr(P)+gr(Q).

Divisão de polinômios

Considere dois polinômios P(x) e D(x), com D(x) não nulo. Dividir P(x), o dividendo, por D(x), o divisor, possui o sentido em definir os polinômios Q(x) e R(x), sendo esses, respectivamente, o quociente e o resto que satisfaz duas condições:

P(x) = Q(x)·D(x) + R(x)

Gr (R) < gr (D) ou R(x) = 0

Observe que:

P(x) | D(x)

R(x)   Q(x)

Método da chave

Para realizar a divisão entre dois polinômios, podemos utilizar a mesma ideia da divisão entre números naturais, usando o método da chave.

Exemplo: Divida P(x) = x^3-6x^2-x^1 +12 por D(x) = x^1 - 2

Etapa 1: Escreva ordenadamente o dividendo e o divisor, seguindo as potências decrescentes do polinômio. Sendo assim:

x^3-6x^2-x^1+12 | x^1 - 2

Etapa 2: Separamos o elemento com o grau mais superior de P(x) pelo termo de grau superior de D(x) (x^3: x^1), obtendo x^2, termo de Q(x).

x3 - 6x2 - x1 + 12 Ix1 - 2

x2

Etapa 3: Multiplicamos o termo x^2 do quociente pelo divisor, subtraímos do dividendo o resultado (x^3+2x^2) e encontramos um resto parcial (-4x^2-x+12).

x^3-6x^2-x^1+12 | x^1 - 2

-x^3+2x^2 x^2

-4x^2-x+12

Etapa 4: Realizamos o processo da divisão com o termo que possui o maior grau do dividendo sobre o termo de grau mais elevado do divisor (-4x^2: x), obtendo -4x. Assim:

x^3-6x^2-x^1+12 | x^1 - 2

-x^3+2x^2 x^2 -4x

-4x^2-x+12

+4x^2-8x

-9x +12

Etapa 5: Replicaremos a mesma ideia da etapa anterior, realizando a divisão com o termo de maior grau do dividendo sobre o termo de maior grau do divisor (-9x: x), obtendo -9. Logo:

x^3-6x^2-x^1+12 | x^1 - 2

-x^3+2x^2 x^2 -4x - 9

-4x^2-x+12

+4x^2-8x

-9x +12

9x^1-18

-6

Etapa 6: A divisão se encerra quando o grau do resto for menor que o grau do divisor (neste caso menor que 1) ou quando obtemos o resto zero.

Portanto, P(x) : Q(x) = x^2 -4x - 9 e com resto R(x) = 6.

Assim, para P(x) = Q(x)·D(x) + R(x), temos que P(x) = (x-2) · (x^2 -4x - 9) + 6.

Observe que gr(Q) = gr(P) – gr(D) e que o maior grau possível para R(x) = gr(D) -1.

Nota: Quando R(x) = 0, dizemos que o polinômio P(x) é divisível por D(x), ou, ainda, que a divisão é exata.

Método de Descartes

O método de Descartes consiste em determinar os coeficientes dos polinômios quociente e divisor, baseando-se na relação já vista anteriormente, em que:

P(x) = Q(x) · D(x) + R(x)

Exemplo: Dividir f = 3x^4-2x^3+7x^1+2 por g = 〚3x〛^3-2x^2+ 〚4x〛^1-1.

Temos: r(Q) = gr(f) - gr(g) = 4 -3 = 1.

Dessa forma, o polinômio Q(x) é do 1° grau, ou seja, é do tipo Q(x) = ax +b. Quanto ao resto, seu grau não pode exceder a 3 (grau do polinômio divisor). Assim, gr(R) < 3.

Na situação menos favorável, vamos considerar que o grau do resto seja 2.

Logo, R(x) = cx^2+dx^1+e

Aplicando o teorema P(x) = Q(x) · D(x) + R(x), temos que:

f = Q(x) · g + R(x)

3x^4-2x^3+7x^1+2 = (ax +b) ·(〚3x〛^3-2x^2+ 〚4x〛^1-1) + cx^2+dx^1+e

Desenvolvendo essa expressão, chegamos a:

3ax^4+(3b-2a)x^3+(4a-2b+c)x^2+(4b-a+d)x^1+(e-b) = 3x^4-2x^3+7x^1+2

Por igualdade de polinômios, temos:

3a = 3 -> a = 1

3b – 2a = -2 -> 3b = -2 + 2(1) = 0 -> b =0

4a -2b+c = 0 -> c = 2b -4a -> c = -4

4b – a +d = 7 -> d =a – 4b +7 -> d = 8

e – b = 2 -> e = b +2 -> r = 2

Resposta: Q(x) = x e R(x) = -4x^2- 8x^1 + 2

Método da dividão por binômois do tipo (x -a)

A divisão de um polinômio P(x) por um binômio do tipo B(x) = x – a merece especial atenção.

Observe que o número a é raiz do binômio, pois B(a) = 0.

Como o binômio possui grau 1, o resto da divisão de P(x), com gr(P) ≥ 1, por B(x) necessariamente terá que ser um polinômio constante (ou de grau zero).

Exemplificando:

Efetuaremos a divisão entre P(x) = x^3-2x^2+x^1-10 por Q(x) = x-3 e vamos calcular P(3).

x^3-2x^2+x^1-10 | x^1 – 3

-x^3+3x^2 x^2 +x +4

x^2+x - 10

-x^2+3x

4x - 10

-4x +12

2

Agora, para o cálculo de P(3) = 〚(3)〛^3-2 〚(3)〛^2+ 〚(3)〛^1-10 = 2.

Observe que o valor obtido em P(3) é o mesmo que o resto da divisão de P(x) por x-3.

Teorema do resto

Dado um polinômio P(x) com grau qualquer, o resto da divisão de P(x) por x-a é igual a P(a).

Exemplos: Na divisão de P(x) por x-a, temos: P(x) = Q(x) · (x-a) + R(x), com R(x) = R, e R E C, ∀ x∈ C. Substituindo x por a, temos que: P(a) = Q(a) · (a-a) + R = 0 + R-> P(a) = R.

Dispositivo de Briot-Ruffini

Este método utiliza apenas os coeficientes do dividendo P(x) e o valor de a, que é a raiz do divisor x-a.

Exemplificando:

Iremos determinar o quociente e o resto da divisão entre P(x) = 2x^3-4x^1+1 por x-4, utilizando Briot-Ruffini.

Para isso, vamos reescrever o polinômio da seguinte forma:

P(x) = 2x^3+0x^2-4x^1+1

Figura 4.1 - Escrevendo polinômio

Fonte: Adaptada de Mello (2009).

O último valor obtido é o resto da divisão e os demais são os coeficientes do quociente, dispostos ordenadamente de acordo com as potências de x.

Dessa forma, Q(x) = 2x^2+8x^1+28 e o resto é R(x)=113.

Divisão de polinômios pelo produto

Um polinômio é divisível por (x-a) e, também, por (x-b), com a ≠ b, se P(x) também for divisível pelo produto de (x-a) (x-b).

Exemplo: Se P(x) = x3 + x2 − 10x + 8, determine P(x) para x = 3, x = 2 e x = 0. A seguir, escreva P(x) como produto de dois fatores (DANTE, 2009, p. 449).

Solução:

•P(3) = 33 + 32 − 10 · 3 + 8 = 14

•P(2) = 23 + 22 − 10 · 2 + 8 = 0

•P(0) = 3 + 2 − 10 · 0 + 8 = 8

Como P(2) = 0, então x−2 é um fator de P(x).

Agora, vamos realizar a aplicação do dispositivo prático feito por Briot-Ruffini, considerando q(x) = x2 + 3x − 4:

P(x) = (x−2) (x2+3x−4)

Exemplo : Iremos verificar se = x3 -3x2 − 6x + 8 é divisível por (x+2) (x-4) sem efetuar divisão. Temos:

P(-2)= 〖(-2)〗 ^3-3 〖(-2)〗 ^2-6 〖(-2)〗 ^1+8 = 0

P(4) = 〖(4)〗 ^3-3 〖(4)〗 ^2-6 〖(4)〗 ^1+8 = 0

Como P(-2) = 0, sabe-se que P(x) é divisível por (x+2). O polinômio também é divisível por (x-4), porque P(4) = 0.

Assim, o polinômio P(x) se divide por (x+2) (x-4).

FATORAÇÃO

A fatoração é a operação inversa da multiplicação, isto é, fatorar um polinômio significa escrevê-lo como produto de polinômios menores, geralmente como produto entre monômios e binômios.

Exemplo: (x+3)(x+4)= x^2+7x^1+12

Veja que realizar o processo de fatoração x^2+7x^1+12 corresponde a simplesmente encontrar os polinômios que resultaram nele próprio.

TIPOS DE FATORAÇÃO

Fatoração por evidência

Ocorre quando todos os termos do polinômio têm, pelo menos, um fator comum.

O fator que se põe em evidência é obtido da seguinte forma:

- Observa-se o MDC entre os coeficientes.
- Observa-se quais são as variáveis que se repetem na parte literal.

Exemplificando:

〖4x〗^2+8x^3

O MDC entre os coeficientes 4 e 8 é 4. A variável comum é x^2. Logo, coloca-se em evidência o termo 4x^2. Dessa forma:

〖4x〗^2+8x^3 = 〖4x〗^2 (1 + 2x)

Fatoração por agrupamento

Trata-se da fatoração que ocorre quando o polinômio tem fatores comuns, mas não a todos os termos.

Exemplo: ab + ac+ db+ dc

Põe-se em evidência a, nos dois primeiros termos, e d, nos dois últimos. Assim: a (b+c) + d(b+c) e depois (b+c). Desse modo, (a+d) (b+c).

Exemplo: x^3+2x^2 〖- x〗^1-2

Põe-se em evidência x^2 nos dois primeiros termos e -1 nos dois últimos, x^2(x+2) - 1(x+2). Agora, coloca-se x+2 em evidência.

Assim, temos que: (x+2)(x^2-1)

Fatoração da diferença dos quadrados

A diferença de dois quadrados resulta no produto da soma e diferença (produtos notáveis).

a^2 - b^2 = (a+b) (a-b)

Exemplos:

x^2 - y^2 = (x+y) (x-y)

a^2 - 9= (a+3) (a-3)

〖16a〗^4- 〖4b〗^2= $(4a^2+2b)$ $(4a^2-2b)$

Fatoração do trinômio quadrado perfeito

É o caso do quadrado da soma e diferença (produtos notáveis).

Para fatorar, extrai-se a raiz quadrada dos coeficientes e das variáveis que são quadrados perfeitos. Depois, é verificado se o dobro do produto do primeiro pelo segundo é o terceiro termo do polinômio. Convém lembrar que:

〖(a+b)〗^2= a^2 + 2ab+b^2

〖(a-b)〗^2= a^2 - 2ab+b^2

Exemplos: x^2+4x +4 = 〖(x+2)〗^2

O produto 2 ·x ·2 = 4x

x^2+4xy +4y² = 〖(x+2y)〗^2

O produto 2 ·x ·2y = 4xy.

A fatoração do trinômio de segundo grau que pode ser decomposto no produto de dois binômios.

Consideramos o produto:

(x+a)(x+b)= x^2 + 2(a+b)+a ·b

Chama-se:

S = a +b (soma)

P = a · b (produto)

Exemplo: x^2+5x +6

Assim, temos: S = 5, e P = 6.

Dessa forma, precisamos encontrar dois números a e b, cujo produto é 6 e, a soma, 5.

Como o produto é positivo, conclui-se que os dois números têm sinais iguais e podem ser:

2 e 3 ou -2 e -3 -> soma ±5

1 e 6 ou -1 e -6 -> soma ±7

Já que a somatória é positiva, os dois números devem ser positivos e resultar em 5. Logo, só podem ser 2 e 3. Portanto, x^2+5x +6 = (x+2)(x+3)

Exemplo: x^2-2x -24

Temos soma S = -2 e produto P = -24

Como o produto é negativo, conclui-se que os números possuem sinais diferentes. Assim:

-1 e 24 ou 1 e -24 -> soma ± 23

-2 e 12 ou 2 e -12 -> soma ± 10

-3 e 8 ou 3 e -8 -> soma ± 5

-4 e 6 ou 4 e -6 -> soma ± 2

As únicas das possibilidades em que a soma é -2 e o produto -24 são os números -4 e 6.

ATIVIDADE

1. Vamos considerar o polinômio:

P(X)= 〖4x〗 ^4+ 〖3x〗 ^3- 〖2x〗 ^2+x+k

Sabendo que P(1) = 2, qual será o valor de P(3) e qual o grau do polinômio, respectivamente?

a) 386 e 4.
b) 405 e 4.
c) 81 e 10.
d) 368 e 5.

GRUPOS

Na matemática, a teoria dos grupos é responsável por estudar as estruturas algébricas que são denominadas “grupos”. Tal conceito é de extrema importância para a álgebra abstrata, pois muitas outras áreas algébricas de que se tem conhecimento, como anéis, campos, espaços e axiomas, podem ser olhadas como grupos.

Os grupos estão presentes em todas as partes da aritmética e seus métodos e processos influenciaram diversos outros ramos da álgebra. Vale dizer que um dos mais importantes avanços da matemática no século XX foi o esforço de colaboração, responsável por um grande espaço nas páginas de periódicos publicados em todo o século passado, a maioria entre as décadas de 1960 e 1980, resultando na organização dos grupos simples finitos.

Grupos são utilizados para capturar a igualdade interna de uma estrutura no formato de automorfismos de grupo. Esta igualdade, ou simetria, geralmente está associada a alguma propriedade que não varia e o conjunto de mudanças que sustenta este invariante, juntamente com a operação de compor essas transformações, forma um grupo de simetria.

GRUPOS E SUBGRUPOS

A ideia essencial por trás da teoria dos grupos se dá em pegar dois elementos de um determinado conjunto e, de alguma forma, combiná-los a um outro elemento deste mesmo conjunto. É justamente essa a função das operações binárias. Desse modo, seja então G um conjunto não vazio, uma operação binária sobre G torna-se uma função $*$, que conecta a cada par ordenado $(a, b) \in G \times G$ um elemento $a * b \in G$.

Denotamos, assim, uma operação binária sobre G da seguinte forma:

$$* : G \times G \rightarrow G$$

$$(a, b) \mapsto a * b$$

Veja que a $*$ b (lê-se: a estrela b) é uma outra maneira de se apontar a função $*$ (a, b), e que uma operação binária irá propor uma combinação entre dois elementos, apenas. Tirando isso, quando houver qualquer operação $*$ definida sobre G, seja binária ou não, dizemos que G é um conjunto carregado da operação $*$.

De modo particular, se $*$ é binário sobre G, assim, podemos concluir que G é fechado em relação à operação $*$.

Primeira Definição:

Consideramos N como o conjunto dos números naturais, incluindo o elemento 0; Z é o conjunto dos inteiros; Q representa os números racionais; R os números reais; e C os números complexos. Assim:

$*$ = +: A soma sobre N, Z, Q, R ou C representa uma operação binária.

$*$ = −: A subtração sobre N, Z, Q, R ou C representa uma operação binária.

$*$ = ·: O produto sobre N, Z, Q, R ou C representa uma operação binária.

$*$ = ÷: A divisão N, Z, Q ou R representa uma operação binária.

$*$ = ◦: A estruturação de funções é uma operação binária sobre o conjunto F (A) = {f | f: A → A} de todas as funções de A em A.

A soma e o produto de matrizes são operações binárias em relação ao conjunto Mn (R) de todas as matrizes quadradas n×n com entradas em R. Do mesmo modo sobre Mn (Q) e Mn (C), respectivamente, os conjuntos das matrizes quadradas n×n com entradas racionais e complexos.

A soma de vetores em um ambiente vetorial V é uma operação binária, já que:

+ : V × V → V

(u, v) 7→ u + v

Porém o produto por escala não é considerado uma operação binária, já que a multiplicação se define como:

$\cdot : R \times V \longrightarrow V$

$(k, v)\ 7 \longrightarrow k \cdot v$

Segunda definição:

Considere um conjunto G, não vazio, carregado de uma operação $*$. Concluímos que G é um grupo que está de acordo com operação $*$ se as afirmações a seguir acontecerem:

I. $\forall a, b \in G \Rightarrow a * b \in G$

II. $\forall a, b, c \in G \Rightarrow a * (b * c) = (a * b) * c$

III. $\exists\ e \in G : \forall a \in G \Rightarrow e * a = a$

IV. $\forall a \in G \Rightarrow \exists\ a^{-1} \in G : a^{-1} * a = e$

Observe que, nesta definição, o item I aponta que G precisa ser fechado, relacionando-se à operação $*$. Isto é, da operação $*$ pelos membros de G continuarão resultando um elemento de G. Já o item II pede que $*$ seja uma operação que se associe, ou seja, a operação $*$ deverá oferecer permissão para agir em mais de dois números sem ter a necessidade de utilizar os parênteses, estando ciente que qualquer comunhão entre os elementos proporciona o mesmo resultado final. Por exemplo:

$$a * b * c * d = (a * b) * (c * d) = a * (b * (c * d)) = a * ((b * c) * d) = \cdots$$

Em seguida, o terceiro item indica que é preciso existir um elemento especial $e \in G$, voltado à operação $*$, descrito como elemento neutro. Por fim, o item IV ordena a garantia de que todos os elementos $a \in G$ tenham, com relação à operação $*$, um inverso $a^{-1} \in G$.

Perceba que, para criar um grupo, será preciso ter um par de objetos: um conjunto G não vazio e uma operação $*$ que deve ser definida sobre ele. Assim, teremos uma notação intuitiva para o grupo $(G, *)$ a ser usada diversas vezes, entretanto, para simplificar, dizemos simplesmente que G é um grupo ou, então, a nomenclatura de grupo G, o que obviamente já pressupõe que a operação exista. Vale lembrar que, quando mencionamos um grupo G mais específico, temos que ter clareza de qual operação está ligada a ele.

Exemplificando:

Considere um conjunto Z com a operação comum de soma (+). Já que a operação + é binária associativa sobre Z, teremos:

I. $\forall a, b \in Z \Rightarrow a + b \in Z$

II. $\forall a, b, c \in Z \Rightarrow a + (b + c) = (a + b) + c$

III. $\exists\ 0 \in Z : \forall a \in Z \Rightarrow 0 + a = a$

IV. $\forall a \in Z \Rightarrow \exists - a \in Z: (-a) + a = 0$

Assim, (Z, +) é um grupo.

De forma parecida ao item anterior, (Q, +), (R, +) e (C, +) também são grupos que possuem suas operações de adição, de modo que, em todos os problemas, o 0 será neutro e o inverso de x é –x.

O conjunto Z suportado pela subtração (-) não possui características de um grupo. Assim, apesar de a operação ser binária e associativa, -Z não tem qualquer elemento neutro com relação ao símbolo negativo (-). Isso ocorre pois não há um elemento $e \in Z$, de modo que, em todo $x \in Z$, terá: $e - x = x$.

Agora, considere Q $*$, conjunto dos números racionais excluindo-se o zero, trazido pela multiplicação usual em Q. Dizemos que (Q, $\cdot$) é um grupo, como observado a seguir:

$$\forall a, b \in Q* \Rightarrow a \neq 0 \text{ e } b \neq 0 \Rightarrow a \cdot b \neq 0 \Rightarrow a \cdot b \in Q*$$

Já sabemos que ($\cdot$) trata-se de uma operação binária associativa, isto é, para todo a, b, c $\in$ Q $*$, tem-se: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Q $*$ contempla o 1 como número neutro da multiplicação, já que em todo a $\in$ Q $*$ teremos: $1 \cdot a = a$.

Assim, (Q $*$, $\cdot$) se caracteriza como grupo.

Similar ao item 4, (R $*$, $\cdot$) e (C $*$, $\cdot$) são grupos com suas comuns operações de multiplicação, sendo que, na totalidade das ocorrências, o 1 é o número neutro e o inverso de x é 1/x

O conjunto R $*$ composto da operação divisão ($\div$) não se considera como grupo. Realmente, a operação de divisibilidade é binária, mas não é associativa, já que:

$(48 \div 12) \div 4 = 4 \div 4 = 1$

$48 \div (12 \div 4) = 48 \div 3 = 16$

Assim: $(48 \div 12) \div 4 \neq 48 \div (12 \div 4)$.

Considere $G = \{1, -1\}$. Vamos dizer que G é um grupo com a operação de multiplicação comum dos números reais. Sempre houver possibilidade, e também por simplicidade, omitiremos a partir de agora o ($\cdot$), que denota a multiplicação usual.

I. Em todo a, b $\in$ G, temos ab $\in$ G, pois:

$1 \cdot 1 = 1$ $1 \cdot (-1) = -1$ $(-1) \cdot 1 = -1$ $(-1) \cdot (-1) = 1$

II. Não há dúvidas. Para todo a, b, c ∈ G, tem-se: a (bc) = (ab) c.

III. G contém um número neutro, que é 1.

IV. Para todo a ∈ G o próprio a torna-se seu inverso, isto é, a −1 = a. Assim, para a = 1 ou a = −1, temos que a −1 a = aa = 1.

Desse modo, G é um grupo multiplicativo.

O conjunto N composto pela operação de potenciação, dada por a, b = a b, não corresponde a um grupo?

Correto, N é fechado, mas a operação não é associativa. Sendo assim, para os números 2, 3, 4 ∈ N, temos:

$(2 * 3) * 4 = 2^3 * 4 = (2^3)\ 4 = 2^3.4 = 2^{12}$

2 *(3 * 4) = 2 * 34 = 2(34) = 281

Portanto, (2 * 3) * 4 ≠ 2 * (3 * 4) e (N, *) não é um grupo.

O conjunto Mn(R) que inclui a operação de multiplicação usual das matrizes não se considera como um grupo. Assim, sendo In ∈ Mn (R) a matriz identidade, temos:

I. ∀A, B ∈ Mn(R) ⇒ AB ∈ Mn(R)

II. ∀A, B, C ∈ Mn (R) ⇒ A(BC) = (AB)C

III. ∀A ∈ Mn(R) ⇒ InA = A

Entretanto, não é toda matriz $A \in Mn\ (R)$ que tem um inverso, já que algumas não possuem matriz quadrada e, sim, um determinante não nulo.

Desse modo, Mn(R) não é um grupo, tendo a operação de multiplicação usual das suas matrizes.

SUBGRUPOS

Considere um grupo G e, H, seu subgrupo, não vazio. Apontamos que H é um subgrupo a partir de G e descrevemos essa relação como $H \leq G$, se o elemento H se formar como operação binária de G. Perceba que {e} e G serão, em todos os casos, subgrupos a partir de G, denominados “triviais”.

Entendemos que H é um subgrupo próprio de G e descrevemos essa expressão por $H < G$, se H é um subgrupo de G, com $H 6= G$ e $H 6= \{e\}$.

É simples observar que:

$Z < Q < R$ em relação à operação usual de soma.

$Q * < R *$ e $R + < R *$ em relação à operação usual de produto.

O grupo formado pelos números pares infinitos, a saber $2Z = \{2k \mid k \in Z\}$, é um subgrupo de (Z, +).

A seguir, mostramos maneiras de realizar uma verificação se um determinado subconjunto H de G é um subgrupo de G, sem a necessidade de que exibir que ele mesmo é um grupo com a operação de G.

Considerando H como subconjunto de (G, ∗), teremos H sendo subgrupo apenas se as seguintes condições acontecerem:

I. $e \in H$ (elemento neutro de G).

II. $\forall a \in H \Rightarrow a -1 \in H$ (fechado para inverso).

III. $\forall a, b \in H \Rightarrow a * b \in H$ (fechado para a operação).

Exemplificando:

Vamos supor que H ≤ G e consideraremos que as restrições I II e III foram cumpridas. Se eh é o membro neutro de H, portanto, eh ∗ eh = eh. Além disso, eh ∈ H ⊆ G, consequentemente, se e é elemento neutro de G, vamos ter e ∗ eh = eh. Entre essas igualdades, decidimos que e ∗ eh = eh ∗ eh. Assim, mostra-se que e = eh ∈ H, o que comprova a condição I.

Sendo (H, ∗) um grupo, temos H sendo fechado em relação à operação ∗, isto é, em todo a, b ∈ H temos a ∗ b ∈ H. Ainda assim, para todo a ∈ H haverá o oposto de a em H, ou seja, a −1 ∈ H. Desse modo, se verificam-se as condições II e III.

Agora vamos supor que os critérios I, II e III são satisfeitos e que H é um subgrupo de G, isto é, vamos provar que (H, ∗) é um grupo. Realmente, em I, temos que H 6?= ∅ e contém um número neutro, já que e ∈ H. No critério III, diz-se que H é fechado em relação à operação ∗. Como a operação ∗ é a operação igual sobre o grupo G, segue de modo imediato que ∗ é uma operação associativa sobre H. Por fim, o critério II traz que todo elemento de H possui oposto, por isso, podemos concluir que H é um grupo.

GRUPOS CÍCLICOS

Dá-se o nome de “grupos cíclicos” para aqueles grupos que têm um dos elementos Î. Neste caso, G é considerado como gerador do grupo (G, *). Portanto, para ser um grupo cíclico, é necessário que existam os elementos Î G, a fim de formar a expressão m’ = a*m.

Outra definição mais resumida é que todo grupo (G, *), criado por um elemento único deste G, é cíclico, gerado por a. Este grupo cíclico, desenvolvido pelo a, é denotado como <a>.

Se a Î (G, *), então H = {am, m Î Z} é o grupo cíclico de G, originado por a. Sendo assim:

<a> = {am | m Î Z}

Devemos lembrar que am = a*a*a....

Em um grupo multiplicativo, am = a.a.a... e <a> é o conjunto das potências de a.

Em um grupo aditivo am = a + a + a + ..., que se descreve m.a, o conjunto <a> é denotado como conjunto dos múltiplos de a.

Exemplificando:

Precisamos demonstrar que (H, *) é um grupo (subgrupo de G).

I. H é distinto de vazio, já que, se a Î G, a1 = a Î H.

II. Como H parte de G, então * é associativa para os membros desse conjunto.

III. Pelo que foi visto na descrição de potenciação em um grupo, a0 = n. Sendo assim, H possui elemento neutro para a operação *.

IV. "x Î H, x = am. Temos que a-m também se envolve a H. Desse modo, am*a-m = am-m = a0 = n. Portanto, todo elemento de H tem oposto.

De acordo com as condições mostradas, H = {am, a Î G e m Î Z) é um grupo e, de acordo com a definição, H é o grupo cíclico gerado por a.

Demonstração 1

(Z, +) é cíclico, pois, para cada m Î Z, m = m.1. Logo, Z = {m.1 | m Î Z} = <1>.

Demonstração 2

(2Z, +) é um grupo (na verdade, subgrupo) de Z, criado pelo número inteiro 2. Isto é: 2Z = {2m | m Î Z} = <2>.

Demonstração 3

O conjunto C’ = {im, i = Ö-1 e m Î N} é um grupo cíclico para a operação multiplicação C’ = <i>.

Demonstração 4

Considere Z4 = {0, 1, 2, 3}. Assim, o Z4 é cíclico e 1 e 3 são criadores de Z4, isto é < 1 >=< 3 >= Z4, levando em conta a operação adição.

Observe:

1 + 0 = 1, 1 + 1 = 2, 1 + 2 = 3 e 1 + 3 = 0 . Desse modo, todos os membros de Z4 são encontrados a partir do 1.

3 + 0 = 3, 3 + 1 = 0, 3 + 2 = 1, 3 + 3 = 2. Todos os membros de Z4 são encontrados a partir do elemento 3.

Veja que qualquer elemento de Z4 é seu gerador, levando em conta a operação adição.

Demonstração 5

Para a multiplicação, Z4 – {0} é um grupo cíclico em que 1 e 3 são iniciadores. Porém 2 não é.

Demonstração 6

O grupo {1, i, -1, -i} é cíclico e considerado como originário i ou –i, utilizando a operação de multiplicação.

Demonstração 7

Dá-se o grupo (Z, +). Determinaremos < 3 >. Neste grupo, a notação é aditiva e < 3 > deverá possuir:

3, 3 + 3 = 6, 3 + 3 + 3 = 9, e assim progressivamente...

0, -3, -3 + (-3) = -6, -3 + (-3) + (-3) = -9, e assim progressivamente...

Em outras palavras, o subgrupo cíclico originado por 3 é composto pelos múltiplos de 3, sejam eles positivos, negativos ou nulos. Dessa maneira, <3> = 3Z. De modo parecido, demonstra que kZ é o grupo cíclico <k> de Z. Veja que 6Z Ì 3Z.

Exemplificando:

Considere G = {im | i = Ö-1 e m Î N} = < i >

A ordenação de G é finita, pois " m Î N, im = ir, sendo que m = 4k + r, com k e r Î N. Ou seja, *r* é o resto da divisão de *m* por 4. Desse modo, tem-se: r = 0, 1, 2, 3.

Outras definições de grupos cíclicos:

Definição 1: Dado o grupo G e a Î G, dizemos que G foi criado por "a" e tem ordenação infinita, caso os elementos a0, a, a2, ... sejam todos diferentes. Neste caso, utiliza-se a denotação O (G) = ¥.

Exemplificando:

Considere um grupo cíclico G =< a > finito. Pela proposição passada, há inteiros positivos r e s diferentes, tais que ar = as. Assim, r < s ou r > s. Sem haver perda de generalidade, podemos concluir que r < s, sendo que s - r > 0. De ar = as, conclui-se que as - r = n. Logo, existe um natural k, tal que ak = n e A = {n Î N | ak = n} ¹ Æ. Por N ser, em parte, ordenado, o conjunto A possui elemento primário e tem-se a = n.

Agora, vamos provar que < a > = {n, a, . . ., ag-1}. É evidente que {n, a, . . ., ag-1} Í < a >. Assim, a' Î < a >.

Considere p > g. Tem-se, então, p = gq + r, sendo que r Î {0, . . . g - 1} e q Î N.

Ficamos, portanto, com ap = aq + r = (ag)qar = nar = ar Î {n, a, . . . , ag-1}. Então, < a > Í {n, a, . . ., ag-1}.

Assim, G = {n, a, . . ., ag-1}.

Definição 2: A ordenação de um grupo G originado por a Î G é igual ao inteiro inferior positivo de k, de modo que ak = n.

A exibição decorre de maneira direta das proposições passadas e da definição da ordenação de um membro. Assim, observamos que a ordenação de i é igual a 4, pois i0 = i4 = 1, e 4 é o menor número natural que corresponde à condição i4 = n. Da proposição demonstrada, tem-se que se < a > é finito, O (G) = 4.

Conclui-se que todo subgrupo de um grupo cíclico é cíclico.

Exemplificando:

Considere um subgrupo H, partido do grupo cíclico G = < a >. Caso H = {n}, então H = < n > é cíclico. Vamos supor que H = {n}, assim, H = < n > é cíclico. Se H ¹ {n}, seja a*m* um dos membros de H, de expoente positivo mínimo. Então, dado arbitrariamente ak Î H e considerando k = mq + r, com 0 < r < m, teremos ar = ak-mq = ak.(am)-q Î H, pelo que r = 0. Assim, ak = amq = (am) q. Ou simplificando, H =< am >.

O resultado deste teorema é que se H ¹ {n} é um subgrupo de G = < a >, então H = < am >, sendo que *m* é o menor inteiro positivo, tal que *am* Î H. Entretanto, se H ¹ {n} é um subgrupo de um grupo cíclico G, H é finito ou infinito se G for finito ou infinito.

ATIVIDADE

2. Analise as afirmações a seguir e escolha a única alternativa verdadeira entre elas:

a) Um grupo não pode ter mais de um elemento neutro.
b) O conjunto vazio pode ser um grupo, independentemente da operação escolhida.
c) Se um grupo tem uma quantidade finita de elementos, então ele é abeliano (comutativo).
d) Uma equação da forma $a * x * b = c$ sempre tem uma única solução x em um grupo.
e) O conjunto dos números inteiros Z é um grupo com a operação de multiplicação usual.

GRUPOS ABELIANOS

Os grupos abelianos possuem suas particularidades e, obviamente, sua importância na área dos grupos. Portanto, neste tópico, vamos defini-los e escrevê-los de forma aditiva.

Considere um grupo G como sendo abeliano, levando em conta g e h como subgrupos, ou elementos a partir de G, com ordenação semelhante a n e m. Nesse momento, considere l = mmc {m, n}. Dessa forma, l(g ± h) = lg ± lh = 0, isto é, g ± h também irá ter uma ordenação finita. É certo que o conjunto G[n] está composto, basicamente, pelos elementos do subgrupo g e do grupo G, sendo que ng = 0 é um subgrupo de G. Fica explícito, também, que o conjunto T = S n∈N G[n] torna-se um dos subgrupos do principal (G). Isso sem contar o conjunto Gp = S n∈N G[p n], sendo mais um dos subgrupos, tendo para todos os primos, denotados p, a denominação p-componente primária de G.

Exemplificando:

Tendo x ∈ T em uma ordem n, iremos escrever n como o resultado de multiplicação das potências de primos, ou seja, n = p k1 1 … pkr r, com p1, ..., pn primos, em pares diferentes.

Considere ni = n/pki i, em cada i ∈ {1, ..., r}. Veja o mdc {n1, ..., nr} = 1. Dessa forma, possuem l1, ..., lr ∈ Z, tais que l1n1 + ... + lrnr = 1. Então, x = (l1n1 + ... + lrnr) x = l1n1x + ... + lrnrx. Pondo xi = nix para cada i ∈ {1, ..., r}, teremos |xi | = p ki i, isto é, xi ∈ Gpi.

Dessa forma, T está contido na somatória dos componentes iniciais de G. Essa soma será direta, seguindo o fato de que Gp ∩ Gq = {1}, se p 6 = q, e que G é abeliano. Como, evidentemente Drp ∈ P Gp 6 T, o resultado continua. Assim, T está contido na soma das componentes primárias de G. Essa soma é direta, pois Gp ∩ Gq = {1}, se p 6= q, e G é abeliano. Como claramente Drp∈P Gp 6 T, o resultado segue. Seja g um membro de G e m um inteiro positivo, dizemos que g é divisível por m se existe h ∈ G, tal que g = mh.

Definição 1: Um grupo abeliano G é dito ser divisível se todos os membros de G também forem divisíveis por qualquer inteiro positivo. Uma demonstração de grupo divisível é o conjunto dos racionais carregados com a operação de adição.

Outra classe relevante de grupos abelianos é a dos grupos que possuem a propriedade injetiva, que definiremos a seguir.

Um grupo abeliano G é dito injetivo se tiver μ: H → K, um monomorfismo de grupos abelianos, e α: H → G, um homomorfismo de grupos. Assim, existirá um homomorfismo β : K → G, tal que α = μβ.

Perceba que, na definição 1, por ser μ um monomorfismo, tem-se H Im (μ) 6? K. Dessa forma, é simples observar que um grupo abeliano G é injetivo se, para qualquer grupo abeliano K, todo homomorfismo α: H → G, com H 6 K, pode ser ampliado a um homomorfismo β: K → G. Possui-se uma relação entre grupos divisíveis e grupos injetivos, como demonstra o teorema de Baer, dizendo que um grupo abeliano G é injetivo se ele for divisível.

CLASSES LATERAIS

Uma das questões mais relevantes a respeito da ordenação de um subgrupo é que se G é um grupo finito e H é um subgrupo de G, então [H] divide [G], ou seja, a ordem (número de membros) de H divide a de G. O resultado disso é compreendido como Teorema de Lagrange.

Dessa forma, um grupo G de 8 elementos, por exemplo, só irá englobar subgrupos de 1, 2, 4 ou 18 membros, mantendo, porém, a possibilidade de G ainda ter inúmeros subgrupos. Para entender melhor o Teorema de Lagrange, vamos descrever o conceito de classes laterais.

Considerando (G, *) um grupo e H um subgrupo de G. Para cada elemento a Î G, será definida uma classe lateral direita de H, determinada por a, como sendo o conjunto H*a = {h*a | h Î H}.

De forma parecida, irá se definir a*H = {a*h | h Î H} como a classe lateral esquerda de H, determinada por a. Da definição de classe lateral, conclui-se que a*H = H*a, "a Î G, se G for um grupo abeliano.

Definição 1: Se pegarmos G, e considerarmos como um grupo e H um subgrupo de G, denotaremos por G/H ou G : H o conjunto das classes laterais H. O conjunto G/H é denominado de grupo quociente.

No exemplo anterior, G/Hd = Z12 /H = {H, H + 1, H + 2}, ou seja, G/H = { {0, 3, 6, 9}, {1, 4, 7, 10}, {2, 6, 8, 11} }.

Teorema 1: se (G, *) é um grupo e H, um subgrupo "a, b Î G, se b Î H*a. Assim, teremos: H*b = H*a.

Exemplificando:

Vamos supor que b Î H*a. Por conceito de H*a, b = h*a para qualquer h Î H.

Teremos b*a-1 = h*a*a-1 Þ b*a-1 = h Þ h = b*a-1, descontando b*a-1 Î H.

Teorema 2: se duas classes laterais do lado direito em um subgrupo H de G são semelhantes ou disjuntas. Ou seja, "a, b Î G, H*a = H*b ou H*a Ç H*b = Æ.

Em particular, H*a = H Û a Î H.

Exemplificando:

Dois conjuntos são disjuntos ou não. Vamos supor, então, que H*a e H*b não são disjuntas.

Logo, existe x Î G, tal que x Î H*a Ç H*b. Então, x = h*a = h'*b, para certos membros h e h' de H.

Teremos que: a*b-1 = h-1*h'. Assim, a*b-1 Î H.

Teorema 3: considerando G finito, a junção de todas as classes laterais direitas de H é resultante em G.

Simbolicamente: $\bigcup_{a \in G} H*a = G$

Exemplificando:

De acordo com o conceito de classe lateral, para cada elemento x de G, temos que xÎH*x.

Dessa forma: $\bigcup_{a \in G} H*a = G$

Em contrapartida, x*H Ì G, para cada x de G.

Assim: $\bigcup_{x \in G} H*x \subset G.$

Portanto: $\bigcup_{a \in G} H*a = G$

Vemos repetidamente as classes laterais em que (G, *) = (Z12, +) e H = <3> = {0, 3, 6, 9}.

É possível analisar de forma imediata, visto que [H + a] = [H] = 4, "a Î Z12 e que duas classes laterais H + a e H + b, com a e b em Z12, são semelhantes iguais ou disjuntas.

Veja, por exemplo, que H + 0 = H + 3 = H + 6 = H + 9 = H, já que 0, 3, 6 e 9 são os membros de H.

Entretanto, já haveria a possibilidade de se prever que H + 1 = H + 4, pois 1 - 4 = -3 º 9 ÎH. De forma, pode-se dizer que H + 11 = H + 5, pois 11 - 5 = 6 Î H.

Acontece também que, como H +1 = {1, 4, 7, 10}, temos então H +1 = H +4 = H + 7 = H + 10.

Teorema 4 (Teorema de Lagrange): considerando um grupo G finito, H um subgrupo de G e G/H o junção das classes laterais direitas.

Temos que |H| divide |G|. Ou, de forma mais precisa, |G/H| = |G|/|H|.

Observação: o símbolo |G/H|, que representa o número de classes laterais de H em G, também pode ser indicado por |G : H|.

Exemplificando:

Considerando G um grupo finito, temos a existência de um número finito de classes laterais direitas em H, já que a união de todas elas é igual a G, Podemos supor, dessa forma, que há s classes laterais direitas de H, sendo s > 1, em pares diferentes. Isto é, G/H = {H*x1, H*x2, . . ., H*xs} para determinados membros x1, x2, . . . , xs de G, sendo as classes H*x1, H*x2, . . ., H*xs diferentes entre elas.

Como classes laterais, mesmo diferentes, são também disjuntas, teremos: G = H*x1 È H*x2 È . . . È H*xs.

Além disso: |G| = |H*x1| + |H*x2 | + . . .+ |H*xs|.

Sendo, porém, |H*xk| = |H|, para cada k, 1 < k < s, resulta |G| = |H| + |H| + ...+ |H| = s.|H|.

Dessa forma: |G|/|H| = s = |G/H|.

ATIVIDADES

3. Considerando o grupo abeliano G = (Z8, +) e H um subgrupo de G, podemos afirmar que:

a) A ordem de H é igual a 4, obrigatoriamente.
b) H pode ter ordem 6.
c) Devemos ter (G: H) = 4, obrigatoriamente.
d) G não pertence a H.
e) H ▹ G.

TEOREMA DO HOMOMORFISMO

Na área da matemática mais abstrata, a teoria do homomorfismo é conhecida, também, como teorema holomórfico fundamental. Como já visto anteriormente, tem como objetivo principal relacionar dois objetos entre os quais há um homomorfismo, considerando o núcleo e a imagem de ambos. O teorema holomórfico é utilizado, basicamente, para se constatar teoremas do isomorfismo.

Considerando E, F ELCs Hausdorff e u ∈ L (E, F), dizemos que u é um homomorfismo se dado U aberto em E, então u (U) é aberto em u (E). De forma equivalente, u é um homomorfismo se a aplicação u: E/ ker u → F, induzida por u, define um isomorfismo topológico entre E/ ker u e u (E).

Se E, F são ELCs Hausdorff e se u ∈ L (E, F), então: (ker u)0 = tu (F′), fecho em σ(E′ , E).

Basta fazer a verificação em que tu (F′)0 = ker u (teorema do bipolar). Uma vez que tu (F′)0 = {f ◦ u: f ∈ F 0} segue que x ∈t u (F′)0 se, e somente se, f (u (x)) = para todo f ∈ F′, que é equivalente a u (x) = 0 (teorema de Hahn-Banach). Valem também as igualdades, quaisquer que sejam, A ⊂ E B ⊂ F′: u (A)0 = (tu) −1 (A0), tu (B)0= u −1 (B0).

TEOREMA DO HOMOMORFISMO (GROTHENDIECK)

Nesta variação do teorema, se E, F são ELCs Hausdorff, e se u ∈ L (E, F), então u será um homomorfismo se as duas propriedades seguintes forem válidas:

tu (F′) É σ (E′ , E)-fechado.

Se M ⊂t u (F′) é equicontínuo em E′, então existe N ⊂ F′ equicontínuo, tal que M ⊂t u (N).

Assumimos que u é um homomorfismo e considere x0′ como pertencente ao fecho de tu (F′) em σ(E′ , E). Então, por (B) teremos que x0′ se anula sobre o kernel de u. Fica então bem definida a aplicação linear.

l: u(E) → K, l (u(x)) = x0′ (x).

Podemos provar que l não se encerra, quando u (E) é carregada da topologia induzida por F. De fato, seja ε > 0. Então U = {x ∈ E: |h x0′, x| ≤ ε} é uma vizinhança de 0 em E e, portanto, u (U) é uma vizinhança de zero em u (E) e | ≤ ε em u (U). Pelo teorema de Hahn-Banach, o funcional l se estende a um elemento y′0 ∈ F0. Agora tu (y′0) = y′0 ◦ u = l ◦ u = x0′ e, portanto, x0′ ∈ tu (F′). Assim, vale (1). Tome agora M como em (2) e seja V ∈ ΦE (0) tal que M ⊂ V o. Como u é um homomorfismo, existe um tonel W ∈ ΦF (0), tal que W ∩ u (E) ⊂ u (V). Logo, V + ker u = u −1 (u (V)) ⊃ u −1 (W ∩ u (E)) = u −1 (W) =tu (Wo) o, já que W é um tonel. Então,

M ⊂t u (F′) ∩ Vo= (ker u) o ∩ Vo ⊂ (ker u + V) o ⊂t u (Wo) oo.

Por fim, com Wo é muito pouco compactado em F′ (Teorema de Banach Alaoglu-Bourbaki) segue que tu (Wo) é fracamente compacto e, portanto, fracamente fechado em E′. Consequentemente, tu (Wo)00 = tu (W0) e (2) fica provada, com N = W0.

É preciso demonstrar, nesse momento, que (1) + (2) implicam que u é um homomorfismo. Para isso, precisamos mostrar que dada V1 ∈ Φe (0) existe W ∈ Φf (0), tal que W ∩ u (E) ⊂ u (V1). Considerando a aplicação canônica Π: E → E/ ker u, existe um tonel V2 ∈ Φe/ ker u (0) tal que V2 ⊂ Π (V1). Logo, V.= Π−1 (V2) ∈ Φe (0) é um tonel em E que contém ker u. Se mostrarmos que existe W ∈ Φf (0) tal que W ∩ u (E) ⊂ u (V), então: W ∩ u (E) ⊂ u (V) ⊂ u (V1).

Já que é dado x ∈ V, existe y ∈ V1 com x − y ∈ ker u.

Considere M.= Vo. Então, M é equicontínuo em E′ e, também, M ⊂ (ker u)0 = tu (F′) por (1). Por (2), existe N equicontínuo, tal que V0 ⊂ tu (N). Seja W ∈ Φf (0) um tonel, tal que N ⊂ W0. Então, W ⊂ No. Assim: u −1 (W) ⊂ u −1 (No) = tu (N) o ⊂ V.

Ao usar (C) e o teorema do bipolar, teremos:

$W \cap u(E) \subset u(V)$

Assim, o teorema está demonstrado.

ATIVIDADES

4. Analise as afirmações e escolha a alternativa correta entre as seguintes:

a) Existem inteiros m > 2 e n > 2, tais que o grupo de permutações (S m, ◦) é isomorfo ao grupo de classes de restos (Zn, +).
b) O grupo de permutações (S 5, ◦) é isomorfo ao grupo de classes de restos (Z120, +) . J.
c) Dados inteiros m > 2 e n > 2, o grupo de permutações (S m, ◦) não é isomorfo ao grupo de classes de restos (Zn, +) . J.
d) O grupo de permutações (S 4, ◦) é isomorfo ao grupo de classes de restos (Z4, +).
e) O grupo de permutações (S 4, ◦) é isomorfo a algum subgrupo do grupo de classes de restos (Z24, +).

FIQUE POR DENTRO

Quando imaginamos a matemática e suas mais diversas áreas, nos atentamos sobre o quão complexa e intrigante ela pode ser. Se pensarmos de uma maneira mais amplificada, somos privilegiados por poder viver, hoje, os resultados de séculos de pesquisas e descobertas matemáticas. Entretanto, esse processo histórico não está chegando em sua conclusão, pois ainda há muito a ser feito. Cada um de nós pode fazer a diferença para construir mais páginas de teorias, equações, esquemas e processos, seja de modo racional ou abstrato.

Para aprofundar seus conhecimentos, acesse o artigo a seguir:

ALTOÉ, T. J. Grupos e Corpos com aplicações em GAP Volta Redonda. 2007. 74 f. Trabalho de Conclusão de Curso (Graduação) – Universidade Federal Fluminense, Volta Redonda, 2007. Disponível em: <https://app.uff.br/riuff/bitstream/1/4175/1/TulioJoaquimAltoe%202016-2.PDF>. Acesso em: 26 fev. 2019.

REFLITA

“A matemática, vista corretamente, possui não apenas verdade, mas também suprema beleza - uma beleza fria e austera, como a da escultura” – (Bertrand Russell).

INDICAÇÕES DE LEITURA

Livro: Fundamentos da matemática.

Editora: LTC; Edição: 1ª, Obra Nova.

Autor: Waldemar de Maio.

ISBN: 8521617054.

Comentário: Neste livro, você terá uma base de todos os conceitos e fórmulas matemáticas de forma resumida e simplificada, tratando especificamente das áreas abstratas, como grupos e subgrupos.

INDICAÇÕES DE FILME

Filme: Sob o domínio do medo.

Gênero: Suspense / Drama.

Ano: 1971.

Elenco Principal: Dustin Hoffman, Susan George e Peter Vaughan.

Sinopse: O filme apresenta a história de um professor de matemática que se refugia no interior da Inglaterra e começa a ser hostilizado, tornando-se um vingador calculista para sobreviver.

CONCLUSÃO DO LIVRO

Não é todo mundo que possui o privilégio e a capacidade de realizar seus estudos da forma que gostaria. Muitas vezes, os conteúdos e os métodos apresentados são enigmáticos e muito complexos, o que desestimula o estudante. Sendo assim, o objetivo deste material foi facilitar ao máximo as ideias matemáticas essenciais para qualquer estudante bem-sucedido. Neste curso buscamos salientar de forma organizada e com um linguajar simples e direto os principais conceitos, definições e opiniões sobre diversos elementos da álgebra. Além do conteúdo teórico, também foram apresentados, em cada capítulo, elementos práticos, como exemplos e exercícios, incluindo dicas e informações para aqueles que desejam complementar o assunto abordado com o intuito de se aprofundarem ainda mais nas matérias apresentadas.

Pudemos, também, no decorrer do curso, estudar a história da álgebra e nos aprofundar em seus principais pontos. Em nosso percurso apresentamos a história e o surgimento da álgebra em nossas vidas e descrevemos um pouco a respeito dos números básicos, enfatizando, de início, as teorias da indução e da boa ordem, afinal, é necessário conhecer os algarismos, sua história, suas características, para assim se familiarizar e trabalhar de modo mais íntimo e com um entendimento mais aguçado. Buscamos, também, apresentar e decodificar conceitos e técnicas a respeito da teoria dos conjuntos numéricos, e para facilitar o entendimento do aluno, foram expostos alguns gráficos e exemplos bem divididos passo a passo, de modo a fixar as regras e a aplicação da teoria dos conjuntos. Vimos ainda, a partir dos conjuntos, a conceituação e os métodos que envolvem o Algoritmo de Euclides ou a Divisão Euclidiana, dividindo-se em assuntos, como a fatoração e os exemplos de MDC e MMC, mínimos e máximos divisores comuns, de determinados números, também de modo explicativo e sendo realizado e executado no sistema passo a passo.

Com esse foco de aprendizado direto, simplificado e compacto também avançamos e trouxemos a temática do Teorema Fundamental da Aritmética, englobando os números primos e aqueles que são os temores de muitos acadêmicos, os algarismos com frações, que neste curso foi aprofundado a partir de exercícios e exemplos no decorrer das explicações.

As diversas teorias aritméticas que existem não caberiam em uma só unidade, entretanto, as principais e relevantes para a prática de um bom matemático foram abordadas como as bases de congruência, as descrições, exemplos e definições de anéis e as características principais de grupos, subgrupos, homomorfismos e diversas áreas de conhecimento.

Além disso, tivemos a preocupação de, ao fim de cada capítulo, inserir dicas e conteúdos a mais, para que o estudante se insira no assunto abordado e consiga prolongar seu aprendizado da maneira que achar conveniente. Estimulamos o debate, através dos fóruns e guias de discussão, já que acreditamos que a troca de experiências pode acarretar em novos ensinamentos.

Por fim, esperamos que os estudantes, leitores e profissionais da área matemática possam fazer um bom uso deste material, assim como esperamos que com nossa fórmula, envolvendo teoria, exemplos, descrições e exercícios, possa ter tornado o entendimento mais claro e sido um grande suporte no desenvolvimento do ensino.

Gostaria de agradecer a todos que se comprometeram em tornar a matemática mais aprofundada e ao mesmo tempo mais acessível e direta aos estudantes, pois um ótimo profissional nasce a partir de uma excelente formação, pessoal e intelectual, e os resultados positivos somente serão vistos com o esforço, o interesse e a perseverança de cada um. Temos a certeza de que os conteúdos apresentados aqui serão úteis e bem aproveitados. A você, aluno(a), nosso muito obrigado e o desejo de sucesso, vitórias e grandes conquistas em cada etapa de sua vida profissional e acadêmica.

REFERÊNCIAS

BEZERRA, M. J. **Matemática para o Ensino Médio**. Volume Único. São Paulo: Scipione, 1997.

BOLDRINI, L. J. **Álgebra Linear**. 3. ed. São Paulo: Harbra, 1986.

BOYER, C. B. **História da matemática**. Tradução de Elza F. Gomide. São Paulo: Edgard Blücher, 1974.

CALCULAR **MMC. Começando bem**. Disponível em: <https://www.comecandobem.com/2018/02/calcular-mmc.html>. Acesso em: 18 mar. 2019.

CALLIOLI, C. A.; DOMINGUES, H. H.; COSTA, R. C. F. **Álgebra linear e aplicações**. 6. ed. São Paulo: Atual, 1993.

CAMARGO, M. A. **Pedagogia e comunicação matemática**. São Paulo: Colégio Ítaca, 2017.

CARAÇA, B. de J. **Conceitos Fundamentais de Matemática**. Lisboa: Gradiva, 1998.

CERRI, C. **Desvendando os Números Reais**. São Paulo: IME-USP, 2006. Disponível em: <http://www.mat.ufg.br/bienal/2006/mini/cristina.cerri.pdf>. Acesso em: 19 fev. 2019.

DANTE, L. R**. Matemática**. São Paulo: Ática, 2009.

D'AMBROSIO, U. **Da realidade à ação: reflexões sobre educação e matemática**. 2 ed. São Paulo: Summus, 1988.

DIEUDONNÉ, J. **A Formação da matemática contemporânea**. Tradução de J. H. Von Hafe Perez. Lisboa: Publicações Dom Quixote, 1990.

DOMINGUES, H. H.; IEZZI, G. **Álgebra moderna**. 4. ed. São Paulo: Atual, 2003.

EVES, H. **Introdução à história da Matemática**. São Paulo: Unicamp, 1995.

GARCIA, A. **Elementos de álgebra**. Rio de Janeiro: IMPA, 2003.

_____.; LEQUAIN, Y. **Álgebra**: um curso de introdução. 1. ed. Projeto Euclides. Rio de Janeiro: IMPA, 1988.

GONÇALVES, A. **Introdução à álgebra**. Rio de Janeiro: SBM, 2001.

HALL JR, M. **The Theory of Groups.** Nova Iorque: Chelsea Publishing Company, 1968.

HENRIQUE, G. Olimpíada Regional de Matemática: Teorema Fundamental da Aritmética. Poa-RS 2013. Disponível em: <http://mat.ufrgs.br/~portosil/aula-4.pdf>. Acesso em: 26 fev. 2019.

HERSTEIN, I. N. **Tópicos de Álgebra**. Tradução de Adalberto P. Bergamasco e L. H. Jacy Monteiro. São Paulo: Polígono, 1970.

IEZZI, G.; DOLCE, O. **Álgebra III**. Editora Moderna, 1973.

JANESCH, O. R.; TANEJA, I. **Álgebra I**. 1. ed. Florianópolis: EAD/UFSC, 2008. 217p.

LANG, S. **Álgebra linear**. Tradução Frederic Tsu. São Paulo: Edgard Blücher, 1977.

LESSA, J. R. **Frações**. Disponível em: <https://www.infoescola.com/matematica/fracoes/>. Acesso em: 19 fev. 2019.

LIMA, E. **Álgebra Linear**. Rio de Janeiro: Coleção Matemática Universitária - IMPA, 1995

MELLO, J. L. P. **Matemática Construção e Significado**. 1. ed. São Paulo: Moderna, 2009.

MONTEIRO, L. H. J. **Elementos de álgebra**. Rio de Janeiro: LTC, 1978.

NÚMEROS primos. **Só Matemática.** Disponível em: <https://www.somatematica.com.br/fundam/primos.php>. Acesso em: 19 fev. 2019.

ROGRIGUES, O. Calcular **Mmc.** Disponível em: <https://www.comecandobem.com/2018/02/calcular-mmc.html>. Acesso em: 19 fev. 2019.

SILVA, L. P. M. **O que são conjuntos numéricos?.** Disponível em: <https://brasilescola.uol.com.br/o-que-e/matematica/o-que-sao-conjuntos-numericos.htm>. Acesso em: 23 nov. 2018.

_____. **Números primos.** Disponível em: <https://brasilescola.uol.com.br/matematica/numeros-primos.htm>. Acesso em: 26 set. 2018.

SODRÉ, J. Princípio da Boa ordem. 2010. Disponível em: <http://matematicaeestatistica.blogspot.com/2010>. Acesso em: 19 fev. 2019.

SOUZA, J. R. de. **Matemática**. São Paulo: FTD, 2010.

STEWART, I. **Os mistérios matemáticos do Professor Stewart**: Resolvidos por Hemlock Soames e o Dr. Watsup. Zahar. Tradução de George Schlesinger. 1. ed. Rio de Janeiro: Zahar, 2015.

STRUIK, D. J. **História concisa das matemáticas.** 4 ed. Tradução de José Cosme Santos Guerreiro. Lisboa: Gradiva, 1986.

SZWARCFITER, J. L.; MARKENZON, L. **Estruturas de Dados e seus Algoritmos**. Rio de Janeiro: Livros Técnicos e Científicos, 1994.

TABUADA. **Tabuada de multiplicar**. Disponível em: <https://www.tabuadademultiplicar.com.br/>. Acesso em: 19 fev. 2019.

WAERDEN, Modern Álgebra, Springer-Verlag, Berlim, 1931.