Unidade I Conjuntos

1. Situando a Temática

Nesta unidade faremos uma breve revisão, introduzindo a noção de conjuntos e suas operações, teoria de fundamental importância para a compreensão de qualquer texto matemático. Usa-se a noção de conjunto no estudo de espaços vetoriais, domínios e contradomínios de funções, conjunto-solução de uma equação, base de soluções de uma equação diferencial linear homogênea de ordem *n* etc.

Este texto complementa-se na plataforma MOODLE, onde estão as listas de exercícios e atividades relacionadas com o mesmo. Lembre que a resolução dos exercícios propostos é de grande importância para o aprendizado de qualquer disciplina matemática.

2. Problematizando a Temática

A ideia de conjunto que temos hoje se deve a Georg Cantor. Cantor (pronuncia-se Cântor) julgava que, para definir um conjunto, bastava que se desse uma propriedade que deveria ser satisfeita por seus elementos. Esta definição apresenta problemas, ou seja, não corresponde exatamente a uma "boa" definição porque há paradoxos em decorrência da imprecisão do conceito de conjunto, ainda hoje à espera de solução. Apesar disso, a importância da Teoria dos Conjuntos não é diminuída.

3. Conhecendo a Temática

3.1 Definição de conjunto

Um conjunto é definido como uma coleção qualquer de objetos: letras do alfabeto, números, pessoas, animais, conjuntos etc. Qualquer coleção de objetos pode ser considerada como conjunto.

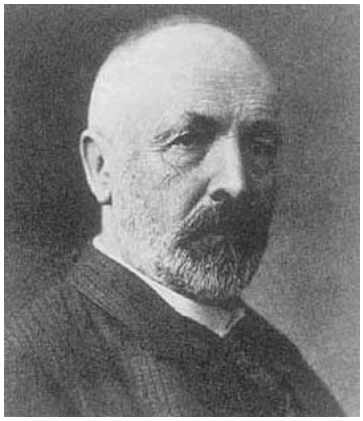
Os objetos de um conjunto são os seus elementos. Por exemplo, considere a coleção I de todos os números naturais ímpares 1,3,5,7,... Qualquer número natural ímpar pertence à coleção (conjunto) I. Denotamos a relação entre um conjunto A e um seu elemento x qualquer por $x \in$ A (lê-se x pertence a A). Se um elemento y não pertence a A, escreve-se $y \notin$ A.

A notação usada para representar um conjunto consiste em colocar seus elementos entre chaves ou em definir uma propriedade a ser satisfeita por todos os seus elementos:

V = {a,e,i,o,u} = conjunto das vogais do nosso alfabeto
$\mathbb{N}$ = {1,2,3, ...} = conjunto dos números naturais

$\mathbb{Z} = \{0,\pm1,\pm2,\pm3, ...\}$ = conjunto dos números inteiros
$\mathbb{Q} = \{p/q \mid p,q \in \mathbb{Z}, q \neq 0\}$ = conjunto dos números racionais
$A = \{1,2,3,4,5,6\} = \{x \in \mathbb{N} \mid 1 \leq x \leq 6\}$ (lê-se: conjunto dos x pertencentes a $\mathbb{N}$ tais que $1 \leq x \leq 6$)

Ampliando seu conhecimento



George Ferdinand Ludwig Philipp Cantor (São Petersburgo, 3 de Março de 1845 - Halle, Alemanha, 6 de Janeiro de 1918) foi um matemático russo de origem alemã conhecido por ter criado a moderna Teoria dos conjuntos. Foi a partir desta teoria que chegou ao conceito de número transfinito, incluindo as classes numéricas dos cardinais e ordinais, estabelecendo a diferença entre estes dois conceitos que colocam novos problemas quando se referem a conjuntos infinitos.

Nasceu em São Petersburgo (Rússia), filho de um comerciante dinamarquês, George Waldemar Cantor, e de uma música russa, Maria Anna Böhm. Em 1856 a sua família mudou-se para a Alemanha, continuando aí os seus estudos. Estudou na Escola Politécnica de Zurique. Doutorou-se na Universidade de Berlim em 1867. Teve como professores Ernst Kummer, Karl Weierstrass e Leopold Kronecker.

Em 1872 foi docente na Universidade alemã de Halle, onde obtém o título de professor em 1879. Toda a sua vida irá tentar em vão deixar Halle, tendo acabado por pensar que era vítima de uma conspiração.

Cantor provou que os conjuntos infinitos não têm todos a mesma potência (potência significando "tamanho"). Fez a distinção entre conjuntos numeráveis (ou enumeráveis) e conjuntos contínuos (ou não-enumeráveis).
Provou que o conjunto dos números racionais $\mathbb{Q}$ é enumerável, enquanto que o conjunto dos números reais $\mathbb{R}$ é contínuo (logo, “maior” que o anterior). Na demonstração foi utilizado o célebre argumento da diagonal de Cantor ou método diagonal. Nos últimos anos de vida tentou provar, sem o conseguir, a "hipótese do contínuo", ou seja, que não existem conjuntos de potência intermdiária entre os enumeráveis e os contínuos - em 1963, Paul Cohen demonstrou a indemonstrabilidade desta hipótese. Em 1897, Cantor descobriu vários paradoxos suscitados pela Teoria dos conjuntos. Foi ele que utilizou pela primeira vez o símbolo $\mathbb{R}$ para representar o conjunto dos números reais.

Durante a última metade da sua vida sofreu repetidamente de ataques de depressão, o que comprometeu a sua capacidade de trabalho e o forçou a ficar hospitalizado várias vezes. Provavelmente ser-lhe-ia diagnosticado, hoje em dia, um transtorno bipolar - vulgo maníaco-depressivo. A descoberta do **Paradoxo de Russell** conduziu-o a um esgotamento nervoso do qual não chegou a se recuperar. Começou, então, a se interessar por literatura e religião. Desenvolveu o seu conceito de Infinito Absoluto, que Georg Cantor identificava a Deus. Ficou na penúria durante a Primeira Guerra Mundial, morrendo num hospital psiquiátrico em Halle.

Os conceitos matemáticos inovadores propostos por Cantor enfrentaram uma resistência significativa por parte da comunidade matemática da época. Os

matemáticos modernos, por seu lado, aceitam plenamente o trabalho desenvolvido por Cantor na sua Teoria dos Conjuntos, reconhecendo-a como uma mudança de paradigma da maior importância.

Nas palavras de David Hilbert: "Ninguém nos poderá expulsar do Paraíso que Cantor criou."

Fonte: *Wikipédia*

3.2 Subconjuntos

Assumiremos que os caros leitores já estejam familiarizados com os conjuntos numéricos: dos números naturais ($\mathbb{N}$), dos números inteiros ($\mathbb{Z}$), dos números racionais ($\mathbb{Q}$), dos números irracionais ($\mathbb{I}$) e dos números reais ($\mathbb{R}$).

Definição 3.2.1 Dizemos que A é subconjunto de B se todos os elementos de A são também elementos de B. Neste caso, escrevemos $A \subset B$ (lê-se A está contido em B).

Temos $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. Dois conjuntos A e B são iguais se os elementos de A são os mesmos elementos de B e vice-versa, ou seja, $A \subset B$ e $B \subset A$.

Observe o conjunto $A = \{x \in \mathbb{Z} \mid x^2 = 1\}$. É fácil identificar seus elementos como sendo -1 e 1, ou seja, $A = \{-1,1\}$. E se fosse $A = \{x \in \mathbb{Z} \mid x^2 = -1\}$? Neste caso não existe valor $x \in \mathbb{Z}$ que satisfaça à propriedade dada, isto é, A não possui elementos! O conjunto assim definido é chamado vazio e denotado por $\varnothing$ ou por $\{\ \}$. Um erro bastante comum é escrever o conjunto vazio como $\{\varnothing\}$, mas este conjunto possui um elemento, o conjunto $\varnothing$, não podendo ser chamado de vazio. Podemos escrever, neste caso, que $\varnothing$ é um elemento de $\{\varnothing\}$, ou seja, $\varnothing \in \{\varnothing\}$.

Muitas vezes, quando queremos provar que uma afirmativa A implica em outra afirmativa B, provamos que a negação de B (~B) implica na negação de A (~A), ou seja, "$A \Rightarrow B$" equivale a "$\sim B \Rightarrow \sim A$". O uso desse tipo de argumentação, denominado *Contraposição*, é muito comum em Matemática e, certamente, você já se deparou com ele. Por exemplo, para provar que $X \subset Y$, precisamos mostrar que todo elemento de X é elemento de Y ou, equivalentemente, que todo elemento que não está em Y também não está em X.

Exemplo Prove que, qualquer que seja o conjunto A, $\varnothing \subset A$.

Prova Se $x \notin A$ então $x \notin \varnothing$, pois $\varnothing$ não possui elementos.

Observação Os símbolos $\subset$ (está contido) e $\supset$ (contém) só podem ser usados entre conjuntos. Já $\in$ (pertence) e $\notin$ (não pertence) são utilizados entre elementos e conjuntos.

Definição 3.2.2 Dados dois conjuntos A e B, a **união** $A \cup B$ é o conjunto de todos os elementos que estão em A **ou** em B, ou seja, $A \cup B$ é o conjunto de todos os elementos que pertencem a, pelo menos, um dos conjuntos. A **interseção** $A \cap B$ é o conjunto de todos os elementos que estão em A **e** em B, ou seja, dos elementos comuns a A e a B. Note que, se $A \cap B = \varnothing$, então A e B não possuem elementos em comum. Neste caso, dizemos que A e B são disjuntos.

Exemplos 1) Se $A = \{1,2,3,4,5\}$ e $B = \{1,3,5,7,9\}$, temos $A \cup B = \{1,2,3,4,5,7,9\}$ e $A \cap B = \{1,3,5\}$

2) $\mathbb{N} \cap \mathbb{Z} = \mathbb{N}$, $\mathbb{N} \cup \mathbb{Z} = \mathbb{Z}$, $\mathbb{Q} \cup \mathbb{I} = \mathbb{R}$ e $\mathbb{Q} \cap \mathbb{I} = \varnothing$, sendo $\mathbb{I}$ o conjunto dos números irracionais.

3.3 O Paradoxo de Russel

Um **paradoxo** é uma declaração aparentemente verdadeira que leva a uma contradição lógica, ou a uma situação que contradiz a intuição comum. Relacionado com a antítese, o paradoxo é uma figura de pensamento que consiste na exposição contraditória de ideias.

Em 1901, Bertrand Russell propôs seu famoso **paradoxo** que prova que a teoria de conjuntos de Cantor e Frege é contraditória:

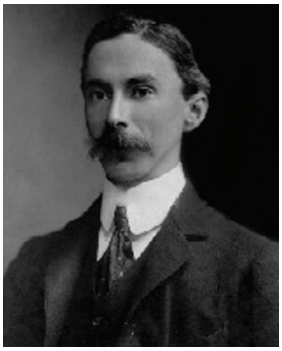
Considere-se o conjunto P como sendo "o conjunto de todos os conjuntos que não contêm a si próprios como membros". Formalmente: A é elemento de P se e só se A não é elemento de A.

$$P = \{A : A \notin A\}$$

No sistema de Cantor, P é um conjunto bem definido. Será que P contém a si mesmo? Se sim, não é membro de P de acordo com a definição. Por outro lado, supondo que P não contém a si mesmo, tem de ser elemento de P, de acordo com a definição de P. Assim, ambas as afirmações "P é elemento de P" e "P não é elemento de P" conduzem a contradições.

Ampliando seu conhecimento

Bertrand Arthur William Russell, 3º Conde Russell (Ravenscroft, País de Gales, 18 de Maio de 1872 — Penrhyndeudraeth, País de Gales, 2 de Fevereiro de 1970) foi um dos mais influentes matemáticos, filósofos e lógicos que viveram (em grande parte) no século XX. Um importante político liberal, ativista e um popularizador da Filosofia. Milhões de pessoas respeitaram Russell como uma espécie de profeta da vida racional e da criatividade. A sua postura em vários temas foi controversa.



Russell nasceu em 1872, no auge do poderio econômico e político do Reino Unido, tendo morrido em 1970, vítima de uma gripe, quando o império se tinha desmoronado e o seu

poder drenado em duas guerras vitoriosas mas debilitantes. Até à sua morte, a sua voz deteve sempre autoridade moral, uma vez que ele foi um crítico influente das armas nucleares e da guerra estadunidense no Vietnam.

Em 1950, Russell recebeu o Prémio Nobel da Literatura "em reconhecimento dos seus variados e significativos escritos, nos quais ele lutou por ideais humanitários e pela liberdade do pensamento".

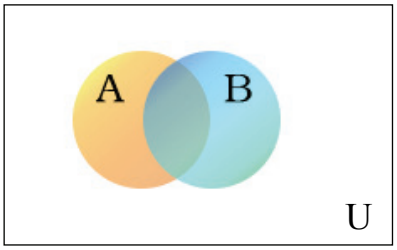
Fonte: Wikipedia

Em http://pt.wikipedia.org/wiki/Paradoxo_do_barbeiro encontramos mais um paradoxo atribuído a Russell que, pode-se dizer, equivale, metaforicamente, ao paradoxo acima. Acesse e veja. Para um acesso mais rápido, busque, no *Google*, Paradoxo do barbeiro.

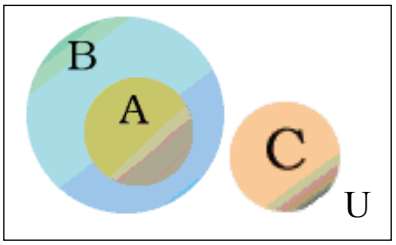
Exercício Dê exemplo de um conjunto que contém a si mesmo como elemento (desafio!).

3.4 Operações com conjuntos e os Diagramas de Euler-Venn

Para estudar de maneira mais simples as operações com conjuntos, Euler (lê-se Óiler) e Venn, separadamente (Leonhard Euler é do século XVIII e John Venn é do século XIX) pensaram numa representação gráfica para conjuntos, pensando seus elementos como limitados por círculos, cada um representando um conjunto diferente. Na verdade Euler criou a representação e Venn a popularizou.



No diagrama ao lado, os conjuntos A e B, representados por círculos, estão imersos em um conjunto maior, o conjunto universo, aqui representado pelo retângulo. Por exemplo, se A e B são subconjuntos de $\mathbb{R}$, U será o conjunto dos números reais. Se A e B são conjuntos de funções deriváveis $f: D \subset \mathbb{R} \to \mathbb{R}$, U será o conjunto de todas as funções deriváveis $f: D \subset \mathbb{R} \to \mathbb{R}$.

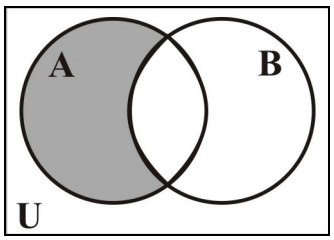


No diagrama ao lado, observe que o conjunto A é subconjunto de B, A e C são disjuntos, B e C são também disjuntos. A ideia é que, com o diagrama de Venn, percebamos claramente todas as operações – e os resultados destas – sem muito esforço intelectual. Temos, para o diagrama ao lado:

$$A \cup B = B;\ A \cap B = A;\ A \cap C = \varnothing \text{ e } B \cap C = \varnothing$$

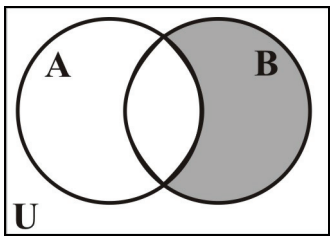
Definição 3.4.1 Dados A e B conjuntos, definimos a **diferença** A – B como sendo o conjunto de todos os elementos de A que não pertencem a B. Em símbolos:

$$A - B = \{x \in A \mid x \notin B\}$$



No diagrama à esquerda temos a representação de A – B.

No diagrama à direita temos a representação de B – A.

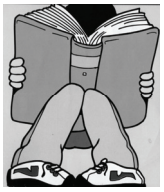


Exemplo Dados $\mathbb{N} = \{1,2,3,4,...\}$ e $P = \{2,4,6,8,...\}$, então $\mathbb{N} - P = \{1,3,5,7,9...\}$ enquanto que $P - \mathbb{N} = \varnothing$. Se $\mathbb{R}$ é o conjunto dos números reais e $\mathbb{Q}$ é o conjunto dos números racionais, então $\mathbb{R} - \mathbb{Q} = \mathbb{I}$ (conjunto dos números irracionais) e $\mathbb{Q} - \mathbb{R} = \varnothing$. Note que, sempre que $A \subset B$, temos $A - B = \varnothing$.

Dialogando e Construindo Conhecimento

Escrevendo para aprender

- Se $A \cup B = B$, então A é subconjunto de B.
- Se $A \cap B = B$, então B é subconjunto de A.



Considere U o conjunto universo e A um subconjunto de U. Definimos o **complementar** de A como sendo o conjunto $A^c = U - A$. Por exemplo, se $U = \mathbb{N}$ e A = conjunto dos números pares, temos $A^c = \{1,3,5,...\}$ = conjunto dos números ímpares.

Teorema 3.4.1 (Leis de **De Morgan**) Dados A e B subconjuntos de U = conjunto universo, então:

1. $(A^c)^c = A$
2. $\varnothing^c = U$ e $U^c = \varnothing$
3. $A \cup A^c = U$ e $A \cap A^c = \varnothing$
4. $A \subset B \Leftrightarrow B^c \subset A^c$
5. $(A \cup B)^c = A^c \cap B^c$ e $(A \cap B)^c = A^c \cup B^c$

Demonstração Vamos provar o item 4 e deixar os outros itens como exercício:

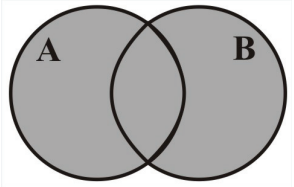
Suponhamos que $A \subset B$. Dado $x \in B^c$, temos que $x \notin B$ e, por conseguinte, $x \notin A$, uma vez que $A \subset B$. Portanto $x \in A^c$, ou seja, $A \subset B \Rightarrow B^c \subset A^c$. A prova da recíproca é análoga.

Exercício Sejam A e B conjuntos. Dê uma condição necessária e suficiente para que seja verdadeira a afirmação: $A \cup (B - A) = A$.

Observe, no diagrama de Venn ao lado, que a afirmação acima não é verdadeira sempre.

O diagrama também "sugere" que condição deve ser imposta para se ter

$$A \cup (B - A) = A.$$



$A \cup (B - A) \neq A$

Definição 3.4.2 O conjunto das partes de um conjunto A é o conjunto que tem por elementos todos os subconjuntos de A. É denotado por $\mathbb{P}(A)$.

Exemplo Se $A = \{1,2\}$, teremos $\mathbb{P}(A) = \{\varnothing,\{1\},\{2\},A\}$.

Observe que o próprio conjunto A e o conjunto vazio sempre são elementos de $\mathbb{P}(A)$. Além disso, temos:

- $\varnothing \subset \mathbb{P}(A)$ e $\varnothing \in \mathbb{P}(A)$
- $A \in \mathbb{P}(A)$ mas, se $A \neq \varnothing$, $A \not\subset \mathbb{P}(A)$, pois os elementos de A não são elementos de $\mathbb{P}(A)$

Denotaremos o número de elementos de um conjunto finito A por n(A). Por exemplo, $n(\varnothing) = 0$

Teorema 3.4.2 Se o número de elementos de A é k então $\mathbb{P}(A)$ possui 2^k elementos.

A demonstração deste teorema, feita por indução, está na Unidade III.

Exercício Dado $A = \{\varnothing,1,\{\varnothing\}\}$, determine $\mathbb{P}(A)$.

Para a solução deste problema, lembre que, como A possui 3 elementos, $n(\mathbb{P}(A)) = 2^3 = 8$.

Definição 3.4.3 Quando A é um conjunto finito, o número n(A) é chamado cardinal de A, ou seja, o cardinal de um conjunto finito é o número de elementos desse conjunto.

O resultado a seguir associa o cardinal da união de dois conjuntos A e B com os cardinais de A e de B.

Teorema 3.4.3 Se A e B são conjuntos finitos, $n(A \cup B) = n(A) + n(B) - n(A \cap B)$.

Exercício Se $n(A) = 10$, $n(B) = 17$ e A é subconjunto de B, quantos elementos tem $A \cup B$?

Dialogando e Construindo Conhecimento

Escrevendo para aprender
Para obter uma demonstração do teorema acima, faça um diagrama de Venn colocando o número de elementos de cada parte envolvida: de A – B, de $A \cap B$ e de B – A. Veja que a soma dos números cardinais de cada uma das partes dá exatamente o cardinal de $A \cup B$. Conclua a demonstração.

3.5 Famílias de conjuntos

Nesta seção, abordaremos operações de união e interseção para uma "família" de conjuntos, indexada em uma coleção infinita L. Na verdade, a definição não difere da que já temos para o caso finito. Vejamos:

Definição 3.5.1 Dada uma família $\{A_\lambda\}$, $\lambda \in L$, o conjunto $\bigcup_{\lambda \in L} A_\lambda = \{x \mid x \in A_\lambda$ para algum $\lambda \in L\}$ e o conjunto $\bigcap_{\lambda \in L} A_\lambda = \{x \mid x \in A_\lambda$ para todo $\lambda \in L\}$.

Exemplo Considere $A_n = [-1/n,1/n]$, com $n \in N$. É fácil perceber que $\bigcup_{n \in N} A_n = A_1 = [-1,1]$, pois para todo $n \in N$, $A_n \subset A_1 = [-1,1]$. Observe também que o número 0 é o único elemento comum a todo A_n e, assim, temos $\bigcap_{n \in N} A_n = \{0\}$.

Exercícios 1. Considere $A_n = (0,1/n)$, com $n \in N$. Mostre que $\bigcap_{n \in N} A_n = \bigcap_{n=1}^{\infty} A_n = \emptyset$.

2. Tente encontrar uma família $\{A_n \mid n \in N\}$ tal que:

- Cada A_n é um intervalo aberto;
- $A_{n+1} \subset A_n$ para todo $n \in \mathbb{N}$;
- $\bigcap_{n \in N} A_n$ é um intervalo fechado.

Observação Quando a indexação se dá no conjunto dos números naturais $\mathbb{N}$, é comum escrever

$$\bigcap_{n \in N} A_n = \bigcap_{n=1}^{\infty} A_n \quad \text{e} \quad \bigcup_{n \in N} A_n = \bigcup_{n=1}^{\infty} A_n .$$

Neste curso, assumimos que o aluno está razoavelmente informado a respeito de funções. Conceitos como domínio, contradomínio, injetividade, sobrejetividade, bijetividade etc, são supostamente conhecidos. Em caso de necessidade, é sempre bom recorrer a textos onde tais assuntos se encontram.

Definição 3.5.2 Dada uma função $f : A \to B$, definimos a imagem inversa de $b \in B$ como sendo o conjunto
$f^{-1}(b) = \{x \in A \mid f(x) = b\}$.
Se $C \subset B$, definimos $f^{-1}(C) = \{x \in A \mid f(x) \in C\}$.

Observações 1. Uma função $f : A \to B$ é sobrejetiva se, e somente se, $f^{-1}(b)$ é não vazio para todo $b \in B$.
A função $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = x^2$, não é sobrejetiva pois $f^{-1}(-2) = \emptyset$.

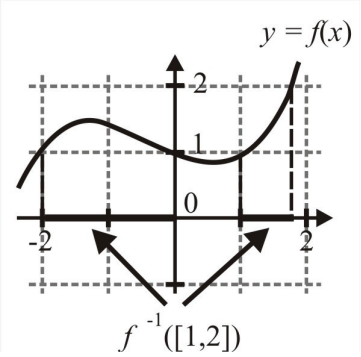
2. Se $f : A \to B$ e $g : B \to C$ são sobrejetivas então a função composta $g \circ f : A \to C$ é sobrejetiva. Se f e g são injetivas, $g \circ f$ é injetiva. Assim, se tivermos f e g bijetivas, $g \circ f$ também será bijetiva.

Exercício Prove as afirmativas das observações 1 e 2.

Exemplo Dada $f : \mathbb{N} \to \mathbb{N}$ definida por $f(x) = x^2$, temos $f^{-1}(3) = \emptyset$ e $f^{-1}(\{1,2,3,4\}) = \{1,2\}$

Exercício Considere a função $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x^2$. Dê um subconjunto não vazio B de R tal que $f^{-1}(B) = \emptyset$.

No gráfico a seguir, temos representada uma função $y = f(x)$ e o conjunto $f^{-1}([1,2])$. No gráfico, notamos que $f^{-1}([1,2]) = [-2,0] \cup [1,a]$, onde a é tal que $f(a) = 2$.



Suponhamos que a função a seguir seja:

- contínua em todo o conjunto $\mathbb{R}$;
- $\lim_{x \to \pm\infty} f(x) = \pm\infty$;
- crescente para $x > 2$ e para $x < -2$.

Sendo assim, o que é $f^{-1}([2,\infty])$?

Exemplo Considere a função $f : \mathbb{N} \to \mathbb{N}$ definida por $f(n)$ = soma dos algarismos da representação decimal de n. Para esclarecer exatamente como é esta função, observe os seguintes exemplos:
$f(30) = 3 + 0 = 3$, $f(37) = 3 + 7 = 10$, $f(307) = 3 + 0 + 7 = 10$.
Mostre que:
a) Dado $n \in \mathbb{N}$, $A_n = f^{-1}(n) = \{k \in \mathbb{N} \mid f(k) = n\}$ é um subconjunto infinito de $\mathbb{N}$, para todo $n \in \mathbb{N}$.
b) Se $n \neq m$, $f^{-1}(n) \cap f^{-1}(m) = \emptyset$.
c) $\bigcup_{n \in N} A_n = \mathbb{N}$.

Solução Provaremos o item (a):
Dado $n \in \mathbb{N}$, temos $f(111...1) = 1 + 1 + 1 + ... + 1 = n$ (o número de vezes que aparece o algarismo 1 é evidente, não?)
Mas $f(111...1) = f(111...10) = f(111...100) = ...$ e, portanto, concluímos que $\{111...1, 111...10, 111...100, ...\}$ é subconjunto – claramente infinito – de $f^{-1}(n)$ e daí $f^{-1}(n)$ é infinito pois um conjunto finito não pode conter um subconjunto infinito.

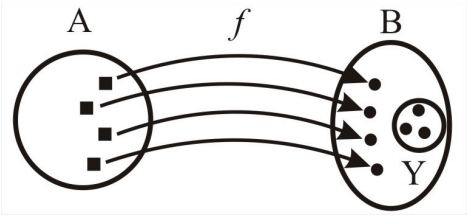
Teorema 3.5.1 Uma função $f : A \to B$ é sobrejetiva se, e somente se, $f(f^{-1}(Y)) = Y$, $\forall\, Y \subset B$ e é injetiva se, e somente se,

$$(f^{-1}(f(X)) = X, \forall\, X \subset A.$$

Exercícios 1) Dê exemplo de uma função não sobrejetiva $f : A \to B$ tal que $f(f^{-1}(Y)) \neq Y$ para algum subconjunto Y de B.

2) Dê exemplo de uma função não injetiva $f : A \to B$ tal que não ocorre $(f^{-1}(f(X)) = X$, para algum subconjunto X de A.

Sugestão: Para a solução do exercício 1 veja o diagrama ao lado, representando uma função não sobrejetiva $f : A \to B$.
Pelo diagrama ao lado, temos $f^{-1}(Y) = \varnothing$. Portanto, temos que $f(f^{-1}(Y)) = \varnothing \neq Y$.



Para a solução de (2), considere $f : A \to B$ tal que o número de elementos de A seja maior do que 1 e $f(x) = b_o \in B$, para todo $x \in A$ (f é uma função constante). Considere X um subconjunto próprio de A, ou seja, $X \subset A$ e $X \neq A$. Desta forma temos $f(X) = \{b_o\}$ e, como f é constante, $(f^{-1}(f(X)) = f^{-1}(b_o) = A \neq X$.

4. Avaliando o que foi construído

Nesta unidade, fizemos uma breve revisão da Teoria dos Conjuntos sobre o que consideramos de fundamental importância para o estudante de Matemática. Além de uma apresentação das operações sobre conjuntos e suas principais propriedades, fizemos ver que, apesar de ser uma teoria que apresenta algumas inconsistências, a sua relevância para o estudo da disciplina não é diminuída, haja vista a sua presença em todos os campos de estudo desta Ciência.

No Moodle

Agora vá à plataforma MOODLE e procure responder as questões e resolver os exercícios referentes ao tema estudado.

Unidade II Relações de Equivalência e Conjunto Quociente

1. Situando a Temática

Nesta unidade introduzimos os conceitos de Relação de Equivalência e de Conjunto Quociente, muito importantes no estudo das Estruturas Algébricas.

2. Problematizando a Temática

A Matemática tem atraído e ocupado grandes pensadores da História da Humanidade, desde Arquimedes e Euclides, na Grécia Antiga, até os dias de hoje, com um enorme contingente de cérebros trabalhando para descobrir novas teorias ou avançando cada vez mais nos campos já existentes, bem como, não menos importante, ajudando a disseminar o conhecimento matemático e motivando novos discípulos para a prática da Ciência.

O que leva a humanidade a estudar Matemática? Muitos hão de responder que é a utilidade demonstrada por essa ciência em praticamente todos os campos do conhecimento humano, notadamente em Física, Economia e Engenharia. Verdade. Mas também é verdade que muito provavelmente Euclides não estava preocupado com aplicações práticas quando escreveu seus famosos *Elementos*, bem como os pesquisadores atuais de Matemática "pura". Nós a estudamos porque somos humanos, pura e simplesmente, e, como humanos, temos a curiosidade de sempre saber mais, não importa se o conhecimento é sobre estrelas que estão a milhões de anos-luz – e que não interferem no nosso planeta – ou se são os mistérios da Natureza, a beleza da Música ou a "simplicidade" e o rigor da Matemática.

Quando estudamos Geometria Euclidiana, segmentos congruentes, bem como ângulos congruentes ou quaisquer figuras geométricas congruentes, são tratados como um único objeto, não importando se um triângulo está localizado aqui e outro, congruente, está a 10 quilômetros. O mesmo pode se dar em qualquer conjunto, quando desejamos tratar da mesma forma elementos que satisfaçam determinadas propriedades. Por exemplo, no conjunto dos números inteiros $\mathbb{Z}$, podemos reunir todos os pares numa classe e tratá-los como se fossem um só elemento e os ímpares (outra classe) também como outro elemento. Desta forma, escolhemos um elemento no conjunto dos pares, pode ser o número 0, como representante de todos eles e escolher o número 1 para representante dos ímpares. Esse "novo" conjunto (das classes de pares e ímpares) é denotado por $\mathbb{Z}_2 = \{0,1\}$.

3. Conhecendo a Temática

3.1 Relações de Equivalência

O produto cartesiano entre dois conjuntos A e B é definido como sendo o conjunto dos pares ordenados (x,y) tais que $x \in A$ e $y \in B$ e é denotado por AxB. Em símbolos,

$AxB = \{(x,y) \mid x \in A \text{ e } y \in B\}$

Exemplo Dados A = {a,b,c} e B = {1,2}, temos AxB = {(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)}

Note que, quando A e B são finitos, o número de elementos de AxB é o produto do número de elementos de A pelo número de elementos de B.

Definição 3.1.1 Uma relação binária R entre os elementos de um conjunto A com os elementos de um conjunto B ($R : A \to B$) é um subconjunto do produto cartesiano AxB. Quando $(x,y) \in R$, escrevemos xRy.

Exemplo Dados A = {a,b,c} e B = {1,2,3,4,5}, considere R = {(a,3), (b,2),(b,5)}. Neste caso, temos aR3, bR2 e bR5, c não está relacionado a nenhum elemento de B e há elementos de B que não se relacionam com qualquer elemento de A, a saber, 1 e 4.

A definição a seguir é a mais importante desta unidade.

Definição 3.1.2 Seja A um conjunto não vazio. Uma relação binária $R : A \to A$ que satisfaz às seguintes propriedades é chamada Relação de Equivalência em A:

- xRx, $\forall\, x \in A$ (R é reflexiva)
- Se xRy então yRx (R é simétrica)
- Se xRy e yRz então xRz (R é transitiva)

É costume adotar a notação $\sim$ para uma relação de equivalência em um conjunto A e será esta notação que adotaremos a partir de agora. Sempre que mencionarmos uma relação de equivalência em um conjunto A, estaremos assumindo que $A \neq \emptyset$.

Exemplos 1. No conjunto $\mathbb{R}$, dos números reais, vamos provar que

$x \sim y$, se, e somente se, $x - y \in \mathbb{Z}$,

é uma relação de equivalência em $\mathbb{R}$:

$\sim$ é reflexiva: $x = y \Leftrightarrow x - y = x - x = 0 \in \mathbb{Z} \Leftrightarrow x \sim x$.

$\sim$ é simétrica: $x \sim y \Leftrightarrow x - y \in \mathbb{Z}$ e daí $y - x = -(x - y) \in \mathbb{Z}$, ou seja, $y \sim x$.

$\sim$ é transitiva: $x \sim y \Leftrightarrow x - y \in \mathbb{Z}$ e $y \sim z \Leftrightarrow y - z \in \mathbb{Z}$ e, portanto, $x - z = (x - y) + (y - z) \in \mathbb{Z}$, ou seja, $x \sim z$.

2. A relação $\leq$ não é uma relação de equivalência em $\mathbb{R}$ pois não é simétrica: $1 \leq 2$ mas 2 não é ≤ 1.

3. Considere $X \neq \varnothing$ e A, B subconjuntos de X. $A \sim B \Leftrightarrow A \subset B$ não é uma relação de equivalência em $\mathbb{P}(X)$ por não ser simétrica: $A \subset B$ não implica $B \subset A$.

4. Em $\mathbb{R}$, a relação $x \approx y \Leftrightarrow |x - y| \leq 1$ não é transitiva ($1 \approx 2$ e $2 \approx 3$ mas $|3 - 1| = 2 > 1$) e, portanto, $\approx$ não é relação de equivalência em $\mathbb{R}$.

5. Considere E^3 o conjunto dos vetores no espaço e $\sim$ a relação definida por: $\mathbf{u} \sim \mathbf{v} \Leftrightarrow \mathbf{u}$ e $\mathbf{v}$ possuem a mesma direção. Neste caso, $\sim$ é uma relação de equivalência em E^3.

6. Se A é o conjunto de todas as retas de um plano. Perpendicularismo não é uma relação de equivalência em A, pois uma reta não é perpendicular a si mesma.

7. Em Álgebra Linear, uma relação de equivalência que se faz sempre presente entre Espaços Vetoriais é dada pelos isomorfismos: $V \sim W \Leftrightarrow$ existe $T : V \to W$ isomorfismo (Transformação linear bijetora), sendo V, W espaços vetoriais. Assim, um espaço vetorial V sobre o corpo $\mathbb{R}$ de dimensão n sempre é associado (equivalente) a $\mathbb{R}^n$.

8. Semelhança entre matrizes quadradas é uma relação de equivalência: $A \sim B \Leftrightarrow$ existe uma matriz invertível P tal que $A = P^{-1}BP$, onde A, B e P são matrizes $n \times n$.

9. No conjunto dos números racionais $\mathbb{Q}$, definimos a relação $\sim$ da seguinte forma: $a/b \sim c/d \Leftrightarrow ad = bc$. Com esta relação, temos $2/4 \sim 1/2$; $3/5 \sim 9/15$; $1/4 \sim 3/12$ etc. Esta relação é exatamente a que define equivalência entre frações.

Exercício Prove que todas as relações definidas abaixo são Relações de Equivalência

1) Se A é o conjunto de todas as retas de um plano, a relação $r \sim s \Leftrightarrow r$ é paralela a s é uma relação de equivalência em A.

2) Se conjunto A é um conjunto não vazio, a relação $a \sim b \Leftrightarrow a = b$ é uma relação de equivalência em A.

3) Dada uma função $f : A \to B$, podemos definir uma relação de equivalência em A da seguinte forma: $x \sim y$ se $f(x) = f(y)$. Na relação definida desta forma para $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x^2$, temos $-1 \sim 1$. Em geral, que elementos se relacionam, desta forma, com $x \in \mathbb{R}$?

4) Considere $f : \mathbb{Z} \to \mathbb{Z}$ definida por $f(n)$ = resto da divisão de n por 2. Com a relação de equivalência definida em (3) temos que $0 \sim p$, para todo número par p, e $1 \sim i$, para todo número ímpar i.

5) Considere A o conjunto de todas as pessoas e ~ a relação "ter a mesma idade".

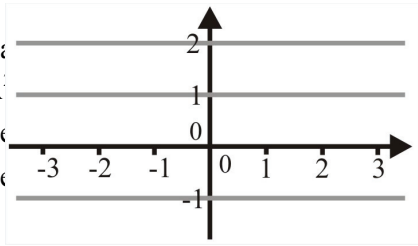
6) A é o conjunto das palavras da língua portuguesa e ~ a relação "ser um anagrama". Com esta relação, rato ~ rota ~ ator, mato ~ toma etc.

Se ~ é uma relação de equivalência em A e $x \sim y$, dizemos que x equivale a y (módulo ~). Assim, com a relação de equivalência ~ do exemplo (4), 102 equivale a 0 (módulo ~) e 27 equivale a 1 (módulo ~).

3.2 Classes de Equivalência

Definição 3.2.1 Dada uma relação de equivalência ~ em um conjunto A, para cada $x \in A$ consideremos o conjunto
$\bar{x} = \{a \in A \mid a \sim x\}$.

$\bar{x}$ é chamado **Classe de Equivalência** de x (módulo ~).



O item (3) do exercício acima nos diz que toda função induz uma relação de equivalência em seu domínio. Considerando a função $f : D \subset \mathbb{R}^2 \to \mathbb{R}$ contínua e ~ a relação de equivalência associada a f, as classes de equivalência módulo ~ são as curvas de nível de f. Se $f(x,y) = y$, as classes de equivalência correspondentes são retas horizontais.

As classes de equivalência (curvas de nível) correspondentes à função $f(x,y) = x^2 + y^2$ são círculos de centro na origem.

No item (2) do exercício acima, a classe de equivalência de x (módulo ~) é o conjunto unitário $\bar{x} = \{x\}$. Já no item (3), temos $\bar{x} = \{-x,x\}$ e,

no exemplo (4), $\overline{x} = \{0,\pm2,\pm4,\pm6,...\}$, se x é par e $\overline{x} = \{\pm1,\pm3,\pm5,...\}$, se x é ímpar.

Exemplo Determine todas as classes de equivalência (módulo ~), onde ~ = {(0,0), (0,1), (0,2), (1,0), (1,2), (2,0), (2,1), (1,1), (2,2), (3,3), (3,4), (4,3), (4,4)} é a relação de equivalência (mostre isto) no conjunto A = {0,1,2,3,4}.

Solução $\overline{0} = \{0,1,2\}$ e $\overline{3} = \{3,4\}$ são as únicas classes de equivalência em A (módulo ~).

Teorema 3.2.1 Dada uma relação de equivalência ~ em um conjunto A e $\overline{x}$, $\overline{y}$ duas classes de equivalência (módulo ~) distintas, então $\overline{x} \cap \overline{y} = \varnothing$.

Prova Suponhamos, por absurdo, que $\overline{x} \cap \overline{y} \neq \varnothing$. Então existe $a \sim x$ para algum $x \in \overline{x}$ e $a \sim y$, para algum $y \in \overline{y}$. Mas, por transitividade, $a \sim x$, $\forall\, x \in \overline{x}$ e, analogamente, $a \sim y$, $\forall\, x \in \overline{y}$ e assim, todos os elementos de $\overline{x}$ são também elementos de $\overline{y}$ e vice-versa, ou seja, $\overline{x} = \overline{y}$, contrariando a hipótese de serem classes de equivalência distintas.

Exemplo Em $\mathbb{R}^2$, suponha a relação: $(a,b) \approx (c,d) \Leftrightarrow (a,b)$ e (c,d) são pontos de uma mesma reta que passa pela origem (0,0). Por exemplo, (1,2) e (2,4) são pontos da reta de equação $y = 2x$, ou seja, $(1,2) \approx (2,4)$. Já (2,2) e (2,3) estão sobre a reta vertical $x = 2$, que não passa pela origem e, por isso, não temos $(2,2) \approx (2,3)$. A relação $\approx$, definida desta maneira, não é uma relação de equivalência em $\mathbb{R}^2$ pois, supondo $\approx$ uma relação de equivalência, teríamos (0,0) em todas as classes de equivalência, o que contradiz o teorema acima. No entanto, com a mesma definição, $\approx$ é uma relação de equivalência em $\mathbb{R}^2 - \{(0,0)\}$.

Exemplo Em $\mathbb{Z}$, considere a relação: $a \sim b \Leftrightarrow a - b$ é múltiplo de 3, ou seja, $a - b = 3n$ para algum n inteiro. Mostre que ~ é uma relação de equivalência e determine todas as classes de equivalência módulo ~.

Solução Para todo $a \in \mathbb{Z}$, $a - a = 0 = 3\cdot0$. Logo $a \sim a$.

Se $a \sim b$, $a - b = 3\cdot n$ para algum inteiro n e, daí, $b - a = -(a - b) = 3\cdot(-n)$. Logo $b \sim a$.

Se $a \sim b$ e $b \sim c$, temos $a - b = 3\cdot n$, para algum inteiro n e $b - c = 3\cdot m$, para algum inteiro m e então temos $a - c = (a - b) + (b - c) = 3\cdot n + 3\cdot m = 3\cdot(n + m)$, donde concluímos que $a \sim c$.

Observe que $\overline{0} = \{0, \pm3, \pm6, \pm9, ...\}$, $\overline{1} = \{\pm1, \pm4, \pm7, ...\}$, $\overline{2} = \{\pm2, \pm5, \pm8, ...\}$ são classes de equivalência módulo ~ e, como $\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2}$, o teorema acima garante que estas são as únicas classes de equivalência módulo ~ em $\mathbb{Z}$.

Definição 3.2.2 A relação de equivalência em $\mathbb{Z}$, definida por

$$a \sim b \Leftrightarrow a - b \text{ é múltiplo de n,}$$

recebe o nome de congruência módulo n e é indicada por $\equiv$ (mod n). Por exemplo, $22 \equiv 1 \pmod 7$.

3.3 Conjunto Quociente

Considere o conjunto A = {1,3,1,1,3,5,5}. Os elementos de A são 1, 3 e 5 e, portanto, escrevemos de uma forma mais simplificada: A = {1,3,5}. Se temos, em um conjunto não vazio X, uma relação de equivalência ~, não há por que repetir os elementos que "equivalem". Por exemplo, se X = $\{x_1,x_2,x_3,x_4\}$ e ~ é a relação de equivalência em X tal que $x_1 \sim x_2$ e $x_3 \sim x_4$, o conjunto que nos interessa, neste caso, é $\{x_1,x_3\}$ já que x_2 "equivale" a x_1 e x_4 "equivale" a x_3. Alguns cuidados se fazem necessários: X e $\{x_1,x_3\}$ são conjuntos diferentes e não podem ser representados pela mesma letra X e essa "simplificação" de X depende do contexto em que se está trabalhando, ou seja, nas situações em que essa "equivalência" entre elementos de X seja considerada. Essa "simplificação" é consequência direta da escolha da relação de equivalência adotada para determindados fins. Intuitivamente, utilizamos relações de equivalência no nosso cotidiano: Numa farmácia, por exemplo, consideramos "equivalentes" os remédios que, em suas fórmulas, possuem o mesmo princípio ativo e optamos por adquirir o de menor preço. Se a carne de primeira é muito cara, compramos a de segunda pois esta tem o mesmo valor nutritivo.

Definição 3.3.1 Dada uma relação de equivalência ~ em A, o conjunto de todas as classes de equivalência (módulo ~) é chamado de conjunto quociente de A pela relação de equivalência ~ e denotamos tal conjunto por A/~. Em símbolos:

$A/\sim = \{\bar{x} \mid x \in A\}$

Observe que uma relação de equivalência ~ em A origina um único conjunto quociente A/~.

Considere, por exemplo, a relação de equivalência em $\mathbb{Z}$: $a \sim b \Leftrightarrow a - b$ é múltiplo de 2. Suas classes de equivalência são $\bar{0}$ e $\bar{1}$. Mas poderíamos definir da seguinte forma: $a \approx b \Leftrightarrow$ resto da divisão de a por 2 = resto da divisão de b por 2. A maneira de definir a relação de equivalência foi diferente, mas a relação é a mesma e $\mathbb{Z}/\sim = \mathbb{Z}/\approx$.

Se $\{A_\lambda \mid \lambda \in L\}$ é uma família de subconjuntos de $A \neq \varnothing$ tal que $\bigcup_{\lambda \in L} A_\lambda = A$ e $A_\lambda \cap A_\mu = \varnothing$ para $\lambda \neq \mu$, então a relação de equivalência ~, definida abaixo, é tal que $A/\sim = \{A_\lambda \mid \lambda \in L\}$

$$x \sim y \Leftrightarrow \exists\, \lambda \in L \text{ tal que } x,y \in A_\lambda.$$

Uma família como a definida acima é chamada de **Partição** do conjunto A. Dada uma partição para A, só existe uma relação de equivalência para o mesmo cujo conjunto quociente seja esta partição.

Exercício Dê exemplo de relação de equivalência em um conjunto $X \neq \varnothing$ tal que
a) $X/\sim = \{X\}$.
b) $\overline{x} = \{x\}$.
c) X seja um conjunto infinito e X/~ contenha exatamente 5 elementos.

Solução de (c): Como X é infinito, tomemos 4 elementos distintos de X: x_1, x_2, x_3 e x_4. Tomemos agora

$A_1 = \{x_1\}$, $A_2 = \{x_2\}$, $A_3 = \{x_3\}$, $A_4 = \{x_4\}$ e $A_5 = X - \{x_1, x_2, x_3, x_4\}$.

$\{A_i \mid i \in \{1,2,3,4,5\}\}$ é uma partição de X e, portanto, define uma (única) relação de equivalência em X e $X/\sim = \{A_1, A_2, A_3, A_4, A_5\}$.
Outra solução Considere $X = \mathbb{Z}$ e ~ a relação de equivalência: $a \sim b \Leftrightarrow a - b$ é múltiplo de 5. As classes de equivalência (módulo 5) são $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$ e $\overline{4}$. Quais são os elementos da classe de equivalência $\overline{3}$?

Exemplo Em $\mathbb{Z}$, a congruência módulo p ($a \sim b \Leftrightarrow a - b$ é múltiplo de p) nos dá $\mathbb{Z}/\sim = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \ldots, \overline{p-1}\}$, que também será representado por $\mathbb{Z}_p$. Qualquer que seja $p \in \mathbb{Z}$, temos que $\mathbb{Z}_p$ possui exatamente p elementos.

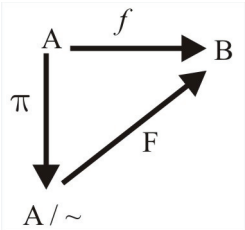
Exercício Descubra todas as relações de equivalência em $A = \{0,1,2\}$.

Sugestão: basta descobrir todas as partições de A.

Dada uma relação de equivalência ~ em A, a função $\pi : A \to A/\sim$, definida por $\pi(x) = \overline{x}$, é chamada de projeção canônica de A sobre A/~.

Dada uma função $f : A \to B$ e a relação de equivalência induzida, temos que $F : A/\sim \to B$, definida por $F(\overline{x}) = f(x)$ para algum $x \in \overline{x}$, é injetiva.

No caso em que f seja sobrejetiva, teremos F bijetiva.Veja o diagrama ao lado:



$$f(x) = F \circ \pi(x) = F(\pi(x)).$$

Exemplos 1. $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x)$ = maior inteiro menor ou igual a x, conhecida como função escada. $f(x)$ também se denota por $INT(x)$ que pode ser pensada como a parte inteira do número real x. Por exemplo, $INT(2{,}74) = 2$ e $\pi(2{,}74) = \overline{2} = [2,3)$. A relação de equivalência em $\mathbb{R}$, induzida por f, é $x \sim y \Leftrightarrow \exists\, n \in \mathbb{Z} \mid n \leq x, y < n + 1$. As classes de equivalência são intervalos do tipo $[a, a+1)$, onde $a \in \mathbb{Z}$. Podemos pensar

nos números inteiros para representantes de suas respectivas classes. Temos: $\overline{2} = [2,3)$, $\overline{n} = [n,n + 1)$, com $n \in \mathbb{Z}$.

A função $\pi : \mathbb{R} \to \mathbb{R}/\sim$ é definida como $\pi(x) = \overline{x} = \overline{INT(x)} = [INT(x), INT(x) + 1)$

Já a função $F : \mathbb{R}/\sim \to \mathbb{R}$ é dada por

$F(\overline{x}) = f(x) = INT(x)$

2. Sejam A e B conjuntos não vazios, com ~ e ≈ relações de equivalência em A e B respectivamente. Uma função $f : A \to B$ induz a função $f_* : A/\sim \to B/\approx$, dada por $f_*(\overline{x}) = \overline{f(x)}$. À direita, temos o diagrama, que é comutativo, ou seja, $f_*(\pi_A(x)) = \pi_B(f(x))$.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi_A"'] & B \arrow[d, "\pi_B"] \\ A/\sim \arrow[r, "f_*"'] & B/\approx \end{tikzcd}$$

3. Em $\mathbb{N}$, considere a relação de equivalência: $a \sim b \Leftrightarrow \exists\, n \in \mathbb{N} \mid 10(n - 1) \leq a, b < 10(n - 1) + 10$. Por exemplo $1 \sim 7$; $12 \sim 19$; $103 \sim 108$. Defina a função $f : N \to N$ como sendo $f(1) = f(2) = \cdots = f(9) = 1$; $f(10) = f(11) = \cdots = f(19) = 2$; $\cdots$; $f(10n) = f(10n + 1) = \cdots = f(10n + 9) = n - 1$; $\cdots$. Esta função induz a relação de equivalência dada e $f^{-1}(n) = \{10(n - 1), 10(n -1) + 1, 10(n - 1) + 2, \cdots , 10(n - 1) + 9\}$ é uma classe de equivalência.

Exercícios 1. Releia o exemplo 2 acima e, a partir da função $f : \mathbb{Z} \to \mathbb{Z}$, dada por $f(n) = 2n + 1$, construa o respectivo diagrama e descreva como é a função $f_* : \mathbb{Z}/\sim \to \mathbb{Z}/\approx$, sendo $\mathbb{Z}/\sim = Z_3$ e $\mathbb{Z}/\approx = Z_5$.

2. Partindo de uma relação de equivalência em um conjunto A, dê uma função $f : A \to A$ que induz esta relação de equivalência.

4. Avaliando o que foi construído

Nesta unidade, apresentamos o conceito de Relação de Equivalência em um conjunto A, verificando que toda relação de equivalência em $A \neq \varnothing$ está associada a uma função $f : A \to B$ e vice-versa, ou seja, dada $f : A \to B$, existe uma relação de equivalência em A associada a f. Com uma relação de equivalência ~ em A, "simplificamos" o conjunto A com o uso do conceito de conjunto quociente A/~.

No Moodle

Agora vá à plataforma MOODLE e procure responder as questões e resolver os exercícios referentes ao tema estudado.

Unidade III Enumerabilidade

1. Situando a Temática

Nesta unidade introduzimos os conceitos de boa ordenação, de número cardinal de um conjunto infinito, enumerabilidade e não enumerabilidade. Quando Cantor concebeu a Teoria dos Conjuntos pensou também em estender o conceito de número de elementos de um conjunto (número cardinal, que ele chamou também de potência) para conjuntos infinitos, no que teve pleno sucesso.

2. Problematizando a Temática

No caso de A e B serem finitos, isso é "mais ou menos" óbvio que f : A $\rightarrow$ B bijeção acarreta n(A) = n(B). Estendendo o conceito para conjuntos infinitos, Cantor define que A e B possuem a mesma potência se existir uma função bijetiva f : A $\rightarrow$ B. Assim o conjunto $\mathbb{N}$ dos números naturais tem a mesma potência que um subconjunto seu, o conjunto P dos números pares, haja visto que a função f : $\mathbb{N} \rightarrow$ P, definida por $f(a) = 2a$, é uma bijeção. A potência de um conjunto A é maior do que a potência de B quando não existe função g : B $\rightarrow$ A sobrejetiva. O nosso problema/objetivo será determinar em que "classe" de potência está um dado conjunto.

3. Conhecendo a Temática

3.1 Conjuntos parcialmente ordenados

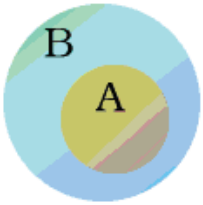
Definição 3.1.1 Dado um conjunto A $\neq \varnothing$, uma ordem parcial em A é uma relação binária $\leq$ que satisfaz:

- $x \leq x$, $\forall\, x \in$A (propriedade reflexiva)
- Se $x \leq y$ e $y \leq x$ então $x = y$ (propriedade antissimétrica)
- Se $x \leq y$ e $y \leq z$ então $x \leq z$ (propriedade transitiva)

O conjunto A, munido de uma ordem $\leq$, é denotado por (A, $\leq$) e é dito **parcialmente ordenado**.

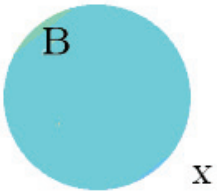
Exemplos 1. A desigualdade usual nos fornece uma ordem parcial para o conjunto dos números reais $\mathbb{R}$. Neste caso, dados dois elementos quaisquer x e y de $\mathbb{R}$, sempre existe a comparação: $x \leq y$ ou $y \leq x$. Observe que esta não é uma exigência para que tenhamos uma ordem parcial.

2. Dado X um conjunto não vazio, definimos uma ordem em $\mathbb{P}$(X), o conjunto das partes de X, por: A $\leq$ B se A $\subset$ B, onde A e B são subconjuntos de X.



$A \leq B$ pois $A \subset B$

Como nem $B \subset C$ nem $C \subset B$ então B e C não se comparam



Como $\varnothing \subset B \subset X$ temos a ordem $\varnothing \leq B \leq X$

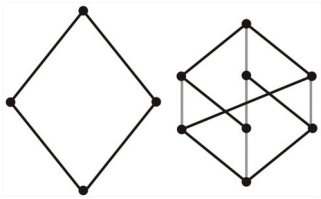
2.1 Em $\mathbb{P}(\mathbb{N})$, $\{1,2,3\} \leq \{1,2,3,4,5\}$ mas não podemos comparar (com a definição de ordem dada) os conjuntos $\{1,2,3\}$ e $\{2,3,4\}$.

3. Em $\mathbb{R}^2$, considere a ordem definida por $(x,y) \leq (u,v)$ se, e somente se, $x \leq u$ e $y \leq v$.Com esta ordem, $\mathbb{R}^2$ é parcialmente ordenado. Neste caso, temos $(1,2) \leq (1,5)$, $(0,0) \leq (3,2)$ mas, com esta ordem, não podemos comparar $(1,3)$ com $(2,1)$.

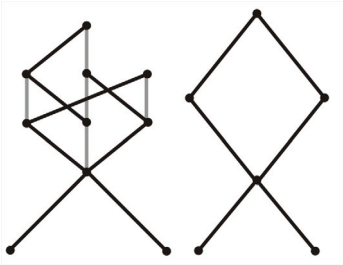
4. Em $\mathbb{R}^2$, considere a ordem definida por $(x,y) \leq (u,v)$ se, e somente se, $x \leq u$ ou, no caso em que $x = u$, $y \leq v$. $\mathbb{R}^2$, com esta ordem, é parcialmente ordenado. Neste caso, temos $(1,2) \leq (1,5)$, $(0,0) \leq (3,2)$ e, com esta ordem, podemos comparar quaisquer pares ordenados $(x,y) \in \mathbb{R}^2$.

3.2 Diagramas de Hasse

Dado um conjunto finito parcialmente ordenado $(X, \leq)$, é possível uma representação gráfica para ele. Tal representação é chamada de *Diagrama de Hasse*. O que indica a ordem $a \leq b$ é a ligação ascendente de a para b.



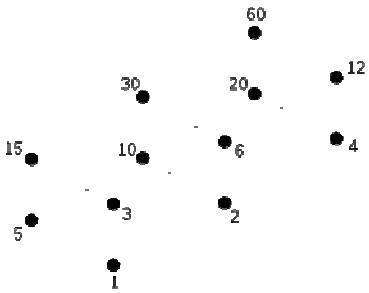
Nos diagramas ao lado, os conjuntos parcialmente ordenados representados possuem um menor elemento, representado, em cada caso, pelo ponto mais baixo do diagrama. Analogamente, possuem também um maior elemento, representado, em cada caso, pelo ponto mais alto do diagrama.



O primeiro diagrama de Hasse à direita representa um conjunto parcialmente ordenado que não possui menor elemento nem maior elemento.

Já o diagrama seguinte representa um conjunto parcialmente ordenado que possui um maior elemento, representado pelo ponto mais alto do diagrama, mas não possui um menor elemento.

O conjunto
$A = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$
de todos os divisores de 60, parcialmente ordenado por divisibilidade, tem o diagrama de Hasse ao lado.



A ordem por divisibilidade significa que $a \leq b$ se a divide b. Com esta ordem temos $1 \leq x \leq 60$, $\forall\, x \in A$.

Observação Quando, em um conjunto parcialmente ordenado A, tivermos a e $b \in$ A com $a \leq b$ e $a \neq b$, escrevemos $a < b$.

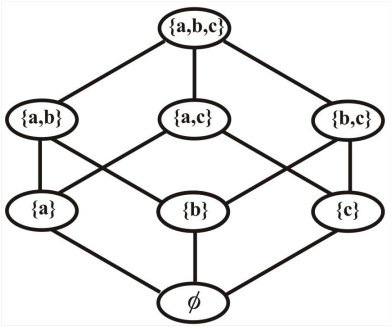
Exercícios 1. Construa um diagrama de Hasse para X = {1,2,3, ... ,10}, com a relação de ordem definida da seguinte forma: $a \leq b \Leftrightarrow b$ é múltiplo de a. Note que, com esta relação, X é parcialmente ordenado.

2. Qual é o diagrama de Hasse para X = {1,2,3, ... ,10}, com a ordem usual?

3. Faça o diagrama de Hasse para X = {1,2,3, ... ,10}, com a ordem definida por: $a \leq b \Leftrightarrow a$ e b são ímpares com a ordem usual ou $1 \leq 2 \leq 4 \leq 6 \leq \cdots \leq 10$.

4. Faça o diagrama de Hasse para X = {1,2,3, ... ,10}, com a ordem definida por: $a \leq b \Leftrightarrow a$ e b são ímpares com a ordem usual ou a e b são pares com a ordem usual. Por exemplo, 2 e 5 não se comparam e $1 \leq 9$.

Exemplo Dado A = $\{x,y,z\}$ e $\mathbb{P}$(A), o conjunto das partes de A, parcialmente ordenado por: X ≤ Y se X ⊂ Y, onde X e Y são subconjuntos de A, o diagrama de Hasse para ($\mathbb{P}$(A), ⊂) é:



Observando o diagrama ao lado, vemos que ∅ é o menor elemento e A = $\{x,y,z\}$ é o maior.

Os exemplos ao lado mostram que, dado um conjunto parcialmente ordenado A e x, y dois elementos quaisquer de A, não necessariamente teremos uma comparação de ordem envolvendo x e y.

3.3 Conjuntos Totalmente Ordenados

Uma relação de ordem parcial ≤ em um conjunto não vazio A é chamada de **total** se, e somente se, dados a e b quaisquer em A, ocorre $a \leq b$ ou $b \leq a$, isto é, dois elementos quaisquer sempre são comparáveis. Um conjunto A com ordem total é chamado de **totalmente ordenado**. Todo subconjunto de $\mathbb{R}$, com a ordem usual ≤, é totalmente ordenado.

Exemplo Em $\mathbb{R}^2$, considere a relação definida por $(x,y) \leq (u,v)$ se, e somente se, $x \leq u$. Esta relação não define uma ordem em $\mathbb{R}^2$ pois $(1,2) \leq (1,3)$ e $(1,3) \leq (1,2)$ mas $(1,2) \neq (1,3)$, ou seja a relação não é antissimétrica.

Note que só podemos chamar de Relação de Ordem Parcial quando forem satisfeitas as três propriedades (reflexiva, antissimétrica e transitiva). No exemplo 1, a propriedade antissimétrica não foi respeitada pela definição

dada. Observe também – e isto é muito importante – que, em um conjunto parcialmente ordenado, dois elementos quaisquer não são necessariamente comparáveis. Quando isso ocorre, temos uma relação de Ordem Total.

Se tivermos uma relação de ordem parcial (ou total) em A e uma função bijetora $f: A \to B$, então temos, em B, uma relação de ordem parcial (ou total), induzida por f, da seguinte forma: $b \leq c$ (em B) se, e somente se, $f^{-1}(b) \leq f^{-1}(c)$ (em A).

Definição 3.3.1 Seja A um conjunto parcialmente ordenado. Um subconjunto $B \subset A$ é dito limitado inferiormente se existir $a \in A$ tal que $a \leq x$, $\forall\, x \in B$. O elemento $a \in A$ é chamado cota inferior de B. Analogamente, definimos limitação superior e cota superior de um subconjunto $B \subset A$.

Exemplos 1. Com a relação de ordem usual de $\mathbb{R}$, o intervalo [2,5) é limitado tanto inferior quanto superiormente, sendo 2, ou qualquer número menor que 2, uma cota inferior e 5, ou qualquer número maior que 5, uma cota superior.

Este primeiro exemplo nos mostra que um conjunto X, mesmo que esteja contido em um conjunto totalmente ordenado como $\mathbb{R}$, pode ser limitado inferiormente (superiormente) sem que possua um menor (maior) elemento.

2. Se $X \neq \emptyset$, e A = conjunto das partes de X, com a relação de ordem $B \leq C$ se, e somente se, $B \subset C$, então todo subconjunto Y de A é limitado inferiormente, sendo o conjunto vazio uma cota inferior para Y. Y é também limitado superiormente. Dê uma cota superior para Y.

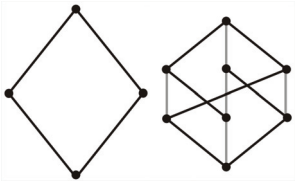
3. Com a relação de ordem usual de $\mathbb{N}$, todo subconjunto $X \neq \emptyset$ é limitado inferiormente, sendo $x_o = 1$ uma cota inferior para $X \subset \mathbb{N}$. No entanto, nem todo subconjunto de $\mathbb{N}$ é limitado superiormente.

3.4 Conjuntos Bem Ordenados e o Axioma da Boa Ordenação

Vamos introduzir agora o conceito de conjunto bem ordenado. Para não fazer confusão com ordem parcial e ordem total, é conveniente e recomendável que volte às definições anteriores e aos exemplos para fixar melhor esses conceitos. Construa você mesmo mais exemplos e o aprendizado será pleno.

Definição 3.4.1 Considere X um subconjunto de $(A, \leq)$. Dizemos que x_o é o menor elemento de X se $x_o \in X$ e $x_o \leq x$, $\forall\, x \in X$. De modo análogo, definimos o maior elemento de X. É claro que nem todo subconjunto de $(A, \leq)$ tem, necessariamente, um menor (ou maior) elemento.

Nos diagramas de Hasse, ao lado, o menor elemento é, em cada caso, o que está representado pelo ponto mais baixo de cada diagrama.



Já o maior elemento se encontra no topo de cada diagrama acima. Os conjuntos ordenados, representados pelos diagramas de Hasse acima, são limitados. Observe também que nenhum desses diagramas representa um conjunto totalmente ordenado.

Definição 3.4.2 Um conjunto não vazio A é dito bem ordenado se, e somente se, todo subconjunto não vazio de A possui um menor elemento.

Exemplos 1. O conjunto dos números inteiros $\mathbb{Z}$, com a ordem usual, não é bem ordenado pois não possui, ele próprio, um menor elemento.

2. Seja X um conjunto não vazio e $\mathbb{P}(X)$ o conjunto das partes de X. $\mathbb{P}(X)$ possui um menor elemento, o conjunto vazio, mas, a menos que X seja unitário (possua apenas um elemento), $\mathbb{P}(X)$ não é bem ordenado.

Considere $X = \{0,1\}$. Neste caso, $\mathbb{P}(X) = \{\varnothing,\{0\},\{1\},\{0,1\}\}$. Se tomamos $A = \{\{0\},\{1\}\} \subset \mathbb{P}(X)$, percebemos que A não possui um menor elemento, pois $\{0\}$ e $\{1\}$ não se comparam.

3. O intervalo $(a,b) \subset \mathbb{R}$, com a ordem usual, não possui um menor elemento, logo não é bem ordenado. Cuidado: o exemplo anterior é um conjunto ordenado que possui um menor elemento mas não é bem ordenado, ou seja, o fato de A ser um conjunto ordenado e possuir um menor elemento não vai significar que A seja bem ordenado. Reveja a Definição 3.2.1.

4. O intervalo $[0,4) \subset \mathbb{R}$, com a ordem usual, possui um menor elemento – o número 0 – mas também não é bem ordenado pois o intervalo $(1,3] \subset [0,4)$ não possui um menor elemento.

Axioma, segundo o dicionário Houaiss da Língua Portuguesa, é "premissa considerada necessariamente evidente e verdadeira, fundamento de uma demonstração, porém ela mesma indemonstrável, originada, segundo a tradição racionalista, de princípios inatos da consciência ou, segundo os empiristas, de generalizações da observação empírica [O princípio aristotélico da contradição ('nada pode ser e não ser simultaneamente') foi considerado desde a Antiguidade um axioma fundamental da filosofia.]"

Axioma da Boa Ordenação $\mathbb{N}$, com a ordem usual, é bem ordenado, ou seja, todo subconjunto não vazio de $\mathbb{N}$ possui um menor elemento.

O conjunto dos números inteiros $\mathbb{Z}$, com a ordem usual, não é bem ordenado mas qualquer subconjunto limitado inferiormente de $\mathbb{Z}$ é. Se a

função $f : \mathbb{N} \to A$ é bijetora, já vimos que a relação de ordem usual (neste caso é uma Boa Ordem) de $\mathbb{N}$ induz uma (boa) ordem em A. Observe a função abaixo:

$$f : \mathbb{N} \to \mathbb{Z} \text{ tal que } f(n) = \begin{cases} \dfrac{n}{2} - 1, \text{ se } n \text{ é par} \\ -\dfrac{n+1}{2}, \text{ se } n \text{ é ímpar} \end{cases}.$$

$f(1) = -1$, $f(2) = 0$, $f(3) = -2$, $f(4) = 1$, $f(5) = -3$, ... É fácil perceber que f é uma bijeção e, como $\mathbb{N}$ é bem ordenado, $\mathbb{Z}$, com a (boa) ordem induzida de $\mathbb{N}$ pela função f, também é bem ordenado. Perceba, no entanto, que esta ordenação de $\mathbb{Z}$, induzida por f, não é a usual. Por exemplo, **com esta ordenação**, temos

$$-1 < 0 < -2 < 1 < \ldots$$

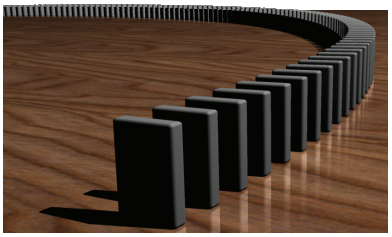
Algo um tanto bizarro para quem está acostumado com a ordem usual. Perceba que, com esta ordenação, -1 é o "menor" elemento de $\mathbb{Z}$. Com a ordem usual, $\mathbb{Z}$ não possui um menor elemento.

Exercício Coloque mais cinco elementos de $\mathbb{Z}$, na sequência $-1 < 0 < -2 < 1 < \ldots$, usando a ordem dada.

Convite Convidamos o caro leitor para refletir sobre os resultados seguintes e apresentar argumentos que justifiquem tais afirmativas:

- Considere a e b números naturais. Existe $n \in \mathbb{N}$ tal que $na > b$.
- Se a e b são números naturais com $a < b$ então $a + 1 \leq b$.
- Todo subconjunto limitado superiormente de $\mathbb{N}$ possui um maior elemento. Isto é verdade para o conjunto $\mathbb{R}$?

3.5 Princípio da Indução



O princípio da indução é frequentemente associado ao efeito dominó: se você tem uma longa fila de dominós em pé e você puder assegurar que (1) o primeiro dominó cairá; e (2) sempre que um dominó cair, seu próximo vizinho também cairá. Então você pode concluir que *todos* os dominós cairão. O princípio da indução é uma decorrência direta do axioma da boa ordenação.

Teorema 3.5.1 (Princípio da Indução) Seja $X \subset \mathbb{N}$ com as seguintes hipóteses:
a) $1 \in X$
b) Dado $n \in \mathbb{N}$, se $n \in X$ então $n + 1 \in X$
Tese: $X = \mathbb{N}$.

Prova Considere $Y = \mathbb{N} - X$ e suponhamos que $Y \neq \varnothing$. Como $\mathbb{N}$ é bem ordenado, Y possui um menor elemento b_o que é maior do que 1, em

virtude da hipótese (a). Como $b_o - 1 \notin Y$ então $b_o - 1 \in X$. Mas, pela hipótese (b), $(b_o - 1) + 1 = b_o \in X$, o que é uma contradição e, portanto, Y não pode ser diferente de vazio e, sendo $Y = \mathbb{N} - X = \varnothing$, temos $X = \mathbb{N}$, como queríamos demonstrar.

Exercícios 1. Mostre que $1 + 3 + 5 + \cdots + (2n - 1) = n^2$, $\forall\, n \in \mathbb{N}$.

Prova Considere $X = \{n \in \mathbb{N} \mid 1 + 3 + 5 + \cdots + (2n - 1) = n^2\}$. É claro que $1 \in X$, pois $1 = 1^2$.
Suponhamos que $n \in X$, ou seja,
$1 + 3 + 5 + \cdots + (2n - 1) = n^2$.
Então
$1 + 3 + 5 + \cdots + (2n - 1) + (2n + 1) = n^2 + (2n + 1) = n^2 + 2n + 1 = (n + 1)^2$.
Daí, $n + 1 \in X$ e, pelo princípio da indução, $X = \mathbb{N}$.

2. Se o número de elementos de A é k então o conjunto das partes $\mathbb{P}(A)$ de A possui 2^k elementos.

Prova Usaremos o Princípio da Indução: Se $k = 0$, temos o conjunto vazio, cujo único subconjunto é ele próprio e assim $\mathbb{P}(\varnothing) = \{\varnothing\}$. Logo o número de elementos de $\mathbb{P}(\varnothing)$ é $2^0 = 1$.
Se A é um conjunto unitário, $n(A) = 1$, seus únicos subconjuntos são $\varnothing$ e A. Portanto, $n(\mathbb{P}(A)) = 2^1 = 2$.

Suponhamos que $n(A) = k$ e $n(\mathbb{P}(A)) = 2^k$ (hipótese de indução). Acrescentando mais um elemento ao conjunto A, ficamos com $n(B) = k + 1$, onde $B = A \cup \{b\}$. Como $A \subset B$, todos os subconjuntos de A são também subconjuntos de B e, para completar o conjunto das partes de B, basta acrescentar a $\mathbb{P}(A)$ todos os subconjuntos de B contendo o elemento b, ou seja, se $\mathbb{P}(A) = \{\varnothing, A_1, A_2, ..., A\}$, então
$\mathbb{P}(B) = \{\varnothing, A_1, A_2, ..., A\} \cup \{\{b\}, A_1 \cup \{b\}, A_2 \cup \{b\}, ..., A \cup \{b\}\}$
e daí, temos
$n(\mathbb{P}(B)) = 2 \cdot (n\mathbb{P}(A)) = 2 \cdot 2^k = 2^{k+1}$.

O resultado que acabamos de provar é o teorema 3.4.2 da Unidade I.

O princípio da indução pode ser generalizado para conjuntos da forma $X = \{a, a + 1, a + 2, a + 3, ...\} \subset \mathbb{Z}$. Neste caso, ficamos com o enunciado: (Princípio da Indução) Seja $A \subset X$ com as seguintes hipóteses:
a) $a \in A$
b) Dado $n \in X$, se $n \in A$ então $n + 1 \in A$
Tese: $A = X$.

Dado $n \in \mathbb{N}$, denotaremos de I_n o conjunto dos números naturais de 1 até n: $I_n = \{1,2,3,...,n\}$.

Teorema 3.5.2 Se $n < m$, não existe bijeção $f : I_n \to I_m$.

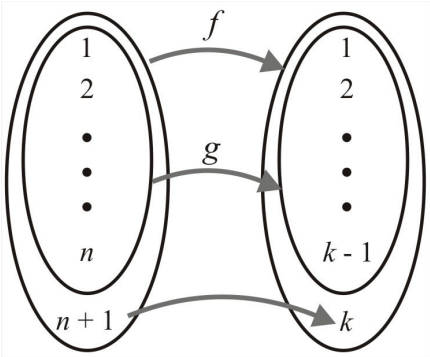
Prova Novamente, o Princípio da Indução:

Para n = 1, é óbvia a impossibilidade de uma função bijetiva f : {1} $\rightarrow$ I_m = {1,2,...,m}, com m > 1.

Suponha (hipótese de indução) que não se pode ter f : {1,2,3,...,n} $\rightarrow$ {1,2,3,...,m}, com m > n.

Se fosse possível uma bijeção f : {1,2,3,...,n,n + 1} $\rightarrow$ {1,2,3,...,k}, com k > n + 1, sem perda de generalidade, podemos supor que f(n + 1) = k. Vamos então definir a função

g : $I_n \rightarrow I_{k-1}$, dada por g(x) = f(x).



O que fizemos foi somente retirar o elemento n + 1 $\in$ In + 1 e o elemento k $\in$ Ik. Mas, sendo f bijetiva, é claro que g também o é, o que contraria a hipótese de indução, pois, como k > n + 1, temos k – 1 > n. Veja no diagrama:

Outra coisa que fizemos foi: Se f : A $\rightarrow$ B é uma bijeção, então
g : A – {a} $\rightarrow$ B – {f(a)}
definida por g(x) = f(x), também é uma bijeção.

3.6 Conjuntos Enumeráveis

O teorema 3.3.2 nos permite definir o número de elementos de um conjunto finito X como sendo n se, e somente se, existe uma bijeção

$$f : I_n = \{1,2,3,...,n\} \rightarrow X.$$

Neste caso, dizemos que o número cardinal de X é n e o citado teorema nos garante a unicidade do cardinal de X. Generalizamos a ideia de número cardinal da seguinte forma: dois conjuntos X e Y possuem o mesmo cardinal se, e somente se, existe uma bijeção

$$f : X \rightarrow Y.$$

Para entendermos melhor a diferença entre conjuntos finitos e infinitos, apresentamos-lhe o **Hotel de Hilbert**:

O Hotel de Hilbert é um fato matemático sobre conjuntos infinitos apresentado pelo matemático alemão David Hilbert (1862-1943). É chamado de paradoxo por ser contraintuitivo, fato bastante comum quando se trata de conjuntos infinitos.

Suponha um hotel hipotético cuja quantidade de quartos seja infinita e que todos estejam ocupados, isto é, o hotel não tem mais vaga. Suponha que uma pessoa chega e quer se hospedar no hotel. Se o hotel tivesse apenas um número finito de quartos, é claro que essa pessoa teria que procurar em

outro local, mas, como o hotel possui um número infinito de quartos, é possível resolver o problema de acomodação do novo hóspede da seguinte forma: move-se o hóspede do quarto 1 para o quarto 2, o hóspede do quarto 2 para o quarto 3 e assim por diante. Desta forma, fica vago o quarto 1 e podemos acomodar o novo hóspede nele. Por um argumento análogo é possível alocar um número infinito enumerável (Definição 3.4.1) de novos clientes: apenas mova o hóspede do quarto 1 para o quarto 2, o hóspede do quarto 2 para o quarto 4 e, em geral, do quarto N para o quarto 2N. Assim todos os quartos de número ímpar estarão livres para os novos hóspedes.

Isso dá um resultado importante e não intuitivo: a situação "todo quarto está ocupado" não é equivalente a "nenhum novo hóspede pode ser acomodado" quando existe um número infinito de quartos.
Alguns acham este fato bastante contraintuitivo. As propriedades de conjuntos infinitos são bastante diferentes daquelas dos conjuntos finitos. Em um hotel comum, ou seja, com um número finito de quartos (maior do que 1), o número de quartos com numeração ímpar é claramente menor que o número total de quartos. Entretanto, no Hotel de Hilbert, a quantidade (cardinalidade) de quartos com numeração ímpar é igual ao número total (cardinal) de quartos. Em termos matemáticos, a cardinalidade do subconjunto contendo apenas os quartos com numeração ímpar é a mesma do conjunto contendo todos os quartos.
Em outras palavras, para qualquer conjunto infinito enumerável X, existe uma bijeção entre X e o conjunto dos números naturais N, mesmo que o conjunto contenha (e seja distinto) do conjunto dos números naturais.

Exemplos 1. X = {0,1,2,3} e Y = {5,6,7,8} possuem o mesmo cardinal pois f : X → Y, dada por $f(x) = x + 5$, é uma bijeção.

2. O conjunto dos números pares P = {2,4,6,...} e o conjunto dos números naturais $\mathbb{N}$ possuem o mesmo cardinal pois $f : \mathbb{N} \to P$, dada por $f(x) = 2x$, é uma bijeção. Veja o **Hotel de Hilbert**.

3. $\mathbb{Z}$ e $\mathbb{N}$ possuem o mesmo cardinal pois a função abaixo é uma bijeção:

$$f : \mathbb{N} \to \mathbb{Z} \text{ tal que } f(n) = \begin{cases} \dfrac{n}{2} - 1, \text{ se } n \text{ é par} \\ -\dfrac{n+1}{2}, \text{ se } n \text{ é ímpar} \end{cases}.$$

Os exemplos 2 e 3 nos mostram que um conjunto A pode ter o mesmo cardinal que um subconjunto próprio B ⊂ A. Isto, no entanto, só é permitido para conjuntos infinitos. Se A ≠ ∅ é finito e B é um subconjunto próprio de A, necessariamente n(A) > n(B), conforme o teorema 3.5.2.

Definição 3.6.1 Conjuntos finitos ou com a mesma cardinalidade de $\mathbb{N}$ são chamados **enumeráveis**.

Teorema 3.6.1 Todo conjunto infinito possui um subconjunto infinito enumerável.

Prova Considere a_1 um elemento qualquer de X. O conjunto X – $\{a_1\}$ é infinito e daí podemos escolher um elemento $a_2 \neq a_1$. Suponhamos que já temos $a_1, a_2, a_3,..., a_n$, com $a_i \neq a_j$, $\forall$ i $\neq$ j. Como X é infinito, o conjunto X – $\{a_1, a_2, a_3,..., a_n\} \neq \varnothing$ e podemos escolher a_{n+1} satisfazendo à condição desejada: ser diferente de todos os termos anteriores da sequência assim construída. Provamos assim, por indução, que X possui um subconjunto infinito enumerável.

Corolário Se X é infinito, existe uma bijeção f : X $\to$ Y, onde Y é um subconjunto próprio de X.

Prova Sendo X infinito, o teorema anterior nos garante a existência de uma sequência (a_n) de X tal que $a_n \neq a_m$, $\forall$ n $\neq$ m.
Y = X – $\{a_1\}$ é um subconjunto próprio de X e a função f : X $\to$ Y, definida por

$$f(x) = \begin{cases} a_{n+1}, \text{se } x = a_n \\ x, \text{ se } x \neq a_n \end{cases},$$

é uma bijeção.

Teorema 3.6.2 Se X é enumerável e Y é subconjunto de X então Y é enumerável.

Prova Se X for finito, não há o que provar pois Y também será finito. Suponhamos, portanto, que existe uma bijeção f : $\mathbb{N} \to$ X. Se Y for finito, não há o que provar. Caso contrário, f^{-1}(Y) é um subconjunto infinito de $\mathbb{N}$. Sendo $\mathbb{N}$ bem ordenado, podemos definir a função g : $\mathbb{N} \to f^{-1}$(Y) da seguinte forma:

g(1) = menor elemento de f^{-1}(Y)
g(2) = menor elemento de f^{-1}(Y) – {g(1)}
⋮
g(n) = menor elemento de f^{-1}(Y) – {g(1),g(2), ...,g(n – 1)}
⋮
A função g, assim definida (por indução) é uma bijeção e, portanto, f^{-1}(Y) é enumerável e a função

$$\begin{aligned} h : f^{-1}(Y) &\to Y \\ x &\mapsto h(x) = f(x) \end{aligned}$$

é uma bijeção, o que nos leva à conclusão de que Y é enumerável.

Observe que a função h é uma restrição de f a um novo domínio, $f^{-1}(Y)$, e novo contradomínio, neste caso, Y.

Corolário 1 Se X é enumerável e $f : Y \to X$ é injetiva, então Y é enumerável.

Prova Como X é enumerável e $f(Y)$ é subconjunto de X, então $f(Y)$ é enumerável. Restringindo o contradomínio de f a $f(Y)$, temos que a função

$$g : Y \to f(Y)$$
$$x \mapsto g(x) = f(x)$$

é uma bijeção e, daí, Y é enumerável.

Corolário 2 Se X é enumerável e $f : X \to Y$ é sobrejetiva, então Y é enumerável.

Prova Considere a relação de equivalência em X, induzida pela função f: $a \sim b \Leftrightarrow f(a) = f(b)$. É claro que o conjunto quociente X/~ é enumerável, pois cada classe de equivalência pode ser representada por um elemento de X, ou seja, X/~ pode ser "pensado" como subconjunto de X embora, é bom salientar, não o seja.
Como a função h : X/~ → Y, dada por $h(\bar{x}) = f(x)$ é claramente injetiva pois $\bar{x} \neq \bar{y} \Rightarrow f(x) \neq f(y)$, onde x e y são representantes quaisquer de $\bar{x}$ e $\bar{y}$, respectivamente. Sendo f sobrejetiva, h também o é e, assim, h é bijetiva e Y é enumerável.

A ideia utilizada acima é a seguinte: quando temos $f : X \to Y$ injetiva é como se X tivesse "menos" elementos do que Y, ou seja, o cardinal de X é menor ou igual ao cardinal de Y e, sendo Y enumerável, X também é. De forma inversa, se $f : X \to Y$ é sobrejetiva, é como se X tivesse "mais" elementos do que Y e, com o mesmo raciocínio, se X é enumerável, Y também é.

Exercício Mostre que, se $f : X \to Y$ é sobrejetiva, então existe $f : Y \to X$ injetiva. Com este resultado, a prova do Corolário 2 fica mais direta.

Exemplo É impossível uma função $f : \mathbb{N} \to (0,1) \subset \mathbb{R}$ sobrejetiva e, portanto, o intervalo (0,1) é não enumerável.

Prova Suponhamos, por absurdo, que $(0,1) = \{x_1, x_2, x_3, \ldots, x_n, \ldots\}$, onde $x_n = f(n)$ e consideremos cada x_n na sua forma decimal:

$x_1 = 0{,}a_{11}a_{12}\ldots a_{1n}\ldots$

$x_2 = 0{,}a_{21}a_{22}\ldots a_{2n}\ldots$

$\vdots$

$x_k = 0{,}a_{k1}a_{k2}\ldots a_{kn}\ldots$

$\vdots$

Por exemplo: se $x_2 = 0{,}175$, teríamos $a_{21} = 1$, $a_{22} = 7$, $a_{23} = 5$, $a_{24} = a_{25} = a_{26} = \cdots = a_{2i} = 0$, $\forall$ i > 3.

Como f é suposta sobrejetiva, todos os números reais do intervalo (0,1) estão listados acima. Considere o número real $y = 0{,}b_1b_2b_3...b_n...$ definido da seguinte forma:

$b_1 = 1$ se $a_{11} \neq 1$. Caso contrário $b_1 = 2$.
$b_2 = 1$ se $a_{22} \neq 1$. Caso contrário $b_2 = 2$.
$\vdots$
$b_n = 1$ se $a_{nn} \neq 1$. Caso contrário $b_n = 2$.
$\vdots$
É fácil perceber que $y \neq x_1$ pois $b_1 \neq a_{11}$. Analogamente, $y \neq x_2$, $y \neq x_3$,..., $y \neq x_n$, $\forall$ n $\in \mathbb{N}$. Conclusão: f não é sobrejetiva pois $y \in (0,1)$ e não está na imagem de f.

O método utilizado acima foi proposto por Cantor e é conhecido como Método da Diagonal de Cantor. Com isto, ele descobriu um número cardinal diferente do de $\mathbb{N}$, já que (0,1) é não enumerável. Este novo número cardinal foi chamado de c (de continuum). O número cardinal de $\mathbb{N}$ é também referido com $\aleph_o$ (lê-se Aleph zero, ph com som de f). Já $\mathbb{R}$ tem cardinal $\aleph_1$ e assim por diante. Em um curso mais avançado, prova-se que, se X possui cardinal $\aleph_n$, o conjunto das partes de X possui cardinal $\aleph_{n+1}$. Assim, o conjunto das partes de $\mathbb{N}$ possui cardinal $c = \aleph_1$.

O fato de o intervalo (0,1) não ser enumerável implica que o intervalo fechado [0,1] também não é enumerável pois [0,1] contém o intervalo (0,1). Da mesma forma concluímos que o conjunto dos números reais $\mathbb{R}$, uma vez que contém o intervalo [0,1], não é enumerável.

A função

$f : (0,1) \to (-\pi/2,\pi/2)$, dada por $f(x) = -\pi/2 + \pi x$

é uma bijeção do intervalo (0,1) sobre o intervalo $(-\pi/2,\pi/2)$ e a função

$g : (-\pi/2,\pi/2) \to \mathbb{R}$, dada por $g(x) = \tan(x)$
é também uma bijeção. Daí, a função composta $g \circ f : (0,1) \to \mathbb{R}$ é uma bijeção e $\mathbb{R}$ possui o mesmo cardinal do intervalo (0,1).

Um intervalo de extremidades a e b é dito *degenerado* se $a = b$.

Em geral, qualquer intervalo (a,b), com $a < b$ (intervalo não degenerado), tem a mesma cardinalidade de $\mathbb{R}$. Em particular, como (0,1) e [0,1] possuem a mesma cardinalidade, existe uma bijeção $f : [0,1] \to (0,1)$. Vamos exibir uma:

Considere A = {0,1,1/2,1/3,...,1/n,...} $\subset$ [0,1]. Definimos $f(x)$ como sendo:

$f(0) = 1/2; f(1) = 1/3; f(1/2) = 1/4; \ldots ; f(1/n) = 1/(n+2); \ldots$

e, se $x \notin$ A, colocamos $f(x) = x$.

Definida desta forma, a função $f(x)$ é claramente uma bijeção.

Exemplo O produto cartesiano $\mathbb{N}$x$\mathbb{N}$ é enumerável.

Prova Considere a função $f : \mathbb{N} \to \mathbb{N}$ definida por $f(n)$ = soma dos algarismos da representação decimal de n. (Esta função já foi vista, lembra?)

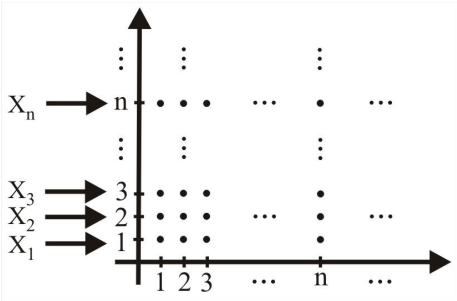
Para cada n $\in \mathbb{N}$, o conjunto $X_n = f^{-1}(n)$ é infinito enumerável, ou seja, existe uma bijeção

$\varphi_n : X_n \to \mathbb{N}$

Vamos definir uma função F : $\mathbb{N} \to \mathbb{N}x\mathbb{N}$ da seguinte forma:

$F(x) = (n, \varphi_n(x))$ para $x \in X_n$.

Como $\mathbb{N}$ = , Xi$\cap$Xj = $\varnothing$, $\forall$ i $\neq$ j e cada φ_n é bijetora, então F é bijetora e $\mathbb{N}$x$\mathbb{N}$ é enumerável.
Graficamente, temos o produto cartesiano:



Na figura ao lado está indicado como seria cada correspondência de $X_n = f^{-1}(n)$ com $\mathbb{N}$x{n}. Uma decorrência direta do fato de $\mathbb{N}$x$\mathbb{N}$ ser enumerável é que, se X e Y são enumeráveis, então o produto cartesiano XxY é enumerável (tente provar isto). Temos também que A^n = AxAx...xA é enumerável se A for enumerável. Em particular, $\mathbb{Z}^n$ é enumerável.

Como $\mathbb{N}$ = , com $X_n = f^{-1}(n)$ e Xi$\cap$Xj = $\varnothing$, $\forall$ i $\neq$ j, temos como corolário deste fato que se A = , com B_n enumerável para todo n, ou seja, A é a união enumerável de conjuntos enumeráveis, então A é também enumerável. Mas, cuidado! A união qualquer de conjuntos enumeráveis pode não ser enumerável. Por exemplo, podemos escrever o intervalo (0,1), que já provamos não ser enumerável, da seguinte forma:

$$(0,1) = \bigcup_{x \in (0,1)} \{x\}.$$

Como, para todo $x \in (0,1)$, o conjunto $\{x\}$ é finito, temos o intervalo (0,1) escrito como união (não enumerável) de conjuntos enumeráveis.

Exercício Prove que A = {m + ni | m,n $\in \mathbb{Z}$ e $i^2 = -1$} é enumerável

Exemplo O conjunto $\mathbb{Q}^+$ dos números racionais positivos é enumerável.

Prova A função F : $\mathbb{N}\times\mathbb{N} \to \mathbb{Q}^+$, definida por F(m,n) = m/n é claramente sobrejetiva – mas não é injetiva, pois F(2,4) = F(3,6) – e, pelo Corolário 2 do Teorema 3.4.2, $\mathbb{Q}^+$ é enumerável. É claro que $\mathbb{Q}^-$, o conjunto dos números racionais negativos, também é enumerável. Como $\mathbb{Q} = \mathbb{Q}^+\cup\{0\}\cup\mathbb{Q}^-$, temos que o conjunto dos números racionais $\mathbb{Q}$ é enumerával.

Exemplo O conjunto $\mathbb{I}$ dos números irracionais é não enumerável.

Prova $\mathbb{R} = \mathbb{Q}\cup\mathbb{I}$. Caso $\mathbb{I}$ fosse enumerável, $\mathbb{R}$ também seria, o que, sabemos, não é verdade.

Um número real a é chamado *algébrico* se existe um polinômio com coeficientes inteiros $p(x) = a_0 + a_1x + ... + a_nx^n$ tal que $p(a) = 0$, ou seja, a é um *zero* de $p(x)$. Todo número racional m/n é algébrico, pois é um *zero* de $p(x) = m - nx$. Números irracionais da forma , com p primo e n > 1, são algébricos, uma vez que é *zero* de $p(x) = x^n - p$. Os números reais não algébricos são chamados de *transcendentes*. Os números π, e ($\cong$ 2,718) são transcendentes.

Exemplo O conjunto dos números algébricos é enumerável. Consequentemente, o conjunto dos números transcendentes é não enumerável.

Prova Para cada n $\in \mathbb{N}$, existe uma "quantidade" enumerável de polinômios de grau n com coeficientes inteiros. A função

$$f : \mathbb{Z}^{n+1} \to P_n$$
$$(a_0,a_1,a_2,...,a_n) \mapsto p(x) = a_0 + a_1x + ... + a_nx^n$$

é uma bijeção. Portanto P_n (= conjunto dos polinômios de grau menor ou igual a n) é enumerável, uma vez que $\mathbb{Z}^{n+1}$ é enumerável.

Cada polinômio de grau n possui, no máximo, n zeros e, assim, o conjunto dos números algébricos, sendo a união enumerável de conjuntos finitos, é enumerável.

Claro que, sendo o conjunto $\mathcal{A}$ dos números algébricos enumerável, o conjunto $\mathcal{T}$ dos números transcendentes é não enumerável pois $\mathbb{R} = \mathcal{A}\cup\mathcal{T}$.

Observação Se A e B são enumeráveis, $A\cup B$ é enumerável. Equivalentemente, sempre que tivermos A enumerável e $A\cup B$ não enumerável, teremos B não enumerável.

Teorema 3.4.3 Seja X um conjunto qualquer e $\mathbb{P}(X)$ o conjunto das partes de X. A cardinalidade de X é diferente da cardinalidade de $\mathbb{P}(X)$.

Prova Se X é finito, não há o que provar pois se n(X) = k, temos $n(\mathbb{P}(X)) = 2^k > k$. Consideremos então que X é infinito e suponhamos, por absurdo, que exista uma bijeção

$$f : X \to \mathbb{P}(X)$$

Para cada $x \in X$, temos que $f(x)$ é um subconjunto de X. Há duas alternativas: (1) $x \in f(x)$ e (2) $x \notin f(x)$. Considere agora o conjunto $A = \{x \in X \mid x \notin f(x)\} \subset X$. Como f é sobrejetiva e A é um elemento de $\mathbb{P}(X)$, existe $x_0 \in X$ tal que $f(x_0) = A$. Agora, tente responder à questão "$x_0 \in A$?". Como esta questão não pode ser respondida satisfatoriamente, temos que não existe $x_0 \in X$ tal que $f(x_0) = A$, isto é, f não pode ser sobrejetiva, o que conclui a nossa demonstração.

Podemos "ordenar" os números cardinais da seguinte forma: Se existe uma função injetiva $f : X \to Y$ mas é impossível uma função sobrejetiva $g : X \to Y$, dizemos que o cardinal de X é menor do que o cardinal de Y.
Como a função

$$f : X \to \mathbb{P}(X)$$
$$x \mapsto \{x\}$$

é claramente injetiva, acabamos de provar que o cardinal de X é menor do que o cardinal de $\mathbb{P}(X)$. Temos também que o cardinal de $\mathbb{R}$ é maior do que o cardinal de $\mathbb{N}$ e que o cardinal de qualquer conjunto infinito é maior ou igual do que o cardinal de $\mathbb{N}$. Podemos definir uma relação de equivalência entre todos os conjuntos por meio de suas cardinalidades. $A \sim B \Leftrightarrow$ cardinal de A = cardinal de B. Portanto, sempre que estamos tratando com um conjunto infinito enumerável, pensamos sempre no conjunto $\mathbb{N}$ e, para provar qualquer resultado sobre enumerabilidade para X infinito enumerável, basta provar que esse resultado é verdadeiro para $\mathbb{N}$. Por exemplo, se X e Y são infinitos enumeráveis e queremos provar que o produto cartesiano XxY é enumerável, basta provar que $\mathbb{N}^2 = \mathbb{N}\mathbf{x}\mathbb{N}$ é enumerável.

Agora vamos tentar hospedar uma quantidade infinita enumerável no **Hotel de Hilbert**, como sempre, já totalmente ocupado. Suponha que um número infinito enumerável de ônibus $O_1, O_2, \ldots, O_n, \ldots$ cada um contendo um número infinito enumerável de passageiros chegou ao hotel de Hilbert, aquele com um número infinito enumerável de quartos. Para fazer este milagre, lembre que o conjunto dos números naturais $\mathbb{N}$ pode ser escrito como a união infinita enumerável de subconjuntos infinitos enumeráveis de $\mathbb{N}$, ou seja, $\mathbb{N} = X_1 \cup X_2 \cup \ldots \cup X_n \ldots$ Agora basta pegar todos os hóspedes que já estavam no hotel e colocá-los nos quartos que tenham numeração de X_1 e, em seguida, acomodar todos os passageiros do ônibus O_1 em X_2, os de O_2 em X_3 e assim por diante.

Isso dá um resultado importante e não intuitivo; a situação "o hotel está totalmente ocupado" e "nenhum novo hóspede pode ser acomodado"

não são equivalentes quando existe um número infinito de quartos. Isso ocorre porque **a união enumerável de conjuntos enumeráveis é enumerável**. Veja a prova de que $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ é enumerável.

Para sua reflexão

Às vezes gostaríamos que todos os resultados, exemplos e exercícios fossem dados e explicados exaustivamente em seus mínimos detalhes. A Matemática, como a Arte, fica banal e sem graça quando excessivamente explicada. Há que se deixar algo, por pequeno que seja, para que seja raciocinado e investigado por quem está com a pretensão de aprender. São essas pequenas (ou grandes) descobertas pessoais que trarão a satisfação, o prazer de aprender e o querer aprender mais e mais.

4. Avaliando o que foi construído

Nesta unidade, apresentamos o conceito de conjunto ordenado (parcial e totalmente) e estendemos a noção de número de elementos de um conjunto finito para conjuntos infinitos. Definimos enumerabilidade de um conjunto e vimos que o produto cartesiano de conjuntos enumeráveis é enumerável e a união enumerável de conjuntos enumeráveis é também enumerável. Constatamos que o conjunto dos números reais é não enumerável, assim como qualquer intervalo não degenerado.

No Moodle

Agora vá à plataforma MOODLE e procure responder as questões e resolver os exercícios referentes ao tema estudado.

Unidade IV Introdução à Teoria dos Números

1. Situando a Temática

A Teoria dos Números é dedicada ao estudo das propriedades dos números inteiros. Apresentaremos, nesta unidade, algumas definições e resultados que serão necessários em cursos subsequentes, principalmente de Álgebra Abstrata. O conceito de número primo é, certamente, o mais importante na teoria dos números. Um dos resultados que se referem aos números primos é o Teorema Fundamental da Aritmética, que afirma que qualquer número natural diferente de 1 pode ser escrito de forma única (desconsiderando a ordem) como um produto de números primos: este processo se chama decomposição em fatores primos ou fatoração.

Os gregos foram os primeiros a perceber que qualquer número natural, exceto o 1, pode ser gerado pela multiplicação de números primos, os chamados "átomos da aritmética". Eratóstenes foi a primeira pessoa que produziu tabelas de números primos, no terceiro século a.C. Para isso, escrevia inicialmente uma lista com todos os números naturais de 1 a 1.000. Em seguida, escolhia o primeiro primo, 2, e eliminava da lista todos os seus múltiplos. Passava ao número seguinte que não fora eliminado, o 3, e procedia também eliminando todos os seus múltiplos. Desta forma Erastótenes produziu tabelas de primos. Este procedimento de eliminação passou a se chamar de crivo de Eratóstenes.

2. Problematizando a Temática

São diversos os problemas que podem ser resolvidos com a utilização da teoria aqui apresentada. Alguns exemplos:

- Um terreno retangular com dimensões de 7.200 metros por 2.700 metros vai ser dividido em lotes iguais e quadrados. Quais devem ser as dimensões desses lotes para que a área de cada lote seja a maior possível?

- Como determinar todos os números inteiros cujo primeiro dígito é 6 e que diminui 25 vezes quando este é descartado? Por exemplo, se descartarmos o 6 de 62 ficaremos somente com o número 2, que é 31 vezes menor do que 62.

- Um problema atual, difícil e ainda não respondido satisfatoriamente é como decidir se um número é primo ou não. Sabemos, por exemplo, que o conjunto dos primos é infinito mas só conhecemos uma quantidade finita deles.

3. Conhecendo a Temática

3.1 Algoritmo da divisão

Dados dois números inteiros a e b, nem sempre a divisão de um desses números pelo outro tem uma resposta exata. Por exemplo, 10 dividido por 2 dá exatamente 5 mas 11 dividido por 2 dá 5 mas a "conta" não é exata, pois 2x5 = 10. O que falta para 11 é o que chamamos de resto. Assim, 11 dividido por 2 fornece o resultado (quociente) $q = 5$ e um resto $r = 1$. Lembramos que o nosso conjunto universo aqui é o dos números inteiros $\mathbb{Z}$. Formalmente, temos o teorema a seguir, conhecido como *Algoritmo da Divisão*:

Teorema 3.1.1 Dados a e b números inteiros com $b > 0$, existem únicos q e r inteiros tais que

$$a = qb + r, \text{ onde } 0 \leq r < b.$$

Prova (Existência) Se $a = 0$, basta tomar $q = r = 0$. Se $0 < a < b$, basta tomar $q = 0$ e $r = a$. Se $a = b$, $q = 1$ e $r = 0$. Suponhamos então $a > b$, o que acarreta $a > a - b > 0$ e consideremos o conjunto $A = \{n \in \mathbb{N} \mid n \cdot b \leq a\}$. Temos que $1 \in A$ e, portanto, $A \neq \emptyset$. A é limitado superiormente pois, se $n \geq a$, então $n \notin A$. Assim, existe $q \in A$ que é o maior elemento de A, ou seja,

$$q \cdot b \leq a \text{ e } (q+1) \cdot b > a \Rightarrow b > r = a - q \cdot b \geq 0 \Rightarrow a = qb + r,$$

onde $0 \leq r < b$.

(Unicidade) Suponhamos que, dados $a, b \in \mathbb{Z}$ com $b > 0$, existam $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, tais que

$$a = q_1 b + r_1, \text{ com } 0 \leq r_1 < b \qquad \text{(I)}$$
$$a = q_2 b + r_2, \text{ com } 0 \leq r_2 < b \qquad \text{(II)}$$

De (I) e (II), concluimos que $0 = (q_1 - q_2)b + (r_1 - r_2)$. Mas $0 \leq r_1 < b$ e $-b < -r_2 \leq 0 \Rightarrow -b < r_1 - r_2 < b$. Daí, $|r_1 - r_2| < b$. Como vale também a igualdade $0 = (q_2 - q_1)b + (r_2 - r_1)$, podemos escrever

$$|q_2 - q_1| \cdot b = |r_2 - r_1| < b,$$

o que acarreta $|q_2 - q_1| = 0$, isto é, $q_2 = q_1$.

Para chegar à conclusão acima, usamos o fato de que o produto de um número inteiro não negativo ($|q_2 - q_1|$) multiplicado por um número inteiro positivo (b) só é menor que este último se for zero.

Exemplo Dados $a, b \in \mathbb{Z}$ determine q e r, nos seguintes casos:

- $a = 13$, $b = 15$. Neste caso $a < b$ e $q = 0$, $r = 13$.
- $a = -17$, $b = 10$. Neste caso $a < 0$ e $q = -2$, $r = 3$. Note que, se tivéssemos $a = 17$ e $b = 10$, teríamos $q = 1$ e $r = 7$.

Podemos apresentar o Algoritmo da Divisão na forma mais geral a seguir:

Teorema 3.1.2 Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$. Então existem únicos q e $r \in \mathbb{Z}$ tais que

$a = qb + r$, onde $0 \leq |r| < b$.

Exemplo Determine a divisão de 50 por – 7.

Solução Como $50 = 7\text{x}7 + 1 = -7\text{x}(-7) + 1$, ou seja, $q = -7$ e $r = 1$.

Definição 3.1.1 Sejam $a, b \in \mathbb{Z}$. Dizemos que a divide b ou b é múltiplo de a se existir $c \in \mathbb{Z}$ tal que $a = bc$. Neste caso, escrevemos $a|b$ (lê-se: a divide b). Caso contrário, dizemos que a não divide b e escrevemos, em símbolos, $a\dagger b$. Dizemos que um número $a \in \mathbb{Z}$ é par se $2|a$ e é ímpar se $2\dagger a$.

Exemplo 2 divide qualquer número par; 1 divide qualquer número inteiro; $5|570$; $3\dagger 328$; $10\dagger 507$.

Teorema 3.1.3 Sejam $a, b, c \in \mathbb{Z}^* = \mathbb{Z} - \{0\}$. Então valem as seguintes afirmativas:

1. $\pm 1|a, \pm a|a$
2. $b|1 \Leftrightarrow b = \pm 1$
3. $b|a$ e $a > 0 \Rightarrow b \leq a$.
4. $b|a \Leftrightarrow bc|ac$.
5. $b|a$ e $a|c \Rightarrow b|c$.
6. $b|a$ e $a|b \Rightarrow a = \pm b$.
7. $b|a$ e $b|c \Rightarrow b|(ax + cy)$, $\forall\, x, y \in \mathbb{Z}$.

Prova Provaremos apenas o item 7, ficando os outros itens como exercício:

$$b|a \Rightarrow \exists\, d \in \mathbb{Z} \text{ tal que } a = bd \Rightarrow xa = xbd,\ \forall\, x \in \mathbb{Z}. \quad \text{(I)}$$

$$b|c \Rightarrow \exists\, d_1 \in \mathbb{Z} \text{ tal que } c = bd_1 \Rightarrow yc = ybd_1,\ \forall\, y \in \mathbb{Z}. \quad \text{(II)}$$

De (I) e (II), concluimos que $xa + yc = xbd + ybd_1 = b(xd + yd_1)$ e, como $xd + yd_1 \in \mathbb{Z}$, $b|(ax + cy)$.

Exemplo item 7: $3|9$ e $3|15 \Rightarrow 3|126$, pois $126 = 4\text{x}9 + 6\text{x}15$.
Item 5: $4|12$ e $12|36 \Rightarrow 4|36$.

Quando escrevemos o número quatrocentos e trinta e um na forma 431, dizemos que este número esta sob a forma decimal, ou seja, na base dez, o que significa que $431 = 4x10^2 + 3x10^1 + 1x10^0$. Como seria este mesmo número escrito numa outra base? Em primeiro lugar, observe que, na base dez, temos dez algarismos (0,1,2,3,...,9) para expressar todos os números. Se resolvermos expressar os números numa base n, devemos ter, de forma análoga, n algarismos para escrever qualquer número. Com n = 2, por exemplo, utilizam-se apenas os algarismos 0 e 1. O teorema seguinte assegura que se expresse qualquer número em uma determinada base e nos diz como é a expressão. Compare-a com a forma decimal.

Teorema 3.1.4 Seja $b \in \mathbb{N}$, com $b > 1$. Então para todo $a \in \mathbb{N}$, existem únicos n, $r_i \in \mathbb{N}$, tais que:

$a = r_n b^n + r_{n-1} b^{n-1} + ... + r_1 b^1 + r_0 b^0$,

onde $r_i \in \{0,1,2, ... ,b-1\}$.

Para escrever um número qualquer na base três, só podemos usar os algarismos 0, 1 e 2. Qual é o significado de 211 nesta base? Como fazer para expressar o número dez na base três? Usaremos a notação $[r_k\, r_{k-1}\, r_{k-2} ... r_0]_b$ para expressar o número

$$r_0 + r_1\, b + r_2 b^2 + ... + r_k b^k$$

Portanto $[211]_3 = 2x3^2 + 1x3 + 1 = 22$ (na base dez). Já o número dez é escrito, na base três, como $[101]_3$ (confira). Qual é o número representado por $[1110]_2$? E $[1112]_3$? E $[14]_5$?

Quando a base é maior do que 10, usamos letras do alfabeto para completar o número de algarismos. Veja os exemplos:

Base	Algarismos	Observação
11	0,1,2,3,4,...,9,*a*	O "número" *a* corresponde ao número dez
16	0,1,2,3,4,...,9,*a*,*b*,*c*,*d*,*e*,*f*	O "número" *a* corresponde ao número dez e *f* é quinze. A base, neste caso, é chamada hexadecimal.

Temos $[10]_{16} = 1x16 + 0 = 16$ (base dez) e $[12a]_{11} = 1x11^2 + 2x11 + a = 121 + 22 + 10 = 153$ (base dez).

Os números r_0, r_1, r_2, ... r_k que expressam o número $a = r_0 + r_1\, b + r_2.b^2 + ... + r_k b^k$ na base b são os restos de divisões por b:

$$\begin{array}{ll} a = q_o b + r_o & 0 \le r_o < b \\ q_o = q_1 b + r_1 & 0 \le r_1 < b \\ q_1 = q_2 b + r_2 & 0 \le r_2 < b \\ \vdots & \vdots \\ q_{n-2} = q_n b + r_n & 0 \le r_n < b \end{array}$$

Exemplo Vamos usar o algoritmo acima para escrever o número 87 na base 2:

$$
\begin{aligned}
87 &= 43\text{x}2 + 1 \quad \Rightarrow r_o = 1\\
43 &= 21\text{x}2 + 1 \quad \Rightarrow r_1 = 1\\
21 &= 10\text{x}2 + 1 \quad \Rightarrow r_2 = 1\\
10 &= 5\text{x}2 + 0 \quad \Rightarrow r_3 = 0\\
5 &= 2\text{x}2 + 1 \quad \Rightarrow r_4 = 1\\
2 &= 1\text{x}2 + 0 \quad \Rightarrow r_5 = 0\\
1 &= 0\text{x}2 + 1 \quad \Rightarrow r_6 = 1
\end{aligned}
$$

Portanto, $87 = [1010111]_2$.

Exercício Usando o algoritmo descrito acima, escreva o número 87 na base 3.

3.2 Máximo Divisor Comum

Dados a e $b \in \mathbb{N}$, o conjunto dos divisores comuns $DC_{a,b} = \{x \in \mathbb{N}$ tais que $x|a$ e $x|b\}$ é sempre não vazio, pois o número 1 é divisor de a e b. Como $DC_{a,b}$ é limitado superiormente, existe $x_o \in DC_{a,b}$ tal que $x_o \geq x$, $\forall\ x \in DC_{a,b}$. Este valor x_o é chamado de Máximo Divisor Comum de a e b. Por exemplo: os divisores comuns de 16 e 20 são 1,2 e 4. Dentre eles, 4 é o maior. Então chamamos o 4 de máximo divisor comum de 16 e 20 e indicamos MDC(16,20) = 4**.**

Definição 3.2.1 O maior divisor comum de dois ou mais números naturais é chamado de máximo divisor comum desses números. Usamos a abreviação MDC(a,b,c, ...) para indicar o máximo divisor comum de a,b,c,...

Poderíamos definir o MDC de dois números naturais a e b como sendo o número d satisfazendo:

1. $d|a$ e $d|b$.
2. Se $c|a$ e $c|b$, então $c|d$.

A condição (1) nos garante que d é divisor comum de a e b e a condição (2) nos diz que d é o maior divisor comum destes números. É claro que MDC(a,b) existe e é único, quaisquer que sejam a e b inteiros não ambos nulos.

Exemplos MDC(6,12) = 6; MDC(12,20) = 4; MDC(20,24) = 4; MDC(12,20,24) = 4; MDC(6,9,15) = 3

Teorema 3.2.1 (Identidade de **Bezout**) Seja d = MDC(a,b). Então existem x e y inteiros tais que $d = xa + yb$.

Prova Seja X = $\{ra + sb \mid ra + sb > 0\} \subset \mathbb{N}$. X $\neq \varnothing$, pois $|a| = 1|a| + 0b \in$ X. Pelo axioma da boa ordenação, X possui um menor elemento $d > 0$. Este número d, como está em X, é da forma $d = xa + yb$. Vamos mostrar que d é o máximo divisor comum de a e b. Pelo algoritmo da divisão,

$a = qd + r$, onde $0 \leq r < d$.

Então $r = a - qd = a - q(xa + yb) = a(1 - qx) + b(-yq)$, o que acarreta $r = 0$, pois $r > 0$ implicaria $r \in$ X, o que não pode porque d é o menor elemento de X. Logo, $a = qd$, ou seja, $d|a$. Analogamente $d|b$. Se $c|a$ e $c|b$, então $c|d$, pelo item 7 do teorema 3.1.3.

Exemplo MDC(20,24) = 4 = (–1)x20 + 1x24; MDC(12,20) = 4 = 2x12 + (–1)x20.

Dois números não nulos a e b são primos entre si quando o único divisor comum positivo de a e b é o número 1. É claro que, se a e b são primos entre si, então existem x e y inteiros tais que $1 = xa + yb$. De modo um pouco mais formal, temos:

Definição 3.2.2 Dizemos que os números inteiros não nulos a e b são relativamente primos ou primos entre si quando MDC(a,b) = 1.

Exemplo 8 e 15 são primos entre si. Se $a \in \mathbb{N}$, a e $a + 1$ são primos entre si.

3.3 O Teorema Fundamental da Aritmética

Definição 3.3.1 Um número natural $a > 1$ é um número primo quando ele tem exatamente dois divisores positivos: o número 1 e ele mesmo. Em outras palavras, é um número maior que um que não é divisível por nenhum outro número maior que 1 e menor que ele mesmo. Um número inteiro que não seja primo é chamado de composto.

Exemplo 2, 3, 5, 7, 11, 13 são os primeiros números primos. Com exceção do número 2, todos os outros números primos são ímpares.

Se $a \in \mathbb{Z}$ e $|a| > 1$, dizemos que a é primo se, e somente se, os únicos divisores positivos de a são 1 e a. Logo, se $a < 0$, a é primo se, e somente se, $|a| = -a$ é primo.

Teorema 3.3.1 Seja $a \in \mathbb{Z}$ tal que $|a| > 1$. Existe um número primo p que divide a.

Prova Se a for primo, basta fazer $p = a$. Se a não é primo, seja $b_1 \in \mathbb{Z}$ tal que $0 < b_1 < |a|$ e $b_1|a$. Se b_1 for primo, basta fazer $p = b_1$, caso contrário, considere b_2 um divisor de b_1, com $0 < b_2 < b_1$ o que acarreta que

b_2 também divide a. Temos assim uma sequência (b_n) decrescente de números inteiros positivos que é, portanto, finita e acaba quando encontramos b_k primo e que divide a.

Teorema 3.3.2 Seja a um número natural composto maior do que 1. Então a possui um divisor primo $\leq \sqrt{a}$.

Prova Como a é composto, existe um número primo $p < a$ tal que $a = pb$. Considere o conjunto $X = \{p$ primo tais que $a = pb$ para algum $b \in \mathbb{N}\} \neq \varnothing$. Pelo axioma da boa ordenação, existe p_o tal que p_o é o menor elemento de X. É claro que $p_o \leq b \Rightarrow p_o \cdot p_o \leq p_o \cdot b = a \Rightarrow p_o \leq \sqrt{a}$.

Reescrevendo o enunciado do teorema 3.3.2 teríamos: Se nenhum número natural $\leq \sqrt{a}$ é divisor de a, então a é um número primo.

Exemplo 101 é primo pois $\sqrt{101} \cong 10$ e os números primos 2, 3, 5 e 7 não dividem 101.

Teorema 3.3.3 O conjunto dos números primos é infinito.

Prova Suponhamos que $X = \{p \in \mathbb{Z} \mid p$ é primo$\}$ seja finito. Neste caso, podemos escrever
$X = \{p_1, p_2, ..., p_n\}$, com $p_1 < p_2 < ... < p_n$. O número $a = 1 + p_1 \cdot p_2 \cdots p_n > p_n$ não é primo e, pelo teorema 3.3.2, existe um número primo p_i que divide a. Como p_i divide $p_1 \cdot p_2 \cdots p_n = a - 1$ então p_i divide $a + (a - 1) = -1$, o que é absurdo pois -1 não possui divisores primos. Concluimos então que X não pode ser finito.

Teorema 3.3.4 Sejam a, $b \in \mathbb{Z} - \{0\}$. Se p é primo e p divide ab, então p divide a ou p divide b.

Prova Se p não divide a, então MDC$(p,a) = 1$ pois se $d =$ MDC(p,a) então d divide p e d divide a. Sendo p primo, $d = p$ ou $d = 1$. Como $d = p$ não pode, temos $d = 1$, ou seja, existem x e y inteiros tais que $ax + py = 1 \Rightarrow abx + pby = b \Rightarrow p$ divide b.

Corolário Se p e $p_1, p_2, ..., p_n$, são números primos e p divide $p_1 p_2 ... p_n$, então $p = p_i$ para algum i.

O resultado a seguir é conhecido como **Teorema Fundamental da Aritmética**. Ele nos assegura que todo número inteiro pode ser decomposto em um produto de números primos e essa decomposição é única, a menos da ordem em que aparecem os fatores. Como exemplos, apresentamos $6 = 3 \times 2 = 2 \times 3$, $12 = 3 \times 2 \times 2 = 2 \times 2 \times 3$, $-20 = -5 \times 2 \times 2 = 2 \times 2 \times (-5)$. Note que os fatores primos são os mesmos e trocamos apenas a ordem.

Teorema 3.3.5 Todo número $a \in \mathbb{Z} - \{-1, 0, 1\}$ pode ser escrito, de modo único, a menos da ordem dos fatores, na forma
$a = up_1p_2...p_n$,
onde $u = 1$, se $a > 0$ e $u = -1$, se $a < 0$ e $p_1,p_2,...,p_n$ são primos.

Prova Basta provar para $a > 1$ pois, se $a < -1$, então $-a > 1$. Considere o conjunto abaixo:

$X = \{x \in \mathbb{N} \mid x > 1 \text{ e } x \neq p_1p_2...p_n\}$

Supondo X não vazio, X possui, pelo axioma da boa ordenação, um menor elemento b. Mas, pelo teorema 3.2.2, existe um número primo p que divide b, ou seja, $b = cp$. Como $c < b$, temos que existe uma decomposição em fatores primos para c: $c = p_1p_2...p_n$, o que acarreta $b = pp_1p_2...p_n$, o que é uma contradição. Logo, $X = \varnothing$ e, por conseguinte, todo número $a \in \mathbb{Z} - \{-1, 0, 1\}$ pode ser escrito como produto de fatores primos.
A unicidade é uma decorrrência direta do teorema 3.3.4 e seu corolário.

Observação Quando os fatores primos se repetem usamos os expoentes para simplificar a notação: $8 = 2^3$; $36 = 2^23^2$; $-100 = (-1)2^25^2$.

Para sua informação

Em se tratando de Matemática em geral e de números primos em particular é perigoso fazer generalizações apenas com base numa observação ou no modo como se apresentam. Vejamos o exemplo: 31, 331, 3.331, 33.331, 333.331, 3.333.331 e 33.333.331 são todos primos mas 333.333.331 é um número composto, pois 333.333.331 = 17x19.607.843.
A forma como se distribuem os números primos revela uma completa irregularidade nessa disposição. Por exemplo existem pequenos e longos intervalos entre os números primos, o número 370.261 é seguido de apenas onze números compostos e não existem primos entre os números 20.831.323 e 20.831.533. Essa irregularidade na distribuição dos números primos é uma das razões de não existir uma fórmula matemática que produza todos os números primos.
Um fato bastante interessante e que mostra o quanto os números primos vão ficando cada vez mais raros é o seguinte:

Teorema 3.3.6 Dado um número inteiro k, existem k inteiros compostos consecutivos.

Prova O fatorial de um número inteiro k é definido como sendo $k! = 1x2x3x ... xk$. É claro que, se $k > 2$, $k!$ é composto pois é divisível por 2. Considere então os seguintes números:
$a_1 = (k + 1)! + 2$, $a_2 = (k + 1)! + 3$, $a_3 = (k + 1)! + 4$, ... , $a_k = (k + 1)! + (k + 1)$

Estes números são consecutivos e todos eles são compostos: $a_1 = (k + 1)! + 2$ é divisível por 2, $a_2 = (k + 1)! + 3$ é divisível por 3, $a_3 = (k + 1)! + 4$ é divisível por 4, ... , $a_k = (k + 1)! + (k + 1)$ é divisível por $k + 1$.
Voltemos ao MDC. Um modo de calcular o MDC de dois ou mais números é utilizar a decomposição desses números em fatores primos.
1) decompomos os números em fatores primos**;**
2) o MDC é o produto dos fatores primos comuns**.**

Exemplo Vamos calcular o MDC entre 36 e 90: 36 = 2x2x3x3 e 90 = 2x3x3x5. O MDC é o produto dos fatores primos comuns MDC(36,90) = 2x3x3 = 18. Escrevendo com expoentes: $36 = 2^2 x 3^2$ e $90 = 2 x 3^2 x 5$.

O MDC de dois ou mais números, quando fatorados, é o produto dos fatores comuns a eles, cada um elevado ao menor expoente. Dados *a* e *b* inteiros positivos, sempre podemos fatorá-los com os mesmos primos: *a* = e *b* = . Por exemplo, $28 = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^1$ e $30 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^0$. Neste caso, $MDC(28,30) = 2^1 \cdot 3^0 \cdot 5^0 \cdot 7^0 = 2$.

O processo que apresentamos a seguir para calcular o MDC(*a*,*b*) é conhecido como Algoritmo de Euclides ou processo das divisões sucessivas. Neste processo, efetuamos várias divisões até chegar a uma divisão exata. O divisor desta ultima divisão é o MDC.
Regra prática: suponhamos que $a > b$

1. dividimos o número maior pelo número menor, ou seja, dividimos *a* por *b*;

   $a/b = c$ (com resto r_1)

2. dividimos *b*, que é divisor da divisão anterior, por r_1, o resto da divisão anterior, e assim sucessivamente, até obtermos resto zero. Uma vez obtida uma divisão exata (resto zero), temos MDC(*a*,*b*) = último divisor deste processo.

Exemplos 1. Calcular MDC(50,20)

50/20 = 2 (resto 10)
20/**10** = 2 (resto zero).
A última divisão é exata e, pelo algoritmo de Euclides, MDC(50,20) = último divisor = 10

2. Calcular MDC (30,48)

48/**30** = 1 (resto **18**)
30/**18** = 1 (resto **12**)
18/**12** = 1 (resto **6**)
12/**6** = 2 (resto **zero**)
Pelo algoritmo de Euclides, MDC(30,48) = 6.

3. Calcular MDC (30,15)

30/15 = 2 (resto zero)
A divisão já é exata e MDC(30,15) = 15.

Podemos generalizar o resultado do exemplo anterior da seguinte forma: se a divide b, então MDC(a,b) = a. Dados dois ou mais números, se um deles é divisor de todos os outros, então ele é o MDC dos números dados. Por exemplo: MDC(15,30,45,120) = 15.

3.4 Mínimo Múltiplo Comum

Se a é divisível por b, dizemos que a é um múltiplo de b. Os múltiplos de b são 0, $\pm b$, $\pm 2b$, ..., $\pm nb$, ... Se $b \neq 0$, o conjunto de seus múltiplos é infinito. Dados a e b, o conjunto M dos múltiplos positivos comuns a a e b é não vazio pois $|ab| \in$ M. Pelo axioma da boa ordenação, M possui um menor elemento m. Este número é chamado Mínimo Múltiplo Comum de a e b e é denotado por m = MMC(a,b).

Exemplo Determinar o mínimo múltiplo comum de 4, 6 e 9.

Os múltiplos positivos de 4 são 4,8,12,16,20,24,... , os de 6 são 6,12,18,24,30,36,... e os de 9 são 9,18,27,36,... Assim, o conjunto M dos múltiplos comuns a 4, 6 e 9 é M = {36,72,...}, sendo o menor elemento de M o número 36 e daí, MMC(4,6,9) = 36.

O processo utilizado para o cálculo de MMC(a,b) é através da decomposição em fatores primos:

- Decompomos os números a e b em fatores primos;
- O MMC é o produto dos fatores primos comuns e não-comuns.

Se $a = p_1^{n_1} p_2^{n_2} p_3^{n_3} \cdots p_k^{n_k}$ e $b = p_1^{m_1} p_2^{m_2} p_3^{m_3} \cdots p_k^{m_k}$, MMC($a$,$b$) = $p_1^{s_1} p_2^{s_2} p_3^{s_3} \cdots p_k^{s_k}$, onde $s_i = max\{n_i,m_i\}$. Por exemplo, $28 = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^1$ e $30 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^0$. Neste caso, MDC(28,30) = $2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1$ = 420. Isto ocorre porque todo múltiplo de $a = p_1^{n_1} p_2^{n_2} p_3^{n_3} \cdots p_k^{n_k}$ tem que ter, em sua fatoração em primos, todos os primos que aparecem na fatoração de a. O mesmo ocorre, é claro, com qualquer múltiplo de $b = p_1^{m_1} p_2^{m_2} p_3^{m_3} \cdots p_k^{m_k}$.

Exemplo Determinar MMC(10,24) e MMC(30,54).

Temos 10 = 2x5 e 24 = 2x2x2x3 = 2^3x3 $\Rightarrow$ MMC(10,24) = 2^3x3x5 = 120.
30 = 2x3x5 e 54 = 2x3x3x3 = 2x3^3 $\Rightarrow$ MMC(30,54) = 2x3^3x5 = 270.

Se MDC(a,b) = 1, isto significa que a e b não possuem fatores primos comuns e, portanto, MMC(a,b) = ab. Como exemplos, temos: MMC(5,6) = 30; MMC(7, 12) = 84; MMC(6,25) = 150. Se um dos números,

digamos a, for múltiplo do outro, b, então MMC(a,b) = a. Por exemplo, MMC(5,10) = 10.

O processo que descrevemos a seguir é útil para calcular o MMC de n números quaisquer e é conhecido como **Processo de Decomposição Simultânea**.

Neste processo decompomos todos os números ao mesmo tempo, num dispositivo como mostra a tabela ao lado. O produto dos fatores primos que obtemos nessa decomposição é o mínimo múltiplo comum desses números. Ao lado vemos o cálculo de MMC(15,24,60). De acordo com a tabela ao lado e o descrito acima, temos

15	24	60	2
15	12	30	2
15	6	15	2
15	3	15	3
5	1	5	5
1	1	1	

MMC(15,24,60) = 2x2x2x3x5 = 120.

O teorema seguinte relaciona o mínimo múltiplo comum com o máximo divisor comum.

Teorema 3.4.1 Sejam a, $b \in \mathbb{N}$, d = MDC(a,b) e m = MMC(a,b). Então $md = ab$.

Prova Se $a = p_1^{n_1} p_2^{n_2} p_3^{n_3} \cdots p_k^{n_k}$ e $b = p_1^{m_1} p_2^{m_2} p_3^{m_3} \cdots p_k^{m_k}$, então $ab = p_1^{s_1} p_2^{s_2} p_3^{s_3} \cdots p_k^{s_k}$, onde $s_i = n_i + m_i$. Como
d = MDC(a,b) = $p_1^{\min\{n_1,m_1\}} p_2^{\min\{n_2,m_2\}} p_3^{\min\{n_3,m_3\}} \cdots p_k^{\min\{n_k,m_k\}}$,

m = MMC(a,b) = $p_1^{\max\{n_1,m_1\}} p_2^{\max\{n_2,m_2\}} p_3^{\max\{n_3,m_3\}} \cdots p_k^{\max\{n_k,m_k\}}$

e $\min\{n_i,m_i\} + \max\{n_i,m_i\} = n_i + m_i$, temos $ab = md$.

Exemplos 1. Como 3 = MDC(9,12), temos que MMC(9,12) = 9x12/3 = 9x4 = 36.

2. Se MDC(a,b) = 1, então MMC(a,b) = ab, ou seja, o MMC de números primos entre si é o produto desses números.

4. Avaliando o que foi construído

Nesta unidade, apresentamos os conceitos de Máximo Divisor Comum e Mínimo Múltiplo Comum, Números Primos e o Teorema Fundamental da Aritmética. Vimos também que o método mais simples de se obter o MMC e o MDC é a decomposição em fatores primos.

No Moodle

Agora vá à plataforma MOODLE e procure responder as questões e resolver os exercícios referentes ao tema estudado.

Unidade V Congruências

1. Situando a Temática

Nesta unidade reintroduzimos o conceito de congruência visto na Unidade II e, a partir das propriedades de congruência módulo n, daremos alguns critérios para verificar a divisibilidade de um número inteiro por outro.

2. Problematizando a Temática

Alguns critérios de divisibilidade são evidentes como, por exemplo, por 2 (basta que o número a ser dividido seja par), por 5 (o número deve terminar em 0 ou em 5), por 10 etc. No entanto, mesmo com critérios simples, fica difícil determinar a divisibilidade quando o número a ser dividido é muito grande. Há muito tempo, sabemos que para um número ser divisível por 3, basta que a soma de seus algarismos seja divisível por 3: por exemplo, 34.752 é divisível por 3 pois 3 + 4 + 7 + 5 + 2 = 21 que, por sua vez, é divisível por 3, mas como saber se o número $20^{7.539} + 34^{765.898}$ é, ou não, divisível por 3?

3. Conhecendo a Temática

3.1 Congruência módulo n

Definição 3.1.1 Dizemos que dois números inteiros a e b são congruentes módulo n, se $n|(a - b)$, ou seja, existe $k \in Z$ tal que $a - b = kn$.

Exemplos $-1 \equiv 6 \pmod 7$; $9 \equiv -1 \pmod{10}$; $5 \equiv -2 \pmod 7$; $19 \equiv 4 \pmod 5 = -1 \pmod 5$.

Usamos a notação $a \equiv b \pmod n$ para indicar a congruência de a com b módulo n. Já vimos, na unidade II, que $a \sim b$ se $a \equiv b \pmod n$ é uma relação de equivalência em $\mathbb{Z}$. O teorema seguinte nos diz quantas são as classes de equivalência módulo n.

Teorema 3.1.1 Dados a e b números inteiros, temos $a \equiv b \pmod n$ se, e somente se, a e b possuem o mesmo resto quando divididos por n.

Prova $a \equiv b \pmod n \Leftrightarrow \exists k \in \mathbb{Z}$ tal que $a - b = kn$.
Pelo algoritmo da divisão, existem q , $r \in \mathbb{Z}$ tais que

$$b = qn + r, \text{ com } 0 \leq r < n.$$

Daí,

$$a - b = kn \Rightarrow a = b + kn = qn + r + kn,$$

ou seja,

$$a = (q + k)n + r, \text{ com } 0 \leq r < n.$$

Portanto, a e b possuem o mesmo resto quando divididos por n.

Como, para cada $n \in \mathbb{Z}$, existem exatamente n "restos" possíveis, 0, 1, 2, ... , n – 1 e a classe de equivalência de $k \in \mathbb{Z}$ é a mesma classe do resto da divisão de k por n, o conjunto quociente $\in \mathbb{Z}/\equiv(\text{mod } n)$ possui exatamente n elementos e é denotado por $\mathbb{Z}_n = \{0,1,2,...,n - 1\}$. Com esta notação simplificada, estamos identificando cada classe de $\mathbb{Z}_n$ por um representante e isto significa que, quando escrevemos $0 \in \mathbb{Z}_n$ estamos nos referindo à classe que contém o zero, que é o conjunto cujos elementos são os múltiplos de n, ou seja, $0 \in \mathbb{Z}_n$ denota o conjunto de todos os elementos x tais que $x \equiv 0(\text{mod } n)$. Você pode continuar colocando a barra sobre o elemento de $\mathbb{Z}_n$ se lhe ficar mais compreensível.

3.2 Operações em $\mathbb{Z}_n$

Em $\mathbb{Z}_n$, é possível definir as operações de soma e produto da seguinte forma:

Definição 3.2.1 Dados $\overline{x}$ e $\overline{y} \in \mathbb{Z}_n$, definimos a soma $\overline{x} + \overline{y} = \overline{x + y}$ e o produto $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$.

Exemplos 1. Em $\mathbb{Z}_3$, os elementos (classes de congruência) são 0, 1 e 2, logo $1 + 2 = 3 \equiv 0(\text{mod } 3)$, ou seja, em $\mathbb{Z}_3$, $1 + 2 = 0$. Ainda em $\mathbb{Z}_3$, $2 + 2 = 4 \equiv 1(\text{mod } 3)$, ou seja, em $\mathbb{Z}_3$, $2 + 2 = 1$.

2. Em $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$, temos $1 + 0 = 1$, $2 + 3 = 5$, $4 + 3 = 1$, $4 + 4 = 2$, $2 \times 3 = 0$, $4 \times 3 = 0$, $3 \times 3 = 3$ e $4 \times 4 = 4$.

Prova 2 + 3 = 5 e 1 + 0 = 1 dispensam maiores explicações. Em $\mathbb{Z}$, $2 \times 3 = 6$ e, como 6 é congruente a zero (módulo 6), podemos escrever que, em $\mathbb{Z}_6$, $6 = 0$. As outras desigualdades ficam como exercício.

Veja as tabelas de soma e produto em $\mathbb{Z}_3$.

a	b	$a + b$
0	0	0
0	1	1
0	2	2
1	0	1
1	1	2
1	2	0
2	0	2
2	1	0
2	2	1

a	b	$a \cdot b$
0	0	0
0	1	0
0	2	0
1	0	0
1	1	1
1	2	2
2	0	0
2	1	2
2	2	1

Exercício Faça tabelas como estas para $\mathbb{Z}_2$ e $\mathbb{Z}_5$.

Definição 3.2.2 Dado um elemento a de $\mathbb{Z}_n$, dizemos que $a \neq 0$ possui inverso multiplicativo em $\mathbb{Z}_n$ se existir $b \neq 0$ em $\mathbb{Z}_n$ tal que $ab = 1$.

Todo elemento $a \neq 0$ de $\mathbb{Z}_p$, com p primo, possui inverso multiplicativo. O inverso de 3, em $\mathbb{Z}_5$, é 2, pois $3 \times 2 = 6 \equiv 1 (\text{mod } 5)$. Tente encontrar, para cada $a \neq 0$ de $\mathbb{Z}_p$, com p = 3 e com p = 5, seu respectivo inverso multiplicativo.

Definição 3.2.3 Dados a, b e c em $\mathbb{Z}_n$ tais que $a = bc$ e $b \neq 0$, dizemos que a é divisível por por b e $a \div b = c$.

Note que, em $\mathbb{Z}_6$, temos algumas divisões que podem ser efetuadas: $4 \div 2 = 2$, $2 \div 2 = 1$, $0 \div 3 = 0$ etc. Mas não pode $3 \div 2$ ou $5 \div 4$. Em $\mathbb{Z}_3$, no entanto, todas as divisões $a \div b$, com $b \neq 0$, podem ser efetuadas: $1 \div 1 = 1$, $1 \div 2 = 2$ (porque $2 \times 2 = 1$, em $\mathbb{Z}_3$), $2 \div 1 = 2$, $2 \div 2 = 1$ e $0 \div a = 0$, para qualquer $a \in \mathbb{Z}_3$. Aqui, a expressão "a divisão pode ser efetuada" significa que o resultado da mesma é um elemento do conjunto no qual se está trabalhando. Quando p é um número primo, podemos definir a operação de divisão em $\mathbb{Z}_p$.

Veja, à direita, como fica a tabela de multiplicação e divisão em $\mathbb{Z}_3$.

Na coluna que indica a divisão $a \div b$, " – " significa que não existe a operação, pois, como em um conjunto numérico, não se pode dividir por 0.

Lembre que, neste caso, os elementos a e b não representam números e sim classes de equivalência (congruência módulo 3).

a	b	$a \cdot b$	$a \div b$
0	0	0	–
0	1	0	0
0	2	0	0
1	0	0	–
1	1	1	1
1	2	2	2
2	0	0	–
2	1	2	2
2	2	1	1

Exercícios 1. Em $\mathbb{Z}_7$, quanto vale $5 \div 4$?

2. Em $\mathbb{Z}_8$, 7 é divisível por 5? Por que?

3. Complete a tabela abaixo para $\mathbb{Z}_2$.

a	b	$a \cdot b$	$a \div b$
0	0		
0	1		
1	0		
1	1		

4. Faça uma tabela de multiplicação e divisão para $\mathbb{Z}_5$.

3.3 Propriedades das Congruências módulo n e Critérios de Divisibilidade

Teorema 3.3.1 Dados a e b números inteiros, se $a \equiv b(\text{mod n})$ e $c \equiv d(\text{mod n})$ então
$a + c \equiv (b + d)(\text{mod n})$.

Prova $a \equiv b(\text{mod n}) \Leftrightarrow \exists\, x \in \mathbb{Z}$ tal que $a = b + x\text{n}$ e $c \equiv d(\text{mod n}) \Leftrightarrow \exists\, y \in \mathbb{Z}$ tal que $c = d + y\text{n}$

Logo,
$a + c = b + d + (x + y)\text{n} \Leftrightarrow a + c \equiv (b + d)(\text{mod n})$.

Exemplos $7 \equiv 2(\text{mod } 5)$ e $15 \equiv 0(\text{mod } 5)$. Logo $22 \equiv 2(\text{mod } 5)$; $143 \equiv 3(\text{mod } 5)$ e $527 \equiv 2(\text{mod } 5) \Rightarrow 670 \equiv 0(\text{mod } 5)$; $20 \equiv -1(\text{mod } 7)$ e $218 \equiv 1(\text{mod } 7) \Rightarrow 237 \equiv 0(\text{mod } 7)$, ou seja, 237 é divisível por 7.

Teorema 3.3.2 Dados a e b números inteiros, se $a \equiv b(\text{mod n})$ e $x \in \mathbb{Z}$ então $ax \equiv bx(\text{mod n})$.

Prova $a \equiv b(\text{mod n}) \Leftrightarrow \exists\, k \in \mathbb{Z}$ tal que $a - b = k\text{n} \Rightarrow ax - bx = kx\text{n} \Leftrightarrow ax \equiv bx(\text{mod n})$.

Exemplos $37 \equiv 2(\text{mod } 5) \Rightarrow 37\text{x}2 = 74 \equiv 4(\text{mod } 5)$; $14 \equiv 3(\text{mod } 11) \Rightarrow 14\text{x}4 = 56 \equiv 12(\text{mod } 11) = 1(\text{mod } 11)$.

A recíproca do teorema 3.1.3, que seria a lei do cancelamento, não vale em $\mathbb{Z}_n$: $7\text{x}2 \equiv 4\text{x}2(\text{mod } 6)$. Se valesse a lei do cancelamento, teríamos $7 \equiv 4(\text{mod } 6)$, o que não ocorre, pois $7 \equiv 1(\text{mod } 6) \neq 4(\text{mod } 6)$.

Teorema 3.3.3 Dados a e b números inteiros, se $a \equiv b(\text{mod n})$ e $c \equiv d(\text{mod n})$ então $ac \equiv bd(\text{mod n})$.

Prova Como $a \equiv b(\text{mod n})$, $\exists\, x \in \mathbb{Z}$ tal que $a = b + x\text{n}$. Analogamente, como $c \equiv d(\text{mod n})$, $\exists\, y \in \mathbb{Z}$ tal que $c = d + y\text{n}$. Portanto,

$ac - bd = (b + x\text{n})(d + y\text{n}) - bd = bd + by\text{n} + dx\text{n} + xy\text{n}^2 - bd = (by + dx + xy\text{n})\text{n}$,
ou seja,
$ac = bd(\text{mod n})$

Exemplo $7 \equiv 2(\text{mod } 5)$ e $101 \equiv 16(\text{mod } 5) \Rightarrow 7\text{x}101 = 707 \equiv 32(\text{mod } 5)$

Teorema 3.3.4 Dados a e b números inteiros, se $a \equiv b(\text{mod n})$ e $x \in \mathbb{N}$ então $a^x \equiv b^x(\text{mod n})$.

Prova Suponhamos que $a \equiv b(\text{mod n})$ e considere $X = \{k \in \mathbb{N} \mid a^k \equiv b^k(\text{mod n})\}$. Usaremos o Princípio da Indução para provar que $X = \mathbb{N}$.

- É claro que $1 \in X$.
- Suponhamos que para algum $k \in \mathbb{N}$, tenhamos $a^k \equiv b^k(\text{mod n})$, ou seja, $k \in X$.
- Como $a \equiv b(\text{mod n})$, temos, pelo teorema 3.1.4, $aa^k \equiv bb^k(\text{mod n})$, isto é, $a^{k+1} \equiv b^{k+1}(\text{mod n})$.

Daí, $k + 1 \in X \Rightarrow X = \mathbb{N}$.

Dos teoremas 3.1.3 e 3.1.5, obtemos o seguinte resultado:

Teorema 3.3.5 Dados a e $b \in \mathbb{Z}$ com $a \equiv b(\text{mod n})$ e $p(x) = a_0 + a_1x + a_2x^2 + ... + a_mx^m$ um polinômio com coeficientes em $\mathbb{Z}$ então $p(a) \equiv p(b)(\text{mod n})$.

Exemplos 1. Como $7 \equiv -1(\text{mod } 8)$ então $7^{55} \equiv -1(\text{mod } 8)$ e $7^{552} \equiv 1(\text{mod } 8)$ e $7^{55} + 7^{552}$ é divisível por 8, pois $7^{55} + 7^{552} \equiv (-1 + 1)(\text{mod } 8) = 0(\text{mod } 8)$.

2. Mostre que $20^{579} + 55^{894}$ é divisível por 3.

Prova Para mostrar que um número $a \in \mathbb{Z}$ é divisível por $b \in \mathbb{Z}$, basta provar que $a \equiv 0(\text{mod } b)$.

Temos que $20 \equiv -1(\text{mod } 3)$ e $55 \equiv 1(\text{mod } 3) \Rightarrow 20^{579} \equiv -1(\text{mod } 3)$ e $55^{894} \equiv 1(\text{mod } 3)$. Portanto, $20^{579} + 55^{894} \equiv 0(\text{mod } 3)$.

3. Mostre que $a_0 + a_1 \times 10 + a_2 \times 10^2 + ... + a_n \times 10^n$ é divisível por 3 se, e somente se, $a_0 + a_1 + a_2 + ... + a_n$ é divisível por 3, ou seja, um número é divisível por 3 se, e somente se, a soma de seus algarismos é divisível por 3.

Prova Considere o polinômio de coeficientes inteiros $p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$. Como $10 \equiv 1(\text{mod } 3)$, pelo teorema 3.1.5, $p(10) \equiv p(1)(\text{mod } 3)$, ou seja,

$$a_0 + a_1 \times 10 + a_2 \times 10^2 + ... + a_n \times 10^n \equiv (a_0 + a_1 + a_2 + ... + a_n)(\text{mod } 3)$$

Logo, $a_0 + a_1 \times 10 + a_2 \times 10^2 + ... + a_n \times 10^n$ é divisível por 3, ou seja,

$$a_0 + a_1 \times 10 + a_2 \times 10^2 + ... + a_n \times 10^n \equiv 0(\text{mod } 3) \qquad \text{(I)}$$

se, e somente se, $a_0 + a_1 + a_2 + ... + a_n$ é divisível por 3, ou seja,

$$a_0 + a_1 + a_2 + ... + a_n \equiv 0(\text{mod } 3) \qquad \text{(II)}$$

e as congruências (I) e (II) são equivalentes.

4. Mostre que $a_0 + a_1 x10 + a_2 x10^2 + ... + a_n x10^n$ é divisível por 4 se, e somente se, $a_0 + a_1 x10$ é divisível por 4. Para testar a divisibilidade por 4 basta verificar os dois últimos algarismos que compõem o número na base 10. Assim, 45.318 não é divisível por 4, pois 18 não é divisível por 4. Já o número 3.748 é divisível por 4 porque 4 divide 48.

Prova Como 4 divide 100, temos $a_k x10^k \equiv 0(\text{mod } 4)$, $\forall$ k $\geq$ 2. Daí,

$$a_0 + a_1 x10 + a_2 x10^2 + ... + a_n x10^n \equiv (a_0 + a_1 x10)(\text{mod } 4)$$

e

$$a_0 + a_1 x10 + a_2 x10^2 + ... + a_n x10^n \equiv 0(\text{mod } 4) \Leftrightarrow a_0 + a_1 x10 \equiv 0(\text{mod } 4).$$

Como $10 \equiv 2(\text{mod } 4)$, o critério de divisibilidade por 4 pode ser ligeiramente melhorado da seguinte forma: $a_0 + a_1 x10 + a_2 x10^2 + ... + a_n x10^n$ é divisível por 4 se, e somente se, $a_0 + 2a_1$ é divisível por 4.

Exemplos 546 não é divisível por 4 pois 6 + 2x4 = 14 não é divisível por 4; 976 é divisível por 4 pois 6 + 2x7 = 20 é divisível por 4.

Exercícios 1. Qual o critério de divisibilidade por 9 de um número inteiro $A = a_0 + a_1 x10 + a_2 x10^2 + ... + a_n x10^n$?

Sugestão: veja como foi feito no exemplo 3 acima.

2. Sejam a, b e $c \in Z$ tais que $a = bc + 1$. Mostre que $a \equiv -1(\text{mod } b)$. Por exemplo, $3.457 \equiv -1(\text{mod } 9)$, pois 3.457 = 3.456 + 1 e 3.456 é divisível por 9.

3. Observe que $a_0 + a_1 x10 + a_2 x10^2 + ... + a_n x10^n \equiv a_0(\text{mod } 10)$, onde $a_0 \in \{0,1,2,...,9\}$, ou seja, para determinar o último algarismo de um número, basta calcular a sua congruência módulo 10. Por exemplo, $44.876 \equiv 6(\text{mod } 10)$. Determine o dígito das unidades (último algarismo) do número $a = 3^{98}$.

Sugestão: Observe que $3^{98} = (3^2)^{49}$ e $3^2 = 9 \equiv -1(\text{mod } 10)$ e, se $a \equiv -1(\text{mod } 10)$, seu último algarismo é 9.

4. Avaliando o que foi construído

Nesta unidade, reapresentamos o conceito de congruência módulo n com o objetivo de expor algumas técnicas para se obter critérios de

divisibilidade. Apresentamos o conjunto quociente $\mathbb{Z}_n = \mathbb{Z}/\equiv(\text{mod } n)$ com uma forma mais simplificada e informamos a possibilidade de se definir a operação de divisão em $\mathbb{Z}_p$ com p primo.

No Moodle

Agora vá à plataforma MOODLE e procure responder as questões e resolver os exercícios referentes ao tema estudado.

5. Bibliografia

GONÇALVES, A. *Introdução à Álgebra*. Projeto Euclides, IMPA. 1979.

HALMOS, P. R. *Naive Set Theory*. Princeton, NJ. Van Nostrand. 1960.

HEFEZ, A. *Curso de Álgebra*, Vol I. Coleção Matemática Universitária, IMPA. 1993.

LIMA, E. L. *Curso de Análise*, Vol I. Projeto Euclides, IMPA. 1976.

SIDKI, S. *Introdução à Teoria dos Números*. 10º Colóquio Brasileiro de Matemática, IMPA. 1975.

SIERPINSKI, W. *250 Problems in Elementary Number Theory*. American Elsevier Publishing Company. 1970.

SILVA, A. A. *Números, Relações e Criptografia*. Notas de aula, Departamento de Matemática, UFPB