Notas de Aula: Matemática para Ciência da Computação

Universidade Federal de Uberlândia

2020

Sumário

Capítulo 1

Tipos de Demonstração

Começaremos o curso com demonstrações. Assumiremos algumas propriedades sobre os números reais e deduziremos outras. No meio do caminho aprenderemos o nome que damos aos tipos de demonstrações.

O material que estou utilizando está baseado no curso que tive na Unicamp chamado Complementos da Matemática, lecionado pelos professores José Mario Martinez e Lúcio Tunes Santos.

1.1 Demonstrações com números reais

Os números reais possuem duas operações chamadas de soma (denotada pelo sinal $+$) e produto (denotado por um ponto .). Também possuem uma relação de ordem (denotada pelo sinal de menor $<$). As seguintes propriedades valem.

S_1. **Associatividade da Soma:** Para quaisquer números reais a, b, c vale $a + (b + c) = (a + b) + c$.

S_2. **Comutatividade da Soma:** Para quaisquer números reais a, b vale $a + b = b + a$.

S_3. **Elemento Neutro da Soma:** Existe um número real que será denotado por 0 (e chamado de zero) tal que para todo número real a vale $a + 0 = a$.

S_4. **Inverso Aditivo:** Para todo número real a existe um número real que será denotado por $-a$ que satisfaz $a + (-a) = 0$.

P_1. **Associatividade do Produto:** Para quaisquer números reais a, b, c vale $a.(b.c) = (a.b).c$

P_2. **Comutatividade do Produto:** Para quaisquer números reais a, b vale $a.b = b.a$.

P_3. **Elemento Neutro do Produto:** Existe um número real diferente de zero que será denotado por 1 (e chamado de um) tal que para todo número real a vale $a.1 = a$.

P_4. **Inverso Multiplicativo:** Para todo número real a diferente de 0 existe um número real que será denotado por a^{-1} que satisfaz $a.a^{-1} = 1$.

D_1. **Distributividade:** Para quaisquer números reais a, b, c vale $a.(b + c) = a.b + a.c$.

O_1. **Tricotomia:** Para quaisquer números reais a, b vale somente uma das seguintes relações: $a < b$ ou $a = b$ ou $b < a$.

O_2. **Transitividade:** Para quaisquer números reais a, b, c vale:
Se $a < b$ e $b < c$ então $a < c$.

O_3. **Consistência com respeito a soma:** Para quaisquer números reais a, b, c vale:
Se $a < b$ então $a + c < b + c$.

O_4. **Consistência com respeito ao produto:** Para quaisquer números reais a, b, c vale:
Se $0 < c$ e $a < b$ então $a.c < b.c$.

N. **Notação:** $a - b = a + (-b)$ e $\frac{a}{b} = a.b^{-1}$ (quando $b \neq 0$)

Exercício 1.1.1. *Sejam a, b, c números reais. A partir das propriedades $S_1, \ldots, O_4$ demonstrar cada uma das seguintes afirmações.*

a) *Se* $a + b = c + b$ *então* $a = c$

b) *Se* $a + a = a$ *então* $a = 0$

c) $a = -(-a)$

d) $0 = -0$

e) $a.0 = 0$

f) *Se* $a \neq 0$ *então* $-a \neq 0$

g) $-(a + b) = (-a) + (-b)$

h) $a + b = a - (-b)$

i) $(-a).b = -(a.b) = a.(-b)$

j) $(-1).a = -a$

k) $(-a)(-b) = a.b$

$l)$ $(-a)(-b)(-c) = -(a.b.c)$

$m)$ $a.(b-c) = a.b - a.c$

$n)$ *Se* $a.b = 0$ *então* $a = 0$ *ou* $b = 0$

$o)$ *Se* $a.a = 1$ *então* $a = 1$ *ou* $a = -1$

$p)$ *Se* $a \neq 0$ *e* $a.b = a.c$ *então* $b = c$

$q)$ $1 = 1^{-1}$ *e* $-1 = (-1)^{-1}$

$r)$ *Se* $a \neq 0$ *então* $a^{-1} \neq 0$ *e* $(-a)^{-1} = -a^{-1}$

$s)$ *Se* $a \neq 0$ *então* $a = (a^{-1})^{-1}$

$t)$ *Se* $a \neq 0$ *e* $b \neq 0$ *então* $(a.b)^{-1} = a^{-1}.\ b^{-1}$

A seguir vamos resolver alguns itens do exercício 1.1.1.

Observação 1.1.2. *A maioria das afirmações que vamos provar são do tipo – se isso então aquilo –. Portanto devemos assumir isso e concluir aquilo utilizando fatos conhecidos. Por exemplo, em* 1.1.1.*a o que assumimos é* $a+b = c+b$ *e o que queremos concluir é* $a = c$*. Vamos fazer isso utilizando as propriedades de* S_1 *a* O_4*. Aquilo que assumimos é chamado de* <u>*hipótese*</u> *e aquilo que queremos concluir é chamado de* <u>*tese*</u>*.*

1.1.1.a) Se $a + b = c + b$ então $a = c$.
Por S_4, existe $-b$. Somando-o aos dos lados da hipótese obtemos
$(a + b) + (-b) = (c + b) + (-b)$.
Por S_1, $a + (b + (-b)) = c + (b + (-b))$
Por S_4, $a + 0 = c + 0$
Por S_3, $a = c$. $\square$

Terminamos a nossa primeira demonstração. O fim dela é indicado por esse quadrado ($\square$).

1.1.1.b) Se $a + a = a$ então $a = 0$
Por S_4, $(a + a) + -a = a + -a$

Por S_1, $a + (a + -a) = a + -a$

Por S_4, $a + 0 = 0$

Por S_3, $a = 0$. $\square$

Observação 1.1.3. *A seguir queremos provar que $a = -(-a)$. Aparentemente não temos hipótese, isto é, não temos de onde partir. Na verdade podemos partir de qualquer coisa que já sabemos ser verdadeira. Por exemplo, as propriedades de S_1 a O_4. Note que $-(-a)$ deve aparecer na sua conclusão. Portanto é natural começar com a propriedade que fala de $-(-a)$.*

1.1.1.*c*) $a = -(-a)$

Por S_4, $-a + -(-a) = 0$

Portanto $a + (-a + -(-a)) = a + 0$

Por S_1, $(a + -a) + -(-a) = a + 0$

Por S_4, $0 + -(-a) = a + 0$

Por S_2, $-(-a) + 0 = a + 0$

Por S_3, $-(-a) = a$. $\square$

1.1.1.*d*) $0 = -0$

Por S_4, $0 + -0 = 0$

Por S_2, $-0 + 0 = 0$

Por S_3, $-0 = 0$. $\square$

1.1.1.*e*) $a.0 = 0$

Por S_3, $0 = 0 + 0$

Portanto $a.0 = a.(0 + 0)$

Por D_1, $a.0 = a.0 + a.0$

Pelo resultado provado em 1.1.1.*b* temos $a.0 = 0$. $\square$

Observação 1.1.4. *Nesse último exercício usamos um resultado que já havíamos estabelecido antes* (1.1.1.*b*). *Cada afirmação provada é uma nova informação que pode ser utilizada na demonstração das outras afirmações.*

Observação 1.1.5. *No seguinte exercício queremos provar que Se $a \neq 0$ então $-a \neq 0$. Aqui $a \neq 0$ significa que $0 < a$ ou $a < 0$ pela propriedade O_1. Portanto temos que provar que : Se $0 < a$ ou $a < 0$ então $0 < -a$ ou $-a < 0$.*

Vamos dividir essa tarefa em duas. Primeiro provaremos que Se $0 < a$ então $-a < 0$ e depois que Se $a < 0$ então $0 < -a$. Note que isso basta pra provar o que queremos, pois as duas possibilidades impostas ao a implica nas duas possibilidades que queremos para o $-a$.

1.1.1.f) Se $a \neq 0$ então $-a \neq 0$

Primeiramente, se $0 < a$.

Por O_3, $0 + -a < a + -a$

Por S_4, $0 + -a < 0$

Por S_3, $-a < 0$. Isso termina a primeira parte.

Agora, se $a < 0$.

Por O_3, $a + -a < 0 + -a$

Por S_4, $0 < 0 + -a$

Por S_3, $0 < -a$. □

Observação 1.1.6. *Até agora todas as demontrações foram **diretas**, isto é, partimos da hipótese e utilizando as propriedades chegamos na tese. O resultado* 1.1.1.f *admite uma demonstração indireta que chamamos de prova por contradição.*

Segunda demonstração de 1.1.1.f

Se supormos que a tese que queremos provar é falsa. Nesse caso significa $-a = 0$.

Então $a + -a = a + 0$

Por S_4, $0 = a + 0$

Por S_3, $0 = a$. Mas isso contraria a hipótese (que é de onde devemos partir).

Isso é uma contradição! O que fizemos de errado?

Nós dissemos que a tese era falsa (negamos a tese). Então a tese não pode ser falsa.

Portanto ela é verdadeira, concluindo a demonstração.

Prova por contradição

Definição 1.1.7. *Assume-se o oposto do que queremos provar e chegamos a uma contradição. Portanto o que queremos provar é verdadeiro (para evitar a contradição).*

Outro exemplo de prova por contradição.

1.1.1.n) Se $a.b = 0$ então $a = 0$ ou $b = 0$.

A negação da tese é $a \neq 0$ e $b \neq 0$.

Por P_4, existe a^{-1} que ao ser multiplicado dos dois lados da hipótese dá

$a^{-1}(a.b) = a^{-1}.0$

Por P_1, $(a^{-1}.a).b = a^{-1}.0$

Por P_4, $1.b = a^{-1}.0$

Por P_3, $b = a^{-1}.0$

Por 1.1.1.e já demonstrado, $b = 0$.

Mas isso contraria o fato no início da demonstração que diz que $b \neq 0$.

O erro veio de negar a tese (dizer que ela é falsa). Portanto ela é verdadeira: $a = 0$ ou $b = 0$.

Exercício 1.1.8. *Sejam a, b, c, d números reais tais que $b \neq 0$ e $d \neq 0$. Prove as seguintes afirmações.*

a) $\dfrac{0}{b} = 0$

b) $\dfrac{a}{b} = \dfrac{c}{d}$ *se e somente se* $a.d = b.c$

c) $\dfrac{a}{\left(\dfrac{b}{d}\right)} = \dfrac{a.d}{b}$

d) $\left(\dfrac{b}{d}\right)^{-1} = \dfrac{d}{b}$

e) $-\dfrac{a}{b} = \dfrac{-a}{b} = \dfrac{a}{-b}$ *e* $\dfrac{-a}{-b} = \dfrac{a}{b}$

f) $\dfrac{a}{b}.\dfrac{c}{d} = \dfrac{a.c}{b.d}$

g) Se $\dfrac{a}{b} = \dfrac{c}{d}$ *então*

- *(i)* $\dfrac{a+b}{b} = \dfrac{c+d}{d}$
- *(ii)* $\dfrac{a-b}{b} = \dfrac{c-d}{d}$

(*iii*) $\dfrac{a+b}{a-b} = \dfrac{c+d}{c-d}$, *quando* $a \neq b$ *e* $c \neq d$

(*iv*) $\dfrac{a}{b} = \dfrac{a+c}{b+d}$, *se* $b+d \neq 0$.

h) $\dfrac{a}{b} \pm \dfrac{c}{d} = \dfrac{a.d \pm b.c}{b.d}$

Observação 1.1.9. *No seguinte exercício aparece o termo* <u>se e somente se</u> . *Para explicá-lo vamos considerar as seguintes frases:*

- *O gramado é molhado somente se chover. Isso significa que – Se o gramado está molhado então choveu.*
- *O gramado é molhado se chover. Isso significa que – Se chover então o gramado é molhado.*

Por exemplo, para demonstrar: $a.b = 0$ *se e somente se* $a = 0$ *ou* $b = 0$.
Devemos provar duas coisas

- *Se* $a.b = 0$ *então* $a = 0$ *ou* $b = 0$. *Isso corresponde a* <u>$a.b = 0$, *somente se* $a = 0$ *ou* $b = 0$.</u>
- *Se* $a = 0$ *ou* $b = 0$ *então* $a.b = 0$. *Isso corresponde a* <u>$a.b = 0$, *se* $a = 0$ *ou* $b = 0$.</u>

(*Note que ambos já foram provados em 1.1.1.n e 1.1.1.e*).

A seguir vamos resolver alguns itens do exercício 1.1.8.

1.1.8.*b*) $\dfrac{a}{b} = \dfrac{c}{d}$ se e somente se $a.d = b.c$

<u>Primeira parte:</u> Se $a.d = b.c$ então $\dfrac{a}{b} = \dfrac{c}{d}$
Como $d \neq 0$ e $b \neq 0$ (está no enunciado do exercício).
Por P_4, existem d^{-1} e b^{-1}.
Multiplicando $d^{-1}.b^{-1}$ dos dois lados da hipótese obtemos $(d^{-1}.b^{-1}).a.d = (d^{-1}.b^{-1}).b.c$
Por P_1 e P_2, $(d^{-1}.d).a.b^{-1} = (c.d^{-1}).b^{-1}b$
Por P_3 e P_4, $a.b^{-1} = c.d^{-1}$.

Pela notação depois das propriedades obtemos $\frac{a}{b} = \frac{c}{d}$.

Segunda parte: Se $\frac{a}{b} = \frac{c}{d}$ então $a.d = b.c$

Pela notação depois das propriedades a hipótese significa $a.b^{-1} = c.d^{-1}$.

Multplicando ambos os lados por $b.d$ obtemos $(b.d).a.b^{-1} = (b.d).c.d^{-1}$.

Por P_1 e P_2, $a.d.(b.b^{-1}) = b.c.(d.d^{-1})$.

Por P_3 e P_4, $a.d = b.c$ $\square$

1.1.8.d) $\left(\frac{b}{d}\right)^{-1} = \frac{d}{b}$

Pela notação $\frac{b}{d} = b.d^{-1}$.

Sabemos que b, d são diferentes de 0 pelo enunciado do exercício 1.1.8.

Por 1.1.1.r, temos $d^{-1} \neq 0$.

Portanto $b.d^{-1} \neq 0$, pela observação acima.

Por P_4, existe $(b.d^{-1})^{-1}$ e $b.d^{-1}(b.d^{-1})^{-1} = 1$

Multiplicando ambos os lados por $d.b^{-1}$, obtemos $(d.b^{-1})(b.d^{-1}(b.d^{-1})^{-1}) = (d.b^{-1}).1$

Por P_1, $(d.b^{-1}.(b.d^{-1}))(b.d^{-1})^{-1}) = (d.b^{-1}).1$

Por P_1 e P_2, $((b^{-1}.b)(d^{-1}.d))(b.d^{-1})^{-1}) = (d.b^{-1}).1$

Por P_3 e P_4, $(b.d^{-1})^{-1} = d.b^{-1}$

Pela notação, $\left(\frac{b}{d}\right)^{-1} = \frac{d}{b}$. $\square$

Exercício 1.1.10. *Sejam a, b, c, d números reais. Prove as seguintes afirmações.*

a) *Se $0 < a$ se somente se $-a < 0$*

b) $0 < 1$

c) *Se $a < b$ então $a - c < b - c$*

d) *Se $a + a + a = 0$ então $a = 0$*

e) *Se $a + a = 0$ então $a = 0$*

f) *Se $a \neq 0$ então $-a \neq 0$*

g) *$0 < a$ se e somente se $0 < a^{-1}$.*

h) *Se $0 < a$ e $0 < b$ então ($a < b$ se e somente se $b^{-1} < a^{-1}$)*

i) *Se* $a \neq 0$ *então* $0 < a.a$

j) $a.a + b.b = 0$ *se e somente se* $a = b = 0$

A seguir vamos resolver alguns itens do exercício 1.1.10.

1.1.10.*b*) $0 < 1$

Como $1 \neq 0$, pela propriedade P_3, então $0 < 1$ ou $1 < 0$.

Vamos supor que $1 < 0$ (Estamos negando a tese).

Por O_3, $1 + -1 < 0 + -1$

Por S_3 e S_4, $0 < -1$ $(*)$

Por O_4, como $0 < -1$ então $1.(-1) < 0.(-1)$

Por P_3 e por 1.1.1.*e*, temos $-1 < 0$. Mas isso contraria $(*)$ acima.

Portanto se assurmirmos que $1 < 0$ chegamos a uma contradição.

Assim $0 < 1$ para evitar a contradição. □

1.1.10.*e*) Se $a + a = 0$ então $a = 0$

Primeira demonstração:

Por P_3, $a + a = a.1 + a.1$

Por D_1 e pela hipótese, $0 = a.(1 + 1)$

Por O_3, como $0 < 1$ então $0 + 1 < 1 + 1$

Assim $0 < 1$ e $1 < 1 + 1$.

Por O_2, $0 < 1 + 1$.

Portanto $1 + 1 \neq 0$.

Como $a.(1 + 1) = 0$ e $1 + 1 \neq 0$, sabemos que $a = 0$ pelo 1.1.1.*n*).

Segunda demonstração:

Neguemos a tese, ou seja, suponha que $a \neq 0$.

Temos duas opções por O_1, $0 < a$ ou $a < 0$.

Por O_3, $0 + a < a + a$ ou $a + a < a + 0$

Por S_3, $(0 < a$ e $a < a + a)$ ou $(a + a < a$ e $a < 0)$

Por O_2, $0 < a + a$ ou $a + a < 0$. Isto é, $a + a \neq 0$.

Isso contraria a hipótese que diz que $a + a = 0$.

Portanto $a = 0$ para evitar a contradição. □

Observação 1.1.11. *Existe uma pequena diferença entre as contradições obtidas em* 1.1.10.*b*) *e na segunda demonstração de* 1.1.10.*e*). *Em* 1.1.10.*b*) *a contradição foi obtida com algum fato que apareceu no meio da demonstração. Já em* 1.1.10.*e*), *a contradição foi com a hipótese. Isto é, negamos a tese e chegamos na negação da hipótese. Isso já havia acontecido antes na segunda demonstração do* 1.1.1.*f*). *Lembre-se que para provar uma afirmação provamos que a negação da sua tese implica na negação da sua hipótese.*

Contrapositiva

Definição 1.1.12. *Dada uma afirmação do tipo: Se p vale então q vale. A sua afirmação contra-positiva é Se q não vale então p não vale. A hipótese da contra-positiva é a negação da tese da afirmação inicial e a tese da contra-positiva é a negação da hipótese da afirmação inicial. Note que a contrapositiva da contrapositiva é a afirmação original.*

Exemplo:

Afirmação: Se choveu então a grama está molhada.
Contrapositiva: Se a grama não está molhada então não choveu.
Contrapositiva da contrapositiva: Se choveu então a grama está molhada.

Outro exemplo: A contrapositiva de Se $a + a = 0$ então $a = 0$ é Se $a \neq 0$ então $a + a \neq 0$.

Pela observação 1.1.11 devemos suspeitar que existe alguma relação entre a afirmação e a sua contrapositiva. Essa relação está descrita no seguinte resultado.

Teorema 1.1.13. *Uma afirmação do tipo – Se p vale então q vale – e sua contrapositiva – Se q não vale então p não vale – significam a mesma coisa.*

Justificativa do teorema 1.1.13:

Aqui usaremos a demonstração por contradição (que já estamos convencidos que funciona) para mostrar que se a afirmação é verdadeira então e a sua contrapositiva também é.

Note que a contrapositiva da contrapositiva é a própria afirmação. Portanto se a contrapositiva é verdadeira, pelo resultado que provaremos, a sua contrapositiva que é afirmação também é. Conclusão: A afirmação é verdadeira se e somente se a sua contrapositiva é verdadeira.

Só falta mostrar que se (Se p vale então q vale) é verdadeira então (Se q não vale então p não vale) também é.

Neguemos a tese, isto é, suponha que (Se q não vale então p não vale) é falsa. Isso significa que é possível ter ambos q não vale e p vale.

Mas se p vale então q vale, pois (Se p vale então q vale) é verdadeiro. Mas isso contraria o que acabamos de dizer que q não vale.

Portanto (Se q não vale então p não vale) não pode ser falsa. □

Prova por contraposição

Definição 1.1.14. *Provar Se p então q é o mesmo que provar a sua afirmação contrapositiva Se não q então não p.*

1.2 Teoria de Conjuntos

A seguir continuaremos a estudar demonstrações, agora no contexto de teoria de conjuntos. Os exemplos e as definições dessa seção foram retiradas do segundo capítulo do livro do Matemática Discreta e Aplicações cujo autor é o K.H. Rosen.

Definição 1.2.1. *Um conjunto é uma coleção não ordenada de objetos. Os objetos do conjunto são chamados elementos ou membros do conjunto. Dizemos que os objetos de um conjunto pertecem a ele.*

Notação: *$c \in A$ significa que c é um elemento do conjunto A, ou seja, c pertence a A.*
$c \notin A$ significa que c não é elemento de A, ou seja, c não pertence a A.

Exemplos:

- O conjunto das vogais pode ser escrito como $\{a, e, i, o, u\}$.
  Note que $a \in \{a, e, i, o, u\}$ e $f \notin \{a, e, i, o, u\}$.
- $\mathbb{N} = \{1, 2, 3, \ldots\}$ é o conjunto dos números naturais.
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ é o conjunto dos números inteiros.
- O conjunto dos números inteiros postivos menores que 100:

$$\{1, 2, \ldots, 98, 99\} \text{ ou } \{x \mid x \text{ é inteiro e } 0 < x < 100\}.$$

- $\mathbb{R}$ = conjuntos dos números reais.

Definição 1.2.2. *Dizemos que dois conjuntos são iguais se possuem os mesmos elementos. Se A e B forem conjuntos iguais escreveremos $A = B$. Portanto $\{3, 2, 1\} = \{1, 2, 3\}$.*

Definição 1.2.3. *Existe um conjunto que não possui elementos. Ele será chamado de vazio e será denotado por $\emptyset$.*

Definição 1.2.4. *Um conjunto A é dito subconjunto de um conjunto de B, se todos os elementos de A também são de B. Denotaremos essa relação entre A e B por $A \subset B$ (A está contido em B). Se existir um elemento de um conjunto C que não pertence a B então diremos que C não é subconjunto de B e denotaremos isso por $C \not\subset B$ (C não está contido em B).*

Exemplos: $\{1, 2\} \subset \{1, 2, 3\}$ e $\{1, 4\} \not\subset \{1, 2, 3\}$.

Teorema 1.2.5. *Para todo conjunto S temos que $\emptyset \subset S$ e $S \subset S$.*

Demonstração. Se $\emptyset \not\subset S$ então existe um elemento de $\emptyset$ que não pertence a S. Isso significa que $\emptyset$ tem elemento. Contradição. Portanto $\emptyset \subset S$.

Todo elemento de S pertence a S. Assim $S \subset S$. □

O próximo exercício diz que se quisermos provar que dois conjuntos são iguais, basta provar que um é subconjunto do outro.

Exercício 1.2.6. *Mostre que se A, B são conjuntos tais que $A \subset B$ e $B \subset A$ então $A = B$.*

Solução: Por contradição, assuma $A \neq B$. Isso significa que os elementos de A e B não são idênticos. Portanto existe um elemento de A que não está em B, contrariando a hipótese $A \subset B$, ou existe um elemento de B que não está em A, contrariando a hipótese $B \subset A$. Contradição. Assim $A = B$. □

Conjuntos finitos e infinitos

Definição 1.2.7. *Um conjunto A formado por n elementos, onde n é um número inteiro positivo, é chamado de conjunto finito. Dizemos que n é a sua cardinalidade e denotamos isso por $\#A = n$. Um conjunto que possui mais do que m elementos, onde m é qualquer número inteiro positivo é chamado de conjunto infinito.*

Exemplos:

• $\#\{a, e, i, o, u\} = 5$.

• $\mathbb{N}$ possui mais do que $1, 2, 3, 4, 5, \ldots$ elementos, ou seja, ele possui mais do que qualquer quantidade finita de elementos. Portanto $\mathbb{N}$ é infinito.

Conjunto das partes

Definição 1.2.8. *Seja S um conjunto. Definimos o conjunto das partes de S, que será denotado por $\mathcal{P}(S)$, o conjunto cujos elemento são os subconjuntos de S. Isto é, $\mathcal{P}(S) = \{A \mid A \subset S\}$.*

Exercício 1.2.9. *Calcule $\mathcal{P}(\{1, 2, 3\})$.*

Solução: Já sabemos que $\emptyset$ e $\{1, 2, 3\}$ são subconjuntos de $\{1, 2, 3\}$. Mas também existem os subconjuntos com um único elemento de $\{1, 2, 3\}$: $\{1\}$, $\{2\}$, $\{3\}$. E os subconjuntos com dois elementos de S: $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$. Assim $\mathcal{P}(\{1, 2, 3\}) = \{\emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{1, 2\},\ \{1, 3\},\ \{2, 3\},\ \{1, 2, 3\}\}$.

Exercício 1.2.10. *Calcule $\mathcal{P}(\emptyset)$, $\mathcal{P}(\mathcal{P}(\emptyset))$ e $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$.*

Solução:

• $\mathcal{P}(\emptyset)$ é o conjunto formado por todos os subconjuntos de $\emptyset$. O único subconjunto de vazio é ele mesmo entao $\mathcal{P}(\emptyset) = \{\emptyset\}$.

• Agora $\mathcal{P}(\emptyset)$ tem um elemento então $\mathcal{P}(\mathcal{P}(\emptyset))$ é formado pelo vazio e pelo conjunto contendo o único elemento de $\mathcal{P}(\emptyset)$, i.e., $\mathcal{P}(\mathcal{P}(\emptyset)) = \mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$.

• Portanto $\mathcal{P}(\mathcal{P}(\emptyset))$ tem dois elementos: $\emptyset$ e $\{\emptyset\}$. Vou chamá-los de a e b, respectivamente. Assim

$$\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) = \mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\} = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}\ .$$

Definição 1.2.11. *Sejam A, B conjuntos.*

- *A união de A e B, denotada por $A \cup B$, é o conjunto formado pelos elementos que estão em A* ***ou*** *em B (ou seja em um dos dois).*

  Exemplo*:* $\{1,3,5\} \cup \{1,2,3\} = \{1,2,3,5\}$.

- *A interseção dos conjuntos A e B, denotada por $A \cap B$, é conjunto formado pelos elementos que estão em A* ***e*** *em B (ao mesmo tempo). Além disso, se $A \cap B = \emptyset$ dizemos que A, B são conjuntos* ***disjuntos****.*

  Exemplo*:* $\{1,3,5\} \cap \{1,2,3\} = \{1,3\}$.

- *A diferença entre A e B, denotada por $A \setminus B$, é o conjunto formado pelos elementos de A que não estão em B. Além disso, se $A \subset B$ então o complemento de A com respeito a B, denotado por A^c, é o conjunto $A^c = B \setminus A$.*

  Exemplos*:* $\{1,3,5\} \setminus \{1,2,3\} = \{5\}$. *O complemento de* $\{1\}$ *com respeito a* $\{1,3,5\}$ *é* $\{1\}^c = \{3,5\}$.

Exercício 1.2.12. *Mostre que se A, B são conjuntos disjuntos então $A \setminus B = A$.*

Solução: Para provar que $A \setminus B = A$ devemos mostrar que $A \setminus B \subset A$ e $A \subset A \setminus B$.

Seja $x \in A \setminus B$. Portanto $x \in A$ e $x \notin B$. Assim provamos que todo $x \in A \setminus B$ também pertence a A, ou seja, $A \setminus B \subset A$.

Seja $x \in A$. Como $A \cap B = \emptyset$, pois A, B são disjuntos, então $x \notin B$. Portanto $x \in A \setminus B$. Assim provamos que todo $x \in A$ também pertence a $A \setminus B$, ou seja, $A \subset A \setminus B$.□

Observação 1.2.13. *Na solução do exercício anterior vimos que para provar que $C \subset D$ temos que pegar um elemento $c \in C$ qualquer e mostrar que ele também está em D. Isso vai se repetir muitas vezes nos proximos exercícios.*

Exercício 1.2.14. *Sejam A, B, C conjuntos. Prove as seguintes afirmações.*

a) $A \subset A \cup B$.

b) $A \cap B \subset A$

$c)$ $A \setminus B \subset A$

$d)$ $A \cap B \subset A \cup B$

$e)$ $B \setminus (B \setminus A) \subset A \cap B$

$f)$ $A \cap (B \setminus A) = \emptyset$

$g)$ $A \cup (B \setminus A) = A \cup B$

$h)$ $A \cup (A \cap B) = A$

$i)$ $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$

$j)$ $C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$

$k)$ $(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$

$l)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$m)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Vamos fazer alguns itens desse exercício abaixo.

1.2.14.a) $A \subset A \cup B$.

Solução: Seja $a \in A$ então $a \in A$ ou $a \in B$. Mas isso garante que $a \in A \cup B$.
Mostramos que qualquer elemento de A também está em $A \cup B$. Portanto $A \subset A \cup B$. $\square$

1.2.14.f) $A \cap (B \setminus A) = \emptyset$.

Solução: Seja $a \in A \cap (B \setminus A)$ então $a \in A$ e $a \in B \setminus A$. Mas $B \setminus A$ significa que $a \in B$ e $a \notin A$, ou seja, $a \in A$ e $a \notin A$. Contradição. Meu único erro foi dizer que $a \in A \cap (B \setminus A)$. Portanto não existe nenhum elemento nessa interseção. $\square$

1.2.14.i) $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$

Solução: Temos que provar duas coisas:

$$C \setminus (A \cup B) \subset (C \setminus A) \cap (C \setminus B) \text{ e } (C \setminus A) \cap (C \setminus B) \subset C \setminus (A \cup B).$$

Primeira parte: $C \setminus (A \cup B) \subset (C \setminus A) \cap (C \setminus B)$

Seja $a \in C \setminus (A \cup B)$ então $a \in C$ e $a \notin A \cup B$.
Portanto ($a \in C$ e $a \notin A$) e ($a \in C$ e $a \notin B$).
Assim $a \in C \setminus A$ e $a \in C \setminus B$. Portanto $a \in (C \setminus A) \cap (C \setminus B)$.

Segunda parte: $(C \setminus A) \cap (C \setminus B) \subset C \setminus (A \cup B)$.

Seja $a \in (C \setminus A) \cap (C \setminus B)$.
Portanto $a \in C \setminus A$ e $a \in C \setminus B$.
Isso significa que ($a \in C$ e $a \notin A$) e ($a \in C$ e $a \notin B$).
Assim $a \in C$ e $a \notin A \cup B$, isto é, $a \in C \setminus (A \cup B)$. □

1.2.14.*l*) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Solução: Primeira parte: $A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$

Seja $a \in A \cup (B \cap C)$. Por contradição, se $a \notin (A \cup B) \cap (A \cup C)$ então

- ou $a \notin (A \cup B)$, que significa que $a \notin A$ e $a \notin B$. Mas isso implica que $a \notin A$ e $a \notin B \cap C$. Isto é, $a \notin A \cup (B \cap C)$. Contradição.
- ou $a \notin (A \cup C)$, que significa que $a \notin A$ e $a \notin C$. Mas isso implica que $a \notin A$ e $a \notin B \cap C$. Isto é, $a \notin A \cup (B \cap C)$. Contradição.

Para evitar a contradição, $a \in (A \cup B) \cap (A \cup C)$.
Isso prova que $A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$.

Segunda parte: $(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$

Seja $a \in (A \cup B) \cap (A \cup C)$. Então $a \in A \cup B$ e $a \in A \cup C$.
Portanto $a \in A$ ou, caso contrário, $a \in B$ e $a \in C$. Isto é, $a \in A \cup (B \cap C)$.

Isso prova que $(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$. $\square$

Exercício 1.2.15. *Sejam A, B, C, D conjuntos. Para cada uma das seguintes afirmações indique a sua hipótese e a sua tese. Por fim prove a afirmação.*
OBS: A seta ($\Rightarrow$) significa então e as duas setas ($\Leftrightarrow$) significam se e somente se.

a) $A \subset B$ *e* $B \subset C \Rightarrow A \subset C$

b) $A \subset (C \setminus B) \Rightarrow A \cap B = \emptyset$

c) $A \cup B = C$ *e* $A \cap B = \emptyset \Rightarrow B = C \setminus A$

d) $A \subset C$ *e* $B \subset D \Rightarrow A \cup B \subset C \cup D$

e) $A \cap C = A \cap B$ *e* $A \cup C = A \cup B \Rightarrow B = C$

f) $\mathcal{P}(A) = \mathcal{P}(B) \Rightarrow A = B$

g) $A \subset B \Rightarrow A \cap (C \setminus B) = \emptyset$

h) $A \cap C = \emptyset \Rightarrow A \cap (B \cup C) = A \cap B$

i) $A \subset B \Rightarrow A = B \setminus (B \setminus A)$

j) $A \cup B \subset A \cap B \Rightarrow A = B.$

k) $A \subset \emptyset \Leftrightarrow A = \emptyset$

l) $A \subset B \Leftrightarrow A \cup B = B$

m) $A \subset B \Leftrightarrow \mathcal{P}(A) \subset \mathcal{P}(B)$

n) $A \subset B$ *e* $B \subset C \Leftrightarrow A \cup B \subset C \cap B$

o) $(A \setminus B) \subset B \Leftrightarrow A \setminus B = \emptyset$

p) $A \cup B \neq \emptyset \Leftrightarrow A \neq \emptyset$ *ou* $B \neq \emptyset$

Vamos fazer alguns itens desse exercício abaixo.

1.2.15a) $A \subset B$ e $B \subset C \Rightarrow A \subset C$

Solução: A hipótese é $\underline{A \subset B \text{ e } B \subset C}$ e a tese é $\underline{A \subset C}$.
Quero provar a tese. Assim seja $a \in A$, temos que mostrar que $a \in C$.
Como $A \subset B$, os elementos de A estão em B. Portanto $a \in B$.
Agora $B \subset C$ então os elementos de B estão em C, incluindo este a. □

1.2.15.m) $A \subset B \Leftrightarrow \mathcal{P}(A) \subset \mathcal{P}(B)$

Solução: Temos que provar duas coisas:

$$A \subset B \Rightarrow \mathcal{P}(A) \subset \mathcal{P}(B) \text{ e } \mathcal{P}(A) \subset \mathcal{P}(B) \Rightarrow A \subset B.$$

Primeira parte: $A \subset B \Rightarrow \mathcal{P}(A) \subset \mathcal{P}(B)$

A hipótese aqui é $\underline{A \subset B}$ e a tese é $\underline{\mathcal{P}(A) \subset \mathcal{P}(B)}$.
Seja $C \in \mathcal{P}(A)$, ou seja, C é subconjunto de A.
Por hipótese, A é subconjunto de B. Portanto pelo 1.2.15a), provado acima, $C \subset B$.
Isto é, $C \in \mathcal{P}(B)$.

Segunda parte: $\mathcal{P}(A) \subset \mathcal{P}(B) \Rightarrow A \subset B$.

A hipótese aqui é $\underline{\mathcal{P}(A) \subset \mathcal{P}(B)}$ e a tese é $\underline{A \subset B}$.
Seja $a \in A$ então $\{a\} \in \mathcal{P}(A)$.
Por hipótese, $\mathcal{P}(A) \subset \mathcal{P}(B)$. Assim $\{a\} \in \mathcal{P}(B)$, isto é, $a \in B$. □

Princípio da Inclusão-Exclusão com 2 conjuntos

Teorema 1.2.16. *Sejam A e B conjuntos finitos. Então $\#(A \cup B) = \#A + \#B - \#(A \cap B)$.*

Demonstração. Quando contamos os elementos de A e depois os de B obtemos $\#A+\#B$, mas estamos contando os elementos de $A \cap B$ duas vezes. Assim temos que subtrair uma vez $\#(A \cap B)$ para obter a $\#(A \cup B)$. □

Exemplo: Sejam $A = \{1, 2, 3\}$ e $B = \{1, 3, 4\}$.

Note que $\#(A) = \#(B) = 3$, $\#(A \cup B) = \#\{1, 2, 3, 4\} = 4$ e $\#(A \cap B) = 2$.

Assim $\#A + \#B - \#(A \cap B) = 3 + 3 - 2 = 4 = \#(A \cup B)$.

Definição 1.2.17. *A união de uma coleção de conjuntos é o conjunto que contém os elementos que são membros de pelo menos um dos conjuntos da coleção.*

Notação: $\bigcup_{i=1}^{n} A_i = A_1 \cup \ldots \cup A_n$ *e* $\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup \ldots$

A interseção de uma coleção de conjuntos é o conjunto que contém os elementos que são membros de todos os conjuntos da coleção.

Notação: $\bigcap_{i=1}^{n} A_i = A_1 \cap \ldots \cap A_n$ *e* $\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap \ldots$

Exercício 1.2.18. *Seja* $A_i = \{1, 2, \ldots, i\}$, $B_i = \{i + 1, i + 2, \ldots\}$. *Calcule:*

a) $\bigcap_{i=1}^{3} A_i$ *b)* $\bigcup_{i=1}^{3} A_i$ *c)* $\bigcap_{i=1}^{3} B_i$ *d)* $\bigcup_{i=1}^{3} B_i$

e) $\bigcap_{i=1}^{\infty} A_i$ *f)* $\bigcup_{i=1}^{\infty} A_i$ *g)* $\bigcap_{i=1}^{\infty} B_i$ *h)* $\bigcup_{i=1}^{\infty} B_i$

Vamos fazer alguns itens desse exercício abaixo.

1.2.18.*g*) Temos que achar os elementos que pertencem a todos os B_i simultaneamente.

Temos que $B_1 = \{2, 3, 4, 5, \ldots\}$, $B_2 = \{3, 4, 5, 6 \ldots\}$, $B_3 = \{4, 5, 6, 7, \ldots\}$, $\ldots$

Agora observe que o $2 \notin B_2$, $3 \notin B_3$, $4 \notin B_4$, $\ldots$ Portanto $2 \notin \bigcap_{i=1}^{\infty} B_i$, $3 \notin \bigcap_{i=1}^{\infty} B_i$, $4 \notin \bigcap_{i=1}^{\infty} B_i$, $\ldots$

Portanto $\bigcap_{i=1}^{\infty} B_i = \emptyset$.

1.2.18.*h*) Temos que achar os elementos que pertencem a pelo menos um dos B_i.

Note que os elementos de $B_2, B_3, B_4, \ldots$ são elementos do B_1.

Então os elementos que pertecem a pelo menos um dos B_i são os elementos do B_1, isto é, $\bigcup_{i=1}^{\infty} B_i = B_1$.

Exercício 1.2.19. *Sejam $A_1, \ldots, A_n$ conjuntos 2 a 2 disjuntos, i.e., $A_i \cap A_j = \emptyset$ quando $i \neq j$. Mostre que se $A_1, \ldots, A_n$ são conjuntos finitos então $\#(A_1 \cup \ldots \cup A_n) = \#A_1 + \ldots + \#A_n$.*

Solução: Chame $A_1 \cup \ldots \cup A_{n-1}$ de B. Então $A_1 \cup \ldots \cup A_n = B \cup A_n$.

Se $x \in B \cap A_n$ então x pertence a algum dos A_i com $1 \leq i \leq n-1$ e $x \in A_n$.

Isto é $x \in A_i \cap A_n$, o que contraria a hipótese. Então $B \cap A_n = \emptyset$.

Pelo princípio da inclusão-exclusão: $\#(B \cup A_n) = \#B + \#A_n - \#(B \cap A_n) = \#B + \#A_n$.

Acabamos de provar que $\#(A_1 \cup \ldots \cup A_n) = \#(A_1 \cup \ldots \cup A_{n-1}) + \#A_n$.

Repetindo o argumento, obtemos $\#(A_1 \cup \ldots \cup A_{n-1}) = \#(A_1 \cup \ldots \cup A_{n-2}) + \#A_{n-1}$.

Assim $\#(A_1 \cup \ldots \cup A_n) = \#(A_1 \cup \ldots \cup A_{n-2}) + \#A_{n-1} + \#A_n$.

Repetindo mais $n-3$ vezes o argumento, temos $\#(A_1 \cup \ldots \cup A_n) = \#A_1 + \ldots + \#A_{n-1} + \#A_n$. □

Exercício 1.2.20. *Sejam $A_1, \ldots, A_n$ conjuntos tais que $A_i \subset A_{i+1}$ para todo $i = 1, \ldots, n$. Mostre que $\bigcup_{i=1}^{n} A_i = A_n$ e $\bigcap_{i=1}^{n} A_i = A_1$.*

1.3 Produto Cartesiano

Produto cartesiano

Definição 1.3.1. *Uma $n-$upla ordenada $(a_1, a_2, \ldots, a_n)$ é uma coleção ordenada com n elementos que tem a_1 como primeiro elemento, a_2 como segundo e etc. Dizemos que duas $n-$uplas são iguais $(a_1, \ldots, a_n) = (b_1, \ldots, b_n)$ se e somente se $a_1 = b_1, \ldots a_n = b_n$.*

Definição 1.3.2. *O produto cartesiano dos conjuntos A e B, denotado por $A \times B$, é o conjunto de todos os pares ordenados (a, b) tais que $a \in A$ e $b \in B$. Isto é, $A \times B = \{(a, b),\ a \in A \text{ e } b \in B\}$. Dizemos que o a ocupa a primeira coordenada de (a, b), enquanto que o b ocupa a segunda.*

Exemplo: $\{1, 2\} \times \{a, b, c\} = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$

Definição 1.3.3. *O produto cartesiano dos conjuntos $A_1, \ldots, A_n$, denotado por $A_1 \times \ldots \times A_n$, é o conjunto de todos as $n-$uplas ordenadas $(a_1, \ldots, a_n)$ tais que $a_1 \in A_1, \ldots, a_n \in A_n$.*
Isto é, $A_1 \times \ldots \times A_n = \{(a_1, \ldots, a_n),\ a_1 \in A_1, \ldots, a_n \in A_n\}$.

Exercício 1.3.4. *Dê um exemplo onde $A \times B \neq B \times A$.*

Observação 1.3.5. *Existe uma maneira de definir um par ordenado através de conjuntos. Definimos $(a, b) = \{\{a\}, \{a, b\}\}$. Com essa definição temos $(a, b) = (c, d)$ se e somente se $a = c$ e $b = d$. Veja o próximo exercício.*

Exercício 1.3.6. *Mostre que $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ se e somente se $a = c$ e $b = d$.*

Solução: É claro que se $a = c$ e $b = d$ então $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. Falta provar a outra direção.

Suponha que $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ e vamos provar que $a = c$ e $b = d$.
Vou dividir a demonstração em dois casos: $a = b$ e $a \neq b$.

Primeiro caso: $a = b$
Se $a = b$ então $\{a, b\} = \{a\}$. Assim $\{\{a\}, \{a, b\}\} = \{\{a\}\} = \{\{c\}, \{c, d\}\}$.
Como $\{\{a\}\}$ tem somente 1 elemento então $\{c\} = \{c, d\}$. Isso implica que $c = d$.
Além disso, $\{\{a\}\} = \{\{c\}\}$, ou seja, $a = c = d$. Portanto $a = c$ e $b = a = d$.

Segundo caso: $a \neq b$
Se $a \neq b$ então $\{a, b\} \neq \{a\}$ e a $\#\{\{a\}, \{a, b\}\} = 2$.
Como $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ então $\#\{\{c\}, \{c, d\}\} = 2$.
Assim $\{c, d\} \neq \{c\}$. Portanto $c \neq d$.
Como $\{a\} \neq \{c, d\}$, pois $\#\{c, d\} = 2$, mas $\{a\}$ é igual a algum dos elementos de $\{\{c\}, \{c, d\}\}$ então $\{a\} = \{c\}$.
Consequentemente, $\{a, b\}$ deve ser igual ao outro elemento, isto é, $\{a, b\} = \{c, d\}$.
Como $\{a\} = \{c\}$ e $\{a, b\} = \{c, d\}$ então $a = c$ e $b = d$. □

Exercício 1.3.7. *Utilizando a definição $(a, b) = \{\{a\}, \{a, b\}\}$, defina $(a, b, c) = (a, (b, c))$. Escreva (a, b, c) utilizando conjuntos.*

Observação 1.3.8. *Quando não temos certeza se uma certa afirmação é verdadeira buscamos um exemplo que a refute. Esse exemplo é chamado de contra-exemplo para a afirmação.*
Por exemplo, se eu afirmo que todos os alunos tem cabelos escuros. Mas um dos alunos for loiro então ele é um contra-exemplo para a minha afirmação. Ele refuta a minha afirmação. Minha afirmação não pode ser provada porque ela é falsa.
No seguinte exercício ele pede para você demonstrar ou dar um contra-exemplo para as afirmações.

Exercício 1.3.9. *Sejam A, B, C, D conjuntos. Prove ou dê contra-exemplo.*

a) $A \subset B$ *e* $C \subset D \Rightarrow A \times C \subset B \times D$

b) $A \neq \emptyset$ *e* $A \times B = A \times C \Rightarrow B = C$

c) $A \times (B \cup C) = (A \times B) \cup (A \times C)$

d) $A \times (B \cap C) = (A \times B) \cap (A \times C)$

e) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$

f) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$

g) $(A \times B) \cap ((C \setminus A) \times B) = \emptyset$

h) $A \cup (B \times C) = (A \cup B) \times (A \cup C)$

i) $A \cap (B \times C) = (A \cap B) \times (A \cap C)$

A seguir vamos resolver alguns itens do exercício 1.3.9.

1.3.9.a) $A \subset B$ e $C \subset D \Rightarrow A \times C \subset B \times D$
Seja $(a, c) \in A \times C$. Pela definição do produto cartesiano, isso significa que $a \in A$ e $c \in C$.
Mas $A \subset B$ e $C \subset D$ então $a \in B$ e $c \in D$, ou seja, $(a, c) \in B \times D$.
Isso prova que $A \times C \subset B \times D$.□

1.3.9.b) $A \neq \emptyset$ e $A \times B = A \times C \Rightarrow B = C$
Como $A \neq \emptyset$, escolha um $a \in A$.

Se $B \neq C$ então existe $d \in B \setminus C$ ou $d \in C \setminus B$.

Se $d \in B \setminus C$ então $(a, d) \in A \times B$ e $(a, d) \notin A \times C$. Portanto $A \times B \neq A \times C$. Contradição.

Se $d \in C \setminus B$ então $(a, d) \in A \times C$ e $(a, d) \notin A \times B$. Portanto $A \times B \neq A \times C$. Contradição.

Para evitar a contradição, $B = C$.□

1.3.9.h) $A \cup (B \times C) = (A \cup B) \times (A \cup C)$

Essa igualdade é estranha. Do lado direito todos os elementos do conjunto são pares ordenados e do lado esquerdo os elementos de A podem não ser.

Contra-exemplo:

Seja $A = \{1\}$ e $B = C = \{2\}$

Por um lado, $A \cup (B \times C) = \{1, (2, 2)\}$.

Por outro lado, $(A \cup B) \times (A \cup C) = \{1, 2\} \times \{1, 2\} = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$.

Claramente esses dois conjuntos não são iguais. Portanto a afirmação 1.3.8.h) é falsa. □

Teorema 1.3.10. *Sejam A, B conjuntos finitos. Então $\#(A \times B) = \#A.\#B$*

Demonstração. Como A e B são conjuntos finitos digamos que suas cardinalidades sejam n e m, respectivamente.

Não sabemos como são os elementos de A e nem de B, mas podemos escrevê-los assim $A = \{a_1, \ldots, a_n\}$ e $B = \{b_1, \ldots, b_m\}$ (Estamos apenas renomeando os elementos).

Então $A \times B = \{(a_1, b_1), \ldots, (a_1, b_m), (a_2, b_1), \ldots, (a_2, b_m), \ldots, (a_n, b_1), \ldots, (a_n, b_m)\}$.

Note que existem

- m pares em $A \times B$ com primeira coordenada a_1,
- m pares em $A \times B$ com primeira coordenada a_2,

$\vdots$

- m pares em $A \times B$ com primeira coordenada a_n.

Portanto $\#(A \times B) = n.m = \#A.\#B$. □

Exercício 1.3.11. *Sejam A, B, C conjuntos. Adaptando a demonstração acima mostre que*

$$\#(A \times B \times C) = \#A.\#B.\#C.$$

Em geral, o mesmo ocorre com n conjuntos. Se $A_1, \ldots, A_n$ *são conjuntos finitos então*

$$\#(A_1 \times A_2 \times \ldots \times A_n) = \#A_1.\#A_2 \ldots \#A_n.$$

1.4 Paradoxo de Russell (Curiosidade)

Estamos trabalhando com conjuntos de maneira ingênua. Russell encontrou uma contradição considerando uma propriedade que o suposto "conjunto de todos os conjuntos" tem. Vejamos a contradição.

Note que o conjunto de todos os conjuntos tem a propriedade estranha de ser elemento de si mesmo (pois supostamente é um conjunto). Defina S como o conjunto cujos elementos são os conjuntos que não possuem essa propriedade estranha, i.e., $S = \{x \mid x \notin x\}$.

Veja a contradição:

- Se $S \in S$ então pela definição de S teríamos $S \notin S$. Contradição!
- Agora, se $S \notin S$ então pela definição de S teríamos que $S \in S$. Contradição!

Para evitar essa contradição dizemos que S não pode ser um conjunto. A pergunta importante é: O que pode ser um conjunto? Para respondê-la devemos estudar a teoria não ingênua de conjuntos.

1.5 Funções

Podemos deixar um borracha cair de uma certa altura e medir com um cronômetro o tempo de queda. Deixando a borracha cair de diversas alturas você obterá tempos distintos, ou seja, o tempo de queda depende da altura. Em português podemos dizer isso de outra maneira, o tempo está em função da altura. Em matemática simplesmente trocamos o verbo e dizemos que o tempo é uma função da altura.

Das duas quantidades, tempo e altura, você tem controle sobre a última. Você pode escolher as alturas de onde a borracha pode cair e medir os tempos correspondentes. Lembre-se que um sinônimo para controle é domínio.

Definição 1.5.1. *Sejam A, B conjuntos não vazios. Uma função de A para B determina para cada elemento de A um único elemento em B. Se f é uma função de A para B escrevemos $f : A \to B$.*

Exemplo: *tempo* : {alturas} $\to$ {tempos}.
A função "tempo" (descrita acima) fornece para cada altura o seu tempo de queda.

Definição 1.5.2. *Se b é o único elemento de B correspondente ao elemento $a \in A$ pela f então escrevemos $b = f(a)$. Esse b é chamado imagem de a pela f. O conjunto A é chamado de domínio da função f e o B de contra-domínio. O conjunto $\{f(a), a \in A\}$ que é formado pelas imagens de todos os elementos de A pela f é chamado de Imagem da f. Ele será denotado por* $\mathrm{Im}(f)$ *ou $f(A)$. Preste atenção na diferença entre $f(a)$ (elemento de B) e $f(A)$ (subconjunto de B).*

Exemplos: $A = \{\text{André, Carlos, Antônio}\}$, $B = \{1, 2, \ldots, 100\}$, $C = \{\text{Uberlândia, Taubaté, Rio}\}$

- Idade : $A \to B$ é uma função determina para cada pessoa de A uma idade em B.
  Idade(André) = 18, Idade(Carlos) = 23, Idade(Antônio) = 75.
- Cidade : $A \to C$ é uma função determina para cada pessoa de A a cidade que vive em B.
  Cidade(André) = Uberlândia, Cidade(Carlos) = Taubaté, Cidade(Antônio) = Rio.
- As alturas de onde você pode deixar a borracha cair formam o domínio da função tempo descrita acima.
- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$

Funções Injetoras, Sobrejetoras e Bijetoras

Funções injetoras e sobrejetoras

Definição 1.5.3. *Seja $f : A \to B$ uma função. Dizemos que*

- *f é injetora (ou injeção) se elementos diferentes de A tem imagens diferentes em B.*
- *f é sobrejetora (ou sobrejeção) se todo elemento de B é imagem de algum elemento de A.*
- *f é bijetora (ou bijeção) se f é injetora e sobrejetora.*

Exemplos: *a*) A função $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x$, é bijetora.

- Vamos mostrar que ela é injetora primeiro.

  Tenho que mostrar: Se $x \neq y$ então $f(x) \neq f(y)$.

  A contrapositiva disso é: Se $f(x) = f(y)$ então $x = y$.

  Mas $2x = f(x) = f(y) = 2y$ implica $x = y$, ou seja, provamos que f é injetora.

- Agora para mostrar que f é sobrejetora, seja z um elemento qualquer do contra-domínio da f.

  Temos que encontrar um elemento w do domínio tal que $f(w) = z$, ou seja, $2w = z$. Portanto o w que procuramos deve ser $\frac{z}{2}$.

  Como $\frac{z}{2}$ é um número real, ele pertence ao domínio da f.

  Achamos um w no domínio da f que satisfaz $f(w) = z$, ou seja, todo elemento do contra-domínio da f é imagem de algum elemento do domínio.

b) A função $g : \mathbb{N} \to \mathbb{N}$, $g(x) = 2x$, é somente injetora.

- A demonstração de que é injetora é idêntica a anterior.

- 1 não é imagem de ninguém do domínio da g, porque 1 é impar e todas as imagens pela g são números naturais pares. Portanto achamos um elemento do contra-domínio da g que não é imagem de nenhum elemento do domínio. Então g não é sobrejetora.

c) A função $h : \{\text{horas do relógio de ponteiro}\} \to \{\text{horas do relógio de ponteiro}\}$, $h(x) = 2x$, não é injetora e nem sobrejetora. Vejamos quais são as imagens da h.

$$h(1) = 2 \quad h(2) = 4 \quad h(3) = 6 \quad h(4) = 8 \quad h(5) = 10 \quad h(6) = 12$$
$$h(7) = 2 \quad h(8) = 4 \quad h(9) = 6 \quad h(10) = 8 \quad h(11) = 10 \quad h(12) = 12.$$

Como $h(1) = h(7)$ então h não é injetora. Como 1 pertence ao contra-domínio da h, mas não é imagem de nenhum elemento pela h então h não é sobrejetora.

Teorema 1.5.4. *Sejam A, B conjuntos finitos não vazios.*

a) Se existir uma injeção $f : A \to B$ então $\#A \leq \#B$.

b) Se existir uma sobrejeção $f : A \to B$ então $\#A \geq \#B$.

c) Se existir uma bijeção $f : A \to B$ então $\#A = \#B$.

Demonstração. *a)* Seja $f : A \to B$ uma injeção.

Como A é um conjunto finito podemos dizer que possui n elementos e escrevê-lo como

$$A = \{a_1, \ldots, a_n\}.$$

Como elementos distintos de A tem imagens distintas em B pela f, pois f é injetora, então

$$\#\{f(a_1), f(a_2), \ldots, f(a_n)\} = n.$$

Mas $\{f(a_1), f(a_2), \ldots, f(a_n)\} \subset B$, portanto $n \leq \#B$. Isto é, $\#A \leq \#B$.

b) Seja $f : A \to B$ uma sobrejeção.

Para cada elemento $b \in B$, escolho um único elemento $a \in A$ que corresponde a ele pela f, isto é, $f(a) = b$. Note que pode haver mais de um elemento caso f não seja injetora, mas existe pelo menos um pois f é sobrejetora.

Seja $g : B \to A$ a função definida por essa escolha. Vou provar que g é injetora.

Sejam $b_1, b_2 \in B$ tais que $g(b_1) = g(b_2)$. Note que $g(b_1)$ foi escolhido como um elemento de A que é levado em b_1 pela f, isto é, $f(g(b_1)) = b_1$. O mesmo ocorre com o b_2, $f(g(b_2)) = b_2$.

Como $g(b_1) = g(b_2)$ então $f(g(b_1)) = f(g(b_2))$. Assim $b_1 = b_2$.

Acabamos de provar que se $g(b_1) = g(b_2)$ então $b_1 = b_2$. A sua afirmação contrapositiva é se $b_1 \neq b_2$ então $g(b_1) \neq g(b_2)$, ou seja, g é injetora.

Finalmente pelo item *a)* desse teorema, como $g : B \to A$ é injetora, $\#B \leq \#A$.

c) Se $f : A \to B$ uma bijeção. Como f é injetora então $\#A \leq \#B$. Como f é sobrejetora $\#A \geq \#B$. Portanto $\#A = \#B$. □

Esse último teorema, que vale para conjuntos finitos serve de inspiração a seguinte definição.

Definição 1.5.5. *Sejam A, B conjuntos não vazios (podem ser infinitos). Dizemos que*

- *a cardinalidade de A é menor ou igual a de B se existir uma injeção $f : A \to B$,*
- *a cardinalidade de A é maior ou igual a de B se existir uma sobrejeção $f : A \to B$,*
- *A e B têm a mesma cardinalidade se existir uma bijeção $f : A \to B$.*

Exemplo: $f : \mathbb{N} \to \{2, 4, 6, 8, \ldots\}$ definida por $f(x) = 2x$ é uma bijeção.
Portanto $\mathbb{N}$ e $\{2, 4, 6, 8, \ldots\}$ tem a mesma cardinalidade.
Note que $\{2, 4, 6, 8, \ldots\}$ não tem todos os elementos de $\mathbb{N}$, mas possuem a mesma cardinalidade.
O que você acha disso?

Exercício 1.5.6. *Seja A um conjunto finito não vazio. Mostre que*

a) Se $f : A \to A$ é injetora então $f : A \to A$ é sobrejetora.

b) Se $f : A \to A$ é sobrejetora então $f : A \to A$ é injetora.

Solução: Como A é um conjunto finito podemos dizer que possui n elementos e escrevê-lo como

$$A = \{a_1, \ldots, a_n\}.$$

a) Como f é injetora então $f(a_1), f(a_2), \ldots, f(a_n)$ são todos distintos.
Assim $\{f(a_1), f(a_2), \ldots, f(a_n)\} \subset A$ e ambos tem a mesma cardinalidade n, ou seja,

$$\{f(a_1), f(a_2), \ldots, f(a_n)\} = A = \{a_1, \ldots, a_n\}.$$

Isso prova que todo a_i é igual a algum $f(a_j)$. Portanto $f : A \to A$ é sobrejetora.

b) Suponha por contradição que f não seja injetora.
Assim $f(a_1), f(a_2), \ldots, f(a_n)$ não são todos distintos. Portanto $\#\{f(a_1), f(a_2), \ldots, f(a_n)\} < n$.
Agora, como todo a_i é igual a algum $f(a_j)$, pois f é sobrejetora, então

$$\{a_1, \ldots, a_n\} \subset \{f(a_1), f(a_2), \ldots, f(a_n)\}.$$

Mas é óbvio que $\{f(a_1), f(a_2), \ldots, f(a_n)\} \subset \{a_1, \ldots, a_n\}$, porque o contradomínio da f é o A.
Portanto

$$\{f(a_1), f(a_2), \ldots, f(a_n)\} = \{a_1, \ldots, a_n\}.$$

Isso mostra que a

$$n = \#\{a_1, \ldots, a_n\} = \#\{f(a_1), f(a_2), \ldots, f(a_n)\} < n.$$

Contradição. Então f deve ser injetora para evitar a contradição $\square$.

Esse exercício nos permite definir conjunto infinito de uma outra maneira. Compare com a definição 1.2.7.

Nova definição de conjunto infinito

Definição 1.5.7. *Seja A um conjunto não vazio. Dizemos que A é infinito se existir uma $f : A \to A$ que é injetora e não sobrejetora.*

Exemplo: $f : \mathbb{N} \to \mathbb{N}$ definida por $f(x) = 2x$ é uma injeção, mas não é sobrejeção. Portanto $\mathbb{N}$ é infinito.

Definição 1.5.8. *Sejam $f : A \to B$ e $g : C \to D$ funções. Se $f(A) \subset C$ então podemos formar a função que é a composição das duas $g \circ f : A \to D$, definida por $g \circ f(a) = g(f(a))$. A função $g \circ f$ é lida como g composta com a f.*

Exemplos: *a*) Considere as funções: $f : \mathbb{N} \to \mathbb{N}$, $g : \mathbb{N} \to \mathbb{R}$

$$f(x) = 2x \qquad g(x) = \sqrt{x}$$

Note que a imagem da f é formada por números naturais e o domínio da g é próprio conjunto dos naturais . Então a composição, $g \circ f : \mathbb{N} \to \mathbb{R}$, pode ser feita e vale $g \circ f(x) = \sqrt{2x}$.

Note que a f só diz o que devemos fazer com x quando $x \in \mathbb{N}$. A imagem da g não é formada apenas por naturais portanto não faz sentido compor $f(g(x)) = f(\sqrt{x})$, já que não sabemos quanto isso vale quando $\sqrt{x}$ não é natural.

b) Considere as funções: $f : \{1,2,3\} \to \{1,2,3\}$, $\quad g : \{1,2,3\} \to \{1,2,3\}$

$$f(1) = 2,\ f(2) = 1,\ f(3) = 3 \qquad g(1) = 1,\ g(2) = 3,\ g(3) = 2.$$

As imagens de $f \circ g : \{1,2,3\} \to \{1,2,3\}$ são $\quad f \circ g(1) = f(g(1)) = f(1) = 2,$

$$f \circ g(2) = f(g(2)) = f(3) = 3,$$
$$f \circ g(3) = f(g(3)) = f(2) = 1.$$

Teorema 1.5.9. *Sejam A, B conjuntos finitos não vazios. Seja C o conjunto de todas as funções de A em B. Então $\#C = (\#B)^{\#A}$.*
Esse resultado é o motivo de denotar o conjunto de todas as funções de A em B por B^A.

Demonstração. Como A é um conjunto finito podemos dizer que possui n elementos e escrevê-lo como $A = \{a_1, \ldots, a_n\}$.

Vamos definir uma função $H : C \to \overbrace{B \times \ldots \times B}^{n \text{ vezes}}$ da seguinte maneira.

Para cada $f : A \to B$ que pertence a C definimos $H(f) = (f(a_1), \ldots, f(a_n))$

(Estamos organizando as imagens da f em uma $n-$upla).

Vou provar que essa H é bijetora. Pelo item c) do teorema 1.5.4 temos que

$$\#C = \#\overbrace{B \times \ldots \times B}^{n \text{ vezes}}.$$

Entretanto já vimos no exercício 1.3.11 que $\#(\overbrace{B \times \ldots \times B}^{n \text{ vezes}}) = (\#B)^n = (\#B)^{\#A}$.

Primeira parte: H é injetora

Sejam $f : A \to B$ e $g : A \to B$ elementos de C. Suponha que $H(f) = H(g)$. Então $(f(a_1), \ldots, f(a_n)) = (g(a_1), \ldots, g(a_n))$, ou seja, as imagens da f e g coincidem em todos os elementos do domínio. Isto é, $f = g$. Portanto H é injetora.

Segunda parte: H é sobrejetora

Seja $(b_1, \ldots, b_n)$ um elemento qualquer de $(\overbrace{B \times \ldots \times B}^{n \text{ vezes}})$.

Preciso encontrar uma função $h : A \to B$ tal que

$$H(h) = (h(a_1), \ldots, h(a_n)) = (b_1, \ldots, b_n).$$

Podemos definir uma função $h : A \to B$ satisfazendo $h(a_1) = b_1, \ldots, h(a_n) = b_n$.

Portanto temos a h que queremos. □

Observação 1.5.10. *Sejam A, B conjuntos finitos não vazios.*

- *Se A e B são disjuntos então $\#(A \cup B) = \#A + \#B$*
- $\#(A \times B) = \#A.\#B$
- $\#\{f : A \to B,\ f \text{ é função}\} = (\#B)^{\#A}$.

Pergunta: Que operações podemos fazer com os conjuntos A, B para obter como resultado conjuntos cuja cardinalidade são $\#A - \#B$ ou $\dfrac{\#A}{\#B}$?

Exercício 1.5.11. *Para cada uma das funções abaixo, prove ou dê um contra-exemplo para as seguintes afirmações: (i) f é injetora (ii) f é sobrejetora*

a) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = ax + b$, *onde* $a, b \in \mathbb{R}$ *e* $a \neq 0$

b) $f : \mathbb{R} \to \mathbb{R} \setminus (-\infty, -1)$, *onde* $f(x) = x^2 - 1$

c) $f : \mathbb{N} \to \mathbb{N}$, $f(x) = 2x$

d) $f : (0, 1] \to [1, \infty)$, $f(x) = \dfrac{1}{x}$

e) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x - |x|$

f) $f : \mathbb{R} \setminus \{1\} \to \mathbb{R}$, $f(x) = \dfrac{1}{1-x}$

g) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \dfrac{1}{1+x^2}$

h) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \dfrac{-1}{2+|x|}$

i) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \sqrt{|x|}$

j) $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = (3x - 1)(2 - x)$

k) $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = \begin{cases} \dfrac{(x-1)}{2}, & \text{se } x \text{ é ímpar} \\ -\dfrac{x}{2}, & \text{se } x \text{ é par} \end{cases}$

l) $f : \mathbb{Z} \to \mathbb{N}$, $f(x) = x^2!$

$m)$ $f : \mathbb{N} \to \mathbb{N}$, $f(x) = \begin{cases} \frac{x}{2}\ , \ se\ x\ é\ par \\ 3x+1,\ se\ x\ é\ ímpar \end{cases}$

$n)$ $f : \mathbb{Z} \to \mathbb{N}$, $f(x) = x^2$

$o)$ $f : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, $f(x) = (x, x)$

$p)$ $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $f(x, y) = x + y + xy$

$q)$ $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $f(x, y) = x + |y|$

$r)$ $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $f(x, y) = x$

$s)$ $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, $f(x, y) = (3x - 1, x + y)$

$t)$ $f : \mathbb{Q} \times \mathbb{R} \to \mathbb{R}$, $f(x, y) = x + y$

$u)$ $f : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, $f(x) = (x, 0)$

$v)$ $f : \mathbb{R} \times \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, $f(x, y, z) = (x + y, x + z)$.

Vamos fazer alguns itens do exercício 1.5.11.

1.5.11$a)$ $f : \mathbb{R} \to \mathbb{R}$, $f(x) = ax + b$, onde $a, b \in \mathbb{R}$ e $a \neq 0$.

Primeira Parte: Verificar se f é injetora.

Quero mostrar que se $x \neq y$ então $f(x) \neq f(y)$.

Vou mostrar sua contrapositiva: Se $f(x) = f(y)$ então $x = y$.

Se $f(x) = f(y)$ então $ax + b = ay + b$.

Subtraindo b dos dois lados obtemos $ax = ay$. $(*)$

Como $a \neq 0$ (hipótese do exercício), existe a^{-1}.

Multiplicando a^{-1} dos dois lados de $(*)$ obtemos $x = y$. Portanto f é injetora.

Segunda Parte: Verificar se f é sobrejetora.

Seja z um elemento do contra-domínio da f.

Queremos achar x no domínio tal que $f(x) = z$, isto é, $ax + b = z$.

Assim $x = \dfrac{z - b}{a}$. Note que esse x é um número real, pois z, a, b são reais. $\square$

1.5.11s) $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, $f(x, y) = (3x - 1, x + y)$

Primeira Parte: Verificar se f é injetora.

Quero mostrar que se $(x, y) \neq (z, w)$ então $f(x, y) \neq f(z, w)$.

Vou mostrar sua contrapositiva: Se $f(x, y) = f(z, w)$ então $(x, y) = (z, w)$.

Se $f(x, y) = f(z, w)$ então $(3x - 1, x + y) = (3z - 1, z + w)$.

Assim $3x - 1 = 3z - 1$ e $x + y = z + w$.

A primeira equação implica $x = z$. Como $x = z$ então a segunda equação fica $x + y = x + w$.

Isso implica que $y = w$, ou seja, $(x, y) = (z, w)$. Portanto f é injetora.

Segunda Parte: Verificar se f é sobrejetora.

Seja (z, w) um elemento do contra-domínio da f.

Queremos achar (x, y) no domínio tal que $f(x, y) = (z, w)$.

Isso significa que $3x - 1 = z$ e $x + y = w$.

A primeira equação implica $x = \dfrac{z+1}{3}$. Portanto a segunda equação fica $\dfrac{z+1}{3} + y = w$.

Isso implica que $y = w - \dfrac{z+1}{3}$, ou seja, $f\left(\dfrac{z+1}{3}, w - \dfrac{z+1}{3}\right) = (z, w)$. Portanto f é sobrejetora.

Definição 1.5.12. *Seja $f : A \to B$ uma função. Dizemos que uma função $g : B \to A$ é*

- *uma inversa à esquerda da $f : A \to B$ se*

  $g \circ f : A \to A$ é a função identidade, i.e., $g(f(a)) = a$ para todo $a \in A$.

- *uma inversa à direita da $f : A \to B$ se*

  $f \circ g : B \to B$ é a função identidade, i.e., $f(g(b)) = b$ para todo $b \in B$.

- *a inversa da $f : A \to B$ se ela é inversa à esquerda e à direita da f ao mesmo tempo.*

  Notação: *Veremos no exercício 1.5.14 que se uma inversa (dos dois lados) da f existir então ela é única e será denotada por $f^{-1} : B \to A$. Note que a inversa da inversa é a própria função.*

Exemplos: a) Sejam $f : \mathbb{R} \to \mathbb{R}$ e $g : \mathbb{R} \to \mathbb{R}$ definidas por $f(x) = 2x$ e $g(x) = \dfrac{x}{2}$.

Note que $f \circ g(x) = f(g(x)) = f\left(\dfrac{x}{2}\right) = 2\dfrac{x}{2} = x$ e que $g \circ f(x) = g(f(x)) = g(2x) = \dfrac{2x}{2} = x$.

Assim f e g são inversas à esquerda e à direita uma da outra.

b) Sejam $f : \mathbb{R} \to [0, \infty[$ e $g : [0, \infty[\to \mathbb{R}$ definidas por $f(x) = x^2$ e $g(x) = \sqrt{x}$.
Note que $f \circ g(x) = f(g(x)) = f\left(\sqrt{x}\right) = (\sqrt{x})^2 = x$, já que $x \in [0, \infty[$.

Portanto g é a inversa à direita da f e f é a inversa à esquerda da g.

Agora note que $g \circ f(-1) = g(f(-1)) = g((-1)^2) = g(1) = \sqrt{1} = 1$, ou seja, $g \circ f(x)$ nem sempre vale x. Portanto g não é a inversa à esquerda da f e nem f é a inversa à direita de g.

Teorema 1.5.13. *Seja $f : A \to B$ uma função. Então*

a) f possui uma inversa à esquerda se e somente se f é injetora,

b) f possui uma inversa à direita se e somente se f é sobrejetora,

c) f possui uma inversa se e somente se f é bijetora.

Demonstração. Primeiro provaremos que se f é injetora ou sobrejetora então existirão as inversas à esquerda ou à direita, respectivamente.

Note que 1) $B = f(A) \cup B \setminus f(A)$,
2) Existe $z \in A$, pois $A \neq \emptyset$
3) Para cada $y \in f(A)$ existe $a \in A$ tal que $y = f(a)$.

Defina a função $g : B \to A$ da seguinte maneira:
Se $y \in f(A)$ escolha um único $a \in A$ tal que $y = f(a)$ e defina $g(y) = a$.
Se $y \in B \setminus f(A)$ defina $g(y) = z$.

Agora, note que se f é injetora então o único elemento de A que tem $f(x)$ como imagem é o próprio x. Então $g(f(x)) = x$ (Não existe outra escolha possível pro $g(f(x))$).
Isso prova que $g : B \to A$ é a inversa à esquerda de $f : A \to B$, quando f é injetora.

Se f é sobrejetora então $B = f(A)$. Assim para todo $y \in B$, $g(y)$ é igual a algum a satisfazendo $f(a) = y$. Juntando essas duas informações temos $f(g(y)) = f(a) = y$.
Isso prova que a g é a inversa da f à direita, quando f é sobrejetora.

Note que usamos a mesma g nos dois casos . Assim se f é injetora e sobrejetora então g é a inversa à esquerda e à direita da f ao mesmo tempo.

Tudo que fizemos até agora prova metade dos itens $a), b)$ e $c)$ do teorema.

Falta provar que se as respectivas inversas existem então f possui as respectivas propriedades.

Seja $h : B \to A$ uma inversa à esquerda da $f : A \to B$.

Se $f(a_1) = f(a_2)$ então $h(f(a_1)) = h(f(a_2))$. Mas $h(f(a_1)) = a_1$ e $h(f(a_2)) = a_2$.

Isso prova que f é injetora.

Seja $j : B \to A$ uma inversa à direita da $f : A \to B$.

Seja b qualquer elemento de $b \in B$, como $f(j(b)) = b$ então existe ao menos um elemento em A que corresponde ao b pela f: o elemento $j(b)$. Isso prova que f é sobrejetora.

Se $t : B \to A$ é uma inversa da $f : A \to B$ então f é inversa à esquerda e à direita. Pelo que acabamos de provar f é bijetora. □

Exercício 1.5.14. *Seja $f : A \to B$ é uma função bijetora. Mostre que existe somente uma inversa para f e que essa inversa também é bijetora.*

Solução: Se $g : B \to A$ e $h : B \to A$ são inversas (dos dois lados) da f então para todo $x \in B$ temos

$$g(x) = g(f \circ h(x))) = g(f(h(x))) = g \circ f(h(x)) = h(x).$$

Portanto g e h são iguais. Isto é, só existe uma.

Como f^{-1} também tem inversa que é a própria f então f^{-1} também é bijetora pelo item $c)$ do teorema 1.5.13. □

Exercício 1.5.15. *Sejam $f : A \to B$ e $g : B \to C$. Mostre que*

a) $g \circ f : A \to C$ é injetora se $f : A \to B$ e $g : B \to C$ forem injetoras.

b) $g \circ f : A \to C$ é sobrejetora se $f : A \to B$ e $g : B \to C$ forem sobrejetoras.

c) $g \circ f : A \to C$ é bijetora se $f : A \to B$ e $g : B \to C$ forem bijetoras.

Definição 1.5.16. *Seja $f : A \to B$ uma função e considere os subconjuntos $X \subset A$ e $Y \subset B$.*

- *Denote por $f(X)$ o subconjunto do contra-domínio da f formado por todas as imagens dos elementos de X, i.e., $f(X) = \{f(x), x \in X\}$. Esse conjunto será chamado de imagem do X pela f.*
- *Denote por $f^{-1}(Y)$ o subconjunto do domínio da f formado pelos elementos cujas imagens pertencem a Y, i.e., $f^{-1}(Y) = \{x \in A,\ f(x) \in Y\}$. Esse conjunto será chamado de pré-imagem do Y pela f.*

  AVISO: *Não confundir $f^{-1}(y)$ com $f^{-1}(\{y\})$. O primeiro só faz sentido se existir a função inversa da f para ser aplicada em y. Agora $f^{-1}(\{y\})$ sempre faz sentido. Ele é o conjunto formado pelo elementos do domínio cuja imagem é y.*

***Exemplos**: Seja $f : \{1, 2, 3\} \to \{4, 5\}$ defina por $f(1) = f(2) = 4$ e $f(3) = 5$.*
Então $f(\{1, 2\}) = \{4\}$ e $f^{-1}(\{4\}) = \{1, 2\}$.

Exercício 1.5.17. *Seja $f : A \to B$ um função. Sejam $X, Y \subset A$ e $Z, W \subset B$. Prove as seguintes proposições.*

a) $X \subset Y \Rightarrow f(X) \subset f(Y)$

b) $f(X \cup Y) = f(X) \cup f(Y)$

c) Se f é injetora então $f(X \cap Y) = f(X) \cap f(Y)$

d) Mostre uma f tal que $f(X \cap Y) \neq f(X) \cap f(Y)$

e) $Z \subset W \Rightarrow f^{-1}(Z) \subset f^{-1}(W)$

f) $f^{-1}(Z \cup W) = f^{-1}(Z) \cup f^{-1}(W)$

g) $f^{-1}(Z \cap W) = f^{-1}(Z) \cap f^{-1}(W)$

h) $X \subset f^{-1}(f(X))$

i) Se f é injetora então $X = f^{-1}(f(X))$

j) Mostre uma f tal que $X \neq f^{-1}(f(X))$

k) $f(f^{-1}(Z)) \subset Z$

l) Se f é sobrejetora então $f(f^{-1}(Z)) = Z$

m) Mostre uma f tal que $f(f^{-1}(Z)) \neq Z$

A seguir resolveremos alguns itens do exercício 1.5.17.

1.5.17.*a*) $X \subset Y \Rightarrow f(X) \subset f(Y)$

Nossa tese é $f(X) \subset f(Y)$. Seja $z \in f(X)$. Pela definição de $f(X)$, esse z é a imagem de algum elemento do conjunto X, i.e., $z = f(w)$, onde $w \in X$.

Mas w também pertence a Y, pois por hipótese $X \subset Y$, então z é a imagem de algum elemento do conjunto Y. Assim $z \in f(Y)$.

Provamos que todo elemento de $f(X)$ também é de $f(Y)$, ou seja, $f(X) \subset f(Y)$.

1.5.17.*h*) $X \subset f^{-1}(f(X))$.

Seja $w \in X$. A definição de pré-imagem de um conjunto A contido no contradomínio da f é o conjunto $f^{-1}(A)$ formado pelos elementos do domínio da f que caem dentro de A quando a f é aplicada neles.

Agora a imgem de w pela f cai dentro de $f(X)$ porque o w está em X.

Assim $w \in f^{-1}(f(X))$. Acabamos de provar que todo elemento de X também pertence a $f^{-1}(f(X))$, ou seja, $X \subset f^{-1}(f(X))$.

Exercício 1.5.18. *Sejam $f : A \to B$ e $g : B \to C$ funções. Seja $h = g \circ f : A \to C$.*
Prove que $h^{-1}(X) = f^{-1}(g^{-1}(X))$ para qualquer subconjunto $X \subset C$.

Capítulo 2

Conjuntos enumeráveis

Quase todos os resultados desse capítulo foram provados por um único matemático: Georg Cantor. Ele provou alguns dos resultados mais bonitos de toda a matemática. A maior surpresa que veremos nesse capítulo é que existem infinitos diferentes.

2.1 Conjuntos enumeráveis e não enumeráveis

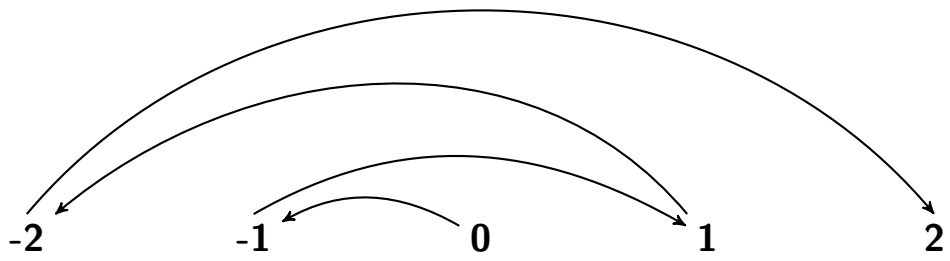
Definição 2.1.1. *Um conjunto A é dito enumerável se existir uma bijeção entre o conjunto dos números naturais ($\mathbb{N}$) e A. Em outras palavras, os elementos de A podem ser enumerados de acordo com essa bijeção.*

***Exemplo**: Se $f : \mathbb{N} \to A$ é uma bijeção então $A = \{f(1), f(2), f(3), \ldots\}$.*

Normalmente escrevemos $A = \{a_1, a_2, a_3, \ldots\}$, onde $a_i = f(i)$.

Exemplos: *a)* $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ é enumerável.

Considere o seguinte zig-zag partindo de 0 percorrendo todos os números inteiros. Note que ele põe todos os números inteiros em fila: 0 é o primeiro da fila, o -1 é o segundo, o 1 é o terceiro e etc.



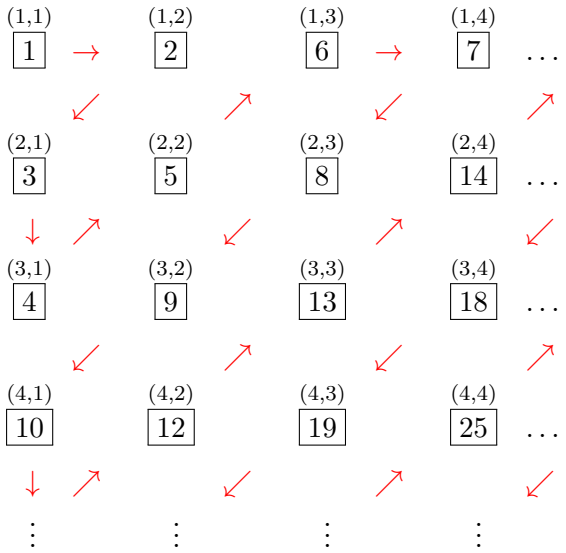
A partir desse zig-zag podemos definir a seguinte bijeção $f : \mathbb{N} \to \mathbb{Z}$

$f(1) = 0 \quad f(2) = -1 \quad f(3) = 1 \quad f(4) = -2 \quad f(5) = 2 \quad \ldots$

Isto mostra que $\mathbb{Z}$ é enumerável.

b) $\mathbb{N} \times \mathbb{N}$ é enumerável.

Podemos construir uma fila contendo todos os pares de $\mathbb{N} \times \mathbb{N}$ seguindo as setas vermelhas abaixo.



A posição do par na fila está escrita dentro da caixa. Isso nos permite construir a bijeção $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ associando a posição na fila ao seu par, isto é,

$$f(1) = (1,1),\ f(2) = (1,2),\ f(3) = (2,1),\ f(4) = (3,1),\ f(5) = (2,2),\ \ldots$$

c) $A \times B$ é enumerável se A, B forem enumeráveis.

Como A, B são enumeráveis podemos escrevê-los $A = \{a_1, a_2, a_3, \ldots\}$, $B = \{b_1, b_2, b_3, \ldots\}$.
Podemos repetir a fila acima substituindo (i, j) por (a_i, b_j).
Obtemos assim a bijeção $f : \mathbb{N} \to A \times B$ definida por

$$f(1) = (a_1, b_1),\ f(2) = (a_1, b_2),\ f(3) = (a_2, b_1),\ f(4) = (a_3, b_1),\ f(5) = (a_2, b_2),\ \ldots$$

d) Qualquer subconjunto infinito de um conjunto enumerável também é enumerável.

Seja $A = \{a_1, a_2, a_3, \ldots\}$ e $B \subset A$ um subconjunto infinito.

A seguinte função é uma bijeção $f : \mathbb{N} \to B$.

$f(1)$ = o elemento de A que está em B e que possui o menor índice.

$f(2)$ = o elemento de A que está em B e que possui o segundo menor índice.

$\vdots$

Note que é impossível que exista um elemento de A dentro de B com o menor e o segundo menor índice ao mesmo tempo, ou seja, $f(1) \neq f(2)$. Mas isso também ocorre com todos os outros números naturais, ou seja, $f(i) \neq f(j)$ quando $i \neq j$. Isso significa que ela é uma injeção.

Além disso, se $a_k \in B$ então existem apenas $k-1$ elementos em A com índice menor que k: $a_1, a_2, \ldots, a_{k-1}$. Em B existem menos ainda. Suponha que em B existam s elementos de A com índice menor que k então $f(s+1) = a_k$. Portanto f é sobrejetora.

O seguinte teorema é muito útil para obtermos mais exemplos de conjuntos enumeráveis.

Teorema 2.1.2. *Seja $f : A \to B$ uma sobrejeção e B um conjunto infinito. Se A é enumerável então B também é.*

Demonstração. Como $f : A \to B$ é uma sobrejeção então, pelo teorema 1.5.13, existe uma função $g : B \to A$ que é a inversa à direita da f, isto é, $f \circ g(x) = x$ para todo $x \in B$.

Note que f é a inversa à esquerda da g. Pelo teorema 1.5.13, g é injetora.

Como g é injetora e A é um conjunto infinito então $g(B)$ (o conjunto imagem de g) também é infinito.

Defina $m : B \to g(B)$, como $m(x) = g(x)$. Note que a única diferença entre m e g é que diminuímos o contra-domínio. Isso garante que todos os elementos do contra-domínio são imagem de alguém, ou seja, m é sobrejetora. Mas como m e g tem as mesma imagens, m também é injetora. Assim m é uma bijeção. Assim a sua inversa $m^{-1} : g(B) \to B$ também é uma bijeção pelo exercício 1.5.14.

Vimos que $g(B)$ é um subconjunto infinito de A e A é enumerável então, pelo exemplo c) acima, $g(B)$ é enumerável. Existe portanto uma bijeção $l : \mathbb{N} \to g(B)$.

Finalmente, a composição $m^{-1} \circ l : \mathbb{N} \to B$ é uma composição de bijeções e portanto também é uma bijeção pelo exercício 1.5.15. Assim provamos que B é enumerável.

□

Mais exemplos de conjuntos enumeráveis

e) $\mathbb{Q} = \left\{ \frac{m}{n},\ m \in \mathbb{Z} \text{ e } n \in \mathbb{N} \right\}$ também é enumerável.

Considere a função $h : \mathbb{Z} \times \mathbb{N} \to \mathbb{Q}$ definida por $h(m, n) = \frac{m}{n}$.

Note que h é uma sobrejeção, pois todo número racional pode ser escrito como $\frac{m}{n}$, onde $m \in \mathbb{Z}$ e $n \in \mathbb{N}$.

Pelos exemplos *a*) e *c*), $\mathbb{Z} \times \mathbb{N}$ é enumerável e note $\mathbb{Q}$ é um conjunto infinito. Portanto h é uma sobrejeção entre um conjunto enumerável $\mathbb{Z} \times \mathbb{N}$ e um infinito $\mathbb{Q}$. Pelo teorema 2.1.2, $\mathbb{Q}$ é enumerável.

f) Sejam $A_1, A_2, A_3, \ldots$ conjuntos enumeráveis então $\bigcup_{i=1}^{\infty} A_i$ também é enumerável.

Podemos escrever $A_1 = \{a_{11}, a_{12}, a_{13}, \ldots\}$

$A_2 = \{a_{21}, a_{22}, a_{23}, \ldots\}$

$\vdots$

Seja $h : \mathbb{N} \times \mathbb{N} \to \bigcup_{i=1}^{\infty} A_i$ definida por $h(i, j) = a_{ij}$. Note que h é sobrejetora, pois qualquer elemento dessa união está descrito como a_{ij}.

Pelo exemplo *b*) acima, $\mathbb{N} \times \mathbb{N}$ é enumerável e claramente a união de conjuntos infinitos é infinito. Portanto h é uma sobrejeção entre um conjunto enumerável $\mathbb{N} \times \mathbb{N}$ e um infinito $\bigcup_{i=1}^{\infty} A_i$. Pelo teorema 2.1.2, $\bigcup_{i=1}^{\infty} A_i$ é enumerável.

Observação 2.1.3. *Note que se $A_n = A_{n+1} = A_{n+2} = \ldots$ no exemplo f) então $\bigcup_{i=1}^{\infty} A_i = \bigcup_{i=1}^{n} A_i$. Portanto uma união de uma quantidade finita de conjunto enumeráveis também é enumerável.*

Conjunto não enumerável

Teorema 2.1.4. *$\mathbb{R}$ não é enumerável.*

Demonstração. O exemplo *d*) acima diz que qualquer subconjunto infinito de um conjunto enumerável também é enumerável. Vou mostrar que o subconjunto $]0, 1[$ dos números reais não é enumerável, portanto $\mathbb{R}$ também não pode ser enumerável.

Vimos nos exemplos acima que se um conjunto é enumerável podemos construir uma fila (ou uma lista) contendo todos os elementos do conjunto.

A estratégia aqui é mostrar que qualquer lista de números de $]0,1[$ não contém todos os seus números, ou seja, ela é sempre incompleta. Portanto não existe uma lista contendo todos os números do intervalo $]0,1[$. Portanto $]0,1[$ não é enumerável.

Considere uma lista qualquer de números de $]0,1[$, por exemplo,

$$\begin{aligned} a_1 &= 0,3789\ldots \\ a_2 &= 0,2489\ldots \\ a_3 &= 0,1217\ldots \\ a_4 &= 0,0021\ldots \\ &\vdots \end{aligned}$$

Seja $b = 0, d_1 d_2 d_3 d_4 \ldots$, onde $d_i \in \{0, 1, \ldots, 9\}$ e satisfazendo

$$\begin{aligned} d_1 &\neq \text{primeiro dígito de } a_1 \\ d_2 &\neq \text{segundo dígito de } a_2 \\ d_3 &\neq \text{terceiro dígito de } a_3 \\ d_4 &\neq \text{quarto dígito de } a_4 \\ &\vdots \end{aligned}$$

Por exemplo, $b = 0,4522\ldots$.

Assim $b \neq a_1$ (pois os primeiros dígitos de b e a_1 são diferentes), $b \neq a_2$ (pois os segundos dígitos de b e a_2 são diferentes), $b \neq a_3$, $b \neq a_4$ e etc. Portanto b não está na lista. Essa lista é incompleta.

Essa argumento pode ser repetido em qualquer lista. Portanto qualquer lista de números de $]0,1[$ é incompleta. □

Observação 2.1.5. *Como não existe bijeção $f : \mathbb{N} \to \mathbb{R}$ então, pela definição 1.5.5, as cardinalidades de $\mathbb{R}$ e $\mathbb{N}$ são diferentes. Como $g : \mathbb{N} \to \mathbb{R}$, $g(x) = x$, é uma injeção então, pela definição 1.5.5, a cardinalidade de $\mathbb{N}$ é menor que a de $\mathbb{R}$. Isso mostra que o infinito dos reais e dos naturais são diferentes.*

Corolário 2.1.6. *$\mathbb{R} \setminus \mathbb{Q}$ também não é enumerável.*

Demonstração. Se $\mathbb{R} \setminus \mathbb{Q}$ fosse enumerável então $(\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q} = \mathbb{R}$ seria a união de dois conjuntos enumeráveis, pois $\mathbb{Q}$ é enumerável. Pela observação 2.1.3, $\mathbb{R}$ seria enumerável. Contradição.

Portanto $\mathbb{R} \setminus \mathbb{Q}$ não é enumerável. □

2.2 Teorema de Cantor

Você lembra do paradoxo de Russell? Nele nós contruímos um "conjunto" S e chegamos a uma contradição. Para resolver o paradoxo, os matemáticos disseram que aquele S não serve como conjunto e tiveram que construir uma teoria que explica o que pode e o que não pode ser conjunto.

Também mencionei o "conjunto" de todos os conjuntos. O teorema a seguir nos permite ver que o "conjunto" de todos os conjuntos também não pode ser um conjunto ou teríamos uma contradição.

Teorema de Cantor

Teorema 2.2.1. *Seja A um conjunto qualquer diferente de vazio. Não existe função $f : A \to \mathcal{P}(A)$ sobrejetora.*

Demonstração. Seja $f : A \to \mathcal{P}(A)$ uma função qualquer. Defina $B = \{x \in A,\ x \notin f(x)\}$.

Note que $B \subset A$, portanto $B \in \mathcal{P}(A)$.

Vamos mostrar que B não é imagem de nenhum elemento de A pela f.

Suponha que exista $y \in A$ tal que $f(y) = B$. Existem duas possibilidades:

1ª) $\underline{y \in B}$: Pela definição de B, $y \notin f(y) = B$. Contradição.

2ª) $\underline{y \notin B}$: Pela definição de B, $y \in f(y) = B$. Contradição

Portanto não existe $y \in A$ tal que $f(y) = B$, ou seja, f não é sobrejetora. □

O "conjunto" de todos os conjuntos não é um conjunto

Observação 2.2.2. *Seja M o "conjunto" de todos os conjuntos. Como os elementos do conjunto das partes de M também são conjuntos então $\mathcal{P}(M) \subset M$.*

Defina a função $F : M \to \mathcal{P}(M)$, $F(y) = \begin{cases} y, \text{ se } y \in \mathcal{P}(M) \\ \emptyset, \text{ se } y \in M \setminus \mathcal{P}(M). \end{cases}$

Note que essa F é sobrejetora, contrariando o teorema de Cantor.

Exercício 2.2.3. *Usando o teorema de Cantor e a definição 1.5.5, explique porque a cardinalidade de $\mathcal{P}(A)$ é maior que a de A.*

2.3 Teorema de Bernstein (Curiosidade)

Para conjuntos finitos A e B, se $\#A \leq \#B$ e $\#B \leq \#A$ então $\#A = \#B$.

Esse teorema também vale para conjuntos infinitos, como veremos no seguinte teorema.

Teorema de Bernstein

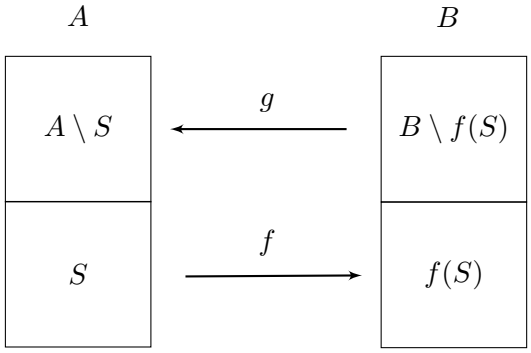
Teorema 2.3.1. *Se existirem injeções $f : A \to B$ e $g : B \to A$ então existe uma bijeção $h : A \to B$. Isso significa, pela definição 1.5.5, que se a cardinalidade de A é menor ou igual que a de B e vice-versa então A, B possuem a mesma cardinalidade.*

Demonstração. Lembre-se da seguinte notação. Se $X \subset A$ e $Y \subset B$ então $f(X) = \{f(x),\ x \in X\}$ e $g(Y) = \{g(y),\ y \in Y\}$. Portanto $f(X) \subset B$ e $g(Y) \subset A$.

Nessa demonstração nosso objetivo é achar um subconjunto S de A satisfazendo

$$g(B \setminus f(S)) = A \setminus S.$$

Em posse desse S teríamos a seguinte situação:



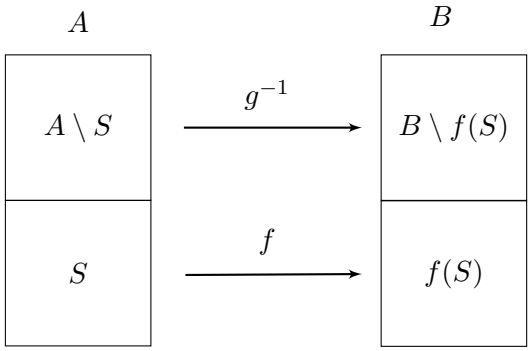
Note que $g : B \setminus f(S) \to A \setminus S$ é sobrejetora, pois $g(B \setminus f(S)) = A \setminus S$.

Lembre-se também que g é injetora por hipótese. Portanto existe a inversa $g^{-1} : A \setminus S \to B \setminus f(S)$.

Note que $f : S \to f(S)$ é sobrejetora e injetora, ou seja, uma bijeção.

Então a seguinte função $h : A \to B$, $h(x) = \begin{cases} g^{-1}(x), \text{ se } x \in A \setminus S \\ f(x), \text{ se } x \in S \end{cases}$ também é uma bijeção.

Veja a função h na figura abaixo.



Agora vamos encontrar esse $S \subset A$.

Defina a função $H : \mathcal{P}(A) \to \mathcal{P}(A),\ H(X) = A \setminus g(B \setminus f(X))$, , onde $f(X) = \{f(x),\ x \in X\}$.

Note duas coisas:

1ª) $g(B \setminus f(S)) = A \setminus S \Leftrightarrow A \setminus g(B \setminus f(S)) = S$.

Portanto o S que buscamos satisfaz $H(S) = S$.

2ª) Se $X \subset Y$ então $H(X) \subset H(Y)$

(Note que não podemos utilizar o item a) do exercício 1.5.17, porque $H(X) \neq \{H(x),\ x \in X\}$. Ele foi definido de outro jeito).

Demonstração: Se $X \subset Y$ então $f(X) \subset f(Y)$. Isso é verdade por causa do item a) do exercício 1.5.17, pois aqui $f(X)$ significa $f(X) = \{f(x),\ x \in X\}$.

Agora $f(X) \subset f(Y)$ implica $B \setminus f(Y) \subset B \setminus f(X)$.

De novo, pelo item a) do exercício 1.5.17, temos $g(B \setminus f(Y)) \subset g(B \setminus f(X))$.

Novamente isso implica $A \setminus g(B \setminus f(X)) \subset A \setminus g(B \setminus f(Y))$, ou seja, $H(X) \subset H(Y)$.

Temos tudo que precisamos para terminar a demonstração.

Defina $C = \{X \in \mathcal{P}(A),\ X \subset H(X)\}$. Note que $\emptyset \in C$.

Seja S a união de todos os conjuntos que pertencem a C.

Vou provar que esse S satisfaz $H(S) = S$ e pela $1^{\underline{a}}$) observação acima ele é o S que queremos para concluir a demonstração.

Primeiro vamos ver que $S \subset H(S)$.

Se $X \in C$ então $X \subset S$, pois S é a união de todos os elementos de C incluindo esse X.

Agora pela $2^{\underline{a}}$) observação acima , como $X \subset S$, então $H(X) \subset H(S)$.

Além disso, pela definição de C, $X \subset H(X)$. Assim $X \subset H(S)$, para todo $X \in C$.

Portanto a união de todos os X que pertencem a C também é um subconjunto de $H(S)$, isto é, $S \subset H(S)$.

Falta provar que $H(S) \subset S$.

Como $S \subset H(S)$ então $H(S) \subset H(H(S))$, pela $2^{\underline{a}}$) observação acima.

Pela definição de C, temos que $H(S) \in C$.

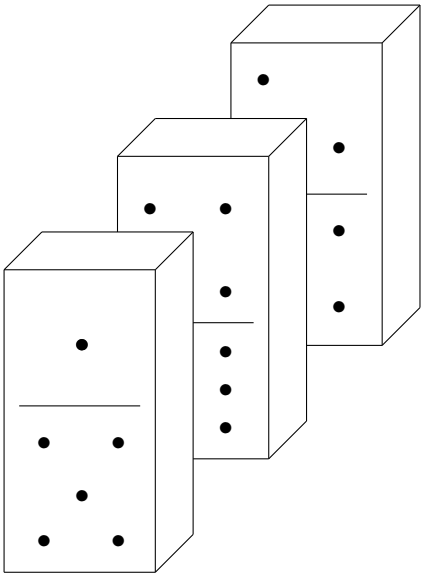
Assim $H(S)$ é um dos elementos da união que forma S, ou seja, $H(S) \subset S$.

Isso completa a demonstração. □

Capítulo 3

Princípio da indução finita

Você conhece o efeito dominó?



Depois de por as peças de dominó enfileiradas como posso ter certeza de que todas vão cair?

- A primeira peça tem que cair.
- Cada peça que cai deve derrubar a próxima.

Se essas duas regras forem cumpridas então todas as peças vão cair.
Vou reescrever isso de maneira mais matemática agora.

Defina a afirmação $P(n) =$ a peça que ocupa a posição n caiu.

Para garantir que $P(n)$ seja verdadeiro para todo n. Preciso garantir que

- $P(1)$ seja verdadeiro.

- Se $P(m)$ então $P(m+1)$ seja verdadeiro (Note que aqui m é qualquer).

A parte incrível dessa história é que $P(n)$ pode ser qualquer afirmação que dependa de um número natural n.

3.1 Indução finita

Vamos provar utilizando o efeito dominó que $P(n) = n^2 + n$ é par para todo $n \in \mathbb{N}$.

- $P(1) = 1^2 + 1 = 2$ é par . É verdade.
- Vamos provar: Se $P(m)$ então $P(m+1)$

  Então por hipótese $m^2 + m$ é par.

  Note que $(m+1)^2 + (m+1) = m^2 + 2m + 1 + m + 1 = m^2 + m + 2(m+1)$.

  Portanto $(m+1)^2 + (m+1)$ é a soma de dois números pares: $m^2 + m$, $2(m+1)$.

  Assim $(m+1)^2 + (m+1)$ é par se $m^2 + m$ for par.

Então $P(1)$ é verdadeiro, o que implica que $P(2)$ é verdadeiro (já que $P(m)$ implica $P(m+1)$). Mas $P(2)$ verdadeiro implica $P(3)$ verdadeiro. E assim sucessivamente. Viu o efeito dominó?

O efeito dominó em matemática recebe o nome de **Indução Finita**.

Princípio da Indução Finita

Para provar que uma afirmação $P(n)$ é válida para todo $n \in \mathbb{N}$, basta fazer duas coisas.

1. Provar: $P(1)$.

   Essa parte é a Base da indução.

2. Provar: Se $P(m)$ então $P(m+1)$.

   Para provar essa parte precisamos assumir que $P(m)$ é verdadeiro para provar $P(m+1)$. Essa hipótese de $P(m)$ ser válida é chamada de **Hipótese de indução**.

Observação. Se você provou a segunda parte e apenas conseguiu provar $P(3)$ (a base foi $P(3)$) então você provou que $P(n)$ é verdadeiro para $n \geq 3$.

Exemplos: *a*) Mostre que $1 + 2 + \ldots + n = \dfrac{n(n+1)}{2}$ para todo $n \in \mathbb{N}$.

Aqui $P(n)$ significa $1 + 2 + \ldots + n = \dfrac{n(n+1)}{2}$.

Base da indução: Note que $1 = \dfrac{1(1+1)}{2}$ então $P(1)$ vale.

Hipótese de indução: $1 + 2 + \ldots + m = \dfrac{m(m+1)}{2}$ (Assuma que $P(m)$ vale)

Vamos provar $P(m+1)$.

Por hipótese de indução, $1 + 2 + \ldots + m + (m+1) = \dfrac{m(m+1)}{2} + (m+1)$.

Agora $\dfrac{m(m+1)}{2} + (m+1) = \dfrac{m(m+1)}{2} + \dfrac{2(m+1)}{2} = \dfrac{(m+2)(m+1)}{2}$.

Portanto $1 + 2 + \ldots + m + (m+1) = \dfrac{(m+1)[(m+1)+1]}{2}$. Isto é, $P(m+1)$ vale.

b) Mostre que $1 + 3 + 5 + \ldots + 2n - 1 = n^2$.

Em outras palavras se somarmos os n primeiros númeors naturais ímpares o resultado dá n^2.

Aqui $P(n)$ significa $1 + 3 + 5 + \ldots + 2n - 1 = n^2$.

Base da indução: Note que $1 = 1^2$ então $P(1)$ vale.

Hipótese de indução: $1 + 3 + 5 + \ldots + 2m - 1 = m^2$ (Assuma que $P(m)$ vale)

Vamos provar $P(m+1)$.

Por hipótese de indução, $1 + 3 + 5 + \ldots + 2m - 1 + [2(m+1) - 1] = m^2 + [2(m+1) - 1]$.

Agora $m^2 + [2(m+1) - 1] = m^2 + 2m + 1 = (m+1)^2$.

Portanto $P(m+1)$ vale.

c) Mostre que $n < 2^n$ para to $n \in \mathbb{N}$.

Aqui $P(n)$ significa $n < 2^n$.

Base da indução: Note que $1 < 2^1 = 2$ então $P(1)$ vale.

Hipótese de indução: $m < 2^m$ (Assuma que $P(m)$ vale)

Vamos provar $P(m+1)$.

Por hipótese de indução, $m < 2^m$. Portanto $m + 1 < 2^m + 1$.

Como 2^m é sempre par então $1 < 2^m$,

Assim $m + 1 < 2^m + 1 < 2^m + 2^m$, isto é, $m + 1 < 2^{m+1}$.

Portanto $P(m + 1)$ vale.

d) Mostre que para qualquer conjunto A finito temos $\#\mathcal{P}(A) = 2^{\#A}$.

Aqui $P(n)$: Se $\#A = n$ então $\#\mathcal{P}(A) = 2^n$.

Base da indução: Se $n = 1$ então $\mathcal{P}(A) = \{\emptyset, A\}$. Portanto $\#\mathcal{P}(A) = 2^1$. ($P(1)$ vale)

Hipótese de indução: Se $\#A = m$ então $\#\mathcal{P}(A) = 2^m$ (Assuma que $P(m)$ vale)

Vamos provar $P(m + 1)$.

Seja $\#A = m + 1$ e $a \in A$.
Podemos dividir os subconjuntos de A em duas categorias, os que não contêm a e os que contêm,

$$\mathcal{P}(A) = \{B \subset A, a \notin B\} \cup \{C \subset A, a \in C\}.$$

Agora note que todo C que contém a pode ser escrito como $C = \{a\} \cup B$, onde B não contém a.
Para obter todos os possíveis subconjuntos do tipo C basta variar B na equação $C = \{a\} \cup B$.
Isso significa que $\#\{C \subset A, a \in C\} = \#\{B \subset A, a \notin B\}$.
Como é impossível que um conjunto contenha e não contenha $-a-$ ao mesmo tempo então

$$\{C \subset A, a \in C\} \cap \{B \subset A, a \notin B\} = \emptyset.$$

Essas duas últimas informações nos dão

$$\#\mathcal{P}(A) = \#\{B \subset A, a \notin B\} + \#\{C \subset A, a \in C\} = 2.\#\{B \subset A, a \notin B\}.$$

Note que $\mathcal{P}(A \setminus \{a\}) = \{B \subset A, a \notin B\}$ e $\#(A \setminus \{a\}) = m$.
Por Hipótese de indução, $\#\mathcal{P}(A \setminus \{a\}) = 2^m$.
Então

$$\#\mathcal{P}(A) = 2.\#\{B \subset A, a \notin B\} = 2.\#\mathcal{P}(A \setminus \{a\}) = 2.2^m = 2^{m+1}.$$

Portanto $P(m + 1)$ vale.

e) Mostre que se $-1 \leq h$ então $1 + nh \leq (1 + h)^n$

Aqui $P(n)$ significa $1 + nh \leq (1 + h)^n$.

Base da indução: Note que $1 + h \leq (1 + h)^1$. Portanto $P(1)$ vale.

Hipótese de indução: $1 + mh \leq (1 + h)^m$ (Assuma que $P(m)$ vale)

Vamos provar $P(m + 1)$.

Como $-1 \leq h$ então $0 \leq 1 + h$.

Pela hipótese de indução, $(1 + mh)(1 + h) \leq (1 + h)^m(1 + h) = (1 + h)^{m+1}$.

Agora $(1 + mh)(1 + h) = 1 + mh + h + mh^2 = 1 + (m + 1)h + mh^2$, ou seja,

$$1 + (m + 1)h = (1 + mh)(1 + h) - mh^2.$$

Como $m > 0$ e $h^2 \geq 0$ então $mh^2 \geq 0$.

Portanto $1 + (m + 1)h \leq (1 + mh)(1 + h)$, mas $(1 + mh)(1 + h) \leq (1 + h)^{m+1}$.

Juntando essas duas informações temos

$$1 + (m + 1)h \leq (1 + h)^{m+1}.$$

Portanto $P(m + 1)$ vale.

Exercício 3.1.1. *Prove por indução que as seguintes afirmações valem para todo* $n \in \mathbb{N}$.

a) $n^3 - n$ *é divisível por 6*

b) Se $a > b > 0$ *então* $a^n > b^n > 0$

c) $1^2 + 2^2 + 3^2 + \ldots + n^2 \leq n^3$

d) $1 + \frac{1}{2} + \frac{1}{2^2} + \ldots + \frac{1}{2^n} < 2$

e) $1^3 + 2^3 + 3^3 + \ldots + n^3 = (1 + 2 + 3 + \ldots + n)^2$

f) $1.2 + 2.3 + 3.4 + \ldots + n.(n + 1) = \frac{n(n+1)(n+2)}{3}$

g) $1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$

h) $1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{2^n} \geq 1 + \frac{n}{2}$

i) O número mínimo de movimentos necessários para resolver o problema da torre de Hanoi com n *peças é* $2^n - 1$.

$j)\ 1 + r + r^2 + \ldots + r^n = \dfrac{r^{n+1} - 1}{r - 1}$, *se* $r \neq 1$.

Vamos fazer alguns items do exercício 3.1.1

3.1.1a) $n^3 - n$ é divisível por 6

Solução: $P(n)$ siginifica $n^3 - n$ é divisível por 6

Base da indução: Verificar $P(1)$.

$1^3 - 1 = 1 - 1 = 0$ é divisível por 6 . Isto é, $P(1)$ vale.

Hipótese de Indução: Suponha que $P(m)$ vale, isto é, $m^3 - m$ é múltiplo de 6.

Vamos provar $P(m + 1)$.

Considere
$$\begin{aligned}(m+1)^3 - (m+1) &= (m+1)(m+1)^2 - (m+1)\\ &= (m+1)(m^2 + 2m + 1) - (m+1)\\ &= m^3 + 2m^2 + m + m^2 + 2m + 1 - (m+1)\\ &= m^3 + 3m^2 + 3m + 1 - m - 1\\ &= (m^3 - m) + 3m^2 + 3m\\ &= (m^3 - m) + 3(m^2 + m)\end{aligned}$$

Note que $m^2 + m$ é sempre par. Esse foi o primeiro exemplo da seção 3.1.

Então $3(m^2 + m)$ é múlitplo de 2 e de 3, ou seja, múltiplo de 6. Podemos escrevê-lo como

$$3(m^2 + m) = 6.r, \text{ onde } r \text{ é inteiro.}$$

Por hipótese de indução, $m^3 - m$ também é múltiplo de 6. Podemos escrevê-lo como

$$m^3 - m = 6.s, \text{ onde } s \text{ é inteiro.}$$

Assim $(m^3 - m) + 3(m^2 + m) = 6.r + 6.s = 6.(r + s)$, ou seja,

$$(m^3 - m) + 3(m^2 + m) = (m+1)^3 - (m+1) \text{ também é múltiplo de 6.}$$

Provamos $P(m + 1)$.

3.1.1c) $1^2 + 2^2 + 3^2 + \ldots + n^2 \leq n^3$

Solução: $P(n)$ significa $1^2 + 2^2 + 3^2 + \ldots + n^2 \leq n^3$

Base da indução: Verificar $P(1)$

$1^2 = 1 \leq 1 = 1^3$. Isto é, $P(1)$ vale.

Hipótese de Indução: Suponha que $P(m)$ vale, isto é, $1^2 + 2^2 + 3^2 + \ldots + m^2 \leq m^3$

Vamos provar $P(m+1)$.

Por hipótese de indução $1^2 + 2^2 + 3^2 + \ldots + m^2 + (m+1)^2 \leq m^3 + (m+1)^2$.

Na item 3.1.1a), vimos que $(m+1)^3 = m^3 + 3m^2 + 3m + 1$.

Agora $m^3 + (m+1)^2 = m^3 + m^2 + 2m + 1 \leq m^3 + 3m^2 + 3m + 1 = (m+1)^3$.

Assim $1^2 + 2^2 + 3^2 + \ldots + m^2 + (m+1)^2 \leq (m+1)^3$.

Provamos $P(m+1)$. $\square$

3.1.1.j) $1 + r + r^2 + \ldots + r^n = \dfrac{r^{n+1} - 1}{r - 1}$, se $r \neq 1$.

Solução: $P(n)$ significa $1 + r + r^2 + \ldots + r^n = \dfrac{r^{n+1} - 1}{r - 1}$

Base da indução: Verificar $P(1)$

Como $(r+1)(r-1) = r^2 - 1$ então $1 + r^1 = \dfrac{r^2 - 1}{r - 1}$. Isto é, $P(1)$ vale.

Hipótese de Indução: Suponha que $P(m)$ vale, isto é, $1 + r + r^2 + \ldots + r^m = \dfrac{r^{m+1} - 1}{r - 1}$

Vamos provar $P(m+1)$.

Por hipótese de indução, $1 + r + r^2 + \ldots + r^m + r^{m+1} = \dfrac{r^{m+1} - 1}{r - 1} + r^{m+1}$

Agora, $\dfrac{r^{m+1} - 1}{r - 1} + r^{m+1} = \dfrac{r^{m+1} - 1 + r.r^{m+1} - r^{m+1}}{r - 1} = \dfrac{r^{(m+1)+1} - 1}{r - 1}$.

Portanto $1 + r + r^2 + \ldots + r^m + r^{m+1} = \dfrac{r^{(m+1)+1} - 1}{r - 1}$. Provamos $P(m+1)$. $\square$

3.2 Indução forte

Quando se demonstra na indução finita que $P(m)$ implica $P(m+1)$, cria-se uma "máquina"que faz o serviço pesado. Entretanto ela não funciona até receber uma informação inicial. A informação inicial é a base da indução, o caso $P(1)$.

Às vezes para demonstrar $P(m+1)$ é necessário mais do que o $P(m)$, talvez precisamos de todos os casos anteriores: $P(1), \ldots, P(m)$. Você pode usá-los sem problema. Nesse caso você está fazendo uma indução forte (ou completa).

Indução forte

- Prova-se a base da Indução, normalmente é $P(1)$
- Assume-se que $P(1), \ldots, P(m)$ é verdadeiro (Hipótese de Indução)
- Prova-se $P(m+1)$

OBS: Essa "máquina" que prova $P(m+1)$ a partir dos anteriores pode precisar de mais de uma condição inicial. Veremos a seguir exemplos que para provar $P(m+1)$ precisamos de $P(m-1)$. Então a sua máquina nao pode provar $P(2)$, pois precisaria de $P(-1)$ para prová-lo ($P(n)$ é uma afimação com n natural, $P(-1)$ não faz sentido). Portanto precisamos de $P(1)$ e $P(2)$ para iniciar a máquina.

Definição 3.2.1. *Vamos usar frequentemente nessa seção uma sequência de números muito famosa chamada de sequência de Fibonacci:* $1, 1, 2, 3, 5, 8, \ldots$
Seja f_n o n-ésimo termo da sequencia de Fibonacci. Cada termo dessa sequencia é a soma dos dois termos anteriores: $f_{n+1} = f_n + f_{n-1}$.

Exercício 3.2.2. *Seja* $\alpha = \dfrac{1+\sqrt{5}}{2}$.

a) Mostre que $\alpha^2 = \alpha + 1$.

b) Mostre que $f_n > \alpha^{n-2}$ *para todo* $n \geq 3$.

Solução: *a)* $\alpha^2 = \left(\dfrac{1+\sqrt{5}}{2}\right)^2 = \dfrac{1+2\sqrt{5}+5}{4} = \dfrac{6+2\sqrt{5}}{2} = \dfrac{3+\sqrt{5}}{2} = 1 + \dfrac{1+\sqrt{5}}{2} = 1+\alpha.$

b) Vamos provar a base da indução depois, pois ainda não sabemos quanto casos base precisaremos nesa indução.

Hipótese de indução: Suponha que $f_3, f_4, \ldots, f_m$ satisfazem a desigualdade.

Provemos a desigualdade para f_{m+1}.

Lembre-se que $f_{m+1} = f_m + f_{m-1}$.

Pela hipótese de indução, sabemos que a desigualdade vale para f_m e f_{m-1}, isto é,

$$f_m > \alpha^{m-2} \text{ e } f_{m-1} > \alpha^{(m-1)-2} = \alpha^{m-3}$$

Assim $f_{m+1} = f_m + f_{m-1} > \alpha^{m-2} + \alpha^{m-3} = \alpha^{m-3}(\alpha + 1)$.

Pelo item a), $1 + \alpha = \alpha^2$.

Portanto $f_{m+1} > \alpha^{m-3}\alpha^2 = \alpha^{m-1} = \alpha^{(m+1)-2}$.

Terminamos de construir nossa máquina. Note que para provar o resultado para f_{m+1} tivemos que usar o resultado para f_m e f_{m-1}.

Observação 3.2.3. *A princípio essa demonstração poderia provar o f_3 sabendo que a desigualdade vale para f_1 e f_2. Só que a desigualdade não vale para f_2, pois $f_2 = 1$ e $\alpha^{2-2} = 1$. Portanto f_2 não é maior que α^{2-2}.*

Essa demonstração pode provar f_4? Também não. Porque de novo ela precisaria do caso f_2 e f_3. Essa demonstração pode provar f_5? Talvez, porque f_5 depende do resultado provado para f_3 e f_4.

Teremos que provar os casos f_3 e f_4 separados. Eles formam a base da indução.

Base da indução

Caso f_3 : $\alpha^{3-2} = \alpha = \dfrac{1+\sqrt{5}}{2} < \dfrac{1+\sqrt{9}}{2} = \dfrac{4}{2} = 2 = f_3$. Portanto resultado vale para f_3.

Caso f_4 : Pelo item a), $\alpha^{4-2} = \alpha^2 = 1 + \alpha$.

Acabamos de ver que $\alpha < f_3$ e sabemos que $1 = f_2$. Portanto $\alpha^{4-2} = 1 + \alpha < f_2 + f_3 = f_4$, ou seja, resultado vale para f_4. □

Exercício 3.2.4. *Considere $P(n)$ afirmação que diz que utilizando somente selos de 3 e 5 centavos podemos postar uma carta de valor n.*

a) Mostre que $P(8)$, $P(9)$ e $P(10)$ são verdadeiros.

b) Mostre que $P(n)$ é verdadeiro para $n \geq 8$.

Solução: *a*) $8 = 1.3 + 1.5$ (1 selo de 3 e 1 de 5), $9 = 3.3$ (3 selos de 3) e $10 = 2.5$ (2 selos de 5)

b) Hipótese de indução: Suponha que $P(8), \ldots, P(m)$ são verdadeiros.

Vamos provar $P(m+1)$.

O menor valor de selo que podemos usar é 3. Já use um selo de 3. O valor que falta para postar carta é $(m+1) - 3$.

Se $(m+1) - 3$ for um número entre 8 e m então, pela hipótese de indução, $(m+1) - 3 = x.3 + y.5$ (onde x e y são inteiros não negativos). Portanto $m + 1 = (x+1).3 + y.5$, ou seja, podemos postar uma carta de valor $m+1$ usando $x+1$ selos de 3 e y selos de 5.

A máquina que construímos tem uma limitação, ela prova o caso $m+1$ utilizando $(m+1) - 3$, mas $(m+1) - 3 \geq 8$. Portanto $m + 1 \geq 11$. A máquina só pode ser usada para números maiores ou iguais a 11. Pois para provar o 11 usamos o caso 8, para o 12 usamos o 9 e etc.

Nossos casos base são $P(8)$, $P(9)$ e $P(10)$ que já foram feitos no item *a*). □

No próximo capítulo falaremos de teoria de números, mas gostaria de provar o seguinte teorema com indução forte. Precisamos de uma definição antes.

Definição 3.2.5. *Seja $a \in \mathbb{N}$. Dizemos que a é primo se $a > 1$ e, além disso, se as únicas maneiras de escrever a como produto de dois naturais são $a = a.1 = 1.a$.*

Exemplo: 2 é primo. Se 2 não for primo então $2 = a.b$, onde a, b são naturais maiores que 1. Então $a \geq 2$ e $b \geq 2$. Então $2 = a.b \geq 4$. Contradição.

Teorema 3.2.6. *Todo número natural diferente de 1 ou é primo ou é produto finito de primos.*

Demonstração. Hipótese de indução: O resultado vale para $2, 3, \ldots, m$.

Vamos provar $m+1$. Se $m+1$ for primo então já temos o resultado.

Se $m+1$ não for primo então $m + 1 = a.b$, onde a, b são naturais maiores que 1.

Note também que nem a e nem b podem ser $m+1$, pois forçaria o outro a ser 1.

Por hipótese de indução, a e b ou são primos ou produto finito de primos. Portanto $a.b$ é produto finito de primos.

Base da indução: 2 é primo, provado no exemplo anterior. □

Exercício 3.2.7. *Seja f_n o n-ésimo termo da sequência de Fibonacci. Prove para qualquer $n \in \mathbb{N}$ que*

a) $-f_1 + f_2 - \ldots - f_{2n-1} + f_{2n} = f_{2n-1} - 1$

b) $f_1^2 + f_2^2 + \ldots + f_n^2 = f_n f_{n+1}$

c) $f_1 + f_3 + \ldots + f_{2n-1} = f_{2n}$

d) $f_{n+1} f_{n-1} - f_n^2 = (-1)^n$

e) $f_1 f_2 + f_2 f_3 + f_3 f_4 + \ldots + f_{2n-1} f_{2n} = f_{2n}^2$

Exercício 3.2.8. *Seja $P(n)$ afirmação que diz que podemos postar uma carta de valor n utilizando selos de*

a) 4 e 7 centavos. Mostre que $P(n)$ é verdadeiro para $n \geq 18$.

b) 3 e 10 centavos. Descubra o menor k tal que $P(n)$ é verdadeiro para $n \geq k$.

c) 2 e 5 centavos. Descubra o menor k tal que $P(n)$ é verdadeiro para $n \geq k$.

3.3 Relações de recorrência

Uma relação de recorrência é uma equação que define uma sequência de números dizendo como um termo da sequência depende dos anteriores. Por exemplo, para a sequência de Fibonacci a relação de recorrência era $f_{n+1} = f_n + f_{n-1}$. Sabendo os termos iniciais $f_1 = f_2 = 1$ obtínhamos todos os outros.

O objetivo dessa pequena seção é mostrar como se resolve alguns tipos básicos de relação de recorrência. Resolver uma relação significa encontrar uma fórmula para os termos da sequência dependendo de n.

Por exemplo, no fim da seção obteremos $f_{n+1} = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}$. Essa fórmula é interessante pois já não precisamos da recorrência para descobrir os termos da sequência de Fibonacci.

As recorrências mais simples

- A relação de recorrência mais simples possível é a $a_{n+1} = a_n$, ou seja, todos os termos iguais. A solução dessa relação é $a_{n+1} = a_1$ para todo n.
- Outra bem simples é a $a_{n+1} = ca_n$. A sua solução é $a_{n+1} = c^n a_1$.

  Para ver isso, basta notar que

$$\frac{a_{n+1}}{\cancel{a_n}}\frac{\cancel{a_n}}{\cancel{a_{n-1}}}\frac{\cancel{a_{n-1}}}{\cancel{a_{n-2}}}\cdots\frac{\cancel{a_2}}{a_1} = \overbrace{ccc\ldots c}^{n\ vezes} \quad \Rightarrow \frac{a_{n+1}}{a_1} = c^n$$

A seguinte relação já é mais complicada.

Teorema 3.3.1. *A solução da relação $a_{n+1} = ca_n + dr^n$, onde $c, d, r \in \mathbb{R} \setminus \{0\}$ é dada por*

$$a_{n+1} = \begin{cases} c^n a_1 + dr^n n\ , & \text{se } c = r \\ c^n a_1 + dr^n . \dfrac{\left(\frac{c}{r}\right)^n - 1}{\frac{c}{r} - 1}, & \text{se } c \neq r \end{cases}$$

Demonstração. Multiplique as equações

$$a_{n+1} - ca_n = dr^n, \quad a_n - ca_{n-1} = cdr^{n-1}, \ldots, \quad a_2 - ca_1 = dr^1$$

por $1, c, c^2, \ldots, c^{n-1}$, respectivamente. Depois some-as como fizemos a seguir. Note que muitos termos serão cancelados.

Note que

$$\begin{aligned}
& a_{n+1} - ca_n = dr^n && \Rightarrow \quad a_{n+1} - \cancel{ca_n} = dr^n \\
& c(a_n - ca_{n-1}) = cdr^{n-1} && \Rightarrow \quad \cancel{ca_n} - \cancel{c^2 a_{n-1}} = cdr^{n-1} \\
& c^2(a_{n-1} - ca_{n-2}) = c^2 dr^{n-2} && \Rightarrow \quad \cancel{c^2 a_{n-1}} - \cancel{c^3 a_{n-2}} = c^2 dr^{n-2} \\
& \qquad \vdots && \qquad\qquad \vdots \\
& c^{n-1}(a_2 - ca_1) = c^{n-1} dr^1 && \Rightarrow \quad \underline{+\cancel{c^{n-1} a_2} - c^n a_1 = c^{n-1} dr^1} \\
& && \qquad a_{n+1} - c^n a_1 = dr^n + cdr^{n-1} + \cdots + c^{n-1} dr^1
\end{aligned}$$

O que sobra é $a_{n+1} - c^n a_1 = dr^n + cdr^{n-1} + c^2 dr^{n-2} + \ldots + c^{n-1} dr^1$.

Podemos reescrevê-lo, $a_{n+1} - c^n a_1 = dr^n \left(1 + \frac{c}{r} + \left(\frac{c}{r}\right)^2 + \ldots + \left(\frac{c}{r}\right)^{n-1}\right)$.

Agora, se $\frac{c}{r} = 1$ então $1 + \frac{c}{r} + \left(\frac{c}{r}\right)^2 + \ldots + \left(\frac{c}{r}\right)^{n-1} = n$.

Se $\frac{c}{r} \neq 1$ então $1 + \frac{c}{r} + \left(\frac{c}{r}\right)^2 + \ldots + \left(\frac{c}{r}\right)^{n-1} = \frac{\left(\frac{c}{r}\right)^n - 1}{\frac{c}{r} - 1}$, pela letra j) do exercício 3.1.1. □

Exercício 3.3.2. *Resolva as seguintes recorrências. Utilize as fórmulas do exercício 3.1.1 se necessárias.*

a) $a_{n+1} = 2a_n + 1$

b) $a_{n+1} = 3a_n + 2^n$

c) $a_{n+1} = a_n + n$

d) $a_{n+1} = a_n + n^2$

Vamos resolver a letra a).

Solução:

Note que
$$\begin{aligned}
a_{n+1} - 2a_n = 1 &\Rightarrow a_{n+1} - \cancel{2a_n} = 1 \\
2(a_n - 2a_{n-1}) = 2.1 &\Rightarrow \cancel{2a_n} - \cancel{2^2 a_{n-1}} = 2.1 \\
2^2(a_{n-1} - 2a_{n-2}) = 2^2.1 &\Rightarrow \cancel{2^2 a_{n-1}} - \cancel{2^3 a_{n-2}} = 2^2.1 \\
\vdots & \qquad\qquad \vdots \\
2^{n-1}(a_2 - 2a_1) = 2^{n-1}.1 &\Rightarrow \underline{+\cancel{2^{n-1} a_2} - 2^n a_1 = 2^{n-1}.1} \\
& \qquad a_{n+1} - 2^n a_1 = 1 + 2 + \cdots + 2^{n-1}
\end{aligned}$$

Pela letra j) do exercício 3.1.1., $1 + 2 + \cdots + 2^{n-1} = \frac{2^n - 1}{2 - 1} = 2^n - 1$.

Assim $a_{n+1} = 2^n a_1 + 2^n - 1$. □

Nas relações anteriores a recorrência relacionava o termo com o antecessor. Agora veremos como resolver certas recorrências que relacionam o termo com dois termos anteriores. Mas antes precisamos de uma definição.

Definição 3.3.3. *Sejam c, d números reais. O polinômio característico associado a recorrência $a_{n+2} = ca_{n+1} + da_n$ é definido por $p(x) = x^2 - cx - d$.*

Exemplo: Associado a relação de Fibonacci $f_{n+2} = f_{n+1} + f_n$ temos o seguinte polinômio característico, $f(x) = x^2 - x^1 - 1$.

Teorema 3.3.4. *Sejam $c, d \in \mathbb{R}$. Denote por r_1, r_2 as raízes do polinômio característico associado a relação $a_{n+2} = ca_{n+1} + da_n$.*

- *Se $r_1 = r_2 = 0$ então a solução dessa relação é dada por $a_{n+2} = 0$.*
- *Se $r_1 = r_2 \neq 0$ então a solução dessa relação é dada por*

$$a_{n+2} = zr_1^{n+1} + w(n+1)r_1^{n+1}, \text{ onde } z = a_1, \ w = \frac{a_2 - r_1 a_1}{r_1}$$

- *Se $r_1 \neq r_2$ então a solução dessa relação é dada por*

$$a_{n+2} = xr_1^{n+1} - yr_2^{n+1}, \text{ onde } x = \frac{a_2 - a_1 r_2}{r_1 - r_2}, \ y = \frac{a_2 - a_1 r_1}{r_1 - r_2}$$

Demonstração. Primeiro caso: $r_1 = r_2 = 0$

Nesse caso $x^2 - cx - d$ tem duas raízes iguais a zero, ou seja, $c = d = 0$.
Então a recorrência fica $a_{n+2} = 0$.

Segundo e Terceiro casos: Existe raíz diferente de 0.

Existe um truque para resolver a recorrência: $a_{n+2} = ca_{n+1} + da_n$
Vamos escrever essa recorrência da seguinte maneira:

$$(a_{n+2} - xa_{n+1}) = z(a_{n+1} - xa_n)$$

Então

$$x + z = c \ \text{ e } \ xz = -d \ \Rightarrow \ x(x+z) = xc \ \Rightarrow \ x^2 + xz = xc \ \Rightarrow \ x^2 - xc - d = 0.$$

Se ao invés de mutiplicar $x + z = c$ por x, multiplicamos por z, obteremos a mesma equação para z. Portanto x e z são as raizes r_1, r_2 do polinômio característico. Escolho z para ser a raiz diferente de 0. Seja $z = r_2 \neq 0$.

Nossa equação fica

$$(a_{n+2} - r_1 a_{n+1}) = r_2(a_{n+1} - r_1 a_n).$$

Porque fizemos isso?

Porque agora podemos definir $b_{n+1} = a_{n+2} - r_1 a_{n+1}$ e obtemos

$$b_{n+1} = r_2 b_n,$$

que é uma das recorrências mais simples de resolver.

Sua solução é $b_{n+1} = r_2^n b_1$, onde $b_1 = a_2 - r_1 a_1$.

Então $a_{n+2} - r_1 a_{n+1} = r_2^n(a_2 - r_1 a_1)$, ou seja,

$$a_{n+2} = r_1 a_{n+1} + r_2^{n+1} \frac{(a_2 - r_1 a_1)}{r_2}.$$

Note que essa é a recorrência que resolvemos no teorema 3.3.1.

Sua solução é

$$a_{n+2} = \begin{cases} r_1^{n+1} a_1 + \dfrac{(a_2 - r_1 a_1)}{r_2} r_2^{n+1}(n+1)\ , & \text{se } r_1 = r_2 \\ r_1^{n+1} a_1 + \dfrac{(a_2 - r_1 a_1)}{r_2} r_2^{n+1} \left(\dfrac{\left(\dfrac{r_1}{r_2}\right)^{n+1} - 1}{\dfrac{r_1}{r_2} - 1} \right), & \text{se } r_1 \neq r_2 \end{cases}$$

A primeira equação já está de acordo com o enunciado do teorema.

A segunda podemos reescrevê-la como:

$$a_{n+2} = r_1^{n+1} a_1 + (a_2 - r_1 a_1)\frac{r_1^{n+1} - r_2^{n+1}}{r_1 - r_2} \ \Rightarrow\ a_{n+2} = \frac{a_2 - r_2 a_1}{r_1 - r_2} r_1^{n+1} - \frac{a_2 - r_1 a_1}{r_1 - r_2} r_2^{n+1}$$

□

Exercício 3.3.5. *Mostre que a fórmula para o n−ésimo termo da sequência de Fibonacci é*

$$f_n = \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2} \right)^n$$

Capítulo 4

Teoria de Números

Agora estudaremos alguns teoremas relativos a números inteiros e naturais.

Relembrando $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ e $\mathbb{N} = \{1, 2, 3, \ldots\}$.

Veja a página 200 do livro Matemática Discreta e Aplicações cujo autor é o K.H. Rosen.

Definição 4.0.1. *Sejam $a, b \in \mathbb{Z}$ e $a \neq 0$. Dizemos que a divide b se existir $c \in \mathbb{Z}$ tal que $b = ac$. Nesse caso dizemos que a é divisor de b e que b é multiplo de a. A notação que usaremos para dizer que a divide b é $a \mid b$. Se a não divide b escreveremos $a \nmid b$.*

Exercício 4.0.2. *Sejam a, b números inteiros tais que $a, b \neq 0$ e $a \mid b$. Prove que $|a| \leq |b|$.*

Note que se a, b forem inteiros positivos então $a \leq b$, ou seja, um divisor de um número inteiro positivo nunca é maior que ele.

Solução: Note que $b = ca$, onde c é inteiro diferente de zero. Assim $|c| \geq 1$. Portanto $|b| = |ac| = |a||c| \geq |a|$. $\square$

Teorema 4.0.3. *Sejam $a, b, c \in \mathbb{Z}$.*

(i) Se $a \mid b$ e $a \mid c$ então $a \mid (b + c)$.

(ii) Se $a \mid b$ então $a \mid bc$.

(iii) Se $a \mid b$ e $b \mid c$ então $a \mid c$.

Demonstração. (i) Se $a \mid b$ e $a \mid c$ então existem $d, d' \in \mathbb{Z}$ tais que $b = ad$ e $c = ad'$.

Então $b + c = ad + ad' = a(d + d')$. Isto é, $a \mid (b + c)$.

(ii) Se $a \mid b$ então existe $d \in \mathbb{Z}$ tal que $b = ad$.

Multiplicando os dois lados por c obtemos $bc = adc$.

Como dc é um número inteiro obtemos $a \mid bc$.

(iii) Se $a \mid b$ e $b \mid c$ então existem $d, d' \in \mathbb{Z}$ tais que $b = ad$ e $c = bd'$.

Assim $c = bd' = adb'$. Como db' é um número inteiro então $a \mid c$. □

Corolário 4.0.4. *Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid b$ e $a \mid c$ então $a \mid mb + nc$ para quaisquer $m, n \in \mathbb{Z}$.*

Demonstração. Se $a \mid b$ e $a \mid c$ então $a \mid mb$ e $a \mid nc$ pelo item (ii) do teorema anterior.

Pelo item (i) do mesmo teorema temos $a \mid mb + nc$. □

Exercício 4.0.5. *Sejam $a, b, c, d \in \mathbb{Z} \setminus \{0\}$. Prove as seguintes afirmações.*

a) Se $a \mid b$ e $b \mid a$ então $a = b$ ou $a = -b$.

b) Se $a \mid b$ e $c \mid d$ então $ac \mid bd$.

c) Se $ac \mid bc$ então $a \mid b$.

Vou resolver a letra a), deixo a letra b) e c) para vocês.

4.0.5a). *Solução*: Se $a \mid b$ e $b \mid a$ então existem $d, d' \in \mathbb{Z}$ tais que $b = ad$ e $a = bd'$.

Assim $b = ad = bd'd$, ou seja, $b(1 - dd') = 0$.

Como $b \neq 0$ então $1 - dd' = 0$, ou seja, $dd' = 1$.

Note que $|d| \geq 1$ e $|d'| \geq 1$, pois d, d' são inteiros diferentes de 0.

Agora $|d|$ e $|d'|$ nao podem ser maiores do que 1 pois $|d|.|d'| = |dd'| = 1$.

Mas 1 e -1 são os únicos inteiros cujo o módulo é 1.

Portanto d, d' só podem ser 1 ou -1 implicando que $a = \pm b$. □

4.1 Algoritmo da divisão

O algoritmo da divisão diz que sempre podemos dividir o dividendo pelo divisor, obter um quociente e um resto, onde o resto é menor que o divisor.

Algoritmo da divisão

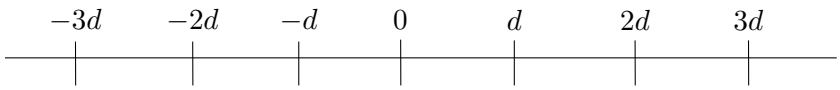
Teorema 4.1.1. *Seja $a \in \mathbb{Z}$ e $d \in \mathbb{N}$. Existem $q \in \mathbb{Z}$ e $r \in \mathbb{Z}$ tais que $a = dq + r$ e $0 \leq r < d$.*

Relembrando: a é o dividendo, d é divisor, q é o quociente e r é o resto.

Além disso, note que os restos na divisão por d só podem ser $0, 1, 2, \ldots, d-1$.

***Notação**: $r = a \bmod d$ (Isso significa que r é o resto de a na divisão por d)*

Demonstração. Abaixo está desenhada a reta que representada todos os números reais e escrevemos sobre ela os múltiplos de d.



Note que $\underline{a}$ vai pertencer a algum dos intervalos formados pelos múltiplos de d.

Isto é, existe $q \in \mathbb{Z}$ tal que $qd \leq a < (q+1)d = qd + d$.

Portanto, subtraindo qd nessa desigualdade obtemos, $0 \leq a - qd < d$.

Se chamarmos $r = a - qd$ então $a = qd + r$. Note que $0 \leq r < d$. □

Exemplos:

a) Como $5 = 0.10 + 5$ então $5 = 5 \mod 10$ (5 é o resto de 5 na divisão por 10)

b) Como $-5 = -0.10 - 5$ então $-5 = -0.10 - 10 + 5$. Assim $-5 = (-1).10 + 5$.

Portanto $5 = -5 \mod 10$ (5 é o resto de -5 na divisão por 10)

c) Como $1374 = 124.11 + 10$ então $10 = 1374 \mod 11$.

d) Como $1374 = 124.11 + 10$ então $-1374 = (-124).11 + -10$.

Assim $-1374 = (-124).11 - 11 + 1 = (-125).11 + 1$. Assim $1 = -1374 \mod 11$.

Exercício 4.1.2. *Seja r um dos possíveis restos na divisão por $d \in \mathbb{N}$, isto é, $r \in \{0, 1, 2, \ldots, d-1\}$. Mostre que*

a) $r = r \mod d$

b) *Se* $r \neq 0$ *então* $d - r = -r \mod d$.

Solução: 4.1.2.*a*) Note que $r = 0.d + r$ e $r \in \{0, 1, 2, \ldots, d-1\}$.

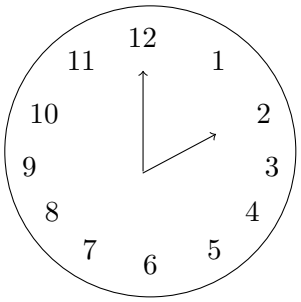
Então o resto na divisão de r por d é o próprio r, ou seja, $r = r \mod d$.

4.1.2.*b*) Como $0 < r < d$ então $0 < d - r < d$.

Assim $-r = -0.d - r = -0.d - 1.d + d - r = -1.d + d - r$.

Portanto o resto da divisão de $-r$ por d é $d - r$, isto é, $d - r = -r \mod d$. □

4.2 Aritmética modular



Utilizando o ponteiro das horas, quanto dá 9 horas mais 7 horas?

Agora utilizando o dos minutos, quanto dá 45 minutos mais 35 minutos?

Congruência

Definição 4.2.1. *Sejam* $a, b \in \mathbb{Z}$ *e* $m \in \mathbb{N}$*, dizemos que* $\underline{a}$ *é congruente a* $\underline{b}$ *módulo* m *se* $m \mid a-b$*. Usamos a notação* $a \equiv b \bmod m$ *para indicar essa congruência e utilizamos* $a \not\equiv b \bmod m$ *para a falta de congruência entre* a *e* b*.*

OBS: Note que $m \mid a$ *se e somente se* $a \equiv 0 \mod m$.

Exemplos:

a) $3 \equiv 15 \mod 12$, pois $12 \mid (3 - 15)$.

b) $5 \not\equiv 10 \mod 12$, pois $12 \nmid (5 - 10)$.

Consegue ver alguma relação com as horas do relógio de ponteiro?

Propriedades da congruência

Teorema 4.2.2. *Sejam $a, b, c \in \mathbb{Z}$ e $m \in \mathbb{N}$. As seguintes propriedades valem.*

a) $a \equiv a \mod m$

b) Se $a \equiv b \mod m$ *então* $b \equiv a \mod m$

c) Se $a \equiv b \mod m$ *e* $b \equiv c \mod m$ *então* $a \equiv c \mod m$

d) $a \equiv r \mod m$*, onde* $r = a \mod m$ *(*r *é o resto da divisão de* a *por* m*).*

Demonstração. *a)* Como $m \mid 0$ então $m \mid a - a$. Assim $a \equiv a \mod m$.

b) Se $a \equiv b \mod m$ então $a - b = md$. Assim $b - a = m(-d)$. Portanto $b \equiv a \mod m$.

c) Se $m \mid a - b$ e $m \mid b - c$ entao $m \mid (a - b) + (b - c)$, pelo item (i) do teorema 4.0.3. Assim $m \mid a - c$, ou seja, $a \equiv c \mod m$.

d) Pelo algoritmo da divisão, $a = qm + r$. Assim $a - r = qm$, ou seja, $a \equiv r \mod m$. □

Observação 4.2.3. *Não confunda* $a \equiv b \bmod m$ *com* $a = b \bmod m$.

- $a \equiv b \bmod m$ *significa que* $m \mid a - b$
- $a = b \bmod m$ *significa que* $\underline{a}$ *é o resto da divisão de* $\underline{b}$ *por* $\underline{m}$.

Mas é claro que existe uma relação entre essas duas coisas. Veja no teorema abaixo.

Teorema 4.2.4. *Sejam $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$. Então*

$$a \equiv b \mod m, \text{ se e somente se, } a \mod m = b \mod m$$

Isto é, $m \mid a - b$, se e só se, os restos de a, b na divisão por m são iguais.

Demonstração. Primeira parte: $(a \equiv b \mod m) \Rightarrow (a \mod m = b \mod m)$

Pelo algoritmo da divisão

$$a = q_1 m + r_1 \text{ e } b = q_2 m + r_2,$$

onde $q_1, q_2 \in \mathbb{Z}$ e $r_1, r_2 \in \{0, 1, \ldots, m-1\}$.

Como $r_1, r_2 \in \{0, 1, \ldots, m-1\}$ então $-m < r_1 - r_2 < m$.

Agora $a - b = m(q_1 - q_2) + r_1 - r_2$ e lembre-se que $a - b = mc$.

Assim $m(c - q_1 + q_2) = r_1 - r_2$. Portanto $r_1 - r_2$ é múlitplo de m.
O único múltiplo de m entre $-m$ e m é zero. Portanto $r_1 - r_2 = 0$.

Segunda parte: $(a \mod m = b \mod m) \Rightarrow (a \equiv b \mod m)$

Pelo algoritmo da divisão $a = q_1 m + r_1$ e $b = q_2 m + r_2$, onde $q_1, q_2 \in \mathbb{Z}$ e $r_1, r_2 \in \{0, 1, \ldots, m-1\}$.

Por hipótese, $r_1 = r_2$ então $a - b = q_1 m + r_1 - q_2 m - r_2 = m(q_1 - q_2)$. Isto é, $a \equiv b \mod m$. □

O teorema anterior já mostra uma vantagem de se trabalhar com congruência. Se você quiser descobrir se dois números a, b possuem o mesmo resto na divisão por m ou não, basta dividir $a - b$ por m. Sem esse teorema você teria que dividir a, b por m, obter os restos e compará-los. Você economizou uma divisão.

Exercício 4.2.5. *Utilize o último teorema para dizer se os números a, b possuem o mesmo resto na divisão por m ou não.*

a) $a = 117$, $b = 40$ *e* $m = 7$

b) $a = 117$, $b = 40$ *e* $m = 11$

c) $a = 117$, $b = 40$ *e* $m = 5$

Classes de congruência

Definição 4.2.6. *Sejam $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$. Dizemos que a, b pertencem a mesma classe de congruência módulo m se $a \equiv b \mod m$.*
OBS: O último teorema diz que só existem m classes de congruência módulo m em $\mathbb{Z}$.
A primeira classe é formada pelo inteiros que deixam resto 0 na divisão por m, a segunda pelo inteiros que deixam resto 1 na divisão por m e assim sucessivamente até a $m-$ésima classe formada pelos inteiros que deixam resto $m-1$ na divisão por m.

O seguinte teorema diz que em uma expressão envolvendo soma e multiplicação de números inteiros, podemos substituir qualquer número da expressão por outro congruente e a nova expressão será congruente a inicial. Isso será muito útil quando formos estudar os critérios de divisibilidade.

Como fazer contas com congruência?

Teorema 4.2.7. *Seja $m \in \mathbb{N}$ e $a, b, c, d \in \mathbb{Z}$.*

Se $a \equiv b \mod m$ e $c \equiv d \mod m$ então $a + c \equiv b + d \mod m$ e $a.c \equiv b.d \mod m$.

Demonstração. Se $a \equiv b \mod m$ e $c \equiv d \mod m$ então $m \mid a - b$ e $m \mid c - d$.

Pelo item (i) do teorema 4.0.3, $m \mid (a - b) + (c - d)$, ou seja, $m \mid (a + c) - (b + d)$.
Portanto $a + c \equiv b + d \mod m$.

Agora, pelo corolário 4.0.4, $m \mid a(c - d) + d(a - b)$.
Mas $a(c - d) + d(a - b) = ac - ad + ad - bd = ac - bd$.
Então $m \mid ac - bd$, ou seja, $ac \equiv bd \mod m$. □

Exercício 4.2.8. *Reduza ao máximo as seguintes expressões na congruência módulo 3 utilizando o teorema anterior.*

a) $13^{15}.27 + 7^9.45$

b) $6! + 5! + 7$

Solução:

a) Como $27 = 9.3 + 0$, $45 = 15.3 + 0$ então $27 \equiv 0 \mod 3$ e o $45 \equiv 0 \mod 3$.

Pelo teorema anterior, $13^{15}.27 \equiv 13^{15}.0 \mod 3$ e $7^9.45 = 7^9.0 \mod 3$.

Novamente, pelo teorema enterior, $13^{15}.27 + 7^9.45 \equiv 0 \mod 3$.

b) Como $6! = 6.5.4.3.2.1$ então $6! \equiv 0 \mod 3$. O mesmo com 5!.

Agora, $7 = 3.2 + 1$ então $7 \equiv 1 \mod 3$.

Pelo teorema anterior, $6! + 5! + 7 \equiv 0 + 0 + 1 \mod 3$.

Observação 4.2.9. *Para que serve reduzir uma expressão númerica em uma determinada congruência módulo m? Quando você faz isso, você está encontrando o menor número natural congruente a expressão. Lembre-se que números congruentes módulo m possuem os mesmos restos na divisão por m, pelo teorema 4.2.4. Com essa ideia você pode encontrar o resto da expressão na divisão por m.*
No exercício anterior você mostrou que a primeira expressão deixa resto 0 na divisão por 3 e a segunda deixa resto 1 na divisão por 3.

Exercício 4.2.10. *Encontre os restos na divisão por 7 dos seguintes números*

a) 475^2

b) $475 + 1232.2789$

c) 475^6

Solução: *a*) Como $475 = 67.7 + 6$ então $475 \equiv 6 \mod 7$, pelo item *d*) do teorema 4.2.2.
Pelo teorema anterior, $475.475 \equiv 6.6 \mod 7$.
Como $475^2 \equiv 36 \mod 7$ então 475^2 e 36 têm o mesmo resto na divisão por 7, pelo teorema 4.2.4.
Como $36 = 7.5 + 1$ então $1 = 36 \mod 7$. Assim $1 = 475^2 \mod 7$.

b) Como $1232 = 176.7 + 0$ e $2789 = 398.7 + 3$.
Então $1232 \equiv 0 \mod 7$ e $2789 \equiv 3 \mod 7$. Assim $1232.2789 \equiv 0.3 \mod 7$
Pela teorema anterior, $475 + 1232.2789 \equiv 6 + 0 \mod 7$.
Portanto $475 + 1232.2789$ e 6 têm o mesmo resto na divisão por 7.
Mas o resto de 6 na divisão por 7 é 6.

c) Pela teorema anterior, como $475^2 \equiv 6.6 \mod 7$ temos $475^3 \equiv 6^3 \mod 7$.
Sucessivamente temos $475^4 \equiv 6^4 \mod 7$, $475^5 \equiv 6^5 \mod 7$ e $475^6 \equiv 6^6 \mod 7$.
Como $6^6 = 36.36.36$ então $475^6 \equiv 1.1.1 \mod 7$, pois $36 \equiv 1 \mod 7$.
Assim 475^6 e 1 têm o mesmo resto na divisão por 7. O resto de 1 por 7 é 1.

4.3 Critérios de divisibilidade

Todo $a \in \mathbb{N}$ pode ser escrito como

$$a = a_n.10^n + a_{n-1}.10^{n-1} + \ldots + a_3.10^3 + a_2.10^2 + a_1.10^1 + a_0,$$

onde $a_n \in \{1, \ldots, 9\}$ e $\{a_0, \ldots, a_{n-1}\} \subset \{0, 1, \ldots, 9\}$.

A representação de a na base 10 é $a_n a_{n-1} \ldots a_3 a_2 a_1 a_0$ e os algarismos $a_0, \ldots, a_n$ são chamados de dígitos de a .

Exemplo: 1374 significa $1.10^3 + 3.10^2 + 7.10 + 4$

Alguns critérios de divisibilidade

Teorema 4.3.1. *Considere $a = a_n a_{n-1} \ldots a_2 a_1 a_0$ na sua representação decimal.*
Os seguintes critérios são válidos:

- $3 \mid a$ *se e somente se* $3 \mid a_n + \ldots + a_0$ (3 *divide a soma de seus dígitos*).
- $7 \mid a$ *se e somente se* $7 \mid 2(a_n a_{n-1} \ldots a_2) + a_1 a_0$.
- $11 \mid a$ *se e somente se* $11 \mid a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^n a_n$

Exemplos:

a) Aplicando o critério da divisão por 3 em 1374, temos que

$$3 \mid 1374 \text{ se e somente se } 3 \mid 1 + 3 + 7 + 4 = 15,$$

o que é verdade. Portanto 1374 é múltiplo de 3.

b) Aplicando o critério da divisão por 7 em 1374 temos que

$$7 \mid 1374 \text{ se e somente se } 7 \mid 2.13 + 74 = 100.$$

Aplicando novamente o critério,

$$7 \mid 100 \text{ se e somente se } 7 \mid 2.1 + 0 = 2,$$

o que não é verdade. Portanto 1374 não é múltiplo de 7.

c) Aplicando o critério da divisão por 11 em 1374 temos que

$$11 \mid 1374 \text{ se e somente se } 11 \mid 4 - 7 + 3 - 1 = -1,$$

o que não é verdade. Portanto $11 \nmid 1374$.

Vamos para a demonstração do teorema.

Demonstração. Provaremos mais do que diz o enunciado. Provaremos que $a = a_n a_{n-1} \dots a_3 a_2 a_1 a_0$ tem o mesmo resto que

- $a_n + \dots + a_0$ na divisão por 3,
- que $2(a_n a_{n-1} \dots a_2) + a_1 a_0$ na divisão por 7
- e que $a_0 - a_1 + a_2 - a_3 + \dots + (-1)^n a_n$ na divisão por 11.

Como eles possuem os mesmos restos ou eles são divisíveis ao mesmo tempo (o resto é zero) ou não. Agora, basta provar que

(i) $a \equiv a_n + \dots + a_0 \mod 3$,

(ii) $a \equiv 2(a_n a_{n-1} \dots a_2) + a_1 a_0 \mod 7$ e

(iii) $a \equiv a_0 - a_1 + a_2 - a_3 + \dots + (-1)^n a_n \mod 11$.

Pois isso já garante que eles possuem os mesmos restos pelo teorema 4.2.4.

(i) Vamos provar que $a \equiv a_n + \dots + a_1 + a_0 \mod 3$.

Como $10 \equiv 1 \mod 3$ então, pelo teorema 4.2.7, $\overbrace{10 \dots 10}^{\text{n vezes}} \equiv \overbrace{1 \dots 1}^{\text{n vezes}} \mod 3$.

Assim $10^n \equiv 1 \mod 3$ para qualque $n \in \mathbb{N}$.

Portanto $a_n.10^n + \dots + a_2.10^2 + a_1.10^1 + a_0 \equiv a_n.1 + \dots + a_1.1 + a_0.1 \mod 3$.

Isto é, $a \equiv a_n + \dots + a_0 \mod 3$.

(ii) Vamos provar que $a \equiv 2(a_n a_{n-1} \dots a_2) + a_1 a_0 \mod 7$.

Como $a = a_n.10^n + \dots + a_2.10^2 + a_1.10^1 + a_0$ então $a = (a_n a_{n-1} \dots a_3 a_2).100 + a_1 a_0$.

Como $100 = 2.50$ e $50 \equiv 1 \mod 7$ então $100 \equiv 2 \mod 7$.

Pelo teorema 4.2.7, temos $(a_n a_{n-1} \dots a_3 a_2).100 + a_1 a_0 \equiv (a_n a_{n-1} \dots a_3 a_2).2 + a_1 a_0 \mod 7$.

Assim $a \equiv (a_n a_{n-1} \dots a_3 a_2).2 + a_1 a_0 \mod 7$.

(iii) Vamos provar $a \equiv a_0 - a_1 + a_2 - a_3 + \dots + (-1)^n a_n \mod 11$.

Como $10 \equiv -1 \mod 11$ então, pelo teorema 4.2.7, $\overbrace{10 \dots 10}^{\text{n vezes}} \equiv \overbrace{(-1) \dots (-1)}^{\text{n vezes}} \mod 11$.

Assim $10^n \equiv (-1)^n \mod 11$ para qualquer $n \in \mathbb{N}$.

Portanto $a_n.10^n + \dots + a_2.10^2 + a_1.10^1 + a_0 \equiv a_n.(-1)^n + \dots + a_2.(-1)^2 + a_1.(-1)^1 + a_0 \mod 11$.

Isto é, $a \equiv a_0 - a_1 + a_2 - \dots + (-1)^n a_n \mod 11$.

Isso termina a demonstração do teorema. □

Exercício 4.3.2. *Considere $a = a_n a_{n-1} \dots a_2 a_1 a_0$ na sua representação decimal. Prove os seguintes critérios:*

- $10 \mid a$ *se e somente se* $a_0 = 0$.
- $5 \mid a$ *se e somente se* $a_0 = 0$ *ou* 5.
- $9 \mid a$ *se e somente se* $9 \mid a_0 + a_1 + a_2 + a_3 + \ldots + a_n$.

Exercício 4.3.3. *Sejam $n, m \in \mathbb{Z}$ tais que $n > m > 1$ e $m \mid n$.*

Mostre que se $a \equiv b \mod n$ então $a \equiv b \mod m$.

Exercício 4.3.4. *Seja $n \in \mathbb{Z}$ um número ímpar qualquer. Mostre que*

a) $n \equiv 1 \mod 2$

b) $n \equiv 1 \mod 4$ *ou* $n \equiv 3 \mod 4$

c) $n^2 \equiv 1 \mod 4$

d) $n^2 \equiv 1 \mod 8$

4.4 Teorema fundamental da aritmética

Definição 4.4.1. *Seja p um número natural maior que 1. Dizemos que p é primo se os únicos números naturais que dividem p são 1 e p. Um número natural maior que 1 que não é primo é chamado de composto.*
OBS: Compare essa definição com aquela dada na definição 3.2.5. As duas significam a mesma coisa.

A seguir provaremos um lema que será muito útil. Esse lema também pode ser provado com o teorema 4.5.5 que veremos depois.

Lema 4.4.2. *Seja $p \in \mathbb{N}$ primo e $r \in \{1, \ldots, p-1\}$. Existem $x, y \in \mathbb{Z}$ tais que $xp + yr = 1$.*

Demonstração. Vamos fazer uma indução em r.

Base da Indução: Se $r = 1$ escolho $x = 0$ e $y = 1$. Assim $xp + yr = 0.p + 1.1 = 1$.

Hipótese de Indução: O resultado vale para todos os $r \in \{1, \ldots, m\}$ e $r < p$.

Vamos provar o resultado para $r = m + 1$.

Como queremos o resultado apenas para $r < p$ devemos impor $m + 1 < p$.

Pelo algoritmo de Euclides, $p = a(m + 1) + s$, onde $a \in \mathbb{Z}$ e $s \in \{0, 1, \ldots, m\}$.

Note que se $s = 0$ então $m + 1 \mid p$. Entretando $m + 1 > 1$ e p é primo. Isso não pode ocorrer. Então $s \in \{1, \ldots, m\}$.

Por hipótese de indução, existem $x, y \in \mathbb{Z}$ tais que $xp + ys = 1$.

Substituindo $s = p - a(m + 1)$ na equação acima obtemos $xp + y(p - a(m + 1)) = 1$.

Portanto $(x+y)p+(-ay)(m+1) = 1$, ou seja, o caso $m+1$ é verdadeiro. Terminamos a indução. □

Lema 4.4.3. *Seja $p \in \mathbb{N}$ primo e $q \in \mathbb{Z} \setminus \{0\}$ tal que $p \nmid q$. Então existe $y \in \mathbb{Z}$ tal que*

$$yq \equiv 1 \mod p.$$

Demonstração. Seja r o resto da divisão de q por p.

Por hipótese, $r \neq 0$. Então $r \in \{1, \ldots, p-1\}$.

Pelo lema anterior, existem $x, y \in \mathbb{Z}$ tais que $xp + yr = 1$.

Como $xp \equiv 0 \mod p$ e $yr \equiv yq \mod p$ (por d) do teorema 4.2.2) então

$$0 + yq \equiv 1 \mod p \text{ (pelo teorema 4.2.7).}$$

□

Lema 4.4.4. *Seja $p \in \mathbb{N}$ primo e $a, b \in \mathbb{Z}$ tais que $p \mid ab$. Então $p \mid a$ ou $p \mid b$.*

Demonstração. Suponha por contradição que $p \nmid a$ e $p \nmid b$.

Agora se $p \nmid a$ e $p \nmid b$ então existem $y, x \in \mathbb{Z}$ tais que $ay \equiv 1 \mod p$ e $bx \equiv 1 \mod p$, pelo lema anterior.

Como $p \mid ab$ então $ab \equiv 0 \mod p$.

Pelo teorema 4.2.7, multiplicando os dois lados por $x.y$ obtemos

$$(ya)(bx) \equiv x.y.0 \mod p.$$

Como $ay \equiv 1 \mod p$ e $bx \equiv 1 \mod p$ então $1 \equiv 0 \mod p$.

Isso é contradição, porque $p \nmid 1$.

Para evitar a contradição temos que concluir que $p \mid a$ ou $p \mid b$. □

Exercício 4.4.5. *Seja $p \in \mathbb{N}$ e primo. Sejam $a_1, \ldots, a_n \in \mathbb{Z}$ tais que $p \mid a_1 a_2 \ldots a_n$. Mostre que p divide algum dos a_i.*

Solução: Indução em n. Note que o caso $n = 2$ já foi provado no lema anterior.

Hipótese de Indução: Suponha que o resultado vale para m, isto é,

$$\text{se } p \mid a_1 a_2 \ldots a_m \text{ então } p \text{ divide algum dos } a_i.$$

Agora se $p \mid a_1 a_2 \ldots a_m a_{m+1}$ então $p \mid b a_{m+1}$, onde $b = a_1 a_2 \ldots a_m$

Pelo lema anterior temos que $p \mid b$ ou $p \mid a_{m+1}$.

Se $p \mid a_{m+1}$ então ele divide algum dos a_i.

Se $p \mid b$ então $p \mid a_1 a_2 \ldots a_m$. Por hipótese de indução p divide algum dos a_i. □

Teorema Fundamental da Aritmética

Teorema 4.4.6. *Seja n um número natural maior que 1. Existe apenas uma maneira de escrever n como produto de primos (ou de um único primo), onde os primos estão ordenados nesse produto em ordem não decrescente.*

Exemplos: 100=2.2.5.5, 641=641, 999= 3.3.3.37, 1024=2.2.2.2.2.2.2.2.2.2

Demonstração. Já provamos no teorema 3.2.6 que todo natural $n > 1$ ou é primo ou é produto finito de números primos. Só falta provar que só existe uma maneira de escrevê-lo como produto de primo em ordem não decrescente.

Suponha que n possa ser escrito de duas maneiras como produtos de primos em ordem não decrescente, isto é, $n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l$, onde cada p_i e q_i são primos e $p_1 \leq p_2 \leq \dots \leq p_k$ e $q_1 \leq q_2 \leq \dots \leq q_l$.

Vamos mostrar que a quantidade de primos de cada lado é igual (isto é, $k = l$) e que $p_i = q_i$. Portanto só existe uma maneira de escrevê-lo como produto de primos em ordem não decrescente.

Se $p_1 < q_1$ então $p_1 \nmid q_1$, pois q_1 é primo. Como $p_1 \mid q_1 q_2 \dots q_l$ então ele divide algum q_i, pelo exercício 4.4.5. Como q_i é primo, o único primo que o divide é ele mesmo. Assim $p_1 = q_i$.

Isso é uma contradição, pois $q_1 \leq q_i = p_1 < q_1$. Para evitá-la, $p_1 \geq q_1$.

Se $q_1 < p_1$ então $q_1 \nmid p_1$, pois p_1 é primo. Como $q_1 \mid p_1 p_2 \dots p_k$ então ele divide algum p_i, pelo exercício 4.4.5. Como p_i é primo, o único primo que o divide é ele mesmo. Assim $q_1 = p_i$.

Isso é uma contradição, pois $p_1 \leq p_i = q_1 < p_1$. Para evitá-la, $q_1 \geq p_1$.

Acabamos de provar que $p_1 = q_1$. Dividindo ambos os lados da equação $p_1 p_2 \dots p_k = q_1 q_2 \dots q_l$ por p_1 obtemos $p_2 p_3 \dots p_k = q_2 q_3 \dots q_l$.

Suponha $k < l$. Podemos repetir o argumento que acabamos de usar para provar que $p_2 = q_2$, $p_3 = q_3$, $\dots$, $p_k = q_k$.

Dividindo ambos os lados da equação $p_1 p_2 \dots p_k = q_1 q_2 \dots q_l$ por $p_1 p_2 \dots p_k$ obtemos $1 = q_{k+1} q_{k+2} \dots q_l$.

Então o primo $q_{k+1} \mid 1$. Isso é contradição, pois o único divisor natural de 1 é ele mesmo e um primo é sempre maior que 1. Para evitar a contradição, $k \geq l$.

Suponha $l < k$. Podemos repetir o argumento que acabamos de usar para provar que $p_2 = q_2$, $p_3 = q_3$, $\dots$, $p_l = q_l$.

Dividindo ambos os lados da equação $p_1 p_2 \dots p_k = q_1 q_2 \dots q_l$ por $q_1 q_2 \dots q_l$ obtemos $1 = p_{l+1} p_{l+2} \dots p_k$.

Então o primo $p_{l+1} \mid 1$. Isso é contradição, pois o único divisor natural de 1 é ele mesmo e um primo é sempre maior que 1. Para evitar a contradição, $l \geq k$.

Assim provamos que $k = l$ e $p_i = q_i$ para todo i. □

Veremos agora algumas consequências do teorema fundamental da aritmética.

Corolário 4.4.7. *Se n é um número natural composto então existe um número primo p que o divide tal que $p \leq \sqrt{n}$.*

Exemplo: $4 = 2.2$, onde 2 é primo e $2 \leq \sqrt{4}$.

$6 = 2.3$, onde 2 é primo e $2 \leq \sqrt{6}$.

Demonstração. Como n é composto então $n = p_1 p_2 \dots p_k$, onde cada p_i é primo e pelo menos $k \geq 2$.

Suponha que todos esses primos satisfazem $p_i > \sqrt{n}$. Então $n = p_1 p_2 \dots p_k > (\sqrt{n})^k \geq (\sqrt{n})^2 = n$.

Isso é uma contradição. Para evitá-la deve existir algum $p_i \leq \sqrt{n}$. □

Exercício 4.4.8. *Mostre que 101 é primo.*

Solução: Basta verificar se existe algum número primo menor ou igual a $\sqrt{101}$ que o divide. Se não existir então ele é primo, pelo corolário anterior. Note $\sqrt{101} < \sqrt{121} = 11$. Os primos menores que 11 são $2, 3, 5, 7$. É fácil ver que nenhum deles divide 101. □

Teorema 4.4.9. *Existem infinitos números primos*

OBS: Essa é uma demonstração de 2000 anos atrás. Ela se encontra no livro IX dos Elementos de Euclides.

Demonstração. Suponha que só existam k números primos. Sejam eles $p_1, p_2, \dots, p_k$.

Forme o número $n = p_1 p_2 \dots p_k + 1$.

Pelo teorema fundamental da aritmética existe algum primo que divide n, pois $n > 1$.

Então algum dos $p_1, p_2, \dots, p_k$ divide n. Seja p_i esse primo.

Como $p_i \mid n$ e $p_i \mid p_1 p_2 \dots p_k$ então, pelo corolário 4.0.4, $p_i \mid n - p_1 p_2 \dots p_k$.

Isso é uma contradição, pois $n - p_1 p_2 \dots p_k = 1$ e o único natural que divide 1 é o próprio 1 que não é primo. Para evitar essa contradição devemos concluir que existem infinitos primos. □

Exercício 4.4.10. *Prove os seguintes resultados.*

a) Se os únicos primos que dividem um natural q são da forma $4n + 1$ então q também é da forma $4n + 1$.

DICA: Use congruência mod 4.

b) Mostre que os primos ímpares são da forma $4n+1$ ou $4n-1$.

c) Sejam $q_1, \ldots q_n$ números naturais. Mostre que existe um primo da forma $4n-1$ que divide o número $4q_1, \ldots q_n - 1$.

d) Mostre que existem infnitos primos da forma $4n-1$.

Exercício 4.4.11. *Prove os seguintes resutados.*

a) Se $2^n - 1$ é primo então n é primo.

DICA: $x^n - 1 = (x-1)(1 + x + x^2 + \ldots + x^{n-1})$

b) Seja $n \in \mathbb{N}$. Mostre que os n números consecutivos

$$(n+1)! + 2 \ , \ (n+1)! + 3 \ , \ \ldots \ , \ \ (n+1)! + (n+1)$$

são todos compostos.

Resultados provados sobre primos que não estudaremos aqui

a) Dado qualquer $n \in \mathbb{N}$ existe um primo p satisfazendo $n < p < 2n$.

Esse resultado é chamado de Postulado de Bertrand.

b) Seja $ln(x)$ o logaritmo na base e. Defina $p(m)$ como o quantidade de primos menores ou iguais a m então $\lim_{m\to\infty} p(m)/(m/ln(m)) = 1$.

Isso significa que a quantidade de primos menores ou iguais a m cresce de maneira parecida com a função $m/ln(m)$. Esse teorema é conhecido como "teorema do número primo".

c) Dois primos são ditos consecutivos se não existir nenhum outro primo entre eles. Por exemplo: 3 e 5 são primos consecutivos. Já 7 e 13 não são, pois o 11 está entre eles.

Existem infinitos pares de primos consecutivos cuja diferença deles é menor ou igual a 246.

Esse resultado é chamado de "Bounded gaps between primes".

d) Todo número ímpar maior que 5 é soma de três números primos.

Esse resultado é conhecido como conjectura de Goldbach fraca.

Conjecturas envolvendo primos

Os seguintes resultados não estão provados, mas os matemáticos acreditam que sejam válidos.

a) Pares de primos cuja diferença vale 2 são chamados de primos gêmeos.

Conjectura: Existem infinitos pares de primos gêmeos.

b) Conjectura de Goldbach: Todo número par maior que 2 é soma de dois números primos.

4.5 Máximo divisor comum e mínimo múltiplo comum

Máximo divisor comum

Definição 4.5.1. *Sejam $a, b \in \mathbb{Z}$. O maior número natural que divide ao mesmo tempo a e b é chamado de máximo divisor comum de a e b. Ele será denotado por $mdc(a, b)$.*

***Exemplo**: Os divisores naturais de 2 são 1 e 2. Os divisores naturais de 6 são $1, 2, 3, 6$. Os divisores naturais comuns a 2 e 6 são $1, 2$. O maior deles é $mdc(2, 6) = 2$.*

Definição 4.5.2. *Dizemos que $a, b \in \mathbb{Z}$ são primos entre si ou coprimos se $mdc(a, b) = 1$. Dizemos que $b_1, b_2, \ldots, b_n \in \mathbb{Z}$ são 2 a 2 primos entre si se $mdc(b_i, b_j) = 1$ para quaisquer $i \neq j$.*

O próximo teorema é um resultado fundamental que nos permitirá calcular o máximo divisor comum de dois números de maneira rápida.

Teorema 4.5.3. *Sejam $a, b, q \in \mathbb{N}$ tais que $a = bq + r$, onde $r \in \{0, 1, 2, \ldots, b-1\}$.*

Se $r = 0$ então o $mdc(a, b) = b$. Se $r \neq 0$ então $mdc(a, b) = mdc(b, r)$.

Demonstração. Se $r = 0$ então b divide a. Além disso, b é o maior divisor de si mesmo. Então $mdc(a, b) = b$, pois o $mdc(a, b)$ não pode maior que b.

Seja $r \neq 0$ e s um divisor comum de a e b.

Pelo corolário 4.0.4, s divide $r = a - qb$. Então r é divisor comum de b e r.

Agora seja t um divisor comum de b e r então t divide $a = bq + r$, pelo corolário 4.0.4. Então t é um divisor comum de a e b.

Acabamos de mostrar que os divisores comuns de a e b também são divisores comuns de b e r e vice-versa, ou seja, são os mesmos divisores comuns. Portanto $mdc(a, b) = mdc(b, r)$. □

Método das divisões sucessivas para calcular o máximo divisor comum

Aqui apresentamos um método para calcular o $mdc(a,b)$ para $a,b \in \mathbb{N}$. Ele está baseado no teorema 4.5.3

Começamos dividindo a por b obtendo

$$a = bq_1 + a_1, \text{ onde } 0 \leq a_1 < b.$$

Se o resto $a_1 \neq 0$, dividimos b por a_1 (o divisor e o resto da divisão anterior) obtendo

$$b = a_1q_2 + a_2, \text{ onde } 0 \leq a_2 < a_1.$$

Se o resto $a_2 \neq 0$, dividimos a_1 por a_2 (o divisor e o resto da divisão anterior) obtendo

$$a_1 = a_2q_3 + a_3, \text{ onde } 0 \leq a_3 < a_2.$$

Assim sucessivamente dividindo sempre o divisor pelo resto (da divisão anterior) até obter

$$a_{n-1} = a_nq_{n+1} + 0, \text{ isto é, } a_{n+1} = 0.$$

Isto vai ocorrer porque os restos estão diminuindo

$$a_1 > a_2 > a_3 > \ldots > a_{n+1} \geq 0 \ .$$

Eles se aproximam de zero.

Como a_n divide a_{n-1} e o maior divisor de a_n é ele mesmo então

$$mdc(a_{n-1}, a_n) = a_n.$$

Pelo teorema 4.5.3,

$$mdc(a,b) = mdc(b,a_1) = mdc(a_1,a_2) = mdc(a_2,a_3) = \ldots = mdc(a_{n-1},a_n) = a_n.$$

Exercício 4.5.4. *Encontre o máximo divisor comum dos seguinte números.*

a) $mdc(579, 832)$

b) $mdc(433, 150)$

c) $mdc(3267, 432)$

Solução: *a)*

Divisões	Restos
$832 = 1.579 + 253$	253
$579 = 2.253 + 73$	73
$253 = 3.73 + 34$	34
$73 = 2.34 + 5$	5
$34 = 6.5 + 4$	4
$5 = 1.4 + 1$	1
$4 = 1.4 + 0$	0

Então $mdc(832, 579) = 1$. □

Teorema 4.5.5. *Sejam $a, b \in \mathbb{N}$. Existem $x, y \in \mathbb{Z}$ tais que $xa + yb = mdc(a, b)$.*

Demonstração. Aplique o método das divisões sucessivas para achar o $mdc(a, b)$.

	Divisões	Algoritmo de Euclides	Restos
	a por b	$a = bq_1 + a_1$	$a_1 = a - bq_1$
Se $a_1 \neq 0$	b por a_1	$b = a_1q_2 + a_2$	$a_2 = b - a_1q_2$
Se $a_2 \neq 0$	a_1 por a_2	$a_1 = a_2q_3 + a_3$	$a_3 = a_1 - a_2q_3$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
Se $a_{n-3} \neq 0$	a_{n-4} por a_{n-3}	$a_{n-4} = a_{n-3}q_{n-2} + a_{n-2}$	$a_{n-2} = a_{n-4} - a_{n-3}q_{n-2}$
Se $a_{n-2} \neq 0$	a_{n-3} por a_{n-2}	$a_{n-3} = a_{n-2}q_{n-1} + a_{n-1}$	$a_{n-1} = a_{n-3} - a_{n-2}q_{n-1}$
Se $a_{n-1} \neq 0$	a_{n-2} por a_{n-1}	$a_{n-2} = a_{n-1}q_n + a_n$	$a_n = a_{n-2} - a_{n-1}q_n$
Se $a_n \neq 0$	a_{n-1} por a_n	$a_{n-1} = a_nq_{n+1} + 0$	$a_{n+1} = 0$

Pelo método das divisões sucessivas já sabemos que $mdc(a, b) = a_n$.

Agora temos que encontrar $x, y \in \mathbb{Z}$ tais que $xa + yb = a_n$.

Na equação $a_n = a_{n-2} - a_{n-1}q_n$, você substitui $a_{n-1} = a_{n-3} - a_{n-2}q_{n-1}$, obtendo

$$a_n = a_{n-2} - (a_{n-3} - a_{n-2}q_{n-1})q_n$$

Assim $a_n = (1 + q_{n-1}q_n)a_{n-2} - q_na_{n-3}$.

Depois você substitui $a_{n-2} = a_{n-4} - a_{n-3}q_{n-2}$, obtendo

$$a_n = (1 + q_{n-1}q_n)(a_{n-4} - a_{n-3}q_{n-2}) - q_na_{n-3}.$$

Assim $a_n = (1 + q_{n-1}q_n)a_{n-4} - ((1 + q_{n-1}q_n)q_{n-2} + q_n)a_{n-3}$.

Depois substitua o a_{n-3}, a_{n-4}, ... até obter uma equação para a_n envolvendo a e b.

Na frente do a e do b estarão o x e o y que você quer. □

Exercício 4.5.6. *Encontre $x, y \in \mathbb{Z}$ tais que $x1347 + y234 = mdc(1347, 234)$.*

Solução: Na seguinte tabela se encontram as divisões necessárias para a solução do problema. No lado direito escrevi os restos dependendo dos dividendos e dos divisores. Isso será útil na substituição.

Divisões	Restos
$1347 = 234.5 + 177$	$177 = 1347 - 5.234$
$234 = 177.1 + 57$	$57 = 234 - 177$
$177 = 57.3 + 6$	$6 = 177 - 3.57$
$57 = 6.9 + 3$	$3 = 57 - 9.6$
$6 = 3.2 + 0$	0

Pelo método das divisões sucessivas sabemos que $mdc(1347, 234) = 3$.

Fazendo as substituições:

- $3 = 57 - 9.6 = 57 - 9.\overbrace{(177 - 3.57)}^{\text{Substituí o 6}} = 28.57 - 9.177$
- $3 = 28.\overbrace{(234 - 177)}^{\text{Substituí o 57}} - 9.177 = 28.234 - 37.177$
- $3 = 28.234 - 37.\overbrace{(1347 - 5.234)}^{\text{Substituí o 177}} = 213.234 - 37.1347$

Finalmente encontramos $x = -37$ e $y = 213$. □

Exercício 4.5.7. *Sejam $a, b, y \in \mathbb{N}$ tais que $mdc(a, b) = 1$. Se $a \mid bc$ então $a \mid c$.*

Solução: Existem $x, y \in \mathbb{N}$ tais que $xa + yb = mdc(a, b) = 1$.

Então $xac + ybc = c$.

Por hipótese, $a \mid bc$. Então $a \mid ybc$.

Como $a \mid xac$ e $a \mid ybc$ então $a \mid xac + ybc = c$, pelo item (i) de 4.0.3. □

Exercício 4.5.8. *Sejam $a, b \in \mathbb{N}$. Prove que se $r \in \mathbb{N}$ divide a e b então $mdc(a,b) = r.mdc\left(\frac{a}{r}, \frac{b}{r}\right)$.*

Solução: Provaremos que $mdc(a,b) \leq r.mdc\left(\frac{a}{r}, \frac{b}{r}\right)$ e $r.mdc\left(\frac{a}{r}, \frac{b}{r}\right) \leq mdc(a,b)$.

Portanto eles devem ser iguais.

Primeira parte: $mdc(a,b) \leq r.mdc\left(\frac{a}{r}, \frac{b}{r}\right)$

Sabemos pelo teorema 4.5.5 que existem $x, y \in \mathbb{Z}$ tais que $x\frac{a}{r} + y\frac{b}{r} = mdc\left(\frac{a}{r}, \frac{b}{r}\right)$.

Portanto $xa + yb = r.mdc\left(\frac{a}{r}, \frac{b}{r}\right)$.

Como $mdc(a,b)$ divide a e b então divide $xa + yb$, pelo corolário 4.0.4.

Assim $mdc(a,b)$ divide $r.mdc\left(\frac{a}{r}, \frac{b}{r}\right)$ e, consequentemente, $mdc(a,b) \leq r.mdc\left(\frac{a}{r}, \frac{b}{r}\right)$

Segunda parte: $r.mdc\left(\frac{a}{r}, \frac{b}{r}\right) \leq mdc(a,b)$.

Agora, seja $x = mdc\left(\frac{a}{r}, \frac{b}{r}\right)$.

Então $\frac{a}{r} = xa'$ e $\frac{b}{r} = xb'$, onde $a', b' \in \mathbb{Z}$.

Portanto $a = (rx)a'$ e $b = (rx)b'$.

Isto é, rx divide a e b, mas o maior divisor de a e b é o $mdc(a,b)$.

Assim $r.mdc\left(\frac{a}{r}, \frac{b}{r}\right) \leq mdc(a,b)$. □

Exercício 4.5.9. *Sejam $a, b \in \mathbb{N}$. Utilizando o exercício 4.5.8, prove que*

$$1 = mdc\left(\frac{a}{mdc(a,b)}, \frac{b}{mdc(a,b)}\right).$$

Exercício 4.5.10. *Considere a seguinte fatoração em fatores primos de $a \in \mathbb{N}$ e $b \in \mathbb{N}$*

$$a = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} \quad e \quad b = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k},$$

onde $p_1, p_2, \dots, p_k$ são primos distintos e $\{n_1, n_2, \dots, n_k, m_1, m_2, \dots, m_k\} \subset \{0, 1, 2, 3, \dots\}$.

Utilizando o exercício 4.5.8, mostre que

$$mdc(a,b) = p_1^{\min\{n_1,m_1\}} p_2^{\min\{n_2,m_2\}} \dots p_k^{\min\{n_k,m_k\}} .$$

Mínimo múltiplo comum

Definição 4.5.11. *Sejam $a, b \in \mathbb{N}$. O mínimo múltiplo comum de a e b é o menor natural que é divisível por a e b ao mesmo tempo. Ele será denotado por $mmc(a, b)$.*

***Exemplo**: Os múltiplos naturais de 4 são $4, 8, 12, \ldots$ Os múltiplos naturais de 6 são $6, 12, 18, 24, \ldots$ O menor múltiplo natural comum é $mmc(4, 6) = 12$.*

Teorema 4.5.12. *Sejam $a, b \in \mathbb{N}$. Então* $\dfrac{a.b}{mdc(a,b)} = mmc(a, b)$.

Demonstração. Como $mdc(a, b)$ divide a e b então

$$\frac{a.b}{mdc(a,b)} = a\frac{b}{mdc(a,b)} = b\frac{a}{mdc(a,b)},$$

ou seja, $\dfrac{a.b}{mdc(a,b)}$ é múltiplo de a e de b.

Nosso objetivo é mostrar que ele é o menor deles.

Vou mostrar que $\dfrac{a.b}{mdc(a,b)}$ divide qualquer outro múltiplo comum de a e b.

Portanto é menor que qualquer outro múltiplo comum de a e b.

Seja c um múltiplo comum de a e b então $c = ax = by$, onde $x, y \in \mathbb{N}$.

Então $\dfrac{a}{mdc(a,b)}x = \dfrac{b}{mdc(a,b)}y$. Assim $\dfrac{a}{mdc(a,b)}$ divide $\dfrac{b}{mdc(a,b)}y$.

Como $\dfrac{a}{mdc(a,b)}$ divide $\dfrac{b}{mdc(a,b)}y$ e o $mdc\left(\dfrac{a}{mdc(a,b)}, \dfrac{b}{mdc(a,b)}\right) = 1$ (pelo ex. 4.5.9) .

Assim $\dfrac{a}{mdc(a,b)}$ divide y, pelo exercicio 4.5.7 .

Então $y = \dfrac{a}{mdc(a,b)}z$, onde $z \in \mathbb{N}$. Assim $c = by = \dfrac{ab}{mdc(a,b)}z$, ou seja, $c \geq \dfrac{ab}{mdc(a,b)}$.

□

Exercício 4.5.13. *Considere a seguinte fatoração em fatores primos de $a \in \mathbb{N}$ e $b \in \mathbb{N}$*

$$a = p_1^{n_1}p_2^{n_2}\ldots p_k^{n_k} \quad e \quad b = p_1^{m_1}p_2^{m_2}\ldots p_k^{m_k},$$

onde $p_1, p_2, \ldots, p_k$ são primos distintos e $\{n_1, n_2, \ldots, n_k, m_1, m_2, \ldots, m_k\} \subset \{0, 1, 2, 3, \ldots\}$.

Utilizando o teorema 4.5.12 e o exercício 4.5.10, mostre que

$$mmc(a, b) = p_1^{\max\{n_1,m_1\}}p_2^{\max\{n_2,m_2\}}\ldots p_k^{\max\{n_k,m_k\}} .$$

4.6 Solução do Problema de Frobenius (Curiosidade)

Nesse capítulo mostraremos que os seguintes resultados são válidos para quaisquer dois números naturais a, b primos entre si (isto é, $mdc(a, b) = 1$).

- Não existem números inteiros $r, s \geq 0$ tais que $ra + sb = (a-1)(b-1) - 1$.
- Para todo $n \in \mathbb{N}$ satisfazendo $n \geq (a-1)(b-1)$ existem números inteiros $r, s \geq 0$ tais que $ra + sb = n$.

Portanto a menor postagem que pode ser feita com selos a, b (primos entre si) e que acima dela todas as postagens também podem ser feitas é $(a-1)(b-1)$. Não precisamos mais de indução para resolver esse problema como fizemos na seção de indução forte.

Esse problema de encontrar a menor postagem que a partir dela todas podem ser feitas é conhecido como problema de Frobenius ou problema da moeda.

Precisaremos de alguns lemas. Já provamos resultados parecidos antes.

Lema 4.6.1. *Sejam $a, b \in \mathbb{N}$. Existe $r \in \mathbb{Z}$ tal que $ra \equiv 1 \mod b$ se e somente se $mdc(a, b) = 1$*

Demonstração. Primeira Parte: Se existir tal r então $mdc(a, b) = 1$.

Se $ra \equiv 1 \mod b$ então $ra - 1 = bc$, para algum $c \in \mathbb{Z}$.

Se $z \in \mathbb{N}$ divide a e b então, pelo corolário 4.0.4, temos que $z \mid ra - bc = 1$. Então $z = 1$.

Assim o único divisor natural de a e b é 1. Isto é, $mdc(a, b) = 1$.

Segunda Parte: Se $mdc(a, b) = 1$ então existe $r \in \mathbb{Z}$ tal que $ra \equiv 1 \mod b$.

Existem $r, s \in \mathbb{Z}$ tais que $ra + sb = mdc(a, b) = 1$ pelo teorema 4.5.5.

Como $sb \equiv 0 \mod b$ então $ra + sb \equiv ra \mod b$, pelo teorema 4.2.7. Isto é, $1 \equiv ra \mod b$. □

Lema 4.6.2. *Sejam $i, j \in \{0, 1, \ldots, b-1\}$. Então $i \equiv j \mod b$ se e somente se $i = j$.*

Demonstração. Primeira Parte: Se $i \equiv j \mod b$ então $i = j$.

Como $i, j \in \{0, 1, \ldots, b-1\}$ então $-b < i - j < b$.

Agora como $i \equiv j \mod b$ então $i - j$ é múltiplo de b.

O único múltiplo inteiro de b que é maior que $-b$ e menor que b é zero. Então $i - j = 0$.

Segunda Parte: Se $i = j$ então $i \equiv j \mod b$.

Se $i - j = 0$ então $b \mid i - j$, ou seja, $i \equiv j \mod b$. □

Teorema 4.6.3. *Sejam $a, b \in \mathbb{N}$ tais que $mdc(a, b) = 1$. Não existem números inteiros $r, s \geq 0$ tais que $ra + sb = (a-1)(b-1) - 1$.*

Demonstração. Suponha que existam inteiros $r, s \geq 0$ tais que $ra + sb = (a-1)(b-1) - 1$.

Como $ra \equiv 0 \mod a$ então $ra + sb \equiv sb \mod a$, pelo corolário 4.0.4.

Como $a - 1 \equiv -1 \mod a$ então $(a-1)(b-1) - 1 \equiv (-1)(b-1) - 1 \mod a$, pelo corolário 4.0.4.

Então $sb \equiv -b \mod a \Rightarrow a \mid (sb) - (-b) = b(s+1)$.

Lembre-se que $mdc(a, b) = 1$ e $a \mid b(s+1)$ então $a \mid s+1$, pelo exercício 4.5.7.

Como $s \geq 0$ então $s + 1 > 0$. Como $a \mid s + 1$ então $s + 1 = am$, para algum $m \in \mathbb{N}$ (m não pode ser 0 nem negativo pois $s + 1 > 0$).

Assim $s = am - 1 \geq a - 1$, pois $m \geq 1$.

Então $ra + sb \geq ra + (a-1)b \geq (a-1)b \geq (a-1)(b-1) > (a-1)(b-1) - 1$.

Provamos que $ra + sb \neq (a-1)(b-1) - 1$. Contradição. Para evitá-la devemos concluir que não existem inteiros $r, s \geq 0$ tais que $ra + sb = (a-1)(b-1) - 1$. □

Teorema 4.6.4. *Sejam $a, b \in \mathbb{N}$ tais que $mdc(a, b) = 1$. Para todo $n \in \mathbb{N}$ satisfazendo $n \geq (a-1)(b-1)$ existem números inteiros $r, s \geq 0$ tais que $ra + sb = n$.*

Demonstração. Seja n um natural satisfazendo $n \geq (a-1)(b-1)$.

Considere os seguintes b números inteiros: $n - 0.a,\ n - 1.a,\ n - 2a,\ \ldots,\ n - (b-1).a$.

Observe que

- esses números têm o formato $n - ia$ com $i \in \{0, 1, \ldots, b-1\}$.
- $n - ia \equiv n - ja \mod b$ se e somente se $i = j$, onde $i, j \in \{0, 1, \ldots, b-1\}$.

  Para perceber isso, podemos subtrair n dos dois lados da congruência, pelo corolário 4.0.4, obtendo $-ia \equiv -ja \mod b$.

  Como $mdc(a, b) = 1$ existe um inteiro r tal que $ra \equiv 1 \mod b$, pelo lema 4.6.1. Então $(-r)(-a) \equiv 1 \mod b$.

  Multiplicando $-ia \equiv -ja \mod b$ dos dois lados por $-r$ obtemos $i \equiv j \mod b$.

  Agora pelo lema 4.6.2, $\underline{i \equiv j \mod b}$ se e somente se $\underline{i = j}$, pois $i, j \in \{0, 1, \ldots, b-1\}$.

Pela segunda observação na caixa acima temos que $i \neq j$ significa $n - ia \not\equiv n - ja \mod b$.

Então $n - 0.a,\ n - 1.a,\ n - 2a,\ \ldots,\ n - (b-1).a$ possuem restos diferentes na divisão por b, pelo teorema 4.2.4. Eles possuem então b restos distintos.

Como só existem b restos possíveis na divisão por b então algum desses restos deve ser 0.

Suponha $n - ia = lb$, onde $l \in \mathbb{Z}$.

Agora vamos provar que $l \geq 0$.

Por hipótese, $n \geq (a-1)(b-1)$ então $lb = n - ia \geq (a-1)(b-1) - ia$.

Como $0 \leq i \leq b-1$ e $-a < 0$ então $-ia \geq -(b-1)a$.

Portanto

$$lb = n - ia \geq (a-1)(b-1) - ia \geq (a-1)(b-1) - (b-1)a = -(b-1) > -b.$$

Assim lb é um múltiplo de b maior que $-b$, ou seja, $l \geq 0$.

Conclusão: $n = ia + lb$, onde $i, l \geq 0$. □

Capítulo 5

Relações

Considere a relação entre estudantes e disciplinas: o aluno $\underline{a}$ está matriculado na disciplina $\underline{b}$.

Podemos definir um subconjunto R de $\{\text{alunos}\} \times \{\text{disciplinas}\}$ formado pelos pares (a, b), onde $\underline{a}$ está matriculado na disciplina $\underline{b}$.

Agora podemos fazer o contrário. Dado um $C \subset A \times B$, dizemos que $\underline{a}$ está relacionado com $\underline{b}$ se $(a, b) \in C$. O subconjunto C define uma relação entre elementos de $A \times B$.

Então uma relação entre elementos dos conjuntos A e B define um subconjunto de $A \times B$ e um subconjunto de $A \times B$ define uma relação entre elementos dos conjuntos A e B.

Veja página 519 do livro Matemática Discreta e Aplicações cujo autor é o K.H. Rosen.

Definição 5.0.1. *Sejam A, B conjuntos. Uma relação binária entre elementos de A e B é um subconjunto de $A \times B$. Uma relação no conjunto A é simplesmente uma relação binária entre elementos de A e A, ou seja, um subconjunto de $A \times A$.*

Exemplos: Os seguintes conjuntos são relações em $\mathbb{Z}$.

a) $\mathcal{R}_1 = \{(a, b),\ a \leq b\}$.

b) $\mathcal{R}_2 = \{(a, b),\ a + b \leq 3\}$

c) $\mathcal{R}_3 = \{(a, b),\ a = b + 1\}$

Exercício 5.0.2. *Quantas relações existem em um conjunto A com n elementos?*

5.1 Tipos de Relação

Relação reflexiva

Definição 5.1.1. *Uma relação $\mathcal{R}$ em um conjunto A é dita reflexiva se $(a, a) \in \mathcal{R}$ para todo $a \in A$.*

Exemplos:

1) Seja $A = \{1, 2, 3, 4\}$. Considere as seguintes relações em A.

a) $\mathcal{S}_1 = \{(1,1),\ (1,2),\ (2,1),\ (2,2),\ (3,4),\ (4,1),\ (4,4)\}$.

$\mathcal{S}_1$ não é reflexiva porque falta $(3, 3)$ nela.

b) $\mathcal{S}_2 = \{(1,1),\ (2,2),\ (3,3)\}$.

$\mathcal{S}_2$ não é reflexiva porque falta $(4, 4)$ nela.

c) $\mathcal{S}_3 = \{(1,1),\ (1,2),\ (2,2),\ (3,3),\ (4,4)\}$.

$\mathcal{S}_3$ é reflexiva porque contém todos os possíveis pares (a, a) com $a \in A$.

2) Seja $\mathcal{R} = \{(a, b),\ a \leq b\}$ uma relação em $\mathbb{Z}$.

Ela é reflexiva pois $a \leq a$ e assim $(a, a) \in \mathcal{R}$ para todo $a \in \mathbb{Z}$.

Relação simétrica

Definição 5.1.2. *Uma relação $\mathcal{R}$ em um conjunto A é dita simétrica se para todo $(a, b) \in \mathcal{R}$ temos que $(b, a) \in \mathcal{R}$.*

Exemplos:

1) A relação a é irmão de b no conjunto das pessoas é simétrica.

Pois se a é irmão de b então b é irmão de a.

2) A relação a é pai de b no conjunto das pessoas não é simétrica.

Pois se a é pai de b então b não pode ser pai de a.

Relação anti-simétrica

Definição 5.1.3. *Uma relação $\mathcal{R}$ em um conjunto A é dita anti-simétrica se possuir a seguinte propriedade. Se $(a, b) \in \mathcal{R}$ e $(b, a) \in \mathcal{R}$ então $a = b$.*

Exemplos:

1) A relação $\mathcal{R} = \{(a, b),\ a \leq b\}$ em $\mathbb{Z}$ é anti-simétrica, pois se $a \leq b$ e $b \leq a$ então $a = b$.

2) A relação $\mathcal{R} = \{(a, b),\ a < b\}$ em $\mathbb{Z}$ é anti-simétrica.

Suponha que não seja. Então existem $(a, b) \in \mathcal{R}$ e $(b, a) \in \mathcal{R}$ tais que $a \neq b$.

Mas isso significa que $a < b$ e que $b < a$. Contradição.

Para evitá-la temos que concluir que essa relação é anti-simétrica.

Relação transitiva

Definição 5.1.4. *Uma relação $\mathcal{R}$ em um conjunto A é dita transitiva se possuir a seguinte propriedade. Se $(a, b) \in \mathcal{R}$ e $(b, c) \in \mathcal{R}$ então $(a, c) \in \mathcal{R}$.*

Exemplo:

1) A relação $\mathcal{R} = \{(a, b),\ a \leq b\}$ em $\mathbb{Z}$ é transitiva, pois se $a \leq b$ e $b \leq c$ então $b \leq c$.

Exercício 5.1.5. *Seja A um conjunto não vazio. Mostre que $\emptyset$ é uma relação de $A \times A$ simétrica, anti-simétrica, transitiva, mas não é reflexiva.*

Solução:

É óbvio que vazio não é reflexivo, pois $(a, a) \notin \emptyset$ para todo $a \in A$.

Se $\emptyset$ não fosse simétrico existiria $(a, b) \in \emptyset$ tal que $(b, a) \notin \emptyset$. Contradição.

Se $\emptyset$ não fosse anti-simétrico existiriam $(a, b) \in \emptyset$ e $(b, a) \in \emptyset$ tais que $a \neq b$. Contradição.

Se $\emptyset$ não fosse transitivo existiriam $(a, b) \in \emptyset$ e $(b, c) \in \emptyset$ tais que $(a, c) \notin \emptyset$. Contradição. □

Relação inversa

Definição 5.1.6. *Seja $\mathcal{R}$ uma relação em A. Definimos a relação inversa de $\mathcal{R}$ em A por $\mathcal{R}^{-1} = \{(b, a),\ \text{onde } (a, b) \in \mathcal{R}\}$.*

Função é uma relação

Definição 5.1.7. *Seja $\mathcal{R}$ uma relação em A tal que para cada $a \in A$ existe um único $(a, b) \in \mathcal{R}$. Chamamos essa relação de função.*

Exercício 5.1.8. *Utilizando a ideia de relação, defina função injetora, sobrejetora e bijetora.*

Exercício 5.1.9. *Mostre que se uma relação $\mathcal{R}$ é uma função bijetora então a relação inversa é a sua função inversa.*

Já vimos anteriormente que a relação $\{(1,1),\ (2,2),\ (3,3)\}$ no conjunto $\{1,2,3,4\}$ não é reflexiva, mas se incluirmos $(4,4)$ ela se torna reflexiva.

A ideia de fecho da relação é de acrescentar pares a uma relação até obter a propriedade desejada.

Fecho reflexivo

Definição 5.1.10. *Seja $\mathcal{R}$ uma relação em A. O fecho reflexivo de $\mathcal{R}$ em A é o conjunto $\mathcal{R} \cup \{(a,a), a \in A\}$.*

Exercício 5.1.11. *Mostre que o fecho reflexivo da relação $\mathcal{R}$ em A é reflexivo.*

Fecho simétrico

Definição 5.1.12. *Seja $\mathcal{R}$ uma relação em A. O fecho simétrico de $\mathcal{R}$ em A é o conjunto $\mathcal{R} \cup \mathcal{R}^{-1}$.*

Exercício 5.1.13. *Mostre que o fecho simétrico da relação $\mathcal{R}$ em A é simétrico.*

5.2 Relações de Equivalência

Relação de equivalência

Definição 5.2.1. *Uma relação em A é chamada de relação de equivalência se for reflexiva, simétrica e transitiva.*

Exemplos:

1) Seja $A = \{\text{pessoas}\}$ e a relação $\mathcal{R} = \{(a,b), a \text{ mora na mesma cidade de } b\}$.

   a) Note que toda pessoa a mora na mesma cidade de a. Portanto $(a,a) \in \mathcal{R}$ para todo $a \in A$, ou seja, $\mathcal{R}$ é reflexiva.

   b) Note que se $(a,b) \in \mathcal{R}$ então a mora na mesma cidade de b e portanto b mora na mesma de a. Assim $(b,a) \in \mathcal{R}$, para todo $(a,b) \in \mathcal{R}$, ou seja, $\mathcal{R}$ é simétrica.

c) Note que se $(a,b) \in \mathcal{R}$ e $(b,c) \in \mathcal{R}$ então a, b e c moram na mesma cidade então $(a,c) \in \mathcal{R}$.

Portanto $\mathcal{R}$ é transitiva.

Conclusão: $\mathcal{R}$ é relação de equivalência.

Exemplo Importante

2) Seja n um número natural. Considere a relação $\mathcal{R} = \{(a,b), a \equiv b \mod n\}$ em $\mathbb{Z}$.

Os itens a), b) e c) do teorema 4.2.2 dizem que $\mathcal{R}$ é relação de equivalência.

Definição 5.2.2. *Seja $\mathcal{R}$ uma relação de equivalência em A. Se $(a,b) \in \mathcal{R}$ dizemos que a e b são equivalentes. Normalmente denotamos isso por $a \sim_{\mathcal{R}} b$, ou simplesmente, $a \sim b$ quando a relação $\mathcal{R}$ estiver subentendida.*

Classes de equivalência

Definição 5.2.3. *Seja $\mathcal{R}$ uma relação de equivalência em A e $a \in A$. O conjunto de todos os elementos de A equivalentes a $\underline{a}$ é chamado de classe de equivalência de $\underline{a}$. Ele será denotado por $[a]_{\mathcal{R}}$, ou simplesmente $[a]$, se a relação estiver subentendida.*
Assim $[a]_{\mathcal{R}} = \{b \in A,$ tal que $(a,b) \in \mathcal{R}\}$.

Exemplo: As classes de congruência módulo m da definição 4.2.6 são simplesmente as classes de equivalência da relação $\mathcal{R} = \{(a,b), a \equiv b \mod m\}$ em $\mathbb{Z}$.

Exercício 5.2.4. *Seja $\mathcal{R}$ uma relação de equivalência em A. Sejam $a \sim_{\mathcal{R}} c$ então $[a]_{\mathcal{R}} = [c]_{\mathcal{R}}$.*
OBS: Em outras palavras, qualquer elemento da classe $[a]_{\mathcal{R}}$ pode representar a classe inteira, pois $[a]_{\mathcal{R}} = [c]_{\mathcal{R}}$.

Solução: Seja $b \in [a]_{\mathcal{R}}$. Então $(a,b) \in \mathcal{R}$.

Como $c \in [a]_{\mathcal{R}}$ também então $(a,c) \in \mathcal{R}$.

Por $\mathcal{R}$ ser simétrica, $(c,a) \in \mathcal{R}$.

Como $(c,a) \in \mathcal{R}$, $(a,b) \in \mathcal{R}$ e $\mathcal{R}$ é transitiva temos $(c,b) \in \mathcal{R}$.

Acabamos de provar $c \sim_{\mathcal{R}} b$, isto é, $b \in [c]_{\mathcal{R}}$.

Assim $[a]_{\mathcal{R}} \subset [c]_{\mathcal{R}}$.

Agora provar que $[c]_{\mathcal{R}} \subset [a]_{\mathcal{R}}$ é a mesma demonstração. $\square$.

Exercício 5.2.5. *Seja $\mathcal{R}$ uma relação de equivalência em A. Se $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} \neq \emptyset$ então $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$.*

Solução: Se $c \in [a]_{\mathcal{R}} \cap [b]_{\mathcal{R}}$ então, pelo exercício anterior, $[a]_{\mathcal{R}} = [c]_{\mathcal{R}}$ e $[b]_{\mathcal{R}} = [c]_{\mathcal{R}}$. Assim $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$. □

Observação 5.2.6. *O exercício anterior diz que ou as classes de equivalência são iguais ou a interseção delas é vazia. Portanto uma relação de equivalência divide um conjunto em subconjuntos disjuntos. Quais são eles? Resposta: As classes de equivalência.*

Exercício 5.2.7. *Quais das seguintes relações no conjunto de pessoas são de equivalência?*

a) $\{(a, b),$ *a e b têm a mesma idade*$\}$

b) $\{(a, b),$ *a e b têm os mesmos pais*$\}$

c) $\{(a, b),$ *a e b têm um progenitor em comum*$\}$

d) $\{(a, b),$ *a e b já se encontraram*$\}$

e) $\{(a, b),$ *a e b falam a mesma língua*$\}$

Exercício 5.2.8. *Seja $f : A \to B$. Considere a seguinte relação $\mathcal{R}$ em A,*

$$\mathcal{R} = \{(a_1, a_2),\ \textit{tal que } f(a_1) = f(a_2)\}.$$

a) Mostre que $\mathcal{R}$ é uma relação de equivalência em A.

b) Quais são as classes de equivalência?

Exercício 5.2.9. *Seja r uma reta no plano. Considere a seguinte relação entre pontos no plano.*

$$\mathcal{R} = \{(a, b),\ a \textit{ e } b \textit{ pertencem a uma reta paralela a } r\}.$$

a) Mostre que $\mathcal{R}$ é uma relação de equivalência no plano.

b) Quais são as classes de equivalência?

Capítulo 6

Análise Combinatória

Combinatória é uma área muito importante da matemática discreta. Ela é dedicada inteiramente a calcular o número de possibilidade de uma certa situação ocorrer. Isso é importantíssimo em cálculo de probabilidades.

Uma situação interessante a computação, cuja combinatória é extremamente necessária é no cálculo de número de operações de um algoritmo para determinar sua complexidade. Outra parte da análise combinatória chamada teoria de grafos também é importantíssima a computação.

Veja a página 335 do livro Matemática Discreta e Aplicações cujo autor é o K.H. Rosen.

6.1 Regras de Contagem

Duas perguntas típicas de análise combinatória são:

- Quantas sequências de 7 bits existem?
- Quantas funções injetoras existem entre um domínio de cardinalidade m e um contra-domínio de cardinalidade n?

Existem duas regras básicas de contagem: A regra do produto e a regra da soma.

Regra do produto

Suponha que um procedimento posso ser divido em uma sequência de duas etapas. Na primeira etapa existem n_1 maneiras de ser realizada e para cada uma dessas existem n_2 maneiras de realizar a segunda etapa. Então existem $n_1.n_2$ maneiras de realizar a tarefa.

OBS: É claro que não precisa ser apenas 2 etapas. Podem ser k etapas, onde existem n_1 formas

de realizar a primeira, e para cada uma dessas existem n_2 maneiras de realizar a segunda, ..., e para cada uma dessas existem n_k de realizar a $k^{\underline{a}}$ etapa. Então há $n_1 n_2 \dots n_k$ maneiras de realizar a tarefa.

Exemplos:

1) Para escrever todos as sequências de 7 bits, precisamos dividir essa tarefa em 7 etapas e em cada etapa devemos escrever 0 ou 1.

Para a primeira etapa existem 2 possibilidades de escolha: $0, 1$

Para a segunda etapa existem 2 possibilidades de escolha: $0, 1$

$\vdots$

Para a sétima etapa existem 2 possibilidades de escolha: $0, 1$

Então essa tarefa pode ser realizada de 2^7 maneiras. Portanto existem 2^7 sequências de 7 bits.

2) Seja A um conjunto de cardinalidade m e B um conjunto de cardinalidade n.

Queremos descobrir quantas funções injetoras $f : A \to B$ existem.

Primeiro já sabemos que se $f : A \to B$ é injetora então $m \leq n$.

Escreva $A = \{a_1, a_2, \dots, a_m\}$.

Para construir um $f : A \to B$ injetora precisamos dividir esse trabalhao em m etapas.

Etapa 1: Definir $f(a_1)$.

Etapa 2: Definir $f(a_2)$, onde $f(a_2) \neq f(a_1)$.

Etapa 3: Definir $f(a_3)$, onde $f(a_3) \neq f(a_2)$ e $f(a_3) \neq f(a_1)$.

$\vdots$

Etapa m: Definir $f(a_m)$, onde $f(a_m) \neq f(a_{m-1})$, $f(a_m) \neq f(a_{m-2})$, ..., $f(a_m) \neq f(a_1)$.

• Para a etapa 1 existem n maneiras de fazê-la.

• Para a etapa 2 existem $n - 1$ maneiras de fazê-la.

(já escolhemos a imagem $f(a_1)$ e não podemos repetí-la pois f é injetora).

• Para a etapa 3 existem $n - 2$ maneiras de fazê-la.

(já escolhemos as imagens $f(a_1), f(a_2)$e não podemos repetí-las pois f é injetora).

$\vdots$

• Para a etapa m existem $n - (m - 1)$ maneiras de fazê-la.

(já escolhemos as imagens $f(a_1), f(a_2), \dots, f(a_{m-1})$ não podemos repetí-las pois f é injetora).

Total de funções injetoras: $n(n-1)(n-2)\dots(n-(m-1))$

Regra da soma

Se uma tarefa puder ser realizada de n_1 formas ou de n_2 formas, onde nenhuma das n_1 primeiras é igual a nenhuma da n_2 outras, então existem $n_1 + n_2$ formas de realizar a tarefa.

Exemplo: Se temos que escolher um aluno (entre n_1 alunos) ou uma aluna (entre n_2 alunas) para ser o representante de classe então o total de maneiras de fazer essa escolha é $n_1 + n_2$.

OBS: É claro que existe a regra de soma mais geral: Se existem $A_1, A_2, \ldots, A_n$ conjuntos disjuntos de maneiras de realizar uma tarefa então o total de possibilidades de realizá-la é $\#A_1 + \ldots + \#A_n$.

As regras do produto e da soma descrevem os seguintes resultados de teoria de conjuntos.
Regra do produto: $\#A_1 \times \ldots \times A_n = \#A_1 \ldots \#A_n$
Regra da soma: $\#A_1 \cup \ldots \cup A_n = \#A_1 + \ldots + \#A_n$, quando $A_i \cap A_j = \emptyset$ para todo $i \neq j$.

Exemplo: Quantas sequências de 8 bits começam com 10 ou 01?

Solução:

$A_1 = \{$sequências de 8 bits começando com 10$\}$ e $A_2 = \{$sequências de 8 bits começando com 01$\}$

A pergunta pede $\#A_1 \cup A_2$. Note que $A_1 \cap A_2 = \emptyset$.

Pela regra da soma $\#A_1 \cup A_2 = \#A_1 + \#A_2$. Vamos calcular $\#A_1$ e de $\#A_2$.

Tarefa: Construir A_1

$A_1 = \Big\{1\ 0\ \boxed{0/1}\ \boxed{0/1}\ \boxed{0/1}\ \boxed{0/1}\ \boxed{0/1}\ \boxed{0/1}\Big\}$

Temos 6 etapas, 2 possibilidades em cada.

Total: 2^6

Tarefa: Construir A_2

$A_2 = \Big\{0\ 1\ \boxed{0/1}\ \boxed{0/1}\ \boxed{0/1}\ \boxed{0/1}\ \boxed{0/1}\ \boxed{0/1}\Big\}$

Temos 6 etapas, 2 possibilidades em cada.

Total: 2^6

Resposta para pergunta: 2^6+2^6.

As aplicações diretas das regras do produto e da soma são bem simples. Como vimos acima a regra da soma está sempre associada a cardinalidade da união de conjuntos disjuntos. Entretanto se não forem disjuntos precisamos mais do que regra da soma, precisamos do princípio da inclusão-exclusão.

Vimos no princípo da inclusão-exclusão (teorema 1.2.16) que para conjuntos A_1,A_2 temos

$$\#(A_1 \cup A_2) = \#A_1 + \#A_2 - \#(A_1 \cap A_2).$$

Esse teorema é muito útil para contar.

Exemplo: Quantas sequências de 8 bits começam com 1 ou terminam com 0?

Solução:

$A_1 = \{$sequências de 8 bits começando com 1$\}$ e $A_2 = \{$sequências de 8 bits terminando com 0$\}$

A pergunta pede $\#A_1 \cup A_2$.

Note que $A_1 \cap A_2 = \{$sequências de 8 bits começando com 1 e terminando com 0$\}$.

Pelo princípo da inclusão-exclusão, $\#(A_1 \cup A_2) = \#A_1 + \#A_2 - \#(A_1 \cap A_2)$.

Vamos calcular $\#A_1$, $\#A_2$ e $\#(A_1 \cap A_2)$.

Tarefa: Construir A_1

$A_1 = \Big\{1 \boxed{0/1} \boxed{0/1} \boxed{0/1} \boxed{0/1} \boxed{0/1} \boxed{0/1} \boxed{0/1}\Big\}$

Temos 7 etapas, 2 possibilidade em cada.

Total: 2^7

Tarefa: Construir A_2

$A_2 = \Big\{\boxed{0/1} \boxed{0/1} \boxed{0/1} \boxed{0/1} \boxed{0/1} \boxed{0/1} \boxed{0/1} 0\Big\}$

Temos 6 etapas, 2 possibilidade em cada.

Total: 2^7

Tarefa: Construir $A_1 \cap A_2$

$A_1 \cap A_2 = \Big\{1 \boxed{0/1} \boxed{0/1} \boxed{0/1} \boxed{0/1} \boxed{0/1} \boxed{0/1} 0\Big\}$

Temos 6 etapas, 2 possibilidade em cada.

Total: 2^6

Resposta para pergunta: 2^7+$2^7 - 2^6$.

Exercício 6.1.1. *Como fica o princípio da inclusão-exclusão com 3 conjuntos? Isto é, em geral quanto vale $\#(A_1 \cup A_2 \cup A_3)$?*

Solução: Como $A_1 \cup A_2 \cup A_3 = (A1 \cup A_2) \cup A_3$, pelo teorema 1.2.16, temos

$$\begin{aligned}\#(A_1 \cup A_2) \cup A_3 &= \#(A_1 \cup A_2) + \#A_3 - \#(A_1 \cup A_2) \cap A_3 \\ &= \#A_1 + \#A_2 - \#(A_1 \cap A_2) + \#A_3 - \#(A_1 \cup A_2) \cap A_3 \\ &= \#A_1 + \#A_2 + \#A_3 - \#(A_1 \cap A_2) - \#(A_1 \cup A_2) \cap A_3.\end{aligned}$$

Pelo exercício 1.2.14.m, $(A_1 \cup A_2) \cap A_3 = (A_1 \cap A_3) \cup (A_2 \cap A_3)$

Novamente, pelo teorema 1.2.16, temos

$$\#(A_1 \cap A_3) \cup (A_2 \cap A_3) = \#(A_1 \cap A_3) + \#(A_2 \cap A_3) - \#(A_1 \cap A_3) \cap (A_2 \cap A_3)$$

Note que $(A_1 \cap A_3) \cap (A_2 \cap A_3) = A_1 \cap A_2 \cap A_3$.

Portanto a fórmula final fica

$$\#(A_1 \cup A_2 \cup A_3) =$$
$$= \#A_1 + \#A_2 + \#A_3 - \#(A_1 \cap A_2) - \#(A_1 \cap A_3) - \#(A_2 \cap A_3) + \#(A_1 \cap A_2 \cap A_3). \square$$

Fórmula geral do princípio inclusão-exclusão

Teorema 6.1.2. *Sejam $A_1, \ldots, A_n$ conjuntos. Então $\#(A_1 \cup \ldots \cup A_n) =$*

$$= \sum_{1 \leq i \leq n} \#A_i - \sum_{\substack{1 \leq i,j \leq m \\ i \neq j}} \#(A_i \cap A_j) + \sum_{\substack{1 \leq i,j,k \leq m \\ i,j,k \text{ distintos}}} \#(A_i \cap A_j \cap A_k) - \ldots + (-1)^{n+1} \#(A_1 \cap \ldots \cap A_n)$$

Demonstração. Deixo como exercício. Faça uma indução em n, use o teorema 1.2.16 para base da indução e use também que $A_1 \cup \ldots \cup A_m \cup A_{m+1} = (A_1 \cup \ldots \cup A_m) \cup A_{m+1}$. $\square$

Exercício 6.1.3. *a) Uma determinada marca de camisetas têm 12 cores, têm opções masculina e feminina e três tamanhos para cada sexo. Quantas camisetas distintas são fabricadas? Justifique sua resposta.*

b) Há 4 estradas principais de Boston a Detroit e 6 de Detroit a Los Angeles. Quantas estradas há para o percurso Boston-Los Angeles via Detroit? Justifique sua resposta.

Exercício 6.1.4. *Quantos números inteiros existem no conjunto* $\{100, 101, \ldots, 999\}$

a) que são divisíveis por 7?

b) que são ímpares?

c) que são divisíveis por 7 ou 11?

d) que são divisíveis por 7 e 11?

e) que não são divisíveis nem por 7 e nem 11?

f) que possuem dígitos distintos?

g) que possuem dígitos distintos e são pares?

6.2 Princípio da Casa dos Pombos

32 pessoas não podem fazer aniversário em dias diferentes do mês pois isso implicaria que algum mês tem 32 dias. Então existem pelo menos duas pessoas fazendo aniversário no mesmo dia entre essas 32 pessoas.

Essa ideia de separar objetos em um número menor de casos é a ideia por trás do princípio das casa dos pombos. Os objetos seriam os pombos e os casos seriam as casas dos pombos.

Princípio da casa dos pombos

Se existem $k+1$ objetos a serem distribídos em k caixas então existe uma caixa com pelo menos 2 objetos.

Esse resultado é uma ideia bem simples, mas muito útil. Ele é utilizado em diversas situações. Veremos algumas muito interessantes abaixo.

Exercício 6.2.1. *Se a quantidade de pessoas em uma festa é maior ou igual a 2, mostre que existem pelo menos 2 pessoas que conhecem a mesma quantidade de pessoas da festa.*

Solução do 6.2.1: A prova vai ser por indução no número de pessoas da festa.

Base da Indução: A festa tem duas pessoas.

Nesse caso ou ela se conhecem e cada uma conhece 1 pessoa da festa ou elas não se conhecem, ou seja, elas conhecem 0 pessoas da festa. Provamos a base.

Hip. de Indução: O resultado vale para um festa com k pessoas onde $2 \leq k \leq m$.

Vamos provar o resultado para uma festa com $m+1$ pessoas.

Se existir alguém da festa que não conhece ninguém as outras m pessoas não conhecem ela. Portanto dentre essas m pessoas existem 2 que conhecem a mesma quantidade de pessoas nessas m pessoas por hipótese de indução.

Agora se todo mundo na festa conhece alguém então o número de conhecidos de cada pessoa varia de 1 até m.

Formo a primeira caixa com as pessoas que só conhecem 1 pessoa, a segunda caixa com as pessoas que conhecem 2 pessoas, ..., a caixa m com as pessoas que conhecem m pessoas. Mas agora temos $m+1$ pessoas distribuídas em m caixas, ou seja, existem 2 na mesma caixa. □

Considere agora as seguintes perguntas.

Pergunta 1: E se eu quisesse uma caixa com pelo menos 5 objetos, qual o número mínimo de objetos que eu teria que distribuir entre as 7 caixas?

Solução: Podemos pensar no pior caso, todas as 7 caixas com 4 objetos. Ainda não temos o que queremos, mas se acrescentarmos 1 objeto então alguma das caixas vai ter 5.

A resposta então é $7.4 + 1 = 29$.

Pergunta 2: Suponha que as possíveis notas de uma prova são A, B, C, D, E. Qual o número mínimo de estudantes que devem fazê-la para termos pelo menos 6 deles com a mesma nota?

Solução: Podemos pensar no pior caso: 5 estudantes com nota A, 5 estudantes com nota B, 5 estudantes com nota C, 5 estudantes com nota D e 5 estudantes com nota E. Ainda não temos o que queremos, mas se acrescentarmos 1 estudante então alguma nota vai ser de 6 estudantes.

A resposta então é $5.5 + 1 = 26$.

A ideia por trás dessas perguntas é o princípio generalizado da casa dos pombos. Antes de enunciá-lo necessitamos a definição da função teto.

Definição 6.2.2. *Seja $x \in \mathbb{R}$. Define-se o teto de x por $\lceil x \rceil = \min\{n \in \mathbb{Z}, n \geq x\}$.*
Isto é, $\lceil x \rceil$ é o menor inteiro que é maior ou igual a x.

Exemplos: $\lceil 3.123 \rceil = 4$, $\left\lceil \frac{1}{2} \right\rceil = 1$ e $\lceil 3 \rceil = 3$.

Princípio generalizado da casa dos pombos

Se n objetos forem distribuídos em k caixas então existe pelo menos uma caixa contendo $\left\lceil \frac{n}{k} \right\rceil$ objetos.

Exemplos: *a*) Em um grupo de 100 pessoas existem pelo menos $\lceil 100/12 \rceil = \lceil 8.333\ldots \rceil = 9$ pessoas que fazem aniversário no mesmo mês.

b) Na pergunta 1 acima, necessitamos de n objetos tal que $\frac{n}{7}$ é um pouco maior que 4 para garantir que $\left\lceil \frac{n}{7} \right\rceil = 5$. Mas o menor n que faz isso é o $n = 7.4 + 1$.

c) Na pergunta 2 acima, necessitamos de n estudantes tal que $\frac{n}{5}$ é um pouco maior que 5 para garantir que $\left\lceil \frac{n}{5} \right\rceil = 6$. Mas o menor n que faz isso é o $n = 5.5 + 1$.

Exercício 6.2.3. *a) Se em uma sala há 30 estudantes, mostre que existem pelo menos 2 cujos os nomes começam com a mesma letra.*

b) Mostre que em um conjunto de 5 números inteiros existem pelo menos dois com o mesmo resto na divisão por 4*.*

c) Quantos números devem ser selecionados de $\{1, 2, 3, 4, 5, 6\}$ *para garantir que a soma de dois deles dê 7?*

Solução do 6.2.3.*c*). Os pares de números de $\{1, 2, 3, 4, 5, 6\}$ cuja soma dão 7 são: $(1, 6)$, $(2, 5)$ e $(3, 4)$.

Aqui temos três caixas nomeadas por $(1, 6)$, $(2, 5)$ e $(3, 4)$.

Nelas você coloca os números que você pegou do conjunto $\{1, 2, 3, 4, 5, 6\}$. Por exemplo, se você pegou 1 ou 6, você deve colocá-los na primeira caixa.

O que queremos garantir é que vamos ter uma caixa com os dois números.

Basta escolher 4 números de $\{1, 2, 3, 4, 5, 6\}$ para isso ocorrer.

Exercício 6.2.4. *Seja* $f : A \to B$ *uma função tal que* $\#B < \#A$*. Mostre que existe um elemento* $b \in B$ *tal que*

$$\#f^{-1}(\{b\}) \geq \left\lceil \frac{\#A}{\#B} \right\rceil.$$

6.3 Aplicações do princípio da casa dos pombos (Curiosidade)

Agora vou mostrar duas aplicações muito interessantes desses dois princípios.

Definição 6.3.1. *Sejam $a_1, a_2, \ldots, a_n$ uma sequência de números reais. Uma subsequência desta sequência é uma sequência da forma $a_{i_1}, a_{i_2}, \ldots, a_{i_m}$, onde $1 \leq i_1 < i_2 < \ldots < i_m \leq n$.*

Isto é, uma subsequência é uma sequência utilizando alguns termos da sequência original respeitando a ordem que eles aparecem.

Exemplo: 1,2,3,4,5,6 é uma sequência. 2,4,6 é um subsequência dela, mas 1,5,3 não é. A ordem dos números deve ser respeitada.

Definição 6.3.2. *Dizemos que uma sequência de números $a_1, a_2, \ldots, a_n$ é*

- *estritamente crescente se $a_1 < a_2 < a_3 < \ldots < a_n$*
- *estritamente decrescente se $a_1 > a_2 > a_3 > \ldots > a_n$*

Primeira aplicação

Teorema 6.3.3. *Toda sequência de $n^2 + 1$ números reais **distintos** contém um subsequência estritamente crescente ou estritamente decrescente com $n + 1$ números.*

Exemplo: A sequência 8, 11, 9, 1, 4, 6, 12, 10, 5, 7 possui $3^2 + 1$ números.
Note que 1, 4, 6, 7 é uma subsequência estritamente crescente com 3+1 números.

Demonstração. Sejam $a_1, a_2, \ldots, a_{n^2+1}$ a sequência de números distintos.

Para cada número a_k considere o par (c_k, d_k), onde

- c_k é o tamanho da maior subsequência estritamente crescente que começa com a_k

  No exemplo acima, a maior subsequência estritamente crescente que começa com $a_2 = 11$ é 11, 12. Assim o seu tamanho é 2. Portanto $c_2 = 2$.

- e d_k o tamanho da maior subsequência estritamente decrescente que começa com a_k.

  No exemplo acima, a maior subsequência estritamente decrescente que começa com $a_2 = 11$ é 11, 9, 6, 5. Assim o seu tamanho é 4. Portanto $d_2 = 4$.

Suponha que o tamanho de todas as subsequências estritamente crescentes e decrescentes não ultrapasse n.

Então $(c_k, d_k) \in \{1, \ldots, n\} \times \{1, \ldots, n\}$ para todo $k = 1, \ldots, n^2 + 1$.

Porém $\#\{1, \ldots, n\} \times \{1, \ldots, n\} = n^2$.

Como temos $n^2 + 1$ pares entre n^2 pares possíveis, existirão 2 pares iguais.

Sejam eles $(c_s, d_s) = (c_t, d_t)$ com $s < t$.

Lembre-se que $a_s \neq a_t$ (todos da sequência são diferentes).

Então temos duas possibilidades $a_s < a_t$ ou $a_t < a_s$.

Primeiro Caso: $a_s < a_t$

Pela definição de c_t, existe uma subsequência estritamente crescente começando em a_t de tamanho c_t.

Coloque a_s na frente dessa subsequência, como $s < t$ e $a_s < a_t$ obtemos uma subsequência estritamente crescente de tamanho $c_t + 1$.

Como $c_t = c_s$ obtemos uma subsequência estritamente crescente começando em a_s de tamanho $c_s + 1$. Isso é contradição. Por definição o maior tamanho possível para uma subsequência desse tipo é o número c_s. Não pode existir uma maior.

Segundo Caso: $a_t < a_s$

Pela definição de d_t, existe uma subsequência estritamente decrescente começando em a_t de tamanho d_t.

Coloque a_s na frente dessa subsequência, como $s < t$ e $a_s > a_t$ obtemos uma subsequência estritamente decrescente de tamanho $d_t + 1$.

Como $d_t = d_s$ obtemos uma subsequência estritamente decrescente começando em a_s de tamanho $d_s + 1$. Isso é contradição. Por definição o maior tamanho possível para uma subsequência desse tipo é o número d_s. Não pode existir uma maior.

Como é possível que ambos os caso gere contradição? Erramos antes, ao dizer que não existe uma subsequência estritamente crescente ou decrescente de tamanho $n + 1$. Portanto para evitar a contradição, ela deve existir. □

Esse resultado mostra como o princípio da casa dos pombos é importante para provar propriedades sobre conjuntos se a quantidade de elementos for suficientemente grande.

Essa é a área da combinatória chamada teoria de Ramsey.

Segunda aplicação

Teorema 6.3.4. *Considere 6 pontos do plano, onde não existem 3 deles na mesma reta, ou seja, estão bem espalhados. Conecte todos esses 6 pontos entre si com segmentos vermelhos ou azuis. Não importa como esses 6 pontos são ligados entre si com segmentos de reta vermelhos ou azuis sempre haverá um triângulo azul ou vermelho cujos vértices são três desses pontos.*

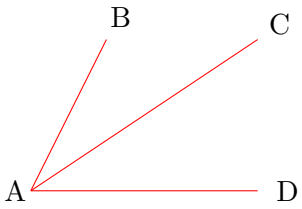


Figura 1.

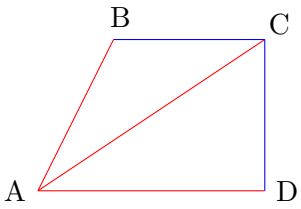


Figura 2.

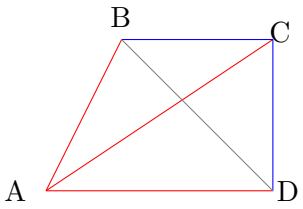


Figura 3.

Demonstração. Chame os 6 pontos de A, B, C, D, E, F.

Temos que ligar todos eles entre si entre si usando apenas segmentos vermelhos ou azuis.

Quando ligarmos o ponto A ao outros 5 pontos B, C, D, E, F usando segmentos vermelhos ou azuis, vão existir pelo menos $\left\lceil \frac{5}{2} \right\rceil = 3$ segmentos com a mesma cor, pelo princípo generalizado da casa dos pombos.

Só pra facilitar suponha que sejam 3 vermelhos: $\overline{AB}, \overline{AC}, \overline{AD}$ como na figura 1.

Agora temos que ligar BC e CD usando segmentos vermelhos ou azuis. Se usarmos vermelho em qualquer um dos dois então já obtemos um triângulo vermelho ($\triangle ABC$ ou $\triangle ACD$).

Então usemos azuis nos dois como na figura 2.

Agora temos que ligar BD usando um segmento vermelho ou azul. Note que se escolhermos vermelho formamos o triângulo vermelho $\triangle ABD$ e se escolhermos azul formamos o triângulo azul $\triangle BCD$.

Não há escapatória, sempre haverá um triângulo de mesma cor cujos vértices são três desses pontos. □

6.4 Permutações e Combinações

Considere as seguintes perguntas:

- De quantas maneiras diferentes podemos escolher 3 atletas em um conjunto de 5 atletas?
- Quantas pódios formados por 3 atletas escolhidos em um conjunto de 5 atletas existem ?

Note que se os atletas no pódio mudarem de posição teremos um novo pódio, isto é, a ordem na segunda questão importa, enquanto que na primeira não.

Matematicamente podemos representar essa diferença por

$$\{\text{atleta } 1, \text{atleta } 2, \text{atleta } 3\} \text{ versus } (\text{atleta } 1, \text{atleta } 2, \text{atleta } 3).$$

No segundo caso estamos arrumando os atletas em uma tripla ordenada.

Em matemática existe uma palavra para "arrumação ordenada"ou um "arranjo ordenado". A palavra é **permutação**.

Definição 6.4.1. *Uma $n-$permutação de objetos distintos é um arranjo ordenado de n objetos retirados de um conjunto. Se o conjunto em questão só tem n objetos então seremos econômicos e chamaremos uma $n-$permutação de permutação.*

Notação: O número total de $n-$permutações em um conjunto de m elementos será denotado por $P(m, n)$.

Exemplos: Seja $S = \{1, 2, 3\}$.

1-permutações de S	2-permutações de S	permutações de S
1	12	123
2	13	132
3	21	213
	23	231
	31	312
	32	321
$P(3,1) = 3$	$P(3,2) = 6$	$P(3,3) = 6$

Número total de permutações

Teorema 6.4.2. *Sejam $m, n \in \mathbb{N}$ tais que $m \geq n$. Assim*

$$P(m,n) = m(m-1)(m-2)\dots(m-(n-1)) = \frac{m!}{(m-n)!}$$

Lembre-se que $m! = m.(m-1).(m-2)\dots 3.2.1$

Além disso, adotamos por convenção que $0! = 1$.

Demonstração. Podemos divir o trabalho de construir uma $n-$permutação em n etapas.

- Etapa 1: Escolher o primeiro elemento entre m possíveis.
- Etapa 2: Escolher o segundo elemento diferente do anterior, pois não podemos repertir.

  Então existem $m-1$ possíveis.
- Etapa n: Escolher o $n-$ésimo elemento diferente dos $n-1$ anteriores.

  Então existem $m-(n-1)$ possíveis.

Pela regra do produto o total de possibilidades é

$$m(m-1)\dots(m-(n-1)) = \frac{m(m-1)\dots(m-(n-1))\cancel{(m-n)\dots 1}}{\cancel{(m-n)\dots 1}} = \frac{m!}{(m-n)!}$$

□

Exercício 6.4.3. *De quantas maneiras diferentes um pódio de 3 lugares pode ser formado em uma competição de 100 atletas?*

Solução: $P(100,3) = \dfrac{100!}{97!} = 100.99.98 = 970200.$

Exercício 6.4.4. *Quantas permutações das letras A, B, C, D, E, F, G, H contêm a sequência ABC nessa ordem?*

Solução: As permutações que possuem a sequência ABC têm um dos seguintes formatos.

1. ABC $\boxed{*}$ $\boxed{*}$ $\boxed{*}$ $\boxed{*}$ $\boxed{*}$
2. $\boxed{*}ABC$ $\boxed{*}$ $\boxed{*}$ $\boxed{*}$ $\boxed{*}$
3. $\boxed{*}$ $\boxed{*}ABC$ $\boxed{*}$ $\boxed{*}$ $\boxed{*}$

4. $\boxed{*}\boxed{*}\boxed{*}ABC\boxed{*}\boxed{*}$

5. $\boxed{*}\boxed{*}\boxed{*}\boxed{*}ABC\boxed{*}$

6. $\boxed{*}\boxed{*}\boxed{*}\boxed{*}\boxed{*}ABC$

Para construir as permutações de cada formato:

Note que existem 5 possíveis letras para o primeiro quadrado, 4 para o segundo, 3 para o terceiro, 2 para o quarto, 1 para o quinto. Então o total de cada formato é $5.4.3.2.1 = 5!$.

Como são 6 formato diferentes (disjuntos) então o total de permutações é

$5! + 5! + 5! + 5! + 5! + 5! = 6.5.4.3.2.1 = 6!$.

Estudaremos agora o caso não ordenado.

Definição 6.4.5. *Uma $n-$combinação de um conjunto é simplesmente um subconjunto com n elementos.*

Notação: O número total de $n-$combinações em um conjunto de m elementos será denotado por $C(m,n)$ ou $\binom{m}{n}$.

Número total de combinações

Teorema 6.4.6. *Sejam $m, n \in \mathbb{N}$ tais que $m \geq n$. Assim*

$$\binom{m}{n} = \frac{m(m-1)(m-2)\ldots(m-(n-1))}{n!} = \frac{m!}{(m-n)!\ n!}$$

Demonstração. Considere o trabalho de construir uma $n-$permutação (Isso mesmo, uma $n-$permutação. Você não leu errado).

Posso dividí-lo em 2 tarefas:

Tarefa 1: Escolher n elementos entre os m possíveis.

Tarefa 2: Ordená-los.

Para a primeria tarefa o número de possibilidades é o número de subconjuntos de n elementos dentro de um conjunto de m elementos, isto é, $\binom{m}{n}$.

Para a segunda tarefa, temos n elementos obtidos na primeira. Podemos ordená-los de todas as maneiras possíveis em n etapas.

Etapa 1: Escolher o primeiro elemento entre n possíveis.

Etapa 2: Escolher o segundo, diferente do primeiro, entre $n-1$ possíveis.

$\vdots$

Etapa n: Escolher o $n-$ésimo, diferente dos $n-1$ anteriores entre $n-(n-1)=1$ possível.

O total de possibilidades da tarefa 2 é $n!$

Pela regra do produto, o total de $n-$permutações obtidas com a realização das duas tarefas é

$$P(m,n) = \binom{m}{n} n!$$

Mas já sabemos que $P(m,n) = \dfrac{m!}{(m-n)!}$, pelo teorema 6.4.2.

Portanto $\binom{m}{n} n! = \dfrac{m!}{(m-n)!}$.

Obtemos finalmente $\binom{m}{n} = \dfrac{m!}{(m-n)!\ n!}$. □

IMPORTANTE

Observação 6.4.7. *A fórmula mais importante do capítulo é essa:* $\binom{m}{n} = \dfrac{m!}{(m-n)!\ n!}$. *Como escolher um subconjunto de n elementos em um conjunto de m elementos é o mesmo que escolher n objetos entre m possíveis. O que essa fórmula diz é o total de maneiras distintas de escolher n objetos ente m possiveis. Isso é muito importante. A usaremos em praticamente todos os outros resultados do capítulo.*

Exemplo: Existem $\binom{5}{3}$ maneiras de escolher 3 alunos entre 5. Isto é, $\dfrac{5.4.\cancel{3!}}{\cancel{3!}\ 2!} = \dfrac{5.4}{2} = 10$.

Exercício 6.4.8. *a) Liste todas as* $3-$*permutações de* $\{1,2,3,4,5\}$.

b) Liste todas as $3-$*combinações de* $\{1,2,3,4,5\}$.

Exercício 6.4.9. *Quantas* $5-$*permutações existem entre 9 elementos?*

Exercício 6.4.10. *Quantas sequências de 10 bits existem contendo*

a) exatamente 4 números iguais a 1?

b) no máximo 4 números iguais a 1?

c) pelo menos 4 números iguais a 1?

d) quantidades iguais de zeros e uns?

Exercício 6.4.11. *Quantos subconjuntos com um número ímpar de elementos possui um conjunto com 10 elementos ?*

Exercício 6.4.12. *Quantos subconjuntos com mais de 2 elementos possui um conjunto com 100 elementos?*

Solução: Provamos no capítulo de indução que o total de subconjuntos de um conjunto com n elementos é 2^n. Então temos 2^{100} subconjuntos, mas a gente quer descartar os subconjuntos que possuem nenhum elemento, 1 elemento e 2 elementos.

Só existe um subconjunto que não possui elemento, o vazio, mas note que a fórmula também funciona aqui se assumirmos que $0! = 1$. Pois $\binom{100}{0} = \frac{\cancel{100!}}{\cancel{(100-0)!}0!} = 1$

O número de subconjuntos com 1 elemento dentro de um conjunto com 100 é igual a

$$\binom{100}{1} = \frac{100!}{(100-1)!1!} = \frac{100.\cancel{99!}}{\cancel{(99)!}1!} = 100.$$

O número de subconjuntos com 2 elementos dentro de um conjunto com 100 é igual a

$$\binom{100}{2} = \frac{100!}{(100-2)!2!} = \frac{100.99.\cancel{98!}}{\cancel{(98)!}2!} = 99.50.$$

Assim o resutado do exercício fica $2^{100} - 1 - 100 - 99.50$.

Exercício 6.4.13. *Mostre que* $\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n} = 2^n$.

Solução: Note que

- $\binom{n}{0}$ é o número de subconjuntos com 0 elementos dentro de um conjunto com n.
- $\binom{n}{1}$ é o número de subconjuntos com 1 elemento dentro de um conjunto com n.

  $\vdots$
- $\binom{n}{n}$ é o número de subconjuntos com n elementos dentro de um conjunto com n.

Então $\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n}$ representa o total de subconjuntos dentro de um conjunto com n elementos e já sabemos que esse total é 2^n.

Exercício 6.4.14. *Uma moeda é lançada 10 vezes e em cada lançamento obtém-se cara ou coroa. Quantos resultados são possíveis*

a) no total?

b) com exatamente 3 caras?

c) com pelo menos 3 caras?

d) com o mesmo número de caras e coroas?

Vou resolver as letras *a)* e da *b)*. As outras deixo para você.

Solução: Represente cara por c e coroa por k. Você quer palavras com 10 letras usando somente c e k.

a) Para cada letra você têm duas opções então o total é 2^{10}

b) Dentre as 10 letras você quer 3 sejam c. Você deve escolher as posições dessas 3 caras dentre 10 possíveis, ou seja, você quer o total de maneiras de escolher três posições dentre 10 possíveis. Resposta: $\binom{10}{3}$.

Exercício 6.4.15. *Quantas permutações das letra A, B, C, D, E, F, G, H contêm*

a) a sequência ED?

b) a sequência CDE?

c) as sequências BA e FGH?

d) as sequências AB, DE e GH?

e) as sequências CAB e BED?

f) as sequências BCA e ABF?

Exercício 6.4.16. *Em um departamento existem 10 homens e 15 mulheres. Quantos comitês com 6 pessoas podem ser formados contendo exatamente 3 homens e 3 mulheres?*

Exercício 6.4.17. *Sejam m, n números inteiros positivos tais que $m \geq n$. Prove que*

$$\binom{m}{n} = \binom{m}{m-n}$$

de duas maneiras diferentes.

a) Utilize a fórmula do teorema 6.4.6.

b) Seja A um conjunto de m elementos. Construa uma bijeção entre o conjunto das $n-$combinações de A com o conjunto das $(m-n)-$combinações de A.

Dica: Para cada subconjunto de n elementos de A existe um subconjunto de $m-n$ elementos correspondente óbvio. Qual é ele?

Exercício 6.4.18. *Sejam m, n números inteiros positivos tais que $m > n$. Prove que*

$$\binom{m}{n} + \binom{m}{n+1} = \binom{m+1}{n+1}.$$

6.5 Binômio de Newton

O binômio de Newton é tão belo como a Vênus de Milo.
O que há é pouca gente para dar por isso
ó ó ó ó − ó ó ó ó ó ó ó ó ó ó − ó ó ó ó ó ó ó ó ó ó ó ó ó ó ó ó (o vento lá fora)

Álvaro de Campos (Heterônimo de Fernando Pessoa)

Binômio de Newton

Teorema 6.5.1. *Considere as variáveis x, y e $n \in \mathbb{N}$. Então*

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j$$
$$= \binom{n}{0} x^n + \binom{n}{1} x^{n-1}y^1 + \ldots + \binom{n}{n-1} x^1 y^{n-1} + \binom{n}{n} y^n$$

Exemplos: *a)* $(x+y)^2 = \binom{2}{0} x^2y^0 + \binom{2}{1} x^1y^1 + \binom{2}{2} x^0y^2 = 1x^2 + 2xy + 1y^2,$

pois $\binom{2}{0} = \frac{2!}{2!\ 0!} = 1$, $\binom{2}{1} = \frac{2!}{1!\ 1!} = 2$ e $\binom{2}{2} = \frac{2!}{0!\ 2!} = 1.$

b) $(x+y)^3 = \binom{3}{0} x^3y^0 + \binom{3}{1} x^2y^1 + \binom{3}{2} x^1y^2 + \binom{3}{3} x^0y^3 = 1x^3 + 3x^2y + 3xy^2 + 1y^3,$

pois $\binom{3}{0} = \frac{3!}{3!\ 0!} = 1$, $\binom{3}{1} = \frac{3.\cancel{2!}}{\cancel{2!}\ 1!} = 3$, $\binom{3}{2} = \frac{3.\cancel{2!}}{1!\ \cancel{2!}} = 3$ e $\binom{3}{3} = \frac{3!}{1!\ 3!} = 1.$

Observação 6.5.2. *Compare o triângulo de Pascal com o binômio de Newton. Percebe alguma semelhança?*

Pascal	Newton
1	$(x+y)^0 = 1$
1 1	$(x+y)^1 = 1x + 1y$
1 2 1	$(x+y)^2 = 1x^2 + 2xy + 1y^2$
1 3 3 1	$(x+y)^3 = 1x^3 + 3x^2y + 3xy^2 + 1y^3$
1 4 6 4 1	$(x+y)^4 = 1x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + 1y^4$
$\vdots$	$\vdots$

Demonstração. (Binômio de Newton)

Note que quando multiplicamos $\overbrace{(x+y)\ldots(x+y)}^{n \text{ vezes}}$ aparecem todas as palavras com n letras utilizando somente as letras x e y:

$$\overbrace{xxx\ldots xxx}^{n \text{ letras } x}, \quad \overbrace{xxx\ldots xxy}^{n-1 \text{ letras } x \text{ e } 1\ y}, \quad \overbrace{xxx\ldots xyx}^{n-1 \text{ letras } x \text{ e } 1\ y}, \quad \ldots, \quad \overbrace{yyy\ldots yyy}^{n \text{ letras } y}.$$

Só depois contraímos essas palavras de forma mais compacta. Por exemplo:

$$xxx\ldots xxx = \underline{x^n}, \quad xxx\ldots xxy = \underline{x^{n-1}y}, \quad xxx\ldots xyx = \underline{x^{n-1}y}, \quad yyy\ldots yyy = \underline{y^n}.$$

Para cada forma compacta $x^{n-j}y^j$ temos que descobrir quantas palavras deram origem a ela quando contraídas. O problema se resume a descobrir quantas palavras de n letras são formadas com $n-j$ letras x e j letras y.

Note que se eu escolher as j posições das letras y, as outras $n-j$ já serão todas x.

Isto é, escolhendo um subconjunto de j posições dentro do conjunto de n posições, isso me dá uma palavra com j letras y e $n-j$ letras x.

Assim o total de palavras com $n-j$ letras x e j letras y é igual ao número de subconjuntos de j elementos dentro de um conjunto de n elementos, isto é, $\binom{n}{j}$.

Portanto na multiplicação $\overbrace{(x+y)\ldots(x+y)}^{n\ vezes}$ aparecem $\binom{n}{j}$ palavras com $n-j$ letras x e j letras y que quando contraídas viram $x^{n-j}y^j$.

Conclusao $(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y^1 + \ldots + \binom{n}{n-1}x^1y^{n-1} + \binom{n}{n}y^n$. □

Exercício 6.5.3. *Utilizando o binômio de Newton calcule*

a) $\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n-1} + \binom{n}{n}$

b) $\binom{n}{0} + \binom{n}{1}2^1 + \binom{n}{2}2^2 + \ldots + \binom{n}{n-1}2^{n-1} + \binom{n}{n}2^n$

c) $\binom{2n-1}{0} + \binom{2n-1}{1} + \ldots + \binom{2n-1}{n-1}$ *Dica: Use o exercício 6.4.17.*

Vamos resolver a letra *b*).

Solução: Sabemos pelo binômio de Newton que

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y^1 + \ldots + \binom{n}{n-1}x^1y^{n-1} + \binom{n}{n}y^n.$$

Se escolhermos $x=1$ e $y=2$ e obtemos a fórmula da letra *b*).

Assim $3^n = (1+2)^n = \binom{n}{0} + \binom{n}{1}2^1 + \binom{n}{2}2^2 + \ldots + \binom{n}{n-1}2^{n-1} + \binom{n}{n}2^n$.

6.6 Permutações e combinações com repetições

As permutações que estudamos duas seções atrás eram de objetos distintos, mas antes disso já havíamos conversado sobre o número total de sequência de 8 bits quando falamos da regra do produto. As sequência de oito bits tem repetição dos objetos $\{0, 1\}$.

Quando não existe restrição quanto ao número de repetições de um objeto na permutação chamamos de permutação com repetição. Portanto as sequências de 8 bits são chamadas de $8-$permutações com repetição.

O próximo teorema repete aquilo já sabemos.

Teorema 6.6.1. *O total de $r-$permutações de n objetos com repetição é n^r.*

OBS: Aqui não há restrição quanto ao número de repetições de um objeto na permutação, inclusive a permutação com r objetos iguais é contada aqui.

Demonstração. Existem n possíveis objetos para cada uma das r posições da permutação, pois podemos repetir à vontade. Assim pela regra do porduto o total é n^r. □

Agora, um problema diferente é quando impomos o número de vezes que um objeto deve ser repetido na permutação.

Exercício 6.6.2. *Quantas sequências diferentes podem ser obtidas a partir da palavra SUCCESS reordenando suas letras?*

Solução: Note que somos obrigados a usar

3 letras S, 2 letras C, 1 letra U e 1 letra E e temos 7 espaços para distribuí-las .

Podemos dividir esse trabalho em 4 tarefas.
Tarefa 1: Escolher as posições das 3 letras S entre 7 posições possíveis.
Tarefa 2: Escolher as posições das 2 letras C entre as 4 posições restantes.
Tarefa 3: Escolher a posição de 1 letra U entre as 2 posições restantes.
Tarefa 4: Escolher a posição de 1 letra E entre a 1 posição restante.

As possibilidades para cada tarefa são:
Tarefa 1: Precisamos do número de subconjuntos de 3 posições em um conjunto de 7: $\binom{7}{3}$.

Tarefa 2: Precisamos do número de subconjuntos de 2 posições em um conjunto de 4: $\binom{4}{2}$.

Tarefa 3: Precisamos do número de subconjuntos de 1 posição em um conjunto de 2: $\binom{2}{1}$.

Tarefa 4: Precisamos do número de subconjuntos de 1 posição em um conjunto de 1: $\binom{1}{1}$.

Pela regra do produto o total é $\binom{7}{3}\binom{4}{2}\binom{2}{1}\binom{1}{1} = \frac{7!}{\cancel{4!}\ 3!}\frac{\cancel{4!}}{\cancel{2!}\ 2!}\frac{\cancel{2!}}{\cancel{1!}\ 1!}\frac{\cancel{1!}}{0!\ 1!} = \frac{7!}{3!\ 2!\ 1!\ 1!}$.

Teorema 6.6.3. *Sejam $n_1, n_2, \ldots, n_k$ números naturais tais que $n_1 + n_2 + \ldots + n_k = n$.*
O total de permutações de n objetos onde há repetição de exatamente n_1 objetos do tipo 1, n_2 objetos do tipo 2, ..., n_k objetos do tipo k é $\frac{n!}{n_1!\ n_2!\ \ldots\ n_k!}$.

Demonstração. Podemos construir todas essas permutações divindo o trabalho em k tarefas.

Tarefa 1: Escolher n_1 posições entre n posições possíveis para os objetos de tipo 1.
O número de possibilidade aqui é $\binom{n}{n_1}$.

Tarefa 2: Escolher n_2 posições entre $n - n_1$ posições restantes para os objetos de tipo 2.
O número de possibilidade aqui é $\binom{n-n_1}{n_2}$.

Tarefa 3: Escolher n_3 posições entre $n - n_1 - n_2$ posições restantes para os objetos de tipo 3.
O número de possibilidade aqui é $\binom{n-n_1-n_2}{n_3}$.

$\vdots$

Tarefa k: Escolher n_k posições entre $n - n_1 - n_2 - \ldots - n_{k-1}$ posições restantes para os de tipo k.
O número de possibilidade aqui é $\binom{n-n_1-n_2-\ldots-n_{k-1}}{n_k}$.

Pela regra do produto, o total de possibilidade é

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\ldots\binom{n-n_1-n_2-\ldots-n_{k-1}}{n_k}.$$

Lembrando que $n - n_1 - n_2 - \ldots - n_{k-1} - n_k = 0$ o produto acima vale

$$\frac{n!}{\cancel{(n-n_1)!}\ n_1!}\frac{\cancel{(n-n_1)!}}{\cancel{(n-n_1-n_2)!}\ n_2!}\cdots\underbrace{\frac{\cancel{(n-n_1-n_2-\ldots-n_{k-1})!}}{\cancel{(n-n_1-n_2-\ldots-n_{k-1}-n_k)!}\ n_k!}}_{=0!} = \frac{n!}{n_1!\ n_2!\ \ldots\ n_k!}.$$

□

Diversos problemas de combinatória recaem nesse de calcular o total de permutações de objetos com número fixo de repetições para cada tipo de objeto. Um que se resolve da mesma maneira é o de distribuir objetos em caixas que devem receber um número fixo de objetos. Vejamos um exemplo antes do teorema.

Exercício 6.6.4. *Quantas maneiras distintas podemos distribuir 5 cartas para cada um dos jogadores A, B, C e D, a partir de um baralho com 52 cartas?*

Solução: **Primeira maneira de resolver**

Esse trabalho deve ser divido em 4 tarefas.

Tarefa 1: Escolher 5 cartas entre 52 para o jogador A. Possibilidades: $\binom{52}{5}$.

Tarefa 2: Escolher 5 cartas entre $52-5=47$ para o jogador B. Possibilidades: $\binom{47}{5}$.

Tarefa 3: Escolher 5 cartas entre $47-5=42$ para o jogador C. Possibilidades: $\binom{42}{5}$.

Tarefa 4: Escolher 5 cartas entre $42-5=37$ para o jogador D. Possibilidades: $\binom{37}{5}$.

Então o total é $\binom{52}{5}\binom{47}{5}\binom{42}{5}\binom{37}{5} = \frac{52!}{\cancel{47!}\ 5!}\frac{\cancel{47!}}{\cancel{42!}\ 5!}\frac{\cancel{42!}}{\cancel{37!}\ 5!}\frac{\cancel{37!}}{32!\ 5!} = \frac{52!}{5!\ 5!\ 5!\ 5!\ 32!}$.

Segunda maneira de resolver

Divida em 2 tarefas.

Tarefa 1: Escolha 20 cartas entre 52 possíveis. Possibilidades: $\binom{52}{20} = \frac{52!}{32!\ 20!}$

Tarefa 2: Coloque 20 cartas na mesa lado a lado. Embaixo delas distribua 5 letras A, 5 letras B, 5 letras C e 5 letras D, representando os jogadores.

$$\underset{A}{\boxed{1}}\ \underset{D}{\boxed{2}}\ \underset{C}{\boxed{3}}\ \underset{A}{\boxed{4}}\ \ldots\ \underset{B}{\boxed{17}}\ \underset{B}{\boxed{18}}\ \underset{A}{\boxed{19}}\ \underset{D}{\boxed{20}}$$

Cada permutação de 20 letras sendo 5 iguais a A, 5 iguais a B, 5 iguais a C e 5 iguais a D dá uma maneira de distribuir as cartas entres o jogadores.

Pelo teorema 6.6.3, o total dessas permutações é $\frac{20!}{5!\ 5!\ 5!\ 5!}$.

Então o total de possibilidades das duas tarefas é $\frac{52!}{32!\ \cancel{20!}}\frac{\cancel{20!}}{5!\ 5!\ 5!\ 5!} = \frac{52!}{32!\ 5!\ 5!\ 5!\ 5!}$.

Teorema 6.6.5. *O total de possibilidades para distribuir n_1 objetos na primeira caixa, n_2 objetos na segunda caixa, ... e n_k objetos na caixa k, a partir de n objetos distintos é*

$$\frac{n!}{n_1!\ n_2!\ \ldots\ n_k!\ (n - n_1 - \ldots - n_k)!}.$$

Demonstração. Exatamente igual a solução do exercício anterior. □

No último problema de distribuir objetos em caixas sabíamos quantos objetos cada caixa teria que receber e que eles eram distintos. No seguinte existem objetos repetidos e não sabemos quanto cada caixa vai receber.

Exercício 6.6.6. *Quantas maneiras existem de escolher 5 cédulas de uma carteira que contém 5 cédulas de cada um dos seguintes valores? 7 Valores possíveis: 1 real, 2 reais, 5 reais, 10 reais, 20 reais, 50 reais e 100 reais*

Solução: Quero convencer você de que as seguintes tarefas possuem o mesmo número de possibilidades.

1. Escolher 5 objetos entre 7 tipos possíveis, podendo repetir a mesma escolha até 5 vezes (porque você tem cédulas de cada tipo suficiente para isso).
2. Distribuir 5 objetos entre 7 caixas distintas.

Podemos ver que essas duas atividades possuem o mesmo número de possibilidades da seguinte maneira.

- Cada escolha de 5 objetos entre 7 tipos, permite distribuir esses objetos em 7 caixas representando cada tipo.
- Cada distribuição de 5 objetos nas 7 caixas, dá uma maneira de escolher os 5 objetos entre os 7 tipos.

Existe uma bijeção entre as escolhas e as distribuições! Portanto a quantidade das duas é igual.

Nesse problema podemos pensar que existem 7 caixas representando os valores acima e vamos distribuir 5 cédulas entre elas.

Existe um argumento visual que usa estrelas e barras para lidar com esse problema.

Os 5 objetos serão representados por 5 estrelas $* \ * \ * \ * \ *$ e as 7 caixas serão representadas pelos 7 espaços que existem entre 6 barras: $|\ \ |\ \ |\ \ |\ \ |\ \ |$

Observe na tabela como representaremos as situações através de barras e estrelas.

Imagem	Situação que representa
$*****\|\|\|\|\|\|$	5 objetos na primeira caixa
$**\|\|*\|\|\|**\|$	2 objetos na $1^{\underline{a}}$ caixa, 1 objeto na $3^{\underline{a}}$ caixa e 2 objetos na $6^{\underline{a}}$ caixa
$\|\|\|\|\|**\|***$	2 objetos na $6^{\underline{a}}$ caixa, 3 objetos na $7^{\underline{a}}$ caixa

Por exemplo, na terceira imagem da tabela. As 2 estrelas entre a $5^{\underline{a}}$ e $6^{\underline{a}}$ barras estão ocupando o sexto espaço entre as barras, portanto os dois objetos estão ocupando a sexta caixa.

Para resolver esse problema temos que simplesmente contar o total de Imagens, ou seja, de permutações de 11 objetos sendo 5 estrelas e 6 barras que já sabemos ser $\dfrac{11!}{6!\ 5!}$, pelo teorema 6.6.3

Exercício 6.6.7. *Quantas soluções existem para a equação* $x_1 + x_2 + x_3 = 11$*, onde* $x_1, x_2, x_3 \in \{0, 1, 2, 3, \ldots\}$*?*

Solução: Note que cada solução dessa equação corresponde a uma maneira de distribuir 11 objetos em 3 caixas: x_1 objetos na primeira, x_2 na segunda, x_3 na terceira.

Exemplo: $3 + 2 + 2 = 11 \Rightarrow$ 3 objetos na primeira, 2 na segunda e 2 na terceira.

Podemos usar a técnica das estrelas e barras. Precisamos de 11 estrelas e 2 barras, pois existem 3 espaços entre duas barras.

O números de permutações de 11 estrelas e 2 barras é $\dfrac{13!}{11!\ 2!}$, pelo teorema 6.6.3.

Observação 6.6.8. *Na solução do exercício 6.6.6, vimos que o total de escolhas de m objetos entre n tipos possíveis (podendo repetir a escolha até m vezes) é igual ao total de distribuições de m objetos em n caixas distintas. Existe um técnica chamada estrelas e barras (Stars and bars) que resolve o problema.*

Definição 6.6.9. *Um escolha de m objetos entre n tipos, onde os objetos podem ser repetidos na escolha até m vezes, é chamado de* $m-$*combinação com repetição.*

Teorema 6.6.10. *O total de $m-$combinações com repetição entre n possíveis tipos de objetos é* $\binom{m+n-1}{m}$.

Demonstração. Vimos na observação 6.6.8 que o total de escolhas de m objetos entre n tipos possíveis (podendo repetir a escolha até m vezes) é igual ao total de distribuições de m objetos em n caixas distintas.

Podemos usar a técnica das estrelas e barras. Serão m estrelas e $n-1$ barras.

Queremos o número total de permutações de $m+n-1$ objetos, onde m são estrelas e $n-1$ são barras.

Sabemos pelo teorema 6.6.3 que esse número é igual a $\binom{m+n-1}{m}$. □

Exercício 6.6.11. *Quantas maneiras diferentes de escolher 10 moedas em um cofrinho que tem 100 moedas de 10 centavos e 80 moedas de 5 centavos?*

Exercício 6.6.12. *Quantos maneiras existem de formar um cofrinho com 20 moedas usando moedas de* $1, 5, 10, 25, 50$ *centavos?*

Exercício 6.6.13. *Uma editora tem 300 cópias de um livro. Quantas maneiras existem de estocá-los em 3 armazéns diferentes?*

Exercício 6.6.14. *Quantas soluçoes são possíveis para a equação* $x_1 + x_2 + x_3 + x_4 + x_5 = 21$*, onde* $x_i \in \{0, 1, 2, \ldots\}$ *e*

a) $x_1 \geq 1$*?*

b) $x_i \geq 2$*, para* $i = 1, 2, 3, 4$ *e* 5*?*

c) $x_1 \leq 10$*?*

d) $x_1 \leq 3$*,* $1 \leq x_2 \leq 4$ *e* $15 \leq x_3$*?*

Solução: *a*) Subtraia 1 dos dois lados da equação.

$$x_1 - 1 + x_2 + x_3 + x_4 + x_5 = 21 - 1$$

Chame $x_1 - 1 = y_1$, $x_2 = y_2$, $x_3 = y_3$, $x_4 = y_4$, $x_5 = y_5$. Obtemos $y_1 + y_2 + y_3 + y_4 + y_5 = 20$.

Como queremos $x_1 \geq 1$, $x_2 \geq 0$, $x_3 \geq 0$, $x_4 \geq 0$, $x_5 \geq 0$, então queremos as soluçoes inteiras não negativas de $y_1 + y_2 + y_3 + y_4 + y_5 = 20$.

Assim o número soluções para a letra a) é o número de soluções para $y_1 + y_2 + y_3 + y_4 + y_5 = 20$, onde cada $y_i \in \{0, 1, 2, \ldots\}$.

Repetindo a solução do exercício 6.6.7, podemos resolver com a técnica das estrelas e barras. Temos 20 estrelas e 4 barras. Portanto queremos o número total de permutações desses 24 objetos sendo 20 estrelas e 4 barras. Assim a resposta é $\frac{24!}{20!4!}$.

b) Subtraia 10 dos dois lados da equação.

$$(x_1 - 2) + (x_2 - 2) + (x_3 - 2) + (x_4 - 2) + (x_5 - 2) = 21 - 10$$

Chame $x_1 - 2 = y_1$, $x_2 - 2 = y_2$, $x_3 - 2 = y_3$, $x_4 - 2 = y_4$, $x_5 - 2 = y_5$.

Obtemos $y_1 + y_2 + y_3 + y_4 + y_5 = 11$.

Repita o item anterior.

c) Parte 1: Calcule o número de soluções para $x_1 + x_2 + x_3 + x_4 + x_5 = 21$ com $x_i \in \{0, 1, 2, \ldots\}$, como fizemos no exercício 6.6.7.

Parte 2: Depois calcule o número de soluções para $x_1+x_2+x_3+x_4+x_5 = 21$ com $x_2, x_3, x_4, x_5 \in \{0, 1, 2, \ldots\}$ e $x_1 \geq 11$, como fizemos no item a).

Finalmente, subtraia a solução da segunda parte da solução da primeira. Entendeu o porquê?

d) Tente resolver você.

Exercício 6.6.15. *Quantas sequências de 10 letras podem ser obtidas com as letras da palavra MISSISSIPI?*

Exercício 6.6.16. *Quantas sequências de 5 letras podem ser formadas com as letras de SEERESS?*

6.7 Números de Bernoulli (Curiosidade)

Definição 6.7.1. *Nessa seção chamaremos de S_k a soma $S_k = 1^k + 2^k + \ldots + n^k$.*

Exemplos: $S_0 = 1^0 + 2^0 + \ldots + n^0 = \overbrace{1 + 1 + \ldots + 1}^{n \text{ vezes}} = n$

$S_1 = 1^1 + 2^1 + \ldots + n^1 = \frac{n(n+1)}{2}$, pelo exemplo a) abaixo do princípio da indução finita.

$S_2 = 1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$, pelo item g) do exercício 3.1.1.

Nessa seção mostraremos que S_k depende de $S_{k-1}, S_{k-2}, \ldots, S_1, S_0$. Portanto sabendo o valor dos anteriores você consegue achar S_k.

Para achar a fórmula de S_k precisamos expandir a expressão $(x-1)^{k+1}$ usnado o binômio de Newton.

Vamos começar com S_2 e S_3, porque o S_0 é óbvio e o S_1 já fizemos no capítulo de indução.

Calculando S_2:

$(x-1)^{2+1} = (x-1)^3 = 1x^3 - 3x^2 + 3x - 1.$

Então $3x^2 - 3x + 1 = x^3 - (x-1)^3$.

	$3x^2 - 3x + 1$		$x^3 - (x-1)^3$
$x = 1$	$3(1)^2 - 3(1) + 1$	$=$	$\cancel{1^3} - 0^3$
$x = 2$	$3(2)^2 - 3(2) + 1$	$=$	$\cancel{2^3} - \cancel{1^3}$
$x = 3$	$3(3)^2 - 3(3) + 1$	$=$	$\cancel{3^3} - \cancel{2^3}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$x = n-1$	$3(n-1)^2 - 3(n-1) + 1$	$=$	$\cancel{(n-1)^3} - \cancel{(n-2)^3}$
$x = n$	$+\ 3(n)^2 - 3(n) + 1$	$=$	$+n^3 - \cancel{(n-1)^3}$
	$3S_2 - 3S_1 + S_0$	$=$	$n^3 - 0^3$

Assim

$$3S_2 - 3S_1 + S_0 = n^3. \tag{6.1}$$

Lembre-se que $S_1 = \dfrac{n(n+1)}{2}$ e $S_0 = n$.

$$\begin{aligned}
\text{Portanto } S_2 &= \tfrac{n^3}{3} + \tfrac{3S_1}{3} - \tfrac{S_0}{3} \\
&= \tfrac{n^3}{3} + \tfrac{3n(n+1)}{6} - \tfrac{n}{3} \\
&= \tfrac{n^3-n}{3} + \tfrac{3n(n+1)}{6} \\
&= \tfrac{n(n^2-1)}{3} + \tfrac{3n(n+1)}{6} \\
&= \tfrac{2n(n+1)(n-1)}{6} + \tfrac{3n(n+1)}{6} \\
&= \tfrac{n(n+1)}{6}(2(n-1)+3) \\
&= \tfrac{n(n+1)(2n+1)}{6}
\end{aligned}$$

Calculando S_3:

$(x-1)^{3+1} = (x-1)^4 = 1x^4 - 4x^3 + 6x^2 - 4x^1 + 1.$

Então $4x^3 - 6x^2 + 4x - 1 = x^4 - (x-1)^4$.

	$4x^3 - 6x^2 + 4x - 1$		$x^4 - (x-1)^4$
$x = 1$	$4(1)^3 - 6(1)^2 + 4(1) - 1$	$=$	$\cancel{(1)^4} - (0)^4$
$x = 2$	$4(2)^3 - 6(2)^2 + 4(2) - 1$	$=$	$\cancel{(2)^4} - \cancel{(1)^4}$
$x = 3$	$4(3)^3 - 6(3)^2 + 4(3) - 1$	$=$	$\cancel{(3)^4} - \cancel{(2)^4}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$x = n-1$	$4(n-1)^3 - 6(n-1)^2 + 4(n-1) - 1$	$=$	$\cancel{(n-1)^4} - \cancel{(n-2)^4}$
$x = n$	$+\ 4(n)^3 - 6(n)^2 + 4(n) - 1$	$=$	$+(n)^4 - \cancel{(n-1)^4}$
	$4S_3 - 6S_2 + 4S_1 - S_0$	$=$	$n^4 - 0^4$

Assim

$$4S_3 - 6S_2 + 4S_1 - S_0 = n^4. \tag{6.2}$$

Lembre-se que $S_3 = \dfrac{n(n+1)(2n+1)}{6}$, $S_2 = \dfrac{n(n+1)}{2}$ e $S_0 = n$.

$$\begin{aligned}
\text{Portanto } S_3 &= \tfrac{n^4}{4} + \tfrac{6S_2}{4} - \tfrac{4S_1}{4} + \tfrac{S_0}{4} \\
&= \tfrac{n^4}{4} + \tfrac{6n(n+1)(2n+1)}{4.6} + \tfrac{4n(n+1)}{4.2} - \tfrac{n}{4} \\
&= \tfrac{1}{4}(n^4 + n(n+1)(2n+1) - 2n(n+1) + n) \\
&= \tfrac{1}{4}(n^4 + n(n+1)(2n+1-2) + n) \\
&= \tfrac{1}{4}(n^4 + n + n(n+1)(2n-1)) \\
&= \tfrac{1}{4}n(n+1)(n^2 - n + 1) + n(n+1)(2n-1)) \\
&= \tfrac{1}{4}n(n+1)(n^2 - n + 1 + 2n - 1) \\
&= \tfrac{1}{4}n(n+1)(n^2 + n) \\
&= \tfrac{1}{4}n(n+1)n(n+1) \\
&= \left(\tfrac{n(n+1)}{2}\right)^2
\end{aligned}$$

OBS; Agora que sabemos $S_0, S_1,\ S_2,\ S_3$ podemos calcular S_4 e assim sucessivamente.

Na verdade existe um jeito mais rápido. Você pode usar o computador inclusive.

Sabemos as seguintes fórmulas

$S_0 = n$

$2S_1 - S_0 = n^2$ (Essa eu não fiz, faça você)

$3S_2 - 3S_1 + S_0 = n^3$ (Essa é a equação 6.1 acima)

$4S_3 - 6S_2 + 4S_1 - S_0 = n^4$ (Essa é a equação 6.2 acima)

Essa equações formam um sistema linear

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 2 & 0 & 0 \\ 1 & -3 & 3 & 0 \\ -1 & 4 & -6 & 4 \end{pmatrix}}_{A} \begin{pmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{pmatrix} = \begin{pmatrix} n \\ n^2 \\ n^3 \\ n^4 \end{pmatrix} \quad \xrightarrow{\text{Olhe o } \triangle \text{ Pascal}} \quad \begin{array}{ccccc} 1 & & & & \\ 1 & 1 & & & \\ 1 & 2 & 1 & & \\ 1 & 3 & 3 & 1 & \\ 1 & 4 & 6 & 4 & 1 \end{array}$$

Um jeito rápido de obter a matriz A é olhando para o triângulo de Pascal ao lado.

Retire do $\triangle$ a primeira diagonal formada pelos uns.

$$\begin{array}{cccc} 1 & & & \\ 1 & 2 & & \\ 1 & 3 & 3 & \\ 1 & 4 & 6 & 4 \end{array}$$

$\xrightarrow{\text{e depois}}$

Troque o sinal para menos nos números da $2^{\underline{a}}, 4^{\underline{a}}, 6^{\underline{a}}, \ldots$ diagonais. Assim obtemos A.

$$\begin{array}{cccc} 1 & & & \\ -1 & 2 & & \\ 1 & -3 & 3 & \\ -1 & 4 & -6 & 4 \end{array}$$

Calculando S_4 e S_5 ao mesmo tempo e rapidamente:

$$\begin{array}{ccccccc} 1 & & & & & & \\ 1 & 1 & & & & & \\ 1 & 2 & 1 & & & & \\ 1 & 3 & 3 & 1 & & & \\ 1 & 4 & 6 & 4 & 1 & & \\ 1 & 5 & 10 & 10 & 5 & 1 & \\ 1 & 5 & 15 & 20 & 15 & 6 & 1 \end{array} \quad \longrightarrow \quad \begin{array}{ccccccc} 1 & & & & & & \\ -1 & 2 & & & & & \\ 1 & -3 & 3 & & & & \\ -1 & 4 & -6 & 4 & & & \\ 1 & -5 & 10 & -10 & 5 & & \\ -1 & 6 & -15 & 20 & -15 & 6 & \end{array}$$

O sistema linear fica

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & 0 & 0 & 0 & 0 \\ 1 & -3 & 3 & 0 & 0 & 0 \\ -1 & 4 & -6 & 4 & 0 & 0 \\ 1 & -5 & 10 & -10 & 5 & 0 \\ -1 & 6 & -15 & 20 & -15 & 6 \end{pmatrix}}_{\text{nova matriz } A} \begin{pmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \\ S_4 \\ S_5 \end{pmatrix} = \begin{pmatrix} n \\ n^2 \\ n^3 \\ n^4 \\ n^5 \\ n^6 \end{pmatrix}$$

Multiplicando pela inversa de A dos dois lados obtemos:

$$\begin{pmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \\ S_4 \\ S_5 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 \\ \frac{1}{6} & \frac{1}{2} & \frac{1}{3} & 0 & 0 & 0 \\ 0 & \frac{1}{4} & \frac{1}{2} & \frac{1}{4} & 0 & 0 \\ -\frac{1}{30} & 0 & \frac{1}{3} & \frac{1}{2} & \frac{1}{5} & 0 \\ -\frac{5}{6} & -\frac{31}{12} & -\frac{1}{6} & \frac{5}{12} & \frac{1}{2} & \frac{1}{6} \end{pmatrix}}_{A^{-1}} \begin{pmatrix} n \\ n^2 \\ n^3 \\ n^4 \\ n^5 \\ n^6 \end{pmatrix}$$

Assim obtemos novamente S_0, S_1, S_2, S_3, mas também

$$S_4 = -\frac{n}{30} + \frac{n^3}{3} + \frac{n^4}{2} + \frac{n^5}{5}$$
$$S_5 = -\frac{5n}{6} - \frac{31n^2}{12} - \frac{n^3}{6} + \frac{5n^4}{12} + \frac{n^5}{2} + \frac{n^6}{6}.$$

Note que todas essas fórmulas para os $S_1, S_2, \ldots$ são polinômios na variável n.

Jacob Bernoulli descobriu a seguinte fórmula para esses polinômios.

Números de Bernoulli

Teorema 6.7.2. *Existe uma sequência de números* $A = \frac{1}{6}, B = -\frac{1}{30}, C = \frac{1}{42}, \ldots$ *chamados de* ***números de Bernoulli*** *que satisfazem*

$$S_k = \frac{n^{k+1}}{k+1} + \frac{n^k}{2} + A\frac{k}{2}n^{k-1} + B\frac{k(k-1)(k-2)}{2.3.4}n^{k-3} + C\frac{k(k-1)(k-2)(k-3)(k-4)}{2.3.4.5.6}n^{k-5} + \ldots$$

Referências Bibliográficas

[1] N. L. Carothers, *Real Analysis*, Cambridge University Press (2000), Cambridge.

[2] J. L. Gersting, *Fundamentos Matemáticos para a Ciência da Computação*, LTC (1995), Rio de Janeiro.

[3] Ch.L. Hemleben, L. Lovasz, and Pelikan, J., *Discrete Mathematics & Applications*, McGraw-Hill (1999), New York.

[4] M. Oberguggenberger, and A. Ostermann, *Analysis for computer scientists*, Springer (2018) New York.

[5] G. O' Regan, *Guide to discrete mathematics*, Springer (2016), Switzerland.

[6] K.H. Rosen, *Discrete Mathematics & Applications*, McGraw-Hill (1999), New York.