# Matemática Discreta:

# Elementar e Além

L. LOVÁSZ, J. PELIKÁN E K. VESZTERGOMBI

Traduzido do original em inglês
***Discrete Mathematics:***
***Elementary and Beyond***
Springer, January 2003, ISBN 0387955852.
por Ruy José Guerra Barretto de Queiroz
Junho 2005

# Índice

**Prefácio** **v**

**1 Vamos contar!** **1**
1.1 Uma festa . . . . . 1
1.2 Conjuntos e similares . . . . . 4
1.3 O número de subconjuntos . . . . . 9
1.4 O número aproximado de subconjuntos . . . . . 13
1.5 Seqüências . . . . . 14
1.6 Permutações . . . . . 16
1.7 O número de subconjuntos ordenados . . . . . 17
1.8 O número de subconjuntos de um dado tamanho . . . . . 18

**2 Ferramentas combinatórias** **23**
2.1 Indução . . . . . 23
2.2 Comparando e estimando números . . . . . 27
2.3 Inclusão-exclusão . . . . . 29
2.4 Casas de Pombo . . . . . 31
2.5 O paradoxo gêmeo e o velho e bom logaritmo . . . . . 33

**3 Coeficientes binomiais e o Triângulo de Pascal** **39**
3.1 O Teorema Binomial . . . . . 39
3.2 Distribuindo presentes . . . . . 40
3.3 Anagramas . . . . . 42
3.4 Distribuindo dinheiro . . . . . 43
3.5 O Triângulo de Pascal . . . . . 45
3.6 Identidades no Triângulo de Pascal . . . . . 46
3.7 Uma visão de olhos de pássaro do Triângulo de Pascal . . . . . 50
3.8 Uma visão de olhos de águia: detalhes finos . . . . . 53

**4 Números de Fibonacci** **60**
4.1 O exercício de Fibonacci . . . . . 60
4.2 Muitas identidades . . . . . 62
4.3 Uma fórmula para os números de Fibonacci . . . . . 65

**5 Probabilidade combinatória** **70**
5.1 Eventos e probabilidades . . . . . 70
5.2 Repetição independente de um experimento . . . . . 71
5.3 A Lei dos Grandes Números . . . . . 73
5.4 A Lei dos Pequenos Números e a Lei dos Números Muito Grandes . . 74

**6 Inteiros, divisores, e primos** **77**
6.1 Divisibilidade de inteiros . . . . . 77
6.2 Os primos e sua história . . . . . 78
6.3 Fatoração em primos . . . . . 80
6.4 Sobre o conjunto de primos . . . . . 82
6.5 O "Pequeno" Teorema de Fermat . . . . . 86
6.6 O Algoritmo Euclideano . . . . . 88
6.7 Congruências . . . . . 94
6.8 Números estranhos . . . . . 96
6.9 Teoria dos números e combinatória . . . . . 103
6.10 Como testar se um número é primo? . . . . . 105

**7 Grafos** **112**
7.1 Graus pares e ímpares . . . . . 112
7.2 Caminhos, ciclos, e conectividade . . . . . 116
7.3 Passeios eulerianos e ciclos hamiltonianos . . . . . 120

**8 Árvores** **127**
8.1 Como definir árvores? . . . . . 127
8.2 Como crescer árvores? . . . . . 129
8.3 Como contar árvores? . . . . . 131
8.4 Como armazenar árvores? . . . . . 133
8.5 O número de árvores não-rotuladas . . . . . 138

**9 Encontrando o ótimo** **142**
9.1 Encontrando a melhor árvore . . . . . 142
9.2 Caixeiro Viajante . . . . . 146

**10 Emparelhamentos em grafos** **150**
10.1 Um problema de dança . . . . . 150
10.2 Um outro problema de emparelhamento . . . . . 151
10.3 O teorema principal . . . . . 153
10.4 Como encontrar um emparelhamento perfeito? . . . . . 156

**11 Combinatória em Geometria** **164**
11.1 Interseções de diagonais . . . . . 164
11.2 Contando regiões . . . . . 166
11.3 Polígonos convexos . . . . . 169

**12 Fórmula de Euler** **172**
12.1 Um planeta sob ataque . . . . . 172
12.2 Grafos planares . . . . . 175
12.3 Fórmula de Euler para Poliedros . . . . . 176

**13 Colorindo mapas e grafos** **179**
13.1 Colorindo regiões com duas cores . . . . . 179
13.2 Colorindo grafos com duas cores . . . . . 181
13.3 Colorindo grafos com muitas cores . . . . . 184
13.4 Coloração de mapas e o Teorema das Quatro Cores . . . . . 186

**14 Geometrias finitas, códigos, quadrados latinos, e outras belas criaturas** **193**
14.1 Pequenos mundos exóticos . . . . . 193
14.2 Planos afins finitos e planos projetivos finitos . . . . . 199
14.3 Desenhos em bloco . . . . . 202
14.4 Sistemas de Steiner . . . . . 206
14.5 Quadrados latinos . . . . . 210
14.6 Códigos . . . . . 213

**15 Uma olhada em complexidade e criptografia** **219**
15.1 Uma aula de Connecticut na corte do Rei Arthur . . . . . 219
15.2 Criptografia clássica . . . . . 222
15.3 Como guardar o último movimento em xadrez? . . . . . 224
15.4 Como verificar uma senha—sem aprendê-la? . . . . . 225
15.5 Como encontrar esses primos? . . . . . 226
15.6 Criptografia de chave pública . . . . . 227

**16 Respostas aos exercícios** **231**

# Prefácio

Para a maioria dos estudantes, o primeiro e único curso em matemática na universidade é cálculo. E é verdade que cálculo é o mais importante campo da matemática, cuja emergência no século XVII sinalizou o nascimento da matemática moderna, foi a chave para as aplicações bem sucedidas da matemática nas ciências e na engenharia.

Mas o cálculo (ou a análise) também é muito técnico. Requer bastante trabalho até mesmo para introduzir suas noções fundamentais como continuidade ou derivadas (afinal de contas, levou 2 séculos somente para desenvolver a própria definição dessas noções). Para se ter um verdadeiro sentimento sobre o poder de seus métodos, digamos através da descrição de uma de suas aplicações importantes em detalhe, leva anos de estudo.

Se você quiser ser um matemático, cientista da computação, ou engenheiro, esse investimento é necessário. Mas se seu objetivo é desenvolver um sentimento sobre o que é a matemática, onde é que os métodos matemáticos podem ser úteis, e que tipo de questões sobre as quais os matemáticos realmente trabalham, você pode querer buscar a resposta em algum outro campo da matemática.

Existem muitas estórias de sucesso da matemática aplicada fora do cálculo. Um tópico quente recente é criptografia matemática, que é baseada na teoria dos números (o estudo dos inteiros positivos $1, 2, 3, \ldots$), e é largamente aplicada, entre outras, em segurança de computadores e transação bancária eletrônica. Outras áreas importantes em matemática aplicada incluem programação linear, teoria dos códigos e a teoria da computação. O conteúdo matemático nessas aplicações é coletivamente chamado de *matemática discreta*. (A palavra "discreta" é usada no sentido de "separados um do outro", o oposto de "contínua"; ela é também comumente usada no sentido mais restritivo de "finita". A versão mais cotidiana dessa palavra é escrita "discreet".[1])

O objetivo deste livro não é cobrir "matemática discreta" em profundidade (deveria ter ficado claro da descrição acima que tal tarefa seria mal-definida e impossível mesmo assim). Ao contrário, discutimos um número de resultados e métodos selecionados, a maioria das áreas de combinatória e teoria dos grafos, com um pouco de teoria elementar dos números, probabilidade e geometria combinatória.

É importante se dar conta de que não existe matemática sem *provas*. Meramente enunciar os fatos, sem dizer algo sobre por que esses fatos são válidos, seria terrivelmente distanciado do espírito da matemática e tornaria impossível dar qualquer idéia

[1] N.T. Trata-se de jogo de palavras: *discreet* em inglês também significa discreto, mas dessa vez no sentido de cuidadoso.

sobre como ela funciona. Daí, sempre que possíel, daremos as provas dos teoremas que enunciamos. Às vezes isso não é possível; fatos um tanto simples e elementares podem ser extremamente difíceis de provar, e algumas dessas provas podem requerer cursos avançados para seguí-las. Nesses casos, enunciaremos pelo menos que a prova é altamente técnica e vai além do escopo deste livro.

Um outro ingrediente importante da matemática é a *resolução de problemas*. Você não será capaz de aprender o quer que seja de matemática sem sujar suas mãos e experimentar as idéias que você aprende na solução de problemas. Para alguns, isso pode soar apavorante, mas na verdade a maioria das pessoas perseguem esse tipo de atividade quase todo dia: todo mundo que joga uma partida de xadrez, ou resolve uma charada, está resolvendo problemas de matemática discreta. O leitor é fortemente aconselhado a responder às questões postas no texto e se envolver com os problemas no final de cada capítulo deste livro. Trate isso como resolver charada, e se você achar que alguma idéia que lhe ocorreu na solução tem algum papel mais adiante, fique satisfeito pois você está começando a pegar a essência de como a matemática se desenvolve.

Esperamos que possamos ilustrar que a matemática é um edifício, onde resultados são construídos sobre resultados anteriores, frequentemente voltando aos grandes matemáticos gregos; que a matemática está viva, com mais idéias novas e mais problemas prementes não-resolvidos que nunca; e que a matemática é também uma arte, onde a beleza de idéias e métodos é tão importante quanto sua dificuldade ou aplicabilidade.

László Lovász József Pelikán Katalin Vesztergombi

# Capítulo 1

# Vamos contar!

## 1.1 Uma festa

Alice convida seis pessoas para sua festa de aniversário: Bob, Carl, Diane, Eve, Frank e George. Quando eles chegam, eles apertam as mãos de cada um (estranho costume Europeu). Esse grupo é estranho mesmo, porque um deles pergunta: "Quantos apertos de mão isso significa?"

"Eu apertei 6 mãos no total" diz Bob, "e eu acho, assim fez todo mundo."

"Como somos sete, isso deveria significar $7 \cdot 6 = 42$ apertos de mão" aventura Carl.

"Isso parece demasiado" diz Diane. "A mesma lógica dá 2 apertos de mão se duas pessoas se encontram, o que está claramente errado."

"Isso é exatamente o ponto chave: todo aperto de mão foi contado duas vezes. Temos que dividir 42 por 2, para chegar ao número certo: 21." resolve Eve a questão.

Quando eles iam para a mesa, eles entraram numa discussão sobre quem senta onde; para contornar isso, Alice sugere:

"Vamos mudar o posicionamento de sentar a cada meia hora, até que cheguemos a cada posicionamento possível."

"Mas você fica na cabeceira da mesa" diz George, "pois é seu aniversário."

Quanto tempo essa festa vai durar? Quantos posicionamentos diferentes existem (com o lugar de Alice fixo)?

Vamos preencher as cadeiras uma a uma, começando com a cadeira à direita de Alice. Podemos por aqui qualquer um dos 6 convidados. Agora olhe para a segunda cadeira. se Bob senta na primeira cadeira, podemos por aqui qualquer um dos 5 convidados remanescentes; se Carl senta aí, temos novamente 5 escolhas, etc. Portanto o número de maneiras de preencher as primeiras duas cadeiras é $5 + 5 + 5 + 5 + 5 + 5 = 6 \cdot 5 = 30$. De forma semelhante, não importa como preenchemos as primeiras duas cadeiras, temos 4 escolhas para a terceira cadeira, o que dá $6 \cdot 5 \cdot 4$ maneiras de preencher as primeiras três cadeiras. Continuando de forma semelhante, encontramos que o número de maneiras de sentar os convidados é $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$.

Se eles trocam de assentos a cada meia hora, isso leva 360 horas, isto é, 15 dias para passar por todas as ordens de assentamento. Que festa, pelo menos no que diz

respeito à duração!

**1.1** Quantas maneiras essas pessoas podem ser sentadas à mesa, se Alice também pode sentar em qualquer lugar?

Após o bolo, a turma quer dançar (rapazes com garotas, lembre-se, essa é uma festa européia conservadora). Quantos pares possíveis podem ser formados?

OK, essa é fácil: existem 3 garotas, e cada uma pode escolher um dos 4 rapazes, e isso faz $3 \cdot 4 = 12$ pares possíveis.

Após cerca de dez dias, eles realmente precisam de algumas idéias novas para manter a festa acontecendo. Frank tem uma:

"Vamos fazer uma vaquinha e tirar um prêmio na loteria! Tudo o que temos que fazer é comprar um número suficiente de bilhetes tal que independente do que eles sorteiem, devemos ter um bilhete com os números certos. De quantos bilhetes precisamos para isso?"

(Na loteria sobre a qual eles estão falando, 5 números são selecionados de 90.)

"Isso é como o assentamento" diz George, "Suponha que façamos o jogo de modo que Alice marca um número, então ela passa o bilhete a Bob, que marca um número e o passa a Carl, ... Alice tem 90 escolhas, e independente do que ela escolha, Bob tem 89 escolhas, de modo que existem $90 \cdot 89$ escolhas para os primeiros dois números, e continuando de forma semelhante, chegamos a $90 \cdot 89 \cdot 88 \cdot 87 \cdot 86$ escolhas possíveis para os cinco números."

"Na verdade, acho que essa é como a questão do aperto de mão" diz Alice. "Se preenchermos os bilhetes da maneira que você sugeriu, obtemos o mesmo bilhete mais que uma vez. Por exemplo, haverá um bilhete onde eu marco 7 e Bob marca 23, e um outro onde eu marco 23 e Bob marca 7."

Carl salta e diz:

"Bem, vamos imaginar um bilhete, digamos, com números $7, 23, 31, 34$ e $55$. De quantas maneiras o obtemos? Alice poderia ter marcado quaisquer deles; qualquer que fosse o que ela marcou, Bob poderia ter marcado qualquer dos quatro restantes. Agora esse é realmente como o problema do assentamento. Obtemos todo bilhete $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ vezes."

"Portanto" conclui Diane, "se preenchermos os bilhetes da maneira que George propôs, então dentre os $90 \cdot 89 \cdot 88 \cdot 87 \cdot 86$ bilhetes que obtemos, toda 5-tupla ocorre não apenas uma vez, mas $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ vezes. Portanto o número de *diferentes* bilhetes é apenas

$$\frac{90 \cdot 89 \cdot 88 \cdot 87 \cdot 86}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}.$$

Precisamos somente de comprar esse número de bilhetes."

Alguém com uma boa calculadora de bolso calculou esse valor numa olhadela; era 43.949.268. Portanto eles tiveram que decidir (recordem, isso acontece em um país europeu pobre) que eles não têm dinheiro suficiente para comprar tantos bilhetes. (Além disso, eles ganhariam muito menos. E para preencher tantos bilhetes estragaria a festa...)

Portanto eles decidiram jogar cartas ao invés de loteria. Alice, Bob, Carl e Diane jogam bridge. Olhando para suas cartas, Carl diz: "Acho que eu tinha a mesma mão na última vez."

"Isso é muito improvável" diz Diane.

*Quão* improvável? Em outras palavras, quantas mãos diferentes pode-se ter em bridge? (O baralho tem 52 cartas, cada jogador recebe 13.) Esperamos que você o tenha notado: isso é essencialmente a mesma questão que a loteria. Imagine que Carl pega suas cartas uma a uma. A primeira carta pode ser qualquer uma das 52 cartas; o que quer que ele pegou primeiro, existem 51 possibilidades para a segunda carta, de modo que existem $52 \cdot 51$ possibilidades para as primeiras duas cartas. Argumentando semelhantemente, vemos que existem $52 \cdot 51 \cdot 50 \cdot \ldots \cdot 40$ possibilidades para as 13 cartas.

Mas, agora toda mão foi contada muitas vezes. Na verdade, se Eve chega a kibitz e olha nas cartas de Carl depois que ele as arrumou, e tenta adivinhar (não sabemos por que) a ordem na qual ele as escolheu, ela poderia pensar: "Ele poderia ter pegado qualquer das 13 cartas primeiro; ele poderia ter pegado qualquer das 12 cartas remanescentes segundo; qualquer das 11 cartas remanescentes terceiro;... Aha, isso é novamente como o assentamento: existem $13 \cdot 12 \cdot \ldots \cdot 2 \cdot 1$ ordens nas quais ele poderia ter pegado suas cartas."

Mas isso significa que o número de mãos *diferentes* em bridge é

$$\frac{52 \cdot 51 \cdot 50 \cdot \ldots \cdot 40}{13 \cdot 12 \cdot \ldots \cdot 2 \cdot 1} = 635.013.559.600.$$

Portanto, a chance de que Carl tivesse a mesma mão duas vezes seguidas é uma em 635.013.559.600, muito pequena mesmo.

Finalmente, os seis convidados decidem jogar xadrez. Alice, que só quer assistí-los, prepara 3 tabuleiros.

"De quantas maneiras vocês turma podem ser emparelhados um com outro?" ela questiona. "Isso é claramente o mesmo problema que sentar vocês em seis cadeiras; não importa se as cadeiras estão ao redor da mesa de jantar ou nos três tabuleiros. Portanto, a resposta é 720 como antes."

"Acho que você não devia contar como um emparelhamento diferente se duas pessoas no mesmo tabuleiro trocam de lugar" diz Bob, "e não deveria importar que par senta diante de qual tabuleiro."

"Sim, acho que temos que concordar sobre o que a questão realmente significa" adiciona Carl. "Se incluirmos nela quem joga com as brancas em cada tabuleiro, então se um par troca de lugar obtemos de fato um emparelhamento diferente. Mas Bob está certo de que não importa qual par usa qual tabuleiro."

"O que você quer dizer com não importa? Você senta diante do primeiro tabuleiro, que é o mais próximo ao amendoim, e eu sento diante do último, que é o mais distante" diz Diane.

"Vamos simplesmente nos fixar à versão de Bob da questão" sugere Eve. "Não é difícil, na verdade. É como nos apertos de mão: a cifra de Alice de 720 conta cada emparelhamento várias vezes. Poderíamos rearranjar os 3 tabuleiros de 6 maneiras diferentes, sem mudar o emparelhamento."

"E cada par pode ou não trocar de lado" adiciona Frank. "Isso significa $2 \cdot 2 \cdot 2 = 8$ maneiras de rearranjar as pessoas sem trocar o emparelhamento. Portanto, na realidade existem $6 \cdot 8 = 48$ maneiras de sentar todas as quais significam o mesmo emparelhamento. Os 720 modos de sentar vêm em grupos de 48, e portanto o número de emparelhamentos é $720/48 = 15$."

"Acho que ainda existe outra maneira de chegar nisso" diz Alice após algum tempo. "Bob é o mais jovem, portanto deixe-o escolher um parceiro primeiro. Ele pode escolher seu parceiro de 5 maneiras. Quem quer que seja o mais jovem entre os restantes, pode escolher seu ou sua parceiro(a) de 3 maneiras, e isso resolve o emparelhamento. Portanto o número de emparelhamento é $5 \cdot 3 = 15$."

"Bem, é bom ver que chegamos na mesma cifra por dois argumentos realmente diferentes. No mínimo, é reconfortante" diz Bob, e nesse tom feliz deixamos a festa.

**1.2** Qual é o número de "emparelhamentos" no sentido de Carl (quando importa quem senta em qual lado do tabuleiro, mas os tabuleiros são todos iguais), e no sentido de Diane (quando é o contrário)?

**1.3** Qual é o número de "emparelhamentos" (nos vários sentidos como acima) em uma festa de 10?

## 1.2 Conjuntos e similares

Queremos formalizar asserções como "o problema de contar o número de mãos em bridge é essentialmente o mesmo que o problema de contar bilhetes na loteria". A ferramenta mais básica em matemática que ajuda aqui é a noção de *conjunto*. Qualquer coleção de coisas, chamadas de *elementos*, é um conjunto. O baralho é um conjunto, cujos elementos são as cartas. Os participantes da festa formam um conjunto, cujos elementos são Alice, Bob, Carl, Diane, Eve, Frank e George (vamos representar esse conjunto por $P$). Todo bilhete de loteria contém um conjunto de 5 números.

Para a matemática, vários conjuntos de números são importantes: o conjunto dos números reais, representado por $\mathbb{R}$; o conjunto dos números racionais, representado por $\mathbb{Q}$; o conjunto dos inteiros, representado por $\mathbb{Z}$; o conjunto dos inteiros não-negativos, representado por $\mathbb{Z}_+$; o conjunto dos inteiros positivos, representado por $\mathbb{N}$. O *conjunto vazio*, o conjunto sem qualquer elemento, é um outro conjunto importante (embora não muito interessante); ele é representado por $\emptyset$.

Se $A$ é um conjunto e $b$ é um elemento de $A$, escrevemos $b \in A$. O número de elementos de um conjunto $A$ (também chamado de *cardinalidade* de $A$) é representado por $|A|$. Por conseguinte, $|P| = 7$; $|\emptyset| = 0$; e $|\mathbb{Z}| = \infty$ (infinito).[1]

Podemos especificar um conjunto listando seus elementos entre chaves; portanto

$$P = \{\text{Alice, Bob, Carl, Diane, Eve, Frank, George}\}$$

é o conjunto de participantes da festa de aniversário de Alice, ou

$$\{12, 23, 27, 33, 67\}$$

[1] Em matemática, pode-se distinguir vários níveis de "infinitude"; por exemplo, pode-se distinguir entre as cardinalidades de $\mathbb{Z}$ e $\mathbb{R}$. Esse é o assunto da *teoria dos conjuntos* e não nos diz respeito aqui.

é o conjunto de números no bilhete de loteria de meu tio. Às vezes substituímos a lista por uma descrição verbal, como

$$\{\text{Alice e seus convidados}\}.$$

Frequentemente especificamos um conjunto por uma propriedade que destaca os elementos em um grande "universo" como os números reais. Escrevemos então essa propriedade dentro das chaves, mas após os dois pontos. Por conseguinte

$$\{x \in \mathbb{Z} : \ x \geq 0\}$$

é o conjunto dos inteiros não-negativos (que chamamos $\mathbb{Z}_+$ anteriormente), e

$$\{x \in P : \ x \text{ é uma garota}\} = \{\text{Alice, Diane, Eve}\}$$

(representamos esse conjunto por $G$). Deixe-me também dizer a você que

$$\{x \in P : \ x \text{ tem mais de 21 anos}\} = \{\text{Alice, Carl, Frank}\}$$

(representamos esse conjunto por $D$).

Um conjunto $A$ é chamado de *subconjunto* de um conjunto $B$, se todo elemento de $A$ é também um elemento de $B$. Em outras palavras, $A$ consiste de certos elementos de $B$. Permitimos que $A$ consista de todos os elementos de $B$ (caso em que $A = B$), ou de nenhum deles (caso em que $A = \emptyset$). Portanto, o conjunto vazio é um subconjunto de todo conjunto. A relação que diz que $A$ é um subconjunto de $B$ é representada por $A \subseteq B$. Por exemplo, entre os vários conjuntos de pessoas consideradas acima, $G \subseteq P$ e $D \subseteq P$. Entre os conjuntos de números, temos uma longa cadeia:

$$\emptyset \subseteq \mathbb{N} \subseteq \mathbb{Z}_+ \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

A notação $A \subset B$ quer dizer que $A$ é um subconjunto de $B$ e diferente de $B$. Na cadeia acima, poderíamos substituir o símbolo de $\subseteq$ por $\subset$.

Se temos dois conjuntos, podemos definir vários outros conjuntos a partir da ajuda deles. A *interseção* de dois conjuntos é o conjunto consistindo daqueles elementos que são elementos de ambos os conjuntos. A interseção de dois conjuntos $A$ e $B$ é representada por $A \cap B$. Por exemplo, temos $G \cap D = \{\text{Alice}\}$. Dois conjuntos cuja interseção é o conjunto vazio (em outras palavras, não têm qualquer elemento em comum) são chamados *disjuntos*.

A *união* de dois conjuntos é o conjunto consistindo daqueles elementos que são elementos em pelo menos um dos conjuntos. A união de dois conjuntos $A$ e $B$ é representada por $A \cup B$. Por exemplo, temos $G \cup D = \{\text{Alice, Carl, Diane, Eve, Frank}\}$.

A *diferença* de dois conjuntos $A$ e $B$ é o conjunto de elementos que pertencem a $A$ mas não a $B$. A diferença de dois conjuntos $A$ e $B$ é representada por $A \setminus B$. Por exemplo, temos $G \setminus D = \{\text{Diane, Eve}\}$.

A *diferença simétrica* de dois conjuntos $A$ e $B$ é o conjunto de elementos que pertencem a exatamente um deles: $A$ ou $B$. A diferença simétrica de dois conjuntos $A$ e $B$ é representada por $A \triangle B$. Por exemplo, temos $G \triangle D = \{\text{Carl, Diane, Eve, Frank}\}$.

Interseção, união, e os dois tipos de diferença são semelhantes à adição, multiplicação, subtração: elas são operações sobre conjuntos, ao invés de operações

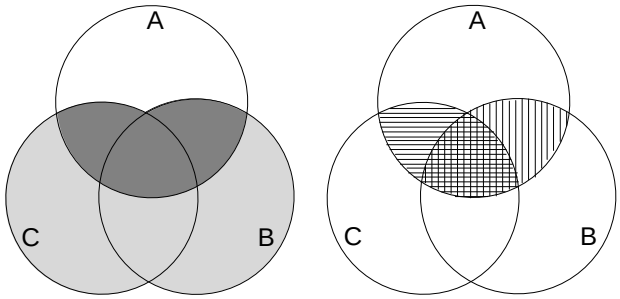


Figura 1.1: O diagrama de Venn de três conjuntos, e os conjuntos em ambos os lados de (1.1).

sobre números. Tal qual operações sobre números, operações de conjuntos obedecem a muitas regras (identidades) úteis. Por exemplo:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C). \tag{1.1}$$

Para ver que isso é o caso, pense num elemento $x$ que pertence ao conjunto no lado esquerdo. Então temos $x \in A$ e também $x \in B \cup C$. Essa última asserção é a mesma que dizer que ou $x \in B$ ou $x \in C$. Se $x \in B$, então (como também temos $x \in A$) temos $x \in A \cap B$. Se $x \in C$, então, de modo semelhante, obtemos $x \in A \cap C$. Portanto sabemos $x \in A \cap B$ ou $x \in A \cap C$. Pela definição da união de dois conjuntos, isso é o mesmo que dizer que $x \in (A \cap B) \cup (A \cap C)$.

Reciprocamente, considere um elemento que pertence ao lado direito. Pela definição de união, isso significa que $x \in A \cap B$ ou $x \in A \cap C$. No primeiro caso, temos $x \in A$ e também $x \in B$. No segundo, obtemos $x \in A$ e também $x \in C$. Portanto em qualquer dos casos $x \in A$, e temos $x \in B$ ou $x \in C$, o que implica que $x \in B \cup C$. Mas isso significa que $x \in A \cap (B \cup C)$.

Esse tipo de argumento fica um tanto cansativo, muito embora não existe nada nele a não ser lógica elementar. Um problema com ele é que é tão comprido que é fácil cometer um erro no argumento. Existe uma boa maneira gráfica de suportar tais argumentos. Representamos os conjuntos $A$, $B$ e $C$ por três círculos sobrepostos (Figura 1.1). Imaginamos que os elementos em comum de $A$, $B$ e $C$ são colocados na parte comum dos três círculos; aqueles elementes de $A$ que também estão em $B$ mas não em $C$ são colocados na parte comum dos círculos $A$ e $B$ fora de $C$, etc. Esse desenho é chamado de *diagrama de Venn* dos três conjuntos.

Agora onde estão aqueles elementos no diagrama de Venn que pertencem ao lado esquerdo de (1.1)? Temos que formar a união de $B$ e $C$, que é o conjunto cinza em (1.1(a)), e então intersectá-lo com $A$, para obter a parte cinza escuro. Para obter o conjunto no lado direito, temos que formar os conjuntos $A \cap B$ e $A \cap C$ (marcados por linhas verticais e horizontais, respectivamente), e então formar sua união. Está claro a partir da figura que obtemos o mesmo conjunto. Isso ilustra que diagramas de Venn provêem uma maneira segura e fácil de provar tais identidades envolvendo operações de conjuntos.

A identidade (1.1) é boa e um tanto fácil de lembrar: se pensamos na "união" como um tipo de adição (isso é um tanto natural), e "interseção" como um tipo de multiplicação (hmm... não tão claro por que, talvez após aprendermos sobre probabilidade no Capítulo 5 você verá), então vemos que (1.1) é completamente análoga à conhecida regra distributiva para números:

$$a(b+c) = ab + ac.$$

Essa analogia vai mais longe? Vamos pensar sobre as outras proprieadades de adição e multiplicação. Duas proporiedades importantes são que elas são *comutativas*::

$$a + b = b + a, \qquad ab = ba,$$

e *associativa*:

$$(a+b)+c = a+(b+c), \qquad (ab)c = a(bc).$$

Acontece que essas são também propriedades das operações de união e interseção:

$$A \cup B = B \cup A, \qquad A \cap B = B \cap A, \tag{1.2}$$

e

$$(A \cup B) \cup C = A \cup (B \cup C), \qquad (A \cap B) \cap C = A \cap (B \cap C). \tag{1.3}$$

A prova dessas identidades fica para o leitor como exercício.

Advertência! Antes de ir longe demais com essa analogia, vamos apontar para o fato de que existe uma outra lei distributiva para conjuntos:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C). \tag{1.4}$$

Chegamos nisso simplesmente trocando "união" e "interseção" em (1.1). (Essa identidade pode ser provada tal qual (1.1), veja o Exercício 1.19.) Essa segunda distributividade é algo que não tem análogo para números: em geral,

$$a + bc \neq (a+b)(a+c)$$

para três números $a, b, c$.

Existem outras identidades importantes envolvendo união, interseção, e também os dois tipos de diferença. Essas são úteis, mas não muito profundas: elas refletem a lógica simples. Portanto não as listamos aqui, mas enunciamos várias delas adiante nos exercícios.

**1.4** Dê exemplo de conjuntos cujos elementos são (a) edifícios, (b) pessoas, (c) estudantes, (d) árvores, (e) números, (f) pontos.

**1.5** Quais são os elementos dos seguintes conjuntos: (a) exército, (b) humanidade, (c) biblioteca, (d) o reino animal?

**1.6** Nomeie conjuntos tendo cardinalidade (a) 52, (b) 13, (c) 32, (d) 100, (e) 90, (f) 2.000.000.

**1.7** Quais são os elementos do seguinte (reconhecidamente peculiar) conjunto: $\{\text{Alice}, \{1\}\}$?

**1.8** O termo “elemento de um conjunto” é um caso especial de um “subconjunto de um conjunto”?

**1.9** Liste todos os subconjuntos de $\{0, 1, 3\}$. Quantos você obtém?

**1.10** Defina pelo menos três conjuntos, dos quais $\{\text{Alice, Diane, Eve}\}$ é um subconjunto.

**1.11** Liste todos os subconjuntos de $\{a, b, c, d, e\}$, contendo $a$ mas não contendo $b$.

**1.12** Defina um conjunto dos quais ambos $\{1, 3, 4\}$ e $\{0, 3, 5\}$ são subconjuntos. Encontre tal conjunto com um menor número possível de elementos.

**1.13** (a) Que conjunto você chamaria de união de $\{a, b, c\}$, $\{a, b, d\}$ e $\{b, c, d, e\}$?

(b) Encontre a união dos primeiros dois conjuntos, e então a união desse com o terceiro. Também, encontre a união do último dos dois conjuntos, e então a união desse com o primeiro conjunto. Tente formular o que você observou.

(c) Dê uma definição da união de mais de dois conjuntos.

**1.14** Explique a conexão entre a noção da união de conjuntos e o exercício 1.12.

**1.15** Formamos a união de um conjunto com 5 elementos e um conjunto com 9 elementos. Quais dos seguintes números podemos obter como a cardinalidade da união: 4, 6, 9, 10, 14, 20?

**1.16** Formamos a união de dois conjuntos. Sabemos que um deles tem $n$ elementos e o outro tem $m$ elementos. Que podemos inferir sobre a cardinalidade da união?

**1.17** Qual é a interseção

(a) dos conjuntos $\{0, 1, 3\}$ e $\{1, 2, 3\}$;

(b) do conjunto de garotas nessa classe e o conjunto de garotos nessa classe;

(c) do conjunto dos números primos e o conjunto de números pares?

**1.18** Formamos a interseção de dois conjuntos. Sabemos que um deles tem $n$ elementos e o outro tem $m$ elementos. Que podemos inferir sobre a cardinalidade da interseção?

**1.19** Prove (1.2), (1.3) e (1.4).

**1.20** Prove que $|A \cup B| + |A \cap B| = |A| + |B|$.

**1.21** (a) Qual é a diferença simétrica do conjunto $\mathbb{Z}_+$ de inteiros não-negativos e o conjunto $E$ de inteiros pares ($E = \{\ldots -4, -2, 0, 2, 4, \ldots\}$ contém inteiros pares tanto negativos quanto positivos).

(b) Formamos a diferença simétrica de $A$ e $B$, para obter um conjunto $C$. Formamos a diferença simétrica de $A$ e $C$. O que você obteve? Dê uma prova da resposta.

## 1.3 O número de subconjuntos

Agora que introduzimos a noção de subconjuntos, podemos formular nosso primeiro problema combinatório geral: qual é o número de todos os subconjuntos de um conjunto com $n$ elementos?

Começamos tentanto com números pequenos. Não tem qualquer importância o que são os elementos do conjunto; chamamos $a, b, c$ etc. O conjunto vazio tem apenas um subconjunto (a saber, ele próprio). Um conjunto com um único elemento, digamos $\{a\}$, tem dois subconjuntos: o conjunto próprio $\{a\}$ e o conjunto vazio $\emptyset$. Um conjunto com dois elementos, digamos $\{a, b\}$ tem quatro subconjuntos: $\emptyset$, $\{a\}$, $\{b\}$ e $\{a, b\}$. Dá mais trabalho listar todos os subconjuntos de um conjunto $\{a, b, c\}$ com 3 elementos:

$$\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}. \tag{1.5}$$

Podemos fazer uma pequena tabela com esses dados:

| No. de elementos | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| No. of subconjuntos | 1 | 2 | 4 | 8 |

Olhando para esses valores, observamos que o número de subconjuntos é uma potência de 2: se o conjunto tem $n$ elementos, o resultado é $2^n$, pelo menos nesses pequenos exemplos.

Não é difícil ver que essa é sempre a resposta. Suponha que você tenha que selecionar um subconjunto de um conjunto $A$ com $n$ elementos; vamos chamar esses elementos $a_1, a_2, \ldots, a_n$. Então podemos ou não querer incluir $a_1$, em outras palavras, podemos tomar duas possíveis decisões nesse ponto. Não importa o que decidimos sobre $a_1$, podemos ou não querer incluir $a_2$ no subconjunto; isso significa duas decisões possíveis, e portanto o número de maneiras que podemos decidir sobre $a_1$ e $a_2$ é $2 \cdot 2 = 4$. Agora não importa como decidimos sobre $a_1$ e $a_2$, temos que decidir sobre $a_3$, e podemos novamente decidir de duas maneiras. Cada uma dessas maneiras pode ser combinada com cada uma das 4 decisões que poderíamos ter tomado sobre $a_1$ e $a_2$, o que perfaz $4 \cdot 2 = 8$ possibilidades para decidir sobre $a_1, a_2$ e $a_3$.

Podemos continuar de modo semelhante: não importa como decidimos sobre os primeiros $k$ elementos, temos duas decisões possíveis sobre o seguinte, e portanto so o número de possibilidades dobra sempre que tomamos um novo elemento. Para decidir sobre todos os $n$ elementos do conjunto, temos $2^n$ possibilidades.

Daí, derivamos o teorema seguinte.

**Teorema 1.3.1** *Um conjunto com $n$ elementos tem $2^n$ subconjuntos.*

Podemos ilustrar o argumento usado na prova através da imagem que aparece na Figura 1.2. Lemos essa figura da seguinte forma. Desejamos selecionar um subconjunto chamado $S$. Começamos do círculo no topo (chamado de *nó*). O nó contém uma pergunta: $a_1$ é um elemento de $S$? As duas setas saindo desse nó são rotuladas com as duas possíveis respostas a essa pergunta (Sim e Não). Tomamos uma decisão e seguimos a seta apropriada (também chamada de *aresta*) rumo ao nó na outra extremidade. Esse nó contém a próxima pergunta: $a_2$ é um elemento de $S$? Siga a seta correspondente à sua resposta rumo ao próximo nó, que contém a terceira (e nesse caso a última)

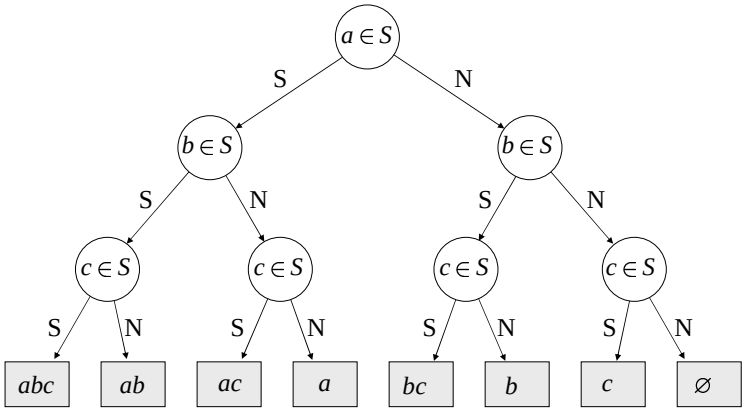


Figura 1.2: Uma árvore de decisão para selecionar um subconjunto de $\{a, b, c\}$.

pergunta que você deve responder para determinar o subconjunto: $a_3$ é um elemento de $S$? Dando uma resposta e seguindo a seta apropriada chegamos a um nó, que contém uma listagem dos elementos de $S$.

Por conseguinte, selecionar um subconjunto corresponde a descer nesse diagrama de cima para baixo. Existem tantos subconjuntos de nosso conjunto quanto nós no último nível. Como o número de nós dobra de nível para nível ao descer, o último nível contém $2^3 = 8$ nós (e se tivéssemos um conjunto de $n$-elementos, ele conteria $2^n$ nós).

**Observação.** Uma figura como essa é chamada de *árvore*.. (Isso não é uma definição matemática; essa virá mais tarde.) Se você quiser saber por que a árvore está crescendo de cabeça para baixo, pergunte aos cientistas da computação que introduziram essa convenção. (A sabedoria convencional é que eles nunca saíram da sala, e por isso eles nunca viram uma árvore de verdade.)

Podemos dar uma outra prova do teorema 1.3.1. Novamente, a resposta ficará esclarecida se fizermos uma pergunta sobre subconjuntos. Mas, agora não queremos selecionar um subconjunto; o que queremos é *enumerar* subconjuntos, o que significa que desejamos rotulá-los com números $0, 1, 2, \ldots$ de modo que possamos falar, digamos, sobre o subconjunto de No. 23 do conjunto. Em outras palavras, queremos arranjar os subconjuntos do conjunto em uma lista e então falar sobre o $23^{\underline{o}}$ subconjunto da lista.

(Na verdade desejamos chamar o primeiro subconjunto da lista de No. 0, o segundo subconjunto na lista de No. 1 etc. Isso é um pouco estranho mas, dessa vez são os lógicos os culpados. Na realidade, você achará isso um tanto natural e conveniente após algum tempo.)

Existem muitas maneiras de ordenar os subconjuntos de um conjunto para formar uma lista. Uma coisa razoavelmente natural a fazer é começar com $\emptyset$, e então listar todos os subconjuntos com 1 elemento, então listar todos os subconjuntos com 2 elementos, etc. Essa é a maneira pela qual a lista (1.5) é montada.

Uma outra possibilidade é ordenar os subconjuntos como um catálogo telefônico.

Esse método será mais transparente se escrevermos os subconjuntos sem chaves e vírgulas. Para os subconjuntos de $\{a, b, c\}$, obtemos a lista

$$\emptyset, a, ab, abc, ac, b, bc, c.$$

Essas são de fato maneiras úteis e naturais de listar todos os subconjuntos. Entretanto, elas têm uma limitação. Imagine a lista dos subconjuntos de 10 elementos, e se pergunte qual é o $233^{\underline{o}}$ subconjunto da lista, sem na verdade escrever a lista inteira. Isso seria difícil! Existe uma maneira de torná-la mais fácil?

Vamos começar com uma outra maneira de representar subconjuntos (uma outra *codificação* no jargão matemático). Ilustramos tal maneira para os subconjuntos de $\{a, b, c\}$. Olhamos para os elementos um por um, e escrevemos um 1 se o elemento ocorre no subconjunto e um 0 se ele não ocorre. Por conseguinte, para o subconjunto $\{a, c\}$, escrevemos 101, pois $a$ está no subconjunto, $b$ não está, e $c$ está novamente. Dessa maneira todo subconjunto é "codificado" por uma cadeia de comprimento 3, consistindo de 0's e 1's. Se especificarmos qualquer cadeia dessa, podemos facilmente extrair dela o subconjunto ao qual ela corresponde. Por exemplo, a cadeia 010 corresponde ao subconjunto $\{b\}$, pois o primeiro 0 nos diz que $a$ não está no subconjunto, o 1 que segue nos diz que $b$ está lá, e o último 0 nos diz que $c$ não está lá.

Agora tais cadeias consistindo de 0's e 1's nos remetem à *representação binária* de inteiros (em outras palavras, representações na base 2). Vamos recordar a forma binária de inteiros não-negativos até 10:

$$\begin{aligned}
0 &= 0_2 \\
1 &= 1_2 \\
2 &= 10_2 \\
3 &= 2 + 1 = 11_2 \\
4 &= 100_2 \\
5 &= 4 + 1 = 101_2 \\
6 &= 4 + 2 = 110_2 \\
7 &= 4 + 2 + 1 = 111_2 \\
8 &= 1000_2 \\
9 &= 8 + 1 = 1001_2 \\
10 &= 8 + 2 = 1010_2
\end{aligned}$$

(Colocamos o índice 2 aí para nos lembrar que estamos trabalhando na base 2, e não 10.)

Agora as formas binárias de inteiros $0, 1, \ldots, 7$ parecem quase como "códigos" de subconjuntos; a diferença é que a forma binária de um inteiro sempre começa com um 1, e os primeiros 4 desses inteiros têm formas binárias mais curtas que 3, enquanto que todos os códigos de subconjuntos consistem de exatamente 3 dígitos. Podemos fazer essa diferença desaparecer se acrescentarmos 0's às formas binárias nos seus inícios, para fazê-las todas ficar com o mesmo comprimento. Dessa maneira obtemos

a seguinte correspondência:

$$\begin{array}{ccccccc} 0 & \Leftrightarrow & 0_2 & \Leftrightarrow & 000 & \Leftrightarrow & \emptyset \\ 1 & \Leftrightarrow & 1_2 & \Leftrightarrow & 001 & \Leftrightarrow & \{c\} \\ 2 & \Leftrightarrow & 10_2 & \Leftrightarrow & 010 & \Leftrightarrow & \{b\} \\ 3 & \Leftrightarrow & 11_2 & \Leftrightarrow & 011 & \Leftrightarrow & \{b,c\} \\ 4 & \Leftrightarrow & 100_2 & \Leftrightarrow & 100 & \Leftrightarrow & \{a\} \\ 5 & \Leftrightarrow & 101_2 & \Leftrightarrow & 101 & \Leftrightarrow & \{a,c\} \\ 6 & \Leftrightarrow & 110_2 & \Leftrightarrow & 110 & \Leftrightarrow & \{a,b\} \\ 7 & \Leftrightarrow & 111_2 & \Leftrightarrow & 111 & \Leftrightarrow & \{a,b,c\} \end{array}$$

Portanto vemos que os subconjuntos de $\{a,b,c\}$ correspondem aos números $0,1,\ldots,7$.

O que acontece se considerarmos, em geral, subconjuntos de um conjunto com $n$ elementos? Podemos argumentar tal qual foi feito acima, para obter que os subconjuntos de um conjunto de $n$ elementos correspondem aos inteiros, começando com 0, e terminando com o maior inteiro que tem apenas $n$ dígitos na sua representação binária (dígitos na representação binária são usualmente chamados de *bits*). Agora o menor número com $n+1$ bits é $2^n$, portanto os subconjuntos correspondem aos números $0,1,2,\ldots,2^n-1$. Está claro que a quantidade desses números é $2^n$, daí a quantidade de subconjuntos é $2^n$.

Agora podemos responder à nossa pergunta sobre o 233º subconjunto de um conjunto de 10 elementos. Temos que converter 233 à notação binária. 233 é ímpar, portanto seu último dígito binário (bit) será 1. Vamos cortar fora esse último bit. Isso é o mesmo que subtrair 1 de 233 e depois dividí-lo por 2: obtemos $(233-1)/2 = 116$. Esse número é par, portanto seu último bit será 0. Vamos cortar fora esse bit novamente; obtemos $(116-0)/2 = 58$. Novamente, o último é 0, e cortando-o fora obtemos $(58-0)/2 = 29$. Esse é ímpar, portanto seu último bit é 1, e cortando-o fora obtemos $(29-1)/2 = 14$. Cortando fora um 0, obtemos $(14-0)/2 = 7$; cortando fora um 1, obtemos $(7-1)/2 = 3$; cortando fora um 1, obtemos $(3-1)/2 = 1$; cortando fora um 1, obtemos 0. Portanto a forma binária de 233 é 11101001.

Segue que se $a_1, ..., a_{10}$ são os elementos de nosso conjunto, então o 233º subconjunto de um conjunto de 10-elementos consiste dos elementos $\{a_{10}, a_7, a_5, a_4, a_3\}$.

**Comentários.** Apresentamos duas provas do teorema 1.3.1. Você pode estar se perguntando por que precisamos de duas provas. Certamente não porque uma única prova não teria provido suficiente confiança na veracidade do enunciado! Diferentemente de um procedimento legal, uma prova matemática ou dá absoluta certeza ou então ela é inútil. Não importa quantas provas incompletas apresentemos, elas não se somam para compor uma prova completa.

Aliás, a propósito, poderíamos lhe pedir para confiar, e não apresentar qualquer prova. Mais adiante em alguns casos isso será necessário, quando enunciaremos teoremas cuja prova é longa demais ou complicada demais para ser incluída nesse livro introdutório.

Portanto, por que cuidamos de apresentar uma prova, imagine duas provas do mesmo enunciado? A resposta é que toda prova revela muito mais que apenas o simples fato enunciado no teorema, e esse elemento a mais pode ser mais valioso que o

próprio teorema. Por exemplo, a primeira prova apresentada acima introduziu a idéia de quebrar a seleção de um subconjunto em decisões independentes, e a representação dessa idéia por uma "árvore de decisão"; usaremos essa idéia repetidamente.

A segunda prova introduziu a idéia de enumeração desses subconjuntos (rotulando-os com inteiros $0, 1, 2, \ldots$). Também vimos um método importante de contagem: estabelecemos uma correspondência entre os objetos que desejamos contar (os subconjuntos) e alguns outros tipos de objetos que podemos contar facilmente (os números $0, 1, \ldots, 2^n - 1$). Nessa correspondência

— para todo subcojunto, tínhamos exatamente um número correspondente, e

— para todo número, tínhamos exatamente um subconjunto correspondente.

Uma correspondência com essas propriedades é chamada de uma *correspondência um-para-um* (ou *bijeção*). Se pudermos fazer uma correspondência um-para-um entre os elementos de dois conjuntos, então eles têm o mesmo número de elementos.

**1.22** Dada a correspondência entre números e subconjuntos descrita acima, que números correspondem a (a) subconjuntos com 1 elemento, (b) o conjunto todo? (c) Que conjuntos correspondem a números pares?

**1.23** Qual é o número de subconjuntos de um conjunto com $n$ elementos, contendo um dado elemento?

**1.24** Mostre que um conjunto não-vazio tem o mesmo número de subconjuntos ímpares (i.e., subconjuntos com um número ímpar de elementos) que subconjuntos pares.

**1.25** Qual é o número de inteiros com (a) no máximo $n$ dígitos (decimais); (b) exatamente $n$ dígitos (não esqueça que existem números positivos e negativos!)?

## 1.4 O número aproximado de subconjuntos

Portanto sabemos que o número de subconjuntos de um conjunto de 100 elementos é $2^{100}$. Esse é um número grande, mas quão grande? Seria bom saber, no mínimo, quantos dígitos terá na forma decimal usual. Usando computadores, não seria muito difícil encontrar a forma decimal desse número ($2^{100} = 1267650600228229401496703205376$), mas suponha que não tenhamos computadores à mão. Podemos pelo menos estimar a ordem de magnitude desse número?

Sabemos que $2^3 = 8 < 10$, e daí $2^{99} < 10^{33}$. Por conseguinte, $2^{100} < 2 \cdot 10^{33}$. Agora $2 \cdot 10^{33}$ é um 2 seguido por 33 zeros; ele tem 34 dígitos, e portanto $2^{100}$ tem no máximo 34 dígitos.

Sabemos também que $2^{10} = 1024 > 1000 = 10^3$; esses dois números são bastante próximos um do outro[2]. Daí $2^{100} > 10^{30}$, o que significa que $2^{100}$ tem pelo menos 31 dígitos.

[2]O fato de que $2^{10}$ é tão prŕximo a $10^3$ é usado — ou mesmo mal-usado — no nome "kilobyte", que significa 1024 bytes, embora ele devesse significar 1000 bytes, tal qual um "kilograma" significa 1000 gramas. Igualmente, "megabyte" significa $2^{20}$ bytes, o que é próximo a 1 milhão de bytes, mas não exatamente igual.

Isso nos dá uma idéia razoavelmente boa do tamanho de $2^{100}$. Com um pouco mais de matemática de segundo grau, podemos obter exatamente o número de dígitos. O que significa dizer que um número tem exatamente $k$ dígitos? Significa que ele está entre $10^{k-1}$ e $10^k$ (o limitante inferior é permitido, o superior não). Desejamos encontrar o valor de $k$ para o qual

$$10^{k-1} \leq 2^{100} < 10^k.$$

Agora podemos escrever $2^{100}$ na forma $10^x$, apenas $x$ não será um inteiro: o valor apropriado de $x$ é $x = \lg 2^{100} = 100 \lg 2$. Temos então

$$k - 1 \leq x < k,$$

o que significa que $k-1$ é o maior inteiro não superior a $x$. Matemáticos têm um nome para isso: é a *parte inteira* ou *piso* de $x$, e é representada por $\lfloor x \rfloor$. Podemos também dizer que obtemos $k$ arredondando $x$ para baixo para o próximo inteiro. Há também um nome para o número obtido arredondando-se $x$ para cima para o próximo inteiro: ele é chamado de *teto* de $x$, e representado por $\lceil x \rceil$.

Usando qualquer calculadora científica (ou tabela de logaritmos), vemos que $\lg 2 \approx 0,30103$, portanto $100 \lg 2 \approx 30.103$, e aproximando isso para baixo obtemos que $k - 1 = 30$. Por conseguinte $2^{100}$ tem 31 dígitos.

**1.26** Quantos bits (dígitos binários) $2^{100}$ tem se for escrito na base 2?

**1.27** Encontre uma fórmula para o número de dígitos de $2^n$.

## 1.5 Seqüências

Motivados pela "codificação" de subconjuntos como cadeias de 0's e 1's, podemos querer determinar o número de cadeias de comprimento $n$ compostas de algum outro conjunto de símbolos, por exemplo, $a$, $b$ e $c$. O argumento que demos para o caso de 0's e 1's pode ser transportado para esse caso sem qualquer mudança essencial. Podemos observar que para o primeiro elemento da cadeia, podemos escolher qualquer dos $a$, $b$ e $c$, isto é, temos 3 escolhas. Independentemente do que escolhermos, existem 3 escolhas para o segundo elemento da cadeia, de modo que o número de maneiras de escolher os primeiros dois elementos é $3^2 = 9$. Continuando de maneira semelhante, obtemos que o número de maneiras de escolher a cadeia inteira é $3^n$.

Na verdade, o número 3 não tem qualquer papel especial aqui; o mesmo argumento prova o seguinte teorema:

**Teorema 1.5.1** *O número de cadeias de comprimento $n$ compostas de $k$ elementos dados é $k^n$.*

O problema seguinte leva a uma generalização dessa questão. Suponha que um banco de dados tem 4 campos: o primeiro, contendo uma abreviação de 8-caracteres do nome de um empregado; o segundo, M ou F para o sexo; o terceiro, o aniversário do empregado, no formato mm-dd-aa (desconsiderando o problema de não ser capaz de distinguir empregados nascidos em 1880 de empregados nascidos em 1980); e o

quarto, um código de função que pode ser um de 13 possibilidades. Quantos registros diferentes são possíveis?

O número será certamente grande. Já sabemos do teorema 1.5.1 que o primeiro campo pode conter $26^8 > 200.000.000.000$ nomes (a maioria desses será muito difícil de pronunciar, e não são prováveis de ocorrer, mas vamos contá-los todos como possibilidades). O segundo campo tem 2 entradas possíveis; o terceiro, 36524 entradas possíveis (o número de dias em um século); o último, 13 entradas possíveis.

Agora como determinamos o número de maneiras pelas quais essas entradas podem ser combinadas? O argumento que descrevemos acima pode ser repetido, tal como "3 escolhas" tem que ser substituído, na ordem, por "$26^8$ escolhas", "2 escolhas", "$36524$ escolhas" e "13 escolhas". Obtemos que a resposta é $26^8 \cdot 2 \cdot 36524 \cdot 13 = 198307192370919424$.

Podemos formular a seguinte generalização do teorema 1.5.1. A prova consiste da repetição do argumento acima.

**Teorema 1.5.2** *Suponha que desejemos formar cadeias de comprimento $n$ de modo que possamos usar qualquer dos elementos de um dado conjunto de $k_1$ símbolos como o primeiro elemento da cadeia, qualquer dos elementos de um dado conjunto de $k_2$ símbolos como o segundo elemento da cadeia, etc., qualquer dos elementos de um dado conjunto de $k_n$ símbolos como o último elemento da cadeia. Então o número total de cadeias que podemos formar é $k_1 \cdot k_2 \cdot \ldots \cdot k_n$.*

Como um outro caso especial, considere o problema: quantos inteiros não-negativos têm exatamente $n$ dígitos (em decimal)? Está claro que o primeiro dígito pode ser qualquer um dos 9 números $(1, 2, \ldots, 9)$, enquanto que o segundo, terceiro, etc. dígitos podem ser qualquer dos 10 dígitos. Por conseguinte obtemos um caso especial da questão anterior com $k_1 = 9$ e $k_2 = k_3 = \ldots = k_n = 10$. Por conseguinte a resposta é $9 \cdot 10^{n-1}$. (cf. exercício 1.25).

**1.28** Desenhe uma árvore ilustrando a maneira que contamos o número de cadeias de comprimento 2 formadas dos caracteres $a, b$ e $c$, e explique como ela dá a resposta. Faça o mesmo para o problema mais geral quando $n = 3$, $k_1 = 2$, $k_2 = 3$, $k_3 = 2$.

**1.29** Numa loja de esportes, existem camisetas de 5 cores diferentes, calções de 4 cores diferentes, e meias de 3 cores diferentes. Quantos uniformes diferentes você pode compor com esses itens?

**1.30** Em um bilhete de loteria esportiva, você tem que apostar 1, 2, ou X para cada um dos 13 jogos. De quantas maneiras você pode preencher o bilhete?

**1.31** Jogamos um dado duas vezes; quantos resultados diferentes você pode ter? (Um 1 seguido por um 4 é diferente de um 4 seguido por um 1.)

**1.32** Temos 20 presentes diferentes que desejamos distribuir para 12 crianças. Não é exigido que toda criança obtenha algo; poderia acontecer que damos todos os presentes à mesma criança. De quantas maneiras podemos distribuir os presentes?

**1.33** Temos 20 tipos de presentes; dessa vez, temos um grande suprimento de cada. Desejamos dar presentes a 12 crianças. Novamente, não é exigido que toda criança obtenha algo; mas nenhuma criança possa ganhar duas cópias do mesmo presente. De quantas maneiras podemos dar presentes?

## 1.6 Permutações

Durante a festa, já havíamos encontrado o problema: de quantas maneiras podemos sentar $n$ pessoas em $n$ cadeiras (bem, havíamos encontrado o problema para $n = 6$ e $n = 7$, mas a questão é suficientemente natural para qualquer $n$). Se imaginarmos que as cadeiras são numeradas, então encontrar um assentamento para essas pessoas é o mesmo que associá-las aos números $1, 2, \ldots, n$ (ou $0, 1, \ldots, n-1$ se desejamos agradar aos lógicos). Ainda uma outra maneira de dizer isso é ordenar as pessoas em uma única fila, ou montar uma lista (ordenada) com seus nomes.

Se temos uma lista de $n$ objetos (um conjunto ordenado, onde é especificado qual elemento é primeiro, segundo etc.), e os rearranjamos de modo que eles estejam em uma outra ordem, isso é chamado de *permutá*-los; a nova ordem é também chamada de uma *permutação* dos objetos. Também chamamos a rearrumação que não muda nada, uma permutação (um pouco no espírito de chamar o conjunto vazio de um conjunto).

Por exemplo, o conjunto $\{a, b, c\}$ tem as seguintes 6 permutações:

$$abc, acb, bac, bca, cab, cba.$$

Portanto, a questão é determinar o número de maneiras pelas quais $n$ objetos podem ser ordenados, i.e., o número de permutações de $n$ objetos. A solução encontrada pelas pessoas na festa funciona em geral: podemos por qualquer das $n$ pessoas no primeiro lugar; independentemente de quem escolhemos, temos $n-1$ escolhas para o segundo. Portanto o número de maneiras de preencher as primeiras duas posições é $n(n-1)$. Independentemente de como tenhamos preenchido a primeira e a segunda posições, existem $n-2$ escolhas para a terceira posição, de modo que número de maneiras de preencher as primeiras três posições é $n(n-1)(n-2)$.

Está claro que esse argumento continua assim até que todas as posições forem preenchidas. A penúltima posição pode ser preenchida de duas maneiras; a pessoa colocada na última posição é determinada, se as outras posições sejam preenchidas. Por conseguinte, o número de maneiras de preencher todas as posições é $n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1$. Esse produto é tão importante que temos uma notação para ele: $n!$ (leia $n$ fatorial). Em outras palavras, $n!$ é o número de maneiras de ordenar $n$ objetos. Com essa notação, podemos enunciar nosso segundo teorema.

**Teorema 1.6.1** *O número de permutações de $n$ objetos é $n!$.*

Novamente, podemos ilustrar o argumento acima graficamente (Figura 1.3). Começamos com o nó no topo, que põe nossa primeira decisão: quem devemos sentar na primeira cadeira? As 3 setas saindo correspondem às três respostas possíveis à questão. Tomando uma decisão, podemos seguir uma das setas em direção ao nó seguinte. Esse carrega o próximo problema de decisão: quem devemos colocar na segunda cadeira? As duas setas saindo do nó representam as duas escolhas possíveis.

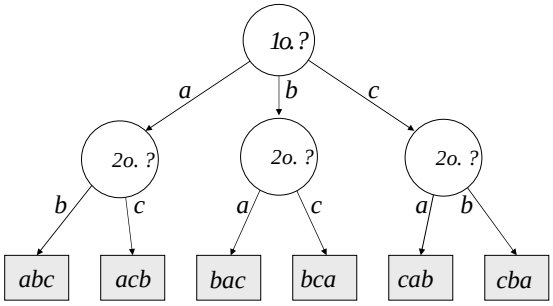


Figura 1.3: Uma árvore de decisão para selecionar uma permutação de $\{a, b, c\}$.

(Note que essas escolhas são diferentes para nós diferentes nesse nível; o que é importante é que existem duas setas saindo de cada nó.) Se tomamos uma decisão e seguimos a seta correspondente para o nó seguinte, sabemos quem senta na terceira cadeira. O nó carrega a "ordem de assentamento" inteira.

Está claro que para um conjunto com $n$ elementos, $n$ setas deixam o nó no topo, e portanto existem $n$ nós no nível seguinte. $n-1$ setas saem de cada um desses, portanto existem $n(n-1)$ nós no terceiro nível. $n-2$ setas saem de cada um desses, etc. O nível mais ao fundo tem $n!$ nós. Isso mostra que existem exatamente $n!$ permutações.

**1.34** $n$ rapazes e $n$ garotas saem para dançar. De quantas maneiras eles podem todos dançar simultaneamente? (Assumimos que somente casais de sexo diferente dançam um com o outro.)

**1.35** (a) De quantas maneiras 8 pessoas podem jogar xadrez na interpretação de Alice da questão?

(b) Você pode dar uma fórmula geral para $2n$ pessoas?

## 1.7 O número de subconjuntos ordenados

Numa competição de 100 atletas, apenas a ordem dos primeiros 10 é registrada. Quantos resultados diferentes tem a competição?

Essa questão pode ser respondida na linha dos argumentos que vimos. O primeiro lugar pode ser vencido por qualquer dos atletas; independente de quem vença, existem 99 possíveis vencedores do segundo lugar, de modo que os dois primeiros prêmios podem sair de $100 \cdot 99$ maneiras. Dados os primeiros dois, existem 98 atletas que podem ser terceiros, etc. Portanto a resposta é $100 \cdot 99 \cdot \ldots \cdot 91$.

**1.36** Ilustre esse argumento por meio de uma árvore.

**1.37** Suponha que registremos a ordem de todos os 100 atletas.

(a) Quantos resultados diferentes podemos então ter?

(b) Quantos desses dão o mesmo para os 10 primeiros lugares?

(c) Mostre que o resultado acima para o número de possíveis resultados para os 10 primeiros lugares podem também ser obtidos usando (a) e (b).

Não há nada especial sobre os números 100 e 10 no problema acima; poderíamos fazer o mesmo para $n$ atletas com os $k$ primeiros lugares registrados.

Para dar uma forma mais matemática ao resultado, podemos substituir os atletas por qualquer conjunto de tamanho $n$. A lista dos $k$ primeiros lugares é dada por uma seqüência de $k$ elementos de $n$, de forma que todos têm que ser diferentes. Podemos também ver esse procedimento como selecionando um subconjunto dos atletas com $k$ elementos, e então os ordenando. Por conseguinte, temos o teorema a seguir.

**Teorema 1.7.1** *O número de subconjuntos ordenados com $k$ elementos de um conjunto com $n$ elementos é $n(n-1)\dots(n-k+1)$.*

(Note que se começarmos com $n$ e contarmos $k$ números, o último será $n-k+1$.)

É longo demais falar em termos de "conjuntos com $n$ elementos" e "subconjuntos com $k$ elementos"; daí é conveniente abreviar essas expressões para "$n$-conjuntos" e "$k$-subconjuntos". Portanto o número de $k$-subconjuntos ordenados de um $n$-conjunto é $n(n-1)\dots(n-k+1)$.

**1.38** Se você generalizar a solução do exercício 1.37, você obtém a resposta na forma

$$\frac{n!}{(n-k)!}$$

Verifique que esse é o mesmo número tal qual dado no teorema 1.7.1.

**1.39** Explique a semelhança e a diferença entre as questões de contagem respondidas pelo teorema 1.7.1 e pelo teorema 1.5.1.

## 1.8 O número de subconjuntos de um dado tamanho

Daqui, podemos facilmente derivar um dos mais importantes resultados de contagem.

**Teorema 1.8.1** *O número de $k$-subconjuntos de um $n$-conjunto é*

$$\frac{n(n-1)\dots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

**Prova.** Recordemos que se contarmos subconjuntos *ordenados*, obtemos $n(n-1)\dots(n-k+1) = n!/(n-k)!$, pelo Teorema 1.7.1. É claro que, se desejamos saber o número de subconjuntos *não-ordenados*, então contamos demais; todo subconjunto foi contado exatamente $k!$ vezes (com toda ordenação possível de seus elementos). Portanto temos que dividir esse número por $k!$ para obter o número de subconjuntos com $k$ elementos (sem ordenação). □

O número de $k$-subconjuntos de um $n$-conjunto é uma quantidade tão importante que é preciso uma notação separada para ele: $\binom{n}{k}$ (leia: 'de $n$ escolha $k$'). Por conseguinte,

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \tag{1.6}$$

Daí o número de bilhetes de loteria diferentes é $\binom{90}{5}$, o número de apertos-de-mão é $\binom{7}{2}$ etc. Os números $\binom{n}{k}$ são também chamados de *coeficientes binomiais* (na Seção 3.1 veremos por que).

**1.40** Quais problemas discutidos durante a festa eram casos especiais do teorema 1.8.1?

**1.41** Faça uma tabela com os valores de $\binom{n}{k}$ para $n, k \leq 5$.

**1.42** Ache os valores de $\binom{n}{k}$ para $k = 0, 1, n-1, n$ através de (1.6), e explique os resultados por meio do significado combinatório de $\binom{n}{k}$.

Coeficientes binomiais satisfazem muitas igualdades importantes. No próximo teorema reunimos algumas dessas; algumas outras igualdades ocorrerão nos exercícios e no próximo capítulo.

**Teorema 1.8.2** *Coeficientes binomiais satisfazem as seguintes igualdades:*

$$\binom{n}{k} = \binom{n}{n-k}; \tag{1.7}$$

*Se* $n, k > 0$*, então*

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}; \tag{1.8}$$

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n-1} + \binom{n}{n} = 2^n. \tag{1.9}$$

**Prova.** Provamos (1.7) apelando para o significado combinatório de ambos os lados. Temos um conjunto de $n$-elementos, digamos $S$. O lado esquerdo conta subconjuntos de $k$-elementos de $S$, enquanto que o lado direito conta subconjuntos de $(n-k)$-elementos de $S$. Para ver que esses números são os mesmos, precisamos apenas observar que juntamente com todo subconjunto de $k$-elementos vai um subconjunto de $(n-k)$-elementos: seu *complemento de um conjunto*, que contém exatamente aqueles elementos de $S$ que não estão contidos no conjunto de $k$-elementos. Isso emparelha subconjuntos de $k$-elementos com os subconjuntos de $(n-k)$-elementos, mostrando que existe o mesmo número de ambos.

Vamos provar (1.8) usando a fórmula algébrica (1.6). Após substituição, a igualdade fica

$$\frac{n!}{k!(n-k)!} = \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-k-1)!}.$$

Podemos dividir ambos os lados por $(n-1)!$, e multiplicar por $(k-1)!(n-k-1)!$; então a identidade fica

$$\frac{n}{k(n-k)} = \frac{1}{n-k} + \frac{1}{k},$$

que pode ser verificada por fácil manipulação algébrica.

Finalmente, provamos (1.9) através da interpretação combinatória novamente. Mais uma vez, seja $S$ um conjunto de $n$-elementos. O primeiro termo no lado esquerdo

conta os subconjuntos de 0-elementos de $S$ (existe apenas um, o conjunto vazio); o segundo termo conta subconjuntos de 1-elemento; o próximo termo, subconjuntos de 2-elementos etc. Na soma completa, todo subconjunto de $S$ é contado exatamente uma vez. Sabemos que $2^n$ (o lado direito) é o número de todos os subconjuntos de $S$. Isso prova (1.9), e completa a prova do Teorema 1.8.2. □

**1.43** Encontre uma prova de (1.7) usando a fórmula algébrica para $\binom{n}{k}$, e de (1.8), usando o significado combinatório de ambos os lados.

**1.44** Prove que $\binom{n}{2} + \binom{n+1}{2} = n^2$; dê duas provas, uma usando a interpretação combinatória e a outra, usando a fórmula algébrica para os coeficientes binomiais.

**1.45** Prove (novamente, de duas maneiras) que $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$.

**1.46** Prove (de duas maneiras) que para $0 \leq c \leq b \leq a$,

$$\binom{a}{b}\binom{b}{c} = \binom{a}{a-c}\binom{a-c}{b-c}$$

# Exercícios de Revisão

**1.47** De quantas maneiras você pode assentar 12 pessoas em duas mesas redondas com 6 lugares em cada uma? Pense nas possíveis maneiras de definir quando dois assentamentos são diferentes, e encontre a resposta para cada um.

**1.48** Nomeie conjuntos com cardinalidade (a) 365, (b) 12, (c) 7, (d) 11.5, (e) 0, (f) 1024.

**1.49** Liste todos os subconjuntos de $\{a, b, c, d, e\}$ contendo $\{a, e\}$ mas não contendo $c$.

**1.50** Não escrevemos todas as relações de subconjunto entre vários conjuntos de números; por exemplo, $\mathbb{Z} \subseteq \mathbb{R}$ também é verdadeiro. Quantas tais relações você pode encontrar entre os conjuntos $\emptyset, \mathbb{N}, \mathbb{Z}_+, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$?

**1.51** Qual é a interseção entre
(a) o conjunto dos inteiros positivos cujo último dígito é 3, e o conjunto dos números pares;
(b) o conjunto dos números divisíveis por 5 e o conjunto dos números pares?

**1.52** Sejam $A = \{a, b, c, d, e\}$ e $B = \{c, d, e\}$. Liste todos os subconjuntos de $A$ cuja interseção com $B$ tenha 1 elemento.

**1.53** Três conjuntos têm 5, 10 e 15 elementos, respectivamente. Quantos elementos podem ter sua união e sua interseção?

**1.54** Qual é a diferença simétrica de $A$ e $A$?

**1.55** Forme a diferença simétrica de $A$ e $B$, para obter um conjunto $C$. Forme a diferença simétrica de $A$ e $C$. Que conjunto você obtém?

**1.56** Sejam $A, B, C$ três conjuntos e assuma que $A$ é um subconjunto de $C$. Prove que

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

Mostre por um exemplo que a condição de que $A$ é um subconjunto de $C$ não pode ser omitida.

**1.57** Qual é a diferença $A \setminus B$, se

(a) $A$ é o conjunto dos números primos e $B$ é o conjunto números ímpares?

(b) $A$ é o conjunto dos números reais não-negativos e $B$ é o conjunto dos números reais não-positivos?

**1.58** Prove que para quaisquer três conjuntos $A, B, C$,

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

**1.59** Seja $A$ um conjunto e suponha que $\binom{A}{2}$ represente o conjunto de todos os subconjuntos de 2-elementos de $A$. Qual dos seguintes enunciados é verdadeiro?

$$\binom{A \cup B}{2} = \binom{A}{2} \cup \binom{B}{2}; \qquad \binom{A \cup B}{2} \supseteq \binom{A}{2} \cup \binom{B}{2};$$

$$\binom{A \cap B}{2} = \binom{A}{2} \cap \binom{B}{2}; \qquad \binom{A \cap B}{2} \subseteq \binom{A}{2} \cap \binom{B}{2}.$$

**1.60** Seja $B$ um subconjunto de $A$, $|A| = n$, $|B| = k$. Qual é a quantidade de subconjuntos de $A$ cuja interseção com $B$ tem 1 elemento?

**1.61** Calcule a forma binária de $25$ e $35$, e calcule sua soma na notação binária. Verifique os resultados em confronto com adicionar $25$ e $35$ na notação decimal usual, e então convertê-lo para binário.

**1.62** Prove que todo inteiro positivo pode ser escrito como a soma de potências diferentes de 2. Prove também que para um dado número, existe apenas uma maneira de fazê-lo.

**1.63** Começando de Washington, DC, de quantas maneiras você pode visitar 5 das outras 50 capitais de estado e retornar a Washington?

**1.64** Encontre o número de todos os inteiros de 20-dígitos nos quais nenhum par de dígitos consecutivos são iguais.

**1.65** Alice tem 10 bolas (todas diferentes). Primeiro, ela as divide em duas pilhas; então ela apanha uma das pilhas com pelo menos dois elementos, e a divide em duas; ela repete isso até que cada pilha tenha apenas um elemento.

(a) Quantos passos isso leva?

(b) Mostre que número de maneiras diferentes nas quais ela pode realizar esse procedimento é

$$\binom{10}{2} \cdot \binom{9}{2} \cdot \ldots \cdot \binom{3}{2} \cdot \binom{2}{2}.$$

[Dica: imagine o procedimento de trás-para-frente.]

**1.66** Você deseja enviar cartões postais a 12 amigos. Na loja, existem apenas 3 tipos de cartões postais. De quantas maneiras você pode enviar os cartões postais, se

(a) existe um número grande de cada cartão postal, e você deseja enviar um cartão a cada amigo;

(b) existe um número grande de cada cartão postal, e você deseja enviar um ou mais cartões para cada amigo (mas ninguém deve receber dois cartões idênticos);

(c) a loja tem apenas 4 exemplares de cada cartão, e você deseja enviar um cartão para cada amigo?

**1.67** Qual é o número de maneiras de colorir $n$ objetos com 3 cores, se cada cor tem que ser usada pelo menos uma vez?

**1.68** Desenhe uma árvore para solução de Alice de quantificar o número de maneiras que 6 pessoas podem jogar xadrez, e explique o argumento de Alice usando a árvore.

**1.69** Quantas palavras diferentes você pode obter rearranjando as letras da palavra MATEMÁTICA?

**1.70** Encontre todos os inteiros positivos $a$, $b$ e $c$ para os quais

$$\binom{a}{b}\binom{b}{c} = 2\binom{a}{c}.$$

**1.71** Prove que

$$\binom{n}{k} = \binom{n-2}{k} + 2\binom{n-2}{k-1} + \binom{n-2}{k-2}.$$

**1.72** 20 pessoas estão sentadas ao redor de uma mesa. De quantas maneiras podemos escolher 3 pessoas, sem que nunca duas delas sejam vizinhas?