Matem@tica na Pr@tica

Curso de Especialização em Ensino de Matemática para o Ensino Médio

UAB UNIVERSIDADE ABERTA DO BRASIL

Matem@tica na Pr@tica

Curso de Especialização em Ensino de Matemática para o Ensino Médio

Módulo II

Matemática discreta

Daniel Cordeiro de Morais Filho
Pedro Luiz Aparecido Malagutti

CENTRAL DE TEXTO

Curso de Especialização em Ensino de Matemática para o Ensino Médio

Equipe de especialistas em formação de professores de Matemática
Coordenação: Paulo Antonio Silvani Caetano (DM-UFSCar)
Especialistas: Cláudio Carlos Dias (UFRN), Daniel Cordeiro de Morais Filho (DME-UFCG), Francisco Roberto Pinto Mattos (UERJ e Colégio Pedro II) João Carlos Vieira Sampaio (DM-UFSCar), Marlusa Benedetti da Rosa (CAp-UFRGS), Pedro Luiz Aparecido Malagutti (DM-UFSCar), Roberto Ribeiro Paterlini (DM-UFSCar), Tomás Edson Barros (DM-UFSCar) e Victor Augusto Giraldo (IM-UFRJ)

Desenvolvimento Instrucional
Coordenação: Cristine Costa Barreto
Designers instrucionais: José Paz, Juliana Silva Bezerra, Leonardo Nahoum, Leticia Terreri, Magno Luiz Ferreira, Maria Matos, Andréia Ramos e Cíntia Nascimento

Responsáveis por este fascículo
Autores: Daniel Cordeiro de Morais Filho e Pedro Luiz Aparecido Malagutti
Leitor: Francisco Roberto Pinto Mattos
Designers instrucionais: Cristine Costa Barreto, José Paz e Letícia Terreri

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Morais Filho, Daniel Cordeiro de
Matemática discreta : módulo II / Daniel Cordeiro de Morais Filho, Pedro Luiz Aparecido Malagutti. -- Cuiabá, MT : Central de Texto, 2013. -- (Matem@tica na pr@tica. Curso de especialização em ensino de matemática para o ensino médio)

Bibliografia.
ISBN 978-85-8060-020-9

1. Ensino médio 2. Matemática - Estudo e ensino 3. Matemática - Formação de professores I. Malagutti, Pedro Luiz Aparecido. II. Título. III. Série.

13-07090 CDD-510.7

Índices para catálogo sistemático:
1. Ensino de matemática para ensino médio 510.7

Produção Editorial - Central de Texto
Editora: Maria Teresa Carrión Carracedo
Produção gráfica: Ricardo Miguel Carrión Carracedo
Projeto gráfico: Helton Bastos
Paginação: Maike Vanni
Revisão para publicação: Henriette Marcey Zanini

Apresentação

O Matem@tica na Pr@tica é um Curso de Especialização para Professores do Ensino Médio de Matemática na modalidade de Educação a Distância, que está inserido no Plano de Ações Articuladas do Ministério da Educação. Esse plano tem como um de seus objetivos promover uma importante atividade de formação continuada dirigida a você, professor do ensino básico, incentivando a renovação de sua prática pedagógica e propondo caminhos para que você possa criar, organizar e compartilhar novos conhecimentos com seus alunos e colegas de trabalho.

Esse segundo módulo consiste em quatro disciplinas e caracteriza-se pela apresentação de conteúdos importantes para o Ensino Médio, de uma forma conectada com o trabalho do professor.

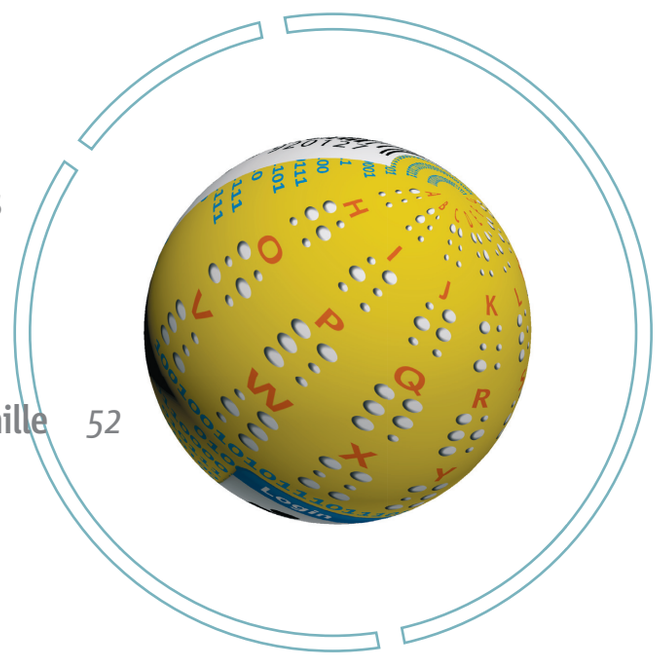
Neste fascículo apresentamos a disciplina denominada "Matemática Discreta", que tem por objetivo refletir sobre a importância dos métodos de contagem no Ensino Médio, explorar as técnicas de combinatória e desenvolver o conceito de probabilidade.

Desejamos a todos bons estudos.

Equipe do Matem@tica na Pr@tica
Março, 2013


Login
Nome do usu
Senha

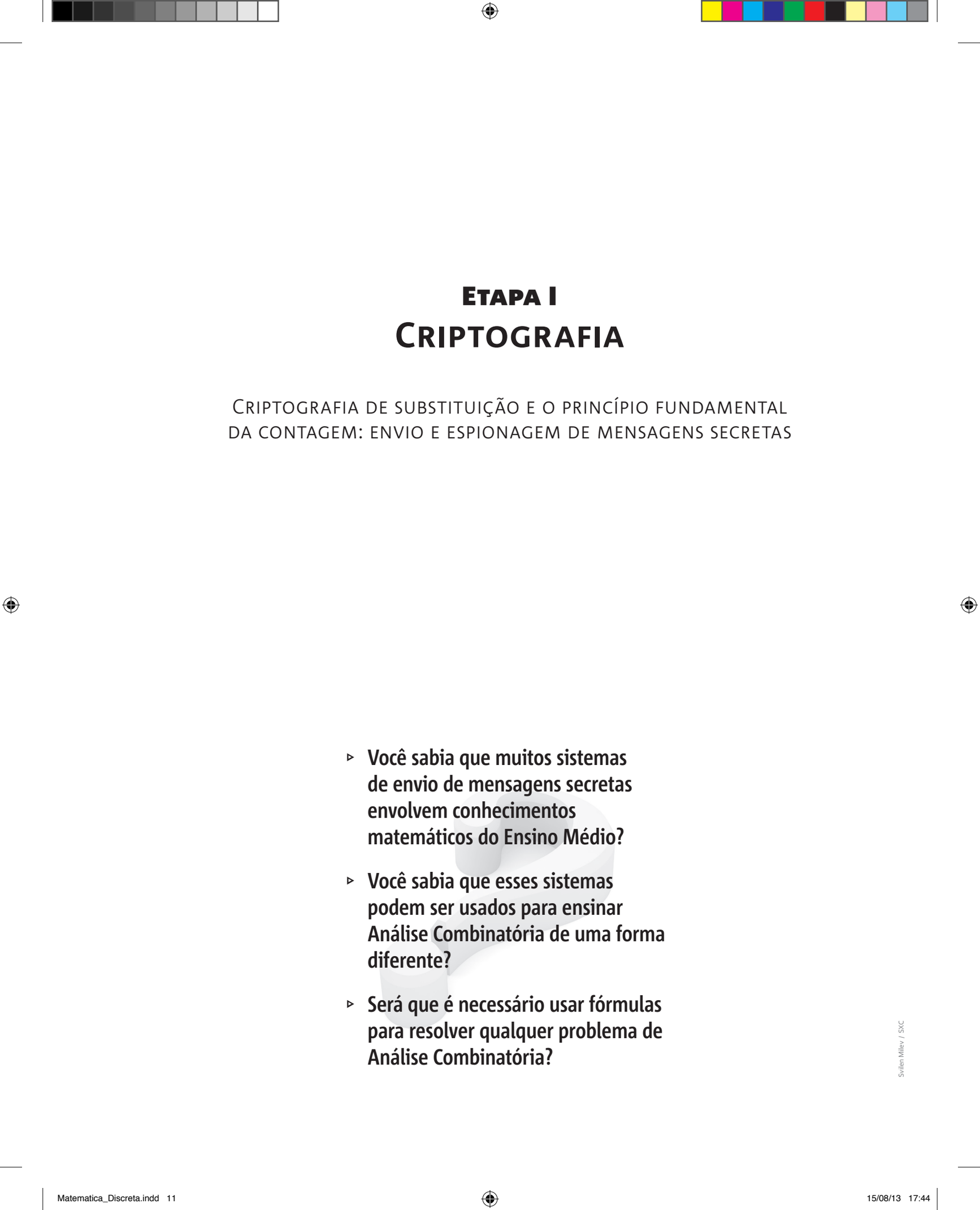
Sumário



Etapa I
Criptografia

Criptografia de substituição e o princípio fundamental da contagem: envio e espionagem de mensagens secretas

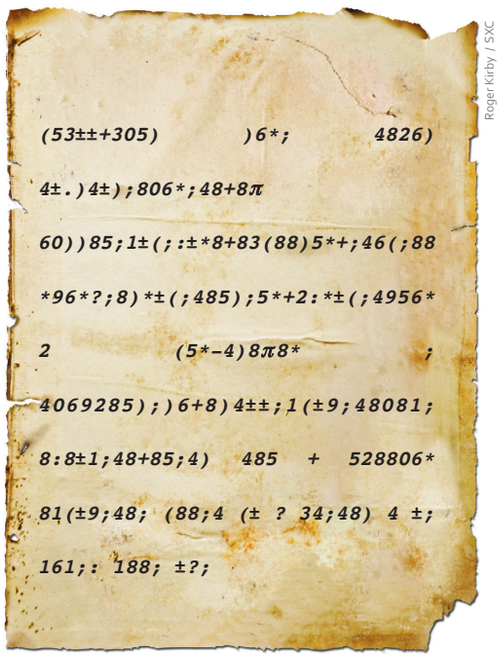
- **Você sabia que muitos sistemas de envio de mensagens secretas envolvem conhecimentos matemáticos do Ensino Médio?**
- **Você sabia que esses sistemas podem ser usados para ensinar Análise Combinatória de uma forma diferente?**
- **Será que é necessário usar fórmulas para resolver qualquer problema de Análise Combinatória?**



Svilen Milev / SXC

1. Introdução

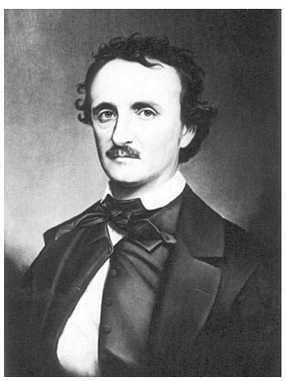
Se você encontrasse um velho pergaminho com a seguinte mensagem, o que você faria? ▶



Roger Kirby / SXC

Suspeitaria ser uma mensagem secreta para encontrar um tesouro? Tentaria desvendá-la? E se quisesse desvendá-la, você recorreria aos seus conhecimentos matemáticos? Quais conhecimentos?

No conto do escritor Edgar Allan Poe (1809-1849), intitulado "O Escaravelho de Ouro", o personagem principal da obra encontra um velho pergaminho com a mensagem ao lado que acredita ser o mapa de um tesouro.


http://upload.wikimedia.org/wikipedia/commons/thumb/f/fb/Edgar_Allan_Poe_portrait_B.jpg/250px-Edgar_Allan_Poe_portrait_B.jpg

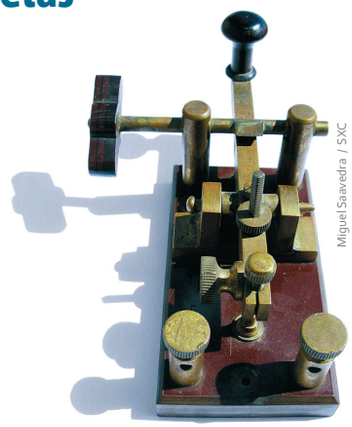
Nessa história, após uma análise feita pelo protagonista, baseada na frequência com que as letras apareciam nos textos escritos em língua inglesa, a mensagem é decifrada e o personagem principal encontra um tesouro há muito tempo enterrado por um pirata que passou pelo lugar descrito na mensagem.


Maksim Shmeljov / Shutterstock

Histórias como essas revelam que cifrar e decifrar mensagens são práticas que já acompanham a humanidade há um bom tempo.

Você suspeitaria que essa técnica pode ser utilizada para o ensino de Matemática no Ensino Médio? Esperamos que ao final dessa disciplina você possa responder positivamente!

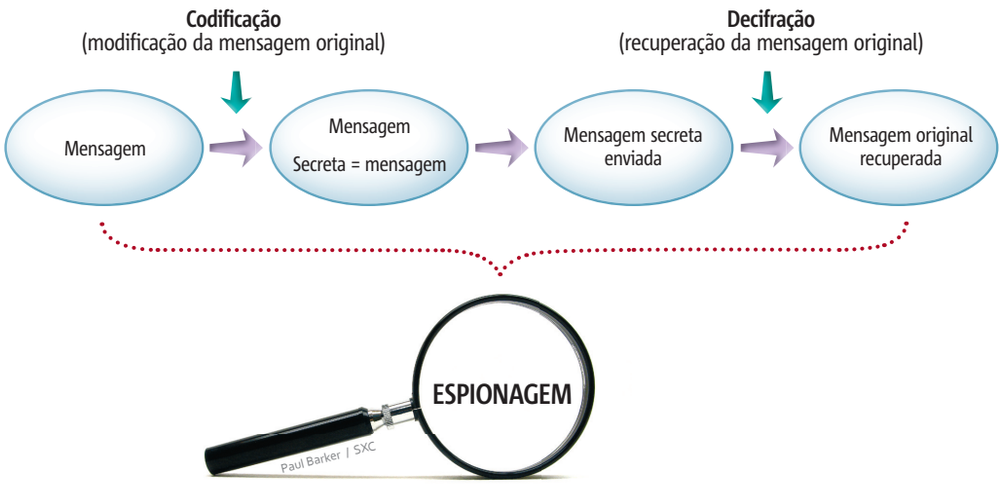
2. A matemática das mensagens secretas


Miguel Saavedra / SXC

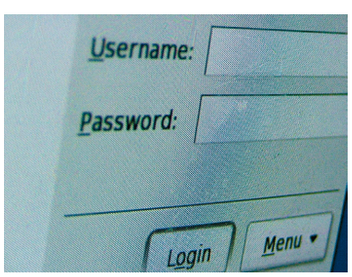
Enviar mensagens secretas é uma tarefa muito antiga. Ao longo da história, ela se intensificou principalmente pelas necessidades diplomáticas e militares de trocar informações que não podiam ser descobertas.

A técnica de enviar e receber mensagens secretas chama-se ***criptografia***. Simplificadamente, uma mensagem é enviada de forma secreta, por um sistema criptográfico, da seguinte maneira:

A **Criptografia** é a ciência que estuda os meios e métodos de se enviar mensagens com segurança. É uma área de grande interesse atualmente, principalmente devido ao extenso uso dos meios eletrônicos de comunicação.



Hoje em dia, principalmente com o advento da comunicação eletrônica, muitas atividades essenciais dependem do sigilo na troca de mensagens, em especial aquelas que envolvem transações financeiras (senhas de banco, senha de cartão de crédito etc.) e o uso seguro da internet.



Joshua Davis / SXC

Sergio Roberto Bichara / SXC


Michel Wagner / SXC

Mas qual é a relação entre a Criptografia e o ensino de Matemática? Você consegue imaginar? Você consegue vislumbrar o estudo da criptografia como uma estratégia para abordar conceitos matemáticos?

Maarten Uilenbroek / SXC

Nosso objetivo, com a disciplina Matemática Discreta, é que você possa responder a essas perguntas. Essa disciplina, que tem a Criptografia como ponto de partida, tratará de conteúdos ligados à Análise Combinatória e à Teoria das Probabilidades, que são apresentados usualmente no Ensino Médio.

A proposta é que a disciplina enfoque conteúdos por meio da resolução de problemas, já que a Análise Combinatória – como você mesmo vai perceber – não envolve muita teoria. Buscaremos contemplar um universo expressivo de aplicações e casos particulares: tanto os que podem aprofundar seus conhecimentos quanto os que podem ser utilizados em sala de aula.

Nessa primeira etapa da disciplina, especialmente, apresentaremos algumas atividades que utilizam a Criptografia. Além disso, exploraremos os aspectos matemáticos dessas atividades a fim de introduzir alguns conceitos básicos da **Análise Combinatória**. Nessas atividades, você perceberá que não é necessário o uso indiscriminado de fórmulas para resolver problemas de Análise Combinatória, as quais tanto assustam nossos alunos.

Ao longo dessa etapa, por meio de exemplos simples, você vai perceber que Criptografia e Análise Combinatória têm muito em comum!

A **Análise Combinatória**, conforme o próprio nome diz, analisa e conta o número de possibilidades de como os elementos de um conjunto podem ser agrupados conforme regras estabelecidas.

3. Criptografia de Júlio César

No Império Romano, o imperador Júlio César (100 a.C - 44 a.C.) criou um dos primeiros sistemas de criptografia conhecido. Para enviar suas mensagens, Júlio César substituía cada letra do alfabeto pela terceira letra que a seguia, da seguinte forma:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

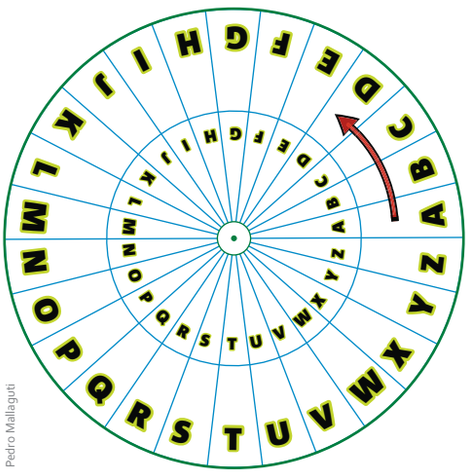
http://pt.wikipedia.org/wiki/Ficheiro:Young_Folks%27_History_of_Rome_illus254.png

Segundo esse sistema, a palavra FELICIDADE passa a ser IHOLFLGDGH.

Agora, decifre a mensagem abaixo, usando a criptografia de Júlio César:

OHJDO FRQVHJXL

Se você encontrou a mensagem **LEGAL CONSEGUI**, acertou. Para decodificar uma mensagem usando a criptografia de Júlio César, precisamos fazer o caminho inverso da codificação: substituir cada letra do alfabeto pela terceira letra que a antecede.



Pedro Mallaguti

A criptografia de Júlio César é um sistema bem simples de codificar/decodificar mensagens secretas, que pode ter diversas variações. Por exemplo, em vez de caminhar 3 letras para frente, como no exemplo anterior, podemos andar um outro número de letras para frente ou para trás e, assim, criar um novo método de cifrar mensagens.

Esse número é chamado ***chave*** ou ***senha*** do sistema criptográfico. Ele deve ser usado para codificar e decodificar a mensagem e deve ser conhecido apenas por quem a envia e por quem a recebe. No exemplo anterior, a chave foi 3 (se quisermos enfatizar a ordem crescente das letras, +3).


Guillermo Alvarez / SXC

Se um espião conhecer a chave, que é o número de letras que andamos (no nosso exemplo a chave é igual a 3), poderá facilmente decifrar uma mensagem interceptada, trocando cada letra pela terceira letra anterior.

Não se conhecendo a chave, como será possível decifrar mensagens criptografadas? Pense um pouco a respeito disso.


Maarten Ullenbroek / SXC

Nos sistemas criptográficos que seguem o princípio da criptografia de Júlio César e conservam a ordem das letras, considerando o nosso alfabeto, podemos usar 26 chaves diferentes que geram 26 sistemas criptográficos. Ora, sabemos que o sistema com chave 0 (ou 26) não codifica nada, já que nesse caso cada letra é substituída por ela mesma. Mas, diante da técnica de contagem que vamos apresentar, é importante incluí-lo.

E se pudermos mudar a ordem das letras?

No sistema criptográfico de Júlio César, o alfabeto é codificado seguindo sua ordem usual, apenas iniciando em um lugar diferente. Vejamos dois exemplos de sistemas criptográficos em que a ordem das letras não é preservada.

- a) Alfabeto quebrado ao meio:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

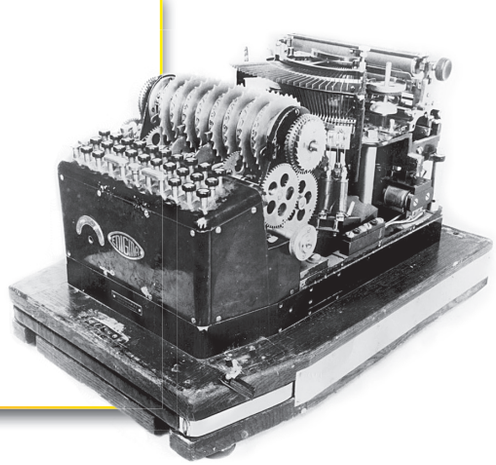
- b) Troca de dois vizinhos:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	A	D	C	F	E	H	G	J	I	L	K	N	M	P	O	R	Q	T	S	V	U	X	W	Z	Y

Observe nos exemplos anteriores que nenhuma letra ficou no seu lugar original.

Curiosidade

A máquina ao lado chama-se ***Enigma***. Foi largamente utilizada pelo exército alemão durante a Segunda Guerra Mundial (1939-1945) para enviar mensagens secretas. A máquina é um dispositivo eletromecânico que utilizava rotores para criar sistemas criptográficos, tidos como indecifráveis e altamente seguros. Entretanto, os sistemas criptográficos foram quebrados pelas Forças Aliadas, que puderam conhecer várias informações secretas importantes. Isso fez com que a Guerra terminasse pelo menos um ano antes do previsto. Sobre essa máquina, assista ao filme ***Enigma***, dirigido por Michael Apted e produzido por Mick Jagger e Lorne Michaels.

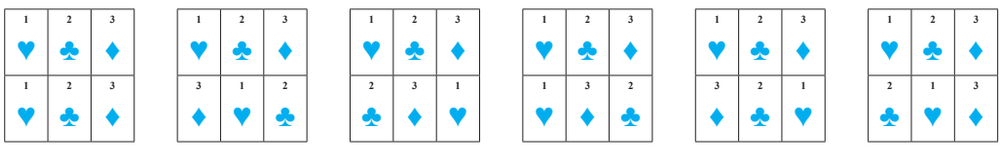


Quantos sistemas criptográficos podemos formar mudando as letras sem respeitar a ordem com que aparecem no alfabeto? Você tem algum palpite?

4. Princípios de contagem em criptografia

Para ensinarmos um método de resposta à pergunta da seção anterior, vamos trabalhar casos mais simples envolvendo alfabetos com menos letras.

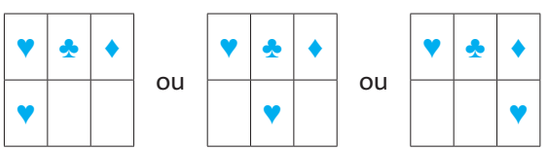
Digamos que no planeta Plunct os alfabetos fossem formados por apenas três símbolos: ♥, ♣ e ♦. Nesse caso, poderíamos criptografar mensagens das seguintes formas:



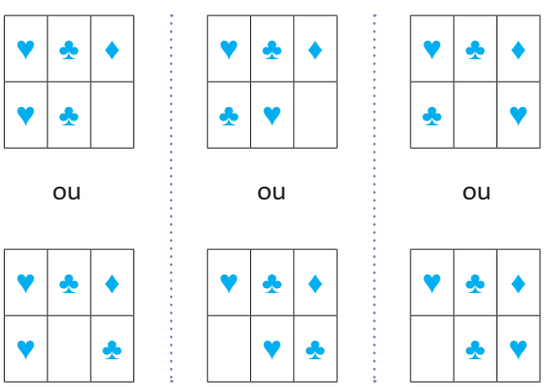
Nas primeiras linhas dessas tabelas aparecem as "letras" do alfabeto em sua "ordem natural" e nas segundas linhas, as letras que devem substituir as da primeira linha, respectivamente, quando efetuarmos uma codificação.

Olhando as tabelas, apesar de a primeira delas ser a "trivial" e não servir para codificar nada, poderíamos concluir que há exatamente seis maneiras de permutar as letras desse alfabeto?

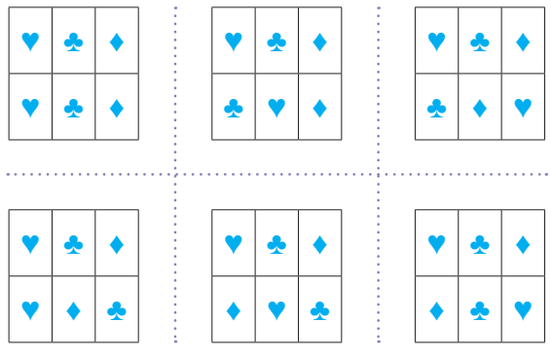
É claro que sim: para a primeira letra, existem três possibilidades de codificação:



Escolhida uma delas, restam apenas duas possibilidades para a segunda letra:



e, uma vez escolhido um desses casos, resta somente uma possibilidade para a terceira letra:



Dessa forma, tem-se:

$$3 \cdot 2 \cdot 1 = 6$$

possibilidades para fazermos uma codificação para o alfabeto utilizado no planeta Plunct.

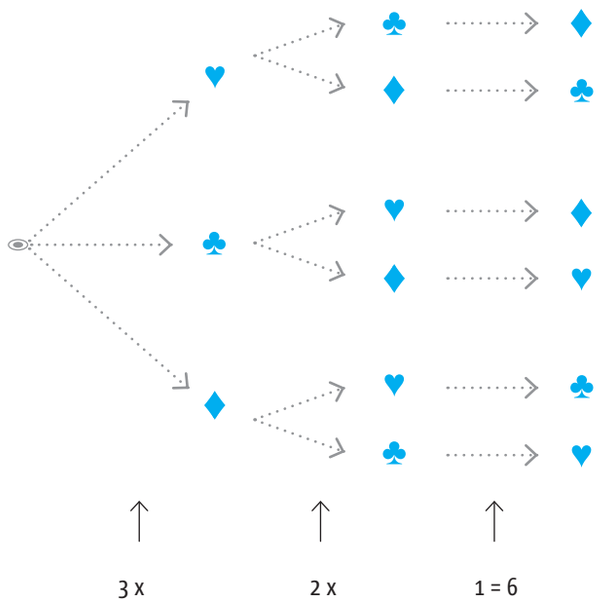
Um esquema prático para resolver esses problemas é dispor as possibilidades da seguinte forma:

3 possibilidades (locais) para se colocar a primeira letra.	Restam **2** possibilidades (locais) para se colocar a segunda letra.	Resta **1** possibilidade (local) para se colocar a terceira letra.

Depois que o esquema estiver pronto, devemos multiplicar os números de possibilidades em cada caso.

Observe que nesses problemas não há repetição de elementos. O elemento que aparece na primeira etapa não entra na segunda nem na terceira etapa. O que aparece na segunda etapa não entra na terceira etapa, e assim por diante. As decisões das escolhas são independentes.

Podemos fazer, ainda, outro esquema de representação das possibilidades, pensando simetricamente na posição e não na letra. Na primeira posição, podemos colocar qualquer uma das três letras, na segunda posição apenas duas delas e na terceira a letra remanescente.



Princípio Multiplicativo da Contagem:
Se uma decisão puder ser tomada de m maneiras diferentes, e se uma vez tomada esta primeira decisão, outra decisão, independente da primeira, puder ser tomada de n maneiras diferentes, então no total serão tomadas $m \times n$ decisões.

Independentemente da maneira de representação escolhida, calculamos o número de possibilidades do problema anterior, usando o **Princípio Multiplicativo da Contagem**, que é muito simples de ser entendido:

O Princípio Multiplicativo é também chamado Princípio Fundamental da Contagem.

Diante do Princípio Multiplicativo, no último exemplo, temos $3 \cdot 2 \cdot 1$ possibilidades de codificação, usando o alfabeto do Planeta Plunct.

Há uma notação muito útil para trabalhar com produtos do tipo acima, essa notação é chamada de ***fatorial***. Por exemplo, o fatorial do número 3 é $3! = 3 \cdot 2 \cdot 1$; o fatorial do número 7 é $7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$. No caso geral, o fatorial de um número inteiro positivo n é definido por $n! = n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1$ e, por convenção, $0! = 1$.

Vamos agora pensar outro exemplo em que se aplica o Princípio Multiplicativo da Contagem.

Em outro planeta imaginário, denominado Plact, o alfabeto possui quatro "letras": ♥, ▶, ☼ e ○. Seguindo da mesma forma que fizemos no exemplo anterior, pelo Princípio Multiplicativo da Contagem, há, neste caso, $4 \cdot 3 \cdot 2 \cdot 1 = 4! = 24$ maneiras diferentes de permutar as letras.

Vamos comprovar nosso cálculo?
Vejamos:

Voltemos agora ao nosso mundo, mais precisamente voltemos à pergunta que fizemos no final da última seção. O que ocorre se usarmos as 26 letras de nosso alfabeto, em qualquer ordem, para criarmos mensagens criptografadas?

Como fizemos com os alfabetos dos planetas Plunct e Plact, se agora usarmos nosso alfabeto, conseguiremos $26!$ maneiras diferentes de criptografar uma mensagem, isto dá

$$26! = 26 \cdot 25 \cdot 24 \cdots 3 \cdot 2 \cdot 1 = 403\,291\,461\,126\,605\,635\,584\,000\,000$$

possibilidades.

Veja o esquema:

26 possibilidades para se colocar a primeira letra	Restam **25** possibilidades para se colocar a segunda letra	Restam **24** possibilidades para se colocar a terceira letra	(...)	Restam **3** possibilidades para se colocar a vigésima quarta letra	Restam **2** possibilidades para se colocar a vigésima quinta letra	Resta **1** possibilidade para se colocar a vigésima sexta letra

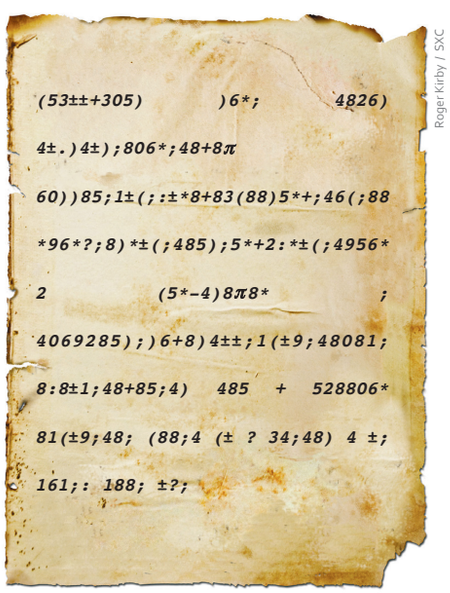
Note que com o Princípio Multiplicativo da Contagem conseguimos verificar uma quantidade enorme de possibilidades de criar sistemas criptográficos a partir do nosso alfabeto.

O número $26!$ é muito grande e pode ser desanimador, pois parece ser impossível descobrir a chave para quebrar um código feito no estilo de Júlio César, caso desconheçamos qual foi a maneira com que as letras foram inicialmente codificadas, não é mesmo?

Não há esperança alguma de se testar todas as possibilidades. Apesar disso, o código de Júlio César e suas variações podem ser quebrados sem muita dificuldade, como você pode ver na seção a seguir.

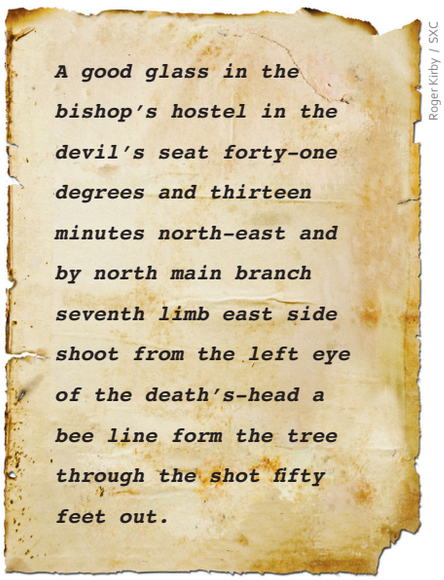
4.1. Mapas de tesouros

Vamos voltar agora à mensagem secreta do texto que abriu essa aula:



Roger Kirby / SXC

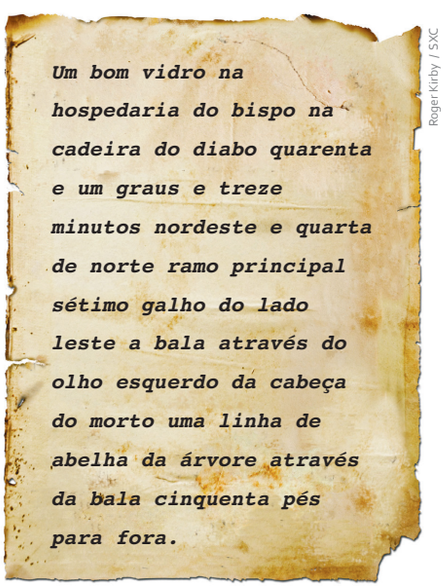
O conto “O Escaravelho de ouro”, de Edgar Allan Poe, ilustra muito bem um exemplo da teoria da decifração. Após uma análise baseada na frequência das letras do alfabeto inglês, feita pelo protagonista, a mensagem toma a seguinte forma:



Roger Kirby / SXC

Como você imagina que o texto foi decifrado?

Para começar, é importante perceber que a letra que aparece com mais frequência na língua inglesa é a letra “e”. Muitas vezes essa letra aparece dobrada: “ee”. Veja que na mensagem secreta acima o símbolo 8 aparece 33 vezes, muito mais do que as outras letras. Portanto, é plausível que 8 signifique a letra “e”. Substituindo 8 por “e” e repetindo o mesmo esquema com outras letras, foi possível decifrar a mensagem. Sua tradução para o português é:



Roger Kirby / SXC

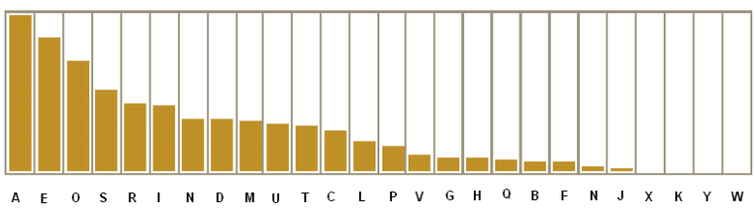
Como você viu no início dessa aula, o conto revela, de uma maneira fantástica, como, a partir dessas informações, o personagem principal encontra um tesouro há muito tempo enterrado por um pirata que havia passado pelo lugar descrito na mensagem.

A Análise Combinatória foi usada para calcularmos a quantidade de sistemas criptográficos que podemos criar, e apesar de essa quantidade ser enorme, vimos que é possível decodificá-las através do estudo da frequência das letras.

Desafio Decodificando uma mensagem

Observe a frequência aproximada das letras em português:

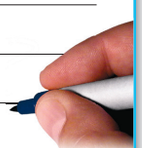
Frequência aproximada das letras em português



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14,6	1,0	3,8	4,9	12,5	1,0	1,3	1,2	6,1	0,4	0,02	2,7	4,7	5,0	10,7	2,5	1,2	6,5	7,8	4,3	4,6	1,6	0,01	0,2	0,01	0,4

Agora, utilize esse estudo de frequência das letras para decodificar a mensagem a seguir:

Roger Kirby / SXC



Adam Ciesielski / SXC

Dica: essa mensagem é uma rima feita a partir de um conhecido poema da literatura brasileira, e tem por finalidade ensinar os alunos a decorar quanto vale $sen(a+b)$.

Para economizar seu tempo, as letras H, P, L e D não foram codificadas.

5. Permutações simples

Nos exemplos da seção anterior, as mensagens foram criptografadas mudando a ordem das letras de um alfabeto, ou melhor, permutando-se essa ordem. Em um alfabeto com 3 letras {♥, ♣, ♦}, vimos que existem $3!$ permutações:

{♥, ♣, ♦}, {♣, ♥, ♦}, {♣, ♦, ♥}, {♥, ♦, ♣}, {♦, ♥, ♣}, {♦, ♣, ♥}

Cada conjunto acima, distintamente ordenado, é chamado de permutação simples do conjunto {♥, ♣, ♦}.

Uma ***permutação simples*** de um conjunto com n elementos é o agrupamento ordenado de n elementos desse conjunto. O termo *simples* significa que não há repetição dos elementos em cada ordenamento.

Com um alfabeto de 26 letras, vimos que existem $26!$ permutações simples dessas letras.

Em geral, para um conjunto com n elementos, existem $P(n) = n!$ permutações simples possíveis.

Muitos problemas interessantes são resolvidos, quando se percebe que sua solução recai em uma simples aplicação do Princípio Multiplicativo ou sobre o cálculo do número de permutações dos elementos de um conjunto (que ainda é uma simples aplicação do Princípio Multiplicativo).

Veremos mais alguns problemas relacionados à Criptografia. Para resolvê-los com sucesso, veja algumas sugestões no boxe a seguir.

Saiba Mais **Atitudes para resolver problemas de contagem**

a) Leia o problema a ser resolvido com bastante atenção. Detalhes como "os elementos são distintos" ou "os elementos podem se repetir" fazem a diferença;

b) Verifique se o problema fica mais simples dividindo-o em casos;

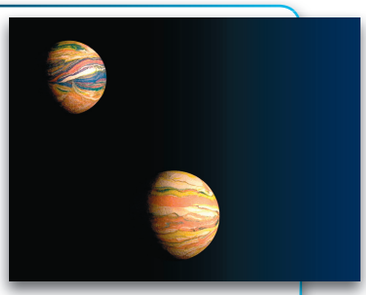
c) Isole as possibilidades mais "problemáticas" ou que oferecem mais dificuldades e comece resolvendo-as por ordem de dificuldade;

d) Para resolver o problema, use diagramas, setas, os esquemas que vimos fazendo, casos particulares etc. Crie sua maneira pessoal de resolver os problemas de contagem;

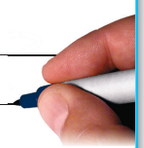
e) Evite usar indiscriminadamente fórmulas. Esse procedimento não funciona em geral, pois há casos que não se enquadram na aplicação de qualquer fórmula. Enfim, é necessário saber usar o Princípio Multiplicativo com bastante atenção. Só isso.

Arjun Kartha / SXC

Atividade 1 Sistemas criptográficos



Um viajante, conhecedor dos alfabetos dos planetas Plunct e Plact, usa os dois alfabetos para criar um sistema para criptografar mensagens. Sua ideia é usar as permutações das letras do alfabeto do planeta Plact para escolher um sistema criptográfico e, após cada palavra criptografada, escrever uma mesma letra do alfabeto do planeta Plunct para confundir os leitores. De quantas maneiras ele pode fazer isso?



Adam Cieslelski / SXC

Resposta comentada

Como o alfabeto do planeta Plact possui 4 letras, é possível formar, com apenas essas letras, $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$ sistemas criptográficos. Ora, o alfabeto do Planeta Plunct possui 3 letras e, portanto, podemos usar cada uma e escrevê-la após cada palavra. Assim, pelo Princípio Fundamental da Contagem, o viajante pode formar $3 \times 4! = 3 \times 24 = 72$ sistemas criptográficos.

Atividade 2

Um agente secreto descobriu que na decodificação de uma palavra com cinco letras as vogais ***a*** e ***e*** aparecem uma única vez. Quantas possíveis sequências de letras existem com essas características?

Resposta Comentada

A solução do problema consiste em determinarmos as possibilidades das posições que as letras ***a*** e ***e*** podem ocupar em uma sequência de letras com cinco letras. Convém fazermos um diagrama:

1ª posição	2ª posição	3ª posição	4ª posição	5ª posição

Uma das duas letras pode ocupar qualquer das 5 posições. Restarão apenas 4 posições para a outra letra ocupar. Note que restarão três posições para serem preenchidas com as 24 letras restantes do alfabeto (observe que as letras ***a*** e ***e*** aparecem apenas uma única vez na palavra).

Uma das letras ***a*** ou ***e*** ocupa 5 posições	Uma das letras ***a*** ou ***e*** ocupa 4 posições	Uma posição pode ser ocupada por qualquer das 24 letras restantes	Uma posição pode ser ocupada por qualquer das 24 letras restantes	Uma posição pode ser ocupada por qualquer das 24 letras restantes
5	**4**	**24**	**24**	**24**

Pelo Princípio Multiplicativo, teremos $5 \cdot 4 \cdot 24 \cdot 24 = 276480$ sequências de letras com essa característica (na realidade teremos muitas combinações de letras que não formam palavra alguma na Língua Portuguesa). Note que as demais letras, diferentes de ***a*** e ***e***, podem se repetir.

O agente secreto deve ter tido muito trabalho para decodificar a palavra, não é mesmo? Ainda bem que nem todas essas sequências de letras formam realmente uma palavra com significado em nossa Língua!

Atividade 3

Considere o mesmo problema anterior, mas, agora, analisando um caso no qual as letras ***a***, ***e*** e ***c*** aparecem em uma palavra decodificada com cinco letras que não termina em ***c***. Quantas sequências de letras têm essas características?

Resposta comentada

Comecemos fazendo um diagrama, que nos ajudará na resolução do problema:

1ª posição	**2ª** posição	**3ª** posição	**4ª** posição	**5ª** posição

Como a sequência de letras não termina em ***c***, temos uma restrição a ser considerada: a letra ***c*** só pode ocupar as 4 primeiras posições. Nesse caso, comecemos com a letra "problemática", a letra ***c***.

Nesse tipo de problema, aconselhamos sempre começar com a possibilidade que ofereça maior dificuldade. Ora, há 4 posições (as quatro primeiras) que a letra ***c*** pode ocupar. A letra ***c***, ao ocupar sua posição, deixa quatro posições que as letras ***a*** e ***e*** podem ocupar. Uma dessas letras (***a*** ou ***e***) pode ocupar 4 posições, deixando 3 posições para a outra. Ocupadas as posições das letras ***c***, ***a*** e ***e***, restam duas posições a serem ocupadas.

Qualquer uma dessas posições pode ser ocupada por qualquer uma das 26 letras do nosso alfabeto, pois não fizemos nenhuma restrição ao fato de as letras ***c***, ***a*** e ***e*** poderem se repetir. Dessa forma, pelo Princípio Multiplicativo, temos $4 \cdot 4 \cdot 3 \cdot 26 \cdot 26 = 32448$ sequências de letras com essas características.

Atenção

Observe que para resolvermos as questões propostas nas atividades 1 e 2, não utilizamos fórmula alguma, apenas o Princípio Multiplicativo.

Atividade 4

Uma senha de banco é formada por seis algarismos. Analisemos as diferentes quantidades de senha formadas ao usar somente os algarismos 3, 5, 7 e 9.

a ▸ Quantas senhas podemos formar com esses algarismos?

b ▸ Quantas senhas contêm apenas dois desses algarismos?

c ▸ Em quantas senhas todos esses algarismos aparecem?

Resposta Comentada

4a) O problema resume-se em saber as posições que os algarismos 3, 5, 7 e 9 podem ocupar na senha. Note que não há restrição ao fato de um algarismo poder se repetir.

1ª posição	2ª posição	3ª posição	4ª posição	5ª posição	6ª posição
Os quatro algarismos podem assumir essa posição. Temos 4 possibilidades.	Os quatro algarismos podem assumir essa posição. Temos 4 possibilidades.	Os quatro algarismos podem assumir essa posição. Temos 4 possibilidades.	Os quatro algarismos podem assumir essa posição. Temos 4 possibilidades.	Os quatro algarismos podem assumir essa posição. Temos 4 possibilidades.	Os quatro algarismos podem assumir essa posição. Temos 4 possibilidades.

Logo, pelo Princípio Multiplicativo, a resposta é $4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 = 4^6$ senhas.

4b) Nesse caso, a palavra "apenas" tem um papel decisivo na resolução do problema.

Para a senha ser formada por dois desses algarismos, precisamos dividir o problema em casos. Aconselhamos sempre proceder dessa maneira, quando pertinente. Uma senha pode ser formada por dois desses algarismos, no caso deles serem: $\{3,5\}$, $\{3,7\}$, $\{3,9\}$, $\{5,7\}$, $\{5,9\}$ ou $\{7,9\}$. Tomemos o par $\{3,5\}$, por exemplo, para formarmos a senha. Nesse caso, temos as seguintes possibilidades:

1ª posição	2ª posição	3ª posição	4ª posição	5ª posição	6ª posição
Os algarismos 3 ou 5 podem assumir essa posição. Temos 2 possibilidades.	Os algarismos 3 ou 5 podem assumir essa posição. Temos 2 possibilidades.	Os algarismos 3 ou 5 podem assumir essa posição. Temos 2 possibilidades.	Os algarismos 3 ou 5 podem assumir essa posição. Temos 2 possibilidades.	Os algarismos 3 ou 5 podem assumir essa posição. Temos 2 possibilidades.	Os algarismos 3 ou 5 podem assumir essa posição. Temos 2 possibilidades.

Para o par $\{3,5\}$, pelo Princípio Multiplicativo, podemos formar $2\cdot2\cdot2\cdot2\cdot2\cdot2=2^6$ senhas. Como podemos proceder dessa forma para os 6 pares, podemos formar $6\cdot2^6$ senhas que contenham apenas dois algarismos.

4c) Para resolver esse item do problema, precisamos fazer uma pequena conta de subtração. Essa é mais uma estratégia para resolvermos problemas de contagem e que pode ser muito útil em certos tipos de problema. Para encontrarmos o número de casos que satisfazem uma propriedade, devemos contar o número de casos geral e subtraímos desse número o número de casos particulares que não satisfazem tal propriedade.

Raciocinemos um pouco: se da quantidade de todas as senhas possíveis formadas pelos algarismos 3, 5, 7 ou 9 retirarmos as formadas apenas por um dos algarismos 3, 5, 7 ou 9, e depois retirarmos as formadas por dois dos algarismos 3, 5, 7, ou 9, e, finalmente, retirarmos as formadas por três dos algarismos 3, 5, 7 ou 9, restarão as formadas pelos quatro algarismos 3, 5, 7 e 9.

Sabemos do item anterior o número de senhas formadas por apenas dois dos algarismos 3, 5, 7 ou 9.

É fácil ver que o número de senhas formadas por apenas um desses algarismos é 4, pois nesse caso temos as senhas 333333, 555555, 777777 e 999999.

Para seguirmos o raciocínio proposto, resta-nos, agora, calcular o número de senhas formadas por três dos algarismos 3, 5, 7 ou 9. Para isso, raciocinemos analogamente sobre as hipóteses em que as senhas são formadas por dois desses algarismos.

As senhas em que aparecem apenas três algarismos podem ser construídas, caso os algarismos formem os ternos $\{3,5,7\}$, $\{3,5,9\}$, $\{3,7,9\}$, $\{5,7,9\}$. Tomemos um desses ternos de algarismos, por exemplo, $\{3,5,9\}$. Logo, temos:

1ª posição	2ª posição	3ª posição	4ª posição	5ª posição	6ª posição
Os algarismos 3, 5 ou 9 podem assumir essa posição. Temos 3 possibilidades.	Os algarismos 3, 5 ou 9 podem assumir essa posição. Temos 3 possibilidades.	Os algarismos 3, 5 ou 9 podem assumir essa posição. Temos 3 possibilidades.	Os algarismos 3, 5 ou 9 podem assumir essa posição. Temos 3 possibilidades.	Os algarismos 3, 5 ou 9 podem assumir essa posição. Temos 3 possibilidades.	Os algarismos 3, 5 ou 9 podem assumir essa posição. Temos 3 possibilidades.

A partir desse raciocínio, pelo Princípio Multiplicativo, concluímos que existem $3\cdot3\cdot3\cdot3\cdot3\cdot3=3^6$ senhas. Como temos quatro ternos de algarismos, tem-se $4\cdot3^6$ senhas formadas por apenas 3 dos algarismos 3, 5, 7 e 9.

Assim:

- Número de senhas formadas por um algarismo do conjunto $\{3,\ 5,\ 7,\ 9\}=4$.
- Número de senhas formadas por dois algarismos do conjunto $\{3,\ 5,\ 7,\ 9\}=6\cdot2^6=6\cdot4^3$.
- Número de senhas formadas por três dos algarismos do conjunto $\{3,\ 5,\ 7,\ 9\}=4\cdot3^6$.
- Número total de senhas 4^6.
- Número de senhas em que aparecem os quatro algarismos = número total de senhas - senhas formadas com 1 algarismo - senhas formadas com 2 algarismos - senhas formadas com 3 algarismos: $4^6-\left(4\cdot3^6+6\cdot4^3+4\right)=4096-\left(2916+384+4\right)=792$.

Assim, temos 792 senhas em que aparecem todos os algarismos 3, 5, 7 e 9.

A seguir, você pode encontrar outros problemas de Análise Combinatória que requerem a aplicação do Princípio Multiplicativo de Contagem para a sua resolução, mas que não estão relacionados à Criptografia.

Atividade 5

De quantas formas distintas 5 pessoas podem sentar em 7 cadeiras, cada pessoa ocupando uma cadeira?
Antes de ver a resposta dessa pergunta, tente resolvê-la sozinho.

Resposta Comentada

Um esquema de resolução como os usados anteriormente pode ser bastante útil. Chamemos as pessoas de P_1, P_2, P_3, P_4 e P_5. Agora, basta preencher a tabela abaixo:

Pessoa P_1	Pessoa P_2	Pessoa P_3	Pessoa P_4	Pessoa P_5
Tem 7 escolhas de cadeiras para ocupar.	Tem 6 escolhas de cadeiras. Note que uma cadeira já foi ocupada pela pessoa P_1.	Tem 5 escolhas de cadeiras. Note que duas cadeiras já foram ocupadas pelas pessoas P_1 e P_2.	Tem 4 escolhas de cadeiras. Note que três cadeiras já foram ocupadas pelas pessoas P_1, P_2 e P_3.	Tem 3 escolhas de cadeiras. Note que quatro cadeiras já foram ocupadas pelas pessoas P_1, P_2, P_3 e P_4.

Pelo Princípio Multiplicativo, chegamos a $7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 = 2520$ formas distintas das 5 pessoas sentarem nas 7 cadeiras.

Atenção

Nos livros didáticos, a resolução da atividade anterior é feita através do conceito de arranjo. O número de arranjos simples de n elementos tomados p a p é por definição $A_n^p = \frac{n!}{(n-p)!}$. Por exemplo, na resolução da atividade 5, temos um arranjo de 7 elementos tomados 5 a 5: $A_p^n = \frac{7!}{(7-5)!} = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3$.

Atividade 6

João vai participar de um sorteio, cujas cartelas são formadas por todos os números de três algarismos, dentre os números de 100 a 999, incluindo-os. João prefere comprar cartelas terminadas em 2, em 4, ou em 8, pois diz ter muita sorte com elas. Quantas das cartelas do sorteio foram as preferidas por João?

Resposta Comentada

Devemos analisar como preencher com os números disponíveis uma cartela do tipo:

Primeiro algarismo	Segundo algarismo	Terceiro algarismo
Número de possibilidades dos algarismos	Número de possibilidades dos algarismos	Número de possibilidades dos algarismos

Conforme nossas sugestões dadas no Boxe Saiba Mais, comecemos pelos casos que apresentam mais dificuldades ou que sejam mais restritivos. Sempre proceda dessa forma. Nesse caso, precisamos formar números pares que terminam em 2, 4 ou 8. Logo, temos 3 possibilidades para o terceiro algarismo. O segundo algarismo pode ser qualquer um do conjunto $\{0,1,2,3,4,5,6,7,8,9\}$, não há restrição alguma para ele. Assim, podemos ter 10 possibilidades para o segundo algarismo. Como o número zero deve ser evitado como primeiro algarismo, temos 9 possibilidades para o primeiro algarismo. Daí a tabela anterior fica da seguinte forma:

Primeiro algarismo	Segundo algarismo	Terceiro algarismo
9	10	3

Pelo Princípio Multiplicativo, temos $9 \cdot 10 \cdot 3 = 270$ cartelas preferidas por João.

Para não assustar os alunos, ressaltamos a importância de escolher exercícios simples ao iniciar os estudos de Análise Combinatória, assim como foi feito ao longo de toda essa Etapa 1. Você deve ter percebido que todos os exercícios podem ser feitos unicamente através do Princípio Multiplicativo, sem que precisássemos recorrer insistentemente ao uso de fórmulas. Esperamos que você aproveite!

6. Conclusão

No ensino de Matemática, a Análise Combinatória muitas vezes é relegada ao esquecimento ou, então, é trabalhada apenas por meio do uso de fórmulas. Na disciplina Matemática Discreta, que começou com esta Etapa 1, queremos mostrar que o ensino desse conteúdo é importante e pode ser muito interessante e estimulante tanto para você, professor, quanto para seus alunos.

Acreditamos que uma abordagem interessante parte do pressuposto de que é possível resolver vários problemas (do cotidiano ou não) usando um recurso bastante simples: o Princípio Multiplicativo. Como você observou ao longo dessa etapa, não foi necessária a utilização de fórmulas e, muitas vezes, esses problemas não podem ser resolvidos por uma aplicação direta delas.

Portanto, esperamos que você se convença de que a maioria dos problemas de contagem pode ser um rico instrumento para ensinar os alunos do Ensino Médio a organizar ideias e contar possibilidades de agrupamentos, utilizando, na maioria das vezes, apenas o Princípio Multiplicativo.

7. Resumo

- A Criptografia pode ser um interessante ponto de partida para abordar conteúdos ligados à Análise Combinatória e à Teoria das Probabilidades no Ensino Médio.
- A Criptografia é a ciência que trabalha com meios e métodos capazes de enviar mensagens com segurança.
- A Análise Combinatória analisa e conta o número de possibilidades de como os elementos de um conjunto podem ser agrupados de acordo com regras estabelecidas.
- Para resolver problemas de Análise Combinatória, não precisamos recorrer indiscriminadamente ao uso de fórmulas.
- A criptografia de Júlio César foi um dos primeiros sistemas criptográficos conhecido. É um sistema bem simples e que pode sofrer diversas variações. Esse sistema conta com uma chave ou senha estipulada previamente.
- No sistema criptográfico de Júlio César, o alfabeto é codificado seguindo sua ordem usual, iniciando, apenas, em um lugar diferente.
- De acordo com o Princípio Multiplicativo de Contagem, se uma decisão puder ser tomada de m maneiras diferentes e, se uma vez tomada essa primeira decisão, outra decisão, independente da primeira, puder ser tomada de n maneiras diferentes, então, no total, serão tomadas $m \times n$ decisões.
- Por meio do Princípio Multiplicativo de Contagem, podemos calcular quantos sistemas criptográficos podem ser formados, alterando as letras sem respeitar a ordem em que aparecem em um alfabeto.
- Fatorial é uma notação muito útil para trabalhar com problemas de Contagem. No caso geral, o fatorial de um número inteiro positivo n é definido por $n! = n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1$ e, por convenção, $0! = 1$.

- A decodificação de sistemas criptográficos simples pode ser feita por meio do estudo da frequência das letras.
- Quando mensagens são criptografadas mudando a ordem das letras de um alfabeto, dizemos que ocorreu uma permutação simples.
- Uma permutação simples de um conjunto com n elementos é um agrupamento ordenado de n elementos desse conjunto. O termo *simples* significa que não há repetição dos elementos em cada ordenamento.
- Para um conjunto com n elementos, existem $P(n) = n!$ permutações (simples) possíveis.
- Muitos problemas interessantes podem ser resolvidos quando percebemos que a solução recai em uma simples aplicação do Princípio Multiplicativo ou alguma de suas variações, como é o caso do cálculo do número de permutações dos elementos de um conjunto.
- Há uma lista de procedimentos para enfrentar problemas de contagem: ler o problema com bastante atenção; verificar se o problema fica mais simples dividindo-o em casos; isolar as possibilidades mais "problemáticas" e resolvê-las por ordem de dificuldade; usar diagramas, criando uma maneira pessoal de solucionar os problemas e evitar o uso indiscriminado de fórmulas.

Resposta do Desafio [p. 24]

"Minha terra tem palmeiras
Onde canta o sabiá,
Seno(a), cosseno(b), seno(b), cosseno(a)"

Roger Kirby / SXC

Etapa II
Código Braille

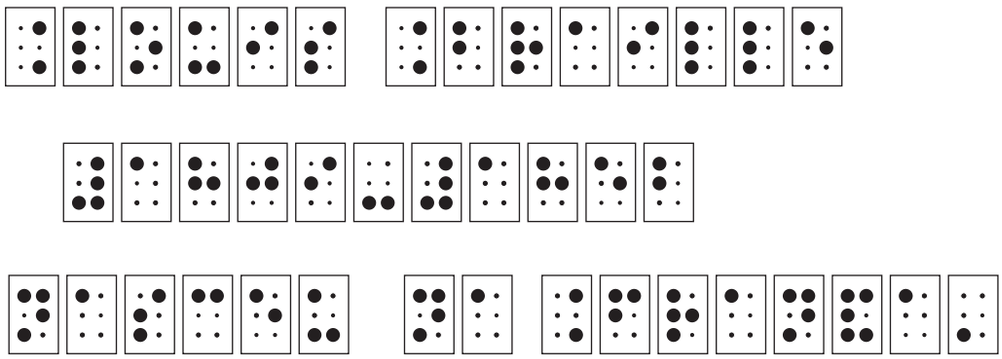
O código Braille e as combinações simples

- Você conhece o sistema de comunicação Braille, utilizado pelos deficientes visuais?
- Sabia que esse sistema pode ser utilizado em sala de aula para estudar Análise Combinatória?
- Sabia que usando o Princípio Multiplicativo podemos desenvolver outras técnicas de contagem?
- O que há em comum entre o sistema Braille, saladas de frutas e o sistema binário de representação numérica usado nos computadores?

Svilen Milev / SXC

1. Introdução

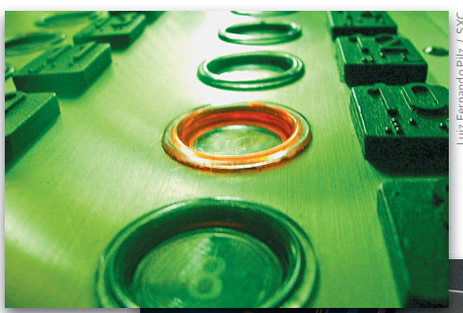
Você consegue ler a seguinte mensagem?



Acreditamos que muitos não conseguem entender a mensagem acima. Provavelmente, você também não... Mas não desanime!

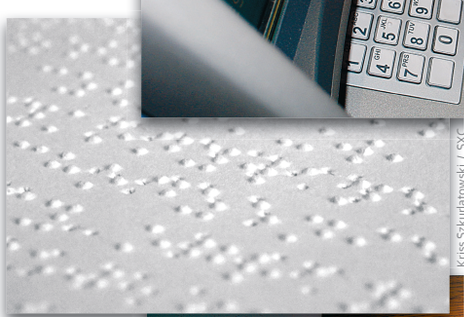
Essa mensagem está escrita em Braille, um método de escrita desenvolvido para que pessoas cegas possam ler usando o tato. Seu criador, Louis Braille (1809-1852), ficou cego aos três anos de idade em razão de um ferimento no olho causado por um objeto pontiagudo que seu pai usava para fabricar selas de animais. O ferimento infeccionou e provocou também a perda da visão do outro olho, deixando-o com deficiência visual total.

Ao inventar seu método de escrita, Braille fez um grande benefício a todos os deficientes visuais e à humanidade. Atualmente, em elevadores, caixas eletrônicos etc., há várias informações escritas em Braille, o que propicia aos deficientes visuais uma inserção social mais efetiva.



Luiz Fernando Pilz / SXC

Vaughan Willis / SXC



Kriss Szkurlatowski / SXC

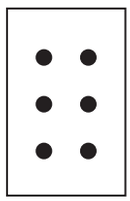
Julia Freeman-Woolpert / SXC

Mas por que falar de código Braille no contexto da disciplina Matemática Discreta, em um curso de Especialização para professores de Matemática do Ensino Médio? Você vai perceber essa relação ao longo dessa etapa!

Adam Cieslelski / SXC

2. O código Braille

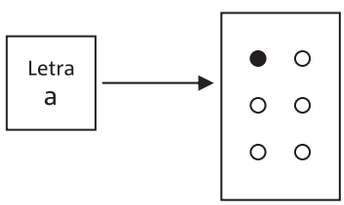
O código Braille é baseado em uma disposição 3×2 de pontos, dispostos como numa pedra de dominó:



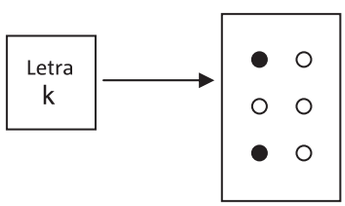
Julia Freeman-Woolpert / SXC

Para registrar uma letra do alfabeto, alguns desses 6 pontos são marcados ou perfurados, para que fiquem sobressalentes e possam ser sentidos com as pontas dos dedos das mãos. E é assim que os deficientes visuais conseguem ler: usando as mãos.

Nos símbolos escritos em Braille a seguir, um círculo negro (preenchido) indica que o ponto está marcado, e um círculo branco indica que o ponto não está marcado. Veja os exemplos:



Somente a primeira casa foi marcada: o ponto que está na primeira linha e na primeira coluna aparece em negro.



A letra k tem dois pontos marcados: o ponto da primeira linha e da primeira coluna e o ponto da terceira linha e da primeira coluna.

Atividade 1


Jacque Stengel / SXC

Mesmo que você esteja tendo contato com o código Braille somente agora, com os conhecimentos e discussões que desenvolvemos na Etapa 1, já é possível responder a algumas questões:

a ▹ Usando as possibilidades de marcar seis pontos em um cartão, quantos padrões (disposições de pontos) diferentes podemos formar usando o código Braille?

b ▹ Quantos padrões podemos formar se dispusermos os pontos em um quadrado 2×2? E em um retângulo 1×4? Por que será que eles não são usados para comunicação de deficientes visuais?

Resposta comentada

a ▹ O código Braille usa um sistema com seis pontos. Para cada ponto, temos duas possibilidades: marcado ou não-marcado. Como temos seis pontos no sistema 3×2, pelo Princípio Multiplicativo, a quantidade de padrões diferentes que pode ser formada é $2\times2\times2\times2\times2\times2=2^6=64$. Na seção 3, você encontrará outra maneira de calcular esse valor.

b ▹ Tanto no sistema 2×2, quanto no sistema 1×4, temos quatro pontos. Então, da mesma forma que no item (a), pelo Princípio Multiplicativo, calculamos que o número de padrões diferentes será $2\times2\times2\times2=2^4=16$. Como essa quantidade de configurações possíveis é muito pequena diante da quantidade de símbolos que utilizamos para nos comunicar, sistemas desses tamanhos não atenderiam a nossa necessidade. Eis a principal razão de não utilizá-los.

O número de padrões formados no item (a) da atividade anterior é suficiente para codificar todas as letras minúsculas do nosso alfabeto?

Além das letras minúsculas, com o número de padrões encontrados, é possível codificar todas as letras maiúsculas?

Lembre-se que ainda temos os números! Além de todas as letras minúsculas e maiúsculas, é possível codificar também os algarismos: 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9?

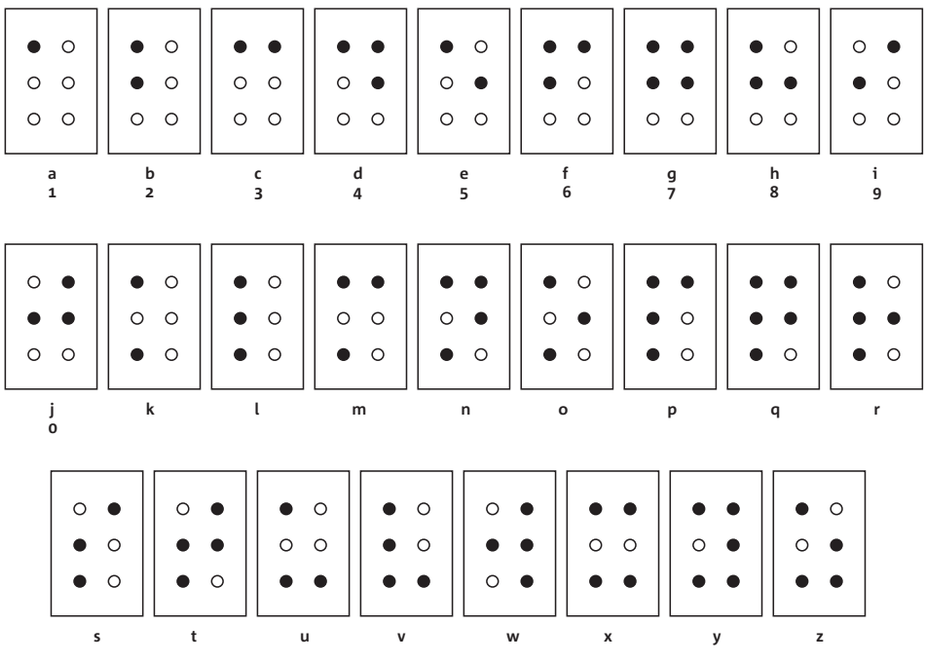
Usando o código Braille, como os deficientes visuais podem saber se está sendo feita uma pergunta, uma exclamação ou uma pausa? Como os sinais de pontuação podem ser representados?

E os sinais de operações matemáticas: $+$, $\times$, $-$ e $\div$?

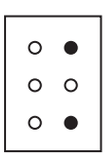

Maarten Uilenbroek / SXC

Pensando nessas questões, você já deve ter se convencido de que devem ser necessários certos artifícios adicionais para que seja possível representar todos os símbolos que aparecem nas perguntas anteriores, usando a linguagem Braille.

A seguir, apresentamos a maneira usual de codificar as letras minúsculas e os algarismos na linguagem Braille:

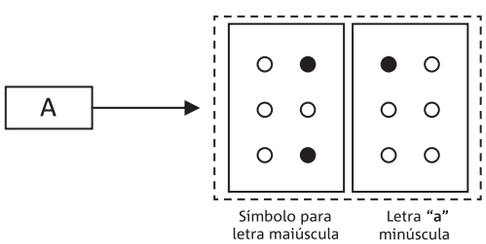


Para codificar letras maiúsculas, usamos o símbolo:



antes da letra que desejamos que seja maiúscula.

Por exemplo, a letra A (maiúscula) se escreve assim:

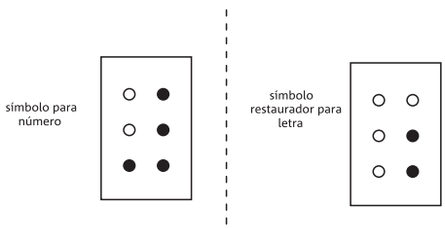


Observe também que as mesmas configurações de pontos que são usadas para denotar as letras de *a* até *j*, são também usadas para denotar os algarismos 1, 2, 3, 4, 5, 6, 7, 8, 9 e 0.

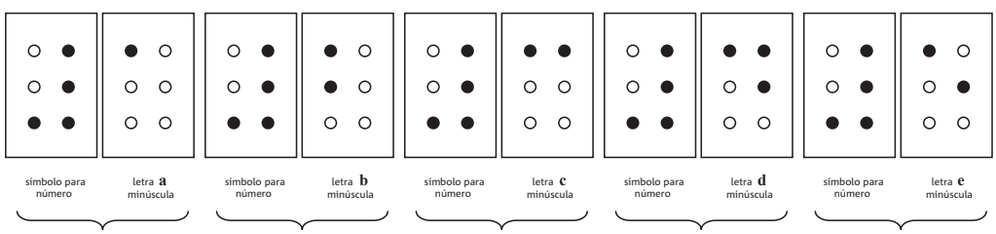
Como distinguir se uma configuração está representando uma letra ou um algarismo?

Adam Ciesielski / SXC

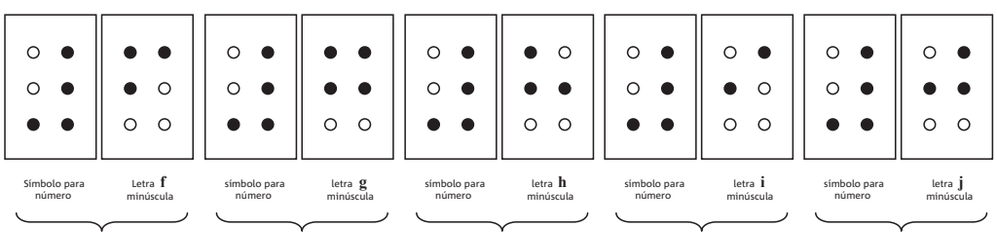
Para utilizarmos uma configuração como um número, devemos antecedê-la com um símbolo que indique esse fato. Existe também outro símbolo chamado restaurador, usado quando há risco de se confundir letras com números. Para indicar que um símbolo deve voltar a indicar uma letra, logo após um número, devemos antecedê-lo com o símbolo restaurador.



Veja como são as representações dos dez algarismos:

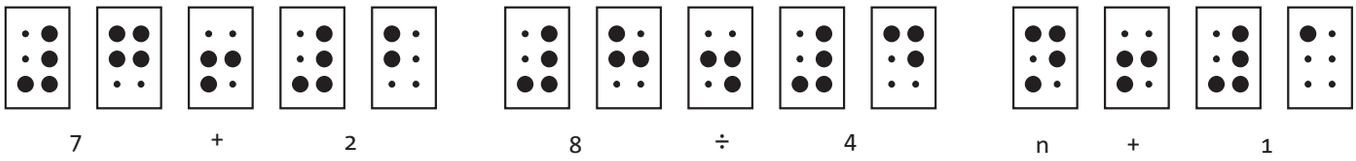


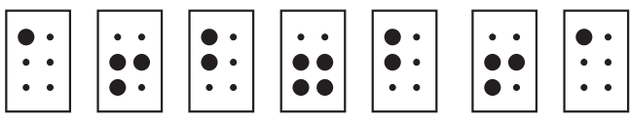
Este conjunto representa o número 1. | Este conjunto representa o número 2. | Este conjunto representa o número 3. | Este conjunto representa o número 4. | Este conjunto representa o número 5.

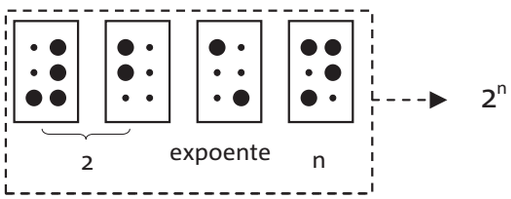


Este conjunto representa o número 6. | Este conjunto representa o número 7. | Este conjunto representa o número 8. | Este conjunto representa o número 9. | Este conjunto representa o número 0.

Veja alguns exemplos de expressões matemáticas em Braille:

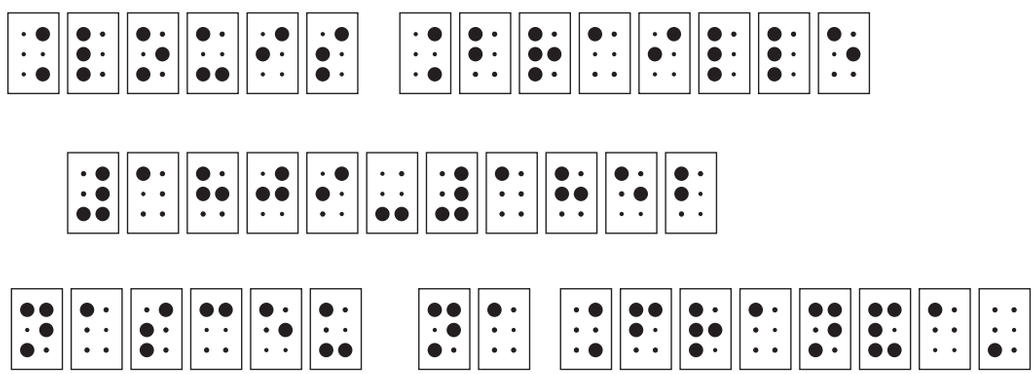






Atividade 2

Agora que você já aprendeu o caminho das pedras, tente decifrar a mensagem da introdução:



Resposta comentada

A mensagem é: **Louis Braille / 1809-1852 / nasceu na França**.

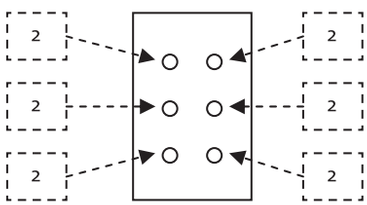
Que relações podemos estabelecer entre o código Braille e o ensino de Matemática?

Adam Ciesielski / SXC

3. Explorando conceitos matemáticos com a linguagem Braille

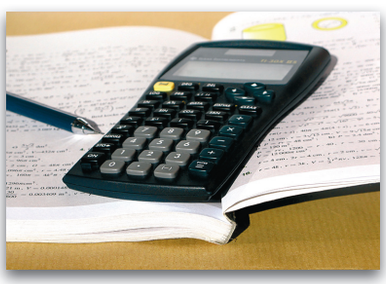
Na atividade 1 da seção anterior, vimos que existem $2^6 = 64$ configurações que podem ser obtidas no código de Braille, usual 3×2. Esse cálculo foi obtido usando o Princípio Multiplicativo da Contagem:

- Só há duas possibilidades para a primeira casa: ou ela é marcada ou não é (ou pintamos de preto ou de branco);
- Do mesmo modo, só há duas possibilidades para cada uma das outras casas, o que resulta em $2 \times 2 \times 2 \times 2 \times 2 \times 2 = 2^6$ possibilidades.



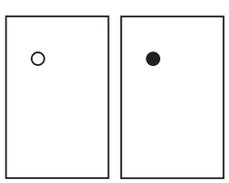
Princípio Multiplicativo da Contagem:
Se uma decisão puder ser tomada de m maneiras diferentes, e se uma vez tomada esta primeira decisão, outra decisão, independente da primeira, puder ser tomada de n maneiras diferentes, então no total serão tomadas $m \times n$ decisões.

Vamos ver agora dois outros métodos de fazer o cálculo anterior para descobrirmos quantas configurações podemos formar com uma disposição de 3×2 pontos usada na linguagem Braille. Afinal, explorando diferentes formas de resolver um mesmo problema, ampliamos nosso leque de opções para quando formos resolver um problema semelhante.

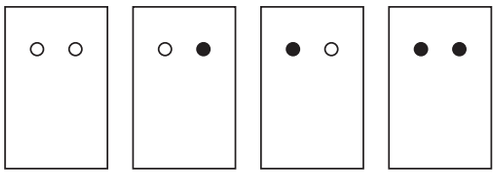

Sanja Gjenero / SXC

Método 1: Focando na quantidade de pontos, independente de estarem pintados ou não

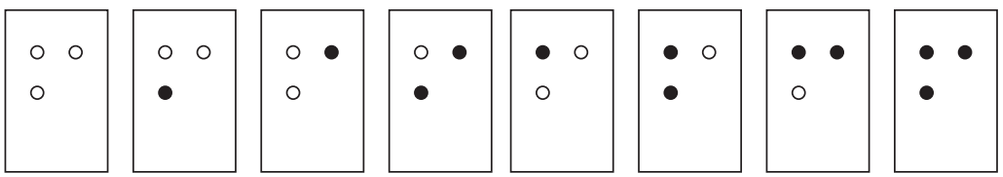
Se o cartão tivesse apenas um ponto, teríamos somente 2 possibilidades:



Caso o cartão tivesse dois pontos, haveria 4 possibilidades, pois há duas escolhas para cada uma das configurações já vistas acima (com um ponto apenas):

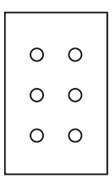


Já no caso de o cartão ter três pontos, haveria 8 possibilidades (duas para cada uma das configurações com dois pontos vistas acima).

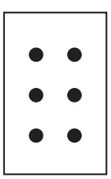


Continuando assim, dobrando a quantidade de possibilidades a cada ponto adicionado, com quatro pontos teríamos 16 configurações distintas, com cinco pontos, 32 configurações e, é claro, com 6 pontos, que é o caso do código Braille, chegaríamos a 64 padrões diferentes de pontos.

Dentre as 64 possibilidades, temos dois casos extremos: aquele em que nenhum dos pontos é marcado e outro em que todos os seis pontos são marcados:



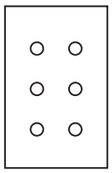
Em Braille, esta configuração não é usada.



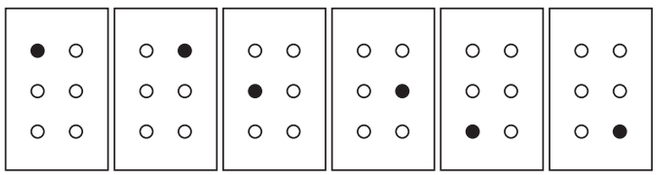
Na linguagem Braille, esta configuração tem a função de referencial de posição, para auxiliar a indicar sinais gráficos tais como a crase ou o trema. É usada para indicar a letra acentuada *é*.

Método 2: Focando na quantidade de pontos pintados

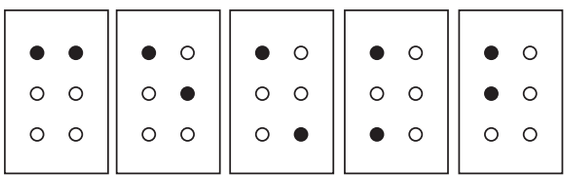
Com nenhum ponto marcado, temos apenas uma configuração:



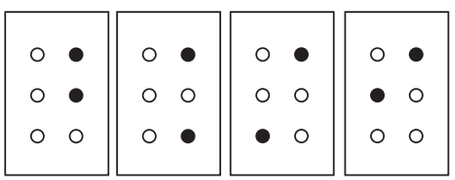
Com apenas um ponto marcado, temos 6 possibilidades:



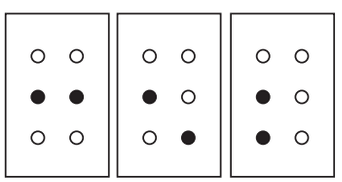
As configurações com dois pontos marcados totalizam 15. Veja:



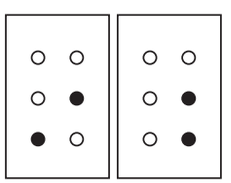
Todas estas configurações têm a primeira casa da primeira linha marcada em preto



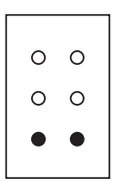
Todas estas configurações têm a segunda casa da primeira linha marcada em preto. Só está faltando uma configuração desse tipo, que já foi contada, pois ela é a primeira configuração do grupo anterior.



Todas estas configurações têm a primeira casa da segunda linha marcada em preto. Só estão faltando duas configurações desse tipo, que já foram contadas, uma em cada das duas configurações anteriores.

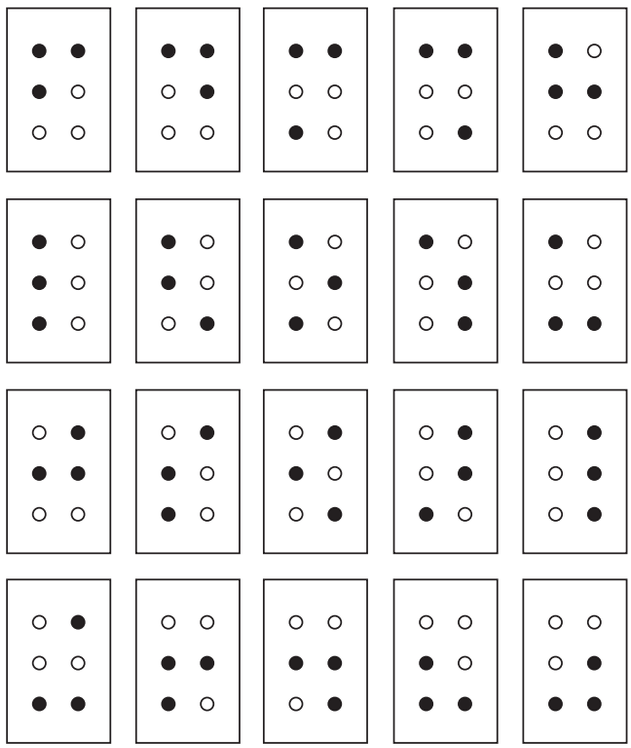


Todas estas configurações têm a segunda casa da segunda linha marcada em preto. Só estão faltando três configurações desse tipo, que já foram contadas, uma em cada uma das três configurações anteriores.



Resta somente esta última configuração que não apareceu em nenhuma das configurações anteriores.

Deste modo, com dois pontos pretos, há $1+2+3+4+5=15$ possibilidades. Com três pontos pretos, há 20 possibilidades. Veja:



Poderíamos agora exibir todas as configurações com 4 pontos pretos (são 15 ao todo), com 5 pontos pretos (são 6 no total) e com 6 pontos pretos (apenas 1), mas não faremos isso porque há um belo argumento de simetria neste raciocínio:

- Note que escolher 4 pontos para pintar de preto, dentre 6 pontos brancos, é o mesmo que escolher 2 pontos para pintar de branco dentre 6 pontos pretos! Mas isso é ainda o mesmo que escolher 2 pontos entre 6 pontos brancos para pintar de preto, e já fizemos essa contagem, obtendo 15 possibilidades!

- Da mesma forma, o número de escolhas de 5 pontos para pintar de preto dentre 6 pontos brancos é o mesmo número de escolhas de 1 único ponto para pintar de branco dentre 6 pontos pretos. Ou o mesmo de escolher um ponto dentre 6 pontos brancos para pintar de preto, e já fizemos essa contagem, obtendo 6 possibilidades.

- Simetricamente, só há uma possibilidade em que todos os pontos estão marcados e só há uma possibilidade em que todos os pontos não estão marcados. Em ambos os casos, temos apenas 1 possibilidade.

As simetrias às quais acabamos de nos referir são mais fáceis de serem percebidas observando a tabela abaixo:

TABELA 1

Número de pontos pretos	Número de possíveis configurações
0	1
1	6
2	15
3	20
4	15
5	6
6	1
Total	64

SIMETRIA

Nos cálculos da tabela anterior, contamos o número de possibilidades de como escolher uma quantidade de elementos dentre os elementos de um conjunto (escolher 2 pontos para pintar de preto dentre 6 pontos brancos; escolher 5 pontos para pintar de preto dentre 6 pontos brancos, etc.).

A contagem da quantidade dessas possibilidades de escolha fundamenta um conceito muito importante, o de combinação simples. Esse tipo de contagem não pode ser feito como na Etapa 1 (por meio de permutação simples), pois, ao escolhermos um agrupamento, a ordem de seus elementos não deve ser levada em conta. Por exemplo, no alfabeto Braille, ao escolher para pintar de preto o agrupamento composto pelos dois pontos da primeira linha, poderíamos escolher o primeiro ponto para pintar e depois o segundo, ou escolher o segundo ponto para pintar e depois o primeiro. A ordem dessa escolha não altera o agrupamento.

4. Combinações matemáticas

Na Etapa 1 deste curso, já trabalhamos com contagem. Existem situações envolvendo contagem em que a ordem dos elementos é importante; e outras, em que a ordem não é importante. Para entendermos melhor este fato, vamos comparar as respostas das duas perguntas feitas nos exemplos a seguir:

Exemplo 1

▹ **De quantas maneiras diferentes podemos estacionar 3 carros em 2 vagas de garagem?**

Julian Frost / www.flickr.com/photos/24013046@N05/3440793353/

A resposta é muito simples, se pensarmos da seguinte maneira:

Existem 3 possibilidades para preencher a primeira vaga, mas apenas duas possibilidades para preenchermos a segunda.

Pelo Princípio Multiplicativo, o número total de maneiras é $3 \times 2 = 6$ possibilidades. Se A, B e C são os carros, essas 6 maneiras são as seguintes: AB, BA, AC, CA, BC e CB.

Observe que, neste caso, a ordem é muito importante, pois a maneira AB de estacionar os carros é distinta da maneira BA.

Jean Scheijen / SXC

ZooFari / http://commons.wikimedia.org/wiki/File:Banana_Fruit.JPG

Elisabetta Grondona / SXC

Exemplo 2

▹ **Quantas saladas de frutas diferentes podemos fazer usando duas das seguintes frutas: abacaxi, banana ou caqui?**

Será que o mesmo método usado na resposta do *Exemplo 1* funciona para respondermos o *Exemplo 2*? Vamos ver:

Primeiramente, temos 3 possibilidades para escolher a primeira das 3 frutas, depois restam 2 possibilidades para escolhermos a segunda. Com isto, teremos $3 \times 2 = 6$ possibilidades para fazermos nossa salada.

Essa resposta está correta? Será que não fomos enganados por nosso procedimento? Pense um pouco...

De fato, o raciocínio está errado. O número de saladas de frutas não é 6, e sim 3. O que houve de errado no nosso raciocínio?

Vejamos: se *a*, *b* e *c* são as frutas, essas 6 escolhas são as seguintes: *ab*, *ba*, *ac*, *ca*, *bc* e *cb*; mas uma salada de frutas feita com abacaxi e banana é a mesma que uma salada feita com banana e abacaxi, ou seja *ab* = *ba*.

De modo semelhante, *ac* = *ca* e *bc* = *cb*.

É importante observar aqui que, quando duas frutas são permutadas, elas produzem a mesma salada. Neste caso, a ordem de escolha das frutas não é importante, tanto faz escolher abacaxi e banana como banana e abacaxi ou escolher abacaxi e caqui ou caqui e abacaxi etc. Logo, o número correto de saladas que podemos formar escolhendo duas das três frutas é:

$$\frac{3 \times 2}{2} = 3$$

Observe ainda que o número 2 no denominador corresponde justamente à permutação de duas frutas. Ou seja, usando esse procedimento, contamos o número de saladas como se a ordem fosse importante e dividimos o resultado pelo número de permutações de 2 elementos.

Nesse último exemplo, aparece o conceito de **combinação simples**.

O primeiro exemplo não é uma combinação e sim uma permutação, pois a ordem em que os carros são estacionados nas vagas é importante. Já o segundo exemplo é uma combinação simples, pois não importa a ordem de escolha das frutas.

Uma **combinação simples** é um agrupamento de alguns objetos de um dado conjunto em que os objetos não podem ser escolhidos de forma repetida e a ordem de seus elementos não é importante. Ou seja, agrupamentos com os mesmos elementos são considerados iguais, independentemente da ordem em que são agrupados.

Observe bem o que fizemos na resposta do *Exemplo 2*:

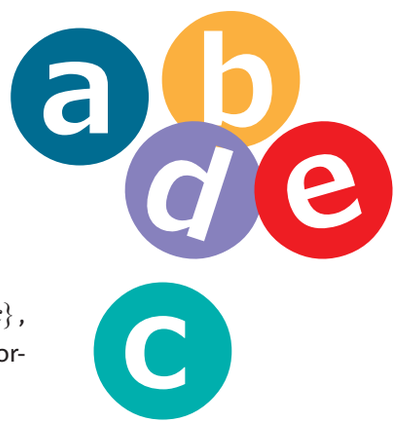
- Aplicamos o Princípio Multiplicativo para obter todas as possibilidades, considerando que a ordem é importante, e encontramos $3\times2\times1=3!$ possibilidades.

- Dividimos o resultado obtido acima pelo número de permutações dos elementos do agrupamento que precisamos escolher. Como intencionamos fazer saladas com 2 frutas, dividimos o número de possibilidades encontradas por $2!=2$, obtendo $\frac{3!}{2!}$.

Como estamos buscando um procedimento geral para resolver problemas como esse, vamos reescrever a resposta usando a notação fatorial, e nossa resposta ficará denotada da seguinte maneira:

$$C_3^2=\frac{3!}{2!(3-2)!}=3$$

Vamos apresentar outro exemplo, com um conjunto um pouco maior, onde você vai perceber que o uso da notação fatorial acima é bastante conveniente.



Exemplo 3

- **Quantos subconjuntos do conjunto $\{a,\ b,\ c,\ d,\ e\}$ possuem exatamente três elementos?**

Primeiramente, observe que, nesse caso, duas escolhas, como $\{b,c,e\}$ e $\{e,b,c\}$, geram um mesmo subconjunto com 3 elementos. Logo, a ordem nesse caso não é importante, mas vamos agir da mesma maneira que fizemos no caso anterior.

Aplicamos o Princípio Multiplicativo para obter todas as possibilidades de escolher 3 elementos dentre os 5 elementos do conjunto, considerando que é importante a ordem desses elementos. Logo, teremos 5 maneiras de escolher o primeiro elemento, 4 maneiras de escolher o segundo elemento e 3 maneiras de escolher o terceiro elemento. Pelo Princípio Multiplicativo, teremos $5\times4\times3$ maneiras de escolher os três elementos. Em notação fatorial, teremos $5\times4\times3=\frac{5!}{2!}$, ou melhor, $\frac{5!}{2!}=\frac{5!}{(5-3)!}$ maneiras.

Entretanto, como já sabemos, procedendo assim estamos contando, por exemplo, conjuntos de três elementos do tipo $\{a,b,e\}$, $\{a,e,b\}$, $\{b,a,e\}$, $\{b,e,a\}$, $\{e,a,b\}$ e $\{e,b,a\}$ como se fossem conjuntos distintos. Logo, devemos retirar dessa nossa contagem esses subconjuntos contados mais de uma vez.

Como certos conjuntos foram contados mais de uma vez, dividimos o resultado obtido acima pelo número de permutações dos elementos do agrupamento que precisamos escolher. Nesse caso, como estamos escolhendo 3 elementos, precisamos dividir a quantidade de maneiras encontrada no passo anterior, que foi $\frac{5!}{(5-3)!}$, pelo número de permutações de 3 elementos, que é $3!$ A resposta, portanto, será:

$$C_5^3 = \frac{5!}{3!(5-3)!}$$

Um agrupamento desse tipo é chamado: ***uma combinação simples de 5 elementos tomados 3 a 3***.

Desenvolvendo o fatorial que aparece na expressão acima, encontramos:

$$C_5^3 = \frac{5!}{3!(5-3)!} = \frac{5\times 4\times 3!}{3!2!} = 10$$

Como nesse exemplo trabalhamos com quantidades pequenas de elementos, é fácil verificar que os dez conjuntos procurados, de fato, são os seguintes: $\{a,b,c\}$, $\{a,b,d\}$, $\{a,b,e\}$, $\{a,c,d\}$, $\{a,c,e\}$, $\{a,d,e\}$, $\{b,c,d\}$, $\{b,c,e\}$, $\{b,d,e\}$, $\{c,d,e\}$.

Uma grande preocupação ao resolver problemas deve ser a investigação e a busca de métodos que possam resolver problemas gerais. Vamos, então, resolver o caso geral dos problemas anteriores?

Exemplo 4 (à procura da solução do caso geral)

Vamos supor que temos n objetos distintos e precisamos escolher, não importando a ordem, p objetos distintos dentre esses (com $n \leq p$) objetos. De quantas maneiras podemos fazer isso? Esse problema reduz-se a calcular o número de combinações simples de n elementos tomados p a p. Para fazermos esse cálculo, vamos proceder como nos casos anteriores:

- Aplicamos o Princípio Multiplicativo para obter todas as maneiras de escolher um agrupamento de p elementos dentre os n elementos em questão, primeiramente considerando que a ordem desses elementos é importante. Veja a tabela a seguir.

Escolha do 1º elemento	Escolha do 2º elemento	Escolha do 3º elemento	...	Escolha do (p-1)-ésimo elemento	Escolha do p-ésimo elemento
n possibilidades	n – 1=n-(2-1) possibilidades	n – 2=n-(3-1) possibilidades	...	n – (p – 1-1) possibilidades	n – (p – 1-1) possibilidades

Pelo Princípio Multiplicativo, obtemos $n \times (n-1) \times (n-2) \times ... \times (n-(p-1))$ maneiras de escolher p elementos dentre n elementos, considerando, primeiramente, que a ordem deles é importante.

Como $n! = n \times (n-1) \times (n-2) \times ... \times (n-(p-1)) \times (n-p)!$ em notação fatorial, escrevemos $n \times (n-1) \times (n-2) \times ... \times (n-(p-1)) = \frac{n!}{(n-p)!}$ maneiras.

Entretanto, note que, procedendo assim, estamos contando certos conjuntos mais de uma vez. Logo, precisamos retirar dessa nossa contagem os conjuntos repetidos. Vale lembrar aqui que a divisão nada mais é do que uma subtração sucessiva de parcelas iguais.

- Dividimos o resultado obtido acima pelo número de permutações dos elementos do subconjunto que escolhemos. Nesse caso, como estamos escolhendo p elementos, dividimos o número $\frac{n!}{(n-p)!}$ encontrado no passo anterior pelo número de permutações de p elementos, que é $p!$ A resposta, portanto, será:

$$C_n^p = \frac{n!}{p!(n-p)!}$$

O símbolo $C_n^p = \frac{n!}{p!(n-p)!}$ é lido como: ***combinação simples de*** n ***elementos tomados*** p ***a*** p**.**

A resolução de vários problemas de contagem reduz-se em saber calcular o número de possibilidades de formar agrupamentos de p elementos de um conjunto com n elementos. Como já fizemos esse cálculo, de agora em diante, para resolver esses tipos de problema, basta calcular o:

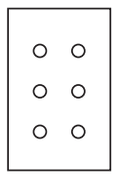
Número de combinações simples de *n* elementos tomados *p* a *p*:

$$C_n^p = \frac{n!}{p!(n-p)!}$$

Como exemplo, na próxima seção, iremos relacionar as combinações com a linguagem Braille.

5. As combinações e a linguagem Braille

Podemos analisar agora todas as possibilidades da escrita Braille em uma célula 3×2, usando a noção de combinação simples que aprendemos nas seções anteriores:



Esse problema se reduz em saber de quantas maneiras podemos pintar de preto a quantidade p desses pontos brancos, nos casos em que $p = 0$, 1, 2, 3, 4, 5 e 6. Ou ainda, podemos pensar em quantos conjuntos (agrupamentos) com p $(p \leq 6)$ elementos podemos formar a partir de um conjunto com 6 elementos. Neste caso, o número de pontos que podemos combinar entre si é $n = 6$, e queremos encontrar a quantidade de combinações de 6 elementos tomados p a p, fazendo $p = 0$, $p = 1$, $p = 2$, ..., $p = 6$.

Vamos colocar os resultados que buscamos na tabela abaixo, isso nos permite visualizar certos comportamentos do número de contagens.

TABELA 2

Número de pontos em preto	Quantidade de combinações distintas
$p = 0$	Não pintamos nenhum ponto dentre os seis pontos: $C_6^0 = \frac{6!}{0!(6-0)!} = 1$
$p = 1$	Número de maneiras de pintar um ponto de preto dentre seis pontos brancos, ou quantos conjuntos distintos de um elemento podemos formar com um conjunto com 6 elementos: $C_6^1 = \frac{6!}{1!(6-1)!} = 6$
$p = 2$	Número de maneiras de pintar dois pontos de preto dentre seis pontos brancos, ou quantos conjuntos distintos de dois elementos podemos formar com um conjunto com 6 elementos: $C_6^2 = \frac{6!}{2!(6-2)!} = 15$

continua...

Número de pontos em preto	Quantidade de combinações distintas
$p = 3$	Número de maneiras de pintar três pontos de preto dentre seis pontos brancos, ou quantos conjuntos distintos de três elementos podemos formar com um conjunto com 6 elementos: $$C_6^3 = \frac{6!}{3!(6-3)!} = 20$$
$p = 4$	Número de maneiras de pintar quatro pontos de preto dentre seis pontos brancos, ou quantos conjuntos distintos de quatro elementos podemos formar com um conjunto com 6 elementos (nesse caso, podemos também usar a simetria, e o problema é o mesmo de pintar dois pontos de preto dentre seis pontos brancos (vide Tabela 1)). $$C_6^4 = \frac{6!}{4!(6-4)!} = 15$$
$p = 5$	Número de maneiras de pintar cinco pontos de preto dentre seis pontos brancos, ou quantos conjuntos distintos de cinco elementos podemos formar com um conjunto com 6 elementos. (nesse caso também podemos usar a simetria, e o problema é o mesmo de pintar um ponto de preto dentre seis pontos brancos (vide Tabela 1)). $$C_6^5 = \frac{6!}{5!(6-1)!} = 6$$
$p = 6$	Número de maneiras de pintar seis pontos de preto dentre seis pontos brancos, ou quantos conjuntos distintos de seis elementos podemos formar com um conjunto com 6 elementos (o argumento de simetria também se aplica aqui (vide Tabela 1)). $$C_6^6 = \frac{6!}{6!(6-6)!} = 1$$

A partir deste exemplo, podemos chegar a uma importante conclusão:

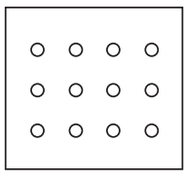
- A simetria dos resultados acima sugere que $C_n^p = C_n^{n-p}$. De fato,

$$C_n^p = \frac{n!}{p!(n-p)!} = \frac{n!}{(n-p)!(n-(n-p))!} = C_n^{n-p}$$

Existem outras igualdades muito curiosas que podem ser provadas a partir da observação dessas simetrias. Deixamos algumas, anexadas a esta seção, para que você possa melhor conhecê-las.

Atividade 3

a ▸ Procedendo como na linguagem Braille, se, em vez de uma célula 3×2, tivermos uma célula 3×4, como a da figura a seguir, quantas configurações diferentes teremos no total?



b ▸ Em uma célula 3×4, quantas são as configurações que possuem exatamente 5 pontos marcados?

c ▸ Em uma célula $n\times m$, quantas configurações diferentes podemos formar?

d ▸ Em uma célula $n\times m$, quantas configurações têm exatamente p pontos marcados?

Resposta comentada

a ▸ Nesse caso, formaremos um sistema com $3\times4=12$ pontos. Para cada ponto, temos duas possibilidades: marcado ou não-marcado. Pelo Princípio Multiplicativo, a quantidade de configurações diferentes que pode ser formada é:

$$2\times2\times2\times2\times2\times2\times2\times2\times2\times2\times2\times2=2^{12}=4096$$

b ▸ Nesse caso, formaremos um sistema com $3\times4=12$ pontos. Temos um conjunto com 12 pontos, dos quais precisamos escolher 5 deles para pintar. A ordem em que esses 5 pontos são escolhidos importa? Certamente não. Dessa forma, o problema se reduz a calcular o número de subconjuntos de 5 elementos que pode ser formado de um conjunto com 12 elementos. Isso é calcular o número de combinações de 12 elementos tomados 5 a 5:

$$C_{12}^{5}=\frac{12!}{5!(12-5)!}=792$$

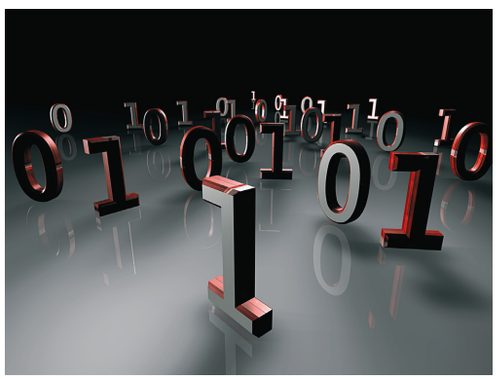
c ▸ Nesse caso, formaremos um sistema com $n\cdot m$ pontos. Para cada ponto, temos duas possibilidades: marcado ou não-marcado. Pelo Princípio Multiplicativo, a quantidade de configurações diferentes que pode ser formada é $2^{n\cdot m}$.

d ▸ Temos, nesse exemplo, um conjunto com $n\cdot m$ pontos, dos quais precisamos escolher p pontos para pintar. A ordem dessa escolha importa? Não. Logo, o problema reduz-se a contarmos o número de subconjuntos com p elementos que podemos formar de um conjunto com $n\cdot m$ elementos. Isso é o mesmo que calcular o número de combinações de $n\cdot m$ elementos tomados p a p $(C_{n\cdot m}^{p})$.

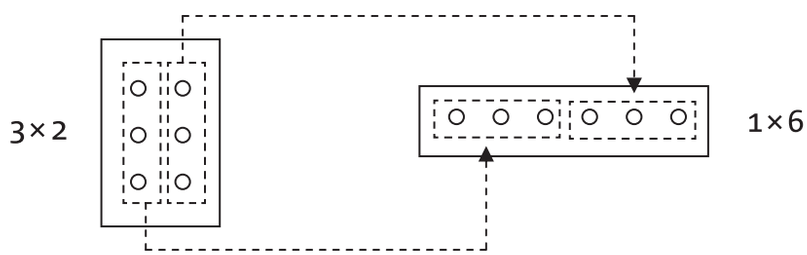
As mesmas ideias de contar certos tipos de agrupamentos que usamos no sistema Braille podem também ser aplicadas para resolver outros tipos de problema de contagem. Essas ideias seguem um mesmo padrão, como você verá a seguir no caso particular do sistema binário de numeração.

6. O sistema Binário

Vamos estudar agora um sistema de representação de objetos em que as configurações possuem somente uma linha e 6 colunas. Ele será muito semelhante ao sistema usual da linguagem Braille 3×2. De fato, observe que no sistema Braille temos 6 pontos para marcar e, nas configurações de uma linha e seis colunas, também temos 6 pontos. Cada um dos pontos do sistema Braille pode ser associado a um único ponto de uma configuração 1×6. Veja:



Autor desconhecido / SXC

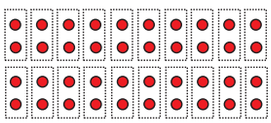


O sistema usual em que escrevemos os números é o decimal, de base 10, mas há outros sistemas em que os números são escritos em outras bases, que são também muito importantes.

Analisemos o sistema em base 2. Sistemas como os anteriores, do tipo $1\times n$, podem servir para escrever números na base 2 e têm muitas aplicações na Matemática, na Informática e nas Engenharias. Podemos representar qualquer número natural na base 2, utilizando apenas os dígitos 0 e 1, que são os únicos algarismos que fazem parte do sistema binário de representação.

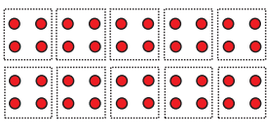
Atenção

Dado um número qualquer, podemos formar diferentes agrupamentos para representá-lo. Nosso objetivo é ensinar como encontrar agrupamentos adequados que nos permitam escrever esse número na base 2. Vejamos:



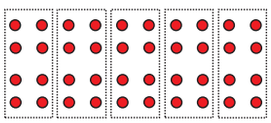
$41 = 20 \times 2 + 1$

Formamos 20 pares, observe que sobra uma unidade.



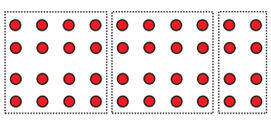
$41 = 10 \times 4 + 1$

Usamos os 20 pares anteriores para formar 10 grupos de quatro elementos cada um.



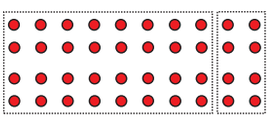
$41 = 5 \times 8 + 1$

Usamos os 10 grupos de quatro elementos obtidos anteriormente para agrupá-los em cinco grupos maiores com oito elementos cada.



$41 = 2 \times 16 + 1 \times 8 + 1$

Usamos os 5 grupos de oito elementos obtidos anteriormente para agrupá-los em dois grupos maiores com dezesseis elementos cada. Note que sobra um grupo de oito elementos e também uma unidade.



$41 = 1 \times 32 + 1 \times 8 + 1$

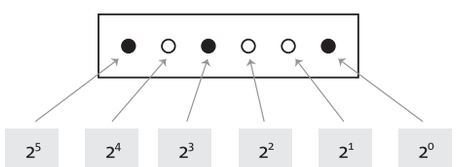
Finalmente usamos os 2 grupos de dezesseis elementos que surgiram no estágio anterior para agrupá-los em um único grupo maior com trinta e dois elementos. Além desses, restam um grupo de oito e uma unidade simples.

Do último agrupamento, conseguimos escrever 41 como soma de potências de 2:

$$41 = 1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$$

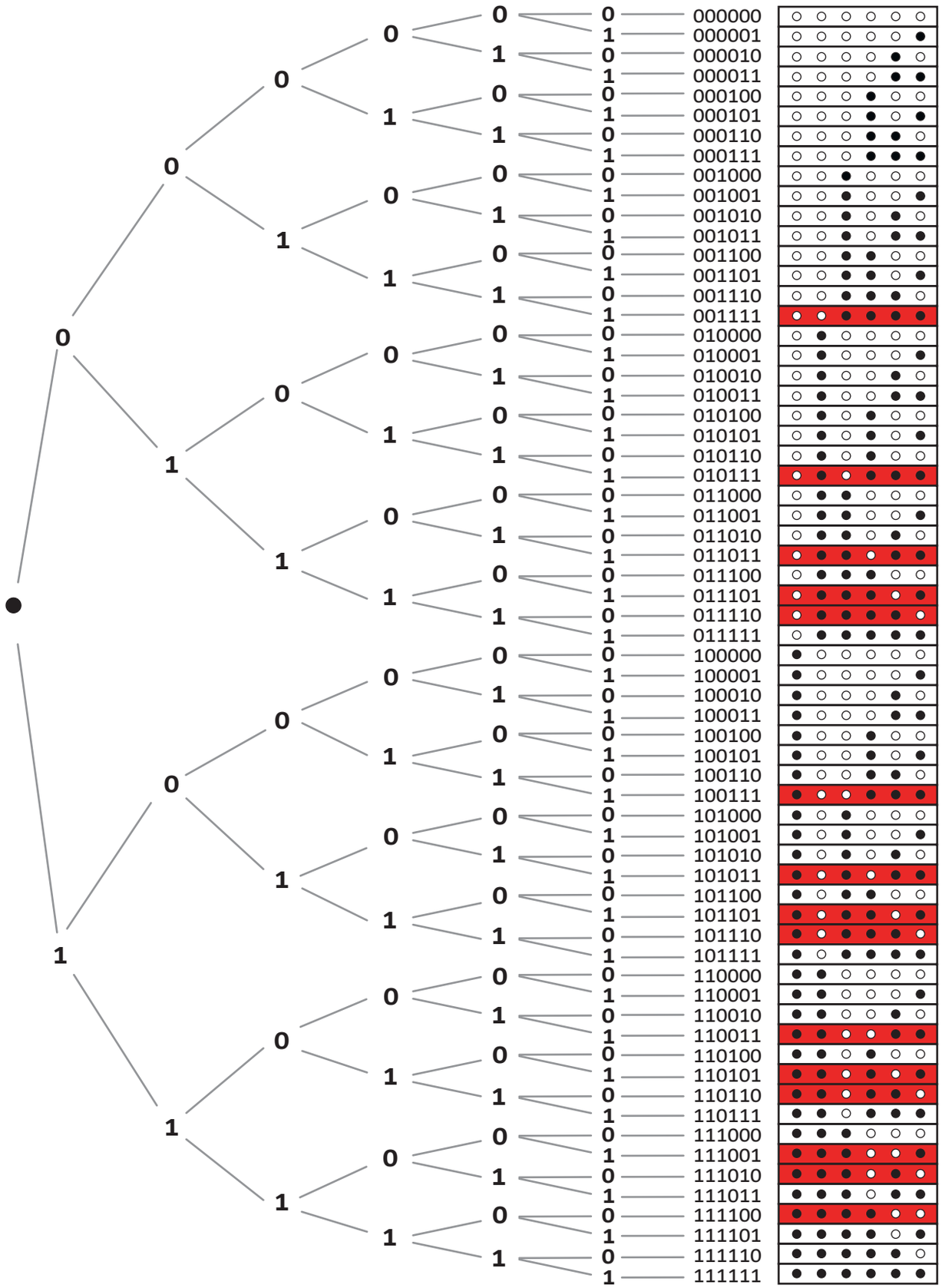
Essa expressão é escrita abreviadamente da seguinte forma: $41 = (\mathbf{1\,0\,1\,0\,0\,1})_2$ (lê-se: 41 é um, zero, um, zero, zero, um, na base 2).

Veja outra forma de representar o número 41:



Pintamos o ponto de preto quando ele representar o 1 e deixamos em branco quando ele representar o 0.

Vamos ver uma maneira simples de encontrar representações binárias? Para exemplificar, escolhemos trabalhar com os números que vão de 0 a 63. Dessa maneira, que é muito prática, é possível ver mais efetivamente a relação entre o sistema binário e as combinações simples. Usando apenas o 0 e o 1 do sistema binário, construamos a seguinte árvore de possibilidades:



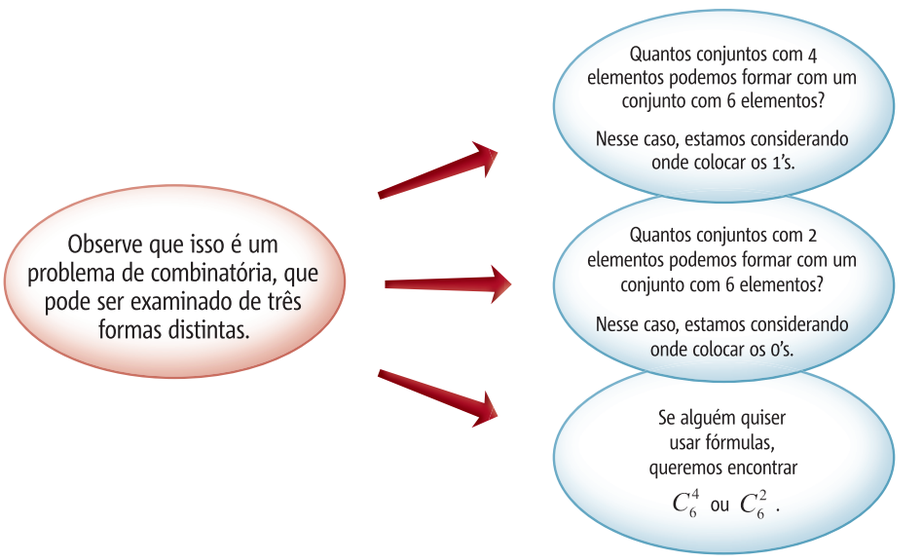
Essa árvore de possibilidades esconde várias informações e tem uma ligação muito grande com problemas de contagem, combinatória e sistema decimal binário. Vamos ver?

Para começar, pense nas seguintes questões:


Maarten Ullenbroek / SXC

1) De quantas maneiras posso dispor quatro 1's em uma configuração 1×6 ? (As outras casas serão completadas com 0's).

Para respondermos a essa pergunta, devemos primeiro responder outra: a ordem de disposição dos 1's é importante? Não!



Agora, recorra à árvore, olhe o "galho" final (as representações por pontos à direita), encontre e conte essas configurações.

Você encontrou a resposta 15? Confira, calculando C_6^4 ou C_6^2 e contando o resultado na árvore de possibilidades (em vermelho).


Maarten Ullenbroek / SXC

2) Na árvore, também podemos encontrar todas as possíveis configurações de permutações do tipo C_6^p, para p variando de 0 a 6. O caso anterior foi um caso particular, em que $p = 4$ (ou, $p = 2$ se simetricamente escolhermos pintar 2 pontos de branco entre 6 pontos pretos). Onde encontramos configurações do tipo C_6^3, por exemplo?

Se você recorrer à árvore, vai perceber que o número total de configurações em que aparecem 3 uns e 3 zeros é $C_6^3 = 20$.

3) Nesta árvore, podemos obter a representação binária de qualquer número entre 0 e 63. Duvida?

Maarten Uilenbroek / SXC

Basta analisar de cima para baixo os agrupamentos de zeros e de uns que encontramos:

$(0,0,0,0,0,0)_2 \rightarrow 0 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 0 \times 2^0 = 0+0+0+0+0+0 = 0,$

$(0,0,0,0,0,1)_2 \rightarrow 0 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 0+0+0+0+0+1 = 1,$

$(0,0,0,0,1,0)_2 \rightarrow 0 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0 = 0+0+0+0+2+0 = 2,$

$(0,0,0,0,1,1)_2 \rightarrow 0 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 0+0+0+0+2+1 = 3,$

$(0,0,0,1,0,0)_2 \rightarrow 0 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 0 \times 2^0 = 0+0+0+2^2+0+0 = 4,$

$(0,0,0,1,0,1)_2 \rightarrow 0 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 0+0+0+2^2+0+1 = 5,$

e assim por diante.

4) Você consegue determinar qual a representação binária do número 63?

Maarten Uilenbroek / SXC

Se respondeu $(111111)_2$, que é o último da lista, acertou.

As ideias de representação binária de números podem ser usadas para resolver diversos problemas, como você pode ver no boxe a seguir.

Saiba Mais **Problemas diferentes podem ter uma mesma resolução?**

Leia atentamente as seguintes perguntas:

a) De quantas maneiras quatro homens e três mulheres podem sentar em sete cadeiras? (Cada pessoa em uma cadeira).

b) Uma equipe de quatro alunos será escolhida de um grupo de sete alunos. De quantas maneiras isso pode ser feito?

c) Em um jantar, há sete opções de pratos distintos. Você deve escolher três deles, sem repeti-los. De quantas formas você pode fazer essas três escolhas?

d) Quantas configurações podemos formar com sete lâmpadas: três apagadas e quatro acesas?

e) Existem quantos subconjuntos com 3 elementos em um conjunto com sete elementos?

f) De quantas maneiras podemos colocar quatro 1's e três 0's em uma configuração 1×7 ?

O que há em comum entre essas seis perguntas?

Para respondê-las, podemos aplicar um mesmo raciocínio, baseado em escolhas. Estamos chamando de uma escolha o processo de decisão em que podemos associar o número 1 a um tipo de escolha e o número 0 ao outro tipo. Por exemplo, na primeira pergunta, podemos associar o número 1 aos homens e 0 às mulheres. No segundo exemplo, os alunos escolhidos podem ser representados por 1 e os não escolhidos por 0. A mesma ideia pode ser aplicada para o terceiro exemplo. Finalmente, no exemplo das lâmpadas, as acesas podem ser representadas por 1 e as apagadas por 0.

Para resolver qualquer dos problemas anteriores, cujas resoluções seguem o mesmo padrão, o importante é ter um modelo em mente e saber aplicá-lo. Podemos utilizar, por exemplo, o sistema binário para resolver qualquer um deles.

Vamos explorar os conceitos de combinação simples, que estávamos estudando, usando a ideia de sistema binário, por meio de um problema envolvendo uma situação de sala de aula.

Atividade 4

Uma professora colocou no quadro a seguinte pergunta:

a ▸ ***Quantas configurações podemos formar com sete lâmpadas: três apagadas e quatro acesas?***

A professora recomendou que uma lâmpada acesa fosse representada pelo dígito 1 e uma lâmpada apagada, pelo dígito 0, associando a resolução do problema ao sistema binário.

Três alunas e dois alunos deram suas respostas, que reproduzimos a seguir. Diga qual, ou quais, dessa(s) resposta(s) está(ão) correta(s) e por quê.

Julien Tromeur / SXC

Resposta do aluno 1:

"Basta que eu me preocupe sobre a posição em que posso colocar os três zeros, pois o restante será mesmo completado com 1. Ora, o problema se reduz a saber como posso dispor três zeros em uma tabela do tipo a seguir:

posição 1	posição 2	posição 3	posição 4	posição 5	posição 6	posição 7

Há 7 possibilidades para o primeiro zero, 6 para o segundo e 5 para o terceiro, resultando em $7 \times 6 \times 5 = 210$ possibilidades. Logo, há 210 configurações de 7 lâmpadas com 3 acesas e 4 apagadas."

Resposta da aluna 2:

"Basta que eu me preocupe sobre a disposição dos quatro 1's em uma tabela como a que segue:

posição 1	posição 2	posição 3	posição 4	posição 5	posição 6	posição 7

pois o restante dos dígitos serão completados com zeros. Observe que a ordem em que posso dispor esses 1's não importa. Assim, o problema fica reduzido a saber em quais dessas posições posso colocar os quatro 1's, ou melhor, a tarefa é a mesma de contar o número de maneiras que posso escolher 4 dentre essas 7 posições. Basta, portanto, calcular:

$$C_7^4 = \frac{7!}{4!(7-4)!} = 35$$

- Resposta: há 35 configurações de 7 lâmpadas com 3 acesas e 4 apagadas."

Resposta da aluna 3:

"Basta que eu me preocupe sobre a forma de dispor os três zeros em uma tabela como a que segue:

posição 1	posição 2	posição 3	posição 4	posição 5	posição 6	posição 7

pois o restante dos dígitos serão completados com 1's. Isso é o mesmo de saber em quais dessas posições posso colocar os três zeros, ou melhor, a tarefa é a mesma de contar o número de maneiras que posso escolher 3 dentre essas 7 posições. Basta, portanto, calcular:

$$C_7^4 = \frac{7!}{4!(7-4)!} = 35$$

- Resposta: há 35 configurações de 7 lâmpadas com 3 acesas e 4 apagadas."

Resposta da aluna 4:

"O raciocínio do aluno 1 está quase correto, mas ele esqueceu de contar as posições que os 1's podem assumir. Além de $7\times6\times5$ maneiras, ele ainda tem 4 maneiras de dispor o primeiro 1, 3 maneiras de dispor o segundo 1, 2 maneiras de dispor o terceiro 1 e 1 maneira de dispor o quarto 1. Portanto, temos

$$7\times6\times5\times4\times3\times2\times1=7!=5040$$

configurações de 7 lâmpadas com 3 acesas e 4 apagadas.

Resposta do aluno 5:

"É muito fácil perceber que já que nós temos quatro 1's e três zeros e eles são iguais, basta contar todas as possibilidades de permutá-los, ou seja, 7!, e depois dividir pelo número de permutações dos agrupamentos iguais entre si. Logo, teremos:

$$\frac{7!}{3!4!}=\frac{7\times6\times5\times4!}{3!4!}=35$$

números de tamanho 7 em representação binária que têm três zeros e quatro 1's.

Resposta comentada

Comentemos a seguir a resposta de cada aluno:

Resposta do aluno 1: Essa resposta está errada. Procedendo dessa forma, o aluno está considerando que a ordem em que os 1's são escolhidos é importante. Desse jeito, se representamos os 1's por cores diferentes, o primeiro por 1, o segundo por **1** e o terceiro por **1**, o aluno está contando, por exemplo, uma configuração do tipo **1,0,0,0,1,0,1** como se fosse diferente das configurações **1,0,0,0,1,0,1** ou **1,0,0,0,1,0,1**. Ou seja, a quantidade que ele encontrou, 210 possibilidades, levou em consideração a ordem, uma dessas configurações era diferente da outra. Logo, esse número deve ser dividido pelo número de permutações de um conjunto com três 1's, que é 3!=6. A resposta correta é:

$$\frac{210}{3!}=\frac{210}{6}=35$$

Resposta da aluna 2: A resposta da aluna está correta. A ordem em que se escolhe os 1's não importa. O problema é de combinação mesmo e reduz-se em contar a quantidade de subconjuntos com 4 elementos que pode ser formada com um conjunto com 7 elementos.

A quantidade de combinações de 7 elementos tomados 4 a 4 é:

$$C_7^4=\frac{7!}{4!(7-4)!}=35$$

Resposta da aluna 3: A resposta também está correta. Ela procedeu como a aluna 2, só que se preocupou onde colocar os 0's e a aluna 2 onde colocar os 1's. O problema mais uma vez reduz-se em calcular a quantidade de combinações.

A quantidade de combinações de 7 elementos tomados 3 a 3 é:

$$C_7^3=\frac{7!}{3!(7-3)!}=35$$

O resultado foi o mesmo do encontrado pela aluna 3. Isso não é novidade alguma, pois antes da Atividade 3 vimos que:

$$C_n^p=C_n^{n-p}$$

expressão que neste caso toma a forma:

$$C_7^3=C_7^{7-3}=C_7^4$$

Resposta da aluna 4: A resposta está errada. Ela calculou as permutações de 7 elementos. Dessa maneira, ela considerou que a ordem importava e permutações do tipo **1,0,0,0,1,0,1** e **1,0,0,0,1,0,1** etc. foram contadas mais de uma vez, apesar de serem iguais. Por isso, ela obteve uma quantidade tão grande de possibilidades.

Resposta do aluno 5: A resposta do aluno está correta. Ao considerar todas as permutações possíveis dos 1's e 0's, encontramos $7!$ possibilidades. Note que há 4 uns e 3 zeros e estamos com um conjunto com $3+4=7$ elementos. Mas, com esse cálculo, estamos contando várias configurações

mais de uma vez. Já explicamos isso nos comentários anteriores das respostas dos alunos. Para compensar as contagens, foram feitas mais de uma vez certas configurações (por exemplo, **1,0,0,0,1,0,1** e **1,0,0,0,1,0,1** etc.), dividimos $7!$ pelo número de permutações de agrupamentos com os 3 zeros, que é $3!$, obtendo:

$$\frac{7!}{3!}$$

Depois, dividimos esse número pelo número de permutações de agrupamentos com os 4 uns, que é $4!$, encontrando:

$$\frac{\frac{7!}{3!}}{4!} = \frac{7!}{3!4!} = \frac{7\times6\times5\times4!}{3!4!} = 35$$

Esta seção nos deixa uma bela lição: que uma mesma ideia matemática – a maneira de contar o número de agrupamentos possíveis de uma quantidade de elementos de um conjunto – pode ser usada para resolver problemas aparentemente bem distintos. Note que a resolução de problemas de contagem, envolvendo a linguagem Braille, o sistema binário de representação numérica e o problema das lâmpadas foram resolvidos com a mesma técnica de contagem, calculando o número de combinações simples.

A seguir, apresentaremos outros problemas interessantes que podem ser resolvidos usando técnicas de contagem, alguns em que a ordem é importante e outros não.

7. Exercícios resolvidos


Jade Gordon / SXC

1. Um grupo de cinco professores comporá uma comissão para falar com o Secretário de Educação do Estado. Os cinco professores serão escolhidos dentre nove professores indicados por seus pares. Quantas comissões poderão ser formadas?

   ▹ **Resolução:** Primeiramente, devemos responder à seguinte pergunta: "A ordem da escolha dos professores é importante?". Nesse caso, escolher {João, José, Maria, Rita, Pedro} é o mesmo que escolher {José, Maria, João, Rita, Pedro}. Logo, a ordem não importa, e o problema resume-se a um problema de combinação simples: contar quantos conjuntos com cinco elementos podemos formar, usando os elementos de um conjunto com nove elementos. A resposta é:

$$C_9^5 = \frac{9!}{5!(9-5)!} = \frac{9\times8\times7\times6\times5!}{5!4!} = 126$$

2. Um grupo de cinco professores comporá uma comissão para falar com o Secretário de Educação do Estado. Três desses professores serão escolhidos dentre sete professores de Matemática e os outros dois serão escolhidos dentre cinco professores de Português (supomos, é claro, que um mesmo professor não ministre duas disciplinas). Neste caso, quantas comissões serão possíveis de ser formadas?

▹ **Resolução:** A resolução segue o mesmo raciocínio do exercício anterior. Podemos escolher $C_7^3 = 35$ professores de Matemática e $C_5^2 = 10$ professores de Português para compor a comissão. Como, para cada professor de Matemática, podemos escolher uma dentre 10 combinações de professores de Português, e temos $C_7^3 = 35$ professores de Matemática, teremos $C_7^3 \times C_5^2 = 10 \times 35 = 350$ comissões possíveis.

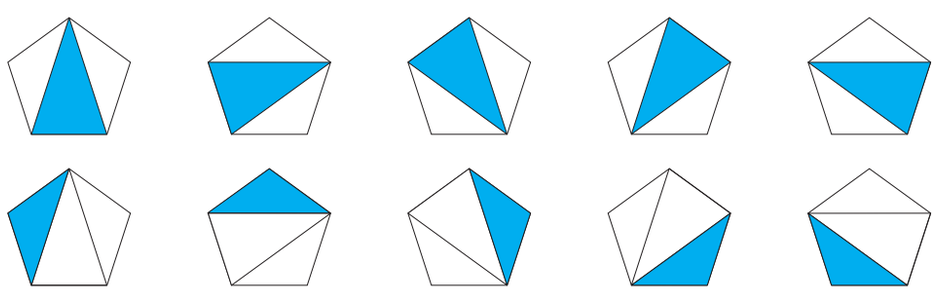
Observação importante: devemos ter muito cuidado ao trabalhar com a divisão de um conjunto em grupos, pois podemos erroneamente contar em demasia. Como exemplo, considere o seguinte problema análogo ao problema que estamos estudando:

3. Queremos dividir um grupo de 8 pessoas em dois grupos de 4 pessoas cada. De quantos modos isto pode ser feito?

▹ **Resolução:** Isto não pode ser feito colocando simplesmente as pessoas em fila (neste caso a resposta seria $8!$). Dentro de cada grupo de 4 pessoas a ordem não é importante e mesmo os dois grupos podem ser permutados sem que se obtenha uma maneira diferente de divisão (por exemplo, a separação 1234|5678 é a mesma que 5678|1234). Para obter a resposta correta, observamos que em $8!$ cada grupo foi contado $4! \cdot 4! \cdot 2$ vezes e a resposta correta é $\frac{8!}{4! \cdot 4! \cdot 2} = 35$ maneiras.

4. Dado um pentágono, quantos triângulos são possíveis de serem construídos com segmentos de retas cujas extremidades são os vértices desse pentágono?

▹ **Resolução:** Antes de ver a resolução desse problema, tente resolvê-lo, treinando sua maneira pessoal de enfrentar problemas desse tipo. Vale a pena tentar.
Agora vamos resolver o problema. Ora, na verdade, os objetos em questão são os vértices do pentágono que geram os triângulos. Devemos escolher três desses vértices. Mais uma vez, a perguntinha de sempre: "a ordem importa?" Note que não. Por exemplo, um triângulo gerado pelos vértices A, B e C é o mesmo do gerado pelos vértices B, A e C.
Logo, o problema é de combinação simples e reduz-se a contar de quantas maneiras podemos escolher três elementos em um conjunto com cinco elementos. A resposta, como já sabemos, é $C_5^3 = 10$.



5. Um ***anagrama*** é uma combinação de letras formada pela permutação das letras de outra palavra. Por exemplo: *roma*, *omar*, *ramo* são anagramas da palavra *amor* que são palavras (isto é, têm significado em português). Já *maor*, *orma* etc. também serão consideradas como anagramas, apesar de não serem propriamente palavras. Uma questão bastante interessante é contar a quantidade de anagramas de uma palavra. Vamos aprender a fazer isso nesse exercício.

a) Quantos anagramas tem a palavra *amor*?
b) Quantos anagramas da palavra *amor* começam com *r*?
c) Quantos anagramas da palavra *amor* começam com *r* e terminam com *a*?
d) Quantos anagramas da palavra *amor* terminam com vogal?
e) Quantos anagramas tem a palavra *amava*?
f) Quantos anagramas tem a palavra *amasse*?

▹ **Resolução:**

a) Mais uma vez, primeiramente, devemos responder à seguinte pergunta: "A ordem das letras é importante?". A resposta é sim, pois *amor* e *maor*, por exemplo, são anagramas distintos, gerados quando permutamos apenas as duas primeiras letras. Observe que qualquer permutação das letras gera um anagrama distinto, pois a palavra *amor* é formada por letras distintas! Dessa forma, a questão é um problema de permutação simples. Como a palavra *amor* tem quatro letras, a resposta é $4!$. Como já fizemos anteriormente, utilizaremos uma tabela para facilitar a visualização do que está acontecendo:

4 possibilidades para a 1ª letra	3 possibilidades para a 2ª letra	2 possibilidades para a 2ª letra	1 possibilidade para a 4ª letra

b) Ora, a primeira letra do anagrama deve ser *R*. Logo, temos uma tabela do tipo abaixo para ser preenchida:

R			

Como a primeira casa ficará sempre ocupada pela letra R, permutaremos apenas três letras em três casas. Portanto, a resposta será $3!$.

c) Da mesma forma que no item anterior, fixamos agora as letras R e A nas primeira e quarta casas, respectivamente:

R			A

Como a primeira casa e a última casa ficarão sempre ocupadas pelas letras R e A respectivamente, permutaremos apenas as duas letras restantes nas duas casas restantes. Portanto, a resposta será $2!$.

d) Desta vez, a restrição no enunciado não prende uma letra numa casa, mas deixa a possibilidade de que apenas uma das duas vogais ocupe a quarta casa.

			A ou O

Então, trabalharemos primeiro com as três casas restantes como no item b), quando tínhamos uma letra presa à primeira casa. Neste caso, teremos a permutação de três letras em três casas: $3!$. Como a última casa possui duas possibilidades, basta multiplicarmos esse resultado por dois, ou seja, a resposta será $2 \times 3! = 12$.

Repare que a diferença entre os itens (b) e (d) está na restrição feita a uma determinada casa: no item (b), uma letra; no item (d), duas letras. Portanto, nada mais natural que o número de permutações do item (d) seja o dobro do item (b).

e) A palavra, aqui, tem algo diferente da que estávamos trabalhando: a palavra ***amava*** tem uma letra que se repete três vezes, a letra *a*. O problema assemelha-se ao que tínhamos no problema 2. Consideramos a palavra como se tivesse todas as letras diferentes. Daí, teríamos $5!$ anagramas. Mas, assim, estamos contando alguns anagramas mais de uma vez, devido às permutações da letra *a*, que se repete 3 vezes e acaba gerando o mesmo anagrama. Veja:

amava, amava, amava, amava, amava, amava.

As permutações das três letras geraram $3! = 6$ palavras iguais. Assim, para descontarmos esses anagramas contados em demasia, dividimos $5!$ por $3!$ obtendo

$$\frac{5!}{3!} = 20 \quad \text{anagramas.}$$

f) A palavra *amasse* tem 6 letras, sendo que duas delas se repetem duas vezes. Logo, raciocinando da mesma forma que no item anterior, dividimos o número de permutações das 6 letras pelos números de vezes que cada letra se repete, eliminando, assim, os anagramas contados mais de uma vez.

$$\frac{6!}{2!2!} = 180 \quad \text{anagramas.}$$

Atenção

A resolução dos itens ***e*** e ***f*** do Exercício 4, bem como a resolução da aluna 5 da Atividade 4, usaram um mesmo procedimento. Nessas resoluções, calculou-se o número total de permutação dos elementos do conjunto e depois se dividiu esse número pelo produto das quantidades das permutações dos elementos que se repetiam. Esse tipo de permutação merece um nome, definido a seguir.

Permutação com repetição – Permutações dos elementos de um conjunto em que certo número de elementos são iguais geram as chamadas ***permutações com repetição***. É fácil verificar que o número de permutações de um conjunto com n elementos em que um elemento se repete n_1 vezes, outro se repete n_2 vezes,..., e um outro se repete n_k vezes (para $n_1 + n_2 + \ldots + n_k$ menor ou igual a n) é dada por:

$$P_n^{(n_1, n_2, \ldots, n_k)} = \frac{n!}{n_1!\, n_2!\ldots n_k!}$$

As respostas dos exercícios anteriores, por exemplo, podem ser escritas da seguinte maneira:

$$P_6^{(2,2)} = \frac{6!}{2!2!} = 180 \quad \text{e} \quad P_6^{(3,4)} = \frac{7!}{3!4!} = \frac{7\times6\times5\times4!}{3!4!} = 35$$

6. O RG (Registro Geral) é ainda hoje, no Brasil, um dos principais documentos de identificação, sendo conhecido como documento de identidade. Vários institutos e empresas têm autonomia para emitir esse documento pelo Brasil, que é único para cada indivíduo.
   Por esses fatores, seria inevitável encontrar números de RG parecidos, ou ainda números que fossem compostos pelos mesmos algarismos. Por exemplo, quantos números de RG distintos podemos obter permutando-se os algarismos do número $95.557.729$?

Ivan Baldivieso / Agecom Bahia

▸ **Resolução:** Esse é um típico problema de permutação com repetição, em que se repetem dois algarismos 9, três algarismos 5 e dois algarismos 7. A resposta, portanto, será:

$$P_6^{(2,3,2)} = \frac{8!}{2!3!2!} = 1680$$

8. Conclusão

Nesta etapa, aprofundamos nossa abordagem acerca de como a Análise Combinatória pode ser trabalhada de uma forma interessante no Ensino Médio.

Esperamos que você tenha percebido que o Princípio Multiplicativo da Contagem deve ser aplicado observando-se dois fatos importantes: o primeiro é a ordem dos elementos e o segundo é a repetição. Quando a ordem é importante, os problemas envolvem os conceitos de permutação. Quando a ordem não é importante, pois não altera o resultado da contagem, os problemas se resolvem usando o conceito de combinação. Quando não há repetições, essas permutações e combinações são chamadas simples. Quando há repetições são chamadas permutações e combinações com repetições.

E mais... Como é comum na Matemática estabelecermos padrões, esperamos que esta etapa o estimule a trabalhar junto a seus alunos o fato de que uma mesma ideia matemática pode ser usada para resolver problemas aparentemente bem distintos. Esse procedimento ajuda a simplificar a resolução de problemas que envolvem Análise Combinatória.

9. Resumo

- O código Braille pode ser um interessante ponto de partida para abordar conteúdos ligados à Análise Combinatória no Ensino Médio.
- O código Braille é baseado em uma disposição 3×2 de pontos. Para registrar uma letra do alfabeto, alguns desses 6 pontos são marcados ou perfurados, para que fiquem sobressalentes e possam ser sentidos com a ponta dos dedos das mãos.
- Como temos seis pontos no sistema 3×2, pelo Princípio Multiplicativo, a quantidade de padrões diferentes que pode ser formada é $2\times 2\times 2\times 2\times 2\times 2 = 2^6 = 64$.
- Há artifícios adicionais para que seja possível representar números, letras maiúsculas e minúsculas, sinais de pontuação e de operações matemáticas, usando a linguagem Braille.
- Há outros métodos, todos baseados no Princípio Multiplicativo de Contagem, para calcular quantas configurações podemos formar usando a linguagem Braille: o método que foca na quantidade de pontos, independente de estarem pintados ou não e o método que foca na quantidade de pontos pintados.
- A linguagem Braille permite a abordagem do conteúdo de combinações simples, já que, ao escolhermos um agrupamento para representar um símbolo nessa linguagem, a ordem de seus elementos não deve ser levada em conta.
- Uma combinação simples é um agrupamento de alguns objetos de um dado conjunto em que a ordem de seus elementos não é importante e em que não há repetição de elementos dentro do mesmo agrupamento.
- Usando o Princípio Multiplicativo para resolver um problema que envolve uma combinação simples, podemos usar a notação fatorial: $C_n^p = \frac{n!}{p!(n-p)!}$ (combinação simples de n elementos tomados p a p).

- No caso da linguagem Braille, o problema se reduz em saber de quantas maneiras podemos pintar de preto a quantidade p desses pontos brancos, nos casos em que $p = 0$, 1, 2, 3, 4, 5 e 6. Podemos também pensar em quantos agrupamentos com p $(p \leq 6)$ elementos podemos formar a partir de um conjunto com 6 elementos. Neste caso, o número de pontos que podemos combinar entre si é $n = 6$ e queremos encontrar as combinações de 6 elementos tomados p a p.
- Uma mesma ideia matemática – a maneira de contar o número de subconjuntos possíveis de uma quantidade de elementos de um conjunto – pode ser usada para resolver problemas aparentemente bem distintos.
- O sistema binário de representação também constitui uma interessante ferramenta para trabalhar Análise Combinatória no Ensino Médio.
- A ideia de representação binária de números pode ser usada para resolver diversos problemas, permitindo a elaboração de um modelo que pode ser aplicado para resolver problemas diversos mas que sigam um mesmo padrão.
- O uso do sistema binário é uma alternativa que permite a exploração do conceito de combinação simples junto aos alunos do Ensino Médio.

10. Anexo

Abaixo citamos alguns resultados provenientes da simetria que está presente nas combinações.

- C_n^2 é igual à soma dos $n-1$ primeiros números naturais. De fato,

$$C_n^2 = \frac{n!}{2!(n-2)!} = \frac{n.(n-1)}{2} = 1+2+...+(n-1)$$

essa última igualdade é bastante conhecida e pode ser provada, por exemplo, através do Princípio de Indução.

- $C_n^0 + C_n^1 + C_n^2 + ... + C_n^n = 2^n$

Para concluirmos porque isto é válido, observe que C_n^p é o número de subconjuntos do conjunto $\{1,2,...,n\}$ com exatamente p elementos e portanto $C_n^0 + C_n^1 + C_n^2 + ... + C_n^n$ é o número total de subconjuntos de $\{1,2,...,n\}$. Devemos responder, então, à seguinte pergunta: quantos são os subconjuntos de $\{1,2,...,n\}$?

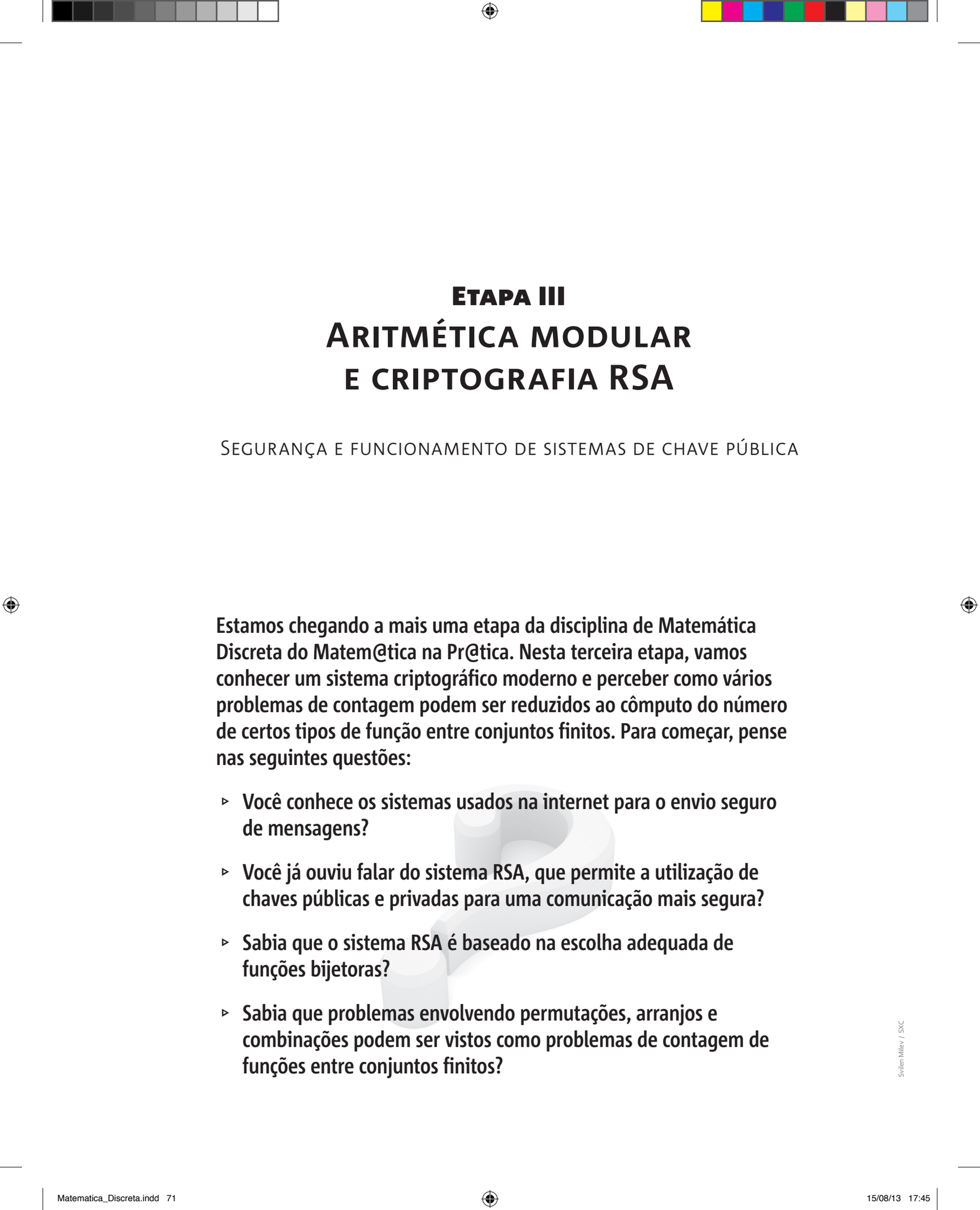
Para determinar um desses subconjuntos, olhamos para o número 1 e perguntamos: ele está ou não no subconjunto? Existem apenas duas respostas: sim ou não. Olhamos para o número 2 e repetimos a pergunta: 2 está ou não no subconjunto em consideração? Mais uma vez, temos duas respostas e continuamos assim até o número n. No total, teremos que tomar *n* decisões, admitindo cada uma delas apenas duas possibilidades. Pelo Princípio Multiplicativo, existirão então $2 \times 2 \times ... \times 2 = 2^n$ decisões, e, como cada decisão determina um e um só subconjunto, teremos que o número total de subconjuntos de $\{1,2,...,n\}$ é 2^n.

Etapa III
Aritmética modular e criptografia RSA

Segurança e funcionamento de sistemas de chave pública

Estamos chegando a mais uma etapa da disciplina de Matemática Discreta do Matem@tica na Pr@tica. Nesta terceira etapa, vamos conhecer um sistema criptográfico moderno e perceber como vários problemas de contagem podem ser reduzidos ao cômputo do número de certos tipos de função entre conjuntos finitos. Para começar, pense nas seguintes questões:

- **Você conhece os sistemas usados na internet para o envio seguro de mensagens?**
- **Você já ouviu falar do sistema RSA, que permite a utilização de chaves públicas e privadas para uma comunicação mais segura?**
- **Sabia que o sistema RSA é baseado na escolha adequada de funções bijetoras?**
- **Sabia que problemas envolvendo permutações, arranjos e combinações podem ser vistos como problemas de contagem de funções entre conjuntos finitos?**



Svilen Milev / SXC

1. Criptografia *x* *Hackers*

"Em Campinas, maio de 1995, um hacker apagou diversos arquivos da Empresa Brasileira de Pesquisas Agropecuárias. Em agosto de 1996, outro hacker, em São Petersburgo, Rússia, roubou US$ 400 mil do Citibank. No início de 1995, um adolescente britânico conseguiu acessar arquivos sigilosos da Força Aérea Norte-Americana sobre inspeções nucleares da Coreia do Norte. Somente em 1993, os computadores do Departamento de Defesa dos EUA foram invadidos 134 vezes." (Fonte: amora.cap.ufrgs.br/2000/projetos/proj1/hac/historias.htm)


Armin Hanisch / SXC


Afonso Lima / SXC

Autor desconhecido / SXC

Nos dias de hoje, relatos como esses ainda são frequentes. Mas poderiam ser mais comuns, caso os sistemas de envio de mensagens não tivessem evoluído. Os meios criptográficos para enviar mensagens secretas são baseados em chaves, distribuídas entre os participantes envolvidos no envio da mensagem. Caso os *hackers* (espiões da era da informática) possuam essas chaves, eles podem ameaçar o sigilo das mensagens, "quebrando o código" e decifrando o arquivo enviado.

Mas como podemos tornar uma chave mais segura e distribuir mensagens com segurança? Haveria outra forma para codificar mensagens, além da criptografia de Júlio César, que foi estudada na Etapa 1?


Adam Cieslelski / SXC

2. Criptografia RSA: um sistema de duas chaves

Por volta do ano de 1977, a fragilidade dos sistemas criptográficos diminuiu muito. Nessa época Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman criaram a Criptografia RSA (iniciais dos sobrenomes dos três autores), que consistia em um sistema com duas chaves baseado em teoremas clássicos, como o da Teoria dos Números. Esse sistema é bastante usado nos dias de hoje.


Zsuzsanna Kilian / SXC

A ideia do sistema é a seguinte: uma das chaves serve para cifrar mensagens e pode ser divulgada livremente – todos têm acesso a ela – por isso é conhecida como ***chave pública***. Por outro lado, para decifrar a mensagem cifrada, há a necessidade de uma chave secreta, conhecida apenas pela pessoa para a qual a mensagem foi enviada, por isto essa chave é conhecida como ***chave secreta***.

A eficácia desse sistema de chaves duplas está na "impossibilidade prática" de se obter a chave secreta a partir da chave pública. Isto porque o sistema utiliza números muito grandes, formados por muitos algarismos. Atualmente, não são conhecidos algoritmos capazes de decompor números muito grandes em fatores primos em um tempo razoável. Essa é uma impossibilidade técnica, ou seja, ainda não pode ser resolvida, mesmo com os avanços da Matemática e da Informática.

Para que você possa entender o funcionamento do sistema de chaves duplas, vamos simular, de modo bem simplificado, uma situação de envio/recepção de uma mensagem.

3. Como funciona um sistema com chave pública?

Vamos mandar uma mensagem para uma pessoa **P**, representando a ideia de como funciona o método RSA.

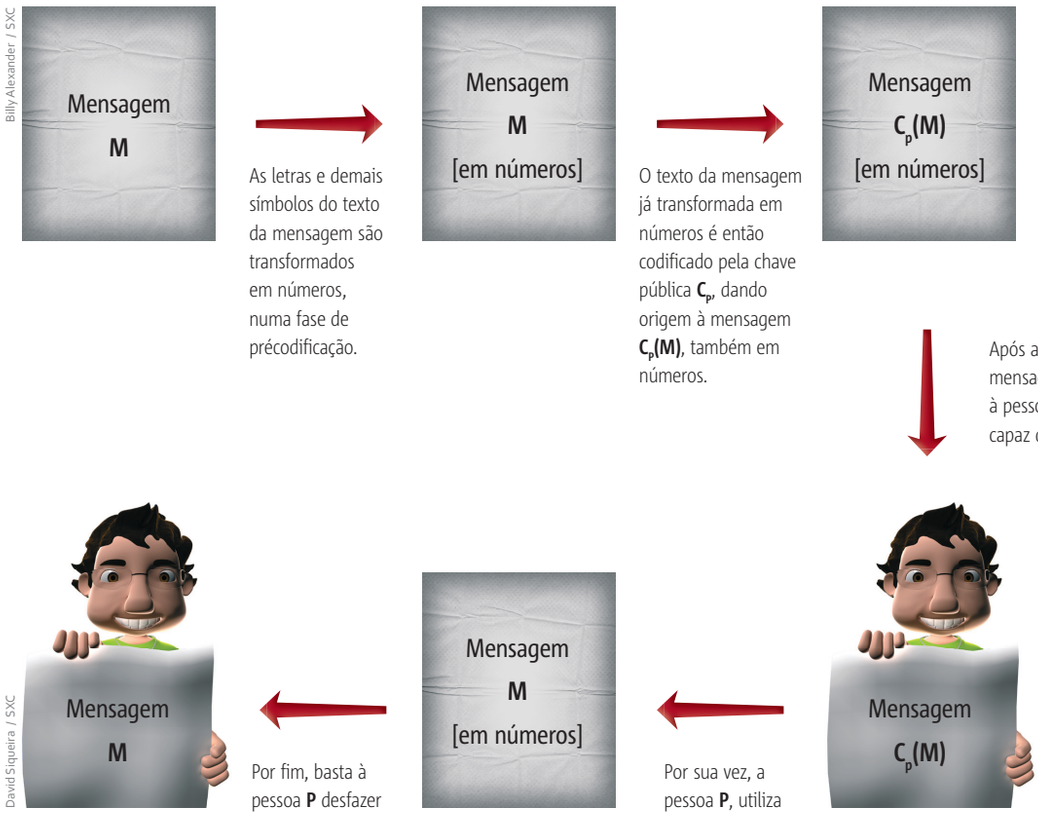
Autor desconhecido / SXC

Assim como nós, **P** deve possuir duas chaves, uma pública e outra secreta. Vamos denotar por $\mathbf{C_p}$ o procedimento que devemos usar para cifrar mensagens dirigidas a **P** e por $\mathbf{D_p}$ o procedimento que **P** deve usar para decifrar as mensagens que recebe, ou seja, $\mathbf{D_p}$ desfaz a codificação $\mathbf{C_p}$.

Considere **M** a mensagem que desejamos enviar a **P**, mas sem nenhuma codificação. Transformamos as letras da mensagem **M** em números. Para enviar **M** secretamente, usamos uma função $\mathbf{C_p}$ (chave pública) que codifica os números associados à mensagem **M**, transformado-a na mensagem codificada que representaremos por $\mathbf{C_p(M)}$.

Quando **P** recebe a mensagem codificada $\mathbf{C_p(M)}$, é necessário que ela conheça outra função $\mathbf{D_p}$ (chave secreta), que inverta a codificação, ou seja, que decodifique os números da mensagem $\mathbf{C_p(M)}$. Para isso, a função $\mathbf{D_p}$ é aplicada aos números associados à mensagem codificada $\mathbf{C_p(M)}$, obtendo-se $\mathbf{D_p(C_p(}\boldsymbol{M}\mathbf{))} = \mathbf{M}$. Assim é possível recuperar a mensagem original e o envio secreto da mensagem é feito com sucesso.

Para compreender melhor todo o processo que acabamos de descrever, observe o esquema a seguir:



Para este processo funcionar, é necessário, então, construir funções C_p e D_p de forma que valha a igualdade $D_p(C_p(M)) = M$ para qualquer mensagem **M**.

Note no processo anterior que a função D_p é a função inversa de C_p, pois a função D_p inverte o que foi feito pela função C_p. As chamadas funções ***bijetoras*** são precisamente as que admitem função inversa.

Assim, as funções C_p e D_p devem ser funções bijetoras, definidas entre conjuntos finitos. Na verdade, observamos que se existir uma função bijetora entre dois conjuntos finitos, estes devem necessariamente ter o mesmo número de elementos.

Uma função de um conjunto *A* em um conjunto *B* é **bijetora** quando é, ao mesmo tempo, injetora (quando elementos distintos do domínio de *A* têm imagens distintas em *B*) e sobrejetora (quando cada elemento de *B* está associado a pelo menos um elemento de *A*, pela função).


Maarten Uilenbroek / SXC

Diante do que explicamos, surgem algumas perguntas:

- Será que esse sistema de envio de mensagens é seguro? Como veremos, isso vai depender muito da escolha das chaves usadas.

- Quantas chaves diferentes podemos ter à disposição para codificar mensagens usando o nosso alfabeto de 26 letras? Veremos que a resposta a essa pergunta pode ser dada com métodos de contagem.

4. As chaves usadas no método RSA


Sergio Ianni / SXC

Entendido o funcionamento de chaves públicas para enviar mensagens, vejamos como a Criptografia RSA se relaciona com esse procedimento.

Qualquer função bijetora **C** serve para codificar mensagens. Entretanto, se for fácil obter a função inversa **D** a partir de **C**, será também fácil "quebrar o código", o que torna o sistema frágil.


Sergio Ianni / SXC

O que o método RSA faz é fornecer uma maneira de obter as funções **C** e **D**, de modo que esse processo seja bastante seguro e dificulte a quebra de sigilo da mensagem.

Vejamos como o sistema RSA funciona por meio de um exemplo simples:

4.1. Exemplo de codificação com funções invertíveis

Simplificadamente, codificaremos mensagens com palavras que usam as nove letras mais frequentes do nosso idioma: A, E, O, S, R, I, N, D, M.

Como uma pré-codificação, associamos cada letra a um número:

Tabela 1

A	E	O	S	R	I	N	D	M
1	2	3	4	5	6	7	8	9

A seguir, vamos montar funções bijetoras **C** e **D**, uma inversa da outra. Isso será feito de acordo com regras de criptografia do sistema RSA.

Para este fim, tomemos como exemplo as seguintes funções bijetoras

$$\begin{array}{rccc} \mathbf{C}\colon & \{1,2,3,4,5,6,7,8,9\} & \to & \{1,2,3,4,5,6,7,8,9\} \\ & n & \mapsto & \mathbf{C}(n) \end{array}$$

em que $\mathbf{C}(n)$ é definida pela tabela:

Tabela 2

As 9 letras mais usadas em Português	A	E	O	S	R	I	N	D	M
Número n associado à letra	1	2	3	4	5	6	7	8	9
Número $\mathbf{C}(n)$ correspondente à letra codificada	1	8	7	4	5	6	3	2	9

Vamos definir a função **D** como:

$$\begin{array}{rccc} \mathbf{D}\colon & \{1,2,3,4,5,6,7,8,9\} & \to & \{1,2,3,4,5,6,7,8,9\} \\ & n & \mapsto & \mathbf{D}(n) \end{array}$$

em que o número $\mathbf{D}(n)$ está definido por:

Tabela 3

As 9 letras mais usadas em Português	A	E	O	S	R	I	N	D	M
Número n associado à letra	1	2	3	4	5	6	7	8	9
Número $\mathbf{D}(n)$ correspondente à letra decodificada	1	8	7	4	5	6	3	2	9

Constate nas funções acima que **C(D(M))** = **D(C(M))** = **M**, para qualquer mensagem **M**, comprovando que as funções **C** e **D** são uma a inversa da outra.

Atenção

Na verdade as funções **C** e **D** de nosso exemplo são iguais, mas isto é apenas uma coincidência. Em sistemas com alto grau de segurança é praticamente impossível estabelecer uma correlação prática entre tais funções.

Agora que já temos as funções **C** e **D**, vejamos como codificar e decodificar uma palavra. Vamos codificar a palavra **M** = **SOMANDO**, usando as chaves do nosso exemplo.

Devido à pré-codificação (vide Tabela 1), a cada letra da palavra associamos um número:

S-O-M-A-N-D-O $\longrightarrow$ torna-se $\longrightarrow$ M = 4-3-9-1-7-8-3

Apliquemos a função C a cada um desses números, obtendo, de acordo com a Tabela 2, o resultado:

$C(M) = C(4) - C(3) - C(9) - C(1) - C(7) - C(8) - C(3) =$

$4 - 7 - 9 - 1 - 3 - 2 - 7$

Para decifrar essa palavra, a pessoa que a recebe procede de modo análogo, usando a função D para decodificá-la:

Aplica-se a função decodificadora D (vide Tabela 3):

$D(C(M)) = D(4) - D(7) - D(9) - D(1) - D(3) - D(2) - D(7)$

$= 4 - 3 - 9 - 1 - 7 - 8 - 3.$

Esses números, quando trocado por letras (Tabela 1), revelam a palavra original que foi enviada:

$D(C(M)) = M =$ SOMANDO.

A maneira que escolhemos as funções **C** e **D** foi baseada no método RSA, que por sua vez usa a Teoria dos Números para criar essas funções.

Atenção

Nossa intenção aqui nesta etapa não é estudar como descrever essas funções, pois isso requer uma teoria bem sofisticada. Apenas queremos ressaltar que o método RSA é pensado de tal forma que fica muito difícil encontrar a função **D**, mesmo conhecendo-se a função **C**. Maiores detalhes sobre esse método podem ser encontrados no livro *Números inteiros e Criptografia RSA* de Severino Collier, ou no *site*: http://www.obmep.org.br/export/sites/default/arquivos/apostilas_pic2008/Apostila7-Criptografia.pdf.

5. Cada chave, uma função... mas quantas?

Como vimos, as chaves são fundamentais para que se possa cifrar e decifrar mensagens no sistema RSA. Essas chaves são funções de um subconjunto finito dos números naturais em outro subconjunto finito dos números naturais.

Como precisamos que o processo de codificação seja desfeito pela decifração, precisamos trabalhar com funções invertíveis, ou seja, com funções bijetoras entre conjuntos numéricos finitos.

Uma pergunta natural que aparece nesse contexto é: no caso de codificações de mensagens, quantas chaves diferentes podemos fabricar?

Ou ainda, dados dois conjuntos finitos de números naturais, quantas funções bijetoras existem entre esses conjuntos?

Adam Ciesielski / SXC

Vamos responder a essas perguntas ao longo desta etapa e, ao conhecer as respostas, você vai perceber que é possível fazer um curso completo de Análise Combinatória, apenas contando o número de determinadas classes de funções entre conjuntos finitos.

5.1. Contagem de funções quaisquer entre conjuntos finitos

Primeiramente, comecemos contando quantas funções existem entre dois conjuntos finitos quaisquer.

Se A e B são conjuntos finitos e f é uma função definida em A com valores em B. Lembremos que cada elemento do conjunto A deve estar associado a um único elemento do conjunto B.

Atividade 1

a ▹ Quantas funções $f: A \to B$ e tem do conjunto $A=\{a_1,a_2,a_3\}$ no conjunto $B=\{b_1,b_2\}$?

b ▹ Quantas funções $f: B \to A$ existem do conjunto $B=\{b_1,b_2\}$ no conjunto $A=\{a_1,a_2,a_3\}$?

Resposta Comentada

Como estamos trabalhando com conjuntos que possuem poucos elementos, podemos enumerar efetivamente todas as possibilidades:

- No item (a), podemos construir as seguintes funções:

$a_1 \mapsto b_1$ $a_2 \mapsto b_1$ $a_3 \mapsto b_1$	$a_1 \mapsto b_1$ $a_2 \mapsto b_1$ $a_3 \mapsto b_2$	$a_1 \mapsto b_1$ $a_2 \mapsto b_2$ $a_3 \mapsto b_1$	$a_1 \mapsto b_2$ $a_2 \mapsto b_1$ $a_3 \mapsto b_1$	$a_1 \mapsto b_1$ $a_2 \mapsto b_2$ $a_3 \mapsto b_2$	$a_1 \mapsto b_2$ $a_2 \mapsto b_1$ $a_3 \mapsto b_2$	$a_1 \mapsto b_2$ $a_2 \mapsto b_2$ $a_3 \mapsto b_1$	$a_1 \mapsto b_2$ $a_2 \mapsto b_2$ $a_3 \mapsto b_2$

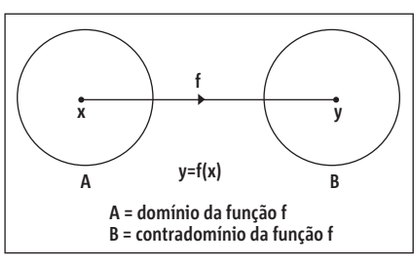
No total são $2^3 = 8$ funções diferentes.

- No item (b), podemos construir as seguintes funções:

$b_1 \mapsto a_1$ $b_2 \mapsto a_1$	$b_1 \mapsto a_1$ $b_2 \mapsto a_2$	$b_1 \mapsto a_1$ $b_2 \mapsto a_3$	$b_1 \mapsto a_2$ $b_2 \mapsto a_2$	$b_1 \mapsto a_2$ $b_2 \mapsto a_1$	$b_1 \mapsto a_2$ $b_2 \mapsto a_3$	$b_1 \mapsto a_3$ $b_2 \mapsto a_3$	$b_1 \mapsto a_3$ $b_2 \mapsto a_1$	$b_1 \mapsto a_3$ $b_2 \mapsto a_2$

No total são $3^2 = 9$ funções diferentes.

A atividade anterior nos fornece um indício de como contar quaisquer tipos de funções entre dois conjuntos finitos. Vamos agora estudar o caso geral.



▹ **Caso geral**: Se o conjunto *A* tem *n* elementos e o conjunto *B* tem *k* elementos, quantas funções existem de *A* em *B*?

Ora, ao primeiro elemento do domínio A, podemos associar qualquer um dos elementos de B. Como B tem k elementos, essa primeira decisão admite k possibilidades. Ao segundo elemento do domínio, também podemos associar qualquer um dos k elementos de B, pois podemos repetir a escolha já realizada de um elemento da imagem. Assim, na segunda decisão também temos k possibilidades. Continuando dessa maneira, após a n-ésima decisão, teremos contado todas as funções de A em B.

Pelo Princípio Multiplicativo, existem:

$\underbrace{k.\ k.\ \ldots\ .\ k}_{n \text{ vezes}} = k^n$ funções de A em B.

Outra maneira de responder a essa pergunta é utilizando o esquema abaixo:

Vamos representar os conjuntos A e B na forma $A=\{a_1, a_2,\ldots, a_n\}$ e $B=\{b_1, b_2,\ldots, b_k\}$.

a_1	a_2	...	a_n
Escrever o número de opções de elementos de B que podem ser associados ao elemento a_1	Escrever o número de opções de elementos de B que podem ser associados ao elemento a_2 (nesse caso é possível que um elemento associado a a_1 possa, em outra possibilidade, ser também associado a a_2)	...	Escrever o número de opões de elementos de B que podem ser associados ao elemento a_3 (nesse caso é possível que um elemento associado a a_1 ou a $a_2,\ldots,a_{n-1}$ possa, em outra possibilidade, ser também associado a a_n)
k	k	...	k

Nesse caso, pode haver repetições, pois um elemento associado ao elemento a_1 pode, em outra possibilidade, ser associado também ao elemento a_2, ao elemento a_3, ..., ao elemento a_n. Note que isso não contraria a definição de função.

Pelo Princípio Fundamental da Contagem, existem:

$\underbrace{k.\ k.\ \ldots\ .\ k}_{n \text{ vezes}} = k^n$ funções do conjunto A no conjunto B.

Atividade 2

Focalizando na ideia de contar funções, e não fazendo uma mera aplicação de fórmulas, resolva os dois problemas a seguir. Fazer diagramas e desenhos ajuda muito a resolver esse tipo de questão.

Adrian Gtz / SXC

Sanja Gjenero / SXC

a ▸ De quantas maneiras distintas podemos colocar 7 cartas em 5 caixas de coleta do correio?

b ▸ Jorge tem 4 camisas para serem guardadas em 6 gavetas de seu guarda-roupa. De quantas maneiras ele pode guardar essas camisas?

Resposta comentada

a ▸ Para simplificar, vamos representar o conjunto de cartas por:

$A=\{a_1, a_2, ..., a_7\}$ e o conjunto de caixas do correio por $B=\{b_1, b_2, b_3\}$. Seguiremos os passos anteriores:

a_1	a_2	...	a_7
Escrever o número de caixas do correio que podem receber a carta a_1.	Escrever o número caixas do correio que podem receber a carta a_2. Nesse caso, é possível que uma caixa que tenha recebido a carta a_1 possa, em outra possibilidade, também receber a carta a_2.	...	Escrever o número caixas do correio que podem receber a carta a_7. Nesse caso, é possível que uma caixa que tenha recebido a carta a_1, ou a carta a_2, ..., ou a carta a_6, possa, em outra possibilidade, também receber a carta a_7.
3	3	...	3

Nesse caso, pode haver repetições, pois uma caixa que recebe a carta a_1 pode, em outra possibilidade, receber a carta a_2, receber a carta a_3, ..., e receber a carta a_7.

Pelo Princípio Multiplicativo, existem $\underbrace{3.3.3....3}_{7 \text{ vezes}} = 3^7 = 2187$ maneiras de colocar 7 cartas em três caixas distintas do correio.

A situação pode ser vista do seguinte modo: tenho três cartas em minhas mãos e coloquei-as em uma determinada ordem. Seleciono a primeira delas e decido em qual caixa de correio vou colocá-la (7 possibilidades). A seguir, seleciono a segunda carta e procedo da mesma forma. Existem 7 possibilidades, pois uma mesma caixa de coleta pode receber mais de uma carta. Finalmente, repito o procedimento com a última carta (outras 7 possibilidades). É cabível que as três cartas ocupem a mesma caixa e que as outras duas fiquem vazias. No total, há 7.7.7 = 2187 possibilidades.

b ▹ Para simplificar, vamos representar o conjunto de camisas por:

$C=\{c_1, c_2, c_3, c_4\}$ e o conjunto de gavetas do guarda-roupa por $G=\{g_1, g_2, ..., g_6\}$. Seguiremos os passos anteriores:

c_1	c_2	...	c_4
Escrever o número de gavetas em que podemos guardar a camisa c_1.	Escrever o número de gavetas em que podemos guardar a camisa c_2. Nesse caso, é possível que uma gaveta em que se guardou a camisa c_1 possa, em outra possibilidade, também ser usada para guardar a camisa c_2.	...	Escrever o número gavetas em que podemos guardar a camisa c_4. Nesse caso, é possível que uma gaveta na qual tenha sido guardada a camisa c_1, ou a camisa c_2, ou a camisa c_3 possa, em outra possibilidade, ser usada para guardar a camisa c_4.
6	6	...	6

Nesse caso, pode haver repetições, pois uma gaveta na qual guardamos a camisa c_1 pode, em outra possibilidade, ser usada para guardar a camisa c_2, guardar a camisa c_3 ou, ainda, para guardar a camisa c_4.

Pelo Princípio Multiplicativo, existem $6.6.6.6 = 6^4 = 1.296$ maneiras diferentes de guardar 4 camisas em 6 gavetas.

Agora que já temos uma noção do que é a contagem de funções, passemos a contar o número de certos tipos de funções especiais entre dois conjuntos.

5.2. Contando funções bijetoras entre conjuntos finitos

Na seção anterior, contamos o número total de funções entre dois conjuntos finitos com quaisquer números de elementos. Mas, agora, queremos contar funções bijetoras. Como vimos, essas funções podem ser usadas em codificações de mensagens e são muito importantes.

No caso de funções bijetoras, lembre-se que o domínio e o contradomínio devem ter o mesmo número de elementos.

Assim, quantas funções bijetoras existem entre dois conjuntos *A* e *B*?

Adam Ciesielski / SXC

Atividade 3

a ▹ Conte quantas funções bijetoras $f: A \to B$ existem do conjunto $A = \{a_1, a_2\}$ no conjunto $B = \{b_1, b_2\}$.

b ▹ Conte quantas funções bijetoras $f: B \to A$ existem do conjunto $A = \{a_1, a_2, a_3\}$ no conjunto $B = \{b_1, b_2, b_3\}$.

Resposta comentada

Proceda como antes, listando as funções e não se esquecendo que numa bijeção *f* entre dois conjuntos *A* e *B* não sobram elementos em *B* que não estejam associados a algum elemento de *A*. Além disso, cada elemento de *B* fica associado a apenas um elemento de *A*.

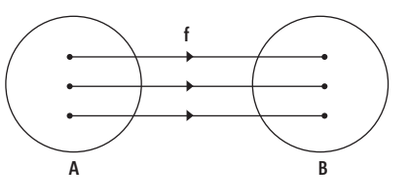
Assim, no item (a), temos apenas duas possibilidades de funções:

$a_1 \mapsto b_1$ $a_2 \mapsto b_2$	$a_1 \mapsto b_2$ $a_2 \mapsto b_1$

Já no item (b), temos seis possibilidades de funções:

$a_1 \mapsto b_1$ $a_2 \mapsto b_2$ $a_3 \mapsto b_3$	$a_1 \mapsto b_2$ $a_2 \mapsto b_1$ $a_3 \mapsto b_3$	$a_1 \mapsto b_1$ $a_2 \mapsto b_3$ $a_3 \mapsto b_2$	$a_1 \mapsto b_3$ $a_2 \mapsto b_1$ $a_3 \mapsto b_2$	$a_1 \mapsto b_2$ $a_2 \mapsto b_3$ $a_3 \mapsto b_1$	$a_1 \mapsto b_3$ $a_2 \mapsto b_2$ $a_3 \mapsto b_1$

Após essa atividade, podemos responder o caso geral de contagem de funções bijetoras.



Caso geral: Se *A* tem n elementos e *B* também tem n elementos, quantas funções bijetoras existem de *A* em *B*?

Ao primeiro elemento do domínio *A*, podemos associar qualquer um dos n elementos de *B*. Feito isto, a escolha para a imagem do segundo elemento de *A* só pode ser feita de $n-1$ maneiras diferentes, já que todo elemento de *B* é associado apenas a um elemento de *A* e a escolha da imagem do primeiro elemento já foi feita. O terceiro elemento de *A* só pode ser associado a um dos $n-2$ elementos restantes de *B* e assim sucessivamente, até o último elemento de *A*.

Quando alcançarmos o último elemento de A, só resta uma última opção entre os elementos de B, já que A e B têm o mesmo número de elementos. Esses procedimentos podem ser resumidos na tabela a seguir:

a_1	a_2	a_3	...	a_n
Escrever o número de opções dos elementos de B que podem ser associados ao elemento a_1	Escrever o número restante de opções dos elementos de B que, após associarmos um elemento a a_1, podem ser associados ao elemento a_2	Escrever o número restante de opções dos elementos de B que, após associarmos um elemento a a_1 e outro a a_2, podem ser associados ao elemento a_3	....	Escrever o número restante de opções dos elementos de B que, após associarmos um elemento a a_1, outro a a_2, outro a a_3, ..., outro a a_{n-1} podem ser associados ao elemento a_n
n elementos	$n-1= n-(2-1)$ elementos	$n-2 = n-(3-1)$ elementos	...	$1= n-(n-1)$

Como não há repetições, ao associarmos um elemento a outro, esse elemento não pode mais ser associado a nenhum dos demais.

Pelo Princípio Multiplicativo, há

$$P(n) = n.(n-1).(n-2)...3.2.1 = n!$$

funções bijetoras entre dois conjuntos com n elementos.

Observe que esse é o número de permutações, sem repetição, de um conjunto com n elementos! Esse fato simplesmente nos diz que uma função bijetora entre conjuntos finitos nada mais faz do que permutar os elementos do conjunto imagem.

É importante ressaltar que existem vários problemas que podem ter apresentações diferentes, mas com soluções absolutamente iguais, que recaem simplesmente em contar o número de funções bijetoras entre conjuntos.

Atividade 4

Resolva os problemas abaixo, utilizando duas abordagens: primeiro, a ideia de permutação e, depois, a ideia de contagem de funções.

a ▸ De quantos modos 7 pessoas podem sentar em uma fila de 7 cadeiras?

b ▸ Em uma festa, com 10 homens e 10 mulheres, de quantas maneiras podemos formar dez casais distintos de um homem e uma mulher?

Resposta comentada

a ▸ Primeira abordagem: contar como 7 pessoas sentarão em 7 cadeiras é o mesmo que saber de quantas maneiras podemos permutar essas pessoas quando sentadas. O problema, portanto, reduz-se a contar o número de permutações de um conjunto com 7 elementos, cuja resposta, como já sabemos, é 7!.
Segunda abordagem: chamemos o conjunto de pessoas de $P=\{p_1, p_2, p_3, p_4, p_5 p_6, p_7\}$ e o conjunto de cadeiras de $C=\{c_1, c_2, c_3, c_4, c_5 c_6, c_7\}$. Associando cada pessoa à cadeira em que ela se sentará, produzimos

uma função entre os conjuntos ***P*** e ***C***. Como duas pessoas distintas irão sentar em cadeiras distintas e como nenhuma cadeira sobrará sem que uma pessoa esteja sentada nela, essa função deve ser bijetora. Mudando a posição das pessoas sentadas, mudamos a função bijetora, e vice-versa. Daí, saber de quantas maneiras sete pessoas se sentarão em sete cadeiras é contar o número de funções bijetoras entre os conjuntos ***P*** e ***C***. Vimos anteriormente que este número é 7!.

b ▸ Proceda como no item (a), associando agora homens com mulheres.

A resposta é 10!

5.3. Contando funções injetoras entre conjuntos finitos *f: A → B*

Lembremos que, em uma função injetora, elementos distintos do conjunto *A* são levados em imagens distintas no conjunto *B*. Devido a esse fato, se os conjuntos *A* e *B* forem finitos, o número de elementos de *A* não pode exceder o número de elementos de *B*. Ou seja, o número de elementos de *A* é menor do que ou igual ao número de elementos de *B*.

Assim, quantas funções injetoras existem entre dois conjuntos *A* e *B*?

Adam Cieslski / SXC

Atividade 5

Utilizando seus conhecimentos de contagem de funções adquiridos até aqui e a definição de função injetora, responda às questões a seguir:

a ▸ Quantas funções injetoras $f: A \rightarrow B$ existem do conjunto $A=\{a_1, a_2\}$ no conjunto $B=\{b_1, b_2, b_3\}$?

b ▸ Quantas funções $f: C \rightarrow D$ existem do conjunto $C = \{c_1, c_2\}$ no $D=\{d_1, d_2, d_3, d_4\}$?

Resposta comentada

Proceda novamente listando todas as funções injetoras e não se esqueça que em uma função injetora *f* entre dois conjuntos *A* e *B,* um elemento de *B*, quando está associado a um elemento de *A*, deve estar associado apenas àquele elemento. Lembre-se ainda que nas funções injetoras podem sobrar elementos no conjunto *B* que não estejam associados a qualquer elemento do conjunto *A*.

Item (a): Como estamos trabalhando com conjuntos que possuem poucos elementos, é possível descrever todas as funções:

$a_1 \mapsto b_1$ $a_2 \mapsto b_2$	$a_1 \mapsto b_2$ $a_2 \mapsto b_1$	$a_1 \mapsto b_1$ $a_2 \mapsto b_3$	$a_1 \mapsto b_3$ $a_2 \mapsto b_1$	$a_1 \mapsto b_2$ $a_2 \mapsto b_3$	$a_1 \mapsto b_3$ $a_2 \mapsto b_2$

Portanto, no item (a) teremos 6 possibilidades de funções.

A maneira mais eficaz de responder a essa resposta, todavia, é preenchendo a tabela a seguir:

a_1	a_2
Escrever o número de opções dos elementos de *B* que podem ser associados ao elemento a_1	Escrever o número restante de opções dos elementos de *B* que, após associarmos um elemento a a_1, podem ser associados ao elemento a_2
3 elementos	2 elementos

Pelo Princípio Multiplicativo, temos 3.2 = 6 funções.

Item (b): Seguiremos o mesmo procedimento do item (a):

$c_1 \mapsto d_1$ $c_2 \mapsto d_2$	$c_1 \mapsto d_1$ $c_2 \mapsto d_3$	$c_1 \mapsto d_1$ $c_2 \mapsto d_4$	$c_1 \mapsto d_2$ $c_2 \mapsto d_3$	$c_1 \mapsto d_2$ $c_2 \mapsto d_4$	$c_1 \mapsto d_3$ $c_2 \mapsto d_4$
$c_1 \mapsto d_2$ $c_2 \mapsto d_1$	$c_1 \mapsto d_3$ $c_2 \mapsto d_1$	$c_1 \mapsto d_4$ $c_2 \mapsto d_1$	$c_1 \mapsto d_3$ $c_2 \mapsto d_2$	$c_1 \mapsto d_4$ $c_2 \mapsto d_2$	$c_1 \mapsto d_4$ $c_2 \mapsto d_3$

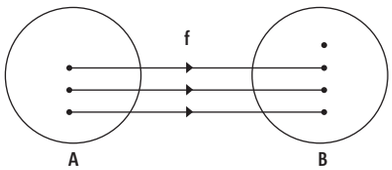
Portanto, no item (b) teremos 12 possibilidades de funções.

Ou, ainda, podemos usar tabelas, que funcionam no caso geral:

c_1	c_2
Escrever o número de opções dos elementos de *D* que podem ser associados ao elemento c_1	Escrever o número restante de opções dos elementos de *D* que, após associarmos um elemento a c_1, podem ser associados ao elemento c_2
4 elementos	3 elementos

Pelo Princípio Multiplicativo, teremos 4.3 = 12 funções.

Agora, passemos ao caso geral.



Caso Geral: Se *A* tem n elementos e *B* tem k elementos e $n \leq k$, quantas funções injetoras existem de *A* em *B*?

Vamos considerar os conjuntos $A = \{a_1, a_2..., a_n\}$ e $B = \{b_1, b_2..., b_k\}$, em que $n \leq k$.

a_1	a_2	a_3	...	a_n
Escrever o número de opções dos elementos de *B* que podem ser associados ao elemento a_1.	Escrever o número restante de opções dos elementos de *B* que, após associarmos um elemento a a_1, podem ser associados ao elemento a_2.	Escrever o número restante de opções dos elementos de *B* que, após associarmos um elemento a a_1 e outro a a_2, podem ser associados ao elemento a_3.	....	Escrever o número restante de opções dos elementos de *B* que, após associarmos um elemento a a_1, outro a a_2, outro a a_3, ..., outro a a_{n-1} podem ser associados ao elemento a_n.
k elementos	*k-1=k-(2-1)* elementos	*k-2=k-(3-1)* elementos	...	*k-(n-1)*

Como não há repetições, ao associarmos um elemento de *A* a um elemento de *B*, esse elemento de *B* não pode mais ser associado a nenhum dos demais.

Pelo Princípio Multiplicativo, há $A_k^n = \dfrac{k!}{(k-n)!} = k.(k-1).(k-2)...(k-(n-1))$

funções injetoras entre um conjunto com n elementos noutro conjunto com k elementos, em que $n \leq k$.

Observe que esse é o número de **arranjos** de n elementos, tomados em um conjunto de k elementos, sem repetições.

Atividade 6

Mais uma vez, ressaltamos: há também vários problemas que podem ter apresentações diferentes, mas com a mesma solução, que recai simplesmente em contar o número de funções injetoras entre conjuntos. Resolva dois deles a seguir, associando sua resolução à contagem de funções injetoras.


Michal Zacharzewski / SXC

a ▸ De quantas maneiras podemos estacionar 4 carros em 7 garagens, se em cada garagem pode ficar apenas um carro?

b ▸ Compare o problema anterior com o problema de se colocar 4 cartas em 7 caixas de coleta do correio. Qual a diferença?

Resposta comentada

a ▸ Faça uma tabela como fizemos no caso geral. Nesse momento, as perguntas a serem feitas são: "Em quantas garagens podemos estacionar o primeiro carro?", "Em quantas garagens podemos estacionar o segundo carro?" e assim por diante. Lembre-se que uma garagem só pode ser ocupada por um carro, podendo ficar vazia.

A resposta será $A_7^4 = \frac{7!}{(7-4)!} = 7.6.5.4 = 840$.

b ▸ No problema dos carros que devem ser estacionados, uma garagem só pode ser ocupada por um carro ou ficar vazia, o que não ocorre com as caixas do correio. No caso de cartas e caixas de coleta, mais de uma carta pode ser colocada em uma mesma caixa e caixas podem ficar vazias. Nesse caso, se procedêssemos como na Atividade 2a), encontraríamos $7^4 = 2401$ possibilidades, que é o número de funções entre o conjunto das cartas e das caixas de coleta, um com 4 elementos (cartas) e outro com 7 elementos (caixas de coleta). Observe que nesse caso, como esperado, o número de possibilidades é bem maior que no caso anterior. A possibilidade de repetição torna este item b) essencialmente diferente do item a).

A seguir, apresentaremos dois tipos de funções bem especiais, cuja contagem nos levará a resolver alguns problemas bem interessantes. Dessa vez, abordaremos outra característica das funções: o crescimento.

5.4. Contando funções que crescem

Dado um conjunto finito qualquer, podemos fixar uma ordem entre seus elementos e, neste caso, dizemos que o conjunto ficou ordenado. Um mesmo conjunto pode ter muitas ordens, mas, uma vez fixada uma delas, esta deve ser mantida durante toda a argumentação. Por exemplo, se A for o conjunto das cinco primeiras letras do alfabeto, o conjunto A pode ser representado, por exemplo, por $A=\{b,d,a,e,c\}$, ou por $A=\{c,a,e,d,b\}$. Vamos adotar uma ordem nos elementos desse conjunto e preservá-la. Na verdade, nesse caso, por conveniência, adotaremos a ordem mais natural: $A=\{a,b,c,d,e\}$ e vamos preservá-la. A partir desse momento, ao falarmos do conjunto A, teremos em mente que seus elementos têm a ordem que acabamos de estabelecer. É comum escrevermos $a<b$, $b<e$ etc. para informar, na ordem adotada, que um elemento vem antes do outro.

Quando um conjunto A é ordenado, podemos saber exatamente qual é o primeiro, o segundo, o terceiro, o quarto etc. elemento desse conjunto. Conjuntos finitos podem facilmente ser ordenados segundo uma ordem escolhida.

Vamos estudar agora as funções entre dois conjuntos ordenados que preservam a ordem desses conjuntos. Funções desse tipo são ditas **estritamente crescentes**.

Uma função $f: A \to B$ entre dois conjuntos ordenados A e B é **estritamente crescente** se $x < y$ acarretar que $f(x) < f(y)$, para todos $x, y \in A$.

Para que a noção de função estritamente crescente fique mais clara, acompanhe os exemplos a seguir.

- Ordenando as letras pela ordem alfabética e os números pela ordem natural, as funções abaixo são crescentes:

$f: \{a, b, c, d\} \rightarrow \{1,2,3,4,5\}$

x	$f(x)$
a	1
b	2
c	4
d	5

$g: \{1,2,3,4\} \rightarrow \{a, b, c, d,e,f\}$

x	$g(x)$
1	a
2	c
3	e
4	f

$h: \{a, b, c, d\} \rightarrow \{1,2,3,4,5\}$

x	$h(x)$
a	1
b	3
c	4
d	5

Para nos ambientarmos com a contagem de funções crescentes entre dois conjuntos finitos, veremos mais um exemplo.
Qual será o conceito de Análise Combinatória que aparecerá ao entendermos estes exemplos?

Adam Ciesielski / SXC

- Vamos considerar novamente funções quaisquer do conjunto $A = \{1, 2, 3\}$ (com a ordem numérica natural) no conjunto $B = \{a, b, c, d\}$ (com a ordem alfabética).

Pelo que aprendemos na subseção 5.1, existe um total de $4^3 = 64$ funções de *A* em *B*. Mas, dentre essas funções, apenas 4 são estritamente crescentes. São elas:

$$\begin{array}{|l|}\hline 1 \mapsto a \\ 2 \mapsto b \\ 3 \mapsto c \\ \hline \end{array} \qquad \begin{array}{|l|}\hline 1 \mapsto a \\ 2 \mapsto b \\ 3 \mapsto d \\ \hline \end{array} \qquad \begin{array}{|l|}\hline 1 \mapsto a \\ 2 \mapsto c \\ 3 \mapsto d \\ \hline \end{array} \qquad \begin{array}{|l|}\hline 1 \mapsto b \\ 2 \mapsto c \\ 3 \mapsto d \\ \hline \end{array}$$

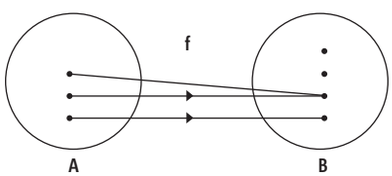
Como o domínio dessas funções é sempre o mesmo, elas podem ser caracterizadas pelos seus conjuntos imagens: {*a, b, c*}, {*a, b, d*}, {*a, c, d*} e {*b, c, d*}. Esse procedimento vai ser usado mais adiante.

Isso, a princípio, corresponde a escolher 3 dos quatro elementos do conjunto *B*, sem respeitar a ordem e sem repetir elementos, ou seja, escolher 3 elementos de um conjunto com 4 elementos.

Observe que após escolhermos esses elementos podemos ordená-los.

Como a ordem em *B* já está estabelecida, só existe uma maneira de ordenar uma determinada escolha de seus elementos, segundo essa ordem. Não importa se dentro de uma escolha os elementos são permutados. Quando eles forem ordenados, somente uma ordenação correta aparecerá. Deste modo, muitas escolhas desordenadas produzirão uma única ordenação correta.

Mas, no caso de nosso exemplo, isso é o mesmo que calcular a **combinação** simples de 4 elementos tomados 3 a 3. Portanto, teremos exatamente $C_4^3 = \frac{4!}{3!1!} = 4$ funções estritamente crescentes e o conceito de combinação simples aparece naturalmente na contagem desse tipo de função!



Caso geral: Se *A* é um conjunto ordenado com n elementos, *B* é um conjunto ordenado com k elementos e $n \leq k$, quantas funções estritamente crescentes existem de *A* em *B*?

Como visto anteriormente, é sempre verdadeiro que podemos identificar cada função estritamente crescente com seu conjunto imagem.

Logo, se *A* tem n elementos e *B* tem k elementos, com $n \leq k$, contar o número de funções estritamente crescentes entre os conjuntos *A* e *B* é a mesma coisa que contar de quantos modos podemos escolher n elementos de um conjunto com k elementos, sem que a ordem seja importante e sem repetições.

Sabemos que essa contagem é igual ao número de combinações de k elementos, tomados n a n sem repetição. Ou seja, é igual a:

$$C_k^n = \frac{k!}{n!(n-k)!}$$

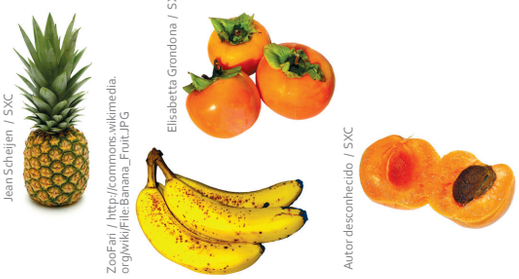
Portanto, contar o número de funções estritamente crescentes entre um conjunto ordenado *A* com n elementos e um conjunto ordenado *B* com k elementos $(n \leq k)$ é o mesmo que contar o número de combinações tomadas n a n de um conjunto com n elementos.

Atividade 7

Na Etapa 2, resolvemos os seguintes exercícios usando combinação:

Jade Gordon / SXC

a ▸ Um grupo de cinco professores comporá uma comissão para falar com o Secretário de Educação do Estado. Os cinco professores serão escolhidos dentre nove professores indicados por seus pares. Quantas comissões poderão ser formadas?



Jean Scheijen / SXC

Elisabetta Grondona / SXC

ZooFari / http://commons.wikimedia.org/wiki/File:Banana_Fruit.JPG

Autor desconhecido / SXC

Agora, resolva esse exercício usando a ideia de contar funções estritamente crescentes.

b ▸ Quantas saladas de frutas diferentes podemos fazer usando três das quatro frutas: abacaxi, banana, caqui e damasco?

Resolva usando a contagem de funções. Para isto, você deve ordenar o conjunto das frutas.

Resposta comentada

a ▸ Chamemos o conjunto dos professores de $P=\{p_1, p_2, \ldots, p_9\}$ e o conjunto dos professores escolhidos de $E=\{e_1, e_2, \ldots, e_5\}$. Escritos dessa forma, os conjuntos estão ordenados. O problema agora pode ser visto da seguinte forma: como contar o número de funções estritamente crescentes entre os conjuntos *E* e *P*?
A partir desse ponto, use a ideia de combinação para fazer essa contagem de funções e você verá que a resposta é 126. Note que, nesse caso, descrever todas essas funções é muito trabalhoso.

b ▸ Chamemos o conjunto de frutas de $F = \{a,b,c,d\}$ (*a* de abacaxi, *b* de banana, *c* de caqui e *d* de damasco) e o conjunto das frutas a serem escolhidas para a salada de $S = \{1,2,3\}$ (1 para a primeira escolha, 2 para a segunda e 3 para a terceira). Esses conjuntos agora estão ordenados. O problema agora pode ser visto da seguinte forma: como contar o número de funções estritamente crescente entre os conjuntos *S* e *F* ?

Como estamos trabalhando com conjuntos que possuem poucos elementos, use diagramas de setas e tabelas para fazer essa contagem e você verá que a resposta é 4. Note que esse número é o número de combinações de um conjunto de 4 elementos tomados 3 a 3.

6. Combinações com repetição e contagem de funções que nunca decrescem

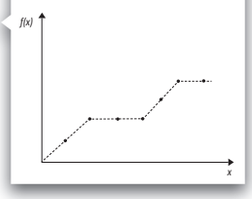
A seguir, vamos apresentar um fato muito interessante. Formularemos dois problemas distintos e veremos que é possível aplicar o mesmo procedimento para resolvê-los.

1. Como calcular a quantidade de maneiras de escolher 3 refrigerantes, se temos à nossa disposição 4 marcas diferentes? Nesse caso, podemos escolher mais de um refrigerante de uma mesma marca.

2. Como você calcularia a quantidade de soluções positivas ou nulas da equação $x_1 + x_2 + x_3 + x_4 = 3$? Uma solução para essa equação é uma quádrupla de números inteiros positivos ou nulos, ordenados da forma (x_1, x_2, x_3, x_4), cuja soma é igual a 3. A ordem dos números nessas soluções é importante. Por exemplo, $(1,0,2,0)$ é uma solução distinta da solução $(0,1,2,0)$.

Na seção anterior, contamos as funções que crescem sempre, chamadas funções estritamente crescentes. Nesta seção, contaremos funções que nunca diminuem, ou seja, as **funções não-decrescentes**.

Uma função $f: A \to B$ entre dois conjuntos ordenados A e B é **não-decrescente** se $x < y$ então $f(x) \leq f(y)$, para todos $x, y \in A$.



Os exemplos a seguir ajudam no entendimento do conceito de função não-decrescente.

Com as letras em ordem alfabética e os números na ordem natural, as funções abaixo são não-decrescentes:

$f: \{1,2,3,4\} \to \{a, b, c, d, e, f\}$

x	$g(x)$
1	a
2	c
3	c
4	f

$g: \{a, b, c, d\} \to \{1,2,3,4,5\}$

x	$f(x)$
a	1
b	2
c	3
d	5

$h: \{a, b, c, d\} \to \{1,2,3,4,5\}$

x	$h(x)$
a	2
b	2
c	5
d	5

A contagem desse tipo de função é bem mais delicada que as anteriores e merece uma explicação mais detalhada.

Comecemos com um exemplo simples.

Quantas funções não-decrescentes existem entre os conjuntos *A* = {*1, 2, 3*} e *B* = {*b1, b2, b3, b4*}, ordenados como se apresentam?

Adam Ciesielski / SXC

Neste caso, como estamos trabalhando com conjuntos que possuem pequenas quantidades de elementos, vamos descrever todas essas funções.

$1\mapsto b_1$ $2\mapsto b_1$ $3\mapsto b_1$	$1\mapsto b_1$ $2\mapsto b_1$ $3\mapsto b_2$	$1\mapsto b_1$ $2\mapsto b_1$ $3\mapsto b_3$	$1\mapsto b_1$ $2\mapsto b_1$ $3\mapsto b_4$	$1\mapsto b_1$ $2\mapsto b_2$ $3\mapsto b_2$	$1\mapsto b_1$ $2\mapsto b_2$ $3\mapsto b_3$	$1\mapsto b_1$ $2\mapsto b_2$ $3\mapsto b_4$	$1\mapsto b_1$ $2\mapsto b_3$ $3\mapsto b_3$	$1\mapsto b_1$ $2\mapsto b_3$ $3\mapsto b_4$	$1\mapsto b_1$ $2\mapsto b_4$ $3\mapsto b_4$
$1\mapsto b_2$ $2\mapsto b_2$ $3\mapsto b_2$	$1\mapsto b_2$ $2\mapsto b_2$ $3\mapsto b_3$	$1\mapsto b_2$ $2\mapsto b_2$ $3\mapsto b_4$	$1\mapsto b_2$ $2\mapsto b_3$ $3\mapsto b_3$	$1\mapsto b_2$ $2\mapsto b_3$ $3\mapsto b_4$	$1\mapsto b_2$ $2\mapsto b_4$ $3\mapsto b_4$	$1\mapsto b_3$ $2\mapsto b_3$ $3\mapsto b_3$	$1\mapsto b_3$ $2\mapsto b_3$ $3\mapsto b_4$	$1\mapsto b_3$ $2\mapsto b_4$ $3\mapsto b_4$	$1\mapsto b_4$ $2\mapsto b_4$ $3\mapsto b_4$

Temos, portanto, 20 funções não-decrescentes entre os conjuntos *A* e *B*. Como obter esse número sem fazer listagens?

6.1. As soluções de uma equação e a contagem de certas escolhas

Você seria capaz de relacionar a contagem de funções não-decrescentes com o número de soluções da equação $x_1 + x_2 + x_3 + x_4 = 3$? Vejamos como fazer isso.

Cada uma dessas funções é caracterizada pelas setas que chegam aos elementos do conjunto *B*. Por exemplo, a primeira função do exemplo anterior tem três setas que chegam ao elemento b_1 e nenhuma seta chega aos demais elementos de *B*. Já a segunda função da primeira linha tem duas setas chegando em b_1, uma seta chegando em b_2 e nenhuma seta chegando em b_3 ou em b_4, e assim sucessivamente.

Se denotarmos por x_i o número de setas que chegam a b_i, (i = 1,2,3,4), teremos associados os seguintes números às 20 funções descritas acima:

Observe que, em cada caso, a soma $x_1 + x_2 + x_3 + x_4$ é igual a 3.

$x_1 = 3$ $x_2 = 0$ $x_3 = 0$ $x_4 = 0$	$x_1 = 2$ $x_2 = 1$ $x_3 = 0$ $x_4 = 0$	$x_1 = 2$ $x_2 = 0$ $x_3 = 1$ $x_4 = 0$	$x_1 = 2$ $x_2 = 0$ $x_3 = 0$ $x_4 = 1$	$x_1 = 1$ $x_2 = 2$ $x_3 = 0$ $x_4 = 0$	$x_1 = 1$ $x_2 = 1$ $x_3 = 1$ $x_4 = 0$	$x_1 = 1$ $x_2 = 1$ $x_3 = 0$ $x_4 = 1$	$x_1 = 1$ $x_2 = 0$ $x_3 = 2$ $x_4 = 0$	$x_1 = 1$ $x_2 = 0$ $x_3 = 1$ $x_4 = 1$	$x_1 = 1$ $x_2 = 0$ $x_3 = 1$ $x_4 = 1$
$x_1 = 0$ $x_2 = 3$ $x_3 = 0$ $x_4 = 0$	$x_1 = 0$ $x_2 = 2$ $x_3 = 1$ $x_4 = 0$	$x_1 = 0$ $x_2 = 2$ $x_3 = 0$ $x_4 = 1$	$x_1 = 0$ $x_2 = 1$ $x_3 = 2$ $x_4 = 0$	$x_1 = 0$ $x_2 = 1$ $x_3 = 1$ $x_4 = 1$	$x_1 = 0$ $x_2 = 1$ $x_3 = 0$ $x_4 = 2$	$x_1 = 0$ $x_2 = 0$ $x_3 = 3$ $x_4 = 0$	$x_1 = 0$ $x_2 = 0$ $x_3 = 2$ $x_4 = 1$	$x_1 = 0$ $x_2 = 0$ $x_3 = 1$ $x_4 = 2$	$x_1 = 0$ $x_2 = 0$ $x_3 = 0$ $x_4 = 3$

Isto se deve ao fato de o domínio da função ter 3 elementos (pois cada função é caracterizada por 3 setas partindo dos elementos de seu domínio). Assim, contar quantas funções não-decrescentes há entre os conjuntos $A = \{1, 2, 3\}$ e $B = \{b_1, b_2, b_3, b_4\}$ é o mesmo que contar quantas são as soluções inteiras positivas ou nulas da equação $x_1 + x_2 + x_3 + x_4 = 3$, pois cada função produz uma solução da equação e cada solução permite definir uma única função não-decrescente.

Temos, portanto, 20 soluções positivas ou nulas para a equação $x_1 + x_2 + x_3 + x_4 = 3$.

O fato de que o número de soluções de uma equação e a contagem de funções não-decrescentes terem uma ligação tão estreita é surpreendente, não? Mas não é só isso.

Outro problema, também aparentemente distinto, pode ser resolvido com essas mesmas ideias: o número de escolhas que podemos fazer quando selecionamos n objetos de um conjunto de k objetos, sem que a ordem dos elementos seja relevante e podendo-se repetir a escolha de elementos (combinações com repetição).

Um problema desse tipo é o que aparece na primeira pergunta no início desta seção:

Quantas são as maneiras de se escolher 3 refrigerantes, se temos à nossa disposição 4 marcas diferentes?

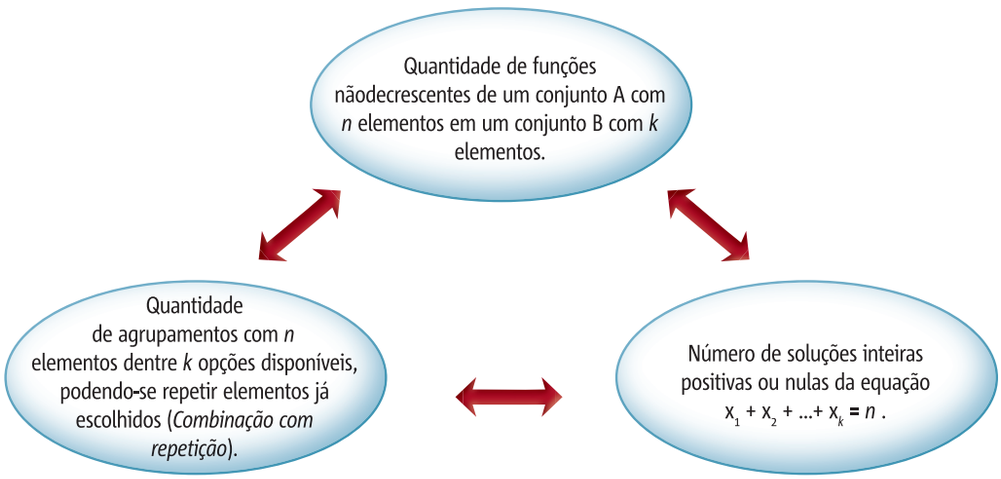
Adam Ciesielski / SXC

Note que alguém pode escolher mais de um refrigerante de uma mesma marca.

Um bom esquema da resposta seria:

Fazendo a identificação de ***b1*** com  , de ***b2*** com  , de ***b3*** com  e de ***b4*** com  , o problema de contagem das escolhas de refrigerantes com repetição é essencialmente o mesmo que o da contagem de funções não-decrescentes entre $\boldsymbol{A} = \{\boldsymbol{1, 2, 3}\}$ e $\boldsymbol{B} = \{\boldsymbol{b1, b2, b3, b4}\}$. Como já fizemos esses cálculos, temos 20 maneiras distintas para escolhermos os três refrigerantes e, assim, respondemos à pergunta.

Diante do que acabamos de ver, temos três problemas aparentemente bem distintos, que podem ser abordados por meio de uma mesma ideia:



Resolvendo um desses problemas, resolvemos todos eles.

Atividade 8

Vamos resolver mais um problema que pode ser solucionado através de uma das três maneiras anteriores.

No laboratório de Biologia da professora Regina, nasceram 6 ratinhos brancos idênticos. Para estudá-los, ela resolveu separá-los em dois grupos, colocando-os em duas gaiolas diferentes. De quantas maneiras diferentes isso pode ser feito?


Rob Owen-Wahl / SXC

Resposta comentada

A maneira mais natural de atacar esse problema é contar o número de ratinhos que podem participar de cada grupo.

Grupo 1	Grupo 2
1	5
2	4
3	3
4	2
5	1

Logo, teremos 5 maneiras de dividir os ratinhos. Porém, essa enumeração não levou em conta duas possibilidades:

1. a primeira gaiola fica vazia e a segunda com 6 ratinhos;
2. a segunda gaiola fica vazia e a primeira com 6 ratinhos.

Levando em conta essas possibilidades, o número de maneiras de dividir os ratinhos cresce para 7.

Uma maneira matemática de encarar esse problema é contar o número de soluções da equação $x_1 + x_2 = 6$. No caso 1), descrito antes, procuraríamos soluções positivas da equação; já no caso 2), nosso interesse incluiria, além das soluções positivas, a possibilidade de alguma das variáveis ser igual a zero. Como seria isso?

▹ **Primeira solução**:

Esse problema é tão simples que podemos enumerar todas as possibilidades. São elas:

x_1	x_2
1	5
2	4
3	3
4	2
5	1

Não consideramos aqui a possibilidade de um dos termos x_1 ou x_2 ser zero. Por isso, obtivemos somente 5 soluções. Se algum dos termos pudesse ser zero, obteríamos mais duas soluções $x_1 = 0$ e, $x_2 = 6$ e $x_1 = 6$ e, $x_2 = 0$.

Da forma que resolvemos o problema, dificilmente a enumeração de todas as soluções pode ser usada em casos mais gerais, em que apareça um número muito grande de elementos.

▹ **Segunda solução** (essa sim é a solução mais inteligente):

Vamos desenvolver uma abordagem mais inteligente para darmos uma outra solução ao problema. Essa abordagem utiliza nossos conhecimentos anteriores sobre combinações (sem repetições) e a solução vai poder ser usada no caso geral.

Vamos a ela!

Desenhamos seis barras para representar o número 6:

| | | | | | |

Com essa representação, as possibilidades para colocar o sinal "**+**" entre essas barras são:

+				
	+			
		+		
			+	
				+

Vamos agora extrair as informações dessa representação, encontrando as soluções numéricas da equação $x_1 + x_2 = 6$.

- **Primeira possibilidade:**

| + | | | | | corresponde à solução $x_1 = 1$ e $x_2 = 5$

Note que $x_1 = 1$ é o número de barras à esquerda do sinal +, e que $x_2 = 5$ é o número de barras à direita do sinal +.

- **Segunda possibilidade:**

| | + | | | | corresponde à solução $x_1 = 2$ e $x_2 = 4$.

- **Terceira possibilidade:**

| | | + | | | corresponde à solução $x_1 = 3$ e $x_2 = 3$.

- **Quarta possibilidade:**

| | | | + | | corresponde à solução $x_1 = 4$ e $x_2 = 2$.

- **Quinta possibilidade:**

| | | | | + | corresponde à solução $x_1 = 5$ e $x_2 = 1$.

Juntando essas possibilidades, encontramos todas as soluções inteiras positivas da equação.

Para usarmos a mesma ideia no caso geral, é importante observar que usamos apenas um sinal + para separar as barras em dois grupos, pois procuramos dois números x_1 e x_2 para solução da equação. Se estivéssemos procurando resolver a equação $x_1 + x_2 + \ldots + x_k = n$, com k números, usamos $k - 1$ sinais + para separar n barras. Por exemplo, se a equação envolvesse três números x_1, x_2 e x_3, usaríamos 2 sinais +, se a equação envolvesse quatro números, usaríamos 3 sinais +, e assim por diante.

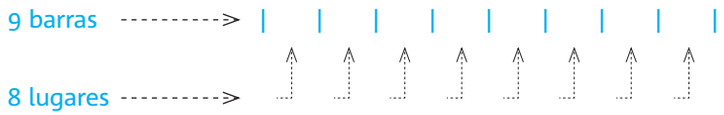
No caso anterior, como procuramos dois números x_1 e x_2, usamos apenas 2 – 1 = 1 sinal + e, como temos 6 barras, teremos 6 – 1 = 5 lugares disponíveis para colocar esse sinal. Ora, dentre os 5 lugares disponíveis, devemos escolher um deles para colocar o sinal +.

Logo, o problema recai em um problema de combinação simples: "De quantas maneiras podemos escolher um elemento de um conjunto com 5 elementos?" Como já sabemos, tal tarefa pode ser feita de $C_5^1 = 5$ maneiras diferentes.

Será que esta técnica também funciona em outros casos? Vejamos.

Quantas soluções positivas têm a equação $x_1 + x_2 + x_3 + x_4 + x_5 = 9$?

Vamos dispor nove barras:



Repetindo as ideias do caso anterior, como procuramos cinco números positivos x_1, x_2, x_3, x_4 e x_5, devemos usar 5 – 1 = 4 sinais + para colocarmos em 9 – 1 = 8 lugares entre as barras.

- **Uma possibilidade:**

Corresponde à solução $x_1 = 1$, $x_2 = 2$, $x_3 = 1$, $x_4 = 4$, $x_5 = 1$.

- **Outra possibilidade:**

Corresponde à solução $x_1 = 3$, $x_2 = 1$, $x_3 = 2$, $x_4 = 2$, $x_5 = 1$.

Note que há muitas outras possibilidades, o que torna muito trabalhoso listarmos todas elas.

Vamos pensar mais um pouco para darmos uma solução inteligente ao problema, que servirá para o caso geral:

- Temos 8 lugares para colocarmos 4 sinais de +, o que é o mesmo que escolher 4 lugares dentre 8 lugares, ou ainda escolhermos 4 elementos de um conjunto com 8 elementos.
- Já que os sinais de + são todos iguais, podemos fazer isso sem nos preocuparmos com a ordem desses sinais.
- Agora, é fácil ver que esse é um problema de combinação. Assim, o número total de soluções da equação é $C_8^4 = \frac{8!}{(8-4)!4!} = 70$

6.2. Resolvendo o caso geral

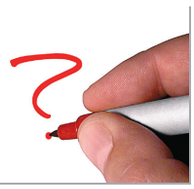
Pelo que acabamos de estudar, a solução do caso geral do problema anterior é:

Resultado Geral:

O número de soluções <u>positivas</u> da equação $x_1 + x_2 + \ldots + x_k = n$, $n \geq k$ é

$$C_{n-1}^{k-1} = \frac{(n-1)!}{(k-1)!(n-k)!}$$

Como resolver o mesmo problema anterior, agora considerando as possibilidades em que os números x_i's possam ser inteiros, positivos ou nulos?



Adam Ciesielski / SXC

- **Problema geral:** Qual é o número de soluções inteiras <u>positivas ou nulas</u> da equação $x_1 + x_2 + \ldots + x_k = n$?

- **Solução:** Façamos um pequeno truque, introduzindo a mudança $y_i = x_i + 1,\ i = 1, 2, 3, \ldots, k$. Recairemos, com isso, no caso anterior, o qual já resolvemos. Como $x_1 + x_2 + \ldots + x_k = n$, somando 1 a cada x_i, obteremos

$$(x_1 + 1) + (x_2 + 1) + \ldots + (x_k + 1) = x_1 + x_2 + \ldots + x_k + k = n + k,$$

ou seja,

$$y_1 + y_2 + \ldots + y_k = n + k.$$

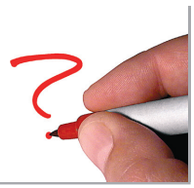
O número de soluções positivas da última equação é igual ao número de soluções positivas ou nulas de $x_1 + x_2 + \ldots + x_k = n$. Pelo resultado geral obtido anteriormente, esse número é C_{n+k-1}^{k-1}

Resultado Geral:

O número de soluções <u>positivas</u> ou <u>nulas</u> da equação $x_1 + x_2 + \ldots + x_k = n$ é

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

Agora tente responder: Qual o número de soluções positivas ou nulas da equação $x_1 + x_2 + x_3 + x_4 = 3$?


Adam Cieslelski / SXC

Diante do que já vimos, a resposta é:

$$C_{3+4-1}^{4-1} = C_6^3 = 20.$$

que é precisamente o número de funções não-decrescentes de um conjunto com $n = 3$ elementos em um conjunto com $k = 4$ elementos.

Nesse momento, é possível comparar essa solução com o número de escolhas de 3 refrigerantes dentre 4 disponíveis, você se lembra desse problema? As soluções são idênticas!

Atividade 9


Vangelis Thomaidis / SXC

Considere a seguinte pergunta: ***"Quantas são as maneiras de se escolher 2 calças, se temos a nossa disposição 3 marcas diferentes?"***

Dê uma resposta para essa pergunta:

a ▸ enumerando os casos;

b ▸ relacionando o problema com uma equação;

c ▸ contando o número de funções.

Resposta comentada

a ▸ Chame o conjunto das marcas das calças de *M*={*A,B,C*}. Basta agora contar os casos dessa escolha: *(A,A), (A,B), (A,C), (B,B), (B,C)* e *(C,C)*. Note que *(A,B)=(B,A), (A,C)=(C,A).*

- Resposta: 6 maneiras.

b ▸ Se o número de calças da marca *A* é x_1, o da marca *B* é x_2 e o da marca *C* é x_3, o problema pode ser resolvido contando-se o número de soluções inteiras positivas ou nulas da equação $x_1 + x_2 + x_3 = 2$. As soluções da equação são: $(2,0,0),(0,2,0),(0,0,2),(1,1,0),(1,0,1),(0,0,1)$.

- Resposta: 6 maneiras.

Compare ainda o resultado com a fórmula dada nesta seção, que conta o número de soluções positivas ou nulas dessa equação, no caso em que $k = 3$ e $n = 2$. A resposta é $C_{3+2-1}^{3-1} = C_4^2 = 6$ maneiras.

c ▸ Chame o conjunto das marcas das calças de *M* = {*A, B, C*} e o conjunto das calças de *K*={c_1, c_2} (ou seja, c_1 é a calça escolhida em primeiro lugar e c_2 a escolhida em segundo lugar) e os ordenemos conforme essa descrição. O problema reduz-se a contar o número de funções não-decrescentes entre *K* e *M*. Enumeremos essas funções por seus pares ordenados:

{(c_1, *A*), (c_2, *A*)},
{(c_1, *A*), (c_2, *B*)},
{(c_1, *A*), (c_2, *C*)},
{(c_1, *B*), (c_2, *B*)},
{(c_1, *B*), (c_2, *C*)} e
{(c_1, *C*), (c_2, *C*)}.

- Resposta: 6 funções não-decrescentes entre *K* e *M*.

6.3. Três aplicações interessantes do caso geral

A) O PROBLEMA DO PARQUE DE DIVERSÕES


Lars Reinholt / SXC

Um menino está em um parque de diversões e resolve comprar dois bilhetes. No parque há 4 tipos de brinquedos:

C – chapéu mexicano
F – trem fantasma
M – montanha russa
R – roda gigante

O menino pode comprar dois bilhetes do mesmo tipo, se ele quiser utilizar o mesmo brinquedo duas vezes. Nessas condições, qual é o número total de possibilidades de compra dos bilhetes?

▹ **Primeira solução:**

É possível resolver esse problema simples enumerando todas as possibilidades. São elas: **CC CF CM CR FF FM FR MM MR RR**.

Observe que aí estão listadas todas as possibilidades e que CF é igual a FC, não importando a ordem do primeiro e do segundo bilhete, mas incluindo repetições. Se não fossem permitidas repetições, o resultado seria $C_4^2 = 6$. Entretanto, nesse cálculo não se incluiu a hipótese de o menino comprar dois bilhetes repetidos e, como listamos, o número correto de possibilidades é 10 = 6 + 4 (quatro repetições foram adicionadas).

▹ **Segunda solução:**

Esta é uma resolução sem que listemos as possibilidades. Sejam:
$x_1 =$ o número de bilhetes de **C – chapéu mexicano**
$x_2 =$ o número de bilhetes de **F – trem fantasma**
$x_3 =$ o número de bilhetes de **M – montanha russa**
$x_4 =$ o número de bilhetes de **R – roda gigante**

Como o número total de bilhetes que o menino quer comprar é 2, temos $x_1 + x_2 + x_3 + x_4 = 2$. Note que, como ele pode escolher o mesmo brinquedo duas vezes, devemos considerar a possibilidade de alguns dos números x_1, x_2, x_3, x_4 serem nulos.

Dessa forma, recaímos no problema geral, já estudado, de contar o número de soluções positivas ou nulas de uma equação. Logo, devemos encontrar o número de soluções inteiras e não-negativas da equação $x_1 + x_2 + x_3 + x_4 = 2$. Mas, pelo o que vimos acima, este número é precisamente $C_{4+2-1}^{4-1} = C_5^3 = 10$, como já esperávamos.

Observe como foi importante anteriormente resolvermos um problema um pouco mais teórico. Basta comparar agora as duas soluções apresentadas e observar que este segundo método de resolução pode ser generalizado, enquanto que a simples listagem pode tornar um problema praticamente impossível de ser resolvido, se o número de possibilidades for grande.

B) O PROBLEMA DO MENINO GULOSO


Lotus Head / SXC

Um menino muito guloso encontra-se no balcão de uma sorveteria que vende 7 opções diferentes de sabores. Ele tem dinheiro para comprar 4 sorvetes e pode escolher sabores repetidos. Nessas condições, quantos pedidos diferentes ele pode fazer?

Não basta apenas calcularmos o número de combinações de 7 sabores tomados 4 a 4, pois o menino pode repetir os sabores. Usando a mesma técnica usada no problema anterior, considere:

x_1 = o número de solicitações de sorvetes do **1º sabor**;
x_2 = o número de solicitações de sorvetes do **2º sabor**;
x_3 = o número de solicitações de sorvetes do **3º sabor**;
x_4 = o número de solicitações de sorvetes do **4º sabor**;
x_5 = o número de solicitações de sorvetes do **5º sabor**;
x_6 = o número de solicitações de sorvetes do **6º sabor**; e
x_7 = o número de solicitações de sorvetes do **7º sabor**.

$\Rightarrow x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 = 4$

O número de soluções positivas ou nulas desta última equação é:

$$C_{7+4-1}^{7-1} = C_{10}^{6} = 210.$$

Se, em cada dia, ele escolher uma combinação diferente de sabores, demorará 210 dias para saborear todas as combinações possíveis. Note que se ele não repetisse sabores, demoraria apenas $C_7^4 = 35$ dias para saborear todas as combinações sem repeti-las!

C) A PINTURA DOS VASOS


John Boyer / SXC

Banjo Ari / SXC

Com 2 cores diferentes, de quantas maneiras distintas podemos pintar 3 vasos, pintando cada vaso de uma única cor? E como seria resolver o mesmo problema com 4 cores e 5 vasos?

Observe que mais de um vaso pode ser pintado de uma mesma cor. Estamos novamente com um problema de combinações com repetição. Digamos que uma tinta seja da cor verde e a outra da cor vermelha.

Se x_1 é o número de vasos pintados na cor vermelha e x_2 é o número de vasos pintados de verde, então $x_1 + x_2 = 3$. O número de soluções positivas ou nulas dessa equação é $C_{3+2-1}^{2-1} = C_4^1 = 4$.

No caso de 4 cores e 5 vasos, o número de combinações possíveis é igual ao número de soluções positivas ou nulas da equação $x_1 + x_2 + x_3 + x_4 = 5$, que é dado por $C_{4+5-1}^{4-1} = C_8^3 = 56$.

Esses exemplos mostram a aplicabilidade das combinações com repetição e ilustram, mais uma vez, como uma mesma ideia matemática pode ser abordada de várias maneiras. Dessa forma, pudemos analisar melhor a contagem do número de combinações com repetição, que é um assunto pouco abordado em sala de aula.

A seguir, você poderá fazer uma atividade que resume todo o conteúdo de Combinatória que estudamos nas Etapas 1, 2 e 3. Como a Etapa 4 abordará, principalmente, o conceito de Probabilidade, essa atividade também servirá como um bom fechamento de todo o estudo de Análise Combinatória feito até aqui em nossa disciplina.

Atividade 10

Nesta atividade final, preparamos um quadro-resumo dos vários tipos especiais de contagem que estudamos durante nossas primeiras três etapas. Sua tarefa é ajudar-nos a preenchê-lo, respondendo às perguntas em alguns quadros.

Obs.: Princípio Multiplicativo – Se uma decisão d_1 puder ser tomada de m maneiras e se, uma vez tomada a decisão d_1, outra decisão d_2 puder ser tomada de n maneiras diferentes, então o número total de se tomarem as decisões é o produto de m por n.

ANÁLISE COMBINATÓRIA – QUADRO-RESUMO

	Respeitando a ordem			
	Simples	**Fórmula**	**Com repetição**	**Fórmula**
Permutações	Ex.: De quantas maneiras diferentes podemos estacionar 6 carros em 6 garagens? **Resp.:**	O número de permutações de n elementos é: **Resp.:**	Ex.: Quantos são os anagramas de URUGUAI que começam com I? **Resp.:**	O número de permutações de n objetos, dos quais p_1 é igual a a_1, p_2 é igual a a_2, ..., p_k é igual a a_k é: **Resp.:**

continua...

Respeitando a ordem				
	Simples	Fórmula	Com repetição	Fórmula
Arranjos	Ex.: De quantas maneiras diferentes podemos estacionar 6 carros em 3 garagens? **Resp.:**	O número de arranjos simples de n elementos, tomados p a p é dado por: **Resp.:**	Ex.: Qual é o número de placas de carro com 3 letras e 4 dígitos, supondo que o alfabeto tenha 26 letras? **Resp.:**	O número de arranjos com repetição de n elementos, tomados p a p é: **Resp.:**
Quando a ordem não é importante				
	Simples	Fórmula	Com repetição	Fórmula
Combinações	Ex.: Quantas saladas de frutas (com frutas diferentes) podemos fazer utilizando 3 frutas se dispomos de 5 tipos diferentes de frutas? **Resp.:**	O número de combinações de n elementos, tomados p a p, é dado por: **Resp.:**	Ex.: De quantos modos diferentes podemos comprar 4 refrigerantes em um bar que vende 2 tipos de refrigerantes? **Resp.:**	O número de combinações com repetição de n elementos, tomados p a p é: **Resp.:**

Procure completar o quadro sem ver as soluções. Vale a pena tentar!

Resposta comentada

ANÁLISE COMBINATÓRIA – QUADRO-RESUMO

Respeitando a ordem				
	Simples	Fórmula	Com repetição	Fórmula
Permutações	Ex.: De quantas maneiras diferentes podemos estacionar 6 carros em 6 garagens? **Resp.: 6!**	O número de permutações de n elementos é $n! = n.(n-1).$ $(n-2)...3.2.1$	Ex.: Quantos são os anagramas de URUGUAI que começam com I? **Resp.: 120**	O número de permutações de n objetos, dos quais p_1 é igual a a_1, p_2 é igual a a_2, ..., p_k é igual a a_k é: $n/[p_1!\,p_2!\,p_3!...p_k!]$
Arranjos	Ex.: De quantas maneiras diferentes podemos estacionar 6 carros em 3 garagens? **Resp.: 6.5.4 = 120**	O número de arranjos simples de n elementos, tomados p a p é: $A_n^p = \frac{n!}{(n-p)!}$	Ex.: Qual é o número de placas de carro com 3 letras e 4 dígitos, supondo que o alfabeto tenha 26 letras? **Resp.: 26.26.26.10.10.10.10 = 175.760.000**	O número de arranjos com repetição de n elementos, tomados p a p é: n^p
Quando a ordem não é importante				
	Simples	Fórmula	Com repetição	Fórmula
Combinações	Ex.: Quantas saladas de frutas (com frutas diferentes) podemos fazer utilizando 3 frutas se dispomos de 5 tipos diferentes de frutas? **Resp.: 10**	O número de combinações de n elementos, tomados p a p, é dado por: $C_p^n = \frac{n!}{(n-p)!\,p!}$	Ex.: De quantos modos diferentes podemos comprar 4 refrigerantes em um bar que vende 2 tipos de refrigerantes? **Resp.: 5**	O número de combinações com repetição de n elementos, tomados p a p é: $C_{n+p-1}^{n-1} = \frac{(n+p-1)!}{(n-1)!\,p!}$

7. Conclusão

A Análise Combinatória envolve raciocínios presentes em vários conteúdos da Matemática. Nesta etapa, pudemos comprovar esse fato por meio da contagem de funções.

Contar funções ou contar escolhas? Dependendo do problema e do contexto, vimos que tanto faz optar por qualquer dessas contagens, o resultado será o mesmo. Essa opção depende de como alguém se sente mais seguro para enfrentar um problema.

Esperamos que, a partir dessas ideias, você explore mais as relações existentes entre a contagem de funções e a Análise Combinatória. Mais ainda, esperamos que você se divirta, identificando relações entre a Análise Combinatória e outros conteúdos matemáticos, e possa se beneficiar muito de tudo que foi estudado até agora.

8. Resumo

- Antigamente, os meios criptográficos utilizados para o envio de mensagens secretas eram baseados apenas em chaves secretas.
- O Sistema RSA trouxe uma grande inovação ao utilizar duas chaves: uma pública, usada para codificar, e outra secreta, usada para decodificar. A chave pública pode ser conhecida por qualquer pessoa, mas a secreta só é conhecida por aqueles que participam do processo de recepção da mensagem.
- A segurança do sistema RSA está baseada no fato de ser muito difícil alguém descobrir a chave decodificadora, mesmo que conheça a chave codificadora. Isso está garantido pela maneira que as chaves são formadas, utilizando números muito grandes que são tecnicamente quase impossíveis de serem decompostos em fatores primos.
- No Sistema RSA, uma chave é uma função bijetora de um conjunto finito em outro conjunto finito. Como toda função bijetora possui uma função inversa, toda chave codificadora possui uma chave decodificadora.
- O número de funções de um conjunto *A* com n elementos em um conjunto *B* com k elementos é k^n.
- O número de funções bijetoras de um conjunto *A* com n elementos em um conjunto *B* também com n elementos é $n!$. Esse também é o número de permutações simples de n elementos.
- O número de funções injetoras de um conjunto *A* com n elementos em um conjunto *B* com k elementos, em que $n \leq k$, é $A_k^n = \frac{k!}{(k-n)!}$. Esse também é o número de arranjos de k elementos tomados n a n, sem repetição.

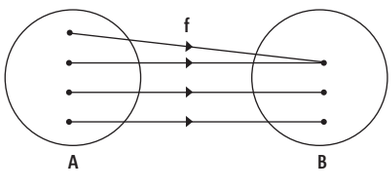
- O número de funções estritamente crescentes de um conjunto ordenado *A* com n elementos em um conjunto ordenado *B* com k elementos, em que $n \leq k$, é $\frac{k!}{n!(n-k)!}$. Esse também é o número de combinações de k elementos tomados n a n, sem repetição.
- O número de funções não decrescentes de um conjunto ordenado *A* com n elementos em um conjunto ordenado *B* com k elementos (em que $n \leq k$) é $\frac{(n+k-1)!}{(k-1)!n!}$. Esse também é o número de soluções positivas ou nulas da equação $x_1 + x_2 + ... + x_k = n$. Esse é ainda o número de combinações com repetição de k elementos tomados n a n.

9. Anexo

Contagem do número de funções sobrejetoras

Durante essa Etapa, dedicamos uma seção para contar funções bijetoras e outra para contar funções injetoras. Talvez você tenha se perguntado: e as funções sobrejetoras? Não vamos contá-las também?

A título de curiosidade, vamos mostrar como contar funções sobrejetoras:



Se *A* tem n elementos e *B* tem k elementos, e $n \geq k$, quantas funções sobrejetoras existem de *A* em *B*?

Vamos subtrair do total de funções aquelas que não são sobrejetoras. O número total de funções de *A* em *B* é k^n.

Sejam b_1, b_2, b_3, ..., b_n os elementos de *B* e seja C_i = { *funções f: A → B tais que* $f^{-1}(\{b_i\}) = \emptyset$}. Note que se *f* está em C_i, então o ponto b_i não está na sua imagem.

Assim, o conjunto das funções que não são injetoras é $C_1 \cup C_2 \cup \ldots \cup C_k$.

Esse **princípio** generaliza, para muitos conjuntos, a contagem do número de elementos da união de dois conjuntos quaisquer (disjuntos ou não):
$n(C_1 \cup C_2) = n(C_1) + n(C_2) - n(C_1 \cap C_2)$

Pelo **princípio da inclusão e exclusão**, o número de elementos deste conjunto é:

$$n(C_1 \cup C_2 \cup \ldots \cup C_k) =$$

$$\sum_{i=1}^{k} n(C_i) - \sum_{1 \leq i < j}^{k} n(C_i \cap C_j) + \sum_{1 \leq i < j < l}^{k} n(C_i \cap C_j \cap C_l) - \ldots$$

Mas,

$$n(C_i) = (k-1)^n, \quad n(C_i \cap C_j) = (k-2)^n, \quad \ldots$$

E, portanto, denotando C_i^k por $\binom{n}{i}$, temos:

$$n(C_1 \cup C_2 \cup \ldots \cup C_k) = \binom{k}{1}(k-1)^n - \binom{k}{2}(k-2)^n + \binom{k}{3}(k-3)^n \ldots \binom{k}{k}(k-k)^n$$

Ou seja,

$$n(C_1 \cup C_2 \cup \ldots \cup C_k) = \sum_{i=1}^{k} (-1)^{i-1} \binom{k}{i} (k-i)^n$$

Logo, o número total de funções sobrejetoras é:

$$k^n - \sum_{i=1}^{k} (-1)^{i-1} \binom{k}{i} (k-i)^n = \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n$$

Etapa IV
Combinatória e probabilidade

Atividades e problemas envolvendo combinatória e probabilidade

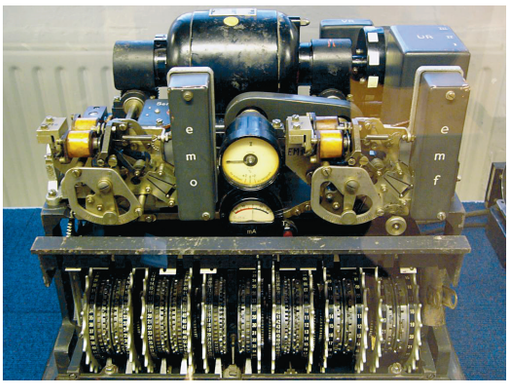
Nas etapas anteriores da disciplina Matemática Discreta, você estudou os fundamentos da Análise Combinatória e estabeleceu relações entre esse conteúdo matemático e a Criptografia. Nesta etapa, iremos desenvolver outro conteúdo matemático – a Teoria de Probabilidades – que pode ser usada na decifração de sistemas criptográficos mais elaborados que os já analisados.

Para iniciar, gostaríamos que você refletisse sobre as seguintes questões:

- **Você sabia que a Teoria das Probabilidades forneceu o arcabouço teórico para a quebra de muitos códigos secretos alemães na época da Segunda Guerra Mundial?**
- **Sabia também que os computadores surgiram para auxiliar a quebra dos sistemas criptográficos gerados por máquinas nazistas?**
- **Você saberia explicar para seus alunos do Ensino Médio como isso foi feito?**

Svilen Milev / SXC

1. Máquinas que criptografam



http://es.wikipedia.org/wiki/Archivo:Lorenz-SZ42-2.jpg

A criptografia sempre esteve presente nas guerras, infelizmente. Durante a Segunda Guerra Mundial, por exemplo, proliferaram máquinas especialmente construídas para uma comunicação mais rápida e segura entre as tropas. Os alemães construíram várias delas, dentre as quais se destaca a máquina Lorenz, usada por membros de alta patente do exército nazista.

Essa máquina gerava mensagens com um código diferente dos já utilizados até a época da Segunda Guerra. Entretanto, com o auxílio da Teoria das Probabilidades, os ingleses conseguiram decifrar os códigos gerados, analisando as mensagens codificadas que conseguiam interceptar. E é incrível como conseguiram fazer isso sem nunca ter acesso a nenhuma dessas máquinas!

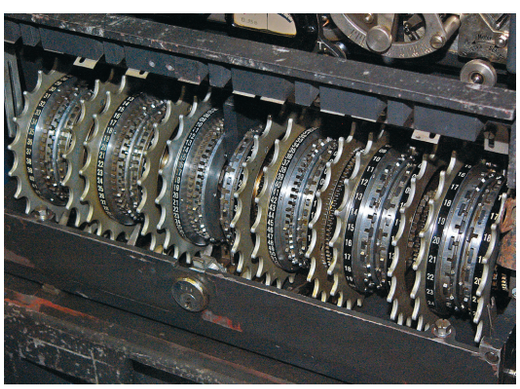
Como fizeram tal façanha? Bem, devido à complexidade dos mecanismos internos dessas máquinas, a simples análise da frequência das letras não se mostrou uma ferramenta eficaz para a decifração de mensagens.

O código gerado não se assemelhava mais ao modelo criptográfico de Júlio César, que vimos na Etapa 1 de nossa disciplina. Nem mesmo técnicas mais sofisticadas de Análise Combinatória se mostraram adequadas a esse propósito. Foi preciso empregar outro conhecimento: a Teoria da Probabilidade.

Nesta última etapa da disciplina Matemática Discreta, veremos como essa teoria foi importante para abreviar a duração da Segunda Grande Guerra, pois permitiu a quebra dos códigos alemães gerados por máquinas criptográficas.

Para começar, vamos conhecer um pouco sobre as máquinas de Lorenz.

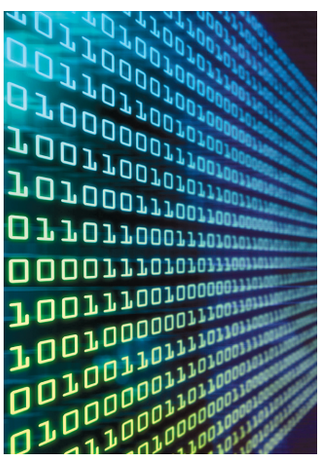
2. A máquina dos generais nazistas



http://es.wikipedia.org/wiki/C%C3%B3digo_Lorenz

Durante a Primeira e a Segunda Guerras Mundiais foram construídos muitos artefatos mecânicos para o envio de mensagens secretas. Vamos estudar uma simplificação de uma dessas máquinas utilizada pelos alemães, a fim de entender a matemática subjacente a ela.

A máquina de Lorenz (modelo SZ 42) possuía 12 rotores que eram usados para embaralhar as letras de uma mensagem. Para criptografar mensagens, a máquina operava da seguinte maneira:



FlavioTakemoto / SXC

- As letras da mensagem eram transformadas em números binários;
- Esses números eram somados, por meio da aritmética binária, a outros números produzidos pela máquina, obtidos pela rotação de suas engrenagens;
- A mensagem criptografada era transformada em pulsos elétricos, enviada como uma mensagem telegráfica e impressa em uma fita perfurada.

Vejamos isto com mais detalhes:

Inicialmente as letras eram transformadas em números: cada letra era codificada por um número binário de cinco algarismos, totalizando $2^5 = 32$ caracteres diferentes, de acordo com a seguinte tabela:

TABELA 1

A	11000	B	10011	C	01110	D	10010	E	10000	F	10110	G	01011
H	00101	I	01100	J	11010	K	11110	L	01001	M	00111	N	00110
O	00011	P	01101	Q	11101	R	01010	S	10100	T	00001	U	11100
V	01111	W	11001	X	10111	Y	10101	Z	10001				
9	00100	8	11111	+	11011	4	01000	3	00010	/	00000		

Observe que, além das 26 letras usuais, seis outros símbolos eram utilizados, ou como sinais de pontuação ou para controlar a impressão. O significado desses últimos seis símbolos não é o usual. Por exemplo, o símbolo + não denota a adição e o algarismo 9 na verdade era usado para separar palavras (espaço em branco).

Se apenas esta codificação fosse feita, o código seria facilmente quebrado pelo método do estudo da frequência das letras, como vimos na Etapa 1 desta disciplina.

Para evitar isto, quando uma letra era introduzida na máquina apertando-se uma tecla correspondente, os rotores giravam e doze novos números eram produzidos.

Adam Cieslelski / SXC

Esses números somados produziam outro número que correspondia a uma letra, de acordo com a Tabela 1. Chamaremos essa letra produzida internamente pela máquina de "letra-chave". A aritmética das adições feitas pela máquina, entretanto, não é a usual. Trata-se da adição binária:

$$0 + 0 = 0$$
$$0 + 1 = 1$$
$$1 + 0 = 1$$
$$1 + 1 = 0$$

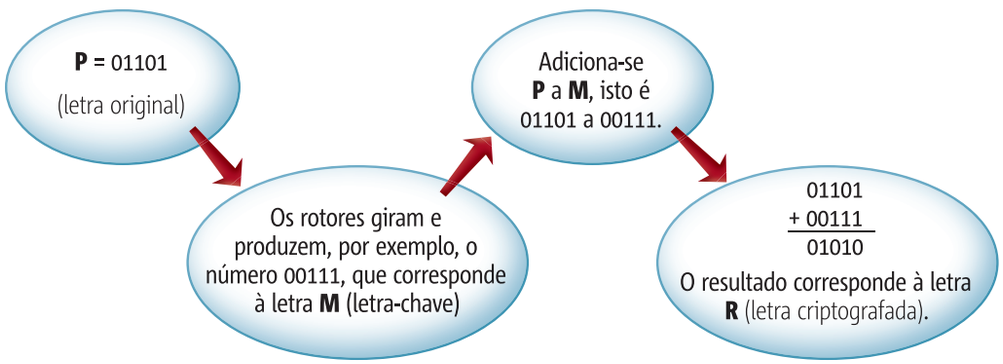
Em seguida, a máquina efetuava automaticamente a soma da letra digitada com a letra-chave e fornecia como saída uma nova letra (correspondente a um novo número). Essa letra final é o resultado criptografado da letra inicialmente digitada.

Para criptografarmos, por exemplo, a letra P, apertamos a tecla correspondente a ela. Quando esta tecla é acionada, as engrenagens da máquina giram.

Adam Ciesielski / SXC

Suponhamos que a letra-chave M é gerada internamente na máquina. Os números binários correspondentes a essas duas letras (a letra original P e a letra-chave M) são somados por adição binária, gerando outro número que corresponde à letra R, que será transmitida na mensagem secreta.

Nesse caso, poderíamos esquematizar o processo de codificação da seguinte forma:



Como consequência, a letra P fica codificada como R.

Da próxima vez que necessitarmos criptografar P, apertamos novamente a tecla correspondente a ela. As engrenagens giram e uma nova letra (talvez diferente de M) é gerada internamente.

Adam Ciesielski / SXC

Logo, P talvez não seja mais criptografada como R, mas sim como uma nova letra ou símbolo. Isto faz com que o código fique imune à análise de frequência de letras.

As somas binárias de todos os símbolos estão descritas na tabela abaixo. A leitura da tabela deve ser feita da seguinte maneira: a soma de uma letra da primeira coluna (1ª parcela) com outra da primeira linha (2ª parcela) está no encontro da linha com a coluna correspondente.

TABELA 2

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	9	8	+	4	3	/
A	/	G	F	R	4	C	B	Q	S	3	N	Z	8	K	+	Y	H	D	I	W	9	X	T	V	P	L	U	M	O	E	J	A
B	G	/	Q	T	O	H	A	F	8	L	P	J	S	Y	E	K	C	W	M	D	V	U	R	9	N	3	X	I	4	+	Z	B
C	F	Q	/	U	K	A	H	G	3	S	E	M	L	4	P	O	B	9	J	V	D	T	X	W	+	8	R	Z	Y	N	I	C
D	R	T	U	/	3	9	W	X	K	4	I	+	Y	S	Z	8	V	A	N	B	C	Q	G	H	M	O	F	P	L	J	E	D
E	4	O	K	3	/	N	+	Y	U	R	C	W	X	F	B	Q	P	J	9	Z	I	8	L	M	H	T	S	V	G	A	D	E
F	C	H	A	9	N	/	Q	B	J	I	4	8	Z	E	Y	+	G	U	3	X	R	W	V	T	O	M	D	L	P	K	S	F
G	B	A	H	W	+	Q	/	C	M	Z	Y	3	I	P	4	N	F	T	8	R	X	9	D	U	K	J	V	S	E	O	L	G
H	Q	F	G	X	Y	B	C	/	L	8	+	I	3	O	N	4	A	V	Z	9	W	R	U	D	E	S	T	J	K	P	M	H
I	S	8	3	K	U	J	M	L	/	F	D	H	G	R	V	T	Z	N	A	P	E	O	Y	+	W	Q	4	B	X	9	C	I
J	3	L	S	4	R	I	Z	8	F	/	9	B	Q	U	W	X	M	E	C	+	N	Y	O	P	V	G	K	H	T	D	A	J
K	N	P	E	I	C	4	Y	+	D	9	/	X	W	A	Q	B	O	S	R	8	3	Z	M	L	G	V	J	T	H	F	U	K
L	Z	J	M	+	W	8	3	I	H	B	X	/	C	V	R	9	S	O	Q	4	Y	N	E	K	U	A	P	F	D	T	G	L
M	8	S	L	Y	X	Z	I	3	G	Q	W	C	/	T	9	R	J	P	B	N	+	4	K	E	D	F	O	A	U	V	H	M
N	K	Y	4	S	F	E	P	O	R	U	A	V	T	/	H	G	+	I	D	M	J	L	8	Z	B	X	3	W	Q	C	9	N
O	+	E	P	Z	B	Y	4	N	V	W	Q	R	9	H	/	C	K	L	X	3	8	I	J	S	F	D	M	U	A	G	T	O
P	Y	K	O	8	Q	+	N	4	T	X	B	9	R	G	C	/	E	M	W	I	Z	3	S	J	A	U	L	D	F	H	V	P
Q	H	C	B	V	P	G	F	A	Z	M	O	S	J	+	K	E	/	X	L	U	T	D	9	R	4	I	W	3	N	Y	8	Q
R	D	W	9	A	J	U	T	V	N	E	S	O	P	I	L	M	X	/	K	G	F	H	B	Q	8	+	C	Y	Z	3	4	R
S	I	M	J	N	9	3	8	Z	A	C	R	Q	B	D	X	W	L	K	/	Y	4	+	P	O	T	H	E	G	V	U	F	S
T	W	D	V	B	Z	X	R	9	P	+	8	4	N	M	3	I	U	G	Y	/	Q	C	A	F	S	E	H	K	J	L	O	T
U	9	V	D	C	I	R	X	W	E	N	3	Y	+	J	8	Z	T	F	4	Q	/	B	H	G	L	P	A	O	M	S	K	U
V	X	U	T	Q	8	W	9	R	O	Y	Z	N	4	L	I	3	D	H	+	C	B	/	F	A	J	K	G	E	S	M	P	V
W	T	R	X	G	L	V	D	U	Y	O	M	E	K	8	J	S	9	B	P	A	H	F	/	C	I	4	Q	N	3	Z	+	W
X	V	9	W	H	M	T	U	D	+	P	L	K	E	Z	S	J	R	Q	O	F	G	A	C	/	3	N	B	4	I	8	Y	X
Y	P	N	+	M	H	O	K	E	W	V	G	U	D	B	F	A	4	8	T	S	L	J	I	3	/	9	Z	R	C	Q	X	Y
Z	L	3	8	O	T	M	J	S	Q	G	V	A	F	X	D	U	I	+	H	E	P	K	4	N	9	/	Y	C	R	W	B	Z
9	U	X	R	F	S	D	V	T	4	K	J	P	O	3	M	L	W	C	E	H	A	G	Q	B	Z	Y	/	+	8	I	N	9
8	M	I	Z	P	V	L	S	J	B	H	T	F	A	W	U	D	3	Y	G	K	O	E	N	4	R	C	+	/	9	X	Q	8
+	O	4	Y	L	G	P	E	K	X	T	H	D	U	Q	A	F	N	Z	V	J	M	S	3	I	C	R	8	9	/	B	W	+
4	E	+	N	J	A	K	O	P	9	D	F	T	V	C	G	H	Y	3	U	L	S	M	Z	8	Q	W	I	X	B	/	R	4
3	J	Z	I	E	D	S	L	M	C	A	U	G	H	9	T	V	8	4	F	O	K	P	+	Y	X	B	N	Q	W	R	/	3
/	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	9	8	+	4	3	/

Observe que a diagonal principal desta tabela é formada apenas pelo símbolo /. Isto se deve ao fato de que a soma binária de parcelas iguais sempre resulta em 00000, o qual é codificado pelo símbolo /. Vejamos um exemplo:

Qual é o resultado da soma binária de R com R? Como R é representado pelo número 01010 e

$$\begin{array}{rccccc} & 0 & 1 & 0 & 1 & 0 \\ + & 0 & 1 & 0 & 1 & 0 \\ \hline & 0 & 0 & 0 & 0 & 0 \end{array}$$

então, R + R = /. Não há nada de especial com a letra R, qualquer símbolo somado com ele mesmo resultará em /.

Isto, como veremos, será importante na quebra do código da máquina, através da análise das mensagens por ela geradas.

Os alemães, por sorte dos aliados, cometiam descuidos ao cifrar suas mensagens. Eles usavam várias palavras com letras repetidas e costumavam usar espaços duplos entre frases e palavras. Por conta disso, muitos símbolos / estavam, de algum modo, presentes nas mensagens criptografadas.

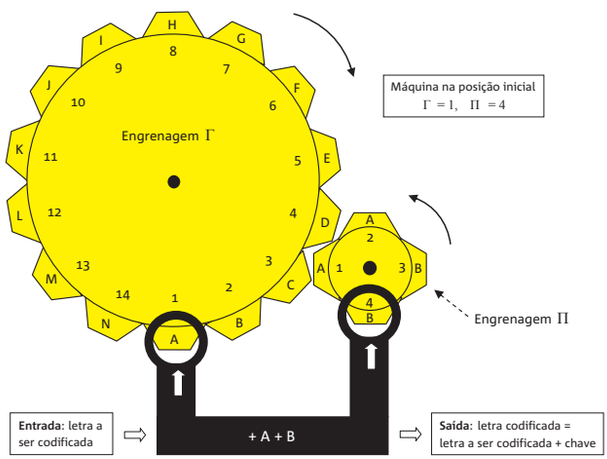
Os aliados perceberam que, se soubessem como as engrenagens estavam dispostas no início do processo, conseguiriam prever qual seria seu comportamento futuro, devido ao funcionamento automático das engrenagens. Não havia, assim, o fator sorte ou escolhas arbitrárias. A máquina não fazia escolhas, apenas realizava movimentos de rotação previsíveis e completamente determinados. Basta conhecer qual é a posição inicial dos rotores para conhecer todas as suas posições futuras.

Nesse ponto é que a Teoria da Probabilidade entra em cena, buscando prever qual a posição inicial dos rotores. Mais adiante explicaremos isso detalhadamente.


Marcus Beltman / SXC

Saiba Mais **Uma simulação simplificada da máquina de Lorentz**

Veja na figura o esquema de uma simulação simplificada da máquina de Lorenz: ela é formada por apenas duas engrenagens, uma grande (Γ) com 14 primeiras letras do alfabeto e outra pequena (Π) com quatro letras: dois A's e dois B's. Na posição inicial, duas engrenagens (no caso $\Gamma = 1$ e $\Pi = 4$) determinam a codificação de todas as demais letras.

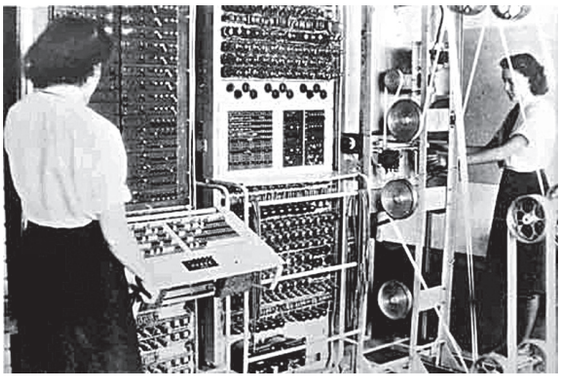


Os números marcam a posição das engrenagens; a maior tem 14 posições possíveis e a menor somente 4. Veja também na primeira foto da máquina de Lorentz, apresentada anteriormente, os números que determinam as posições dos rotores.

Uma vez determinado como as engrenagens estão dispostas inicialmente, toda a mensagem pode ser lida sem problemas.

Os ingleses encontraram uma maneira de descobrir a posição inicial das engrenagens a partir de uma mensagem criptografada. Fizeram isso analisando mensagens longas, pois assim podiam usar a Teoria da Probabilidade.

Para isto, eles se aproveitaram do descuido que os alemães tinham em criptografar textos com muitos símbolos repetidos. Eles tiveram que testar todas as possibilidades para as posições iniciais das 12 engrenagens e, para auxiliá-los, desenvolveram os primeiros computadores com dispositivos eletromecânicos.


http://pt.wikipedia.org/wiki/Ficheiro:Colossus.jpg

A fim de avançar na decifração do código da máquina de Lorenz, passaremos agora ao estudo da Teoria Básica das Probabilidades.

3. A matemática do acaso

Em nosso dia a dia, é comum tentarmos adivinhar qual a melhor alternativa diante de mais de uma opção que tenhamos de escolher.

É natural perguntas como:


Rodrigo Vieira / SXC
Dinko Verzi / SXC
Dimitris Petridis / SXC

Quais as chances de meu time ser campeão? Quais as possibilidades de alguém ganhar no próximo sorteio da Mega Sena? E meu candidato, quais as chances de ele ser eleito na próxima eleição?


Adam Ciesielski / SXC

Basta uma olhada nas revistas, jornais e telejornais que diariamente acessamos, para encontrarmos números que tentam responder a essas perguntas, dando-nos um indício das chances que temos em acertar ou errar nas nossas escolhas. Esses fatos fazem parte do nosso cotidiano.

Nesta seção, aprenderemos uma maneira de medir matematicamente as possibilidades de certos fatos virem a acontecer. Assim você vai entender como foi possível quebrar o código da máquina Lorenz e também como são calculados os números associados a incertezas que são divulgadas pela mídia.

A parte da Matemática que tenta responder a todas essas perguntas chama-se ***Teoria das Probabilidades***. Essa teoria estuda modelos que descrevem fenômenos aleatórios (que ocorrem ao acaso) e serve para medir a chance de ocorrência desses fenômenos.

Janela Pedagógica **Probabilidade e Análise Combinatória na escola**

Buscando estabelecer uma relação entre esta etapa da nossa disciplina com as etapas anteriores, convém ressaltar que os textos didáticos, em geral, trazem os estudos sobre probabilidade após o desenvolvimento de técnicas de contagem oriundas da Análise Combinatória. Quanto a isso, não faremos exceção em nossa disciplina. Embora sejam áreas distintas, elas estão intimamente ligadas, como veremos no decorrer das próximas seções. Essa relação se dá, sobretudo, quando estudamos fenômenos discretos provenientes de situações em que o espaço amostral (o conjunto de todas as possibilidades de um estudo) é finito e os fenômenos envolvidos são equiprováveis.

A Teoria das Probabilidades é, entretanto, mais abrangente e se aplica também em situações descritas por variáveis contínuas (que variam no conjunto dos números reais) como, por exemplo, no problema dos jogos dos discos desenvolvido no Módulo 1, em que foram realizadas experiências envolvendo probabilidade geométrica.

Equipe do Matem@tica na Pr@tica

Miguel Ugalde / SXC

Nesta etapa de nossa disciplina, entretanto, usaremos a Teoria das Probabilidades em situações discretas onde são necessários métodos de contagem, já estudados nas etapas anteriores em Análise Combinatória.

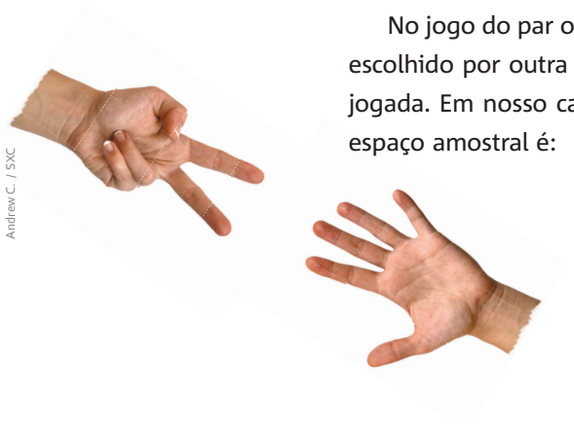
A origem da Teoria das Probabilidades é relativamente recente e esteve ligada, desde o início, aos jogos de azar. Por isso, os primeiros estudos probabilísticos descreviam situações em que os eventos eram igualmente prováveis (***equiprováveis***), ou seja, a chance de qualquer um deles ocorrer seria a mesma. Por exemplo, a chance de sair cara ou coroa no lançamento de uma moeda é a mesma se a moeda for honesta; a chance de sair qualquer número da Mega Sena é a mesma etc.

A seguir, vamos apresentar alguns experimentos, na intenção de introduzir a Teoria das Probabilidades.

3.1. O acaso em toda parte

Ao iniciar esta apresentação, é importante ressaltar que, quando realizamos um experimento, constituído de eventos elementares, devemos selecionar com precisão o conjunto de todos os casos possíveis desses eventos. Esse conjunto é chamado ***espaço amostral*** e é usualmente denotado pela letra grega Ω (ômega maiúsculo).

A menos que explicitemos o contrário, todos os eventos a seguir são considerados aleatórios e os objetos presentes nesses eventos são honestos. Ou seja, os dados não são viciados, nem as moedas têm apenas cara em ambos os lados ou apenas coroa em ambos os lados, por exemplo.



Andrew C. / SXC

No jogo do par ou ímpar, se x for o número escolhido por uma pessoa e y o número escolhido por outra pessoa, representaremos por (x, y) os números escolhidos em uma jogada. Em nosso caso, não consideraremos que se possa escolher o zero. Nesse caso o espaço amostral é:

$$\Omega_1 = \begin{Bmatrix} (1,1) & (1,2) & \dots & (1,5) \\ (2,1) & (2,2) & \dots & (2,5) \\ (3,1) & (3,2) & \dots & (3,5) \\ (4,1) & (4,2) & \dots & (4,5) \\ (5,1) & (5,2) & \dots & (5,5) \end{Bmatrix}$$

Maria Li / SXC

No lançamento de uma moeda, se C=cara e K=coroa, temos como espaço amostral Ω_2 = {C, K}.

No lançamento simultâneo de duas moedas, o espaço amostral é:

$$\Omega_3 = \{(K, K), (K, C), (C, K), (C, C)\}.$$

Dimitris Petridis / SXC

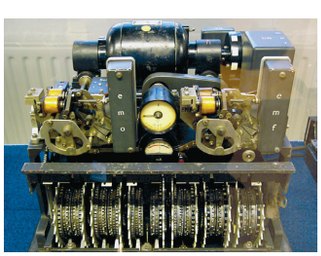
Na Mega Sena, devemos escolher 6 dentre 60 dezenas. O espaço amostral será o número de subconjuntos possíveis de 6 elementos que podemos formar de um conjunto de 60 elementos. Observe que, embora seja inviável listar todas as possibilidades, a Análise Combinatória nos permite responder a seguinte pergunta:

- "Quantos subconjuntos de 6 elementos podemos formar de um conjunto com 60 elementos?"

Basta calcularmos a combinação:

$$C_{60}^{6} = \frac{60!}{54!6!} = \frac{60 \times 59 \times 58 \times 57 \times 56 \times 55}{720} = 50.063.860$$

Esse é o número de elementos do espaço amostral da Mega Sena, que chamaremos de Ω_4 .



http://es.wikipedia.org/wiki/Archivo:Lorenz-SZ42-2.jpg

- Ao selecionarmos dois símbolos para serem adicionados segundo a soma binária na máquina de Lorenz, quantas são as possibilidades de escolha?

Como os dois símbolos podem ser repetidos, há 32. 32 = 1024 possibilidades (permutação com repetição). Ou seja, em experimentos que envolvem a soma binária de símbolos da máquina de Lorenz, o espaço amostral que denotaremos por Ω_5 tem 1024 elementos. Isso quer dizer que 1024 eventos são possíveis, como podemos observar na Tabela 2, da Seção 2.

3.2. Voltando aos exemplos: os casos favoráveis

Dentre os casos possíveis de um espaço amostral Ω, estão aqueles que escolhemos ou que desejamos que ocorram. Estes são chamados ***casos favoráveis***. Vejamos nos exemplos já apresentados algumas situações favoráveis.

- Se alguém diz que vai dar 7 à soma dos números do jogo do par e ímpar, os casos favoráveis do espaço amostral Ω_1 para ocorrência desse evento estão no conjunto: A_1={(2,5),(3,4), (4,3),(5,2)}.

- Se no espaço amostral Ω_2, escolhemos cara, o caso favorável é apenas A_2 = {C}.

- Se jogarmos duas moedas e esperarmos que ocorram duas coroas, os casos favoráveis no espaço amostral Ω_3 estão no conjunto A_3 = {(K,K)}.

- Se na Mega Sena acumulada do dia 27 de janeiro de 2010, você tivesse jogado os números **48 – 32 – 29 – 55 – 27 – 28**, o seu caso favorável no enorme espaço amostral Ω_4 seria o conjunto A_4 = {48, 32, 29, 55, 27, 28}.

Você bem que deveria ter jogado esses números, pois foram os sorteados e ninguém ganhou naquele sorteio, acumulando o prêmio em 9 milhões de reais para o sorteio seguinte.

- Se quisermos encontrar pares de símbolos repetidos na máquina de Lorenz, basta verificar se sua soma resulta no símbolo /. Verificando a Tabela 2, pode-se constatar que o conjunto desses pares, que denotaremos por A_5, tem 32 elementos.

Diante dos conceitos de espaço amostral, casos possíveis e casos favoráveis, chegou o momento de estabelecermos um conceito que possibilite medir as chances de acertarmos em uma escolha: o conceito de probabilidade.

Faremos isto em duas etapas. Em um primeiro momento, considerando o estudo de fenômenos equiprováveis e, posteriormente, considerando o caso geral.

4. Quais são as chances?

Autor desconhecido / SXC

Para definir o conceito de probabilidade, vamos denotar o número de elementos de um conjunto B pelo símbolo $\#B$.

Quando um espaço amostral é formado por eventos elementares, cada um com a mesma chance de ocorrer, esses eventos são chamados ***equiprováveis***.

No caso de eventos equiprováveis, a ***probabilidade de ocorrer um caso favorável*** no conjunto de casos favoráveis A, dentre os casos possíveis de um espaço amostral Ω, é definida por:

$$P(A) = \frac{\text{número de casos favoráveis}}{\text{número de casos possíveis}} = \frac{\#A}{\#\Omega}$$

Andrew C. / SXC

Tendo isso em mente, vejamos o que ocorre com os exemplos da seção anterior. Considerando que todos eles envolvem eventos equiprováveis, podemos aplicar a definição de probabilidade que acabamos de apresentar.

▹ Qual a probabilidade de o resultado do jogo do par e ímpar dar 7?

Nesse caso, os casos prováveis são A_1 ={(2,5),(3,4),(4,3),(5,2)} e os casos possíveis do espaço amostral Ω_1 , já descrito, têm 25 (= 5x5) casos possíveis.

A partir dessas informações, a probabilidade do resultado do jogo ser 7 é:

$$P(soma\ ser\ 7) = \frac{\#A_1}{\#\Omega_1} = \frac{4}{25} = 0,16$$

É comum a probabilidade ser expressa em porcentagem. Logo, a probabilidade de o resultado no jogo do par ou ímpar sair 7 é 16%.

Maria Li / SXC

▹ Ao jogar uma moeda, qual a probabilidade de sair cara?

Nesse caso:

$$P(cara) = \frac{\#A_2}{\#\Omega_2} = \frac{1}{2} = 0,5$$

Logo, a probabilidade de sair cara é 50%. Com cálculo análogo, vê-se que a probabilidade de dar coroa é também de 50%. Assim, comprovamos que as chances de sair cara ou coroa são iguais.

Maria Li / SXC

▹ Ao jogar duas moedas simultaneamente, qual a probabilidade de dar duas caras?

Nesse caso, o conjunto dos casos favoráveis é A_3={(K,K)}. Logo,

$$P(duas\ caras) = \frac{\#A_3}{\#\Omega_3} = \frac{1}{4} = 0,25$$

e a probabilidade de dar duas caras é 25%.

▹ Qual a probabilidade de ganhar na Mega Sena com um jogo simples de 6 números?

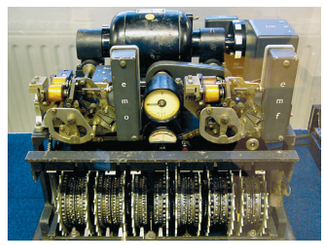
Nesse caso, #A_4 = 1, pois dentre as $\#\Omega_3$ = 50.063.860 possibilidades do espaço amostral, escolhemos apenas uma.

Daí:

$$P(ganhar\ na\ MegaSena) = \frac{\#A_4}{\#\Omega_4} = \frac{1}{50.063.860} = 0,00000002$$

Dimitris Petridis / SXC

Ou seja, a chance de ganhar na Mega Sena com a aposta mais simples é de 0,000002%. Realmente, muito baixa. Não é à toa que é difícil ganhar nesse jogo!



http://es.wikipedia.org/wiki/Archivo:Lorenz-SZ42-2.jpg

- Qual é a probabilidade de, ao alimentarmos a máquina de Lorenz com um símbolo qualquer, sair o símbolo / ? (desconhecendo-se, é claro, o funcionamento interno da máquina).

Como vimos, nesse caso, $\#A_5 = 32$ e $\#\Omega_5 = 1024 = 32 \times 32$ e a probabilidade de encontrá-lo em uma mensagem criptografada é:

$$P(x + y = /) = \frac{\#A_5}{\#\Omega_5} = \frac{32}{32 \times 32} = \frac{1}{32} \approx 0,03$$

ou seja, aproximadamente 3%.

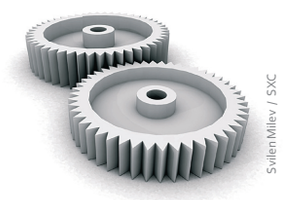
5. E os ingleses nessa história de probabilidade e guerra?

Com base no que você viu até aqui, já é possível desvendar como os ingleses conseguiram decifrar as mensagens criptografadas pela máquina Lorenz. Eles simplesmente testaram todas as possibilidades para as posições iniciais da máquina. Vejamos como isso foi feito.

Em cada teste realizado, há dois casos a analisar:

1. ou as engrenagens estão na posição inicial correta;
2. ou as engrenagens estão na posição inicial incorreta.

- **Mas o que seria uma posição inicial correta? Você consegue imaginar?**



Svilen Milev / SXC

Conforme dissemos anteriormente, os alemães usavam descuidadamente repetições de símbolos. Como vimos na Tabela 2, símbolos repetidos, quando somados, resultam no símbolo /. Logo, se a posição inicial das engrenagens estiver correta, esperamos encontrar uma porcentagem grande do símbolo /.

Os decifradores perceberam esse fato e conseguiam afirmar se a posição inicial estava correta ou não.

Andrew C. / SXC

- **E a posição inicial incorreta?**

Seguindo o mesmo raciocínio, se a posição inicial das engrenagens estiver incorreta, a probabilidade de encontrar o símbolo / será muito baixa, aproximadamente de 3%, conforme calculamos na seção anterior.

Por exemplo, em um texto com 50 caracteres, pode-se mostrar que a probabilidade de se encontrar o símbolo / passa de 3% para aproximadamente 20%, se as engrenagens estiverem na posição inicial correta.

Basta, então, testar todas as possíveis combinações de engrenagens e verificar aquela que produz o maior número possível de símbolos /. Muito provavelmente esta será a posição inicial correta das engrenagens. Quanto mais longa a mensagem, mais a probabilidade aumenta.

Atenção

A probabilidade está relacionada à frequência com que um evento se repete, quando um experimento é realizado um número muito grande de vezes (tendendo ao infinito). Esse princípio é conhecido como a **Lei dos Grandes Números** e estabelece a conexão fundamental entre a Probabilidade e a Estatística.

É aqui que entram os computadores, pois o número de testes que devem ser realizados é enorme.

O esforço para os aliados compensou, pois, uma vez descoberta a posição inicial mais provável das engrenagens, toda a mensagem pôde ser automaticamente decifrada. Com certeza isso ajudou a antecipar o final da Segunda Guerra Mundial e é neste sentido que a Matemática foi usada para vencer a guerra!

Na próxima seção, vamos generalizar os estudos desenvolvidos até agora, para compreender fenômenos probabilísticos mais complexos e fundamentar a teoria desenvolvida.

6. A definição geral de probabilidade

Como já dissemos anteriormente, os primeiros estudos probabilísticos descreviam situações em que os eventos eram igualmente prováveis.

Podemos, entretanto, generalizar a definição de probabilidade de modo a incluir também situações em que os eventos não são equiprováveis. Isso é feito por meio dos seguintes axiomas:

- **Definição:** Em um espaço amostral Ω, consideremos o conjunto $\wp(\Omega)$ das partes de Ω (seus elementos são os subconjuntos de Ω). Dizemos que uma função P definida de $\wp(\Omega)$ com valores no conjunto dos números reais é uma ***probabilidade*** se:
  a) $0 \leq P(A) \leq 1$, para todo $A \in \wp(\Omega)$.
  b) $P(\Omega) = 1$ e $P(\varnothing) = 0$.
  c) $P(A \cup B) = P(A) + P(B)$, se $A \cap B = \varnothing$.

Caso o espaço amostral seja finito e formado por eventos elementares equiprováveis, a definição $P(A) = \dfrac{\text{número de casos favoráveis}}{\text{número de casos possíveis}} = \dfrac{\#A}{\#\Omega}$ fornece uma função que claramente satisfaz a definição acima, nos mostrando que a definição dada inclui o caso equiprovável.

Existem, entretanto, muitos outros casos em que os eventos não são equiprováveis e mesmo assim as propriedades a), b) e c) da definição anterior são válidas. Pode ocorrer também que, no mesmo espaço amostral, possamos definir mais de uma função probabilidade.

Vamos explorar algumas consequências da definição apresentada.

A condição c), na definição de probabilidade, nos diz que $P(A \cup B) = P(A) + P(B)$, desde que A e B sejam subconjuntos disjuntos do espaço amostral. O que ocorre se $A \cap B \neq \varnothing$?

No caso de eventos elementares equiprováveis, como $\#(A \cup B) = \#(A) + \#(B) - \#(A \cap B)$, então:

$$P(A \cup B) = \frac{\#(A \cup B)}{\#(\Omega)} = \frac{\#(A)}{\#(\Omega)} + \frac{\#(B)}{\#(\Omega)} - \frac{\#(A \cap B)}{\#(\Omega)}$$

e daí:

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Mas isto também é válido no caso geral. De fato, como cada uma das decomposições a seguir é uma união disjunta:

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

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

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

então:

$$P(A \cup B) = P(A - B) + P(A \cap B) + P(B - A)$$

$$= P(A) - P(A \cap B) + P(A \cap B) + P(B) - P(A \cap B)$$

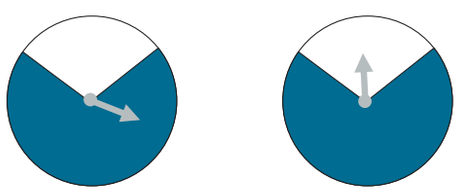
$$= P(A) + P(B) - P(A \cap B)$$

Note que, quando $A \cap B = \phi$, temos $P(A \cup B) = P(A) + P(B)$ e, nesse caso, os eventos A e B chamam-se ***excludentes***. Por exemplo, ao jogar um dado e uma moeda, sair cara na moeda e 5 no dado são eventos excludentes.

Antes de prosseguirmos, precisamos estabelecer uma definição muito importante, a definição de eventos independentes.

6.1. Eventos independentes

Considere duas pequenas roletas como as da figura:



▹ Em cada círculo, a parte preta ocupa 2/3 de sua área. Qual é a probabilidade de, ao girarmos as duas roletas, os dois ponteiros pararem na área branca?

Como as áreas pretas e brancas são diferentes, este experimento não é, *a priori*, constituído por eventos equiprováveis elementares. Mas, se dividirmos a região preta em duas partes iguais, como nas figuras a seguir, podemos trabalhar com outro experimento análogo e equiprovável:

O espaço amostral, nesse caso, é formado pelos seguintes eventos:

$$\Omega = \{ (B_1, B_2), (B_1, P_{21}), (B_1, P_{22}), (P_{11}, B_2), (P_{11}, P_{21}), (P_{11}, P_{22}), (P_{12}, B2), (P_{12}, P_{21}), (P_{12}, P_{22})\}$$

e o único evento favorável é (B_1, B_2), cuja probabilidade é $P((B_1, B_2)) = 1/9$.

Existe, ainda, outra maneira de resolver esse problema.

Pensando somente no primeiro disco, a probabilidade de que a roleta pare na área branca é 1/3 e, pensando somente no segundo disco, a probabilidade de parar na região branca é, analogamente, igual a 1/3. Note que a ocorrência de um desses eventos não interfere na ocorrência do outro. A probabilidade de se obter branco nas duas roletas pode ser obtida como o produto dessas probabilidades:

$$P((B_1, B_2)) = (1/3).(1/3) = 1/9$$

▹ Será que isso funciona sempre ou foi apenas uma coincidência?

Na verdade funciona sempre que os eventos forem independentes, como é o caso em estudo. O resultado obtido na primeira roleta não influencia o resultado na segunda. Matematicamente, temos a seguinte definição:

Definição: Dizemos que dois eventos A e B são independentes se $P(A \cap B) = P(A).P(B)$.

Como veremos nos exercícios posteriores, ao lançarmos duas vezes uma moeda e sair cara em ambos os lançamentos são também eventos independentes. Nos exercícios, disponibilizaremos mais exemplos de eventos independentes.

Para entendermos melhor a definição de eventos independentes, devemos considerar dois eventos e estudar o que acontece com a probabilidade de um deles ocorrer, na certeza de que o outro já ocorreu. Se a ocorrência do primeiro evento não interferir na ocorrência do segundo, os eventos serão independentes, como definido antes. Mas, e se a ocorrência do primeiro evento influenciar na ocorrência do segundo evento? Isto nos leva ao estudo de probabilidades condicionais que desenvolveremos na próxima seção.

7. Probabilidades condicionais

Em um dado espaço amostral, a informação sobre a ocorrência de um evento B pode mudar, ou não, a probabilidade de ocorrência de um evento A. A ***probabilidade condicional*** de um evento A, na certeza absoluta de que ocorreu B é denotada por $P(A \mid B)$ e definida por:

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)}$$

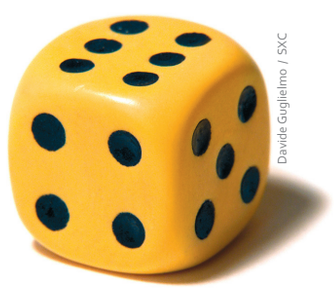
Ora, caso os eventos sejam independentes, então $P(A \cap B) = P(A).P(B)$ e, portanto, $P(A \mid B) = P(A)$. Isto nos diz que, de fato, a ocorrência de B em nada influencia a probabilidade de ocorrer ou não A.

Exemplo 1

Um dado é jogado duas vezes. Qual é a probabilidade de se obter o número 1 na primeira jogada, sabendo-se que a soma dos pontos obtidos foi 2?

Adam Ciesielski / SXC

O espaço amostral é formado pelas 6 x 6 = 36 possibilidades que são obtidas quando se jogam os dois dados. Se F é o evento "resultado do primeiro lançamento" e G é "resultado do segundo lançamento":



Davide Guglielmo / SXC

$$P(F=1 \mid F+G=2) = \frac{P(F=1 \text{ e } F+G=2)}{P(F+G=2)} = \frac{P(F=1 \text{ e } G=1)}{P(F+G=2)} = \frac{(1/6).(1/6)}{1/36} = 1$$

Isto confirma algo evidente: se a soma dos pontos foi 2, então, no primeiro dado, saiu certamente o número 1 (e é claro que no segundo dado também saiu 1).

Exemplo 2

Em um colégio, o número de docentes de Geografia e Português é disposto conforme a seguinte tabela:

TABELA 3

	M = Mulheres	H = Homens
$g =$ docentes de Geografia	7	8
$p =$ docentes de Português	9	3
TOTAL	16	11

Suponha que um mesmo professor não ministra as duas disciplinas e seja selecionado aleatoriamente um dos docentes acima.

Caso saibamos que o evento "ser homem" (H) ocorre, qual a probabilidade de o docente escolhido "ser professor de Geografia"? Ou melhor, qual a probabilidade de o evento "ser professor de geografia (g)" ocorrer, na condição de que o evento "ser homem (H)" ocorra?

Adam Cieslelski / SXC

Tulane Publications / www.flickr.com/photos/jpburch_tulane/4422230743/

Denotemos essa probabilidade por $P(g \mid H)$ (o docente é professor de Geografia na condição de ser um homem). Chamemos $\#T$ o número total de docentes da escola. A partir dos números da tabela anterior, temos:

$$P(g \mid H) = \frac{\#(g \cap H)}{\#(H)} = \frac{8}{11} = \frac{8/27}{11/27} = \frac{P(g)}{P(H)}.$$

Veja que, no cálculo da probabilidade acima, a probabilidade de um primeiro evento (ser homem) influencia no cálculo da probabilidade de um segundo evento (ser homem e docente de Geografia). Note que as probabilidades $P(H)$ e $P(g)$ condicionam o que ocorre com a probabilidade $P(g \mid H)$. Por isto, o nome *probabilidade condicional*.

A seguir, iniciaremos uma seção de resolução de problemas envolvendo os estudos teóricos apresentados nesta etapa. A maioria dos problemas envolve jogos de azar.

8. Resolução de problemas envolvendo probabilidade

Como toda teoria matemática, a Teoria das Probabilidades só revela sua importância quando resolvemos problemas nos quais ela se aplica. Nesta seção, apontaremos alguns problemas interessantes que podem ser apresentados e comentados com seus alunos do Ensino Médio.

8.1. Problemas introdutórios

Atividade 1

Um dado é lançado em cima de uma mesa. Encontre a probabilidade do número com a face voltada para cima ser:

a ▸ par;

b ▸ estritamente maior que 4;

c ▸ estritamente menor que 4;

d ▸ maior que 8;

e ▸ menor que 7.

Ivan Prole / SXC

Resposta comentada

a ▸ Para o evento do item (a), representemos $\#\Omega_{(a)} = 6$ e $A_{(a)} = \{2,4,6\}$. Logo, a probabilidade do item (a) é: $P_{(a)} = \frac{\#A_{(a)}}{\#\Omega_{(a)}} = \frac{3}{6} = \frac{1}{2} = 0,5$, ou seja, 50%.

b ▸ $P_{(b)} = \frac{\#A_{(b)}}{\#\Omega_{(b)}} = \frac{2}{6} = \frac{1}{3} \approx 0,33$, ou seja, aproximadamente 33%.

c ▸ $P_{(c)} = \frac{\#A_{(c)}}{\#\Omega_{(c)}} = \frac{3}{6} = \frac{1}{2} = 0,5$, ou seja, 50%.

d ▸ Nesse caso, $A_{(d)} = \varnothing$. Resposta: $P_{(d)} = \frac{\#A_{(d)}}{\#\Omega_{(d)}} = \frac{0}{6} = 0$, ou seja, 0%, o que era de se esperar.

e ▸ Nesse caso, $A_{(e)} = \{1,2,3,4,5,6\}$. Resposta: $P_{(e)} = \frac{\#A_{(e)}}{\#\Omega_{(e)}} = \frac{6}{6} = 1$, ou seja, 100%, probabilidade que era esperada.

Atividade 2

Andrew C. / SXC

No jogo do par ou ímpar, como apresentamos, é melhor escolher par, ímpar ou tanto faz? Observação: nesse jogo **não** consideramos o número zero.

Resposta comentada

Chamemos $A = \{(x,y)\ tais\ que\ x+y = número\ par\}$. Uma simples listagem mostra que $\#A = 13$ e daí a probabilidade é $P = \frac{\#A}{\#\Omega_1} = \frac{13}{25} = 0,52$, ou seja, 52%.

Se a escolha for um número ímpar, a probabilidade será $P = = \frac{12}{25} = 0,48$, ou seja, 48%. Logo, é melhor escolher um número par.

Desdobramento da Atividade 2

Ainda no jogo do par ou ímpar, qual o número (soma dos dois números escolhidos pelos participantes) que tem a maior probabilidade de ocorrer?

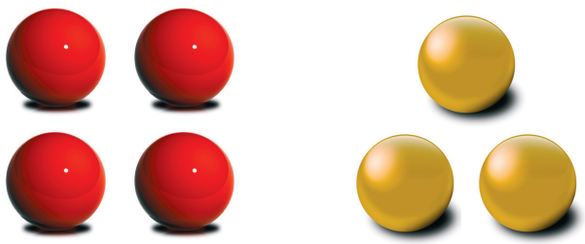
Sugestão: conte quais eventos (x,y) de Ω_1 são tais que $x+y$ é um número par.

Resposta comentada

Resposta: Vê-se que 6 é o número que tem a maior quantidade de pares (x,y), tais que $x+y=6$. Há exatamente 5 pares desses números. Logo, 6 é o número com maior probabilidade de ocorrer: $P = \frac{5}{25} = 0.2$, ou seja, 20%.

Atividade 3

Uma caixa contém 4 bolas vermelhas e 3 bolas amarelas de mesmo peso e tamanho.



Autor desconhecido / SXC

a ▹ Uma bola é escolhida ao acaso. Qual a probabilidade de ela ser vermelha? E de ser amarela?

b ▹ Agora, se duas bolas são retiradas da caixa ao mesmo tempo, qual a probabilidade de elas terem cores diferentes? E qual é a probabilidade de elas terem a mesma cor?

Sugestão para o item b): veja sempre esse tipo de espaço amostral Ω como composto por elementos da forma (x, y), onde x e y são as bolas escolhidas. Para calcular $\#\Omega$, quantos elementos (x, y) podemos formar com os dados do problema? A ordem de x e y importa?

c ▹ Suponha, agora, que tiramos uma bola e que, sem reposição, tiramos novamente outra bola da caixa. Qual a probabilidade de nas duas vezes em que tiramos as bolas terem cor diferente? E qual é a probabilidade de terem a mesma cor?

d ▹ Compare os resultados dos itens b) e c).

Resposta comentada

- A probabilidade de a bola ser vermelha é $P_V = \frac{4}{7} \approx 0,57$. Ou seja, aproximadamente de 57%.
  A probabilidade de a bola ser amarela é $P_B = \frac{3}{7} \approx 0,43$. Aproximadamente 43%.

- Vamos escolher 2 elementos a partir de um conjunto com 7 elementos. A ordem não importa. Logo, $\#\Omega = C_7^2 = \frac{7!}{2!(7-2)!} = 21$. Como temos 4 bolas vermelhas e 3 amarelas, se A é o conjunto dos pares de bolas diferentes, temos, pelo Princípio Multiplicativo, que $\#A = 12$. Logo $P_{cores \neq} = \frac{\#A}{\#\Omega} = \frac{12}{21} = \frac{4}{7} \approx 0,57$. Ou seja, aproximadamente 57%.
  O número dos elementos do conjunto B dos pares serem de bolas de cores iguais é $\#B = 21 - 12 = 9$. Logo $P_{mesma\ cor} = \frac{\#B}{\#\Omega} = \frac{9}{21} = \frac{3}{7} \approx 0,43$. Ou seja, aproximadamente 43%.

Para escolhas de cores diferentes, podemos retirar bolas com a primeira de cor vermelha e a segunda de cor amarela ou a primeira de cor amarela e a segunda de cor vermelha.
Estudemos cada caso.
Primeiro caso: calculemos a probabilidade de a primeira bola ser vermelha e de a segunda ser amarela. Esse é um caso de probabilidade condicional, como se poderá perceber.

- Probabilidade de a primeira bola ser vermelha = $P(1_V) = \frac{4}{7}$.
  Probabilidade de a segunda bola ser amarela, visto que a primeira foi vermelha = $P(2_A \mid 1_V) = \frac{3}{6}$. Note que, após retirarmos a primeira bola, sobraram apenas 6 bolas.
  Chamemos a probabilidade de a primeira bola ser vermelha e de a segunda ser amarela de $P(1_V \cap 2_A)$.
  Ora, sabemos, do cálculo de probabilidade condicional, que $P(2_A \mid 1_V) = \frac{P(1_V \cap 2_A)}{P(1_V)}$, donde $P(1_V \cap 2_A) = P(1_V).P(2_A \mid 1_V)$. Assim:
  A probabilidade de a primeira bola ser vermelha e de a segunda ser amarela é $P(1_V \cap 2_A) = P(1_V).P(2_A \mid 1_V) = \frac{4}{7} \times \frac{3}{6}$.

Segundo caso: calculemos a probabilidade de a primeira bola ser amarela e de a segunda ser vermelha.
Probabilidade de a primeira bola ser amarela $= P(1_A) = \frac{3}{7}$.
Probabilidade de a segunda bola ser vermelha, visto que a primeira foi amarela $= P(2_V \mid 1_A) = \frac{4}{6}$. Note que, após retirarmos a primeira bola, sobraram apenas 6 bolas.
Chamemos a probabilidade de a primeira bola ser amarela e de a segunda ser vermelha de $P(1_A \cap 2_V)$.
Ora, sabemos, do cálculo de probabilidade condicional, que $P(2_V \mid 1_A) = \frac{P(1_A \cap 2_V)}{P(1_A)}$, donde $P(2_V \cap 1_A) = P(1_a).P(2_V \mid 1_A)$. Assim:
A probabilidade de a primeira bola ser vermelha e de a segunda ser amarela é $P(1_A \cap 2_V) = P(1_A).P(2_V \mid 1_A) = \frac{3}{7} \times \frac{4}{6}$.

Note que os eventos *primeira bola de cor vermelha e segunda bola amarela* e *primeira bola amarela e segunda vermelha* são excludentes. Logo, devemos somar as probabilidades desses eventos para calcularmos a probabilidade do evento que queremos: *as bolas terem cores diferentes:*

- Probabilidade de as bolas terem cores diferentes =

$$P(1_A \cap 2_V) + P(1_V \cap 2_A) = \frac{4}{7} \times \frac{3}{6} + \frac{3}{7} \times \frac{4}{6} = 2 \times \frac{12}{42} = \frac{12}{21} = \frac{4}{7},$$

que, no item a), vimos ser aproximadamente 0,57. Ou seja, a probabilidade de tirarmos bolas de cores diferentes é 57%, aproximadamente.

O mesmo procedimento segue para cores iguais. A probabilidade neste caso é 43%, aproximadamente.

d) Os resultados são os mesmos.

Atividade 4

Em uma prateleira, há exatamente 3 CD's de música clássica e 8 CD's de música popular. Uma pessoa retira aleatoriamente 5 CD's dessa prateleira.

a ▸ Quantos elementos têm o espaço amostral dos CD's para essa escolha aleatória?
Sugestão: Quantos subconjuntos de 5 elementos podemos formar com um conjunto de 11 elementos? Isso lembra algum tópico estudado nos módulos anteriores?

b ▸ Qual a probabilidade de nessa escolha terem sido escolhidos 2 CD's de música clássica e 3 de música popular?
Sugestão: Tente resolver sozinho o problema. Só recorra a nossa sugestão em último caso. Aqui vai ela:


Bruno Neves / SXC

Primeiro passo: De quantas maneiras posso escolher 2 CD's dentre 3 CD's de música clássica, ou melhor, quantos subconjuntos de 2 elementos podemos formar a partir de um conjunto com 3 elementos?

Segundo passo: De quantas maneiras posso escolher 3 CD's dentre 8 CD's de música popular, ou melhor, quantos subconjuntos de 3 elementos podemos formar a partir de um conjunto com 8 elementos?

Terceiro passo: De quantas formas posso escolher 2 CD's de música clássica e 3 de música popular, dentre 3 CD's de música clássica e 8 CD's de música popular? Lembre-se do Princípio Multiplicativo da Contagem!

Quarto passo: Agora é só calcular a probabilidade.

Resposta comentada

a ▸ $\#\Omega = C_{11}^5 = \dfrac{11!}{5!(11-5)!} = 462$.

b ▸ $C_3^2 = \dfrac{3!}{2!(3-2)!} = 3$

$C_8^3 = \dfrac{8!}{3!(8-3)!} = 56$

$\#A = C_3^2 \times C_8^3 = 168.$

$P = \dfrac{\#A}{\#\Omega} = \dfrac{168}{462} \approx 0{,}36$

A probabilidade será de aproximadamente 36%.

Bruno Neves / SXC

8.2. Desafios

Desafio 1

Dado um subconjunto de casos favoráveis A de um espaço amostral Ω, denotemos por A^C os eventos complementares de A em relação a Ω. Verifique que vale a seguinte probabilidade:

$$P(A^C) = 1 - P(A)$$

Sugestão: $\Omega = A \cup A^C$, $A \cap A^C = \varnothing$ e use as propriedades da definição geral de probabilidade.

Logo, se já tiver sido calculada a probabilidade de um evento ocorrer, essa fórmula nos fornece prontamente a probabilidade de ocorrer os eventos complementares.

Em quais exercícios anteriores poderíamos ter diretamente usado esse cálculo?

Resposta comentada

Pelas propriedades da probabilidade:

$$P(\Omega) = P(A \cup A^C) = P(A) + P(A^C) \Rightarrow 1 = P(A) + P(A^C) \Rightarrow P(A^C) = 1 - P(A).$$

esse cálculo pode ser usado diretamente nos Exercícios 2a e 3a.

Desafio 2

No sorteio de uma rifa, o ganhador será a pessoa que comprar um dos bilhetes que tiver o número sorteado entre 1 e 500, incluindo-os. Qual a probabilidade de o número sorteado ser maior que 350 ou múltiplo de 10? (note, nesse caso, que o "ou" ***não*** é exclusivo!)

Resposta comentada

Nesse caso, Ω = {1, 2, 3,..., 500} e consideramos os eventos A= {351, 352,..., 499, 500} (número maior que 350) e B = {10, 20, 30,..., 480, 500} (número sorteado ser múltiplo de 10). Queremos calcular $P(A \cup B)$. Note que $A \cap B \neq \phi$, ou seja, os eventos A e B não são mutuamente excludentes. Como fazer para calcular esse tipo de probabilidade?

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

(já provada anteriormente)

Agora, usemos essa fórmula para resolvermos o problema inicial:

Como:

$\#\Omega = 500$

$\#A = 150$

$\#B = 50$

$\#A \cap B = 15$, pois $A \cap B$ = {360, 370,..., 480, 500}

$$P(A) = \frac{\#A}{\#\Omega} = 150/500 = 3/10 = 0{,}3$$

$$P(B) = \frac{\#B}{\#\Omega} = 50/500 = 1/10 = 0{,}1$$

$$P(A \cap B) = \frac{\#(A \cap B)}{\#\Omega} = 15/500 = 3/100 = 0{,}01$$

Temos $P(A \cup B) = P(A) + P(B) - P(A \cap B) = 0{,}3 + 0{,}1 - 0{,}01 = 0{,}39$. Ou seja, a probabilidade de o número escolhido ser maior que 350 ou par é de 39%.

Desafio 3

Um aluno, bastante aplicado e dedicado, fez a seguinte observação:

Professor, vimos que a probabilidade de obter duas caras ao jogarmos duas moedas simultaneamente era ¼. Ora, a probabilidade de dar cara em um só lançamento é ½. Como um lançamento é um evento independente do outro, ao lançar uma moeda duas vezes consecutivas, a probabilidade de dar cara nesses dois lançamentos é 1/2x1/2=1/4. Essa é justamente a probabilidade de dar duas caras em dois lançamentos simultâneos. Logo, a probabilidade de dar duas caras em lançamentos simultâneos de duas moedas é a mesma de dar cara em dois lançamentos consecutivos.

O mesmo ocorre com a probabilidade calculada ao retiramos duas bolas ao mesmo tempo de uma urna ou retirar uma bola e depois outra, sem repor. A mesma coisa acontece, ainda, com o cálculo das probabilidades ao lançarmos dois dados simultaneamente ou lançarmos um dado e depois outro.

O aluno tem razão? Justifique sua resposta.

Resposta comentada

Sim, o aluno tem toda razão. No caso das moedas, já vimos que o espaço amostral, ao lançarmos duas moedas, é Ω_3 = {(K, K), (K, C), (C, K), (C, C)}. Logo, a probabilidade de dar duas caras é ¼, que é o produto da probabilidade de em dois lançamentos obtermos duas caras 1/4 = 1/2 x 1/2.

No caso das bolas, ver o Exercício 3, que comprova a afirmação do aluno.

Desafio 4

Verifique que a probabilidade de jogarmos uma moeda 25 vezes e nessas jogadas obtermos 25 caras consecutivas é uma vez e meia maior do que a probabilidade de acertar na Mega Sena com uma aposta simples de 6 números. Compare os casos.

Sugestão: Em cada jogada, qual a probabilidade de dar cara? Cada jogada é um evento independente da outra jogada? Veja o que ocorre no exercício anterior no caso de jogarmos a moeda duas vezes.

Resposta comentada

A comparação dessas probabilidades é incrível, não? Se não achar, tente obter 25 caras consecutivas ao lançar uma moeda 25 vezes consecutivas!

Como no exercício anterior, ao jogarmos uma moeda 25 vezes, a probabilidade de dar 25 caras consecutivas é $\underbrace{\frac{1}{2}\times\frac{1}{2}\times\ldots\frac{1}{2}}_{25\ vezes}=\frac{1}{2^{25}}\approx 0,00000003$, que é maior do que a probabilidade de acertar na Mega Sena, que vimos ser $0,00000002$.

9. Conclusão

Nesta etapa, mais uma vez, você pode perceber que a Criptografia é um tema bastante fértil para introduzir conteúdos matemáticos no Ensino Médio. Além de servir de ponto de partida para a abordagem de conteúdos relacionados à Análise Combinatória de forma interessante e envolvente, esse tema pode também ser um fio condutor para a abordagem da Teoria das Probabilidades.

Você já deve ter percebido que nas escolas os textos didáticos costumam trazer os estudos sobre probabilidade após o desenvolvimento de técnicas de contagem oriundas da Análise Combinatória. Por isso, optamos por trilhar esse mesmo caminho na disciplina Matemática Discreta, considerando que esta pudesse ser bastante proveitosa para você refletir sobre sua sala de aula e sobre o trabalho que desenvolve junto aos seus alunos.

10. Resumo

- A máquina de Lorenz foi construída pelos alemães na época da Segunda Guerra Mundial para criar mensagens secretas. Essa máquina gerava um código diferente dos utilizados até então.
- A análise da frequência das letras não era suficiente para quebrar o código da máquina de Lorenz.
- Os ingleses conseguiram decifrar os códigos gerados pela máquina de Lorenz com o auxílio da Teoria das Probabilidades.
- A operação da máquina se dava por meio de 3 passos fundamentais: transformar letras originais em números binários; criar uma letra-chave que também é transformada em um número binário; somar os números binários (aritmética binária) dando origem a um terceiro número, que corresponde à letra codificada.
- Qualquer símbolo somado com ele mesmo resultava em /.
- Os ingleses perceberam que, se soubessem como as engrenagens estavam dispostas no início do processo, conseguiriam prever qual seria seu comportamento futuro, devido ao funcionamento automático das engrenagens.
- A Teoria da Probabilidade entra em cena na medida em que busca prever qual a posição inicial dos rotores.
- A Teoria da Probabilidade estuda modelos que descrevem fenômenos aleatórios (que ocorrem ao acaso) e serve para medir a chance de ocorrência desses fenômenos.
- Quando realizamos um experimento constituído de eventos elementares, selecionamos com precisão o conjunto de todos os casos possíveis desses eventos. Esse conjunto é chamado ***espaço amostral*** e é usualmente denotado pela letra grega Ω.
- Dentre os casos possíveis de um espaço amostral Ω, estão aqueles que escolhemos ou desejamos que ocorram. Estes são chamados ***casos favoráveis***.
- Quando um espaço amostral é formado por eventos elementares, cada um com a mesma chance de ocorrer, esses eventos são chamados ***equiprováveis***.

- No caso de eventos equiprováveis, a probabilidade de ocorrer um caso favorável no conjunto de casos favoráveis A, dentre os casos possíveis de um espaço amostral Ω, é definida por $P(A) = \frac{\text{número de casos favoráveis}}{\text{número de casos possíveis}} = \frac{\#A}{\#\Omega}$, sendo #A o número de elementos do conjunto A.
- Podemos generalizar a definição de probabilidade, incluindo eventos não equiprováveis da seguinte forma: em um espaço amostral Ω, consideramos o conjunto $\wp(\Omega)$ das partes de Ω (seus elementos são os subconjuntos de Ω). Dizemos que uma função P definida nas partes de Ω com valores no conjunto dos números reais é uma probabilidade se (a) $0 \leq P(A) \leq 1$, para todo $A \in \wp(\Omega)$; (b) $P(\Omega) = 1$ e $P(\varnothing) = 0$; (c) $P(A \cup B) = P(A) + P(B)$, se $A \cap B = \varnothing$.
- Podemos dizer que dois eventos A e B são independentes se $P(A \cap B) = P(A).P(B)$.
- Em um dado espaço amostral, a informação sobre a ocorrência de um evento B pode mudar ou não a probabilidade de ocorrência de um evento A. A probabilidade condicional de um evento A, na certeza absoluta de que ocorreu B, é denotada por $P(A \mid B)$ e definida por $P(A \mid B) = \frac{P(A \cap B)}{P(B)}$.
- Os eventos são independentes, quando $P(A \cap B) = P(A).P(B)$ e daí $P(A \mid B) = P(A)$. Assim, a ocorrência de B em nada influencia a probabilidade de ocorrer ou não A.

Encerramento

Chegamos ao final da disciplina Matemática Discreta. Esperamos que você tenha aproveitado todo o conhecimento desenvolvido para refletir sobre o ensino de Matemática, bem como sobre seu trabalho cotidiano em sala de aula.

Ao longo deste estudo abordamos importantes conceitos da Matemática, com o objetivo de mostrar que podemos contextualizar e repensar seu ensino na escola. Desejamos que o curso tenha sido mais uma oportunidade de proporcionar reflexões e experimentações pedagógicas e que você possa continuar o seu trabalho como professor criando e incorporando novas propostas.

Mas nossos trabalhos não param por aqui! Continuaremos caminhando juntos e refletindo sobre a melhoria do ensino de Matemática em nossas escolas.

Bibliografia

Bletchley Park. Disponível em: <http://www.bletchleypark.org.uk/>. Acesso em: 26 jul. 2010.

MALAGUTTI, P. L. A. *Atividades de Contagem a partir da Criptografia* - OBMEP, vol. 10. Disponível em <http://www.obmep.org.br>. Acesso em: 26 jul. 2010.

MORGADO, PITOMBEIRA, CARVALHO, FERNANDEZ. *Análise Combinatória e Probabilidade*. IMPA, 1991.

SGARRO, A. *Códigos Secretos: Criptografia*. São Paulo: Editora Melhoramentos, 1989.

Disponível em: <http://www.cimt.plymouth.ac.uk/resources/codes/default.htm>. Acesso em: 21 jul. 2010.

Disponível em: <http://www.ibc.gov.br/?catid=110&blogid=1&itemid=479>. Acesso em: 21 jul. 2010.