Atividades de Contagem a partir da Criptografia

Pedro Luiz Malagutti

versão 2015

Impresso no Brasil/Printed in Brazil
Primeira edição
Décima primeira impressão

Capa: Rogério Kaiser

Malagutti, Pedro
Atividades de Contagem a partir da Criptografia
Rio de Janeiro, IMPA, 2015
77 páginas
ISBN 978-85-244-0337-8

Distribuição
IMPA/OBMEP
Estrada Dona Castorina, 110
22460-320 Rio de Janeiro, RJ
e-mail: cad_obmep@obmep.org.br
www.obmep.org.br

Texto já revisado pela nova ortografia.

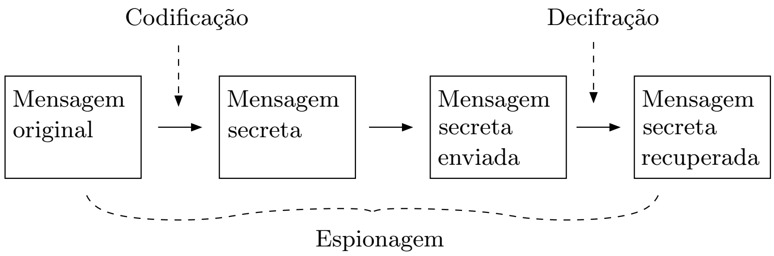
Sumário

Capítulo 1

Mensagens Secretas Obtidas por Substituição – Introdução ao Estudo de Permutações

Enviar mensagens secretas é uma tarefa muito antiga; ela nasceu com a diplomacia e com as transações militares. Hoje em dia, entretanto, com o advento da comunicação eletrônica, muitas atividades essenciais dependem do sigilo na troca de mensagens, principalmente aquelas que envolvem transações financeiras e uso seguro da Internet.

A ciência que estuda sistemas de envio e recepção de mensagens secretas chama-se CRIPTOLOGIA. Simplificadamente, temos o seguinte diagrama:



Nosso objetivo é apresentar atividades com criptografia através de aparatos que possam efetivamente ser construídos com materiais simples (papel, palito de dente, clipe, furador de papel, cola e tesoura) para explorar alguns aspectos matemáticos destas construções, principalmente os ligados à contagem.

1.1 Criptografia de Júlio César

Um dos primeiros sistemas de criptografia conhecido foi elaborado pelo general Júlio César, no Império Romano. Júlio César substituiu cada letra, pela terceira letra que a segue no alfabeto.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Q	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
T	U	V	W	X	Y	Z	A	B	C

Segundo este sistema, a palavra MATEMÁTICA passa a ser PDWHPDWLFD.

Atividade 1: Decifre a mensagem:

OHJDO FRQVHJXL

Ao invés de caminhar 3 letras para frente, podemos andar um outro número de letras e teremos um novo método de cifrar mensagens. Este número é chamado de <u>chave</u> ou <u>senha</u> do sistema criptográfico; ele deve ser conhecido apenas por que envia a mensagem e por quem a recebe.

Podemos também transformar letras em números, segundo uma ordem preestabelecida. Por exemplo:

A=0	B=1	C=2	D=3	E=4	F=5	G=6	H=7
I=8	J=9	K=10	L=11	M=12	N=13	O=14	P=15
Q=16	R=17	S=18	T=19	U=20	V=21	W=22	X=23
Y=24	Z=25						

Deste modo, a letra codificada é obtida da letra original, somando-se 3 ao número correspondente. E se o resultado ultrapassar 25? Caso isto ocorra, a letra codificada estará associada ao resto da divisão por 26 do número associado à letra original somado com 3. Por exemplo, a letra Y corresponde originalmente ao número 24, somando-se 3, obteremos $24 + 3 = 27$ e, dividindo 27 por 26, obteremos resto 1 que corresponde à letra B. Assim Y deve ser codificado por B.

Se um espião conhecer a chave (o número de letras que andamos – no nosso exemplo igual a 3), poderá facilmente decifrar uma mensagem interceptada, trocando cada letra pela terceira anterior. Mas, não se conhecendo a chave, como decifrar mensagens criptografadas? Pense um pouco a respeito disso.

1.2 Construção de Aparatos que Ajudam a Criptografar

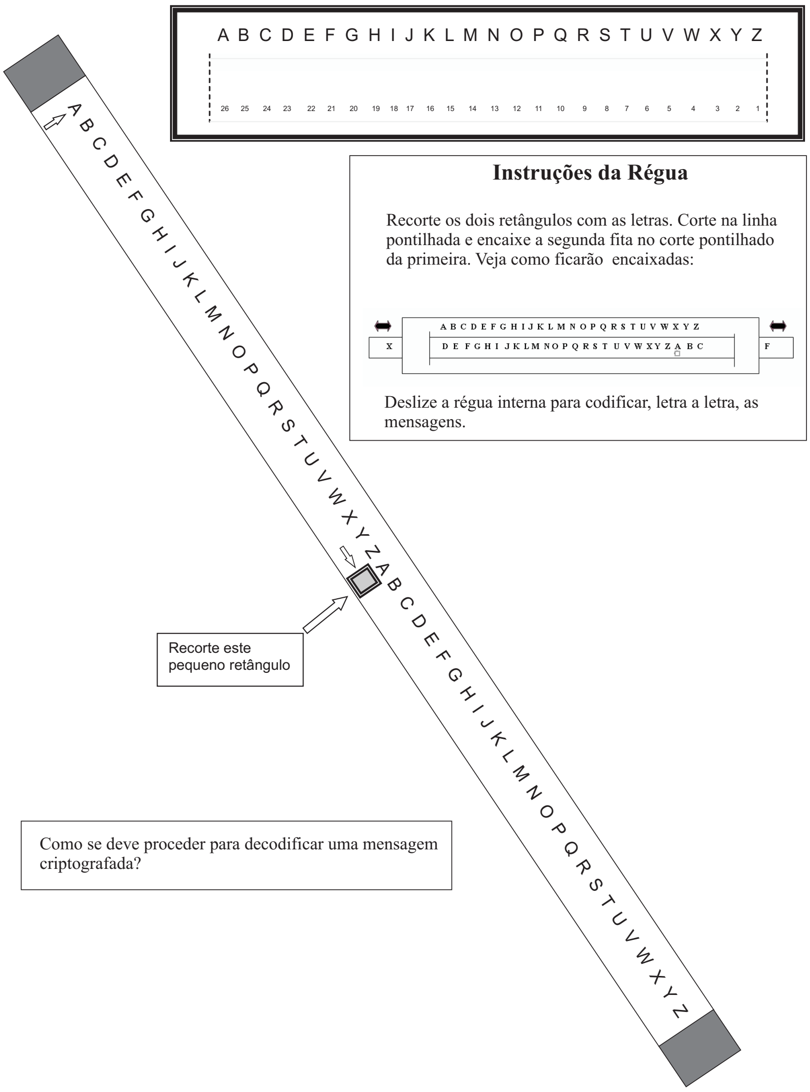
Vamos apresentar cinco aparatos simples para agilizar a criptografia no estilo de Júlio César:

- as réguas deslizantes;
- o quadrado de Vigenère[1];
- os círculos giratórios; e
- dois projetos: a lata de criptografar e o CD para criptografar.

Como veremos, são todos variações simples de um mesmo tema.

Atividade 2: Recorte e monte as réguas deslizantes, conforme as instruções na página seguinte.

[1] Blaise Vigenère foi um diplomata francês, estudioso de Criptografia, que viveu no século XVI.



Aviso: Esta página está no encarte que veio junto com a apostila.

As diferentes posições que a régua deslizante ocupa quando movimentada podem ser simultaneamente visualizadas no quadrado de Vigenère:

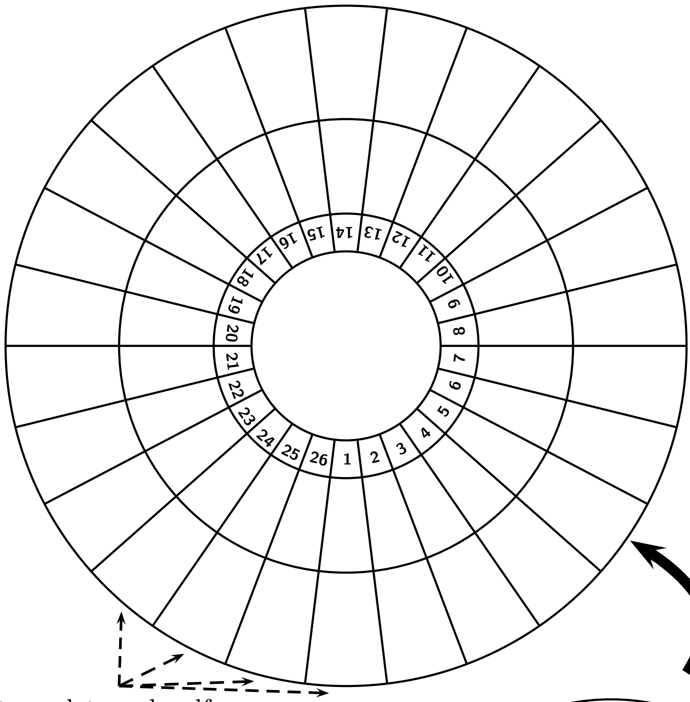
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z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

Atividade 3: Utilizando a régua deslizante ou o quadrado de Vigenère, decifre a mensagem:

UHV JVUZLNBP KLJPMYHY UHKH

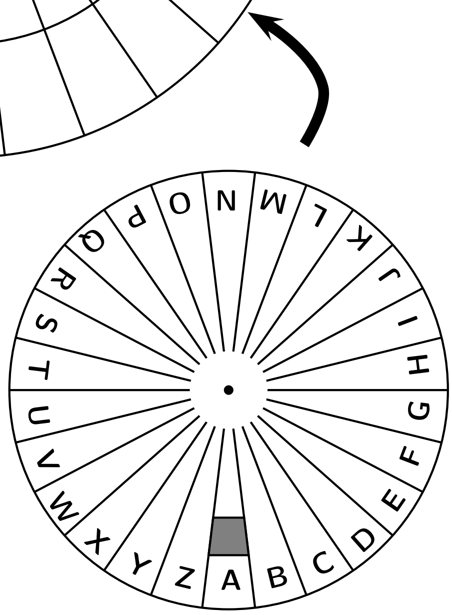
Leia em voz alta o que você decifrou.

Atividade 4: Recorte e monte os discos giratórios, conforme as instruções da próxima página. Nos espaços vazios complete cada um deles com uma letra diferente à sua escolha para que você tenha sua maneira de criptografar.



Recorte as letras do alfabeto abaixo, embaralhe-as e cole-as uma a uma nos espaços vazios do círculo maior.

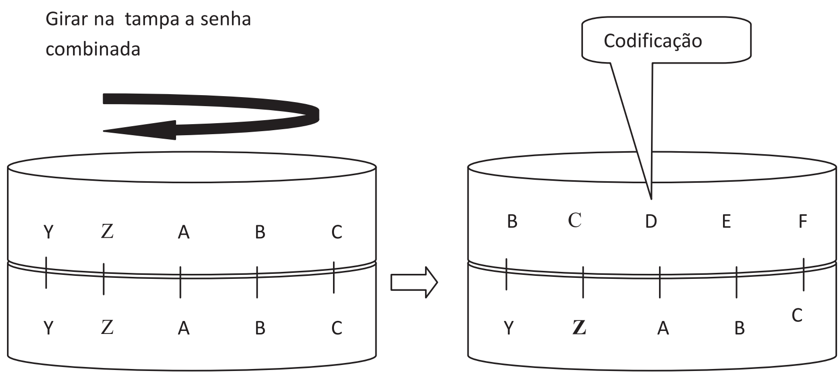
A	B	C	D	E	F
G	H	I	J	K	L
M	N	O	P	Q	R
S	T	U	V	W	X
Y	Z				



Atividade 5:

Projetos práticos de criptografia

Lata de criptografar

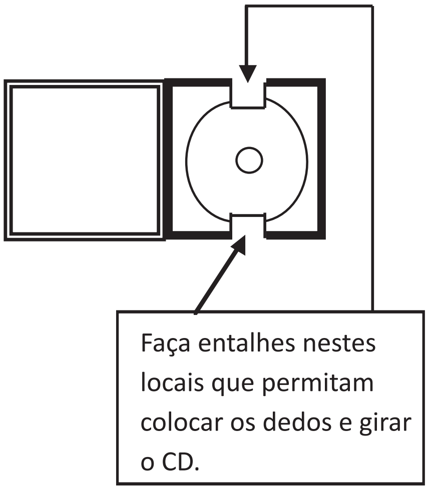


CD para criptografar

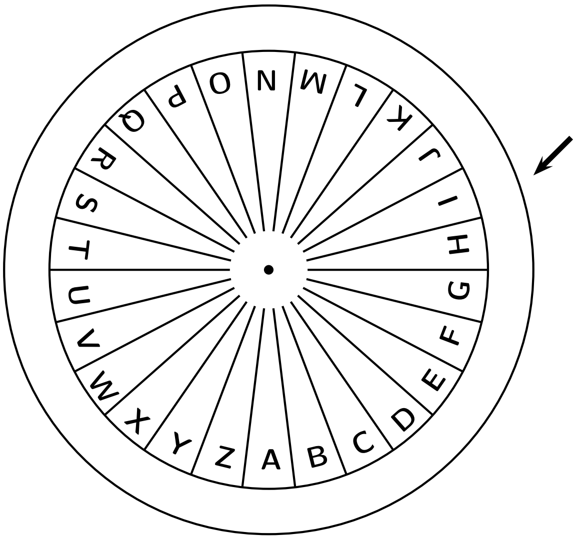
Para confeccionar este aparato você vai precisar de um CD que não tenha mais uso e também de sua caixinha.

Reproduza, recorte o círculo e cole-o no CD. O CD deve ser encaixado dentro da caixinha.

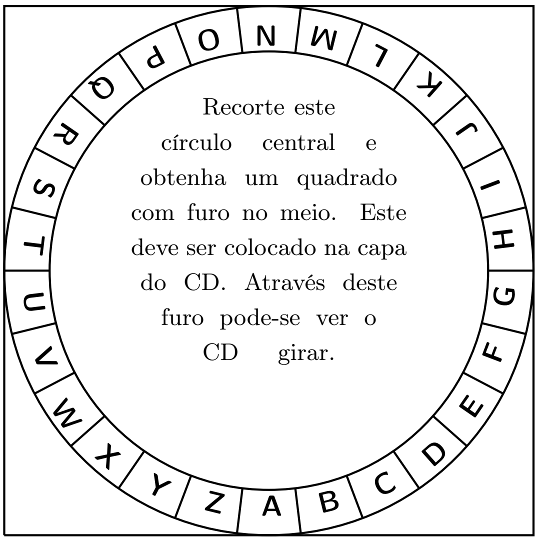
O quadrado com o furo no meio deve ser colocado na capa do CD. Para fazer a máquina funcionar você deve recortar na parte detrás da caixinha dois pequenos retângulos, suficientes para introduzir os dedos e girar o CD.


Faça entalhes nestes locais que permitam colocar os dedos e girar o CD.

Círculo para Criptografia



Recorte este círculo e cole em um CD que já foi descartado. Encaixe o CD na posição usual dentro da caixinha.



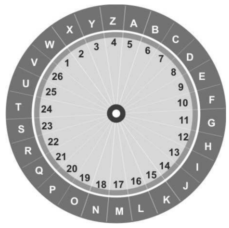
Aviso: Use um CD usado como molde em uma folha de papel e copie a figura ajustando o tamanho para ser igual ao do CD.

"principal"
2010/4/20
page 14
Estilo OBMEP

Atividade 6: Resolva a seguinte questão (OBMEP 2007)

3ª OLIMPÍADA BRASILEIRA DE MATEMÁTICA DAS ESCOLAS PÚBLICAS
OBMEP 2007
Somando novos talentos para o Brasil

Um antigo método para codificar palavras consiste em escolher um número de 1 a 26, chamado *chave* do código, e girar o disco interno do aparelho ilustrado na figura até que essa chave corresponda à letra A. Depois disso, as letras da palavra são substituídas pelos números correspondentes, separados por tracinhos. Por exemplo, na figura ao lado a chave é 5 e a palavra *PAI* é codificada como 20-5-13.



(a) Usando a chave indicada na figura, descubra qual palavra foi codificada como 23-25-7-25-22-13.

(b) Codifique *OBMEP* usando a chave 20.

(c) Chicó codificou uma palavra de 4 letras com a chave 20, mas esqueceu de colocar os tracinhos e escreveu 2620138. Ajude o Chicó colocando os tracinhos que ele esqueceu e depois escreva a palavra que ele codificou.

(d) Em uma outra chave, a soma dos números que representam as letras *A*, *B* e *C* é 52. Qual é essa chave?

1.3 Princípios de Contagem em Criptografia

Nos sistemas que seguem o princípio de Júlio César, podemos usar 25 chaves diferentes para obter codificações diferentes, já que o sistema com chave 0 (ou 26), não codifica nada. Nestes sistemas o alfabeto é codificado seguindo a ordem usual, apenas iniciando em um lugar diferente. Se, entretanto, pudermos alterar a ordem, obteremos um enorme número de maneiras de criptografar. Vejamos alguns exemplos:

a) Alfabeto quebrado ao meio:

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

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

P	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
O	R	Q	T	S	V	U	X	W	Z	Y

Observe que nenhuma letra ficou no seu lugar original. Neste caso, dizemos que houve um **desordenamento**.

c) Usando a sequência que aparece no teclado do computador:

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

P	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
H	J	K	L	Z	X	C	V	B	N	M

Aqui também houve desordenamento.

Atividade 7: Usando o código:

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

M	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**
N	M	L	K	J	I	H	G	F	E	D

X	**Y**	**Z**
C	B	A

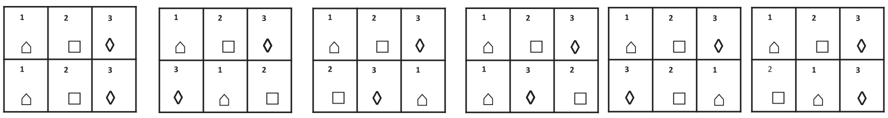
Decifre a mensagem:

Z TIZNZ V' ZNZITZ

Leia de trás para frente a mensagem decifrada.

1.4 Quantas Maneiras Diferentes de Criptografar Podemos Construir?

Digamos que no planeta Plunct os alfabetos fossem formados por apenas três símbolos: ⌂, □ e ◊. Poderíamos criptografar mensagens de seis maneiras diferentes:



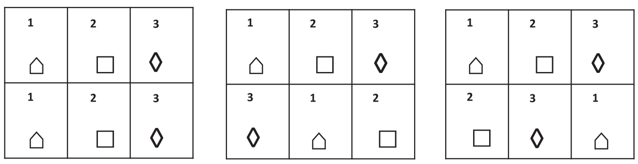
A primeira dessas maneiras é a "trivial" e não serve para codificar nada. Sem listar as mensagens, poderíamos concluir que existem seis maneiras diferentes de permutar as letras deste alfabeto? É claro que sim: para a primeira letra existem três possibilidades de codificação, para a segunda apenas duas e para a terceira resta somente uma possibilidade. Pelo **Princípio Multiplicativo da Contagem**, são

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

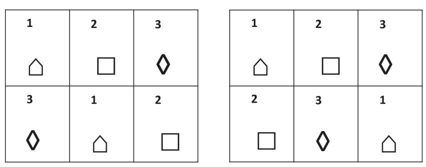
> **O Princípio Multiplicativo da Contagem:**
>
> Se uma decisão puder ser tomada de m maneiras diferentes e se, uma vez tomada esta primeira decisão, outra decisão puder ser tomada de n maneiras diferentes, então, no total serão tomadas $m \times n$ decisões.

as possibilidades. Há uma notação muito útil para se trabalhar como produtos do tipo acima, camada **fatorial**. Por exemplo, o fatorial de 3 é $3! = 3 \cdot 2 \cdot 1$. No caso geral, para um inteiro positivo n, define-se $n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$ e, por convenção, $0! = 1$.

Observe que dentre estas, são três as possibilidades que mantém a "ordem usual" ⌂ $\rightarrow \square \rightarrow \Diamond \rightarrow$ ⌂ $(1 \rightarrow 2 \rightarrow 3 \rightarrow 1)$ inalterada:

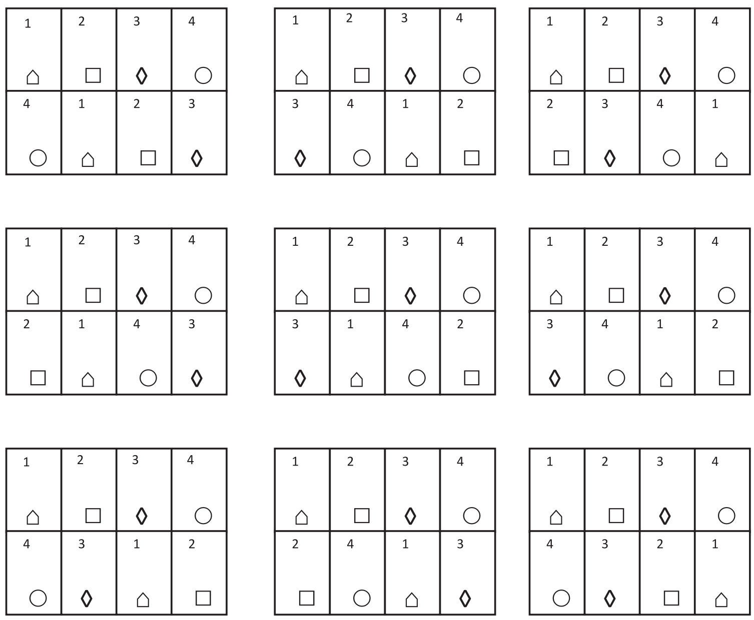


Quantos desordenamentos há neste caso? Apenas dois:



No planeta Plact (talvez mais evoluído que Plunct) são quatro as letras empregadas: ⌂, $\Box$, $\diamondsuit$ e $\bigcirc$. Há, neste caso, $4 \cdot 3 \cdot 2 \cdot 1 = 4! = 24$ maneiras diferentes de permutar as "letras". Dentre estas, apenas 4 respeitam a ordem usual ⌂ $\to \Box \to \diamondsuit \to \bigcirc \to$ ⌂. Quais são elas?

Há 9 desordenamentos:



O que ocorre se usarmos as 26 letras de nosso alfabeto? Podemos inferir algo?

Existem 26! maneiras diferentes de criptografar, isto dá

$$403 \quad 291 \quad 461 \quad 126 \quad 605 \quad 635 \quad 584 \quad 000 \quad 000$$

possibilidades! Se, entretanto, quisermos preservar a ordem usual das letras, temos somente 26 maneiras, incluindo a trivial em que cada letra é trocada por ela mesma.

Em geral, se tivermos n letras, teremos

$$n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$$

permutações diferentes e somente n delas respeitam a ordem usual. É possível também calcular os desordenamentos (em que nenhuma letra fica no seu lugar natural). O número total de desordenamentos com n letras é:

$$n! \left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + \frac{(-1)^n}{n!} \right)$$

(para ver a dedução desta fórmula veja o livro *Análise Combinatória e Probabilidade* de Morgado, Pitombeira de Carvalho, Pinto Carvalho e Fernandez – IMPA, 1991).

Como curiosidade, com 26 letras o número de desordenamentos é: 148 362 637 348 470 135 821 287 825.

Com tantas possibilidades de codificação, parece extremamente difícil se descobrir a chave para se quebrar um código 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 disto o código de Júlio César e suas variações são muito fáceis de serem quebradas, como veremos a seguir.

1.5 Como Quebrar o Código de Júlio César

Mapas de tesouros

Vamos ilustrar a teoria da decifração com um trecho de um conto do escritor Edgar Allan Poe, intitulado "O Escaravelho de ouro".[2]

O personagem principal deste conto, em uma certa altura da obra, encontra um velho pergaminho que acredita ser um mapa de um tesouro, com os seguintes dizeres:

(53±±+305))6*; 4826) 4±.)4±);806*;48+8π
60))85;1±(;:±*8+83(88)5*+;46(;88*96*?;8)*±(;485);5*+2:*±(;4956* 2
(5*-4)8π8* ; 4069285);)6+8)4±±;1(±9;48081 ; 8:8±1;48+85;4) 485 +
528806* 81(±9;48; (88;4 (± ? 34;48) 4 ± ; 161 ; : 188; ±?;

No conto, após uma análise baseada na frequência das letras do alfabeto inglês feita pelo protagonista, a mensagem toma a seguinte forma:

> *A good glass in the bishop's hostel in the devil's seat forty-one degrees and thirteen minutes north-east and by north main branch seventh limb east side shoot from the left eye of the death's-head a bee line form the tree through the shot fifty feet out.*

[2]Este conto faz parte do livro *História de Mistério e Imaginação* de Edgar Allan Poe, Editorial Verbo, nº 15, Lisboa.

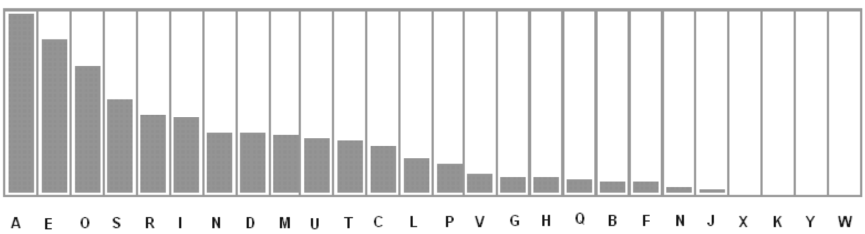
Como isto foi obtido? A letra que aparece com mais frequência na língua inglesa é a letra e; muitas vezes ela aparece dobrada **ee**. Na mensagem secreta acima o símbolo 8 aparece 33 vezes, muito mais do que as outras letras e, portanto, é plausível que 8 deva significar a letra **e**. Substituindo 8 por **e** e tentando o mesmo esquema com outras letras é possível decifrar a mensagem. Sua tradução para o português é:

> *Um bom vidro na hospedaria do bispo na cadeira do diabo quarenta e um graus e treze minutos nordeste e quarta de norte ramo principal sétimo galho do lado leste a bala através do olho esquerdo da cabeça do morto uma linha de abelha da árvore através da bala cinquenta pés para fora.*

O conto então revela, de uma maneira fantástica, como, a partir destas informações, o personagem principal encontra um tesouro há muito tempo enterrado por um pirata que passou pelo lugar descrito na mensagem.

O estudo da frequência das letras do alfabeto constitui um método eficaz para se quebrar mensagens no estilo de Júlio César.

Frequência aproximada das letras em português (%)



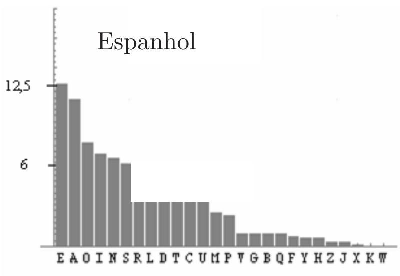
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
14,6	1,0	3,8	4,9	12,5	1,0	1,3	1,2	6,1	0,4	0,02	2,7

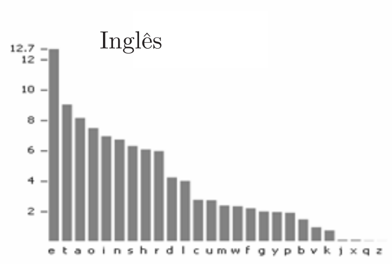
M	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**
4,7	5,0	10,7	2,5	1,2	6,5	7,8	4,3	4,6	1,6	0,01	0,2

Y	**Z**
0,01	0,4

Curiosidade: apesar da letra a aparecer em quase todos os textos escritos em português, é possível encontrar textos em que esta letra não aparece nunca ou quase nunca. Você conseguiria escrever um texto com 5 linhas sem usar nenhuma vez a letra a?

Como curiosidade, veja como aproximadamente se distribuem as letras no espanhol e no inglês:





Atividade 8: Usando as frequências das letras em português, decifre a mensagem abaixo e complete a tabela para registrar as substituições encontradas.

Urtklm tr dqapuakcftr ltr iasqtr aj nmqsuouar lacfdqa t jakrtoaj tetfxm a cmjniasa t steait ntqt qaofrsqtq tr ruersfsufcmar akcmksqtltr.

Observe na tabela as ocorrências:

Letra	**Número de vezes que aparece na frase**	**Letra**	**Número de vezes que aparece na frase**
t	18	l	4
a	16	j	4
r	13	n	3
q	9	i	3
s	8	o	3
u	6	e	3
m	6	d	1
f	6	p	1
k	5	x	1
c	5		

Como a frequência de letras em português segue a ordem A E O R S I N $\cdots$, muito provavelmente a letra t deve ser a codificação da letra A, pois é a mais frequente, assim como a letra a deve ser a codificação da letra E, que é a segunda mais frequente, mas isto, por enquanto, é só uma especulação.

Se substituirmos as letras t por A e a por E na mensagem criptografada, chegaremos a

> UrAklm Ar dqEpuEkcfAr lAr iEsqAr Ej nmqsuouEr lEcfdqE A jEkrAoEj AeAfxm E cmjniEsE A sAeEiA nAqA qEofrsqAq Ar ruersfsufcmEr EkcmksqAlAr.

Será que já conseguimos descobrir o que está escrito? Vamos analisar a terceira letra mais frequente; a letra r que aparece 13 vezes na frase. Ela pode estar codificando as seguintes letras: O ou R ou S.

Se r codificar O a mensagem fica:

> UOAklm AO dqEpuEkcfAO lAO iEsqAO Ej nmqsuouEO lEcfdqE A jEkOAoEj AeAfxm E cmjniEsE A sAeEiA nAqA qEofOsqAq AO OueOsfsufcmEO EkcmksqAlAO.

Se r codificar R a mensagem fica:

> URAklm AR dqEpuEkcfAR lAR iEsqAR Ej nmqsuouER lEcfdqE A jEkRAoEj AeAfxm E cmjniEsE A sAeEiA nAqA qEofRsqAq AR RueRsfsufcmER EkcmksqAlAR.

Se r codificar S a mensagem fica:

> USAklm AS dqEpuEkcfAS lAS iEsqAS Ej nmqsuouES lEcfdqE A jEkSAoEj AeAfxm E cmjniEsE A sAeEiA nAqA qEofSsqAq AS SueSsfsufcmES EkcmksqAlAS.

Das três opções acima a mais provável é a terceira, pois muitas palavras terminam em S.

A quarta letra a ser analisada é a letra q. Provavelmente ela é a codificação da letra O ou da letra R.

Se for da letra O, a mensagem fica:

> USAklm AS dOEpuEkcfAS lAS iEsOAS Ej nmOsuouES lEcfdOE A jEkSAoEj AeAfxm E cmjniEsE A sAeEiA **nAOA** OEofSsOAO AS SueSsfsufcmES EkcmksOAlAS.

(Observe a palavra nAOA em negrito, ela corresponde a alguma palavra em português?) É melhor ficar com a segunda opção em que a letra q corresponde à letra R:

> USAklm AS dREpuEkcfAS lAS iEsRAS **Ej** nmRsuouES lEcfdRE A jEkSAoEj AeAfxm E cmjniEsE A sAeEiA nARA REofSsRAR AS SueSsfsufcmES EkcmksRAlAS.

A palavra Ej em negrito é uma pista de que a letra j deve ser a codificação da letra m. Se for, a mensagem se transforma em:

> USAklm AS dREpuEkcfAS lAS iEsRAS EM nmRsuouES lEcfdRE A **MEkSAoEM** AeAfxm E cmMniEsE A sAeEiA nARA REofSsRAR AS SueSsfsufcmES EkcmksRAlAS.

A palavra MEkSAoEM deve ser a codificação de MENSAGEM. Logo a letra k corresponde à letra N e a letra o corresponde à letra G. Fazendo essas substituições:

> USANlm AS dREpuENcfAS lAS iEsRAS EM nmRsuGuES **lEcfdRE** A MENSAGEM AeAfxm E cmMniEsE A sAeEiA nARA **REGfSsRAR** AS SueSsfsufcmES ENcmNsRAlAS.

Podemos reconhecer as palavras em negrito: lEcfdRE deve ser DECIFRE e REGfSsRAR deve ser REGISTRAR. Se assim for, l é D, c é C mesmo, f é I, d é F e s é T. Fazendo estas substituições:

> USANDm AS FREpuENCIAS DAS iETRAS EM nmRTuGuES DECIFRE A MENSAGEM AeAIxm E CmMniETE A TAeEiA nARA REGISTRAR AS SueSTITuICmES ENCmNTRADAS.

É possível decifrar agora? Se você não conseguir, volte e releia o enunciado da atividade 8.

Se você achou trabalhoso decifrar a mensagem da Atividade acima, saiba que existem vários *softwares* que fazem esta tarefa brincando. Veja por exemplo os *sites*:

http://demonstrations.wolfram.com/CipherEncoder/

http://demonstrations.wolfram.com/LetterHighlightingInText/

Veja também a beleza do recurso criptográfico utilizado na poesia abaixo:

PULSAR

Poesia Concreta de Augusto de Campos

Variações

1) Uma maneira de encriptar mensagens consiste em escolher uma palavra-chave que deve ser mantida em segredo por quem as envia e por quem as recebe. Esta palavra não deve ter letras repetidas. Por exemplo, consideramos a palavra TECLADO. Para fazer a troca de letras, podemos usar a seguinte correspondência:

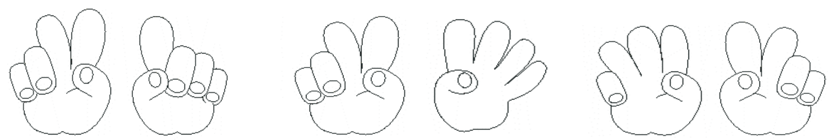
A	B	C	D	E	F	G	H	I	J	K	L	M	N
T	**E**	**C**	**L**	**A**	**D**	**O**	B	F	G	H	I	J	K

O	P	Q	R	S	T	U	V	W	X	Y	Z
M	N	P	Q	R	S	U	V	W	X	Y	Z

2) Outra maneira também inventada pelos gregos para codificar mensagens é feita trocando-se letras por números, de acordo com a seguinte tabela:

	1	**2**	**3**	**4**	**5**
1	**A**	**B**	**C**	**D**	**E**
2	**F**	**G**	**H**	**I**	**J**
3	**K**	**L**	**M**	**N**	**O**
4	**P**	**Q**	**R**	**S**	**T**
5	**U**	**V/W**	**X**	**Y**	**Z**

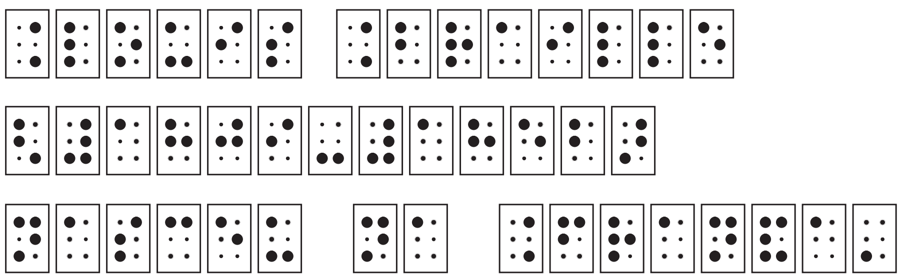
Por exemplo, a palavra LEGAL pode ser codificada como 32-15-22-11-32. Este código pode ser transmitido com as mãos: os dedos da mão direita indicam as linhas e os da esquerda as colunas. O que dizem as mãozinhas abaixo?



Capítulo 2

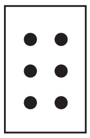
A Escrita Braille e o Código Binário – Introdução ao Estudo de Combinações

Você consegue ler a seguinte mensagem?



Trata-se de um texto escrito em Braille, um método de escrita desenvolvido para que pessoas com deficiências visuais possam ler pelo tato. Seu criador, Louis Braille, ficou cego aos três anos de idade devido a um ferimento no olho feito com um objeto pontiagudo que seu pai usava para fabricar selas de animais; o ferimento infeccionou e isto provocou também a perda da visão no outro olho, ocasionando sua deficiência visual total.

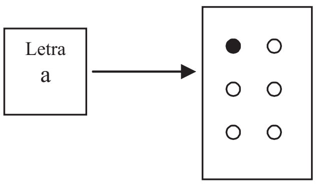
O código Braille é baseado em um arranjo 3×2 de pontos, dispostos como nas pedras de um dominó:



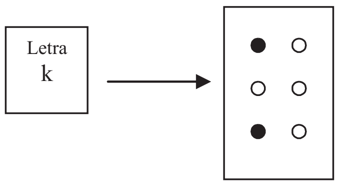
3×2
(Três linhas e duas colunas)

Para registrar uma dada letra do alfabeto, alguns desses 6 pontos são marcados ou perfurados, de modo a se tornarem sobressalentes, para que possam ser sentidos com as pontas dos dedos das mãos.

Neste texto, quando um ponto estiver marcado, usaremos um círculo negro e, quando não estiver, um círculo branco. 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 marcas pretas em dois pontos: o ponto da primeira linha e da primeira coluna e o ponto da terceira linha e primeira coluna.

Atividade 1:

a) Quantos diferentes padrões (disposições de pontos) podemos formar usando o sistema 3×2 descrito acima?

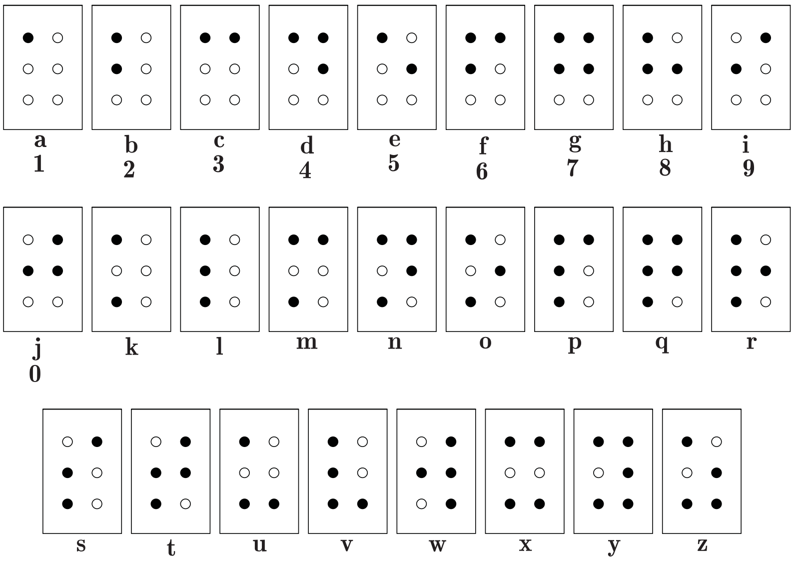
b) Se quisermos codificar

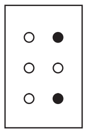
- todas as letras minúsculas;
- todas as letras maiúsculas;
- os algarismos: 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9;
- os sinais de pontuação: **.** (ponto final), **:** (dois pontos), **?** (ponto de interrogação), **!** (ponto de exclamação) e **,** (vírgula);
- os sinais de operações matemáticas: $+$, $\times$, $-$ e $\div$;

os padrões obtidos nas dimensões 3×2 serão suficientes?

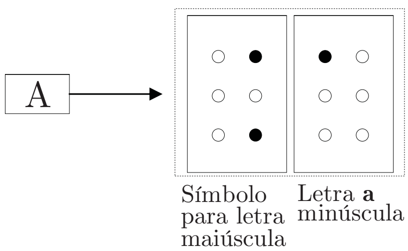
c) Quantos padrões podemos formar se dispusermos pontos arranjados em um quadrado 2×2? E em um retângulo 1×4? Porque será que eles não são usados?

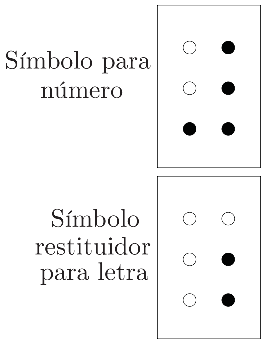
Eis aqui a maneira usual de codificar em Braille as letras minúsculas e os algarismos:



Para codificar letras maiúsculas, usamos o símbolo:  antes da letra que desejamos que seja maiúscula.

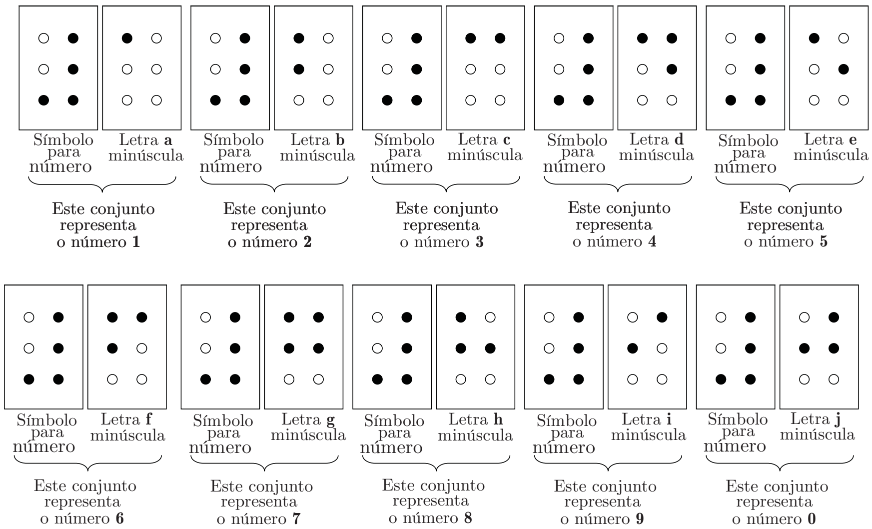
Por exemplo, a letra A (maiúscula) se escreve como:





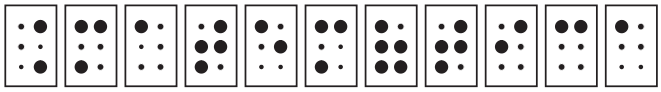
Observe também que a mesma configuração de pontos é usada ora para denotar algumas letras, ora para denotar os algarismos 1, 2, 3, 4, 5, 6, 7, 8, 9 e 0. A fim de evitar confusão, para representar os números, usa-se um símbolo inicial, antecedendo as 10 primeiras letras do alfabeto. Quando houver risco de confusão, para voltar novamente a usar o símbolo para significar letras, devemos antecedê-las com outro símbolo inicial, indicando a restauração, ou seja, indicando que os símbolos que virão serão novamente letras.

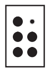
Veja como são as representações dos 10 algarismos:



Atividade 2:

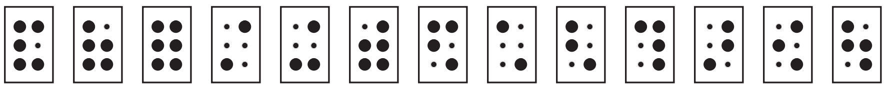
a) Traduza para a linguagem usual



O que você acha que  significa?

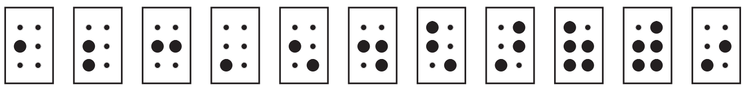
b) Escreva em Braille a frase: Louis Braille (1809-1852) nasceu na França. Não se esqueça de usar o símbolo para maiúsculas e o símbolo que transforma letras em números. Você já leu esta frase antes?

Você deve ter notado na atividade anterior que apenas letras e números não são suficientes para escrever todas as frases que desejamos. Na verdade existem muitos outros símbolos que são usados em Braille; eles também variam de país para país. Veja alguns exemplos típicos usados em português:



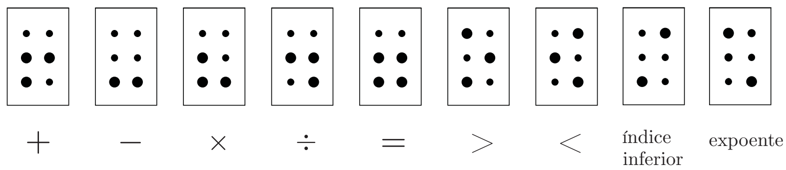
ç á é í ó ú à â ê ô ã õ ü

Todos os sinais gráficos têm representação em Braille. Veja alguns:



, ; : . ? ! ( ) [ ] *

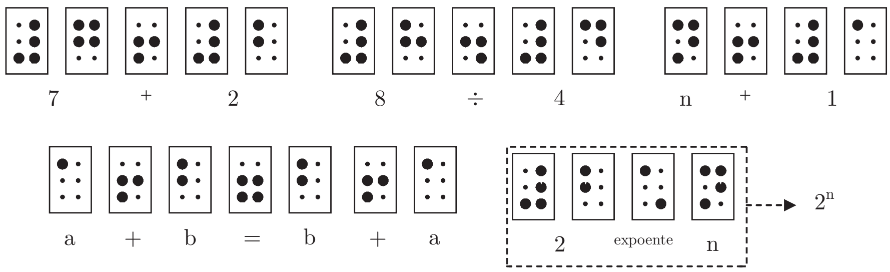
Veja também alguns símbolos usuais da Matemática:

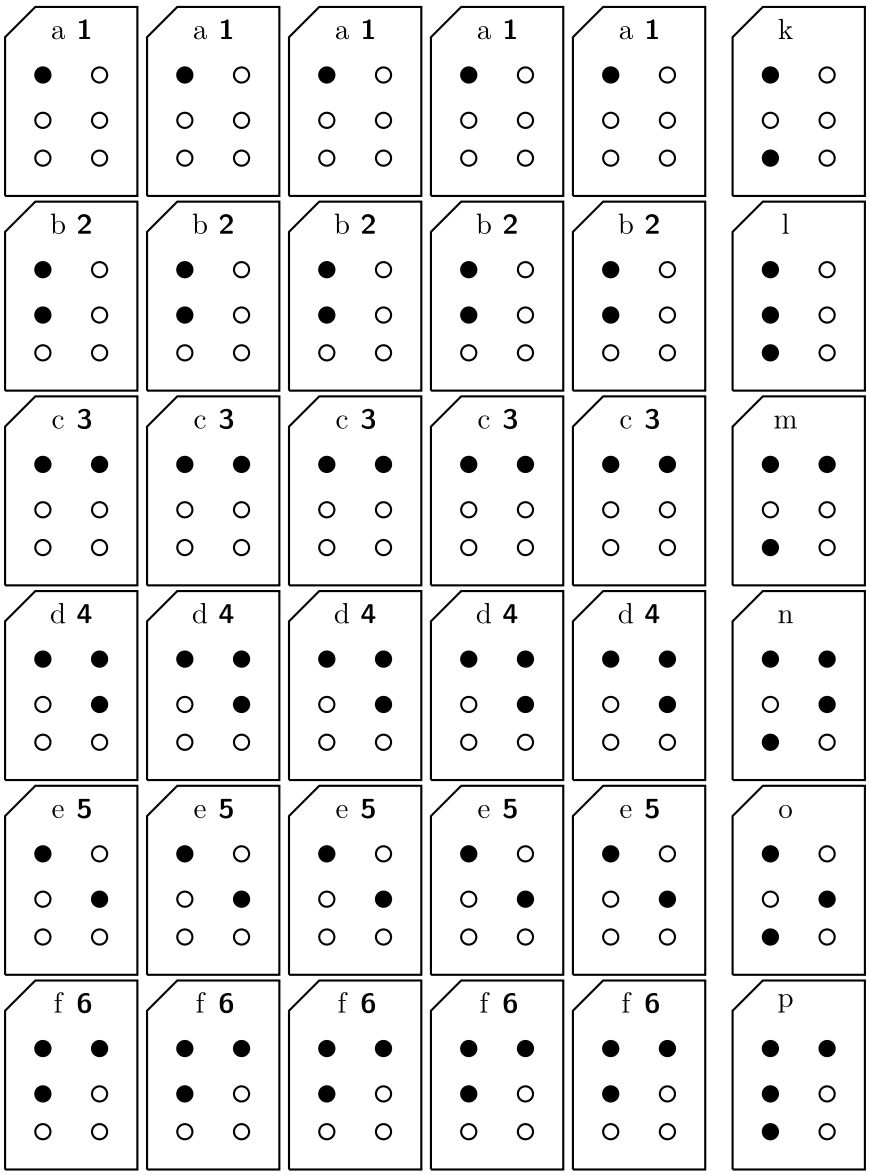


Para mais informações consulte o *site* do Instituto Benjamin Constant: http://www.ibc.gov.br/?catid=110&blogid=1&itemid=479

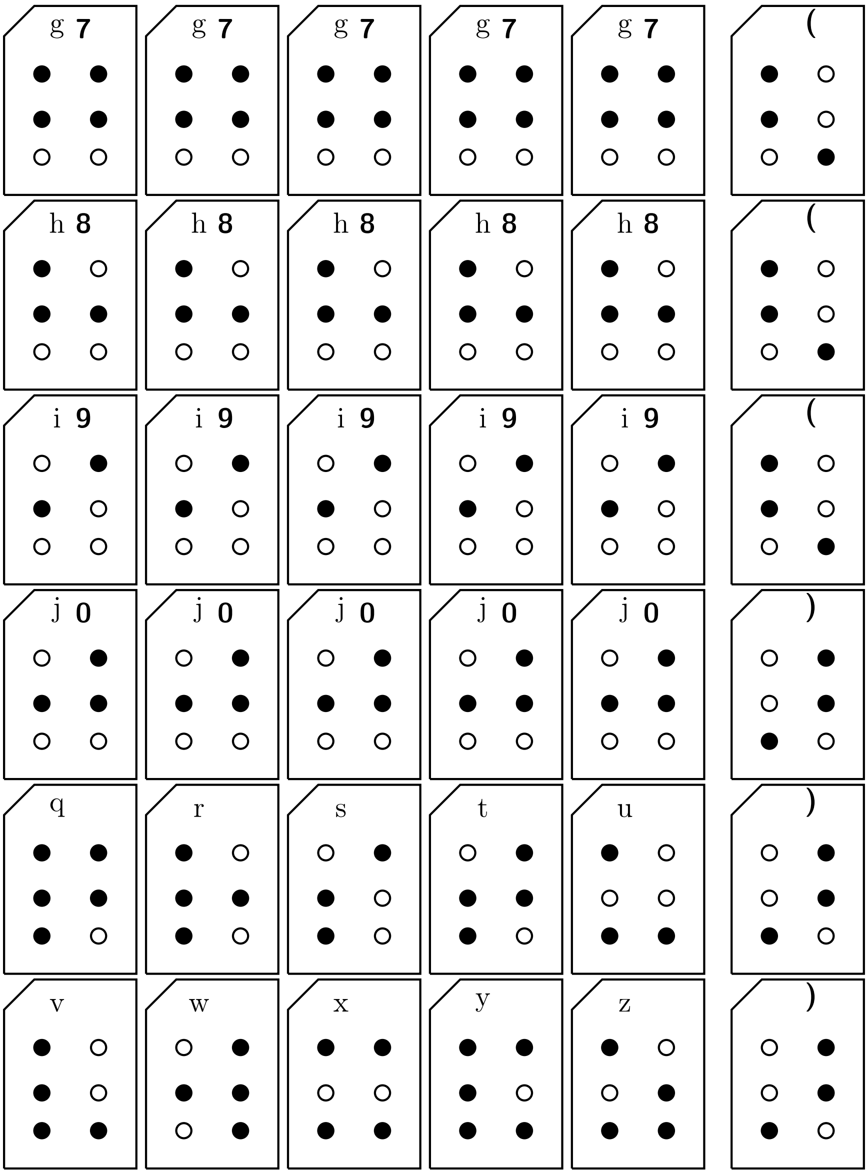
Atividade 3: Esta atividade tem o objetivo de simular a leitura em Braille de frases e fórmulas matemáticas feitas pelos deficientes visuais. Você deve recortar as fichas e perfurar os círculos marcados em preto com um furador de papel (um clipe ou um palito também podem ser usados).
Depois de recortadas monte com as fichas algumas expressões matemáticas para que um amigo consiga ler o que você escreveu, mas sem que ele as olhe!
Com as mãos, seu amigo deve sentir as perfurações de cada ficha e, a partir deste ponto, pode consultar a tabela da página 45 para descobrir o valor da letra ou número correspondente que está "lendo com suas mãos". Mas observe: ele não pode de modo algum ver diretamente a ficha que está manuseando.

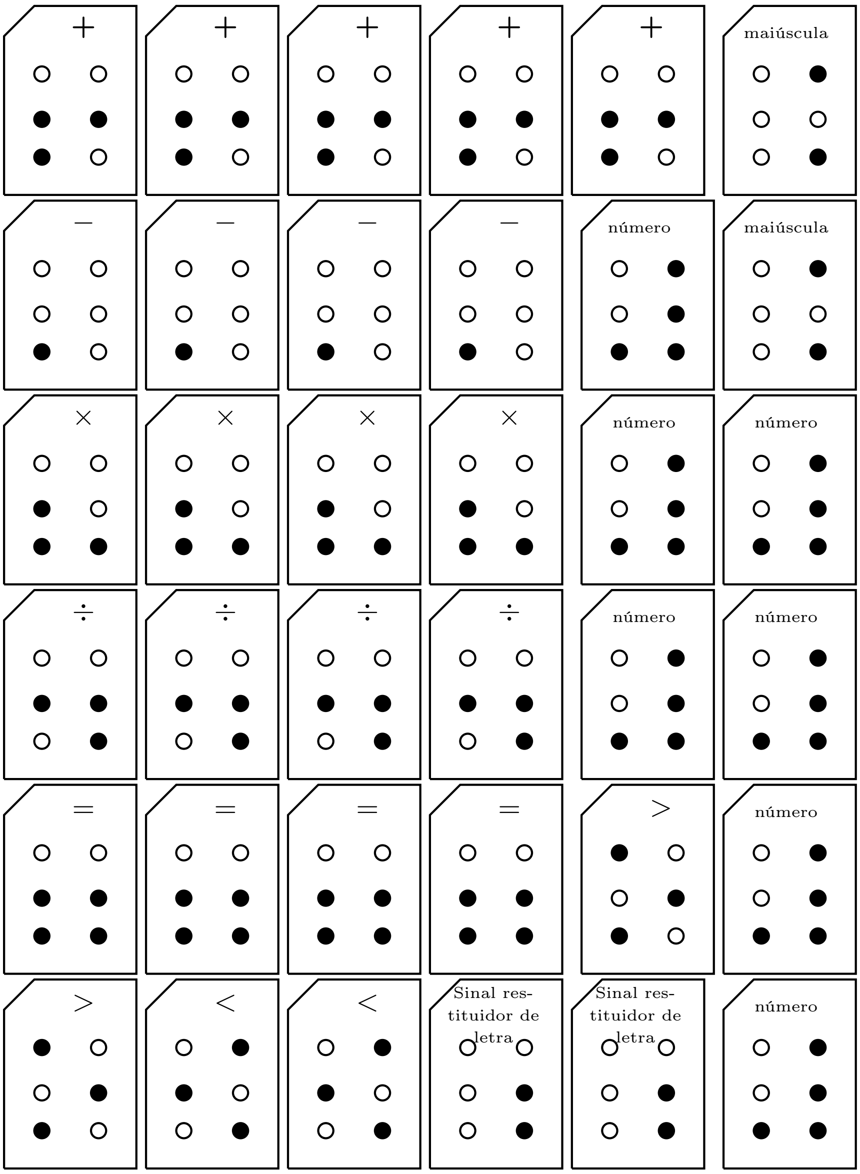
Veja alguns exemplos de expressões matemáticas em Braille:




a 1
a 1
a 1
a 1
a 1
k
b 2
b 2
b 2
b 2
b 2
l
c 3
c 3
c 3
c 3
c 3
m
d 4
d 4
d 4
d 4
d 4
n
e 5
e 5
e 5
e 5
e 5
o
f 6
f 6
f 6
f 6
f 6
p

“principal”
2010/4/20
page 40
Estilo OBME

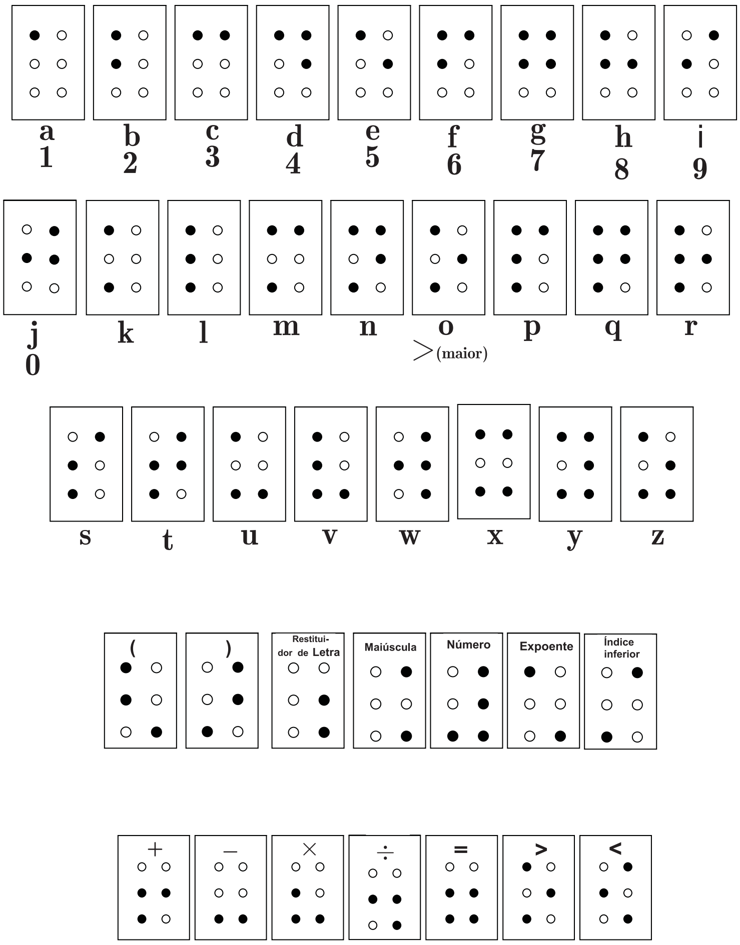

g 7 g 7 g 7 g 7 g 7 (
h 8 h 8 h 8 h 8 h 8 (
i 9 i 9 i 9 i 9 i 9 (
j 0 j 0 j 0 j 0 j 0)
q r s t u)
v w x y z)


+
+
+
+
+
maiúscula
−
−
−
−
número
maiúscula
×
×
×
×
número
número
÷
÷
÷
÷
número
número
=
=
=
=
>
número
>
<
<
Sinal restituidor de letra
Sinal restituidor de letra
número

"principal"
2010/4/20
page 44
Estilo OBME

Tabela para consulta:

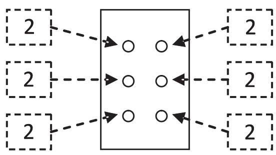
Letras e números em Braille



2.1 Explorando Conceitos Matemáticos com a Linguagem Braille

Existem $2^6 = 64$ configurações que podem ser obtidas no código de Braille usual 3×2. É fácil descobrir que isto é verdade, quando aplicamos o Princípio Multiplicativo da Contagem: há duas possibilidades para a primeira casa – ou ela é marcada ou não é (ou pintamos de preto ou de branco) – do mesmo modo há duas possibilidades para cada uma das outras casas, o que resulta em

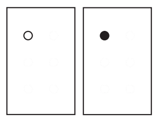
$$2 \times 2 \times 2 \times 2 \times 2 \times 2 = 2^6 \text{ possibilidades.}$$



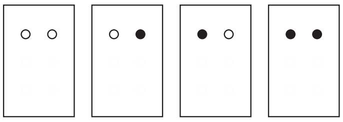
> **O Princípio Multiplicativo da Contagem:**
> Se uma decisão puder ser tomada de m maneiras diferentes e se, uma vez tomada esta primeira decisão, outra decisão puder ser tomada de n maneiras diferentes, então, no total serão tomadas $m \times n$ decisões.

Vale a pena explorar este exemplo com estratégias diferentes.

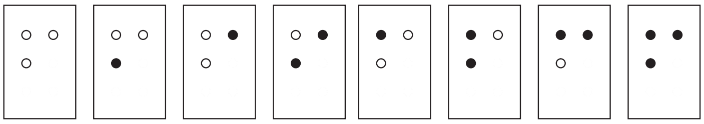
Método 1: Focando na quantidade de pontos, independente de estarem pintados ou não:

Começando com um só ponto, teremos só 2 possibilidades: 

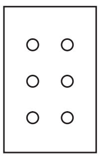
Com dois pontos há 4 possibilidades, pois há duas escolhas para cada uma das configurações já vistas anteriormente (com um ponto apenas):



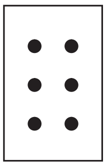
Já com três pontos há 8 possibilidades (duas para cada uma das configurações com dois pontos vistas acima):



Continuando assim, com quatro pontos teremos 16 configurações distintas, com cinco pontos 32 configurações e, é claro, com 6 pontos chegaremos a 64 padrões diferentes de pontos. Isto é fácil de entender: cada configuração em um estágio anterior produz duas novas configurações no estágio seguinte. Dentre as 64 possibilidades, temos dois casos extremos: um em que nenhum dos pontos é marcado e outro em que todos os seis pontos são marcados:



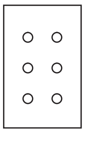
Em Braille, por motivos óbvios, esta configuração não é usada.



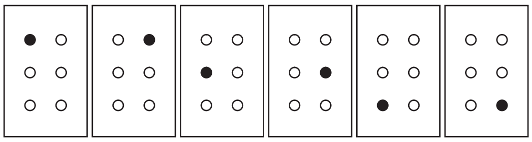
Na linguagem Braille, esta configuração tem a função de referencial de posição, para auxiliar na indicação de sinais gráficos tais como a crase ou o trema. É usada para indicar a letra "**é**" .

Método 2: Focando na quantidade pintada de pontos:

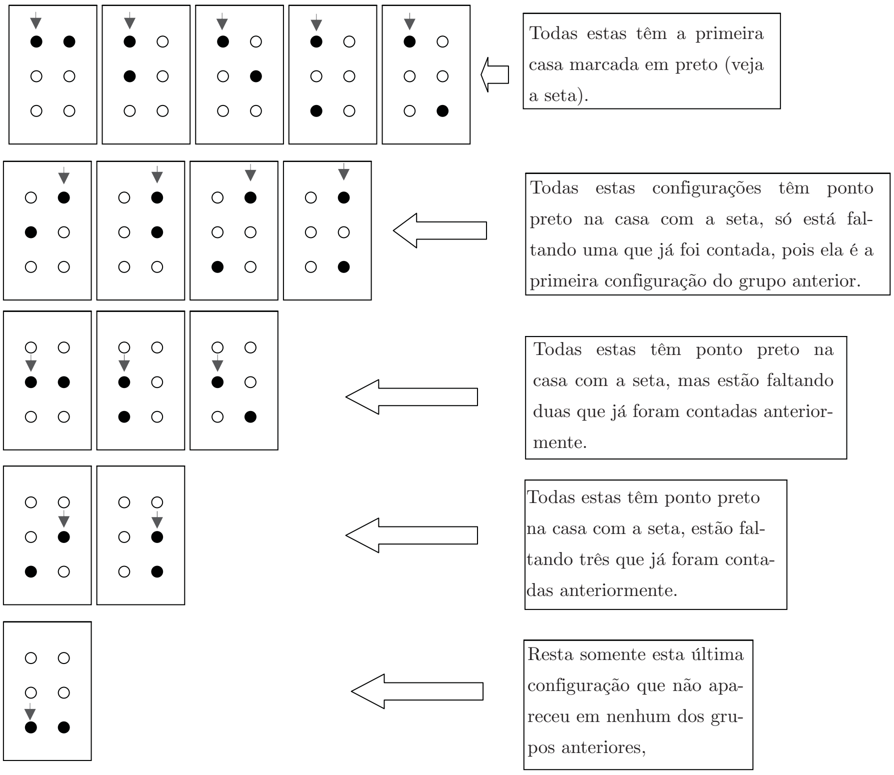
Com nenhum ponto marcado temos apenas uma configuração:



Com apenas um ponto marcado, temos 6 possibilidades:

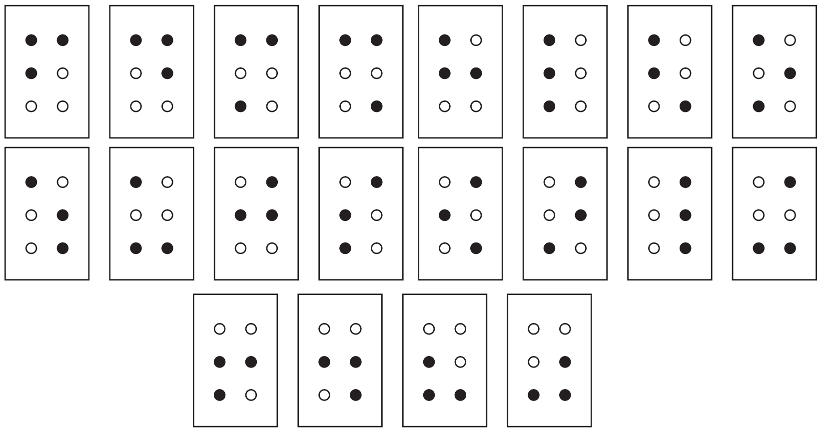


As configurações com dois pontos marcados totalizam 15. Veja:



Deste modo, com dois pontos pretos há $1 + 2 + 3 + 4 + 5 = 15$ possibilidades.

Com três pontos marcados em negro, há 20 possibilidades. Veja:



Poderíamos continuar agora exibindo todas as configurações com 4 pontos negros (são 15 ao todo), todas com 5 pontos pretos (são 6 no total) e todas com 6 pontos negros (apenas 1), mas não faremos isto porque há um belo argumento de simetria aqui:

- Escolher 4 pontos para marcar com preto entre 6 pontos brancos é o mesmo que escolher 2 pontos para marcar de branco entre 6 negros!
- De modo análogo, o número de escolhas de 5 pontos para pintá-los de preto dentre 6 pontos brancos é o mesmo número de escolhas de 1 único ponto para pintar de branco dentre 6 pontos negros.
- 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.

Resumidamente, temos:

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

SIMETRIA

Estes padrões são encontrados nas combinações, que passaremos a estudar.

2.2 Combinações Matemáticas

Existem situações envolvendo contagens em que a ordem dos elementos é importante e outras em que não. Para entender melhor este fato, vamos comparar os dois exemplos abaixo:

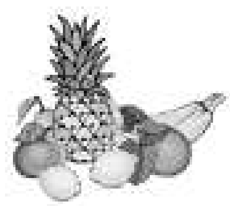
Exemplo 2.1. *De quantas maneiras diferentes podemos estacionar 3 carros em 2 garagens?*

Solução:

A resposta é muito simples, se pensarmos da seguinte maneira: existem 3 possibilidades para preencher a primeira garagem, mas apenas duas para a estacionarmos na segunda; pelo Princípio Multiplicativo, o número total de maneira 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.

Exemplo 2.2. *Quantas saladas de frutas diferentes podemos fazer usando duas das seguintes frutas: abacaxi, banana ou caqui?*

Solução:



Procedemos como antes: primeiro escolhemos umas das três frutas (3 possibilidades), depois a segunda e última fruta (2 possibilidades). Com isto teremos $3 \times 2 = 6$ possibilidades. Entretanto o número de saladas de frutas não é 6 e sim 3. Porquê?

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 feita com banana e abacaxi, ou seja $ab = ba$ e de modo semelhante, $ac = ca$ e $bc = cb$. O que é importante observar aqui é que quando duas frutas são permutadas, elas produzem a mesma salada. Neste caso a ordem de escolha das frutas não é importante e o número correto de saladas é

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

O número 2 no denominador corresponde à permutação de duas frutas. Ou seja, contamos tudo como se a ordem fosse importante e dividimos o resultado pelo número de permutações de 2 elementos.

Este último exemplo é o protótipo do que se chama em Matemática de uma **combinação simples**. Observe bem o que fizemos:

- Aplicamos o Princípio Multiplicativo para se obter todas as possibilidades, respeitando a ordem ($3 \times 2 = 6$).

- Dividimos o resultado obtido acima pelo número de permutações da quantidade previamente combinada que dá o tamanho de cada escolha (como combinamos fazer saladas com apenas 2 frutas, dividimos por $2! = 2$, obtendo $(3 \times 2)/2 = 3$).

No caso geral, se tivermos n objetos distintos à nossa disposição e tivermos que escolher p objetos distintos dentre esses, obteremos as combinações simples de n elementos tomados p a p. É claro que $p \leq n$.

O número total dessas combinações é denotado por C_n^p e é calculado da seguinte maneira:

$$C_n^p = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-(p-1))}{p \cdot (p-1) \cdot (p-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1}$$

ou, em notação fatorial:

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

(Você sabe justificar porque vale esta última fórmula?).

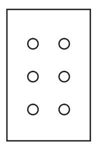
No exemplo das saladas de frutas, $n = 3$, $p = 2$ e o número de saladas de frutas é $C_3^2 = \frac{3!}{2!(3-2)!} = \frac{3 \cdot 2!}{2!1!} = 3$. Vejamos mais um exemplo:

Exemplo 2.3. *Quantos são os subconjuntos de $\{a, b, c, d, e\}$ que possuem exatamente três elementos?*

Solução: A resposta é $C_5^3 = \frac{5!}{3!(5-3)!} = \frac{5 \cdot 4 \cdot 3!}{3!2!} = 10$ pois a ordem dos elementos listados em um conjunto não é relevante. De fato os subconjuntos são os seguintes: $\{a, b, c\}$, $\{a, b, d\}$, $\{a, b, e\}$, $\{a, c, d\}$, $\{a, c, e\}$, $\{a, d, e\}$, $\{b, c, d\}$, $\{b, c, e\}$, $\{b, d, e\}$, $\{c, d, e\}$.

2.3 As Combinações e a Linguagem Braille

Podemos analisar agora todas as possibilidades da escrita Braille em uma célula 3×2:



Neste caso, o número de pontos que podemos combinar entre si é $n = 6$.

Número de pontos em preto	Quantidade de combinações distintas
$p = 0$	$C_6^0 = \dfrac{6!}{0!(6-0)!} = 1$
$p = 1$	$C_6^1 = \dfrac{6!}{1!(6-1)!} = 6$
$p = 2$	$C_6^2 = \dfrac{6!}{2!(6-2)!} = 15$
$p = 3$	$C_6^3 = \dfrac{6!}{3!(6-3)!} = 20$
$p = 4$	$C_6^4 = \dfrac{6!}{4!(6-4)!} = 15$
$p = 5$	$C_6^5 = \dfrac{6!}{5!(6-1)!} = 6$
$p = 6$	$C_6^6 = \dfrac{6!}{6!(6-6)!} = 1$

Podemos, a partir deste exemplo, inferir algumas conclusões:

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

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

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

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

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

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

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 de tomar n decisões e, cada uma delas, admite apenas duas possibilidades. Pelo Princípio Multiplicativo, existirão então

$$2 \times 2 \times \ldots \times 2 = 2^n \quad \text{decisões,}$$

e como cada decisão determina um e um só subconjunto, teremos que o número total de subconjuntos de $\{1, 2, \ldots, n\}$ é 2^n.

Atividade 4:

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

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

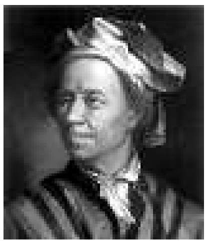
c) Em uma célula $n \times m$, quantas configurações diferentes podemos formar?

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

2.4 Matemáticos com Problemas Visuais

Eratóstenes (nasceu em 276 a.C. e faleceu em 194 a.C.) foi o diretor da Biblioteca de Alexandria e um homem de grande distinção em muitos ramos do conhecimento.

Em Matemática trabalhou com o problema da duplicação do volume do cubo, com números primos – o crivo de Eratóstenes até hoje é empregado na Teoria dos Números – e, surpreendentemente, calculou com precisão o raio da Terra, comparando sombras em duas diferentes cidades do Egito. Ele também calculou a distância entre o Sol e a Lua, usando medições durante eclipses e fez muitas descobertas em Geografia. Mesmo atuando em tantos ramos do conhecimento seu apelido era “Beta”, pois em cada área específica sempre havia um outro pensador cujo trabalho especializado tinha mais volume ou profundidade que o de Eratóstenes. Na velhice se tornou deficiente visual e conta-se que morreu de inanição, deixando voluntariamente de comer.



Leonhard Euler (1707-1783, lê-se “óiler”), foi um grande matemático do século XVIII, trabalhou em quase todos os ramos da Matemática: teoria dos números, equações diferenciais, cálculo das variações, fundamentos do Cálculo e Topologia – ramo da Geometria que foi fundador. Para Euler estes campos de pesquisa estavam intimamente conectados; seus trabalhos, eram tão criativos, que chegam a beirar a genialidade. Perdeu totalmente a visão de um olho em 1738, época em que uma catarata começou a se desenvolver no outro olho. Em 1771 uma operação malsucedida da catarata deixou-o com deficiência visual total. Apesar da cegueira, devido à sua notável memória, mais da metade de seu volumoso trabalho foi realizado depois que se tornou deficiente visual.

Joseph Plateau (1801-1883, lê-se "platô") era professor de uma escola secundária em Liège (França); durante o período que lecionava elaborou sua tese de doutorado sobre as impressões que a luz exerce no olho. Em 1829, realizou um experimento imprudente que consistia em olhar diretamente para a luz do sol, por isto seus olhos ficaram irritados durante anos e sua visão ficou restrita. Em 1841 sofreu uma infecção nos olhos e, em dois anos, perdeu completamente sua visão. Antes disto, porém, realizou experimentos para estudar as formas das bolhas de sabão, originando assim o estudo das superfícies mínimas em Geometria Diferencial. Sua velhice foi atípica: bem humorado, apesar dos problemas com a visão, seu estado físico e mental eram excelentes, sempre envolvido com ensino, em contato direto com estudantes.

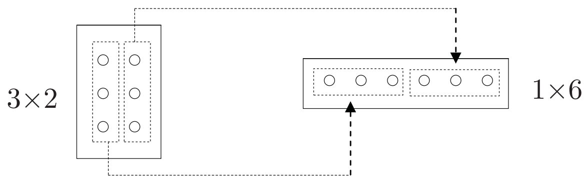
Lev Pontryagin (1908-1988), nasceu quando sua mãe Tatyana Pontryaguin tinha 29 anos de idade. Ela foi uma costureira e uma mulher notável que teve um importante papel na carreira matemática de seu filho. Com 14 anos de idade Pontryagin sofreu um acidente com uma explosão que o tornou deficiente visual total. Desta época em diante sua mãe assumiu completamente a responsabilidade de cuidar de todos os aspectos de sua vida. Apesar de grandes dificuldades, ela trabalhou por muitos anos como sua secretária, lendo artigos científicos em diversas línguas, escrevendo fórmulas em manuscritos, corrigindo trabalhos etc. Pontryagin foi um dos grandes matemáticos do século XX, foi chefe de departamento de Matemática na Rússia e vice-presidente da União Internacional de Matemática. Atuou em quase todas as áreas de Matemática, com destaque em Topologia, Álgebra, Equações Diferenciais, Teoria do Controle e Sistemas Dinâmicos.

Para maiores informações consulte o *site*:

http://turnbull.mcs.st-and.ac.uk/∼history/

2.5 O Sistema Binário

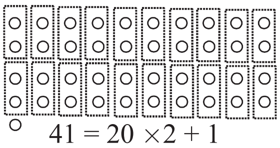
Vamos estudar agora o sistema em que as células possuem uma linha somente e 6 colunas. Ele será muito semelhante ao sistema usual da linguagem Braille 3×2, pois existe uma correspondência um-a-um entre as configurações com células 3×2 e configurações em células 1×6. Veja:



Sistemas do tipo $1 \times n$ servem para escrever números na base 2 e, assim sendo, têm muitas aplicações na Matemática e na Informática.

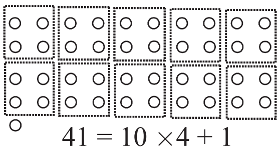
Podemos escrever qualquer número natural na base 2, utilizando-se para isto apenas os dígitos 0 e 1. Para compreender como isto pode ser realizado, trabalharemos, por simplicidade, com os números que vão de 0 a 63.

Dado um número qualquer (tomaremos como exemplo o número 41), veja como agrupar para escrever o número na base 2:



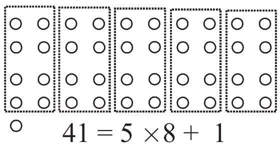
$41 = 20 \times 2 + 1$

Formamos 20 pares, observe que sobra uma unidade.



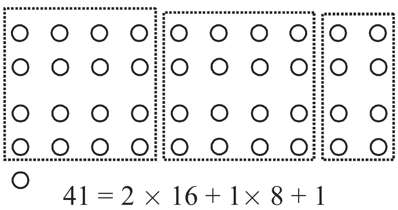
$41 = 10 \times 4 + 1$

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



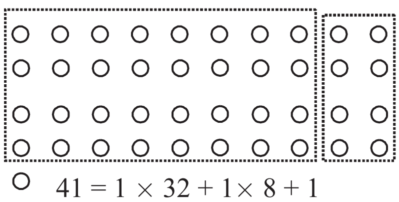
$41 = 5 \times 8 + 1$

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 dois 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.

Conclusão:

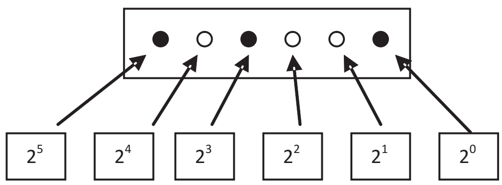
$$\mathbf{41} = \mathbf{1} \times \mathbf{2}^5 + \mathbf{0} \times \mathbf{2^4} + \mathbf{1} \times \mathbf{2^3} + \mathbf{0} \times \mathbf{2^2} + \mathbf{0} \times \mathbf{2^1} + \mathbf{1} \times \mathbf{2^0}\,.$$

Esta expressão é escrita abreviadamente na seguinte forma:

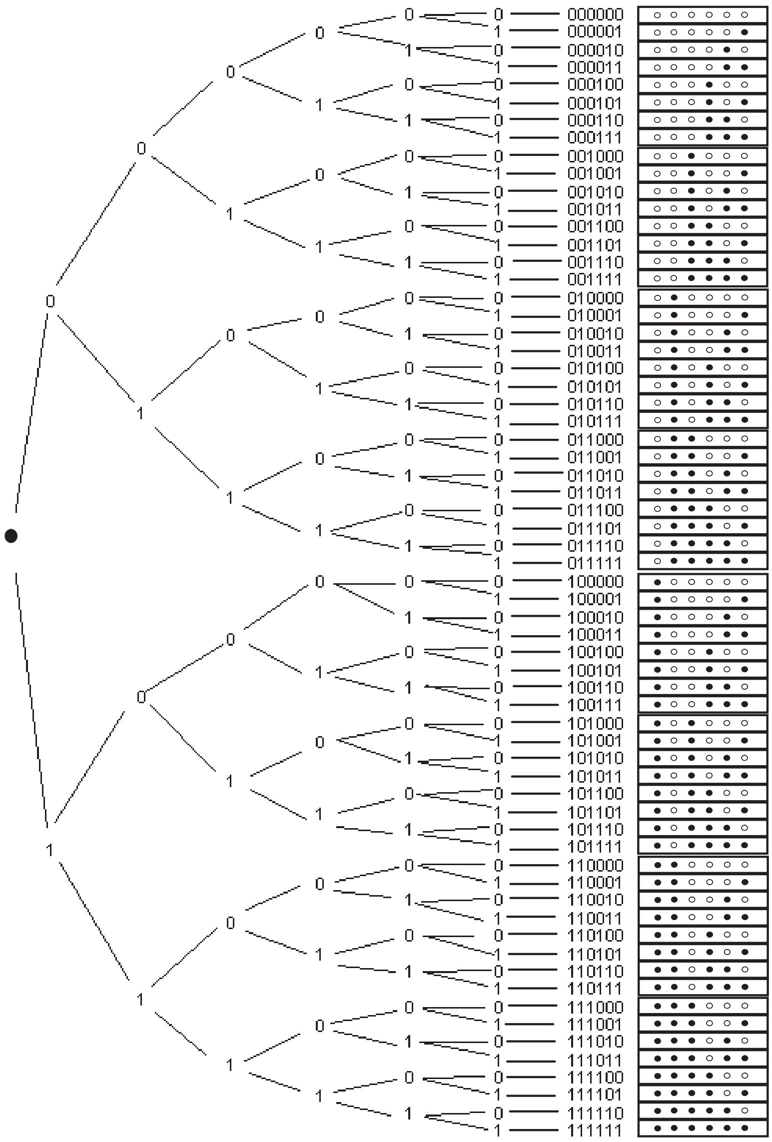
$$41 = (\mathbf{1\ 0\ 1\ 0\ 0\ 1})_2$$

(lê-se: 41 é um, zero, um, zero, zero, um, na base 2).

Veja como representá-lo no estilo Braille:



Os números de 0 a 63 podem ser representados na base 2, de acordo com o seguinte diagrama de árvore:


000000
000001
000010
000011
000100
000101
000110
000111
001000
001001
001010
001011
001100
001101
001110
001111
010000
010001
010010
010011
010100
010101
010110
010111
011000
011001
011010
011011
011100
011101
011110
011111
100000
100001
100010
100011
100100
100101
100110
100111
101000
101001
101010
101011
101100
101101
101110
101111
110000
110001
110010
110011
110100
110101
110110
110111
111000
111001
111010
111011
111100
111101
111110
111111

Atividade 5: Resolva o seguinte problema (OBMEP 2007)

3ª OLIMPÍADA BRASILEIRA DE MATEMÁTICA DAS ESCOLAS PÚBLICAS
OBMEP 2007
Somando novos talentos para o Brasil

Fernando e Isaura inventaram um jogo diferente, cujas regras são as seguintes:

1. eles começam uma partida com 128 palitos cada um;
2. em cada jogada, eles tiram par ou ímpar; se sai par, Fernando dá metade dos palitos que tem para Isaura e, se sai ímpar, Isaura dá a metade dos palitos que tem para Fernando.
3. eles repetem o procedimento da regra 2 até que um deles fique com um número ímpar de palitos, quando a partida acaba. Ganha quem ficar com maior número de palitos.

Veja o que acontece em uma partida onde a sequência das três primeiras jogadas é **par**, **ímpar**, **par**:

Fernando	Isaura		Fernando	Isaura		Fernando	Isaura		Fernando	Isaura	
128	128	**par** → 1ª jogada	64	192	**ímpar** → 2ª jogada	160	96	**par** → 3ª jogada	80	176	...

(a) Complete o esquema com o número de palitos de Fernando e Isaura, de acordo com as jogadas indicadas.

Fernando	Isaura		Fernando	Isaura		Fernando	Isaura		Fernando	Isaura	
128	128	**ímpar** → 1ª jogada			**ímpar** → 2ª jogada			**par** → 3ª jogada			...

(b) Uma partida acabou quando Fernando ficou com 101 palitos. Na última jogada saiu par ou ímpar?

(c) Qual foi a sequência de pares e ímpares da partida que acabou quando Fernando ficou com 101 palitos?

(d) Mostre que qualquer partida acaba com exatamente sete jogadas.

Atividade 6: Um pequeno computador de papel – os cartões binários

Vamos utilizar cartões de cartolina perfurados para trabalhar com números de 0 a 31, utilizando-se a base 2. Esses números podem ser escritos com apenas 5 dígitos, observe:

Base 10	Base 2	Base 10	Base 2	Base 10	Base 2	Base 10	Base 2
0	00000	8	01000	16	10000	24	11000
1	00001	9	01001	17	10001	25	11001
2	00010	10	01010	18	10010	26	11010
3	00011	11	01011	19	10011	27	11011
4	00100	12	01100	20	10100	28	11100
5	00101	13	01101	21	10101	29	11101
6	00110	14	01110	22	10110	30	11110
7	00111	15	01111	23	10111	31	11111

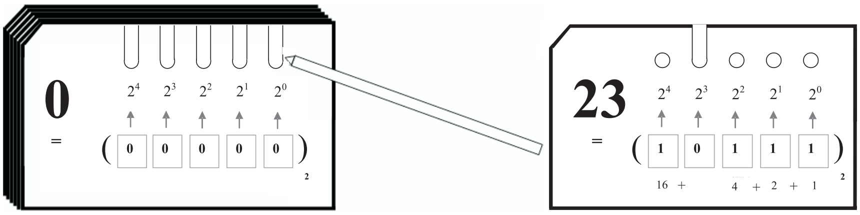
a) Recorte, perfure e corte as fendas dos cartões das páginas seguintes.

b) Cada buraco representará o número 1 e cada fenda o número 0. Faça um maço com as cartas. Se você colocar um palito (um canudo ou um clipe) por alguns dos buracos do maço, e levantá-lo, algumas cartas cairão e outras ficarão presas no palito. Repetindo organizadamente este procedimento você poderá realizar várias operações com os números binários de 0 a 31. Veja algumas delas:

- Separar as cartas pares da ímpares. Basta colocar o palito no primeiro furo à direita e levantar. Todas os cartões com números pares cairão.

- Com somente 5 colocações de palitos e levantamentos é possível colocar as cartas de 0 a 31 em ordem crescente. Embaralhe as cartas. Comece colocando o palito no primeiro buraco da direita (casa das unidades). Com cuidado levante o maço, deixando que as cartas caiam, mas mantendo a ordem. Coloque as cartas que caíram na frente das demais e repita o mesmo procedimento para todos os demais 4 buracos, sempre mantendo a ordem. Quanto terminar as cartas estarão em ordem.

- Pode-se localizar qualquer número de 0 a 31 com a colocação do palito e levantamento do maço 5 vezes. Isto se deve ao fato de que qualquer número natural tem representação única na base 2. Veja como você pode fazer para localizar a carta 23:



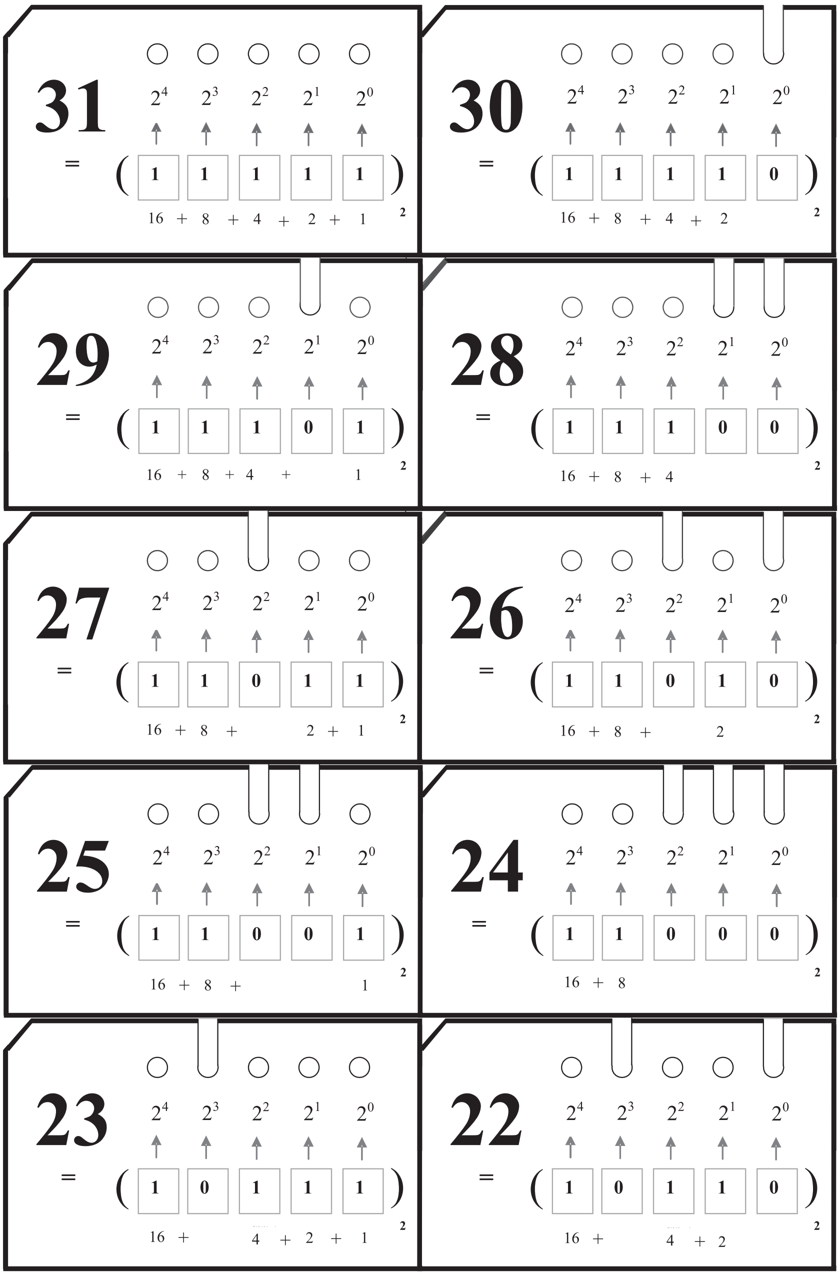
Coloque o palito na casa das unidades e levante o maço, descarte as que caíram. A seguir coloque no buraco 2^1, levante e descarte as que caíram. Prossiga, colocando o palito na casa 2^2, descarte as que caíram. Coloque na casa 2^3, levante e descarte as que ficaram presas. Agrupe as cartas que caíram e mais uma vez use o palito na casa 2^4, levantando o maço. A carta que ficou presa é a 23.

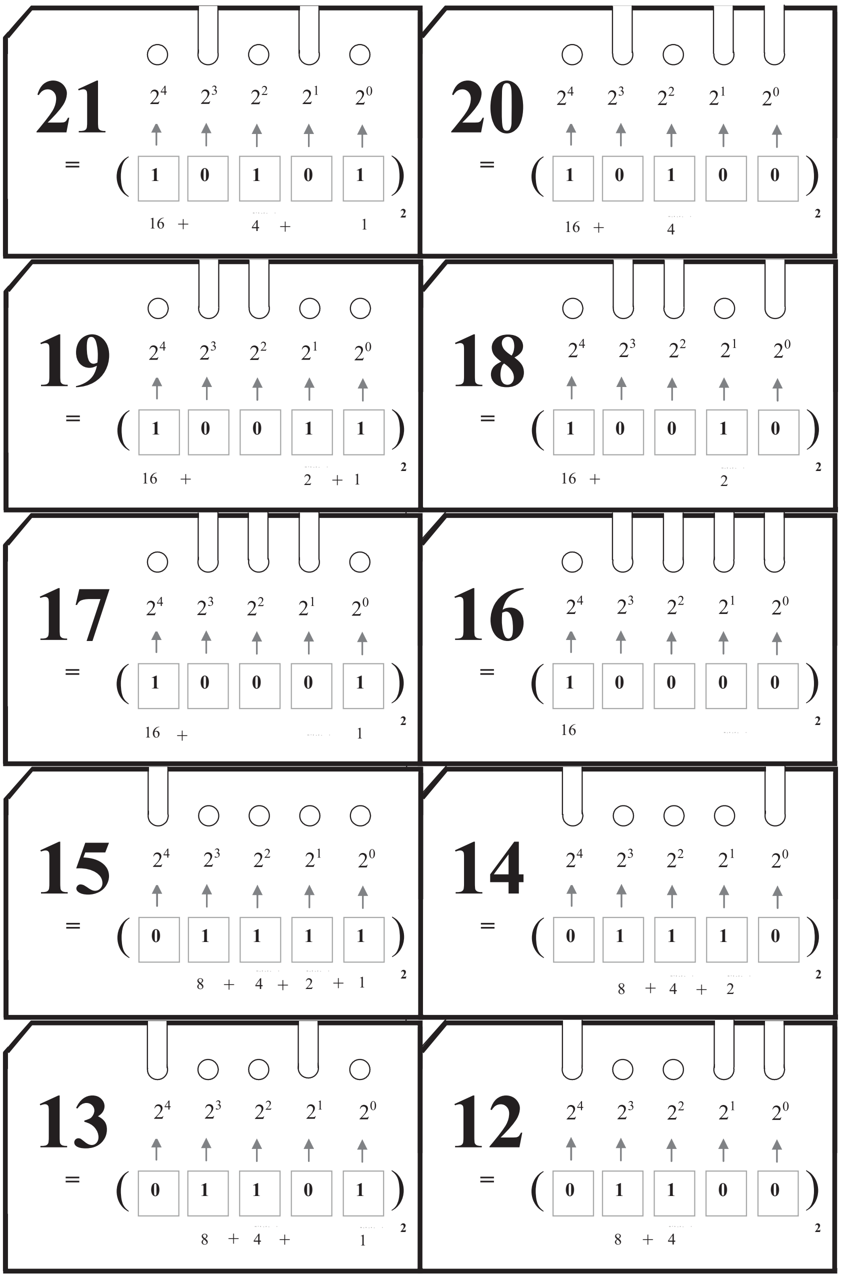
Responda:

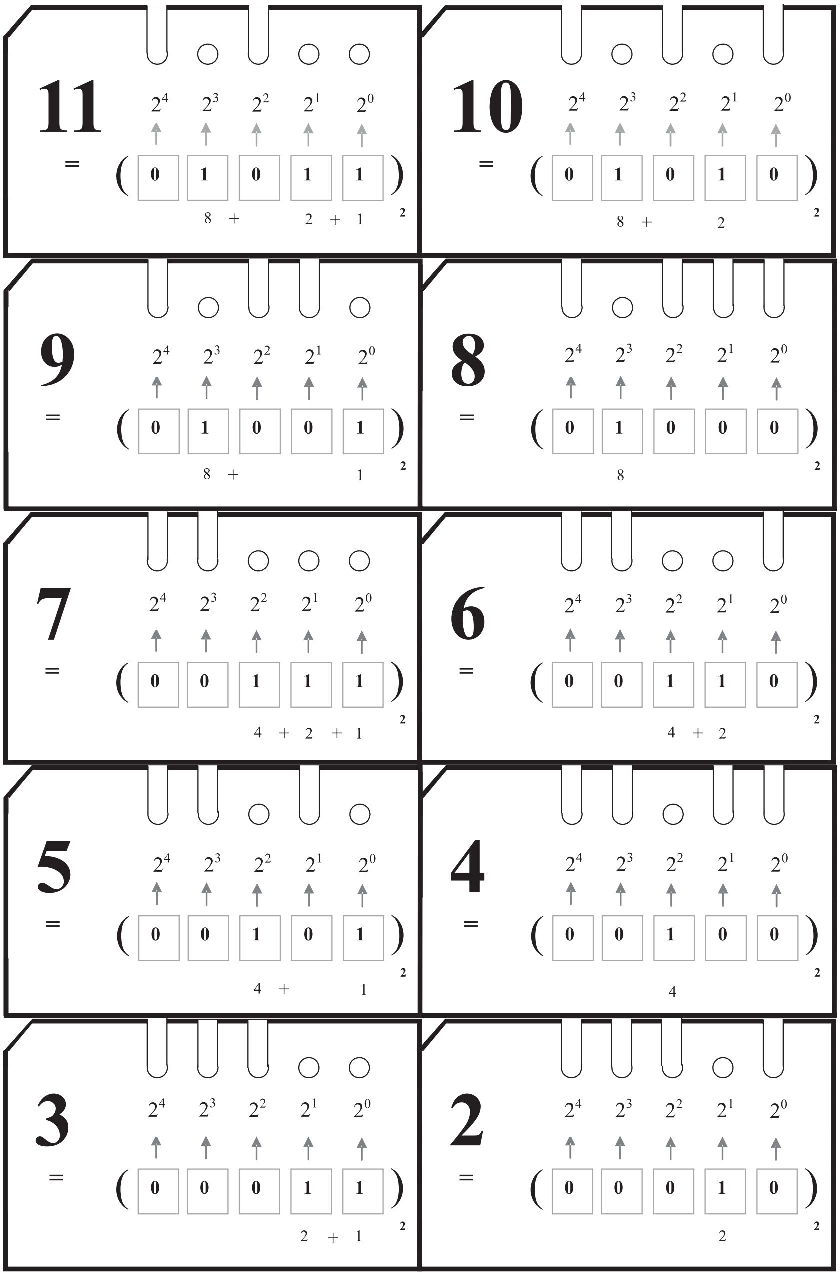
1. Se fizermos cartas com 6 buracos ao invés de 5, quantos números diferentes obteremos?

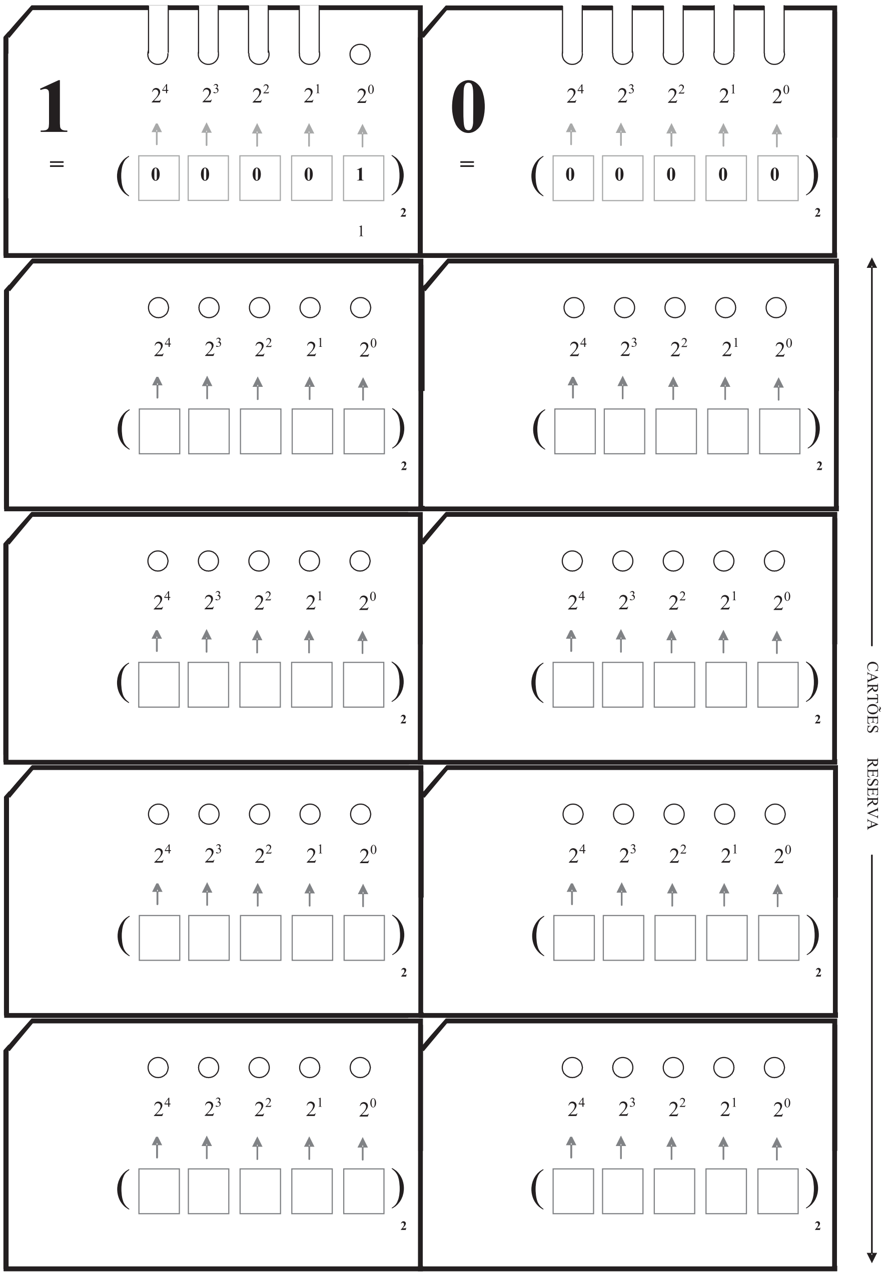
2. Qual é o número mínimo de buracos que teremos de fazer nos cartões para representar os números de 0 até 127?

3. Leia a próxima atividade "O dia do aniversário" na página 73 e descreva uma maneira de adivinhar o aniversário de uma pessoa usando os cartões perfurados que você fabricou.


31
2⁴ 2³ 2² 2¹ 2⁰
= (1 1 1 1 1)₂
16 + 8 + 4 + 2 + 1
30
2⁴ 2³ 2² 2¹ 2⁰
= (1 1 1 1 0)₂
16 + 8 + 4 + 2
29
2⁴ 2³ 2² 2¹ 2⁰
= (1 1 1 0 1)₂
16 + 8 + 4 + 1
28
2⁴ 2³ 2² 2¹ 2⁰
= (1 1 1 0 0)₂
16 + 8 + 4
27
2⁴ 2³ 2² 2¹ 2⁰
= (1 1 0 1 1)₂
16 + 8 + 2 + 1
26
2⁴ 2³ 2² 2¹ 2⁰
= (1 1 0 1 0)₂
16 + 8 + 2
25
2⁴ 2³ 2² 2¹ 2⁰
= (1 1 0 0 1)₂
16 + 8 + 1
24
2⁴ 2³ 2² 2¹ 2⁰
= (1 1 0 0 0)₂
16 + 8
23
2⁴ 2³ 2² 2¹ 2⁰
= (1 0 1 1 1)₂
16 + 4 + 2 + 1
22
2⁴ 2³ 2² 2¹ 2⁰
= (1 0 1 1 0)₂
16 + 4 + 2


21 = $(10101)_2$
16 + 4 + 1
20 = $(10100)_2$
16 + 4
19 = $(10011)_2$
16 + 2 + 1
18 = $(10010)_2$
16 + 2
17 = $(10001)_2$
16 + 1
16 = $(10000)_2$
16
15 = $(01111)_2$
8 + 4 + 2 + 1
14 = $(01110)_2$
8 + 4 + 2
13 = $(01101)_2$
8 + 4 + 1
12 = $(01100)_2$
8 + 4
2^4 2^3 2^2 2^1 2^0


11 = $(01011)_2$ = 8 + 2 + 1
10 = $(01010)_2$ = 8 + 2
9 = $(01001)_2$ = 8 + 1
8 = $(01000)_2$ = 8
7 = $(00111)_2$ = 4 + 2 + 1
6 = $(00110)_2$ = 4 + 2
5 = $(00101)_2$ = 4 + 1
4 = $(00100)_2$ = 4
3 = $(00011)_2$ = 2 + 1
2 = $(00010)_2$ = 2
2^4 2^3 2^2 2^1 2^0


1
=
2^4 2^3 2^2 2^1 2^0
(0 0 0 0 1)
2
1
0
=
2^4 2^3 2^2 2^1 2^0
(0 0 0 0 0)
2
2^4 2^3 2^2 2^1 2^0
2
CARTÕES RESERVA

"principal"
2010/4/20
page 72
Estilo OBME

Atividade 6: O dia de aniversário

Mágica Matemática

Para adivinhar o dia que uma pessoa nasceu

Um sim um não

dom	seg	ter	qua	qui	sex	sab
			$\underline{1}$	2	$\underline{3}$	4
$\underline{5}$	6	$\underline{7}$	8	$\underline{9}$	10	$\underline{11}$
12	$\underline{13}$	14	$\underline{15}$	16	$\underline{17}$	18
$\underline{19}$	20	$\underline{21}$	22	$\underline{23}$	24	$\underline{25}$
26	$\underline{27}$	28	$\underline{29}$	30	$\underline{31}$	

De dois em dois

dom	seg	ter	qua	qui	sex	sab
			1	$\underline{2}$	$\underline{3}$	4
5	$\underline{6}$	$\underline{7}$	8	9	$\underline{10}$	$\underline{11}$
12	13	$\underline{14}$	$\underline{15}$	16	17	$\underline{18}$
$\underline{19}$	20	21	$\underline{22}$	$\underline{23}$	24	25
$\underline{26}$	$\underline{27}$	28	29	$\underline{30}$	$\underline{31}$	

De quatro em quatro

dom	seg	ter	qua	qui	sex	sab
			1	2	3	$\underline{4}$
$\underline{5}$	$\underline{6}$	$\underline{7}$	8	9	10	11
$\underline{12}$	$\underline{13}$	$\underline{14}$	$\underline{15}$	16	17	18
19	$\underline{20}$	$\underline{21}$	$\underline{22}$	$\underline{23}$	24	25
26	27	$\underline{28}$	$\underline{29}$	$\underline{30}$	$\underline{31}$	

De oito em oito

dom	seg	ter	qua	qui	sex	sab
			1	2	3	4
5	6	7	$\underline{8}$	$\underline{9}$	$\underline{10}$	$\underline{11}$
$\underline{12}$	$\underline{13}$	$\underline{14}$	$\underline{15}$	16	17	18
19	20	21	22	23	$\underline{24}$	$\underline{25}$
$\underline{26}$	$\underline{27}$	$\underline{28}$	$\underline{29}$	$\underline{30}$	$\underline{31}$	

Meio mês sim meio não

dom	seg	ter	qua	qui	sex	sab
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	$\underline{16}$	$\underline{17}$	$\underline{18}$
$\underline{19}$	$\underline{20}$	$\underline{21}$	$\underline{22}$	$\underline{23}$	$\underline{24}$	$\underline{25}$
$\underline{26}$	$\underline{27}$	$\underline{28}$	$\underline{29}$	$\underline{30}$	$\underline{31}$	

Como funciona o truque:

Como adivinhar o dia em que uma pessoa nasceu:

1. Peça à pessoa que indique em quais dos calendários a data de seu nascimento aparece sublinhada.
2. Some os **primeiros** números sublinhados que aparecem nos calendários que a pessoa escolheu e você descobrirá a data de seu aniversário, sem que ela lhe conte.

Por exemplo: Se a pessoa nasceu no dia 7, os calendários em que este número aparece sublinhado são: o primeiro, o segundo e o terceiro. Somando os **primeiros números sublinhados** destes três calendários teremos $\mathbf{1 + 2 + 4 = 7}$. Não é legal? Se você seguir o roteiro abaixo, poderá descobrir o mês em que a pessoa nasceu.

Como adivinhar o mês em que uma pessoa nasceu – consulte seu horóscopo para encontrar o mês de nascimento:

Áries 21 de março a 20 de abril

Hoje é um dia muito favorável para lidar com cálculos matemáticos. Abra sua mente para a beleza da Matemática e não deixe de acreditar no seu potencial criativo. Você nasceu no dia ...

Touro 21 de abril a 20 de maio

Um ciclo de novas ideias se abre para você. Tudo se alterna tal qual uma função trigonométrica. É tempo de estudar e desenvolver os seus potenciais criativos. Você nasceu no dia...

Gêmeos 21 de maio a 20 de junho

Hoje é um dia em que muitas coisas não caminham muito de acordo com seus planos, mas lembre-se que problemas devem estar nos livros de Matemática e mesmo assim eles podem ser solucionados! Você nasceu no dia ...

Câncer 21 de junho a 21 de julho

Alegre-se! Hoje é um dia harmonioso para você interagir, fazer novas amizades e dar início a projetos pessoais como o estudo da Matemática. Você nasceu no dia ...

Leão 22 de julho a 22 de agosto

Problemas existem, mas com disposição, talento e criatividade você vence qualquer obstáculo. Quando estudar Matemática, não desista, a solução sempre estará a seu alcance. Você nasceu no dia ...

Virgem 23 de agosto a 22 de setembro

Hoje é um dia de muita sensibilidade e pensamento positivo. Realize hoje mesmo seus sonhos, estudando Matemática com dedicação. Acredite no seu potencial. Você nasceu no dia ...

Libra 23 de setembro a 22 de outubro

Hoje é um dia favorável para lidar com os assuntos da Geometria. Comece investindo no seu visual e surpreenda a todos, principalmente seu professor, fazendo todos os exercícios de Matemática. Você nasceu no dia ...

Escorpião 23 de outubro a 21 de novembro

É bem provável que o que você esteja procurando externamente esteja dentro de você, por isto, resolva você mesmo seus problemas de Matemática, sem procurar ajuda. Você consegue! Você nasceu no dia ...

Sagitário 22 de novembro a 21 de dezembro

Descubra seu potencial criativo, resolvendo problemas de Matemática. Com isso estará afastando a rotina e admirando a beleza desta ciência. Observe o mundo com os olhos da razão! Você nasceu no dia ...

Capricórnio 22 de dezembro a 20 de janeiro

Não se aborreça com pequenos atritos do dia a dia. Não se deixe abalar quando não encontrar imediatamente a solução de um problema de Matemática. Não desista e entenda que há propósitos maiores cujas portas serão abertas pela dedicação e estudo. Você nasceu no dia ...

Aquário 21 de janeiro a 19 de fevereiro

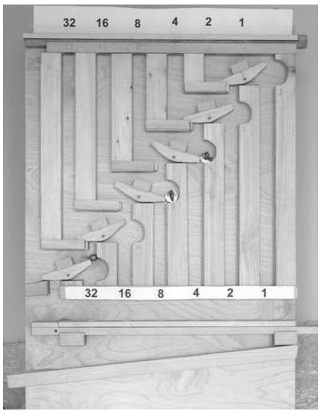
Hoje a vida lhe dará tudo para ser feliz. Há tesouros que temos e muitas vezes não os percebemos; por exemplo, há uma satisfação enorme quando resolvemos um belo problema de Matemática. Você nasceu no dia ...

Peixes 20 de fevereiro a 20 de março

Hoje é um dia de oportunidades e novidades, principalmente nos estudos. Você irá resolver com facilidade todos os problemas de Matemática que lhe forem apresentados. É tempo de fazer planos, trabalhar as ideias criativas e executá-las. Você nasceu no dia...

Podemos implementar todas as operações que são realizadas na base 10 também na base 2. Existem máquinas simples que ajudam a entender como estas operações são feitas. Uma delas está indicada abaixo.

A foto ao lado mostra uma máquina que efetua adições no sistema binário com bolinhas de gude. Para ver o funcionamento da máquina consulte o *site*:
http://www.youtube.com/watch?v=GcDshWmhF4A&NR=1



Bons estudos! Bom divertimento!