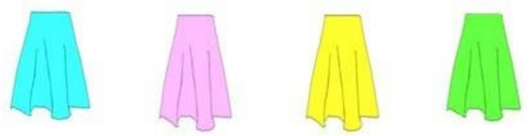
Matemática Discreta

Thales Azevedo Silva – 20172014040005

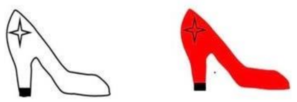
- **Princípio fundamental da contagem –PFC**

A análise combinatória é utilizada para resolver problemas de contagem. Utilizando os processos combinatórios é possível determinar o número de combinações, arranjos e permutações possíveis. Para cada uma destas aplicações, alguns critérios devem ser respeitados.
Resumindo, serve para calcular de quantas maneiras diferentes as coisas podem acontecer!

Como funciona?
Devemos usar operadores lógicos “E” (multiplicação) e “OU” (soma). Atenção: Dado um problema, você terá que identificar se a questão deverá ser solucionada fazendo o uso de "E", ou "OU"
Exemplo 1:
Jeniffer irá participar da promoção de uma loja de roupas que está dando um vale compras no valor de R$ 1000,00 reais. Ganhará o desafio o primeiro participante que conseguir fazer o maior número de combinações como kit de roupa cedido pela loja. No kit temos: seis camisetas, quatro saias e dois pares de sapato do tipo salto alto. De quantas maneiras distintas Jeniffer poderá combinar todo o vestuário que está no quite de roupa?

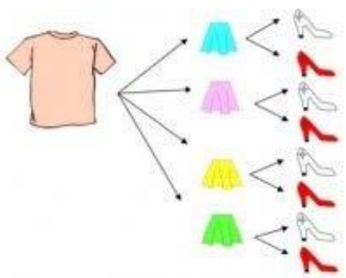


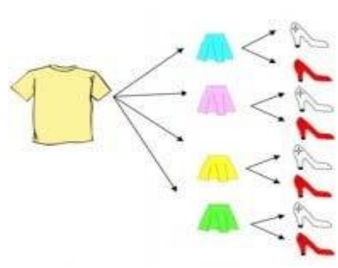
6
camisetas 4 Saias



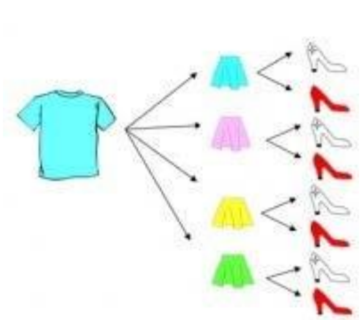
2 Sapatos

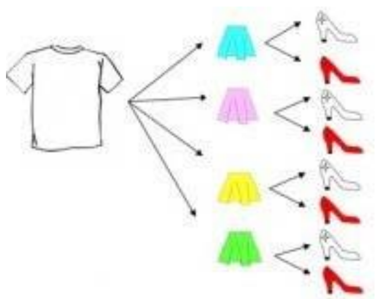
A forma que temos para resolver este problema é utilizando o Princípio Fundamental da Contagem.





8 combinações possíveis. 8 combinações possíveis.



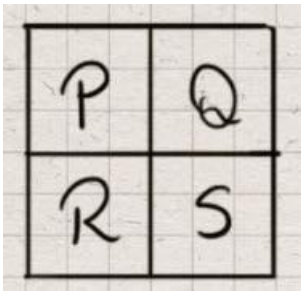


8 combinações possíveis. 8 combinações possíveis.

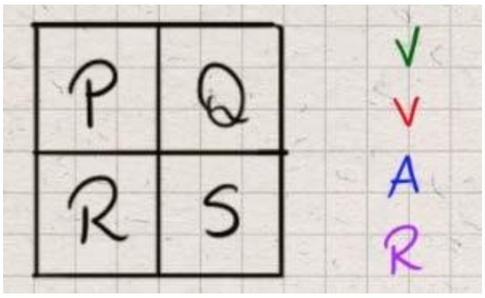
Total de camisetas x Total de Saias x Total Sapatos = Total de combinações possíveis 6 x 4 x 2 =48
Resultado do exemplo 1

Ao realizar a contagem iremos constatar a quantidade referente à 48 combinações possíveis.
Exemplo 2:
Dispondo de 4 cores para colorir o mapa da figura com os países "P", "Q", "R" e "S", de modo que países cuja fronteira é uma linha não podem ser coloridos com a mesma cor, de quantas maneiras é possível colorir o mapa?

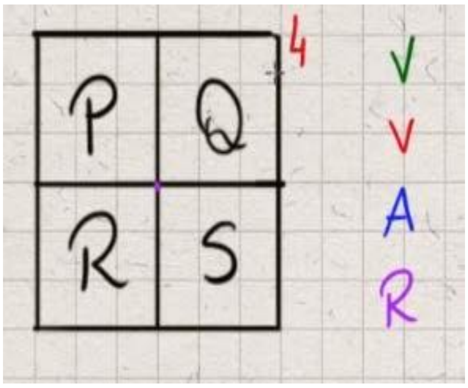
Inicio:



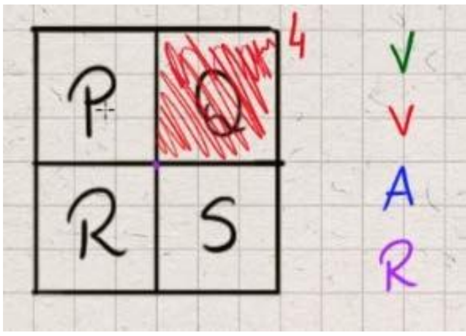
01:



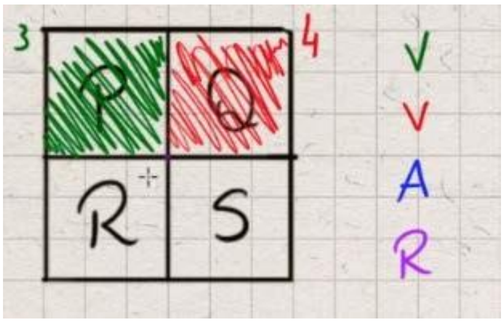
02:



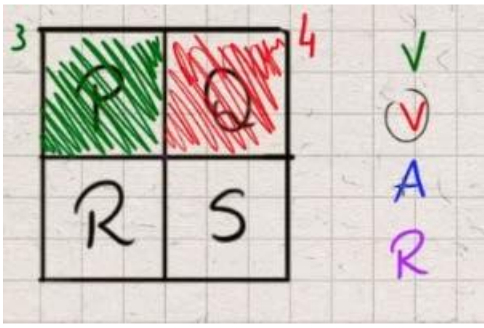
03:



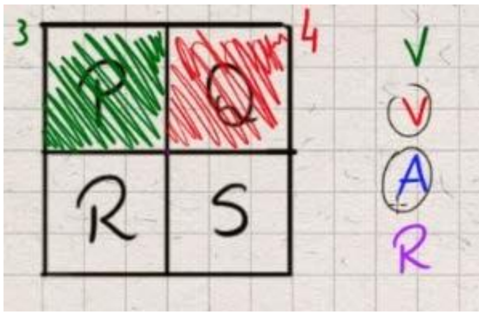
04:



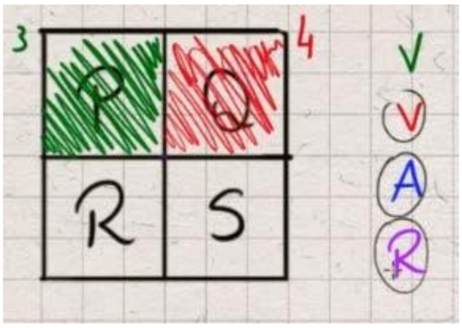
05:



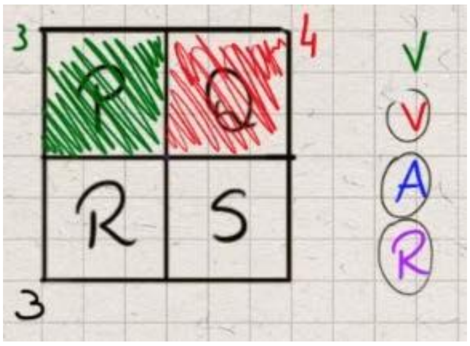
06:



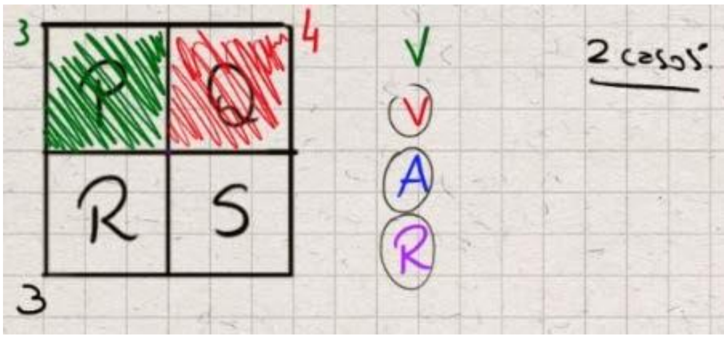
07:



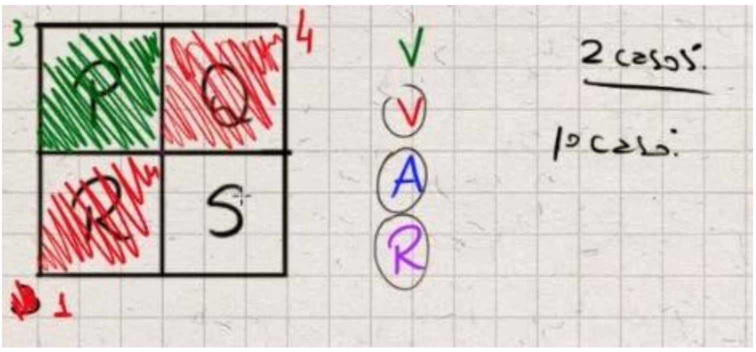
08:



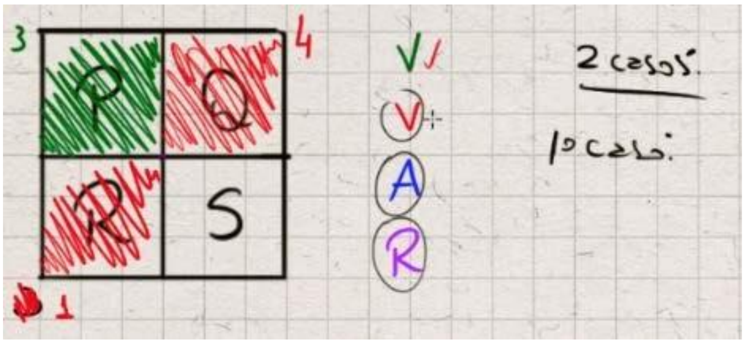
09:



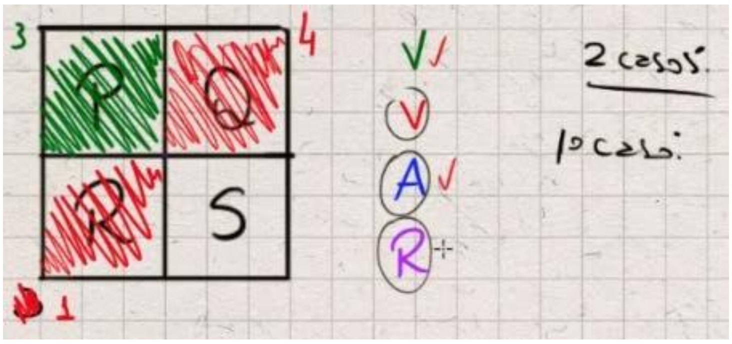
10:



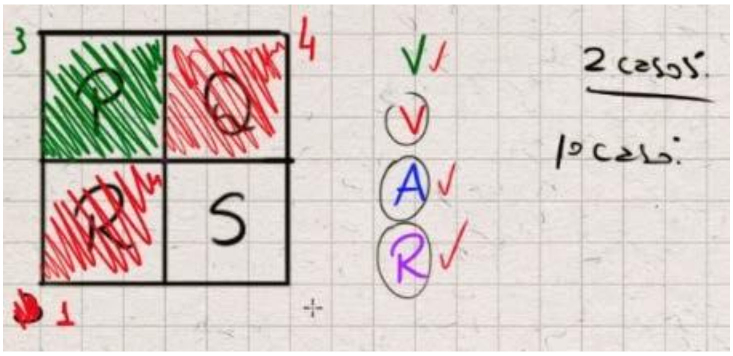
11:


3
4
P
Q
R
S
1
2 casos:
1º caso:

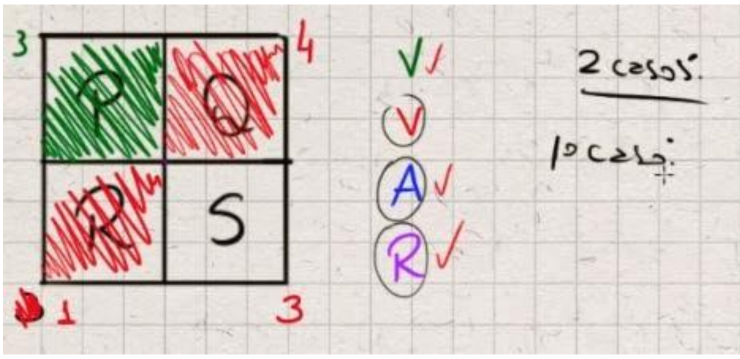
12:


3
4
P
Q
R
S
1
2 casos:
1º caso:

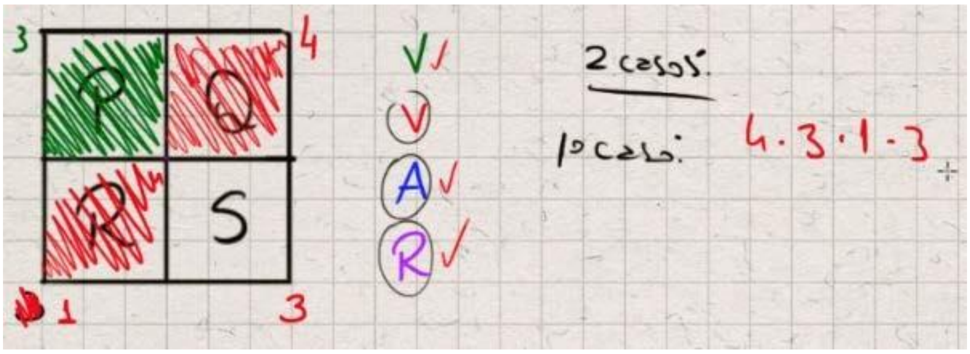
13:


3
4
P
Q
R
S
1
2 casos:
1º caso:

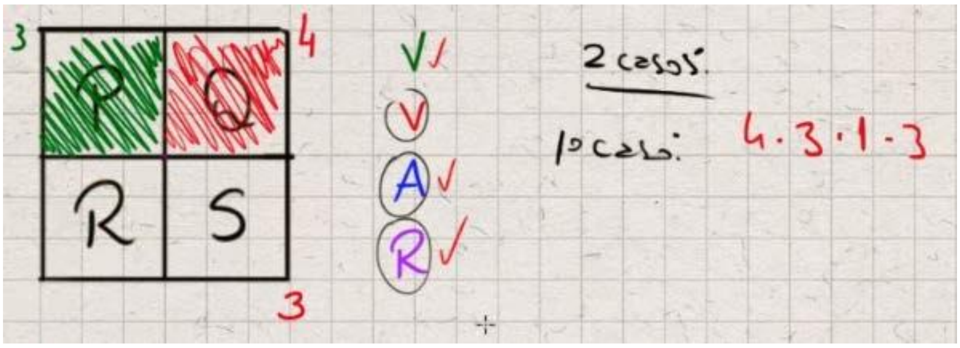
14:


3
4
P
Q
R
S
1
3
2 casos:
1º caso:

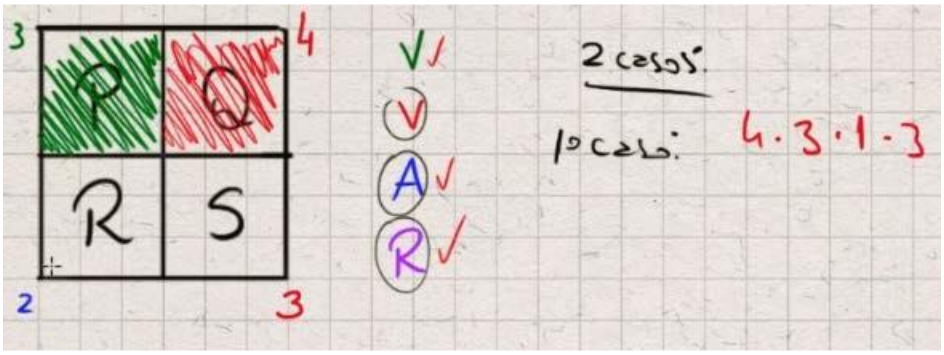
15:


3
4
P
Q
R
S
1
3
V
V
A
R
2 casos:
1º caso:
4·3·1·3

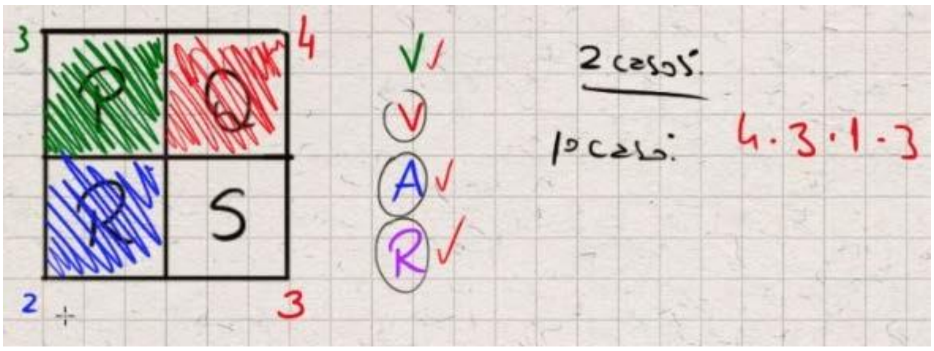
16:


3
4
P
Q
R
S
3
V
V
A
R
2 casos:
1º caso:
4·3·1·3

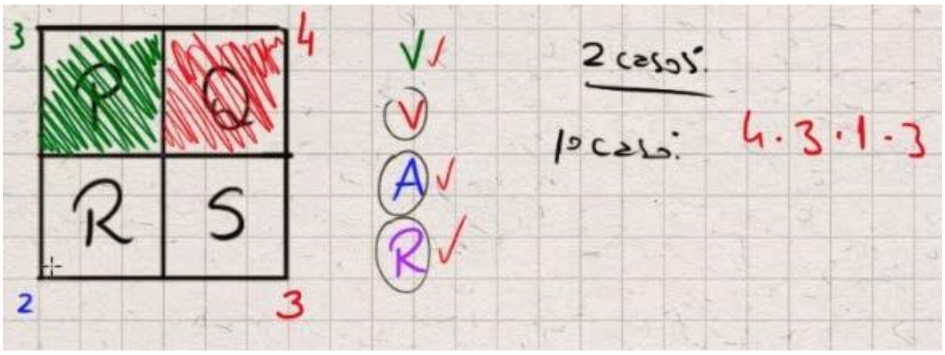
17:


3
4
P
Q
R
S
2
3
V
V
A
R
2 casos:
1º caso:
4·3·1·3

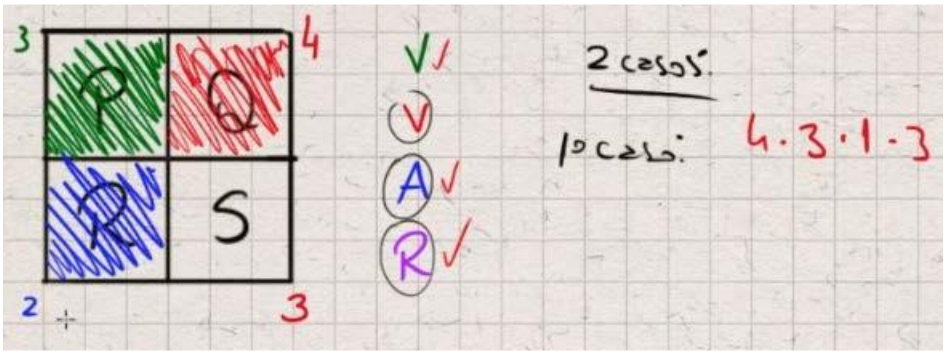
18:


3
4
P
Q
R
S
2
3
V
V
A
R
2 casos:
1º caso:
4·3·1·3

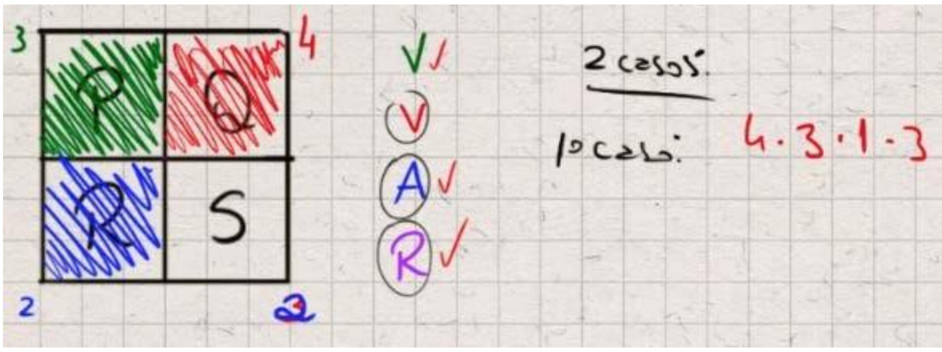
19:


3
4
P
Q
R
S
2
3
V
V
A
R
2 casos:
1º caso:
4·3·1·3

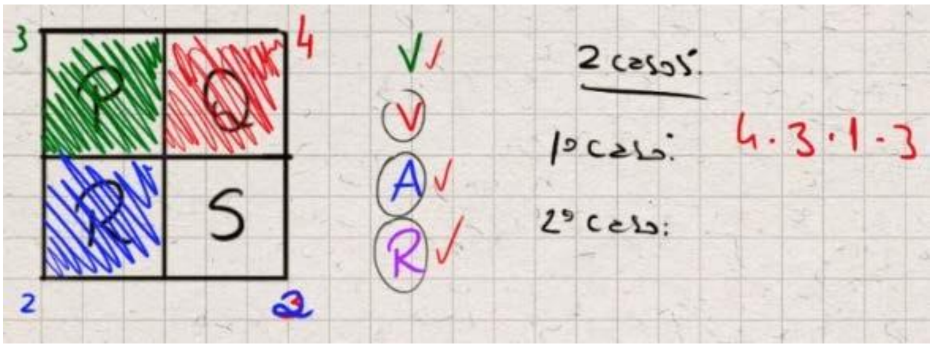
20:


3
4
P
Q
R
S
2
3
V
V
A
R
2 casos:
1º caso:
4·3·1·3

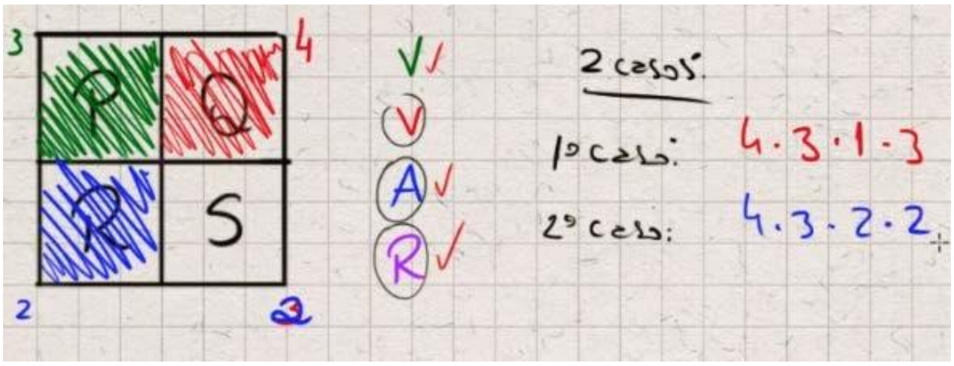
21:


3
4
P
Q
R
S
2
2
V
V
A
R
2 casos:
1º caso:
4·3·1·3

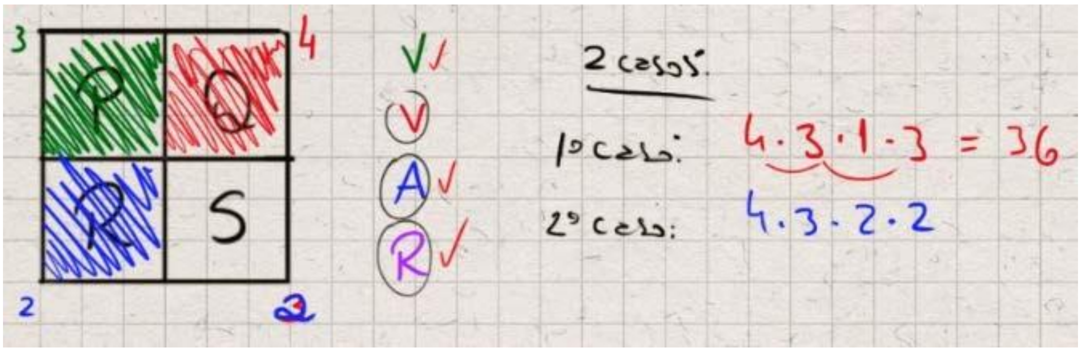
22:



23:



24:



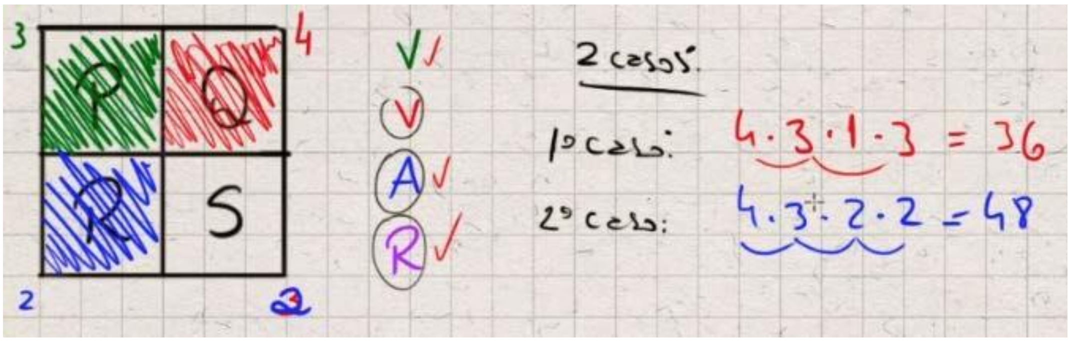
25:

2 casos:

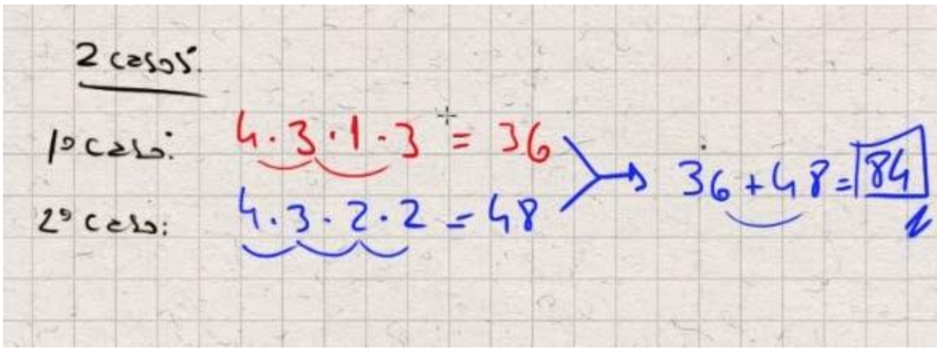
1º caso: $4\cdot3\cdot1\cdot3 = 36$

2º caso: $4\cdot3\cdot2\cdot2 = 48$

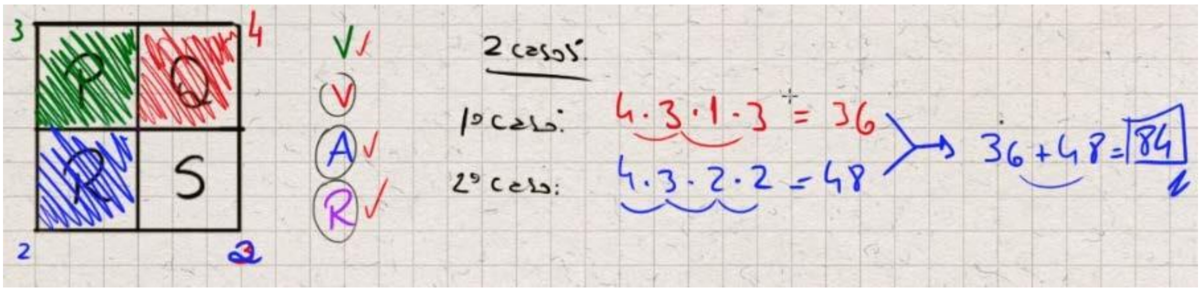
26:



27:



28:



- **Arranjo**

Análise Combinatória é a parte da Matemática que estuda os métodos de contagem e desenvolveu-se pela necessidade de os jogadores calcularem o número de possibilidades existentes nos chamados “jogos de azar”. Os primeiros estudos foram iniciados já no século XVI, pelo matemático italiano Niccollo Fontana (1500-1557), sucedido dos franceses Pierre de Fermat (1601-1665) e Blaise Pascal (1623-1662).
Análises Combinatórias possibilitam a construção de diferentes grupos de elementos e conjuntos por meio de vários procedimentos. É onde se estudam as propriedades das ordenações e esquemas definidos por meio de classes finitas de objetos. Permutações, Arranjos e Combinações são os três tipos principais de agrupamentos.
Conceitua-se como arranjo todos os possíveis agrupamentos de um conjunto de elementos. O arranjo pode ser de dois tipos: arranjo simples e com repetição.

- **Arranjo Simples**

No arranjo simples temos n elementos dos quais queremos tomar p. Isso seria a mesma coisa que ter n objetos com os quais queremos preencher p lugares. O primeiro lugar pode ser preenchido de n maneiras diferentes. Tendo preenchido a posição 1 restam (n-1) objetos e, portanto, a posição 2 pode ser preenchido de (n-1) maneiras diferentes. Após preencher a posição 2, haverá (n-2) maneiras de se preencher a posição 3 e, assim sucessivamente, vamos preenchendo as posições de forma que a posição p terá (n-(p-1)) maneiras diferentes de ser preenchido. Pelo princípio multiplicativo, podemos dizer que as p posições podem ser preenchidas sucessivamente de n.(n-1). (n-2) ...(n-(p-1)) formas diferentes.

O princípio multiplicativo é um método algébrico utilizado para determinar o número de possibilidades de escolhas, sem precisar descrever todas as possibilidades. A quantidade total de possibilidades de escolha é a multiplicação entre si de todas elas.
Sabendo que uma igualdade não se altera se a multiplicarmos e dividirmos o valor, então:

$A(n, p) = [n.(n-1).(n-2)...(n-(p-1))].[(n-p).(n-p-1)...2.1]/(n-p).(n-p-1)...2.1$

Podendo ser simplificada para:
$A(n, p) = n!/(n-p)!$

Onde, n é o número de elementos do conjunto e p é a quantidade de elementos por agrupamento.

O arranjo simples de n elementos tomados p a p , onde n >=1 e p é um número natural, tal que p < n , são todos os grupos de p elementos distintos que diferem entre si pela ordem e pela natureza dos elementos que compõe cada grupo. No arranjo simples dentro dos agrupamentos a ordem dos elementos é considerada, portanto, a mudança na ordem desses elementos resulta na alteração do agrupamento, não ocorrendo a repetição dos elementos.

Assumindo o exemplo abaixo, onde temos como conjunto o alfabeto de 23 letras (excluindo-se k, w e y), aplicando-se a fórmula para calcular quantas possibilidades de obter diferentes anagramas com 2 letras distintas, temos:
$A(n, p) = n!/(n-p)!$

$A(2, 23) = 23!/(23-2)!$

$A(2, 23) = 23!/21$

$A(2, 23) = (23.22.21.20.19.18.17.16.15.14.13.12.11.10.9.8.7.6.5.4.3.2.1)/$
$21.20.19.18.17.16.15.14.13.12.11.10.9.8.7.6.5.4.3.2.1 A(2, 23) = 23.22$

$A(2, 23) = 506$

Tomemos agora o seguinte exemplo: Considere os algarismos 1, 2, 3, 4 e 5.

Quantos números distintos, superiores a 100 e inferiores a 1.000 podemos formar se o
número é par?

Os números a serem considerados tem 3 dígitos, o que equivale a pensarmos que há 3 posições a serem preenchidas.

/P1 /P2 /P3

Se o número é par, a posição P3 pode ser preenchida ou com o algarismo 2 ou com 4. Há, portanto, 2 maneiras diferentes desse preenchimento ser feito. Tomemos, por exemplo o 4:

/P1 /P2 4/P3

Para o preenchimento das posições P1 e P2, temos à disposição os algarismos 1, 2, 3 e 5. Esse preenchimento pode se dar de:
$A(2, 4) = 4!/2!$
$A(2, 4) = (4.3.2.1)/2.1$
$A(2, 4) = 4.3$
$A(2, 4) = 12$

Consequentemente, existe 2.(A(2,4)), ou seja, 24 maneiras diferentes de preencher as 3 posições, isto é, há 24 números pares superiores a 100 e inferiores a 1.000, formados com os algarismos 1, 2, 3, 4 e 5.

- **Arranjo com Repetição**

O que diferencia o arranjo simples do arranjo com repetição é que o segundo permite a repetição de elementos em uma combinação dentro dos possíveis agrupamentos. No arranjo simples tal repetição não acontece.

Considere um conjunto com n elementos diferentes.

Denominamos arranjos com repetição de n elementos diferentes p a p todo agrupamento ordenado formado por elementos iguais ou diferentes escolhidos entre os n elementos dados.

Para calcular a quantidade total de possibilidades de escolha multiplicamos entre si todas elas. Para o arranjo com repetição o número de possibilidades para cada posição sempre será a quantidade n de elementos. Então o cálculo fica da seguinte forma:

$$A(n,p) = n.n.n.n...n$$

Sendo o n multiplicado entre si p vezes.
Simplificando, temos a fórmula geral para o arranjo com repetição representada por:

$$A(n, p) = n^p$$

Onde n é o número de elementos do conjunto e p é a quantidade de elementos por agrupamento.

Tomemos como exemplo a criação de uma senha. Nela temos quatro dígitos, onde em cada dígito podemos escolher entre dez números, do zero ao nove. Podemos repetir os algarismos quantas vezes quisermos, ou seja, códigos 1111 e 5544 são válidos. E a ordem conta, ou seja, o código 1234 é diferente do 4321.

Então quando há repetição e a ordem importa estamos diante de arranjos com repetição.

No caso desse exemplo temos arranjos de dez algarismos possíveis, quatro a quatro.
A (10, 4) = 10 4
A (10, 4) = 10.000
Existem então 10.000 possíveis senhas que podem ser utilizadas.

Agora tomemos esse outro exemplo: o problema abaixo foi proposto em uma das listas de exercícios de programação no site do URI, que é utilizado por professores como método de avaliação dos discentes. O mesmo, foi elaborado pela Universidade de São Paulo.

URI ONLINE JUDGE
PROBLEMS & CONTESTS

1890

Descrição
Tela Cheia
Enviar
Ranking
Fórum
uDebug

AD-HOC

URI Online Judge | 1890

Emplacando os Tuk-tuks

Por Marcio T. I. Oshiro, Universidade de São Paulo Brazil

Timelimit: 1

Na Tailândia, um tipo popular de transporte público é o chamado tuk-tuk (ตุ๊กตุ๊ก), também conhecido como auto-riquixá. O governo de Phuket decidiu criar um novo sistema de placas para os tuk-tuks, com a finalidade de diferenciá-los dos outros tipos de veículos. Devido ao turismo, que é uma das principais atividades econômicas da província, a frota de tuk-tuks vem crescendo rapidamente. Espera-se que com o novo sistema de placas seja possível criar uma quantidade suficiente de placas distintas para atender à demanda pelos próximos 42 anos.

Um sistema de placas é definido por dois números, *C* e *D*. Uma placa nesse sistema é uma cadeia com *C* consoantes seguidas por *D* dígitos. Uma placa não pode ser vazia (sem consoantes e sem dígitos).

No alfabeto tailandês existem 44 consoantes e 10 dígitos. No entanto, como os símbolos de algumas consoantes são parecidos com os de outras, o governo decidiu que serão utilizadas somente 26 consoantes, cujos símbolos foram considerados suficientemente diferentes.

Para garantir que existirão tuk-tuks suficientes para os competidores da Final Mundial da Maratona de Programação em 2016, o governo de Phuket quer saber qual o número de placas distintas é possível gerar com um determinado sistema de placas.

Entrada

A primeira linha da entrada contém um inteiro **T** indicando o número de instâncias.

Cada instância consiste em uma linha contendo os números inteiros **C** ($0 \le$ **C** ≤ 6) e **D** ($0 \le$ **D** ≤ 9) representando as quantidades de consoantes e dígitos, respectivamente, em um sistema de placas.

Saída

Para cada instância, imprima uma linha com a quantidade de placas distintas que podem ser geradas pelo sistema correspondente. É garantido que a resposta sempre será menor que 2^{31}.

De início, para resolução do problema, vamos retirar alguns dados necessários para a interpretação da questão. Iremos trabalhar usando 2 grupos, o das letras (consoantes) e dos dígitos (números) do alfabeto tailandês, mas para exemplificar melhor optamos por usar o nosso alfabeto e o nosso sistema numérico, que coincidentemente possui a mesma quantidade que o deles.
Logo em seguida, analisando a entrada dos dados do problema, é possível observar que será digitado pelo usuário a quantidade de vezes que o programa irá rodar e em cada volta será informado a quantidade de elementos por agrupamento, tanto para as letras, como para os dígitos. Para isso, iremos utilizar o arranjo com repetição, pois não é especificado qualquer restrição em relação às repetições nos agrupamentos.
Tomando como exemplo a segunda entrada da questão, iremos aplicar a fórmula.

Exemplo de Entrada	Exemplo de Saída
3 0 6 2 4 0 0	1000000 6760000 0

A (n, p) = n p

Para as letras, iremos formar o agrupamento com 2 elementos:

{A,A}, {A,B}, {A,C},...{Z,Z}

Aplicando a fórmula, temos:

A (n, p) = 26 2 = 6 76

Do mesmo modo, iremos aplicar a fórmula para os dígitos, porém, com os agrupamentos possuindo 4 elementos:

{0,0,0,0}, {0,0,0,1}, {0,0,0,2},...{9,9,9,9}
A (n, p) = 10 4 = 1 0.000

Por fim, para sabermos quantos agrupamentos teremos no final, só
multiplicarmos o resultado do primeiro arranjo com o do segundo arranjo.
6 76 * 1 0.000 = 6 .760.000

Código da resolução em python:

```
T = int(input())
for i in range (0, T):
	C,D = map(int,input().split())
	if C!=0 or D!=0:
		result = (26**C)*(10**D)
		print(result)
	else:
		print('0')
```

Referências:

ALFA CONNECTION.
Arranjos comrepetição .Disponível em <http://www.alfaconnection.pro.br/matematica/analise-combinatoria-e-probabilidade/ arranjos/arranjos-com-repeticao/>. Acesso em 20 de Maio de 2018.
FERREIRA, João Pimentel. Como distinguir Arranjos completos, Arranjos simples e Combinações? Disponível em <https://www.matematicaviva.pt/2010/01/como-distinguir-arranjos-completos.html>. Acesso em 20 de Maio de 2018.
OLIVEIRA, Naysa Crystine Nogueira. Arranjo com repetição. Disponível em <https://www.infoescola.com/matematica/arranjo-com-repeticao/>. Acesso em 16 de Maio de 2018.
SANTOS, José Plínio de Oliveira; MELLO, Margarida P. ; MURARI , Idani T. C. Introdução à análise combinatória . 4. ed. rev. Rio de Janeiro: Ciência Moderna, 2007. 390 p. il.
UNICAMP. O Princípio Multiplicativo. Disponível em: <https://www.ime.unicamp.br/~deleo/MA220/n01.pdf>. Acesso em 18 de Maio de 2018.
URI. Emplacando os Tuk-tuks . Disponível em <https://www.urionlinejudge.com.br/judge/pt/problems/view/1890 >. Acesso em 20 de Maio 2018

- **PERMUTAÇÃO**

Análise combinatória

A permutação é um processo de contagem, que faz parte do conteúdo de análise combinatória.
O objetivo principal de estudar Análise Combinatória é desenvolver métodos que permitam contar - de uma forma indireta - o número de elementos de um conjunto, estando esses elementos agrupados sob certas condições.
Permutações, Arranjos e Combinações, são os três tipos principais de agrupamentos, sendo que eles podem ser simples , com repetição ou circulares.

PERMUTAÇÃO
Seja uma sequência ordenada qualquer com um número “n” de elementos distintos, qualquer
outra sequência formada pelos mesmos “n” elementos reordenados é chamada
de PERMUTAÇÃO.

PERMUTAÇÃO SIMPLES
Seja A um conjunto com n elementos distintos. Os arranjos simples desses elementos tomados
n a n são chamados de permutações simples de A.

P n = n!

A palavra MITO tem 4 elementos distintos. Para calcular o número de permutações dessa palavra, utilizaremos a fórmula acima:
P n = n!
P 4 = 4!
P 4 = 4·3·2·1
P 4 = 24

De quantas maneiras distintas podemos colocar em fila indiana 6 homens e 6 mulheres iniciando com homem e terminando com mulher ?
6 __ __ __ __ __ __ __ __ __ __ 6
←----------------10!---------------->

P = (6*6)*10!
P = 36*10! = 130.636.800

PERMUTAÇÃO COM REPETIÇÕES
Dividimos o valor da permutação de todos os elementos pelo resultado da permutação dos elementos repetidos. Seja A um conjunto com n elementos, dos quais k elementos repetem-se. A fórmula para o cálculo das permutações de A é:

P^nk = n!/k!

Determinar os anagramas da palavra MORANGO.

Os anagramas serão formados a partir de uma sequência de 7 letras, das quais duas são iguais a O. Dessa forma temos:

$P^k{}_n = 7!/2! = (7.6.5.4.3.2.1)/2.1 = 5040/2 = 2520$

Caso o conjunto A, com n elementos, possua k repetições de um elemento e j repetições de
outro, o cálculo acontecerá da seguinte maneira:

$P_n^{k*j} = n!/k!*j!$

Quantos anagramas podem ser formados com a palavra ITALIANA, aplicando essa formula teremos:

$P_8^{2,3} = 8!/2!.3! = (8.7.6.5.4.3!)/2.1.3! =3360$

- **PERMUTAÇÃO CIRCULAR**

Na matemática, permutação circular é um tipo de permutação composta por um ou mais conjuntos em ordem cíclica. Ocorre quando temos grupos com n elementos distintos formando uma circunferência.

$P_n = n!/n =(n-1)!$

De quantas maneiras seis crianças podem se organizar para brincar em circulo?
P=(6-1)!
P=5!
P=120

120 maneiras de organizar as crianças para brincar em circulo.

Uma família é composta por seis pessoas: o pai, a mãe e mais 4 filhos. Num restaurante, essa
família vai ocupar uma mesa redonda. Em quantas disposições diferentes essas pessoas podem se sentar em torno da mesa de modo que o pai e mãe fiquem juntos?
Pc5= P4 = (5-1)! = 4! = 4 .3 .2 . 1 = 24

- **Combinações**

A análise combinatória é um ramo da matemática em que se estuda as possibilidades em um conjuntos de elementos finitos baseando-se em critérios que possibilitam a contagem. Dentro da análise combinatória estudamos três segmentos:
arranjo, permutação e combinação e conteúdos como o princípio fundamental de contagem e fatorial.

Exemplo :
Descubra quantos números com 3 algarismos conseguimos formar com o conjunto numérico {1, 2, 3}.

Conjunto de elementos finito : {1, 2, 3}

Conjunto de possibilidades de números com 3 algarismos : {123, 132, 213, 231, 312, 321}

Resposta Final : Com o conjunto numérico {1, 2, 3}, é possível formar 6 números.

No exemplo anterior a ordem dos elementos é um critério para a formação de um um novo número com três algarismos, de forma que o número 123 é diferente do número 321 mesmo contendo os mesmos elementos. Na combinação veremos que a ordem não importa
ao realizar agrupamentos entre elementos de um conjunto.

Combinação Simples
A combinação simples trata do agrupamento de elementos de um conjunto em subconjuntos independente da ordem. Durante a formação dos conjuntos, a partir de um conjunto {A, B, C}, os subconjuntos {A, B} e {B, A} são iguais e, portanto, apenas um, uma vez que a mudança na ordem dos elementos não torna os subconjuntos diferentes. Além disso, na combinação simples, os subconjuntos são formados de elementos distintos e $p \leq n$, onde p representa o número de elementos por subconjuntos e n o número de elementos do conjunto. Podemos sabemos as possibilidades de combinação simples de um

determinado problema a partir da seguinte fórmula:

$C_{n,p} = n!/(n - p)!\ p!$
n: números de elementos do conjunto.
p: números de elementos por subconjunto.

Exemplo 1
Uma prova consta de 15 questões das quais o aluno deve resolver 10. De quantas formas ele poderá escolher as 10 questões?
Antes de aplicarmos a fórmula para resolver este exemplo, devemos relembrar o conceito de fatorial e como resolvê-lo.

Resolução de um fatorial
Definição:
O fatorial de um número qualquer é representado pelo produto:
$n! = n . (n - 1) . (n - 2) . (n - 3) . ... . 1!$
Obs.: Subtraímos 1 de n enquanto $(n - 1) = / 0$.

Demonstração:
Calcule o fatorial de 4.
$n! = n . (n - 1) . (n - 2) . (n - 3) . ... . 1!$
$4! = 4 . (4 - 1) . (4 - 2) . (4 - 3)$
$4! = 4 . 3. 2 . 1$
$4! = 24$

Solução do exercício de Combinação Simples:
Observe que a ordem das questões não muda a resolução do teste. Logo, podemos concluir que trata-se de um problema de combinação de 15 elementos com taxa 10 (p = 10).
Na fórmula utilizamos fatorial pra chegar ao resultado. Dessa forma, é necessário o conhecimento sobre como resolver um fatorial.

Aplicando simplesmente a fórmula chegaremos a:

$C_{15,10} = 15!/(15-10)!\ 10!$
$\Rightarrow (15.14.13.12.11.10!)/5!\ 10!$
$\Rightarrow (15.14.13.12.11)/5.4.3.2.1$
$\Rightarrow$ 3 003 possibilidades
Obs.: Note que abrimos o fatorial para cancelar o 10! do numerador com o do denominador, já que os termos são iguais e estão num produto.

Exemplo 2
Numa reunião com 7 rapazes e 6 moças, quantas agrupamentos podemos formar com 3 rapazes e 4 moças?

Solução
Rapazes - $C_{7,3}$
n = 7 rapazes no total
p = 3 rapazes por agrupamento

Moças - $C_{6,4}$
n = 6 moças no total
p = 4 moças por agrupamento

A quantidade de possibilidades de agrupamento de acordo com as especificações do problema será dada pelo produto entre $C_{7,3} . C_{6,4}$.
Logo, temos que:

$C_{7,3} . C_{6,4} = 7!/(7-3)!\ 3! * 6!/(6-4)!\ 4!$
$\Rightarrow (7.6.5.4!)/3!\ 4! * (6.5.4!)/2!\ 4!$
$\Rightarrow (210)/3.2.1 * 30/2$
$\Rightarrow$ 5 25 agrupamentos

Combinação com Repetição
Na combinação simples vimos que os subconjuntos ou agrupamentos eram formados por elementos distintos. Na combinação com repetição, um elemento poderá ser repetido em um subconjunto, de forma a ter o mesmo elemento em um agrupamento. O agrupamento de elementos ocorrerá de maneira que $p \leq n$ ou $p > n$, sem restrição da repetição de elementos em um mesmo agrupamento. No entanto, os agrupamentos que possuírem os mesmos elementos e em mesma quantidade apenas em ordem diferente não serão diferenciados, contando apenas como um agrupamento. Por exemplo, temos o conjunto {A, B, C, D, E} e os subconjuntos {A, A, B, C} e {A, B, A, C}, de acordo com a
definição, estes subconjuntos são iguais, pois a ordem não tem importância. Para resolver os problemas de repetição com combinação utilizamos a seguinte fórmula:

$C_{n,p} = ((n + p - 1)!)/(n - 1)!\ p!$

Exemplo :
De quantos modos podemos comprar 4 salgadinhos, considerando a possibilidade de repetição, em uma lanchonete que oferece 7 opções de escolha de salgadinhos?
Solução:
A lanchonete oferece 7 opções de salgadinhos.
$n = 7$
Queremos comprar 4 salgadinhos.
$p = 4$

Utilizando a fórmula de combinação com repetição, temos que:
$C\ 7,4 = ((7 + 4 - 1)!)/(7 - 1)!\ 4!$
$\Rightarrow (10!)/6!\ 4!$
$\Rightarrow (10.9.8.7.6!)/4!\ 6!$
$\Rightarrow (10.9.8.7)/4.3.2.1$
$\Rightarrow$ 210 modos diferentes

Referências Bibliográficas:
Análise Combinatória .
Disponível em:
[https://www.infoescola.com/matematica/analise-combinatoria/].
Combinação Simples .
Disponível em:
[https://www.infoescola.com/matematica/combinacao-simples/].
Combinação Simples.
Disponível em:
[https://www.youtube.com/watch?v=fvPIb7Vtez4&t=0s&index=18&list=LLRwewWfR FDwmgc
TBe0txRag].
Combinação com Repetição.
Disponível em:
[http://www.centralexatas.com.br/matematica/analise-combinatoria/959184].

- **Partições**

Ordenadas e não ordenadas
Partições ordenadas
Suponha que um saco contém sete bolas de gude numeradas de 1 a 7. Calculamos o número de
maneiras que podemos retirar, primeiramente, duas bolas do saco, depois três bolas, e finalmente duas bolas. Em outras palavras, queremos calcular o número de partições ordenadas.

$$[A_1, A_2, A_3]$$

do conjunto de sete bolas de gude em células A, contendo duas bolas, A_2 contendo três bolas e
A_3 contendo duas bolas. Denominamos essas partições como ordenadas porque distinguimos que definem a mesma partição de A.

[{1,2}, {3,4,5}, {6,7}] e [{6,7}, {3,4,5}, {1,2}]

Começamos por sete bolas no saco; logo , existem (7/2) maneiras de retirar as primeiras duas
bolas, i, e., de determinar a primeira célula A_1. Depois disso, existem cinco bolas no saco (5/3)
maneiras de pegar as três bolas, i, é, de determinar a segunda célula A_2. Finalmente, restam duas
bolas de gude no saco e, existem (2/2) maneiras de determinar a última célula A_3.
Portanto, existem

(7/2) (5/3) (2/2) =(7.6)/1.2 * (5.4.3)/1.2.3 * (2.1)/1.2 = 210

partições ordenadas distintas de A em células A_1 contendo duas bolas de gude, A_2 contendo três
bolas de gude, e A_3 contendo duas bolas de gude.
Agora observe que

(7/2) (5/3) (2/2) =(7!)/2! 5! * (5!)/3! 2! * (2!)/2! 0! = (7!)/2! 3! 2!

já que cada numerador, após o primeiro, é cancelado pelo segundo termo no denominador do
fator prévio.

Teorema
Suponha que A contém n elementos e sejam n1, n2,..., ni , inteiros positivos cuja soma é n isto é , n1+n2+...+ni = n . Então existem

(n!)/n1! n2! n3!...ni!

partições distintas ordenadas de A da forma [A1, A2,..., Ar], onde A_1 contém n_1 elementos, A2
contém n_2 elementos, ..., e A_r contém n_i elementos.

Exemplo: Ache o número m de maneiras que nove brinquedos podem ser
divididos entre quatro crianças se a mais jovem deve receber três brinquedos e cada
uma das outras , dois brinquedos.
Queremos achar o número m de partições ordenadas de nove brinquedos em
quatro células contendo 3, 2, 2 e 2 brinquedos respectivamente.

m =(9!)/3!2!2!2!=7.560

Partições não ordenadas
Frequentemente, desejamos particionar um conjunto A em uma coleção de subconjuntos A1, A2, ..., Ar , onde os subconjuntos, agora, não estão ordenados. Da mesma forma que o número de permutações com repetição foi obtido do número de permutações, dividindo por k! quando k objetos eram equivalentes, também podemos obter o número de partições não ordenadas a partir do número de partições ordenadas. dividindo por k! quando k
dos conjuntos têm o mesmo número de elementos. Isso é ilustrado no próximo exemplo, no
qual resolvemos o problema de duas maneiras.

Exemplo: Ache o número n de maneiras que 12 estudantes podem ser divididos em três times A1, A2, e A3 , de tal forma que cada time contenha quatro estudantes.

Método 1: Seja A um dos estudantes. Então, existem (11/3)
maneiras de escolher três outros estudantes para serem do mesmo time que A. Agora, seja B um estudante que não está no time de A; então existem (3/7) maneiras de escolher três estudantes entre os remanescentes para ficarem no mesmo time de B. Os quatro estudantes restantes constituem o terceiro time. Juntando todas as informações, o número de maneiras de dividir os estudantes é:

n =(11 /3) * (37) = 165 * 35 = 5775

Método 2: Observe que cada partição { A1, A2, e A 3 } de estudantes pode ser organizada de 3! = 6 maneiras como em uma partição ordenada. Pelo teorema 6.8, existem (12!)/4!4!4! = 34 650
partições ordenadas. Portanto, existem n = 34 650/6 = 5775 partições (não ordenadas).

Exemplo: Suponha que eu possua uma bolsa, com 9 bolsas vazias dentro dela e eu numero essas bolsas de 1 a 9. Suponha também que eu desejo fazer três grupos de bolsas (B1,
B2, B3) com 3 bolsas cada, de quantas maneiras eu poderia fazer isso?

Resolução: Utilizando o método 2, podemos utilizar a fórmula de partições ordenadas primeiro, obtendo: (9!)/3!3!3!, que solucionando obtemos 362880/216, resultando em 1680 partições ordenadas. Como as partições possuem o mesmo tamanho, pode-se mudar a partição de lugar e não obter uma nova configuração, assim devemos “descontar” essa configurações. Para fazer isso devemos dividir o resultado por x!, onde x é o número de partições com o mesmo número
de elementos. Assim, dividimos 1680 por 3! obtendo: 280 maneiras.

- **COEFICIENTES BINOMIAIS**

1- Números Binomiais

Os números binomiais são relações estabelecidas entre dois números naturais, podendo ser chamados também de coeficiente binomiais.

É chamado número binomial à relação que se estabelece entre dois números naturaisnep, tais quenseja maior ou igual ap(n ≥ p)

Equação:

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

Dado $\binom{n}{p}$, chamados de número binomial de classe p do número n.

De forma semelhante às frações. Onde, pode-se dizer que n é o numerador e p o denominador.

Exemplos de números binomiais:

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

$$\binom{5}{2} = \frac{5!}{2!\,(5-2)!} = \frac{5!}{2!\,3!} = \frac{5.4.\cancel{3!}}{2.1.\cancel{3!}} = \frac{20}{2} = 10$$

$$\binom{10}{6} = \frac{10!}{6!\,(10-6)!} = \frac{10!}{6!\,4!} = \frac{10.9.8.7.\cancel{6!}}{\cancel{6!}.4.3.2.1} = \frac{5040}{24} = 210$$

Há casos particulares que não é preciso fazer seu desenvolvimento, ou seja, pode-se concluir rapidamente seu resultado.

1° CASO →Quando n =p:

$$\binom{n}{n} = \frac{n!}{n!\,(n-n)!} = \frac{n!}{n!\,0!} = 1$$

2° CASO →Quando p=0:

$$\binom{n}{0} = \frac{n!}{0!\,(n-0)!} = \frac{n!}{0!\,n!} = 1$$

3° CASO →Quando p=1:

$$\binom{n}{1} = \frac{n!}{1!\,(n-1)!} = \frac{n.\cancel{(n-1)!}}{1!\,\cancel{(n-1)!}} = n$$

- **2- Coeficiente Binomiais**

Os números binomiais podem ser chamados também de coeficiente binomiais.

2 2
(Númerobinomial)(1 1)= 2 (Coeficiente Binomial)

- **Binomiais complementares**

Dizemos que dois coeficientes binomiais são complementares se seus numeradores foram iguais ea soma de seus denominadores for igual ao numerador.

Exemplo, considerando os números naturaisn,peq,p + q = n, então os binômios

$\binom{n}{p}$ e $\binom{n}{q}$ são complementares. Podendo afirmar então, que todos os coeficientes binomiais complementares são iguais.

Vejamos a seguir:

$$\binom{n}{p} = \binom{n}{q}$$

$$\frac{n!}{p!\,(n-p)!} = \frac{n!}{q!\,(n-q)!}$$

$$\frac{n!}{p!\,q!} = \frac{n!}{q!\,p!}$$

Exemplos:

$$\binom{10}{7} = \binom{10}{3} \quad \binom{6}{2} = \binom{6}{4} \quad \binom{9}{5} = \binom{9}{4}$$

Ao calcular os números binomiais e organizar os números binomiais em linhas e colunas, iniciando as com 0 (zero) e definindo as colunas sendo o termo de cima e as linhas o termo de baixo do número binomial é possível criar o Triângulo de Pascal

Ex.:
00
(00)
11 11
(00) (11)
22 22 22
(00)(11)(22)
33 33 33 33
(00)(11)(22)(33)
. . . .
.
.

Resultado:

1

1 1

1 2 1

1 3 3 1

. . . .

.

.

1° Cada linha inicia e termina com o número 1.

2° Em cada linha, os termos equidistantes (mesma distância), dos extremos possuem valor igual.

$\binom{8}{0}$	$\binom{8}{1}$	$\binom{8}{2}$	$\binom{8}{3}$	$\binom{8}{4}$	$\binom{8}{5}$	$\binom{8}{6}$	$\binom{8}{7}$	$\binom{8}{8}$
1	8	28	56	70	56	28	8	1

$\binom{9}{0}$	$\binom{9}{1}$	$\binom{9}{2}$	$\binom{9}{3}$	$\binom{9}{4}$	$\binom{9}{5}$	$\binom{9}{6}$	$\binom{9}{7}$	$\binom{9}{8}$	$\binom{9}{9}$
1	9	36	84	126	126	84	36	9	1

3- Triângulo de Pascal

1

1 1

1 2 1

1 3 3 1

. . . .

.

.

- **Relação de Stifel**

Sejam n e p números naturais tais que n maior ou igual a p menos um maior ou igual azero(n≥ p – 1 ≥ 0), podemos dizer que:

$$\binom{n}{p-1}+\binom{n}{p}=\binom{n+1}{p}$$

Outra forma de apresentar a relação de Stifel sem qualquer perda de valor é:

$$\binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1}$$

Exemplos:

$$\binom{5}{2} = \binom{4}{2} + \binom{4}{1} \qquad \binom{13}{9} = \binom{12}{9} + \binom{12}{8}$$

Sendo então o coeficiente binomial, “simétrico”. E foi baseado nessa simetria que um rapaz muito estudioso montou um triângulo com coeficientes binomiais. O Triângulo de Pascal.

4- Propriedades das Colunas

Na soma de todos os termos da coluna a resposta será imediatamente o termo a baixo e a direita do último termo somado

1

1 1

1 2 1

1 3 3 1

. . . .

.

.

1+2= 3 (termo abaixo3a sua direita3)

5- Propriedades das Diagonais
Na soma de todos de uma diagonal a resposta será imediatamente o termo a baixo:

1

1 1

1 2 1

1 3 3 1

. . . .

.

.

1+1+1= 3 (termo abaixo3)

6- Propriedades das Soma das Linhas
Na soma de todos de uma diagonal a resposta será imediatamente o termo a baixo:

2^0 1

2^1	1	1			
2^2	1	2	1		
2^3	1	3	3	1	
2^n	.	.	.	.	.

$1+2+1 = 2^2 = 4$

7- Binômio de Newton:
Binômio de Newton: (a + b)n para n = 2 ou seja, o clássico a^2 + 2ab + b^2.
É só pegarmos a^2 + 2ab + b^2 e olhar quais são os coeficientes inteiros de a e b.

1, 2 e 1 (3° linha do triângulo).

Ex:

$$(x+y)^0 = \mathbf{1}$$ 0th row

$$(x+y)^1 = \mathbf{1}x + \mathbf{1}y$$ 1st row

$$(x+y)^2 = \mathbf{1}x^2 + \mathbf{2}xy + \mathbf{1}y^2$$ 2nd row

$$(x+y)^3 = \mathbf{1}x^3 + \mathbf{3}x^2y + \mathbf{3}xy^2 + \mathbf{1}y^2$$ 3rd row

$$(x+y)^4 = \mathbf{1}x^4 + \mathbf{4}x^3y + \mathbf{6}x^2y^2 + \mathbf{4}xy^3 + \mathbf{1}y^4$$ 4th row

$$(x+y)^5 = \mathbf{1}x^5 + \mathbf{5}x^4y + \mathbf{10}x^3y^2 + \mathbf{10}x^2y^3 + \mathbf{5}xy^4 + \mathbf{1}y^5$$ 5th row

- **8- Desenvolvimento Binômio de Newton:**
  1º: Coloque os números binomiais do expoente:
  2º: Coloque o x e vai diminuindo os expoentes de forma decrescente 3º: Coloque o y e vai aumentando os expoentes de forma crescente

00
$(x+y)^0$ = (00)x^0y^0
11 11
$(x+y)^0$ = (00)x^1y^0+(11) x^0y^1
22 22 22
$(x+y)^0$ = (00)x^2y^0+(11)x^1y^1+(22) x^0y^2
33 33 33 33
$(x+y)^0$ = (00)x^3y^0+(11)x^2y^1+(22)x^1y^2+(33) x^0y^3

- **Referência Bibliográfica**

Mundo Educação – Coeficientes Binomiais. Disponível em:

<http://mundoeducacao.bol.uol.com.br/matematica/coeficientes-binomiais.htm>. Mundo Educação – Triângulo de Pascal. Disponível em: <http://mundoeducacao.bol.uol.com.br/matematica/triangulo-pascal-ou-tartaglia.htm>.

Youtube:
Matemática - Binômio de Newton - Números Binomiais:https://www.youtube.com/watch?v=C5Vw00yWWzc
Binômio de Newton e Triângulo de Pascal - Extensivo Matemática | Descomplica:https://www.youtube.com/watch?v=SX8JwHAIfXQ&t=15s
NUMEROS BINOMIAIS TRIANGULO PASCAL-PROF.CHUCK:

https://www.youtube.com/watch?v=2-ctEASuKSY&t=833sBINÔMIO DE NEWTON DESENVOLVIMENTO-CHUCK: https://www.youtube.com/watch?v=HfcPAXVJKg8

- **JOGOS E CRIPTOGRAFIA**
- **JOGOS**
- **A MATEMÁTICA DO POKER**

Apesar do Poker não ser uma ciência exata os números representam um papel importante, principalmente na versão Texana, principalmente na questão das probabilidades. Então com isso em mente podemos dizer que o jogador que tem um conhecimento melhor de matemática terá uma vantagem significativa sobre o jogador que não possui.
O Texas poker e os outros tipos de Poker tem várias regras com vários tipos de mãos para bater, uma mais rara que a outra e sendo assim uma vale mais que a outra, não iria dar tempo de passar por todas elas (e também ia ser um trabalho muito exaustivo) então vou passar apenas pelas básicas e a lógica basicamente se aplica a maioria já que todas funcionam com probabilidade. O baralho do Texas Hold'em é composto por 52 cartas, com quatro naipes diferentes.
Sendo que o total de possibilidades de hole cards é calculada como: 52 x 51 = 2652 possibilidades. Como para o jogo não faz diferença a ordem das cartas pegamos apenas metade das possibilidades, sobrando apenas 1326 possibilidades de hole cards. Agora utilizando um par de Ás como base.
Existem 6 possibilidades: Ás de copas com Ás de ouro, Ás de copas com Ás de espada, Ás de copas com Ás de paus, Ás de paus com Ás de ouro, Ás de paus com Ás de espada e Ás de ouro com Ás de espada.
Com isso temos 6/1326 = 0,00452, em porcentagem isso vale 0,45%, se inverter o resultado você chega a 221, ou seja, a cada 220 mãos você receberá um Ás. A informação de 1 a cada 220 é inútil, porém a informação para chegar nesse resultado não é.Primeira delas são as combinações, sabemos agora que cada par possui 6 combinações, segundo essa porcentagem de 0,45%.
Onde usar: as combinações serão bem uteis para fazer call sem pot odds, saber se o vilão está blefando, saber se cabe uma value bet no river etc.
Onde usar a porcentagem, para quem utiliza tracker aparece um número em porcentagem para alguns stats do vilão então se você visualizar um vilão com um PFR de 0,45% a chance de o vilão só abrir AA é de 99%.
Então sabemos que os pares são 6 combinações e representam 0,45%. Falta determinar os outros conjuntos. Frisando que cada par tem 6 combinações.
Para todos os outros tipos de mãos será apenas uma questão de pegar esses dados já fornecidos e alterar os números das possibilidades, o que irá gerar diferentes porcentagens de chances. Esse é o básico da matemática do poker, sempre lembrando que o poker é influenciado por várias outras coisas como.
Se você tem um par de 5, além das chances do seu oponente ter outros tipos de mãos mais fortes que um par, ainda existe a chance de ele ter um par mais forte que o seu, por exemplo um par de 6, então existiria uma possibilidade de 9/13 dele ter uma mão mais forte que a sua.

- **MEGA SENA E SUA RELAÇÃO COM A ANÁLISE COMBINATÓRIA**

A Mega-Sena é uma loteria realizada pela Caixa Econômica Federal que premia o jogador que acertar um certo valor de números. A loteria consiste em um jogo onde um apostador tem que acertar 6 números dos 6 sorteados entre 60 disponíveis. Nesse esquema, a ordem da aposta não importa e nenhum número da mesma pode ser repetido. Nesse jogo é possível apostar até 15 números, assim aumentando suas chances de êxito.

Apesar de poder apostar até 15 números, a tarefa de ganhar na Mega-Sena ainda é difícil. Em um jogo de uma aposta mínima (de até 6 números), a possibilidade de vencer é de 1 em 50.063.860.

Como se trata de uma Combinação, para conseguirmos chegar na possibilidade de vitória dita anteriormente, precisamos seguir a lógica da fórmula da Combinação, que consiste em um número n que representa a quantidade de elementos do conjunto e um p que é um número natural menor ou igual a n, que representa a quantidade de elementos que irão formar os agrupamentos. A fórmula segue abaixo:

$$C_{n,p} = \frac{n!}{p!\,(n-p)!}$$

Na situação da aposta mínima, fazendo as devidas alterações, chegamos no seguinte resultado:

$$C_{60,6} = \frac{60!}{6!\,(60-6)!} = \frac{60.59.58.57.56.55.\cancel{54!}}{6!.\cancel{54!}} = \frac{36\,045\,979\,200}{720}$$

$$C_{60,6} = 50\,063\,860$$

Resultado representa a quantidade de possibilidades possíveis com a escolha de 6 números, ou seja, um pouco mais de 50 milhões de jogos possíveis. Como só 1 jogo pode ser o vencedor, temos uma chance em 50 milhões.
Visto as possibilidades disponíveis, agora podemos calcular a porcentagem de vitória em cima desse exemplo. Segue o esquema abaixo:

$$P(A) = \frac{n(A)}{n(\Omega)}$$

Eventos possíveis pelo número total de eventos

$$P = \frac{1}{50\,063\,860} = 0{,}00000002 = 0{,}000002\%$$

Vimos então que com uma aposta simples, nossa possibilidade de ganhar é 0,000002%.

CRIPTOGRAFIA

Desde a antiguidade já havia a necessidade do envio e recebimento de informações sigilosas, de modo que apenas o emissor e receptor deveriam possuir acesso a informação. Daí a criptografia surgiu como uma ferramenta essencial e sua complexidade foi aumentando com o tempo e necessidade.
Um exemplo muito comum de criptografias ocorre em guerras, visto que o segredo sobre a forma de operação é essencial para o efetivo sucesso das manobras militares.
O termo criptografia é formado pela fusão de duas palavras gregas "Kryptós" e "gráphein", que significam “oculto” e “escrever”, respectivamente. Sendo assim,acriptografia trata-se de um conjunto de regras na maneira de escrever e ler uma informação, de modo que apenas os possuidores das regras conseguem acesso a mensagem.
Atualmente o uso de criptografias é muito importante, visto que nos tempos modernos passamos a transmitir mensagens pessoais e direcionadas através de meios de

comunicação de acesso comum a vários usuários. A ausência da criptografia permitiria o acesso irrestrito a mensagem enviada.

CIFRA DE CÉSAR

A Cifra de César é uma técnica simples de criptografia que consiste em substituir as letras do alfabeto por outras. Essa troca entre as letras se dá através de um deslocamento definido do alfabeto, como pode ser visto abaixo:

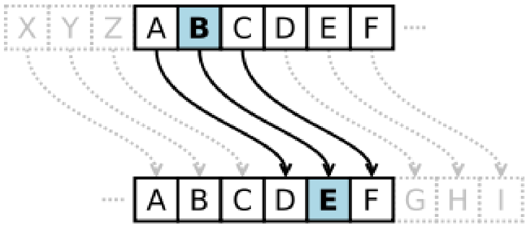


Figura 1. Imagem do descolamento gerado no alfabeto

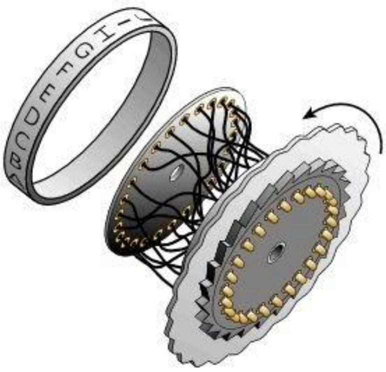
Ex.: Com um descolamento de 3 letras.
A → d, B → e, C → f, D → g, … / Sendo assim, a palavra “ABADA” seria escrita por: “dedgd”

MÁQUINA ENIGMA

Enigma é o nome pelo qual ficou conhecida a máquina de criptografia utilizada por boa parte das forças militares alemãs durante a segunda guerra mundial. Enigma é uma máquina eletromecânica que utiliza rotores como elementos básicos para gerar a criptografia. A máquina possui ainda diversos modelos que são indicados por uma letra, por exemplo: Enigma A e Enigma D. Os modelos D e G foram os mais divulgados devido ao fato de terem sido utilizados pelas forças militares da Alemanha.

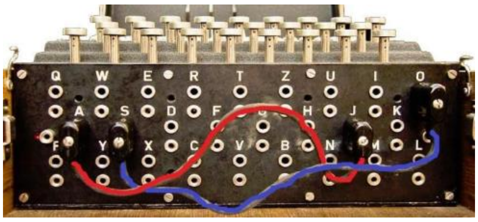
FUNCIONAMENTO

A máquina possuía um teclado e um visor, quando é pressionado uma tecla acende uma letra correspondente no visor. Desse modo, a criptografia era realizada digitando a mensagem e copiando as letras que iam sendo indicadas. A descriptografia se dava de maneira similar, escrevendo o código criptografado na máquina e obtendo as letras correspondentes para remontar a mensagem original.
Para o efetivo processo de descriptografia um cuidado é necessário, a máquina precisa está montada nas configurações iniciais idênticas de quando foi realizado a criptografia da mensagem. Isso se deve pela maneira como a máquina é construída.
A enigma era composta por rotores (peças giratórias) que possuíam contatos de entrada e saída, sendo possível realizar diferentes associações entre os contatos de entrada e saída. Cada contato de saída estava ainda associado a uma letra. Os rotores contavam ainda com um sistema de engrenagens que possuía número de dentes diferentes entre os rotores, de modo que a máquina tinha vários rotores com quantidade a depender do modelo.



A Enigma permite a montagem de um certo número de rotores, garantindo a permutação ou arranjo dos rotores a serem utilizados. Esses rotores quando instalados rotacionam sempre que uma tecla é pressionada e o rotor vizinho só rotaciona quando o anterior gira uma vez. Com isso, a posição inicial dos rotores é de fundamental importância para o código gerado.

Não o bastante, quando a Enigma foi adotada para propósitos militares foi adicionado um painel de plugs, que através do uso de fios permitia trocar duas letras, aumentando ainda mais a complexidade da encriptação.



NÚMERO TOTAL DE CRIPTOGRAFIAS POSSÍVEIS

Devido o número de variáveis que geram a criptografia, uma das coisas que chamam mais atenção na Enigma é o extenso número de possibilidade de criptografar uma mensagem, inviabilizando os esforços de tentar quebrar a criptografia por força bruta (testando todas as possibilidades).

A fim de mostrar a força da segurança produzida pela Enigma será calculado o número de possibilidades possíveis utilizando como base a Enigma I. Na Enigma I era utilizado 3 rotores dentro 5 existentes. Os rotores possuíam 26 dígitos, podendo permutar os 26 contatos de entrada com os 26 contatos de saída.

O Enigma I possui ainda o sistema de plugs permitindo a conexão de até 13 cabos conectando as letras de 2 em 2.

Probabilidade de conexão dos cabos:
Com os plugs é possível conectar 2 letras dentre 26 possibilidades. Sabendo que a ligação entre as letras independe de ordem, o número de maneiras de conectar duas letras é uma combinação dos 26 elementos 2 a 2:

$$C_{(c,n)}= (n!)/p!*(n-p)$$
$$C_{(26,2)}= (26!)/2!*(26-2)$$

Adicionando um novo cabo, temos um novo conjunto de possibilidades para esse novo cabo, porém o número de contatos disponível é menor, sendo assim, o número de possibilidades possíveis para esse novo cabo é dado por:
$C_{(26-2,2)}=((26-2)!)/2!*((26-2)-2)! = ((26-2)!)/2!*(26-4)$

De maneira análoga com mais um cabo, temos:
$C_{(26,4,2)}$= ((26-4)!)/2!*((26-4)-2!) = ((26-4)!)/2!*(26-6!)

De maneira análoga com o n-ésimo cabo, temos:
$C_{(26-2n+2,2)}$=((26-2n+2)!)/2!*(26-2n+2-2)! = ((26-2n+2)!)/ 2!*(26-2n)!

Sendo assim, para encontrar o número de possibilidades utilizando n cabos basta multiplicar o número de possibilidades dos cabos dividido pelo fatorial do número de cabos, visto que a ordem em que se utiliza os cabos não é importante. Daí temos:

($C_{(26,2)}$*$C_{(26-2,2)}$*$C_{(26-4,2)}$*...*$C_{(26-n2,2)}$)/n!

$$\frac{1}{n!}\left(\frac{\frac{\frac{(26)!}{2!\times(26-2)!}\times(26-2)!}{2!\times(26-4)!}\times\ldots\times(26-2n+2)!}{2!\times(26-2n)!}\right)$$

$$\frac{26!}{n!\times2^{n}\times(26-2n)!}$$

Cabos (n)	Combinações possiveis
0	1
1	325
2	44.850
3	3.453.450
4	164.038.875
5	5.019.589.575
6	100.391.791.500
7	1.305.093.290.000
8	10.767.019.640.000
9	53.835.098.190.000
10	150.738.274.900.000

11	205.552.193.100.000
12	102.776.096.500.000
13	7.905.853.580.550
Total:	532.985.208.200.000

Probabilidade de ordem dos rotores:

Para a ordem dos rotores temos um arranjo simples dado por:

$$A_{(n,p)} = \frac{n!}{(n-p)!}$$

$$A_{(5,3)} = \frac{5!}{(5-3)!} = 5 \times 4 \times 3 = 60$$

Probabilidade de interconexão dos rotores:

Para a interconexão dos contatos do rotor basta realizar:
2 6 × 2 6 = 6 76

Probabilidade de posição inicial dos rotores:

Para calcular a possibilidade da posição inicial dos rotores temos um arranjo de repetição dado por:
2 6 × 2 6 × 2 6 = 1 7.576

Com esses valores, o número total de possibilidades de criptografia é:
5 32.985.208.200.000 × 6 0 × 6 76 × 1 7.576 ≃ 3 , 7 99558597 × 10^{23}

Indução: Técnica de demonstração matemática onde algum parâmetro da proposição a ser mostrado envolve números.

*Seja T uma proposição que queremos provar que é verdadeira para todo valor natural (K+1). Ao invés de provar diretamente que T é valido para todos os valores de K, basta provar que as condições 1 e 3 são validas.

1) Passo Base: Provar que T é válido para T (1)
2) Hipótese de Indução: Assumimos que T(K) é valido
3) Passo Indutivo: Sabendo que T(K) é valido devemos provar que T(K+1) é valido.

Ex.:Teorema: A soma dos n primeiros números é n(n+1) /2
n(n+1) /2 = 1+2+3+...+n

Prova:
- Passo Base: para n = 1
    1=1(1+1) /2
    1=1
- Hipótese de Indução:
Assumimos que a propriedade é válida para um determinado K.
S(K)= K(K+1) /2 = 1+2+3+...+K
- Passo Indutivo:
Devemos mostrar que é valido para S(K+1)
Por definição:
S(K+1)=S(K)+K+1
Por Hipótese de Indução sabemos que S(K)=K(K+1) /2, logo: S(K+1) =(K+1) (K+2)/2
S(K+1) =S(K)+(K+1) =K(K+1)/2 + 2(K+1)/2 = (K+1) (K+2)/2

Ex.: Suponha que um ancestral casou-se e teve dois filhos que formaram a geração 1. Suponha agora que cada um desses filhos teve dois filhos, geração 2 contém 4 descendentes. Imagine que esse processo continua de geração em geração.

Geração	**Descendentes**
1	$2=2^1$
2	$4=2^2$
3	$8=2^3$
n	2^n

Podemos escrever a seguinte proposição: P(n)=2^n (A geração n possui 2^n descendentes)

Passo Base:
$P(1)=2^1=2$
Hipótese de Indução:
P(K)=2^K
Passo Indutivo: Devemos mostrar que P(K+1) =2^K+1
P(K+1) =2*P(K) (P(K)=>Geração anterior)
=2*2^K =2*^K+1

Ex1.:Prove que a equação a seguir é verdadeira para qualquer inteiro n ≥ 1:
1+3+5+...+(2n-1) =n^2 Passo Base:
P (1) $=1=1^2$
    1=1
Hipótese de Indução:
P(K)=1+3+5+...+(2K-1) =K^2

Passo Indutivo:

Tenho que mostrar que:

$P(K+1) = 1+3+5+...+(2K-1) + (2(K+1)-1) = (k+1)^2$
$= K^2+(2(K+1)-1)$
$= K^2+2K+2-1$
$= K^2+2K+1 \rightarrow (K+1)^2$

Ex2.:Prove que a equação é verdadeira para todo $n \geq 1$:

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

Prova:

Passo Base:

$P(1) = 1+2=2^0+2^1=2^1+1-1$
$3=4-1$
$3=3$

Hipótese de Indução:

$P(K)=1+2+2^2+...2^k=2^k+1-1$

Passo Indutivo: Deve mostrar que:

$P(k+1) = 1+2+2^2+\dots 2^k+1=2^(k+1) +1-1$
$=1+2+2^2+\dots 2^k+1$
$=1+2+2^2+\dots+2^k+2^k+1$
$=2^k+1-1+2^k+1$
$=2*2^k+1-1$
$=2^(k+1) +1 -1$ C.Q.D

Ex3.:Prove que para qualquer inteiro positivo n, 2^2n-1 é divisível por 3.

Prova:

Passo Base:

$P(1) = 2^2-1 -1=4-1=3$

Hipótese de Indução:

Supomos que p é válida para n=k

P(k)=2^2k-1 é divisível por 3, ou seja, existe um inteiro m tal que:

2^2k-1=3m
2^2k=3m+1

Passo Indutivo: Provamos que p é válida para k+1

p(k+1) =2^2(k+1) -1 é divisível por 3

2^2(k+1) -1
2^2k+2-1
2^2*2^2k-1
2^2(3m+1) -1
4*3m+4-1
3m*4+3
3(4m+1) que é divisível por 3

EXERCÍCIOS PROPOSTOS:

1)Considere P(n) como a proposição de que $1^2+2^2+...+n^2=(n(n+1)(2n+1))/6$ para todo número inteiro positivo n.

-Qual a proposição P(1)?

-Mostre que P(1) é verdadeira, completando o passo base de demonstração.

-Qual é a hipótese de indução?

-O que você precisa para demostrar o passo indutivo?
-Complete o passo indutivo.
Passo Base:
$P(1)= 1^2 = (1(1+1)(2*1+1))/6$
$1 = 6/6$
$1 = 1$

Hipótese de Indução:
$P(k) =1^2+2^2+...+k^2=(k(k+1)(2k+1))/6$

Passo Indutivo:
$P(k+1) = 1^2+2^2+...+k^2+(k+1)^2=((k+1)((k+1)+1)((2n+1)+1))/6$
$P(k+1) = (k(k+1)(2k+1))/6+(k+1)^2$
$P(k+1) = ((k(k+1)(2k+1))+6(k+1)^2)/6$
$P(k+1) = ((k+1)[k(2k+1)+6(k+1)^2])/6$
$((k+1)(2k^2+7k+6))/6$
$((k+1)(k+2)(2k+3))/6$

2)Considere P(n) como a proposição de que $1^2+2^2+...+n^2=(n(n+1)^2)/2$ para todo numero inteiro positivo n.
-Qual a proposição P(1)?
-Mostre que P(1) é verdadeira, completando o passo base de demonstração.
-Qual a hipótese de indução?
-O que você precisa para demonstrar o passo indutivo?
-Complete o passo indutivo.

3)Demonstre que $1^2+2^2+3^2+...+(2n+1)^2=((n+1)(2n+1)(2n+3))/3$ sempre que n for um numero inteiro não negativo.
Passo Base:
$P(0)= (2*0+1)^2 = ((0+1)(2*0+1)(2*0+3))/3$
$(1)^2 = (1*1*3)/3$
$1 = 3/3$
$1 = 1$
Hipótese de Indução:
$P(k)=1^2+2^2+3^2+...+(2k+1)^2=((k+1)(2k+1)(2k+3))/3$

Passo Indutivo:
$P(k+1)= 1^2+2^2+3^2+...+(2n+1)^2+(2(k+1)+1)^2=(((k+1)+1)(2(k+1)+1)(2(k+1)+3))/3$
$P(k+1)= P(k)+(2(k+1)+1)^2=((k+2)(2k+3)(2k+5))/3$
$P(k+1)= ((k+1)(2k+1)(2k+3))/3+(2k+3)^2=$
$P(k+1)= (2k+3)/3 * [(k+1)(2k+1)(2k+3)]=$
$P(k+1)= (2k+3)/3 * [(k+1)(2k+1)]+(3(2k+3))/3=$
$P(k+1)= ((2k+3)(2k^2+k+2k+1+6k+9))/3=$
$P(k+1)= ((2k+3)(2k^2+9+10))/3=$
$P(k+1)= ((2k+3)(2k+5)(k+2))/3= ((k+2)(2k+3)(2k+5))/3$

4)Demonstre que 2 divide n^2+n sempre que n for um numero inteiro positivo.
Passo Base:
$P(1)= 1^2+1$
P(1)= 2 é divisível por 2

Hipótese de Indução:
P(k)= $k^2+k=2m$

Passo Indutivo:
P(k+1)= $(k+1)^2 + (k+1)$
P(k+1)= $(k^2+2k+1) + (k+1)$
P(k+1)= $(k^2+k) + 2(k+1)$
P(k+1)= 2m+2(k+1) a soma de dois múltiplos de 2 é divisível por 2

5)Demonstre que 3 divide n^3+2n sempre que n for um numero inteiro positivo.
Passo Base:
P(1)= $(1)^3 + 2*1$
P(1)= 3 é divisível por 3

Hipótese de Indução:
P(k)= $k^3+2k=3m$

Passo Indutivo:
P(k+1)= $(k+1)^3+2(k+1)$
P(k+1)= (k+1)(k+1)(k+1)+2(k+1)
P(k+1)= $(k^2+2k+1)(k+1)+2(k+1)$
P(k+1)= $(k^3+k^2+2k^2+2k+k+1)+2k+2$
P(k+1)= $(k^3+3k^2+3k+1)+2k+2$
P(k+1)= $k^3+3k^2+3k+2k+3$
P(k+1)= $k^3+2k+3k^2+3k+3$
P(k+1)= $3m+3k^2+3k+3$
P(k+1)= $3(m+k^2+k+1)$ => t = $m+k^2 + k + 1$
P(k+1)= 3*t => 3 um numero inteiro qualquer positivo retorna um valor divisível por 3

6)Demonstre que 21 divide 4^n+1 + 5^2m+1 sempre que n for um numero inteiro positivo.
Passo Base:
P(1)= 4^1+1 + 5^2*1-1
P(1)= $4^2 + 5^1$
P(1)= 21 que é divisível por 21

Hipótese de Indução:
P(k)= 4^k+1 + 5^2k-1 = 21m

Passo Indutivo:
P(k+1)= 4^(k+1)+1 + 5^2(k+1)-1
P(k+1)= 4*4^k+1 + 5^2k-1+2
P(k+1)= 4*4^k+1 + 5^2k-1 * 5^2
P(k+1)= 4*4^k+1 + 5^2k-1 * 25
P(k+1)= 4*4^k+1 + 5^2k-1 * (21+4)

P(k+1)= 4*4^k+1 + 5^2k-1 * 21+5^2k-1
P(k+1)= 4*(4^k+1 + 5^2k-1) + 21*5^2k-1
P(k+1)= 4* P(k)+ 21*5^2k-1 => P(k) = 21m
P(k+1)= 4* 21m+ 21*5^2k-1 => a soma de 2 termos múltiplos de 21 gera um valor divisível por 21

- **Introdução a Lógica Matemática:**

-Logica Proposicional
Calculo de Predicador: validos e inválidos
Proposição: sentença declarativa a qual podemos atribuir um valor lógico, V ou F, nunca ambos. Em geral pode ser definida à questão de pertinência de um elemento a um conjunto.

Ex.: 2+2=5 P.E.
Brasília é a capital do Brasil P.V.
10>3 P.V.
João é estudante de TADS P.V.
Que horas são?
Leia isso cuidadosamente
x+1=2
Ele é estudante de TADS

-Variáveis proposicionais são indicadas pelas letras p, q,r e s. Seu valor verdade é indicado por V ou F.
-Proposição Simples: não pode ser dividida em proposições menores.
Ex.: q:10>3
r:Natal é a capital de AL
-Proposição Composta: pode ser dividida em proposições menores.
Ex.: Q: 10>3 e Natal é a capital de AL
R: João é magro e alto

-Conectivos Lógicos: utilizados para formar as proposições compostas. São eles:
e: indicado por $\wedge$
ou: indicado por $\vee$
não: indicado por $\neg$ ou ~

Ex.: $2 \geq 3 \equiv p \vee q$
$p: 2 > 3$
$q: 2 = 3$

Ex.: $10 < 5 < -4 \equiv p \wedge q$
$p: 5 > 10$
$q: 5 < -4$

Tabelas dos Conectivos Lógicos:

	p	q			p	q			¬	p	¬p
	F	F			F	F				V	F
	V	F			F	V				F	V
	F	V			V	F					
	V	V			V	V					

Ex.:Construa a tabela verdade para $(p \vee q) \wedge \neg(p \wedge q)$
FAZER
*Proposição Condicional:
Se p então q: $p \rightarrow q$

p	q	$p\rightarrow q$
F	F	V
F	V	V
V	F	F
V	V	V

Ex.: Se Angélica aprender matemática discreta então ela vai arranjar um bom emprego.
Se hoje é sexta então 2 +3 = 5
Obs.: $p \rightarrow q$: $\neg p \vee q$
$\neg (p \rightarrow q)$: $p \wedge \neg q$

*Proposição Bicondicional:
p se e somente se q: $p \leftrightarrow q$

p	q	$p\leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	V	V

$(p\leftrightarrow q) \wedge (q \wedge p)$
Ex.: Você pode tomar o avião se e somente se possui uma passagem.

- **Prioridades de Operadores:**

1º $\neg$ / 2º $\wedge$ / 3º $\vee$ / 4º$\rightarrow$ / 5º$\leftrightarrow$

- **Equivalência Lógica:**

Duas proposições são equivalentes quando possuem a mesma tabela verdade.
$\neg(p\vee q)\equiv\neg p\wedge\neg q$ $\neg(p\wedge q)\equiv\neg p\vee\neg q$

- **Tautologia:**

t é uma tautologia quando for verdadeira independente dos valores assumidos.
Ex.: $t = q\vee\neg q$

- **Contradição:**

c é uma contradição quando for falsa independente dos valores assumidos.
Ex.: $c= q\wedge\neg q$

-Seja t uma tautologia e q uma contradição:
$q\vee t=t$
$q\wedge t=q$
$q\vee a=a$
$q\wedge a=q$

-Proposições Compostas:P e Q são chamadas de logicamente e equivalentes se $p \leftrightarrow q$ for uma tautologia:

$$p \equiv q$$

Ex.:Mostre que $\neg(p \vee q)$ é $\neg p \wedge \neg q$ são equivalentes:
p q
$p \vee q$
$\neg (p \vee q)$
$\neg p$ $\neg q$
$\neg p \wedge \neg q$
$(\neg(p \vee q)$ $(\neg p \wedge \neg q))$

- **Logica de Predicados:**

-Predicados são somente que envolvem variáveis:
$x>3$, $x=y+3$, $x+y=2$
O pc está sob ataque.

-Não são nem verdadeiras e nem falsas enquanto o valor das variáveis não for especificado.
$x>3$: (x):sujeito (é maior que 3):predicado;
-Se $P(x)$: $x>3$. Qual o valor verdade para $P(2)$ e $P(25)$?
$P(2)$:F $P(25)$:V
Logo: $25>3$
-Se $Q(x,y)$: $x=y+3$, quais os valores verdade de $Q(1,2)$ e $Q(3,0)$?
$Q(1,2)$:F $Q(3,0)$:V
Logo: $3=0+3$

Vp:Conjunto verdade de P(x)
D:Domínio
P(x):Predicados em D
-Predicados compostos fazem uso de conectivos lógicos: $\wedge$, $\vee$ e $\neg$

*Qualificadores Lógicos:
-Existencial: $\exists$
-Universal: $\forall$
Qualificadores transformam um predicado em uma proposição.

*Existencial:
$\exists x P(x)$:Proposição
$\exists x P(x)=V \leftrightarrow Vp = \emptyset$
$\exists x P(x)=F \leftrightarrow Vp \neq \emptyset$

Ex.: D={1,2,3,4,5}
    $P(x): x^2>x$
    Vp={2,3,4,5} $\exists x P(x)$? =V
Ex.:$Q(x)$: $x>x^2$
    $Vp=\emptyset$ $\exists x Q(x)$? =F

- **Universal:**

$\forall x P(x)$: Proposição
$\forall x P(x)=V \leftrightarrow Vp = D$
$\forall x P(x)=F \leftrightarrow Vp \neq D$
Ex.:D={1,2,3,4,5}
P(x): $x^2>x$
Vp={2,3,4,5} $\forall x P(x)$? =F
$\neg \forall x P(x)=\exists x \neg P(x)$

- **Quantificadores Agrupados:**

-Ocorre quando um quantificador está no escopo do outro.
Ex.: $\forall x \exists y(x+y=0)$

-Tudo que está no escopo de um quantificador pode ser considerado uma função proposicional.

$\forall x Qx \Rightarrow Qx$ é $\exists y P(x,y) \Rightarrow P(x,y) = (x+y=0)$
$\forall x \forall y((x>0) \wedge (y<0)) \Rightarrow (xy<0)$

Ex.:$\exists x \forall y(x + y = 0)$
Ex.:$\forall x \forall y(x + y = x + y)$
Ex.:$\forall x \exists y(x + y = 0)$
Ex.:$\exists z \forall y(x + y = z)$
Ex.:$\neg \forall x \exists y(x + y = 0)$
$\exists x \neg \exists y(x + y = 0)$
$\exists x \forall y \neg (x + y = 0)$

Exercícios Propostos:

1)Considere que p e q são as proposições: “Nadar na praia em Recife é permitido.” e “Foram descobertos tubarões perto da praia.”, respectivamente. Expresse cada uma das proposições compostas como uma sentença em português.
a)$\neg q$ = Não foram descobertos tubarões perto da praia.
b)$p \rightarrow \neg q$ = Se nadar na praia em Recife é permitido então não foram descobertos tubarões perto da praia.
c)$p \leftrightarrow \neg q$ = Nadar na praia em Recife é permitido se e somente se não forem descobertos tubarões perto da praia.
d)$p \wedge q$ = Nadar na praia em recife é permitido e faram descobertos tubarões perto da praia.
e)$\neg q \leftrightarrow p$ = Se não foram descobertos tubarões perto da praia então nadar na praia em Recife é permitido.
f)$\neg p \wedge (p \vee \neg q)$ =

2)O que é necessário para que uma expressão lógica seja uma tautologia? A expressão $(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$ é uma tautologia?
Quando for verdadeiro independente dos valores assumidos.

p	q	r	$p\to q$	$q\to r$	$p\to r$	$(p\to q)\land(q\to r)\to(p\to r)$
V	V	V	V	V	V	V
V	V	F	V	F	F	F
V	F	V	F	V	V	V
V	F	F	V	V	F	V
F	V	V	V	V	V	V
F	V	F	V	F	V	V
F	F	V	V	V	V	V
F	F	F	V	V	V	V

A expressão não é uma tautologia.

3)O que é necessário para que duas expressões sejam logicamente equivalentes? Determine se as seguintes expressões são logicamente equivalestes utilizando apenas tabela verdade:
$(p\to q)\land(r\to s)$ e $(p\to r)\to(q\to s)$
Quando ambos os resultados são iguais.

p	q	r	s	$p\to q$	$r\to s$	$(p\to q)\land(r\to s)$		$p\to r$	$q\to s$	$(p\to r)\to(q\to s)$
V	V	V	V	V	V	V		V	V	V
V	V	V	F	V	F	F		V	F	F
V	V	F	V	V	V	V		F	V	V
V	V	F	F	V	V	V		F	F	V
V	F	V	V	F	V	F		V	V	V
V	F	V	F	F	F	F		V	V	V
V	F	F	V	F	V	F		F	V	V
V	F	F	F	F	V	F		F	V	V
F	V	V	V	V	V	V		V	V	V
F	V	V	F	V	F	F		V	F	F
F	V	F	V	V	V	V		V	V	V
F	V	F	F	V	V	V		V	F	F
F	F	V	V	V	V	V		V	V	V
F	F	V	F	V	F	F		V	V	V
F	F	F	V	V	V	V		V	V	V
F	F	F	F	V	V	V		V	V	V

A expressão não é logicamente equivalente.

4)Reescreva cada uma das proposições para que as negações apareçam apenas nos predicados:
a)$\neg\exists y\exists x P(x,y)$

$\forall y \neg \exists x P(x,y)$
$\forall y \forall x \neg P(x,y)$

b) $\neg \exists y (Q(y) \wedge \forall \neg R(x,y))$
$\forall y (\neg Q(y) \wedge \forall \neg R(x,y))$

c) $\neg \exists y (\forall x \exists z T(x,y,z) \vee \exists x \forall z U(x,y,z))$
$\forall y (\neg \forall x \exists z T(x,y,z) \vee \exists x \forall z U(x,y,z))$
$\forall y (\exists x \neg \exists z T(x,y,z) \vee \exists x \forall z U(x,y,z))$
$\forall y (\exists x \forall z \neg T(x,y,z) \vee \exists x \forall z U(x,y,z))$
$\forall y (\exists x \forall z \neg T(x,y,z) \forall x \wedge \forall z U(x,y,z))$
$\forall y (\exists x \forall z \neg T(x,y,z) \forall x \exists z \vee U(x,y,z))$