Fernanda Maria de Sousa Vieira

UMA INTRODUÇÃO À COMBINATÓRIA

TÉCNICAS DE CONTAGEM

Universidade Portucalense

Porto, 2007

Fernanda Maria de Sousa Vieira

UMA INTRODUÇÃO À COMBINATÓRIA
TÉCNICAS DE CONTAGEM

Tese submetida ao Departamento de Matemática da Universidade Portucalense para obtenção do grau de Mestre em Matemática / Educação, realizada sob a orientação do Professor Doutor António José Pascoal, professor desta Universidade.

Universidade Portucalense

Infante D. Henrique

Departamento de Matemática

Porto

2007

Aos meus pais.

Agradecimentos

Em primeiro lugar quero agradecer ao meu orientador, Professor Doutor António Pascoal, pela sua total disponibilidade para me receber sempre que o solicitei, pelas suas sugestões e esclarecimentos, pela forma afável com que sempre me tratou mas, principalmente, pelo incentivo e motivação que sempre me deu, não só enquanto orientador mas, também, enquanto professor de duas cadeiras do ano curricular do mestrado. Foi a sua apreciação positiva do meu primeiro trabalho, sobre “Séries de Fourier”, no âmbito da cadeira “Novas Perspectivas da Matemática Aplicada” que, num momento crucial, me convenceu de que valia a pena o esforço e que devia continuar.

À minha família, pelo carinho e pela compreensão demonstrada nos momentos em que não pude estar presente.

Aos meus amigos, pelo apoio e pelas palavras de incentivo pronunciadas no momento certo.

A todos muito obrigada.

Resumo

Todas as civilizações desenvolveram métodos de representação de números - Sistemas de Numeração, sendo os mais antigos que se conhecem os dos Egípcios e dos Sumérios, cerca de 3 mil anos antes da nossa era.

Por volta do início da era cristã surgiram dois conceitos de enorme relevância para a escrita numérica: a numeração de posição e um "acessório" fundamental, o zero.

Foi Leonardo de Pisa que, no séc. XIII, introduziu na Europa o nosso actual sistema de numeração, indo-árabe, que considerava mais adequado às necessidades que, na época, resultavam do desenvolvimento das transacções comerciais entre diversos povos.

Depois dos números inteiros e fraccionários, as ampliações do conceito de número passaram pelos irracionais e pelos imaginários, para já não falar nos hiperreais, nos surreais e nos hipercomplexos.

As propriedades dos números inteiros constituem, ainda hoje, um vasto campo de investigação. Problemas de enunciados extremamente simples mas cuja resolução, é ou ainda desconhecida ou extremamente difícil, têm motivado o desenvolvimento desta área. Como exemplos, podemos referir a demonstração do "Último Teorema de Fermat" que demorou mais de dois séculos a ser encontrada e a inexistência, até hoje, de um algoritmo eficiente para saber se um dado número é ou não primo. Na Teoria dos Números, propriedades que se pensava terem apenas um interesse teórico, revelam-se cada vez mais úteis em aplicações práticas. Um exemplo é a utilização dos números primos na Criptografia.

As necessidades de contagem foram surgindo ao longo da História da Humanidade e, com elas, técnicas cada vez mais complexas. É no séc XVI que, devido às exigências do cálculo das probabilidades ligadas aos seguros de vida e a estudos realizados por diversos matemáticos, sobre os jogos de azar, que o desenvolvimento das técnicas de contagem sofreu um grande impulso. As combinações e as permutações poderão, talvez, ser consideradas as mais simples e as que têm uma utilização mais ampla.

A importância das questões de enumeração tem crescido enormemente nas últimas décadas, muito em função das questões colocadas pela Teoria dos Grafos que se presta à modelação matemática de muitos problemas importantes.

George Pólya, no séc. XX, introduziu uma nova técnica de contagem que se tem prestado às mais variadas aplicações, permitindo tratar desde enumeração do número de isómeros de uma substância até à enumeração de grafos.

A Combinatória, embora tal possa não ser percepcionada pela maioria de nós, contribui decisivamente, e cada vez mais, para a resolução dos problemas da vida moderna.

Abstract

All civilizations have developed methods of representation of numbers - Systems of Numeration, being the oldest known those of the Egyptians and the Sumerios, dated about 3 thousand years b. C.

By the beginning of the Christian age, two concepts of huge relevance for the numerical writing had emerged: the numeration of position and a "main accessory", the zero.

It was Leonardo de Pisa, who, in the XIII. th century , introduced in Europe our current system of numeration, indo-arabe, considered to be more adequate to the requests of the commercial transactions, increasing greatly at the time.

Besides integers and fractionary numbers, the irracitionals and imaginary (not to mention the surreal and the hypercomplex) have been included in the scope of number concept

The properties of integers numbers form, yet, a wide field for research. Development on this area has been achieved due to hard efforts of investigators in order to solve problems of very simple enunciation but whose resolution tends to be, either unknown, or extremely hard to find. Good examples of these are, for instance, the demonstration of the "Last Theorem of Fermat", found only after more than two centuries of research, as well as the inexistence, until today, of an efficient algorithm to verify if a certain number is prime or not. In what Theory of the Numbers concerns, there are some properties that, used to be thought as no more than theoretically interesting, are becoming more and more important and useful in practical applications. An example of such is the use of the prime numbers in Criptografia.

Counting has been a demand of humankind along History, requiring the development of more and more sophisticated techniques. A noticeable increase on this area has been reached in the XVI.th century, as a result of the requirements of the probability calculation associated with life insurance issues and the studies on gambling (games of chance) carried out by several mathematicians. Amongst counting techniques, the simplest and most used are, perhaps, combinations and permutations. The importance of the enumeration subject has grown enormously

in the last decades, due to the questions set up by the Graph Theory, very appropriate for mathematical modeling of many important problems.

George Pólya, in the XX.th century, introduced a new enumeration technique, allowing a large range of applications, from the counting of isomers contained in a substance, to the graphs enumeration matter. The Combinatória, despite some unawareness from most people about the fact, concurs decisively and increasingly for the resolution of many problems of modern life.

Índice

Índice de Figuras

Índice de Tabelas

Introdução

Na escolha do tema para a dissertação do Mestrado em Matemática/Ensino quis, desde logo assegurar a respectiva ligação à minha actividade como professora de Matemática do Ensino Secundário.

Assim, foi considerado que, de entre as diversas opções possíveis, um tema que, para além de cumprir esse requisito, se me afigurou um interessante e vasto campo de investigação, foi o das técnicas de contagem que acabou por dar origem ao meu trabalho.

Julgo que ao enveredar por este caminho terei conseguido, não só enriquecer os meus conhecimentos, como também criado melhores condições para leccionar, como era meu propósito.

Neste âmbito, vem-me imediatamente à ideia a aplicação prática que pode ser conseguida no capítulo do programa de Matemática do Ensino Secundário dedicado ao tema " Probabilidades e Combinatória" considerado difícil por muitos alunos e mesmo por alguns professores.

Sem menosprezar essa reserva que às vezes nos intimida na abordagem de um tema tão especial, devo dizer que sempre me senti fascinada pela sua peculiaridade: a organização e o engenho necessários na resolução (quando conseguimos lá chegar…) de problemas só aparentemente simples e, uma vez encontrada a "chave", a sensação de que, afinal, era tão simples !

Sendo os números a base das contagens pareceu-nos adequado contextualizar, no tempo, a forma como foram surgindo. Assim, o primeiro capítulo apresenta um breve resumo histórico do aparecimento dos números, com particular destaque para o algarismo zero, não só por significar um avanço no conceito abstracto de número mas também, pelas implicações que sua existência/inexistência têm na vida quotidiana: pense-se no nosso calendário e na discussão que teve lugar, aquando da mudança do milénio.

No capítulo seguinte, referimos algumas propriedades dos números inteiros, pelo interesse e entusiasmo que sempre despertaram nos Homens de Ciência e pela relevância de algumas dessas noções para a compreensão dos capítulos seguintes. Destacamos a noção de congruência, os números primos e os problemas de aplicação apresentados.

O terceiro capítulo refere técnicas de contagem, do princípio fundamental da contagem às permutações e combinações. A distribuição de objectos em caixas, nas suas diversas variantes, tem um destaque especial, por servir de modelo matemático na resolução de inúmeros problemas. O famoso triângulo de Pascal é também aqui abordado pela sua riqueza matemática.

Poderá estranhar-se não haver qualquer referência aos "arranjos". Essa omissão é deliberada, porquanto entendemos ser possível resolver os problemas de contagem sem a utilização dessa noção, optando, assim, por seguir a linha da escola anglo-saxónica. Aliás, o excesso de fórmulas é por vezes castrador do raciocínio matemático. De facto, constata-se que, na leccionação do tema "Probabilidades e Combinatória", no Ensino Secundário, os alunos antes de serem munidos das fórmulas de permutações, arranjos e combinações, procuram estratégias de contagem para resolver os problemas que lhes são colocados. Após a apresentação das fórmulas referidas, observa-se que deixam de reflectir na resolução do problema, manifestando apenas preocupação em rotulá-los como arranjos ou combinações limitando-se, em seguida, a aplicar a respectiva "receita". Exige-se nesta fase, um grande esforço por parte dos professores para combater esta atitude, que alguns alunos persistem em manter mesmo após ser mostrado, com exemplos, que nem todos os problemas se "encaixam" numa dessas categorias. Enquanto que a fórmula das combinações facilita a contagem, principalmente quando o número de objectos é elevado, os arranjos são desnecessários.

No capítulo seguinte, "Grafos" é feita uma abordagem às noções base desta teoria. A par do clássico problema das "Sete Pontes de Königsberg", um marco no início da Teoria dos Grafos e do tão conhecido "Teorema das Quatro Cores", outros exemplos de aplicação são apresentados.

Funções geradoras são um instrumento matemático desenvolvido por De Moivre, Stirling e Euler no séc XVIII e são frequentemente usadas em Combinatória. No último capítulo deste trabalho, abordamos apenas a fórmula de Pólya e o Teorema de Burnside com algumas aplicações concretas.

1. Breve resenha histórica do aparecimento dos números

"Os números governam o mundo". (Platão)[1]

O aparecimento do conceito de número surgiu da necessidade que o Homem teve de contar. Contar os indivíduos da sua tribo, os animais do seu rebanho, controlar as trocas comerciais, etc. Conta-se que os pastores usavam pedrinhas para "contar" as ovelhas dos seus rebanhos, efectuando uma correspondência biunívoca, em que a cada pedra correspondia uma ovelha e a cada ovelha uma pedra. Através deste processo era possível saber se tinham perdido algum animal. Utilizavam, também, para contar, os dedos, nós em cordas, marcas em ossos,… O conceito de número surge, assim, da noção de correspondência, objecto a objecto.

Como Aristóteles observou há muito tempo, o uso, hoje difundido, do sistema decimal é, apenas, o resultado do acidente anatómico de que quase todos nós nascemos com dez dedos nas mãos e dez dedos nos pés. Embora historicamente, contar pelos dedos, ou o uso de contar por grupos de cinco e dez pareça ter surgido mais tarde que a contagem por dois e três, os sistemas quinário e decimal quase invariavelmente, sobrepuseram-se ao binário e ao ternário. Um estudo de várias centenas de tribos entre os índios americanos, por exemplo, mostrou que, quase um terço, usava a base decimal e, aproximadamente outro terço, usava um sistema quinário ou quinário-decimal, menos de um terço tinha um sistema binário e, os que usavam um sistema ternário, formavam menos de um por cento do grupo. O sistema vigesimal, com base vinte, ocorria em cerca de 10 por cento das tribos. (Boyer, C.)

O mais antigo registo conhecido é talvez o que aparece nas tábuas de argila dos Sumérios, habitantes da Mesopotâmia[2] que datam da primeira metade do 3º milénio a.C. [3] A matemática na Mesopotâmia surgiu como uma ciência prática, com o objectivo de facilitar o cálculo do calendário, a administração das colheitas e a cobrança de impostos.

[1] http://www.somatematica.com.br/frases.php
[2] Geograficamente a Mesopotâmia está situada entre os rios Tigre e Eufrates no Oriente Médio, no chamado crescente fértil, onde actualmente se localiza o Iraque e a Síria. Em grego, a palavra Mesopotâmia significa entre rios.
[3] http://www.educ.fc.ul.pt/icm/icm2002/icm101/pagina1.html

O início da ciência ocidental é situado por volta de 3000 a. C. Nessa altura a Mesopotâmia foi invadida por um povo cuja origem é desconhecida: os Sumérios. Instalaram-se no país de Sumes, na região entre o que veio a ser a cidade de Babilónia e o Golfo Pérsico.

Este povo habitava cidades-estado cujos nomes ainda hoje são mencionados: Ur (Abraão), Uruk, Nippur, Zagash.

A sua linguagem era do tipo aglutinante e é hoje muito difícil de decifrar nos seus escritos em tábuas de argila.

Mais uma vez, a linguagem matemática foi a mais simples de interpretar e assim verificou-se que o seu sistema de numeração tinha base 60, e a escrita dos números era uma combinação:

- Numeração de justaposição.
- Aglomeração de unidades.

Os números do intervalo [1, 59] eram formados de maneira análoga à posterior numeração romana e isso, talvez, porque 60 é uma base relativamente elevada. De 60 em 60, usavam o sistema de numeração de posição.

Marcas em forma de cunha eram feitas em tábuas de argila mole que depois eram cozidas. Este tipo de escrita chama-se cuneiforme (do latim *cuneus*, cunha). O sistema sumério foi posteriormente adoptado pelos Babilónios que usavam o sistema sexagesimal, com símbolos individuais para 1, γ e ◀ para 10.

Ainda hoje usamos o sistema sexagesimal para medir ângulos em graus e medir o tempo em horas.

São várias as explicações apresentadas para a escolha da base 60.

Uma explicação, talvez a mais popular, está relacionada com o facto de, entre esses povos, a astronomia estar muito desenvolvida, por motivos religiosos; ter-se-ão dado conta de que o ano tem 365 dias e tomado 360 para arredondar. Isso tê-los-á conduzido à divisão do círculo em 360 partes iguais (graus) e, também por motivos geométricos, atribuir importância a 1/6 do círculo, isto é, 60 graus, e daí a base escolhida. (Nogueira, J.)

Uma outra explicação refere que a base 60 surge como combinação de duas bases, a base 5 que utilizava os dedos das mãos para contar e a base 12 que utilizava as três falanges de cada dedo. Na mão direita, contavam-se as

falanges, tal como na base 12, "guardando" o número de contagens na mão esquerda, assim como na base 5, como ilustra a figura seguinte:[4]

***Figura 1* - Sistema de contagem sexagesimal.**

No entanto, Boyer em "História da Matemática", considera que provavelmente adoptaram a base 60 pela facilidade em dividir sessenta unidades em metades, terços, quartos, etc.

Os Egípcios construíram uma representação hieroglífica dos números na base 10, em que as potências de 10 são representadas por símbolos especiais.

Símbolo Egípcio	Descrição do símbolo	O número na nossa notação
|	Traço vertical	1
∩	Osso do calcanhar	10
𓍢	Rolo de corda	100
𓆼	Flor de lótus	1000
𓂭	Dedo a apontar	10 000
𓆛	Peixe	100 000
𓁨	Homem ajoelhado	1 000 000

Figura 2 – Numeração Egícia

[4] *http://www.educ.fc.ul.pt/docentes/opombo/seminario/algarismos/sumeria.htm*

Por exemplo representavam o número 3252 da seguinte forma:

O conhecimento dos métodos de cálculo egípcios provém de alguns papiros[5], sendo o papiro de Rhind[6] um dos mais importantes, escrito por volta de 1650 a. C. mas só adquirido em 1858, no Egipto, por um antiquário chamado A. Henry Rhind. O papiro, com aproximadamente 30 cm de largura e vários metros de comprimento, cerca de 5 m, encontrava-se danificado, faltando-lhe alguns fragmentos, só encontrados anos mais tarde no Museu de Brooklyn. Eles tinham sido obtidos, pelo coleccionador Edwin Smith e permitiram esclarecer alguns pontos. Actualmente, o papiro faz parte da colecção Rhind, existente no British Museum.

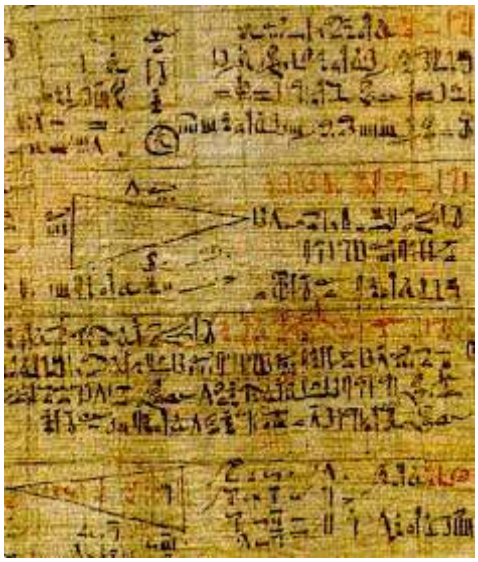


Figura 3 - Papiro de Rhind[7]

O papiro de Rhind mostra o uso de fracções[8], a resolução de equações simples e de progressões, a medição de áreas de triângulos, trapézios e rectângulos, o cálculo de volumes de cilindros e prismas, etc. Das indicações dadas pelo papiro de Rhind, infere-se que os geómetras egípcios atribuíam ao número *pi* um valor equivalente ao quadrado da fracção 16/9 que daria, em número decimal, 3,1605, valor no qual *pi* apresenta um erro que não chega a dois centésimos da unidade![9]

---

[5] O papiro é uma planta originária do Egipto. Aproveitavam-se as folhas humedecidas e colocavam-se a secar sobre tábuas. Obtinham-se assim longos rolos onde se faziam registos.

[6] Também conhecido por papiro de Ahmes, nome do escriba egípcio que o copiou por volta de 1650 a. C.

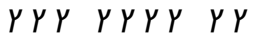
[7] http://www.educ.fc.ul.pt/docentes/opombo/seminario/rhind/inicio.htm

[8] *Os egípcios tinham uma notação especial para as fracções unitárias, isto é, de numerador 1, colocavam um símbolo oval acima do número inteiro, por exemplo, 1/30*

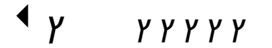
[9] http://www.educ.fc.ul.pt/icm/icm99/icm36/papiro_de_rhind.htm

Enquanto que os Mesopotâmios usavam as placas de argila, muito resistentes, para os seus registos e os Egípcios usavam os papiros, com grande poder de conservação, os Chineses e Indianos usavam material mais frágil como a casca de árvore e o bambu, dificultando a localização temporal das suas descobertas.

As matemáticas mesopotâmicas atingiram um nível mais elevado do que as matemáticas egípcias. Enquanto que, nestas últimas cada unidade mais elevada era indicada por um novo símbolo, os Sumérios usavam o mesmo símbolo, mas indicavam o seu valor pela sua posição. Assim por exemplo,



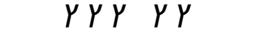
ou seja, 3 seguido de 4, seguido de 2 significava $3\times 60^2+4\times 60+2=11042$. Este sistema, semelhante ao actual, de base 10, tinha vantagens enormes para o cálculo. No entanto, havia algumas ambiguidades e incertezas, como por exemplo, o espaço em branco que significava por vezes zero, de modo que



Isto é, (11, 5) podia representar $11\times 60^2+5=39605$ mas, facilmente era confundido com $11\times 60+5=665$. Só muito mais tarde é que apareceu um símbolo para representar o zero. (Struik)

No tempo dos Alexandrinos (Período Helenístico) usava-se um sinal para indicar ausência de unidades de certa ordem, sinal que corresponde ao zero actual e que era originário da letra grega “omicron”. Foi encontrado com grande surpresa em escritos da época, pois até aí admitia-se que zero teria sido inventado pela civilização Hindu.

O facto de também usarem o princípio da posição nas fracções permitia escrever fracções diferentes das unitárias, ultrapassando assim o sistema dos Egípcios . De facto, a representação,



era usada não só para $3\times 60+2$ mas também, para $3+2\times 60^{-1}$ ou $3\times 60^{-1}+2\times 60^{-2}$.

Um sistema não posicional semelhante ao Egípcio é o sistema Romano. Usavam neste caso, letras para representar números.

I	1
V	5
X	10
L	50
C	100
D	500
M	1000

***Figura 4* - Sistema numeração romana**

Roma, fundada em 753 a.C foi o centro de uma das mais notáveis civilizações da antiguidade. Por volta do século III, o império romano atravessou uma enorme crise económica e política. A corrupção dentro do governo e os gastos sumptuários desviaram os recursos necessários ao investimento no exército romano. Com o fim das conquistas territoriais, diminuiu o número de escravos, o que provocou uma queda na produção agrícola.

Em crise, com o exército enfraquecido e as fronteiras cada vez mais desprotegidas, Roma era invadida por outros povos. Foi o fim do Império Romano do Ocidente. No entanto o Império Romano do Oriente, também conhecido como Império Bizantino, com capital em Constantinopla, sobreviveu até 1453.

Embora os romanos sejam autores de muitas construções impressionantes, conservaram um sistema numérico, onde até uma simples adição ou mesmo a representação de grandes números era difícil de fazer. Um romano sentir-se-ia certamente embaraçado se, com o seu sistema numérico, tivesse de representar a quantidade “um milhão”. Teria, pura e simplesmente, de dispor de espaço suficiente para escrever mil vezes o símbolo M, que representa, como se sabe mil e é o mais “valioso” símbolo do sistema.

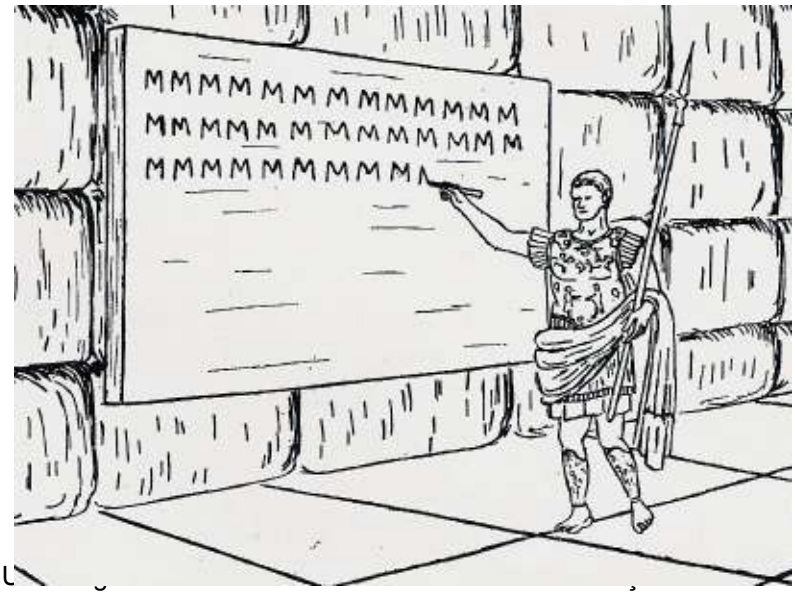


Figura 5 – Um romano a escrever um milhão

A notação usada sofreu ao longo do tempo algumas variações, por isso, é fácil encontrar inscritos em monumentos datas cuja leitura não é igual à que conhecemos actualmente. O sistema Romano é, ainda hoje, usado na representação de séculos, nomes de reis e papas, capítulos de livros,…

O sistema de numeração grego baseava-se na escrita da primeira letra do número para representá-lo, por exemplo, usavam P (pente) para 5, H para Hekaton (100), X para Xhilioi (1000) e M para Murioi (10 000). Neste sistema, o algarismo 1 era escrito com uma linha vertical "I", à semelhança da numeração romana.

Figura 6 – Numeração Grega

Progressivamente este sistema evoluiu e passou a usar os sucessivos símbolos do alfabeto grego para exprimir, primeiro, os nossos

algarismos 1, 2, ..., 9, depois, as dezenas de 10 a 90 e, finalmente, as centenas de 100 a 900.

Três letras arcaicas extra, foram acrescentadas às 24 letras do alfabeto grego, para que se obtivessem os 27 símbolos necessários. Com a ajuda deste sistema, qualquer número menor que 1000 podia ser escrito com, no máximo três símbolos.

A representação dos números era feita da seguinte forma:

Figura 7 – Símbolos da numeração Grega

Por exemplo,
781 em numeração grega escreve-se $\psi\pi\alpha$ (700+80+1);

Para representar milhares, até 10.000 exclusive, fazia-se uma marca à esquerda da letra. Por exemplo:

5000 em numeração grega escreve-se $'\varepsilon$

9888 em numeração grega escreve-se $'\theta\omega\pi\eta$ (9000+800+80+8);

Foi o célebre sábio do Sec. III a. C., Arquimedes[10], que demonstrou ser possível representar grandes números através da escrita. Para ele, deveria ser

[10] Arquimedes, matemático e inventor grego, nasceu em Siracusa, na ilha da Sicília. Foi o mais importante matemático da Antiguidade. Os seus principais achados pertencem aos campos da aritmética, mecânica e hidrostática. Deve-se a ele a invenção do parafuso, das roldanas, da roda dentada, o cálculo do número "pi" e a medição de áreas de figuras geométricas. Formula, também,

possível representar números para além do que pudessem ser as necessidades de contagem, por maiores que elas fossem, como por exemplo os grãos de areia da Terra inteira, (ou do Universo).

O método por ele então proposto é semelhante ao usado na actualidade: partindo do maior número existente – na altura, no sistema da sua civilização, a míriade, correspondente a 10 milhões – introduziu um novo número, a miríade de míriade, equivalente, portanto, a 100 milhões, que designou por óctuplo, unidade de segunda classe, depois óctuplo do óctuplo, unidade de terceira classe e, assim sucessivamente. Este processo possibilitou a escrita de um número colossal que designou por *"myriakis mtriostas periodou myriakis myrioston arithmon myriai myriades",* que corresponde em notação actual a 10^{80}. Posteriormente calculou o número de grãos de areia que seriam necessários para preencher todo o Universo então conhecido e apercebeu-se que era inferior: aproximadamente 10^{63} (esta conjectura é muito interessante, pois hoje, séc. XXI estima-se em 10^{60} o número de estrelas no Universo conhecido).

E no tempo dos antigos quando se falava em grandes números, nem sequer era preciso pensar em coisas como os grãos de areia de toda a terra ou todos os peixes do mar. Eles surgiam em situações bem menos extraordinárias e muitas vezes de forma inesperada. Um exemplo pode ser configurado pela célebre história que se conta como tendo sido passada entre o grão-vizir Sissa Ben Dahir, hábil matemático, e o Rei Shiram das Índias. Reza a lenda que o Rei tendo ficado maravilhado com a invenção do jogo de xadrez, quis recompensar o seu autor, o grão-vizir, deixando à livre escolha deste o prémio. O inventor propôs-lhe, então, a oferta de um grão de trigo pela primeira casa do tabuleiro do jogo, dois grãos pela segunda casa, quatro pela terceira e, assim, sucessivamente, duplicando a quantidade de grãos de uma casa para a casa seguinte, até serem cobertas as 64 casas do tabuleiro.

O soberano, considerando o pedido bem modesto, ordenou que fosse trazido um saco de trigo para o efeito e a contagem começou de acordo com a regra estabelecida. No entanto, rapidamente se verificou que todo o saco não

a teoria da alavanca simples, resumida na célebre frase : «Dai-me um ponto de apoio e levantarei a Terra.»

ultrapassou a necessidade de preenchimento da vigésima casa do tabuleiro. Um segundo saco tomou o lugar do primeiro e um terceiro e um quarto vieram e foram esvaziados, até se concluir que nem toda a colheita de trigo das Índias seria suficiente para que o rei pudesse cumprir a sua promessa.

Para poder fazê-lo, precisaria de dar ao seu grão-vizir 18 446 744 073 709 551 615 grãos! Este valor corresponde à soma dos primeiros 64 termos de uma progressão geométrica de razão 2, cujo primeiro termo é 1.

***Figura 8* - O grão-vizir e Sissa Ben Dahir e o Rei Shiram das Índias**

Por maiores que sejam todos estes números de que temos vindo a falar, todos eles são, na verdade, passíveis de representação numérica, visto serem finitos.

Há mais de dois mil anos que o Homem anda às voltas com o infinito. Essa noção surge em questões como: Quantos são os números inteiros?; Qual o número de pontos de uma recta?. Será possível comparar dois números infinitos?

Esta última questão foi estudada, em 1638, por Galileu. Chegou à conclusão de que as relações *igual, maior* e *menor* podem aplicar-se a conjuntos finitos mas não aos infinitos.

Mas foi George Cantor (1845 – 1918)[11] o matemático que mais contribuiu para a evolução do conceito de infinito, através do seu trabalho no âmbito da teoria dos conjuntos. Considerou que se entre dois conjuntos infinitos é possível fazer corresponder um elemento de um dos conjuntos a um elemento do outro conjunto, sem que sobrem elementos, então os dois infinitos são iguais. Se pelo contrário, ao considerar esses pares de elementos, sobrarem elementos num dos conjuntos, este é um infinito maior que o outro.

Esta simples análise conduz a algo extraordinário. Aceita-se facilmente que existem tantos números pares como ímpares, visto que usando a ideia de Cantor, pode-se fazer corresponder ao primeiro número par o primeiro número ímpar, ao segundo número par o segundo número ímpar e assim sucessivamente. Mas quando comparamos por exemplo, o conjunto de todos os números naturais com o conjunto dos números pares, poder-se-ia pensar que o primeiro conjunto tem um cardinal superior ao segundo. No entanto, usando novamente, a ideia de Cantor, da correspondência entre os elementos dos dois conjuntos, temos

1	2	3	4	5	6	7	8	
↕	↕	↕	↕	↕	↕	↕	↕	....
2	4	6	8	10	12	14	16	

Ou seja, é possível estabelecer uma correspondência biunívoca entre os dois conjuntos pelo que têm ambos o mesmo cardinal.

Assim, Cantor chegou à notável conclusão de que, quando estamos a considerar quantidades infinitas, o todo nem sempre é maior do que cada uma das suas partes. Qualquer conjunto infinito cujos elementos sejam os elementos de qualquer subconjunto de números inteiros, tem exactamente a mesma cardinalidade que o conjunto de todos os números inteiros.

Existem vários paradoxos sobre números infinitos, um dos mais conhecidos é o paradoxo do “Hotel de Hilbert”, apresentado pelo matemático alemão David Hilbert.

[11] Matemático alemão de origem russa. Desenvolveu a Teoria dos Conjuntos, foi considerado o inventor da “aritmética do infinito” Foi professor da Universidade de Halle, a partir de 1872. Apresentou um teorema sobre a diferenciação de cardinalidade entre os números reais e racionais. *Provou que o conjunto dos números racionais Q é numerável, enquanto que o conjunto dos números reais IR é contínuo (logo, maior que o anterior).* Mas ao tentar provar a hipótese do contínuo, foi duramente atacado por não chegar a uma conclusão consistente, o que agravou o seu estado de saúde mental. Uma forte depressão o abateu obrigando o seu internamento num manicómio, onde terminou seus dias, antes de ser reconhecido como pensador genial.

Quando um hotel com um número finito de quartos fica cheio, não há mais espaço para novos hóspedes. Agora, imagine-se um hotel com um número infinito de quartos. Quando todos os quartos forem ocupados por infinitos hóspedes, como alojar um novo hóspede? A solução para este problema seria mover o hóspede do quarto 1 para o quarto 2, o do quarto 2 para o 3, e assim por diante. Dessa forma, seria possível hospedar mais uma pessoa no quarto 1. Analogamente será possível hospedar infinitos hóspedes, mesmo com o hotel lotado: muda-se a pessoa do quarto 1 para o quarto 2, a pessoa do quarto 2 para o quarto 4, a pessoa do quarto 3 para o quarto 6, e assim por diante. Todos os quartos que ficarem vazios poderão ser ocupados por mais infinitas pessoas. É aí que está o paradoxo: se os primeiros infinitos hóspedes saírem, o hotel ainda terá infinitos hóspedes.

E se definirmos conjunto infinito como aquele cuja cardinalidade é igual à de qualquer um dos seus subconjuntos infinitos? Dentro da definição de Cantor, deixa de haver paradoxos.

O nosso actual sistema de numeração decimal teve a sua origem na matemática hindu.

A notação indiana mais antiga consistia em traços verticais dispostos em grupos. Posteriormente, deu-se uma evolução na representação destes algarismos, tendo sido adoptados novos símbolos para representar quatro, dez, vinte e cem. Essa escrita foi sofrendo alterações, dando lugar aos algarismos ditos “brahmi”.

Provavelmente, os chamados numerais hindus foram resultado de desenvolvimento interno, apenas; talvez se desenvolvessem primeiro ao longo dos limites ocidentais entre a Índia e a Pérsia, onde a lembrança da notação posicional babilónica pode ter levado à modificação do sistema “brahmi”. (Boyer, C.)

A transformação do sistema “brahmi” em sistema posicional reduziu os símbolos existentes aos primeiros nove (ainda não era conhecido o zero).

Algarismos *brahmi*	Representam
	1
	2
	3
	4
	5
	6
	7
	8
	9

Figura 9 – Algarismos brahmi

O Mundo Árabe rico em cultura e tradições, participou activamente no desenvolvimento da cultura Europeia. O seu povo viajava constantemente, contactando com outras civilizações e saberes que assimilavam e desenvolviam.

Foi assim, que conheceram o sistema numérico hindu, no qual foram introduzindo diversas alterações.

O 1 indiano 	*tornou-se*
O 2 indiano 	*tornou-se* ...  ...
O 3 indiano 	*tornou-se* ...  ...
O 4 indiano 	*tornou-se* ...  ...
O 5 indiano 	*tornou-se* ... ...
O 6 indiano 	*tornou-se* ... ...
O 7 indiano	*tornou-se* ... ...
O 8 indiano	*tornou-se* ... ...
O 9 indiano	*tornou-se* ... ...

Figura 10 – Símbolos do sistema numérico hindu

Al-Khwarizmi[12] teve um papel importante na história da matemática, tendo sido através dos seus livros de matemática e astronomia que os numerais indianos e a álgebra árabe chegaram à Europa Ocidental.

***Figura 11* - Al-Khwarizmi**

Supõe-se que um tratado de aritmética intitulado *"Algoritmi de numero Indorum",* que se encontra na biblioteca da Universidade de Cambridge e foi publicado pelo príncipe Boncompagni em Roma, em 1857, seja a tradução latina da aritmética que *Alguarismi* ou *Alkarismi* (forma incorrecta de Al-Khovarismî, nome pelo qual é conhecido o mais ilustre dos matemáticos árabes, Abucháfar Mohámed Abenmusa, de Khorassan na Pérsia), escreveu em Bagdad (em 839), quando regressou de uma missão científica ao Afeganistão e à Índia, realizada por ordem do califa Almamon, de quem Alkarismi foi bibliotecário. (Vasconcellos)

O nosso sistema é por isso chamado de indo-arábe, construído pelos hindus e divulgado pelos árabes.

Um matemático que se debateu pela introdução na Europa do sistema indo-árabe foi Leonardo de Pisa (1180-1250) mais conhecido por Fibonacci (por ser um diminutivo de fillius Bonacci que queria provavelmente dizer filho de Bonacci). Desde cedo contactou com os negócios do pai, um comerciante habituado a transacções com vários países. Interessado pela matemática aprendeu, durante as suas viagens, vários sistemas numéricos incluindo os métodos hindus de cálculo (aritmética de posição), que considerou como os melhores.

Figura 12 – Leonardo de Pisa

[12] Também chamado Alkarismi. Matemático, astrónomo, nasceu em Khiva, hoje no Uzbequistão, por volta de 780 e morreu em Bagdad por volta de 850. A palavra álgebra deriva do título de um de seus livros *al-Kitāb al-mukhtasar fi hisab al-jabr wa'l-muqābalah* ("Compêndio sobre a transposição e a redução") e por conseguinte ele é considerado o "pai" da álgebra. As palavras algarismo e algoritmo são derivadas do seu nome. Devem-se também a Al Khawarizmi um tratado de geometria, tábuas astronómicas e outros trabalhos em geografia, como o seu livro "Suratul Ardh" (imagem da Terra).

No regresso do Oriente a Pisa, escreveu, em 1202, a célebre obra "*Liber Abaci*". Não é um livro sobre o ábaco como o título poderia sugerir, mas um tratado sobre métodos e problemas algébricos, nos quais utiliza e explica o sistema de numeração indo-árabe e salienta as vantagens deste sistema em relação ao sistema romano.

John de Halifax (cerca de 1200-1256), também conhecido por Johannes Sacrobosco[13], escreveu "*Algorismus vulgaris"* baseado nas obras de Al-Khwarizmi e Fibonacci, o qual se tornou no livro de matemática mais popular nas universidades medievais e, assim, divulgou o sistema posicional decimal e suas técnicas de cálculo na comunidade científica. No entanto só mais tarde e de forma muito lenta, é que se começou a adoptar este sistema.

O Zero

O número zero, hoje tão banal, nem sempre existiu, porque durante muito tempo, não foi compreendida a necessidade de representar o nada. Foi necessária uma considerável dose de abstracção para a invenção e uso do zero.

A noção de zero é uma das mais fundamentais da Matemática, mas há que distinguir a noção de algarismo zero, símbolo numérico usado para formar números (por exemplo 4503 é diferente de 453), da noção de número zero, associado à ideia de quantidade.

Em alguns sistemas numéricos, o zero foi inicialmente representado por um espaço vazio, como já foi referido no caso da Mesopotâmia, o que gerava por vezes alguma confusão na leitura dos números, alguns só entendidos mediante o contexto em que surgiam. Os babilónios chegaram a empregar um símbolo, formado por duas cunhas inclinadas para representar o zero, representando a ausência de uma potência de base 60, mas nunca usaram esse símbolo no início ou no final de um número.

[13] *Matemático e astrónomo britânico, grande conhecedor dos métodos árabes de aritmética, álgebra e astronomia. As suas obras foram de grande influência na Europa entre os séculos XIII e XVII. Estudou em Oxford e foi morar em Paris (1220), onde permaneceu até sua morte, e foi nomeado professor de matemática na Universidade de Paris (1221)*

É possível que o mais antigo símbolo hindu para zero tenha sido o ponto negrito, que aparece no manuscrito Bakhshali,[14] cujo conteúdo talvez remonte ao século III ou IV.[15]

Na obra "*Liber Abaci*" Fibonacci, descreve os nove algarismos indianos juntamente com o símbolo 'O' chamado "*zephirum''* (forma latina) e "*sifr*", em árabe. É destas palavras que derivam os nomes actuais de "zero" e "cifra". (J.M.E.)

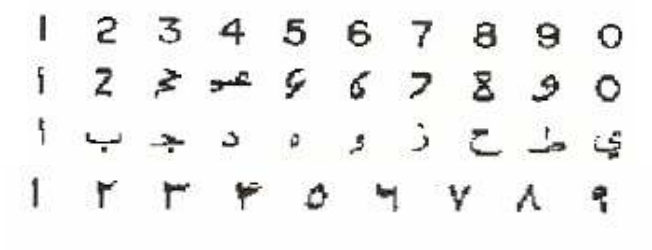


***Figura 13* - Evolução dos algarismos**

A inexistência do ano zero no calendário da era cristã causou, recentemente, confusão quanto à passagem do milénio. Muitas pessoas foram de opinião que a mudança de milénio ocorreria às zero horas do dia 1 de Janeiro de 2000, enquanto que, para outras, ocorreria precisamente daí a um ano.

O nosso calendário está baseado no que em Astronomia se chama o Ano Trópico que corresponde a 365.242199 dias, o tempo que a Terra demora a efectuar uma revolução em torno do Sol, em relação ao ponto vernal, início da Primavera.

O calendário, resultando de uma convenção tem sofrido, ao longo da História, alguns ajustes.

A primeira alteração data de 46 a. C. e foi efectuada por ordem de Júlio César que instituiu os anos bissextos, isto é, anos com 366 dias de quatro em quatro anos. Assim, em média, cada ano teria 365.25 dias o que corresponde a

[14] *Descoberto em 1881 por um agricultor numas ruínas perto da aldeia de* Bakhshali, *actualmente no Paquistão. Não se sabe ao certo a sua data de origem; alguns autores apontam como sendo de entre 200 a 400 d.C. O manuscrito contém diferentes regras e problemas, juntamente com as suas soluções. Os problemas dizem respeito sobretudo a aritmética, "álgebra", e alguns problema de geometria e medida.*

[15] http://www.somatematica.com.br/historia/zero.php

cerca de 11 minutos e 14 segundos a mais do que o ano Trópico, gerando ao fim de um número significativo de anos, desajustes em relação às estações do ano.

Novamente no século VI, o calendário foi alterado pelo monge Dionysius Exiguus que, por incumbência do Papa João I, fez um estudo para determinar, nos 95 anos seguintes, as datas do Domingo de Páscoa, primeiro domingo após a primeira lua cheia depois do equinócio[16] de Primavera.

Para facilitar os cálculos[17], Dionysius propôs uma redefinição da contagem dos anos, tendo pensado num acontecimento histórico para assinalar o início da nova era. O facto de ser monge cristão deve ter influenciado a escolha do nascimento de Cristo. O ano do nascimento de Cristo passou, então, a ser considerado o ano 1 do século I e os períodos anteriores e acontecimentos anteriores passaram a ser datados com a sigla a. C. (antes de Cristo) e contados de trás para diante

Muito provavelmente, Cristo não nasceu nesse ano e muito menos em 25 de Dezembro. A história parece mostrar que Cristo terá nascido nos anos 7 a 4 *antes de Cristo.* O Evangelho segundo São Mateus afirma que Cristo nasceu durante o reinado de Herodes, a mando do qual ocorreu a “degola dos inocentes” e este terá morrido quatro anos antes da nova era. (Buescu)

A reforma que instituiu o actual calendário data de 1582, quando o Papa Gregório XIII, com o fim de novamente colocar o início da Primavera em 21 de Março, ordenou: um salto de dez dias, o dia seguinte a 4 de Outubro de 1582 passou a ser o dia 15 de Outubro de 1582 e proclamou que os anos divisíveis por 100 só seriam bissextos se fossem também divisíveis por 400. Assim, 1700, 1800, 1900 não foram bissextos, mas 1600 e 2000 já foram.

Com esta alteração, o calendário Gregoriano voltou a ser ajustado ao ano Trópico, com um erro de 1 dia em cada 3300 anos.

O facto de o ano zero não fazer parte do calendário construído por Dionysius e a numeração começar no ano 1, conduz a que todos os séculos comecem em anos como, por exemplo, 1, 101, 1001, 1901, 2001, etc.

[16] A palavra equinócio vem do Latim e significa "noites iguais". Os equinócios acontecem em Março e Setembro, as duas ocasiões em que o dia e a noite têm duração igual. No hemisfério Norte o equinócio de Março é o Equinócio de Primavera (chamado de Verão ou Vernal), e o de Setembro é o Equinócio de Outono. O inverso ocorre no hemisfério Sul.

[17] No livro “ Da Falsificação de Euros aos Pequenos Mundos” de Jorge Buescu encontra-se uma explicação detalhada dos cálculos efectuados por Dyonisius.

Possivelmente na próxima passagem de século voltará a discussão sobre a não existência do ano zero na era Cristã.

Mas num trabalho como este, em que se pretende estudar Técnicas de Contagem, não poderemos ficar por aqui.

Quando se chegou à conclusão que era necessário o zero (e neste domínio a civilização ocidental esteve sempre muito atrasada em relação a outras civilizações), verificou-se o erro de escala cometido pelo monge Dionysius ao não designar o primeiro ano, por ano zero. Então teríamos três hipóteses possíveis:

1. Seguir a convenção estabelecida pelo monge, e consequentemente os séculos (e portanto os milénios) começam a contar nos anos 1, 101, …, 1001, …

2. O ano anterior ao ano 1 de Dionysius passa a ser o ano zero, como deveria ter sido e o ano 1 do monge, e os séculos (milénios) começam a contar nos anos 100, …, 1000, …

3. O primeiro século teve somente 99 anos (convenção à moda do papa Gregório XIII) e a partir daí entramos na hipótese 2.

Qual destas soluções é preconizada?

Todas são obviamente possíveis, pois, em princípio, o calendário é convencional (até depende das diferentes religiões, como sabemos), e os adeptos históricos da hipótese 1 não devem esquecer-se de Gregório XIII.

O problema é nitidamente um problema de contagem de tempo, e os ramos da Ciência que precisam de consultar os arquivos com o fim de efectuar previsões, como sucede com a Astronomia, a Geologia, etc. não podem prescindir do zero, como fez o monge. Trata-se de um caso de medição em que medição é igual a contagens, e por isso a convenção da Astronomia é análoga à que se segue para avaliar ou medir a idade de um indivíduo: trata-se de seguir a hipótese número 2, e assim (a.C.) significa ano antes do ano zero. Não nos devemos esquecer que só interessa saber qual o zero da unidade de medida ano (uma criança nasce: ao fim de 10 dias a sua idade é 0 anos 0 meses e 10 dias). É claro que os meses contam-se de 1 a 12 (não há mês zero), mas um mês é um conjunto de dias que neste caso o zero da unidade de medida é o dia.

É claro que a convenção astronómica não coincide com a convenção histórica, mas na verdade nenhuma delas se preocupa muito com o salto ordenado pelo papa Gregório XIII.

2. Introdução à Teoria dos Números

"A Matemática é a rainha das ciências e a teoria dos números é a rainha das matemáticas." (Gauss)[18]

A Teoria dos Números é um ramo da Matemática que estuda principalmente a estrutura dos sistemas numéricos, as propriedades dos números inteiros e as relações que estes estabelecem entre si. Esta área exerceu desde sempre, um grande fascínio nos matemáticos, decorrente, em larga medida, da extrema complexidade de resolução de alguns problemas de enunciados aparentemente simples. Um exemplo disso é o famoso *"Último Teorema de Fermat*" o qual afirma que, a equação $x^n + y^n = z^n$ não tem soluções inteiras positivas para *n* maior que 2. Este teorema foi enunciado no século XVII por Fermat[19] e só recentemente, em 1994, é que foi demonstrado por Wiles[20].

Foi só no século XIX que Giuseppe Peano[21] construiu a primeira axiomática para os números naturais. Anteriormente, os matemáticos não tinham sentido necessidade de definir, com rigor, os números naturais, de tal forma estes lhes pareciam intuitivos.

No seu livro *"Arithmetices Principia Nova Methodo Exposita"* Peano enuncia os cinco axiomas da Teoria dos Números:

- O número 1 é um número natural;
- Todo o número natural tem um sucessor;
- Não existe nenhum número natural cujo sucessor é 1;
- Números naturais diferentes têm sucessores diferentes;

[18] http://www.somatematica.com.br/frases.php

[19] Pierre de Fermat (1601-1665) foi juiz em Toulouse e matemático "amador" muito admirado pela comunidade científica pelas brilhantes contribuições em diversos ramos da Matemática

[20] Andrew Wiles, (nascido a 11 de Abril de 1953) é um matemático britânico, professor na Universidade de Princeton, famoso por ter demonstrado, com a colaboração de Richard Taylor, o Último Teorema de Fermat.

[21] Nasceu em 1858 em Itália. Estudou matemática na Universidade de Turim, onde foi professor desde 1890 até à sua morte. Leccionou, também, na Academia Militar de Turim. Na Matemática distinguiu-se principalmente em dois campos: no cálculo diferencial e integral e nos fundamentos da Matemática. Foi pioneiro na lógica simbólica e no método axiomático. Faleceu em 1932

- Se o número natural 1 possui uma determinada propriedade e, se for verdade que sempre que um número natural possui essa propriedade o seu sucessor também a possui, então, essa propriedade é válida para todos os números naturais.

O último axioma, apresentando uma formalização mais elaborada que os anteriores, é muitas vezes usado como método de demonstração conhecido como ***Principio de Indução*** ou ***Método de Indução Matemática***, do qual apresentamos uma definição mais formal:

Método de Indução Matemática – Para provar que uma propriedade P(n) é válida no conjunto IN, dos números naturais, mostra-se que:

1) P(1) é verdadeira;
2) Se P(n) é válida para o número natural *k*, arbitrário, então também é válida para o número natural *k+1*, isto é, a propriedade P(n) é hereditária.

Então, conclui-se que P(n), é verdadeira para todo o número natural.

Este método, aplicado na demonstração de uma propriedade, exige que esta se verifique para um primeiro número natural[22] e que seja hereditária. Caso não se verifiquem essas duas condições, simultaneamente, podemos "provar" absurdos. Vejamos um exemplo:

A igualdade $sen(2n\pi)=1$ - falsa para qualquer número natural *n,* visto que, $sen(2n\pi)=0$ - pode considerar-se hereditária, isto é, supondo que $sen(2k\pi)=1$ para algum *k* natural, então também seria $\mathrm{sen}(2(\mathrm{k}+1)\pi)=1.$

De facto, sob uma tal hipótese, tem-se:

$sen(2(k+1)\pi)=sen(2k\pi+2\pi)=sen(2k\pi)=1$, o que é absurdo!

Uma propriedade dos números naturais que está relacionada com o método de indução é o chamado princípio da boa ordenação.

[22] Há propriedades que só são válidas a partir de um certo número natural *a*. Neste caso, a primeira condição deste método é substituída por: P(*a*) é verdadeira.

Princípio da Boa Ordenação – Todo o conjunto A não vazio de números naturais contém um elemento mínimo, isto é, existe pelo menos um elemento de A tal que $a \leq b$ para todos os elementos b de A.

Esta propriedade não é válida, por exemplo, no conjunto dos números reais positivos, IR^+, pois não existe um número real positivo menor que todos os outros. O conjunto dos números inteiros negativos também não possui esta propriedade porque por menor que seja o número r inteiro negativo, $r-1$ é também um número inteiro negativo e menor que r.

O Princípio da Boa Ordenação pode ser utilizado em demonstrações, substituindo o método de indução matemática.

Vejamos um exemplo: na sucessão de Fibonacci, cuja sequência é 1, 1, 2, 3, 5, 8, 13, 21, … e que pode ser definida recursivamente, do seguinte modo,

$$\begin{cases} F_1 = 1 \\ F_2 = 1 \\ F_n = F_{n-1} + F_{n-2} \ , \text{ para } n \geq 3 \end{cases}$$

prova-se que, para todo o $n \in \mathrm{IN}$ tem-se $F_n \leq 1{,}7^{n-1}$.

Demonstração: Suponhamos, por redução ao absurdo, que a afirmação anterior é falsa. Seja então X o conjunto de contra-exemplos, isto é,

$$X = \left\{ n \in IN : F_n > 1{,}7^{n-1} \right\}$$

Por hipótese $X \neq \{\ \}$. Assim, pelo Princípio da Boa Ordenação, X contém um elemento mínimo x.

Por observação, sabemos que $x \neq 1$ porque $F_1 = 1 = 1{,}7^0$ e $x \neq 2$ porque $F_2 = 1 < 1{,}7^1$. Assim $x \geq 3$ e sabemos, também, que

$$F_x = F_{x-1} + F_{x-2}$$

e como $x-1$ e $x-2$ são números naturais menores que x, não pertencem a X pelo que,

$$F_{x-1} \leq 1{,}7^{x-2} \quad \text{e} \quad F_{x-2} \leq 1{,}7^{x-3}$$

Então

$$\begin{aligned} F_x &= F_{x-1} + F_{x-2} \\ &\leq 1{,}7^{x-2} + 1{,}7^{x-3} \\ &= 1{,}7^{x-3} \cdot (1{,}7 + 1) \\ &= 1{,}7^{x-3} \cdot (2{,}7) \\ &< 1{,}7^{x-3} \cdot (2{,}89) \\ &= 1{,}7^{x-3} \cdot (1{,}7^2) \\ &= 1{,}7^{x-1} \end{aligned}$$

ou seja, $F_x < 1{,}7^{x-1}$ o que é absurdo porque $x \in X$. Concluímos, então, que $F_n \leq 1{,}7^{n-1}$ para todo o $n \in \mathrm{IN}$, admitindo que o princípio do terceiro excluído é válido.

2.1 Números Primos

Associados a códigos de segurança, à protecção de dados pessoais ou de mensagens enviadas por Internet, ou seja, na base da Criptografia, estão os números primos. Estes números ganharam particular importância com o desenvolvimento tecnológico, tendo passado a ter relevante aplicação prática na "Era da Informação" e as suas propriedades e características, deixaram de constituir mera curiosidade.

Um número natural superior a 1 diz-se **primo** se for divisível apenas por si próprio e pela unidade.

Esta noção remonta às civilizações mais antigas tendo Euclides[23], na sua obra *"Elementos"*, desenvolvido o estudo dos números primos. Mas já anteriormente os Pitagóricos, que consideravam que os números governavam o mundo e tinham propriedades místicas, dividiam os números naturais em três classes: a unidade, os números primos e os números compostos.

Qualquer número natural diferente de 1 e não primo pode ser expresso, de forma única (não considerando a ordem dos factores), como produto de números

[23] Viveu em Alexandria por volta de 300 a. C.

primos. Esta propriedade é conhecida como **Teorema Fundamental da Aritmética[24].**

Pode parecer estranho o número 1 não ser considerado primo, uma vez que só é divisível por si próprio e pela unidade (que é o próprio número). Uma das explicações para este facto está relacionada com a unicidade da decomposição de um número em factores primos, referida no teorema anterior. Se o número 1 fosse primo haveria infinitas factorizações distintas de um mesmo número como, por exemplo,

$$42 = 2 \times 3 \times 7$$
$$42 = 1 \times 2 \times 3 \times 7$$
$$42 = 1 \times 1 \times 2 \times 3 \times 7$$
…

O estudo dos números primos é fascinante e muitíssimo misterioso, em virtude da simplicidade de alguns dos seus problemas cuja solução, no entanto, não foi até hoje encontrada pelos matemáticos. (O estudo dos grafos, que vamos desenvolver no capítulo 4, tem muitas semelhanças com o dos números primos, dentro desse contexto).

Um dos mais antigos problemas consiste na procura de um método eficiente que permita saber se um dado número é, ou não, primo uma vez que se sabe que a sucessão destes é infinita, como demonstra Euclides na sua obra *"Elementos".*

Existem várias referências a essa demonstração em diversos livros, apresentamos a seguir duas delas.

"Consideremos disse Euclides, que existe um número finito de primos. Então um deles, chamemos-lhe P, será o maior. Consideremos agora o número Q, maior do que P, que é igual ao produto de todos os inteiros consecutivos de 2 até P mais o número 1. Por outras palavras $Q = (2 \times 3 \times 4 \times ... \times P) + 1$*. Da forma de Q é obvio que nenhum inteiro entre 2 e P é seu divisor inteiro: qualquer divisão inteira deixaria resto 1. Se Q não é primo, então deve ser divisível por algum número primo maior do que P. Se Q é primo, ele próprio é um número primo maior do que P. Qualquer das hipóteses implica a existência de um número primo*

[24] Demonstrado no livro de Santos, "Introdução à Teoria dos Números", página 9.

maior do que P, que tínhamos considerado como o maior número primo. Então o número de primos é infinito." (Hoffman)

" Tomemos um número finito qualquer de primos, digamos $p_1, p_2, ..., p_k$ *, e consideremos o número* $N = p_1 \cdot p_2 \cdot ... \cdot p_k + 1$. *Este número N não pode ser divisível por nenhum dos primos* $p_1, p_2, ..., p_k$ *, pois se algum deles, digamos* p_i, *dividisse N, então* p_i, *que, obviamente, também divide* $p_1 \cdot p_2 \cdot ... \cdot p_k$, *dividiria* $N - p_1 \cdot p_2 \cdot ... \cdot p_k = 1$, *o que é impossível. Mas, pelo Teorema Fundamental da Aritmética, N há-de ter algum factor primo q, o qual, portanto, terá de ser distinto de todos os primos considerados. Isto mostra que o conjunto dos primos é infinito porque, dado um seu subconjunto finito qualquer, é sempre possível, pelo processo anterior, acrescentar mais um, distinto dos anteriores."* (Nogueira)

Durante séculos, houve tentativas de encontrar fórmulas capazes de gerar números primos mas, infelizmente, sem sucesso. Optou-se, então, por encontrar critérios que permitissem atestar se um número é ou não primo.

Teorema: Se n não é primo, então n possui, necessariamente, um factor primo menor ou igual a $\sqrt{n}$.

Assim, para testar se um número *n* é primo, é suficiente testarmos a divisibilidade apenas pelos primos menores ou iguais a $\sqrt{n}$, visto que, se um número não é primo, pode decompor-se num produto de factores primos. Se um desses factores for maior do que $\sqrt{n}$, os outros têm de ser inferiores a $\sqrt{n}$, pois o produto de dois factores superiores a $\sqrt{n}$ dá um resultado superior a *n.* Por exemplo, se pretendermos obter todos os primos menores do que 60, devemos excluir dentre os números de 2 a 60, os múltiplos de 2, 3, 5 e 7 que são os primos inferiores a $\sqrt{60}$. Estamos perante o denominado Crivo de Eratóstenes[25], que é o

[25] Eratóstenes, matemático, astrónomo, geógrafo, historiador, poeta e atleta, nasceu em Cirene, Grécia, em 276a.C. Passou grande parte da sua vida em Alexandria. Em 236 a.C., foi escolhido como director da famosa Biblioteca de Alexandria. Ficou conhecido por ter inventado o célebre *Crivo de Eratóstenes* (230 a. C.) e por ter sido o primeiro a estimar o comprimento da circunferência terrestre, numa altura em que poucos acreditavam que a Terra fosse redonda, medindo a diferença de latitude entre as cidade de Siena e de Alexandria, no Antigo Egipto,

processo mais antigo para encontrar números primos, sem utilizar fórmulas. Foi este o método usado na construção da tabela publicada em 1914, por Derick Norman Lehemer, que continha os números primos menores do que 10 milhões. Actualmente, os computadores, cada vez mais rápidos, criam tabelas de números primos com facilidade, desde que não se pretendam números primos com um número exagerado de algarismos.

2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17
18	19	20	21	22	23	24	25
26	27	28	29	30	31	32	33
34	35	36	37	38	39	40	41
42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57
58	59	60					

Figura 14 - Crivo de Eratóstenes

Apresentamos, a seguir, alguns critérios para averiguar se um dado número é, ou não, primo.

O **teorema de Wilson** diz que um número p é primo se e só se $p \neq 1$ e *p* é um divisor de $(p-1)!+1$. Este teorema permite testar se um número é ou não primo. Por exemplo, $(7-1)!+1 = 721$ e como 7 é um divisor de 721, então concluímos que 7 é primo. No entanto, este método não é muito eficaz, visto que o cálculo do factorial de $(p-1)$ torna-se moroso quando p é elevado.

O **Pequeno Teorema de Fermat** diz que se *p* é primo e não divide o inteiro a então *p* divide $a^{p-1}-1$. Por exemplo, sendo $p=7$ e $a=2$ tem-se que se 7 é primo e não divide 2, então divide $2^{7-1}-1=63=7\times 9$. O recíproco - ou seja se p divide $a^{p-1}-1$ então p é primo - seria um óptimo teste de primalidade mas, infelizmente, não é verdadeiro.

situadas sobre o mesmo meridiano mas em latitudes diferentes. Sabendo que a distância entre as duas cidades era de cinco mil estádios egípcios, estimou o perímetro da sua circunferência em cerca de 250 000 estádios (37 000 quilómetros). (Excelente para a época).

Fermat mostrou, também, que os números $F_n = 2^{2^n} + 1$ são primos para $n = 0, 1, 2, 3, 4$ e conjecturou que todo o número dessa forma é primo. Esses números ficaram por isso conhecidos por Números Primos de Fermat. Mas cerca de cem anos mais tarde, em 1732, Euler demonstrou que a conjectura de Fermat era falsa, visto que

$$F_5 = 2^{2^5} + 1 = 4\,294\,967\,297 = 641 \times 6700417$$

ou seja, o número F_5 é composto porque é divisível por 641.

Mais tarde, em 1880 Landry provou que F_6 também é composto.

O facto de continuar por descobrir uma fórmula simples que permita gerar primos arbitrariamente grandes, bem como a circunstância de os métodos conhecidos para investigar se determinado número é, ou não, primo se revelarem pouco eficientes, transforma cada descoberta de um novo número primo num acontecimento digno de constituir notícia em revistas científicas. No site da "Ciência Hoje" pode ler-se, num artigo de 2006-01-18:

"O primo de Mersenne

Um novo primo de Mersenne foi descoberto em Dezembro de 2005! Esta descoberta recente foi alcançada por um projecto de computação no âmbito do Great Internet Mersenne Prime Search (GIMPS - sigla em inglês para Grande Busca do Primo de Mersenne na Internet), conduzido por uma Universidade do Missouri (EUA), constituído por 700 computadores, pertencentes a uma rede de mais de 200 mil computadores.

Este novo recorde, o maior primo de Mersenne de sempre é o 43º encontrado, ou seja 2 elevado à potência de 30.402.457 menos 1 e é composto por mais de 9,152 milhões de dígitos. Foi a segunda vez no ano de 2005 que um número primo com estas proporções astronómicas foi calculado. Porém, tal como o anterior (anunciado em 18 de Fevereiro de 2005), os especialistas continuam à espera da descoberta de um primo de Mersenne com mais dez milhões de dígitos, cuja descoberta tem como aliciante o direito a um prémio de 100 mil dólares prometidos pela Electronic Frontier Foundation.

A busca de primos de Mersenne já conta com cerca de 2000 anos desde que Euclides escreveu sobre essa classe de primos no seu famoso livro "Os Elementos" e desde então, só foram encontrados mais 39, com a confirmação deste último".

Entretanto, em 4 de Setembro de 2006, a mesma equipa que encontrou o número referido no artigo anterior, descobriu mais um número de Mersenne[26], o 44º, corresponde a 2 elevado à potência de 32.582.657 menos 1 e é composto por mais de 9,808 milhões de dígitos, o que, contudo, ainda não permitiu conquistar os cem mil dólares! Este prémio tem dois objectivos principais, estimular a pesquisa matemática tão importante no desenvolvimento da Ciência e testar o comportamento dos últimos avanços em software e hardware.

Os **primos de Mersenne** são números da forma $2^n - 1$ em que *n* é um número natural e, curiosamente, também primo. Obviamente, só uma pequena percentagem dos números da forma $2^n - 1$ são primos. O facto de *n* ser primo não garante que o número $2^n - 1$ correspondente, seja primo. Quando *n* é substituído pelos primeiros quatro números primos, geram-se realmente números primos de Mersenne:

Para $n = 2,\ \ 2^2 - 1 = 3$

Para $n = 3,\ \ 2^3 - 1 = 7$

Para $n = 5,\ \ 2^5 - 1 = 31$

Para $n = 7,\ \ 2^7 - 1 = 127$

No entanto, quando n é substituído pelo quinto número primo 11, verifica-se que $2^{11} - 1 = 2047$ é um número composto, cujos factores primos são 23 e 89. Em 1644, o próprio Mersenne afirmou, correctamente, que, quando *n* toma os valores do sexto, sétimo e oitavo números primos, ou seja, 13, 17, 19, os números

[26] Marin Mersenne, frade, nasceu em 1588 em Maine, França, e morreu em 1648, em Paris. Investigou principalmente os números primos, e tentou encontrar uma fórmula que representasse todos os primos. Continuou alguns dos trabalhos de Galileu, tendo tornado este seu antecessor conhecido fora da Itália. Em 1633 publicou o Traité des Mouvements e, em 1634, publicou Le Méchanique de Galilée que era uma versão de aulas de Galileu sobre mecânica. Escreveu outras obras importantes na física matemática, L'Harmonie Universelle (1636) e Cogitata Physico-Mathematica (1644).

$2^n - 1$ correspondentes, são primos. Mersenne afirmou, também, que $2^{67} - 1$ era primo. Esta afirmação não foi posta em causa durante mais de 250 anos. No entanto, em 1903, Frank Nelson Cole, da Universidade de Colômbia, durante uma conferência, num encontro da Sociedade Americana de Matemática, calculou,

$$2^{67} - 1$$

e o produto

$$193\,707\,721 \times 761\,838\,257\,287$$

obtendo o mesmo valor $147\,573\,952\,589\,676\,412\,927$ mostrando, assim, que Mersenne se tinha enganado.

Seja dito como curiosidade que Cole, quando foi chamado para apresentar a sua comunicação, levantou-se, foi ao quadro e, sem dizer qualquer palavra, escreveu os valores numéricos acima indicados, tendo voltado para o seu lugar sob uma "chuva" de palmas.

Os números primos de Mersenne estão relacionados com os números perfeitos[27]. A partir de um número primo da forma $2^n - 1$ pode-se gerar um número perfeito, bastando multiplicá-lo por 2^{n-1}. Não se conhecem, actualmente, números perfeitos ímpares e conjectura-se, com fortes indícios experimentais, que não existe nenhum.

Os números primos dividem-se em vários grupos, conforme as suas características.

Os primos *titânicos* são os números primos com mais de 1000 algarismos.

Os primos *gémeos* são os números primos que diferem duas unidades, por exemplo 11 e 13.

Atentemos, o que a esse respeito pode ser encontrado no site http://www.ime.uerj.br/~progerio/.

" Em 1919, o matemático norueguês Viggo Brun demonstrou que a soma dos inversos dos primos gémeos é finita. O valor dessa soma é conhecido como constante de Brun. O resultado mais recente sobre o valor dessa constante é de 1998 obtida por Nicely, ou seja:

[27] Um número diz-se perfeito se é igual à soma dos seus divisores.
Por exemplo 6 é perfeito pois 6 = 1+2+3

$$\sum\left(\frac{1}{p}+\frac{1}{p+2}\right)=\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\ldots=1{,}90216051823$$

Os primos gémeos abalaram um gigante da industria electrónica. Em 1993, Thomas Nicely, professor de matemática, tentando melhorar o valor da constante de Brun através da utilização de cinco computadores 486 e um Pentium, obteve resultados diferentes nos dois tipos de computadores. O resultado do 486 estava de acordo com os valores publicados, mas o do Pentium, não. Após inúmeras verificações conseguiu localizar o problema. O Pentium que a Intel garantia dar 19 casas decimais correctas em cálculos matemáticos, dava apenas 9, um erro 10^{10} *vezes superior ao anunciado. A notícia espalha-se o "bug" é confirmado por dezenas de pessoas. A Intel recebe imensas reclamações que ignora, até que a IBM anuncia que vai deixar de comercializar PCs com Pentium. A cotação das acções da Intel caem na Bolsa de Valores, levando a empresa a admitir o erro e a substituir os Pentium que tinham o "bug".*"[28]

Como já foi referido, alguns problemas relacionados com os números primos continuam por resolver e, nesse âmbito, várias conjecturas continuam por provar, sendo uma das mais famosas a conjectura de Goldbach, de 1742, que diz que todo o número par, superior a 2 é soma de dois números primos como, por exemplo 10=3+7. Já foi verificado que a conjectura é válida para números pares até pelo menos 2×10^{16}. A respectiva demonstração figura na lista dos 23 problemas de matemática por resolver, apresentada pelo matemático alemão, David Hilbert[29] na conferência do Congresso Internacional de Matemática de Paris em 1900.

A ausência de qualquer padrão ou regularidade aparentes nos números primos é surpreendente. Sabe-se que todos os números primos excepto o 2, são

[28] Retirado de http://www.ime.uerj.br/~progerio/.

[29] Hilbert nasceu na cidade de Königsberg em 1862 e morreu em 1943 em Gottingen. Tinha 38 anos e era professor na prestigiosa Universidade de Götingen quando apresentou a lista dos 23 problemas matemáticos. No ano anterior, tinha publicado o livro "Grundlagen der Geometrie" (Fundamentos da Geometria) no qual inicia o seu projecto de fundamentação da Matemática. Segundo Hilbert, os matemáticos deveriam reduzir os conceitos matemáticos a axiomas rigorosos, listas de termos fundamentais, relações e regras, cuja consistência seria depois demonstrada, de modo a alicerçar a descoberta matemática em princípios inexpugnáveis.
É considerado como um dos maiores matemáticos do século XX, ao mesmo nível de Poincaré.

ímpares, sendo portanto, a diferença entre dois números primos consecutivos um número par. Mas o valor dessa diferença parece ser completamente aleatória.

Entre 9 999 900 e 10 000 000 existem nove números primos:

9 999 901	9 999 907	9 999 971
9 999 937	9 999 943	9 999 931
9 999 991	9 999 929	9 999 973

Mas entre os cem números seguintes, de 10 000 000 até 10 000 100 só há dois: 10 000 019 e 10 000 079

No entanto, quando se estuda a distribuição dos números primos parece surgir alguma ordem.

Primeiro, Legendre, e depois, Gauss em 1792 com apenas 15 anos, conjecturaram que o número de primos $\pi(n)$ menores ou iguais a um determinado número natural n podia ser aproximado pela função $\frac{n}{\ln n}$ e que essa aproximação seria tanto melhor quanto maior fosse n.

A prova rigorosa dessa conjectura data de 1896 dos trabalhos independentes de Charles de la Vallé Poussin e Jacques Hadamard, que enunciaram o teorema dos números primos:

Teorema dos números primos:

$$\lim_{n\to+\infty} \frac{\pi(n)}{n/\ln n} = 1$$

Este teorema permite estimar o número de números primos que devemos esperar encontrar até um determinado valor. Quanto maior é esse valor, melhor será a estimativa encontrada pelo quociente:

$$\pi(n) \approx \frac{n}{\ln n}$$

Considerando uma tabela constituída pelos valores de n, em potências de base 10, por $\pi(n)$ e pelo quociente $n/\pi(n)$, podemos observar que quando

avançamos uma linha, isto é, ao passarmos para a potência seguinte de base 10, a razão $n/\pi(n)$ aumenta, aproximadamente, 2,3.

$$10{,}4 - 8{,}1 = 2{,}3\,;\quad 12{,}7 - 10{,}4 = 2{,}3\,;\quad 15{,}0 - 12{,}7 = 2{,}3\quad \ldots$$

n	$\pi(n)$	$\frac{n}{\pi(n)}$
10	4	2.5
10^2	25	4.0
10^3	168	6.0
10^4	1 229	8.1
10^5	9 592	10.4
10^6	78 498	12.7
10^7	664 579	15.0
10^8	5 761 455	17.4
10^9	50 847 534	19.7
10^{10}	455 052 512	22.0

Tabela 1

Ora como $\ln 10 \approx 2.3$, conjecturou-se que até 10^n, número que representaremos por N, aproximadamente, 1 em cada $2.3n = (\ln 10)\cdot n = \ln 10^n$ é primo. Daí que para N suficientemente grande,

$$\frac{\pi(N)}{N} \approx \frac{1}{\ln N}\text{, ou seja, } \frac{\pi(N)}{1} \approx \frac{N}{\ln N}$$

Obviamente, o que acabamos de expor não pretende ser uma demonstração do teorema dos números primos, apenas uma explicação para uma melhor compreensão desse teorema.

Apesar da expressão $n/\ln n$ ser uma aproximação simples para $\pi(n)$, não é especialmente boa. Sendo assim, os matemáticos têm-se esforçado por obter

funções que melhorem a aproximação, de forma a diminuir o erro entre a estimativa e os valores encontrados.

Actualmente, a função que apresenta uma aproximação mais satisfatória é a função $R(n)$, definida por:

$$R(n) = 1 + \sum_{k=1}^{\infty} \frac{1}{k\,\xi(k+1)} \times \frac{(\ln n)^k}{k!}$$

onde $\xi(z)$ representa a função zeta de Riemann,

$$\xi(z) = 1 + \frac{1}{2^z} + \frac{1}{3^z} + \frac{1}{4^z} + \ldots$$

A função $R(n)$ é uma aproximação para $\pi(n)$ já que o surgimento dos números primos não obedece a nenhuma lei conhecida. No entanto, essa função, $R(n)$, permite, de alguma forma, colocar alguma ordem no caos dos números primos.

2.2 Congruências

Um conceito importante, em Teoria dos Números, é o conceito de divisibilidade. Enquanto que o quociente entre números reais é sempre um número real, o caso dos números inteiros é diferente. Um inteiro *a* só é divisível pelo inteiro *b* se existir um número inteiro *c* tal que $a = b \cdot c$, ou seja, o resto da divisão de *a* por *b* é nulo. Nesse caso, diz-se que *b* divide *a*, simbolicamente $b \mid a$, ou que *b* é um divisor de *a* ou, ainda, que *a* é um múltiplo de *b,* simbolicamente $a = \overset{\bullet}{b}$.

As congruências estão associadas aos conceitos de divisibilidade e resto. Para o estudo das congruências, o que é relevante é o resto da divisão de dois números inteiros.

Seja *m* um número inteiro positivo. Diz-se que os inteiros ***a* e b são congruentes *módulo m***, ou seja, $a \equiv b \pmod{m}$, se $m \mid (a-b)$, isto é, se *m* divide

a diferença entre *a* e *b* ou, por outras palavras, se *a* e *b* diferem por um múltiplo de *m*. Se *m* não divide $(a-b)$ diz-se que *a* é *incongruente* com *b* módulo *m.*

Assim, por exemplo,

$17 \equiv 5 (mod\, 12)$ porque $17-5=12$ é múltiplo de 12.

$17 \equiv 2 (mod\, 5)$ porque $17-2=15$ é múltiplo de 5.

A relação *de congruência com mod m* é uma relação de equivalência, visto que goza das propriedades:

- reflexiva – se *a* é um número inteiro qualquer então $a \equiv a (mod\, m)$;
- simétrica – se $a \equiv b (mod\ m)$ então $b \equiv a (mod\ m)$;
- transitiva – se $a \equiv b (mod\ m)$ e $b \equiv c (mod\ m)$ então $a \equiv c (mod\ m)$.

Existem vários exemplos do dia-a-dia onde se podem encontrar congruências, por exemplo, os relógios que trabalham com módulo 12 para as horas e módulo 60 para os minutos e segundos.

Considerando o exemplo $17 \equiv 2 (mod\, 5)$, atrás referido, temos que $17-2$ é um múltiplo de 5, ou seja, $17-2=5k$, para algum *k,* o que equivale a dizer que $17=5k+2$, isto é , o resto da divisão inteira de 17 por 5 é 2 e, simbolicamente, podemos escrever $17\ mod\, 5=2$. No entanto, nesta expressão *mod* não tem o mesmo significado que na expressão anterior.

A expressão *mod* (módulo) pode ser usada como uma relação de equivalência ou como uma operação binária. Embora os dois conceitos sejam diferentes estão relacionados.

Proposição: Sejam a e b números inteiros e n um número natural. Então

$$a \equiv b\ (mod\, m) \quad \Leftrightarrow \quad a\, mod\, m = b\, mod\, m$$

Quer dizer que os restos das divisões de a e b por m são iguais.

Exemplo1

$75 \equiv 35 \pmod{10}$ porque $75 - 35 = 40$ é um múltiplo de 10 (relação de equivalência)

$75 \equiv 35 \pmod{10} \quad \Leftrightarrow \quad 75 \bmod 10 = 35 \bmod 10$

$75 \bmod 10 = 5$ porque 5 é o resto da divisão de 75 por 10 (operação binária)

Neste último exemplo, ao resto 5 dá-se, também, o nome de resíduo, isto é, diz-se que k é um resíduo de h módulo m, se h e k são dois números inteiros tais que $h \equiv k \pmod{m}$. O conjunto $\{0, 1, 2, 3, ..., m-1\}$ é um sistema completo de resíduos módulo m.

A aplicação das congruências nos problemas de divisibilidade conduz ao estudo de equações do tipo $a\,x \equiv b \pmod{m}$, chamada congruência linear numa variável. Por exemplo, encontrar todos os números da forma $5k+9$ que são múltiplos de 11, corresponde a resolver a equação $5k + 9 \equiv 0 \pmod{11}$.

No conjunto dos números reais, para encontrar a solução da equação $a\,x = b$, multiplicamos ambos os membros pelo inverso de *a.* Na resolução de equações de congruências lineares, utiliza-se um processo semelhante.

Definição: Dado um número *a* chama-se **inverso de *a* módulo *m*** (ou inverso multiplicativo de *a* módulo *m*) ao número $\bar{a}$ tal que $\bar{a} \cdot a \equiv 1 \pmod{m}$.

Exemplo 2:

O inverso de 6 módulo 11 é 2 visto que $2 \cdot 6 = 12 \equiv 1 \pmod{11}$. De facto, o inverso $\bar{a}$ de 6 módulo 11 é tal que $6 \cdot \bar{a} \equiv 1 \pmod{11}$ isto é, $11 \mid (6 \cdot \bar{a} - 1)$, ou seja $6 \cdot \bar{a} - 1 = \dot{11}$, donde $\bar{a} = 2$.

Mas nem sempre existe inverso, como se constata ao tentar encontrar o inverso de 2 módulo 8. Procedendo analogamente ao exemplo anterior deveríamos encontrar $\bar{a}$ tal que $8 \mid (2 \cdot \bar{a} - 1)$, o que é impossível visto que $2 \cdot \bar{a} - 1$ é um número ímpar!

Surge, então, a questão: quando é que um número tem inverso multiplicativo módulo m? A resposta é dada pelo teorema seguinte:

Teorema: Se *a* e *m* são primos entre si[30] e m é maior do que 1 então existe um inverso multiplicativo de a módulo *m.*

Demonstração:

Sabe-se que se $m.d.c.(a,m)=1$ então existem inteiros s e t tais que

$$s \cdot a + t \cdot m = 1$$

ou seja,

$$s \cdot a + t \cdot m \equiv 1 \pmod{m}$$

pois o resto da divisão da combinação linear $s \cdot a + t \cdot m$ por 1 é 1 (pois ela vale 1).

Como $t \cdot m \equiv 0 \pmod{m}$

Terá de ser

$$s \cdot a \equiv 1 \pmod{m}$$

Esta demonstração descreve um método para determinar o inverso multiplicativo de a módulo m, quando a e m são primos entre si:

1. Determinar uma combinação linear de a e m que seja igual a 1.
2. O coeficiente de a nesta combinação é um inverso de a módulo m.

Para determinar o inverso multiplicativo de um número, pelo processo que acabamos de descrever, é importante, referir o algoritmo de Euclides para a determinação do m. d. c. de dois inteiros. É o mais antigo algoritmo conhecido, o que o torna muito importante em termos de História do Pensamento Matemático.

Algoritmo de Euclides: Sejam $r_0 = a$ e $r_1 = b$ inteiro não negativos com $b \neq 0$. Se o algoritmo da divisão for sucessivamente aplicado para obter-se $r_j = q_{j+1} \cdot r_{j+1} + r_{j+2}$, $0 \leq r_{j+2} < r_{j+1}$ para $j = 0, 1, 2, \ldots, n-1$ e $r_{n+1} = 0$ então $m\,d\,c(a,b) = r_n$, o último resto não nulo.

[30] Dois números inteiros, a e b, dizem-se primos entre si se e só se m.d.c. (a, b) =1.

Trata-se de um algoritmo recursivo, aspecto que confere vantagens ao cálculo computacional e permite verificar que o m.d.c.(a, b) pode, sempre, transformar-se numa combinação linear do tipo $s \cdot a + t \cdot b$ com s e t números inteiros.

Exemplo 3:

Determinar um inverso multiplicativo de 3 módulo 7.

Como $m.d.c.(3, 7) = 1$, sabemos que esse inverso existe devido ao teorema anterior.

Usando o algoritmo de Euclides das divisões sucessivas temos

	2	3	
7	3	1	$7 = 2 \times 3 + 1 \Rightarrow 1 = -2 \times 3 + 1 \times 7$
1	0		

Logo -2 é um inverso multiplicativo de 3 módulo 7.

Note-se que todos os inteiros congruentes com -2 módulo 7 são, também, inversos multiplicativos de 3, ou seja, a classe dos inversos de 3 módulo 7 é:

$[3]_7 = \{..., -9, -2, 5, 12, ...\}$

ou seja

$12 \times 3 - 1 = \overset{\bullet}{7}$ $\quad$ $5 \times 3 - 1 = \overset{\bullet}{7}$

$-2 \times 3 - 1 = \overset{\bullet}{7}$ $\quad$ $-9 \times 3 - 1 = \overset{\bullet}{7}$, etc.

Aplicação: Resolver a equação de congruência linear $3x \equiv 4 \pmod 7$.

Devemos começar por determinar o inverso multiplicativo de 3 módulo 7. Sabemos que esse número existe, pelo teorema anterior, visto que 3 e 7 são primos entre si.

Pretendemos, então, encontrar $\bar{a}$ tal que $3 \cdot \bar{a} - 1 = \overset{\bullet}{7}$, ou seja, $\bar{a} = 5$.

Logo, $5 \cdot 3x \equiv 5 \cdot 4 \pmod 7 \Leftrightarrow 1 \cdot x \equiv 20 \pmod 7 \Leftrightarrow x \equiv 20 \pmod 7$

O conjunto-solução da congruência linear é: $\{\ldots, 13, 20, 27, \ldots\}$

Um resultado extremamente importante na resolução de sistemas de equações de congruências é o Teorema Chinês dos Restos, assim chamado por ter sido formulado na China, presumivelmente no século IV, por um estudioso chamado Sun Tsu Suan-Ching. Num livro de aritmética apresentou o seguinte problema:

"Temos uma quantidade desconhecida de objectos, que dividida por 3 dá resto 2, por 5 dá resto 3 e por 7 dá resto 2. Qual é essa quantidade?"[31]

Este e outros problemas podem ser resolvidos utilizando o teorema atrás referido.

Teorema Chinês dos Restos: Sejam $m_1, m_2, \ldots, m_{k-1}, m_k$ números naturais primos entre si dois a dois. Então o sistema de equações

$$\begin{aligned} x &\equiv a_1 \ (mod\ m_1) \\ x &\equiv a_2 \ (mod\ m_2) \\ &\ldots\ldots\ldots\ldots \\ x &\equiv a_{k-1} \ (mod\ m_{k-1}) \\ x &\equiv a_k \ (mod\ m_k) \end{aligned}$$

admite uma única solução módulo m, onde $m = m_1 \cdot m_2 \cdot \ldots \cdot m_{k-1} \cdot m_k$.

Representando por $y_i \ (i = 1, 2, \ldots, k)$ o inverso multiplicativo de $\frac{m}{m_i}$, ou seja, $\frac{m}{m_i} \times y_i \equiv 1 \ (mod\ m_i)$, a solução do sistema é dada por,

$$x \equiv a_1 \times \frac{m}{m_1} \times y_1 + \ldots + a_k \times \frac{m}{m_k} \times y_k$$

Diz-se que uma solução x_0 de $x \equiv a \ (mod\ m)$ é única módulo *m* quando qualquer outra solução x_1 for congruente a x_0 módulo *m*.

O problema enunciado por Sun Tsu Suan-Ching, pode ser equacionado usando a linguagem das congruências. O que se pretende é determinar um número natural *x* que seja solução do sistema:

[31] Retirado do livro de Nogueira, "Contar e Fazer Contas", página 194.

$$\begin{cases} x \equiv 2 \,(mod\ 3) \\ x \equiv 3 \,(mod\ 5) \\ x \equiv 2 \,(mod\ 7) \end{cases}$$

Como 3, 5 e 7 são primos entre si dois a dois, podemos garantir pelo Teorema Chinês dos Restos que o sistema tem solução.

$m = 3 \times 5 \times 7 = 105$.

designemos por,

$$M_1 = \frac{105}{3} = 35$$

$$M_1 = \frac{105}{5} = 21$$

$$M_1 = \frac{105}{7} = 15$$

determinemos, agora, os inversos multiplicativos de M_1, M_2 e M_3.

– 2 é o inverso multiplicativo de M_1 módulo 3, porque $35 \times 2 - 1 = \dot{3}$.

– 1 é o inverso multiplicativo de M_2 módulo 5, porque $21 \times 1 - 1 = \dot{5}$.

– 1 é o inverso multiplicativo de M_3 módulo 7, porque $15 \times 1 - 1 = \dot{7}$.

Assim,

$x \equiv (2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1) \,(mod\ 105) \Leftrightarrow x \equiv 233 \,(mod\ 105)$

Uma solução é 233 mas também o são $233 - 105 = 128$ e $128 - 105 = 23$

Há uma infinidade de soluções, sendo 23 a solução positiva mais pequena.

O Teorema Chinês dos Restos permite resolver vários problemas como, por exemplo o seguinte:

Quatro rapazes decidiram medir, usando os seus pés, a largura de um certo quarto. Os pés dos rapazes que, designaremos por A, B, C e D, medem, respectivamente, 7, 8, 9 e 11 polegadas. Após as medições apenas recordam que a A faltaram 2 polegadas, para concluir a medição da largura do quarto com os seus pés, a B e a C faltaram 5 polegadas e a D faltaram 6 polegadas. Qual é a largura do quarto?

Representando por L a largura do quarto, temos que

$$\begin{cases} L \equiv 2 \,(mod\ 7) \\ L \equiv 5 \,(mod\ 8) \\ L \equiv 5 \,(mod\ 9) \\ L \equiv 6 \,(mod\ 11) \end{cases}$$

O Teorema Chinês dos Restos garante que o sistema tem solução, visto que os números 7, 8, 9 e 11 são primos entre si, dois a dois.

Usando um processo semelhante ao do problema anterior temos, $m = 7 \times 8 \times 9 \times 11 = 5544$ e

$$M_1 = \frac{5544}{7} = 792$$

$$M_2 = \frac{5544}{8} = 693$$

$$M_3 = \frac{5544}{9} = 616$$

$$M_4 = \frac{5544}{11} = 504$$

os inversos multiplicativos de M_1, M_2, M_3 e M_4 são:

– 1 é o inverso multiplicativo de M_1 módulo 7, porque $792 \times 1 - 1 = \dot{7}$.

– 5 é o inverso multiplicativo de M_2 módulo 8, porque $693 \times 5 - 1 = \dot{8}$.

– 7 é o inverso multiplicativo de M_3 módulo 9, porque $616 \times 7 - 1 = \dot{9}$.

– 5 é o inverso multiplicativo de M_4 módulo 11, porque $504 \times 5 - 1 = \dot{11}$.

Logo,

$$x \equiv \left(\left(2 \times 792 \times 1 \right) + \left(5 \times 693 \times 5 \right) + \left(5 \times 616 \times 7 \right) + \left(6 \times 504 \times 5 \right) \right) \left(mod\ 5544 \right)$$

ou seja,

$$x \equiv 55589 \left(mod\ 5544 \right)$$

Uma solução é 55589, mas também são soluções: $55589 - 5544 = 50045$, $50045 - 5544 = 44501$, … .

Há uma infinidade de soluções: a solução positiva mais pequena é 149.

O Teorema Chinês dos Restos revelou-se muito importante com o desenvolvimento dos computadores pois permite simplificar os cálculos. Em vez de se trabalhar com números muito elevados, trabalha-se com os seus restos. Suponhamos que num certo processador, os cálculos efectuados com números inferiores a 100 são muito mais rápidos do que os efectuados com números superiores a 100. Podemos restringir quase todos os cálculos a inteiros inferiores a 100, desde que os representemos pelos seus restos em congruências cujos módulos são números primos entre si de valor inferior a 100. Por exemplo, os módulos 99, 98, 97, 95 são primos entre si logo, usando o Teorema Chinês dos Restos, todos os inteiros não negativos inferiores a

$$99 \times 98 \times 97 \times 95 = 89\,403\,930$$

podem ser representados univocamente pelos seus restos, quando divididos por esses quatro módulos.

Por exemplo, 123684 é representado por (33, 8, 9, 89), visto que

$$1234684 \left(mod\ 99\right) = 33$$
$$1234684 \left(mod\ 98\right) = 8$$
$$1234684 \left(mod\ 97\right) = 9$$
$$1234684 \left(mod\ 95\right) = 89$$

Desta forma, podemos representar números que, por excederem a capacidade do computador, não são por ele aceites.

A linguagem das congruências foi desenvolvida por Karl Friedrich Gauss[32] no início do século XIX e apresentada na sua grande obra *"Disquisitiones Arithmeticae"*, quando o autor tinha apenas 24 anos de idade. É neste trabalho que surge a notação das congruências que hoje utilizamos.

[32] Gauss nasceu em 1777 em Brunswich, na Alemanha. Foi um famoso matemático, astrónomo e físico. Era conhecido como *o príncipe dos matemáticos*. Deu grandes contributos em áreas como a Teoria dos Números, a Álgebra, a Análise, a Geometria, a teoria das Probabilidades e a Teoria dos Erros. Ao mesmo tempo, efectuava uma intensiva pesquisa empírica e teórica em muitos outros ramos, incluindo Astronomia, Mecânica Celeste, levantamento topográfico, Geodesia, Electromagnetismo e Mecanismos Ópticos. Morreu em 1855, em Göttingen, na Alemanha

Mas foi o matemático português Daniel Augusto da Silva[33] o primeiro a encontrar um método para resolver os sistemas de congruências lineares e a fazer o estudo geral das congruências binomiais, já abordadas por Gauss, Legendre e outros matemáticos, mas apenas para casos particulares e usando métodos mais complicados dos que os encontrados pelo matemático português. Estas e outras questões da Teoria dos Números foram apresentadas na obra *"Propriedades gerais e resolução directa das congruências binomiais; introdução à Teoria dos Números"* publicada em 1854. No entanto, devido ao isolamento em que no séc XIX se encontrava a ciência portuguesa em relação ao resto do mundo e, provavelmente, por não se colocar, à época, a questão do registo de patentes de descobertas científicas e da divulgação das mesmas, alguns dos resultados obtidos por Daniel da Silva na sua investigação, surgiram mais tarde, atribuídos a outros matemáticos que desenvolveram trabalhos na mesma área, desconhecendo os avanços já alcançados pelo matemático português. Assim, por exemplo, é indevidamente atribuído ao aritmético inglês Smith o método para resolver os sistemas de congruências lineares apesar de ele só o ter apresentado em 1861, após a publicação da obra atrás referida de Daniel da Silva.

Uma das aplicações das congruências verifica-se nos sistemas de identificação numérica usados, por exemplo, na formação do número de série das notas de Euro, como mecanismo de segurança contra a falsificação e contra erros de comunicação de dados entre instituições bancárias.

Um ou mais algarismos do número de série funcionam como dígitos de controlo que permitem detectar erros.

Os números de série das notas de Euro são formados por uma letra, identificando o país onde foi emitida e por 11 algarismos em que o último, que toma valores apenas entre 1 e 9, é de controlo. A cada letra é associado um número, como o valor 5 associado à letra M que identifica as notas emitidas em Portugal. Desta forma, cada nota "apresenta" 12 algarismos. Para esse número ser válido, a soma dos seus 12 algarismos tem de ser congruente com $0\ (mod\ 9)$.

Este é um dos 11 mecanismos de segurança elaborados pelo Banco Central Europeu para as notas de Euro.

[33] Daniel da Silva nasceu em Lisboa a 16 de Maio de 1814. Foi Oficial de Marinha, Bacharel em Matemática pela Universidade de Coimbra, professor na Escola Naval. Da sua actividade científica apresentou três obras à Academia das Ciências de Lisboa. Além da referida no texto escreveu "*Da transformação e redução dos binários de forças"* e "*Sobre a rotação das forças em torno dos pontos de aplicação".* Morreu em 6 de Outubro de 1878.

Um outro exemplo de aplicação envolvendo a noção de número primo, a noção de congruência e o pequeno teorema de Fermat, surgiu por volta de 1977 na criptografia de chave pública, usualmente conhecida por RSA, em homenagem aos seus inventores Ronald Rivest, Adi Shamir, ambos professores no Massachusetts Institute of Technology e Leonard Adleman, professor na University of Southern California.

O sistema consiste em gerar duas chaves: uma pública, conhecida por todos e que permite codificar a mensagem e outra privada, conhecida apenas pelo descodificador da mensagem e difícil de ser descoberta por outras pessoas.

Suponha-se que a Ana deseja enviar uma mensagem ao Pedro e como pretende que esta não seja conhecida por outros, usa a criptografia de chave pública. O processo consiste no seguinte: o Pedro cria duas funções, D e E, inversas uma da outra, isto é, D[E(M)]=M e revela a função E à Ana, mantendo a função D em segredo; A Ana usa a função E para codificar a mensagem, isto é, N=E(M) e envia N a Pedro, este usa a função D que só ele conhece para descobrir M, ou seja, a mensagem da Ana.

A função E é fácil de calcular, dado que está relacionada com o produto de dois números primos grandes mas a função D, relacionada com os factores primos é muito difícil de encontrar, tanto mais difícil quanto maiores forem os factores primos, uma vez que se sabe que a decomposição de números grandes em factores primos é difícil de conseguir, mesmo com ajuda de computadores.

Vejamos um exemplo concreto.

Suponhamos que a Ana deseja enviar a Pedro uma mensagem codificada. A mensagem a codificar é a palavra STOP.

Começa por converter as letras em números, efectuando a correspondência $A \to 01,\ \ B \to 02$, etc., obtendo,

$$S = 18,\ T = 19,\ O = 14 \text{ e } P = 15$$

Os oito algarismos são partidos em dois blocos com quatro algarismos cada: 1819 e 1415.

O Pedro selecciona dois números primos distintos e que deveriam ser enormes para ser muito difícil encontrá-los em tempo útil. Neste exemplo, vamos considerar dois primos pequenos para facilitar a compreensão do método.

Neste caso,

$$p = 43 \text{ e } q = 59$$

e calcula:

$$n = 43 \times 59 = 2537$$
$$\phi(n) = (p-1)(q-1) = 2436 .$$

Selecciona um inteiro positivo e tal que $0 < e < \phi(n)$ e e e $\phi(n)$ sejam primos entre si, por exemplo $e = 13$.

Escolhe um número d tal que $(e \cdot d - 1)$ seja divisível por $(p-1)(q-1)$, isto é, $(13 \cdot d) \bmod 2436 = 1$, ou seja, determina o inverso multiplicativo de $13 \bmod 2436$, isto é, $d = 937$.

Note-se que para calcular *d* é necessário conhecer os factores primos de n.

O par (n, e) constitui a chave pública que o Pedro envia à Ana.

O par (n, d) é a chave privada. Os valores *p* e *q* devem ser mantidos em segredo ou destruídos.

A Ana ao conhecer a chave pública calcula:

$C = 1819^{13}$ e o resto da divisão de C por 2537. Esse resto é 2081.

$D = 1415^{13}$ e o resto da divisão de D por 2537. Esse resto é 2182.

A mensagem codificada é:

2081 2182

O Pedro tem que efectuar o processo inverso para descodificar a mensagem, ou seja, tem de determinar:

- o resto da divisão de 2081^{937} por 2537 que é 1819;
- o resto da divisão de 2182^{937} por 2537 que é 1415.

A mensagem descodificada é:

1819 1415, ou seja,

STOP

2.3 Partições

As partições de um inteiro positivo são as diferentes maneiras de expressar esse número como soma de inteiros positivos. Os números que compõem uma partição são designados por partes.

O problema de determinar o número $p(n)$ de partições de um inteiro positivo n foi objecto de estudos durante longo tempo e, uma fórmula para o seu cálculo, só surgiu no século XX, fruto do trabalho dos matemáticos G. H. Hardy, S. Ramanujan e H. Rademacher.

Representemos as partições de, por exemplo, o número 5.

$$5=4+1=3+2=3+1+1=2+2+1=2+1+1+1=1+1+1+1+1$$

temos, então, que $p(5)=7$.

A função $p(n)$ cresce de forma muito rápida.

Temos, por exemplo, que $p(20)=627$, $p(100)=190\,569\,292$,

$p(200)=3\,972\,999\,029\,388$ e

$p(1000)=24\,061\,467\,864\,032\,622\,473\,692\,149\,727\,991$

Designando por $p_k(n)$ o número de partições de n em que o maior valor é k, temos que $p_n(n)=1$ e que para $k>n$, $p_k(n)=0$, visto que, por definição de partição de um número, nenhuma parte pode superar o número n.

No caso do exemplo anterior, partições de 5, tem-se

k	1	2	3	4	5
$p_k(5)$	1	2	2	1	1

Tabela 2 – $p_k(5)$

e que $\sum_{k=1}^{5} p_k(5) = p(5)$

No caso geral, $\sum_{k=1}^{n} p_k(n) = p(n)$

Designando, agora, por $q_k(n)$ o número de partições de n com exactamente k partes, temos para o exemplo anterior,

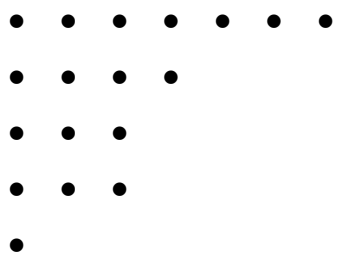
k	1	2	3	4	5
$q_k(5)$	1	2	2	1	1

Tabela 3 – $q_k(5)$

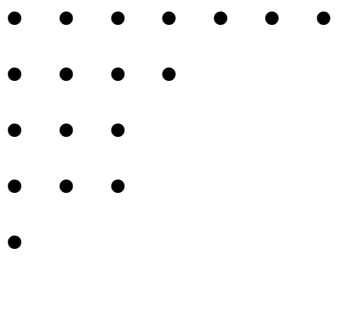
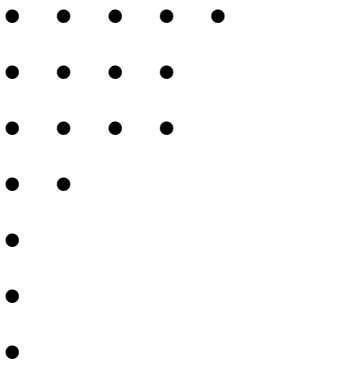
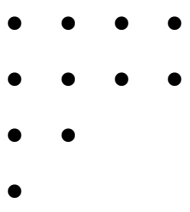
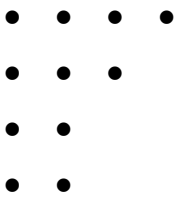
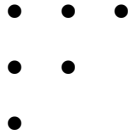
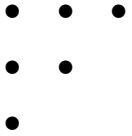
Observa-se que os valores das duas tabelas são os mesmos, isto é, $p_k(5) = q_k(5)$

Uma partição de um número pode ser representada graficamente por um **diagrama de Ferrer**, o qual consiste numa matriz de pontos, com tantas linhas como número de partes da partição, e em cada linha tantos pontos quantos o valor da parte da partição, a representar.

O gráfico da partição $7+4+3+3+1$ de 18 é:



Se na representação gráfica de uma partição de n trocarmos as linhas pelas colunas, obtemos outra partição de n, designada por **conjugada** da partição inicial.

Partição	Partição conjugada
$7+4+3+3+1$	$5+4+4+2+1+1+1$
	
$4+4+2+1$	$4+3+2+2$
	
$3+2+1$	$3+2+1$
	

No último exemplo, verifica-se que a conjugada de uma partição pode ser igual à partição, e diz-se, nesses casos, que a partição é autoconjugada.

Teorema: O número $p_k(n)$, de partições de n, sendo k a maior parte é igual ao número $q_k(n)$ de partições de n, com exactamente k partes, isto é,

$$p_k(n) = q_k(n)$$

Demonstração:

Por definição de partição conjugada de uma partição de um número n, tem-se que toda a partição tendo k como a maior parte é transformada numa partição, conjugada, que possui exactamente k partes. Por outro lado uma partição que possui k partes é transformada numa partição, conjugada, que possui k como a maior parte. Conclui-se, então que $p_k(n) = q_k(n)$.

3. Análise Combinatória

3.1 Introdução

Combinatória é a parte da Matemática que analisa estruturas e relações discretas. Dela faz parte a Análise Combinatória que aliás esteve na sua origem e que trata essencialmente de: demonstrar a existência de subconjuntos de elementos de um conjunto finito dado, satisfazendo certas condições, e contar ou classificar esses subconjuntos, sem que seja necessário enumerar os seus elementos.

A Análise Combinatória possui **técnicas de contagem** para resolver esses problemas. No entanto, para encontrar a solução dum problema, para além de um certo engenho é necessária a compreensão plena do enunciado. São esses aspectos que tornam fascinante esta parte da Matemática, em que problemas fáceis de enunciar se revelam, por vezes, difíceis de resolver, exigindo criatividade e astúcia.

Aparentemente, a Análise Combinatória teve origem no tempo de Arquimedes (287 a. C. – 212 a. C.). Estudos de velhos pergaminhos e manuscritos feitos pelo historiador de Matemática, Reviel Netz, da Universidade de Stanford, na Califórnia parecem confirmar que Arquimedes terá sido pioneiro nessa área da Matemática.

Os pergaminhos passaram pelas mãos de vários povos durante a Idade Média e, para além de quase terem sido destruídos pelo mofo, foram usados por monges que, por cima dos textos originais, neles escreviam as suas orações. Vieram a ser reencontrados e analisados nos últimos anos por cientistas, matemáticos e especialistas em grego. Com o auxílio de raios ultravioleta e de programas de computador, foi possível obter a escrita original, transcrição do trabalho de Arquimedes, designado por *Stomachion*[34] que, segundo Reviel Netz, é um autêntico tratado sobre Análise Combinatória. O Stomachion é, aparentemente, um jogo, semelhante ao Tangran (um jogo chinês de 7 peças bastante conhecido), mas constituído por 14 peças que devem ser encaixadas de maneira a formarem um quadrado. Os estudos de Arquimedes pretendiam

[34] Não se sabe o significado preciso desta palavra apenas que tem a mesma raiz que a palavra grega para estômago.

determinar de quantas maneiras as peças se podiam colocar, de forma a construir o quadrado. Não se sabe ao certo se Arquimedes conseguiu resolver esse problema, mas estudos recentes mostraram que existem $17\,152$ ou 268 soluções considerando ou não, respectivamente, as soluções simétricas[35].

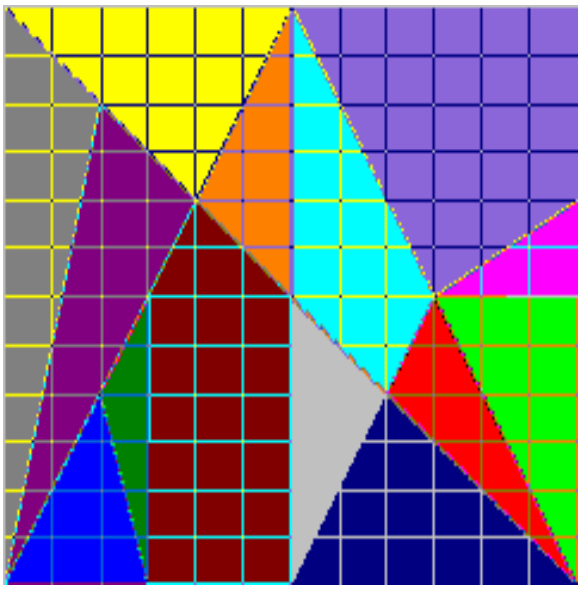


Figura 15 - Stomachion

O desenvolvimento da Análise Combinatória deve-se, em grande parte, à necessidade de resolver problemas de contagem, originados na teoria das probabilidades.

A noção de probabilidade tem a sua origem mais remota ligada à instituição dos seguros usados já pelas civilizações mais antigas, nomeadamente pelos fenícios, a fim de protegerem a sua actividade comercial marítima. Esta prática foi continuada pelos gregos e pelos romanos, tendo chegado até a civilização cristã medieval através dos comerciantes marítimos italianos. Pouco se sabe das técnicas então utilizadas pelos seguradores mas, parece que se baseavam em estimativas empíricas das probabilidades de acidentes, para estipularem as taxas e os prémios correspondentes.

No fim da Idade Média com o crescimento dos centros urbanos, surge um novo tipo de seguro, o seguro de vida. O primeiro estudo matemático sobre este seguro deve-se a Girolano Cardan (1501-1576), em 1570, apresentado no seu

[35] 536 soluções podem ser vistas em:
http://www.maa.org/editorial/mathgames/mathgames_11_17_03.html

livro *"De proportionibus Libri V)"* mas parece ter-se revelado muito teórico e pouco prático. Foi Halley quem, em 1693, no seu trabalho, *"Degree of Mortality of Mankind"*, mostrou como calcular o valor da anuidade do seguro em função da expectativa de vida e da probabilidade da pessoa sobreviver por um ou mais anos. A consolidação da aplicação da matemática nos seguros surge com o trabalho de Daniel Bernoulli (1700-1782). Calculou o número esperado de sobreviventes após *n* anos a partir do número de nascimentos e inovou na criação de novos tipos de seguros, calculando, por exemplo, a mortalidade causada pela varíola em pessoas de determinada idade. É nesta altura que surgem as primeiras grandes companhias de seguros.

Outro factor que contribuiu para o desenvolvimento da Análise Combinatória foram os problemas originados nos chamados jogos de azar. É curioso que se designem por jogos de azar muitos daqueles que dependem apenas do acaso, tais como o de dados, a roleta, certos jogos de cartas, etc. Todos envolvem um fenómeno de acaso cujo resultado só muito raramente é favorável ao jogador. Daí ser, de facto, apropriado chamar-lhes jogos de azar. A palavra "azar" é proveniente do árabe *"az-zahar",* por sua vez proveniente do persa *"az-zar"*, significando jogos de dados. Os jogos de azar são, provavelmente, tão antigos como a Humanidade. As mais antigas ligações destes jogos com a matemática reduzem-se à enumeração das possibilidades de se obter um dado resultado no jogo, sem referência ao cálculo da probabilidade de se obter esse resultado. Os jogadores queriam encontrar formas seguras de ganhar em jogos de cartas, dados ou moedas. É no século XVI que os matemáticos italianos Luca Paccioli (1445-1518), Cardan e Niccoló Tartaglia (1499-1557) apresentam as primeiras considerações matemáticas sobre os jogos de azar. É de Cardan a primeira obra sobre jogos de azar, *"De ludo Aleae"* publicado apenas em 1663. No entanto, o contributo decisivo para o início da Teoria das Probabilidades foi dado através da correspondência entre os matemáticos franceses Blaise Pascal e Pierre Fermat acerca de problemas surgidos nos jogos de azar.

O Conde de Méré, nobre francês e jogador assíduo, colocou a Pascal vários problemas dos quais se apresenta o seguinte:

"Eu e um amigo meu estávamos a jogar quando recebemos uma mensagem e tivemos de interromper o jogo. Tínhamos colocado em jogo 32 pistolas[36] cada um. Ganharia as 64 pistolas o que primeiro obtivesse 3 pontos, isto é, 3 vezes o número que escolheu no lançamento de um dado.

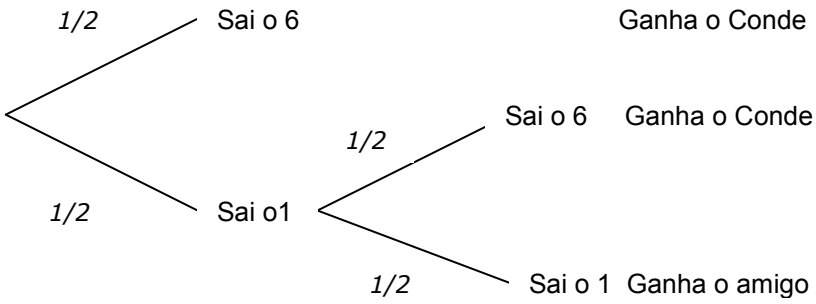
Eu tinha escolhido o 6 e quando o jogo foi interrompido eu já tinha obtido o 6 duas vezes. O meu amigo escolheu o 1 e, quando interrompemos o jogo, tinha obtido o 1 uma vez.

Como dividir as 64 pistolas?"

Vejamos uma resolução possível,

No próximo lançamento válido, ou sai o 6 e ganha o Conde, sendo a probabilidade de isso acontecer ½, ou sai o 1 (também com probabilidade ½) e o jogo tem de continuar. No lançamento seguinte, se sair o 6, ganha o Conde, neste caso com probabilidade $\frac{1}{4}=\frac{1}{2}\times\frac{1}{2}$, se sair o 1 ganha o amigo, também com probabilidade de ¼ .

Assim, a probabilidade de o Conde ganhar o jogo é de $\frac{3}{4}=\frac{1}{2}+\frac{1}{4}$, logo deve receber ¾ das 64 pistolas, ou seja, 48 pistolas. Esquematizando,



Pascal interessou-se por este problema da divisão das apostas, que anteriormente já tinha motivado outros matemáticos, como Paccioli, Cardan e Tartaglia, mas estes não tinham conseguido obter a solução correcta. Sobre o assunto, Pascal trocou ideias com o seu amigo Fermat e chegou a várias conclusões, ainda hoje válidas. Uma dessas conclusões constitui o seguinte teorema:

[36] Moeda de ouro utilizada em vários países europeus até ao século XIX.

Teorema: Suponha-se que um jogo é interrompido quando faltam r jogos ao primeiro jogador para vencer, enquanto que ao segundo jogador faltam s jogos, sendo r e s superiores a zero. O montante das apostas deve ser dividido de maneira que o primeiro jogador fique com a proporção de $\sum_{k=0}^{n-1}\binom{n}{k}$ para 2^n, onde $n = r + s - 1$ (número máximo de jogos que faltam efectuar).[37]

Aplicando este teorema ao problema anterior, temos que $r = 1$, visto que o Conde já tem dois pontos e só lhe falta 1 para ganhar e $s = 2$, visto que o amigo precisa de mais dois pontos para ganhar. Então a proporção da aposta que o Conde deve receber é:

$$\sum_{k=0}^{n-1}\binom{n}{k} / 2^n = \sum_{k=0}^{1}\binom{2}{k} / 2^2 = \frac{1+2}{4} = \frac{3}{4}$$

Um outro problema histórico foi proposto, no século XVI, pelo Grão-duque da Toscana. Este tinha reparado que, no lançamento de três dados, numerados de 1 a 6, era mais frequente obter soma das pontuações igual a 10 do que igual a 9, facto que o surpreendia, uma vez que, segundo ele, podia obter-se cada uma das somas de 6 maneiras diferentes.

Soma igual a 9	Soma igual a 10
1+2+6	1+3+6
1+3+5	1+4+5
1+4+4	2+2+6
2+2+5	2+3+5
2+3+4	2+4+4
3+3+3	3+3+4

Tabela 4 – Problema do Grão-duque da Toscana

Este problema foi estudado por Cardan, mas foi Galileu (1564-1642) quem, mais tarde, no seu livro intitulado *" Sopra le Scoperte dei Dadi"* (Análise do jogo

[37] A demonstração deste teorema pode ser analisada no site: http://www.educ.fc.ul.pt/docentes/opombo/seminario/pasca_l/probabilidades.htm

de Dados) apresenta, entre outros assuntos, uma explicação para o problema proposto pelo Grão-duque da Toscana. É, também, nessa obra que, para além de algumas técnicas de contagem, surgem já conceitos como a equiprobabilidade de acontecimentos e o ganho esperado num jogo.

Aparentemente, somos levados a pensar que, de facto, só há 6 formas diferentes de obter a soma 9 e a soma 10 mas, basta pensar que temos três dados de cores diferentes, para verificarmos que a soma de três parcelas diferentes, como, por exemplo, 1+2+6, pode ser obtida de 6 maneiras diferentes, a soma de duas parcelas iguais e uma diferente, como, por exemplo, 1+4+4, pode ser obtida de 3 maneiras diferentes e, obviamente, só há uma maneira para obter a soma de três parcelas iguais, isto é:

	1º dado	**2º dado**	**3ºdado**
1+2+6	1	2	6
	1	6	2
	2	1	6
	2	6	1
	6	1	2
	6	2	1
1+4+4	1	4	4
	4	1	4
	4	4	1

Tabela 5 – Lançamento de três dados cuja soma é 9

Desta forma, existem 25 (3x6+2x3+1) maneiras diferentes de obter a soma 9 e 27 (3x6+3x3) maneiras diferentes de obter a soma 10. Confirma-se, assim, a conclusão baseada na experiência do Grão-duque da Toscana.

Além dos matemáticos já referidos, pelo seu contributo no desenvolvimento da Análise Combinatória, devemos salientar, também, os trabalhos realizados nessa área por Leibniz (1646-1716), Jacques Bernoulli (1654-1705), Moivre (1667-1754), Newton (1646-1727), Euler (1707-1783), entre outros.

Leibniz escreveu, em 1666, *"Dissertatio de Arte Combinatória"*, resultado dos seus estudos na Universidade de Leipzig em diferentes áreas, Filosofia,

História, Matemática e Direito. Nesse trabalho, apresenta as suas ideias fundamentais sobre combinatória e reduz todo o raciocínio, toda a descoberta, a uma combinação de elementos básicos tais como números, letras, sons ou cores. Eis o tipo de ideia característico de Leibniz. Tentar reduzir problemas matemáticos a uma forma simples e básica, que não só permitisse o seu entendimento, como também a sua rápida resolução. Não esqueçamos que foi Leibniz que defendeu a ideia da existência do infinitésimo no Cálculo, tentando resolver os problemas de Cálculo Infinitesimal com essa ideia básica, ao contrário de Newton, que criou uma outra forma de trabalhar esses problemas (criando os conceitos de fluente e de fluxão típicos da Análise Funcional) que foi a seguida pelos matemáticos anglo-saxónicos até ao aparecimento da Análise Não-Standart no séc. XX, que ressuscitou as ideias de Leibniz, que aliás estavam dentro da tradução lógico – algébrica que vinha desde Eudóxio de Cnido (408-355 a. C.).

Deve-se a Jacques Bernoulli, professor de matemática em Basileia e grande figura científica da época, o primeiro tratado importante sobre a teoria das probabilidades, num livro de edição póstuma chamado *"Ars Conjectandi"* de 1713. Esta obra contém vários problemas relacionados com contagens e probabilidades, conhecidos até essa altura, com as respectivas resoluções, nomeadamente os problemas estudados por Pascal e Fermat; enuncia um teorema cuja generalização é hoje conhecida como a "Lei dos grandes números" e apresenta a teoria geral das permutações e combinações.

Abraham De Moivre, na sua obra *"Doctrine of Changes"*, dedicou-se ao estudo das leis do acaso. Foi o primeiro a usar funções geradoras para resolver a relação de recorrência $x_n = x_{n-1} + x_{n-2}$, relacionada com a sucessão de Fibonacci (problema da multiplicação dos coelhos de Leonardo de Pisa). De Moivre é um dos nomes que, no séc. XVIII, aparecem ligado à Teoria das Probabilidades.

Isaac Newton mostrou como calcular directamente $(1+x)^n$ sem antes calcular $(1+x)^{n-1}$, e daí o desenvolvimento do hoje chamado Binómio de Newton.

Leonard Euler destaca-se pelas suas importantes contribuições. Foi o fundador da teoria das partições de um número e a ele se deve o enunciado e a

solução do Problema das Sete Pontes de Konigsberg, um marco no início da Teoria dos Grafos.

Em 1812, Laplace publicou uma importante obra, *"Théorie Analytique des Probabilités",* em que sintetizou os conhecimentos da época e onde é apresentada a Lei de Laplace para o cálculo da probabilidade de um acontecimento.

Foi a partir da obra de Laplace que os estudos na área das probabilidades se intensificaram, interessando grandes matemáticos como o russo Gauss (1777-1855), os franceses Poisson (1781-1840), Poincaré (1854-1912), Borel (1871-1956), entre outros.

No desenvolvimento do estudo das probabilidades surgiram, ao longo dos anos, vários paradoxos, como o conhecido Paradoxo de Condorcet.

Marie-Jean-Antoine-Nicolas Caritat Condorcet, marqués de Condorcet (1743-1794), matemático e político, mostrou que é possível numas eleições, a maioria preferir o candidato B ao A, a maioria preferir o candidato C ao B, e ainda assim, a maioria preferir o candidato A ao candidato C!

Este paradoxo centra-se na questão de a "maioria preferir" não ser uma relação de transitividade. Intuitivamente, acreditar-se-ia que se a maioria prefere B a A, a maioria prefere C a B então a maioria deveria preferir C a A, mas isso não se verifica necessariamente.

Este paradoxo pode ser apresentado relacionado com o seguinte jogo: consideramos três piascas como na figura. Joga-se dois a dois. Cada um dos dois jogadores escolhe uma piasca que faz rodopiar. Ganha aquele cuja piasca, ao parar, encoste à mesa a face com maior número.

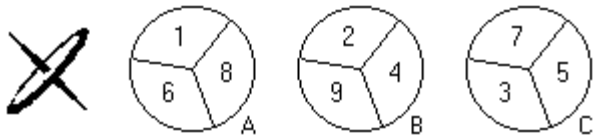


Figura 16 – Três piascas

Verificamos, nesta situação, que B tem mais hipóteses de ganhar do que A, C tem mais hipóteses de ganhar do que B e que, contrariamente ao que poderíamos esperar, C tem menos hipóteses de ganhar do que A, como se pode observar pelas tabelas seguintes:

A \ B	2	4	9
1	B	B	B
6	A	A	B
8	A	A	B

P(B) > P(A)

B \ C	3	5	7
2	C	C	C
4	B	C	C
9	B	B	B

P(C) > P(B)

A \ C	3	5	7
1	C	C	C
6	A	A	C
8	A	A	A

P(A) > P(C)

Um outro problema curioso e que contraria o senso comum, constituindo a sua solução um paradoxo, é apresentado no livro "O Acaso" de Sá, J., designado por "O problema da porta Certa".

"Este problema surgiu nos EUA e é conhecido pelo paradoxo de Monty Hall. Considere-se um concurso de televisão em que são apresentadas três portas ao concorrente, por trás de uma das quais se encontra um prémio aliciante, e atrás das outras o prémio é irrisório. O concorrente indica uma das portas ao apresentador do concurso. Este, que sabe o que se encontra por trás das portas, abre uma das duas restantes e revela a ausência do prémio grande. Pergunta-se: deve ou não o concorrente mudar a sua escolha inicial de porta? Quando um colunista de um jornal americano recomendou que se deveria mudar a escolha inicial, o jornal recebeu várias cartas de matemáticos insurgindo-se contra tal recomendação, dizendo que a probabilidade de ganhar com tal estratégia era de 0,5. Vejamos se isso é verdade. Comecemos por numerar as portas de 1 a 3 e supor que é a porta 1 a escolha inicial do concorrente. Se este não muda a sua escolha inicial, terá 1/3 de probabilidade de escolher a porta certa. Se, pelo contrário, opta por mudar a sua escolha, temos as seguintes situações:

Prémio atrás de	*Escolha inicial*	*Apresentador abre*	*Nova escolha*
Porta 1	*Porta 1*	*Porta 2*	*Porta 3*
Porta 2	*Porta 1*	*Porta 3*	***Porta 2***
Porta 3	*Porta 1*	*Porta 2*	***Porta 3***

Tabela 6 – As três portas do concurso

A probabilidade de ganhar mudando a escolha duplica, é 2/3 "

Este resultado contraria de tal forma o senso comum que, até o matemático húngaro Paul Erdős (1913-1996), famoso pelas suas contribuições na resolução de problemas, nomeadamente na teoria dos números, teve bastante dificuldade em aceitar a solução.

Um dos factores que mais contribuíram para o desenvolvimento da Combinatória, desde o início do século XX, foi a Teoria dos Grafos dadas as diversas aplicações na modelação de problemas de áreas como química, física, economia, redes de transportes, comunicações, etc.

3.2 Técnicas de Contagem

A contagem baseia-se na ideia da correspondência biunívoca entre dois conjuntos, o dos elementos a contar e o conjunto dos números naturais.

No nosso quotidiano surgem, frequentemente, problemas de contagem, desde os mais simples, possíveis de resolver através de um diagrama de árvore, até aos mais complexos, que exigem técnicas especiais de contagem.

Neste capítulo, pretendemos abordar algumas dessas técnicas de contagem, começando pelas mais elementares, para determinar o número de elementos de conjuntos formados de acordo com certas regras, sem que seja necessário enumerar os seus elementos.

3.2.1 Princípio Fundamental da Contagem

Esta técnica também chamada Princípio da Multiplicação diz o seguinte: se determinado acontecimento ocorre em k etapas diferentes e, a primeira etapa pode ocorrer de n_1 maneiras diferentes e, para cada uma dessas maneiras, há n_2 maneiras diferentes de ocorrer a segunda etapa e assim sucessivamente, então, o número total, *n,* de ocorrer o acontecimento é dado por

$$n = n_1 \times n_2 \times ... \times n_k = \prod_{i=1}^{k} n_i$$

desde que as maneiras sejam independentes.

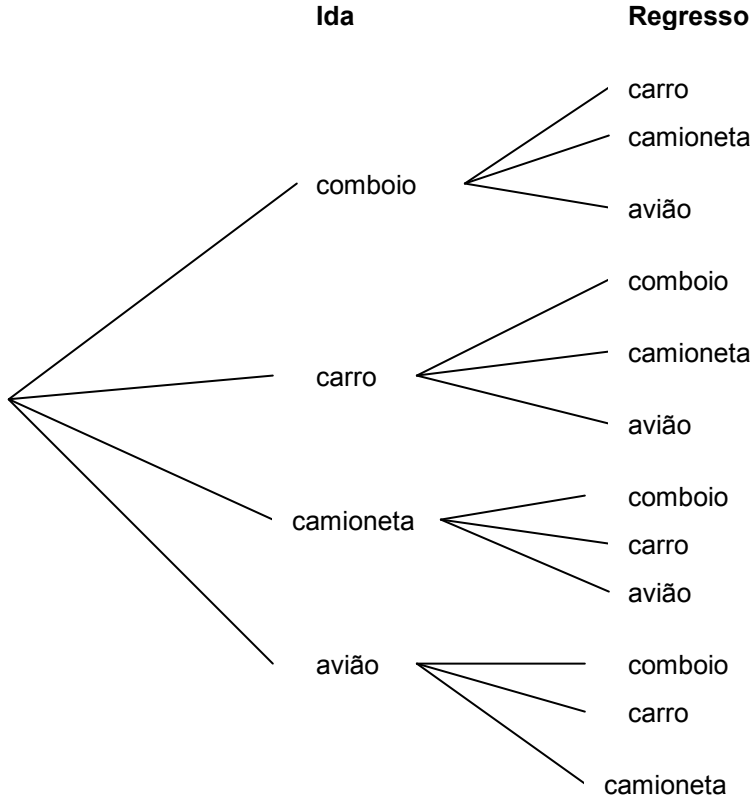
Exemplo 1

Para fazer uma viagem Porto-Lisboa-Porto, podemos usar como transporte o comboio, o carro, a camioneta ou o avião. De quantas maneiras podemos escolher os transportes de forma que o transporte usado no regresso seja diferente do usado na ida?

Há 4 maneiras de escolher o transporte de ida. Depois disso, temos 3 alternativas para escolher o transporte de regresso. Assim, existem, pelo princípio

da multiplicação, $4 \times 3 = 12$ formas diferentes de realizar essa viagem sem repetir o meio de transporte.

Esta técnica de resolução está relacionada com o diagrama de árvore, uma vez que, o número de resultados possíveis de uma experiência é dado pelo número de ramos terminais da árvore e é igual ao produto do número de resultados possíveis da primeira etapa pelo número de resultados possíveis das etapa(s) seguinte(s) da experiência. No entanto, a utilização de um diagrama de árvore pode ser inviável, quando a experiência em estudo é complexa ou, desnecessária, quando pretendemos apenas contar o número de resultados possíveis de uma determinada experiência.



Exemplo 2

Quantos números naturais de três algarismos distintos existem?

O primeiro algarismo pode ser escolhido de 9 maneiras, uma vez que não podemos usar o zero, o segundo algarismo de 9 maneiras, visto que não podemos escolher o algarismo escolhido anteriormente e o terceiro de 8 maneiras, para não repetir os dois algarismos anteriormente escolhidos. Assim temos, $9 \times 9 \times 8 = 648$.

Podemos, também, resolver este problema começando por não considerar o zero por ser o algarismo mais problemático, visto que não pode ocupar o primeiro lugar. Nessas condições, teríamos 9 maneiras de escolher o primeiro, 8 o segundo e 7 o terceiro, ou seja, podemos formar nessas condições $9 \times 8 \times 7 = 504$ números. Falta agora considerar os números onde, necessariamente, o zero é escolhido. Temos dois lugares possíveis para o zero, o segundo ou o terceiro algarismo. Escolhido esse lugar temos, para o outro algarismo, 9 possibilidades de escolha e, para o primeiro, 8 possibilidades. Assim, podemos formar $8 \times 9 \times 2 = 144$ números nessas condições. Em conclusão, existem $504 + 144 = 648$ números de três algarismos diferentes.

Neste exemplo, se começássemos pelo último algarismo, teríamos 10 maneiras de o escolher e 9 maneiras de escolher o segundo. No entanto, temos dificuldade em determinar o número de maneiras de escolher o primeiro algarismo, ou seja, seriam, respectivamente, 8 ou 7, consoante o algarismo zero já tenha sido escolhido ou não.

Nesta exposição, torna-se evidente a importância da escolha da estratégia para a resolução de um problema e a conveniência de saber recuar, quando a estratégia escolhida se revela inadequada.

Os problemas de contagem têm, por vezes, várias resoluções possíveis, umas mais imediatas, outras mais elaboradas. Nalguns casos, é até difícil perceber o raciocínio efectuado, se este não for explicado. Talvez seja essa a razão pela qual, nos critérios específicos do Exame Nacional de 12º Ano do último ano lectivo (2005-2006), se consideravam válidas respostas aparentemente sem nexo mas, cujo resultado, era idêntico ao correcto.

Na segunda resolução deste último exemplo usamos, para encontrar a resposta, o Princípio da Adição.

Princípio da Adição: Se A e B são dois conjuntos disjuntos, constituídos por objectos do mesmo tipo, com *p* e *q* elementos, respectivamente, então $A \cup B$ possui *p*+*q* elementos.

Este princípio e o Princípio Fundamental da Contagem, constituem as ferramentas básicas para a resolução de problemas de contagem.

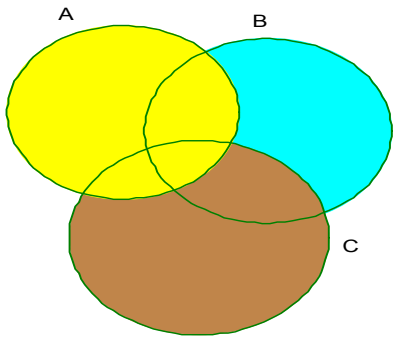
3.2.2 Princípio de Inclusão-Exclusão

Nem sempre é possível usar o princípio da adição, enunciado anteriormente, quando os dois conjuntos A e B não são disjuntos. Neste caso, a soma do número de elementos de A, isto é, do cardinal de A, com o do conjunto B, ou seja, $|A|+|B|$ seria superior ao cardinal de $A \cup B$, uma vez que os elementos pertencentes a $A \cap B$ seriam contados duas vezes.

Assim, o Princípio de Inclusão-Exclusão diz que: Se A e B são dois conjuntos finitos quaisquer, então

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Este resultado pode estender-se a mais de dois conjuntos. Consideremos os conjuntos A, B e C.



Então, $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

Exemplo 3

Numa escola do Ensino Superior, no curso de Matemática há:

- 81 alunos inscritos em Matemática Discreta;
- 72 alunos inscritos em Álgebra;
- 64 alunos inscritos em Cálculo;
- 56 alunos inscritos em Matemática Discreta e Álgebra;
- 46 alunos inscritos em Matemática Discreta e Cálculo;
- 47 alunos inscritos em Álgebra e Cálculo;
- 31 alunos inscritos nas três cadeiras.

Quantos alunos frequentam o curso?

Representando por A, B e C, os alunos inscritos em Matemática Discreta, Álgebra e Cálculo, respectivamente, tem-se:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| =$$
$$= 81 + 72 + 64 - 56 - 46 - 47 + 31 = 99$$

ou seja, frequentam o curso de Matemática 99 alunos.

Generalizando o princípio de Inclusão-Exclusão, obtém-se uma fórmula para determinar o cardinal da reunião finita de conjuntos finitos chamada fórmula de Daniel da Silva. Foi este matemático português quem primeiro publicou esta fórmula que surge anos mais tarde num trabalho de Sylvester, publicado em 1883. O desconhecimento da primeira publicação levou a que algumas pessoas a designem, incorrectamente, como fórmula de Sylvester.

$$\left|A_1 \cup ... \cup A_p\right| = \sum_i |A_i| - \sum_{i<j} \left|A_i \cap A_j\right| + \sum_{i<j<k} \left|A_i \cap A_j \cap A_K\right| - ...$$
$$= \sum_i |A_i| + (-1)^1 \sum_{i<j} \left|A_i \cap A_j\right| + (-1)^2 \sum_{i<j<k} \left|A_i \cap A_j \cap A_K\right| + ...$$

Exemplo 4

Quantos são os anagramas da palavra CONTAGEM que têm o C em 1º lugar, ou A em 2º lugar, ou T em 3º lugar ou M em 4º lugar?

Designemos por:

A_1 o conjunto dos anagramas de CONTAGEM que têm C em 1º lugar,

A_2 o conjunto dos anagramas de CONTAGEM que têm A em 2º lugar,

A_3 o conjunto dos anagramas de CONTAGEM que têm T em 3º lugar,

A_4 o conjunto dos anagramas de CONTAGEM que têm M em 4º lugar.

Pretendemos calcular $|A_1 \cup A_2 \cup A_3 \cup A_4|$. Temos que,

$|A_1| = |A_2| = |A_3| = |A_4| = 7! = 5040$ corresponde ao número de anagramas de CONTAGEM que têm uma letra fixa.

$|A_1 \cap A_2| = |A_1 \cap A_3| = |A_1 \cap A_4| = |A_2 \cap A_3| = |A_2 \cap A_4| = |A_3 \cap A_4| = 6! = 720$

corresponde ao número de anagramas com duas letras fixas.

$|A_1 \cap A_2 \cap A_3| = |A_1 \cap A_2 \cap A_4| = |A_1 \cap A_3 \cap A_4| = |A_2 \cap A_3 \cap A_4| = 5! = 120$

corresponde ao número de anagramas com três letras fixas.

$|A_1 \cap A_2 \cap A_3 \cap A_4| = 4! = 24$, corresponde ao número de anagramas de CONTAGEM com quatro letras fixas.

Assim, pelo princípio da Inclusão-Exclusão, vem

$|A_1 \cup A_2 \cup A_3 \cup A_4| = 4 \times 5040 - 6 \times 720 + 4 \times 120 - 24 = 16\,296$

Portanto, o número de anagramas de CONTAGEM nas condições do enunciado é 16 296.

3.2.3 Permutações

As permutações podem ser simples, completas, com repetição ou circulares.

3.2.3.1 Permutação simples ou sem repetição

Dado um conjunto $A = \{a_1, a_2, ..., a_n\}$ com ***n*** elementos distintos, chama-se permutação dos ***n*** elementos de *A* a qualquer sequência formada por esses ***n*** elementos. Cada sequência difere de outra apenas na ordem de colocação dos seus elementos. O número de permutações que é possível formar com os elementos do conjunto *A*, representa-se por P_n e é dado por,

$$\boldsymbol{P_n = n \times (n-1) \times (n-2) \times ... \times 3 \times 2 \times 1 = n!, \quad n \in IN}$$

Informalmente, pode-se dizer que P_n representa o número de maneiras de distribuir ***n*** objectos por ***n*** lugares.

Exemplo 5

Seis amigos vão ao cinema e sentam-se numa fila de 6 lugares. De quantas maneiras diferentes podem ocupar os lugares?

Uma ocupação dos lugares é uma permutação de 6 elementos e, portanto, o número total é $P_6 = 6! = 720$.

3.2.3.2 Permutações com repetição

Suponhamos que pretendemos determinar o número de anagramas que é possível formar com as letras da palavra ARARA. Podemos observar que a letra A aparece três vezes e a letra R duas vezes. Se todas as letras dessa palavra fossem diferentes, o número total de permutações seria dado por $P_5 = 5! = 120$. No entanto, a troca das três letras iguais (A), num anagrama não resulta num novo, pelo que ao considerar como número de permutações P_5 estamos a contabilizar como 3! a troca das letras A e, pela mesma razão, também estamos a contabilizar como 2! a troca das letras R. Assim, o número de permutações distintas que é possível formar é dado por

$$\frac{5!}{3! \cdot 2!} = 10$$

Chama-se permutação com repetição à permutação de *n* elementos, onde temos n_1 elementos iguais a a_1, n_2 elementos iguais a a_2, ..., n_k elementos iguais a a_k, de modo que $n_1 + n_2 + \ldots + n_k = n$, e existem k tipos de elementos diferentes. O número de permutações desses *n* elementos é dado por:

$$P^{n}_{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1! \cdot n_2! \cdot \ldots \cdot n_k!}$$

3.2.3.3 Permutações completas

As permutações completas de *n* elementos, representam-se por π_n, sendo permitida a repetição de elementos sem que seja necessário que se utilizem todos os elementos existentes no conjunto dado, numa sequência, contrariamente às permutações com repetição. Nesta situação, as sequências de *n* elementos diferem entre si pela natureza e/ou pela ordem dos elementos escolhidos. O número de permutações completas de n elementos é dado por,

$$\pi_n = n^n \quad , \quad n \in IN$$

Exemplo 6

Quantos números de seis algarismos se podem formar com os algarismos de 1 a 6?

Pretendemos formar números de seis algarismos, repetidos ou não, com os números de 1 a 6. Podemos resolver este problema usando o princípio fundamental da contagem, sendo que para o primeiro algarismo temos 6 hipóteses de escolha, para o segundo também, visto que pode haver repetição e assim sucessivamente. Podemos, então, formar $6\times6\times6\times6\times6\times6=6^6=46656$ números diferentes, o que corresponde a calcular o número de permutações completas de 6 elementos, $\pi_6=6^6=46656$.

3.2.3.4 Permutações circulares

Comecemos por resolver o seguinte problema: De quantas maneiras diferentes podemos sentar 6 pessoas para jantar se a mesa for redonda?

Podemos ser levados a pensar que este problema se resolve da mesma forma que o exemplo 5 (sentar as 6 pessoas em fila), ou seja, $6!=720$. No entanto, designando as pessoas por A, B, C, D, E e F, podemos verificar que as duas disposições representadas na figura seguinte são iguais, pois na mesa redonda o que é importante é a posição relativa das pessoas entre si, nas duas representações da figura, a pessoa A tem à sua direita F e à sua esquerda B e o mesmo acontece com as outras pessoas. Assim, a mesa pode ser "rodada" de seis modos, mantendo a mesma distribuição das pessoas. Então o número de maneiras de sentar essas pessoas é

$$\frac{6!}{6}=5!=120$$

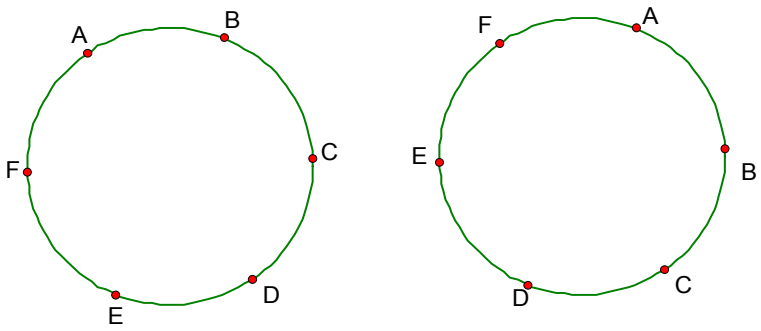


Figura 17 – Pessoas em mesas circulares

E se, em vez de 6, tivermos que dispor *n* pessoas em torno de uma mesa circular, o número de maneiras diferentes de fazer essa distribuição é dado pelas permutações circulares de *n* elementos, representadas, simbolicamente, por C_n, e definidas por

$$C_n = (n-1)! \ , \quad n \in IN$$

3.2.4 Combinações

Considere-se um conjunto com ***n*** elementos, a partir do qual se pretende formar um subconjunto com ***p*** elementos, considerando como distintos dois subconjuntos quaisquer desde que difiram pela natureza de, pelo menos, um dos seus elementos. O número de maneiras diferentes de escolher os ***p*** elementos, para formar o subconjunto a partir dos ***n*** elementos do conjunto universo, é dado pelas combinações de ***n*** elementos ***p*** a ***p***.

Como já foi referido, dois subconjuntos diferem pela natureza dos seus elementos, não pela ordem com que são apresentados, visto que $\{a, b\} = \{b, a\}$, ou seja, no cálculo das combinações a ordem não interessa, contrariamente ao que acontece nas permutações, em que, por exemplo, a sequência (a, b) é diferente da sequência (b, a).

Se a repetição de elementos no subconjunto não é permitida, o número de formas diferentes de obter o subconjunto é dado pelas combinações simples, mas

se a repetição de elementos é permitida, então o número de maneiras de obter o subconjunto é dado pelas combinações completas.

3.2.4.1 Combinações simples

Seja $A=\{a_1, a_2,..., a_n\}$ um conjunto de ***n*** elementos distintos. Chama-se combinação dos elementos desse conjunto, a qualquer dos seus subconjuntos. O número total de combinações, com ***p*** elementos distintos escolhidos de entre ***n,*** representa-se por C_p^n, ou por ${}^nC_p$, ou, ainda, por $\binom{n}{p}$.

Assim, por exemplo, as combinações de três elementos dos objectos a_1, a_2, a_3, a_4, a_5 são:

$$\{a_1, a_2, a_3\} \quad \{a_1, a_2, a_4\} \quad \{a_1, a_2, a_5\} \quad \{a_1, a_3, a_4\} \quad \{a_1, a_3, a_5\}$$
$$\{a_1, a_4, a_5\} \quad \{a_2, a_3, a_4\} \quad \{a_2, a_3, a_5\} \quad \{a_2, a_4, a_5\} \quad \{a_3, a_4, a_5\}$$

O número de combinações de 5 objectos 3 a 3 é $C_3^5=10$

O mesmo problema pode ser resolvido considerando que há 5 maneiras diferentes para escolher o primeiro elemento da combinação, 4 maneiras para o segundo e 3 maneiras para o terceiro, ou seja, $5\times 4\times 3=60$. No entanto, dessa forma, estamos a considerar diferentes as combinações que diferem apenas na ordem. Ora as combinações $\{a_1, a_2, a_3\}, \{a_1, a_3, a_2\}, \{a_2, a_1, a_3\},...$ em número de 6, correspondendo às permutações dos três elementos, são idênticas, pelo que o número de combinações dos cinco elementos três a três é $\frac{5\times 4\times 3}{3!}=10$

Generalizando, tem-se

$$C_p^n=\frac{n\cdot(n-1)...(n-p+1)}{p!}$$

Multiplicando ambos os termos da fracção por $(n-p)!$, obtém-se a fórmula conhecida,

$$\boldsymbol{C_p^n=\frac{n!}{p!\cdot(n-p)!}\ ,\ n,p\in IN_0\ ,\ n\geq p}$$

Da definição é evidente que

$$C_p^n = C_{n-p}^n$$

visto que, seleccionar *p* objectos entre *n* objectos distintos é equivalente a "tirar" os $n - p$ objectos que não são seleccionados.

Uma outra propriedade das combinações, usada na resolução de problemas, diz que:

$$C_p^n + C_{p+1}^n = C_{p+1}^{n+1} \quad , \quad \text{para } p < n \ , \ p \in IN_0$$

De facto,

$$\begin{aligned} C_p^n + C_{p+1}^n &= \frac{n!}{p!\cdot(n-p)!} + \frac{n!}{(p+1)!\cdot[n-(p+1)]!} = \\ &= \frac{n!}{p!\cdot(n-p)!} + \frac{n!}{(p+1)!\cdot(n-p-1)!} = \\ &= \frac{n!\cdot(p+1)}{(p+1)!\cdot(n-p)!} + \frac{n!\cdot(n-p)}{(p+1)!\cdot(n-p)!} = \\ &= \frac{n!\cdot(p+1+n-p)}{(p+1)!\cdot(n-p)!} = \\ &= \frac{(n+1)!}{(p+1)!\cdot(n+1-(p+1))!} = C_{p+1}^{n+1} \end{aligned}$$

Exemplo 7

De quantas maneiras diferentes podemos escolher três números inteiros, de 1 a 300 de forma que a sua soma seja divisível por 3?

Designemos por *A* o conjunto constituído pelos 300 números, $A = \{1, 2, 3, ..., 300\}$ e consideremos os seguintes subconjuntos de *A*:

- $A_1 = \{n \in A : n \equiv 0 \pmod 3\}$
- $A_2 = \{n \in A : n \equiv 1 \pmod 3\}$
- $A_3 = \{n \in A : n \equiv 2 \pmod 3\}$

Os subconjuntos são disjuntos dois a dois, têm o mesmo cardinal, 100 e a reunião dos três é o conjunto *A*.

Para a soma de três números ser divisível por 3, só podemos escolher os três números do mesmo subconjunto ou um número de cada subconjunto. Assim,

o número de maneiras diferentes de escolher três números do conjunto *A* de forma que a sua soma seja divisível por 3, é dado por

$$C_3^{100} + C_3^{100} + C_3^{100} + 100 \times 100 \times 100 = 1\,485\,100$$

Exemplo 8 (permutações e combinações)

Tem-se 15 livros distintos, 5 de Matemática e 10 de História. De quantas maneiras podem ser colocados numa estante de modo que não fiquem dois livros de Matemática juntos?

Colocados os 10 livros de História temos, entre eles, 9 espaços para serem ocupados pelos livros de Matemática. Como estes também podem ocupar as posições extremas, há 11 lugares disponíveis para serem ocupados pelos livros de Matemática. Assim, temos C_5^{11} maneiras diferentes para escolher os lugares a ocupar pelos livros de Matemática, verificando-se que para cada uma dessas maneiras, existem $10! \cdot 5!$ formas diferentes de colocar os livros, visto que são todos diferentes. Portanto, a resposta ao problema é $C_5^{11} \times 5! \times 10!$

3.2.4.2 Combinações de objectos distintos com repetição

As combinações com repetição de ***n*** elementos distintos, ***p*** a ***p,*** são os grupos de p elementos que se podem formar com os n elementos dados, sem considerar a ordem e podendo haver elementos repetidos. Assim, por exemplo, as combinações com repetição dos elementos *a, b* e *c,* dois a dois, são:

aa, ab, ac, bb, bc, cc

Uma forma de representar as combinações com repetição de n elementos $a_1, a_2, ..., a_n$ é na forma de um monómio, $a_1^{i1}\ a_2^{i2} \ldots a_n^{in}$, onde o expoente de cada elemento a_j , $j = 1,2,...,n$ representa o número de vezes que esse elemento surge na combinação e $p = i_1 + i_2 + ... + i_n$. Para contar o número desses monómios, faz-se corresponder, a cada um, uma sucessão de zeros e uns, escrevendo para cada a_j , $j = 1,2,...,n$ uma fila de tantos *uns* quanto o

valor do expoente e usando *zeros* para separar as filas de *uns*. Se algum dos expoentes é nulo, a fila de *uns* correspondente estará vazia, surgindo dois ou mais *zeros* seguidos. Cada sucessão, correspondente a um monómio, terá $n-1$ zeros e $i_1+i_2+...+i_n+n-1=p+n-1$ elementos.

Vejamos como representamos essas sucessões, correspondentes a monómios do sexto grau em quatro variáveis *a, b, c, d*.

a^2bc^2d	1 1 0 1 0 1 1 0 1
b^4d^2	0 1 1 1 1 0 0 1 1
d^6	0 0 0 1 1 1 1 1 1

O número total de sucessões que é possível formar é C_p^{n+p-1} pois corresponde a contar o número de maneiras de, dos $p+n-1$ elementos da sucessão, escolher os p elementos que vão ser ocupados pelos *uns*, ficando obviamente os restantes ocupados pelos *zeros.*

Assim, o número de combinações com repetição de ***n*** elementos ***p*** a ***p,*** representam-se por CR_p^n e tem-se

$$\boldsymbol{CR_p^n = C_p^{n+p-1} \quad , n \in IN,\ p \in IN_0}$$

Exemplo 9

Com os quatro primeiros números primos, 2, 3, 5 e 7, quantos produtos de dois factores se podem obter?

Devemos começar por observar que a ordem dos factores não interfere no valor do produto e que pode haver repetição dos factores. Logo, o número de produtos é dado pelas combinações com repetição, de quatro dois a dois, ou seja,

$$CR_2^4 = C_2^{4+2-1} = C_2^5 = 10$$

De facto, podemos obter os seguintes produtos:

$2\times 2=4$, $2\times 3=6$, $2\times 5=10$, $2\times 7=14$, $3\times 3=9$, $3\times 5=15$,
$3\times 7=21$, $5\times 5=25$, $5\times 7=35$, $7\times 7=49$

3.2.4.3 Combinações de objectos nem todos distintos

Sejam n objectos não todos distintos entre si. Destes n objectos, sejam q_1 do primeiro tipo, q_2 do segundo tipo e assim sucessivamente até q_t o número de objectos do t-ésimo tipo. Então, o número de maneiras pelas quais podemos seleccionar um ou mais objectos é

$$(q_1+1)\cdot(q_2+1)\cdot\ldots\cdot(q_t+1)-1$$

De facto, pela regra do produto temos que para os objectos do tipo 1 podemos não escolher nenhum ou escolher um, ou dois, ou…, ou q_1. Logo existem q_1+1 maneiras de escolher objectos do primeiro tipo. De modo análogo, existem q_2+1 maneiras de escolher objectos do segundo tipo e assim sucessivamente. Então, pela regra do produto temos $(q_1+1)\cdot(q_2+1)\cdot\ldots\cdot(q_t+1)$ maneiras de seleccionar os objectos. Acontece, contudo que, na contagem assim obtida está considerado o caso de não ser seleccionado nenhum objecto de nenhum tipo, ora como se pretende o número de maneiras de seleccionar pelo menos um objecto deve-se retirar uma unidade àquele produto.

Exemplo 10

Quantos divisores tem o número 2800?

Decompondo o número no produto de factores primos temos,

$$2800=2^4\times5^2\times7^1$$

Assim, temos 4 factores iguais a dois, 2 iguais a cinco e 1 factor correspondente ao número sete, ou seja, $q_1=4$, $q_2=2$ e $q_3=1$.

Logo, existem $(4+1)\cdot(2+1)\cdot(1+1)-1=29$ modos de seleccionar um ou mais números entre os factores primos que, multiplicados entre si, geram os divisores de 2800. Mas, como 1 também é divisor, temos $29+1=30$ divisores de 2800.

Estudamos neste capítulo todos os agrupamentos possíveis sem ser necessário referir ou definir outro tipo de agrupamento: o Arranjo que os autores

da escola francófona não anglo-saxónica habitualmente consideram. Então seguindo o princípio de Occam[38], que a matemática deve seguir, pois não se trata senão de uma consequência do Princípio do Mínimo do Universo, que a Física-Matemática faz questão de considerar em todos os seus problemas, excepto nos incorrectamente resolvidos.

3.2.5 Distribuição de objectos em caixas

As técnicas usadas para contar o número de maneiras de distribuir *n* objectos iguais ou diferentes em *k* caixas, revelam-se extremamente úteis na resolução de outros problemas de contagem, donde se justifica dedicarmos uma secção a este assunto.

3.2.5.1 Distribuição de objectos distintos em caixas distintas

Suponhamos que temos *n* objectos diferentes e pretendemos saber de quantas maneiras os podemos distribuir por *k* caixas. As distribuições diferem umas das outras não só pelo número de objectos em cada caixa mas, também, pelos objectos de cada caixa, uma vez que esses são diferentes.

Se a distribuição dos objectos nas caixas se fizer sem qualquer restrição, o problema pode ser resolvido usando o Princípio Fundamental da Contagem. Para colocar o primeiro objecto nas caixas, temos *k* possibilidades, para colocar o segundo, continuam a existir *k* possibilidades, e assim, sucessivamente. Temos então,

$$\underbrace{k \times k \times \ldots \times k}_{n \text{ vezes}} = k^n$$

[38] O princípio de Occam (também conhecido por Navalha de Occam) é um princípio lógico atribuído ao inglês do século XIV, William de Ockham e que hoje em dia se enuncia: "*se há várias explicações igualmente válidas para um facto, então devemos escolher a mais simples*". Este princípio defende a intuição como ponto de partida para o conhecimento do universo. William de Ockham defendeu o princípio de que natureza é por si mesma económica, sempre escolhendo o caminho mais simples.

maneiras de efectuar a distribuição dos objectos pelas caixas.

O problema anterior torna-se bem mais complexo se, na distribuição dos n objectos distintos pelas *k* caixas, se exigir que **nenhuma fique vazia**.

Poderíamos pensar que basta começar por colocar um objecto em cada caixa para atender à restrição e, a seguir, distribuir os restantes objectos pelas caixas, da mesma forma que na situação anterior. Mas, vamos mostrar através de um exemplo, que este raciocínio está errado, visto que distribuições iguais são contabilizadas como distintas.

Consideremos seis objectos distintos, que representaremos por A, B, C, D, E e F, para distribuir por duas caixas, sem que nenhuma fique vazia.

Suponhamos, então, que colocamos, por exemplo, o objecto A na primeira caixa e o objecto F na segunda caixa, para garantir que estas não fiquem vazias. Uma distribuição possível é:

Caixa 1: A, C, E Caixa 2: F, B, D

No entanto, se começássemos por colocar o objecto C na primeira caixa e o B na segunda, uma distribuição possível seria:

Caixa 1: C, A, E Caixa 2: B, D, F

As distribuições apresentadas são idênticas (observe-se que a composição de cada caixa é a mesma), mas contabilizadas como diferentes, se usarmos o raciocínio atrás referido para contar o número de maneiras de distribuir os n objectos diferentes pelas *k* caixas, de forma a todas terem, pelo menos, um objecto.

O processo correcto consiste em: ao número de maneiras de distribuir os *n* objectos pelas *k* caixas sem restrições - e que já vimos que é dado por k^n - retirar o número de casos em que uma ou mais caixas ficam vazias.

Representemos por

$$A_i = \{\text{formas de distribuir os objectos, ficando a caixa } i \text{ vazia}\}, \quad \text{para } i = 1, 2, ..., k$$

O número de casos em que pelo menos uma caixa fica vazia é obtido através do Principio de Inclusão-Exclusão por

$$\left|A_1 \cup \ldots \cup A_k\right| = \sum_i \left|A_i\right| - \sum_{i<j} \left|A_i \cap A_j\right| + \sum_{i<j<p} \left|A_i \cap A_j \cap A_p\right| - \ldots$$

$$= \sum_i \left|A_i\right| + (-1)^1 \sum_{i<j} \left|A_i \cap A_j\right| + (-1)^2 \sum_{i<j<p} \left|A_i \cap A_j \cap A_p\right| + \ldots$$

Para a caixa i ficar vazia, devem distribuir-se os objectos pelas $k-1$ caixas restantes, logo

$$\left|A_i\right| = (k-1)^n \quad \text{e} \quad \sum_i \left|A_i\right| = k(k-1)^n \Leftrightarrow \sum_i \left|A_i\right| = C_1^k (k-1)^n$$

Para duas caixas ficarem vazias, devem escolher-se estas de entre as k caixas e distribuir-se os objectos pelas $k-2$ restantes, logo

$$\left|A_i \cap A_j\right| = (k-2)^n \quad \text{e} \quad \sum_{i<j} \left|A_i \cap A_j\right| = C_2^k (k-2)^n$$

e, assim, sucessivamente.

Para $k-1$ caixas ficarem vazias, devem escolher-se estas de entre as k caixas e distribuir os objectos pela única caixa restante, logo

$$\left|A_1 \cap A_2 \cap \ldots \cap A_{k-1}\right| = 1^n \quad \text{e} \quad \text{a parcela correspondente} \quad C_{k-1}^k \cdot 1^n = C_{k-1}^k = k$$

Note-se que uma vez que não podem ficar todas as caixas vazias, tem-se

$$\left|A_1 \cap A_2 \cap \ldots \cap A_k\right| = 0$$

Concluímos, então, que o número de maneiras diferentes de distribuir n objectos por k caixas, sem que nenhuma caixa fique vazia, é dado por:

$$k^n - C_1^k (k-1)^n + C_2^k (k-2)^n - C_3^k (k-3)^n + \ldots + (-1)^{k-1} C_{k-1}^k 1^n$$

ou seja,

$$k^n + \sum_{p=1}^{k-1} (-1)^p C_p^k (k-p)^n$$

e como $(-1)^0 C_0^k = 1$, a expressão anterior pode escrever-se da seguinte forma:

$$\boldsymbol{\sum_{p=0}^{k-1} (-1)^p C_p^k (k-p)^n}$$

Este problema, de contar o número de maneiras possíveis de distribuir n objectos distintos por k caixas distintas, sem que nenhuma fique vazia, pode, também ser resolvido, através da fórmula:

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} \cdot k!$$

$\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ representa o número de subconjuntos de Stirling, isto é, o número de maneiras de particionar um conjunto de n objectos em k subconjuntos (disjuntos dois a dois) não vazios, em que

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} = k\left\{ \begin{matrix} n-1 \\ k \end{matrix} \right\} + \left\{ \begin{matrix} n-1 \\ k-1 \end{matrix} \right\} \quad , \quad k > 0 \quad \text{e} \quad \left\{ \begin{matrix} n \\ 0 \end{matrix} \right\} = \begin{cases} 0 & \text{se} \quad n \neq 0 \\ 1 & \text{se} \quad n = 0 \end{cases}$$

O número de subconjuntos de Stirling é dado em tabelas, por exemplo:

n \ k	0	1	2	3	4	5	6	7	8	9	10
0	1										
1	0	1									
2	0	1	1								
3	0	1	3	1							
4	0	1	7	6	1						
5	0	1	15	25	10	1					
6	0	1	31	90	65	15	1				
7	0	1	63	301	350	140	21	1			
8	0	1	127	966	1701	1050	266	28	1		
9	0	1	255	3035	7770	6951	2646	462	36	1	
10	0	1	511	9360	34115	42525	22827	5880	750	45	1

Tabela 7 – Número de subconjuntos de Stirling

Exemplo 11

De quantas maneiras diferentes é possível despachar oito cartas, dispondo de três carteiros? E se nenhum carteiro pode ficar sem trabalhar?

Este problema pode ser resolvido considerando que as cartas, obviamente distintas, correspondem aos objectos (n=8), e que os carteiros correspondem às caixas (k=3).

Assim, existem $3^8 = 6561$ maneiras de distribuir as missivas pelos carteiros.

E se nenhum carteiro pode ficar sem trabalhar?

Agora pretende-se distribuir as cartas pelos carteiros de modo a que, cada carteiro tenha pelo menos uma carta, o que corresponde a distribuir 8 objectos distintos por 3 caixas, não ficando nenhuma vazia.

Assim, existem $3^8 - C_1^3 2^8 + C_2^3 1^8 = 5796$ maneiras de distribuir as missivas pelos carteiros, despachando, cada um, pelo menos uma carta.

Ou, usando o número de subconjuntos de Stirling,

$$\left\{ \begin{matrix} 8 \\ 3 \end{matrix} \right\} \cdot 3! = 966 \times 6 = 5796$$

Se numa distribuição de objectos distintos em caixas, for à partida exigido que em cada caixa fique um determinado número de objectos, isto é, k_i na caixa i, $(i = 1,...,j)$, sendo o número de caixas j, menor do que n e $k_1 + k_2 + ... + k_j = n$, o número de maneiras de distribuir os n objectos pelas j caixas obedecendo a essas condições é dado por:

$$\frac{n!}{k_1!k_2!...k_j!}$$

Exemplo 12

De quantas maneiras se podem distribuir mãos de 5 cartas por 4 jogadores, tendo o baralho 52 cartas?

Ao primeiro jogador podemos dar 5 cartas de C_5^{52} maneiras diferentes, ao segundo jogador de C_5^{47}, etc. Então pela regra do produto, o número total de maneiras é dado por: $C_5^{52} \cdot C_5^{47} \cdot C_5^{42} \cdot C_5^{37}$.

Outra forma de resolver este problema é encará-lo como se distribuíssemos 52 objectos diferentes por 5 caixas distintas, ficando em quatro caixas (correspondem aos jogadores) 5 objectos e na outra caixa 32 objectos (corresponde às cartas que ficam por distribuir), assim, o número total de maneiras é dado por: $\frac{52!}{5!\cdot 5!\cdot 5!\cdot 5!\cdot 32!}$

3.2.5.2 Distribuição de objectos idênticos em caixas distintas

Suponhamos que temos n objectos idênticos e pretendemos saber de quantas maneiras os podemos distribuir por k caixas. As distribuições diferem umas das outras, apenas pelo número de objectos em cada caixa, uma vez que estes são todos iguais

Consideremos n objectos, todos idênticos, posicionados em fila. Determinar o número de maneiras de os colocar em k caixas, corresponde a determinar de quantos modos podem ser colocados $k-1$ separadores entre eles, formando, assim, as k caixas. Ou seja, o número de objectos até ao primeiro separador corresponde aos objectos da primeira caixa, o número de objectos entre o primeiro e o segundo separador corresponde aos da segunda caixa e, assim, sucessivamente.

Ora, se temos n objectos, existem entre eles $n-1$ lugares para colocar os separadores; considerando, também, as duas extremidades, existem ao todo $n+1$ lugares possíveis para os $k-1$ separadores, podendo haver repetição, isto é, entre dois objectos pode ser colocado mais do que um dos $k-1$ separadores, correspondendo a caixas vazias. O número de modos de efectuar essa distribuição pode ser dado pelas combinações, com repetição, de $n+1$ elementos a $k-1$, ou seja

$$CR_{k-1}^{n+1} = C_{k-1}^{n+k-1} = C_n^{n+k-1}$$

Exemplifiquemos, considerando oito bolas idênticas para serem colocadas em cinco caixas.

Uma distribuição possível é

significando que a primeira caixa está vazia, a segunda tem cinco bolas, a terceira duas bolas a quarta está vazia e a última tem um bola.

Contar o número de maneiras diferentes de efectuar a distribuição das oito bolas nas cinco caixas, corresponde a contar o número de modos de colocar os 4 separadores nos 9 lugares disponíveis. Note-se que, a ordem pela qual se seleccionam os lugares onde vão ser colocados os separadores não interessa e que, no mesmo lugar, pode ser colocado mais do que um separador. Assim, o número pretendido é dado por

$$CR_{5-1}^{8+1} = C_4^{9+4-1} = C_4^{12} = 495$$

Exemplo 13

Quantas são as soluções inteiras e não negativas da equação $x + y + z + t = 10$?

Duas soluções distintas são, por exemplo,

$$x = 2 \ , \ y = 2 \ , \ z = 0 \ , \ t = 6$$

$$x = 0 \ , \ y = 2 \ , \ z = 6 \ , \ t = 2$$

em que, os valores, apesar de serem os mesmos em ambas as soluções, correspondem a incógnitas diferentes.

A primeira solução pode ser interpretada como a distribuição de 10 objectos iguais todos representando o número um, por quatro caixas diferentes, correspondendo dois à primeira e à segunda caixas, nenhum à terceira e seis à quarta caixa. Com base nessa interpretação, determinar o número de soluções inteiras não negativas da equação, corresponde a determinar o número de maneiras de distribuir 10 objectos iguais por quatro caixas, ou seja,

$$CR_{4-1}^{10+1} = C_3^{11+3-1} = C_3^{13} = 286$$

Exemplo 14

De quantas maneiras é possível distribuir 4 pessoas por 2 andares, atendendo apenas ao número de pessoas em cada andar?

Esta situação pode ser resolvida considerando que se distribuem 4 objectos idênticos (visto só interessar o número de pessoas) por duas caixas que correspondem aos andares, desta forma, temos

$$CR_{2-1}^{4+1} = C_{2-1}^{4+2-1} = C_1^5 = 5$$

De facto há 5 maneiras de o fazer,

1º Andar	2º Andar
4	0
3	1
2	2
1	3
0	4

Vejamos, agora, de quantas maneiras é possível distribuir n objectos iguais por k caixas, de forma a que **nenhuma caixa fique vazia**.

Considerando, novamente, os n objectos posicionados em fila temos, nesta situação, $n-1$ lugares disponíveis para colocar os $k-1$ separadores. Visto que não pode haver caixas vazias, os separadores não podem ser colocados nos extremos e não pode haver repetição, isto é, não se pode colocar mais do que um separador no mesmo lugar. Assim, o número de maneiras de distribuir esses separadores, ou seja, o número de modos de distribuir os n objectos idênticos pelas k caixas sem nenhuma ficar vazia, é dado pelo número de modos de entre os $n-1$ lugares disponíveis, escolher $k-1$ lugares para colocar os separadores, ou seja,

$$\boldsymbol{C_{k-1}^{n-1}}$$

Exemplo 15

Quantas são as soluções inteiras positivas da equação $x + y + z + t = 10$?

Resolver este problema consiste em determinar o número de maneiras de distribuir 10 objectos iguais todos representando o número um, por quatro caixas, de tal modo que nenhuma fique vazia.

Logo, o número de soluções positivas da equação é dado por

$$C_{4-1}^{10-1} = C_3^9 = 84$$

3.2.5.3 Distribuição de objectos idênticos em caixas idênticas

O número de maneiras de distribuir n objectos idênticos por k caixas indistinguíveis, é dado pela soma das partições de n, em que o número de partes varia de 1 a k, ou seja,

$$\sum_{i=1}^{k} q_i(n) \quad , \quad k \leq n$$

Exemplo 16

De quantas maneiras diferentes se podem distribuir 5 objectos indistintos por 3 caixas iguais?

Corresponde a calcular

$$\sum_{i=1}^{3} q_i(5),$$

ou seja,

$$\underline{5} \quad \underline{0} \quad \underline{0}$$

$$\underline{4} \quad \underline{1} \quad \underline{0}$$

$$3 \quad \underline{2} \quad \underline{0}$$

$$3 \quad \underline{1} \quad \underline{1}$$

$$2 \quad \underline{2} \quad \underline{1}$$

Logo, existem 5 configurações possíveis.

Mas a questão é diferente se se pretender, por exemplo, determinar o número de partições de 5 com exactamente 3 elementos.

Esta situação pode ser interpretada como a colocação de 5 objectos iguais, todos representando o número um, em 3 caixas que são consideradas iguais (uma vez que a ordem das parcelas numa partição não interessa) de forma a que **nenhuma fique vazia**.

Na secção 2.3 do segundo capítulo, vimos as partições de 5. Dessas as que têm três elementos são apenas duas: $3+1+1$ e $2+2+1$, ou seja $q_3(5)=2$.

Generalizando tem-se que o número de maneiras de distribuir n objectos idênticos em k caixas idênticas $n \geq k$, sem que nenhuma fique vazia, é igual a

$$\boldsymbol{q_k(n) \quad , \quad k \leq n}$$

3.2.5.4 Distribuição de objectos distintos em caixas idênticas

O número de maneiras de distribuir n objectos distintos em k caixas idênticas **sem que nenhuma fique vazia** é dado pelo número de Stirling, ou seja, por

$$\left\{ \begin{matrix} \boldsymbol{n} \\ \boldsymbol{k} \end{matrix} \right\}$$

Observe-se que sendo as caixas idênticas não existe ordem entre elas nem, obviamente dentro de cada caixa.

No entanto, se apenas fixarmos o número de objectos distintos n mas não o número de caixas, então, o número de maneiras de os distribuir é dado pelo número de Bell. O número de Bell, $\boldsymbol{B_n}$, representa o número total de partições de um conjunto de n elementos.

$$\boldsymbol{B_n = \sum_{k=1}^{n} \left\{ \begin{matrix} n \\ k \end{matrix} \right\}}$$

Exemplo 17

De quantas maneiras é possível distribuir 2 bolas por 3 caixas?

a) Se as bolas e as caixas forem distintas, temos $3^2 = 9$ maneiras de distribuir as bolas pelas caixas. Representando as bolas por a e b as configurações possíveis são as seguintes:

1	$(ab, \_\_, \_\_)$	4	$(a, b, \_\_)$	7	$(b, a, \_\_)$
2	$(\_\_, ab, \_\_)$	5	$(a, \_\_, b)$	8	$(b, \_\_, a)$
3	$(\_\_, \_\_, ab)$	6	$(\_\_, a, b)$	9	$(\_\_, b, a)$

b) Se as bolas são idênticas mas as caixas distintas, temos $CR_{k-1}^{n+1} = C_{k-1}^{n+k-1} = C_2^4 = 6$ maneiras de distribuir as bolas pelas caixas. As configurações possíveis são as seguintes:

1	$(\_\_, 1, 1)$	4	$(\_\_, \_\_, 2)$
2	$(1, \_\_, 1)$	5	$(\_\_\ 2, \_\_)$
3	$(1, 1, \_\_)$	6	$(2, \_\_, \_\_)$

c) Se as bolas são idênticas e as caixas também, temos apenas duas configurações possíveis, uma bola e cada caixa, ou as duas bolas numa caixa.

1	$(\_\_, 1, 1)$	2	$(\_\_, \_\_, 2)$

3.2.6 Princípio da Casa dos Pombos

O Princípio da Casa dos Pombos também é conhecido como Princípio da Caixa de Sapatos ou Princípio de Dirichlet[39]. Este princípio é usado para responder a questões como: existe algum elemento, ou objecto, que possua determinada propriedade?

Das várias definições desse princípio existentes, apresentaremos, a seguir, três versões: uma mais formal, outra mais prática e uma terceira que pode ser considerada como uma versão generalizada.

Versão 1: Se f é uma função de um conjunto finito *X* para um conjunto finito *Y* e $|X| > |Y|$, então existem x_1 e $x_2 \in X$ com $x_1 \neq x_2$ tais que

$$f(x_1) = f(x_2)$$

Versão 2: Se n pombos voam para k casas que designamos por gaiolas e se n > k, então alguma gaiola vai ficar com pelo menos dois pombos.

Demonstração: Suponhamos que a afirmação é falsa: Então cada gaiola tem no máximo um pombo, logo existem k pombos o que é absurdo pois por hipótese existem mais de k pombos.

Versão 3: Se n objectos distintos são colocados em k caixas então há pelo menos uma caixa que contém $\left\lceil \frac{n}{k} \right\rceil$ objectos, onde $\lceil x \rceil$ representa o menor inteiro igual ou superior a x.

Este princípio, aparentemente ingénuo, é um dos recursos mais utilizados para resolver problemas de combinatória e, não raras vezes, surge em outras

---

[39] Peter Gustav Lejeune Dirichlet, (1805-1859) nasceu na Renânia e ensinou em Berlim durante quase 30 anos, antes de se transferir para Götingen, como sucessor de Gauss.. Embora seja mais conhecido por seus trabalhos em análise e equações diferenciais, Dirichlet foi também, um dos mais importantes matemáticos na área de teoria dos números do século XIX. O Princípio da Casa dos Pombos é devido a Dirichlet.

áreas da matemática. Há vários problemas interessantes que podem ser resolvidos recorrendo ao Princípio da casa dos pombos Para aplicá-lo, devemos identificar, na situação dada, o que faz o papel dos pombos e o que faz o papel das gaiolas.

Vejamos alguns exemplos:

Exemplo 18

Numa festa de aniversário com mais de 12 crianças, mostre que existem pelo menos duas nascidas no mesmo mês.

Como temos mais crianças (pombos) do que meses (gaiolas), pelo menos num mês deverá haver duas crianças a fazer anos.

Exemplo 19

Entre 100 pessoas, quantas, no mínimo, nasceram no mesmo mês?

Temos neste problema 100 “pombos” e 12 “gaiolas”, logo, basta calcular

$$\left\lceil \frac{100}{12} \right\rceil = 9,$$

ou seja, existem pelo menos 9 pessoas que fazem anos no mesmo mês.

Exemplo 20

Mostre que em Madrid, com mais de 4 milhões de habitantes, há pelo menos vinte pessoas com o mesmo número de cabelos.

Nota: É razoável supor-se que nenhuma pessoa tem 200 mil ou mais fios de cabelo, normalmente uma pessoa tem no máximo 150 mil fios de cabelo.

Considerando que os habitantes correspondem aos pombos, vamos colocá-los na respectiva gaiola, de acordo com o número de fios de cabelo.

Supondo que todas as gaiolas têm menos de 20 pessoas, teríamos um total de habitantes inferior a $20 \times 200000 = 4 \times 10^6$, o que é absurdo pois sabe-se que Madrid tem mais de 4 milhões de habitantes.

Exemplo 21

Um exame possui 10 questões de múltipla escolha, com quatro alternativas cada. Qual deverá ser o menor número de alunos a fazer exame para podermos garantir que, pelo menos dois deles, dão exactamente as mesmas respostas a todas as questões?

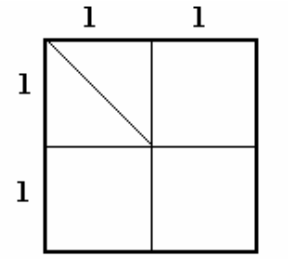
Neste caso, aos pombos correspondem os alunos e, às gaiolas, as possíveis sequências de respostas. Como cada questão pode ser respondida de 4 modos, o exame pode ser respondido de $4^{10} = 1\,048\,576$ maneiras diferentes. Logo, só se pode ter a certeza de que dois alunos dão exactamente as mesmas respostas, se houver, pelo menos, 1 048 577 examinandos.

Exemplo 22

Escolhem-se 5 pontos ao acaso, sobre a superfície de um quadrado de lado 2. Mostre que, pelo menos um dos segmentos que esses pontos determinam, tem comprimento menor ou igual a 2.

Dividimos o quadrado de lado 2 em quatro quadrados de lado 1, de acordo com a figura seguinte.

Os 5 pontos correspondem aos pombos e as gaiolas serão os 4 quadrados. Em cada gaiola, a distância máxima entre dois pontos é igual à sua diagonal que é $\sqrt{2}$.



Portanto, usando o princípio, temos que pelo menos 2 pontos estarão na mesma gaiola e, assim, determinam um segmento com comprimento menor ou igual a $\sqrt{2}$.

Exemplo 23

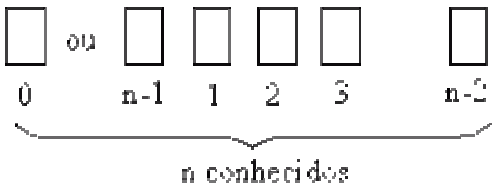
Mostre que, em qualquer conjunto com *n* números inteiros, existem, pelo menos dois, cuja diferença é um múltiplo de $n-1$.

Neste caso, temos n pombos. Considerando r o resto da divisão de um número inteiro por $(n-1)$, sabemos que r pertence ao conjunto $\{0,1,2,\ldots,n-2\}$. As $(n-1)$ classes de restos serão as gaiolas. Como temos um conjunto com n inteiros, então, pelo menos dois deles que designaremos por a e b, têm o mesmo resto r na divisão por $(n-1)$, ou seja, $a = p(n-1)+r$ e $b = q(n-1)+r$, onde *p* e *q* são inteiros e *r* pertence ao conjunto $\{0,1,2,\ldots,n-2\}$. Portanto, $a-b=(p-q)\cdot(n-1)$, isto é, $a-b$ é um múltiplo de $(n-1)$.

Exemplo 24

Mostre que, numa sala com n pessoas, há sempre duas pessoas que conhecem exactamente o mesmo número de pessoas que se encontram na sala.
Nota: supõem-se que se a conhece b, b conhece a, ou seja, "conhecer" é uma relação simétrica.

Neste caso, as pessoas serão os nossos pombos e, em cada gaiola, estarão agrupadas as pessoas que conhecem o mesmo número de pessoas, isto é, que têm o mesmo número de conhecidos. Assim, as possíveis quantidades de conhecidos são 0,1, 2, 3, ..., $n-1$. À primeira vista, parece que temos n gaiolas e n pombos, o que inviabilizaria a utilização do princípio. No entanto, observe-se que se alguma das pessoas conhece todas as outras $n-1$ pessoas, então é impossível que haja alguma pessoa que não conheça ninguém, 0 pessoas. Assim, a gaiola 0 ou $n-1$ permanecerá desocupada e os n pombos devem ser, portanto, distribuídos em $n-1$ gaiolas.



Logo, pelo princípio de Dirichlet, uma das gaiolas será ocupada pelo menos por dois pombos, ou seja, há pelo menos duas pessoas que conhecem exactamente o mesmo número de participantes.

3.3 Aplicação às Estatísticas da Física

Suponhamos um conjunto de *n* partículas elementares (electrões, protões, neutrões, etc.). Em Mecânica Estatística admite-se que há *k* estados microscópicos nos quais se pode encontrar cada partícula (por exemplo *k* níveis de energia). Para descrever uma configuração possível do conjunto escrevemos

$$n_1 , n_2 ,..., n_j ,..., n_k$$

cuja componente n_j representa o número de partículas no estado j.

1. Estatística de Maxwell - Boltzmann. Nesta estatística admite-se que as partículas são distinguíveis umas das outras e então, sendo

   $$n_1 + n_2 + ...,+n_k = n$$

   Temos que o número de configurações possíveis é dado pelo número de permutações com repetição (distribuição de *n* partículas por *k* níveis de energia):

   $$P^n_{n_1,n_2,...,n_k} = \frac{n!}{n_1!n_2!...n_k!} \text{ sendo } n_1 , n_2 ,..., n_k \in IN \text{ e } \sum_{i=1}^{k} n_i = n$$

2. Estatística de Bose – Einstein: aplica-se a fotões, núcleos e átomos que contenham um número par de partículas elementares em número *n* e consideradas indistinguíveis. Temos assim uma distribuição de *n* partículas indistinguíveis por *k* estados (caixas) distinguíveis, logo o número de configurações possíveis é

   $$C_n^{n+k-1} \text{ pois } n < k \text{ , em princípio.}$$

3. Estatística de Fermi – Dirac: aplica-se a protões, electrões e neutrões e baseia-se no princípio de exclusão de Pauli que afirma não poderem duas ou mais partículas encontrar-se no mesmo estado (nível de energia). O número de configurações possíveis é dado por

   $$C_n^k \text{ , sendo } \begin{cases} k \text{ o número de estados de energia distinguíveis} \\ \text{n o número de partículas indistinguíveis} \end{cases}$$

A diferença dos resultados a que conduzem as Estatísticas de Maxwell–Boltzmann, de Bose – Einstein e de Fermi – Dirac poderia fazer pensar que só uma delas tem aplicação na Física. Na realidade a Mecânica Ondulatória leva à distinção entre dois tipos de partículas, para as quais a Estatística Clássica de Maxwell – Boltzmann não deve ser aplicada, umas para as quais é válida a Estatística de Bose – Einstein e que são os bosões e outras para as quais é válida a Estatística de Bose – Einstein e que são os fermiões . A diferença entre os dois tipos de partículas encontra-se na simetria da função de onda. Os bosões são representados em Mecânica Quântica por funções de onda simétricas, ou seja, funções que não mudam de sinal quando as partículas permutam, enquanto os fermiões são representados por funções de onda antissimétricas devido ao facto de obedecerem ao Princípio de Exclusão de Pauli no qual se baseia a Estatística de Fermi – Dirac.

Assim os electrões e os protões que obedecem ao Princípio de Exclusão de Pauli seguem a Estatística de Fermi – Dirac, enquanto os átomos neutros obedecem à Estatística de Bose – Einstein. Quer dizer, todos os conjuntos que têm um número par de partículas elementares, como é o caso do átomo de Hidrogénio, (um protão mais um electrão) seguem a Estatística de Bose – Einstein, enquanto os conjuntos com um número ímpar de partículas elementares seguem a Estatística de Fermi – Dirac.

3.4 Números Binomiais, Polinomiais e Triângulo de Pascal

3.4.1 Números Binomiais

Aos números C_p^n dá-se o nome de coeficientes binomiais porque correspondem aos coeficientes sucessivos do desenvolvimento da potência de expoente n (inteiro e positivo) do binómio $x + y$.

Teorema Binomial: Seja $n \in IN$. Então,

$$\boldsymbol{(x+y)^n = \sum_{k=0}^{n} C_k^n \; x^{n-k} \; y^k}$$

Demonstração:

A chave da demonstração está relacionada com a forma como multiplicamos polinómios. Quando desenvolvemos,

$$(x+y)^2 = (x+y)(x+y) = xx + xy + yx + yy$$

e agrupamos os termos semelhantes, obtemos $x^2 + 2xy + y^2$

O processo para $(x+y)^n$ é precisamente o mesmo. Escrevemos *n* factores $(x+y)$:

$$\underbrace{(x+y)}_{1}\underbrace{(x+y)}_{2}\underbrace{(x+y)}_{3}...\underbrace{(x+y)}_{n}$$

Formamos, então, todos os termos possíveis tomando um *x* ou um *y* dos factores 1, 2, 3, …, *n.* Obtemos, assim, uma soma de monómios de grau n. Para cada valor de k, $0 \le k \le n$, se escolhermos y em k dos *n* parênteses, x será escolhido nos restantes parênteses, ou seja, em $n-k$ dos parênteses e o produto será igual a $x^{n-k}y^k$. A escolha dos k parênteses dos *n,* onde o y vai ser escolhido pode ser feita de C_k^n modos diferentes. Então $(x+y)^n$ é uma soma onde, para cada valor de $k \in \{0,1,...,n\}$, há C_k^n parcelas iguais a $x^{n-k}y^k$, isto é,

$$(x+y)^n = \sum_{k=0}^{n} C_k^n \; x^{n-k} \; y^k$$

Obviamente que a demonstração pode ser feita por indução.

Não confundir coeficiente binomial com o coeficiente "normal" de um monómio.

Vejamos a seguinte questão:

Qual é o coeficiente do termo de grau 6 do polinómio reduzido equivalente a $\left(x^2-\frac{1}{2}\right)^{12}$?

Pela fórmula do binómio de Newton,

$$\left(x^2-\frac{1}{2}\right)^{12}=\sum_{k=0}^{12} C_k^{12}\cdot\left(x^2\right)^{12-k}\cdot\left(-\frac{1}{2}\right)^k$$

para ter grau 6, k terá de ser 9 , $2(12-k)=6\Leftrightarrow k=9$.

Contudo, o coeficiente pedido não corresponde ao coeficiente binomial C_9^{12}, mas sim ao produto de C_9^{12} por $\left(-\frac{1}{2}\right)^9$, ou seja, $-\frac{220}{512}=-\frac{55}{120}$

O teorema binomial parece ter sido descoberto por Omar Khayyam (1050-1123), poeta persa e matemático. No entanto, é hoje conhecido como binómio de Newton, pois Newton utilizou-o frequentemente nos seus cálculos.

3.4.2 Números Polinomiais

Uma generalização do binómio de Newton corresponde ao polinómio de Leibniz.

Polinómio de Leibniz: Seja $n\in IN$. Então,

$$\left(x_1+x_2+...+x_p\right)^n=\sum\frac{n!}{\alpha_1!\alpha_2!...\alpha_p!}\cdot x_1^{\alpha_1}\cdot x_2^{\alpha_2}\cdot...x_p^{\alpha_p}$$

onde o somatório é estendido a todos os valores inteiros, positivos ou nulos de, $\alpha_1,\alpha_2,...,\alpha_p$ tais que $\alpha_1+\alpha_2+...+\alpha_p=n$.

Demonstração:

O termo genérico do produto é obtido escolhendo um x_i em cada um dos n parênteses e multiplicando-os uns pelos outros. Se em α_1 dos parênteses escolhermos x_1, em α_2 dos parênteses escolhermos x_2, etc…obteremos $x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot ... x_p^{\alpha_p}$ ($\alpha_1, \alpha_2, ..., \alpha_p$ inteiros não negativos e $\alpha_1 + \alpha_2 + ... + \alpha_p = n$).

O termo $x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot ... x_p^{\alpha_p}$ aparece tantas vezes quanto os modos de escolher, de entre os *n* parênteses, α_1 para seleccionar x_1 para factor, de entre os restantes $n - \alpha_1$ parênteses, α_2 para seleccionar o x_2 como factor e assim sucessivamente, ou seja,

$$C_{\alpha_1}^{n} \cdot C_{\alpha_2}^{n-\alpha_1} \cdot C_{\alpha_3}^{n-\alpha_1-\alpha_2} \cdot ... \cdot C_{\alpha_p}^{n-\alpha_1-...-\alpha_{p-1}} = \frac{n!}{\alpha_1!\alpha_2!...\alpha_p!}$$

De facto,

$$C_{\alpha_1}^{n} \cdot C_{\alpha_2}^{n-\alpha_1} \cdot C_{\alpha_3}^{n-\alpha_1-\alpha_2} \cdot ... \cdot C_{\alpha_p}^{n-\alpha_1-...-\alpha_{p-1}} =$$

$$= \frac{n!}{\alpha_1!(n-\alpha_1)!} \times \frac{(n-\alpha_1)!}{\alpha_2!(n-\alpha_1-\alpha_2)!} \times \frac{(n-\alpha_1-\alpha_2)!}{\alpha_3!(n-\alpha_1-\alpha_2-\alpha_3)!} \times ... \times \frac{(n-\alpha_1-...-\alpha_{p-1})!}{\alpha_p!(n-\alpha_1-...-\alpha_p)!} =$$

$$= \frac{n!}{\alpha_1!\alpha_2!...\alpha_p!}$$

Note-se que $(n-\alpha_1-...-\alpha_p)! = (n-n)! = 0! = 1$

Logo, $x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot ... x_p^{\alpha_p}$ aparece no desenvolvimento do polinómio $\frac{n!}{\alpha_1!\alpha_2!...\alpha_p!}$ vezes.

Aos números $\frac{n!}{\alpha_1!\alpha_2!...\alpha_p!}$ que generalizam os coeficientes binomiais, chamam-se, por analogia, coeficientes polinomiais.

Exemplo 25

Calculemos $\left(x^2+2x-1\right)^4$.

$$\left(x^2+2x-1\right)^4=\sum\frac{4!}{\alpha_1!\alpha_2!\alpha_3!}\cdot\left(x^2\right)^{\alpha_1}\cdot(2x)^{\alpha_2}\cdot(-1)^{\alpha_3}=\sum\frac{24}{\alpha_1!\alpha_2!\alpha_3!}\cdot 2^{\alpha_2}(-1)^{\alpha_3}x^{2\alpha_1+\alpha_2}$$

onde $\alpha_1,\alpha_2,\alpha_3$ são inteiros não negativos tais que $\alpha_1+\alpha_2+\alpha_3=4$

Vejamos os possíveis valores para $\alpha_1,\alpha_2,\alpha_3$ e os correspondentes termos do desenvolvimento.

α_1	α_2	α_3	Termo
0	0	4	1
0	1	3	$-8x$
0	2	2	$24x^2$
0	3	1	$-32x^3$
0	4	0	$16x^4$
1	0	3	$-4x^2$
1	1	2	$24x^3$
1	2	1	$-48x^4$
1	3	0	$32x^5$
2	0	2	$6x^4$
2	1	1	$-24x^5$
2	2	0	$24x^6$
3	0	1	$-4x^6$
3	1	0	$8x^7$
4	0	0	x^8

Somando e reduzindo os termos semelhantes temos,

$$\left(x^2+2x-1\right)^4=x^8+8x^7+20x^6+8x^5-26x^4-8x^3+20x^2-8x+1$$

3.4.3 Triângulo de Tartaglia - Pascal

O triângulo aritmético também conhecido por Triângulo de Pascal é um modelo numérico famoso no mundo da Matemática, porquanto é uma fonte inesgotável de riquezas matemáticas, escondendo propriedades e curiosidades em número tão elevado que constitui, por si só, um pequeno universo matemático de grande utilidade no campo numérico.

O triângulo aritmético é conhecido por Triângulo de Pascal por ter sido este matemático a apresentar o primeiro tratado sobre o triângulo aritmético. No entanto, Niccolò Fontana (1499-1577), matemático italiano, mais conhecido por Tartaglia (nome que lhe foi atribuído por ser gago) cerca de um século antes de Pascal, já usara o triângulo aritmético nos seus trabalhos, nomeadamente no cálculo dos coeficientes do binómio de Newton. Foi o italiano o primeiro a divulgá-lo na Europa, razão pela qual alguns designam este triângulo por Triângulo de Tartaglia. Mas, muito antes, os matemáticos árabes e os chineses já o utilizavam. O documento chinês mais antigo associado ao triângulo data de 1050 e o mais famoso matemático chinês com ele relacionado foi Yang Hui, em 1250, razão pela qual a denominação chinesa mais comum para o triângulo aritmético é Triângulo de Yang Hui. No entanto, parece que a mais remota referência ao triângulo aritmético é atribuída a Omar Khayyam que, possivelmente, precedeu Yang Hui.

A sua construção é extremamente simples. No vértice superior, designada por linha zero, colocamos C_0^0, na primeira linha colocamos C_0^1 e C_1^1, na linha seguinte C_0^2, C_1^2 e C_2^2 e assim sucessivamente. Este triângulo pode-se continuar indefinidamente aumentando o número de linhas.

$$
\begin{array}{ccccccccccccc}
 & & & & C_0^0 & & & & & & & & \\
 & & & C_0^1 & & C_1^1 & & & & & & & \\
 & & C_0^2 & & C_1^2 & & C_2^2 & & & & & & \\
 & C_0^3 & & C_1^3 & & C_2^3 & & C_2^3 & & & & & \\
C_0^4 & & C_1^4 & & C_2^4 & & C_3^4 & & C_4^4 & & & & \\
 & C_0^5 & & C_1^5 & & C_2^5 & & C_3^5 & & C_4^5 & & C_5^5 & \\
C_0^6 & & C_1^6 & & C_2^6 & & C_3^6 & & C_4^6 & & C_5^6 & & C_6^6
\end{array}
$$

Figura 18 – Triângulo de pascal com os coeficientes binomiais

Substituindo cada coeficiente binomial pelo valor numérico correspondente, obtemos outra versão do triângulo.

$$
\begin{array}{ccccccccccccc}
 & & & & 1 & & & & & & & & \\
 & & & 1 & & 1 & & & & & & & \\
 & & 1 & & 2 & & 1 & & & & & & \\
 & 1 & & 3 & & 3 & & 1 & & & & & \\
1 & & 4 & & 6 & & 4 & & 1 & & & & \\
 & 5 & & 10 & & 10 & & 5 & & 1 & & & \\
6 & & 15 & & 20 & & 15 & & 6 & & 1 & & \\
 & 21 & & 35 & & 35 & & 21 & & 7 & & 1 & \\
28 & & 56 & & 70 & & 56 & & 28 & & 8 & & 1
\end{array}
$$

Figura 19 – Triângulo de Pascal

Existe uma estreita relação entre os elementos do triângulo e os coeficientes no desenvolvimento do binómio de Newton.

Observemos que, por exemplo, os elementos da segunda linha, 1, 2, 1, são os coeficientes do desenvolvimento de $(x+y)^2 = x^2 + 2xy + y^2$ e os elementos da terceira linha, 1, 3, 3, 1 são os coeficientes do desenvolvimento de $(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$. Os elementos da linha *n* correspondem aos coeficientes do desenvolvimento do binómio $(x+y)^n$.

Como já referido, este triângulo é prodigioso em propriedades numéricas; vejamos algumas.

Observando-o verificamos que qualquer elemento que o constitui pode ser obtido através da soma dos dois elementos que estão imediatamente acima dele, ou seja, um elemento genérico, C_p^n, (linha n, posição p) pode ser escrito como a soma de C_{p-1}^{n-1} com C_p^{n-1}, isto é,

$$\boldsymbol{C_p^n + C_{p+1}^n = C_{p+1}^{n+1}}$$

designada como a **Relação de Stifel**, já provada anteriormente.

O triângulo de Pascal é simétrico. Por isso numa mesma linha os elementos equidistantes dos extremos são iguais, ou seja, em linguagem matemática,

$$\boldsymbol{C_p^n = C_{n-p}^n \quad , n, p \in IN_0 \ , \ p \leq n}$$

Se adicionarmos os elementos de cada linha obtemos os seguintes números: 1, 2, 4, 8, 16, 32, 64, 128, 256, …, ou escritos de outra forma, $2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, \ldots$.

Será que a soma dos elementos da linha n é igual a 2^n?

Ora a soma dos elementos da linha n é $\sum_{p=0}^{n} C_p^n$, o que corresponde a adicionar os coeficientes do desenvolvimento do binómio de Newton,

$$(x+y)^n = \sum_{k=0}^{n} C_k^n \, x^{n-k} \, y^k$$

Como esta fórmula é válida para quaisquer valores de x e y, em particular é válida para $x=1$ e $y=1$, tem-se, então

$$(1+1)^n = \sum_{k=0}^{n} C_k^n \, 1^{n-k} \, 1^k \Leftrightarrow \sum_{k=0}^{n} C_k^n = 2^n$$

o que demonstra o chamado,

Teorema das linhas: a soma dos elementos da linha n é igual a 2^n, ou seja,

$$C_0^n + C_1^n + C_2^n + ... + C_n^n = 2^n .$$

A igualdade anterior é de grande utilidade em alguns problemas de contagem, vejamos um exemplo.

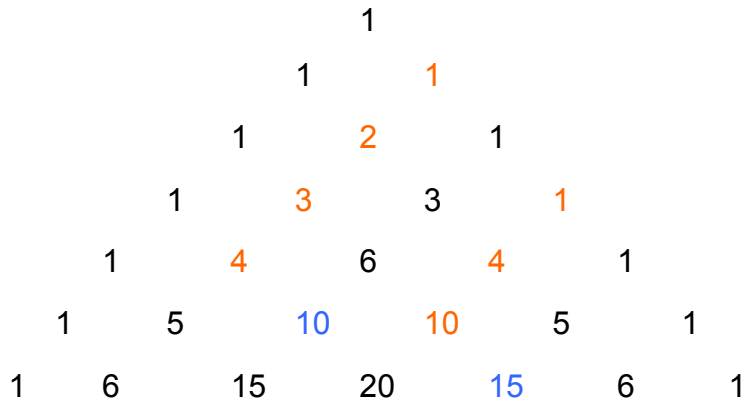
Exemplo 26

Quantos subconjuntos se podem formar a partir de um conjunto A com 10 elementos?

Além do conjunto vazio, podem-se formar conjuntos com um, dois, três,…, dez elementos. O número de subconjuntos que se podem formar a partir do conjunto A é dado pela soma,

$$C_0^{10} + C_1^{10} + C_2^{10} + C_3^{10} + C_4^{10} + C_5^{10} + C_6^{10} + C_7^{10} + C_8^{10} + C_9^{10} + C_{10}^{10} = 2^{10} = 1024$$

A soma de elementos de uma diagonal (começando no primeiro) é igual ao elemento que está avançado uma linha e uma coluna em relação à última parcela da soma. Dois exemplos:
1 + 2 + 3 + 4 = 10 e
1 + 4 + 10 = 15



Generalizando,

$$C_n^n + C_n^{n+1} + C_n^{n+2} + ... + C_n^{n+k} = C_{n+1}^{n+k+1}$$

Demonstração:

Sabemos que,

$C_{n+1}^{n+1} = C_n^n$ e pela relação de Stifel temos,

$C_{n+1}^{n+2} = C_{n+1}^{n+1} + C_n^{n+1}$

$C_{n+1}^{n+3} = C_{n+1}^{n+2} + C_n^{n+2}$

...

$C_{n+1}^{n+k} = C_{n+1}^{n+k-1} + C_n^{n+k-1}$

$C_{n+1}^{n+k+1} = C_{n+1}^{n+k} + C_n^{n+k}$

Somando membro a membro e simplificando as parcelas iguais em membros opostos, temos

$$C_{n+1}^{n+k+1} = C_n^n + C_n^{n+1} + C_n^{n+2} + \ldots + C_n^{n+k-1} + C_n^{n+k}$$

Na segunda diagonal encontramos a sequência dos números naturais. Quando um deles for primo então todos os elementos dessa linha, excluindo o 1, são divisíveis por ele.

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

Na terceira diagonal temos a sequência dos números triangulares, assim designados por formarem triângulos. O termo geral desta sucessão é $T_n = \frac{n(n+1)}{2}$

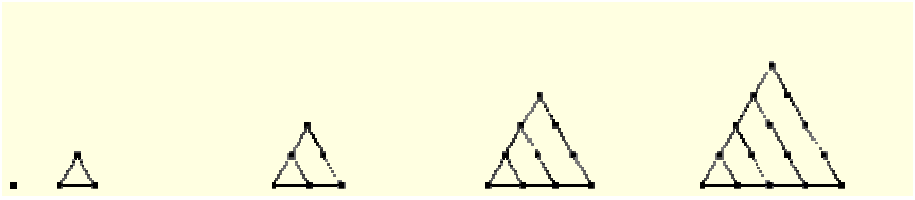


Figura 20 – Números triangulares

No triângulo de Pascal podemos, também, encontrar os termos da famosa sucessão de Fibonacci,

$$1 \quad 1 \quad 2 \quad 3 \quad 5 \quad 8 \quad 13 \quad 21 \quad 34 \quad 55 \ldots$$

e que é definida recursivamente por,

$$F_n = \begin{cases} F_1 = 1 \\ F_2 = 1 \\ F_{n+2} = F_n + F_{n+1} \quad , \quad n \in IN \end{cases}$$

sendo $F_{n+2} = F_n + F_{n+1}$ a relação de recorrência.

A soma dos elementos de cada uma das linhas traçadas no triângulo abaixo, designadas por diagonais ascendentes, corresponde a um termo da sucessão de Fibonacci.

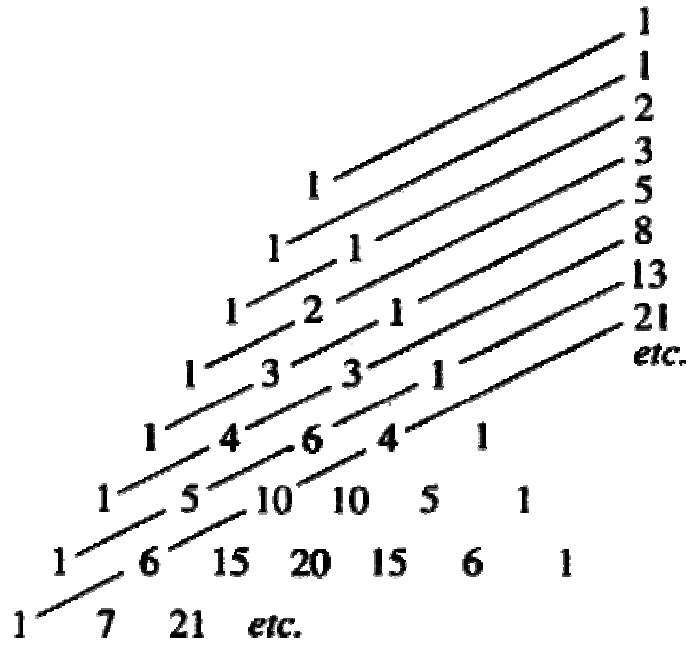


Figura 21 – Triângulo de pascal e a sucessão de Fibonacci

Demonstremos a afirmação anterior.

As duas primeiras diagonais ascendentes do triângulo de Pascal, consistem em um só número, o número um, representando os dois primeiros termos da sucessão.

Comecemos por demonstrar que toda a diagonal ascendente, a partir da terceira, é obtida como soma dos elementos das duas diagonais anteriores.

Designemos por d_n a soma dos elementos da n-ésima diagonal e mostremos, por indução, que:

$d_{n+2} = d_n + d_{n+1} \quad , \quad \forall n \in IN$ (1)

1º) Para $n = 1$, a igualdade $d_3 = d_1 + d_2 \Leftrightarrow 2 = 1 + 1$ é verdadeira.

2º) Vamos supor a validade da proposição (1) para p e $p+1 \in IN$, arbitrários, tendo deste modo,

$$d_p = \binom{p-1}{0} + \binom{p-2}{1} + \binom{p-3}{2} + \ldots$$

$$d_{p+1} = \binom{p}{0} + \binom{p-1}{1} + \binom{p-2}{2} + \ldots$$

Queremos provar que para $p+2 \in IN$, $d_{p+2} = d_p + d_{p+1}$

$$d_p + d_{p+1} = \left[\binom{p-1}{0} + \binom{p-2}{1} + \binom{p-3}{2} + \ldots\right] + \left[\binom{p}{0} + \binom{p-1}{1} + \binom{p-2}{2} + \ldots\right] =$$

$$= \binom{p}{0} + \left[\binom{p-1}{0} + \binom{p-1}{1}\right] + \left[\binom{p-2}{1} + \binom{p-2}{2}\right] + \ldots =$$

$$= \binom{p}{0} + \binom{p}{1} + \binom{p-1}{2} = \qquad \text{(pela relação de Stifel)}$$

$$= \binom{p+1}{0} + \binom{p}{1} + \binom{p-1}{2} = \qquad \text{visto que} \binom{p}{0} = \binom{p+1}{0}$$

$$= d_{p+2}$$

Logo, $d_{n+2} = d_n + d_{n+1} \quad , \quad \forall n \in IN$

Para concluir a demonstração falta provar que $d_n = F_n \quad , \quad \forall n \in In$

Mostremos, por indução, que $d_{n+2} = F_{n+2} \quad , \quad \forall n \in In$ (2)

1º) Para $n = 1$ temos $d_3 = \binom{2}{0} + \binom{1}{1} = 1 + 1 = 2 = F_3$ e note-se que $d_1 = 1 = F_1$ e $d_2 = 1 = F_2$

2º) Vamos supor que (2) é válida para p e $p+1 \in IN$, arbitrários, e queremos provar que é válida para $p+2 \in IN$

Temos, então, que $d_p = F_p$ e $d_{p+1} = F_{p+1}$ e queremos mostrar que $d_{p+2} = F_{p+2}$

Ora, já provamos que $d_{n+2} = d_n + d_{n+1}$, $\forall n \in IN$ pelo que, então, temos

$$\begin{aligned} d_{p+2} &= d_p + d_{p+1} \\ &= F_p + F_{p+1} \qquad \text{(por hipótese)} \\ &= F_{p+2} \qquad \text{(pela propriedade recursiva dos números de Fibonacci)} \end{aligned}$$

Concluímos, assim, que a soma dos elementos de cada diagonal ascendente, corresponde a um termo da sucessão de Fibonacci.

É extremamente interessante encontrar conexões entre assuntos que parecem à partida distantes. Um exemplo surpreendente é a relação entre o triângulo de Pascal e o triângulo de Sierpinski.

Se no triângulo de Pascal, pintarmos de preto os números ímpares e de branco os pares obtemos a seguinte figura:

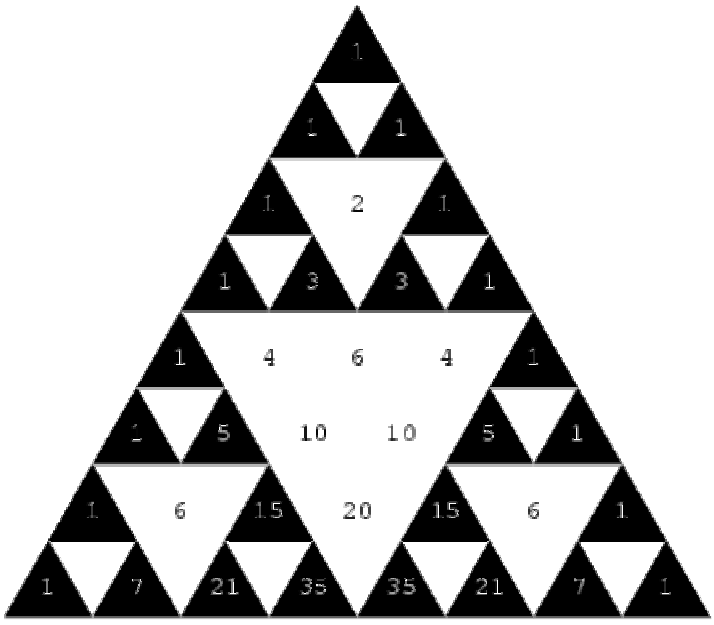


Figura 22 – Triângulo de Sierpinski

O triângulo de Pascal "transforma-se" assim no triângulo de Sierpinski!

O triângulo de Sierpinski é um fractal. Os fractais nunca perdem a sua estrutura qualquer que seja a distância de visão, isto é, são auto-semelhantes,

são independentes da escala considerada. Podem então ser gerados por um processo iterativo e a sua dimensão, D, que é uma dimensão fractal é calculada através de $D = \frac{\log N}{\log(1/r)}$ em que r representa a razão de semelhança da redução e N é o número de partes iguais entre si em que a figura é transformada. A dimensão do triângulo de Sierpinski é aproximadamente, $D = \frac{\log 3}{\log\left(\frac{1}{1/2}\right)} \approx 1.6$

Figura 23 - Construção do triângulo de Sierpinski.

3.4.4 Aplicação do Binómio de Newton e do Triângulo de Pascal na Genética

A cor da pele considerando apenas cinco fenótipos, envolve dois pares de alelos, P/p e B/b. Os alelos representados por maiúsculas determinam a produção de grande quantidade de melanina, enquanto que os representados por letras minúsculas determinam uma menor produção de melanina.

Assim, temos

Genótipos	**Fenótipos**
PPBB	Negro
PpBB ou PPBb	Mulato escuro
PPbb ou PpBb ou ppBB	Mulato médio
Ppbb ou ppBb	Mulato claro
ppbb	Branco

Tabela 8 – Categorias de coloração da pele

No casamento de uma pessoa do genótipo negro (PPBB) com uma de genótipo branco (ppbb), todos os descendentes serão mulatos médios. Como o

negro só produz gâmetas PB e o branco apenas pb, todos os indivíduos oriundos desses gâmetas serão PpBb, ou seja mulatos médios.

Se, agora, cruzássemos dois desses mulatos médios, quais serão as proporções fenotípicas da descendência?

Como os gâmetas produzidos por ambos são: PB, Pb, pB e pb, temos

Gametas	**PB**	**Pb**	**pB**	**pb**
PB	PPBB	PPBb	PpBB	PpBb
Pb	PPBb	PPbb	PpBb	Ppbb
pB	PpBB	PpBb	ppBB	ppBb
pb	PpBb	Ppbb	ppBb	ppbb

Tabela 9 – Gâmetas

Analisando a tabela temos: 1 negro, 4 mulatos escuros, 6 mulatos médios, 4 mulatos claros e 1 branco. Em percentagem temos: 6.25% de negros, 25% e mulatos escuros, 37.5% de mulatos médios, 25% de mulatos claros e 6.25% de brancos.

O mesmo problema pode ser resolvido aplicando o binómio de Newton. Os fenótipos distribuem-se segundo os coeficientes do desenvolvimento de $(a+b)^4$, onde a representa os genes aditivos, ou efectivos (P,B); b representa os genes não efectivos e 4 representa o número de genes envolvidos.

Assim,

$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$

ou seja,

1 negro, com 4 genes efectivos,

4 mulatos escuros, com 3 genes efectivos,

6 mulatos médios, com 2 genes efectivos,

4 mulatos claros, com 1 gene efectivo,

1 branco, com nenhum gene efectivo.

Podemos chegar à mesma conclusão recorrendo aos elementos da quarta linha do triângulo de Pascal. Permite, assim, resolver o problema sem ter de construir o quadro de cruzamentos nem desenvolver o Binómio de Newton.

4. Grafos

A primeira referência conhecida sobre a Teoria dos Grafos data de 1736, quando o matemático suíço Leonard Euler propôs apresentar uma solução para o chamado problema das Pontes de Königsberg. A cidade russa de Königsberg, hoje conhecida como Kaliningrad, situa-se junto do Rio Pregel, sendo constituída por margem Norte(C), margem Sul(B), ilha Oeste(A) e ilha Este(D). A unir estes 4 pontos havia 7 pontes: 2 entre N e A, 2 entre S e A e outras 3 unindo D a respectivamente, N, S e A, conforme ilustra a figura abaixo.

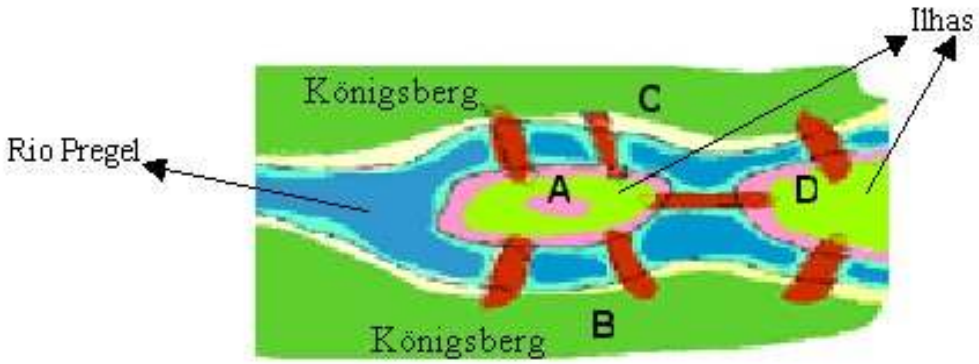
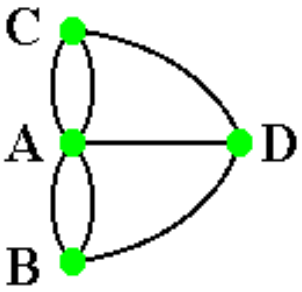


***Figura 24 – Pontes de** Königsberg*

O problema que se colocava a Euler traduzia-se em determinar se seria possível partir de um determinado ponto da cidade e voltar ao mesmo ponto, atravessando cada ponte uma e uma só vez.

A ideia de Euler consistiu em representar as quatro zonas da cidade, delimitadas pelo rio, por vértices e as pontes por arestas entre esses vértices, ou seja, representou o mapa por um grafo. O problema proposto passa a poder ser enunciado do seguinte modo: será possível percorrer o diagrama inteiro do grafo, sem passar na mesma aresta mais do que uma vez ?



Ora, o caminho pretendido só é possível se cada vértice estiver ligado a um número par de arestas pois, se se chega a uma zona por uma ponte, a condição de que cada ponte seja percorrida uma só vez implica que se possa sair por uma outra. Dado que todos os vértices do grafo têm grau ímpar, o problema proposto é

impossível. Por outras palavras o problema é impossível porque não admite um circuito de Euler.

A Teoria dos Grafos, com origem no século XVIII, passou a ser objecto de um enorme interesse, até então não verificado no âmbito da ciência matemática, a partir da década de 30 do Século XX. Tal terá tido a ver com o potencial de aplicações deste ramo da matemática na resolução de questões práticas da vida moderna numa diversidade de áreas como, na química, na economia, na gestão, no marketing, na transmissão de informação, na distribuição de produtos, no desenho de circuitos electrónicos, no planeamento de redes de comunicações viárias, na investigação operacional, entre outras. Na verdade, muitos dos problemas que se colocam nestas áreas podem ser enunciados como grafos ou redes e, portanto, resolvidos nessa base. A Teoria dos Grafos constitui, assim, uma preciosa ferramenta para formular problemas e estabelecer inter-relações estruturais e, em seguida, explorar caminhos para a resolução propriamente dita.

O primeiro livro de grafos foi publicado há cerca de 70 anos, existindo hoje, muitas publicações nesta área. As inúmeras aplicações e a complexidade de problemas, como, por exemplo, a demonstração do teorema das quatro cores, resolvido apenas computacionalmente – mas ainda não analiticamente – após cerca de um século de tentativas, estão na base da motivação do desenvolvimento da teoria dos grafos, bem como a aparente ingenuidade de alguns resultados que se podem tornar extremamente complexos.

4.1 Definição de Grafo e sua terminologia

Um Grafo $G=(V,E)$ é um par ordenado de conjuntos disjuntos que consiste:

- num conjunto finito V de vértices ou nodos;
- num conjunto finito *E* de arestas ou ligações ou arcos;

tal que a cada aresta **e** corresponde um par de vértices não ordenado escreve-se $e=\{u,v\}$ ou $\{v,u\}$ e diz-se que **e** é uma aresta entre u e v, **e** é incidente em u e em v, **e** liga os vértices u e v. Neste caso, u e v são **vértices adjacentes** e a aresta **e** que os une diz-se **incidente** em cada um dos vértices.

Num grafo, duas **arestas** dizem-se **adjacentes** se tiverem um vértice comum.

Um vértice diz-se **isolado** se não tem nenhuma aresta que lhe seja incidente.

Uma aresta que liga um vértice com ele próprio é chamada **lacete.**

Se há mais do que uma aresta unindo dois vértices de um grafo, este designa-se por **multigrafo**. As duas ou mais arestas que ligam o mesmo par de vértices no multigrafo designam-se por **arestas múltiplas**. Se existirem três arestas da **a** para **b** diz-se que a aresta tem multiplicidade três.

Um grafo que não tenha arestas múltiplas nem lacetes é denominado **grafo simples**.

A **ordem** de um grafo representa o número de vértices desse grafo, $|V|$.

A **dimensão** de um grafo representa o número de arestas, $|E|$, desse grafo.

Sendo n a ordem de um grafo e $\binom{n}{k}$ o número de combinações de n, k a k, dado como sabemos por

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$$

verifica-se que

$$0 < |E| \leq \binom{|V|}{2}$$

Designa-se por **grafo nulo** o grafo que tem dimensão nula.

Designa-se por **grafo vazio** o grafo (Ø,Ø).

O **grau de um vértice v** pertencente a V, representa-se por g(v), e corresponde ao número de arestas que incidem em v, ou ao número de vértices adjacentes a v.

Obs.: Um lacete conta duas vezes para o grau de um vértice.

Um vértice isolado tem grau zero.

Um vértice de grau 1 diz-se terminal.

Técnicas de Contagem de Número de Grafos Simples

Os grafos podem ser **etiquetados**, se os nodos são distintos (por exemplo por meio de letras) ou **não etiquetados**.

O número de grafos simples etiquetados com n nodos é dado por

$$2^{C_2^n} = 2^{\frac{n\cdot(n-1)}{2}}$$

Com efeito, entre cada par de nodos pode existir uma aresta.

Qualquer nodo pode unir-se a $n-1$ nodos e então o número de arestas é dado por

$$C_2^n = \frac{n\cdot(n-1)}{2}$$

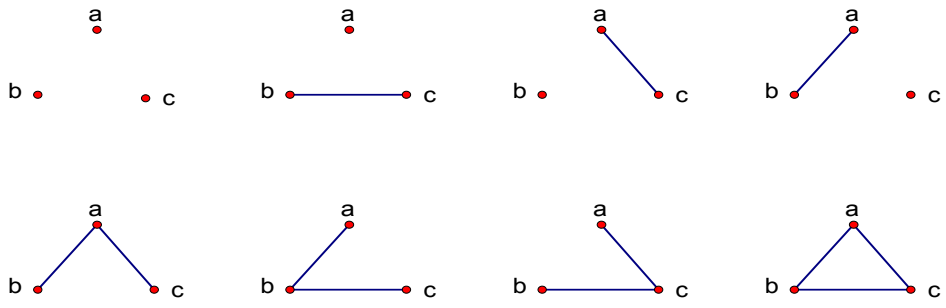
Ora os grafos simples que se podem constituir com um conjunto de $\frac{n\cdot(n-1)}{2}$ elementos (que são as arestas) são então em número de

$$2^{\frac{n\cdot(n-1)}{2}}$$

pois um conjunto com p elementos tem um total de 2^p subconjuntos diferentes (Rosen, pág 245)

Exemplo 1

a) Grafos simples com três vértices etiquetados. São $2^{\frac{3\cdot(3-1)}{2}} = 2^3 = 8$.



b) Grafos simples com três vértices (não etiquetados). São somente 4.

Um grafo é **regular** de grau *k*, quando todos os seus vértices têm o mesmo grau *k,* designando-se por *k-regular.*

Teorema: A soma dos graus dos vértices de um grafo é igual ao dobro do número de arestas, logo é sempre par, ou seja:

$$\sum_{v \in V} g(v) = 2|E| \text{ ou seja } \sum_{v \in V} g(v) \equiv 0 \pmod 2$$

A demonstração é inspirada no Lema do Aperto de Mãos que diz: Se várias pessoas apertam a mão entre si, o número total de mãos apertadas tem que ser par. Isto, porque duas mãos estão envolvidas em cada aperto. Em grafos, cada aresta contribui duas unidades para o computo geral do grau dos vértices, pois cada aresta possui dois extremos. Portanto, a soma total é par e duas vezes o número de arestas do grafo.

Em qualquer grafo, o número de vértices com grau ímpar é par.
De facto, como

$$\sum_{v \in V} g(v) = 2|E| \qquad \text{tem-se que} \qquad \sum_{v \text{ ímpar}} g(v) + \sum_{v \text{ par}} g(v) = 2|E|$$

Logo, para a soma ser par, o primeiro somatório tem que gerar um resultado par, portanto o numero de vértices de grau ímpar, é par.

É costume representar por $\delta(G)$ o menor dos graus dos nodos do grafo G por $\Delta(G)$ o maior desses graus.

Se representarmos por $\lfloor x \rfloor$ a característica de x, isto é, o maior inteiro não superior a x, a partir de

$$\sum_{v \in V} g(v) = 2|E|$$

vem

$$n \cdot \delta(G) \leq \sum_{v \in V} g(v) = 2|E|$$

e

$$\sum_{v \in V} g(v) \leq n \cdot \Delta(G)$$

logo

$$\delta(G) \leq \left\lfloor 2.\frac{|E|}{n} \right\rfloor \leq \Delta(G)$$

Será interessante referir que em qualquer grafo G de ordem $n \geq 2$ existem pelo menos dois nodos com graus iguais, como resulta da aplicação do Princípio das Casas dos Pombos (Dirichlet). Com efeito, supondo que em G todos os nodos têm graus distintos, se existir um nodo isolado (grau igual a zero) então

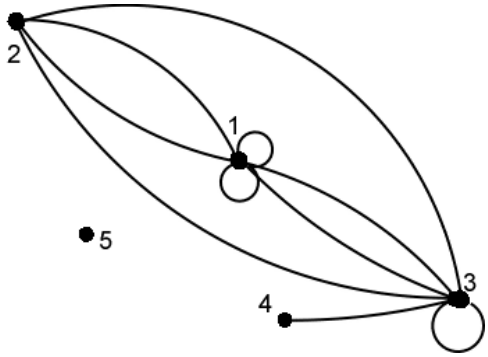
$$\Delta(G) \leq n - 2$$

quer dizer, qualquer dos restantes nodos é adjacente no máximo a $n-2$ nodos. Portanto os n nodos têm $n-1$ graus possíveis e atendendo ao princípio de Dirichlet é possível, pois existem $n-1$ graus possíveis para n nodos.

Exemplo 2

A figura ao lado representa um multigrafo.

$|V| = 5$ e $|E| = 10$



Existem três lacetes, dois em 1 e outro em 3.

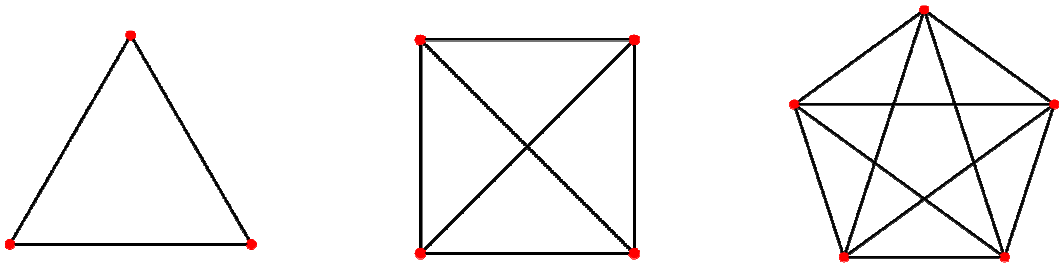
O vértice 5 diz-se isolado.

O vértice 4 diz-se terminal.

$$\sum_{v \in V} g(v) = g(1) + g(2) + g(3) + g(4) + g(5) = 8 + 4 + 7 + 1 + 0 = 20 = 2|E|$$

Um **grafo completo** é um grafo simples em que todo o vértice é adjacente a todos os outros vértices, isto é, para cada vértice do grafo, existe uma aresta conectando este vértice a cada um dos demais. O grafo completo de *n* vertices é frequentemente denotado por K_n.

O número de arestas do grafo K_n é dado por $C_2^n = \frac{n(n-1)}{2}$, correspondendo a todas as possíveis escolhas de pares de vértices.



K_3 K_4 K_5

Figura 25 – Grafos completos

Seja G um grafo simples com um conjunto de vértices V. O **complemento** de G é o grafo simples que possui V como conjunto de vértices, em que dois vértices são adjacentes no complemento se e só se, não o são em G, ou seja, se para todo o par de vértices distintos v, w pertencentes a V, tem-se que (v, w) é aresta se e só se não o for em G.

Um **caminho** α em G com origem em v_0 e fim em v_n é uma sequência alternada de vértices e arestas da forma:

$$v_0, e_1, v_1, e_2, ..., e_n, v_n$$

onde cada e_i é incidente nos vértices v_{i-1} e v_i. Num caminho não há arestas repetidas nem vértices repetidos.

O número ***n*** de arestas designa-se por **comprimento** de α. Quando não há ambiguidade, indica-se α pela sua sequência de arestas $\alpha = (e_1, e_2, ..., e_n)$ ou pela sua sequência de vértices $\alpha = (v_0, v_1, ..., v_n)$.

O caminho $\alpha = (v_0, v_1, ..., v_n)$ diz-se fechado se $v_0 = v_n$, isto é, se começa e acaba no mesmo vértice, tendo portanto um único par de vértices repetidos.

Um **percurso** é uma sequência de vértices e arestas, podendo haver repetição de arestas e vértices, ou seja, é qualquer forma de percorrer um grafo "sem levantar o lápis do papel". Se os vértices extremos da sequência coincidirem o percurso diz-se fehado.

Se num percurso *x – y* nenhuma aresta é repetida, então o percurso designa-se por **trajecto**, que se diz fechado se começa e acaba no mesmo vértice.

Designa-se por **ciclo** um caminho (que tenha pelo menos uma aresta) cujos únicos vértices coincidentes são os vértices inicial e final do percurso, ou seja, trata-se de um percurso fechado.

Designa-se por **cintura** de um grafo G, o comprimento do ciclo de menor comprimento contido em G.

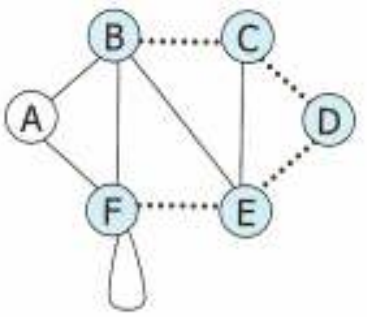
Designa-se por **circuito** um trajecto (que tenha pelo menos uma aresta) fechado, isto é, cujos vértices inicial e final coincidem. Repare-se que um circuito pode ter vértices repetidos.

Pode dizer-se que um caminho é um trajecto sem vértices repetidos.

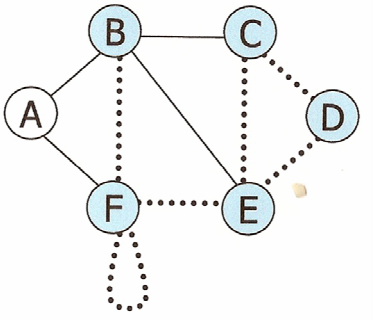
Vértice(s) repetido(s)	Aresta(s) repetida(s)	Aberto	Fechado	Designação
Não	Não	Sim		Caminho
Não	Não		Sim	Ciclo
Sim	Sim	Sim		Percurso (aberto)
Sim	Sim		Sim	Percurso (fechado)
Sim	Não	Sim		Trajecto
Sim	Não		Sim	Circuito

Exemplo 3

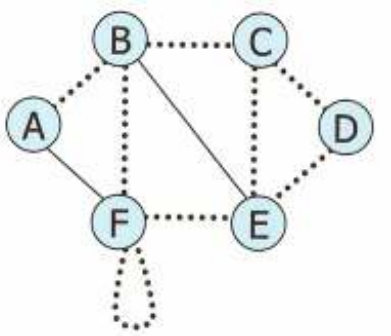
BCDEF é um **caminho** entre os vértices B e F, não há repetição de vértices nem de arestas.



BFFECDE é um **trajecto** entre os vértices B e E, em que são repetidos os vértices F e E e não há repetição de arestas.



ABCDECBFFE é um **percurso** entre os vértices A e E, em que são repetidos os vértices B, C, E e F e a aresta BC.



A **distância** $d(u,v)$ entre dois vértices de um grafo G é o comprimento do caminho mais curto entre u e v se $u \neq v$. A distância é nula se $u = v$.

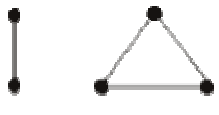
O **diâmetro** de um grafo G, representa-se por $diam(G)$ e é a distância máxima entre dois dos seus vértices.

Deve notar-se que, não sendo ainda a teoria dos grafos um "verdadeira" teoria no sentido matemático do termo, ou seja, não havendo ainda um padrão ou um consenso entre os estudiosos dos grafos, os conceitos de ciclo e de circuito são por vezes diferentes de autor para autor. Seguimos as definições que nos parecem mais correctas para uma melhor compreensão da teoria.

Claro que o número de arestas de um caminho será o **comprimento do caminho** e o número de arestas de um circuito será o **comprimento do circuito**. Se o número for par (ímpar) em qualquer um dos casos temos obviamente um comprimento par (ímpar).

Um grafo (ou multigrafo) é **conexo** se existe um caminho entre dois quaisquer dos seus vértices, caso contrário, diz-se **desconexo**. Num grafo conexo qualquer vértice está ligado por uma aresta ou por uma sequência de arestas, a qualquer um dos outros vértices.

Um grafo desconexo pode ser expresso como a união de um número finito de grafos conexos. Cada um desses grafos é designado como **componente conexa** de G. Na figura abaixo pode-se observar um exemplo de grafo desconexo.



$K_2 \cup K_3$

4.2 Representação de um grafo

Além da representação pictórica que temos vindo a apresentar, um grafo pode ser representado por matrizes, estabelecendo-se, assim, uma estreita ligação de grafos com Álgebra.

Matriz de adjacência. Seja $A = \lfloor a_{ij} \rfloor$ uma matriz mxm definida por

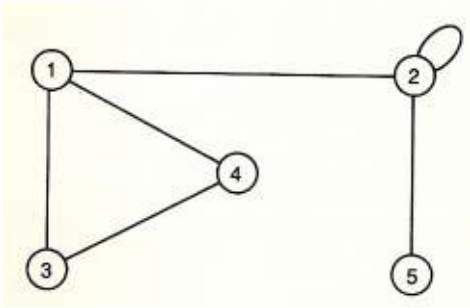
$$a_{ij} = \begin{cases} 1 & , se \quad \{v_i, v_j\} é\ uma\ aresta \\ 0 & , nos\ outros\ casos \end{cases}$$

Então A designa-se por matriz de adjacência. A matriz de adjacência de um grafo é simétrica.

Exemplo 4

Um grafo e sua matriz de adjacência.

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$



Matriz de incidência. Seja $M = \lfloor m_{ij} \rfloor$ uma matriz mxm definida por

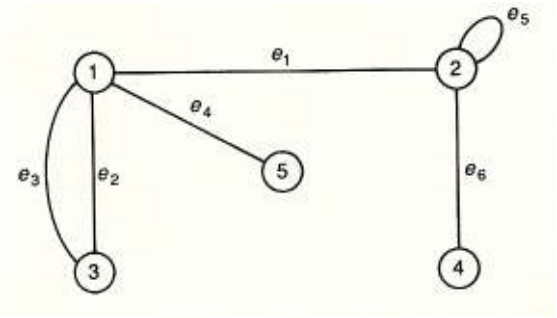
$$m_{ij} = \begin{cases} 1 & , se\ o\ vértice\ v_i\ é\ incidente\ com\ a\ aresta\ a_j \\ 0 & , nos\ outros\ casos \end{cases}$$

Então, M designa-se por matriz de incidência.

Exemplo 5

Um grafo e a sua matriz de incidência.

$$M = \begin{array}{c} \begin{matrix} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \end{matrix} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \end{array}$$



Podemos também, representar um grafo pela chamada **lista representativa associada** a G, lista que mostra cada vértice v de G seguido do conjunto de vértices adjacentes.

4.3 Grafos Orientados

Um grafo $G = (V, E)$ diz-se **orientado, dirigido** ou **digrafo** se V é um conjunto finito, não vazio de vértices e E um conjunto de pares **ordenados** de elementos de V, chamado o conjunto de arcos.

Um digrafo diz-se **simples** se não possui lacetes e os arcos são todos distintos.

Exemplo 6

V = {1, 2, 3, 4}
A = {(1,2), (2,1), (3,4), (2,3)}

Num digrafo, distingue-se o **grau de saída** de um vértice, número de arestas que saem desse vértice, do **grau de entrada**, número de arestas que são dirigidas a esse vértice. O grau de um vértice é igual à soma dos graus de saída e de entrada.

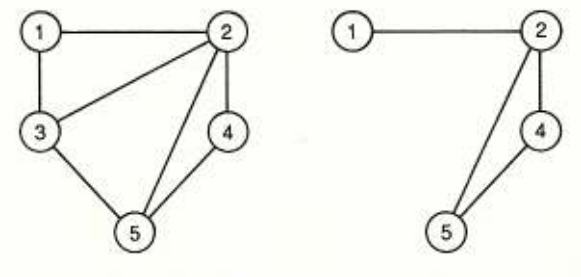
Quando nos referimos a um grafo, se nada for dito em contrário, reportamo-nos a um grafo não orientado.

4.4 Subgrafos e Isomorfismo entre grafos

O grafo $G'=(V',E')$ é um subgrafo de $G=(V,E)$ se V' é um subconjunto de V e E' é um subconjunto de E.

Se W é um subconjunto de V, o subgrafo de G induzido por W é o grafo $H=(W,Z)$ onde z é uma aresta de Z se $z=\{u,v\}$ em que $z\in E$ e $u,v\in W$.

Na figura abaixo $W=\{1,2,4,5\}$ é um subconjunto de vértices do conjunto V do grafo G e o subgrafo de G induzido por W é H.



$G=(V,E)$ $\qquad\qquad$ $\boldsymbol{H=(W,Z)}$

Dois grafos não orientados, G_1 e G_2, dizem-se **isomorfos** se existir uma correspondência f, um a um, entre os vértices de G_1 e G_2, com a propriedade de que o número de arestas unindo os vértices em G_1 é igual ao número de arestas unindo os vértices correspondentes em G_2, ou seja,

– $f:V_1\rightarrow V_2$ é uma função injectiva;

– para qualquer $a,b\in V_1,\{a,b\}\in E_1$ existe um e um só $\{f(a),f(b)\}\in E_2$.

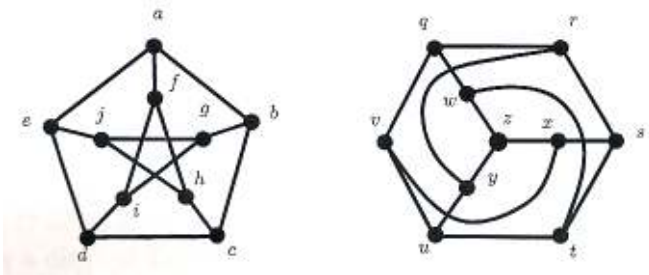


Figura 26 – Grafos isomorfos

Na figura anterior pode-se encontrar a correspondência dada por

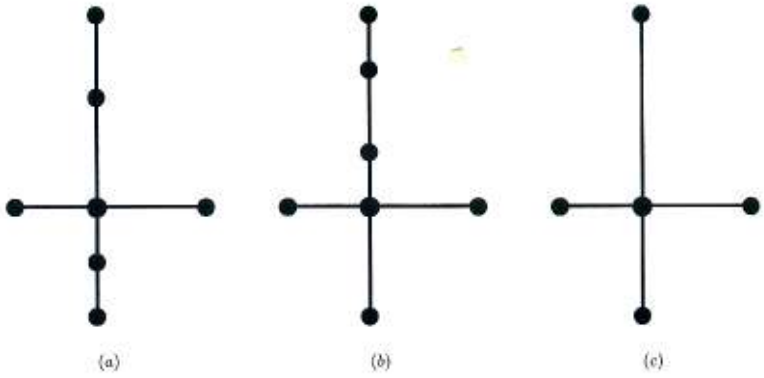
$$a \to q \quad c \to u \quad e \to r \quad g \to x \quad i \to z$$
$$b \to v \quad d \to \quad f \to w \quad h \to t \quad j \to s$$

Nem sempre é fácil verificar se dois grafos são isomorfos, principalmente se o número de vértices for elevado. Por vezes, recorre-se à ajuda de computadores para fazer tal determinação. No entanto, existem algumas condições sob as quais se torna fácil concluir que dois grafos não são isomorfos. Por exemplo, se:

- um grafo tem mais vértices do que outro;
- um grafo tem mais arestas do que outro;
- um grafo tem arestas múltiplas e o outro não;
- um grafo tem lacetes e o outro não;
- um grafo tem um vértice de grau *k* e o outro não;
- um grafo é conexo e o outro não;
- um grafo tem um ciclo e o outro não.

Dois grafos são **homeomorfos** se puderem ser obtidos a partir de um mesmo grafo por subdivisões elementares, nas quais uma única aresta x-y é substituída por duas novas arestas, x-v e v-y que se conectam a um novo vértice.

Exemplo 7



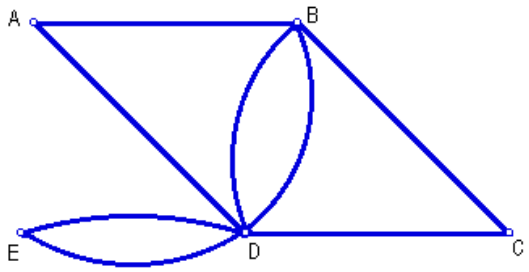
Os grafos (a) e (b) são homeomorfos porque foram obtidos de (c) por divisões elementares, adicionando vértices adequados. No entanto os grafos (a) e (b) não são isomorfos.

4.5 Trajectos e Circuitos de Euler

Seja $G=(V,E)$ um grafo não orientado ou um multigrafo sem vértices isolados. Então, diz-se que G admite um **trajecto de Euler** se G admite um trajecto que percorre todas as arestas (uma única vez), isto é, pode ser desenhado continuamente e sem repetir qualquer aresta. Se o trajecto de Euler é fechado, diz-se que G admite um **circuito de Euler**. Um grafo diz-se euleriano se admite um circuito de Euler.

Exemplo 8

O grafo da figura admite um circuito de Euler. A partir de A, podemos percorrer todas as arestas e voltar a A, sem qualquer repetição de arestas. A-B-D-E-D-C-B-D-A.



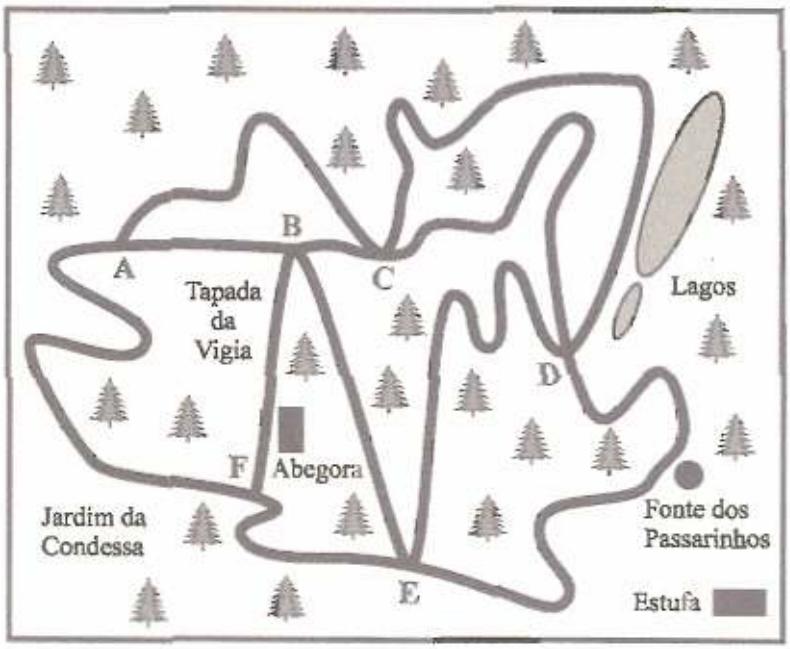
Teorema: Seja $G=(V,E)$ um grafo não orientado ou um multigrafo sem vértices isolados. Então G admite um circuito de Euler se e só se G é conexo e todos os seus vértices são de grau par.

Corolário: Seja $G=(V,E)$ um grafo não orientado ou um multigrafo sem vértices isolados. Então, é possível construir em G um trajecto de Euler se e só se G é conexo e tem exactamente dois vértices de grau ímpar. Tal trajecto terá início num dos vértices de grau ímpar e termina no outro vértice de grau ímpar.

Teorema: : Seja $G=(V,E)$ um digrafo sem vértices isolados. Então, G é um **circuito de Euler orientado** se e só se G é conexo e, para qualquer vértice, o seu grau de entrada é igual ao de saída.

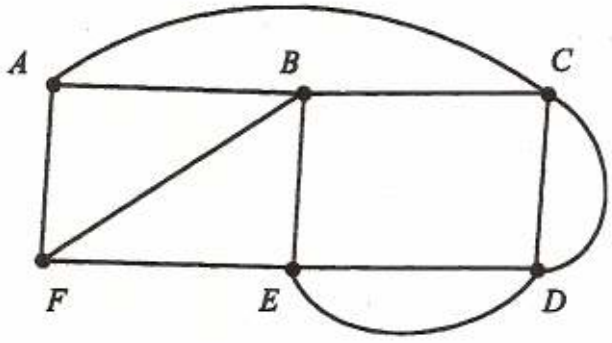
Exemplo 9

Um grupo de jovens amantes da natureza decide, numa tarde, recolher todo o lixo existente nos caminhos duma zona do Parque da Pena, em Sintra. Na figura abaixo, está um mapa dessa zona do parque.



Será possível o grupo de jovens partindo de A percorrer todos os caminhos assinalados, sem passar duas vezes pelo mesmo caminho, e regressar a A?

A situação apresentada pode ser modelada pelo seguinte grafo.



Encontrar o caminho pretendido, corresponde a verificar se o grafo admite um circuito de Euler. Ora, podemos observar que, por exemplo, o vértice A tem grau ímpar, logo concluímos que o problema é impossível.

Mas se pretendêssemos apenas percorrer todos os caminhos assinalados, apenas uma única vez, sem a obrigatoriedade de voltar ao ponto de partida a questão já tinha solução, visto que, como apenas dois vértices têm grau ímpar, é possível encontrar um trajecto de Euler. Por exemplo, ACDEDCBEFBAF.

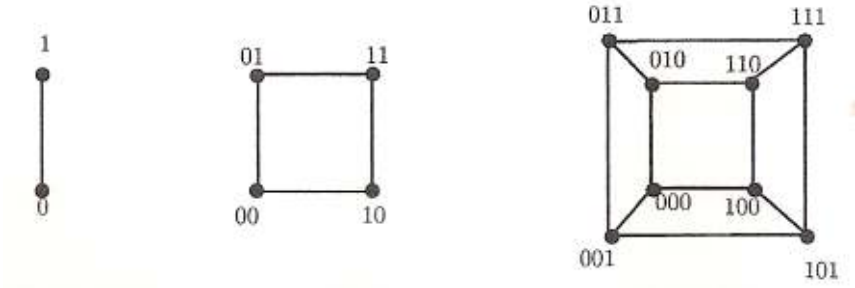
O problema do carteiro (muitas vezes designado carteiro chinês) é um dos mais conhecidos como exemplo de um circuito de Euler (admitindo que o carteiro deseja voltar ao local de onde partiu para distribuir a correspondência postal). Com efeito, se o carteiro pretender "minimizar" o seu trabalho, não deve percorrer duas (ou mais vezes) a mesma rua, mas sim uma única vez. Trata-se de seguir um circuito Euleriano.

4.6 Grafo Bipartido e Grafo Planar

O grafo $G=(V,E)$ designa-se por **bipartido** se $V=V_1\cup V_2$ onde $V_1\cap V_2=\phi$ e qualquer aresta de G é da forma $\{a,b\}$ em que $a\in V_1$ e $b\in V_2$. Se qualquer vértice de V_1 é adjacente a todos os vértices de V_2, tem-se um grafo **bipartido completo**. Nesse caso, se $|V_1|=m$, $|V_2|=n$ o grafo designa-se por $K_{m,n}$. No caso geral designa-se por $G=(V_1,V_2,E)$.

Exemplo 10

Os grafos Q_1, Q_2 e Q_3 da figura são bipartidos.



Q_1	Q_2	Q_3
$V_1=\{0\}$	$V_1=\{00,11\}$	$V_1=\{000,011,101,110\}$
$V_2=\{1\}$	$V_2=\{01,10\}$	$V_2=\{001,010,100,111\}$

Nem todos os grafos admitem uma bipartição. Mas existe uma condição necessária e suficiente para que um grafo admita uma bipartição, que é dada pelo seguinte teorema:

Teorema: Um grafo admite uma bipartição se e só se não tem circuitos de comprimento ímpar.

A demonstração é um caso de contagem especial. Com efeito:

1. Se $G=(V_1,V_2,E)$ é um grafo bipartido, é óbvio que todos os circuitos têm comprimento par, pois sendo V_1 e V_2 conjuntos disjuntos, ao unir um vértice de V_1 com um vértice de V_2 para obter um circuito, ter-se-à de voltar a V_1 na aresta seguinte, logo qualquer circuito tem comprimento par.

2. Admitindo que o grafo $G=(V,E)$ não tem circuitos de comprimento ímpar e é conexo (o que não significa qualquer perda de generalidade). Considerando um vértice arbitrário $x\in V$ e sendo $V_1=\{y\in V\}$ tais que o comprimento da aresta (x,y) é ímpar, então não existirão arestas que liguem vértices de V_1, pois então existiriam circuitos de comprimento ímpar. Ora todos os vértices do complementar de V_1 em V unidos com x dão um número par de arestas, logo não existem vértices adjacentes no complementar de V_1 em V, pois, em tais condições e por razões idênticas às anteriores, existiriam circuitos de comprimento ímpar. Portanto se V_2 for o complementar de V_1 em V, obtém-se uma bipartição de G que será $G=(V_1,V_2,E)$.

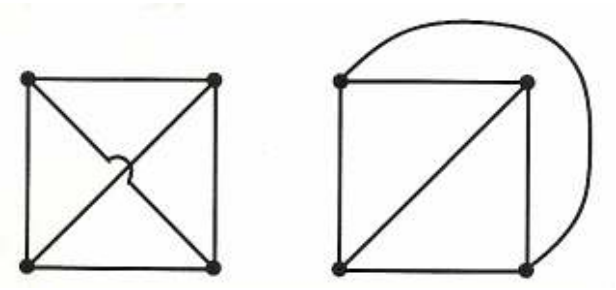
As **árvores** representam uma classe particular de grafos bipartidos. Com efeito, $G=(V,E)$ designa-se por **árvore** se for conexa e não tiver circuito. Claro que não tendo circuitos é um grafo bipartido.

Designa-se por **floresta** um grafo acíclico (ou seja, que não contém qualquer ciclo). Quer dizer uma floresta é um grafo cujas componentes são árvores.

Um grafo (ou multigrafo) G chama-se **planar** se G puder ser representado no plano ou na superfície esférica de forma a que as arestas só se intersectem nos vértices de G.

Exemplo 11

As representações seguintes mostram que K_4 é planar.



Nem todos os grafos são planares.

$K_{3,3}$ e K_5 não admitem representações planares.

Repare-se que, para o mesmo grafo, podem existir representações em que as arestas se cruzem e outras em que não se cruzem. Por isso, não podemos dizer que um grafo não é planar só porque numa determinada representação as arestas se cruzam.

De um modo geral, não é fácil decidir se um grafo é planar. Os teoremas sobre grafos planares dão-nos condições que ajudam a descobrir se um grafo não é planar, mas não nos permitem afirmar se é planar.

Leonhard Euler percebeu que um grafo simples, planar (desenhado na sua forma planar) e conexo divide o plano em um certo número de regiões, incluindo regiões totalmente fechadas e a região infinita exterior. Euler estabeleceu uma relação entre o número de arestas, o número de vértices e o número de regiões.

Teorema Fórmula de Euler: Se G é um grafo simples, planar e conexo com ***v*** vérices, ***e*** arestas e ***r*** regiões, então

$$\boldsymbol{v - e + r = 2}$$

Demonstração por indução:

Suponhamos que o grafo conexo G consiste num único vértice. Então tem-se:

$$v = 1 \qquad e = 0 \qquad r = 1$$

verificando a fórmula de Euler.

Suponhamos, agora, que a fórmula é válida para qualquer grafo conexo, planar e simples, com *k* arestas, e consideremos o grafo com *k+1* arestas. Relacionemos o grafo de *k+1* arestas com o de k arestas. Podemos considerar dois casos:

1) O grafo tem um vértice de grau 1 como o da figura ao lado. Eliminando esse vértice e a aresta obtemos um grafo com um numero *v* de vértices e um número *r* de regiões, para os quais

$v - e + r = 2$

No grafo original, antes de eliminar o vértice e a aresta temos

$(v+1)-(e+1)+r = v+1-e-1+r = v-e+r = 2$ por hipótese.

2) O grafo não tem vértices de grau 1, como o da figura ao lado. Retiramos então uma aresta que define uma região fechada. Obtém-se um grafo planar simples com *k* arestas, um número *v* de vértices e *r* regiões, para os quais

$v - e + r = 2$

No grafo original, antes de eliminar a aresta temos

$v-(e+1)+(r+1) = v-e-1+r+1 = v-e+r = 2$ por hipótese.

Assim, está demonstrado o teorema.

1º Corolário: Seja $G = (V, E)$ um grafo conexo, simples e planar com v vértices, $e > 2$ arestas e r regiões, então $\mathbf{3r \le 2e}$ e $\mathbf{e \le 3v - 6}$.

Exemplo 12

O grafo K_5 é simples e conexo com dez arestas e cinco vértices. Logo, $3v-6=3\times5-6=9<10=e$. Consequentemente, pelo corolário, concluímos que K_5 não é planar.

Exemplo 13

O grafo $K_{3,3}$ é simples e conexo com nove arestas e seis vértices. Tem-se $3v-6=3\times6-6=12\geq9=e$. Seria um erro concluir que este grafo é planar. Significa que a condição dada pelo corolário é necessária mas não é suficiente para concluir a planaridade de um grafo.

Se $G=(V,E)$ for um grafo conexo, simples com $e>2$, então se $e>3v-6$, segue-se que G não é planar. No entanto se $e\leq3v-6$ não se pode concluir que G é planar, isto é, o recíproco do corolário é falso.

2º Corolário: Seja $G=(V,E)$ um grafo conexo, simples e planar com E arestas e V vértices (sendo $V\geq3$) e sem circuitos de comprimento 3.
Então

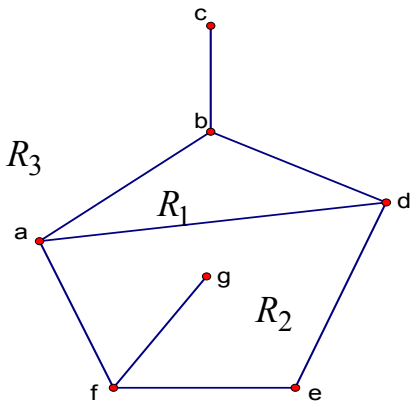
$$|E|\leq2|V|-4 \quad \text{ou} \quad e\leq2v-4$$

A demonstração é análoga à do 1º corolário, excepto que é necessário definir o que se entende por grau de uma região.

Grau de uma região é o número de arestas que constituem a fronteira dessa região.

Se uma aresta está “envolvida” pela região ela contribui com o valor 2 para o grau da região.

Exemplo 14



A aresta (b,c) contribui com valor 2 (por convenção) pois está envolvida (rodeada) por pontos da região R_3.

A aresta (f,g) está nas mesmas condições em relação à região R_2.

Se considerarmos **multigrafos** (com arestas múltiplas), elas dariam origem a regiões de grau 2. Se considerarmos lacetes haverá regiões de grau 1.

Verifica-se facilmente que:

A soma dos graus das regiões é igual a duas vezes o número de arestas do grafo, se este for simples, planar e conexo.

$$\sum_{\textit{todas as regiões}} \textit{graus das regiões} = 2 \cdot |E| = 2e$$

Agora podemos demonstrar o 2º Corolário da Fórmula de Euler pois temos

$$\sum_{todas\ as\ regiões} graus\ das\ regiões = 2e \geq 4r$$

pois não havendo circuitos de comprimento 3, o grau de qualquer região do grafo tem de ser pelo menos 4.

Logo

$$\frac{1}{2} e \geq r$$

usando a fórmula de Euler vem

$$\frac{1}{2} e \geq e - v + 2$$

logo

$$e \leq 2v - 4$$

Usando este **2º corolário**, podemos mostrar que o grafo $K_{3,3}$ é **não planar.**

Como $K_{3,3}$ não tem circuitos de comprimento 3, pois é um grafo bipartido, podemos usar o 2º corolário de Euler e vem

$$v = 6$$

como temos $9 \leq 2 \cdot 6 - 4$ ou seja $9 \leq 8$

$$e = 9$$

logo $K_{3,3}$ **não é planar**.

Um dos resultados mais utilizado para decidir se um grafo é, ou não, planar é o teorema de Kuratowski.

Teorema de Kuratowski: Um grafo é não planar se e só se contém um subgrafo homeomorfo a K_5 ou $K_{3,3}$.

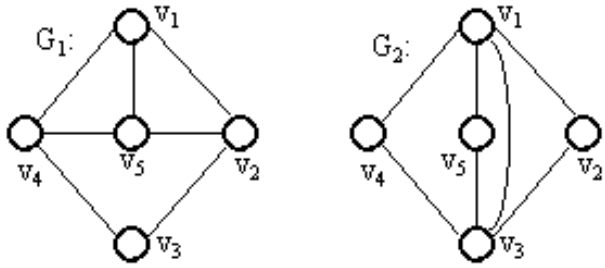
Este teorema foi apresentado pelo matemático polaco Kuratowski em 1930. A sua demonstração é bastante longa e complexa. É óbvio que um grafo contendo um subgrafo homeomorfo a K_5 ou $K_{3,3}$ é não planar. A demonstração do recíproco é que é muito trabalhosa (Harady, pág 109). Apesar de apresentar uma condição necessária e suficiente para a planaridade de um grafo que não é dependente da sua representação pictórica, na prática o teorema não tem aplicação. Não existe nenhum algoritmo eficiente nele baseado que permita testar a planaridade/não planaridade de um grafo. Na verdade, testar todos os subgrafos e verificar se são homeomorfos a K_5 ou a $K_{3,3}$ não é tarefa exequível em tempo útil.

4.7 Caminhos e Ciclos Halmiltonianos

Um **caminho hamiltoniano** é um caminho que permite passar por todos os vértices de um grafo G, não repetindo nenhum. Caso com esse caminho, seja possível descrever um ciclo, este é denominado **ciclo hamiltoniano** em G. Um grafo que possua tal ciclo é chamado de **grafo hamiltoniano**.

Exemplo 15

Considere os grafos G_1 e G_2 ao lado. É fácil notar que G_1 contém o ciclo (v_1, v_2, v_3, v_4, v_5, v_1) que é hamiltoniano. Logo, G_1 é um grafo hamiltoniano. O mesmo não acontece com G_2.



O adjectivo “hamiltoniano” é usado em honra ao matemático Sir William Hamilton (1805-1865) que investigou a existência de uma solução para um jogo chamado “À Volta do Mundo” no qual, é pedido ao jogador que encontre uma rota ao longo das arestas de um dodecaedro visitando cada vértice, representando uma cidade, exactamente uma vez e regresse ao ponto de partida. Agora, o dodecaedro pode ser representado como um grafo G no plano. Assim, o jogo tem solução se e somente se G é um grafo Hamiltoniano.

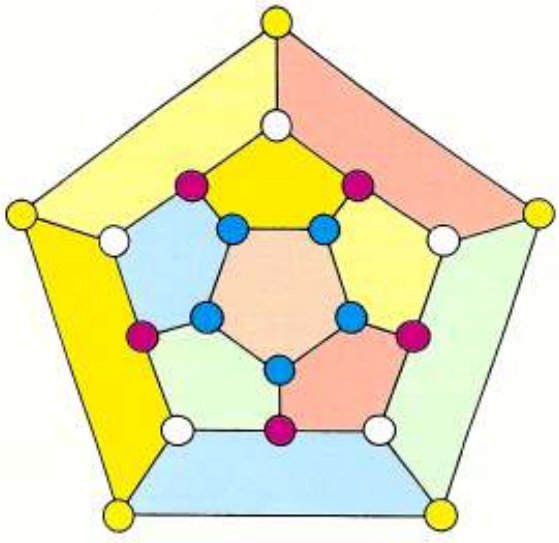


Figura 27 – Grafo Hamiltoniano

O conhecido problema do "Caixeiro Viajante", que consiste em encontrar uma rota que permita visitar várias cidades, passando por cada cidade exactamente uma vez e retornar à cidade de origem, pode ser modelado por um grafo $G=(V,E)$, onde V representa o conjunto das cidades a visitar e E as ligações, estradas entre duas cidades, sem passar por outra cidade. A solução do problema reduz-se a verificar se o grafo é hamiltoniano.

Não se conhece, ainda, uma boa caracterização dos grafos hamiltonianos, isto é, não foi encontrada uma condição necessária e suficiente para determinar se um grafo contém um ciclo de Hamilton. Há diversas famílias de grafos para os quais existe um ciclo hamiltoniano (um exemplo trivial é um grafo completo, em que cada vértice é ligado a todos os outros). É muito fácil convencer alguém da existência de um ciclo hamiltoniano num grafo: basta exibir tal caminho. No entanto, é difícil, em geral, convencer alguém da não-existência de um tal ciclo. Não existe um algoritmo eficiente para determinar, no caso geral, se um grafo é hamiltoniano.

Além do método de tentativa e erro podemos considerar algumas observações úteis.

1. Se G tem um ciclo hamiltoniano, então para todo o vértice $v \in V$, $g(v) \geq 2$.
2. Se $v \in V$ e $g(v) = 2$, então as duas arestas incidentes no vértice v devem aparecer em qualquer ciclo de Hamilton de G.
3. Se $v \in V$ e $g(v) > 2$, então se tentarmos construir um ciclo de Hamilton após passar por esse vértice, as arestas não utilizadas incidentes com o referido vértice devem ser apagadas.
4. Na construção do ciclo de Hamilton para G, não podemos obter um ciclo de Hamilton para um subgrafo de G a não ser que este contenha todos os vértices de G.

Os resultados que se seguem são condições suficientes mas não necessárias para a existência de ciclos de Hamilton.

Teorema (Teorema de Ore 1961): Se $G=(V,E)$ é um grafo conexo e simples com número de vértices *n* superior ou igual a 3, e se $g(x)+g(y)\geq n$ para cada par de vértices não adjacentes $x,y\in V$,então G contém um ciclo de Hamilton.

Corolário (Teorema de Dirac 1952): Se $G=(V,E)$ é um grafo conexo e simples com número de vértices superior ou igual a 3, tal que $g(v)\geq\frac{n}{2}$ para todo o vértice $v\in V$, então G é hamiltoniano.

Esta condição é suficiente para garantir que um grafo **G** seja hamiltoniano, mas não é necessária. Por exemplo, no grafo da figura abaixo, o grau de cada vértice é 2, menor que $\frac{6}{2}=3$, ou seja, não verifica o corolário anterior e, no entanto, é um grafo hamiltoniano. De facto, podemos indicar o seguinte ciclo de Hamilton: A B C D E F A

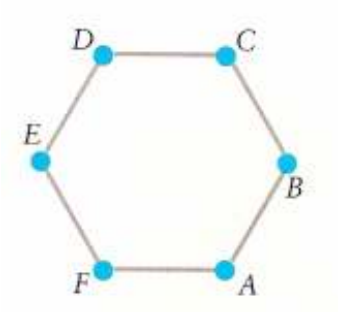


Figura 28 – Grafo

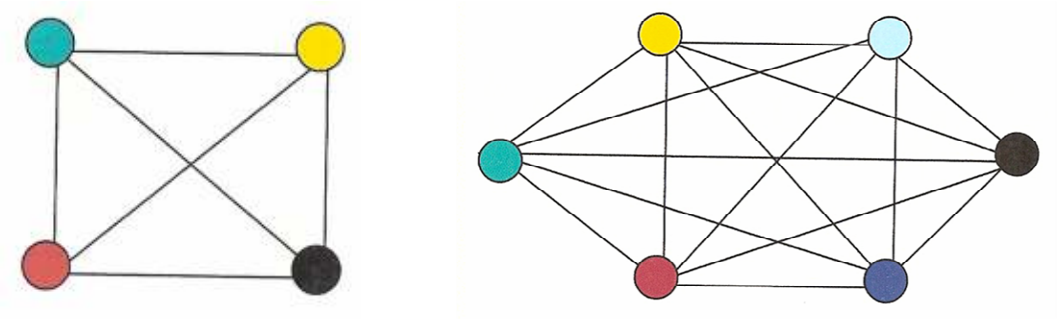
4.8 Coloração de Grafos

A coloração de um grafo é uma atribuição de cores aos vértices, de modo a que vértices adjacentes tenham cores diferentes. Um grafo é **n- colorável** se pode ser pintado com **n** cores.

O **número cromático** de um grafo representa o menor número de cores necessárias para colorir os seus vértices de forma a que vértices adjacentes não tenham a mesma cor e representa-se por $\chi(G)$.

Exemplo 16

Para colorir um grafo completo de 4 vértices (K_4) são necessárias 4 cores e para colorir um grafo completo (K_6) são precisas 6 cores.



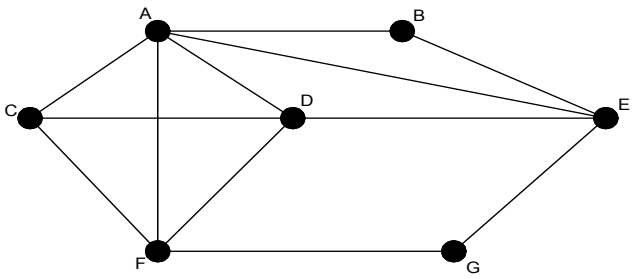
Generalizando, o número cromático de um grafo completo de n vértices é igual ao número de vértices, isto é, $\chi(K_n)=n$.

Algoritmo Welch-Powell para coloração de um grafo.

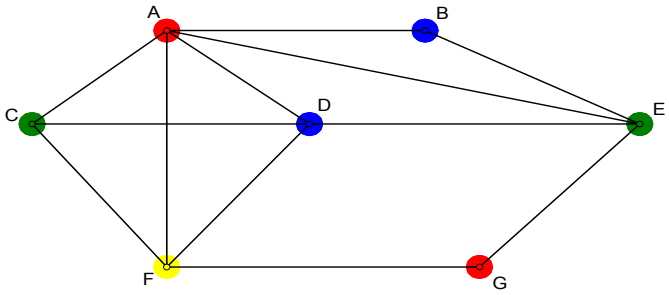
1. Ordene os vértices de G por ordem decrescente de grau. Tal ordem pode não ser única, dado que alguns vértices podem ter o mesmo grau.
2. Use uma cor para pintar o primeiro vértice e para pintar, numa ordem sequencial, cada vértice da lista que não é adjacente ao primeiro.
3. Volte ao início da lista e repita o processo pintando, noutra cor, o vértice não colorido anteriormente.
4. Continue o processo com outras cores, até todos os vértices estarem pintados.

Exemplo 17

Utilizemos o algoritmo Welch-Powell para colorir o grafo G da figura.



O vértice de G, de maior grau (5) é **A**. Atribuímos a esse vértice a cor, por exemplo, vermelha. Ao vértice **G**, não adjacente a **A**, atribuímos, também, a cor vermelha. De seguida, atribuímos a cor, por exemplo, azul, ao vértice **D** e ao vértice não adjacente **B**. Repetimos este processo até todos os vértices estarem coloridos.



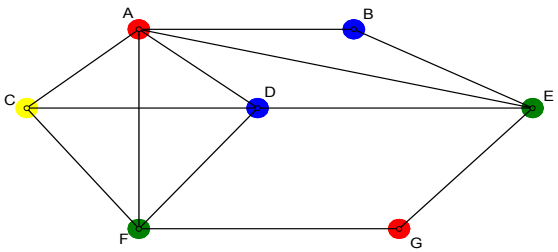
Resumindo,

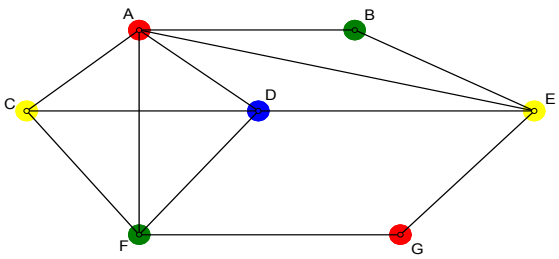
Vértice	A	B	C	D	E	F	G
Grau	5	2	3	4	4	4	2
Cor	vermelha	azul	verde	azul	verde	amarela	vermelha

Os vértices A, C, D e F estão ligados uns aos outros, logo necessitam de ser pintados de cores diferentes. São necessárias quatro cores para colorir o grafo. Significa que o número cromático deste grafo é quatro, ou seja, $\chi(G)=4$

Este algoritmo pode conduzir a mais do que um resultado e nessa medida, pode considerar-se não eficiente.

Vejamos, neste exemplo, outras formas de colorir o mesmo grafo.





Teorema: Num grafo G, as afirmações seguintes são equivalentes:

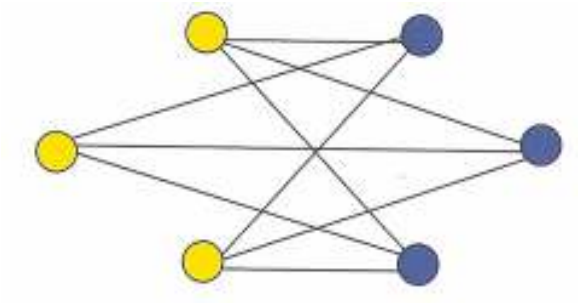
a) G é 2-colorável.

b) G é bipartido.

c) cada ciclo de G tem o mesmo o comprimento.

Exemplo 18

No grafo bipartido da figura ao lado (V_1 constituído pelos vértices de cor amarela e V_2 constituído pelos vértices de cor azul), o número cromático é dois, como sucede em qualquer grafo bipartido.



Exemplo 19

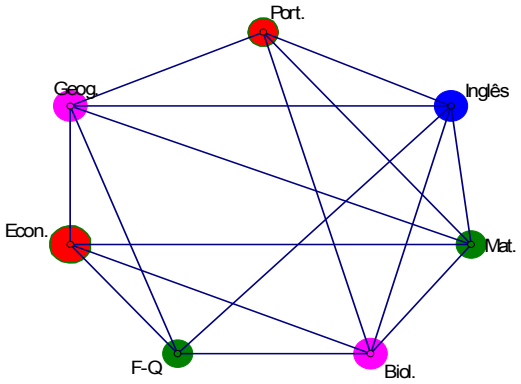
Suponhamos que é necessário elaborar um calendário de exames de sete disciplinas de um curso de forma a que não haja um aluno com duas disciplinas com exame ao mesmo tempo.

A tabela seguinte mostra a existência de disciplinas com alunos comuns, assinalados com X.

	Port.	Inglês	Mat.	Biol.	F.-Q.	Econ.	Geog.
Port.	—	X	X	X	—	—	X
Inglês		—	X	X	X	—	X
Mat.			—	X		X	X
Biol.				—	X	X	
F.-Q.					—	X	X
Econ.						—	X
Geog.							—

Este problema pode ser resolvido por coloração de vértices de um grafo. Os vértices representam as disciplinas e existe uma aresta entre dois vértices se essas disciplinas têm um aluno em comum.

Temos então,



Assim ,concluímos que são necessários quatro horários diferentes:

Horário 1: Português e Economia.

Horário 2: Inglês.

Horário 3: Matemática e Físico-Química.

Horário 4: Biologia e Geografia.

Facilmente se percebe que a solução não é única, uma vez que, por exemplo, podia começar por atribuir a mesma cor às disciplinas de Inglês e Economia.

Dual de um grafo G^d: Dado um grafo G, em cada região definida pelo grafo, incluindo a região infinita, coloca-se no seu interior um vértice do dual e, por cada aresta de G partilhada por duas regiões, desenha-se uma aresta do dual que liga os vértices colocados no interior dessas regiões.

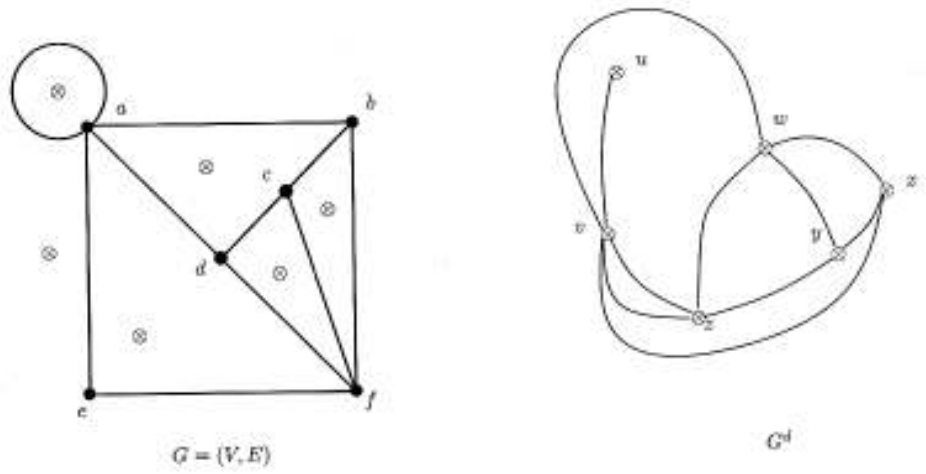


Figura 29 – Grafo e Dual

O exemplo anterior é um exemplo típico que faz parte das possíveis aplicações da teoria da coloração e planaridade dos grafos. Entre os domínios em que esta teoria tem grande interesse podemos citar a Investigação Operacional, a construção de Circuitos Impressos, a Teoria da Informação, e claro, além da própria Teoria dos Grafos (como no caso da "Extremal Graph Theory" iniciada por Paul Erdös com o seu artigo "On the Grph Theorem of Turán" de 1970), as Técnicas Avançadas da Contagem em Grafos tais como:

1. Várias contagens em Digrafos como por exemplo o número de digrafos transitivos.
2. O número de grafos Hamiltonianos.
O número de Trajectos Eulerianos.
3. O número de grafos *k*-coloráveis.
O número de grafos *k*-coloráveis planares.
4. O número de grafos simétricos.
O número de subgrafos pares em vários contextos.
5. O número de quadrados latinos
O número de grafos lineares.

Harary enumera (pág. 193) diversos problemas não resolvidos de contagens não conseguidas em grafos e que poderão constituir possíveis trabalhos a efectuar.

4.9 Coloração de mapas e Teorema das Quatro cores

Considere-se o seguinte problema: Quantas cores são necessárias para colorir um mapa qualquer de modo a que dois países vizinhos não tenham a mesma cor? Por países vizinhos entendem-se aqueles que têm uma fronteira geográfica comum. Mas, se dois países se encontram somente num ponto podem ter a mesma cor.

Este problema foi formulado em 1852 por Francis Guthrie, que acreditava que com quatro cores era possível colorir qualquer mapa no plano. Francis Guthrie, que foi advogado, botânico e, sobretudo, matemático, tinha um irmão

mais novo, Frederick Guthrie, que era aluno de Augustus De Morgan. A questão intrigou De Morgan, tendo sido sobretudo através deste matemático que a comunidade científica tomou conhecimento da "Conjectura das Quatro Cores". Mas foi apenas em 1878 que o matemático Cayley o apresentou formalmente na London Mathematical Society. Um ano depois, Alfred Bray Kempe publicou uma demonstração completa do "Teorema das Quatro Cores" no *American Journal of Mathematics*. A demonstração de Kempe foi estudada por vários matemáticos de renome. Portanto, em 1879, considerava-se definitivamente estabelecido o "Teorema das Quatro Cores". Mas, em 1890, Percy John Heawood provou que a demonstração de Kempe tinha um erro. No mesmo artigo, Heawood lamentava não ter sido capaz de obter nenhuma demonstração alternativa do teorema. Conseguiu, no entanto, dar mais um passo positivo tendo, nomeadamente, provado o Teorema das Cinco Cores: demonstrou que não são necessárias mais do que cinco cores para colorir um mapa plano, onde países de fronteira comum têm cores diferentes.

A Conjectura das Quatro Cores, impulsionou o desenvolvimento da Teoria de Grafos uma vez que, todo o mapa pode ser identificado com um grafo.

Finalmente em, 1976 o "Teorema das Quatro Cores" foi provado por Wolfgang Haken e Kenneth Appel. Quando a notícia do feito se espalhou pelos vários departamentos de matemática, houve um enorme entusiasmo, tendo muitos professores interrompido as aulas para comemorar. Mas a euforia esfriou em muitos deles quando souberam que essa demonstração incluía mais de mil horas do uso de computadores de alta velocidade. O que Appel e Haken fizeram, foi demonstrar que todos os mapas possíveis eram variações de mais de 1500 casos fundamentais, cada um dos quais foi então possível pintar por computador, com um máximo de quatro cores. A prova era demasiado longa para ser verificada à mão e havia sempre a possibilidade de os computadores terem cometido algum erro de difícil detecção. Hoje em dia, a validade da demonstração é aceite na generalidade da comunidade matemática, mas muitos consideram-na insatisfatória. Está em causa reconhecer uma argumentação baseada numa enorme quantidade de cálculos por computador, os quais é impossível verificar detalhadamente por um ser humano, mesmo que gaste nisso todo o tempo da sua vida.

"Não sou especialista no problema das quatro cores, mas admito que a demonstração seja verdadeira. No entanto, não é bela. Preferia ver uma demonstração que permitisse discernir porque são suficientes quatro cores".

Erdös

Até hoje, não se conhece uma demonstração do "Teorema das Quatro Cores", sem o auxílio de computadores.

5. Fórmulas de Contagem de Burnside / Pólya

Considere-se o problema de contagem do número de tabuleiros de xadrez com 2x2 casas, brancas e pretas. Na figura seguinte pode-se observar $2^4 = 16$ tabuleiros diferentes.

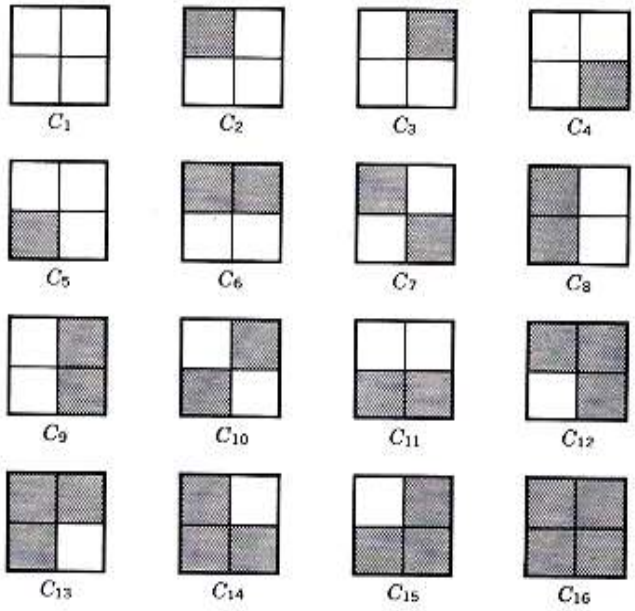


Figura 30 – Tabuleiros de xadrez 2x2

Considerando que os lados dos tabuleiros não estão marcados, então dois tabuleiros são considerados "equivalentes" se um deles pode ser obtido a partir do outro por rotação. Assim, são considerados equivalentes:

– C_2, C_3, C_4, C_5

– C_6, C_8, C_9, C_{11}

– C_7, C_{10}

– C_{12}, C_{13}, C_{14}, C_{15}

Restam, então, 6 que não são equivalentes.

Suponha-se, agora, que não vão ser consideradas as diferenças baseadas na cor, preto e branco, somente o padrão de contraste dos tabuleiros. Assim, o tabuleiro todo branco e o tabuleiro todo preto têm o mesmo padrão de contraste. O mesmo acontece aos tabuleiros C_2 e C_{15}. Temos, então, apenas 4 padrões de contraste não equivalentes.

A teoria de enumeração de Pólya de 1938, permite determinar o número de objectos não equivalentes, isto é, o número de configurações diferentes.

Algumas noções têm de ser referidas para compreender o Teorema de Pólya, de grande importância em Combinatória.

5.1 Grupos de Permutações e Polinómios de índice cíclicos

Uma permutação sobre um conjunto S é uma aplicação one-to-one (injectiva) de S em si próprio. Os elementos de S chamam-se objectos.

Se $S = \{a, b, c, d\}$, então representa-se por

$$\begin{pmatrix} a & b & c & d \\ b & d & c & a \end{pmatrix}$$

a permutação que leva *a* em *b, b* em *d, c* em *c*, e *d* em *a*.

Uma permutação $\pi : S \to S$ é um ciclo de dimensão n (permutação cíclica) se existir um subconjunto de S de dimensão n $(a_1, a_2, ..., a_n)$ tal que cada objecto a_j é aplicado por π no objecto seguinte do ciclo e todo o objecto de S que não pertença ao ciclo é fixado por π, isto é, aplicado em si próprio.

A forma tabular de uma permutação π num conjunto finito S é uma matriz com duas linhas. Na primeira linha listam-se os objectos de S uma só vez. Por baixo do objecto a fica a sua imagem $\pi(a)$ na forma

$$\begin{pmatrix} a_1 & a_2 & ... & a_n \\ \pi(a_1), & \pi(a_2), & ..., & \pi(a_n) \end{pmatrix}$$

Por exemplo, na permutação, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$ temos os ciclos $\begin{pmatrix} 1 & 2 & 5 \\ 2 & 5 & 1 \end{pmatrix}$ e $\begin{pmatrix} 3 & 4 \\ 4 & 3 \end{pmatrix}$ de dimensões três e dois, respectivamente. Pode-se utilizar uma forma mais simples para representar os dois ciclos, mantendo a ordem dos elementos indicada pelo ciclo. Neste caso tem-se $(1 \quad 2 \quad 5)(3 \quad 4)$.

A decomposição de ciclo (forma) de uma permutação π é uma concatenação de permutações de ciclo cujas subcolecções (subconjuntos) de objectos são disjuntas e cujo produto é π.

Os ciclos de grau 1, 2, 3,… designam-se por ciclos unitários, binários (ou biciclos), ternários (ou triciclos), etc. Algumas vezes os ciclos unitários são explicitamente escritos e outras vezes são omitidos. De uma maneira geral, um ciclo de grau maior que 1, designa-se por policiclo. O ciclo de grau *n,* sendo *n* o número de elementos de S, designa-se por ciclo pleno, que é a própria permutação; neste caso diz-se que a permutação é cíclica. Por exemplo, para S={1, 2, 3, 4, 5} a permutação (1 5) (2 3) (4) tem dois biciclos e um ciclo unitário; e a permutação (2 5 3 4 1) é um ciclo pleno, a permutação é cíclica.

Um conjunto P de permutações de um conjunto S é **fechado** em relação à composição, se a composição de cada par de permutações em P está também em P.

Um conjunto P de permutações de um conjunto S é fechado em relação a inversão se, para cada permutação $\pi \in P$ se tem $\pi^{-1} \in P$.

Um **grupo permutação** $G = (P, S)$ é um conjunto P não vazio de permutações num conjunto S tal que P é fechado sob composição e inversão.

Note-se que:

1. Cada permutação tem uma forma tabular.
2. A forma tabular é única até à ordem em que os objectos do conjunto permutado são listados na primeira linha.
3. Cada permutação tem uma decomposição cíclica.
4. A decomposição cíclica de uma permutação num produto de permutações cíclicas disjuntas é única até à ordem dos factores.
5. A colecção de todas as permutações de um conjunto S forma um grupo permutação.

A estrutura de ciclo de uma permutação π é uma expressão (polinómio multivariado) da forma $x_1^{m_1} x_2^{m_2} \ldots x_k^{m_k}$, onde m_j é o número de ciclos de dimensão j na decomposição cíclica de π.

O índice do ciclo de um grupo de permutações G é o polinómio multivariado que é a soma de estruturas de ciclo de todas as permutações em G. Escreve-se

$$P_G(x_1, x_2, ..., x_n)$$

sendo P_G uma notação em honra de George Pólya (1887 – 1985).

Exemplo 1

O grupo simétrico (grupo de todas as permutações sobre $\{1, 2, ..., n\}$ sob a operação de composição) $\sum_3$ de todas as 6 possíveis permutações de $\{a, b, c\}$ tem os elementos seguintes:

$$(a)(b)(c) \quad , \quad (ab)(c) \quad , \quad (ac)(b) \quad , \quad (a)(bc) \quad , \quad (a\,b\,c) \quad , \quad (a\,c\,b)$$

com as respectivas estruturas de ciclo

$$x_1^3 \quad , \quad x_1x_2 \quad , \quad x_1x_2 \quad , \quad x_1x_2 \quad , \quad x_3 \quad , \quad x_3$$

Então o polinómio de índice cíclico é

$$P_{\sum_3} = \frac{1}{6}\left(x_1^3 + 3x_1x_2 + 2x_3\right)$$

Exemplo 2

O grupo $\sum_4$ de todas as 24 permutações de $\{a, b, c, d\}$ tem os seguintes elementos

$(a)(b)(c)(d)$	$(ab)(c)(d)$	$(ac)(b)(d)$	$(ad)(b)(c)$
$(a)(bc)(d)$	$(a)(bd)(c)$	$(a)(b)(cd)$	$(abc)(d)$
$(acb)(d)$	$(abd)(c)$	$(adb)(c)$	$(acd)(b)$
$(adc)(b)$	$(a)(bcd)$	$(a)(bdc)$	$(ab)(cd)$
$(ac)(bd)$	$(ad)(bc)$	$(abcd)$	$(abdc)$
$(acbd)$	$(acdb)$	$(adbc)$	$(adcb)$

Tabela 10 – Permutações de 4 elementos

O polinómio de índice cíclico é

$$P_{\Sigma_4} = \frac{1}{24}\left(x_1^4 + 6x_1x_1x_2 + 8x_1x_3 + 3x_2x_2 + 6x_4\right) =$$
$$= \frac{1}{24}\left(x_1^4 + 6x_1^2x_2 + 8x_1x_3 + 3x_2^2 + 6x_4\right)$$

5.2 Classes de equivalência sob um grupo de permutação e Teorema de Burnside

Seja $G = (P, S)$ um grupo de permutação. Uma relação binária, R, em S é uma relação binária induzida por G, se

$$a\ R\ b \Leftrightarrow \text{existe } \pi \in P \text{ tal que } \pi(a) = b \quad a, b \in S$$

Ou seja, um elemento $a \in S$ está relacionado com um elemento $b \in S$, se e só se existe uma permutação π em G que transforma a em b.

Qualquer relação binária num conjunto, induzida por um grupo de permutação do conjunto, é uma relação de equivalência.

Dado $G = (P, S)$ um grupo de permutação, como determinar o número de classes de equivalência? Quando S tem poucos elementos, a contagem pode ser feita determinando a relação de equivalência e contando as classes de equivalência. No entanto, esse processo torna-se inviável quando o número de elementos de S é elevado. Nestes casos, usamos o Teorema de Burnside que determina o número de classes de equivalência pela contagem do número de elementos que são fixos (ou invariantes) sob a permutação do grupo

Um elemento de um conjunto S diz-se **fixo** sob uma permutação sobre *S*, se a permutação levar este elemento nele próprio, $\pi(a) = a$. O conjunto de todos os pontos fixos de π é designado por $fix(\pi)$. Obviamente, que o número de pontos fixos de uma permutação π é igual ao número de ciclos unitários na decomposição de ciclo.

No problema do tabuleiro de xadrez 2x2, referido no início deste capítulo, considerem-se as permutações $\pi_1, \pi_2, \pi_3, \pi_4$ dos tabuleiros que correspondem

às rotações horárias de 90º, 180º, 270º, 0º. $G = \{\pi_1, \pi_2, \pi_3, \pi_4\}$ é um grupo de permutações sobre o conjunto dos tabuleiros. Na relação de equivalência induzida por G temos, por exemplo, que o tabuleiro C_3, cuja primeira casa é preta, está relacionado com os outros tabuleiros que também possuem uma só casa preta, por uma das permutações $\pi_1, \pi_2, \pi_3, \pi_4$. Logo, estes tabuleiros pertencem todos à mesma classe de equivalência, pois são indistinguíveis por rotações. De modo análogo, se podem analisar as outras classes de equivalência. Conclui-se que existem 6 classes de equivalência induzidas por G.

Teorema de Burnside: O número de classes de equivalência nas quais um conjunto S é dividido pela relação de equivalência induzida por um grupo de permutação sobre S é dado por

$$\frac{1}{|G|}\sum_{\pi \in G} |fix(\pi)|$$

onde $|G|$ representa o número de elementos de G e $|fix(\pi)|$ o número de elementos que são fixos sob a permutação π.

O cálculo da soma no Teorema de Burnside fica simplificado se se usar o polinómio de índice de ciclo e pelo facto de o número de pontos fixos de uma permutação π ser igual ao número de ciclos unitários na decomposição de ciclo. Para cada termo do polinómio deve-se multiplicar o coeficiente pelo expoente de x_1 e somar depois estes produtos.

Nota: Este Teorema que é atribuído a William Burnside (1852-1927) já tinha sido formulado por Georg Frobenius (1848-1917).

Exemplo 3

Qual o número de fiadas diferentes de duas contas que se podem fazer com contas azuis e vermelhas?

Temos as seguintes fiadas

vv av va aa

Figura 31 – Fiadas de duas contas, azuis e vermelhas

Suponhamos que as extremidades de uma fiada não sejam diferenciadas, então duas fiadas são consideradas indistinguíveis se uma delas pode ser obtida a partir da outra por troca das extremidades. Assim as fiadas

av e va

são consideradas não distintas. Logo, existem três conjuntos de fiadas distintas, ou seja, três classes de equivalência,

$$\{aa\} \quad , \quad \{av, va\} \quad , \quad \{vv\}$$

Podemos chegar à mesma conclusão usando o Teorema de Burnside, consideremos

$$S = \{aa, av, va, vv\}$$

dividido pela relação de equivalência induzida pelo grupo de permutação $G = \{\pi_1, \pi_2\}$, onde

$$\pi_1 = \begin{pmatrix} aa & av & va & vv \\ aa & av & va & vv \end{pmatrix} \qquad \text{e} \qquad \pi_2 = \begin{pmatrix} aa & av & va & vv \\ aa & va & av & vv \end{pmatrix}$$

A permutação π_1 indica que cada fiada é equivalente a si mesma e a permutação π_2 indica a equivalência de fiadas quando as extremidades são trocadas. Então temos

$$|G| = 2 \quad , \quad |fix(\pi_1)| = 4 \quad , \quad |fix(\pi_2)| = 2$$

logo pelo Teorema de Burnside, verificamos que são três as classes de equivalência

$$\frac{1}{2}(4+2) = 3$$

ou seja, existem três fiadas distintas sob a relação de equivalência.

Uma **simetria** de uma figura (ou movimento simetria) é um movimento espacial da figura sobre si próprio.

Note-se que:

1. O conjunto de todas as simetrias sobre uma figura forma um grupo.
2. O conjunto de simetrias num polígono induz uma acção grupo permutação sobre os seus vértices (sobre o seu conjunto de vértices) e uma acção grupo permutação sobre o seu conjunto de arestas.

Exemplo 4

Actuando no conjunto $\{a,b,c,d,e\}$ temos o seguinte grupo permutação

$$(a)(b)(c)(d)(e) \quad , \quad (ab)(c)(d)(e) \quad , \quad (a)(b)(cd)(e) \quad , \quad (ab)(cd)(e)$$

As classes de equivalência deste grupo são $\{a,b\}$, $\{c,d\}$, $\{e\}$

O índice de ciclo é $\frac{1}{4}\left(x_1^5 + 2x_1^3x_2 + x_1x_2^2\right)$

Usando o cálculo simplificado do Teorema de Burnside tem-se

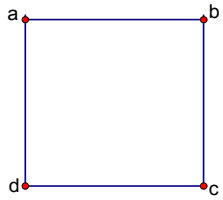
$$\frac{1}{4}(1\cdot 5 + 2\cdot 3 + 1\cdot 1) = \frac{12}{4} = 3$$

ou seja, é confirmada a existência de três classes de equivalência.

Exemplo 5

Um quadrado com vértices a, b, c, d tem oito simetrias possíveis: quatro rotações no plano em torno do centro do quadrado e quatro reflexões (que podem também ser obtidas por rotações espaciais de 180º fora do plano).

Pode-se ver isso na figura seguinte:



	Rotação	Reflexão
0º	$(a)(b)(c)(d)$	Eixo Horizontal $(ad)(bc)$
90º	$(abcd)$	Eixo Vertical $(ab)(cd)$
180º	$(ac)(bd)$	Eixo Diagonal Baixo $(a)(c)(bd)$
270º	$(adcb)$	Eixo Diagonal Cima $(b)(d)(ac)$

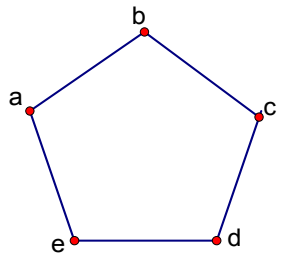
Figura 32 – Quadrado de vértices a, b, c, d

Existe somente uma só classe de equivalência $\{a,b,c,d\}$, e o índice de ciclo para o grupo de simetria de um quadrado, actuando no seu conjunto de vértices (o grupo octal D_4[40]) é

$$P_{D_4} = \frac{1}{8}\left(x_1^4 + 2x_4 + 3x_2^2 + 2x_1^2 x_2\right)$$

Exemplo 6

Um pentágono tem 10 simetrias diferentes: cinco rotações no plano em torno do centro do pentágono e cinco reflexões (ou equivalentemente, rotações espaciais de 180º fora do plano) em torno de eixos rectilíneos que passam num vértice e no meio do lado oposto:



	Rotação	Reflexão
0º	$(a)(b)(c)(d)(e)$	$(a)(be)(cd)$
72º	$(abcde)$	$(b)(ac)(de)$
144º	$(acebd)$	$(c)(ae)(bd)$
216º	$(adbec)$	$(d)(ab)(ce)$
288º	$(aedcb)$	$(e)(ad)(bc)$

Figura 33 – Pentágono de vértices a, b, c, d, e

Existe só uma classe de equivalência $\{a,b,c,d,e\}$ e o índice de ciclo associado é

$$\frac{1}{10}\left(x_1^5 + 4x_5 + 5x_1 x_2^2\right)$$

5.3 Padrões de cor e Permutações Induzidas

Uma coloração de um conjunto S a partir de um conjunto de n cores é uma função de S para o conjunto $\{1,...,n\}$ cujos elementos são vistos como “cores”. O conjunto de todas essas colorações designa-se por $C(S,n)$.

[40] D_n é o grupo de movimentos rápidos (rotações e reflexões) de um polígono regular com n lados sob composição

Uma coloração de vértices de uma figura geométrica (poligonal ou poliedral) é uma coloração do seu conjunto de vértices.

Uma coloração de arestas de uma figura geométrica é uma coloração do seu conjunto de arestas.

Sejam c_1 e c_2 as colorações do conjunto S e seja π uma permutação de S. Escreve-se $\pi(c_1)=c_2$ se $c_1(a)=c_2(\pi(a))$ para qualquer $a \in S$. A correspondência $c_1 \to c_1 \circ \pi^{-1}$ é o mapa induzido por π sobre as colorações de S. (A composição $c_1 \circ \pi^{-1}$ assegura uma cor a qualquer objecto $a \in S$, nomeadamente a cor $c_1\left(\pi^{-1}(a)\right)$.

Duas colorações de vértice de uma figura são equivalentes se uma pode ser mapeada por uma simetria. Definições análogas aplicam-se a colorações de aresta e a coloração de face.

Duas colorações c_1 e c_2 de um conjunto S são equivalentes sob um grupo $G=(P,S)$ se existir uma permutação $\pi \in P$ tal que $\pi(c_1)=c_2$.

Um padrão de coloração de vértices de uma figura, em relação a um conjunto de simetrias, é um conjunto de colorações mutuamente equivalentes da figura.

Note-se que:

1. Seja $G=(P,S)$ um grupo permutação. Então, a acção induzida de P sobre um conjunto $C(S,n)$ de coloração com n cores é uma acção de grupo permutação.
2. Quando P actua sobre o conjunto $C(S,n)$ de cores de S, o número de objectos permutados e de classes de equivalência, e o índice de ciclo polinomial, são diferentes de quando P actua sobre o próprio S.
3. Ao permutar o conjunto de vértices de uma figura, uma simetria de uma figura induz simultaneamente uma permutação do conjunto de todas as suas colorações de vértices. E o mesmo sucede com a coloração de arestas.

Exemplo 7

No exemplo 5 (do quadrado) um grupo permutação de 8 elementos actua nos quatro vértices de um quadrado. Existe, somente, uma classe de equivalência e o índice de ciclo é

$$\frac{1}{8}\left(x_1^4 + 2x_4 + 3x_2^2 + 2x_1^2 x_2\right).$$

A figura seguinte, representa uma situação semelhante ao problema inicial deste capítulo (tabuleiro de xadrez), e mostra o que sucede quando o mesmo grupo actua sobre o conjunto de colorações preto branco. O conjunto permutado tem 16 colorações, existindo 6 classes de equivalência

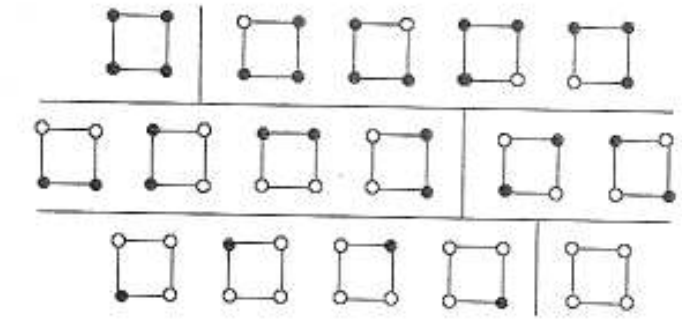


Figura 34 – Quadrado com vértices a preto e branco

e o índice de ciclo polinomial é

$$\frac{1}{8}\left(x_1^{16} + 2x_1^2 x_2 x_4^3 + 3x_1^4 x_2^6 + 2x_1^8 x_2^4\right)$$

Usando o cálculo simplificado do Teorema de Burnside, temos

$$\frac{1}{8}\left(1\cdot 16 + 2\cdot 2 + 3\cdot 4 + 2\cdot 8\right) = \frac{48}{8} = 6,$$

ou seja, 6 classes de equivalência.

Teorema especial de Burnside (para colorações): Seja G um grupo de permutação actuando num conjunto S. Então, o número de classes de equivalência induzidas em $C(S,n)$ (o conjunto de colorações de S obtido a partir de um conjunto de n cores) pode ser obtido substituindo *n* para cada variável, no polinómio de índice de ciclo.

A tabela seguinte dá informação sobre o número de padrões de coloração de vértices de determinadas figuras.

Figura	**Cores**			
	2	**3**	**4**	**m**
Triângulo	4	11	20	$\frac{1}{6}\left(m^3+3m^2+2m\right)$
Quadrado	6	21	55	$\frac{1}{8}\left(m^4+2m^3+3m^2+2m\right)$
Pentágono	8	39	136	$\frac{1}{10}\left(m^5+4m+5m^3\right)$
Hexágono	13	92	430	$\frac{1}{12}\left(m^6+3m^4+4m^3+2m^2+2m\right)$
Heptágono	18	198	1 300	$\frac{1}{14}\left(m^7+7m^4+6m\right)$
Octógono	30	498	4 183	$\frac{1}{16}\left(m^8+4m^5+5m^4+2m^2+4m\right)$

Exemplo 8

Vimos, no exemplo 6, que o índice de ciclo de grupo de simetrias do pentágono é

$$\frac{1}{10}\left(x_1^5+4x_5+5x_1x_2^2\right)$$

Pelo Teorema especial de Burnside, o número de m-colorações dos vértices de um pentágono não orientado é

$$\frac{1}{10}\left(m^5+4m+5m^3\right).$$

Para $m=3$, obtém-se $\frac{1}{10}\left(243+12+135\right)=39$ padrões de três colorações do pentágono.

5.4 A fórmula de contagem de Pólya

Uma contagem – padrão é uma função geradora que conta o número de padrões de coloração de uma dada figura.

Fórmula de contagem de Pólya: Seja $G=(P,S)$ um grupo de permutação e seja $\{c_1,...,c_n\}$ um conjunto de nomes para n cores dos objectos de S. Então a contagem – padrão relativa a *G* para o conjunto de todas as n colorações de S obtém-se substituindo x_j por $\{c_1^j+...+c_n^j\}$ no índice de ciclo $P_G=(x_1,...,x_m)$.

A fórmula de contagem de Pólya tem muitas aplicações na modelação de problemas que se baseiam em coloração de grafos.

Exemplo 9

A contagem da coloração a preto e branco dos vértices de um triângulo é

$$1p^3+1p_2b+1pb^2+1b^3$$

Significando que há um padrão de coloração para os três vértices pretos, um padrão para dois vértices pretos e um vértice branco etc.

Exemplo 10

Relativamente à coloração a preto e branco dos vértices do quadrado, vimos que o índice de ciclo é

$$P_{D_4}=\frac{1}{8}\left(x_1^4+2x_4+3x_2^2+2x_1^2x_2\right)$$

Pela fórmula de contagem de Pólya, a contagem – padrão das colorações a preto e branco dos vértices do quadrado é:

$$P_{D_4}\left[(p+b),\left(p^2+b^2\right),\left(p^3+b^3\right),\left(p^4+b^4\right),\right]$$

$$=\frac{1}{8}\left[(p+b)^4+2(p+b)^2\left(p^2+b^2\right)+3\left(p^2+b^2\right)^2+2\left(p^4+b^4\right)\right]$$

$$=\frac{1}{8}\left[8p^4+8p^3b+16p^2b^2+8pb^3+8b^4\right]$$

$$=1p^4+1p^3b+2p^2b^2+1pb^3+1b^4$$

Esta contagem pode ser confirmada observando a figura 28.

Exemplo 11

Relativamente ao exemplo 6, da coloração dos vértices do pentágono, o índice de ciclo é

$$\frac{1}{10}\left(x_1^5 + 4x_5 + 5x_1x_2^2\right)$$

Pela fórmula de contagem de Pólya, a contagem – padrão das colorações a preto e branco (verificável através de figuras), dos vértices do pentágono é:

$$\begin{aligned}
&P_{D_5}\left[(p+b),\left(p^2+b^2\right),\left(p^3+b^3\right),\left(p^4+b^4\right),\left(p^5+b^5\right)\right] \\
&= \frac{1}{10}\left[(p+b)^5 + 4\left(p^5+b^5\right) + 5(p+b)\left(p^2+b^2\right)^2\right] \\
&= \frac{1}{10}\left[10p^5 + 10p^4b + 20p^3b^2 + 20p^2b^3 + 10pb^4 + 10b^5\right] \\
&= 1p^5 + 1p^4b + 2p^3b^2 + 2p^2b^3 + 1pb^4 + 1b^5
\end{aligned}$$

Exemplo 12 Química orgânica

Dois componentes estruturalmente diferentes mas com a mesma fórmula química designam-se por isómeros. Por exemplo, para dois dos seis átomos de carbono (C) numa molécula, deve juntar-se um átomo de hidrogénio (H) e para cada um dos outros quatro átomos de carbono um outro radical (R), obtendo-se desse modo a fórmula química $C_6H_2R_4$. O número de diferentes isómeros (configurações estruturalmente diferentes dos radicais) é o mesmo número de padrões de coloração de um hexágono, quando dois dos vértices têm a "coloração" H e quatro têm a "coloração" R. O índice de ciclo para as simetrias de um hexágono, em termos de permutação de vértices, é

$$P_{D_6} = \frac{1}{12}\left[x_1^6 + 2x_6 + 2x_3^2 + 4x_2^3 + 3x_1^2x_2^2\right]$$

Substituindo x^j por $\left(H^j + R^j\right)$ obtém-se uma contagem – padrão que inventaria o número de isómeros de $C_6H_iR_{6-i}$:

$$\frac{1}{12}\left[(H+R)^6+2\left(H^6+R^6\right)+2\left(H^3+R^3\right)^2+4\left(H^2+R^2\right)^3+3(H+R)^2\left(H^2+R^2\right)^2\right]$$
$$=\frac{1}{12}\left[12H^6+12H^5R+36H^4R^2+36H^3R^3+36H^2R^4+12HR^5+12R^6\right]$$
$$=1H^6+1H^5R+3H^4R^2+3H^3R^3+3H^2R^4+1HR^5+1R^6$$

Os três possíveis padrões de "coloração" correspondentes a $3H^2R^4$ podem ser visualizados na figura seguinte

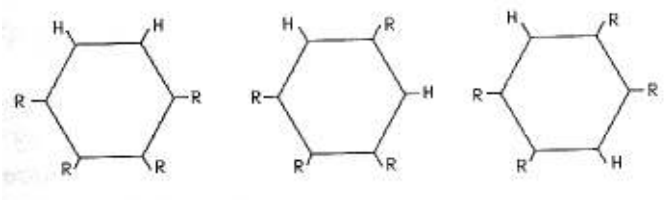


Figura 35 – Padrões de "coloração" de $3H^2R^4$

Conclusão

A Combinatória (e o seu ramo mais conhecido, a Análise Combinatória) é absolutamente essencial como suporte a vários campos da matemática, exemplificados pelas probabilidades, determinantes, teoria dos números, topologia, teoria dos grupos, etc. Tem, igualmente, aplicações nas mais diversas áreas do conhecimento como: a física, a química, a engenharia, a biologia, o planeamento urbano, entre outras

O interesse pela Combinatória tem aumentado nos últimos anos, em grande parte devido ao desenvolvimento da Ciência da Computação: basta pensar que na análise e estudo da eficácia de algoritmos é necessário efectuar contagens do número de passos efectuados numa operação.

Em relação a futuros trabalhos de investigação, pode-se sugerir o aprofundamento de qualquer um dos sub-temas abordados neste trabalho, especialmente na área dos Grafos, como aliás é proposto no respectivo capítulo, ou, ainda, o estudo dos “Designs Combinatórios”, assunto que, no âmbito da Combinatória se afigura extremamente interessante mas ainda não muito explorado, por se tratar de um tema relativamente recente.

Entretanto, a empenhada tarefa que concluí, podendo embora não ter dado mais do que um ínfimo contributo para a sistematização do conhecimento matemático, deixa-me a sensação do cumprimento do objectivo proposto e ainda da realização pessoal no âmbito do enriquecimento do meu saber.

.

Bibliografia

[1] Balakrishnan, V. K., *"Introductory Discrete Mathematics",* Dover, 1996.

[2] Barbosa, Ruy Madsen, *"Grupos e Combinatória"*, Departamento de Análise Numérica e Estatística IBILCE – UNESP, 1979.

[3] Berge, C., *"Graphs"* North-Holland, 3rd Edition, 1991.

[4] Boyer, Carl, *"História da Matemática*", Editora Edgard Blucher, 1991.

[5] Buescu, Jorge, *"Da Falsificação de Euros aos Pequenos Mundos",* Gradiva, 2005.

[6] Caraça, Bento de Jesus, *"Conceitos Fundamentais da Matemática",* Gradiva, 2003.

[7] Caraça, Bento de Jesus, *"Lições de Álgebra e Análise",* Depósito Livraria Sá da Costa, 1945.

[8] Davis, Philip, *" A Experiência Matemática",* Gradiva, 1981.

[9] Diestel, R.,*"Graph Theory"*, Springer, 1997.

[10] Gamow, G. *" Un, deux, trois,...., l'infini "*, Paris Dunod, 1955.

[11] Graham, R. L., Grostschel, M., lovász, L., (ed.), *"Handbook of Combinatorics"*, North-Holland, 1995.

[12] Haray, F., *"Graph Theory",* Addison-Wesley Publishing Company, Inc., 1969.

[13] Harary, F. and Palmer, E.M. *"Graphical Enumeration",* Academic Press, 1973.

[14] Hardy, G. H., *"Na Introduction to the Theory of Numbers",* Clarendon Press – Oxford, 1979.

[15] Hoffman, Paul, *"O Homem que Só Gostava de Números"*, Gradiva, 2000.

[16] Hogg, Robert, *"Probability and Statistical Inference",* Sixth Edition, 2001.

[17] Jornal de Matemática Elementar, *"Galeria de Matemáticos",* 1991.

[18] Jorge, A*, "Infinito 12",* volume 1, Areal Editores, 1999.

[19] Kramer, S., *" Os Sumérios",* Livraria Bertrand, 1977.

[20] Liu, C., L., *"Introduction to Combinatorial Mathematics",* McGraw-Hill, New York, 1968.

[21] Merayo, Félix Garcia, *"Matemática Discreta",* Thomson, 2005.

[22] Morgado, Augusto César de Oliveira, *"Análise Combinatória e Probabilidade"*, Colecção do Professor de Matemática, 1991.

[23] Nogueira, J. Eurico*, "Contar e Fazer Contas",* Gradiva, 2004.

[24] Oliveira, Cristina, *"Introdução à Análise Combinatória"*, Escolar Editora, 2004.

[25] Pascoal, António, Apontamentos das aulas das cadeiras: *"Novas Perspectivas da Matemática Aplicada"* e *"Metodologia da Matemática"* de Mestrado de Matemática / Ensino, 2005-2006.

[26] Rosen , K.H. et al., *"Handbook of Discrete and Combinatorial Mathematics"*, C R C Press, 2000.

[27] Rosen, Kenneth H., *"Discrete Mathematics and its Applications",* McGRAW-Hill, 1990.

[28] Santos, José, *"Introdução à Teoria dos Números",* Rio de Janeiro, Instituto de Matemática Pura e Aplicada, 2000.

[29] Sá, Joaquim, *"O Acaso – A vida do Jogo e o Jogo da Vida",* Gradiva, 2006.

[30] Scheinerman, Edward R., *"Matemática Discreta",* Thomson, 2003.

[31] Struik, Dirk, *"História Concisa das Matemáticas",* Gradiva, 1989.

[32] Vasconcellos, Fernando, *"História das Matemáticas na Antiguidade",* Livrarias Aillaud e Betrand, 1978.

Sites

http://www.educ.fc.ul.pt/icm/icm2002/icm101/pagina1.html

http://www.educ.fc.ul.pt/docentes/opombo/seminario/

http://www.educ.fc.ul.pt/icm/icm99/icm36/

http://pt.wikipedia.org/

http://www.dec.ufcg.edu.br/biografias/JohndeHa.html

http://www.somatematica.com.br/

http://www.obm.org.br/eureka/artigos/inducao.doc

http://www.educ.fc.ul.pt/docentes/opombo/

http://www.mat.uc.pt/~jaimecs/

http://www.cienciahoje.pt/

http://www.ime.uerj.br/

http://revistagalileu.globo.com/

http://www.mat.ufrgs.br/~portosil/histo2c.html

http://www.icmc.usp.br/~sma181/Teoria%20de%20Contagem.pdf

http://www.estatistica.ccet.ufrn.br/biografias/leibniz.html

http://www.matematicas.net/paraiso/historia.php?id=newton_raciona

http://mipagina.cantv.net/jhnieto/tc.pdf

http://www.mat.uel.br/jornal.htm#toc26

http://www.educ.fc.ul.pt/docentes/opombo/seminario/pasca_l/index.htm

http://thales.cica.es/rd/Recursos/rd97/Otros/SISTNUM.html#G

http://www.lmc.fc.ul.pt/~albuquer/fibonacci/trabalho/nfcb.htm

http://www.educ.fc.ul.pt/icm/icm99/icm48/sierpinski.htm

http://www.famat.ufu.br/revista/revistadez2003/salaaula/ProjetoGiovana.pdf

http://twiki.dcc.ufba.br/bin/view/MAT156/WebHome

http://www.gave.pt

http://www2.dem.inpe.br/ijar/Grafos%20Isomorfos.doc

http://www2.egi.ua.pt/cursos_2005/files/AOS/Conceitos_Grafos.pdf

http://66.102.9.104/search?q=cache:v8COOmiQRvwJ:www.prof2000.pt/users/adam/grafos/dois11.htm+Grafos+-blogs+-forum+-ementa+-sumario+-programa+Euler&hl=pt-PT&ct=clnk&cd=1&gl=pt

http://www.cin.ufpe.br/~if670/2-2005/Aulas4gr.ppt#439

http://w3.ualg.pt/~mpires/Home_ficheiros/Planaridade.doc