FUNDAMENTOS DE MATEMÁTICA DISCRETA

CARLOS A. A. FLORENTINO
FEVEREIRO 2021

CONTEÚDO

PREFÁCIO

Estas notas constituem uma abordagem introdutória ao que se designa, correntemente, por "Matemática Discreta". Existem vários textos dedicados a esta vasta área da Matemática, e quase todos eles incluem, com maior ou menor detalhe, noções elementares de teoria dos números, incluindo a aritmética modular, vários aspectos de combinatória e funções de contagem, e uma introdução à teoria dos grafos.

Da mesma forma, as presentes notas estão organizadas em três partes, cada uma das quais aborda um destes temas. Na primeira parte – "Números", apresenta-se uma introdução à teoria dos números elementar, onde se inclui a demonstração do teorema fundamental da aritmética, e se introduzem algumas técnicas simples de resolução de problemas em aritmética modular. O estudo culmina com os fundamentos teóricos de um dos algoritmos mais usados em criptografia: o algoritmo RSA de "chave pública".

Na segunda parte – "Funções e Combinatória", apresentam-se os vários princípios gerais da combinatória enumerativa, incluindo o princípio de incluusão-exclusão e algumas das suas aplicações. Também se apresentam métodos de resolução de problemas de recorrência lineares, ao mesmo tempo que se aborda o conceito de função geradora de uma sucessão. Finalmente, é sucintamente introduzida a teoria dos grupos de permutações, acções em conjuntos finitos e contagens com simetria, culminando no célebre Lema de Burnside-Cauchy-Frobenius.

Finalmente, na última parte, é apresentada uma introdução à teoria dos grafos. Esta teoria, relativamente moderna, se compararmos com os dois temas anteriores, reveste-se de uma importância crescente na matemática actual, e encontra aplicações em inúmeras áreas do conhecimento científico e tecnológico. A presente abordagem toca, sem aprofundar em demasia devido a questões de espaço, nalguns aspectos clássicos desta teoria, incluindo o tratamento de grafos dirigidos ou orientados. Para além disso, abordam-se também os aspectos matemáticos que estão na base do algoritmo "page-rank", usado pelo popular "motor de busca" Google, omnipresente na nossa interacção com o mundo da internet.

Parte 1. **NÚMEROS**

Nesta primeira parte, vamos estudar alguns aspectos elementares da teoria dos números. Começando pela familiar aritmética dos números *inteiros*, vamos apresentar e demonstrar o teorema fundamental da aritmética, que nos garante que qualquer número inteiro se pode escrever, de forma essencialmente única, como produto de números *primos*.

Seguidamente, introduz-se a aritmética modular, que é a aritmética de números "cíclicos" – números que somados um determinado número fixo de vezes, dão sempre zero como resultado. Muitas propriedades dos inteiros modulares são análogas às correspondentes propriedades dos números inteiros, embora, devido à sua finitude, os primeiros sejam naturalmente bem adaptados a processos de cálculo automatizado, como os algoritmos inplementados num computador.

Terminamos esta introdução à teoria dos números com os fundamentos teóricos de um dos algoritmos mais usados em criptografia: o algoritmo de encriptação de mensagens usando "chave pública" conhecido por algoritmo RSA.

1. Números Inteiros

Um número inteiro é um elemento do conjunto:

$$\{\cdots, -2, -1, 0, 1, 2, 3, \cdots\}.$$

O conjunto de todos os números inteiros é denotado por $\mathbb{Z}$. Há dois importantes subconjuntos dos números inteiros: Os números naturais,

$$\mathbb{N} := \{1, 2, 3, \cdots\},$$

que também são chamados os inteiros positivos, e os números inteiros não negativos,

$$\mathbb{N}_0 := \{0, 1, 2, \cdots\} = \mathbb{N} \cup \{0\}.$$

Menos usada é a notação $\mathbb{N}_- := \{\cdots, -3, -2, -1\}$, para o conjunto dos inteiros negativos.

Nestas notas, vamos usar sempre a expressão ":=" para indicar que o elemento/expressão que fica do lado esquerdo é definido(a) pela expressão do lado direito.

Acima, usámos livremente as notações comummente aceites da teoria dos *conjuntos*, como a notação dos parêntesis, "$\{\cdots\}$", que serve para descrever um conjunto (mesmo quando ele é *infinito*, através das reticências) e a operação "$\cup$" que denota a *união* de dois (ou mais) conjuntos. Outros exemplos de *identidades* entre conjuntos são:

$$\mathbb{Z} = \mathbb{N}_0 \cup \mathbb{N}_-, \qquad \mathbb{N} \cap \mathbb{N}_- = \varnothing,$$

onde "$\cap$" representa a *intersecção* de conjuntos, e $\varnothing$ é o *conjunto vazio*. Um resumo das noções e propriedades elementares dos conjuntos encontra-se no Apêndice 1 (a elaborar).

Outra terminologia úbiqua é a que se usa para abreviar que um dado *elemento pertence* ($\in$), ou *não pertence* ($\notin$), a um dado conjunto. Por exemplo, como -217 é um inteiro negativo, podemos escrever

$$-217 \in \mathbb{Z}, \qquad -217 \notin \mathbb{N}.$$

As várias propriedades e operações em conjuntos, em particular para o caso de conjuntos *finitos*, serão fundamentais na segunda parte do livro, dada a sua importância para os processos de contagem e combinatória.

1.1. **Artimética dos inteiros.** A importância dos números inteiros vem do facto de podermos fazer operações úteis com eles. O estudo das operações mais simples com inteiros: a *adição* (ou *soma*), a *subtracção* (ou *diferença*), a *multiplicação* (ou *produto*) e a *divisão* (com *resto*) designa-se, no seu conjunto, por *Aritmética* dos inteiros. Obviamente, vamos assumir que tudo

isto é muito bem sabido, bastando-nos rever sucintamente alguma da terminologia corrente na aritmética.

Recorde-se, por exemplo, que em expressões de soma (+) ou de subtração (−), tais como:

$$6+13, \quad 6-13,$$

os inteiros 6 e 13 chamam-se *parcelas*. Para o produto é normalmente usada a notação "×" ou "·". Vamos usar a segunda, por ser mais simples. Numa expressão de produto, como:

$$6 \cdot 13,$$

os inteiros 6 e 13 designam-se por *factores*.

Sabemos que $a+b=b+a$ para qualquer par de inteiros $a,b \in \mathbb{Z}$. Da mesma forma $a \cdot b = b \cdot a$ para quaisquer $a,b \in \mathbb{Z}$. Assim, dizemos que a adição e a multiplicação são operações *comutativas*, o que não se passa com a subtração.

Há um *elemento neutro* da adição, o zero (0), e outro da multiplicação, o número 1, pois temos:

$$\begin{aligned} a+0 &= 0+a=a, \\ a \cdot 1 &= 1 \cdot a = a, \quad \forall a \in \mathbb{Z}. \end{aligned}$$

O símbolo "∀" deve ler-se "para todo". Outras propriedades que tomamos como certas e sabidas são a *associatividade* da soma e do produto:

$$\begin{aligned} a \cdot (b \cdot c) &= (a \cdot b) \cdot c, \\ a+(b+c) &= (a+b)+c, \quad \forall a,b,c \in \mathbb{Z}, \end{aligned}$$

bem como a *distributividade do produto em relação à soma*:

$$a \cdot (b+c) = a \cdot b + a \cdot c, \quad \forall a,b,c \in \mathbb{Z}.$$

Também é bem sabido que, dado um inteiro qualquer, $a \in \mathbb{Z}$, existe um outro, chamado o seu simétrico e denotado por $-a$ tal que[1]

$$a+(-a)=0.$$

Recorde-se que o 0 é também chamado o elemento *absorvente* da multiplicação, porque $a \cdot 0 = 0 \cdot a = 0$ para todo $a \in \mathbb{Z}$ (Exercício 1.1(c)).

Finalmente, realçamos uma das mais importantes regras referentes ao produto de inteiros: a chamada *"lei do corte de factores iguais"* ou simplesmente *"lei do corte"*. Ela diz-nos que, para todo o inteiro a **não nulo** (isto é, $a \neq 0$) temos

$$a \cdot b = a \cdot c \quad \Leftrightarrow \quad b = c, \quad \forall b,c \in \mathbb{Z}.$$

Acima, o símbolo $\Leftrightarrow$ significa que existe uma *equivalência lógica* entre a expressão do lado direito e a expressão do lado esquerdo. Por outras palavras, sempre que $a \neq 0$, podemos substituir a expressão "$a \cdot b = a \cdot c$" por "$b = c$" e vice-versa sem cometer nenhum erro.

Convém enfatizar que, se $b = c$ então $a \cdot b = a \cdot c$ para qualquer valor de $a \in \mathbb{Z}$. No entanto, a implicação contrária apenas se verifica quando $a \neq 0$.

Exercício 1.1. Mostre, de acordo com as propriedades de $\mathbb{Z}$, $+$, $\cdot$, 0 e 1, acima enunciadas, as seguintes regras, para quaisquer $a,b \in \mathbb{Z}$:

(a) A subtracção não é comutativa nem associativa,

(b) O produto é distributivo em relação à subtracção,

(c) $a \cdot 0 = 0 \cdot a = 0$, [Aqui, pretende-se mostrar que esta regra é consequência das outras regras enunciadas],

(d) $(-1) \cdot a = -a$,

[1] Note-se que, de acordo com esta terminologia, o número zero é o seu próprio simétrico.

(e) $(-a)\cdot(-b)=a\cdot b$,

(f) Se $a\cdot b=0$, então $a=0$ ou $b=0$. [Sugestão: use a lei do corte].

A lei do corte, se incorrectamente aplicada, pode dar origem a resultados estranhos...!

Exercício 1.2. Considere a seguinte "demonstração de que $1=2$". Seja x uma variável que representa um número inteiro. Podemos escrever $x^2-x^2=x^2-x^2$. Factorizando, temos $x(x-x)=(x+x)(x-x)$, logo pela lei do corte $x=x+x=2x$. Novamente pela lei do corte $1=2$. Onde está o erro no argumento anterior?

Os seguintes exercícios são também imediatos, e abordam a relação entre os inteiros e os naturais, que são, como definimos, os inteiros positivos.

Exercício 1.3. Mostre, usando as propriedades acima enunciadas, as seguintes regras:

(a) O número 0 é o único inteiro igual ao seu simétrico.

(b) Se $a\in\mathbb{Z}$ não é zero, temos $a\in\mathbb{N}$ ou $-a\in\mathbb{N}$ (e um dos casos exclui o outro).

(c) A soma e o produto de dois números naturais é um número natural, mas o mesmo não se verifica para a subtracção.

(d) O produto de dois números negativos é positivo.

Notação: De ora em diante, por brevidade, omitiremos o ponto na multiplicação de números representados por letras; por exemplo, "$a\,b$" designa o produto dos dois números $a,b\in\mathbb{Z}$. Usaremos o ponto apenas para números concretos, como em "$23\cdot 7=161$".

Propositadamente, a operação de divisão com resto foi deixada para uma próxima subsecção, para dar-lhe um tratamento mais detalhado, o que será extremamente útil na demonstração do teorema fundamental da aritmética, na Subsecção 1.8.

Entretanto, vamos recordar outras propriedades dos inteiros, nomeadamente a sua estrutura de ordem.

1.2. **Ordenação em $\mathbb{Z}$ e em $\mathbb{N}$.** Para além das suas propriedades aritméticas, o conjunto $\mathbb{Z}$ tem uma outra propriedade muito importante, que reflecte a possibilidade de ordenarmos os números inteiros: dados dois inteiros diferentes, existe sempre um deles *maior* que o outro. Isto acontece também para conjunto dos números naturais $\mathbb{N}$.

Concretamente, podemos definir a relação de ordem em $\mathbb{Z}$ da seguinte forma. Começamos por dizer que um número inteiro $a\in\mathbb{Z}$ é *positivo* se $a\in\mathbb{N}$, e escrevemos "$a>0$".

Definição 1.1. Sejam $a,b\in\mathbb{Z}$. Dizemos que o inteiro a é maior que o inteiro b, se $a-b\in\mathbb{N}$, ou seja, se $a-b$ é positivo, e escrevemos $a>b$. Neste caso, também dizemos que b é menor que a, ou $b<a$.

Assim, por definição:

$$a>b \quad\Leftrightarrow\quad b<a \quad\Leftrightarrow\quad a-b>0 \quad\Leftrightarrow\quad b-a<0 \quad\Leftrightarrow\quad a-b\in\mathbb{N}.$$

Podemos também entender esta relação de ordem dizendo que o número maior se obtém do menor somando um número positivo. De facto, $a<b$ se e só se existe $n\in\mathbb{N}$ tal que $a+n=b$. Outra terminologia e notação que se usa com frequência é a de "maior ou igual" ($\geq$) e de "menor ou igual" ($\leq$).

Notação: Sejam $a,b\in\mathbb{Z}$. Dizemos que a é maior ou igual a b, e escrevemos $a\geq b$ se $a-b\in\mathbb{N}_0$, ou seja, se $a>b$ ou se $a=b$. De forma análoga usamos a expressão "menor ou igual" e a notação "$\leq$".

Usando estas notações, podemos escrever por exemplo,

$$\forall a,b>0,\quad a\,b>0 \quad\text{e}\quad a+b>0,$$

de acordo com o Exercício 1.1(c).

Proposição 1.2. *As relações* $>$, $<$, $\geq$ *e* $\leq$ *são* transitivas*, isto é se* $a > b$ *e* $b > c$*, então* $a > c$*. As outras 3 relações verificam a mesma propriedade.*

Demonstração. As condições $a > b$ e $b > c$, para números inteiros a, b, c, significam que existem m e n positivos tais que $a = b + n$ e $b = c + m$. Assim, $a = c + m + n$ o que significa, como $m + n$ é positivo, que $a > c$. Da mesma forma se demonstra a transitividade das outras relações. □

As seguintes propriedades bem conhecidas são deixadas como exercício.

Exercício 1.4. (a) Tricotomia: Dados dois inteiros temos sempre uma das seguintes situações, e se uma ocorre, as outras não: (i) $a > b$ (ii) $a < b$ (iii) $a = b$.

(b) Se $a > b$ e $c > 0$, então $a\,c > b\,c$

(c) Se $a > b$ então $-b > -a$

(d) Se $a > b$ então $a + c > b + c$, $\quad \forall c \in \mathbb{Z}$.

É fácil de ver, usando as relações de ordem e as propriedades aritméticas, que ambos os conjuntos $\mathbb{Z}$ e $\mathbb{N}$ são *infinitos*. Vamos estudar conjuntos *finitos* e *infinitos* em maior detalhe no Capítulo....

Proposição 1.3. *Os conjuntos* $\mathbb{Z}$ *e* $\mathbb{N}$ *são infinitos.*

Demonstração. Vamos supor que $\mathbb{N}$ é um conjunto finito. Então, comparando todos os elementos dois a dois, e usando a tricotomia (Exercício 1.2(a)) e a transitividade da relação $<$ (Proposição 1.2) obtemos o natural a, o *maior* de todos os elementos de $\mathbb{N}$. Mas $a + 1$ é também natural e é maior que a. Obtemos uma contradição, o que significa que a nossa hipótese estava errada. Assim, $\mathbb{N}$ é infinito. Para $\mathbb{Z}$ o racioncício é análogo. □

A demonstração acima ilustra uma das técnicas de demonstração muito frequentes em matemática, designada por "demonstração por contradição". Nela, fazemos a hipótese contrária ao que pretendemos mostrar, assumindo também todas as outras hipóteses do enunciado. Usando propriedades e resultados previamente demonstrados, chegamos a uma contradição lógica. Nesse caso, pelo menos uma das hipóteses que usámos estava errada. Mas como todas as hipóteses estavam no enunciado, à excepção da contrária à que queríamos provar, é esta última que está a ser negada, quando assumimos as outras.

1.3. **Divisão e divisores.** O algoritmo de divisão de números inteiros, com resto, aparece descrito por primeira vez na história conhecida, no tratado de Euclides chamado "Os Elementos".

Consideremos em primeiro lugar a divisão de um número inteiro $a \in \mathbb{Z}$ por um número natural $b \in \mathbb{N}$ (em particular, temos $b \neq 0$). É bem sabido que podemos sempre *resolver* a equação:

$$a = b\,q + r,$$

encontrando inteiros q, $r \in \mathbb{Z}$ que a satisfaçam.

É muito importante nesta equação o facto de que q e r ficam **unicamente determinados** desde que se exija que $0 \leq r < b$. Quando se verifica esta condição, q e r são únicos (Exercício 1.3 (d)), e chamados então, respectivamente, o *quociente* e o *resto* da divisão de a por b.[2]

[2] Os inteiros a e b, chamam-se também o *dividendo* e o *divisor*, respectivamente; esta terminologia não será muito usada, para evitar confusões com a importante noção de *divisor*, na Definição 1.5 (abaixo).

Exemplo 1.4. Vamos elaborar o algoritmo de divisão no caso seguinte: a divisão de $a = 487$ por $b = 32$. Temos:

$$\begin{array}{rl} 487 & |\underline{32\quad} \\ \underline{32\quad} & |\,15 \\ 167 & | \\ \underline{160} & | \\ 7 & \end{array}$$

Concluímos então: $487 = 32 \cdot 15 + 7$. Desta forma, o quociente da divisão de 487 por 32 é 15, e o resto é 7. Como podemos verificar $r = 7 \in \{0, \cdots, 31\}$.

Exercício 1.5. Mostre o seguinte para a divisão $a = bq + r$:
(a) Se $a, b \in \mathbb{N}$, então $a \geq b$ se e só se $q \geq 1$;
(b) Se $0 \leq a < b$, então $q = 0$ e $r = a$, respectivamente;
(c) O mesmo resto r obtém-se dividindo $a + k\,b$ por b, para qualquer inteiro $k \in \mathbb{Z}$;
(d) [Unicidade da divisão com resto] As igualdades $a = bq + r = bq' + r'$, com a condição $r, r' \in \{0, \cdots, n-1\}$ implicam $r = r'$ e $q = q'$.

Em geral, o resto da divisão de um inteiro por um natural é não nulo. Quando o resto é zero, temos uma situação especial.

Definição 1.5. Sejam $a, b \in \mathbb{Z}$. Diz-se que b divide a, ou que b é um divisor de a, ou ainda que a é um divisível por b, se existe um outro inteiro $q \in \mathbb{Z}$ tal que

$$a = b\,q.$$

Se um tal inteiro não existe, diz-se que b não divide a.

Por outras palavras, supondo a e b positivos, b divide a se e somente se o resto da divisão de a por b é zero.

Notação 1.5. Quando b divide a, escrevemos $b \mid a$. Se b não divide a, escrevemos $b \nmid a$. Quando $b \mid a$ também dizemos que a é um múltiplo de b.

Exemplo 1.6. Temos $5 \mid 15$, uma vez que $15 = 5 \cdot 3$. Por outro lado $5 \nmid 16$, uma vez que o resto da divisão de 16 por 5 é $1 \neq 0$.

De modo a familiarizar o leitor com esta notação e terminologia, mostramos algumas das propriedades desta relação e deixamos outras como simples exercícios.

Proposição 1.7. *Sejam $a, b, c \in \mathbb{Z}$.*
(1) Se $a \mid b$ e $b \mid c$ então $a \mid c$.
(2) Se $b \mid a$ e $a \mid b$ então $|a| = |b|$.
(3) Se $a, b \in \mathbb{N}$ e $a \mid b$, então $a \leq b$.

Acima, usámos a notação do valor absoluto, ou módulo, definido por:

$$|a| := \begin{cases} a, & a \geq 0 \\ -a, & a \leq 0, \end{cases}$$

de modo que temos sempre $|a| \geq 0$ e $|a| = |-a|$ para qualquer inteiro a.

Demonstração. (1) A hipótese afirma que existem n e m, inteiros, tais que $b = na$ e $c = mb$. Portanto $c = mna$ e, sendo mn um inteiro, $a \mid c$. (2) Supomos primeiro que $ab \neq 0$. Se $a = mb$ e $b = na$, então $ab = mnab$. Usando a lei do corte, concluímos que $mn = 1$. É fácil verificar que as únicas soluções são $m = n = 1$ ou $m = n = -1$ (Exercício ...). Logo, $a = b$ ou $a = -b$. O caso em que $ab = 0$ é deixado ao leitor. (3) Seja $q \in \mathbb{Z}$ tal que $b = qa$ (pois $a \mid b$). Sendo a e b

positivos, vemos que também q deve ser positivo, ou seja, natural. Assim, $q \geq 1$. Multiplicando por $a > 0$ temos $aq \geq a$, ou seja $b \geq a$. □

Exercício 1.6. Sejam a, b, c inteiros. Mostre as seguintes afirmações:
(a) $1 \mid a$, e $a \mid 0$, para todo a.
(b) Se $a \mid b$, então $a \mid b\,k$, e $a\,k \mid b\,k$ para todo o $k \in \mathbb{Z}$.
(c) $a \mid b$ é equivalente a $|a| \mid |b|$.
(d) Se $a \mid b$ e $a \mid c$, então $a \mid (b+c)$ e $a \mid (b-c)$.
(e) Numa divisão $a = b\,q + r$, se $c \mid a$ e $c \mid b$, então $c \mid r$.

Notação: Usamos a notação $\mathsf{Div}(a)$ para o conjunto de todos os divisores positivos de $a \in \mathbb{Z}$.

Exercício 1.7. Seja $n \in \mathbb{Z}$. Mostre que $\mathsf{Div}(n)$ é um conjunto finito, excepto quando $n = 0$; e que $\mathsf{Div}(0) = \mathbb{Z}$.

Observação 1.8. Embora qualquer inteiro tenha divisores positivos e negativos (se $d \mid n$, então também $-d \mid n$), para evitar redundâncias irrelevantes, no conjunto $\mathsf{Div}(n)$ (bem como na definição de número *primo*, abaixo), consideramos apenas os divisores positivos. Em particular $\mathsf{Div}(-n) = \mathsf{Div}(n)$ para todo natural n.

Exemplo 1.9. Sendo $n = 12$ temos $\mathsf{Div}(12) = \{1,2,3,4,6,12\}$. Com mais detalhe podemos considerar o que se chama um *diagrama de divisores*: um diagrama que mostra todas as relações de divisão entre os divisores de n. Por exemplo, o diagrama de divisores de $n = 12$ é:

$$\begin{array}{ccccccc} 1 & \to & 2 & \to & 4 & & \\ & \searrow & & \searrow & & \searrow & \\ & & 3 & \to & 6 & \to & 12. \end{array}$$

As setas $a \to b$, $a \neq b$, surgem sempre que a é divisor de b, e evita-se incluir setas que são composição de 2 ou mais setas. Num destes diagramas, os primeiros naturais que aparecem logo a seguir ao 1 (o 1 está sempre presente (Exercício 1.3(a))) chamam-se *números primos*.

1.4. **Números primos.**

Definição 1.10. Diz-se que um número natural $p \in \mathbb{N}$, $p > 1$, é um número primo se os únicos divisores (positivos) de p são 1 e p. Os números naturais (maiores que 1) que não são primos chamam-se números compostos.[3]

Assim, n é primo se e só se $\mathsf{Div}(n) = \{1, n\}$ (com $n \in \mathbb{N}$ e $n \neq 1$), ou seja $|\mathsf{Div}(n)| = 2$.

Exemplo 1.11. O número 191 é primo; o número 192 é composto. De facto, $\mathsf{Div}(191) = \{1, 191\}$ e

$$\mathsf{Div}(192) = \{1,2,3,4,6,8,12,16,24,32,48,64,96,192\},$$

como se pode verificar directamente.

Exercício 1.8. Mostre que um natural n é composto se e só se tem um divisor maior ou igual a 2 e diferente de n.

Ao contrário do processo de divisão, não existe nenhum algoritmo simples e rápido para determinar se um número muito grande é ou não primo. Estudaremos melhor este tipo de problemas mais tarde, e veremos a sua aplicação à criptografia.

Proposição 1.12. *Qualquer número natural, maior que 1, é divisível por algum primo.*

[3] Por convenção, 1 não é primo nem composto.

Demonstração. Seja $a \in \mathbb{N}$. Se a é primo, nada há a provar. Seja então $a = a_1$ um número composto e $b \in \mathsf{Div}(a)$ com $b \neq 1$ e $b \neq a_1$ (b existe porque $|\mathsf{Div}(a)| > 2$). Então $a_1 = a_2 b$ para certo $a_2 > 1$. Como $b > 1$, temos $a_2 < a_1$. Se a_2 é primo, a demonstração termina. Caso contrário, repetimos o processo para a_2. Continuando desta forma, e como o número de naturais menores que a é finito, este processo termina num número $a_n \geq 2$, que é forçosamente primo. Por construção

$$a_n \mid a_{n-1} \mid \cdots \mid a_2 \mid a_1 = a,$$

($a_k \mid a_{k-1}$, para $k = 2, \cdots, n$) pelo que o primo a_n divide a, como queriamos provar. □

Observação 1.13. Da mesma forma, qualquer inteiro não nulo, diferente de ± 1 é divisível por algum primo.

Teorema 1.14. *(Teeteto/Euclides) O número de primos é infinito.*

Demonstração. Vamos supor que $\{p_1, p_2, \cdots, p_n\}$ é o conjunto finito de todos os números primos. Podemos ordená-los de forma crescente: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc. Assim, estamos a supor que p_n é o maior número primo, e que $n \in \mathbb{N}$ é o número de primos.

Consideremos o número $m = p_1 p_2 \cdots p_n + 1$. Como m é maior que o maior primo (pois $m = p_1 \cdots p_n + 1 > p_1 \cdots p_n > p_n$), m tem que ser composto. Pela proposição anterior, existe um primo que divide m, por exemplo $p_k \mid m$, para certo $k \in \{1, \cdots, n\}$. Como $p_k \mid p_1 p_2 \cdots p_n$ temos

$$p_k \mid (m - p_1 p_2 \cdots p_n) \qquad \Leftrightarrow \qquad p_k \mid 1.$$

Obtemos uma contradição, porque nenhum primo divide 1. Portanto, o número de primos não é finito. □

Existem imensos problemas em aberto sobre os números primos. Por exemplo, sabe-se que existem sequências arbitrariamente grandes de números consecutivos que são compostos: veja-se o Problema 1.8 (14). Por outro lado, a mesma questão para números primos é extremamente difícil.

Um exemplo é o seguinte. Sendo $n \in \mathbb{N}$, os números n, $n+2$ chamam-se *primos gémeos* se ambos são primos (logo, n tem que ser ímpar). Apesar de ter mais de 2000 anos é ainda um problema em aberto saber se o número de primos gémeos é ou não infinito.

1.5. **O Algoritmo de Euclides.** Embora pareça surpreendente à primeira vista, é uma tarefa muito difícil para humanos, e até para computadores, determinar se um dado número é primo, caso esse número seja mesmo muito grande.

Existe outra noção, relacionada com o conceito de número primo, que resulta ser muito mais manejável, e cujas propriedades permitem provar resultados importantes, tal como o próprio teorema fundamental da aritmética. Esta noção torna-se assim muito útil na prática, ao trabalhar com números inteiros, bem como com os números modulares que estudaremos no capítulo 3.

Estamos a falar de pares de números que se chamam *primos entre si*, e das noções associadas de *máximo divisor comum* e de *menor múltiplo comum*.

Estas noções são extremamente importantes por si só, em muitos problemas concretos. O algoritmo de Euclides é um processo extretamente útil e versátil no cálculo destes números.

Definição 1.15. Sejam dados inteiros $a, b \in \mathbb{Z}$, em que pelo menos um deles é não nulo. O máximo divisor comum d (abreviadamente mdc) entre a e b é o maior elemento do conjunto:

$$\mathsf{Div}(a) \cap \mathsf{Div}(b).$$

Notação 1.15. Sendo $a, b \in \mathbb{Z}$ não ambos nulos, o único máximo divisor comum entre a e b é denotado por $\mathrm{mdc}(a, b)$, ou mais frequentemente, por (a, b).

Note-se que este máximo elemento existe pois um dos dois conjuntos acima é finito (ou $a \neq 0$ ou $b \neq 0$, ver exercício 1.3).

Temos então as seguintes propriedades imediatas, que se deixam ao leitor. Sendo muito frequente lidarmos com condições para números não nulos, vamos usar a notação $\mathbb{Z}^\times$ para denotar o conjunto dos inteiros que não são zero. Assim,

$$\mathbb{Z}^\times = \mathbb{N} \cup \mathbb{N}_-.$$

Exercício 1.9. Sejam $a, b \in \mathbb{Z}$ não ambos nulos.
(a) $(a,b) \leq \min\{|a|, |b|\}$
(b) $(a,b) = (b,a) = (|a|, |b|)$
(c) $(ka, kb) = k(a,b)$
(d) $(b,0) = (0,b) = |b|$, para $b \in \mathbb{Z}^\times$
(e) $(b,1) = (1,b) = 1$
(f) Seja $a > b > 0$. Mostre que $\mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(a-b) \cap \mathrm{Div}(b)$.

Observação 1.16. Note-se que $(0,0)$ não está definido. De facto, como qualquer inteiro divide 0, não existe um máximo divisor comum entre 0 e 0. Esta é a razão porque nos restrigimos ao caso em que a, b não são ambos nulos.

O máximo divisor comum entre dois inteiros pode também ser definido pela seguinte propriedade: qualquer outro divisor comum a a e b, divide (a,b).

Proposição 1.17. *Sejam dados inteiros $a, b \in \mathbb{Z}$, em que pelo menos um deles é não nulo, e seja $d = (a,b)$ o seu máximo divisor comum. Se $c \in \mathbb{N}$ é divisor de a e divisor de b, então $c \mid d$.*

Demonstração. É fácil ver que podemos assumir, sem perda de generalidade, que $a > b > 0$. Esta demosntração usa o princípio de indução forte, que veremos adiante; a indução é relativa à soma $a + b$. O passo base é então quando $a = 2$, $b = 1$. O máximo divisor comum é 1, e qualquer divisor positivo de a e b é 1, pelo que a propriedade está verificada. Vamos então assumir que a proposição é válida para quaisquer a e b naturais com $a + b < n$. Seja $a + b = n$ com $a > b$ (sem perda de generalidade). Então, por hipótese temos $c \mid a$ e $c \mid b$ pelo que $c \mid (a-b)$ e $c \mid b$. Como $(a-b, b) = (a,b) = d$ pelo exercício 1.5(f), temos $c \mid d$ pelo passo de indução, uma vez que $(a-b) + b = a < n$. □

Definição 1.18. Sejam $a, b \in \mathbb{Z}^\times$. Se 1 é o máximo divisor comum de a e b, $\mathrm{mdc}(a,b) = 1$, então a e b dizem-se primos entre si.

Exercício 1.10. Sejam $a, b \in \mathbb{Z}^\times$ e d tal que $\frac{a}{d}$ e $\frac{b}{d}$ são inteiros. Mostre que d é o máximo divisor comum entre a e b se e só se $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si.

Proposição 1.19. *Sejam $a, b \in \mathbb{Z}^\times$. Então, a e b são primos entre si, se e só se não existe nenhum primo p que os divide a ambos.*

Demonstração. Seja $(a,b) = d$. Se o primo p divide a e b, então $p \mid d$, por definição de d. Como tal, $d \geq p > 1$, pelo que a e b não são primos entre si. Reciprocamente, se $d > 1$, seja p um primo que divide d. Então $p \mid a$ e $p \mid b$. □

Observação 1.20. Na definição acima poderíamos ter considerado a ou b (embora não ambos) zero. No entanto, é fácil verificar que o zero nunca é primo com nenhum outro inteiro maior que 1 (Exercício 1.5(d)).

Vamos agora descrever o algoritmo de Euclides, que determina o máximo divisor comum d entre dois inteiros $a, b \in \mathbb{Z}$. O caso em que a ou b é nulo, bem como o caso $a = b$ são imediatos. Como o caso de inteiros negativos é equivalente ao dos seus módulos (Exercício 1.5), vamos considerar como **dados iniciais um par a, b de números naturais distintos**.

Podemos supor, sem perda de generalidade, que $a > b$. Começamos por aplicar o algoritmo da divisão de a por b, com resto. Por uma razão que será rapidamente evidente, vamos colocar $d_0 := a$ e $d_1 := b$. Definimos então d_2 como o resto da divisão de a por b, ou seja:

$$a = bq_1 + d_2 \qquad \Leftrightarrow \qquad d_0 = d_1 q_1 + d_2,$$

para certo $q_1 \in \mathbb{N}$, onde por definição de resto, temos $0 \leq d_2 < d_1$. Se $d_2 = 0$, paramos, pois $d_1 = d = (a,b)$, como podemos facilmente verificar.

Caso contrário, continuamos. O segundo passo é dividir d_1 por d_2, e novamente chamamos a d_3 o resto desta divisão. Obtemos então $0 \leq d_3 < d_2$; se $d_3 = 0$ paramos, caso contrário continuamos. Vamos então construindo uma sucessão estritamente decrescente de números naturais:

$$a = d_0 > b = d_1 > d_2 > \cdots > d_n > d_{n+1} = 0,$$

até chegar a zero, altura em que obtemos o máximo divisor comum: $d_n = (a,b)$. Dada a sua importância, convém enunciar estes resultados numa Proposição.

Teorema 1.21. *[Algoritmo de Euclides] O processo acima termina sempre num número finito de passos. Sendo $d_{n+1} = 0$, então o máximo divisor comum de a e b é $(a,b) = d_n$.*

Demonstração. O facto de haver um número finito de passos é simples. De facto, o conjunto

$$D := \{d_0, d_1, \cdots, d_n, \cdots\} \subset \{0, 1, \cdots, d_0\},$$

tem cardinal $|D| < a = d_0$. Seja $d_1 := b$ e $d_{n+1} = 0$. Então, por construção temos

$$\begin{aligned} d_0 &= d_1 q_1 + d_2 \\ d_1 &= d_2 q_2 + d_3 \\ &\vdots \\ d_{n-1} &= d_n q_n + 0. \end{aligned} \tag{1.1}$$

Isto significa que $d_n \mid d_{n-1}$. Pela equação $d_{n-2} = d_{n-1} q_{n-1} + d_n$ vemos que $d_n \mid d_{n-2}$ e assim sucessivamente. Concluímos então que $d_n \mid d_1$ e que $d_n \mid d_0$. Ou seja, d_n divide b e divide a. Seja agora $c > 0$ tal que $c \mid a$ e $c \mid b$. Então, a primeira equação diz-nos que $c \mid d_2$, a segunda equação implica $c \mid d_3$, etc (cf. 1.3). Continuando da mesma forma, concluímos que $c \mid d_n$ e portanto, por definição de máximo divisor comum, temos $d_n = (a,b)$. □

1.6. **A equação de Bézout e o algoritmo de Euclides estendido.** A seguinte identidade, chamada equação de Bézout, é de grande utilidade em várias situações.

Teorema 1.22. *Sejam dados inteiros a e b não nulos. Se $d = (a,b)$ então existem inteiros u e v, tais que*

$$d = a\,u + b\,v.$$

Além disso, existem soluções (u_0, v_0) que verificam $|u| < \left|\frac{b}{d}\right|$ e $|v| < \left|\frac{a}{d}\right|$.

Demonstração. A demonstração usa o algoritmo de Euclides, no "sentido inverso", o que também se chama "algoritmo de Euclides *estendido*" . Usemos a mesma notação que na demonstração do Teorema 1.21, onde temos várias equações (1.1) da forma $d_{k-1} = d_k\, q_k + d_{k+1}$, com

$k = 1, \cdots, n-1$. Escrevemos então:

$$\begin{aligned}
(d_n \text{ em termos dos anteriores}): \quad & d_n = d_{n-2} - d_{n-1} q_{n-1} \\
(d_{n-1} \text{ em termos dos anteriores}): \quad & d_n = d_{n-2} - (d_{n-3} - d_{n-2} q_{n-2}) q_{n-1} = \\
& \quad = d_{n-2}(1 - q_{n-2} q_{n-1}) - d_{n-3} q_{n-1} = \\
(d_{n-2} \text{ em termos dos anteriores}): \quad & d_n = (d_{n-4} - d_{n-3} q_{n-3})(1 - q_{n-2} q_{n-1}) - d_{n-3} q_{n-1} \\
& \cdots = \cdots . \\
& d_n = u\, d_0 + v\, d_1
\end{aligned}$$

Como $d_n = d$ e chegamos, num número finito de passos, a uma expressão de d_n como combinação dos inteiros $d_0 = a$ e $d_1 = b$, como queriamos. A única parte que fica por demonstrar é a existência de uma solução que verifique as desigualdades indicadas para u e v. Para isso, pode usar-se o Exercício 1.6. □

Quando o mdc se encontra num número pequeno de passos, o método indicado nesta demonstração é suficiente para determinar as soluções u e v da equação de Bézout. Por outro lado, se há muitas operações envolvidas, convém recorrermos a uma tabela para sistematizar os cálculos e evitar erros, como no seguinte exemplo.

Exemplo 1.23. Vamos encontrar o máximo divisor comum, e seguidamente resolver a respectiva equação de Bézout, para o par de inteiros $a = 711$ e $b = 132$. Primeiro o algoritmo de Euclides:

$$\begin{aligned}
711 &= 132 \cdot 5 + 51 \\
132 &= 51 \cdot 2 + 30 \\
51 &= 30 \cdot 1 + 21 \\
30 &= 21 \cdot 1 + 9 \\
21 &= 9 \cdot 2 + 3 \\
9 &= 3 \cdot 3 + 0.
\end{aligned}$$

Assim, obtemos $d = \text{mdc}(711, 132) = 3$.

Vamos escrever cada equação acima como $d_i = d_{i+1} q_{i+1} + d_{i+2}$, com i começando em zero. Podemos agora encontrar, recursivamente, os inteiros x_i e y_i que verificam a equação

$$d_i = 711\, x_i + 132\, y_i, \tag{1.2}$$

com a ajuda de uma tabela. Esta é elaborada da seguinte forma. Colocamos os d_i na primeira coluna (esquerda) e os q_i na coluna seguinte. Nas primeiras duas linhas de x_i e y_i colocamos as soluções óbvias da equação (1.2), ou seja, $x_0 = 1$, $y_0 = 0$; $x_1 = 0$, $y_1 = 1$. Seguidamente, cada par (x_i, y_i) é obtido fazendo

$$\begin{cases} x_{i+1} := & x_{i-1} - q_i x_i \\ y_{i+1} := & y_{i-1} - q_i y_i. \end{cases}$$

Obtemos então, a seguinte tabela:

i	d_i	$-q_i$	x_i	y_i
0	711		1	0
1	132	-5	0	1
2	51	-2	1	-5
3	30	-1	-2	11
4	21	-1	3	-16
5	9	-2	-5	27
6	3	-3	13	-70
7	0		-44	237

Nesta tabela, na linha i, x_{i+1} é obtido somando a x_{i-1} (2 linhas acima) o produto de $(-q_i)$ por x_i (uma linha acima), e analogamente para y_{i+1}. Finalmente, podemos escrever $d = 3 = 13 \cdot 711 - 70 \cdot 132$, que é a solução da equação de Bézout desejada.

Note-se que, continuando o mesmo método após a solução da equação $3 = 711x + 132y$, obtemos uma *representação de zero*:

$$0 = 711(-44) + 132 \cdot 237,$$

que é válida, e notamos que os coeficientes $(-44, 237)$ são precisamente, a menos de sinal, os números

$$\frac{b}{d} = \frac{132}{3} = 44, \quad \frac{a}{d} = \frac{711}{3} = 132.$$

Exercício 1.11. Mostre que o algoritmo acima termina sempre como no último exemplo. Ou seja, sendo x_{k+1}, y_{k+1} os coeficientes da representação: $d_{k+1} = 0 = a x_{k+1} + b y_{k+1}$, temos sempre $|x_{k+1}| = |b|/d$ e $|y_{k+1}| = |a|/d$, sendo $d = d_k = (a, b)$.

Consideremos agora o problema da unicidade na equação de Bézout. É fácil ver que, para $a, b \in \mathbb{Z}^\times$ e $d = (a, b)$, se temos uma solução (u, v) da equação:

$$d = a u + b v,$$

então o par $(u', v') := (u + kb, v - ka)$ é também solução, para qualquer inteiro $k \in \mathbb{Z}$. De facto, $d = a u + b v = a(u + kb) + b(v - ka)$.

Exercício 1.12. Mostre que, dada uma solução (u_0, v_0) da equação de Bézout $d = a u + b v$ então todas as soluções são da forma $(u_0 + kb,\ v_0 - kb)$ para certo $k \in \mathbb{Z}$.

Vale a pena salientar uma caso particular muito importante.

Corolário 1.24. *Se a e b são inteiros primos entre si, então podemos escrever:*

$$1 = a x + b y$$

para certos x, y com $|x| < |b|$ e $|y| < |a|$. Dada uma solução (x_0, y_0), todas as outras soluções são da forma $(x_0 + kb,\ y_0 - ka)$.

Demonstração. A existência de solução segue imediatamente do teorema anterior, pois neste caso $d = 1 = (a, b)$. A descrição de todas as soluções segue do Exercício 1.6. □

A identidade de Bézout permite-nos resolver todas as equações lineares do mesmo tipo.

Teorema 1.25. *Sejam dados inteiros não nulos a, b, c, com $d = (a, b)$. Então, a equação*

$$c = a u + b v$$

tem solução $(u_0, v_0) \in \mathbb{Z}$ se e só se $d \mid c$. Neste último caso, a solução geral *desta equação é:*

$$u = u_0 + \frac{b}{d} k, \quad v = v_0 - \frac{a}{d} k, \qquad k \in \mathbb{Z}.$$

Demonstração. Se a equação tem solução, ou seja, temos $c = a u + b v$ para certos $u, v \in \mathbb{Z}$, então $d \mid a u + b v$ (porque $d \mid a$ e $d \mid b$), ou seja, $d \mid c$. Para provar o recíproco, consideramos a

nova equação:

$$1 = \frac{a}{d}x + \frac{b}{d}y,$$

que tem solução $(x,y) \in \mathbb{Z}^2$, porque $\frac{a}{d}$ e $\frac{b}{d}$ são inteiros primos entre si (Exercício 1.5). Supondo que $d \mid c$ então existe m tal que $c = md$ pelo que

$$m = \frac{c}{d} = \frac{a}{d}mx + \frac{b}{d}my,$$

que equivale a $c = a(mx) + b(my)$, pelo que $(u_0, v_0) = m(x,y)$ é uma solução da equação original. Deixamos ao leitor a conclusão que a solução geral passa por fazer as substituições $u_0 \mapsto u_0 + \frac{b}{d}k$, $v_0 \mapsto v_0 - \frac{a}{d}k$ para $k \in \mathbb{Z}$. □

A equação de Bézout permite-nos mostrar os seguintes resultados.

Corolário 1.26. *Sejam a,b,c inteiros não nulos, com $(a,b) = (a,c) = 1$. Então $(a,bc) = 1$.*

Demonstração. Sabemos que existem inteiros u,v,s,t tais que:

$$au + bv = 1 = as + ct.$$

Multiplicando $bv = 1 - au$ por $ct = 1 - as$ obtemos $bc\,vt = (1-au)(1-as) = 1 - a(s + u - aus)$ ou, de outra forma:

$$1 = bc\,vt + a(s + u - aus).$$

Isto significa que existe solução da equação de Bézout para os números bc e a (a solução é o par: $(vt\,,\, s+u-aus)$). Assim, pelo Teorema 1.25 $d = 1$ é múltiplo de (a,bc). Ou seja, $(a,bc) = 1$ como queríamos mostrar. □

Uma propriedade fundamental dos números primos é a seguinte.

Proposição 1.27. *[Lema de Euclides] Seja p um número primo, e a,b inteiros arbitrários. Então $p \mid ab$ se e só se $p \mid a$ ou $p \mid b$.*

Demonstração. Se $p \mid a$ ou $p \mid b$, então $p \mid ab$, sendo isto uma regra geral (não é preciso que p seja primo). Vamos provar o contrarecíproco. Isto é, vamos supor que $p \nmid a$ e $p \nmid b$. Então, $(a,p) = (b,p) = 1$, pois p é primo, e a possibilidade $(a,p) = p$ foi excluída por hipótese. Então, pelo Corolário anterior, temos $(p,ab) = 1$. Novamente, porque p é primo, obtemos que $p \nmid ab$. □

1.7. **O Princípio de Indução.** O *Princípio de Indução*, às vezes também chamado *Princípio de Indução Matemática*, é um argumento utilizado, com muita frequência, na dedução de propriedades gerais dos números naturais ou inteiros. Usaremos este princípio na demonstração do Teorema Fundamental da Aritmética.

O Princípio de Indução usa a ordenação dos números inteiros introduzido na subsecção 1.2, embora seja *independente* das propriedades das relações "maior que" ou "menor que".

Notação: Dados dois conjuntos A, B, escrevemos $A \subset B$ e dizemos "A é subconjunto de B" se todo o elemento de A pertence também a B. Ou seja, se $a \in A$, então $a \in B$. Esta terminologia admite também os casos extremos: $A = B$, $A = \emptyset$.

Definição 1.28. Seja $A \subset \mathbb{Z}$ um conjunto arbitrário de números inteiros. Dizemos que A tem um elemento mínimo m, se $m \in A$ e se $m \leqslant a$ para qualquer $a \in A$.

De forma análoga, podemos definir um elemento máximo, trocando o sentido das desigualdades.

Exercício 1.29. Mostre que se $A \subset \mathbb{Z}$ tem mínimo, então ele é único.

Consideremos o seguinte axioma, chamado "Axioma da boa ordenação".

Axioma **(da Boa Ordenação)** Seja $A \subset \mathbb{N}$ um conjunto não vazio de números inteiros. Então A tem um mínimo.

Observação 1.30. Note-se que para o conjunto $\mathbb{Z}$, o mesmo princípio não é válido em geral (Exercício 1.7(1)), a não ser que adicionemos uma hipótese. Dizemos que um subconjunto $A \subset \mathbb{Z}$ é limitado inferiormente, se existe $x \in \mathbb{Z}$ tal que $x \leq a$ para qualquer $a \in A$. Em particular, qualquer conjunto com um mínimo é limitado inferiormente. Reciprocamente, se $A \subset \mathbb{Z}$ é não vazio e limitado inferiormente, então o Axioma da Boa Ordenação diz-nos que A tem um mínimo (Exercício 1.7(2)).

Exercício 1.13. (1) Dê exemplos de subconjuntos (não vazios) $A \subset \mathbb{Z}$ que não são limitados inferiormente, e que, portanto, não possuem mínimo.
(2) Mostre o "axioma da boa ordenação para $\mathbb{Z}$": Qualquer subconjunto $A \subset \mathbb{Z}$ não vazio e limitado inferiormente tem um mínimo.
(3) Enuncie um outro "axioma da boa ordenação" para $\mathbb{Z}$ e $\mathbb{N}$ envolvendo limites superiores e máximos, em lugar de limites inferiores e mínimos. Mostre que este novo axioma é equivalente ao anterior.
(4) Mostre que qualquer subconjunto *finito* de $\mathbb{Z}$ tem um mínimo e um máximo, sem usar o axioma da boa ordenação.

Embora estas propriedades dos números inteiros e dos naturais sejam intuitivas, devemos tomar consciência de que não são consequências imediatas das outras propriedades. De facto, existem conjuntos (infinitos) com as mesmas propriedades aritméticas, e as mesmas relações de ordem, que **não verificam** o axioma da boa ordenação. Como exemplo, temos o conjunto dos *números racionais*.

Exercício 1.14. Mostre que, se em lugar dos inteiros, considerarmos *números racionais*, e as mesmas definições acima, o conjunto infinito

$$A := \left\{ \frac{1}{n} : n \in \mathbb{N} \right\},$$

não tem um elemento mínimo (embora seja limitado inferiormente: $0 \leqslant a$ para todo o $a \in A$). Mostre que qualquer conjunto *finito* de númerios racionais tem um mínimo e um máximo.

Estamos agora em condições de enunciar o Princípio de Indução Matemática, e demonstrá-lo usando o axioma da boa ordenação.

Este enunciado é mais abstracto que a maioria dos teoremas que tratamos neste livro, uma vez que nele utilizamos a noção de uma *proposição arbitrária* sobre números naturais. Uma tal proposição vai ser denotada por $P(n)$, onde $n \in \mathbb{N}$. Para dar exemplos muito simples, $P(n)$ pode referir-se a uma das seguintes proposições:

(1) $P(n)$: $(n+1)^2 = n^2 + 2n + 1$,
(2) $P(n)$: $\sqrt{n} \leq 28$.
(3) $P(n)$: $\sum_{m=1}^{n}(2m-1) = n^2$.

É fácil ver que a primeira proposição é sempre válida em $\mathbb{N}$ (e é válida mesmo em $\mathbb{Z}$), enquanto que a segunda é falsa em geral, pois existem naturais cujas raízes são maiores que 28.

Vamos agora dar um exemplo de como usar o Princípio da Indução para demonstrar a validade da terceira proposição:

$$\sum_{m=1}^{n}(2m-1) = n^2,$$

para todo o natural n. Em primeiro lugar, a proposição $P(1)$ é a igualdade com $n = 1$: $\sum_{m=1}^{1}(2m-1) = 1^2$, o que facilmente se verifica: o somatório reduz-se a uma parcela. Vamos supor que $P(n)$ é verdadeira. Então, $P(n+1)$ designa a proposição

$$\sum_{m=1}^{n+1}(2m-1) = (n+1)^2.$$

Como a soma é associativa, o somatório decompõe-se num somatório de n parcelas adicionado ao último termo. Assim, obtemos:

$$\begin{aligned}\sum_{m=1}^{n+1}(2m-1) &= \left[\sum_{m=1}^{n}(2m-1)\right]+2(n+1)-1=\left[\sum_{m=1}^{n}(2m-1)\right]+2n+1= \\ &= n^2+2n+1=(n+1)^2.\end{aligned}$$

Na passagem da primeira para a segunda linha, usámos a validade de $P(n)$, e na última igualdade usamos a fórmula do binómio. Assim, vemos que a validade de $P(n)$ implica a de $P(n+1)$. Embora pareça que estamos a fazer um raciocínio circular, o Princípio de Indução Matemática diz-nos que isto basta para provar a validade de $P(n)$ para qualquer natural n.

Teorema 1.31. *(Princípio de Indução). Seja $P(n)$ uma proposição, para cada $n \in \mathbb{N}$. Para provar que $P(n)$ é verdadeira para qualquer $n \in \mathbb{N}$, basta:*

- [passo inicial] *Mostrar que $P(1)$ é válida e,*
- [passo de indução] *Mostrar que a validade de $P(n)$ implica a de $P(n+1)$, para todo $n \geq 1$.*

Demonstração. Consideremos o conjunto $A_P \subset \mathbb{N}$ dos naturais $n \in \mathbb{N}$ para os quais a proposição $P(n)$ *não é válida*:

$$A_P := \{n \in \mathbb{N} : P(n) \text{ não é válida}\} \subset \mathbb{N}.$$

Vamos supor a validade de $P(1)$ e que, sempre que $P(n)$ é veradeira, então $P(n+1)$ também o é. Seja $a \in A_P$ um elemento arbitrário. Assim, $P(a)$ não é válida. Sabemos que $a \geq 2$, pois $P(1)$ é válido ($1 \notin A_P$). Mas então, $a-1 \geq 1$ e o contrarecíproco do passo de indução, diz-nos que $P(a-1)$ também não é válido, pelo que $a-1 \in A_P$. Como $a-1 < a$, o inteiro a não é um mínimo de A_P. Assim, não há elementos mínimos em A_P. Finalmente, o axioma da boa ordenação, diz-nos então que $A_P = \emptyset$, ou seja, $P(n)$ é válida para todo o $n \in \mathbb{N}$. □

O princípio de Indução tem outras formas, que são igualmente úteis em problemas. De facto, com certas variações das hipóteses, tanto do *passo inicial* como do *passo de indução,* obtemos conclusões semelhantes. Se, por exemplo, alterarmos o passo inicial admitindo que $P(1)$ e $P(2)$ não nos interessam, mas que $P(3)$ é válido (e mantemos o passo de indução na forma $P(n)$ implica $P(n+1)$, neste caso para todo $n \geq 3$), então poderemos concluir que $P(n)$ é válido para qualquer $n \in \mathbb{N}$ com $n \geq 3$.

Mais geralmente, temos a seguinte variação, por vezes chamada *Princípio de Indução Forte*, quando é necessário distinguir do caso mais simples de indução. Este enunciado foi generalizado para o conjunto dos inteiros, uma vez que a eles também se aplica o axioma da boa ordenação.

Teorema 1.32. *(Princípio de Indução Forte) Seja $P(n)$ uma proposição que depende do inteiro $n \in \mathbb{Z}$. Se se verificarem ambas as condições:*

- [passo inicial] *$P(n_0)$ é válida,*
- [passo de indução] *A validade de todas as proposições $P(n_0), \cdots, P(n)$ implica a de $P(n+1)$, para todo $n \geq n_0$,*

Então $P(n)$ é válida para todo o $n \in \mathbb{Z}$ maior ou igual a n_0. Aqui, o inteiro n_0 é chamado a base da indução.

Embora lhe chamemos forte, pois o enunciado é aparentemente mais geral, o facto é que ambos os princípios são equivalentes, e equivalentes ao axioma da boa ordenação.

Exercício 1.15. Mostre o princípio de indução forte, a partir do Princípio de Indução (Teorema 1.31). Prove que o Princípio de Indução (e o de indução forte) é equivalente ao Axioma da Boa Ordenação.

É importante realçar a importância do passo base para a validade de uma demonstração por indução. De facto, existem proposições $P(n)$ que são falsas, mas sobre as quais se pode mostrar que $P(n)$ implica $P(n+1)$.

Exercício 1.16. Seja $P(n)$ a proposição: "n^2-3n+5 é par", com $n \in \mathbb{N}$. Mostre que a validade de $P(n)$ implica a de $P(n+1)$. Modifique $P(n)$ de forma a que se torne verdadeira.

1.8. **O teorema Fundamental da Aritmética.**

Teorema 1.33. *[Teorema Fundamental da Aritmética, versão 1]. Qualquer número natural $n \in \mathbb{N}$ se pode escrever na forma:*

$$n = p_1 \cdots p_m,$$

onde $p_1, \cdots, p_m$ são números primos (não necessariamente distintos), para certo $m \in \mathbb{N}_0$.[4] *Esta factorização é única a menos de reordenação dos factores.*

Demonstração. Esta será uma demonstração usando o Princípio de Indução Forte, Teorema 1.32 com base $n_0 = 2$. Para $n = 2$ a representação é verdadeira, pois 2 é primo. Dado $n > 2$ vamos supor, por hipótese de indução, que todo natural menor que n admite uma factorização em primos. Se n é primo, não há nada a mostrar (neste caso $m = 1$). Se n não é primo, então é composto $n = n_1 n_2$ com $n_1, n_2 \in \{2, \cdots, n-1\}$. Assim, por hipótese, temos factorizações:

$$n_1 = p_1' \cdots p_m', \qquad n_2 = p_1'' \cdots p_k'',$$

pelo que $n = p_1' \cdots p_m' p_1'' \cdots p_l''$ é a factorização pretendida para n. Falta mostrar a unicidade da representação, a menos de reordenação dos factores. Vamos supor que temos duas representações diferentes:

$$n = p_1 \cdots p_m = q_1 \cdots q_k.$$

Como p_1 é primo e $p_1 \mid n$, então $p_1 \mid q_i$ para algum q_i, com $i \in \{1, \cdots, k\}$. Mas como q_i é também primo, temos $p_1 = q_i$. Reordenando os q_i's, que é o mesmo que trocar-lhes os índices, podemos assumir que $p_1 = q_1$. Assim,

$$n = p_1 p_2 \cdots p_m = p_1 q_2 \cdots q_k.$$

Usando novamente $p_1 \mid n$ podemos dividir, e encontrar as duas factorizações:

$$n' = \frac{n}{p_1} = p_2 \cdots p_m = q_2 \cdots q_k.$$

Procedendo de igual forma, agora com p_2 obtemos $p_2 = q_2$ (com possível nova troca de índices), e assim sucessivamente, e concluímos que $p_j = q_j$ para todo $j \in \{1, \cdots, m\}$ e $m = k$. □

É fácil enunciar um resultado análogo usando uma decomposição em primos distintos, e notar que a factorização de números negativos é idêntica.

Teorema 1.34. *[Fundamental da Aritmética, versão 2] Qualquer número natural $a \in \mathbb{N}$ se pode escrever na forma*

$$a = p_1^{c_1} \cdots p_k^{c_k},$$

onde $p_1, \cdots, p_k$ são números primos distintos*, e os expoentes são naturais: $c_1, \cdots, c_k \in \mathbb{N}$ sendo $k \in \mathbb{N}_0$. Esta factorização é única a menos de reordenação dos factores.*

Observação 1.35. Se pretendermos uma decomposição de um número inteiro $a \in \mathbb{Z} \setminus \{0\}$, não nulo, mas não necessariamente positivo, poderíamos escrever

$$a = \mathrm{s}(a)\, p_1^{c_1} \cdots p_k^{c_k},$$

[4] Quando $n = 1$, a representação mantém-se válida, convencionando que um produto vazio de primos é 1.

usando a noção de sinal de a:

$$s(a) := \begin{cases} -1, & a < 0 \\ 1, & a > 0. \end{cases}$$

Note-se que, temos sempre $a = s(a)|a|$, para todo $a \in \mathbb{Z} \setminus \{0\}$.

De acordo com o Teorema Fundamental, a factorização de um dado natural n em primos está bem determinada, se soubermos os primos que nela aparecem e as respectivas potências. De facto, este teorema diz-nos que os primos que aparecem na factorização de n são:

$$P_n := \{p \text{ primo} : p \mid n\},$$

e que $P_n = \emptyset$ sse $n = 1$. Além disso, n é primo se e só se $|P_n| = 1$.

Assim, a factorização de n, é equivalente à determinação de P_n, o conjunto dos primos que aparecem na factorização de n, e, para cada primo $p \in P_n$ do expoente que tem nessa factorização:

$$e_p(n) := \max\{r \in \mathbb{N} : p^r \mid n\}.$$

Exemplo 1.36. Por exemplo, encontrar a factorização

$$693 = 3 \cdot 3 \cdot 7 \cdot 11 = 3^2 \cdot 7 \cdot 11,$$

(a primeira forma corresponde ao teorema 1.33 e a segunda ao teorema 1.34) é o mesmo que dizer que $P_{693} = \{3, 7, 11\}$ e que $e_3(693) = 2$, $e_7(693) = e_{11}(693) = 1$.

Corolário 1.37. *Seja $n = p_1^{c_1} \cdots p_k^{c_k}$ a factorização do natural n. O conjunto dos seus divisores positivos é:*

$$\mathrm{Div}(n) = \{p_1^{e_1} \cdots p_k^{e_k} : 0 \le e_j \le c_j, \text{ para todo } j\}$$

Demonstração. Seja $d \mid n$. Pelo Teorema 1.34, podemos escrever $d = q_1^{d_1} \cdots q_l^{d_l}$, onde $q_1, \cdots, q_l$ são primos. Cada um destes primos divide d, $q_i \mid d$, pelo que $q_i \mid n$. Pelo lema de Euclides, q_i divide algum dos primos p_j; mas como ambos são primos, q_i é um *igual* a um dos p_j. Desta forma, provámos que o conjunto de primos na factorização de d é um *subconjunto* dos primos na factorização de n. Assim, escrevemos $d = p_1^{e_1} \cdots p_k^{e_k}$ (os mesmos primos que na factorização de n) e vemos que a condição $d \mid n$ equivale precisamente a dizer que $e_j \in \{0, 1, \cdots, c_j\}$, para todo o j. □

Exemplo 1.38. Aplicando o corolário ao número $693 = 3^2 \cdot 7 \cdot 11$ imediatamente concluímos que:

$$\mathrm{Div}(693) = \{1, 7, 11, 7 \cdot 11, 3, 3 \cdot 7, 3 \cdot 11, 3 \cdot 7 \cdot 11, 3^2, 3^2 \cdot 7, 3^2 \cdot 11, 3^2 \cdot 7 \cdot 11\},$$

que correspondem a considetar todas as possibilidades para os expoentes dos primos envolvidos, de forma que os expoentes máximos de 3,7 e 11 sejam respectivamente, 2,1 e 1.

Uma outra consequência da demonstração anterior é o seguinte resultado.

Corolário 1.39. *Dois naturais a, b são primos entre si se e só se $P_a \cap P_b = \emptyset$.*

Dados dois inteiros a e b (não simultaneamente nulos), vamos denotar por $[a, b]$ o *menor múltiplo comum* entre eles. Existe uma reciprocidade entre divisores comuns e múltiplos comuns que podemos concretizar da seguinte forma

Proposição 1.40. *Sejam $a, b \in \mathbb{Z} \setminus \{0\}$. Então, para cada divisor d comum a a e b, o inteiro*

$$c := \frac{ab}{d}$$

é múltiplo comum a a e a b, e vice-versa (se c é múltiplo comum a a e a b, então $d = ab/c$ é um divisor comum a a e a b).

Demonstração. Se $d \mid a$ e $d \mid b$ então existem inteiros k e l tais que: $a = kd$ e $b = ld$. Assim,

$$c = \frac{ab}{d} = \frac{kdld}{d} = kld = al = bk.$$

As duas últimas expressões mostram que c é múltiplo de a e que é múltiplo de b. Para o recíproco, usa-se um método inteiramente análogo. □

Corolário 1.41. *Dados 2 inteiros $a, b \in \mathbb{Z}$, não nulos, o seu menor múltiplo comum é finito e pode determinar-se através da fórmula*

$$[a,b](a,b) = |ab|$$

Demonstração. Vamos assumir que $a, b > 0$, e mostrar que $[a,b] = ab/(a,b)$ (o caso de números inteiros não positivos, é semelhante, e deixa-se para o leitor). Pela proposição anterior, para cada divisor d, comum a a e a b, existe um múltiplo comum $c = ab/d$. Por outro lado, se $d_1 > d_2$, então:

$$c_1 := \frac{ab}{d_1} < \frac{ab}{d_2} =: c_2.$$

Assim, o maior dos divisores comuns $d = (a,b)$ dá origem ao menor múltiplo comum $[a,b] = ab/(a,b)$. □

Problemas de Revisão.

1.1 Considere as expressões $53 = 11 \cdot 5 - 2$, $53 = 10 \cdot 5 + 3$ e $53 = 11 \cdot 4 + 9$. Qual delas representa a divisão de 53 por 5? A útlima expressão representa alguma divisão?

1.2 (a) Sejam $\{1, 2, 4, 7, 8, a, b, c\}$ o conjunto dos divisores de um dado natural n. Determine n e a, b, c.
(b) Determine todos os números naturais que têm $1, 3, , 5, 6$ como divisores.

1.3 Considere números naturais a, b, c. Seja r o resto da divisão de c por a e s o resto da divisão de c por b. Supondo que $a \mid b$, qual é o resto da divisão de s por a?

1.4 Sejam $a, b \in \mathbb{N}$ e $c, d \in \mathbb{Z}$ tais que $a = bc + d$.
(a) Mostre que $(a,b) = (b,d)$.
(b) No caso em que $d = 0$, mostre que $(a,b) = b$.

1.5 Prove que para qualquer inteiro $a \in \mathbb{Z}$ temos $a - 1 \mid a^2 - 1$. Mostre, mais geralmente que $a - 1 \mid a^n - 1$ para todo $n \in \mathbb{N}$.

1.6 Prove que para quaisquer $a, b \in \mathbb{Z}$ se tem $(a, a + b) \mid b$. Mostre que dois naturais conseutivos são primos entre si.

1.7 Encontre o máximo divisor comum d, de 2163 e 910, e inteiros x, y que satisfaçam

$$d = 2163x + 910y,$$

com $0 < x < \frac{910}{d}$.

1.8 Encontre uma solução em inteiros $(x, y) \in \mathbb{Z}^2$ da equação

$$325x + 26y = 91.$$

1.9 Determine todas as soluções da equação diofantina:

$$54x + 21y = 906.$$

1.10 Sejam $a, b \in \mathbb{Z}$ não ambos nulos. O mínimo múltiplo comum de a e b é o menor natural m, tal que $a \mid m$ e $b \mid m$. O mínimo múltiplo comum, abreviadamente mmc, de a e b denota-se por $[a,b]$. Mostre que:
(a) $[a,b] = [b,a] = [|a|, |b|]$,
(b) $[ka, kb] = k[a,b]$,
(c) $(a,b) \cdot [a,b] = |ab|$.

1.11 Sejam $a_1, \cdots, a_n \in \mathbb{N}$ e $d = (a_1, \cdots, a_n)$. Prove que existem inteiros $x_1, \cdots, x_n$ tais que

$$d = x_1 a_1 + \cdots + x_n a_n.$$

1.12 Mostre que, se $n \geq 2$ e n não é primo então existe um primo p que divide n e tal que $p^2 \leq n$. Use este resultado para mostrar que 467 é primo.

1.13 Quantos zeros aparecem no extremo à direita da expansão decimal de 100! ? [Sugestão: quais as potências de 2 e de 5 na expansão de 100! em factores primos?]

1.14 Seja $k \in \mathbb{N}$. Mostre que existem k números consecutivos, nenhum dos quais é primo. [Sugestão: considere a sequência $(k+1)!+2, \cdots, (k+1)!+(k+1)$].

1.15 Mostre, por indução, que o natural $4^{2n+1} + 3^{n+2}$ é divisível por 13, para todo o $n \geq 0$.

1.16 Considere a sucessão de Fibonacci, definida por: $F_0 = 0$, $F_1 = 1$ e pela recorrência $F_{n+2} = F_{n+1} + F_n$, para $n \geq 0$. Prove, por indução:
(a) $F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$.
(b) $F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}$.

1.17 Seja P um polígono convexo. Uma diagonal de P é um segmento de recta que une dois vértices não consecutivos. Mostre por indução que, se P tem $n \geq 3$ lados, o número de diagonais de P é $\frac{1}{2}n(n-3)$.

1.18 Determine uma fórmula para a soma dos primeiros n cubos, $1^3+2^3+\cdots+n^3 = \sum_{k=1}^{n} k^3$, em função de $n \in \mathbb{N}$, e demonstre-a por indução.

1.19 Seja $\binom{n}{k} = \frac{n!}{k!(n-k!)}$ o coeficiente binomial, com $n \geq k \geq 0$ inteiros. Mostre, por indução, a igualdade:

$$\binom{2n}{n} = \frac{2^n}{n!} \prod_{k=1}^{n} (2n-1).$$

1.20 Mostre que o axioma da boa ordenação é equivalente ao princípio de indução finita (uma das implicações foi demonstrada acima) [Sugestão para a outra implicação: Considere a afirmação $P(n)$ "qualquer subconjunto de $\mathbb{N}$ com um número $\leq n$ tem um mínimo" e prove-a por indução.]

1.21 Seja $\Delta(n)$ a cardinalidade do conjunto dos divisores positivos de n. Por exemplo $\Delta(6) = 4$, uma vez que $\mathrm{Div}(6) = \{1,2,3,6\}$. Seja $n = p_1^{k_1} \cdots p_r^{k_k}$, a factorização de n em primos. Prove que $\Delta(n) = (k_1+1)\cdots(k_r+1)$.

1.22 Com a mesma notação do problema anterior, prove que $\Delta(n)$ é ímpar se e só se n é um quadrado, isto é existe $m \in \mathbb{N}$ tal que $m^2 = n$.

1.23 Considere a factorização de $n \in \mathbb{N}$ em primos não necessáriamente distintos, sendo p o menor desses primos. Mostre que o número de factores é, no máximo, $\log_p n$.

1.24 Prove que se $n \in \mathbb{N}$ não é um quadrado, então $\sqrt{n}$ é um número irracional.

1.25 Um *triplo pitagórico* é $(x,y,z) \in \mathbb{N}^3$ de tal forma que $x^2 + y^2 = z^2$.
(a) Mostre que, se $n > m > 0$ são primos entre si, com $m+n$ ímpar, então $(n^2 - m^2, 2nm, n^2+m^2)$ é um triplo pitagórico, e que $\mathrm{mdc}(n^2-m^2, 2nm, n^2+m^2) = 1$.
(b) Prove que todos os triplos pitagóricos são múltiplos da forma indicada na alínea (a), ou seja, da forma $(a(n^2-m^2), 2amn, a(n^2+m^2))$ com $a, m, n \in \mathbb{N}$ e $n > m > 0$ não ambos ímpares.

2. Números Racionais

Os números racionais são quocientes ou razões de inteiros. Como exprimem razões entre quantidades inteiras, são naturalmente usados quando se pretende comparar medições de objectos físicos ou geométricos. Estas medições são normalmente efectuadas relativamente a uma unidade básica, ou unidade padrão, a que matematicamente corresponde o número 1. Em particular, existe uma infinidade de números racionais entre 0 e 1, as chamadas fracções próprias, e qualquer racional é a soma de um inteiro com uma fracção própria.

Definição 2.1. Um número racional x é um número da forma $x = \frac{a}{b}$ onde $a \in \mathbb{Z}$ e $b \in \mathbb{N}$.

Por outras palavras, um número é x racional se existe um natural b tal que a multiplicação bx é novamente um inteiro. Assim, os números racionais incluem os números inteiros: qualquer inteiro $n \in \mathbb{Z}$ se pode escrever como $n = \frac{n}{1}$.

Tal como com os números inteiros, a importância dos números racionais deve-se muito às suas propriedades aritméticas. O método de somar, subtrair, multiplicar e dividir fracções é bem conhecido.

Assim, se $x = \frac{a}{b}$ e $y = \frac{c}{d}$ temos ($a, c \in \mathbb{Z}$ e $b, d \in \mathbb{N}$):

$$x \pm y = \frac{ad \pm cb}{bd}, \qquad xy = \frac{ac}{bd}, \qquad \text{e } x/y = \frac{x}{y} = \frac{ad}{cb}, \text{ (quando } c \neq 0).$$

Também as propriedades de ordem são bem sabidas, e tal como com os números inteiros, dizemos que $x > y$ se $ad > bc$ (na mesma notação que acima). Assim, se $x = \frac{a}{b}$ e a, b são ambos positivos, então x é positivo. Se $a < 0 < b$ ou $b < 0 < a$ então x é negativo; quando $a = 0$, temos $x = 0$.

Notação: O conjunto dos números naturais designa-se por $\mathbb{Q}$. Temos então a sequência de inclusões: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$. O conjunto dos racionais positivos denota-se por $\mathbb{Q}_+$, pelo que $\mathbb{N} \subset \mathbb{Q}_+$.

2.1. **Fracções irredutíveis e fracções próprias.** A representação de um número racional como o quociente de dois inteiros **não é única**. De facto, temos por exemplo: $\frac{2}{5} = \frac{-4}{-10} = \frac{8}{20}$. De forma a encontrar uma representação o mais simples possível, fazemos a seguinte definição.

Definição 2.2. Quando um número racional x se encontra escrito como $x = \frac{a}{b}$ onde a e $b \neq 0$ são inteiros *primos entre si*, dizemos que está escrito na forma irredutível e usaremos a notação $x = \left\langle \frac{a}{b} \right\rangle$. Também se diz que $\left\langle \frac{a}{b} \right\rangle$ é uma fracção irredutível.

Recorde-se que a e b são primos entre si se não existe nenhum número primo que divide ambos (Proposição 1.19). Pode provar-se que qualquer número racional pode ser escrito como fracção irredutível, e que, além disso, a fracção irredutível de um certo racional **já é única** (a menos de sinal).

Proposição 2.3. *Qualquer número racional, não nulo, admite uma representação em fracção irredutível. Se*

$$x = \left\langle \frac{a}{b} \right\rangle = \left\langle \frac{a'}{b'} \right\rangle$$

(ou seja as fracções acima são irredutíveis, pelo que $(a, b) = (a', b') = 1$*), então* $a' = a$ *e* $b' = b$ *ou* $a' = -a$ *e* $b' = -b$.

Demonstração. Seja $x = \frac{a}{b}$ um número racional com a e b não necessariamente primos entre si. Então $b \neq 0$. Podemos supor que x é positivo (o caso em que x é negativo trata-se da mesma forma), e que $a, b > 0$. Seja $d = \text{mdc}(a, b)$ e sejam:

$$a' = \frac{a}{d}, \qquad b' = \frac{b}{d},$$

que são números naturais. Então $x = \frac{a}{b} = \frac{a'}{b'}$ e

$$(a', b') = \left(\frac{a}{(a,b)}, \frac{b}{(a,b)} \right) = \frac{(a,b)}{(a,b)} = 1.$$

Assim, podemos escrever $x = \left\langle \frac{a}{b} \right\rangle$ porque esta fracção é irredutível. Para provar a unicidade, novamente podemos assumir a, b, a', b' positivos. A igualdade $\frac{a}{a'} = \frac{b}{b'}$ implica a existência de $m \in \mathbb{N}$ tal que $m = ab' = a'b$. Como ambas as fracções são irredutíveis, temos $(a, b) = (a', b') =$

1. Então

$$a = a(a',b') = (aa', ab') = (aa', a'b) = a'(a,b) = a'.$$

Logo, $m = ab' = ab$ e pela lei do corte, $b = b'$. □

Exercício 2.1. Recorde que P_n é o conjunto dos primos que dividem n. Sejam $a, b \in \mathbb{N}$. Mostre que se $P_a \cap P_b$ é vazio se e só se a/b é uma fracção irredutível.

Qualquer racional é a soma de um inteiro com um número racional entre 0 e 1.

Definição 2.4. Um número racional $x \in \mathbb{Q}$ (ou uma fracção que o representa) diz-se **próprio** se está entre 0 e 1. Mais precisamente, se $0 \leq x < 1$.

Desta forma, uma fracção própria é um racional da forma $x = \frac{a}{b}$ com $0 \leq a < b$.

Como é bem sabido, qualquer número racional que não seja inteiro está compreendido entre 2 inteiros consecutivos. Por exemplo, $x = \frac{78}{31}$ está entre 2 e 3 porque

$$2 \cdot 31 < 78 < 3 \cdot 31.$$

Proposição 2.5. *Qualquer número racional é a soma de um número inteiro com um racional próprio, e esta decomposição é única. Mais precisamente, dado $x \in \mathbb{Q}$, existem $n, r, b \in \mathbb{Z}$, $b \neq 0$ tais que:*

$$x = n + \frac{r}{b},$$

e estes são únicos, se exigirmos a condição $b > a \geq 0$.

Demonstração. Seja $x = \frac{a}{b} \in \mathbb{Q}$ positivo (o caso de x negativo é análogo). Então, $a, b \in \mathbb{Z}$ e podemos supor $b > 0$, $a \geq 0$.

Se $0 \leq a < b$, x é uma fracção própria, pelo que $x = 0 + x$ é a decomposição pretendida ($n = 0$ e $r = a$). Caso contrário, temos $0 < b \leq a$. Fazendo a divisão com resto, de a por b obtemos $a = bq + r$, para certo quociente $q \geq 1$ e $r \in \{0, 1, \cdots, b-1\}$. Logo

$$x = \frac{a}{b} = \frac{bq + r}{b} = q + \frac{r}{b},$$

é a decomposição pretendida, porque $q \in \mathbb{Z}$ e $\frac{r}{b}$ é uma fracção própria, uma vez que $0 \leq r < b$. □

Notação: Quando um racional x se escreve como $n + y$ onde n é um inteiro e y um racional próprio, n chama-se a *parte inteira* de x, e y chama-se a *parte própria* de x. Escrevemos $n = \lfloor x \rfloor$ e $y = /x\backslash$.

Exemplo 2.6. Seja $x = \frac{78}{31}$. Então $\frac{78}{31} = 2 + \frac{16}{31}$, pelo que $2 = \left\lfloor \frac{78}{31} \right\rfloor$ e $\frac{16}{31} = \left/ \frac{78}{31} \right\backslash$.

2.2. **Representações em bases.** A representação de um número em produto de primos, embora muito conveniente para estudar múltiplos e divisores, não é útil para realizar operações aritméticas básicas. De facto, os algoritmos de adição, subtracção, multiplicação e divisão que aprendemos, são baseados na representação decimal de um número inteiro.

Quando escrevemos $n = 47093$ na *base decimal*, isto significa que os algarismos $4, 7, 0, 9$ e 3 correspondem, cada um deles, a uma potência de 10. Assim, começando da direita para a esquerda: 3 é o algarismo das unidades, ou seja da potência $10^0 = 1$; 9 é o algarismo das dezenas, ou seja $10^1 = 10$; zero representa as centenas, 10^2; 7 é o número de milhares, 10^3, e finalmente 4 é o número de dezenas de milhar, a quarta potência de 10. Sucintamente, temos:

$$n = 47093 = 4 \cdot 10^4 + 7 \cdot 10^3 + 0 \cdot 10^2 + 9 \cdot 10^1 + 3 \cdot 10^0.$$

Não há justificação especial, do ponto de vista teórico, para considerarmos a base 10. As razões para tal, são de índole prática: é um número não muito pequeno nem muito grande. De facto, uma base muito pequena, como a base 2, também designada *base binária*, é muito

usada nos computadores, mas são precisos mais de 10 algarismos para representar números maiores que $1024 = 2^{10}$, por exemplo, pelo que esta base não é prática para o dia a dia. Se a base fosse muito grande, como o número 60, por exemplo, seria muito difícil decorar uma tabuada, consistindo em essencialmente $\frac{60 \cdot 59}{2}$ multiplicações diferentes.

Além disso, 10 é também o número de dedos nas mãos, pelo que ensinar às crianças a contar pelos dedos é uma tarefa realizável com sucesso.

Definição 2.7. Seja $m \in \mathbb{N}$, $m > 1$. A representação de um natural n na base m é uma expressão da forma:

$$n = a_k m^k + a_{k-1} m^{k-1} + \cdots + a_1 m + a_0,$$

onde $k \in \mathbb{N}_0$, $a_k \neq 0$ e $a_j \in \{0, \cdots, m-1\}$. Dizemos que n tem $k+1$ algarismos na base m, e escrevemos abreviadamente:

$$n = [a_k a_{k-1} \cdots a_1 a_0]_m.$$

A representação de números naturais em bases é biunívoca, ou seja, a duas representações distintas correspondem números distintos e a números distintos correspondem representações (ou seja, coeficientes $a_0, \cdots, a_k$) distintas.

Também podemos representar um número racional em qualquer base $m > 1$. Por exemplo temos:

$$\frac{159}{8} = 19{,}875.$$

Isto significa que

$$\frac{15}{8} = 1 \cdot 10^1 + 9 \cdot 10^0 + 8 \cdot 10^{-1} + 7 \cdot 10^{-2} + 5 \cdot 10^{-3}.$$

Assim, os números racionais têm representações em que aparecem as potências negativas da base. No entanto, um problema que surge com esta representação são as chamadas dízimas infinitas. De facto, por exemplo

$$\frac{159}{7} = 22{,}714285(714285)\cdots,$$

pelo que a representação de números racionais em bases não é sempre finita. Acima, usámos os parêntesis para indicar que o conjunto de algarismos 714285 repete-se infinitas vezes.

Definição 2.8. Seja $m \in \mathbb{N}$, $m > 1$. A representação de um número racional $x \in \mathbb{Q}$ na base m é uma expressão da forma

$$x = a_k m^k + \cdots + a_1 m + a_0 + a_{-1} m^{-1} + \cdots + a_{-j} m^{-j} + \cdots = \sum_{j=-\infty}^{k} a_j m^j,$$

onde $k \in \mathbb{Z}$, $a_k \neq 0$ e $a_j \in \{0, \cdots, m-1\}$ para todo o $j \in \mathbb{Z}$ com $j \leq k$. Os coeficientes a_k são ainda chamados algarismos, e pode haver um número infinito de algarismos não nulos, para as potências negativas de m.

Note-se que a representação decimal dos números racionais, não é sempre única (embora seja única no caso em que a séria acima é finita). De facto, por exemplo:

$$0{,}239(9) = 0{,}24 = \frac{24}{100}.$$

Proposição 2.9. *Seja $x = \sum_{j=-\infty}^{k} a_j m^j$ a representação de x na base m, e seja k o menor inteiro tal que $a_j = 0$ para todo o $j > k$. Então x é próprio se e só se k é negativo.*

Demonstração. ... □

Problemas.

2.1 Escreva os números 37 e 73 na base 2.

2.2 Considere os naturais $a = 10101$, $b = 1111$, escritos na base 2. Determine $a+b$ na base 2 e na base 10.
2.3 Escreva em notação decimal as fracções $\frac{53}{16}$, $\frac{1}{7}$.
2.4 Escreva na forma de fracção irredutível os seguintes números racionais: 0,36; 3,235; 0,(23); 0,(9).

3. Números Modulares

Para cada número natural $m \in \mathbb{N}$, denominado o *módulo*, existe um conjunto de números modulares. Estes são muitas vezes usados em situações onde certas quantidades se repetem de forma regular.

Por exemplo, se forem 15 horas da tarde, e a Alice disser que vai viajar daqui a 18 horas, isso significa que prevê partir às $15+18-24 = 9$ horas da manhã, do dia seguinte. Desta forma, para o módulo $m = 24$, dizemos que

$$15 + 18 \equiv 9 \bmod 24. \tag{3.1}$$

De facto, contando as horas de 0 a 23, como na Europa continental, depois da hora 23 vem a hora 24 (meia-noite) que corresponde à hora 0 de um novo dia. Assim, o módulo 24 está bem adaptado a operações relativas às horas de um determinado dia, que está subentendido.

De igual forma, podemos associar a cada dia da semana um certo número, por exemplo, domingo poderá ser o dia 1, segunda-feira o dia 2, e assim por diante, até sábado, o dia 7. Naturalmente, esta associação pode ser feita de várias formas diferentes: podemos começar com o zero, e terminar com o 6. O importante é que, tal como os dias da semana, os números modulares repetem-se após adicionarmos várias vezes uma unidade, o que não acontece com os números inteiros. Podemos ter em mente estes exemplos, ao trabalhar com números modulares.

3.1. Congruências módulo m.

Para ser mais preciso, introduzimos a noção de *congruência*, definida no conjunto dos números inteiros.

Definição 3.1. Seja $m \in \mathbb{N}$ um natural fixo. Definimos em $\mathbb{Z}$ a seguinte relação, chamada *congruência módulo* m. Dizemos que a e b são congruentes módulo m, e escrevemos

$$a \equiv b \bmod m$$

se m divide $a-b$, ou seja, se $a-b$ é múltiplo de m, ou $b = a + km$ para certo inteiro $k \in \mathbb{Z}$.

Exemplo 3.2. (1) Seja $m = 18$. Temos $45 \equiv 81 \bmod 18$, uma vez que $81 - 45 = 2 \cdot 18$.
(2) Com $m = 39$, temos $38 \equiv -1 \bmod 39$, $37 \equiv -2 \bmod 39$, etc. Em geral $39 - a \equiv -a \bmod 39$ para $a \in \mathbb{Z}$.
(3) Podemos *somar* congruências da seguinte forma. Se $a \equiv 2 \bmod 23$ e $b \equiv 5 \bmod 23$, então $a + b \equiv 7 \bmod 23$. Isto ocorre porque $a - 2 = 23k$ e $b - 5 = 23l$ para certos inteiros k, l. Então $a + b - 7 = 23(k + l)$.

Proposição 3.3. *Seja $m \in \mathbb{N}$ e $a \in \mathbb{Z}$. Então existe um único $r \in \{0, 1, \cdots, m-1\}$ tal que*

$$a \equiv r \bmod m.$$

Demonstração. Dividindo a por m temos $a = qm + r$ com $r \in \{0, 1 \cdots, m-1\}$. Logo, $a - r = qm$ o que nos diz que $a \equiv r \bmod m$. A unicidade de r reflete a unicidade do resto na divisão inteira. □

Assim, dois inteiros são congruentes módulo m precisamente quando as suas divisões por m têm o mesmo resto.

Exercício 3.1. Mostre que $a \equiv b \bmod m$ se e só se a divisão de a por m, tem o mesmo resto que a divisão de b por m. Em particular, $a \equiv 0 \bmod m$ se e só se a é múltiplo de m.

Para qualquer módulo m, a congruência módulo m é uma *relação de equivalência*. Por outras palavras, verificam-se as seguintes propriedades.

Proposição 3.4. *Seja $m \in \mathbb{N}$ um natural, e a, b, c números inteiros. Temos:*

- (Reflexividade) $a \equiv a \bmod m$
- (Simetria) *Se* $a \equiv b \bmod m$, *então* $b \equiv a \bmod m$
- (Transitividade) *Se* $a \equiv b \bmod m$ *e* $b \equiv c \bmod m$, *então* $a \equiv c \bmod m$

Demonstração. Estas propriedades seguem directamente das da divisibilidade. Como m divide $a - a = 0$, temos a reflexividade. Como $m \mid (a-b)$ equivale a $m \mid (b-a)$, temos a simetria, e finalmente, como $m \mid (a-b)$ e $m \mid (b-c)$, existem inteiros s e t tais que $b = a + sm$, $c = b + tm$. Obtemos então $c = a + (s+t)m$, o que significa que $a \equiv c \bmod m$. □

Um caso particular da noção de congruência, que é constantemente utilizado na prática, é a congruência módulo 2. Neste caso, com $m = 2$, dois números inteiros são congruentes módulo 2 se e só se têm a mesma *paridade*.

Exercício 3.2. Seja $a \in \mathbb{Z}$. Mostre que a é par se e só se $a \equiv 0 \bmod 2$ e que a é ímpar se e só se $a \equiv 1 \bmod 2$.

Outro exemplo muito comum é relativo ao módulo $m = 10$. Seja $a \in \mathbb{N}$ um natural escrito como $a = [a_n a_{n-1} \cdots a_0]_{10}$ na base 10. Então, $a_i \in \{0, 1, \cdots, 9\}$ para qualquer i, e a_0 é o *algarismo das unidades*.

Exercício 3.3. Mostre que, com a notação acima, $a \equiv a_0 \bmod 10$.

Por vezes, as congruências são também úteis como teste de divisibilidade. Por exemplo, para testar se um natural é múltiplo de 3, usamos normalmente o seguinte teste.

Exercício 3.4. Seja novamente $a \in \mathbb{N}$ o natural $a = [a_n a_{n-1} \cdots a_0]_{10}$ na base 10. (a) Mostre que $a \equiv 0 \bmod 3$ se e só se $a_n + a_{n-1} + \cdots + a_1 + a_0 \equiv 0 \bmod 3$. (b) verifique se 613425 é múltiplo de 3.

3.2. **O conjunto (anel) $\mathbb{Z}_m$.** As relações de congruência levam naturalmente à definição de *números modulares*. De forma abstracta, podemos dizer que um número modular é uma *classe de congruência módulo m*, no seguinte sentido.

Vamos considerar, por exemplo, o módulo $m = 3$. Podemos dividir o conjunto dos inteiros $\mathbb{Z}$, em 3 subconjuntos disjuntos, chamados *classes de congruência módulo 3*:

$$\begin{aligned} \underline{0}_3 : &= \{\cdots, -6, -3, 0, 3, 6, \cdots\} \\ \underline{1}_3 : &= \{\cdots, -5, -2, 1, 4, 7, \cdots\} \\ \underline{2}_3 : &= \{\cdots, -4, -1, 2, 5, 8, \cdots\}. \end{aligned}$$

Na lista acima, o primeiro conjunto tem todos os inteiros que são congruentes com 0 módulo 3 (e tem apenas estes inteiros), o segundo contém os que são congruentes com 1, ou seja, dão resto 1 quando divididos por 3. E no terceiro, temos os inteiros que são $\equiv 2 \bmod 3$. Como é fácil de ver, o conjunto $\mathbb{Z}$ é a união disjunta destas classes:[5]

$$\mathbb{Z} = \underline{0}_3 \sqcup \underline{1}_3 \sqcup \underline{2}_3,$$

De facto, qualquer inteiro é congruente com 0,1 ou 2 (mod 3), e não pode estar em duas destas classes simultaneamente. Além disso, por exemplo:

$$\underline{1}_3 = \underline{4}_3 = \underline{7}_3 = \cdots,$$

[5] Usamos a notação $A \sqcup B$ para denotar a união $A \cup B$ quando é *disjunta*, ou seja, quando $A \cap B = \emptyset$. Mais geralmente, $A_1 \sqcup A_2 \sqcup \cdots \sqcup A_n$ denota a união $A_1 \cup \cdots \cup A_n$, dos conjuntos A_i, $i = 1, \cdots, n$, quando qualquer intersecção de dois destes conjuntos distintos é vazia: $A_i \cap A_j = \emptyset$ para $i \neq j \in \{1, \cdots, n\}$.

como subconjuntos de $\mathbb{Z}$. Mais geralmente $\underline{a+3k}_3 = \underline{a}_3$ para quaiquer $a, k \in \mathbb{Z}$. Ou seja, $\underline{a}_3 = \underline{b}_3$ se e só se $a \equiv b \bmod 3$.

Nota-se também que se somarmos um elemento da classe $\underline{0}_3$ com um da classe $\underline{2}_3$ obtemos um elemento de $\underline{2}_3$. De facto, se $x \in \underline{a}_3$ e $y \in \underline{b}_3$ então $x+y \in \underline{a+b}_3$ e $xy \in \underline{ab}_3$, como facilmente se verifica.

Para todos os módulos m, ocorre uma situação semelhante.

Proposição 3.5. *Seja $m \in \mathbb{N}$ um natural. Temos:*
(a) $\mathbb{Z} = \underline{0}_m \sqcup \underline{1}_m \sqcup \cdots \sqcup \underline{m-1}_m$,
(b) $\underline{a}_m = \underline{b}_m$ se e só se $a \equiv b \bmod m$.
(c) Se $x \in \underline{a}_m$ e $y \in \underline{b}_m$, então $x+y \in \underline{a+b}_m$ e $xy \in \underline{ab}_m$.

Demonstração. Deixada ao leitor. □

Esta proposição motiva a seguinte definição.

Definição 3.6. Seja $m \in \mathbb{N}$ um natural. O conjunto dos inteiros módulo m é o conjunto das classes de congruência módulo m:

$$\mathbb{Z}_m := \{\underline{0}_m, \underline{1}_m, \cdots, \underline{m-1}_m\}.$$

Assim, $\mathbb{Z}_m$ tem exactamente m elementos. A soma, a diferença e o produto de classes de congruência em $\mathbb{Z}_m$ são definidos por:

$$\underline{a}_m \pm \underline{b}_m := \underline{a \pm b}_m, \qquad \underline{a}_m \cdot \underline{b}_m := \underline{ab}_m.$$

Convém verificar que estas operações estão bem definidas.

Exercício 3.5. Mostre que a soma e o produto em $\mathbb{Z}_m$ estão bem definidos. Isto é, se $\underline{a}_m = \underline{a'}_m$ então $\underline{a+b}_m = \underline{a'+b}_m$ e $\underline{ab}_m = \underline{a'b}_m$ para todos os $a, a', b \in \mathbb{Z}$.

Estas propriedades fazem com que não exista problema em usar a mesma notação tanto para os números modulares como para os inteiros. De facto, podemos pensar em $\mathbb{Z}_m$ como o conjunto finito:

$$\mathbb{Z}_m \quad \longleftrightarrow \quad \{0, 1, \cdots, m-1\},$$

e, em $\mathbb{Z}_m$, podemos fazer as operações de soma, diferença e produto de classes de congruência da mesma forma que em $\mathbb{Z}$, como fizémos na equação (3.1). Como exemplo, abaixo temos algumas tabelas de adição e multiplicação em $\mathbb{Z}_4$ e $\mathbb{Z}_7$, onde, para simplificar a notação, escrevemos cada classe simplesmente como a em vez de $\underline{a}_4$ ou $\underline{a}_7$:

$\mathbb{Z}_4, +$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_4, \times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}_7, \times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1.

Como patente nestes exemplos, as operações de adição, subtracção e multiplicação de classes de congruência módulo m verificam as mesmas propriedades que as correspondentes operações em $\mathbb{Z}$. De facto: a soma e o produto em $\mathbb{Z}_m$ são comutativos e associativos, o produto é distributivo em relação à soma e à subtracção; existe um elemento neutro da soma e do produto, e o zero é elemento absorvente do produto.

Há, no entanto, uma diferença fundamental: Em geral, a **lei do corte não é válida** (embora permaneça válida nalguns casos). Por exemplo, em $\mathbb{Z}$, a expressão $2a = 2b$ implica $a = b$.

Mas, se considarmos a mesma expressão $2a = 2b$ em $\mathbb{Z}_4$, temos aqui duas hipóteses: $a = b$ ou $a = 3b$. De facto, se $a = 3b$ temos $2 \cdot 3 \cdot b = 2 \cdot b$ o que é válido, uma vez que $\underline{2}_4 \cdot \underline{3}_4 = \underline{2}_4$ em $\mathbb{Z}_4$ (veja a tabela acima).

3.3. **Aritmética modular.** A aritmética modular é o estudo da soma, subtracção, produto e divisão no conjunto dos números modulares $\mathbb{Z}_m$, ou seja, das classes de congruência módulo m, como definido na subsecção anterior.

Já vimos que isto equivale a fazer operações, módulo m, no conjunto $\mathbb{Z}$, de todos os inteiros (Proposição 3.5). Como trabalhar com inteiros é bastante conveniente, vamos continuar neste contexto, por ora. Podemos verificar o seguinte.

Proposição 3.7. *Sejam $m, n \in \mathbb{N}$ e $a, b, c, d \in \mathbb{Z}$. Então:*

(1) $a \equiv b \bmod m$ se e só se $a + c \equiv b + c \bmod m$
(2) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a + c \equiv b + d \bmod m$ e $ac \equiv bd \bmod m$
(3) Se $a \equiv b \bmod m$, então $a^k \equiv b^k \bmod m$, para qualquer $k \in \mathbb{N}$.
(4) Se $n \mid m$ e $a \equiv b \bmod m$ então $a \equiv b \bmod n$.
(5) Se $a \equiv b \bmod m$ e $d = mdc(a, b, m)$ então $\frac{a}{d} \equiv \frac{b}{d} \bmod \frac{m}{d}$.

Demonstração. (1) Basta ver que $m \mid (a - b)$ equivale a $m \mid (a + c - (b + c))$. (2) Se $m \mid (a - b)$ e $m \mid (c - d)$ então $m \mid (a + c - (b + d))$; por outro lado, existem inteiros k e l tais que $b = a + km$ e $d = c + lm$, pelo que $bd = (a + km)(c + lm) = ac + (kc + al)m + klm^2$ o que implica que $m \mid (ac - bd)$. (3) Basta usar a propriedade multiplicativa em (2) um número k de vezes: $a \equiv b \bmod m$ implica $a \cdot a \equiv b \cdot b \bmod m$, etc. (4) Se $m \mid (a - b)$ e $n \mid m$, então $n \mid (a - b)$. (5) Se $m \mid (a - b)$ e $d = \text{mdc}(a, b, m)$ então $\frac{m}{d} \mid \frac{1}{d}(a - b)$. □

Estas propriedades são muito úteis na prática e simplificam muitos cálculos.

Exercício 3.6. Seja $f : \mathbb{Z} \to \mathbb{Z}$ dado por $f(x) = x^2 + x + 1$. Mostre que $f(x) \equiv 0$ ou $f(x) \equiv 1 \bmod 3$.

Uma simples aplicação da aritmética modular são os critérios para quadrados.

Proposição 3.8. *Seja n um quadrado. Então $n \equiv 0 \bmod 4$ ou $n \equiv 1 \bmod 4$.*

Demonstração. Seja $n = m^2$, $m \in \mathbb{N}$, e seja $r \in \{0, 1, 2, 3\}$ o resto da divisão de m por 4. Por definição $m \equiv r \bmod 4$. Assim, $m^2 = r^2 \bmod 4$, pela aplicação da Proposição 3.7(3). Mas os possíveis valores de r^2 estão dados na tabela multiplicativa de $\mathbb{Z}_4$. De facto, $0^2 \equiv 2^2 \equiv 0 \bmod 4$ e $1^2 \equiv 3^2 \equiv 1 \bmod 4$. Assim $n = m^2$ só pode ser congruente com 0 ou 1, módulo 4. □

A técnica usada acima pode ser chamada de *"redução módulo m"*: Temos uma igualdade para inteiros, e dessa igualdade obtemos uma outra igualdade para números modulares, ou seja, para classes de congruência módulo m.

Exemplo 3.9. Mostre que, se n é quadrado, $n \equiv r \bmod 7$ onde $r \in \{0, 1, 2, 4\}$.

Observação 3.10. A Proposição 3.7(3) diz-nos que $a \equiv b \bmod m$ implica $a^k \equiv b^k, \bmod m$, para qualquer expoente positivo $k \in \mathbb{N}$. No entanto, *não podemos aplicar congruências aos expoentes*, de forma directa. Por exemplo $2^8 = 256$ não é congruente com $2^3 = 8$ módulo 5, como se pode verficar, apesar de $8 \equiv 3 \bmod 5$.

3.4. **Invertibilidade módulo m.** Vamos agora analisar em mais detalhe a lei do corte e a noção de inverso módulo m.

Definição 3.11. Diz-se que $a \in \mathbb{Z}$ é invertível módulo m, se existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \bmod m$. Neste caso escrevemos $a^{-1} \equiv b \bmod m$.

Proposição 3.12. *Um elemento $a \in \mathbb{Z}$ é invertível módulo m se e só se $(a, m) = 1$. O inverso é único módulo m.*

Demonstração. Se $(a,m)=1$, a identidade de Bézout diz-nos que existem $x,y\in\mathbb{Z}$ tais que $ax+my=1$. Reduzindo a equação módulo m obtemos

$$ax\equiv 1 \bmod m,$$

pelo que x é um inverso de a, $\bmod m$. Sabemos que as várias soluções são da forma $(x+km, y-ka)$, para $k\in\mathbb{Z}$. Como $x\equiv x+km \bmod m$ vemos que x é o *único* inverso módulo m. Reciprocamente, se $ax\equiv 1 \bmod m$ então $ax-1\equiv 0 \bmod m$ pelo que $ax-1=my$ para certo y, o que nos diz que $(a,m)=1$, pela identidade de Bézout. □

Proposição 3.13. *Seja p um número primo. Então, qualquer inteiro $a\in\mathbb{Z}$ que não seja múltiplo de p é invertível módulo p. Da mesma forma, a lei do corte é válida em $\mathbb{Z}_p$.*

Demonstração. Deixa-se como exercício. □

Para módulos que não são primos, há uma generalização desta Proposição que é muito útil na resolução de equações modulares.

Teorema 3.14. *Sejam $a,b\in\mathbb{Z}$ inteiros invertíveis módulo m. Então,*
(1) ab é invertível módulo m.
(2) Se $ax\equiv 0 \bmod m$ então $x\equiv 0 \bmod m$.
(3) A congruência $ac\equiv ad \bmod m$, para certos $c,d\in\mathbb{Z}$ é equivalente à congruência $c\equiv d \bmod m$.

Demonstração. (1) Se $(m,a)=(m,b)=1$ então $(m,ab)=1$, pelo Corolário 1.26. Como o (2) é um caso particular de (3), com $d=0$, mostramos este. Para $a,c,d\in\mathbb{Z}$ quaisquer, a expressão $c\equiv d \bmod m$ implica $ac\equiv ad \bmod m$ (mesmo com a não invertível). Reciprocamente, partindo de $ac\equiv ad \bmod m$, e sendo a invertível, com inverso a^{-1} obtemos:

$$a^{-1}ac\equiv a^{-1}ad \bmod m,$$

que equivale a $c\equiv d \bmod m$, como queriamos provar. □

3.5. **Invertibilidade em $\mathbb{Z}_m$ e a função totiente.** O item (1) do teorema acima mostra que o conjunto dos números inteiros invertíveis módulo m é preservado pela multiplicação, e portanto tem a estrutura de *grupo*. Dada a equivalência entre operações com inteiros módulo m, e operações com classes de congruência para o mesmo módulo, podemos concluir que o conjunto das classes de congruência invertíveis módulo m forma um grupo.

Este grupo denota-se por

$$\mathbb{Z}_m^\times := \{\underline{a}_m\in\mathbb{Z}_m \,:\, (a,m)=1\},$$

e chama-se o grupo dos *números modulares invertíveis módulo m,* ou simplesmente, *os invertíveis módulo m*. Um problema interessante e útil, é o cálculo do cardinal de $\mathbb{Z}_m^\times$, isto é, do número de elementos invertíveis em cada $\mathbb{Z}_m$.

A função *totiente de Euler* faz precisamente isso: fornece, para cada m, o número de inteiros, de 1 a m, que são invertíveis módulo m. De agora em diante, sendo $n\in\mathbb{N}$, usamos as notações:

$$[n]:=\{1,\cdots,n\},\qquad [n]_0:=\{0,1,\cdots,n\},$$

para estes conjuntos de números consecutivos, com cardinais n e $n+1$, respectivamente.

Definição 3.15. A função totiente de Euler é a função $\varphi:\mathbb{N}\to\mathbb{N}$ definida por:

$$\varphi(n)=\left|\mathbb{Z}_m^\times\right|=|\{x\in[n] : (x,n)=1\}|,$$

ou seja $\varphi(n)$ é o *número de naturais entre 1 e n que são primos com n*.

Observação 3.16. Note-se que a igualdade na definição decorre da Proposição 3.12: o conjunto dos números inteiros, de 0 a $m-1$ que são primos com m (que tem o mesmo cardinal que o conjunto dos números inteiros, de 1 a m que são primos com m) é bijectivo ao conjunto de elementos invertíveis em $\mathbb{Z}_m$.

Exemplo 3.17. Seja $n = 45 = 3^2 \cdot 5$. Assim, os divisores próprios de n são $\{3,5,9,15\}$. Assim, todos os múltiplos destes não são primos com n. Usando o crivo, obtemos o conjunto de números que são primos com 45: $\{2,4,7,8,11,14,16,17,19,22,23,26,28,31,32,34,37,38,41,43,44\}$. Este conjunto tem cardinal 21, pelo que $\varphi(45) = 45 - 21 = 24$.

Como vemos, seria muito útil ter uma fórmula directa para calcular $\varphi(n)$ para qualquer n, de acordo a sua factorização em números primos. Este é um importante resultado de Euler que deduzimos agora.Este problema foi resolvido por Leonard Euler, que introduziu a famosa *função totiente*, também designada a função φ de Euler. Antes de abordá-lo, no capítulo 4, vejamos como resolver equações lineares em $\mathbb{Z}_m$.

3.6. **A equação linear.** A equação para o inverso de $a \in \mathbb{Z}$ módulo m ($ax \equiv 1 \bmod m$) é um caso particular de uma equação linear da forma $ax \equiv b \bmod m$. Vamos exemplificar a resolução de uma tal equação.

Exemplo 3.18. Vejamos como resolver a equação $15x = 21 \bmod 72$. O máximo divisor comum entre 15, 21 e 72 é 3. Assim, veremos que existem 3 soluções distintas módulo 72. Podemos dividir toda a equação por 3, (Proposição 3.7(5)) e obtemos a equação auxiliar:

$$5x \equiv 7 \bmod 24.$$

Agora temos $(5,24) = 1$ pelo que 5 é invertível módulo 24. De facto $5 \cdot 5 = 25 \equiv 1 \bmod 24$, e portanto $5^{-1} \equiv 5 \bmod 24$. A solução da equação auxiliar é então

$$x \equiv 5^{-1} \cdot 7 \equiv 5 \cdot 7 = 35 \equiv 11 \bmod 24.$$

Assim, $x \equiv 11 \bmod 72$ é também uma solução da equação inicial. As outras são:

$$x \equiv 11 + 24k \bmod 72, \quad k = 0,1,2.$$

De facto, a expressão acima é a solução geral em $\mathbb{Z}$ (com $k \in \mathbb{Z}$). No entanto, basta $k = 0,1,2$ para obter soluções módulo 72, porque com $k = 3$ vem $24 \cdot 3 = 72$ e a classe de congruência módulo 72 obtida será a mesma que com $k = 0$. Para outros valores de k passa-se o mesmo.

Teorema 3.19. *Sejam dados $m \in \mathbb{N}$ e $a, b \in \mathbb{Z}$. Seja $d = (a,m)$.*

(1) A equação

$$ax \equiv b \bmod m$$

tem solução se e só se $d \mid b$.

(2) A solução existe e é única (módulo m) quando $d = 1$. É dada por $x_0 \equiv a^{-1}b \bmod m$ onde a^{-1} é o inverso de a módulo m.

(3) No caso $d \neq 1$ e $d \mid b$, a equação pode ser resolvida dividindo primeiro por d, ou seja, resolvendo a ***equação reduzida:***

$$a'x \equiv b' \bmod m' \tag{3.2}$$

sendo $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, $m' = \frac{m}{d}$, e a solução geral é

$$x = x_0 + km' \bmod m,$$

com $x_0 \equiv (a')^{-1}b' \bmod m'$ (solução da equação (3.2)) e $k \in \{0,1,\cdots,d-1\}$.

Demonstração. Se $d = (a,m)$ divide b, sabemos que existem inteiros x, y tais que

$$ax + my = b,$$

e a solução geral para x é $x = x_0 + k\frac{m}{d}$, $k \in \mathbb{Z}$ onde x_0 é uma solução particular (obtida por exemplo, pelo algoritmo de Euclides). Por outro lado, se $d \nmid b$ então sabemos que tal equação não tem solução, pelo que $ax \equiv b \bmod m$ também não tem solução. Isto mostra (1). Para provar (2) basta ver que a solução e a sua unicidade resultam da Proposição 3.12. Para verificar

a solução do caso geral, em primeiro lugar verificamos que $(a',m') = \frac{1}{d}(a,m) = 1$. Assim, $x_0 \equiv (a')^{-1}b' \bmod m'$ é solução da equação $a'x \equiv b' \bmod m'$. Assim $da'x_0 \equiv db' \bmod m'$, pelo que x_0 é também solução da equação $ax \equiv b \bmod m'$ e da equação $ax \equiv b \bmod m$. □

A seguinte proposição é frequentemente útil.

Proposição 3.20. *Nas mesmas condições do Teorema, seja $c \in \mathbb{Z}$ com $(c,m) = 1$. O conjunto de soluções da equação*

$$ax \equiv b \bmod m \tag{3.3}$$

é o mesmo que o conjunto de soluções da equação:

$$cax \equiv cb \bmod m. \tag{3.4}$$

Demonstração. Se $ax \equiv b \bmod m$ (ou seja, x é uma solução da equação (3.3)), então $cax \equiv cb \bmod m$. Reciprocamente, se $cax \equiv cb \bmod m$ então, como por hipótese c tem um inverso módulo m, multiplicando por c^{-1} obtemos $ax \equiv b \bmod m$, como pretendido. □

Este método permite também resolver certos sistemas de equações lineares, como no próximo exemplo.

Exemplo 3.21. Considere-se o sistema de equações com o mesmo módulo 9:

$$\begin{cases} 2y - 2x \equiv 4 & \bmod 9 \\ 5x - 8y \equiv 2 & \bmod 9. \end{cases}$$

Podemos resolver estas equações, eliminando uma variável: se multiplicarmos a primeira equação por 4, a Proposição (3.20) garante que mantemos as soluções (uma vez que $(4,9) = 1$) e obtemos

$$\begin{cases} 8y - 8x \equiv 16 & \equiv 7 \bmod 9 \\ 5x - 8y \equiv 2 & \bmod 9. \end{cases}$$

Adicionando agora as duas equações, obtemos $-3x \equiv 9 \equiv 0 \bmod 9$. Como 3 não é invertível módulo 9 e uma solução desta equação é $x_0 \equiv 0$, a solução geral é $x \equiv 0 + 3k \bmod 9$, $k = 0,1,2$. Isto é, $x \equiv 0$, $x \equiv 3$ ou $x \equiv 6$ módulo 9. Substituindo cada solução numa das equações iniciais, temos:

$$\begin{aligned} 2y \equiv 4 \bmod 9 &\iff y \equiv 2^{-1} \cdot 4 \equiv 20 \equiv 2 \bmod 9 \\ 2y - 6 \equiv 4 \bmod 9 &\iff y \equiv 2^{-1} \cdot 10 \equiv 5 \bmod 9 \\ 2y - 12 \equiv 4 \bmod 9 &\iff y \equiv 2^{-1} \cdot 16 \equiv 8 \bmod 9. \end{aligned}$$

Finalmente temos as 3 soluções do sistema: $(x,y) \equiv (0,2)$, $(x,y) \equiv (3,5)$ ou $(x,y) \equiv (6.8)$ módulo 9.

3.7. **O Teorema chinês dos restos.** Consideremos o seguinte sistema de três congruências:

$$\begin{cases} x \equiv 1 & \bmod 3 \\ x \equiv 2 & \bmod 4 \\ x \equiv 3 & \bmod 5. \end{cases}$$

Vamos resolvê-lo por sucessivas substituições. A primeira equação diz-nos $x = 1 + 3y$, para certo $y \in \mathbb{Z}$. Se substituímos na segunda equação, vem:

$$1 + 3y \equiv 2 \bmod 4.$$

Esta equação fica $3y \equiv 1 \bmod 4$ ou seja $y \equiv 3^{-1} \equiv 3 \bmod 4$. Note-se que $(3,4) = 1$. Logo $y = 3 + 4z$, para $z \in \mathbb{Z}$, e portanto

$$x = 1 + 3y = 10 + 12z.$$

Substituindo na terceira equação temos:

$$10+12z \equiv 3 \bmod 5,$$

e como $(5,12)=1$, e -2 é inverso de 12 (mod 5), temos

$$z \equiv 12^{-1}(-7) \equiv (-2)\cdot(-7) = 14 \equiv 4 \bmod 5.$$

Assim, $x = 10+12\cdot 4 = 58$ é a única solução módulo $m_1 m_2 m_3 = 60$. A mesma solução é $x=-2$ uma vez que $58 \equiv -2 \bmod 60$.

Teorema 3.22. *[Teorema Chinês dos Restos] Sejam $m_1, \cdots, m_r$ naturais primos dois a dois (ou seja $(m_i, m_j)=1$ para quaisquer índices distintos $i \neq j$), e seja $M = m_1 \cdots m_r$. Então o sistema de congruências*

$$\begin{cases} x \equiv b_1 & \bmod m_1 \\ x \equiv b_2 & \bmod m_2 \\ \vdots & \vdots \\ x \equiv b_r & \bmod m_r. \end{cases}$$

tem uma e uma só solução, módulo M. A solução é dada recursivamente, substituindo sucessivamente a solução geral de uma equação na seguinte equação. Explicitamente, a solução é dada por

$$x_0 \equiv b_1 \frac{M}{m_1} y_1 + \cdots + b_r \frac{M}{m_r} y_r, \bmod M \tag{3.5}$$

onde y_k é um inverso de $\frac{M}{m_k}$, módulo m_k, para todo $k = 1, \cdots, r$.

Demonstração. Seja x_0 dado pela expressão (3.5). Vamos reduzir x_0 módulo cada um dos $m_i \in \mathbb{N}$, $i = 1, \cdots, r$. Todos os números $\frac{M}{m_i}$ são inteiros, e além disso

$$m_i \mid \frac{M}{m_j}, \qquad \text{ou seja} \qquad \frac{M}{m_j} \equiv 0 \bmod m_i,$$

sempre que $i \neq j$. Por exemplo $\frac{M}{m_2} \equiv 0 \bmod m_1$ porque $\frac{M}{m_2} = m_1 m_3 \cdots m_r$. Assim, a redução de x_0 módulo m_i é:

$$x_0 \equiv b_i \frac{M}{m_i} y_i \equiv b_i \bmod m_i, \qquad \forall i \in \{1, \cdots, r\}$$

porque, por definição $y_i \equiv (\frac{M}{m_i})^{-1} \bmod m_i$. Deste modo, provámos que x_0 é solução. Deixamos a unicidade da solução, mod M, para o leitor. □

Problemas de Revisão.

3.1 Calcule os valores das seguintes expressões algébricas em $\mathbb{Z}_{13}$:
- (a) $4 \times (11^2 + 12 - 7)$,
- (b) 10^{34},
- (c) $4^{-1} \times (25 - 12)$.

3.2 Diga, justificando, se as seguintes afirmações são verdadeiras ou falsas.
- (a) $35 - 4^3 \equiv -1 \bmod 5$,
- (b) Se $a \equiv b$, mod m, então $b + 3a \equiv 4a + mb$, mod m,
- (c) Se $a \equiv b$, mod m, então $a^k \equiv b^{k+m}$, mod m.

3.3 Diga, justificando, se algum dos seguintes elementos 7, 22, 3, 49 são invertíveis em $\mathbb{Z}_{60}$ e calcule o seu inverso, em caso afirmativo. Quantos elementos de $\mathbb{Z}_{60}$ são invertíveis?

3.4 Seja $n = [a_k \cdots a_1 a_0]_{10} \in \mathbb{N}$ (isto é, a representação decimal tem os dígitos $a_k, \cdots, a_0 \in \{0, \cdots, 9\}$). Mostre que n é múltiplo de 11 se e só se a soma alternada dos dígitos também é. Ou seja, $11 \mid n$ se e só se $a_0 - a_1 + a_2 - a_3 + \cdots \equiv 0 \,(\text{mod } 11)$ [Sugestão: $10^k \equiv (-1)^k \,(\text{mod } 11)$, para todo o inteiro $k \geq 0$].

3.5 Seja $n = 6k+5$ com $k \in \mathbb{Z}$. Mostre que existe um divisor primo p de n tal que $p \equiv 5 \pmod 6$. Deduza que existem infinitos primos que verificam $p \equiv 5$ módulo 6.

3.6 Mostre que se n é um número primo então $n|\binom{n}{k}$ para qualquer $k \in \{1, \cdots, n-1\}$. A mesma afirmação é verdadeira caso n não seja primo?

3.7 [Relação entre módulos múltiplos] Sejam $m, n, d \in \mathbb{N}$ tais que $m = nd$. Se $x \equiv a \bmod n$, mostre que x é congruente, módulo m, com um elemento do conjunto $\{a, a+n, a+2n, \cdots, a+(d-1)n\}$.

3.8 [Cálculo eficiente de potências] Seja $n = [a_{k-1}a_{k-2}\cdots a_1a_0]_2 = a_0 + a_1 2^1 + a_2 2^2 + \cdots + a_{k-1}2^{k-1}$, e $a_k \in \{0,1\}$, um natural representado na base 2 com k bits.
(a) Sendo $a \in \mathbb{N}$, prove que a^n pode ser calculado com menos de $2k$ multiplicações (mais precisamente, com $2k-l$ multiplicações, onde l é o número de bits a_j nulos, $j = 0, ..., k-1$).
(b) Use a alínea anterior para calcular 7^{71} módulo 29.

3.9 Numa ilha há 13 camaleões verdes, 15 camaleões castanhos e 17 camaleões encarnados. Se dois camaleões de cores diferentes se encontram mudam ambos para a terceira cor (não mudam de cor em nenhuma outra situação). Será possível que a certa altura os camaleões fiquem todos da mesma cor? [Sugestão: analise o resultado do encontro de dois camaleões de cor diferente em cada conjunto módulo 3].

3.10 A que classes de congruência, *módulo 8*, pertencem os quadrados perfeitos? O número 6834923 pode ser um quadrado perfeito, ou a soma de 2 quadrados perfeitos?

3.11 Seja p um número primo. (1) Mostre que $a \in \mathbb{Z}$ é invertível módulo p se e só se $p \nmid a$. (2) Mostre que a lei do corte é válida em $\mathbb{Z}_p$.

3.12 Encontre um inverso de 89 módulo 232.

3.13 Prove que qualquer que seja $a \in \mathbb{Z}$ se verifica $a^2 \equiv 0, 1$ ou 4 módulo 8. Mostre que nenhum número natural da forma $8k+7$ pode ser escrito como soma de três quadrados perfeitos.

3.14 Resolva as seguintes congruências (encontrando todas as soluções, ou justificando que não existem soluções)
(a) $5x \equiv 3 \bmod 11$
(b) $9x \equiv 21 \bmod 12$

3.15 Determine todas as soluções (eventualmente nenhuma) das equações:
(a) $3x \equiv 9 \bmod 13$
(b) $3x \equiv 9 \bmod 12$

3.16 Determine todas as soluções (eventualmente nenhuma) das equações:
(a) $30x \equiv 45 \bmod 60$
(b) $25x \equiv 45 \bmod 60$

3.17 Identifique o conjunto de soluções das seguintes equações lineares em duas variáveis:
(a) $6x + 2y \equiv 0 \bmod 11$
(b) $6x + 2y \equiv 5 \bmod 11$
(c) $6x + 2y \equiv 0 \bmod 12$
(d) $6x + 2y \equiv 5 \bmod 12$

3.18 Determine o conjunto de soluções em $\mathbb{Z}_{13}$ das seguintes sistemas de equações lineares:
(a) $\begin{cases} 3x + 4y &= 1 \\ 2x + 3y &= 3 \end{cases}$
(b) $\begin{cases} 2x + 3y &= 3 \\ 3x - 2y &= 10 \end{cases}$

3.19 Determine a solução geral dos seguintes sistemas de equações:

(a) $\begin{cases} x \equiv 1 \mod 8 \\ x \equiv 4 \mod 15 \end{cases}$

(b) $\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 5 \mod 8 \\ x \equiv 11 \mod 17 \end{cases}$

3.20 Determine, usando o teorema chinês dos restos, as soluções, se existirem, da equação

$$507x \equiv 312 \mod 3025$$

3.21 Determine as soluções da equação

$$15x^2 + 19x + 6 \equiv 0 \mod 11$$

[Sugestão: factorize o polinómio]

3.22 Seja $\varphi(n)$ a função totiente de Euler. Mostre que $\Delta(n) + \varphi(n) \leq n+1$. Para que valores de n há igualdade?

3.23 Uma função $f : \mathbb{N} \to \mathbb{N}$ diz-se multiplicativa se $f(mn) = f(m)f(n)$ sempre que m, n sejam primos entre si.

(a) Mostre que Δ e φ são multiplicativas [Sugestão: aplique o Teorema Chinês dos Restos]

(b) Mostre que, se f é multiplicativa, então também o é $F(n) := \sum_{d|n} f(d)$.

3.24 Mostre que, se $p_1, \cdots, p_r$ são os primos que dividem um dado natural $m \in \mathbb{N}$, então

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

[Sugestão: use o facto, no Exercício 3(a), de que φ é multiplicativa]

4. Fermat, Euler e Criptografia

No capítulo anterior, estudámos como resolver algumas equações modulares. Analisámos, com algum detalhe, as equações e os sistemas lineares.

Neste capítulo, vamos estudar as equações modulares que envolvem expoentes da incógnita. São equações com potências da variável x, e que são muito úteis nalgumas aplicações em informática, como a criptografia de "chave pública". Este tipo de equações também se relaciona com o chamado *problema do logaritmo discreto*.

4.1. **O Teorema das potências de Fermat.** A seguinte é uma propriedade fundamental dos números modulares com módulo primo. Sendo p um número primo, vamos considerar o conjunto

$$\mathbb{Z}_p^\times := \{\underline{1}_p, \underline{2}_p, \cdots, \underline{p-1}_p\},$$

dos números modulares invertíveis em $\mathbb{Z}_p$. Como sabemos, $\mathbb{Z}_p^\times$ está em correspondência bijeciva com $[p-1]$, pelo que $\left|\mathbb{Z}_p^\times\right| = p-1$.

Proposição 4.1. *Seja p um número primo e $a \in \mathbb{Z}$ invertível módulo p. Então a aplicação de multiplicação por a é uma bijecção no conjunto dos números invertíveis de $\mathbb{Z}_p$. Dito de outra forma, se $(a,p) = 1$ a função*

$$\begin{array}{rccc} m_a : & \mathbb{Z}_p^\times & \to & \mathbb{Z}_p^\times \\ & b & \mapsto & a\,b, \end{array}$$

é bijectiva.

Demonstração. Vamos verificar que é injectiva e sobrejectiva. Para ver que m_a é sobrejectiva, consideramos $y \in \mathbb{Z}$ invertível módulo p, ou seja $(y,p) = 1$, e temos que resolver a equação

$m_a(x) = a\,x \equiv y \bmod p$. Como a é também invertível $\bmod p$, $(a,p) = 1$ (e $1 \mid y$) a equação resolve-se pondo $x \equiv c\,a^{-1} \bmod p$. Para ver que m_a é injectiva, consideramos $m_a(b) \equiv m_a(c) \bmod p$, ou seja $ab \equiv ac \bmod p$. Nesse caso, como $(a,p) = 1$, pela lei do corte, $b \equiv c \bmod p$, o que mostra a injectividade. □

No resultado acima é essencial considerarmos o conjunto dos números modulares $\mathbb{Z}_p$. Caso considerássemos os números inteiros $\mathbb{Z}$, a conclusão seria diferente.

Exercício 4.1. Mostre que a função de multiplicação por $a \in \mathbb{Z}$, $m_a : \mathbb{Z} \to \mathbb{Z}$, $b \mapsto ab$ não é sobrejectiva, se $a \neq \pm 1$ e não é injectiva se $a = 0$.

O seguinte resultado é frequentemente chamado o "Pequeno Teorema de Fermat", mas vamos referi-lo como o Teorema das potências de Fermat.

Teorema 4.2. *[Teorema das potências de Fermat] Seja $a \in \mathbb{Z}$ e p um número primo. Se $(a,p) = 1$, então $a^{p-1} \equiv 1 \bmod p$.*

Demonstração. Consideremos o número inteiro $a^{p-1} \cdot (p-1)!$. A sua redução, módulo p, coincide com a de $(p-1)!$. De facto:

$$\begin{aligned} a^{p-1}(p-1)! = a^{p-1}(1 \cdot 2 \cdot \cdots \cdot (p-1)) &\equiv (a \cdot 1)(a \cdot 2) \cdots (a \cdot (p-1)) \mod p \\ &\equiv m_a(1) \cdot m_a(2) \cdots \cdot m_a(p-1) \mod p \\ &\equiv 1 \cdot 2 \cdot \cdots \cdot (p-1) \equiv (p-1)! \mod p. \end{aligned}$$

Acima, usámos a comutatividade do produto, e a Proposição 4.1 da segunda para a terceira linha. Como todos os números de 1 a $p-1$ são invertíveis módulo p, e o produto de invertíveis é invertível, a lei do corte implica $a^{p-1} \equiv 1 \bmod p$ como queriamos provar. □

Exemplo 4.3. Verifiquemos o teorema de Fermat módulo $p = 11$. Ignorando casos triviais, basta considerar $a \in \{2, \cdots, 10\}$. Temos então, as potências $p - 1 = 10$ (com a ajuda duma calculadora):

$$2^{10} = 1024 = 93 \cdot 11 + 1 \equiv 1 \bmod 11, \quad 3^{10} = 59049 \equiv 1 \bmod 11,$$

e da mesma forma:

$$4^{10} = 1048576 \equiv 1 \bmod 11, \qquad 5^{10} = 9765625 \equiv 1 \bmod 11,$$

e não é necessário verificar as outras bases, uma vez que temos as congruências $11 - a \equiv -a \bmod 11$ (por ex: $-6 \equiv 5 \bmod 11$) e $(-a)^{10} = a^{10}$, para qualquer $a \in \mathbb{Z}$.

Exercício 4.2. Seja p primo. Mostre que, para qualquer $a \in \mathbb{Z}$, $a^p \equiv a \bmod p$. Se a é invertível $\bmod p$, verifique que $a^{-1} \equiv a^{p-2} \bmod p$.

Teste de Fermat. Dado um natural muito grande, $n \in \mathbb{N}$, como podemos saber se é primo? Determinar se todos os números $m < n$ são divisores pode ser uma tarefa ingrata (ou todos os primos $p < \sqrt{n}$, ver o exercício 12 §1.9). O Teorema de Fermat permite, nalguns casos, saber se n é composto, sem considerar divisores.

Recorde-se que, para divisores concretos, temos alguns testes de congruência bem conhecidos. Por exemplo, se a soma dos algarismos de n é congruente com 0 módulo 3, então $3 \mid n$; se n acaba em 0 ou em 5 sabemos que tem o divisor 5. Nestes casos, n é composto. O seguinte exemplo é um critério de divibilidade por 11.

Exemplo 4.4. Seja n dado, e $[a_k a_{k-1} \cdots a_0]_{10}$ a sua representação decimal. Se $a_0 + a_1 + \cdots + a_k \equiv 0 \bmod 3$ então n é composto, pois é divisível por 3. Se $a_0 - a_1 + \cdots \pm a_k \equiv 0 \bmod 11$, então é divisível por 11.

Por outro lado, com o Teorema de Fermat, obtemos um critério que não depende de testarmos um ou outro divisor.

De facto sabemos que, se n é primo, então $a^{n-1} \equiv 1 \bmod n$ para qualquer $a \in [n-1]$. De forma equivalente, $a^n \equiv a \bmod n$, quando n é primo. Isto sugere o teste de Fermat.

Teste de Fermat Seja dado $n \in \mathbb{N}$, e $a \in [n-1]$. Se a^n não é congruente com a, módulo n, então n é composto.

No entanto, caso o teste seja positivo, ou seja, se $a^n \equiv a \bmod n$ para todo o $a \in [n-1]$ não podemos, ainda assim, concluir que n é primo. De facto, existem números compostos tais que $a^n \equiv a \bmod n$ para todo o $a \in [n-1]$.

O menor destes números é o $n = 561$. Este número é composto $561 = 3 \cdot 11 \cdot 17$, mas $a^{561} \equiv a \bmod 561$ para todo o $a \in [560]$!

4.2. **A função totiente e o teorema de Euler.** Recorde-se a definição da função totiente de Euler (função φ de Euler):

$$\varphi(m) := |\{x \in [m] : (x,m) = 1\}|.$$

Assim, dado $m \in \mathbb{N}$, $\varphi(m)$ é o cardinal do conjunto dos números modulares que têm inverso $\bmod m$:

$$\mathbb{Z}_m^\times \cong \{x \in [m-1]_0 : (x,m) = 1\} \cong \{x \in [m] : (x,m) = 1\}.$$

Fórmula de Euler para a função totiente. Vamos agora determinar a fórmula de Euler para esta função, começando pelo caso de uma potência de número primo.

Lema 4.5. *Seja p um número primo. Então $\varphi(p) = p-1$. Mais geralmente, para $k \in \mathbb{N}$ temos $\varphi(p^k) = p^k - p^{k-1}$.*

Demonstração. Por definição, $\mathrm{Div}(p) = \{1, p\}$. Assim, com $1 \leq x \leq p$, temos que $(x,p) = 1$ sempre que $x < p$, ou seja o máximo divisor comum (x,p) é 1 precisamente quando $x \in [p-1]$, pelo que $\varphi(p) = |[p-1]| = p-1$. Mais geralmente, para $k \in \mathbb{N}$, os divisores de p^k são $\mathrm{Div}(p^k) = \{1, p, \cdots, p^k\}$, pois estes são precisamente os que não têm outros factores primos. Assim, para $x \in [p^k]$, temos que $(x,p) \neq 1$ se e só se x é múltiplo de p (os múltiplos de p^2, p^3, etc são também múltiplos de p):

$$\{x \in [p^k] : (x,p) \neq 1\} = \{p, 2p, 3p, \cdots, p^{k-1}p = p^k\}$$

que é um conjunto em bijecção com $\{1, \cdots, p^{k-1}\}$ (basta dividir todos os elementos por p), e portanto $\varphi(p^k)$ é o cardinal do complementar, ou seja $\varphi(p^k) = p^k - p^{k-1}$. □

Para deduzir a fórmula de Euler para $\varphi(n)$ a partir da factorização de n em primos, usa-se também o facto de que φ é uma *função multiplicativa*, no seguinte sentido: se $n, m \in \mathbb{N}$ são primos entre si, então $\varphi(nm) = \varphi(n)\varphi(m)$.

Proposição 4.6. *Sempre que $n, m \in \mathbb{N}$ verificam $(n,m) = 1$ temos $\varphi(nm) = \varphi(n)\varphi(m)$.*

Demonstração. Sendo $N \in \mathbb{N}$, vamos designar por P_N o conjunto finito

$$P_N := \{x \in [N-1]_0 : (x,N) = 1\},$$

pelo que $\varphi(n) = |P_n|$, por definição. Dados n, m naturais primos entre si, definimos a seguinte função:

$$\begin{aligned} f : P_{nm} &\to P_n \times P_m \\ a &\to (r_n(a),\, r_m(a)) \end{aligned}$$

onde $r_n(a)$, $r_m(a)$ são os restos da divisão de a por n, e por m, respectivamente. Assim $a \equiv r_n(a) \bmod n$, e $a \equiv r_m(a) \bmod m$. A função está bem definida, porque se $a \in P_{nm}$ significa que $(a, nm) = 1$, pelo que $(a,n) = 1$ e $(a,m) = 1$ (pois $(n,m) = 1$) o que implica também $(r_n(a), n) =$

$(r_m(a), m) = 1$. Esta função é bijectiva porque, dado um par $(r, r') \in P_n \times P_m$ existe um e um só $x \in P_{nm}$ tal que:

$$\begin{cases} x \equiv r & \mod n \\ x \equiv r' & \mod m, \end{cases}$$

pois isto é garantido pelo Teorema Chinês dos Restos. Assim, P_{nm} tem o mesma cardinal de $P_n \times P_m$. Concluímos então:

$$\varphi(nm) = |P_{nm}| = |P_n \times P_m| = |P_n| \cdot |P_m| = \varphi(n)\varphi(m),$$

como queríamos provar. □

Corolário 4.7. *Seja $n \in \mathbb{N}$ com factorização $n = p_1^{k_1} \cdots p_r^{k_r}$. Então*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

A demonstração deste corolário deixa-se como exercício.

Exemplo 4.8. Verifiquemos que a fórmula acima nos dá $\varphi(45) = 12$, como no exemplo anterior. De facto, como $45 = 3^2 \cdot 5$, temos

$$\varphi(45) = 45(1 - \frac{1}{3})(1 - \frac{1}{5}) = 45 \cdot \frac{2}{3} \cdot \frac{4}{5} = 3 \cdot 2 \cdot 4 = 24.$$

Exercício 4.3. Mostre que, se p e q são números primos, então:

$$\varphi(pq) = (p-1)(q-1).$$

Teorema das potências de Euler. A função totiente de Euler permite generalizar o teorema de Fermat para módulos que não são primos, começando por generalizar a Proposição 4.1.

Proposição 4.9. *Seja $m \in \mathbb{N}$, $a \in \mathbb{Z}$ e $(a, m) = 1$. Então a aplicação de multiplicação por a é uma bijecção no conjunto dos números invertíveis de $\mathbb{Z}_m$. Ou seja, a aplicação*

$$\begin{array}{rccc} m_a : & \mathbb{Z}_m^\times & \to & \mathbb{Z}_m^\times \\ & x & \mapsto & a\,x, \end{array}$$

é uma bijecção.

Demonstração. A demonstração é análoga à da Proposição 4.1, fazendo apenas uma pequena variação. Para ver que m_a é bijectiva, consideramos $c \in \mathbb{Z}$ e temos que resolver a equação $m_a(x) = ax \equiv c \mod m$. Como $(a, m) = 1$ e $1 \mid c$ existe solução x_0, pela identidade de Bézout:

$$ax_0 + my = c,$$

e além disso qualquer outra solução é obtida somando km, $k \in \mathbb{Z}$ a x_0. Desta forma, a solução é única, módulo m, pelo que m_a é bijectiva. □

Teorema 4.10. *[Teorema das potências de Euler] Seja $a \in \mathbb{Z}$ e $m \in \mathbb{N}$. Se $(a, m) = 1$, então $a^{\varphi(m)} \equiv 1 \mod m$.*

Demonstração. A demonstração é inteiramente análoga à do Teorema de Fermat. Consideremos o produto de todos os invertíveis em $\mathbb{Z}_m$, isto é, o número inteiro

$$y = \prod_{x \in \mathbb{Z}_m^\times} x,$$

bem definido a menos de múltiplos de m. A redução de $a^{\varphi(m)}y$, módulo m, coincide com a do próprio y. De facto:

$$\begin{array}{rcl} a^{\varphi(m)}y = a^{\varphi(m)} \prod_{x \in \mathbb{Z}_m^\times} x & \equiv & \prod_{x \in \mathbb{Z}_m^\times} (a \cdot x) \mod p \\ & \equiv & \prod_{x \in \mathbb{Z}_m^\times} (m_a(x)) \mod p \\ & \equiv & \prod_{x \in \mathbb{Z}_m^\times} x \mod p \quad \equiv \quad y \mod p. \end{array}$$

Usámos novamente a comutatividade do produto, o facto de que $\varphi(m)$ é o cardinal de $\mathbb{Z}_m^\times$ e a Proposição 4.9 da segunda para a terceira linha. Como todos os $x \in \mathbb{Z}_m^\times$ são invertíveis módulo m, y também o é, e a lei do corte implica $a^{\varphi(m)} \equiv 1 \bmod p$, como queriamos provar. □

Exercício 4.4. Seja $(a,m)=1$, e k um inteiro qualquer. Mostre que $a^{k\varphi(m)} \equiv 1 \bmod m$.

O teorema de Euler permite calcular potências, em artimética modular, de uma forma expedita, como podemos ver no seguinte exemplo.

Exemplo 4.11. Vamos calcular $25^{544} \bmod 279$ (obtendo um número em $[279]_0$). Como $279 = 9 \cdot 31 = 3^2 \cdot 31$, temos $\varphi(279) = \varphi(9)\varphi(31) = (3^2-3)\cdot 30 = 180$. Assim, o teorema de Euler diz-nos que $25^{180} \equiv 1 \,(\mathrm{mod}\, 279)$, uma vez que $25 = 5^2$ e então $(25, 279) = 1$.

Desta forma o expoente pode ser reduzido módulo 180 sem afectar o valor da potência. Uma vez que $543 = 180 \cdot 3 + 3$ temos:

$$25^{544} = 25^{180\cdot 3+4} = \left(25^{180}\right)^3 \cdot 25^4 \equiv 1^3 \cdot 25^4 \equiv 390625 \equiv 25 \,(\mathrm{mod}\, 279).$$

Assim, $x = 25$ é a solução do problema. Concluímos então que $25^4 \equiv 25 \,(\mathrm{mod}\, 279)$ o que também nos diz que $25^3 \equiv 1 \,(\mathrm{mod}\, 279)$.

Exercício 4.5. Usando o método do exercício acima, determine $19^{375} \bmod 35$.

Observação 4.12. O teorema das potências de Euler diz-nos que $a^{k\varphi(m)} \equiv 1 \bmod m$ quando $(a,m) = 1$ e $k \in \mathbb{Z}$. O exemplo acima mostra que podem haver outros expoentes j, além dos múltiplos de $\varphi(m)$ que também verificam $a^j \equiv 1 \bmod m$. O menor expoente que o verifica é chamado a ordem de a módulo m.

Definição 4.13. Seja $a \in \mathbb{Z}$ e $m \in \mathbb{N}$. Se a é invertível módulo m (ou seja, $(a,m) = 1$) o *menor natural* j tal que $a^j \equiv 1 \bmod m$ chama-se a ordem de a módulo m e escreve-se $j = \mathrm{ord}_m(a)$.

Proposição 4.14. *A ordem de qualquer $a \in \mathbb{Z}$, invertível módulo m, divide $\varphi(m)$. Isto é*

$$ord_m(a) \mid \varphi(m).$$

Mais geralmente $ord_m(a) \mid k$ para qualquer $k \in \mathbb{Z}$ que verifique $x^k \equiv 1 \bmod m$.

Demonstração. Seja $j = \mathrm{ord}_m(a)$ e $k \in \mathbb{Z}$ tal que $x^k \equiv 1 \bmod m$. Vamos dividir k por j: $k = qj + r$ com $r \in \{0, 1, \cdots, m-1\}$. Então,

$$1 \equiv a^k \equiv \left(a^j\right)^q a^r \equiv a^r.$$

Como j é o *menor natural* tal que $a^j \equiv 1 \bmod m$, isto contradiz $r < j$, a menos que $r = 0$. Assim $j \mid k$. Também temos $j \mid \varphi(m)$ uma vez que, pelo Teorema de Euler, $a^{\varphi(m)} \equiv 1 \bmod m$. □

Exemplo 4.15. No exemplo acima $25^3 \equiv 1 \,(\mathrm{mod}\, 279)$. Isto não contradiz a Proposição acima, uma vez que $3 \mid 180$ onde $180 = \varphi(279)$. É fácil de verificar que, precisamente $\mathrm{ord}_{279}(25) = 3$.

4.3. **O Teorema de Daniel Augusto da Silva.** A fórmula de Euler teve uma grande relevância no desenvolvimento da teoria dos números, bem como na teoria dos conjuntos finitos, pois a demonstração envolve conjuntos finitos e o conceito de cardinalidade. Este mesmo método foi usado pelo matemático português mais proeminente do século XIX, Daniel Augusto da Silva (1814-1876). Foi ao estudar problemas de aritmética modular que este matemático notável introduziu o famoso princípio de Inclusão-Exclusão, um dos métodos fundamentais em combinatória enumerativa, para determinar o cardinal de uma reunião arbitrária de conjuntos finitos (ver a Parte 2 destas notas, e a Secção 4.2, abaixo).

Daniel Augusto da Silva descobriu também a seguinte elegante generalização da fórmula das potências de Euler.

Teorema 4.16. *Sejam $n_1, \cdots, n_r$ naturais primos entre si. Então:*

$$n_1^{\varphi(n)/\varphi(n_1)} + \cdots + n_r^{\varphi(n)/\varphi(n_r)} \equiv r - 1 \bmod n,$$

onde $n = n_1 \cdots n_r$.

Demonstração. Fixemos um $j \in [r]$. Pelo teorema das potências de Euler, temos:

$$n_i^{\varphi(n_j)} \equiv 1 \bmod n_j, \quad \forall i \neq j$$

uma vez que $(n_i, n_j) = 1$. Notando que $\varphi(n) = \varphi(n_1) \cdots \varphi(n_r)$, calculamos:

$$n_i^{\varphi(n)/\varphi(n_i)} \equiv n_i^{\varphi(n_1)\cdots\varphi(n_{i-1})\varphi(n_{i+1})\cdots\varphi(n_r)} \equiv 1^{r-1} \equiv 1 \bmod n_j.$$

Por outro lado $n_j^{\varphi(n)/\varphi(n_j)}$ é um múltiplo de n_j. Assim, fazendo a soma das r congruências, módulo n_j temos:

$$\sum_{j=1}^{r} n_j^{\varphi(n)/\varphi(n_j)} \equiv r - 1 \bmod n_j.$$

Desta forma, mostrámos que:

$$n_j \mid \left(r - 1 - \sum_{j=1}^{r} n_j^{\varphi(n)/\varphi(n_j)} \right),$$

o que implica, dado que todos os n_j são primos entre si,

$$n \mid \left(r - 1 - \sum_{j=1}^{r} n_j^{\varphi(n)/\varphi(n_j)} \right),$$

ou seja: $\sum_{j=1}^{r} n_j^{\varphi(n)/\varphi(n_j)} \equiv r - 1 \bmod n$, como queríamos mostrar. □

Podemos imediatamente escrever a fórmula de Daniel da Silva, para $r = 2$ e $r = 3$.

Corolário 4.17. *Dados três naturais a, b, c primos entre si, temos:*

$$\begin{aligned} a^{\varphi(b)} + b^{\varphi(a)} &\equiv 1 \bmod ab \\ a^{\varphi(bc)} + b^{\varphi(ac)} + c^{\varphi(ab)} &\equiv 2 \bmod abc. \end{aligned}$$

A fórmula de Daniel da Silva passou despercebida à comunidade matemática durante várias décadas, e só esporadicamente foi mencionada no século XX e XXI; desta forma, não houve o desenvolvimento que frequentemente ocorre com outras descobertas. Este texto deixa, assim, um desafio para a comunidade dos futuros matemáticos.

Exercício 4.6. Usando a fórmula de Daniel Augusto da Silva, mostre que

$$b^{\varphi(ac)} + c^{\varphi(ab)} \equiv 2 \bmod a,$$

quando $a, b, c \in \mathbb{N}$ são primos entre si.

4.4. **O algoritmo RSA.** O algoritmo de criptografia mais usado hoje em dia nas comunicações através da internet foi desenhado por R. Rivest, A. Shamir and L. Adleman, num artigo que agora ficou famoso.[6] Este é um sistema assimétrico em que o emissor e o receptor da mensagem efectuam cálculos diferentes para codificar ou descodificar uma mensagem.

[6] R.L. Rivest, A. Shamir, and L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, disponível em https://people.csail.mit.edu/rivest/Rsapaper.pdf © ACM, 1977.

O processo pode ser resumido da seguinte forma. O emissor *codifica uma mensagem* M, usando uma *chave* (às vezes também chamada *cifra*) E. Desta forma obtém a mensagem codificada (também designada *encriptada*) C, mensagem esta que parece incompreensível a qualquer pessoa que a leia. Então, o receptor recebe C, e usando uma outra chave D, descodifica-a obtendo novamente a mensagem M.

Vamos exemplificar este processo com a chamada *cifra de César*, um dos métodos de criptografia mais simples e antigos que se conhecem (de facto, refere-se a um processo usado no tempo de Júlio César). Consideramos o alfabeto usual $A = \{a, b, \cdots, u, v, wx, y, z\}$, que tem 26 letras, e associamos a cada letra um número $a = 1$, $b = 2$, $c = 3$, etc. Vamos supor que a nossa mensagem é $M = eureka$ e, usando aritmética modular de módulo $m = 26$, decidimos (por exemplo) que o processo de encriptação é *"somar 4 módulo 26"*. Assim, cada letra se transforma naquela que se obtém somando 4, módulo 26, por exemplo como a letra a corresponde a 1, a sua codificação é a letra que corresponde a 5, ou seja e. Da igual forma:

$$\begin{aligned} & a \mapsto e, \quad b \mapsto f, \quad c \mapsto g, \quad \cdots \\ \ldots, \quad & x \mapsto b, \quad y \mapsto c, \quad z \mapsto d. \end{aligned}$$

Assim, a mensagem codificada fica $C = iyvioe$, como se pode facilmente verificar. A chave de descodificação é o inverso da chave de codificação e, por isso, neste caso muito simples, é *"subtrair 4 móduo 26"*, o que é obviamente o processo inverso. Desta forma, a única informação que o emissor e receptor precisam de guardar (a infromação secreta) é o número 4, que permite codificar e descodificar mensagens sem problemas.

Para descrever o RSA, que é naturalmente mais complexo, supomos que as mensagens M e C são números inteiros x e y, e vamos trabalhar módulo N, um inteiro muito grande. Para que o algoritmo funcione, temos que escolher N de modo a que seja o produto de apenas dois primos. Assim, escrevemos $N = pq$, onde p e q são primos enormes. O inteiro N pode ser tornado público, enquanto que p e q têm que se manter secretos.

De seguida, o receptor (o emissor não precisa fazer nada nesta fase), faz duas importantes escolhas, para as quais usa a aritmética módulo $\varphi(N) = \varphi(pq) = (p-1)(q-1)$ (segue da propriedade multiplicativa da função totiente de Euler). O receptor escolhe inteiros e e d que são inversos módulo $\varphi(N)$, ou seja, verificam:

$$ed \equiv 1 \bmod \varphi(N).$$

Para terminar a sua parte, o receptor publica a chave (N, e) (a sua *chave de encriptação*) e mantém secreta a chave de decriptação (N, d). Uma vez que a chave (N, e) fica disponível para qualquer pessoa enviar mensagens ao receptor, esta designa-se uma *chave pública*.

Finalmente, entra em jogo o emissor, que sabe (N, e) (pois o receptor publicou estes dois números). Para enviar a mensagem (número) x (que supomos, para simplificar $x < \min\{p, q\}$) ele envia a mensagem codificada, que é o inteiro modular:

$$y \equiv x^e \bmod N.$$

O receptor recebe y, mensagem incompreensível inicialmente, e então calcula:

$$y^d \bmod N,$$

e descobre que x é exactamente igual a y^d, pelo que recebeu a mensagem original! Note-se que somente o receptor conhece o inteiro d. O seguinte resultado, mostra que este processo funciona.

Teorema 4.18. *Sejam p e q números primos, $N = pq$, e $x < \min\{p, q\}$ inteiro. Se e e d são inversos módulo $\varphi(N)$, então:*

$$x \equiv y^d \equiv (x^e)^d \bmod N.$$

Demonstração. Uma vez que $ed \equiv 1 \bmod \varphi(N)$, temos que existe um inteiro k tal que

$$ed = 1 + k\varphi(N).$$

Assim, temos:

$$x^{ed} = x^{1+k\varphi(N)} = x \cdot (x^{\varphi(N)})^k \equiv x \cdot 1^k \equiv x \bmod N.$$

Na penúltima passagem usou-se o teorema de Euler, que se pode aplicar, uma vez que a condição $x < \min\{p,q\}$ implica que x é primo com $N = pq$. □

A razão pela qual este algoritmo é seguro deve-se a que os processos de encriptação ou descodificação (sabendo as chaves) são fáceis de implementar em computador. Mas, por outro lado, determinar d a partir de e envolve saber $\varphi(N)$ o que não é fornecido, apesar de se saber m.

Exemplo 4.19. Seja $p = 61$, $q = 53$. Então $N = pq = 3233$. Assim, $\varphi(N) = 60 \cdot 52 = 3120$. Percebe-se facilmente que $\varphi(N)$ será muito difícil de adivinhar para p, q muito grandes (uma vez que p e q são mantidos em segredo). Vamos escolher e primo com 3120. Por exemplo $e = 661$, e determinamos pelo algoritmo de Euclides estendido, $d = 1501$. Vamos dar ao João a nossa chave de encriptação $(N,e) = (3233,661)$ e esperamos que ele nos envie uma mensagem.

O João quer enviar a mensagem $M = x = 2762$. Nós recebemos a mensagem codificada $y = x^e = 2762^{661} \equiv 78 \bmod 3233$. E então calculamos $y^d = 78^{1501}$ e tiramos o resto da divisão por 3233, o que dá $78^{1501} \equiv 2762 \bmod 3233$, pelo que recuperámos a mensagem inicial !

Problemas de Revisão.

4.1 Use o teorema de Euler para determinar o inverso de 3 módulo 28.

4.2 Determine o menor natural a que satisfaz as congruências.
- (a) $a \equiv 9^{794} \mod 73$;
- (b) $a \equiv 7^{670} \mod 83$.

4.3 Determine o menor inteiro positivo congruente com $2^{12500} + 5^{32}$ módulo 10^6.

4.4 Qual é o algarismo das unidades de 7^{888}? E o das dezenas?

4.5 Determine uma solução da equação

$$47x^{120} + 7x^{100} + 54x^{20} + 25x + 2 \equiv 0 \mod 101,$$

e justifique que é única.

4.6 Considere a seguinte chave pública do sistema RSA (209,47). Determine os números primos p e q, e mostre que a chave é válida. Calcule a chave privada correspondente.

4.7 Considere os primos $p = 7$ e $q = 13$, e seja $N = pq$.
- (a) Determine $\varphi(N)$ e mostre que $e = 11$ é um expoente de encriptação válido.
- (b) Qual a encriptação $E(M)$ da mensagem $M = 20$?
- (c) Qual a mensagem M, se a mensagem encriptada recebida é $E(M) = 3$?

4.8 Considere os primos $p = 17$ e $q = 23$, e seja $N = pq$.
- (a) Determine $\varphi(N)$ e indique o conjunto E de expoentes de encriptação válidos.
- (b) Mostre que $7 \in E$ e determine o expoente de decriptação.
- (c) Qual a mensagem M, se a mensagem encriptada recebida é $E(M) = 2$?

4.9 Use o pequeno teorema de Fermat para calcular o inverso de 5 em $\mathbb{Z}_7$ e o inverso de 7 em $\mathbb{Z}_{11}$.

4.10 Mostre que a seguinte afirmação é equivalente ao pequeno teorema de Fermat: "Se p é primo e $a \in \mathbb{Z}$ não é múltiplo de p então $a^p \equiv a \bmod p$."

Parte 2. **FUNÇÕES e COMBINATÓRIA**

Esta segunda parte dedica-se a um tratamento introdutório de alguns aspectos de combinatória enumerativa. Começa-se por abordar os métodos de contagem baseados em sequências e em funções entre conjuntos finitos; introduzem-se também os números binomiais e multinomiais. De seguida, enunciam-se os princípios gerais de contagem, incluindo o princípio dos cacifos e o princípio de Inclusão-Exclusão e algumas das suas aplicação.

O terceiro tópico é o estudo das sucessões definidas por recorrência; em particular, considera-se o importante caso das recorrências lineares, e o versátil método das funções geradoras, bem como algumas aplicações. Finalmente, abordam-se alguns métodos de contagem com simetria, para o que é necessário introduzir a noção de grupo finito e de acções de grupos em conjuntos finitos.

5. Conjuntos, Funções e Números Binomiais

Muitos problemas de combinatória, nomeadamente, o que designamos por "combinatória enumerativa", se reduzem a algum tipo de contagem de elementos num certo conjunto dado. Assim, o cálculo do cardinal de um conjunto que nos é fornecido, e definido por uma certa propriedade, é um dos problemas que queremos abordar.

5.1. **Sequências e sequências sem repetição.** Vários problemas de contagem podem ser explicados com o conceito de sequência, como no exemplo anterior. Dado um conjunto X e um natural $k \in \mathbb{N}$, podemos considerar *sequências ordenadas* de elementos de X.

Definição 5.1. Seja X um conjunto, e k um natural. Uma *k-sequência em X* é uma lista *ordenada*:

$$(x_1, x_2, \cdots, x_k)$$

de elementos $x_i \in X$. Por outras palavras, uma k-sequência em X é um elemento do produto cartesiano $X^k = X \times \cdots \times X$ (onde X aparece k vezes).

Exemplo 5.2. Por exemplo, se $X = \{a, b, c, d, e\}$, e $k = 7$,

$$(a, d, c, d, a, b, b)$$

é uma 7-sequência de elementos de X. Esta sequência não é o mesmo que o conjunto

$$\{a, d, c, d, a, b, b\} = \{a, b, c, d\} = \{d, c, b, a\},$$

devido a duas importantes diferenças. Nos conjuntos, como indicado acima, não consideramos repetições de elementos, e os conjuntos não se alteram se trocarmos a ordem pela qual listamos os seus elementos. Por contraste, nas sequências **importa a ordem** pela qual listamos os elementos, e podemos ou não repeti-los numa dada sequência.

Recorde-se que, se X é um *conjunto finito*, o seu cardinal denota-se por $|X| \in \mathbb{N}$. Este é o único natural tal que existe uma bijecção $[n] \longleftrightarrow X$. Uma consequência imediata da definição anterior, e das propriedades dos produtos cartesianos é que o número total de k-sequências num conjunto finito X, é $|X|^k$. Outra consequência é a seguinte proposição. Recorde-se que $\mathscr{F}(X, Y)$ designa o conjunto das funções entre os conjuntos X e Y.

Proposição 5.3. *Existem bijecções naturais entre:*

$$\{k\text{-sequências em } X\} \quad \longleftrightarrow \quad \mathscr{F}([k], X) \quad \longleftrightarrow \quad X^k.$$

Em particular, temos a bijecção:

$$\mathscr{F}([k], [n]) \quad \longleftrightarrow \quad [n]^k$$

Deixamos ao leitor a demosntração desta Proposição, que não é mais do que sistematizar o que foi enunciado.

Exemplo 5.4. A 7-sequência em $X = \{a,b,c,d\}$ indicada no exemplo anterior corresponde ao elemento $(a,d,c,d,a,b,b) \in X^7$, e à função $f : [7] \to X$ dada por $f(1) = f(5) = a$, $f(2) = f(4) = d$, $f(3) = c$, $f(6) = f(7) = b$.

Também podemos considerar sequências, num conjunto X, sem repetição.

Definição 5.5. Seja X um conjunto, e k um natural. Uma *k-sequência, sem repetição,* em X é uma sequência $(x_1, x_2, \cdots, x_k)$ de elementos $x_i \in X$, em que impomos $x_i \neq x_j$ para todos os índices diferentes $i \neq j \in [k]$.

Observação 5.6. Uma sequência é também por vezes designada como "arranjo com repetição". Da mesma forma, sequências sem repetição também se chamam "arranjos sem repetição". No entanto, vamos usar mais o termo sequência, tanto pela relação natural com os produtos cartesianos, como pelo facto que a expressão "sequência em X" é útil pois imediatamente encerra informação sobre o conjunto com que estamos a lidar.

Recorde a definição de **factorial**. Sendo $n \in \mathbb{N}$, temos:

$$n! := n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1.$$

Proposição 5.7. *Dado um conjunto X com $n \in \mathbb{N}$ elementos, e um natural $k \in \mathbb{N}$, o número de sequências sem repetição em X é*

$$A_k^n := \frac{n!}{(n-k)!} = n(n-1)\cdots(n-k+1).$$

Demonstração. Todas as sequências sem repetição $(x_1, \cdots, x_k) \in X^k$ podem ser obtidas da seguinte forma. Primeiro, escolhemos $x_1 \in X$ arbitrariamente: há n escolhas possíveis porque $|X| = n$. Depois escolhemos $x_2 \in X \setminus \{x_1\}$ e agora temos $|X \setminus \{x_1\}| = n-1$ possibilidades. Continuando desta forma, chegamos a x_k que deve ser escolhido do conjunto $X \setminus \{x_1, \cdots, x_{k-1}\}$, com $n-(k-1) = n-k+1$ elementos. Como todas estas escolhas são independentes, o número de sequências possíveis é o produto indicado. □

Como é bem sabido, aos números A_k^n chamam-se k-arranjos de n. Note-se, em particular, que $A_n^n = n!$. Enunciamos uma consequência importante dos resultados anteriores.

Proposição 5.8. *O número de funções bijectivas $f : [n] \to [n]$ é $n!$*

Demonstração. De acordo com a Proposição 5.3, uma função $f : [n] \to [n]$ corresponde a uma sequência $(x_1, x_2, \cdots, x_n)$, com $x_i = f(i) \in [n]$. No entanto, para que f seja bijectiva é necessário (e suficiente) que $x_i \neq x_j$ sempre que $i \neq j$. Assim, o subconjunto das funções bijectivas em $\mathscr{F}([n],[n])$ está, por sua vez, em bijecção com as n-sequências sem repetição em $[n]$. O seu cardinal é, portanto,

$$|\{\text{funções bijectivas } [n] \to [n]\}| = |A_n^n| = n(n-1)(n-2)\cdots 2 \cdot 1 = n!,$$

como pretendido. □

Terminamos esta subsecção com uma interpretação conceptualmente diferente do conjunto

$$\mathscr{F}(X, \{0,1\})$$

das funções entre X e $\{0,1\}$.

Exemplo 5.9. Seja X um conjunto finito. O **conjunto potência** de X, também designado conjunto das partes de X, é definido por:

$$\mathscr{P}(X) := \{Y \subset X\},$$

ou seja $Y \in \mathscr{P}(X)$ se e só se Y é um subconjunto de X (assim, $\mathscr{P}(X)$ é o conjunto de todos os subconjuntos de X, incluindo o vazio $\varnothing$ e o próprio X). $\mathscr{P}(X)$ é também um conjunto finito e podemos determinar o seu cardinal em função de $n = |X|$. Assumimos, sem perda de generalidade, que $X = [n]$. A cada subconjunto $Y \in \mathscr{P}(X)$ associamos a n-sequência $(x_1, x_2, \cdots, x_n) \in \{0,1\}^n$ definida por

$$x_i := \begin{cases} 1, & \text{se } i \in Y \\ 0, & \text{se } i \notin Y. \end{cases}$$

Deixamos para o leitor a prova de que esta associação é uma bijecção. Assim, conlui-se que $|\mathscr{P}(X)|$ é igual ao número de n-sequências em $\{0,1\}$, ou seja 2^n.

5.2. **Números binomiais e a fórmula do binómio de Newton.** Muitas operações de contagem utilizam os números binomiais. Por exemplo, o número de formas de escolher 3 frutas de uma fruteira com 5 peças distintas, é igual a $\binom{5}{3} = \frac{5\cdot 4}{2} = 10$. Estes números binomiais aparecem tanto no triângulo de Pascal, como na fórmula do binómio de Newton.

Definição 5.10. Os números binomiais são os números $\binom{n}{m}$, com $n, m \in \mathbb{N}_0$ definidos por

$$\binom{n}{m} := \frac{n!}{m!(n-m)!} = \frac{n \cdot (n-1) \cdot \cdots \cdot (n-m+1)}{m \cdot (m-1) \cdot \cdots \cdot 1},$$

quando $n \geq m \geq 1$. Convenciona-se que $0! = 1$ e, por isso, $\binom{n}{0} = 1$ para todo o $n \in \mathbb{N}_0$. Por convenção, definimos também $\binom{n}{m} = 0$ nos casos "indesejados" em que m não está entre 0 e n, ou seja, quando $m < 0$ e também quando $m > n$.

Exemplo 5.11. O número binomial $\binom{n}{m}$ representa a forma de escolher m elementos de um conjunto de n elementos. Mais concretamente, seja $X = [n]$ e queremos saber quantos subconjuntos $Y \subset X$ existem com cardinal $m \leq n$. Dito de outra forma, queremos calcular o cardinal de

$$\mathscr{P}_m(X) := \{Y \subset X : |Y| = m\}.$$

A um tal subconjunto $Y = \{x_1, \cdots, x_m\} \subset X$, podemos associar a sequência $(x_1, \cdots, x_m)$ com entradas $x_i \in X$ todas distintas, mas como Y é o mesmo conjunto que $\{x_{f(1)}, \cdots, x_{f(m)}\}$, para qualquer bijecção $f : [m] \to [m]$, não podemos distinguir entre as correspondentes sequências. Isto significa que devemos dividir o número destas sequências (os m-arranjos sem repetição de n, ou seja $\frac{n!}{(n-m)!}$) pelo número de bijecções de $[m]$. Assim:

$$|\mathscr{P}_m(X)| = \frac{1}{m!} \frac{n!}{(n-m)!} = \binom{n}{m}$$

Os números binomiais aparecem na famosa fórmula do binómio de Newton. Há várias formas de a demonstrar, e escolhemos uma que relaciona com a também famosa fórmula de Taylor, que deve ser bem conhecida de todos.

Na realidade, só precisamos da fórmula de Taylor para um polinómio $f(x) \in \mathbb{R}[x]$, de grau $n \in \mathbb{N}$, e só precisamos da expansão em $x = 0$ (também chamada fórmula de Maclaurin) que é a seguinte relação:

$$f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(0)}{k!} x^k,$$

onde $f^{(k)}(0)$ designa a k-ésima derivada do polinómio f, calculada na origem. Recorde-se que $\mathbb{R}[x]$ designa o anel dos polinómios na variável x (ver também o apêndice).

Teorema 5.12. *[Fórmula do Binómio de Newton] Para qualquer $n \in \mathbb{N}$ e variáveis x, y, temos a igualdade de polinómios:*

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

Demonstração. Consideramos o polinómio $f(x) = (x+1)^n$, na variável x. Sabemos que as várias derivadas de $f(x)$ são dadas por:

$$f'(x) = n(x+1)^{n-1}, \qquad f''(x) = n(n-1)(x+1)^{n-2}, \qquad \text{etc.}$$

Assim, a derivada de ordem $k \in [n]$ é então:

$$f^{(k)}(x) = n(n-1)\cdots(n-k+1)(x+1)^{n-k} = \frac{n!}{(n-k)!}(x+1)^{n-k},$$

pelo que, usando a fórmula de Taylor em $x = 0$:

$$(x+1)^n = \sum_{k=0}^{n} \frac{f^{(k)}(0)}{k!}x^k = \sum_{k=0}^{n} \frac{1}{k!}\frac{n!}{(n-k)!}x^k = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

Agora, fazendo a mudança de variável $x \mapsto \frac{x}{y}$, e multiplicando por y^n obtemos:

$$(x+y)^n = y^n(\frac{x}{y}+1)^n = y^n \sum_{k=0}^{n} \binom{n}{k}(\frac{x}{y})^k = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k},$$

como queriamos provar. □

Como mencionado, os números binomiais aparecem também no bem conhecido "triângulo de Pascal".

5.3. **O triângulo de Pascal.** O triângulo de Pascal é o triângulo que começa com 1 no vértice superior e em que cada entrada é a soma dos 2 números imediatamente acima:

$$\begin{array}{ccccccccccc}
 & & & & 1 & & & & & & \\
 & & & 1 & & 1 & & & & & \\
 & & 1 & & 2 & & 1 & & & & \\
 & 1 & & 3 & & 3 & & 1 & & & \\
1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 5 & & 10 & & 10 & & 5 & & & \\
 & & & & \cdots & & & & & &
\end{array}$$

Vamos indexar as linhas horizontais do triângulo de Pascal, começando de cima para baixo com a linha índice zero e, em cada linha indexamos os elementos da esquerda para a direita começando também no zero. Assim, na linha n, vamos designar o k-ésimo elemento por C_k^n. Desta forma, a propriedade que define estes números é:

$$C_k^{n+1} = C_{k-1}^n + C_k^n, \tag{5.1}$$

quando $n \geq k \geq 0$. Esta relação chama-se a relação de Pascal.

Como sucede muitas vezes na matemática, existem relações simples entre conceitos, funções ou números que, à partida, não teriam nada a ver uns com outros. No nosso caso, não deixa de ser surpreendente a estreita relação entre os números binomiais - definidos com *factoriais* - e os números do triângulo de Pascal - definidos por *somas recursivas*.

Corolário 5.13. *Para quaisquer $n \in \mathbb{N}_0$, $k \in [n]_0$, temos $C_k^n = \binom{n}{k}$.*

Demonstração. Vamos provar por indução em n. É fácil de ver que $C_0^0 = \binom{0}{0}$, $C_0^1 = \binom{1}{0}$ e $C_1^1 = \binom{1}{1}$. Agora supomos que $C_k^n = \binom{n}{k}$ para todo o $k \in [n]_0$. No teorema vimos a fórmula

$$(x+1)^n = \sum_{k=0}^{n} \binom{n}{k} x^k,$$

para todo o $n \in \mathbb{N}$, pelo que:

$$\begin{aligned}(x+1)^{n+1} = (x+1)(x+1)^n &= \sum_{k=0}^{n} \binom{n}{k} x^{k+1} + \sum_{k=0}^{n} \binom{n}{k} x^k = \\ &= \sum_{k=1}^{n+1} \binom{n}{k-1} x^k + \sum_{k=0}^{n} \binom{n}{k} x^k = \\ &= \sum_{k=0}^{n+1} \left[\binom{n}{k-1} + \binom{n}{k} \right] x^k,\end{aligned}$$

onde se usou $\binom{n}{-1} = \binom{n}{n+1} = 0$. Concluímos então que

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} = C_{k-1}^n + C_k^n = C_k^{n+1},$$

como pretendido. □

A fórmula do binómio de Newton permite várias conclusões interessantes sobre os números binomiais.

Proposição 5.14. *Para qualquer $n \in \mathbb{N}$ temos $\sum_{j=0}^{n} \binom{n}{j} = 2^n$.*

Demonstração. Fazendo $x = y = 1$ na fórmula do binómio de Newton, temos:

$$2^n = (1+1)^n = \sum_{j=0}^{n} \binom{n}{j} 1^j 1^{n-j} = \sum_{j=0}^{n} \binom{n}{j},$$

como pretendido. □

Exercício 5.15. Mostre que $\sum_{j=0}^{k} (-1)^j \binom{k}{j} = 0$.

5.4. **Números multinomiais.** Os números binomiais podem generalizar-se da seguinte forma.

Definição 5.16. Seja $k \in \mathbb{N}$. Um número k-multinomial (ou simplesmente multinomial) é definido por uma partição de um natural n em k parcelas não negativas: $n = n_1 + \cdots + n_k$, onde $n_j \in \mathbb{N}_0$. Define-se então:

$$\binom{n}{n_1, n_2, \cdots, n_k} := \frac{n!}{n_1! n_2! \cdots n_k!}$$

A fórmula do binómio de Newton generaliza-se também a potências de somas de várias variáveis.

Proposição 5.17. *Sendo $x_1, \cdots, x_k$ variáveis, temos:*

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{n_1 + \cdots + n_k = n} \binom{n}{n_1, n_2, \cdots, n_k} x_1^{n_1} \cdots x_k^{n_k}.$$

Exemplo 5.18. Vamos calcular o coeficiente de $x^5 y^3 z^2$ em $(x+y+z)^{10}$. Como os expoentes de x, y e z são, respectivamente, 5, 3 e 2, o coeficiente pretendido é simplesmente

$$\binom{10}{5,3,2} = \frac{10!}{5!3!2!} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{3 \cdot 2 \cdot 2} = 10 \cdot 9 \cdot 4 \cdot 7 = 2520.$$

Problemas de Revisão.

5.1 Se o menu de um restaurante tem 4 entradas, 6 pratos principais e 3 sobremesas, quantos menus completos diferentes se podem compor? Quantas combinações diferentes tem um cadeado com código composto por 4 algarismos (de 0 a 9)?

5.2 Quantos números em $\mathbb{N}_0$ têm 6 ou menos algarismos? Quandos destes são múltiplos de 5? Quantos destes têm exactamente um algarismo igual a 3 e outro igual a 4?

5.3 No Euromilhões são sorteados 5 números de 1 a 50. Qual a probabilidade de sairem 3 números pares e dois ímpares? Fazendo uma aposta com 7 números, qual a probabilidade de acertar em pelo menos 3 números?

5.4 Uma moeda (perfeita) é atirada ao ar 20 vezes.
(a) Qual a probabilidade de sairem 10 caras e 10 coroas?
(b) Qual das seguintes apostas é mais vantajosa? (A) "vão sair 10 caras e 10 coroas"; (B) "vai sair um número de caras diferente do número de coroas"

5.5 Sendo X e Y conjuntos finitos, determine o número de funções $f : X \to Y$ em função de $n = |X|$ e $m = |Y|$? Quantas são as funções injectivas entre os mesmos conjuntos?

5.6 Sendo $\mathscr{P}(X)$ o conjunto das partes do conjunto finito X, encontre uma bijecção entre $\mathscr{P}(X)$ e o conjunto das funções $X \to [2]$ (Justifique que a função encontrada é injectiva e sobrejectiva).

5.7 Prove a seguinte igualdade de números binomiais (para $n \geq k \geq 1$):

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

5.8 Prove a seguinte igualdade:

$$\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}.$$

5.9 Determine os coeficientes de x^2y^8, y^5z^5 e de $x^2y^3z^5$ no polinómio $(x+y+z)^{10}$. Calcule os coeficientes de y^2x e de x^2y no polinómio $(2+x-y)^5$.

5.10 Quantos anagramas têm as palavras PULGA, ASSIS e MATEMÁTICA? Quantos anagramas da palavra MATEMÁTICA têm as 5 vogais seguidas? [ignore o acento do "A"]

5.11 De quantas maneiras diferentes se podem colocar 7 bolas brancas (idênticas entre si) e 8 bolas pretas (também iguais) em 15 caixas numeradas de 1 a 15?

5.12 Uma cidade tem ruas na direcção Este-Oeste e avenidas na direcção Norte-Sul. Supomos que só podemos deslocar-nos para Este ou para Norte. (a) Quantos trajectos diferentes existem entre um determinado cruzamento A e outro cruzamento B, que se encontra 3 avenidas a Este, e 5 ruas a Norte de A? (b) Em geral, quantos trajectos diferentes existem entre A e o cruzamento que fica m avenidas a Este, e n ruas a Norte de A, $m, n \in \mathbb{N}$?

5.13 Mostre que, para quaisquer naturais $n.m \in \mathbb{N}$, temos $m \mid \binom{mn}{n}$. Use esta propriedade para mostrar que

$$m! \mid \binom{nm}{n, n, \cdots, n}$$

(o coeficiente multinomial tem m entradas iguais a n em baixo).

5.14 Mostre que, num conjunto de 6 pessoas, existem sempre 3 pessoas que se conhecem todas entre si, ou 3 que são desconhecidas 2 a 2 (ou ambos os casos).

5.15 Quantos pares de subconjuntos (X, Y) existem tais que $X \subset Y \subset [n]$?

6. Os Princípios Gerais de Contagem

No sentido de sistematizar os vários argumentos de contagem que foram utilizados na secção anterior, vamos agora estabelecer algumas regras simples, mas de aplicação muito ampla, a que chamamos os *princípios gerais de contagem*.

6.1. **Princípios da identidade e da adição.** O princípio da identidade é óbvio, pelo que vimos antes, mas não deixa de ser importante mencioná-lo. Recorde-se que escrevemos $X \longleftrightarrow Y$ quando existe uma bijecção (função bijectiva) $f : X \to Y$ (ver Apêndice).

Princípio da Identidade:

- Podemos determinar o número de elementos de um conjunto X, encontrando uma bijecção com outro conjunto A cujo cardinal conhecemos. Sucintamente, $|X| = |A|$ sempre que existe uma bijecção $A \longleftrightarrow X$.

Exemplo 6.1. Esta prinícpio foi usado na determinação do cardinal do conjunto potência, $\mathscr{P}(X) := \{Y \subset X\}$, sendo X um conjunto finito. Agora, fazendo uma pequena variação, consideremos a seguinte bijecção:

$$\begin{aligned} F : \mathscr{P}(X) &\to \mathscr{F}(X, \{0,1\}) \\ Y &\mapsto \chi_Y, \end{aligned}$$

onde $\chi_Y : X \to \{0,1\}$ é a chamada função característica do subconjunto $Y \subset X$. Esta é definida como:

$$\begin{aligned} \chi_Y : X &\to \{0,1\} \\ x &\mapsto \begin{cases} 1, & \text{se } x \in Y \\ 0, & \text{se } x \notin Y. \end{cases} \end{aligned}$$

Não é muito difícil ver que existe uma correspondência biunívoca entre subconjuntos $Y \subset X$ e funções características. Assim, concluímos que $|\mathscr{P}(X)| = |\mathscr{F}(X, \{0,1\})|$. Por sua vez, a proposição 5.3 dá-nos uma bijecção entre $\mathscr{F}(X, \{0,1\})$ e o conjunto das n-sequências no conjunto $\{0,1\}$, onde $|X| = n$, que tem cardinal 2^n. Assim, finalmente:

$$|\mathscr{P}(X)| = |\mathscr{F}(X, \{0,1\})| = 2^{|X|}.$$

Exercício 6.2. Mostre que a função inversa da função $F : \mathscr{P}(X) :\to \mathscr{F}(X, \{0,1\})$ do exemplo acima é:

$$\begin{aligned} F^{-1} : \mathscr{F}(X, \{0,1\}) &\to \mathscr{P}(X) \\ f &\mapsto f^{-1}(1), \end{aligned}$$

sendo $f^{-1}(1)$, a pré-imagem de 1, naturalmente um subconjunto de X, e por isso, elemento de $\mathscr{P}(X)$.

O cardinal de uma união disjunta é também intuitiva.

Princípio da adição:

- O número de elementos de uma união disjunta é a soma dos cardinais de cada um deles. Sucintamente:

$$|A_1 \sqcup \cdots \sqcup A_n| = |A_1| + \cdots + |A_n| = \sum_{j=1}^{n} |A_j|.$$

Exemplo 6.3. O princípio da adição permite determinar os cardinais de $A \setminus B$ e de $A \cup B$, em função de $|A|$ e $|B|$. Assim, por definição, $A \setminus B = A \setminus (A \cap B)$. Desta forma, temos a união disjunta $A = (A \setminus B) \sqcup (A \cap B)$ e, pelo princípio da adição:

$$|A \setminus B| = |A| - |A \cap B|.$$

De igual forma, podemos escrever $A \cup B$ como a união disjunta:

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

Logo, o princípio da adição, dá-nos:

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

Este é o caso mais simples do famoso princípio de inclusão-exclusão, que abordaremos abaixo, no caso geral.

6.2. **Princípio dos cacifos ("pigeonhole").** Este princípio é também bastante evidente, embora tenha, por vezes, aplicações que parecem surpreendentes:

Princípio dos cacifos:

- Se $n+1$ cartas (ou mais) são distribuídas por n cacifos, então fica, pelo menos, um cacifo com mais de uma carta.

Obviamente, este princípio não é mais que uma reformulação do Corolário A.13 que afirma que não podem haver funções injectivas $f:[n+1]\to[n]$ (ou $f:[m]\to[n]$ com $m>n$).

Aqui deixamos três exemplos de aplicação deste princípio.

Exemplo 6.4. Num conjunto de $n+1$ pontos (arbitrários, iguais ou não) no intervalo $[0,n]\subset\mathbb{R}$, há sempre dois cuja distância é menor ou igual a 1. De facto, considerando cada um dos n subintervalos $[i,i+1]\subset[0,n]$ (com $i=0,\cdots,n-1$) como um "cacifos" (de modo a que todos os "cacifos" sejam conjuntos disjuntos, cada ponto inteiro pode ser considerado parte do subintervalos à direita ou à esquerda, a escolha é indiferente). Então, temos $n+1$ pontos em n cacifos, pelo que há dois num certo subintervalo. Assim, estes dois pontos não podem distar mais que uma unidade.

Exemplo 6.5. Em cada escolha de 257 bytes de forma aleatória (um byte é um conjunto de 8 bits ou, de forma equivalente, um número que, na base 2, tem ≤ 8 algarismos), há pelo menos 2 bytes iguais. De facto, os bytes estão em correspondência com 8-sequências de zeros e uns, e portanto há 256 bytes diferentes. Assim, pelo princípio dos cacifos, se escolhemos 257 temos necessariamente dois iguais.

O princípio dos cacifos pode ser extendido à seguinte forma mais geral.

Proposição 6.6. *Se distribuímos $n>mk$ cartas por k cacifos, então há pelo menos um cacifo que fica com mais que m cartas.*

Demonstração. A distribição de n cartas diferentes por k cacifos diferentes corresponde a uma aplicação $f:[n]\to[k]$. Se todos os cacifos ficam com m cartas ou menos, isto equivale a ter $|f^{-1}(j)|\leq m$ para todo $j\in[k]$. Assim, pelas propriedades da imagem inversa, temos:

$$n=|[n]|=|f^{-1}([k])|=|f^{-1}(1)\sqcup\cdots\sqcup f^{-1}(k)|\leq km,$$

o que prova o enunciado: $n>km$ implica que existe $j\in[k]$ com $|f^{-1}(j)|>m$. □

Exemplo 6.7. Vamos supor que sortearmos 12 exercícios, um exercício para cada aluno de uma turma de 49 alunos. Como a cada aluno apenas se atribui um exercício o papel das cartas é representado pelos alunos e o dos cacifos é representado pelos 12 exercícios. Assim, como $49>4\cdot 12$, haverá pelo menos um exercício que foi atribuído a 5 ou mais alunos.

6.3. **Princípio da multiplicação e da divisão. Princípio da multiplicação:**

- Se todos os elementos x de um dado conjunto X são obtidos através de n escolhas parciais $x_i\in X_i$ e independentes entre si, de elementos dos conjuntos $X_1,\cdots,X_n$, então o cardinal de X é o produto dos cardinais dos X_i, $i=1,\cdots,n$. Abreviadamente:

$$|X_1\times\cdots\times X_n|=|X_1|\cdots|X_n|=\prod_{j=1}^{n}|X_i|.$$

Exemplo 6.8. Vimos que o cardinal do conjunto $\mathcal{F}(X,Y)$, das funções de X em Y (conjuntos finitos) é precisamente $|\mathcal{F}(X,Y)|=|Y|^{|X|}$.

Outra forma de enunciar este princípio é a seguinte:

Proposição 6.9. *O número de escolhas ordenadas de 1 elemento de X_1, 1 elemento de X_2 etc, é o produto das cardinais: $|X_1|\cdots|X_n|$. Em particular, o número de escolhas ordenadas e com possível repetição, de n elementos de um mesmo conjunto Y, é $|Y|^n$.*

Demonstração. Para a segunda afirmação note-se que estamos a considerar elementos do conjunto $Y\times\cdots\times Y=Y^{\times n}$. □

Exemplo 6.10. Vamos determinar o cardinal do conjunto dos divisores de n, sabendo a sua decomposição em números primos. Seja $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ onde os primos p_j são todos distintos dois a dois. Sabemos que um divisor d tem a decomposição $d = p_1^{c_1} \cdots p_k^{c_k}$ com $c_i \in \{0, 1, \cdots, e_i\} = [e_i]_0$ para todo o $i \in [k]$, e todos estes divisores são distintos (para expoentes diferentes). Assim d é obtido escolhendo um valor de $c_i \in [e_i]_0$ para cada $i \in [k]$. Ou seja

$$|\mathsf{Div}(n)| = |[e_1]_0| \cdot |[e_2]_0| \cdots |[e_k]_0| = (e_1 + 1) \cdots (e_k + 1).$$

Alternativamente, temos uma bijecção entre $\mathsf{Div}(n)$ e o produto cartesiano $[e_1]_0 \times \cdots \times [e_k]_0$.

No mesmo círculo de ideias temos o seguinte enunciado evidente.

Princípio da dupla contagem:

- Se contarmos o número de elementos de um dado conjunto de duas formas distintas, obtemos o mesmo número.

O exemplo seguinte, ilustrando o príncipio da dupla contagem, usa uma combinação de outros princípios de contagem mencionados anteirormente.

Exemplo 6.11. (Identidade de Vandermonte) Podemos usar o princípio da dupla contagem para mostrar a seguinte fórmula

$$\binom{n+m}{k} = \sum_{j=0}^{k} \binom{n}{j} \binom{m}{k-j}.$$

De facto, podemos calcular quantas são as escolhas de k elementos em $X \sqcup Y$ (união disjunta), com $|X| = n$ e $|Y| = m$, de duas formas diferentes. A primeira forma dá o coeficiente binomial da esquerda $\binom{n+m}{k}$, pois $|X \sqcup Y| = n + m$. Para a segunda forma, consideramos subconjuntos $A \subset X$ com j elementos e $B \subset Y$ com $k - j$ elementos, de forma a que $|A \cup B| = k$. Estas escolhas são independentes, pelo que podemos multiplicá-las, obtendo $\binom{n}{j}\binom{m}{k-j}$. Como, temos que considerar todos os $j \in [n]$, que são mutuamente exlcusivos (intersecção vazia para j's diferentes), estamos perante uma união disjunta, o que nos dá o somatório, pelo princípio da adição.

Princípio do quociente, ou da divisão: Este é também um princípio evidente, que pode ser descrito da seguinte forma:

- Se um conjunto X é a união disjunta de vários subconjuntos, todos com o mesmo cardinal n, então o número de subconjuntos é:

$$k = |X|/n.$$

Na forma $|X| = kn$, este enunciado torna-se uma consequência imediata do princípio da adição. No entanto, na forma indicada $k = |X|/n$, o princípio do quociente é útil quando temos $|X|$, o cardinal de um conjunto dado, e queremos o número de subconjuntos com uma dada propriedade (que é uniforme: todos os subconjuntos com igual cardinal).

Exemplo 6.12. Queremos distribuir 12 presentes, todos diferentes, a 4 crianças, de forma a que cada criança fique com 3. De quantas formas diferentes podemos fazer a distribuição?

Podemos considerar as distribuições dos 12 presentes numerados de 1 a 12 como uma sequência. Por exemplo, a sequência:

$$(4, 2, 11, 1, 7, 5, \cdots)$$

significa que a criança 1 fica com os primeiros 3 presentes da sequência: 4, 2 e 11; a criança 2 fica com os presentes 1, 7 e 5, etc. O conjunto X de todas estas sequências (sendo as permutações de 12) tem cardinal 12!. Mas como, naturalmente, ficar com os presentes 1, 7 e 5 é o mesmo que ficar com os presentes 1, 5 e 7, podemos considerar a divisão do conjunto X em subconjuntos de cardinal $(3!)^4$, que são as distribuições com os mesmos presentes para

cada criança, uma vez que correspondem a permutações dos 3 presentes, para cada criança, independentemente. Assim, como queremos o número de subconjuntos, o número de distribuições verdadeiramente diferentes é $\frac{12!}{(3!)^4}$.

O prinípio do quociente pode ser abordado de uma forma mais geral usando a noção de relação de equivalência. Recorde-se que uma relação de equivalência no conjunto X é uma relação reflexiva, simétrica e transitiva. Por isso, dada uma relação de equivalência $\sim$ num conjunto finito X, podemos escrever:

$$X = X_1 \sqcup X_2 \sqcup \cdots \sqcup X_k$$

onde cada X_i é uma classe de equivalência. Dito de outra forma, se $x \sim y$ então x e y estão no mesmo subconjunto X_i e vice-versa: se x e y não estão relacionados por $\sim$ então pertencem a diferentes subconjuntos X_i.

O princípio do quociente pode então exprimir-se da seguinte forma alternativa:

- Se um conjunto X, de cardinal n, tem uma relação de equivalência em que todas as classes de equivalência têm cardinal k, o número total de classes de equivalência é:

$$k = |X|/n.$$

A equivalência entre esta formulação e a anterior deverá ser evidente.

6.4. **O princípio de Inclusão-Exclusão.** O princípio de Inclusão-Exclusão generaliza a fórmula para o cardinal da união. Acima, vimos que

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

para quaisquer dois conjuntos finitos A e B. Não é muito difícil ver que, para 3 conjuntos, aplicando o princípio da adição a uma união disjunta conveniente, vamos obter:

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

É conveniente encontrar uma fórmula geral para a união de um número arbitrário (finito) de conjuntos finitos.

Vamos então tratar da união de vários conjuntos e podemos assumir, sem perda de generalidade, que *todos eles* são subconjuntos de um grande conjunto U a que chamamos *universo*. Sendo $X \subset U$, denotamos por X^c o complementar de X no universo U, isto é:

$$X^c := U \setminus X.$$

Recordemos que a função χ_X função característica de X (em U) é a única função $\chi_X : U \to \{0,1\}$ que vale 1, nos elementos de X e zero nos elementos de X^c. Observemos que esta função verifica as seguintes propriedades:

$$\chi_{X\cap Y} = \chi_X \chi_Y, \qquad |X| = \sum_{x \in U} \chi_X(x), \tag{6.1}$$

que são de fácil demonstração.

Teorema 6.13. *[Princípio de Inclusão-Exclusão]. Sejam $X_1, \cdots, X_n$ conjuntos finitos, considerados como subconjuntos de um conjunto X. Então temos:*
(a) (versão união)

$$|X_1 \cup \cdots \cup X_n| = \sum_{k=1}^{n} (-1)^{k-1} S_k;$$

(b) (versão intersecção)

$$\left|X_1^c \cap \cdots \cap X_n^c\right| = \sum_{k=0}^{n} (-1)^k S_k.$$

Aqui, $S_k = \sum_{1 \le i_1 < \cdots < i_k \le n} \left|X_{i_1} \cap \cdots \cap X_{i_k}\right|$ (soma por todos os índices crescentes) e $S_0 := |X|$.

Demonstração. Em primeiro lugar, observe-se que as duas verões são equivalentes. De facto:

$$X \setminus (X_1 \cup \cdots \cup X_n) = (X \setminus X_1) \cap \cdots \cap (X \setminus X_n) = X_1^c \cap \cdots \cap X_n^c,$$

e $|X \setminus Y| = |X| - |Y|$. Vamos provar a segunda versão. Seja 1 a função identicamente 1 em todo o X, e vamos denotar por $\chi_i : X \to \{0,1\}$ a função característica de X_i. Considere-se a função:

$$\chi_{X_1^c} \cdots \chi_{X_n^c} = (1-\chi_1)(1-\chi_2)\cdots(1-\chi_n) = \sum_{k=0}^{n} (-1)^k \prod_{1 \le i_1 < \cdots < i_k \le n} \chi_{i_1} \cdots \chi_{i_k}.$$

Isto dá o resultado, de acordo com as fórmulas (6.1). □

Exemplo 6.14. Como sabemos, existem 5^7 palavras de 7 letras apenas com as vogais $\{a,e,i,o,u\}$. Quantas destas palavras existem sem a sequência uau?

Para responder a esta questão, vamos considerar o universo X, de cardinal 5^7 de todas as palavras de 7 letras só com vogais. Precisamos de determinar o cardinal do complementar das palavras que contém a sequência uau. Assim, definimos:

$$A_i = \{\text{palavras em } X \text{ com a sequência } uau \text{ a começar na posição } i\},$$

e é fácil de ver que $A_i = \varnothing$ para $i \ge 6$. Portanto só temos $A_1, \cdots, A_5$ e cada um destes tem o mesmo cardinal. Por exemplo

$$A_3 = \{xyuauwz \,:\, x,y,w,z \text{ são vogais abitrárias}\}$$

Assim, $|A_j| = 5^4$ para $j \in [5]$. Agora, vemos que as duplas intersecções verificam:

$$|A_1 \cap A_3| = |A_3 \cap A_5| = |A_2 \cap A_4| = 5^2, \qquad \text{e} \qquad |A_1 \cap A_4| = |A_2 \cap A_5| = |A_1 \cap A_5| = 5$$

(as restantes são vazias) e a única tripla intersecção não vazia é:

$$|A_1 \cap A_3 \cap A_5| = 1.$$

Assim, o PIE, na versão complementar, fornece a resposta:

$$|X| - \sum_{j=1}^{5} |A_j| + \sum_{1 \le i < j \le 5} |A_i \cap A_j| - |A_1 \cap A_3 \cap A_5| = 5^7 - 5 \cdot 5^4 + 3 \cdot 5^2 + 3 \cdot 5 - 1 = 75089.$$

O PIE pode ser usado para determinar o número de funções sobrejectivas.

Proposição 6.15. *Sejam $n > k$ números naturais. O número de funções $f : [n] \to [k]$ sobrejectivas distintas é dado por:*

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

Demonstração. Vamos usar o PIE. O nosso universo é o conjunto $\mathscr{F}([n],[k])$ de todas as funções $f : [n] \to [k]$. Este conjunto tem cardinal k^n, como vimos antes. Agora temos que retirar a este conjunto as funções que não são sobrejectivas. Seja:

$$A_i := \{\text{funções cuja imagem é disjunta de } \{i\}\} = \{f : [n] \to [k] \,:\, f^{-1}(i) = \varnothing\},$$

para índice $i \in [k]$. Da mesma forma, para cada conjunto de j índices distintos $1 \le i_1 < \cdots < i_j \le n$, definimos:

$$A_{i_1,i_2,\cdots,i_j} := \{f : [n] \to [k] \,:\, f^{-1}(i_1) = \cdots = f^{-1}(i_j) = \varnothing\},$$

que são sa funções cuja imagem é disjunta do conjunto $\{i_1, \cdots, i_j\}$, de cardinal j. Então $|A_{i_1,i_2,\cdots,i_j}| = (k-j)^n$, para todo o $j \in [k]$. Como há $\binom{k}{j}$ diferentes conjuntos com j índices, o PIE fornece a fórmula acima. □

6.5. **Polinómios simétricos.** É interessante notar a estreita relação entre a fórmula do Binómio de Newton e o Princípio de Inclusão-Exclusão que, em particular, torna clara a última igualdade na demonstração do Teorema 6.13.

Esta ligação pode ser vista como uma elementar (embora não trivial) aplicação da propriedade distributiva, e como uma forma de introdução à teoria dos polinómios simétricos. Esta teoria começa com a propriedade distributiva aplicada a números reais x e y:

$$(1+x)(1+y) = 1+x+y+xy.$$

Com três variáveis, temos:

$$(1+x)(1+y)(1+z) = 1+(x+y+z)+(xy+xz+yz)+xyz,$$

em que os parêntesis agrupam monómios do mesmo grau. Podemos generalizar estes produtos a qualquer número de variáveis.

Proposição 6.16. *Seja $n \in \mathbb{N}$, e sejam $x_1, \cdots, x_n \in \mathbb{R}$. Então, temos:*

$$\begin{aligned}\prod_{i=1}^{n}(1+x_i) &= 1+\sum_{k=1}^{n} x_k + \sum_{1\le i<j\le n} x_i x_j + \\ &\quad + \cdots + \sum_{1\le i_1<\cdots<i_k\le n} x_{i_1}\cdots x_{i_k} + \cdots + x_1 x_2 \cdots x_n.\end{aligned}$$

Demonstração. Vamos fazer a demonstração por indução em n. O caso $n=1$ é simples:

$$(1+x_1) = 1+x_1,$$

pois, para o lado direito da expressão, não existem dois índices $1 \le i < j \le 1$. Vamos agora desenvolver, usando o passo de indução:

$$\begin{aligned}(1+y)\left(\prod_{i=1}^{n}(1+x_i)\right) &= \prod_{i=1}^{n}(1+x_i) + y\prod_{i=1}^{n}(1+x_i) = \\ &= 1+\sum_{k=1}^{n} x_k + \sum_{1\le i<j\le n} x_i x_j + \cdots + x_1 x_2 \cdots x_n, \\ &\quad + y + \sum_{k=1}^{n} x_k y + \sum_{1\le i<j\le n} x_i x_j y + \cdots + x_1 x_2 \cdots x_n y \\ &= 1 + \left(y + \sum_{k=1}^{n} x_k\right) + \left(\sum_{1\le i<j\le n} x_i x_j + \sum_{k=1}^{n} x_k y\right) + \\ &\quad + \cdots + x_1 \cdots x_n y \\ &= 1 + \sum_{k=1}^{n+1} x_k + \sum_{1\le i<j\le n+1} x_i x_j + \cdots + x_1 x_2 \cdots x_n x_{n+1}\end{aligned}$$

onde se fez, no último passo, a substituição $x_{n+1} = y$. □

Observação 6.17. Os polinómios importantes na Proposição são (além de $e_0 := 1$):

$$\begin{aligned}e_1 &:= x_1 + x_2 + \cdots + x_n \\ e_2 &:= \sum_{1\le i<j\le n} x_i x_j = x_1x_2 + x_1x_3 + \cdots + x_n x_{n-1} \\ &\vdots \\ e_n &:= \prod_{k=1}^{n} x_k = x_1 x_2 \cdots x_n\end{aligned}$$

e são fundamentais na teoria dos polinómios simétricos, que não poderemos desenvolver. Limitamo-nos a fazer a definição seguinte.

Definição 6.18. Sendo $x_1, \cdots, x_n$ variáveis, os polinómios $1, e_1, e_2, \cdots, e_n$ que aparecem na Proposição 6.16 chamam-se os *polinómios simétricos elementares* nas variáveis x_i, $i \in [n]$.

Observação 6.19. Note-se também que a propriedade distributiva é válida em qualquer corpo, como por exemplo o corpo $\mathbb{C}$ dos números complexos. Mais geralmente, as fórmulas acima também são válidas em qualquer anel comutativo! Assim, para funções $f_1, \cdots, f_n$ de uma variável x, temos também:

$$\begin{aligned}\prod_{i=1}^{n}(1+f_i(x)) &= 1+\sum_{k=0}^{n} f_k(x)+\sum_{0\le i<j\le n} f_i(x)f_j(x)+\cdots+ \\ &\quad+\sum_{0\le i_1<\cdots<i_k\le n} f_{i_1}(x)\cdots f_{i_k}(x)+\cdots+f_1(x)f_2(x)\cdots f_n(x).\end{aligned}$$

Esta última fórmula permite mostrar tanto o PIE, como a fórmula do binómio de Newton.

De facto, O PIE é consequência de tomarmos $f_i(x) = -\chi_i(x)$, a (o simétrico da) função característica do conjunto $X_i \subset X$, tal como foi usado no Teorema 6.13. Por seu lado, a fórmula do binómio de Newton é consequência de tomarmos $f_i(x) = x$ para todo o $i \in [n]$. Neste caso, a fórmula acima fica:

$$(1+x)^n = 1+\binom{n}{1}x+\binom{n}{2}x^2+\cdots+\binom{n}{k}x^k+\cdots+\binom{n}{n}x^n,$$

que foi o passo fundamental na prova do Teorema 5.12.

6.6. **Distribuições de bolas em caixas.** Como temos visto, vários dos problemas de combinatória podem ser interpretados como problemas de distribuição de bolas em caixas.

Dados números naturais n e k, vamos então considerar o número de formas diferentes de distribuir n bolas por k caixas. É muito importante distinguir os casos em que as bolas e as caixas são ou não são indistinguíveis.

É também muito útil considerar **distribuições injectivas** - aquelas em que nenhuma das caixas fica com mais de uma bola, e as **distribuições sobrejectivas** - as que não deixam nenhuma caixa sem bolas.

O primeiro caso é aquele em que tanto as n bolas como as k caixas são distintas. Neste caso, numerando as bolas de 1 a n e as caixas de 1 a k interpretamos imediatamente uma tal distribuição como uma função $f : [n] \to [k]$. De facto, se colocamos a bola número j na caixa número l, então definimos $f(j) := l$, e vice-versa: a função determina f a forma de distribuição das bolas. Dessa forma, temos 3 casos que já vimos anteriormente: o de todas as funções $[n] \to [k]$, o das funções injectivas, e o das sobrejectivas.

Proposição 6.20. *Dadas n bolas diferentes, e k caixas diferentes, o número de formas de distribuir as bolas pelas caixas é k^n. As distribuições injectivas são $\frac{k!}{(k-n)!}$, se $k \ge n$ (e zero, caso contrário), e as distribuições sobrejectivas são:*

$$\sum_{j=0}^{k-1}(-1)^j\binom{k}{j}(k-j)^n, \quad \text{se } n \ge k$$

(e zero, caso contrário).

Como segundo caso, temos o caso de bolas iguais e caixas diferentes. Neste caso, usamos o método das *"bolas e paredes"*. Como as bolas são todas iguais, e podemos organizar as caixas ordenadamente da esquerda para a direita, cada distribuição deste tipo pode ser descrita como uma sequência de " $\circ$ ", que representam bolas, e de " $\times$ ", que representam paredes entre as

caixas. Por exemplo, com $n=7$, $k=5$ podemos ter a distribuição:

$$\circ\circ\circ\circ\times\times\circ\circ\times\circ\times,$$

que corresponde a colocar 4, 0, 2, 1, 0 bolas nas caixas 1 a 5, respectivamente. Assim, como o número de cruzes é igual ao número de caixas menos 1, temos $n+k-1$ objectos, e devemos escolher as $k-1$ posições das cruzes (ou equivalentemente as n posições das bolas). Novamente, estes casos já foram vistos, pelo que deixamos os detalhes para o leitor.

Proposição 6.21. *Dadas n bolas iguais (indistinguíveis) e k caixas diferentes, o número de formas de distribuir as bolas pelas caixas, é:*

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

O número de distribuições injectivas (resp. sobrejectivas) é:

$$\binom{k}{n}, \quad (\textit{resp.} \quad \binom{n-1}{k-1})$$

no casos $k \geq n$ (resp. $n \geq k$).

6.7. **Números de Stirling e partições.** Para prosseguir, consideramos os casos das caixas iguais. A primeira observação é a seguinte.

Lema 6.22. *Se temos n bolas (iguais ou diferentes) e $k \geq n$ caixas iguais, há apenas uma forma de distribuição* injectivas *das bolas pelas caixas.*

Demonstração. Para distribuições injectivas, uma vez que só pode haver zero ou uma bola por caixa, todas as distribuições são equivalentes a colocar todas as caixas ocupadas para a esquerda e as desocupadas para a direita. □

Necessitamos agora de introduzir os chamados números de Stirling.

Definição 6.23. O **número de Striling** $\left\{ {n \atop k} \right\}$ é o número de formas diferentes de escrever o conjunto $[n]$ como *união disjunta* de k subconjuntos *não vazios.*

Observação 6.24. Estes números são frequentemente chamados números de *Stirling de segunda espécie*, mas vamos chamá-los simplesmente "números de Stirling" porque não falaremos dos de primeira espécie.

Exemplo 6.25. Temos $\left\{ {4 \atop 2} \right\} = 7$ uma vez que há 7 formas distintas de escrever o conjunto $[7]$ como união disjunta de 2 conjuntos não vazios:

$$\begin{aligned} \{1,2,3,4\} &= \{1,2\}\sqcup\{3,4\} = \{1,3\}\sqcup\{2,4\} = \{1,4\}\sqcup\{2,3\} = \\ &= \{1,2,3\}\sqcup\{4\} = \{1,2,4\}\sqcup\{3\} = \{1,3,4\}\sqcup\{2\} = \{2,3,4\}\sqcup\{1\}. \end{aligned}$$

É muito fácil verificar que $\left\{ {n \atop k} \right\}$ é o número de *distribuições sobrejectivas* de n bolas diferentes em k caixas iguais, pois cada caixa corresponde a um dos subconjuntos de $[n]$, e não há caixas vazias.

Proposição 6.26. *Temos a equação:*

$$k!\left\{ {n \atop k} \right\} = \sum_{j=0}^{k-1} (-1)^j \binom{k}{j} (k-j)^n$$

Demonstração. Vimos anteriormente que uma distribuição sobrejectiva de n bolas diferentes em k caixas *diferentes* equivale a uma função sobrejectiva $f : [n] \to [k]$, e o número destas é:

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

pelo Princípio de Inclusão-Exclusão. Uma vez que agora não queremos distingtuir as caixas, pelo princípio do quociente, temos apenas que dividir por $k!$, o número de permutações das k caixas. □

Finalmente, notamos também o seguinte, consequência de considerarmos todos os casos, com caixas vazias ou não.

Lema 6.27. *O número de distribuições de n bolas diferentes em k caixas iguais é igual a*

$$\sum_{j=1}^{k} \left\{ {n \atop j} \right\}$$

6.8. **Partições.** Finalmente, para estudar as distribuições de bolas iguais em caixas iguais, precisamos do conceito de partição de um natural.

Definição 6.28. Seja $n \in \mathbb{N}$. Uma partição de n é uma forma de escrever n como soma de várias parcelas. Mais precisamente, uma igualdade:

$$n = n_1 + n_2 + \cdots + n_k,$$

com $n_1 \geq n_2 \geq \cdots n_k > 0$ representa uma partição de n em k partes.

Exemplo 6.29. (1) Para $n = 6$ temos as seguintes partições em 3 partes

$$6 = 3+2+1, \qquad 6 = 4+1+1$$

(2) O número total de partições de $n = 4$ é 5. De facto:

$$4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1.$$

Definição 6.30. Denotamos por $P_k(n)$ o número de partições de n com k partes, de modo a que $P(n) = \sum_{k=1}^{n} P_k(n)$. Note-se que uma "parte" é sempre um natural (e portanto $\neq 0$).

Proposição 6.31. *As partições de n em k partes estão em bijecção com as distribuições sobrejectivas de n bolas iguais em k caixas iguais.*

Corolário 6.32. *O número de distribuições de n bolas iguais em k caixas iguais é igual a:*

$$\sum_{j=1}^{k} P_j(n).$$

Terminamos este capítulo com a chamada "Tabela das 12 entradas", que incluí todos as distribuições de bolas em caixas que considerámos.

número de distribuições	n bolas dif.	n bolas iguais	n bolas dif.	n bolas iguais
de bolas em caixas	k caixas diferentes		k caixas iguais	
Total	k^n	$\binom{n+k-1}{k-1}$	$\sum_{j=1}^{k} \left\{ {n \atop j} \right\}$	$\sum_{j=1}^{k} P_j(n)$
Injectivas ($n \leq k$)	$\frac{k!}{(k-n)!}$	$\binom{k}{n}$	1	1
Sobrejectivas ($n \geq k$)	$k! \left\{ {n \atop k} \right\}$	$\binom{n-1}{k-1}$	$\left\{ {n \atop k} \right\}$	$P_k(n)$

Problemas de Revisão.

6.1 Seja X um conjunto de 38 números naturais todos menores que 1000. Mostre que há dois elementos $x, y \in X$ tais que $|x - y| \leq 26$.

6.2 Considere o conjunto Y das 3-sequências em $\{a,b,c,d\}$ com possível repetição. Mostre que qualquer sequência de 65 elementos de Y (com possível repetição) tem pelo menos 2 elementos iguais.

6.3 Seja X um conjunto de 22 inteiros arbitrários. Mostre que existe $k \in \{0,1,\cdots,5,6\}$, e pelo menos quatro elementos $x \in X$, que verificam $x \equiv k \bmod 7$.

6.4 Queremos distribuir 10 bolas iguais por 4 caixas diferentes. (a) Quantas distribuições diferentes existem? (b) Destas, quantas não deixam nenhuma caixa vazia? (c) E quantas há, de forma a que uma das caixas fique com 8 bolas?

6.5 Queremos resolver a equação $x_1+x_2+x_3+x_4=10$ com $x_i \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$. (a) Quantas soluções (diferentes) há? (b) E se restringirmos a $x_i \leq 7$ (c) E quantas soluções há com $x_1 = x_2$?

6.6 Fez-se o seguinte inquérito sobre hobbies numa turma de 40 alunos. Há 18 alunos que gostam de xadrez, 23 que gostam de natação, e vários de skate. Os que gostam simultaneamente de xadrez e natação são 9. Há 7 que gostam de xadrez e skate, e 12 que gostam de natação e skate. Os que gostam das 3 actividades são 4 (todos os alunos gostam de alguma actividade). Quantos alunos gostam de skate?

6.7 Quantos naturais $n \leq 200$ são divisíveis por 2, por 3 ou por 5?

6.8 Queremos colorir n objectos com uma de 3 cores: azul, verde ou encarnado. (a) De quantas formas o podemos fazer se os objectos forem iguais? (b) E se os objectos são todos diferentes? (c) Responda às mesmas perguntas (a) e (b), considerando que todas as 3 cores são usadas.

6.9 Quantas palavras de 8 letras, no alfabeto usual de 26 letras, não têm uma ou mais vogais?

6.10 Quantas 10-sequências sem repetição no conjunto $\{0,1,2,\cdots,9\}$ existem que contenham (pelo menos) uma das sequências $(1,2,3)$, $(3,4,5)$ ou $(4,5,6)$ como subsequência?

6.11 Quantas palavras com quatro letras A, seis B e cinco C (15 letras no total), contêm a sequência "ABBA"?

6.12 Considere os conjuntos $A=\{a,b,c,d,e,f\}$ e $B=[4]$. (a) Quantas funções existem de A para B? (b) Quantas funções $f: A \to B$ são sobrejectivas? (c) Quantas funções $f: A \to B$ têm $|f^{-1}(1)|=3$?

6.13 Seja $\left\{ {n \atop k} \right\}$ o número de Stirling (de 2ª espécie), o número de partições do conjunto $[n]$ em k subconjuntos não vazios. (a) Usando a relação de recorrência

$$\left\{ {n+1 \atop k} \right\} = k \left\{ {n \atop k} \right\} + \left\{ {n \atop k-1} \right\}$$

determine $\left\{ {n \atop k} \right\}$ para $1 \leq k \leq n \leq 7$

(b) Mostre que $\left\{ {n \atop n-1} \right\} = \binom{n}{2}$ e que $\left\{ {n \atop 2} \right\} = 2^{n-1}-1$.

6.14 Seja $P(n,k)$ o número de distribuições de n bolas iguais em k caixas iguais, sem caixas vazias. (a) Mostre que $P(n,1)=1$, e $P(n,k)=P(n-1,k-1)+P(n-k,k)$

(b) Determine a fórmula geral de $P(n,2)$, $n \geq 2$

(c) Determine $P(n,k)$ para $1 \leq k \leq n \leq 6$.

6.15 [Desafio difícil] Seja p um número primo.

(a) Mostre que $p \mid \binom{p}{k}$, para qualquer $k \in [p-1]$

(b) Mostre que $p \mid \left\{ {p \atop k} \right\}$, para qualquer $k \in [p-1]$.

7. Funções Geradoras e Recorrências Lineares

No capítulo anterior estudámos n-sequências num conjunto X, que são n-tuplos ordenados:

$$(x_1, x_2, \cdots, x_n) \in X^n$$

ou, de forma equivalente, funções $f : [n] \to X$. Vamos agora considerar sequências *infinitas* $(x_1, x_2, \cdots, x_k, \cdots)$ em conjuntos bem conhecidos como os números reais $\mathbb{R}$ ou os complexos $\mathbb{C}$ e que, em Análise, se chamam sucessões. Na realidade, estamos principalmente interessados em sucessões de números inteiros $\mathbb{Z}$ ou racionais $\mathbb{Q}$, mas o tratamento é igual em $\mathbb{R}$ ou em $\mathbb{C}$, havendo algumas vantagens em usar estes últimos, como veremos.

7.1. **Funções geradoras.** Uma n-sequência de números reais é simplesmente um elemento $(a_1, a_2, \cdots, a_n)$ do espaço vectorial $\mathbb{R}^n$, ou seja, um vector com n entradas, tal como se estuda em Álgebra Linear.

Há outra forma de pensar em k-sequências de números reais: como polinómios de grau $< k$, numa variável x. Para isso, usando índices começando em zero, à sequência $(a_0, a_1, \cdots, a_{k-1})$ associamos o polinómio:

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \in \mathbb{R}[x],$$

que tem grau $< k$. Aqui, $\mathbb{R}[x]$ denota o anel dos polinómios com coeficientes reais[7]. A motivação para esta associação pode não ser muito clara, mas na verdade, já usámos esta técnica anteriormente ao demonstrar a fórmula do binómio de Newton.

Exemplo 7.1. Fixemos $n \in \mathbb{N}$. O polinómio de grau n associado à sequência de números naturais $a_k := \binom{n}{k}$, ou seja, a $(\binom{n}{0}, \binom{n}{1}, \cdots, \binom{n}{n})$ é:

$$\sum_{k=0}^{n} \binom{n}{k} x^k = (x+1)^n,$$

tal como vimos na demonstração do Teorema 5.12.

Vamos agora sistematizar e generalizar esta observação com as seguintes definições, passando a usar o termo *sucessão*, em vez de *sequência*.

Definição 7.2. Uma sucessão (finita ou) infinita de números reais $(a_0, a_1, \cdots)$ será denotada simplesmente por (a_n) (ou por $(a_n)_{n \in \mathbb{N}_0}$ quando for necessário explicitar o conjunto de índices, usualmente $\mathbb{N}_0$, mas pode ser outro conjunto adequado). A série

$$f(x) := \sum_{n=0}^{\infty} a_n x^n$$

será chamada a **função geradora** da sucessão (a_n).

Assim, uma função geradora $f(x)$ é uma generalização de um polinómio, tal como as séries em análise, mas há uma enorme diferença: não estamos preocupados em saber se a série converge ou tem algum limite, como na Análise. Assim, esta função geradora pode ser considerada simplesmente como uma *série formal*.

Com esta terminologia, o exemplo anterior diz-nos que $(x+1)^N$ é a função geradora da sucessão dos números binomiais $(\binom{N}{n})$.

O exemplo mais importante de função geradora que não é um polinómio é o da série geométrica.

Exemplo 7.3. A série geométrica, escrita como a função racional $1/(1-x)$, é a função geradora da sucessão infinita $(1, 1, \cdots)$. De facto, para $|x| < 1$,

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n,$$

como é bem sabido.

[7] Note-se que $\mathbb{R}[x]$ (bem como $\mathbb{C}[x]$) é de facto um anel com as operações de soma e produto usuais)

Observação 7.4. Como argumentámos, não estamos interessados na questão da convergência das séries. Se estivéssemos, diríamos que a igualdade acima só é válida se a série do lado direito converge, o que acontece para $|x|<1$, mas não para $|x|>1$. A menos que explicitamente se mencione o contrário, todas as igualdades que escreveremos serão válidas para uma região do tipo $|x|<\delta$ para certo δ real positivo. Mas como este "raio de converência" será absolutamente acessório, não precisaremos de indicá-lo, nem repetir este tipo de observação doravante.

Exercício 7.5. (a) Mostre que a função geradora da sucessão $(a_n)=(1,1,\cdots,1,0,0,\cdots)$ em que o primeiro zero aparece na posição N é $\frac{1-x^N}{1-x}$. (b) Mostre que a função geradora da sucessão $(\frac{1}{n!})$ é a função exponencial.

Em combinatória, muitas funções geradoras são funções racionais, tal como o caso da série geométrica. Recorde que uma *função racional* é o quociente de dois polinómios, ou seja, uma função da forma:

$$f(x)=\frac{p(x)}{q(x)},$$

onde $p(x),q(x)\in\mathbb{R}[x]$ e $q(x)$ não é o polinómio nulo.

Exercício 7.6. Determine, como função racional, a função geradora da sucessão: $(a_n)=(3^n)$.

No estudo das sucessões as funções geradoras permitem usar todas as ferramentas da análise (apesar de se tratar tipicamente de séries formais). De facto, sem nos preocuparmos com questões de convergência, podemos derivar e primitivar séries de potências e assim, encontrar funções geradoras para novas sucessões.

Exemplo 7.7. Derivando a igualdade

$$\frac{1}{1-x}=\sum_{n=0}^{\infty}x^n,$$

obtemos:

$$\frac{1}{(1-x)^2}=\sum_{n=0}^{\infty}n\,x^{n-1}=0+1x^0+2x^1+\cdots=\sum_{n=0}^{\infty}(n+1)x^n.$$

Desta forma, acabámos de calcular a função geradora da sucessão $(1,2,3,\cdots)=(n+1)_{n\in\mathbb{N}_0}$.

O *método das fracções simples* permite determinar todas as sucessões cujas funções geradoras são funções racionais. Vamos ilustrar o método com o seguinte exemplo.

Exemplo 7.8. Queremos determinar a sucessão (u_m) cuja função geradora é:

$$f(x)=\frac{4x-23}{2x^2+5x-3}.$$

Para aplicar o método das fracções simples, começamos por factorizar o denominador:

$$2x^2+5x-3=0 \quad\Leftrightarrow\quad x=\frac{-5\pm\sqrt{25+24}}{4}=\frac{\pm7-5}{4},$$

logo $2x^2+5x-3=2(x+3)(x-\frac{1}{2})=(x+3)(2x-1)$. Agora escrevemos:

$$\frac{4x-23}{2x^2+5x-3}=\frac{A}{x+3}+\frac{B}{2x-1},$$

e para determinar A e B fazemos:

$$4x-23=A(2x-1)+B(x+3).$$

o que nos dá: $A=5$ e $B=-6$. Desta forma, temos:

$$f(x)=\frac{5}{x+3}-\frac{6}{2x-1}=\frac{\frac{5}{3}}{1+\frac{x}{3}}+\frac{6}{1-2x}=\frac{5}{3}\sum_{n\geq0}(-\frac{x}{3})^n+6\sum_{n\geq0}(2x)^n.$$

Assim, a sucessão pretendida é:

$$(u_n) = \left(\frac{5}{3}\left(-\tfrac{1}{3}\right)^n + 6 \cdot 2^n \right).$$

7.2. **Sucessões definidas por recorrência.** Uma sucessão de números reais

$$(u_n)_{n\in\mathbb{N}_0} = (u_0, u_1, \cdots, u_k, \cdots)$$

diz-se que é *definida por recorrência* se temos uma fórmula para u_n que envolve os termos anteriores u_{n-1}, u_{n-2}, etc (um número finito de termos).

Exemplo 7.9. A sucessão mais famosa das definidas por recorrência é a sucessão dos inteiros de Fibonacci $F_0, F_1, F_2, \cdots$, dada por:

$$F_{n+2} = F_{n+1} + F_n,\ n \geq 0,$$

e com as condições iniciais (ie, os 2 primeiros termos) $F_0 = 0$, $F_1 = 1$. Dada a equação de recorrência acima, é fácil calcular alguns dos primeiros termos. De facto, $F_2 = F_1 + F_0 = 1$, $F_3 = 1+1 = 2$, $F_4 = 2+1 = 3$, $F_5 = 3+2 = 5$, $F_6 = 8$, etc. Torna-se claro que seria útil ter uma fórmula geral que calculasse F_n, para todo o $n \in \mathbb{N}$. Vamos obter esta fórmula, como caso particular de um método muito útil para este tipo de *recorrências lineares*.

Em geral, uma equação entre u_n e k os termos anteriores só determina unicamente a sucessão (u_n) se indicarmos os primeiros k termos. Estes termos chamam-se assim, em paralelo com a teoria das Equações Diferenciais, as *condições iniciais* (da equação de recorrência).

Vamos então concentrar-nos nas *recorrências lineares*, isto é, nas recorrências da forma:

$$u_{n+k} = F(u_n, u_{n+1}, \cdots, u_{n+k-1}),$$

onde F é uma função linear das suas k variáveis, para certo $k \in \mathbb{N}$. Mais precisamente, fazemos a seguinte definição.

Definição 7.10. Uma equação de **recorrência linear homogénea de ordem** $k \in \mathbb{N}$ é uma equação da forma:

$$u_{n+k} = a_{k-1}u_{n+k-1} + \cdots + a_1 u_{n+1} + a_0 u_n, \quad n \in \mathbb{N}_0,$$

onde $a_0, \cdots, a_{k-1}$ são constantes, usualmente números inteiros, racionais ou reais. Se, ao membro direito adicionarmos b_n, $n \in \mathbb{N}_0$ (uma outra sucessão dada), a equação chama-se recorrência linear **não homogénea** (de ordem k). Se temos uma destas recorrências (de ordem k) e um conjunto de k condições iniciais, $(u_0, u_1, \cdots, u_{k-1}) \in \mathbb{R}^k$ então dizemos que temos um **problema de recorrência de ordem** k.

Exemplo 7.11. A sucessão dos números de Fibonacci $(0, 1, 1, 2, 3, 5, 8, 13, \cdots)$ é a solução do problema de recorrência:

$$F_{n+2} = F_{n+1} + F_n,\ n \geq 0, \quad F_0 = 0, \quad F_1 = 1$$

que consiste numa recorrência linear homogénea de ordem 2 e nas condições iniciais indicadas. Se mudarmos as condições iniciais, por exemplo: $F_0 = F_1 = 4$, mantendo a equação de recorrência, obteríamos a sucessão:

$$(4, 4, 8, 12, 20, 32, \cdots)$$

bem diferente dos números de Fibonacci originais.

7.3. **Problemas de recorrência lineares homogéneos.** Vamos descrever um método para obter o termo geral de um problema de recorrência linear. Para isso, começamos com a observação de que a linearidade permite somar soluções diferentes.

Proposição 7.12. *Se x_n e y_n são soluções da equação de recorrência linear homogénea, então $ax_n + by_n$ também o é, para qualquer $a, b \in \mathbb{R}$.*

Demonstração. Isto é consequência dos seguintes cálculos, usando a hipótese:

$$\begin{aligned} ax_{n+k}+by_{n+k} &= a(a_{k-1}x_{n+k-1}+\cdots+a_0x_n)+b(a_{k-1}y_{n+k-1}+\cdots+a_0y_n)= \\ &= a_{k-1}(ax_{n-k+1}+by_{n+k-1})+\cdots+a_0(ax_n+by_n), \end{aligned}$$

pelo que a sucessão $(z_n) := (ax_n + by_n)$ verifica a mesma recorrência que (x_n) e que (y_n). □

Definição 7.13. O **polinómio característico** da equação de recorrência (linear homogénea de ordem k)

$$u_{n+k} = a_{k-1}u_{n+k-1}+\cdots+a_1u_{n+1}+a_0u_n$$

é $p(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_1x - a_0$, que é um polinómio (mónico) de ordem k.

Recorde-se que um polinómio chama-se mónico quando o coeficiente do monómio de maior grau (neste caso x^k) é 1.

Proposição 7.14. *Se λ é raiz do polinómio $p(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_1x - a_0$, então, a sucessão definida por:*

$$u_n := \lambda^n$$

é uma solução da equação de recorrência linear $u_{n+k} = a_{k-1}u_{n+k-1}+\cdots+a_1u_{n+1}+a_0u_n$.

Demonstração. Por hipótese $p(\lambda) = 0$ o que equivale a

$$\lambda^k - a_{k-1}\lambda^{k-1} - \cdots - a_1\lambda - a_0 = 0.$$

Com $u_n := \lambda^n$, temos:

$$u_{n+k} = \lambda^{n+k} = a_{k-1}\lambda^{n+k-1}+\cdots+a_1\lambda^{n+1}+a_0\lambda^n = a_{k-1}u_{n+k-1}+\cdots+a_1u_{n+1}+a_0u_n,$$

como queriamos provar. □

Vamos agora ver alguns casos de problemas de recorrência que, como aplicação dos dois resultados anteriores, podem já ser resolvidos: casos em que podemos encontrar de forma sistemática, uma fórmula geral para u_n.

Teorema 7.15. *Considere o seguinte problema de recorrência linear homogéneo de ordem 2:*

$$\begin{cases} u_{n+2} = a\,u_{n+1} + b\,u_n, \quad n \geq 0 \\ u_0 = c \\ u_1 = d, \end{cases}$$

e suponha que o polinómio caracterísico $x^2 - ax - b = 0$ tem duas raízes distintas $\lambda \neq \mu$. Então, a solução é única, e tem a forma:

$$u_n = \alpha\lambda^n + \beta\mu^n,$$

onde α e β verificam: $\alpha + \beta = c$, $\alpha\lambda + \beta\mu = d$.

Demonstração. Como λ e μ são soluções do polinómio característico, sabemos que $(\alpha\lambda^n + \beta\mu^n)_{n\in\mathbb{N}}$ é uma solução da recorrência $u_{n+2} = a\,u_{n+1} + b\,u_n$. De facto, pela Proposição 7.14, as sequências (λ^n) e que (μ^n) são soluções, e pela Proposição 7.12, sabemos que uma combinação linear é também solução. Com $n = 0$, temos $u_0 = \alpha + \beta$ e com $n = 1$, temos $u_1 = \alpha\lambda + \beta\mu$. Pelo que α e β são solução da seguinte equação matricial linear:

$$\begin{pmatrix} 1 & 1 \\ \lambda & \mu \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix},$$

que existe sempre e é única, uma vez que a matriz é invertível (pois o seu determinante é $\mu - \lambda \neq 0$). □

Note-se que, na notação do teorema, o polinómio característico factoriza-se como

$$x^2 - ax - b = (x - \lambda)(x - \mu),$$

pelo que $a = \lambda + \mu$ e $b = -\lambda\mu$.

Exemplo 7.16. Vamos, finalmente, determinar o termo geral da sucessão de Fibonacci, e a sua função geradora. A equação de recorrência é $F_{n+2} = F_{n+1} + F_n$ pelo que o polinómio característico é $x^2 - x - 1$. Vamos denotar as raizes, obtidas pela fórmula resolvente, por ϕ e ψ:

$$\frac{1 \pm \sqrt{1+4}}{2}, \quad \Rightarrow \quad \phi = \frac{1+\sqrt{5}}{2}, \quad \psi = \frac{1-\sqrt{5}}{2}$$

pelo que temos

$$F_n = \alpha \left(\frac{1+\sqrt{5}}{2}\right)^n + \beta \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Agora, temos $0 = F_0 = \alpha + \beta$, pelo que $\beta = -\alpha$ e $1 = F_1 = \alpha\frac{1+\sqrt{5}}{2} + \beta\frac{1-\sqrt{5}}{2} = \alpha\sqrt{5}$. Assim, encontrámos o termo geral:

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n \right] = \frac{1}{\sqrt{5}}(\phi^n - \psi^n).$$

Note-se que $\phi := \frac{1+\sqrt{5}}{2}$ é o chamado número de ouro pelas suas interessantes relações com várias quantidades na natureza, e que $\psi = 1 - \phi$.

A função geradora dos números de Fibonacci é então:

$$f(x) = \frac{1}{\sqrt{5}} \left[\frac{1}{1-\phi x} - \frac{1}{1-\psi x} \right] = \frac{1}{\sqrt{5}} \frac{(\phi - \psi)x}{1 - (\phi+\psi)x + \phi\psi x^2} = \frac{x}{1 - x - x^2}.$$

Tal como mencionado antes, muitas das funções geradoras estudadas no contexto da combinatória são funções racionais, e a sucessão de Fibonacci é exemplo disso. Note-se ainda, neste caso, a simetria entre o polinómio característico $p(x) = x^2 - x - 1$, e o denominador de $f(x)$ que é igual a $1 - x - x^2 = x^2 p(\frac{1}{x})$. Este fenómeno é bastante geral, como podemos observar.

Corolário 7.17. *A função geradora do problema de recorrência do Teorema 7.15 é uma função racional. Mais precisamente é da forma*

$$f(x) = \frac{q(x)}{1 - ax - bx^2} = \frac{q(x)}{x^2 p(\frac{1}{x})},$$

onde $q(x)$ é um polinómio de grau ≤ 1, com $q(0) = u_0$.

Demonstração. Sejam λ e μ as raizes do polinómio característico, como no teorema. As funções geradoras das sucessões (λ^n) e (μ^n) são

$$\frac{1}{1-\lambda x}, \quad \text{e} \quad \frac{1}{1-\mu x},$$

respecivamente. Assim, a função geradora da solução $(u_n) = (\alpha\lambda^n + \beta\mu^n)$ é precisamente

$$\frac{\alpha}{1-\lambda x} + \frac{\beta}{1-\mu x} = \frac{\alpha + \beta - x(\alpha\mu + \beta\lambda)}{1 - (\lambda+\mu)x + \lambda\mu x^2},$$

o que nos dá o resultado pretendido uma vez que $a = \lambda + \mu$ e $b = -\lambda\mu$. Finalmente note-se que $\alpha + \beta = u_0$: o termo constante de q é precisamente o termo zero da sucessão (u_n). □

O seguinte resultado trata das recorrências lineares quando o polinómio característico tem duas raízes iguais.

Teorema 7.18. *Considere o seguinte problema de recorrência (linear homogéneo) de ordem 2:*

$$\begin{cases} u_{n+2} = a\,u_{n+1} + b\,u_n, & n \geq 0 \\ u_0 = c \\ u_1 = d, \end{cases}$$

e suponha que o polinómio caracterísico $x^2 - ax - b = 0$ tem uma raiz múltipla λ. Então, a solução é única, e tem a forma:

$$u_n = \alpha\lambda^n + \beta n\lambda^n,$$

onde α e β verificam: $\alpha = c$, $\alpha\lambda + \beta\lambda = d$. Note-se que, neste caso, $\lambda = \frac{a}{2}$.

Demonstração. Pelo Teorema 7.14, sabemos que (λ^n) é uma solução. Deixamos para o leitor a verificação que $(n\lambda^n)$ é também uma solução. Assim, o resultado segue da linearidade. □

No caso de problemas de recorrência de ordem superior, o seguinte resultado generaliza os teoremas anteriores.

Teorema 7.19. *Considere o seguinte problema de recorrência linear homogéneo de ordem k:*

$$\begin{cases} u_{n+k} = a_{k-1}u_{n+k+1} + \cdots + a_1 u_{n+1} + a_0 u_n, \quad n \geq 0 \\ u_0 = b_0, \quad u_1 = b_1, \quad \cdots, u_{k-1} = b_{k-1}, \end{cases}$$

com polinómio característico $p(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_1 x - a_0$. Então, a função geradora da solução é uma função racional da forma:

$$f(x) = \frac{q(x)}{x^k p(\frac{1}{k})},$$

em que $q(x)$ tem grau $< k$. Se λ é uma raiz de $p(x)$ com multiplicidade $m \leq k$, então

$$\alpha_1\lambda^n + \alpha_2 n\lambda^n + \cdots + \alpha_m n^{m-1}\lambda^n$$

é uma solução da equação de recorrência (ignorando as condições iniciais). Finalmente, há uma única sólução do problema de recorrência, que é uma combinação linear de soluções deste tipo, para cada raiz de $p(x)$.

7.4. **Caso linear não homogéneo.** Para lidarmos com o caso linear não homogéneo temos o seguinte resultado.

Chamamos *solução geral* de um problema de recorrência (linear ou não) uma solução arbitrára (apenas) da equação de recorrência, sem se ter que verificar as condições iniciais. Assim, pelo Teorema anterior, a solução geral de um problema de recorrência limear homogéneo é uma combinação linear arbitrária de parcelas da forma:

$$\alpha_1\lambda^n + \alpha_2 n\lambda^n + \cdots + \alpha_m n^{m-1}\lambda^n,$$

uma para cada raiz λ do polinómio característico.

Teorema 7.20. *A solução geral de um problema de recorrência linear não homogéneo é igual à soma de uma solução particular (do sistema não homogéneo) com a solução geral do problema homogéneo associado.*

Demonstração. ... □

Infelizmente, não há método geral para encontrar uma solução particular de uma equação de recorrência não homogénea, embora existam métodos para casos concretos. Normalmente, tentam-se soluções do mesmo género que os termos não homogéneos.

Exemplo 7.21. Pretende-se resolver o Problema de Recorrência seguinte:

$$\begin{cases} u_{n+1} = n2^n - \frac{1}{2}u_n, \quad n \geq 0 \\ u_0 = 1. \end{cases}$$

Neste caso a equação de recorrência homogénea do mesmo é $u_{n+1} = -\frac{1}{2}u_n$ pelo que a sua solução geral é $u_n = \alpha(-\frac{1}{2})^n$ (uma vez que o polinómio característico $p(x) = x + \frac{1}{2}$ tem raiz $-\frac{1}{2}$).

Sendo $n2^n$ o termo não homogéneo, vamos tentar uma solução particular da forma:

$$u_n = an2^n + b2^n.$$

Substituindo na equação de recorrência, vem:

$$u_{n+1} = a(n+1)2^{n+1} + b2^{n+1} = n2^n - \frac{1}{2}(an2^n + b2^n),$$

que, removendo o factor comum 2^n, equivale a

$$2a(n+1)+2b = n - \frac{an}{2} - \frac{b}{2} \quad \Leftrightarrow \quad \begin{cases} 2an + \frac{an}{2} & = n \\ 2a + 2b & = -\frac{b}{2} \end{cases}$$

cuja solução (única) é $a = \frac{2}{5}$ e $b = -\frac{8}{25}$. A solução particular é então $(\frac{2}{5}n2^n - \frac{8}{25}2^n)$. Assim, a solução do problema de recorrência é $\alpha(-\frac{1}{2})^n + \frac{2}{5}n2^n - \frac{8}{25}2^n$, com α a ser determinado pela condição inicial $u_0 = 1$. Assim, com $n = 0$ vem $\alpha - \frac{8}{25} = 1$, pelo que $\alpha = \frac{33}{25}$, e a solução do problema é:

$$u_n = \frac{33}{25}(-\tfrac{1}{2})^n + \frac{n2^{n+1}}{5} - \frac{2^{n+3}}{25}.$$

Problemas de Revisão.

7.1 Escreva, como funções racionais, as funções geradoras das sequências $u_n = 4^{n+2} + 5$ e $v_n = 2^n + (-3)^{n+1}$.

7.2 Escreva, como funções racionais (ou polinomiais), as funções geradoras das sequências $a_n = \binom{23}{n}$ e $b_n = 2\binom{n}{2}$.

7.3 Pelo método das frações simples, determine a sucessão (u_n) cuja função geradora é

$$\frac{6+5x}{1-3x+2x^2}.$$

7.4 Defina, através de *recorrências lineares*, as seguintes sequências e e determine o respectivo termo geral:
(a) Número de subconjuntos de um conjunto com n elementos
(b) Número de n-sequências no conjunto $\{0,1,2\}$
(c) $u_n = n^2$.

7.5 Duas rectas concorrentes no plano definem 4 regiões (o seu complemento em $\mathbb{R}^2$). Quantas regiões são determinadas por n rectas no plano, supondo que todas são concorrentes duas a duas e que não há 3 rectas concorrentes no mesmo ponto? Consegue determinar o termo geral da respectiva sucessão?

7.6 Determine o termo geral e a função geradora racional do problema de recorrência: $u_{n+2} = 4u_n$, $u_0 = 1$, $u_1 = 3$.

7.7 Determine o termo geral e a função geradora racional do problema de recorrência: $u_{n+2} = 4u_{n+1} - 4u_n + n$, $u_0 = 3$, $u_1 = 5$ [tente uma solução particular da forma $an + b$].

7.8 Determine o termo geral do problema de recorrência: $u_{n+1} = 4u_n + n^2$, $u_0 = 1$. [tente uma solução particular da forma $an^2 + bn + c$].

7.9 Considere a sucessão de números pentagonais (p_n). Esta sucessão é dada por $p_n = \sum_{k=0}^{n-1} a_k$ onde (a_n) é a sucessão de termo geral $a_n = 1 + 3n$, $n \geq 0$. Defina a sucessão (p_n) por recorrência, determine o seu termo geral e a sua função geradora racional.

7.10 Determine o termo geral e a função geradora racional do problema de recorrência: $u_{n+4} = 8u_{n+2} - 16u_n$, $u_0 = u_2 = 0$, $u_1 = 24$, $u_3 = 160$.

7.11 Considere o seguinte problema de recorrência linear

$$a_0 = 1,\ a_1 = 2, \quad a_{n+2} = 5a_{n+1} - 4a_n, \quad n \geq 0.$$

Mostre que a função geradora de (a_n) é $f(x) = \frac{7-8x}{3-12x}$ e determine o seu termo geral.

7.12 Sabendo que a função geradora do problema de recorrência: $u_n = au_{n-1} + bu_{n-2} + cu_{n-3}$, é $f(x) = \frac{\alpha}{x-1} + \frac{\beta x+\gamma}{4+6x+x^2}$ determine os coeficientes a, b e c. Sabendo que $u_0 = 0$, $u_1 = u_2 = 1$, calcule α, β e γ.

7.13 Seja $A(x)$ a função geradora da sequência (a_n), $n \geq 0$. Determine as funções geradoras $P(x)$, $Q(x)$ e $R(x)$, respectivamente, das sequências $p_n := 5a_n$, $q_n := a_n + 5$ e $r_n := a_{n+5}$.

7.14 Supomos que temos um número ilimitado de moedas de 5, 10, 20 cêntimos. Determine a função geradora para o número de maneiras b_n de escolher n moedas com as seguintes restrições: o número de moedas de 5 cêntimos é múltiplo de 4, o número de moedas de 10 cêntimos é ≤ 3 e o número de moedas de 20 cêntimos é superior a 2. Qual o termo geral de b_n?

7.15 [Desafio] Seja (u_n) uma sucessão que verifica uma relação de recorrência linear homogénea de ordem k com polinómio característico $p(x)$. Mostre que a função geradora respectiva é racional, tendo como denominador o polinómio $x^k p(\frac{1}{k})$, e como numerador um polinómio de grau menor que k.

8. Permutações e Contagens com Simetria

Neste capítulo, vamos considerar problemas de *contagem com simetria*. O conceito de simetria é um conceito fundamental, tanto em Matemática, como em qualquer Ciência Natural ou Humana. Não é muito difícil encontrar padrões e simetrias na natureza, o que foi sempre motivação histórica para o desenvolvimento da Ciência e da Tecnologia. Por exemplo, uma bola de sabão toma sempre a forma esférica, e ninguém duvida da utilidade da roda, um objecto particularmente simétrico, na construção, na indústria e em múltiplos outros contextos.

Para entender rigorosamente o conceito de simetria torna-se necessário introduzir a estrutura algébrica de *grupo*. No contexto da matemática finita, um grupo que adquire particular relevância é o chamado grupo simétrico de n elementos, pelo que começamos por estudar este grupo.

8.1. Permutações de n elementos.

Seja $n \in \mathbb{N}$.

Definição 8.1. Uma permutação de n elementos, é uma bijecção do conjunto $[n]$. Por outras palavras, é uma função $\sigma : [n] \to [n]$ que é bijectiva: injectiva e sobrejectiva.

Tipicamente, as permutações denotam-se por letras gregas, e o conjunto das permutações de n elementos designa-se por S_n. A permutação $\sigma \in S_n$ que envia $i \in [n]$ em $\sigma(i) \in [n]$, pode escrever-se como a sequência das suas imagens $\sigma = (\sigma(1), \sigma(2), \cdots, \sigma(n))$, ou da seguinte forma explícita:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Veremos abaixo uma notação abreviada para as permutações.

Como são funções bijectivas definidas no mesmo conjunto, as permutações podem compor-se da mesma forma que as funções. Além disso, qualquer permutação tem um inverso, dado pela correspondente função inversa. A permutação que corresponde à função identidade, $\sigma(i) = i$, para todo $i \in [n]$) denota-se por $\mathbf{1}$.

Exemplo 8.2. Para $n = 6$, seja $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}$ e $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 1 & 6 \end{pmatrix}$. Então podemos determinar as permutações inversas e as compor as permutações ρ e π de forma imediata:

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix} \qquad \rho^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 2 & 3 & 4 & 6 \end{pmatrix}$$

e

$$\rho\circ\pi=\begin{pmatrix}1&2&3&4&5&6\\3&4&2&5&6&1\end{pmatrix},\qquad \pi\circ\rho=\begin{pmatrix}1&2&3&4&5&6\\3&1&4&6&2&5\end{pmatrix}\neq\rho\circ\pi.$$

O último cálculo mostra que a composição de permutações não é comutativo. Ou seja, em geral, dados $\pi,\rho\in S_n$, $\pi\circ\rho\neq\rho\circ\pi$.

Como sabemos, o conjunto das permutações de n elementos tem cardinal $n!$ (Proposição 5.8):

$$|S_n|=n!$$

Dada uma permutação σ, e $k\in\mathbb{N}$, designamos por σ^k a composição de $\sigma\circ\cdots\circ\sigma$ (operação de composição repetida k vezes).

Lema 8.3. *Seja $\sigma\in S_n$. Então, existe $k\in[n]$, tal que $\sigma^k=1$.*

Demonstração. De facto, como S_n é um conjunto finito, o conjunto das potências de σ, $\{\sigma,\sigma^2,\sigma^3,\cdots,\sigma^k,\cdots\}\subset S_n$ é também finito. Assim, tem que haver repetição de elementos, ou seja $\sigma^m=\sigma^n$ para certos $m,n\in\mathbb{N}$, distintos e, sem perda de generalidade, $m>n$. Assim, sendo $m=n+k$ com $k\in\mathbb{N}$,

$$\sigma^{n+k}=\sigma^n\quad\Leftrightarrow\quad(\sigma^n)^{-1}\sigma^{n+k}=(\sigma^n)^{-1}\sigma^n\quad\Leftrightarrow\quad\sigma^k=1,$$

onde usámos a associatividade e o inverso: $(\sigma^n)^{-1}\sigma^{n+k}=(\sigma^n)^{-1}\circ\sigma^n\circ\sigma^k=\sigma^k$. Deixamos para o leitor a verificação que podemos sempre tomar $k\leq n$. □

Definição 8.4. Dado $\sigma\in S_n$, o menor número natural k que verifica $\sigma^k=1$ é chamado a ordem de σ.

Exemplo 8.5. As permutações $\sigma\in S_n$ que apenas trocam dois elementos são chamados **transposições**. A transposição σ que troca $i\neq j$ ($\sigma(i)=j$ e $\sigma(j)=i$) mas fixa todos os outros elementos de $[n]$, tem ordem 2. De facto $\sigma^2(i)=i$ e $\sigma^2(j)=j$, tal como sucede com todos os outros elementos de $[n]$.

Definição 8.6. Seja $k\in\mathbb{N}$. Um ciclo de tamanho k é uma permutação σ para a qual existem k elementos distintos $i_1,\cdots,i_k\in[n]$, tal que σ envia i_1 em i_2, i_2 em i_3, etc, e envia i_k novamente em i_1. Abreviadamente, denotamos este ciclo por $(i_1\cdots i_k)$.

Exercício 8.7. (a) Mostre que uma transposição é um ciclo de tamanho 2 e que tem ordem 2. (b) Prove que um ciclo de tamanho k é uma permutação de ordem k.

Dois ciclos $(i_1\cdots i_k)$ e $(j_1,\cdots,j_l)$, no mesmo grupo simétrico S_n. dizem-se *disjuntos* se $\{i_1\cdots i_k\}\cap\{j_1,\cdots,j_l\}=\emptyset$.

Proposição 8.8. *Todas as permutações são composições de ciclos disjuntos.*

Demonstração. Esta prova é construtiva e pode ser deixada para o leitor. □

Com esta proposição podemos usar uma notação abreviada para as permutações, como composição de ciclos.

Exemplo 8.9. A composição de ciclos disjuntos (123)(584)(67) designa a seguinte permutação:

$$\pi=\begin{pmatrix}1&2&3&4&5&6&7&8\\2&3&1&5&8&7&6&4\end{pmatrix}.$$

8.2. **Grupos e Subgrupos.**

Definição 8.10. Um **grupo** é um conjunto G munido de uma operação (pensada como sendo uma multiplicação) associativa, um elemento neutro e (também chamado elemento identidade), e em que todos os elementos têm inverso. Por outras palavras, se $g,h,j\in G$ então a multiplicação $g\cdot h\in G$ verifica:

- $(g \cdot h) \cdot j = g \cdot (h \cdot j)$,
- $g \cdot e = e \cdot g = g$, onde $e \in G$ é o elemento neutro,
- $\exists g^{-1} \in G$ tal que $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Quando $g \cdot h = h \cdot g$ para quaisquer elementos, diz-se que o grupo é **comutativo** ou **abeliano**. Quando a operação e a identidade estão subentendidos, em vez do triplo $(G, \cdot, e)$, este grupo denota-se simplesmente por G. Para simplificar, vamos também deixar de usar o ponto, e escrever gh em vez de $g \cdot h$.

Exemplo 8.11. O conjunto dos números reais, não nulos, é um grupo com a operação de multiplicação. Qualquer espaço vectorial é um grupo, com a operação de soma de vectores. Estes dois casos são grupos comutativos, como se verifica facilmente. Um exemplo de grupo que *não é comutativo* é o grupo das matrizes 2×2 que são invertíveis.

É fácil verificar que o conjunto de bijecções $f : X \to X$ de um qualquer conjunto X é um grupo. Em particular, temos o caso das permutações, detalhado acima.

Proposição 8.12. *O conjunto das permutações de $n > 2$ elementos, S_n, com a operação de composição, é um grupo (não comutativo).*

O grupo S_n é também chamado o *grupo simétrico* de n elementos e tem cardinal $n!$. Neste texto, estamos particularmente interessados em grupos finitos. Quando G é um grupo finito, o seu cardinal $|G|$ também se chama a **ordem de** G.

Definição 8.13. Seja G um grupo finito e $H \subset G$ é um subconjunto que verifica a propriedade: $g \cdot h^{-1} \in H$ para quaisquer $g, h \in H$. Então H diz-se um **subgrupo** de G.

Exemplo 8.14. Seja $m \in \mathbb{N}$. O conjunto dos inteiros modulares $\mathbb{Z}_m$ é um grupo abeliano, com a operação de adição módulo m. Como vimos na parte 1, este conjunto está em bijecção com o conjunto dos restos da divisão inteira por m, ou seja podemos identificar:

$$\mathbb{Z}_m \longleftrightarrow \{0, 1, 2, \cdots, m-1\}$$

O mesmo $\mathbb{Z}_m$ não é um grupo com a operação de multiplicação, pois a classe do zero não é invertível. Se $n \mid m$, por exemplo $m = d \cdot n$, com $d > 1$, deixamos para o leitor a verificação de que

$$\{0,\ n,\ 2n, \cdots, (d-1)n\} \subset \mathbb{Z}_m$$

é um subgrupo de $(\mathbb{Z}_m, +, 0)$.

No contexto da teoria de grupos $\mathbb{Z}_m$ (ou seja, $(\mathbb{Z}_m, +, 0)$) chama-se o **grupo cíclico** de ordem m.

Exercício 8.15. Seja $H \subset G$ um subconjunto de um grupo G.
(a) Mostre que H é um subgrupo se e só se contém a identidade e é fechado para inverso e multiplicação. Isto é, se e só se: (i) $e \in H$; (ii) $g \in H$ implica $g^{-1} \in H$; (iii) $g, h \in H$ implica $g \cdot h \in H$.
(b) Mostre que as 3 condições acima se podem reduzir a uma única, da seguinte forma: H é um subgrupo se e só se $gh^{-1} \in H$ para todo $g, h \in H$.

Dado um grupo finito G e um seu subgrupo H, podemos considerar o conjunto das classes de equivalência por translação. Seja

$$G/H := G/\sim,$$

onde a relação de equivalência é dada por $x \sim y$ se e só se existe $h \in H$ tal que $y = hx$.

Exercício 8.16. Mostre que a relação acima é de facto uma relação de equivalência.

Recorde-se que dado qualquer conjunto X e uma relação de equivalência $\sim$ em X, temos sempre uma aplicação canónica de X em $X/\sim$, que associa a cada elemento $x \in X$ a sua classe de equivalência.

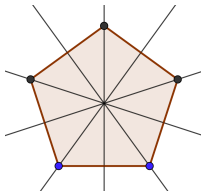


FIGURA 8.1. Simetrias de reflexão do pentágono regular

No caso da relação de equivalência em G dada por um subgrupo H, tal como definido acima, a classe de equivalência de $x \in G$ é dada por:

$$[x] = \{hx : h \in H\}.$$

Proposição 8.17. *[Teorema de Lagrange] Seja G um grupo finito e $H \subset G$ um subgrupo. Então*

$$|G/H| = |G|/|H|.$$

Em particular, se $H \subset G$ é subgrupo, então $|H|$ divide $|G|$.

Demonstração. Consideremos a aplicação natural de G nas classes de equivalência relativas ao subgrupo H:

$$\begin{array}{rcl} \pi : G & \to & G/H \\ g & \to & [g], \end{array}$$

sendo $[g]$ a classe de equivalência de $g \in G$. Esta aplicação é sobrejectiva, por definição de G/H. Assim $|G/H| < |G|$ é finita. Por outro lado, G é a união disjunta das classes de equivalência, e todas estas classes têm o mesmo número de elementos que H. Assim, $|G| = \sum_{\alpha \in G/H} |H| = |H| \cdot |G/H|$. □

Definição 8.18. Dado um grupo G e um seu elemento $g \in G$, diz-se que k **é a ordem de** g se k é o menor natural tal que $g^k = e$ (o elemento neutro de G).

Uma demonstração completamente paralela à do Lema 8.3, mostra que todos os elementos (de um grupo finito) têm ordem finita, e com o teorema de Lagrange podemos mostrar que essa ordem divide a ordem do grupo.

Corolário 8.19. *Seja G um grupo, e $g \in G$. Então a ordem de g divide $|G|$.*

Demonstração. Naturalmente, $H = \{e, g, g^2, g^3, \cdots\}$ é um subgrupo de G. Como $g^k = 1$, sendo k a ordem de g, vemos que $|H| = k$. Assim, pelo Teorema de Lagrange, k divide $|G|$. □

Vamos agora definir os grupos diedrais, que são úteis no estudo das simetrias dos polígonos no plano.

Definição 8.20. O grupo D_n, chamado grupo diedral de ordem $2n$, é o grupo de simetrias de um polígono regular com n lados (onde se incluem todas as rotações e reflexões apropriadas) e tem ordem $2n$.

De forma mais concreta, se colocarmos o nosso polígono na origem de $\mathbb{R}^2$ com um vértice no semi-eixo $x > 0$, o grupo D_n tem n elementos que consistem nas rotações de um ângulo de $\frac{2\pi j}{n}$, com $j = 0, \cdots, n-1$ (no sentido directo, vamos convencionar), e tem outros n elementos que são as reflexões em cada uma das rectas que passam na origem e em vértices ou no ponto médio das arestas. Não é muito difícil verificar que estas rectas fazem ângulos de $\frac{\pi j}{n}$, $j = 0, \cdots, n-1$, com a direcção horizontal, e também se pode provar que estes esgotam todas as simetrias do polígono.

A figura ilustra as simetrias do pentágono, com indicação das rectas de simetria. Há também as rotações de múltiplos de 72º que corresponde a $\frac{2\pi}{5}$ radianos.

8.3. **Acções e simetrias.** Como acabámos de ver no exemplo dos polígonos regulares, a noção de grupo (nesse caso, os grupos diedrais) é muito importante quando estudamos objectos com algum grau de simetria. Quando pretendemos contar o número de certos objectos *tomando em conta as suas simetrias*, isto é o mesmo que introduzir uma relação de equivalência nesse conjunto de objectos, em que tornamos *equivalentes* os objectos que se relacionam por essa simetria.

Para tornar precisas estas considerações precisamos da noção de *acção de um grupo num conjunto*.

Definição 8.21. Uma **acção de um grupo** finito G (com elemento identidade e) **num conjunto** finito X é uma aplicação:

$$\begin{aligned} \psi : G \times X &\to X \\ (g,x) &\mapsto g \cdot x, \end{aligned}$$

que verifica $e \cdot x = x$ e $(gh) \cdot x = g \cdot (h \cdot x)$, para todos os elementos $g, h \in G$, $x \in X$.

Quando temos uma acção de G em X também dizemos que X é um G-conjunto.

As seguintes noções são também extremamente úteis.

Definição 8.22. Seja X um G-conjunto e $x \in X$. O **subgrupo de isotropia** (também chamado **estabilizador**) de x é o subgrupo:

$$G_x := \{g \in G : g \cdot x = x\}.$$

A **órbita** de $x \in X$ é o subconjunto de X:

$$G \cdot x := \{g \cdot x : g \in G\}.$$

Por outras palavras, uma órbita da acção de G em X é uma classe de equivalência da seguinte relação:

$$x \sim y \qquad \text{sse} \quad \exists g \in G : g \cdot x = y$$

Desta forma, quando temos um G-conjunto X, temos, de forma natural uma decomposição de X nas suas órbitas disjuntas.

Teorema 8.23. *[Teorema da órbita-estabilizador] Seja G um grupo finito que actua no conjunto finito X. Temos:*

$$|G| = |G \cdot x| \cdot |G_x|,$$

para todo o $x \in X$.

Demonstração. Fixando $x \in X$ considere-se a aplicação órbita:

$$\begin{aligned} \varphi_x : G &\to G \cdot x \\ g &\mapsto g \cdot x. \end{aligned}$$

Então φ_x é sobrejectiva, e induz uma aplicação nas classes de equivalência $G/G_x \to G \cdot x$. Esta última é bijectiva, como se pode verificar. Assim, como $G_x \subset G$ é um subgrupo, pelo teorema de Lagrange, $|G/G_x| = |G|/|G_x| = |G \cdot x|$. □

Vamos agora estudar o problema de calcular o número de órbitas de um G-conjunto X.

Definição 8.24. O **espaço das órbitas** é o conjunto das classes de equivalência da acção de G em X e denota-se por X/G. Dado $g \in G$, o subconjunto fixo por g é:

$$X^g := \{x \in X : g \cdot x = x\} \subset X.$$

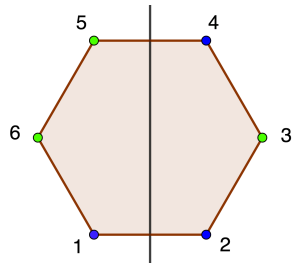


FIGURA 8.2. hexágono com vértices coloridos

Teorema 8.25. *[Teorema de Cauchy-Frobenius-Burnside] Seja G um grupo finito e X um G-conjunto finito. Então:*

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g|.$$

Demonstração. Vamos calcular o número $\sum_{g\in G}|X^g|$ usando a Proposição anterior:

$$\begin{aligned}\sum_{g\in G}|X^g| = \left|\{(g,x)\in G\times X : g\cdot x = x\}\right| = \sum_{x\in X}|G_x| = \\ = |G|\sum_{x\in X}\frac{1}{|G\cdot x|} = \\ = |G|\sum_{Y\in X/G}\sum_{x\in Y}\frac{1}{|Y|} = \\ = |G|\sum_{Y\in X/G}1 = |G|\cdot|X/G|.\end{aligned}$$

como pretendido. □

Este teorema tem inúmeras aplicações interessantes. Vejamos alguns exemplos.

Exemplo 8.26. As órbitas da acção de rotação em torno de um eixo vertical que contem 2 vértices opostos de um octaedro, são apenas 3. Verifiquemos que este número é obtido pela fórmula acima. O nosso conjunto tem 6 vértices, um em cima, outro em baixo, e 4 no "equador". Neste caso o grupo de simetria é $G\cong\mathbb{Z}_4$, o grupo cíclico de ordem 4. Vamos escrever

$$G = \{1, R, R^2, R^3\},$$

onde $1\in G$ é a identidade do grupo, pelo que age sem mover o octaedro; $R\in G$ roda 90º, na direcção positiva (contrário aos ponteiros do relógio, embora isto seja apenas uma convenção); de forma que R^2 roda 180º e $R^3\in G$ roda 270º.

Assim, calculando o número de elementos fixos por cada $j\in\mathbb{Z}_4$, temos:

$$|X^1| = 6, \qquad |X^R| = |X^{R^2}| = |X^{R^3}| = 2,$$

pelo que o Teorema 8.25 diz:

$$|X/G| = \frac{1}{4}(6+2+2+2) = 3,$$

como previsto.

Vamos agora ver um outro problema típico de aplicação do Teorema 8.25.

Exemplo 8.27. Queremos determinar todas as possíveis colorações dos 6 vértices de um hexágono regular com 2 cores: azul e verde. Vamos considerar dois casos distintos: (a) considerando as simetrias de rotação do hexágono; (b) considerando as simetrias de rotação e de reflexão.

(a) Neste caso o grupo de simetria é $G = \{1, R, \cdots, R^5\} \cong \mathbb{Z}_6$, o grupo cíclico de ordem 6, numa notação semelhante à do exemplo anterior. A sua acção no hexágono é por rotação. Assim, cada elemento $R^j \in \mathbb{Z}_6$ roda $j\frac{2\pi}{6}$, na direcção positiva (convenção) com $j = 0, 1, \cdots, 5$.

Agora definimos o conjunto $V = \{a, b, c, d, e, f\}$ dos vértices do hexágono, e $X = \mathscr{F}(V, [2])$ o conjunto das colorações de V com 2 cores,

$$|X^1| = |X| = 2^{|V|} = 2^6, \qquad |X^R| = |X^{R^5}| = 2, \qquad |X^{R^2}| = |X^{R^4}| = 4, \qquad |X^{R^3}| = 8$$

pois as rotações de 60º ou 300º apenas preservam as colorações com todos os vértices iguais, mas as rotação de 120º preserva 4 colorações diferentes, e a de 180º preserva 8. Assim, o Teorema 8.25 implica:

$$|X/\mathbb{Z}_6| = \frac{1}{6}(2^6 + 2 + 4 + 8 + 4 + 2) = \frac{84}{6} = 14.$$

(b) Para considerar as reflexões temos que considerar o grupo diedral D_6. Este é o grupo de todas as reflexões e rotações de um hexágono, e tem 12 elementos: as 6 rotações como acima, e as reflexões em cada uma das rectas com inclinação $j\frac{\pi}{6}$ em relação à recta horizontal, $j = 0, \cdots, 5$, como na figura. Podemos escrever:

$$D_6 = \{e, R, \cdots, R^5, r, rR, \cdots, rR^5\} = \{e, R, \cdots, R^5, r_0, r_1, \cdots, r_5\},$$

onde r_j são as reflexões que fixam as rectas que fazem ângulos de $j\frac{\pi}{6}$ com a recta horizontal.

Temos então:

$$|X^1| = |X| = 2^{|V|} = 2^6, \qquad |X^R| = |X^{R^5}| = 2, \qquad |X^{R^2}| = |X^{R^4}| = 4, \qquad |X^{R^3}| = 8,$$

como na situação (a) e temos ainda:

$$|X^{r_0}| = |X^{r_2}| = |X^{r_4}| = 2^4, \qquad |X^{r_1}| = |X^{r_3}| = |X^{r_5}| = 2^3.$$

Assim, pelo Teorema 8.25 concluímos:

$$|X/D_6| = \frac{1}{12}(2^6 + 2 + 4 + 8 + 4 + 2 + 3 \cdot 2^4 + 3 \cdot 2^3) = \frac{84 + 3 \cdot 24}{12} = 13.$$

Na figura, temos uma coloração que é diferente da obtida por reflexão através da recta vertical. Assim, as duas colorações estão em órbitas diferentes por acção de $\mathbb{Z}_6$, mas na mesma órbita por acção de D_6.

Notando que as órbitas da acção de $\mathbb{Z}_6$ são 14 e as de D_6 são 13, este é precisamente o único caso em que temos uma identificação extra, no caso do grupo D_6.

Problemas de Revisão. Nestes exercícios S_n denota o grupo simétrico em n letras, e $\mathbb{Z}_m = \{0, 1, \cdots, m-1\}$ o grupo cíclico dos inteiros módulo m (com a soma módulo m).

8.1 Considere as permutações $\sigma, \tau \in S_8$ dadas, como composição de ciclos, por $\sigma = (123)(456)(78)$ e $\tau = (1357)(26)(4)(8)$. Determine, na mesma notação, as permutações $\sigma\tau$, $\tau\sigma$, σ^2, σ^{-1}, τ^{-1}.

8.2 Seja $\sigma = (1, \cdots, k)(k+1, \cdots, k+m) \in S_n$ $(k+m \leq n)$. (a) Mostre que a ordem de σ é igual ao mínimo múltiplo comum entre k e m. (b) Se π é um produto de ciclos disjuntos de comprimentos $n_1, \cdots, n_k$ com $n_1 + \cdots + n_k = n$ qual a ordem de π?

8.3 Seja $m \in \mathbb{N}$, e $d \mid m$. (a) Mostre que:

$$\{0, d, 2d, \cdots, m-d, d\} \subset \mathbb{Z}_m$$

é um subgrupo e indique a sua ordem. (b) Se m é primo, quantos subgrupos tem $\mathbb{Z}_m$?

8.4 Quais são os grupos de simetria das letras: "A", "B", "H", "M" e "L" (como subgrupos do grupo D_4, diedral de ordem 8). Qual o grupo de simetria do sinal "+"?

8.5 Seja X um G-conjunto, e $x, y \in X$. Mostre que, se $x \sim y$ (estão na mesma órbita) então os estabilizadores G_x e G_y têm a mesma ordem.

8.6 Considere o grupo $G = \{1, (12), (34), (12)(34)\}$, actuando nas permutações dos 4 algarismos do conjunto $X = \{0, 1, \cdots, 9999\}$ (inteiros de 0 a 9999). Quantas são as órbitas desta acção?

8.7 Seja X o conjunto dos vértices de um cubo e G o subgrupo de S_8 das permutações de X que correspondem a rotações do cubo. Mostre que a acção tem apenas uma órbita e que $|G_x| = 3$, para todo $x \in X$. Qual a ordem de G?

8.8 Considere um colar que pode ser considerado como estando sobre uma circunferência. Considerando as simetrias de rotação e reflexão, quantos colares distintos se podem fazer com 7 contas pretas e 3 brancas? E com 8 pretas e 2 brancas?

8.9 Quantas são as possíveis colorações dos vértices (pontas) da letra "H" com 4 cores, considerando as suas suas simetrias?

8.10 Considere um hexágono regular, com conjunto de vértices X. Quantas colorações distintas podemos dar a X, usando n cores, tomando em conta todas as simetrias de rotação e reflexão?

8.11 Considere um jogo do galo que termina com 5 cruzes e 4 bolas. Quantas são estas possíveis terminações, considerando todas as simetrias do quadrado?

Parte 3. **GRAFOS**

Um grafo é, intuitivamente, um conjunto de pontos, chamados vértices, ligados por linhas, chamadas arestas. Os grafos constituem um conceito matemático importante no estudo das estruturas de comunicação, tais como estradas que ligam cidades, redes neuronais, redes de computadores, ou ainda a internet e as redes sociais.

9. Grafos e suas Matrizes

Existem vários tipos de grafos, consoante a natureza das ligações entre vértices, simples ou múltiplas, ou a possibilidade de haver ligações de um vértice a si próprio.

Há também os grafos cujas ligações entre vértices são orientadas, chamados grafos dirigidos, ou orientados. Caso contrário, falamos de grafos não dirigidos e começamos por estes.

9.1. **Os vários tipos de grafos.** Começamos pela seguinte definição.

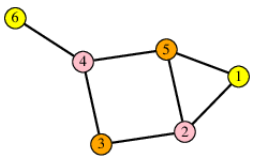
Definição 9.1. Um grafo é um par $\Gamma = (V, A)$ constituído por um conjunto de **vértices** V, e um conjunto de **arestas** ou ligações A (ambos conjuntos finitos), sendo A formado por pares (não ordenados) de elementos distintos de V. Por outras palavras, cada aresta $\alpha \in A$ é um subconjunto de V composto por **dois vértices** $\alpha = \{v, \omega\} \subset V$, com $v \neq \omega$ (e não há arestas com apenas um elemento).

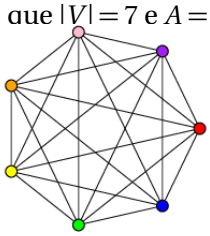
Recordando que $\mathscr{P}_k(V)$ é o conjunto dos subconjuntos de V com cardinal k, podemos então dizer que, num grafo $\Gamma = (V, A)$ temos $A \subset \mathscr{P}_2(V)$.

Exemplo 9.2. A seguinte imagem mostra dois grafos: o da esquerda tem 6 vértices, numerados de 1 a 6, e 7 arestas. Assim, podemos escrever $V = [6]$ e

$$A = \{\{1,2\},\ \{1,5\},\ \{2,3\},\ \{2,5\},\ \{3,4\},\ \{4,5\},\ \{4,6\}\}$$

O da direita tem 7 vértices, e todas as arestas entre eles pelo que $|V| = 7$ e $A = \mathscr{P}_2(V)$.





Como no grafo da esquerda, é frequente etiquetar os vértices com os números naturais de 1 a $|V|$, mas podemos igualmente usar letras ou nomes. De facto, os vértices podem ser elementos de um conjunto (finito) arbitrário V.

Terminologia: Quando precisamos de distinguir vértices e arestas de diferentes grafos, escrevemos os conjuntos de vértices e arestas de Γ como V_Γ e A_Γ. Quando $\alpha = \{v, \omega\} \in A$ dizemos que v e ω são *os extremos de* α; da mesma forma, dizemos que α *incide em* v e em ω. Sempre que $v, \omega \in V$ são dois vértices ligados por uma aresta dizemos também que v e ω são *adjacentes*.

Exemplo 9.3. Vejamos agora algumas famílias de grafos, dependendo de $n \in \mathbb{N}$.

- Se Γ tem n vértices, e não tem arestas (ou seja $|V| = n$ e $A = \varnothing$) temos um grafo *totalmente desconexo* em n vértices.
- Se Γ tem n vértices, e tem uma aresta entre cada par de vértices distintos, então Γ chama-se o *grafo completo* de n vértices, e denota-se por K_n. Este é um grafo com $\binom{n}{2}$ arestas. A figura acima inclui o grafo K_7.
- O grafo P_n com $V = [n] = \{1, \cdots, n\}$, e com arestas $\alpha_1, \cdots, \alpha_{n-1}$ dadas por $\alpha_i = \{i, i+1\}$ é chamado o *grafo caminho* de n vértices (ou de tamanho $n-1$), uma vez que α_i liga o vértice i ao vértice $i+1$ e não há mais arestas.

- O grafo C_n com $V=[n]$, e com arestas $\alpha_1,\cdots,\alpha_n$ tais que $\alpha_i=\{i,i+1\}$ para $i=1,\cdots,n-1$ e $\alpha_n=\{n,1\}$, chama-se o *grafo ciclo* de ordem/tamanho n.

Há várias quantidades importantes a reter quando temos um grafo.

Definição 9.4. Sendo $\Gamma=(V,A)$, a ordem de Γ é o número de vértices $|V|$, e o tamanho de Γ é o número de arestas $|A|$.

Como mencionado acima, existem algumas variantes da definição de grafo. Em particular, podemos considerar grafos com várias arestas que incidem nos mesmos dois vértices ou arestas que incidem num único vértice.

Definição 9.5. Um **multigrafo** é um triplo $\Gamma=(V,A,\phi)$ sendo V e A conjuntos finitos de vértices e arestas e $\phi:A\to\mathscr{P}_2(V)$ uma aplicação que associa a cada aresta um par de vértices. Quando $\phi(\alpha)=\{\upsilon,\omega\}$, os vértices $\upsilon,\omega\in V$ dizem-se os extremos da aresta $\alpha\in A$.

Neste caso, ao contrário dos grafos da definição 9.1, pode haver arestas diferentes que incidem nos mesmos dois vértices.

Há também uma definição mais geral que inclui arestas cujos extremos coincidem.

Definição 9.6. Um **pseudo-grafo** é um triplo $\Gamma=(V,A,\psi)$ sendo V o conjunto de vértices V, A o de arestas e $\psi:A\to V\sqcup\mathscr{P}_2(V)$ uma aplicação que associa a cada aresta $\alpha\in A$ um par de vértices, ou apenas um vértice. Nessa última situação, em que $\psi(\alpha)=\{\upsilon\}$, para certo $\upsilon\in V$, α chama-se um **lacete**.

Assim, um lacete é uma ligação do vértice υ consigo próprio. Neste caso, podemos dizer que α incide duplamente em υ, ou que υ é um extremo duplo de $\alpha\in A$.

Exemplo 9.7. A seguinte imagem mostra um grafo, e um pseudo-grafo. Retirando o lacete no vértice 1, o pseudo-grafo da direita torna-se um multigrafo.

Observação 9.8. Naturalmente um grafo é um multigrafo sem arestas múltiplas entre os mesmos vértices, e um multigrafo é um pseudo-grafo sem lacetes. Quando se trabalha com frequência com multigrafos ou pseudo-grafos, os grafos da Definição 9.1 são chamados de *grafos simples*, para mais facilmente os distinguir. Como estudamos essencialmente os grafos da Definição 9.1, omitiremos, em geral, o adjectivo simples. Por coerência, neste texto, ao considerar multigrafos ou pseudo-grafos, estes adjectivos serão explicitamente indicados.

Para cada vértice $\upsilon\in V$ podemos considerar o número de arestas que nele incidem.

Definição 9.9. Seja Γ um grafo, e υ um dos seus vértices. O **grau** de $\upsilon\in V$, denotado por d_υ é o número de arestas que incidem nele:

$$d_\upsilon:=|\{\alpha\in A:\upsilon\in\alpha\}|.$$

Se Γ tem todos os vértices do mesmo grau k, dizemos que Γ é k-**regular**.

Observação 9.10. Esta definição também se aplica a pseudo-grafos, se cada lacete num certo vértice υ for contado duas vezes na determinação de d_υ.

Exemplo 9.11. Se $\Gamma=K_n$ é o grafo completo de ordem n, temos que cada vértice é adjacente a todos os outros, pelo que $d_\upsilon=n-1$ para todos os vértices υ. Desta forma K_n é $(n-1)$-regular. Um grafo ciclo é 2-regular para qualquer número de vértices.

9.2. **Matrizes de incidência, adjacência e grau.** Apesar das representações de grafos numa folha de papel serem muito importantes para a nossa intuição, há também ferramentas algébricas de enorme utilidade no estudo dos grafos. De facto, muitas das ferramentas computacionais para trabalhar com grafos, se não todas, baseiam-se na estreita ligação entre grafos e certas propriedades das matrizes a eles associados.

Cada grafo tem associada uma matriz rectangular, a *matriz de incidência*, e duas matrizes quadradas, a de *adjacência* e a *matriz de valência ou grau.* Há também outras matrizes muito importantes que serão introduzidas mais tarde.

Definição 9.12. Seja Γ um grafo (ou multigrafo) com vértices $V=\{v_1,\cdots,v_n\}$ e $A=\{\alpha_1,\cdots,\alpha_m\}$. A **Matriz de Incidência** de Γ é a matriz $M=M_\Gamma$ com $m=|A|$ linhas e $n=|V|$ colunas, cuja entrada na linha i e coluna j (correspondente à aresta α_i e ao vértice v_j) é dada por:

$$M_{ij}=\begin{cases}1, & \text{se } \alpha_i \text{ incide em } v_j\\ 0, & \text{se } \alpha_j \text{ não incide em } v_j,\end{cases}\qquad i\in[m],\quad j\in[n].$$

A **Matriz de Adjacência** de Γ é uma matriz quadrada $J=J_\Gamma$, simétrica, com $n=|V|$ linhas e colunas, cuja entrada i,j é dada por

$$J_{ij}=\begin{cases}k, & \text{se } v_i \text{ e } v_j \text{ estão ligados por } k \text{ arestas}\\ 0, & \text{se } v_i \text{ e } v_j \text{ não são adjacentes, ou } i=j\end{cases}$$

(naturalmente J é uma matriz de 0's e 1's quando Γ é um grafo simples). Finalmente, a **Matriz de Valência** (ou **Matriz de Grau**) é a matriz quadrada diagonal $D=D_\Gamma$, com $n=|V|$ linhas e colunas, dada por

$$D_{ii}=d_{v_i}\quad (D_{ij}=0, \text{ se } i\neq j).$$

Observação 9.13. Note-se que a matriz de incidência M não está definida de forma única para um dado grafo Γ. De facto, se permutarmos os vértices, ou seja, se os ordenarmos de outra forma, e fizermos o mesmo com as arestas, vamos encontrar uma matriz M' que difere da primeira por uma troca de linhas (correspondente à permutação das arestas) e uma troca de colunas (correspondente à permutação das arestas).

Designamos por A^{t} a transposta da matriz A.

Proposição 9.14. *Seja $\Gamma=(V,A)$ um grafo ou multigrafo. As matrizes de incidência, adjacência e valência verificam a igualdade matricial:*

$$M^{\mathsf{t}}\cdot M=J+D.$$

Demonstração. Vamos provar para grafos simples. Cada linha da matriz M, que corresponde a um vértice, é um vector com zeros e uns. Cada entrada deste vector corresponde a uma aresta, e é zero se aresta que não incide no vector, e é um se nele incide. A multiplicação de M por M^{t} é uma matriz quadrada em que, na linha i e coluna j, temos o produto interno dos vectores correspondentes a v_i e a v_j. Assim, se $i\neq j$, apenas obtemos 1 se v_i e v_j são adjacentes, e obtemos zero caso contrário. Quando $i=j$ temos uma soma de 1's, tantos quantos as arestas incidentes em $v_i=v_j$. Em ambos os casos, obtemos $J_{ij}+D_{ij}$ como queríamos provar.

Deixamos o caso de multigrafos como exercício. □

Apesar de ser elementar, o próximo resultado é muito importante nesta teoria, pelo que se designa o teorema fundamental da teoria de grafos (não dirigidos).

Teorema 9.15. *Seja Γ um grafo. A soma dos graus de todos os vértices é igual ao dobro do tamanho de Γ (número de arestas). Ou seja:*

$$\sum_{v\in V} d_v=2|A| \tag{9.1}$$

Demonstração. Vamos somar todas as entradas da matriz M. Cada linha tem 2 entradas iguais a 1, e todas as outras são zero. Cada coluna tem tantos valores 1 quantos o grau do vértice correspondente. Por um lado, somando linha a linha, obtemos $2|A|$, uma vez que as linhas correspondem às arestas. Por outro lado, somando coluna a coluna, obtemos $\sum_{v\in V} d_v$ uma vez que cada coluna corresponde a um vértice distinto. □

Corolário 9.16. *Em qualquer grafo o número de vértices de grau ímpar é par.*

Demonstração. Basta considerar a igualdade (9.1) módulo 2, ou seja $\sum_{v\in V} d_v \equiv 0 \mod 2$, e notar que, novamente módulo 2,

$$\sum_{v\in V} d_v \equiv \sum_{v\in W} d_v \equiv \sum_{v\in W} 1 = |W|,$$

onde W é o conjunto dos vértices v tais que d_v é ímpar. Os outros termos não contribuem para a soma, pois essas parcelas têm $d_v \equiv 0 \bmod 2$. □

Corolário 9.17. *Seja Γ um grafo de ordem $n \in \mathbb{N}$. Se n é par, o número de vértices de grau par é par. Se n é ímpar, o número de vértices de grau par é ímpar.*

Observação 9.18. Na verdade, o Teorema 9.15, bem como os seus cololários são válidos para multigrafos, e mesmo para pseudo-grafos (com a dupla contagem de cada lacete para o grau do vértice onde incide). Deixa-se para o leitor as respectivas demonstrações, nestes casos mais gerais.

Exercício 9.19. Mostre que num grupo de pessoas em número ímpar, há sempre pelo menos uma delas que conhece um número par das restantes (estamos, naturalmente, a assumir que se a pessoa A conhece a pessoa B, então B conhece A).

9.3. **Sequências gráficas; complementar de um grafo.** Dado um grafo Γ com vértices $V = \{v_1, \cdots, v_n\}$ (em bijecção com $[n] = \{1, \cdots, n\}$) podemos naturalmente considerar a sequência de inteiros não negativos

$$(d_1, d_2, \cdots, d_n)$$

onde d_i é o grau do vértice v_i, $i \in [n]$. Note-se que esta é a sequência dos elementos da diagonal da matriz de valência: $\mathrm{diag} D = (d_1, d_2, \cdots, d_n)$.

Como não nos interessa a ordem dos índices dos vértices, podemos sempre assumir que esta sucessão é não-decrescente:

$$d_1 \leq d_2 \leq \cdots \leq d_n.$$

Uma sequências destas, obtida a partir de um grafo, chama-se uma sequência gráfica. Mas podemos perguntar-nos: dada uma sequência não-decrescente de números inteiros, será que é uma sequência gráfica? Por outras palavras, será que existe um grafo Γ tal que os graus dos seus vértices sejam os números da sequência dada?

Proposição 9.20. *Seja $d_1 \leq d_2 \leq \cdots \leq d_n$ uma sequência gráfica de um grafo* simples. *Então temos:*
(i) $\sum_{i=1}^n d_i$ é par,
(ii) $d_n < n$.
Em particular, a condição 2 implica $d_i < n$, $\forall i \in [n]$, e $\sum_{i=1}^n d_i \leq n(n-1)$.

Demonstração. Seja Γ um grafo (simples) com essa sequência de graus. (1) Já foi visto. Como, num grafo simples, cada vértice não se pode ligar a mais que $n-1$ dos restantes vértices, temos (2). Da mesma forma $d_i \leq d_n < n$, para todo $i \in [n]$ e a soma de todos os graus verifica $\sum_{i=1}^n d_i \leq n\, d_n \leq n(n-1)$. □

Proposição 9.21. *Considere a sequência*

$$d_1 \leq d_2 \leq \cdots \leq d_n \leq d_{n+1},$$

e seja $\Delta := d_{n+1}$ *o maior inteiro da sequência. Esta sequência é gráfica se e só se uma ordenação dos números*

$$d_1, d_2, \cdots, d_k, d_{k+1}-1, \cdots, d_n-1,$$

onde $k = n-\Delta$ *também for gráfica.*

Demonstração. Supondo que $d_1 \leq d_2 \leq \cdots d_k \leq d_{k+1}-1 \leq \cdots \leq d_n-1$ é gráfica, ao juntarmos o vértice v_{n+1}, com grau $\Delta := d_{n+1}$ obtemos um grafo com $n+1$ vértices e a sequência gráfica de cima. Reciprocamente, caso a de cima seja gráfica, aplicamos o processo inverso, removendo o último vértice. □

Observação 9.22. Para os multigrafos (e pseudo-grafos), nem todas as restrições acima se têm que verificar. De facto, pode mostrar-se que, para qualquer sequência que verifique a condição (1), existe um multigrafo que a realiza.

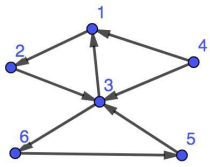
Quando falamos em grafos (em contraste com multigrafos ou pseudo-grafos) é por vezes útil considerar o chamado *grafo complementar*.

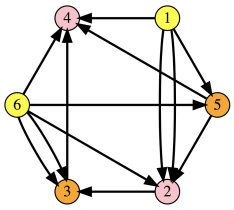
Definição 9.23. Dado um grafo $\Gamma = (V, A)$ o seu complementar é o grafo $\Gamma^c := (V, A^c)$ onde A^c é o complemento de A em $\mathscr{P}_2(V)$. Por outras palavras, os vértices de Γ são os mesmos, mas as suas ligações são as complementares: se v é adjacente a ω em Γ, então estes dois vértices não são adjacentes em Γ' e vice-versa.

Exercício 9.24. (a) Mostre que $(\Gamma^c)^c = \Gamma$. (b) Mostre que o complementar de um grafo completo é um grafo totalmente desconexo e vice-versa. (c) Determine o complementar do grafo C_5 (grafo ciclo com 5 vértices).

Problemas de Revisão.

9.1 Determine as matrizes de incidência, adjacência e grau dos seguintes grafo e multigrafo, obtidos ignorando as setas.





9.2 Considere as seguintes matrizes onde os espaços representam zeros:

$$B = \begin{pmatrix} 1 & 1 & 1 & & & \\ 1 & & & 1 & 1 & \\ & 1 & & 1 & & 1 \\ & & 1 & & 1 & 1 \end{pmatrix}, \qquad C = \begin{pmatrix} 1 & 1 & 1 & 1 & & & & \\ 1 & 1 & & & 1 & 1 & & \\ & & & & 1 & & 1 & 1 \\ & & 1 & & & & 1 & 1 & 1 \\ & & & 1 & & 1 & & & 1 \end{pmatrix}$$

Desenhe um grafo Γ e um multigrafo Γ' cujas matrizes de incidência são $M = B^{\mathsf{t}}$ e $M' = C^{\mathsf{t}}$. Determine as respectivas matrizes de adjacência e de grau.

9.3 Sejam M, J e D as matrizes de incidência, adjacência e grau de um multigrafo Γ. Mostre que $M^{\mathsf{t}} \cdot M = J + D$ e que $\sum_{i,j} M_{ij} = 2|A_\Gamma|$.

9.4 Mostre que, se Γ e Γ^c são isomorfos, então a ordem de Γ, $n = |V_\Gamma|$ verifica: $n \equiv 0$ ou $n \equiv 1$ módulo 4.

9.5 Considere as seguintes sequências de naturais. Verifique quais delas são gráficas (correspondem a sequência de graus de um grafo) e, no caso afirmativo, desenhe um grafo com essa sequência de graus.
(a) $(1,2,2,2,3,3)$

(b) $(2,2,4,4,6,6,6)$
(c) $(1,2,4,5,6,6,6,6)$
(d) $(3,3,4,4,6,6,6)$

9.6 Considere a sequência $(6,3,3,3,3,2,2,2,2,1,1)$. Mostre que é gráfica, e construa um grafo com esta sequência de graus.
9.7 Desenhe um miltigafo com a seguinte sequência de graus: $(1,2,3,4)$. Porque é que isto não contradiz a Proposição 9.20?
9.8 Seja Γ um grafo com matriz de adjacência J e grau D. (a) Determine as matrizes de adjacência e de grau do grafo complementar Γ^c em função de J e D.

10. Caminhos, Conexidade; Grafos Planares

Vamos agora analizar percursos em grafos, e a informação que a existência de determinados percursos no grafo nos dá.

A primeira noção é a de passeio num grafo. Isto é uma sequência de vértices e arestas percorridas através de incidência. Como estamos em grafos simples, um passeio é determinado por uma sucessão de vértices em que os vértices podem aparecer um após o outro somente quando são adjacentes.

Em toda esta secção, "grafo" significa "grafo simples". Ou seja, não há lacetes nem arestas múltiplas nos grafos aqui considerados.

10.1. **Passeios e caminhos em grafos.**

Definição 10.1. Um **passeio** num grafo Γ é uma sequência alternada de vértices e arestas: $v_0\alpha_1 v_1\alpha_2\cdots\alpha_n v_n$ em que α_i incide em v_{i-1} e em v_i. Nesta sucessão (embora não consecutivamente), podemos repetir o mesmo vértice várias vezes, mas devemos começar e terminar num vértice. Desta forma, v_0 é chamado o vértice inicial, e v_n o vértice final.

Pensamos neste passeio como uma sucessão de etapas: primeiro vamos de v_0 a v_1 pela (única) aresta que os une, depois de v_1 a v_2 pela aresta que os liga, e assim sucessivamente. Se temos $n+1$ vértices, ou seja n arestas, dizemos que o passeio tem **comprimento** n (que é o número de arestas percorridas). Se v_0 coincide com v_n dizemos que é um passeio fechado.

Observação 10.2. Se o nosso grafo Γ é simples, como há apenas uma aresta (no máximo) entre cada 2 vértices, para definir unicamente um passeio basta considerar a sequência de vértices, ou a sequência de arestas, desde que a relação de adjacência seja mantida.

Também é importante a definição de caminho e de ciclo.

Definição 10.3. Um **caminho** em Γ é um passeio em que não se repetem arestas. Um **ciclo** (também chamado caminho fechado) é um caminho cujos vértices inicial e final coincidem.

O *comprimento* de um caminho é definido da mesma forma que para os passeios: é o número de arestas percorridas.

Exemplo 10.4. Consideremos novamente o grafo do Exemplo 9.2. Utilizando apenas a sequência de vértices, temos:

- $(6,4,3,4,5,1)$ é um passeio de comprimento 5,
- $(6,4,5,1)$ é um caminho de comprimento 3,
- $(5,4,3,2,1,5)$ é um ciclo de comprimento 5.

Definição 10.5. Um grafo diz-se **conexo** se dados quaisquer dois vértices, existe um passeio que começa num deles e termina no outro.

Observação 10.6. Não é muito difícil de mostrar que, se existe um passeio que começa em v_0 e termina em v_n então existe um caminho com os mesmos extremos. Assim, podemos definir conexidade usando caminhos em lugar de passeios.

Não é muito difícil de verificar que qualquer grafo se pode decompor como uma união disjunta de grafos conexos. Ou seja, se $\Gamma = (V, A)$ então

$$V = V_1 \sqcup \cdots \sqcup V_k, \quad \text{e} \quad A = A_1 \sqcup \cdots \sqcup A_k$$

com $\Gamma_i = (V_i, A_i)$ conexo, sendo $A_i \subset A$ as arestas que ligam os vértices de V_i.

Definição 10.7. Se Γ é um grafo escrito da forma acima, cada subgrafo $\Gamma_i = (V_i, A_i)$ é designado uma **componente conexa** de Γ.

10.2. **Distâncias em grafos.** Num grafo conexo, pode definir-se uma noção de distância entre vértices. De facto, um grafo conexo é naturalmente um espaço métrico.

Para definir distâncias em grafos, vamos usar caminhos. Se γ designa um caminho no grafo Γ, vamos denotar o seu comprimento por $|\gamma|$. Assim, $|\gamma|$ é o número de arestas que o caminho γ contém.

Definição 10.8. Seja $\Gamma = (V, A)$ um grafo conexo. A distância do vértice $v \in V$ ao vértice $\omega \in V$ é definida por:

$$d(v, \omega) = \min\{|\gamma| : \gamma \text{ é um caminho entre } v \text{ e } \omega\}.$$

Naturalmente $d(v, \omega) \in \mathbb{N}_0$ e verifica as seguintes propriedades.

Proposição 10.9. *Seja Γ um grafo conexo. A distância verifica:*
(a) $d(v, \omega) = 0$ se e só se $v = \omega$
(b) $d(v, \omega) = d(\omega, v)$
(c) $d(v, \omega) + d(\omega, \mu) \geq d(v, \mu)$

Demonstração. A demonstração de (a) e (b) é trivial e a de (c) deixa-se como exercício. □

Com estas noções podem definir-se outros conceitos como excentricidade de um dado vértice um grafo, raio e diâmetro.

Definição 10.10. A excentricidade do vértice $v \in V$ no grafo conexo Γ é:

$$e(v) := \max\{d(v, \omega) : \omega \in V\}.$$

O raio e o diâmetro de Γ são definidos, respectivamente, por:

$$R_\Gamma := \min\{e(v) : v \in V\}, \qquad D_\Gamma := \max\{e(v) : v \in V\}.$$

Exercício 10.11. Determine a excentricidade de todos os vértices, o raio e o diâmetro dos grafos caminho, ciclo e completo de ordem n: P_n, C_n e K_n.

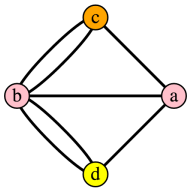
10.3. **Grafos Eulerianos e Hamiltonianos.** Há um problema, em particular, que esteve na origem da teoria dos grafos, e ficou famoso quando L. Euler o resolveu matematicamente. Numa cidade chamada Königsberg, com 7 pontes, os habitantes queriam saber se seria possível dar um passeio que percorresse todas as pontes apenas uma vez, começando e terminando no mesmo lugar.

Se consideramos as pontes como arestas, o problema reduz-se a saber se podemos encontrar um ciclo num grafo, que percorra todas as arestas.

Definição 10.12. Um passeio euleriano num grafo Γ é um passeio que percorre todas as arestas de Γ, podendo repetir vértices, mas não arestas. Um passeio euleriano que começa e termina no mesmo vértice chama-se ciclo euleriano.

Obviamente não há passeios eulerianos em grafos desconexos.

Exemplo 10.13. O grafo de Königsberg não é um grafo simples; é o seguinte multigrafo. O próximo resultado, devido a Euler, mostra que não há solução para o tal passeio em Königsberg, a menos que se mude o grafo ou seja, se adicione uma nova ponte.



Um multigrafo diz-se euleriano se admite um ciclo euleriano.

Proposição 10.14. *Um multigrafo conexo é Euleriano se e só se todos os vértices têm grau par. Um grafo admite um passeio euleriano (não necessariamente fechado) se e só se tem exactamente dois vértices com grau ímpar, que são os extremos do passeio.*

Também se definem passeios e caminhos que passam por todos os vértices sem repetição, estes caminhos chamam-se hamiltonianos.

Definição 10.15. Seja Γ um grafo simples. Um caminho diz-se hamiltoniano se percorre todos os vértices de Γ. Um caminho hamiltoniano fechado chama-se ciclo hamiltoniano.

Um grafo hamiltoniano é um grafo que admite um ciclo hamiltoniano

Exemplo 10.16. Vemos aqui exemplos de grafos com passeios eulerianos e caminhos hamiltonianos. O logótipo da ULisboa é um grafo hamiltoniano, como podemos verificar:

10.4. **Isomorfismos entre grafos; subgrafos.** É natural numerar os vértices de um grafo com os números $\{1,2,\cdots,n\}$, com $n = |V|$. No entanto, esta etiquetagem é arbitrária, e podemos trocar a ordem dos vértices, usando qualquer bijecção $f : [n] \to [n]$, sem alterar nenhuma das propriedades importantes desse grafo. O que é importante é reter as ligações - as arestas - entre os vértices que estavam ligados.

Consideremos o primeiro grafo do Exemplo 9.2. É fácil ver que, em vez de números podemos tomar $V = \{a,b,c,d,e,f\}$ e

$$A = \{\{a,b\},\ \{a,e\},\ \{b,c\},\ \{b,e\},\ \{c,d\},\ \{d,e\},\ \{d,f\}\}$$

e obter um grafo essencialmente igual.

Mais geralmente, um isomorfismo entre dois grafos Γ_1 e Γ_2 é simplesmente uma associação biunívoca entre as etiquetas do primeiro grafo e as do segundo, de forma que dois vértices ligados (resp. não ligados) em Γ_1 correspondam a vértices ligados (resp. não ligados) em Γ_2. De forma mais precisa, podemos fazer a seguinte definição de isomorfismo.

Definição 10.17. Dois grafos $\Gamma_1 = (V_1, A_1)$ e $\Gamma_2 = (V_2, A_2)$ dizem-se **isomorfos** se existe uma bijecção $f : V_1 \to V_2$ de tal forma que: $\alpha = \{\upsilon, \omega\} \in A_1$ se e só se $\alpha' := \{f(\upsilon), f(\omega)\} \in A_2$.

É importante observar o seguinte: dois grafos podem não parecer isomorfos, ao estarem desenhados de formas fundamentalmente distintas no plano, mas uma inspecção mais detalhada mostrar que são, de facto, isomorfos.

Abaixo estão duas representações diferentes do grafo K_4. Uma das diferenças fundamentais dessas duas representações é o facto de que numa delas há arestas que se cruzam. No entanto, este é um caso em que se encontra facilmente uma bijecção entre o conjunto de vértices de um e de outro: $f(1)=a$, $f(2)=b$, $f(3)=c$ e $f(4)=d$ induz o isomorfismo pretendido. Assim, ambas são representações do grafo K_4 e a primeira serve para mostrar que K_4 é um grafo planar.

Naturalmente, dois grafos isomorfos, têm em comum todas as propriedades que estudámos:

- A mesma sequência gráfica, a menos de permutação das entradas,
- As mesmas matrizes incidência, adjacência e grau, a menos de permutação das linhas e colunas,
- Os mesmos grafos complementares, a menos de isomorfismo.

Acabamos esta subsecção com a noção de subgrafo de um grafo.

Definição 10.18. Seja $\Gamma=(V,A)$ um grafo, e $A'\subset A$ um subconjunto dos vértices. O subgrafo gerado por A' é o grafo $\Gamma'=(V',A')$ onde $V'\subset V$ tem todos os vértices incidentes às arestas de A'. De forma mais rigorosa,

$$V' := \{v\in V : v\in A'\}.$$

Desta forma, por definição, um subgrafo de Γ é sempre associado a um subconjunto das arestas de Γ. Quando Γ' é um subgrafo de Γ, e os conjuntos de vértices e arestas estão subentendidos, escrevemos abreviadamente $\Gamma'\subset\Gamma$.

10.5. **Grafos planares e representações planares.** A representação dos grafos numa folha de papel ou num quadro é extremamente útil para raciocinar sobre grafos. No entanto há grafos, como o K_7, que não podem ser representados num papel de forma a que as arestas não se cruzem. Isto causa por vezes confusão, uma vez que, como no exemplo K_7, não queremos considerar estas intersecções de arestas como novos vértices! Assim, surge a noção de grafo planar: um grafo que se pode desenhar num plano de forma que as suas arestas nunca se cruzem.

Definição 10.19. Um grafo $\Gamma=(V,A)$ diz-se planar, se admite uma representação no plano $\mathbb{R}^2$ de forma a que:

- A vértices distintos $v\neq\omega\in V$ correspondem pontos distintos no plano,
- a cada aresta $\alpha\in A$ entre v e ω corresponde uma curva no plano, entre v e ω,

e as curvas correspondentes a arestas diferentes nunca se cruzam.

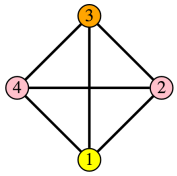
É frequente encontrarmos grafos que são planares mas a sua representação gráfica tem arestas que se cruzam. O que se passa é que podemos desenhar o mesmo grafo ou um grafo isomorfo que evite essas intersecções.

Assim, convém distinguir o grafo abstracto Γ, em cuja definição só intervêm a informação sobre os conjuntos V e A, de uma sua possível representação no plano R. A um único grafo (melhor dizendo a uma classe de isomorfismo de grafos) correspondem infinitas formas de o representar no plano, com ou sem intersecções entre as arestas.

Uma representação de um grafo no plano da forma indicada na definição acima, diz-se uma representação planar. Assim, podemos dizer que um grafo é planar se admite (pelo menos uma) representação planar.

Por outro lado, existem grafos que não são planares - **pois não admitem nenhuma representação planar** - como os grafos K_n com $n\geq 5$.

Exercício 10.20. Mostre que K_4 é um grafo planar, apesar do esquema abaixo apresentar um cruzamento entre 2 arestas diferentes.



Proposição 10.21. *Os grafos caminho P_n e os grafos ciclo C_n são planares. Qualquer grafo sem ciclos é planar. Uma união disjunta de grafos planares é planar.*

Demonstração. A demonstração é fácil e deixada ao leitor. □

Como se pode verificar, uma representação planar R de um grafo Γ consiste em:

- objectos de dimensão zero, os vértices que podem ser representados por pontos,
- objectos de dimensão um, que são as arestas, ou os caminhos que ligam os vários vértices
- as várias regiões bidimensionais que são o complementar dos vértices e arestas.

Estas regiões chamam-se faces da representação R. Há uma região especial, porque é a única que é ilimitada. De facto, sendo o grafo dado por um conjunto finito de vértices e arestas, ele está sempre contido num conjunto compacto do plano, pelo que o complemento desse conjunto é ilimitado. A face ilimitada de uma representação planar chama-se a **face exterior**.

Uma representação planar R de um grafo Γ admite um grafo dual.

Definição 10.22. Seja R a representação planar de um grafo $\Gamma = (V,A)$, com conjunto de faces F. Então o grafo dual $\check{\Gamma} = (\check{V},\check{A})$ é definido por $\check{V} := F$, e $\{f_1,f_2\} \in \check{A}$ se e só se f_1 e f_2 são faces adjacentes em R.

Proposição 10.23. *O dual $\check{\Gamma}$ de uma representação planar R (de um grafo Γ) é um grafo planar.*

Demonstração. Uma representação planar de $\check{\Gamma}$ é construída da seguinte forma:

- Coloca-se um vértice $f \in \check{V}$ no interior de cada face $f \in F$
- Unem-se por arestas $\check{\alpha} \in \check{A}$ os vértices f_1, f_2 que correspondem a faces que são adjacentes em R.

□

10.6. **O teorema de Euler, grafos duais, poliedros.** A cada face podemos associar um número natural, que é o número de arestas que estão no seu bordo. Por simplicidade, vamos restringir-nos ao caso em que o grafo Γ não tem vértices de grau 1. Assim, estamos a considerar agora grafos que não podem ter componentes conexas que são árvores.

Teorema 10.24. *(Fórmula de Euler) Dada uma representação planar R do grafo Γ, com v vértices, a arestas e f faces temos:*

$$v - a + f = 2$$

contando com a face exterior.

Definição 10.25. Um poliedro convexo é sólido geométrico em $\mathbb{R}^3$ limitado por um conjunto de faces, que são polígonos, e que é convexo. Ou seja, para quaisquer 2 pontos no interior do poliedro, o segmento de recta que os une está ainda no interior do poliedro.

Um poliedro tem naturalmente arestas, na junção de duas das suas faces (quando se tocam) e vértices, que são também os vértices das faces (que são polígonos).

Seja P um poliedro convexo. Podemos ver que o grafo que se obtém tomando o par (V,A) em que V é o conjunto de vértices de P e A o conjunto das suas arestas, é um grafo simples Γ_P.

Além disso, este grafo é sempre planar. De facto, uma representação planar R_P pode ser obtida projectando o conjunto das arestas a partir de um ponto no exterior de P, mas muito próximo de uma das faces.

O seguinte resultado de Steinitz caracteriza os cardinais v, a e f, dos vértices, arestas e faces dos grafos planares obtidos a partir de poliedros.

Teorema 10.26. *Seja R uma representação planar do grafo $\Gamma=(V,A)$. Então R provém de um poliedro se e só se:*
(i) $v-a+f=2$ (a fórmula de Euler)
(ii) $a\geq 6$ e tanto v como f estão no intervalo $[4,\frac{2a}{3}]$.

10.7. **Problemas de Revisão.**

10.1 Desenhe o grafo que tem a seguinte matriz de incidência. Qual o seu número de componentes conexas?

10.2 Desenhe um representante para todas as classes de isomorfismo de grafos conexos com 4 vértices.

10.3 Seja k um número natural. Um grafo diz-se k-regular se $d_v=k$ para todo o $v\in V$. Mostre que se G é k-regular com k ímpar, então $|V|$ é par. Mostre que se G é conexo e 1-regular, então $|V|=2$. Mostre que se G é 2-regular e conexo, então é um ciclo.

10.4 Seja K_n o grafo completo com n vértices e seja v_0 um deles. Quantos caminhos diferentes têm v_0 como caminho final?

10.5 Seja G um grafo conexo e regular com 22 arestas. Quantos vértices pode ter G? Construa um tal grafo, que não seja um ciclo.

10.6 Um edifício tem 27 salas iguais, dispostas como no cubo de Rubik, tendo escadas ou portas entre todas as salas adjacentes. É possível percorrer todas as salas uma única vez começando num sala vértice e terminando na sala do centro?

10.7 Mostre que, se Γ é um grafo desconexo (com mais de uma componente conexa) então o seu complementar é conexo. A afirmação recíproca é verdadeira?

10.8 Seja Γ um grafo conexo (simples). Mostre que há pelo menos dois vértices distintos com o mesmo grau [Sugestão: note que $0<d_v\leq|V|-1$ para todo o $v\in V$]. Construa um multigrafo conexo com 4 vértices de graus todos distintos.

10.9 Seja J a matriz de adjacência do grafo Γ com conjunto de vértices $V=[n]$, e seja J^k a sua k-ésima potência, $k\in\mathbb{N}$. Mostre, por indução, que

$$(J^k)_{i,j}$$

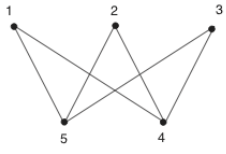
(a entrada i,j da matriz J^k) é o número de passeios diferentes, de comprimento k, começando no vértice i e terminando no vértice j.

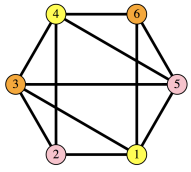
10.10 Mostre que, num grafo conexo, quaisquer dois caminhos de comprimento máximo têm pelo menos um vértice em comum.

10.11 Mostre que um grafo conexo, sem ciclos, verifica necessariamente $|V|=|A|+1$.

10.12 Mostre a fórmula de Euler generalizada: para um grafo planar, com v vértices, a arestas, f faces e c componentes conexas, temos $v-a+f=c+1$ (contando a face exterior).

10.13 Verifique que os grafos da figura são planares, desenhe-os sem intersecções das arestas, e construa o grafo dual.



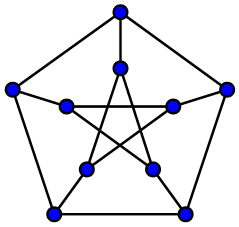


10.14 Seja P um poliedro convexo cujas faces são triângulos ou octógonos. Sabendo que P tem 24 vértices, todos de grau 3, determine o número de faces de cada tipo (triângulos e octógonos).

10.15 Existe algum poliedro convexo P satisfazendo as condições:
(a) P tem 6 faces, 10 arestas e 7 vértices?
(b) P tem 4 faces, 10 arestas e 8 vértices?
(b) P tem 6 faces, 11 arestas e 7 vértices?

10.16 Prove que qualquer grafo planar tem pelo menos um vértice de grau menor que 6.

10.17 Considere o grafo Γ da figura, chamado *grafo de Petersen*. Mostre que não é planar, encontrando um subgrafo de Γ que é uma subdivisão de $K_{3,3}$.



11. Árvores e o Teorema de Kirchhoff

Vamos agora estudar uma classe de grafos muito importantes: os grafos conexos e sem ciclos, que se chamam árvores. Apesar da sua aparente simplicidade, as árvores dão origem a questões bastante sofisticadas na teoria de grafos. Em particular, temos o célebre teorema de G. Kirchhoff, o físico alemão que formalizou as leis dos circuitos eléctricos, naturalmente modelados por grafos.

Nesta secção todos os grafos são simples.

11.1. **Árvores.** Os grafos que não têm ciclos são chamados árvores ou florestas, consoante sejam ou não conexos. Estes são tipos de grafos muito importantes, especialmente em problemas de matemática aplicada e na consideração de algoritmos eficientes para trabalhar com grafos gerais.

Definição 11.1. Uma árvore é um grafo conexo sem ciclos. Uma floresta é um grafo sem ciclos, ou seja, uma união disjunta de árvores.

Num grafo simples arbitrário a única relação entre o número de arestas m e o número de vértices n é $m \leq \binom{n}{2}$ como vimos. Para árvores, $n = |V|$ determina $m = |A|$ e vice-versa.

Teorema 11.2. *Seja Γ um grafo com $|V| = n$. As seguintes afirmações são equivalentes:*
(a) Γ é uma árvore
(b) Γ é conexo com $n-1$ arestas
(c) Γ não tem ciclos e tem $n-1$ arestas

Demonstração. Vamos provar $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$. Quando Γ é uma árvore com $n = 2$ vértices o resultado é evidente: só há uma aresta (com $n = 1$ também é evidente). Supondo o resultado válido para qualquer árvore com n vértices ou menos, seja Γ uma árvore de $n+1$ vértices. Ao retirarmos uma aresta Γ fica desconexo, pois caso contrário haveria um ciclo. Seja $\Gamma = \Gamma_1 \sqcup \Gamma_2$ a decomposição em componentes conexas. $\Gamma_1 = (V_1, A_1)$ e $\Gamma_2 = (V_2, A_2)$ são ambas árvores pois não têm ciclos; e têm menos vértices que Γ (estritamente, pois $V_i \neq \varnothing$). Assim, $|A_i| = |V_i| - 1$, para $i = 1, 2$, por hipótese de indução e portanto:

$$|A| = |A_1| + |A_2| + 1 = |V_1| - 1 + |V_2| - 1 + 1 = |V| - 1,$$

como pretendido. Seja agora Γ conexo com $n-1$ arestas, e por contradição, supomos que Γ tem um ciclo. Assim, retirando uma aresta desse ciclo, o grafo continuaria conexo. Fazendo isto para todos os ciclos, terminamos com uma árvore com menos que $n-1$ arestas que contradiz o passo $(a) \Rightarrow (b)$. Finalmente, se Γ não tem ciclos Γ é uma floresta; sejam $\Gamma_1, \cdots, \Gamma_k$ as componentes conexas de Γ que são, por definição, árvores. Então, sendo cada uma verifica $|A_i| = |V_i| - 1$ pelo que, supondo $|A| = n-1$ temos

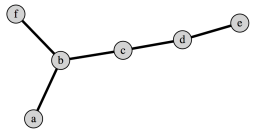
$$n-1 = |A| = \sum_{i=1}^{k} |A_i| = \sum_{i=1}^{k} (|V_i| - 1) = \left(\sum_{i=1}^{k} |V_i| \right) - k = n - k$$

o que implica $k = 1$, ou seja Γ é conexo, pelo que é uma árvore. □

Vamos agora analisar o tipo de sequências gráficas de uma árvore. Não é muito difícil verificar que qualquer árvore tem necessariamente pelo menos dois vértices de grau 1. Estes vértices são extremos, justificando a seguinte definição.

Definição 11.3. Sendo $\Gamma = (V, A)$ uma árvore, um vértice $v \in V$ com grau 1 chama-se folha. Os vértices com grau maior que dois dizem-se vértices de ramificação.

Exemplo 11.4. O seguinte grafo é uma árvore com sequência gráfica $(1,1,1,2,2,3)$, pelo que tem 3 folhas, e um vértice de ramificação.



Teorema 11.5. *Sendo* $0 < d_1 \leq d_2 \leq \cdots \leq d_n$, $(d_1, \cdots, d_n)$ *é a sequência gráfica de uma árvore com n vértices se e só se:*

$$\sum_{i=1}^{n} d_i = 2n - 2$$

Demonstração. Se Γ é uma árvore com n vértices, então o Teorema implica

$$2n - 2 = 2|A| = \sum_{i=1}^{n} d_i$$

pelo que a sua sequência gráfica verifica a fórmula dada. Reciprocamente, supomos que $\sum_{i=1}^{n} d_i = 2n-2$ e vamos, por indução no número n de vértices, tentar construir uma árvore com esta sequência gráfica.

No caso $n = 2$, temos $d_1 + d_2 = 2$ logo $d_1 = d_2 = 1$ e há obviamente uma árvore com esta sequência gráfica: a única árvore com uma aresta. Supomos agora que o resultado é válido para sequências com n entradas, e consideremos a sequência de $n+1$ naturais $(d_0, \cdots, d_n)$ com $0 < d_0 \leq d_1 \leq \cdots \leq d_{n+1}$ e $\sum_{i=0}^{n} d_i = 2n$. Observamos primeiro que forçosamente $d_0 = d_1 = 1$ uma vez que, caso $d_1 \geq 2$, teríamos:

$$\sum_{i=0}^{n} d_i = d_0 + d_1 + \cdots + d_n \geq d_0 + d_1 n \geq d_1 + 2n = d_0 + \sum_{i=0}^{n} d_i$$

o que é uma contradição, pois $d_0 \in \mathbb{N}$. Ou seja, há pelo menos dois vértices que são folhas. De forma análoga vemos que $d_n \geq 2$. Agora tomamos a sequência:

$$(d'_1, d'_2, \cdots, d'_{n-1}, d'_n) := (d_1, d_2, \cdots, d_{n-1}, d_n - 1)$$

que verifica: $\sum_{i=1}^{n} d'_i = (\sum_{i=0}^{n} d_i) - d_0 - 1 = 2n - 2$. Assim, por hipótese é a sequência gráfica de uma árvore Γ', com vértices $v_1, \cdots, v_n$. Ligando o vértice v_0 ao vértice v_n (e a mais nenhum outro vértice de Γ' aumentamos o grau de v_n uma unidade, e obtemos a árvore Γ com a sequência pretendida. □

No caso das árvores, os caminhos têm propriedades especiais, e por isso são espaços métricos particulares. Por exemplo, não é muito difícil mostrar que, numa árvore só há um caminho possível entre dois vértices dados.

Exercício 11.6. Mostre que, dados v, ω vértices numa árvore Γ, só há um caminho que começa em v e termina em ω.

11.2. **Árvores geradoras.** Quando temos um grafo simples Γ com muitos vértices, e pretendemos resolver problemas relacionados com caminhos nesse grafo, é muito útil considerar árvores dentro de Γ. Por exemplo, se se pretende percorrer um caminho entre os vértices v e ω de Γ, e $T \subset \Gamma$ é uma árvore contendo v e ω, então há um único caminho entre estes dois vértices em T (pelo exercício anterior) que é também um caminho em Γ. Aqui, usámos a definição de subgrafo de um dado grafo $\Gamma = (V, A)$ que consiste em tomar um subconjunto de A e os vértices incidentes às arestas desse subconjunto.

Desta forma, se houver uma árvore $T \subset \Gamma$ que contenha todos os vértices de Γ (mas nem todas as arestas de Γ) reduzimos a complexidade do nosso problema, uma vez que podemos tomar sempre o único caminho em T entre dois vértices dados. Uma tal árvore T, que contenha todos os vértices de um grafo Γ, chama-se árvore geradora de Γ.

Definição 11.7. Seja Γ um grafo (simples). Uma árvore geradora de Γ é um subgrafo $T \subset \Gamma$, tal que T é uma árvore (é conexo e não tem ciclos) e T contém todos os vértices de Γ.

Não é muito difícil ver que qualquer grafo conexo Γ tem pelo menos uma árvore geradora. Se Γ é desconexo, então não tem árvores geradoras por um motivo evidente: qualquer subgrafo de um grafo desconexo é desconexo.

Proposição 11.8. *Seja $\Gamma = (V, A)$ um grafo conexo. Então existe uma árvore geradora de Γ.*

Demonstração. Pode provar-se por indução no número de arestas. Se o grafo só tem um vértice, a árvore geradora é também apenas esse vértice. Supondo, por hipótese de indução que qualquer grafo conexo com m arestas tem uma árvore geradora, seja Γ um grafo conexo com $m+1$ arestas. Há pelo menos uma aresta a tal que $\Gamma \setminus \{a\}$ é ainda conexo. Assim, seja $T \subset \Gamma \setminus \{a\}$ uma árvore geradora de $\Gamma \setminus \{a\}$. Então, ou T é também uma árvore geradora para Γ, ou T não incluí um dos vértices de Γ. Neste último caso, isto significa que a tem grau 1 em $T \cup \{a\}$, ou seja $T \cup \{a\}$ é árvore geradora para Γ, uma vez que $T \cup \{a\}$ não tem ciclos (num ciclo todos os vértices têm grau ≥ 2). □

Definição 11.9. Seja Γ um grafo simples com n vértices, e sejam J e D as matrizes de adjacência e de grau, respectivamente. A matriz Laplaciana de Γ é a matriz $n \times n$:

$$L = D - J.$$

Seja $v \in V$. O cofactor de L associado a v, designado por L_v, é a matriz $(n-1) \times (n-1)$ obtida de L eliminando a linha e coluna correspondente ao vértice v.

A matriz Laplaciana é extremamente importante na teoria de grafos, em particular na chamada *teoria espectral de grafos*. O seu nome provém do facto que ela desempenha, nesta teoria, um papel análogo ao do operador diferencial Laplaciano, bem conhecido do cálculo diferencial a várias variáveis.

Teorema 11.10. *Seja L a matriz Laplaciana de um grafo Γ, e $v, \omega \in V$. Então:*
(i) $\det L_v = \det L_w$*;*
(ii) $\det L_v$ *é o número de árvores geradoras em* Γ

Exemplo 11.11. Considere-se o grafo ciclo C_{n+1} de tamanho $n+1$, com vértices numerados de 1 a $n+1$. Temos então, associado ao vértice $n+1$ (i.e, retirando a última linha e coluna da

matriz Laplaciana) o cofactor (matriz quadrada de lado n):

$$L_{n+1} = B(n) = \begin{pmatrix} 2 & -1 & 0 & \cdots \\ -1 & \ddots & \ddots & \ddots \\ 0 & \ddots & 2 & -1 \\ \vdots & \ddots & -1 & 2 \end{pmatrix},$$

onde usamos a notação $B(n)$ para as matrizes desta forma de tamanho n. Calculando o seu determinante, pela expansão de Laplace (lá está!) da primeira linha obtemos a fórmula recursiva:

$$\det B(n) = 2\det B(n-1) - \det B(n-2)$$

o que nos dá um problema de recorrência cuja solução (aplicar os resultados da secção 7), com a condição inicial $B(1) = 2$, é então:

$$\det L_{n+1} = B(n) = n+1.$$

Este é precisamente o resultado esperado, pois há $n+1$ árvores geradoras em C_{n+1}, cada uma delas obtida retirando uma aresta de cada vez.

Problemas de Revisão.

11.1 Seja Γ uma árvore com mais de 1 vértice.
(a) Mostre que Γ tem pelo menos 2 vértices de grau 1 (tem pelo menos duas folhas).
(b) Mostre que, se Γ tem número ímpar de vértices, tem pelo menos um vértice de grau par.

11.2 Dada uma árvore Γ com mais de 1 vértice, mostre que o número de folhas é igual a $2 + \sum_{d_v > 1}(d_v - 2)$ onde a soma incide apenas sobre vértices $v \in V$ que não são folhas: $d_v > 1$.

11.3 Construa duas árvores não isomorfas com a seguinte sequência gráfica $(1,1,1,2,2,3)$. Justifique.

11.4 Mostre que qualquer representação planar de uma árvore tem uma única face: a face exterior.

11.5 Mostre que numa árvore Γ, quaisquer dois caminhos de comprimento máximo têm um vértice em comum.

11.6 Um vértice v de Γ chama-se *vértice de corte* se $\Gamma \setminus v$ (grafo obtido retirando v e todas as arestas nele incidentes) tem mais componentes conexas que Γ. Mostre que, se Γ é uma árvore, qualquer vértice que não seja folha é vértice de corte.

11.7 A *excentricidade* de um vértice v (de um grafo conexo Γ) é definida por $\varepsilon(v) := \max\{d(v,\omega) : \omega \in V\}$. Mostre que um vértice de excentricidade máxima é uma folha.

12. Grafos dirigidos e o Algoritmo Google

12.1. **Grafos dirigidos.** Há uma outra classe muito importante, e de facto a mais geral, de grafos. Estes são os *grafos dirigidos*, em que cada aresta tem um sentido associado, passando a ser uma *flecha* ou seta que começa num vértice e termina noutro.

Definição 12.1. Um grafo dirigido é um triplo $\Gamma = (V, A, \psi)$ onde V e A são os conjuntos de vértices e arestas (mais precisamente, flechas) e $\psi : A \to V^2 = V \times V$ é uma simples função. Sendo $\psi(\alpha) = (v_1, v_2) \in V^2$ interpretamos v_1 como o vértice de onde *sai a flecha* α, e v_2 o vértice onde *entra a flecha* α. Neste caso, chamamos a v_1 e v_2 os extremos de α, sendo v_1 o início de α e v_2 o fim de α.

Convém observar que esta definição de grafo dirigido permite todas as possibilidades que existiam nos pseudo-grafos. Ou seja, podem haver flechas α_1 e α_2 cujos extremos são os mesmos $\psi(\alpha_1)=\psi(\alpha_2)$ e também flechas cujo início e fim são o mesmo vértice:

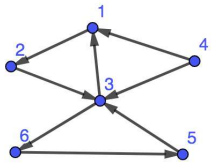
$$\psi(\alpha)=(v,v),$$

para certo $v\in V$.

Observação 12.2. Se Γ é um grafo dirigido, então podemos imediatamente associar a Γ um pseudo-grafo Γ': basta esquecer as direcções das flechas e passam todas a ser arestas. Se, além disso, retirarmos os lacetes e ignorarmos as ligações múltiplas, obtemos um grafo simples.

Na prática, não se usa muito o conjunto A e a função ψ. Em seu lugar, torna-se mais útil e directo descrever um grafo dirigido listando todas as flechas e os vértices que elas ligam.

Por exemplo, para definir o grafo da seguinte figura:



Escrevemos simplesmente:

$$1\to 2;\quad 2\to 3;\quad 3\to\{1,6\};\quad 4\to\{1,3\};\quad 5\to 3;\quad 6\to 5.$$

Também se podem definir, para grafos dirigidos, matrizes de incidência, adjacência e grau, com algumas variações. De facto, temos que distinguir *dois tipos de graus de vértices*, uma vez que cada vértice pode ter várias flechas a sair e outras tantas a entrar.

Definição 12.3. Seja Γ um grafo dirigido e $v\in V$ um seu vértice. O **grau de saída** de v, denotado $d^{>}_{v}$, é o número de arestas que saem de v (ou seja, as arestas que têm v como início) e o **grau de entrada**, denotado $d^{<}_{v}$, é o número de arestas que entram em v.

Usando estas noções podemos agora definir as matrizes de incidência, adjacência e graus para grafos dirigidos.

Definição 12.4. Seja Γ um grafo dirigido com vértices $V=\{v_1,\cdots,v_n\}$ e flechas $A=\{\alpha_1,\cdots,\alpha_m\}$. A **Matriz de Incidência** de Γ é a matriz $M=M_\Gamma$ com $m=|A|$ linhas e $n=|V|$ colunas, cuja entrada na linha i e coluna j (correspondente à aresta α_i e ao vértice v_j) é dada por:

$$M_{ij}=\begin{cases}1, & \text{se } v_j \text{ é o início de } \alpha_i\\ -1 & \text{se } v_j \text{ é o fim de } \alpha_i\\ 0, & \text{se } v_j \text{ não é extremo de } \alpha_i,\end{cases}\qquad i\in[m],\quad j\in[n].$$

A **Matriz de Adjacência** de Γ é uma matriz quadrada $J=J_\Gamma$, simétrica, com $n=|V|$ linhas e colunas, cuja entrada i,j é dada por

$$J_{ij}=\begin{cases}k, & \text{se } i\neq j \text{ e há } k\geq 0 \text{ flechas de } v_j \text{ para } v_i\\ 0, & \text{se } i=j\end{cases}$$

Finalmente, para um grafo dirigido, temos as **Matrizes de Grau de saída e de entrada**, que são matrizes quadradas diagonais $D^{>}=D^{>}_{\Gamma}$ e $D^{<}=D^{<}_{\Gamma}$ com $n=|V|$ linhas e colunas, dada por

$$D^{>}_{ii}=d^{>}_{v_i},\quad D^{<}_{ii}=d^{<}_{v_i},$$

e $D^{>}_{ij}=D^{<}_{ij}=0$, se $i\neq j$.

Definição 12.5. Um grafo dirigido Γ diz-se **fortemente conexo** se dados dois vértices v,w existe um passeio entre eles, sempre percorrendo na direcção das setas.

Exemplo 12.6. O grafo da figura acima, embora seja conexo como grafo simples, esquecendo a direcção das setas, não é fortemente conexo porque, por exemplo, partindo do vértice 1, não se pode chegar ao 4 percorrendo um passeio na direcção das setas.

12.2. **Matrizes estocásticas e o Teorema de Perron-Frobenius.** Vamos agora introduzir um tipo de matrizes, as matrizes estocásticas, de grande utilidade para modelar o funcionamento dinâmico de várias redes de comunicação tais como a internet.

Definição 12.7. Um vector $\mathbf{v} \in \mathbb{R}^n$ chama-se *probabilístico* ou *estocástico* se todas as coordenadas são não negativas e a sua soma é 1. Uma matriz quadrada $n \times n$ com entradas reais diz-se *estocástica*, se todas as suas colunas são vectores estocásticos.

Observação 12.8. É frequente usar-se a terminologia "matriz estocástica por colunas" para as matrizes quadradas que verificam a definição anterior. Mas como apenas consideramos este caso, por simplicidade, omitimos a parte "por colunas".

Lema 12.9. *O produto de duas matrizes estocásticas (do mesmo tamanho $n \times n$) é ainda uma matriz estocástica.*

Demonstração. Sejam A e B duas matrizes estocásticas $n \times n$. Então, para todo $i \in [n]$, temos $\sum_j A_{ij} = \sum_k B_{jk} = 1$. Assim:

$$\sum_k (AB)_{ik} = \sum_k \sum_j A_{ij} B_{jk} = (\sum_j A_{ij})(\sum_k B_{jk}) = 1,$$

para todo o $i \in [n]$, tal como queríamos provar. □

Exercício 12.10. Mostre que Mv é um vector estocástico, se M e v o forem.

Recordemos os conceitos de valor próprio e de vector próprio de uma matriz quadrada.

Definição 12.11. Seja M uma matriz quadrada. Um número real $\lambda \in \mathbb{R}$ diz-se valor próprio de M se é raíz do polinómio característico:

$$p(x) = \det(M - \lambda I).$$

Um vector não nulo $\mathbf{v}$ chama-se vector próprio (de valor próprio λ) se verifica:

$$M\mathbf{v} = \lambda \mathbf{v}.$$

Proposição 12.12. *Uma matriz estocástica tem sempre um valor próprio igual a 1.*

Demonstração. Seja M matriz estocástica. Como $\det M = \det M^t$, sendo M^t a matriz transposta de M, temos $\det(M - \lambda I) = \det(M - \lambda I)^t = \det(M^t - \lambda I)$, pelo que os valores próprios de M e de M^t coincidem. Seja $\mathbf{e} = (1, 1, \cdots, 1) \in \mathbb{R}^n$ (vector com todas as entradas iguais a 1). Para cada linha de M^t, a soma das entradas é 1. Assim:

$$M^t \mathbf{e} = \mathbf{e}.$$

Isto significa que $\mathbf{e}$ é vector próprio de M^t com valor próprio 1. □

É importante observar que M e M^t, apesar de terem os mesmos valores próprios, *não têm os mesmos vectores próprios*! Assim, o vector $\mathbf{e}$ não é usualmente vector próprio de M. No entanto, temos o seguinte resultado de enorme relevância.

Dizemos que uma matriz estocástica é *positiva* se todas as suas entradas são positivas (ou seja, não têm zeros).

Teorema 12.13. *Seja M uma matriz estocástica positiva. Então:*

- *1 é valor próprio de M*
- *Existe um único vector próprio estocástico $\mathbf{p}$ com valor próprio 1*

- *Todos os outros valores próprios de M têm módulo menor que 1.*
- *$M^n\mathbf{v}$ tende para $\mathbf{p}$, para qualquer $\mathbf{v}$ estocástico.*

Definição 12.14. Dada uma matriz estocástica positiva M, chamamos ao vector $\mathbf{p}$ do teorema anterior, o **vector de Perron-Frobenius**.

12.3. **Aplicação à internet.** Vamos considerar um grafo Γ como um mini-modelo de internet. Assim, cada vértice de Γ representa uma página da internet, e vamos considerar que temos os vértices numerados de 1 a $n = |V|$. Se uma aresta sai do vértice i e entra no vértice j significa que a página i aponta (tem um "hyperlink") para página j.

Vamos agora imaginar que estamos a "navegar" na internet percorrendo as ligações que nos são apresentadas. Vamos supor que a página $i \in V$ aponta para as páginas:

$$\{i_1, \cdots, i_k\} \subset V$$

e que a probabilidade de seguirmos para qualquer uma delas é a mesma. Então, teremos probabilidade $\frac{1}{k}$ de visitar cada uma das k páginas.

Assim, cada grafo dirigido com n vértices, determina uma matriz estocástica $n \times n$ da seguinte forma: para cada vértice $i \in [n]$ consideramos o vector estocástico:

$$\mathbf{v}_i = (v_{1i}, v_{2i}, \cdots, v_{ni}), \qquad v_{ji} := \begin{cases} 1/d_i^>, & i \to j \text{ e } d_i^> > 0 \\ 0, & i \not\to j \text{ e } d_i^> > 0 \\ 1/n, & d_i^> = 0 \end{cases}$$

onde $d_i^>$ é o grau de saída do vértice i. Note-se que, no caso em que o grau de saída é zero, o vector $\mathbf{v}_i$ terá todas as entradas iguais a $1/n$ uma vez que estamos a assumir que o utilizador da internet poderá continuar a navegar, mas sem preferência especial por qualquer outra página.

Lema 12.15. *A matriz E, cujas colunas são $\mathbf{v}_1$,$\mathbf{v}_2$, ..., $\mathbf{v}_n$ é uma matriz estocástica.*

Demonstração. Isto é claro, uma vez que cada vector $\mathbf{v}_i = (v_{1i}, v_{2i}, \cdots, v_{ni})$ é estocástico. De facto, para cada $i \in [n]$, se $d_i^> > 0$ temos:

$$\sum_{j=1}^{n} v_{ji} = d_i^> \cdot \frac{1}{d_i^>} = 1,$$

como pretendido, e se $d_i^> = 0$ temos $\sum_{j=1}^{n} v_{ji} = n\frac{1}{n} = 1$. □

Definição 12.16. Dado um grafo dirigido Γ, à matriz E do Lema anterior chamamos a **matriz estocástica associada ao grafo Γ.**

Exemplo 12.17. Considere o grafo dirigido dado por grafo dado por $1 \to \{2,3,4\}$; $2 \to \{3,4\}$; $4 \to 1$. A matriz estocástica associada é:

$$E = \begin{pmatrix} & & \frac{1}{4} & 1 \\ \frac{1}{3} & & \frac{1}{4} & \\ \frac{1}{3} & \frac{1}{2} & \frac{1}{4} & \\ \frac{1}{3} & \frac{1}{2} & \frac{1}{4} & \end{pmatrix}$$

onde os espaços representam zeros.

Observação 12.18. O exemplo anterior mostra que a matriz estocástica associada a um grafo dirigido não é, em geral, positiva. Assim, não podemos aplicar directamente o teorema de Perron-Frobenius. No entanto, com uma pequena modificação, obtemos facilmente uma matriz estocástica positiva a partir de E.

Exercício 12.19. Sejam $s, t \in \mathbb{R}$ com $s + t = 1$ e seja B uma matriz estocástica. Mostre que a matriz:

$$M = sB + \frac{t}{n}\mathbf{1},$$

é ainda uma matriz estocástica, onde **1** é a matriz cujas entradas são todas iguais a 1.

Definição 12.20. Dado um grafo dirigido Γ e um peso $\rho \in]0,1[$, chamamos **vector pagerank de peso** ρ, ao vector de Perron-Frobenius da matriz: $M = (1-\rho)E + \frac{\rho}{n}\mathbf{1}$, sendo E a matriz estocástica associada a Γ.

Um valor típico para ρ é 0.15. Este é um valor que não tem muita relevância do ponto de vista teórico, mas permite uma boa convergência, tal como garantido pelo próximo resultado.

Corolário 12.21. *Dado um grafo dirigido* Γ, *com* $n = |V|$, $\rho \in]0,1[$, *e*

$$M = (1-\rho)E + \frac{\rho}{n}\mathbf{1},$$

o vector pagerank de peso ρ, $\mathbf{p}$, *é dado por:*

$$M\mathbf{p} = \mathbf{p}$$

Além disso, a sequência:

$$\mathbf{v}, M\mathbf{v}, M^2\mathbf{v}, \cdots, M^n\mathbf{v}, \cdots$$

converge, para qualquer $\mathbf{v}$ *estocástico, para* $\mathbf{p}$.

De acordo com o modelo probabilístico, a maior entrada do vector pagerank $\mathbf{p}$ será correspondente ao vértice onde um utilizador da internet passará, em média mais tempo, se navegar na internet de forma aleatória.

Assim, para um grafo Γ que modela a internet, *vector pagerank* atribui a cada vértice a sua importância de acordo com a estrutura interna do grafo.

Problemas de Revisão.

11.8 Determine as matrizes de incidência, adjacência, grau de entrada e grau de saída dos grafos dirigidos do problema 9.1.

11.9 Desenhe um representante para todas as classes de isomorfismo de grafos dirigidos com 3 vértices sem ciclos orientados, e cujo grafo simples associado seja conexo.

11.10 Seja Γ um grafo dirigido com $d^{>}_{v} > 0$ para todo $v \in V$. Mostre que Γ tem um ciclo orientado. Pode concluir o mesmo, caso $d^{<}_{v} > 0$ para todo $v \in V$?

11.11 Considere as seguintes matrizes onde os espaços representam zeros:

$$B = \begin{pmatrix} 1 & 1 & -1 & & & & \\ -1 & & & -1 & 1 & & \\ & -1 & & 1 & & -1 & \\ & & 1 & & -1 & 1 & \end{pmatrix}, \quad C = \begin{pmatrix} -1 & -1 & -1 & -1 & & & & & \\ 1 & 1 & & & -1 & 1 & & & \\ & & & & 1 & & -1 & -1 & \\ & & 1 & & & & 1 & 1 & 1 \\ & & & 1 & & -1 & & & -1 \end{pmatrix}$$

Desenhe grafos dirigidos Γ e Γ' cujas matrizes de incidência são $M = B^{\mathrm{t}}$ e $M' = C^{\mathrm{t}}$. Determine as respectivas matrizes de adjacência e de grau de entrada e de saída.

Apêndice A. Conjuntos Finitos, Funções e Cardinal

Neste apêndice, recordam-se os conceitos de conjunto, de cardinal de um conjunto finito, e das operações básicas que podemos fazer com eles.

A.1. **Operações com conjuntos.** Recorde-se que, se X é um conjunto, a expressão $x \in X$ significa que x é um elemento de X, ou seja, que x *pertence a* X. O conjunto vazio, denotado por $\emptyset$, é o conjunto sem elementos.

Dados dois conjuntos A, B a expressão $A \subset B$ significa que A está contido em B, ou equivalentemente, que A é um subconjunto de B (permite-se a igualdade dos dois conjuntos, ou seja

$A \subset A$ verifica-se sempre). Para que $A \subset B$, é necessário e suficiente que qualquer elemento de A pertença também a B.

Definição A.1. Dados dois conjuntos A, B, definimos as seguintes operações:

- **União**: $A \cup B := \{x \in A \vee x \in B\}$
- **Intersecção**: $A \cap B := \{x \in A \wedge x \in B\}$
- **Diferença**: $A \setminus B := \{x \in A \wedge x \notin B\}$
- **Diferença simétrica**: $A \triangle B := (A \setminus B) \cup (B \setminus A)$
- **Produto (Cartesiano)**: $A \times B := \{(a,b) : a \in A, b \in B\}$

Quando trabalhamos apenas com subconjuntos de um grande conjunto U, designado o conjunto universal ou **universo** (usualmente está subentendido), temos também a operação:

- **Complementar:** $A^c := U \setminus A$

Dois conjuntos cuja intersecção é vazia dizem-se disjuntos. Se A e B são conjuntos disjuntos, dizemos que a sua união é uma **união disjunta** e usa-se a notação:

$$A \sqcup B := A \cup B, \qquad \text{sempre que } A \cap B = \emptyset.$$

Na definição de produto usámos a notação $(a,b) \in A \times B$ para denotar um par ordenado. Isto representa uma escolha simultânea de um elemento a de A e de um elemento b de B.

Algumas operações acima são associativas, pelo que podemos aplicá-las, de forma imediata, a mais que dois conjuntos. Por exemplo, a união e a intersecção de uma colecção (finita) de conjuntos $\{X_i\}_{i=1}^k$ denota-se, respectivamente, por:

$$X_1 \cup \cdots \cup X_k = \bigcup_{i=1}^{k} X_i, \qquad X_1 \cap \cdots \cap X_k = \bigcap_{i=1}^{k} X_i.$$

Estas operações verificam várias propriedades, que podemos usar para facilitar o seu estudo. Algumas das propriedades mais importantes são:

- **Distributividade:** $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ e $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $A \cap \emptyset = \emptyset, \qquad A \cup \emptyset = A$
- $A \setminus \emptyset = A, \qquad A \setminus B = A \setminus (A \cap B)$
- $A \times (B \cap C) = (A \times B) \cap (A \times C), \qquad A \times (B \cup C) = (A \times B) \cup (A \times C)$

Exercício A.2. Verifique estas propriedades usando apenas as definições acima (Definição A.1).

A.2. **Funções.** Sejam X e Y dois conjuntos. Recorde-se que uma função f entre X e Y (também se diz f de X para Y) é uma regra que associa a cada elemento $x \in X$ um elemento (e um só) de Y denotado por $f(x) \in Y$. A notação usada é:

$$\begin{aligned} f : X &\to Y \\ x &\mapsto y = f(x). \end{aligned}$$

Os conjuntos X e Y chamam-se, respectivamente, os conjuntos de partida e de chegada da função $f : X \to Y$. Por vezes, X chama-se também o domínio da função f.

Exemplo A.3. Como exemplos de funções temos:
(1) Exemplo de função *constante* $f : \mathbb{N} \to \mathbb{Z}$ dada por $f(n) = 23$.
(2) Exemplo de função *linear* $g : \mathbb{Q} \to \mathbb{Q}$, onde $g(x) = 5x$.
(3) Exemplo de função *polinomial* $h : \mathbb{Z} \to \mathbb{Q}$, definida por $h(a) = \frac{1}{3}a^2 + \frac{5}{4}a + \frac{3}{2}$.
(4) Exemplo de função *trigonométrica* $\psi : \mathbb{R} \to [-1,1]$ com $\psi(x) = \cos(x)$.

Definição A.4. Sejam $A \subset X$ e $B \subset Y$ subconjuntos e $f : X \to Y$ uma função. A **imagem directa** (ou simplesmente **imagem**) de A é o conjunto

$$f(A) := \{f(x) \in Y : x \in A\} \subset Y,$$

e a **imagem inversa** de B é o conjunto:

$$f^{-1}(B) := \{x \in X : f(x) \in B\} \subset X.$$

Quando consideramos um subconjunto de Y com um único elemento $\{y\} \subset Y$ escrevemos $f^{-1}(y)$ em vez de $f^{-1}(\{y\})$. Da mesma forma, quando $f^{-1}(B)$ é um conjunto com um único elemento, escrevemos $f^{-1}(B) \in X$ em vez de $f^{-1}(B) \subset X$.

Proposição A.5. *Sejam $A, B \subset X$, $C, D \subset Y$ e $f : X \to Y$ uma função. As imagens directas e inversas verificam:*

$$\begin{aligned} f(A \cup B) &= f(A) \cup f(B) \\ f(A \cap B) &\subset f(A) \cap f(B) \\ f^{-1}(C \cap D) &= f^{-1}(C) \cap f^{-1}(D) \\ f^{-1}(C \cup D) &= f^{-1}(C) \cup f^{-1}(D) \\ f^{-1}(C \setminus D) &= f^{-1}(C) \setminus f^{-1}(D), \\ A &\subset f^{-1}(f(A)) \\ f(f^{-1}(D)) &\subset D. \end{aligned}$$

Como consequência da terceira e quarta igualdades acima, vemos que a imagem inversa de uma união disjunta é também disjunta.

$$f^{-1}(C \sqcup D) = f^{-1}(C) \sqcup f^{-1}(D), \tag{A.1}$$

e em particular $f^{-1}(y_1) \cap f^{-1}(y_2) = \varnothing$ sempre que $y_1 \neq y_2 \in Y$.

Exercício A.6. Prove a Proposição A.5. Prove a igualdade (A.1), bem como a última afirmação acima.

Na disciplina de cálculo, estudam-se funções no conjunto X com valores reais, ou seja $f : X \to \mathbb{R}$. Duas destas funções podem somar-se ou multiplicar-se, porque $\mathbb{R}$ tem essa estrutura algébrica. Mas, quando o conjunto imagem não admite essas operações, não podemos somar nem multiplicar funções.

Por outro lado, caso o conjunto imagem de f coincida com o conjunto de partida de g, podemos fazer a *composição* de g com f, que é uma das operações mais importantes com funções.

Definição A.7. A composição das funções $f : X \to Y$ e $g : Y \to Z$ é a função definida por

$$\begin{aligned} g \circ f : X &\to Z \\ x &\mapsto g(f(x)). \end{aligned}$$

Note-se que $g \circ f$ está bem definida porque $f(x) \in Y$, e Y é o conjunto de partida de g. A composição pela outra ordem $f \circ g$ só estaria definida se $g(y) \in X$ para todo o $y \in Y$, ou seja se $g(Y) \subset X$.

Exemplo A.8. Seja $f(n) := \log n$, $f : \mathbb{N} \to \mathbb{R}$ e $g(x) := x^2 + 1$, $g : \mathbb{R} \to \mathbb{R}$. Então $g \circ f(n) = (\log n)^2 + 1$.

Exercício A.9. Se duas funções têm o mesmo conjunto de partida e chegada $f, g : X \to X$ então podemos sempre compor das duas formas: $f \circ g$ e $g \circ f$. Mostre que, mesmo neste caso, $f \circ g \neq g \circ f$, em geral.

A.3. **Funções Injectivas, Sobrejectivas, e Bijectivas.**

Definição A.10. A função f diz-se **injectiva** se $f(x) \neq f(x')$ sempre que $x \neq x'$ para $x, x' \in X$. Diz-se que f é **sobrejectiva** se para todo o $y \in Y$ existe $x \in X$ tal que $f(x) = y$. Finalmente, diz-se que f é **bijectiva** se for injectiva e sobrejectiva.

Exercício A.11. Seja $f : X \to Y$. Mostre que $f^{-1}(Y) = X$ e que f é sobrejectiva se e só se $f(X) = Y$. Classifique, justificando, as funções do Exemplo A.3 quanto à injectividade, sobrejectividade, e bijectividade.

As seguintes propriedades das funções injectivas e sobrejectivas são fundamentais em combinatória.

Proposição A.12. *Seja $f : X \to Y$ uma função. Então:*
(1) f é injectiva sse $f^{-1}(y)$ não contém mais que um único elemento $\forall y \in Y$.
(2) f é sobrejectiva sse $f^{-1}(y)$ é não vazio $\forall y \in Y$.
(3) f é bijectiva sse $f^{-1}(y)$ é um único elemento de X, ou seja, sse a regra $y \in Y \mapsto f^{-1}(y) \in X$ define uma função, a função inversa $f^{-1} : Y \to X$.
(4) A composição de duas funções injectivas (resp. sobrejectivas, bijectivas) é injectiva (resp. sobrejectiva, bijectiva).
(5) Seja $g : X \to Y$ bijectiva. Se $f_1 : Y \to Z$ e $f_2 : W \to X$ são sobrejectivas, então $g \circ f_2$ e $f_1 \circ g$ também são sobrejectivas; o mesmo se passa com a injectividade.

Demonstração. (1) Se $f^{-1}(y)$ tem mais de um elemento, sejam $x_1, x_2 \in f^{-1}(y)$ elementos distintos de X. Então $f(x_1) = y = f(x_2)$, pelo que f não é injectiva. Reciprocamente, se f não é injectiva, então existem $x_1 \neq x_2$ em X tais que $f(x_1) = f(x_2)$. Seja $y = f(x_1) = f(x_2) \in Y$. Logo $\{x_1, x_2\} \subset f^{-1}(y)$, pelo que $f^{-1}(y)$ tem 2 elementos ou mais.
(2) Se $f^{-1}(y) = \{x \in X \mid f(x) = y\} = \emptyset$ então não existe nenhum $x \in X$ com $f(x) = y$ pelo que f não é sobrejectiva. Reciprocamente, se f não é sobrejectiva, existe pelo menos um y tal que nenhum x verifica $f(x) = y$. Ou seja $f^{-1}(y) = \{x \in X \mid f(x) = y\} = \emptyset$, como pretendido. As outras propriedades são deixadas para o leitor. □

Notação: Por simplicidade, vamos adoptar notações especiais para os seguintes conjuntos muito usados :

$$\begin{aligned} [n] &:= \{1, 2, \cdots, n\} \\ [n]_0 &:= \{0, 1, 2, \cdots, n\}. \end{aligned}$$

Assim, $[n]$ tem exactamente n elementos (e $[n]_0$ tem $n+1$). Note-se que se escrevermos $[n]$ como união disjunta:

$$[n] = A_1 \sqcup A_2 \sqcup \cdots \sqcup A_k \tag{A.2}$$

então a soma do número de elementos de todos os subconjuntos A_i é precisamente igual a n. O primeiro resultado acerca de funções entre conjuntos finitos é o seguinte.

Corolário A.13. *Não existe nenhuma bijecção entre $[n]$ e $[m]$ se $n \neq m$. Mais precisamente, seja $f : [n] \to [m]$ uma função. Então:*

- *Se $n < m$, então f não é sobrejectiva,*
- *Se $n > m$ então f não é injectiva.*

Demonstração. Sejam $n, m \in \mathbb{N}$ e supomos $f : [n] \to [m]$ sobrejectiva, pelo que $f^{-1}(x) \neq \emptyset$, para cada número $x \in [m]$. Pelo exercício A.6, temos que $f^{-1}(x) \cap f^{-1}(y) = \emptyset$ sempre que $x \neq y \in [m]$. Assim, temos uma união *disjunta*:

$$[n] = f^{-1}(\{1, 2, \cdots, m\}) = f^{-1}(1) \sqcup \cdots \sqcup f^{-1}(m),$$

por subconjuntos não vazios, cada qual com pelo menos um elemento. Assim $n \geq m$, de acordo com a observação da Equação (A.2). Supomos agora $f : [n] \to [m]$ injectiva. Então $f^{-1}(x)$ tem, no máximo, um elemento, para todo $x \in [m]$. Logo, a mesma união disjunta fornece a desigualdade oposta: $n \leq m$. □

De imediato, concluímos o seguinte.

Corolário A.14. *Se $f : [n] \to [m]$ é uma função bijectiva, então $n = m$.*

Uma vez que as bijeções são fundamentais na combinatória, vamos usar uma notação especial. Escrevemos $X \longleftrightarrow Y$ quando existe uma bijecção (função bijectiva) $f : X \to Y$.

A.4. **Cardinal.**

Definição A.15. Diz-se que um conjunto X é **finito** se existe $n \in \mathbb{N}_0$ e uma função bijectiva $f : [n] \to X$. Este número n, que é único pelo corolário anterior, designa-se por cardinal de X, e escreve-se $n = |X|$ ou $n = \#X$.

Por exemplo, temos $|[n]| = n$ e $|[n]_0| = n+1$. Nota-se também que o conjunto vazio $\varnothing$ é o *único* conjunto com cardinal zero. Usando a noção de cardinal, o Corolário A.13 assume ainda outra forma, consequência imediata da anterior formulação.

Corolário A.16. *Dois conjuntos finitos, A e B tem o mesmo cardinal se e só se existe uma bijecção entre eles. Se $f : A \to B$ então, f não pode ser sobrejectiva quando $|A| < |B|$, e não pode ser injectiva quando $|A| > |B|$.*

Frequentemente, é importante calcular o cardinal de um conjunto de funções. Assim, vamos introduzir a seguinte notação.

Sendo X e Y conjuntos finitos, denotamos por:

$$\mathscr{F}(X,Y) \qquad \text{ou por} \qquad Y^X,$$

o conjunto de todas as funções $f : X \to Y$. Assim $f \in \mathscr{F}(X,Y)$ se e só se f tem domínio X e conjunto imagem Y. Vamos ver que $\mathscr{F}(X,Y)$ é também um conjunto finito.

Exemplo A.17. Seja $|X| = n$, e vamos determinar o número de funções $f : X \to \{0,1\}$. Como X é bijectivo a $[n]$, isto equivale a contar funções $f : [n] \to \{0,1\}$. Uma tal função fica completamente especificada pela sequência $(f(1), f(2), \cdots, f(n))$, em que $f(i) \in \{0,1\}$ para $i \in [n]$. Estas sequências de "zeros" e "uns" correspondem a números escritos em base 2. Por exemplo, um *bite* é uma sequência de 8 "zeros" e "uns" e representa um número entre 0 e $255 = 2^8 - 1$ (admitimos números escritos com "zeros à esquerda", por exemplo $[00010001]_2 = 17$). Da mesma forma, as sequências de n "zeros" e "uns" representam os números de 0 a $2^n - 1$. Assim, concluímos:

$$|\mathscr{F}(X,\{0,1\})| = 2^n,$$

sempre que $|X| = n$.

A.5. **Relações de equivalência.** O conceito de relação de equivalência serve para analisarmos melhor os conjuntos em que alguns elementos podem ser considerados, de alguma forma, equivalentes. Por exemplo, num conjunto de moedas, podemos agrupar as moedas segundo o seu valor: as moedas de 5 cêntimos são consideradas equivalentes, etc.

Dado um conjunto X, uma *relação de equivalência em X* é uma *partição* de X em subconjuntos disjuntos, de forma que cada subconjunto fica com os objectos que estamos a considerar **equivalentes**.

Exemplo A.18. (1) Sendo $X = \{x, y, \xi, \phi, \psi, \mathfrak{g}, \mathfrak{h}\}$, podemos tornar equivalentes as letras do mesmo alfabeto. Em X temos letras latinas, gregas e germânicas, que corresponde à união (disjunta):

$$X = \{x, y\} \sqcup \{\xi, \phi, \psi\} \sqcup \{\mathfrak{g}, \mathfrak{h}\}.$$

Usualmente, em vez de nos referirmos ao conjunto X, uma relação de equivalência é descrita por um símbolo, por exemplo o símbolo $\sim$, entre dois elementos do conjunto X. No exemplo acima, escrevemos $x \sim y$, $\xi \sim \phi$ e $\mathfrak{g} \sim \mathfrak{h}$. Qualquer relação de equivalência verifica sempre as seguintes propriedades.

Proposição A.19. *Se $\sim$ é uma relação de equivalência, então verifica, para todos os elementos $x, y, z \in X$ (iguais ou diferentes):*

- $x \sim x$ *($\sim$ é reflexiva)*

- *Se $x \sim y$, então $y \sim x$ ($\sim$ é simétrica)*
- *Se $x \sim y$ e $y \sim z$, então $x \sim z$ ($\sim$ é transitiva)*

Esta proposição mostra que uma relação de equivalência é precisamente caracterizada pelas 3 propriedades: reflexiva, simétrica e transitiva.

Exercício A.20. (a) Considere a relação, em $\mathbb{Z}$, dada por: $x \sim y$ se $x - y$ é um número par. Mostre que $\sim$ é uma relação de equivalência.
(b) Considere, no conjunto dos seres humanos, as relações: $\rightarrow$ definida por: $x \rightarrow y$ se x é pai de y, e $\wedge$ dada por: $x \wedge y$ se x e y nasceram no mesmo dia. Mostre que $\wedge$ é uma relação de equivalência, mas que $\rightarrow$ não o é.

Dado um conjuto X com uma relação de equivalência $\sim$, podemos sempre considerar vários novos conjuntos. Em particular, dado $x \in X$ podemos ver quais os $y \in X$ que são equivalentes a x, isto é considerar o conjunto:

$$E_x := \{y \in X \mid y \sim x\}$$

Ao conjunto E_x chamamos a **classe de equivalência de** x (omitindo a relação $\sim$, se esta estiver subentendida).

Há ainda outra conjunto importante, chamado o conjunto das classes de equivalência da relação $\sim$.

Definição A.21. Dado um conjunto finito $X = \{x_1, \cdots, x_n\}$, e uma relação de equivalência $\sim$ em X, o **conjunto das classes de equivalência** é o conjunto:

$$\{E_{x_1}, \cdots, E_{x_n}\}$$

(em que se omitem repetições caso hajam elementos iguais).

Exemplo A.22. No exemplo anterior $X = \{x, y, \xi, \phi, \psi, \mathfrak{g}, \mathfrak{h}\}$ temos 3 classes de equivalência:

$$E_x = \{x, y\} = E_y, \qquad E_\xi = \{\xi, \phi\}, \qquad \text{e} \qquad E_\mathfrak{g} = \{\mathfrak{g}, \mathfrak{h}\}.$$

REFERÊNCIAS

[Big85] Norman L. Biggs, *Discrete mathematics*, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1985. MR 826531

[GKP94] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik, *Concrete mathematics*, second ed., Addison-Wesley Publishing Company, Reading, MA, 1994, A foundation for computer science. MR 1397498

[LPV03] L. Lovász, J. Pelikán, and K. Vesztergombi, *Discrete mathematics*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2003, Elementary and beyond. MR 1952453

[Mer03] Russell Merris, *Combinatorics*, second ed., Wiley-Interscience Series in Discrete Mathematics and Optimization, Wiley-Interscience [John Wiley & Sons], New York, 2003. MR 2000100

[Ros18] Kenneth H. Rosen, *Discrete mathematics and its applications*, 8th ed., McGraw-Hill Higher Education, 2018.

[Sta99] Richard P. Stanley, *Enumerative combinatorics. Vol. 2*, Cambridge Studies in Advanced Mathematics, vol. 62, Cambridge University Press, Cambridge, 1999, With a foreword by Gian-Carlo Rota and appendix 1 by Sergey Fomin. MR 1676282

[Sti03] John Stillwell, *Elements of number theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2003. MR 1944957