FUNDAMENTOS DE MATEMÁTICA DISCRETA

CARLOS A. A. FLORENTINO
NOVEMBRO 2014

Conteúdo

Prefácio 2

Parte 1. NÚMEROS 3
1. Números Inteiros 3
2. Números Racionais 19
3. Números Modulares 23
4. Números Cardinais Finitos 30
5. Fermat, Euler e Criptografia 32

Parte 2. FUNÇÕES e COMBINATÓRIA 40
6. Conjuntos e Contagens 40
7. Funções Polinomiais 48
8. Séries Formais e Funções Geradoras 57
9. Funções Geradoras em Combinatória 59
10. Permutações e Simetrias 63

Parte 3. GRAFOS 66
11. Grafos e Matrizes 66
12. Caminhos e Conexidade 69
13. Grafos Planares 70
14. Árvores 70
15. Colorações 70
16. Emparelhamentos 70
Apêndice A. Raízes e Factorização de Polinómios 71
Apêndice A. O Teorema fundamental da Álgebra 73
Referências 75

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", estudam-se, com algum detalhe, várias propriedades das funções polinomiais, das funções racionais e das séries de potências, sendo estas últimas interpretadas como funções geradoras de problemas combinatórios. Estudam-se também problemas de combinatória enumerativa mais gerais, e introduz-se a teoria das permutações e contagens com simetria.

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, nos vários aspectos clássicos desta teoria. Tenta-se também cobrir a maioria dos aspectos teóricos 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 implementados 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 *reunião* 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*.

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

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

Faremos um estudo bastante mais detalhado de várias propriedades e operações em conjuntos, em particular para o caso de conjuntos *finitos*, na segunda parte do livro, ao abordar 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 "$\times$" ou "$\cdot$". 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 "$\forall$" 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) $(-1) \cdot a = -a$,

(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].

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

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 1.4. 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 1.3(c).

Proposição 1.5. *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 1.6. *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 1.4(a)) e a transitividade da relação $<$ (Proposição 1.5) 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 1.5 (d)), e chamados então, respectivamente, o *quociente* e o *resto* da divisão de a por b.[2]

[2]Numa terminologia menos usada, a e b, chamam-se o *dividendo* e o *divisor*, respectivamente.

Exemplo 1.7. Vamos elaborar o algoritmo de divisão no caso seguinte: a divisão de $a = 487$ por $b = 32$. Temos:

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

Concluímos então: $487 = 32 \cdot 15 + 7$. Assim, 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 1.8. 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 1.8. 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 1.9. 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 1.10. *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 $a, b > 0$ 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 $a \mid bk$, e $ak \mid bk$ 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 $a = bq + r$, se $c \mid a$ e $c \mid b$, então $c \mid r$.

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

Observação 1.11. 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.

Um *diagrama de divisores* é um diagrama que mostra os divisores (positivos) de um dado natural e suas relações de divisão. 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 $a \to b$ aparecem sempre que a é o maior divisor de b distindo de b. Num destes diagramas, os primeiros naturais que aparecem logo a seguir ao 1 (o 1 está sempre presente (Exercício 1.6(a))) chamam-se *números primos*.

1.4. **Números primos.**

Definição 1.12. 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 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 $n > 1$).

Exemplo 1.13. 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 1.14. 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 1.15. *Qualquer número natural é divisível por algum primo.*

Demonstração. Seja $a \in \mathbb{N}$. Se a é primo, nada há a provar. Seja então $a = a_1$ um número composto: $a_1 = a_2 b$ para certos números naturais a_2, $b > 1$ (Exercício 1.14). 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. □

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

Observação 1.16. Da mesma forma, qualquer inteiro não nulo, diferente de ± 1 é divisível por algum primo.

Teorema 1.17. *(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 1.9 (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 1.18. Sejam dados inteiros $a, b \in \mathbb{Z}$, em que pelo menos um deles é não nulo. Dizemos que d é um máximo divisor comum b (abreviadamente mdc) de a e b, se d é positivo, divide ambos os inteiros a e b, e se qualquer outro $c \in \mathbb{N}$ com as mesmas propriedades divide d (ou seja, se as condições $c \mid a$ e $c \mid b$ implicam $c \mid d$).

Esta definição garante que o máximo divisor é único. Mas, à partida, não é imediatamente evidente que exista um natural d com as propriedades indicadas (para todos os pares a, b nas condições indicadas). Isto será mostrado no Teorema 1.26.

Proposição 1.19. *Dados inteiros a e b não ambos nulos, existe um único máximo divisor comum de a e b.*

Demonstração. Sejam d e d' dois máximos divisores comuns de a e b. Então, como tanto d como d' dividem simultaneamente a e b, a última condição da definição diz-nos que $d \mid d'$ e $d' \mid d$. Então, pela Proposição 1.10(2) temos $d' = \pm d$. Finalmente, como tanto d como d' são positivos, por definição, concluimos $d = d'$. □

Notação 1.18. Sendo $a, b \in \mathbb{Z}$ não ambos nulos, o único máximo divisor comum entre a e b é denotado por $\text{mdc}(a, b)$, ou por vezes, simplesmente por (a, b).

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 1.20. 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) $(b, 1) = (1, b) = 1$

Observação 1.21. 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.

Definição 1.22. Sejam $a, b \in \mathbb{Z}^\times$. Se 1 é o máximo divisor comum de a e b, $\text{mdc}(a, b) = 1$, então a e b dizem-se primos entre si.

Exercício 1.23. 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 1.24. *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 1.25. 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 1.20(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 1.20), 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 1.26. *[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

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

Assim, D tem cardinalidade inferior a $a = d_0$. Seja $d_{n+1} = 0$. 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 a e b. 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. 1.6). Assim, concluímos que $c \mid d_n$ e portanto, por definição de máximo divisor comum, o mdc entre a e b existe, e é igual a $d_n = (a, b)$. □

1.6. **A equação de Bézout.** A seguinte identidade, chamada equação de Bézout, é de grande utilidade em várias situações.

Teorema 1.27. *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, u e v são as únicas soluções, a menos de sinal, 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". Usemos a mesma notação que na demonstração do Teorema 1.26, 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 aos índices 0 e 1, ou seja, escrevemos 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. Estas têm uma interessante interpretação geométrica que deixaremos para o capítulo dos números racionais. □

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. No entanto, quando há muitas operações envolvidas, convém recorrermos a uma tabela para sistematizar os cálculos e evitar erros, como no seguinte exemplo.

Exemplo 1.28. 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, o seguinte:

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		13	-70

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

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:

$$d = au + bv,$$

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

Exercício 1.29. Mostre que, dada uma solução (u_0, v_0) da equação de Bézout $d = au + bv$ 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 1.30. *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 1.29. □

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

Teorema 1.31. *Sejam dados inteiros não nulos a, b, c, com $d = (a, b)$. Então, a equação*

$$c = a\,u + b\,v$$

tem solução $u, v \in \mathbb{Z}$ 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 $c = au + bv$ para certos $u, v \in \mathbb{Z}$, então $d \mid au + bv$ (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 1.23). 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 1.32. *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 1.31 $d = 1$ é múltiplo de (a, bc). Ou seja, $(a, bc) = 1$ como queríamos mostrar. □

Uma propriedade fundamental dos números primos é a seguinte.

Proposição 1.33. *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: $A = B$, $A = \varnothing$.

Definição 1.34. 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 1.35. 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 1.36. Note-se que para o conjunto $\mathbb{Z}$, o mesmo princípio não é válido em geral (Exercício 1.37(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 1.37(2)).

Exercício 1.37. (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 1.38. 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 1.39. *(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 $A_P = \varnothing$, 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 1.40. *(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 1.41. Mostre o princípio de indução forte, a partir do Princípio de Indução (Teorema 1.39). 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 1.42. 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 1.43. *("Teorema Fundamental da Aritmética"). 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 necessriamente 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 1.40 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:

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

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

Procedendo de igual forma, agora com p_2 obtemos $p_2 = q_2$ (com possível nova troca de índices), e assim sucessivamente, e concluimos 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 1.44. *[Fundamental da Aritmética, versão 2] Qualquer número natural $a \in \mathbb{N}$ se pode escrever na forma*

$$a = p_1^{k_1} \cdots p_l^{k_l},$$

onde $p_1, \cdots, p_m$ são números primos distintos*, e os expoentes são naturais: $k_1, \cdots, k_l \in \mathbb{N}$ sendo $l \in \mathbb{N}_0$. Esta factorização é única a menos de reordenação dos factores.*

Observação 1.45. Se pretendermos uma decomposição de um número inteiro $a \in \mathbb{Z} \setminus \{0\}$, não nulo, mas não necessariamente positivo, poderíamos escrever

$$a = \mathrm{s}(a)\, p_1^{k_1} \cdots p_l^{k_l},$$

usando a noção de sinal de a:

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

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. 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 1.46. 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 1.43 e a segunda ao teorema 1.44) é o mesmo que dizer que $P_{693} = \{3, 7, 11\}$ e que $e_3(693) = 2$, $e_7(693) = e_{11}(693) = 1$.

O teorema fundamental diz-nos que os primos que aparecem na factorização de n são:

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

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

Proposição 1.47. *Dois naturais a, b são primos entre si se e só se $P_a \cap P_b = \varnothing$.*

Demonstração. Se p é um primo que aparece na factorização de a e na de b, então $p \mid a$ e $p \mid b$. Assim, $p \mid (a, b)$ pelo que $(a, b) > 1$ e a e b não podem ser primos entre si. Reciprocamente, se $(a, b) = d > 1$ então seja p um primo que divide d, $p \mid d$. Então $p \mid d \mid a$ e $p \mid d \mid b$ pelo que $p \in P_a$ e $p \in P_b$, ou seja $P_a \cap P_b$ não é vazio. □

Proposição 1.48. *O mdc e o mmc podem ser calculados através das factorizações em primos. De facto,*

$$(a, b) = p_1^{k_1} \cdots p_m^{k_m}$$

se e só se $P_a \cap P_b = \{p_1, \cdots, p_m\}$ e $k_i = \min\{e_{p_i}(a),\, e_{p_i}(b)\}$ para cada $i = 1, \cdots, m$. Da mesma forma,

$$[a, b] = p_1^{k_1} \cdots p_m^{k_m}$$

se e só se $P_a \cup P_b = \{p_1, \cdots, p_m\}$ e $k_i = \max\{e_{p_i}(a),\, e_{p_i}(b)\}$ para cada $i = 1, \cdots, m$.

Demonstração. A determinação do mdc, segue ao examinar com cuidado a demonstração anterior. A fórmula para o mmc conclui-se da fórmula $(a,b)\cdot[a,b]=ab$ que se encontra no Exercício 10. □

1.9. **Problemas de Revisão.**

(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?

(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.

(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?

(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 $(a,b)=b$.

(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 $n\in\mathbb{N}$.

(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.

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

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

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

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

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

(9) Determine todas as soluções da equação diofantina:

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

(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) $(a,b)\cdot[a,b]=|ab|$.

(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

$$d=x_1a_1+\cdots+x_na_n.$$

(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.

(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?]

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

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

(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) $F_1+F_3+\cdots+F_{2n-1}=F_{2n}$.

(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 $\frac{1}{2}n(n-3)$.

(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.

(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:

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

(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.]

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

(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 $m^2 = n$.

(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, $\log_p n$.

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

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

(26) 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.

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

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

(28) 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
(b) Mostre que, se f é multiplicativa, então também o é $F(n) := \sum_{d|n} f(d)$.

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 $a, b \in \mathbb{Z}$ e $b \neq 0$.

Por outras palavras, um número é x racional se existe um inteiro b tal que a multiplicação bx é novamente um inteiro. Assim, os números racionais incluem os números inteiros. De facto, 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 ($a, b, c, d \in \mathbb{Z}$ e por hipótese b e d não se anulam):

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

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 1.24). 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 $(a,b) = (a',b') = 1$. Seja $k = aa'$. Então

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

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

Exercício 2.4. 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 2.5. 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 2.6. *Qualquer número racional é a soma de um número inteiro com um racional próprio, e esta decomposição é única.*

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.

Seja então $0 < b \leq a$. 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 2.7. Seja $x = \frac{78}{31}$. Então $\frac{78}{31} = 2 + \frac{16}{31}$, pelo que $2 = \left\lfloor \frac{78}{31} \right\rfloor$ e $\frac{16}{31} = /\frac{78}{31}\backslash$.

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 é útil para os computadores, mas são precisos mais de 10 algarismos para representar números maiores que $1024 = 10^{10}$, 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 2.8. Seja $b \in \mathbb{N}$, $b > 1$. A representação de um natural n na base b é uma expressão da forma:

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

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

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

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 $b > 1$. 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 2.9. Seja $b \in \mathbb{N}$, $b > 1$. A representação de um número racional $x \in \mathbb{Q}$ na base b é uma expressão da forma

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

onde $k \in \mathbb{Z}$, $a_k \neq 0$ e $a_j \in \{0, \cdots, b-1\}$ 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 b.

Note-se que a representação decimal dos números racionais não é sempre única, embora isto não represente um grande problema. De facto:

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

Proposição 2.10. *Seja $x = \sum_{j=-\infty}^{k} a_j b^j$ a representação de x na base b, 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. ... □

2.3. **Fracções continadas.** A representação dos números racionais através de fracções é sem dúvida a forma mais comum de identificar e fazer cálculos com estes números.

Existe, no entanto outra representação também útil, chamada a representação por fracções continuadas. Para obter esta representação, usamos novamente o algoritmo de Euclides, que já usámos na determinação do mdc e do mmc de dois inteiros.

Seja, por exemplo: $x = 688/219$. Então temos:

$$\begin{aligned} 688 &= 219 \cdot 3 + 31 \\ 219 &= 31 \cdot 7 + 2 \\ 31 &= 15 \cdot 2 + 1. \end{aligned}$$

Assim, podemos escrever

$$x = \frac{688}{219} = 3 + \frac{31}{219} = 3 + \frac{1}{\frac{219}{31}} = 3 + \frac{1}{7 + \frac{2}{31}} = 3 + \frac{1}{7 + \frac{1}{\frac{31}{2}}} = 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{2}}}.$$

Para abreviar a notação, escrevemos esta fracção continuada como $x = [3, 7, 15, 2]$.

Definição 2.11. Uma fracção continuada é uma expressão da forma

$$[a_0; a_1, a_2, \cdots] := a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\cdots}}},$$

onde $a_0 \in \mathbb{Z}$, e $a_k \in \mathbb{N}$ para $k \in \mathbb{N}$.

Tal como a representação em bases, a representação por fracções continuadas é essencialmente única. Esta representação é obtida, usando o algoritmo de Euclides, como foi feito no exemplo acima.

Por outro lado, ao contrário da representação em bases, a representação em fracções continuadas é **finita** sempre que temos um número racional.

Além disso, pode definir-se fracção continuada para qualquer número real, e esta propriedade de finitude caracteriza os números racionais, de entre todos os números reais.

Teorema 2.12. *Qualquer número racional é representado por uma fracção contínua finita.*

Demonstração. A demonstração baseia-se no facto de que o algoritmo de Euclides termina num número finito de passos, e que é precisamente este algoritmo que está na base do desenvolvimento em fracções continuadas. □

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 certo dia, que não interessa precisar qual.

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 $b = a + km$ 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 $a + b - 7 = 23(k + l)$.

Exercício 3.3. Mostre que $a \equiv 0 \bmod m$ se e só se a é múltiplo de m.

Proposição 3.4. *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 3.5. 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.

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

Proposição 3.6. *Seja $m \in \mathbb{N}$ um natural, e a, b, c números inteiros. Temos:*

(1) (Reflexividade) $a \equiv a \bmod m$
(2) (Simetria) *Se* $a \equiv b \bmod m$, *então* $b \equiv a \bmod m$
(3) (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 3.7. 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 3.8. 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 3.9. 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 $\mathbb{Z}_m$.** 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 destas classes:

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

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

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

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. Vamos usar a notação $A \sqcup B$ para denotar a união $A \cup B$ quando é disjunta, ou seja, quando $A \cap B = \varnothing$. Mais geralmente, $A_1 \sqcup A_2 \sqcup \cdots \sqcup A_n$ denota a união $A_1 \cup \cdots \cup A_n$, dos n conjuntos A_i, $i = 1, \cdots, n$, onde qualquer intersecção de dois destes conjuntos distintos é vazia: $A_i \cap A_j = \varnothing$ sempre que $i \neq j \in \{1, \cdots, n\}$.

Proposição 3.10. *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 3.11. 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 3.12. 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:

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

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 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 3.10). Como trabalhar com inteiros é bastante conveniente, vamos continuar neste contexto, por ora. Podemos verificar o seguinte.

Proposição 3.13. *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 $n \mid m$ e $a \equiv b \bmod m$ então $a \equiv b \bmod n$.
(4) 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) Se $m \mid (a - b)$ e $n \mid m$, então $n \mid (a - b)$. (4) 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.

Por exemplo, mostrar que o quadrado de um número ímpar é ímpar torna-se quase trivial: Seja $a \in \mathbb{Z}$ um número ímpar: $a \equiv 1 \bmod 2$. Então $a \cdot a \equiv 1 \cdot 1 \equiv 1 \bmod 2$ pelo que a^2 também é ímpar!

Exercício 3.14. 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 3.15. *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 3.13(2). 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 3.16. Mostre que, se n é quadrado, $n \equiv r \bmod 7$ onde $r \in \{0, 1, 2, 4\}$.

Observação 3.17. Por aplicação da regra do produto na Proposição 3.13(2) vemos que $a \equiv b \bmod m$ implica $a^k \equiv b^k, \bmod m$, para qualquer expoente positivo $k \in \mathbb{N}$. No entanto, a regra análoga para potências não é válida. 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 3.18. 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 3.19. *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 fórmula 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 3.20. *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 3.21. *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 equação $ac \equiv ad \bmod m$, para certos $c, d \in \mathbb{Z}$ é equivalente à equação $c \equiv d \bmod m$.

Demonstração. (1) Se $(m,a) = (m,b) = 1$ então $(m,ab) = 1$, pelo Corolário 1.32. 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. □

Este teorema 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.*

3.5. **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 3.22. 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 3.13(4)) 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 3.23. *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 $d \mid b$, a equação pode ser resolvida por $x_0 \equiv (a')^{-1}b' \bmod m'$ onde

$$a' = \frac{a}{d}, \quad b' = \frac{b}{d}, \quad m' = \frac{m}{d}.$$

Se uma solução é $x_0 \equiv (a')^{-1}b'$, a solução geral é $x = x_0 + km' \bmod m$ com $k \in \{0, 1, \cdots, d-1\}$.

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 3.19. 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 $ax \equiv b \bmod m$. □

3.6. **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 substituimos 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 $(\bmod 5)$, 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 $m_1m_2m_3 = 60$. A mesma solução é $x = -2$ uma vez que $58 \equiv -2 \bmod 60$.

Teorema 3.24. *[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 recusrsivamente, substituindo sucessivamente a solução geral de uma equação na seguinte equação. Explicitamente, a solução é dada por

$$x_0 \equiv b_1\frac{M}{m_1}y_1 + \cdots + b_r\frac{M}{m_r}y_r, \bmod M \tag{3.2}$$

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 (3.2). 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, $\bmod M$, para o leitor. □

4. Números Cardinais Finitos

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

No capítulo seguinte, vamos estudar equações que envolvem expoentes da incógnita. Estas são muito úteis nalgumas aplicações em computadores, como a criptografia de "chave pública".

As aplicações da aritmética modular usam de forma essencial o facto de estarmos a trabalhar com conjuntos finitos, neste caso os conjuntos $\mathbb{Z}_m$, para certo $m \in \mathbb{N}$. Assim, começamos por recordar alguns conceitos, e desenvolver outros, acerca de conjuntos finitos e funções entre eles.

4.1. **Funções e conjuntos finitos.** Sejam X e Y dois conjuntos. É bem sabido que uma função f entre X e Y é uma regra que associa a cada elemento $x \in X$ um elemento 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 4.1. 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 4.2. Sejam $A \subset X$ e $B \subset Y$ subconjuntos e $f : X \to Y$ uma função. A imagem directa 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:

$$f^{-1}(B) := \{x \in X : f(x) \in B\} \subset X.$$

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 4.3. 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 acima quanto à injectividade, sobrejectividade, e bijectividade.

Quando consideramos um subconjunto de Y com um único elemento $\{y\} \subset Y$ escrevemos $f^{-1}(y)$ em lugar 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 $f^{-1}(B) \subset X$.

Definição 4.4. 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 4.5. Seja $f(n) := \log n$, $f : \mathbb{N} \to \mathbb{R}$ e $g(x) := x^2 + 1$, $g : \mathbb{R} \to \mathbb{R}$. Então $g \circ f(n) = (\log n)^2 + 1$.

Proposição 4.6. *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 $f^{-1} : Y \to X$.
(4) A composição de duas funções injectivas (resp. sobrejectivas, bijectivas) é injectiva (resp. sobrejectiva, bijectiva).

Demonstração. Deixamos estas demonstrações como exercício. □

Notação: Por simplicidade, usamos as seguintes notações:

$$\begin{aligned} [n] &:= \{1, 2, \cdots, n\} \\ [n]_0 &:= \{0, 1, 2, \cdots, n\}. \end{aligned}$$

Corolário 4.7. *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. Pode mostrar-se por indução finita. Supomos primeiro $n < m$ e $f : [n] \to [m]$ sobrejectiva. Seja $f(n) = y \in [m]$. Então $f : [n-1] \to [m] \setminus \{y\}$. Definindo $g : [m] \setminus \{y\} \to [m-1]$ como a função que envia x em x, caso $x < y$ e x em $x - 1$, caso $x > y$ obtemos $f_1 := g \circ f : [n-1] \to [m-1]$ sobrejectiva. Continuando desta forma, ao fim de um número finito de passos, temos $f_n : \varnothing \to [m-n]$ sobrejectiva, o que é um absurdo. A prova que $f : [n] \to [m]$ não pode ser injectiva quando $n > m$ é semelhante. □

4.2. **Cardinalidade e conjuntos finitos.**

Definição 4.8. 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 cardinalidade 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 cardinalidade zero.

Proposição 4.9. *O conjunto dos números modulares $\mathbb{Z}_m$ tem cardinalidade m.*

Demonstração. De facto, temos uma bijecção $f : [m-1]_0 \to \mathbb{Z}_m$, definida por $x \mapsto [x]_m$. A demonstração que isto é uma bijecção é deixada ao leitor. □

O Corolário 4.7 pode ser escrito de outra forma.

Corolário 4.10. *Dois conjuntos finitos, A e B tem a mesma cardinalidade se e só se existe uma bijecção entre eles. Seja $f : A \to B$ uma função. Então, f não pode ser sobrejectiva quando $|A| < |B|$, e f não pode ser injectiva quando $|A| > |B|$.*

5. Fermat, Euler e Criptografia

Neste capítulo, vamos estudar as equações que envolvem expoentes da incógnita. São, desta forma, equações com potências da variável x, e que são muito úteis nalgumas aplicações em computadores, como a criptografia de "chave pública". A este tipo de equações chama-se o *problema do logaritmo discreto.*

5.1. **Teorema 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 5.1. *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 os números modulares. Caso considerássemos os números inteiros, por exemplo, a conclusão seria muito diferente.

Exercício 5.2. 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 $a = 0$.

Teorema 5.3. *(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:

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

Acima, usámos a comutatividade do produto, e a Proposição 5.1 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. □

Exercício 5.4. 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 $a^{-1} \equiv a^{p-2} \bmod p$.

Exemplo 5.5. ...

5.2. **Testes de Primalidade.** Dado um natural muito grande, $n \in \mathbb{N}$, como podemos saber se é primo? Determinar se todos os números $m < n$ são divisores parece ser tarefa ingrata.

Naturalmente, determinar se um número é composto é mais fácil. Por exemplo, temos testes de congruência bem conhecidos.

Exemplo 5.6. 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.

Pelo teorema de Fermat, 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 $a \in [560]$.

O teste de Miller-Rabin evita esta situação nalguns casos.

Como as únicas raízes de 1, módulo um número primo são ± 1, se n é primo, então $a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$, para qualquer base $a \in [n-1]$. Iterando este procedimento chegamos à seguinte conclusão.

Seja $n \in \mathbb{N}$ um número primo ímpar, e seja $n - 1 = 2^k q$ a factorização de $n-1$, sendo q o produto de primos ímpares (logo, q é ímpar). Seja $a \in [n-1]$ e consideremos a sucessão:

$$a^{n-1} = a^{2^k q},\ a^{2^{k-1} q},\ a^{2^{k-2} q},\ \cdots,\ a^{2q},\ a^q. \tag{5.1}$$

Se $a^{2^k q}$ não é congruente com 1, módulo n, então n é composto (isto é o teste de Fermat para a base a). Caso $a^{2^k q} \equiv 1 \bmod n$, então determinamos $a^{2^{k-1} q} \bmod n$. Se não é ± 1, então n é composto, etc. Temos então:

Teste de Miller-Rabin Seja dado $n \in \mathbb{N}$, e $a \in [n-1]$, com $n - 1 = 2^k q$ e q ímpar. Caso aconteça (pelo menos) uma das seguintes condições, então n é composto:
(1) O primeiro termo da sucessão (5.1) não é $\equiv 1 \bmod n$,
(2) Algum $a^{2^j q}$ não é congruente com $\pm 1 \bmod n$, para certo $j \in \{0, \cdots, k-1\}$.

Uma vez mais, existem vários n e várias bases a que fazem com que este teste seja inconclusivo. Ou seja, se ocorrem as condições (1) ou (2) ficamos a saber que n é composto, mas teriamos que verificar todas as bases para poder concluir que n é primo.

5.3. **Invertibilidade em $\mathbb{Z}_m$ e a função de Euler.** Tal como para os módulos primos, para qualquer módulo $m \in \mathbb{N}$, podemos considerar o conjunto dos números modulares que têm inverso $\bmod m$:

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

A função de Euler fornece, para cada m, o número de inteiros, de 1 a m, que são invertíveis módulo m.

Definição 5.7. A função de Euler é a função $\varphi : \mathbb{N} \to \mathbb{N}$ definida por:

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

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

Proposição 5.8. *Para qualquer $m \in \mathbb{N}$ temos:*

$$\varphi(m) = \left|\mathbb{Z}_m^\times\right|.$$

Demonstração. De facto, o conjunto dos números inteiros, de 0 a $m-1$ que são primos com m (os invertíveis módulo m, de acordo com a Proposição 3.19) tem a mesma cardinalidade que o conjunto dos números inteiros, de 1 a m que são primos com m. □

Exemplo 5.9. 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 não são primos com 45: $\{2, 4, 8, 14, 16, 22, 26, 28, 32, 34, 38, 44\}$. Este conjunto tem cardinalidade 12, pelo que $\varphi(45) = 12$.

Teorema 5.10. *Para qualquer natural n, temos a igualdade:*

$$\sum_{0<d|n} \varphi(d) = n.$$

Demonstração. Para cada $d \mid n$, seja S_d o conjunto $S_d = \{1 \leq c \leq d \,:\, (c,d) = 1\}$, e seja

$$S = \bigcup_{0<d|n} S_d = \{(c,d) \in \mathbb{N}^2 \,:\, (c,d) = 1,\ 1 \leq c \leq d\}.$$

Então temos $\sum_{0<d|n} \varphi(d) = \sum_{0<d|n} |S_d| = |S|$, pois todos os conjuntos S_d são disjuntos, dois a dois. Vamos agora contar os elementos de S doutra forma. Defina-se a função:

$$\begin{array}{rcl} f \,:\, S & \to & [n] \\ (c,d) & \mapsto & \dfrac{cn}{d}. \end{array}$$

Note-se que $f(c,d)$ é natural $\leq n$, para qualquer $(c,d) \in S$, pois $d \mid n$ e $\frac{c}{d} \leq 1$. Vamos provar que f bijectiva. Para a injectividade, seja $f(c,d) = f(c',d')$. Então $\frac{cn}{d} = \frac{c'n}{d'}$ logo $\frac{c}{d} = \frac{c'}{d'}$. Isto implica, como são fracções irredutíveis, que $c = c'$ e $d = d'$. Para verificar a sobrejectividade, seja $x \in [n]$, $d_x = n/(x,n)$, e $c_x = x/(x,n)$. Assim, c_x e d_x são primos entre si. Alem disso, $f(c_x, d_x) = \frac{c_x n}{d_x} = \frac{xn}{d}$ como queriamos provar. □

Exemplo 5.11. Consideremos $n = 28 = 2^2 \cdot 7$. Podemos calcular. $\varphi(1) = \varphi(2) = 1$, $\varphi(4) = 2$, $\varphi(7) = 6$, $\varphi(14) = 6$ e $\varphi(28) = 12$. E, de facto, $28 = 1 + 1 + 2 + 6 + 6 + 12$.

A fórmula do Teorema 5.10, permite uma recorrência para determinar o valor de $\varphi(n)$. De facto, podemos escrever:

$$n = \varphi(n) + \sum_{0<d|n,\, d\neq n} \varphi(d), \tag{5.2}$$

onde o somatório inclui todos os divisores $d \mid n$, positivos, excepto o próprio n.

Existe uma forma expedita de calcular $\varphi(n)$ quando se sabe a factorização de n em primos. De facto, φ é uma função multiplicativa, no sentido em que, para quaisquer $n, m \in \mathbb{N}$ primos entre si, temos $\varphi(nm) = \varphi(n)\varphi(m)$, como veremos. Resta, por isso, saber o valor de φ para as potências de primos.

Lema 5.12. *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. Vamos usar a fórmula (5.2) e indução em $k \in \mathbb{N}$. Os únicos divisores de p são $\{1, p\}$. Assim, para $k = 1$ (base da indução), esta fórmula dá:

$$p = \varphi(p) + \varphi(1), \qquad \Leftrightarrow \qquad \varphi(p) = p - 1.$$

Vamos agora assumir que $\varphi(p^j) = p^j - p^{j-1}$ é válida para $j = 1, \cdots, k$ (indução forte). Os divisores de p^{k+1} são $\mathsf{Div}(p) = \{1, p, \cdots, p^{k+1}\}$. Assim, a mesma fórmula diz-nos:

$$\begin{aligned}\varphi(p^{k+1}) = p^{k+1} - \sum_{0<d|p^{k+1},\, d\neq p^{k+1}} \varphi(d) &= p^{k+1} - \textstyle\sum_{j=0}^{k}\varphi(p^j) = \\ &= p^{k+1} - 1 - \textstyle\sum_{j=1}^{k}\varphi(p^j) = \\ &= p^{k+1} - 1 - \textstyle\sum_{j=1}^{k}\left(p^j - p^{j-1}\right) = \\ &= p^{k+1} - 1 - (p^k - 1) = p^{k+1} - p^k,\end{aligned}$$

como pretendido. O passo de indução foi aplicado entre a segunda e a terceira linha. □

Proposição 5.13. *Sempre que $n, m \in \mathbb{N}$ verificam $(n, m) = 1$ temos $\varphi(nm) = \varphi(n)\varphi(m)$.*

Demonstração. Vamos usar novamente a fórmula (5.2). Quando n e m são primos entre si, qualquer divisor é o produto de um divisor de n por um divisor de m. Ou seja, qualquer $d \in \mathsf{Div}(nm)$ admite uma factorização única $d = d'd''$ onde $d' \in \mathsf{Div}(n)$ e $d'' \in \mathsf{Div}(m)$. Vamos admitir que a fórmula $\varphi(ab) = \varphi(a)\varphi(b)$ é válida para qualquer natural $ab < mn$, e vamos proceder por indução (sendo que a base $\varphi(1) = 1 = \varphi(1)\varphi(1)$ é imediata). Assim, temos:

$$\begin{aligned}nm = \left(\textstyle\sum_{d'|n}\varphi(d')\right)\left(\textstyle\sum_{d''|m}\varphi(d'')\right) &= \textstyle\sum_{d'|n,\, d''|m}\varphi(d')\varphi(d'') = \\ &= \varphi(n)\varphi(m) + \sum_{d'|n,\, d''|m,\, d'd''\neq nm}\varphi(d')\varphi(d'') = \\ &= \varphi(n)\varphi(m) + \sum_{d'|n,\, d''|m,\, d'd''\neq nm}\varphi(d'd'') = \\ &= \varphi(n)\varphi(m) + \sum_{d'd''|nm,\, d'd''\neq nm}\varphi(d'd'') = \\ &= \varphi(n)\varphi(m) + \textstyle\sum_{d|nm,\, d\neq nm}\varphi(d) = \\ &= \varphi(n)\varphi(m) + (nm - \varphi(nm)),\end{aligned}$$

Logo, $\varphi(nm) = \varphi(n)\varphi(m)$. Usou-se o passo de indução na segunda linha. □

Vamos agora generalizar o teorema de Fermat para módulos que não são primos.

Proposição 5.14. *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 $\mathbb{Z}_m$. Dito de outra forma, a aplicação*

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

é uma bijecção.

Demonstração. A demonstração é semelhante à da Proposição , mas podemos apresentar agora uma pequena variação. Para ver que m_a é bijectiva, consideramos $c \in \mathbb{Z}$ e temos que resolver a equação $m_a(x) = ax \equiv c \bmod m$. 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 5.15. *(Euler) Seja $a \in \mathbb{Z}$ e $m \in \mathbb{N}$. Se $(a, m) = 1$, então $a^{\varphi(m)} \equiv 1 \bmod m$.*

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

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

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

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

Usámos novamente a comutatividade do produto, o facto de que $\varphi(m)$ é a cardinalidade de $\mathbb{Z}_m^\times$ e a Proposição 5.14 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 $a^{\varphi(m)} \equiv 1 \mod p$, como queriamos provar. □

Exercício 5.16. Seja $(a, m) = 1$, e k um inteiro qualquer. Mostre que $a^{k\varphi(m)} \equiv 1 \mod m$.

Exemplo 5.17. Vamos determinar o $x \in [279]$ tal que $x \equiv 25^{544} \pmod{279}$. 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 $25^{180} \equiv 1 \pmod{279}$, 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:

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

Assim, $x = 25$ é a solução do problema. Concluimos então que $25^4 \equiv 25 \pmod{279}$ o que também nos diz que $25^3 \equiv 1 \pmod{279}$.

Observação 5.18. O teorema de Euler diz-nos que $a^{k\varphi(m)} \equiv 1 \mod m$ 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 $a^j \equiv 1 \mod m$. O menor expoente que o verifica é chamado a ordem de a módulo m.

Definição 5.19. 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 $a^j \equiv 1 \mod m$ chama-se a ordem de a módulo m e escreve-se $j = \mathrm{ord}_m(a)$.

Proposição 5.20. *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 $x^k \equiv 1 \mod m$.

Demonstração. Seja $j = \mathrm{ord}_m(a)$ e $k \in \mathbb{Z}$ tal que $x^k \equiv 1 \mod m$. Vamos dividir k por j: $k = q\,j + r$ 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 $a^j \equiv 1 \mod m$, 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, $a^{\varphi(m)} \equiv 1 \mod m$. □

Exemplo 5.21. No exemplo acima $25^3 \equiv 1 \pmod{279}$. Isto não contradiz a Proposição acima, uma vez que $3 \mid 180$ onde $180 = \varphi(279)$. É fácil de verificar que, precisamente $\mathrm{ord}_{279}(25) = 3$.

5.4. **Raízes primitivas e o problema do logaritmo discreto.** Vamos agora considerar algumas equações não lineares. Em particular, estudaremos as equações da forma

$$x^k \equiv b \mod m. \tag{5.3}$$

Se tanto a variável x, como $b > 0$, fossem números reais, teríamos $x = (b)^{\frac{1}{jk}}$ como solução, uma vez que $\left(b^{\frac{1}{k}}\right)^k = b^{k\cdot\frac{1}{k}} = b$.

Por analogia com o caso real, faz sentido procurar soluções da equação (5.3), na forma $x \equiv b^u \bmod m$, onde u é um inverso de k módulo $\varphi(m)$, uma vez que $b^{\varphi(m)} \equiv 1 \bmod m$, como advém do teorema de Euler.

Proposição 5.22. *Sejam m, $k \in \mathbb{N}$ e $b \in \mathbb{Z}$. Se $(b, m) = (k, \varphi(m)) = 1$ então a equação $x^k \equiv b \bmod m$ tem uma solução única $\bmod m$ e é dada por*

$$x \equiv b^u \bmod m,$$

onde $u \equiv k^{-1} \pmod{\varphi(m)}$.

Demonstração. Seja u um inverso de k módulo $\varphi(m)$. Assim, existe $v \in \mathbb{Z}$ tal que $1 = uk + v\varphi(m)$. O facto de que b^u é solução, verifica-se substituindo na equação:

$$((b)^u)^k \equiv b^{uk} \equiv b^{1-v\varphi(m)} \equiv b \cdot \left(b^{\varphi(m)}\right)^{-v} \equiv b \cdot 1^{-v} \equiv b \bmod m.$$

Note-se que usámos a hipótese de b ser invertível módulo m, $(b, m) = 1$. Supomos agora que há duas soluções $x^k \equiv y^k \equiv b$. Então $\left(xy^{-1}\right)^k \equiv 1$. Então $\mathrm{ord}_m(xy^{-1}) \mid k$ e também $\mathrm{ord}_m(xy^{-1}) \mid \varphi(m)$. Como $(k, \varphi(m)) = 1$ concluímos que $\mathrm{ord}_m(xy^{-1}) = 1$ ou seja $xy^{-1} \equiv 1 \bmod m$, o que significa que $x \equiv y \bmod m$, como queríamos provar. □

Exemplo 5.23. Vamos resolver a equação $x^{29} \equiv 2 \bmod 117$. Neste caso $b = 2$, $m = 117 = 13 \cdot 9$ que são primos entre si. Temos também $\varphi(117) = \varphi(9)\varphi(13) = 6 \cdot 12 = 72$, pelo que $k = 29$ é primo com $\varphi(117)$, e estamos nas condições da Proposição. A única solução é então $x \equiv 2^u$ onde $29u \equiv 1 \bmod 72$. Calculando o inverso de 29 obtemos: $u \equiv 5 \bmod 72$, e portanto a solução é $x \equiv 2^5 \equiv 32 \bmod 117$.

O teorema de Euler e a proposição acima, em conjunção com o teorema chinês dos restos, permitem simplificar bastante as equações a resolver.

Exemplo 5.24. Vamos resolver a equação $x^{199} \equiv 17 \bmod 91$. Temos $91 = 7 \cdot 13$, logo $\varphi(91) = 6 \cdot 12 = 72$ e $(199, 72) = 1$ pelo que esperamos uma solução única. Pelo teorema de Euler, como $x^{72} \equiv 1$, $x^{199} = x^{2\cdot 72}x^{55} \equiv x^{55}$ ficamos com $x^{55} \equiv 17 \bmod 91$. Pelo teorema chinês dos restos, temos

$$\begin{cases} x^{55} \equiv 17 \mod 7 \\ x^{55} \equiv 17 \mod 13 \end{cases} \Leftrightarrow \begin{cases} x \equiv 3 \mod 7 \\ x^7 \equiv 4 \mod 13, \end{cases}$$

uma vez que $\varphi(7) = 6$ e $55 = 9 \cdot 6 + 1$, $\varphi(13) = 12$ e $55 = 4 \cdot 12 + 7$. A segunda equação tem $k = 7$ $(7, 12) = 1$. Logo a solução é $x \equiv 4^y$ onde $y \equiv 7^{-1} \bmod 12$. Como $7 \cdot 7 \equiv 1 \bmod 12$ temos $7^{-1} \equiv 7 \bmod 12$ e logo $x \equiv 4^7 \bmod 13$ é a solução. $4^7 \equiv 3 \cdot 3 \cdot 3 \cdot 4 \equiv 9 \cdot (-1) \bmod 13$. Finalmente, reduzimos o problema a resolver o sistema $x \equiv 3 \bmod 7$ e $x \equiv -9 \bmod 13$.

A equação no caso em que $(k, \varphi(m)) > 1$ é mais difícil de resolver. Para estudá-la, vamos usar o conceito de raiz primitiva. Vimos atrás que a ordem de um inteiro a (invertível módulo m) divide $\varphi(m)$, não sendo superior a $\varphi(m)$, pois $a^{\varphi(m)} \equiv 1 \bmod m$.

Vamos, por exemplo para o módulo $m = 7$, usar uma tabela para determinar a ordem de cada $a \in \{1, 2, \cdots, 6\}$. Abaixo, listamos as potências a^k, para k entre 1 e $\varphi(7) = 6$, e

verificamos que elas se repetem.

$a \setminus k$	1	2	3	4	5	6
1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	3	2	6	4	5	1
4	4	2	1	4	2	1
5	5	4	6	2	3	1
6	6	1	6	1	6	1

Olhando para a tabela, vemos que, por exemplo, o conjunto das potências de 2 é $\{1, 2, 4\}$, mas que as potências de 3 são todos os elementos de $\mathbb{Z}_7^\times$:

$$\begin{aligned} \{2^k \pmod 7 \,:\, k \in \mathbb{N}\} &= \{1, 2, 4\} \subset \mathbb{Z}_7^\times, \\ \{3^k \pmod 7 \,:\, k \in \mathbb{N}\} &= \mathbb{Z}_7^\times. \end{aligned}$$

Os números 3 e 5 são especiais. As suas potências permitem obter todas as classes módulo 7. Dito de outra forma, dada qualquer classe de congruência invertível módulo 7, $b \in \mathbb{Z}_7^\times$, existe $k \in \mathbb{N}$ tal que $3^k \equiv b \bmod 7$. Assim, a classe $3 \in \mathbb{Z}_7^\times$ é uma raiz, (embora para diferentes k), de qualquer $b \in \mathbb{Z}_7^\times$. Estes números modulares chamam-se raízes primitivas módulo 7. Para qualquer módulo temos um conceito análogo.

Definição 5.25. Uma raiz primitiva módulo m é uma classe a, cujo conjunto de potências coincide precisamente com $\mathbb{Z}_m^\times$. Isto é:

$$\left\{a^k : k \in \mathbb{Z}\right\} = \mathbb{Z}_m^\times.$$

Assim, o conjunto de potências de uma raiz primitiva módulo m tem cardinalidade igual a $\varphi(m)$.

Proposição 5.26. *Seja $m \in \mathbb{N}$. Então $a \in \mathbb{Z}_m^\times$ é uma raiz primitiva módulo m se e só se*

$$ord_m(a) = \varphi(m) = \left|\mathbb{Z}_m^\times\right|.$$

Demonstração. Seja $j := \mathrm{ord}_m(a)$. O conjunto das potências de a verifica:

$$\{a^k : k \in \mathbb{Z}\} = \{a^1, a^2, \cdots, a^j\},$$

pois $a^j \equiv 1 \equiv a^0 \bmod m$. Se $j = \varphi(m)$ então, uma vez que $j = |\mathbb{Z}_m^\times|$, a única forma do conjunto da direita não ser $\mathbb{Z}_m^\times$ é que dois (ou mais, claro) dos seus elementos coincidam. Assim, vamos supor, por contradição, que $a^k \equiv a^l$ para certos $k, l \in \{1, \cdots, j\}$ distintos. Podemos supor que $k > l$. Assim $a^{k-l} \equiv 1 \bmod m$. Mas como $k - l < j$ isto contradiz a hipótese $j = \mathrm{ord}_m(a)$. Logo, $\{a^k : k \in \mathbb{Z}\} = \mathbb{Z}_m^\times$ e a é uma raiz primitiva. Reciprocamente, se $j < \varphi(m)$ então $a^j \equiv 1 \bmod m$ pelo que

$$\{a^k : k \in \mathbb{Z}\} \subset \{a^1, a^2, \cdots, a^j\}.$$

Como o conjunto da direita tem cardinalidade $j < \varphi(m) = |\mathbb{Z}_m^\times|$ o conjunto de potências não coincide com $\mathbb{Z}_m^\times$ e a não é uma raiz primitiva. □

A noção de raiz primitiva permite resolver equações com potências da seguinte forma.

Exemplo 5.27. Vamos resolver a equação $x^3 \equiv -1 \bmod 14$, sabendo que 3 é uma raíz primitiva $\bmod 14$ e que além disso $3^3 \equiv -1 \bmod 14$. Assim, uma solução é precisamente $x \equiv 3 \bmod 14$. Mas esta não é a única solução. Se fizermos $x \equiv 3^y \bmod 14$ e substituimos na equação $(3^y)^3 \equiv 3^3 \bmod 14$. Como $\varphi(14) = 6$, isto dá-nos, para os expoentes:

$$3y \equiv 3 \bmod 6.$$

As soluções são $y \equiv 1$ ou 3 ou 5, pelo que, finalmente $x \equiv 3$ ou $3^3 \equiv -1$ ou $3^5 \equiv 5 \bmod 14$.

Quando não sabemos raizes primitivas é mais complicado saber condições que garantam a existência de soluções.

Proposição 5.28. *Para todos os módulos primos, existem raizes primitivas.*

Assim, vamos agora considerar apenas o caso de módulos primos. Pretendemos saber se $x^k \equiv b \bmod p$ tem solução. Se β é uma raiz primitiva módulo p, então podemos escrever:

$$x \equiv \beta^y \bmod p, \qquad b \equiv \beta^j \bmod p,$$

e temos então

$$\beta^{ky} \equiv \beta^j \bmod p.$$

Resta-nos resolver a equação $ky \equiv j \bmod p-1$, em que a incógnita é y ($\bmod \varphi(p) = p-1$). Seja $d = \mathrm{mdc}(k, p-1)$. Sabemos então que:
(1) Uma solução existe, se $d \mid j$
(2) Nesse caso, existem d soluções distintas, módulo $p-1$.

No caso de $\frac{j}{d}$ ser inteiro temos $b^{\frac{(p-1)}{d}} \equiv \left(\beta^{p-1}\right)^{\frac{j}{d}} \equiv 1 \bmod p$. Reciprocamente, se $b^{\frac{(p-1)}{d}} \equiv \beta^{\frac{j}{d}(p-1)} \equiv 1 \bmod p$ então, como $\mathrm{ord}_p\beta = p-1$, temos que $p-1 \mid \frac{j}{d}(p-1)$, ou seja $d \mid j$ e temos soluções.

Proposição 5.29. *[Critério de Euler] Seja p primo, e $b \in \mathbb{Z}$ invertível módulo p. Seja $k \in \mathbb{N}$ e $d = (k, p-1)$. Então, relativamente à equação $x^k \equiv b \bmod p$ existem d soluções se*

$$b^{\frac{p-1}{d}} \equiv 1 \bmod p$$

e não tem soluções no caso contrário.

O nome critério de Euler é normalmente usado no caso quadrático ($k = 2$). Este critério é também válido para módulos compostos, desde que exista uma raiz primitiva. Note-se que o critério apenas garante existência (ou não) de solução, mas não permite a resolução da equação, a menos que se saiba uma raiz primitiva β e como escrever o termo independente b como potência de β.

Parte 2. FUNÇÕES e COMBINATÓRIA

Nesta segunda parte, estudamos alguns conceitos de combinatória enumerativa. Também se introduzem funções racionais e séries, que serão usadas para obter fórmulas para problemas enumerativos definidos por relações de recorrência. Finalmente, apresentam-se também 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.

6. Conjuntos e Contagens

6.1. **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 que x pertence a X. O conjunto vazio, denotado por $\varnothing$, é o conjunto sem elementos.

Dados dois conjuntos A, B podemos fazer 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: $A \Cap B := (A \setminus B) \cup (B \setminus A)$
- Produto: $A \times B := \{(a, b) | a \in A, b \in B\}$

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 de conjuntos $\{X_i\}_{i=1}^k$ denota-se, respectivamente, por:

$$\begin{aligned} X_1 \cup \cdots \cup X_k &= \bigcup_{i=1}^{k} X_i \\ X_1 \cap \cdots \cap X_k &= \bigcap_{i=1}^{k} X_i. \end{aligned}$$

Uma outra notação de grande utilidade é a de união disjunta. Definimos:

$$A \sqcup B := A \cup B, \qquad \text{sempre que } A \cap B = \varnothing.$$

Temos as seguintes propriedades das operações:

...

Dados dois conjuntos A, B escrevemos $A \subset B$, que significa A contido em B (permite-se a igualdade dos dois conjuntos), se qualquer elemento de A pertence também a B.

6.2. **Funções.** Sejam X e Y dois conjuntos. Como visto na secção..., uma função f entre X e Y é uma regra que associa a cada elemento $x \in X$ um elemento 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 6.1. 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 6.2. Sejam $A \subset X$ e $B \subset Y$ subconjuntos e $f : X \to Y$ uma função. A imagem directa 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:

$$f^{-1}(B) := \{x \in X : f(x) \in B\} \subset X.$$

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 6.3. 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 acima quanto à injectividade, sobrejectividade, e bijectividade.

Quando consideramos um subconjunto de Y com um único elemento $\{y\} \subset Y$ escrevemos $f^{-1}(y)$ em lugar 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 6.4. *Sejam $A, B \subset X$, $C, D \subset Y$ e $f : X \to Y$ uma função. As imagens directas e inversas verificam:*

$$\begin{aligned}
f^{-1}(C \cap D) &= f^{-1}(C) \cap f^{-1}(D) \\
f^{-1}(C \cup D) &= f^{-1}(C) \cup f^{-1}(D) \\
f^{-1}(C \setminus D) &= f^{-1}(C) \setminus f^{-1}(D), \\
f(A \cup B) &= f(A) \cup f(B) \\
f(A \cap B) &\subset f(A) \cap f(B) \\
A &\subset f^{-1}(f(A)) \\
f(f^{-1}(D)) &\subset D.
\end{aligned}$$

Definição 6.5. 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 6.6. Seja $f(n) := \log n$, $f : \mathbb{N} \to \mathbb{R}$ e $g(x) := x^2 + 1$, $g : \mathbb{R} \to \mathbb{R}$. Então $g \circ f(n) = (\log n)^2 + 1$.

6.3. **Funções Injectivas, Sobrejectivas, e Bijectivas.** asd

Proposição 6.7. *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 $f^{-1} : Y \to X$.
(4) A composição de duas funções injectivas (resp. sobrejectivas, bijectivas) é injectiva (resp. sobrejectiva, bijectiva).

Demonstração. ... □

Notação: Por simplicidade, usamos as seguintes notações:

$$\begin{aligned}[n] &:= \{1, 2, \cdots, n\} \\ [n]_0 &:= \{0, 1, 2, \cdots, n\}.\end{aligned}$$

Corolário 6.8. *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. Pode mostrar-se por indução finita. Supomos primeiro $n < m$ e $f : [n] \to [m]$ sobrejectiva. Seja $f(n) = y \in [m]$. Então $f : [n-1] \to [m] \setminus \{y\}$. Definindo $g : [m] \setminus \{y\} \to [m-1]$ como a função que envia x em x, caso $x < y$ e x em $x-1$, caso $x > y$ obtemos $f_1 := g \circ f : [n-1] \to [m-1]$ sobrejectiva. Continuando desta forma, ao fim de um número finito de passos, temos $f_n : \varnothing \to [m-n]$ sobrejectiva, o que é um absurdo. A prova que $f : [n] \to [m]$ não pode ser injectiva quando $n > m$ é semelhante. □

6.4. **Cardinalidade.**

Definição 6.9. 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 cardinalidade 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 cardinalidade zero.

Proposição 6.10. *O conjunto dos números modulares $\mathbb{Z}_m$ tem cardinalidade m.*

Demonstração. De facto, temos uma bijecção $f : [m-1]_0 \to \mathbb{Z}_m$, definida por $x \mapsto [x]_m$. A demonstração que isto é uma bijecção é deixada ao leitor. □

O Corolário 6.8 pode ser escrito de outra forma.

Corolário 6.11. *Dois conjuntos finitos, A e B tem a mesma cardinalidade 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 $|A| > |B|$.*

Recordemos as seguintes notações. Para $n \in \mathbb{N}$ definimos os conjuntos:

$$\begin{aligned}[n] &:= \{1, 2, \cdots, n\} \\ [n]_0 &:= \{0, 1, 2, \cdots, n\}.\end{aligned}$$

Se A designa um conjunto finito, a expressão $|A| = n$ significa que A tem cardinalidade $n \in \mathbb{N}$, ou de forma equivalente, que existe uma bijecção (uma função bijectiva) $f : A \to [n]$. A cardinalidade está unicamente definida para cada conjunto finito, uma vez que não é possível haver bijecções entre $[n]$ e $[m]$ para $n, m \in \mathbb{N}$ distintos (ver corolário...).

Por exemplo, temos $|[n]| = n$ e $|[n]_0| = n + 1$. Nota-se também que o conjunto vazio $\varnothing$ é o único conjunto com cardinalidade zero.

6.5. **Números binomiais.**

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 $\binom{5}{3} = \frac{5 \cdot 4}{2} = 10$. Estes números binomiais aparecem tanto no triângulo de Pascal, como na fórmula do binómio de Newton.

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 enumerar as linhas horizontais do triângulo de Pascal, começando de cima para baixo com a linha zero e, em cada linha enumeramos 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:

$$C_k^{n+1} = C_{k-1}^n + C_k^n, \tag{6.1}$$

quando $n \geq k \geq 0$.

Tal como sucede muitas vezes na matemática, existe uma fórmula fechada para todos os coeficientes deste triângulo! De facto, não deixa de ser surpreendente a frequência com que aparecem relações simples entre conceitos ou números que, à partida, não teriam nada a ver uns com outros.

Definição 6.12. Os números binomiais são os números $\binom{n}{m}$ onde $0 \leq m \leq n$ com $n, m \in \mathbb{N}_0$ definidos por

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

Na fórmula acima, convenciona-se que $0! = 1$, e que, por isso, $\binom{n}{0} = 1$ para todo o $n \in \mathbb{N}_0$. Também se convenciona que $\binom{n}{m} = 0$ nos casos indesejados em que m não está entre 0 e n, ou seja, quando $m < 0$ e também quando $m > n$.

Observação 6.13. $\binom{n}{m}$ é o número de m-subconjuntos de um n-conjunto. $n!$ é o número de permutações de um n-conjunto, ou seja de bijecções $f : [n] \to [n]$.

Proposição 6.14. *Enumeremos Então, a n-ésima linha do triângulo é constituida pelos números:*

$$1 = \binom{n}{0},\ n = \binom{n}{1},\ \frac{n(n-1)}{2} = \binom{n}{2},\ \cdots,\ \binom{n}{n-1} = n,\ \binom{n}{n} = 1.$$

Demonstração. Dado que cada entrada do triângulo de Pascal é obtida por recorrência usando a fórmula (6.1) e tudo começa com $1 = \binom{0}{0} = \frac{0!}{0!0!}$, basta mostrar que os números binomiais verificam a mesma propriedade que os números do triângulo, ou seja:

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

sempre que $n \geq k \geq 0$. Esta fórmula verifica-se directamente:

$$\begin{aligned}
\binom{n}{k-1} + \binom{n}{k} &= \frac{n!}{(k-1)!\,(n+1-k)!} = \\
&= \frac{n!}{k!(n-k)!}\,\frac{n!\,[k!(n-k)! + (k-1)!\,(n+1-k)!]}{(k-1)!\,(n+1-k)!\,k!\,(n-k)!} = \\
&= \frac{n!\,[k(k-1)!(n-k)! + (n+1-k)(k-1)!(n-k)!]}{(k-1)!\,(n+1-k)!\,k!\,(n-k)!} \\
&= \frac{n!(k-1)!(n-k)!\,[k+(n+1-k)]}{(k-1)!\,(n+1-k)!\,k!\,(n-k)!} \\
&= \frac{(n+1)n!}{(n+1-k)!\,k!} = \frac{(n+1)!}{(n+1-k)!\,k!} = \binom{n+1}{k},
\end{aligned}$$

como queriamos provar. Note-se a fórmula mantém-se válida com $k = 0$ pois $\binom{n}{-1} = 0$. □

Como já mencionámos, os mesmos números aparecem na fórmula do binómio de Newton, que é a seguinte.

Proposição 6.15. *Considere-se duas variáveis x, y (podem considerar-se inteiros), e seja $n \in \mathbb{N}_0$. Então o polinómio $(x+y)^n$ é um polinómio homogéneo cujos coeficientes são números binomiais. Mais precisamente*

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

Demonstração. Indução em $n \in \mathbb{N}$. O caso $n = 1$ é simples.

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

Note-se que na terceira para a quarta linha há dois termos que foram incluídos, mas que são nulos e por isso não afectam o somatório. São os termos $\binom{n}{-1} = 0$, no primeiro somatório, e $\binom{n}{n+1} = 0$, no segundo somatório. □

Exercício 6.16. Mostre que $\sum_{j=0}^{n}\binom{n}{j} = 2^n$ e que $\sum_{j=0}^{k}(-1)^j\binom{k}{j} = 0$.

Podemos generalizar estes números.

6.6. **Números multinomiais.**

Definição 6.17. 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:

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

Exemplo 6.18. Calcular o coeficiente de $x^5 y^3 z^2$ em $(x+y+z)^{10}$.

Outro exemplo

Exemplo 6.19. O número de maneiras de formar 8 grupos de 4 elementos com 32 alunos e com 8 projectos diferentes é... Se não houver distinção entre projectos é ... Se a turma tiver 30 alunos, e quisermos formar 6 grupos de 4 elementos e 2 de 3, cada qual com tarefas diferentes são...

Vamos agora rever algumas propriedades e operações com conjuntos finitos.

6.7. **Princípios gerais de contagem. Princípio da identidade:** Podemos determinar o número de elementos de um conjunto, encontrando uma bijecção com outro conjunto cuja cardinalidade conhecemos. Sucintamente, $|A| = |B|$ sempre que existe uma bijecção $f : A \to B$.

Exemplo 6.20. Seja X um conjunto finito. O conjunto potência de X:$\mathcal{P}(X) := \{Y \subset X\}$ é o conjunto de todos os subconjuntos de X (incluindo o vazio $\varnothing$ e o próprio X), e é também um conjunto finito. Para determinar a sua cardinalidade consideremos a função:

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

onde $f : X \to \{0,1\}$ é uma dada função e $f^{-1}(1)$, a pré-imagem de 1 é naturalmente um subconjunto de X. É fácil ver que $\mathcal{F}$ é uma bijecção. De facto, a aplicação inversa associa a um dado subconjunto $Y \subset X$ a função $\chi_Y : X \to \{0,1\}$ definida por:

$$\chi_Y(x) := \begin{cases} 1, & x \in Y \\ 0, & x \in X \setminus Y. \end{cases}$$

Dada a sua importância em vários contextos, esta função χ_Y é chamada a função característica do subconjunto $Y \subset X$. Veremos a sua aplicação à demonstração de um outro princípio de contagem muito importante: o chamado princípio de inclusão-exclusão.

Princípio da adição: O número de elementos de uma união disjunta é a soma das cardinalidades de cada um deles. Sucintamente:

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

Exemplo 6.21. Cardinalidades de $A \setminus B$ e de $A \cup B$.

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 de outros conjuntos $X_1, \cdots, X_n$, então a sua cardinalidade é o produto das cardinalidades 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 6.22. As funções de X em Y.

Outra forma de enunciar este princípio é a seguinte:

Proposição 6.23. *O número de escolhas ordenadas de 1 elemento de X_1, 1 elemento de X_2 etc, é o produto das cardinalidades: $|X_1|\cdots|X_n|$. 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 6.24. Os divisores de n.

No mesmo círculo de ideias temos o seguinte:

Proposição 6.25. *[Princípio da dupla contagem] Se contarmos o número de elementos de um dado conjunto de duas formas distintas, obtemos o mesmo número.*

Exemplo 6.26. Vamos mostrar que

$$2^n = \sum_{k=0}^{n} \binom{n}{k}$$

Outro exemplo: mostrar que

$$\binom{n+m}{k} = \sum_{j=0}^{k} \binom{n}{j}\binom{m}{k-j}$$

Para isto, usamos um conjunto $X \cup Y$, com $|X| = n$ e $|Y| = m$ e subconjuntos $A \subset X$ com j elementos e $B \subset Y$ com $k-j$ elementos, de forma a que $|A \cup B| = k$.

Princípio do Pombal (caixas de correio): Se m objectos são distribuidos por n caixas, e $m > n$ então pelo menos uma das caixas ficará com mais de um objecto.

Outra forma de dizer que não há funções injectivas $f : [m] \to [n]$ com $m > n$.

Exemplo 6.27. Dados 5 pontos distintos (x_i, y_i), $i = 1, \cdots, 5$, em $\mathbb{Z}^2 \subset \mathbb{R}^2$, existe pelo menos 1 par de pontos para o qual o ponto médio do segmento de recta que os une tem também coordenadas inteiras. Dados 4 pontos, mostrar que o mesmo não é verdade.

Para isso vamos reduzir as coordenadas módulo 2. $(x_i, y_i) \equiv (0,0)$, $(0,1)$, $(1,0)$ ou $(1,1)$ $\mathsf{mod}\,2$. Assim, existe um par $i \neq j$ com $x_i \equiv x_j$ e $y_i \equiv y_j$ $\mathsf{mod}\,2$. Para estes 2 pontos, o ponto médio

$$(\frac{x_i + x_j}{2}, \frac{y_i + y_j}{2})$$

tem coordenadas inteiras.

6.8. **O princípio de Inclusão-Exclusão.** O princípio de Inclusão-Exclusão generaliza a fórmula para a cardinalidade da união. Sendo $Y \subset X$, denotamos por Y^c o complementar de Y em X, isto é:

$$Y^c := X \setminus Y.$$

Recordemos que $\chi_Y : X \to \{0,1\}$ designa a função característica de $Y \subset X$: a função que vale 1 em Y e zero fora de Y. Observemos que esta função verifica o seguinte:

$$\chi_{Y\cap Z} = \chi_Y \chi_Z, \qquad |Y| = \sum_{x\in X} \chi_Y(x). \tag{6.2}$$

Teorema 6.28. *[Princípio de Inclusão-Exclusão]. Sejam $X_1, \cdots, X_n$ conjuntos finitos, considerados como subconjuntos de um conjunto X. Então temos:*
(a) (versão união)

$$|X_1 \cup \cdots \cup X_n| = \sum_{j=1}^{n} (-1)^{j-1} S_j;$$

(b) (versão intersecção)

$$|X_1^c \cap \cdots \cap X_n^c| = \sum_{j=0}^{n} (-1)^j \, S_j.$$

Aqui, $S_j = \sum_{i_1<i_2<\cdots<i_j} \left|X_{i_1} \cap \cdots \cap X_{i_j}\right|$ *(soma por todos os índices crescentes) e* $S_0 := |X|$.

Demonstração. Em primeiro lugar, observe-se que ambas as 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 escrever $\chi_i : X \to \{0,1\}$ a função característica de X_i. Considere-se a função:

$$\chi_{X_1^c} \cdots \chi_{X_n^c} = (1-\chi_1)(1-\chi_2)\cdots(1-\chi_n) = \sum_{j=0}^{n} (-1)^j \prod_{i_1<i_2<\cdots<i_j} \chi_{i_1} \cdots \chi_{i_j}.$$

Isto dá o resultado, de acordo com as fórmulas (6.2). □

Exemplo 6.29. Quantas palavras de 7 letras se podem escrever com $\{a, e, i, o, u\}$ sem a sequência *uau*? Existem 5^7 palavras de 7 letras com apenas vogais.

6.9. **Escolhas com e sem reposição; com e sem ordem.** Uma das formas de entender conceptualmente um problema de contagem é modelá-lo como um problema de escolhas, tal como foi feito para o Princípio da Multiplicação. Neste caso, vimos na Proposição 6.23 que, em particular, o número de escolhas ordenadas de k elementos de um n-conjunto X é n^k.

Estas escolhas correspondem a k-tuplos ordenados $(x_1, \cdots, x_k) \in X^{\times k}$ que são, por definição, elementos do produto cartesiano $X^{\times k}$. Podemos, naturalmente ter $x_i = x_j$ com $i \neq j \in [k]$. Desta forma, dizemos que escolhemos k elementos do conjunto X, com ordem e com possível repetição. Isto é, interessa a ordem com que são escolhidos os elementos, e além disso, depois de escolher um elementos de $[n]$, podemos escolhê-lo novamente, ou não. A este processo também se designa "escolhas com reposição".

Por outro lado, sabemos que as escolhas de k elementos de um n-conjunto X, sem ordem e sem repetição (sem reposição) correspondem à escolha de um subconjunto $Y \subset X$ com k elementos. O número destas escolhas é, como sabemos $\binom{n}{k}$ e, naturalmente $k \in \{0, 1, \cdots, n\}$ caso contrário, não existem destas escolhas.

Podemos então perguntar-nos qual o número de escolhas ordenadas sem reposição; e o número de escolhas de k elementos de um n-conjunto sem ordem, mas com reposição.

Obtemos então a seguinte Tabela.

Escolha de k elementos de um n-conjunto	
c/ ordem & s/ repos.	$\frac{n!}{(n-k)!}$
s/ ordem & s/ repos.	$\binom{n}{k}$
c/ ordem & c/ repos.	n^k
s/ ordem & c/ repos.	$\binom{n-1+k}{k} = \binom{n-1+k}{n-1}$

Note-se que o número de escolhas ordenadas de k elementos sem reposição se obtém multiplicando o número de escolhas sem ordem pela ordenação dos k elementos escolhidos:

$$\frac{n!}{(n-k)!} = k! \binom{n}{k}.$$

A última fórmula pode pensar-se da seguinte forma. Precisamos de fazer k escolhas, sem nos preocuparmos com a ordem, no conjunto $[n] = \{1, \cdots, n\}$ e, de cada vez, repomos o

objecto escolhido para possivelmente o escolhermos novamente. Por exemplo, sendo $k = 7$ e $n = 5$, uma das escolhas pode ser:

$$(1, 1, 1, 2, 2, 4, 5),$$

onde $X = [5] = \{1, \cdots, 5\}$ e assumimos que a ordem não interessa). A esta escolha de 7 elementos corresponde a colocar 7 bolas, todas iguais, em caixas diferentes, numeradas de 1 a 5, da seguinte forma: colocamos 3 bolas na caixa 1, 2 na caixa 2, uma nas caixas 4 e 5, e deixamos a caixa 3 vazia.

Como é que vamos contar o número destas escolhas? Um método muito útil para isto é o seguinte, ao qual se chama, por vezes, o *Princípio do Bibliotecário*.

O número de escolhas que temos que fazer é o mesmo que considerar k livros, todos iguais, numa estante onde cabem k livros e $n-1$ separadores, e em que nos interessa a ordem pela qual colocamos os livros e os separadores. Começando da ponta esquerda da estante para a direita, a escolha acima corresponde a colocar 3 livros antes do primeiro separador, 2 livros entre o primeiro e o segundo separador, etc:

$$\circ \circ \circ \times \circ \circ \times \times \circ \times \circ,$$

onde $\circ$ designa um livro, e $\times$ um separador. Como podemos verificar, existem 7 livros e 4 separadores. Não há nenhum livro entre os separadores 2 e 3, o que corresponde ao facto de não termos escolhido o elemento $3 \in [5]$. A sequência podia também começar ou terminar com separadores, o que corresponderia a não escolher o primeiro elemento ou o último, respectivamente.

Desta forma, obtemos um método para contar o número de escolhas de k elementos de um n conjunto, sem ordem e com reposição: é o mesmo que escolher as posições de k elementos (os livros) num conjunto com $k + n - 1$ elementos: os k livros e os $n - 1$ separadores (e que é o mesmo que escolher $n-1$ separadores de um conjunto com $k+n-1$ elementos):

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

7. Funções Polinomiais

Neste capítulo e nos próxpimos vamos estudar, com algum detalhe, algumas propriedades das funções polinomiais, das funções racionais e das séries de potências, com um duplo propósito.

Um dos objectivos é mostrar como se obtêm *fórmulas explícitas* para o *termo geral* de uma sequência de números que satisfazem relações simples de *recorrência*. Este tipo de sequências são ubíquas na combinatória enumerativa, um protótipo das quais é a famosa sequência de Fibonacci:

$$(F_1, F_2, \cdots) = (1, 1, 2, 3, 5, 8, 13, \cdots),$$

que é definida pelo problema de recorrência:

$$\begin{cases} F_1 = F_2 = 1, \\ F_{n+1} = F_n + F_{n-1}, \quad n \geq 2. \end{cases}$$

Na secção 5.1 mostra-se a dedução da seguinte fórmula, misteriosa à primeira vista, para o *termo geral*:

$$F_n = \frac{1}{\sqrt{5}} \left(\phi^n - (-\phi)^{-n} \right), \quad n \geq 1,$$

onde $\phi = \frac{1+\sqrt{5}}{2}$ é a famosa constante chamada *razão dourada*. O mesmo método para obter termos gerais de sequências é aplicável a todos os problemas de recorrência *lineares*.

O outro objectivo é realçar a fortíssima analogia entre as propriedades aritméticas do anel dos *polinómios* (sobre um corpo) e o anel dos *números inteiros*, bem como a analogia entre o corpo das *funções racionais* e o corpo dos *números racionais*, e finalmente a importância destes objectos algébricos no estudo das séries, formais ou convergentes.

Números	Funções
Inteiros, $\mathbb{Z}$	Polinómios
Racionais, $\mathbb{Q}$	Funções racionais
Reais, $\mathbb{R}$	Séries

Estranhamente, a apresentação destas analogias quase não têm lugar na literatura universitária, apesar da utilidade de todos os números e funções neste quadro conceptual. De igual forma, também não é fácil encontrar uma análise detalhada do corpo das funções racionais, apesar do método de decomposição em fracções simples, ser uma das ferramentas mais importantes no currículo universitário, tanto no cálculo real a uma variável (essencial na primitivação de funções racionais) como na resolução explícita de equações diferenciais lineares.

Vamos usar a letra x para designar uma *variável*. Um *polinómio* é uma expressão da forma

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

isto é, uma soma em que cada parcela é um múltiplo de uma potência da variável x. Nesta expressão, $a_0, \cdots, a_n$ são chamados os *coeficientes* do polinómio, e podem ser números inteiros, racionais, reais ou complexos. Da mesma forma, a variável x pode ser substituida por números inteiros, reais, etc. Desta forma, os polinómios tornam-se exemplos importantes de *funções*.

Aqui, vamos considerar os casos em que os coeficientes são racionais ou reais (e o mesmo para x), comentando outros casos apenas pontualmente.

Os polinómios possuem várias propriedades em comum com os números inteiros. Por exemplo, podemos somar, subtrair e multiplicar dois polinómios dados, pelas regras usuais da aritmética. Mais interessante é o facto de que podemos dividir um polinómio por outro, da mesma forma que se faz com os inteiros.

No nosso estudo dos polinómios, vamos focar-nos neste estreito paralelismo; em partiuclar, estudamos a noção de máximo divisor comum, o algoritmo de Euclides, a identidade de Bézout, e a factorização de polinómios em factores irredutíveis.

7.1. **Aritmética dos polinómios.** Começamos pelas definições e exemplos.

Definição 7.1. Seja $n \in \mathbb{N}_0$. Um polinómio $p(x)$ de grau n (e coeficientes racionais) é uma expressão da forma

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0, \tag{7.1}$$

onde $a_0, a_1, \cdots, a_n \in \mathbb{Q}$ e $a_n \neq 0$.

O grau de um polinómio é, portanto, igual à *menor potência de x cujo coeficiente é não nulo*.[5] De igual forma, definem-se polinómios de coeficientes reais colocando, na definição acima, $a_0, \cdots, a_n \in \mathbb{R}$ (e novamente $a_n \neq 0$ para o coeficiente que define o grau).

Exemplo 7.2. Alguns exemplos de polinómios são:

- $p(x) = -\frac{1}{3}x^2 + 27x - \frac{5}{4}$,
- $q(x) = 1 + x + \cdots + x^{16} + x^{17}$,
- $r(x) = \frac{2}{5} - \frac{\pi}{4}$,

[5]Note-se que, desta forma, o polinómio 0 (todos os coeficientes nulos) não tem grau definido.

- $s(x) = \sqrt{3} + \pi x + \frac{1}{9}x^2 - e\,x^3$. ($e$ é a base dos logaritmos naturais)

Os graus destes polinómios são, respectivamente, 2, 17, 4 e 3. Os dois primeiros têm coeficientes racionais, e os dois últimos (de facto, todos) têm coeficientes reais. Os polinómios de grau zero, como $r(x)$, bem como o polinómio *nulo* (aquele que tem todos os coeficientes iguais a zero) também se designam por *constantes* ou *polinómios constantes.*

NOTAÇÃO: Por vezes, escrevemos simplesmente p em vez de $p(x)$. Usamos a notação δp para designar o grau do polinómio p. O conjunto de todos os polinómios na variável x denota-se por $\mathbb{Q}[x]$ ou por $\mathbb{R}[x]$, consoante os coeficientes sejam racionais ou reais.

Por exemplo, escrevemos $\delta p = n$ para o polinómio da equação (7.1), e em termos de conjuntos, temos naturalmente $\mathbb{Q}[x] \subset \mathbb{R}[x]$.

Os polinómios podem somar-se e multiplicar-se, pelas regras bem conhecidas, que se descrevem sucintamente com ajuda da notação abreviada de *somatório.*

Definição 7.3. Sejam $p(x) = a_0 + a_1x + \cdots + a_nx^n = \sum_{j=0}^{n} a_jx^j$, e $q(x) = \sum_{k=0}^{m} b_kx^k$ dois polinómios. Temos

$$\begin{aligned}(p+q)(x) &:= \sum_{j=0}^{\max\{m,n\}} (a_j + b_j)x^j \\ (p\cdot q)(x) &:= \sum_{k=0}^{m+n} c_kx^k, \qquad c_k = \sum_{j=0}^{k} a_jb_{k-j},\end{aligned}$$

onde, por convenção, colocamos $a_j := 0$ para $j > n$ e $b_j := 0$ para $j > m$, de modo a que as expressões façam sentido para quaisquer índices $i, j, k \in \mathbb{N}_0$.

Exemplo 7.4. Sejam $p(x) = (1+x)^2$, $q(x) = 1 - x$, e $r(x) = 1 + x + \cdots + x^n$, com $n \in \mathbb{N}$. São exemplos de operações aritméticas com polinómios:

- $p(x) - (x^2 + 2x) = (1+x)^2 - x^2 - 2x = 1 + 2x + x^2 - 2x - x^2 = 1$;
- $q(x)\,r(x) = (1-x)(1 + x + \cdots + x^n) = 1 - x^{n+1}$.

Os seguintes exercícios ilustram algumas propriedades básicas do grau dos polinómios e a sua relação com a soma e multiplicação.

Exercício 7.5. (1) Mostre que $\delta(p\cdot q) = \delta p + \delta q$, para todos os polinómios $p, q \in \mathbb{Q}[x]$ não nulos.[6]

(2) Prove que $\delta(p \pm q) \leq \max\{\delta p, \delta q\}$ para todo $p, q \in \mathbb{Q}[x]$. Mostre que $\delta(p \pm q) = \max\{\delta p, \delta q\}$, sempre que $\delta p \neq \pm\delta q$. Dê um exemplo em que $\delta(p+q) < \max\{\delta p, \delta q\}$.

(3) Mostre que o produto não tem *divisores de zero*. Ou seja, se u e v são dois polinómios em $\mathbb{Q}[x]$, então $u \cdot v = 0$ implica que $u = 0$ ou $v = 0$ (ou ambos, claro).

O conjunto dos polinómios, com as operações de soma e produto de polinómios, formam assim um *anel*. Mais precisamente, o *anel dos polinómios*, $\mathbb{Q}[x]$, tem as seguintes propriedades:

Proposição 7.6. *Sejam $p, q, r \in \mathbb{Q}[x]$, polinómios arbitrários. Então:*

(1) A soma $+$ é associativa, comutativa, tem elemento neutro 0, e todos os polinómios têm simétrico. Ou seja,

$$(p+q)+r = p+(q+r), \quad p+q = q+p,$$
$$p+0 = 0+p = 0, \quad \forall p\ \exists q\ :\ p+q = q+p = 0.$$

[6] A equação $\delta(p\cdot q) = \delta p + \delta q$ não está definida quando $p = 0$ (ou $q = 0$). No entanto, podemos garantir a sua validade para qualquer p, q, se adoptarmos a convenção de que $\delta 0 = -\infty$ (e que $-\infty + n = -\infty$ para todo $n \in \mathbb{N}_0$).

(2) O produto $\cdot$ é associativo, comutativo e tem elemento neutro 1. Ou seja,

$$(p \cdot q) \cdot r = p \cdot (q \cdot r), \quad p \cdot q = q \cdot p,$$
$$p \cdot 1 = 1 \cdot p = p.$$

(3) O produto é distributivo em relação à soma, ou seja

$$p \cdot (q + r) = p \cdot q + p \cdot r.$$

(4) ("lei do corte") $\forall p \neq 0$, temos $p \cdot q = p \cdot r \Leftrightarrow q = r$.

Note-se que as propriedades (1), (2) e (3) nesta Proposição, constituem precisamente a definição de *anel comutativo com identidade*. Por outras palavras, um anel comutativo com identidade é, por definição um conjunto munido de 2 operações, "+" (soma) e "·" (produto), que verifica todas as propriedades (1), (2) e (3).

As mesmas propriedades são válidas para polinómios com coeficientes reais, ou seja quaisquer $p, q, r \in \mathbb{R}[x]$ verificam as propriedades acima.

Demonstração. A única propriedade que não tem demonstração evidente é a propriedade (4), chamada, por razões evidentes, a lei do corte. Assim, as restantes são deixadas ao leitor. Naturalmente, uma vez que $q = r$ implica $p \cdot q = p \cdot r$ (mesmo que p seja nulo), só temos que ver o recíproco. Seja p um polinómio não nulo, e vamos supor que $p \cdot q = p \cdot r$. Nesse caso, usando as propriedades (1) e (3), temos $p \cdot (q - r) = 0$. No Exercício 7.5(3) o leitor verificou que $u \cdot v = 0$, com $u, v \in \mathbb{Q}[x]$, implica $u = 0$ ou $v = 0$. Assim, como por hipótese $p \neq 0$, concluímos que $q - r = 0$, ou seja $q = r$. □

O exercício seguinte ilustra a natureza especial da lei do corte. De facto, se considerássemos que os coeficientes dos polinómios eram classes de congruência módulo m, para um certo $m \in \mathbb{N}$ (por outras palavras, se tivéssemos polinómios em $\mathbb{Z}_m[x]$) então a lei do corte já não seria válida.

Exercício 7.7. De acordo com a nossa notação, um polinómio $p(x) \in \mathbb{Z}_m[x]$ escreve-se na forma $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ com $a_i \in \mathbb{Z}_m$ para $i = 0, \cdots, n$, sendo $\delta p = n$ se $a_n \neq 0$.

(a) Mostre que, para polinómios em $\mathbb{Z}_m[x]$, verificam-se todas as propriedades (1) a (3) da Proposição 7.6 (sendo que, na soma e produto, os coeficientes verificam as regras aritméticas de $\mathbb{Z}_m$).

(b) Dê um exemplo de um natural $m \in \mathbb{N}$, e de polinómios $u(x), v(x) \in \mathbb{Z}_m[x]$, tais que u, v não são nulos, mas $u \cdot v = 0$. (Assim, no Exercício 7.5(3), não se pode substuir $\mathbb{Q}[x]$ por $\mathbb{Z}_m[x]$).

Observação 7.8. É fácil ver que, no anel dos polinómios $\mathbb{Q}[x]$, bem como em $\mathbb{R}[x]$, em geral, não existem *inversos* para o produto, tal como em $\mathbb{Z}$. De facto, a menos que um polinómio tenha grau zero, ele não é invertível.

Exercício 7.9. Mostre que se $p(x)$ tem um inverso $q(x)$, então $\delta p = \delta q = 0$; ou seja, se $p(x) \cdot q(x) = 1$, então tanto p como q são constantes (e não nulos).

Dados polinómios $a(x), b(x) \in \mathbb{Q}[x]$ não nulos, podemos dividir um pelo outro, da mesma forma que se faz com números inteiros. Por outras palavras, o algoritmo da divisão, com *resto*, pode aplicar-se de forma análoga.

7.2. Divisibilidade em $\mathbb{Q}[x]$.

Proposição 7.10. *Sejam $a(x), b(x) \in \mathbb{Q}[x]$ dois polinómios, com $b \neq 0$. Então, existem polinómios $q(x)$ e $r(x)$, únicos, que verificam simultaneamente*

$$a(x) = b(x)\, q(x) + r(x), \quad e \quad \delta r < \delta b. \tag{7.2}$$

Definição 7.11. Quando q e r são obtidos da forma indicada na Proposição 7.10, dizemos que q é o quociente, e que r é o resto da divisão de a por b. Na equação de divisão (7.2), chamamos a a e a b, respectivamente, o divendendo e o divisor.

Demonstração. A demonstração faz-se da mesma forma que com a divisão de inteiros, com divisor não nulo. A única novidade é o facto do grau de um polinómio substituir o módulo (ou valor absoluto) do divisor. Assim, embora os coeficientes do resto possam ser arbitrariamente grandes, o seu grau está limitado pelo do divisor. □

Exemplo 7.12. Sejam $a(x) = 3x^3 - 2x^2 + 4x - 3$ o dividendo e $b(x) = x^2 + 3x + 3$ o divisor. Vamos aplicar o algoritmo de divisão com resto:

$$\begin{array}{rl} 3x^3 - 2x^2 + 4x - 3 & |x^2 + 3x + 3 \\ -(3x^3 + 9x^2 + 9x + 0) & 3x - 11 \\ -11x^2 - 5x - 3 & \\ -(-11x^2 - 33x - 33) & \\ 28x + 30 & \end{array}$$

Obtemos, assim, $q(x) = 3x - 11$ e $r(x) = 28x + 30$. Como esperado $\delta r = 1 < 2 = \delta b$ (os coeficientes do resto podem ser, como neste caso, maiores que os de $b(x)$, em módulo).

Exercício 7.13. (1) Mostre que, se $\delta a < \delta b$, então o quociente e o resto da divisão de a por b são $q(x) = 1$ e $r(x) = b(x)$, respectivamente.
(2) Numa divisão com resto, $a = bq + r$, $(b \neq 0)$ mostre que $\delta b + \delta q = \delta a$.

Em geral, o resto da divisão de um polinómio por outro, é não nulo. Quando o resto é zero, temos uma situação especial, pois o dividendo decompõe-se no produto do divisor pelo quociente.

Definição 7.14. Sejam $a, b \in \mathbb{Q}[x]$. Diz-se que b divide a, ou que b é um divisor de a, ou ainda que a é um múltiplo de b, se o resto da divisão de a por b é zero. Neste caso, escrevemos $b|a$.

Por outras palavras, o polinómio $b(x)$ divide o polinómio $a(x)$ se existe um outro polinómio $q(x)$ tal que $a(x) = b(x)q(x)$.

Exemplo 7.15. Seja $p(x) = \frac{x^3}{2} - 2x^2 + \frac{3}{2}x$. Então, $p(x) = \frac{1}{2}x(x^2 - 4x + 3)$ e (usando, por exemplo, a fórmula resolvente das equações do segundo grau) ainda podemos factorizar p na forma:

$$\frac{x^3}{2} - 2x^2 + \frac{3}{2}x \;=\; \frac{1}{2}x(x-1)(x-3).$$

Assim, por exemplo, x e $(x-1)$ dividem $p(x)$, mas também temos $-\frac{2}{5}(x-3) \,|\, p(x)$. Observe que, em termos de divisores, uma constante multiplicativa não nula é irrelevante.

Exercício 7.16. Sejam p, q, r polinómios em $\mathbb{Q}[x]$.
(1) Mostre que $1 \,|\, p$ para todo p.
(2) Prove que $p \,|\, 0$ para todo p.
(3) Prove que se $p \,|\, q$ e $p \,|\, r$ então $p \,|\, (q \pm r)$.
(4) Mostre que, se $p \,|\, q$, então $ap \,|\, bq$, para quaisquer constantes $a, b \in \mathbb{Q}$ não nulas.

Definição 7.17. Seja $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$. Diz-se que p é mónico de grau $n \geq 1$, se $a_n = 1$.

Note-se que, para qualquer $p(x)$ de grau $n \geq 1$ escrito na forma indicada, $\frac{1}{a_n}p(x)$ é um polinómio mónico, uma vez que $a_n \neq 0$. Temos também as seguintes propriedades que se deixam como exercícios.

Exercício 7.18. (1) Prove que qualquer polinómio de grau $n \geq 1$ é o produto de uma constante (não nula) por um polinómio mónico (de grau n).
(2) Sejam p, q dois polinómios mónicos. Mostre que, se $p|q$ e $q|p$, então $p = q$. Qual a relação entre p e q se $p|q$ e $q|p$, mas p e q não forem necessariamente mónicos?

Como vemos, as propriedades de divisibilidade são, aparte a constante multiplicativa, análogas às correspondentes propriedades dos inteiros. De facto, podemos definir máximo divisor comum entre dois polinómios dados, e usar uma versão completamente análoga do algoritmo de Euclides, para determiná-lo. Também a identidade de Bézout se verifica.

7.3. **O Algoritmo de Euclides para polinómios.**

Definição 7.19. Sejam dados polinómios $a, b \in \mathbb{Q}[x]$ não nulos. Dizemos que $d \in \mathbb{Q}[x]$ é um máximo divisor comum entre a e b se $d|a$, $d|b$, e se qualquer outro $c \in \mathbb{Q}[x]$ com as mesmas propriedades divide d, ou seja, se as condições $c|a$ e $c|b$ implicam $c|d$.

Uma pequena diferença entre os casos de inteiros e de polinómios, é que um máximo divisor comum não é único. No entanto, basta restringirmos a nossa atenção a polinómios mónicos para recuperarmos a unicidade.

Proposição 7.20. *Dados polinómios a e b não nulos, existe um único máximo divisor comum mónico entre a e b.*

Demonstração. Sejam d e d' máximos divisores comuns de a e b. Então $d|d'$ e $d'|d$ por definição. Como ambos d e d' são mónicos, então, pelo Exercício 7.18(2) temos $d' = d$, como queriamos mostrar. □

NOTAÇÃO Sendo $a, b \in \mathbb{Q}[x]$ não nulos, o único máximo divisor comum mónico entre a e b é designado por $\text{mdcm}(a, b)$.

Exemplo 7.21. Sejam $a(x) = x^4 - 9x^2 - 4x + 12$ e $b(x) = x^3 + 5x^2 + 2x - 8$. Vamos encontrar o máximo divisor comum mónico entre a e b usando o algoritmo de Euclides. Primeiro dividimos a por b, obtendo

$$x^4 - 9x^2 - 4x + 12 = (x - 5)(x^3 + 5x^2 + 2x - 8) + 14x^2 + 14x - 28.$$

Depois, dividimos $x^3 + 5x^2 + 2x - 8$ pelo resto $14x^2 + 14x - 28 = 14(x^2 + x - 2)$, e obtemos

$$x^3 + 5x^2 + 2x - 8 = \frac{1}{14}(x + 4) \cdot 14(x^2 + x - 2) = (x + 4)(x^2 + x - 2).$$

Como desta vez o resto é zero, e $x^2 + x - 2$ é mónico, temos $\text{mdcm}(a, b) = x^2 + x - 2$.

Tal como para inteiros, a identidade de Bézout é ainda válida para polinómios.

Teorema 7.22. *Sejam dados polinómios $a(x)$ e $b(x)$ não nulos. Se $d(x) = mdcm(a, b)$ então existem polinómios $u(x)$ e $v(x)$ tais que*

$$d(x) = a(x) \cdot u(x) + b(x) \cdot v(x).$$

Além disso, nesta equação podemos tomar $\delta u < \delta b$ e $\delta v < \delta a$.

Demonstração. A demonstração prossegue da mesma forma que no caso de números inteiros. A única parte que fica por demonstrar é a existência de uma solução que verifique as desigualdades indicadas para os graus de u e v. Deixamos esta tarefa para a próxima secção, pois a interpretação destas desigualdades ficará mais clara no contexto das funções racionais. □

Exemplo 7.23. Voltemos ao exemplo 7.21. Temos $a(x) = (x - 5)b(x) + r(x)$, e $r(x) = 14 \cdot d(x)$ onde $d(x) = \text{mdcm}(a, b) = x^2 + x - 2$. Assim, podemos imediatamente escrever

$$d(x) = \frac{a(x)}{14} + \frac{(5 - x) \cdot b(x)}{14},$$

a identidade de Bézout pretendida. Note-se que $\delta(\frac{1}{14}) = 0 < \delta b = 3$ e $\delta(\frac{x-5}{14}) = 1 < \delta a = 4$, como previsto no Teorema 7.22.

Definição 7.24. Se dois polinómios não nulos $p, q \in \mathbb{Q}[x]$ têm 1 como máximo divisor comum mónico, $\text{mdcm}(p, q) = 1$, então dizem-se *primos entre si*.

Exercício 7.25. Mostre que, tal como no caso dos números inteiros, a equação

$$c = au + bv$$

tem solução $u, v \in \mathbb{Q}[x]$ se e só se c é um múltiplo de $d = \text{mdcm}(a, b)$.

7.4. **Factorização em Irredutíveis.**

Exemplo 7.26. Voltemos ao caso $p(x) = \frac{x^3}{2} - 2x^2 + \frac{3}{2}x$ (Exemplo 7.15). Acima, factorizámos p na forma:

$$p(x) = \frac{1}{2}x\,(x-1)\,(x-3).$$

É fácil verificar que não é possível continuar a factorizar $p(x)$. Isto motiva a definição de polinómio irredutível.

Definição 7.27. Um polinómio $p(x) = a_0 + a_1x + \cdots + a_nx^n$ chama-se irredutível se tem grau positivo $\delta p = n > 0$, e os seus únicos divisores mónicos são 1 e $\frac{1}{a_n}p(x)$.

Os seguintes exercícios indicam noções equivalentes à de irredutibilidade, bem como as primeiras propriedades elementares.

Exercício 7.28. (1) Mostre que $p \in \mathbb{Q}[x]$ é irredutível se e só se, sempre que factorizarmos p na forma $p = uv$, para certos $u, v \in \mathbb{Q}[x]$, então $\delta u = 0$ ou $\delta v = 0$.

(2) Mostre que um polinómio $p \in \mathbb{Q}[x]$, de grau n, é irredutível se e só se tem apenas divisores de grau 0 e n.

(3) Prove que qualquer polinómio de grau 1 é irredutível.

(4) Dê um exemplo de um polinómio irredutível de grau superior a um (veja-se também a próxima subsecção).

O leitor terá reparado na analogia entre a noção de polinómio irredutível e o conceito de número primo. Isto não é uma simples coincidência, pois da mesma forma que qualquer número natural maior que 1 se pode escrever como produto de primos (o teorema fundamental da aritmética) qualquer polinómio não constante se escreve como produto de irredutíveis.

Teorema 7.29. *("Teorema Fundamental da Aritmética" para Polinómios - versão simples). Qualquer polinómio $p \in \mathbb{Q}[x]$ de grau $n > 0$ pode se escrever na forma:*

$$p(x) = c\,p_1(x) \cdots p_m(x),$$

onde $p_1, \cdots, p_m$ são polinómios mónicos irredutíveis, e $c \in \mathbb{Q}$. Esta factorização é única a menos de troca dos factores.

Demonstração. A demonstração é análoga à do teorema fundamental da aritmética dos naturais, e faz-se por indução. A existência da factorização é consequência do algoritmo de Euclides. Se p é irredutível, então a factorização pretendida é o produto de uma constante por um polinómio mónico irredutível, ou seja, simplesmente $p(x) = a_n \cdot \frac{1}{a_n}p(x)$. Se $p(x)$ não é irredutível, então p tem grau maior que 1 (pelo Exercício 7.28(2)) e tem divisores de grau positivo: $p = uv$ onde $\delta u > 0$ e $\delta v > 0$, com $\delta u + \delta v = \delta p$, pelo Exercício 7.5(1). Assim, como $\delta u < \delta p$, por indução no grau, vemos que todos os polinómios possuem uma decomposição em irredutíveis. A unicidade da decomposição, a menos de reordenação dos factores, é deixada ao leitor. □

Em vista destes resultados, duas perguntas naturais são: Como caracterizar os polinómios irredutíveis? Já sabemos que um polinómio de grau 1 é irredutível. Mas, se o nosso polinómio tem grau superior, como obter a sua decomposição em irredutíveis?

Ao contrário da teoria desenvolvida até aqui, as respostas a estas perguntas **dependem** do conjunto onde "vivem" os coeficientes. Por exemplo, a resposta em $\mathbb{Q}[x]$ é diferente da resposta em $\mathbb{R}[x]$. De facto, as respostas mais simples verificam-se no anel $\mathbb{C}[x]$, ou seja, para polinómios com coeficientes que são números *complexos*. Esta é precisamente uma das fortes razões para estudar o corpo dos números complexos. O teorema fundamental da álgebra, diz-nos precisamente que qualquer polinómio de grau n com coeficientes complexos tem precisamentre n factores irredutíveis (podem ser repetidos), cada um dos quais é um polinómio de grau 1. No caso de coeficientes reais (e complexos, claro!), a forma mais útil de entender a factorização em irredutíveis é usando o conceito de *raiz de um polinómio* $p(x)$.

Por outro lado, como estamos interessados na aplicação da teoria dos polinómios e funções racionais à combinatória, onde os coeficientes que surgem são naturalmente racionais, ou reais, deixamos um estudo detalhado destas questões para o Apêndice, e vamos agora abordar as funções racionais.

7.5. **Funções Racionais.** Vamos agora considerar as funções mais simples a seguir aos polinómios. Doravante, todos os polinómios têm coeficientes reais, a menos que o contrário seja expressamente indicado.

Definição 7.30. Uma função racional é o quociente de dois polinómios em que o denominador não é o polinómio nulo. Assim, uma função racional é da forma

$$f(x) = \frac{q(x)}{p(x)}$$

onde $p, q \in \mathbb{R}[x]$ e $\delta q \geq 0$.

Observação 7.31. Note-se que f não define unicamente p e q, pois podemos multiplicar p e q pelo mesmo polinómio não nulo, obtendo a mesma função racional. Assim, sem perda de generalidade, e salvo expressa menção em contrário, *assumiremos sempre que f é uma fracção escrita em forma irredutível, ou seja, p e q são polinómios primos entre si.*

Em contraste com os polinómios, as funções racionais são invertíveis, com a excepção da função nula (identicamente igual a zero).

Exercício 7.32. (1) Mostre que uma função racional $f = q/p$ (na forma reduzida) é um polinómio se e só se $\delta p = 0$.

(2) Mostre que qualquer função racional tem um inverso, excepto a função nula. Mais precisamente, prove que, se $f \neq 0$ é uma função racional, então existe outra função racional, única, $g(x)$ tal que $f(x)g(x) = 1$.

Definição 7.33. Uma função racional própria é uma função racional $q(x)/p(x)$ em que $\delta q < \delta p$. Uma função racional simples é uma função racional própria da forma $q(x)/p(x)^k$, para certo $k \in \mathbb{N}$ e $p(x)$ irredutível mónico. Por vezes, usam-se também as expressões *fracção própria* e *fracção simples*, respectivamente.

Exercício 7.34. Mostre que, se $f_1(x)$ e $f_2(x)$ são funções racionais próprias, então $f_1(x)f_2(x)$ e $f_1(x) \pm f_2(x)$ também são funções racionais próprias.

As funções racionais podem decompor-se usando o algoritmo de divisão dos polinómios.

Proposição 7.35. *Qualquer função racional se pode escrever como a soma de um polinómio e de uma função racional própria. Mais precisamente, seja $f(x)$ uma função racional. Então existem polinómios $a, b, c \in \mathbb{R}[x]$ tais que $f(x) = a(x) + \frac{b(x)}{c(x)}$ e verificando $\delta b < \delta c$.*

Demonstração. Esta demonstração é uma aplicação directa do algoritmo de divisão de polinómios. Seja $f(x) = \frac{q(x)}{p(x)}$, escrito na forma reduzida. Se f é própria, não temos nada

a mostrar (uma vez que serve $a \equiv 0$, $b = q$, $c = p$). No caso contrário $\delta q > \delta p$, pelo que, dividindo q por p, obtemos

$$q(x) = p(x)a(x) + b(x),$$

com $\delta b < \delta p$. Logo

$$f = \frac{q}{p} = \frac{pa + b}{p} = a + \frac{b}{p},$$

que é a expressão pretendida, se pusermos $c = p$. □

Um resultado muito importante, que permite a simplificação de muitos problemas que envolvem funções racionais é o da decomposição em fracções simples. Um dos casos mais úteis de aplicação deste resultado, pode ser escrito na seguinte forma.

Proposição 7.36. *Seja $f(x) = \frac{q(x)}{p(x)}$ uma função racional própria e seja $p(x) = p_1(x)\, p_2(x)$ uma factorização do denominador em factores primos entre si, ou seja*

$$\text{mdcm}(p_1, p_2) = 1.$$

Então podemos escrever $f(x)$ como soma de funções racionais próprias

$$f(x) = \frac{q_1(x)}{p_1(x)} + \frac{q_2(x)}{p_2(x)}.$$

Desta forma, temos $\delta(q_i) < \delta(p_i)$ para $i = 1, 2$.

Demonstração. Como p_1 e p_2 são primos entre si, aplicando a identidade de Bézout, existem polinómios u e v tais que

$$vp_1 + up_2 = q. \tag{7.3}$$

Dividindo por $p = p_1 p_2$ obtemos uma soma de funções racionais:

$$f = \frac{q}{p} = \frac{q}{p_1 p_2} = \frac{u}{p_1} + \frac{v}{p_2}. \tag{7.4}$$

À partida, dado que as soluções da identidade de Bézout não são únicas, não podemos garantir que $\frac{u}{p_1}$ ou $\frac{v}{p_2}$ são próprias. Vamos supor que $\delta u \geq \delta p_1$, e vamos então dividir u por p_1, de modo a obter uma função racional própria. Escrevemos $u = p_1 \cdot s + r$ onde o resto $r(x)$ verifica $\delta r < \delta p_1$. Substituindo u por r obtemos

$$f = \frac{u}{p_1} + \frac{v}{p_2} = \frac{u}{p_1} - s + \frac{v}{p_2} + s = \frac{u - p_1 \cdot s}{p_1} + \frac{v + p_2 \cdot s}{p_2} = \frac{r}{p_1} + \frac{v + p_2 \cdot s}{p_2}.$$

Desta forma, considerando $q_1 := r$, $q_2 := v + p_2 \cdot s$ temos que r/p_1 é uma função racional própria, pois $\delta r < \delta p_1$, e como

$$\frac{q_2}{p_2} = \frac{q}{p} - \frac{q_1}{p_1},$$

o exercício 7.34 mostra que q_2/p_2 também é própria. □

Por indução, obtemos o seguinte resultado.

Teorema 7.37. *Seja $p(x) = cp_1(x)^{k_1} \cdots p_r(x)^{k_r}$ a decomposição do polinómio $p \in \mathbb{R}[x]$ (não nulo) em factores irredutíveis. Então, qualquer função racional própria, tendo p como denominador, se escreve como*

$$\frac{q}{p} = \frac{q_1}{p_1^{k_1}} + \cdots + \frac{q_r}{p_r^{k_r}},$$

onde todas as fracções do lado direito são simples (em particular, $\delta q_i < \delta(p_i^{k_i}) = k_i \delta p_i$ para todo $i = 1, \cdots, r$).

Exemplo 7.38. Vamos representar em frações simples a seguinte função:

$$f(x) = \frac{x^2}{(x^2+9)(x-3)^2}.$$

De acordo com o teorema, temos:

$$\frac{x^2}{(x^2+9)(x-3)^2} = \frac{ax+b}{x^2+9} + \frac{cx+d}{(x-3)^2} = \frac{(ax+b)(x-3)^2 + (cx+d)(x^2+9)}{(x^2+9)(x-3)^2}.$$

Desenvolvendo o numerador, obtemos:

$$x^2 = ax^3 - 6ax^2 + 9ax + bx^2 - 6bx + 9b + (cx^3 + dx^2 + 9cx + 9d)$$

e igualando os coeficientes de todos os graus, temos então:

$$\begin{aligned} a + c &= 0 \\ -6a + b + d &= 1 \\ 9a - 6b + 9c &= 0 \\ 9b + 9d &= 0, \end{aligned}$$

o que, após alguns cálculos, nos fornece a solução única: $c = -a = \frac{1}{6}$ e $b = d = 0$, de onde:

$$f(x) = \frac{-\frac{x}{6}}{x^2+9} + \frac{\frac{x}{6}}{(x-3)^3}.$$

Este estudo das funções racionais pode ser resumido, com o que mostrámos até aqui, da seguinte forma: Qualquer função racional é a soma de um polinómio com uma função racional própria. Qualquer função racional própria se pode escrever como a soma de fracções simples.

No entanto, para podermos aplicar convenientemente o método das fracções simples a vários problemas concretos, tanto em combinatória, como na determinação de primitivas, como na resolução de equações diferenciais, precisamos de saber desenvolver fracções simples em séries de potências na variável x. Para isso, introduzimos a noção de série formal.

8. Séries Formais e Funções Geradoras

Nesta secção, estuda-se uma generalização dos polinómios que, de certa forma, se podem pensar como polinómios infinitos.

Começamos por dar um exemplo, de enorme importância, o exemplo da *série geométrica*. É bem sabido que, para qualquer número real $x \neq 1$, temos a igualdade:

$$1 + x + \cdots + x^n = \frac{1 - x^{n+1}}{1 - x}.$$

Se, além disso, $|x|<1$, sabemos que x^n tende para zero, quando n tende a infinito. Assim, podemos escrever

$$\frac{1}{1-x} = 1 + x + \cdots + x^n + \cdots = \sum_{n=0}^{\infty} x^n, \quad |x| < 1.$$

Nestas notas, não estamos interessados nas propriedades de convergência de uma dada série, e consideramos x como uma mera variável formal. Assim, vamos considerar expressões da forma

$$a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{n=0}^{\infty} a_n \, x^n,$$

onde os coeficientes a_n são em geral, números racionais, mas podem igualmente ser reais ou complexos. Esta expressão chama-se uma série formal, mas também a "função geradora" dos números a_n.

Definição 8.1. Uma série formal (de coeficientes racionais) é uma expressão da forma $a_0 + a_1x + a_2x^2 + \cdots = \sum_{n=0}^{\infty} a_n\, x^n$, com $a_n \in \mathbb{Q}$. Por vezes, escrevemos

$$a(x) = a_0 + a_1x + a_2x^2 + \cdots = \sum_{n=0}^{\infty} a_n\, x^n$$

para referir uma série formal. Note-se que, no entanto, não estamos a dar a $a(x)$ nenhuma interpretação como função da variável x.

Tal como os polinómios, as séries formais podem somar-se e multiplicar-se, usando regras idênticas às desse caso.

Definição 8.2. Sejam $a(x) = \sum_{j=0}^{n} a_jx^j$, e $b(x) = \sum_{k=0}^{m} b_kx^k$ duas séries formais. Temos

$$\begin{aligned}(a+b)(x) &:= \sum_{j=0}^{\infty}(a_j + b_j)x^j \\ (a\cdot b)(x) &:= \sum_{k=0}^{\infty} c_kx^k, \qquad c_k = \sum_{j=0}^{k} a_jb_{k-j}.\end{aligned}$$

Tal como no caso dos polinómios, temos um elemento neutro para a soma, a série nula, e um elemento neutro para a multiplicação, que é a série $1 = 1 + 0x + 0x^2 + \cdots$.

Temos o seguinte critério para a invertibilidade de uma série.

Proposição 8.3. *Seja $a(x) = \sum_{j=0}^{n} a_jx^j$ uma série formal. Então a tem inverso se e só se $a_0 \neq 0$.*

Demonstração. ... □

Exercício 8.4. Mostre que o produto de séries formais não tem *divisores de zero*. Ou seja, se u e v são séries formais, então $u \cdot v = 0$ implica que $u = 0$ ou $v = 0$ (ou ambos, claro).

A teoria das séries formais é vasta e apenas podemos indicar algumas das suas características. Em particular, estando interessados em aplicações à combinatória (e da mesma forma para a primitivação ou resolução de equações diferenciais), as séries formais que nos interessam são as que correspondem à expansão em série de funções racionais

8.1. **Séries formais de funções racionais.** A série geométrica é de grande importância pelo facto de que muitas outras séries se podem deduzir dela por operações algébricas simples. Assim, temos, por exemplo:

Exemplo 8.5.

- $\frac{1}{2+x} = \frac{1}{2}\frac{1}{1+\frac{x}{2}} = \frac{1}{2}\frac{1}{1-(-\frac{x}{2})} = \frac{1}{2}\sum_{n=0}^{\infty}(-\frac{x}{2})^n = \frac{1}{2}\sum_{n=0}^{\infty}\frac{(-1)^n}{2^n}x^n$
- $\frac{1}{1+4x^3} = \sum_{n=0}^{\infty}(4x^3)^n = \sum_{n=0}^{\infty}4^nx^{3n}$

O nosso objectivo aqui será o de obter desenvolvimento em série de qualquer função racional. Uma vez que qualquer função racional é a soma de um polinómio com uma sequência finita de fracções simples, vamos concentrar-nos neste caso.

Teorema 8.6. *Considere-se a fracção simples $f(x) = \frac{1}{p(x)}$ com $p(x) = (1-x)^n$. Então, é válido o desenvolvimento*

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

Demonstração. Note-se que o coeficiente de x^k é o número de formas de distribuir k bolas iguais por n caixas diferentes. Vamos usar a série de Taylor: □

O seguinte enunciado resume o essencial dos resultados das duas últimas secções.

Teorema 8.7. *Qualquer função racional é a soma de um polinómio com uma função racional própria. Qualquer função racional própria se pode escrever como a soma de fracções simples. Qualquer fracção simples se pode desenvolver em série usando a série geométrica, e as suas derivadas.*

9. Funções Geradoras em Combinatória

9.1. **Sucessões definidas por recorrência.** Uma sequência de números inteiros $\{u_n\}_{n\in\mathbb{N}}$ 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.

Vamos concentrar-nos nas sequências 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 $k \in \mathbb{N}$.

9.2. **Um exemplo: a sucessão de Fibonacci.** Consideremos a sequência dos inteiros de Fibonacci $F_0, F_1, F_2, \cdots$, definida por

$$F_0 = 0,\ F_1 = 1, \quad F_{n+2} = F_{n+1} + F_n,\ n \geq 0.$$

Vamos combinar a teoria das funções geradoras com o método das fracções simples para encontrar uma fórmula para o termo geral F_n. Seja:

$$f(x) = \sum_{n=0} F_n\, x^n = F_0 + F_1 x + F_2 x^2 + \cdots$$

a função geradora da sucessão de Fibonacci. O primeiro passo é encontrar funções geradoras para F_{n+1} e para F_{n+2}, os outros termos envolvidos na equação de recorrência. Temos:

$$f(x) - F_0 = f(x) = x\,(F_1 + F_2 x + \cdots + F_{n+1}x^n + \cdots) = x \sum_{n=0} F_{n+1}\, x^n,$$

ou seja:

$$\sum_{n=0} F_{n+1}\, x^n = \frac{f(x)}{x}.$$

Da mesma forma,

$$f(x) - F_0 - F_1 x = x^2\,(F_2 + F_3 x + \cdots + F_{n+2}x^n + \cdots) = x^2 \sum_{n=0} F_{n+2}\, x^n,$$

pelo que concluímos,

$$\sum_{n=0} F_{n+2}\, x^n = \frac{f(x) - F_0 - F_1 x}{x^2} = \frac{f(x) - x}{x^2}.$$

O segundo passo consiste em usar relação de recorrência $F_{n+2} = F_{n+1} + F_n$ para obter uma relação algébrica para a função f, isto é:

$$\frac{f(x) - x}{x^2} = \sum_{n=0} F_{n+2}\, x^n = \sum_{n=0} (F_{n+1} + F_n)\, x^n = \sum_{n=0} F_{n+1}\, x^n + \sum_{n=0} F_{n+1}\, x^n =$$

$$= \frac{f(x)}{x} + f(x).$$

De facto, podemos agora escrever $f(x)$ como uma função racional própria:

$$\frac{f(x)-x}{x^2} = \frac{f(x)}{x} + f(x), \quad \Leftrightarrow \quad f(x) - x = x\, f(x) + x^2\, f(x), \quad \Leftrightarrow \quad f(x) = \frac{x}{1-x-x^2}.$$

Desta forma, podemos aplicar o método das fracções simples, o terceiro passo. Para isso, começamos por factorizar o denominador $1 - x - x^2$. Pela fórmula resolvente:

$$-x^2 - x + 1 = 0 \quad \Leftrightarrow \quad x = \mu := \frac{-1+\sqrt{5}}{2} \quad \text{ou } x = \nu := \frac{-1-\sqrt{5}}{2},$$

obtemos (usando $\mu\upsilon = -1$):

$$1 - x - x^2 = -(x-\mu)(x-\nu) = (1 - \frac{x}{\mu})(\mu x + 1) = (1-\phi x)(1+\frac{x}{\phi}).$$

Como veremos, a última factorização resulta ser mais conveniente, onde considerámos o famoso número de ouro:

$$\phi = \frac{1}{\mu} = -\nu = \frac{1+\sqrt{5}}{2}.$$

Assim, chegámos ao quarto passo, que consiste em aplicar o método das fracções simples, para escrever:

$$f(x) = \frac{x}{1-x-x^2} = \frac{x}{(1-\phi x)(1+\frac{x}{\phi})} = \frac{A}{1-\phi x} + \frac{B}{1+\frac{x}{\phi}}.$$

Os valores de A e B são determinados por

$$A(1+\frac{x}{\phi}) + B(1-\phi x) = x,$$

de onde concluímos que $A+B=0$ e que $A\frac{1}{\phi} - B\phi = 1$, pelo que $A(\phi + \frac{1}{\phi}) = A(\phi+\mu) = 1$, ou seja

$$A = \frac{1}{\sqrt{5}} \quad B = -\frac{1}{\sqrt{5}}.$$

O quinto passo é escrever as fracções simples novamente em termos de séries usando a série geométrica (e as suas derivadas, caso fosse necessário). Temos, assim:

$$\begin{aligned} f(x) = \frac{\frac{1}{\sqrt{5}}}{1-\phi x} - \frac{\frac{1}{\sqrt{5}}}{1+\mu x} &= \frac{1}{\sqrt{5}}\left(\frac{1}{1-\phi x} - \frac{1}{1+\frac{x}{\phi}}\right) = \\ &= \frac{1}{\sqrt{5}}\left(\sum_{n=0}(\phi x)^n - \sum_{n=0}(-\frac{x}{\phi})^n\right) = \\ &= \frac{1}{\sqrt{5}}\sum_{n=0}(\phi^n - (-\phi)^{-n})\, x^n. \end{aligned}$$

Finalmente, por comparação com a série inicial $f(x) = \sum_{n=0} F_n\, x^n$, obtemos a fórmula desejada

$$F_n = \frac{1}{\sqrt{5}}(\phi^n - (-\phi)^{-n}).$$

Teorema 9.1. *Seja u_n uma sucessão definida por recorrência linear homogénea. Então a respectiva função geradora é uma função racional.*

O que podemos dizer sobre recorrências lineares não homogéneas?

Teorema 9.2. *Seja u_n uma sucessão definida por recorrência linear não homogénea, com termo não homogéneo a_n. Se $\sum_n a_n x^n$ é uma função racional, então a função geradora $f(x)$ para a sequência u_n é também uma função racional. Além disso, se $\sum_n a_n x^n$ é própria, $f(x)$ também é própria.*

Exemplo 9.3. Considere a recorrência não homogénea

$$a_{n+1} = 3a_n + \frac{(-1)^n}{2^n},\ n \geq 0; \quad a_0 = 2.$$

Vamos encontrar uma fórmula para o termo geral. Seja $f(x) = \sum_{n=0} a_n x^n$ a função geradora. Então

$$\frac{f(x) - a_0}{x} = \frac{f(x) - 2}{x} = \sum_{n=0} a_{n+1} x^n, \qquad \text{e} \qquad \frac{1}{1+\frac{x}{2}} = \sum_{n=0} (-\frac{1}{2})^n x^n.$$

Assim, temos

$$\frac{f(x)-2}{x} = 3f(x) + \frac{1}{1+\frac{x}{2}} \quad \Leftrightarrow \quad f(x) - 2 - 3xf(x) = \frac{x}{1+\frac{x}{2}} \quad \Leftrightarrow \quad f(x) = \frac{2}{1-3x} + \frac{1}{1-3x} \cdot \frac{x}{1+\frac{x}{2}}.$$

Decompondo em fracções simples, temos:

$$f(x) = \frac{2}{1-3x} + \frac{\frac{2}{7}}{1-3x} - \frac{\frac{2}{7}}{1+\frac{x}{2}} = ...$$

9.3. **Funções geradoras em combinatória.** O uso de funções geradoras em combinatória permite sistematizar muitas técnicas de contagem que vimos anteriormente. De facto, o número de escolhas de k elementos de um n-conjunto, com e sem repetição, com e sem ordem, é um determinado coeficiente de uma função geradora.

Por exemplo, o número de maneiras de escolher k elementos (sem repetição e sem ordem) de um n-conjunto é o coeficiente de x^k na função (polinomial):

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

Por outro lado, como observámos no Teorema 8.6, o número de formas de escolher k elementos sem ordem, mas com possível repetição, de um n-conjunto é o coeficiente de x^k da função:

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

Outras funções geradoras também se podem encontrar facilmente. Por exemplo, vamos supor que, de uma caixa de 36 bolas de golf, pretendermos retirar bolas, mas apenas em múltiplos de 4 bolas. A função geradora é então:

$$1 + x^4 + x^8 + \cdots + x^{36} = \frac{1-x^{40}}{1-x^4},$$

porque há 1 maneira de escolher 0 bolas, 0 maneiras de escolher 1,2 ou 3 bolas, 1 forma de escolher 4 bolas, etc.

Até agora, parece que não se ganhou nada em particular com a consideração de funções geradoras, pois estes números combinatórios, já tinham sido obtidos por outros métodos. No entanto, iremos ilustrar o método das funções geradoras, que é especialmente vantajoso em duas situações:

(1) quando se pretende saber, não apenas um número combinatório em particular, mas uma sucessão de números combinatórios que dependem de parâmetros.

(2) quando se supõe que estamos a escolher elementos de um conjunto potencialmente infinito.

Exemplo 9.4. Vamos supor que temos um conjunto ilimitado de maças, laranjas, bananas, e peras. De quantas formas podemos compor uma cesta com k frutas, obedecendo às seguintes regras:

- O número de maçãs deve ser par e o número de bananas deve ser múltiplo de 5;

- Não pode haver mais que 4 laranjas, nem mais que uma pera;

Este problema pode ser resolvido porque as escolhas dos vários tipos de frutas são independentes. Desta forma, a função geradora para as k escolhas, $f(x)$, é o produto das funções geradoras para as várias escolhas:

$$\begin{aligned} m(x) &= 1 + x^2 + x^4 + \cdots = \frac{1}{1-x^2} \\ b(x) &= 1 + x^5 + x^{10} + \cdots = \frac{1}{1-x^5} \\ l(x) &= 1 + x + x^2 + x^3 + x^4 = \frac{1-x^5}{1-x} \\ p(x) &= 1 + x, \end{aligned}$$

Assim, temos:

$$f(x) = m(x)b(x)l(x)p(x) = \frac{1}{1-x^2}\frac{1}{1-x^5}\frac{1-x^5}{1-x}(1+x) = \frac{1+x}{(1-x)^2(1+x)} = \frac{1}{(1-x)^2}.$$

Escrevendo a respectiva série, temos:

$$f(x) = \sum_{k=0}^{\infty} \binom{k+2-1}{k} x^k = \sum_{k=0}^{\infty} (k+1)x^k.$$

Conclusão: o número de maneiras de colocar k frutas na cesta, obedecendo às regras é $k+1$!

9.4. **Distribuições de bolas em caixas diferentes.** Anteriormente vimos a forma de contar escolhas com e sem repetição, com e sem ordem. Agora, vamos considerar um modelo semelhante, mas em que temos bolas, iguais ou diferentes, e vamos distribuí-las por caixas diferentes (ou caixas etiquetadas). O caso em que as caixas são iguais será visto na próxima secção.

A seguinte tabela resume a situação quando temos escolhas de k elementos de um n-conjunto, ou distribuimos k bolas por n caixas **diferentes**.

Escolha de k elementos de um n-conjunto		k bolas em n caixas $\neq$	funções $f : [k] \to [n]$
c/ ordem & s/ rep.	$\frac{n!}{(n-k)!}$	bolas $\neq$, caixas pequenas	injectivas
s/ ordem & s/ rep.	$\binom{n}{k}$	bolas $=$, caixas pequenas	inject. / permut. $[k]$
c/ ordem & c/ rep.	n^k	bolas $\neq$, caixas grandes	todas
s/ ordem & c/ rep.	$\binom{n-1+k}{k} = \binom{n-1+k}{n-1}$	bolas $=$, caixas grandes	todas / permut. $[k]$
c/ ordem, todos (c/rep.)	$n!\, S(k,n)$	bolas $\neq$, caixas $\neq \varnothing$	sobrejectivas
s/ ordem, todos (c/rep.)	$\binom{k-1}{n-1}$	bolas $=$, caixas $\neq \varnothing$	sobrej. / permut. $[k]$

Os números de Stirling (de segunda espécie) $S(k,n)$ representam as partições de um k-conjunto em n partes não vazias.

9.5. **Distribuições de bolas por caixas iguais e partições.** A consideração de distribuições de bolas (iguais ou diferentes) em caixas iguais pode ser mais facilmente entendida com o conceito de partições de conjuntos, ou de números naturais.

Consideremos o número, $p(k,n)$ de partições de um número natural k em n partes. Por exemplo,

$$5 = 3 + 2, \quad 5 = 4 + 1,$$

são as únicas formas de escrever 5 como soma de 2 naturais, pelo que $p(5,2) = 2$.

...

10. Permutações e Simetrias

Seja $n \in \mathbb{N}$.

Definição 10.1. 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.

Notação: O conjunto das permutações de n elementos designa-se por S_n. A permutação $\sigma \in S_n$ que envia $i \in [n]$ em $\sigma(i) \in [n]$, indica-se da seguinte forma:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Como são funções definidas no mesmo conjunto, as permutações podem compor-se da mesma forma que as funções. Por outro lado, como são funções bijectivas, qualquer permutação tem um inverso, dado pela correspondente função inversa.

Exemplo 10.2. Para $n = 6$, seja $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ & & & & & \end{pmatrix}$ e $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ & & & & & \end{pmatrix}$.
Então podemos compor as permutações ρ e π da seguinte forma

Definição 10.3. Um grupo (finito) é um conjunto G onde existe uma operação (pensada como sendo uma multiplicação) associativa, um elemento neutro, e 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 $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Exemplo 10.4. O conjunto dos números reais não nulos é um grupo. Qualquer espaço vectorial é um grupo, com a operação de soma de vectores a fazer o papel da operação $\cdot$ (nestes dois casos até temos a comutatividade $x \cdot y = y \cdot x$). Um exemplo de grupo que não é comutativo é o grupo das matrizes 2×2 que são invertíveis. Outro exemplo é o conjunto das permutações de $n > 2$ elementos, com a operação de composição.

Dado um grupo finito G e um seu subgrupo H, podemos considerar o conjunto das classes de equivalência por translacção. 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 $y = h \cdot x$.

Proposição 10.5. *Teorema de Lagrange Seja G um grupo e $H \subset G$ um subgrupo. Então*

$$|G/H| = |G|/|H|.$$

Demonstração. Consideremos a aplicaçã natural de G nas classes de equivalência

$$\begin{aligned} \pi : G &\to G/H \\ g &\to [g], \end{aligned}$$

onde $[g]$ designa a classe de equivalência a que pertence $g \in G$. 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 10.6. Uma acção de um grupo finito G num conjunto finito X é uma aplicação:

$$\begin{aligned} \psi : G \times X &\to X \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

Terminologia Quando temos uma acção de G em X também dizemos que X é um G-conjunto.

As seguintes noções são também muito úteis.

Definição 10.7. Seja X um G-conjunto e $x \in X$. O subgrupo de isotropia (ou subgrupo 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.

Proposição 10.8. *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 10.9. 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:

$$X^g := \{x \in X \,:\, g \cdot x = x\} \subset X.$$

Teorema 10.10. *[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:

$$\begin{aligned} \sum_{g \in G} |X^g| = |\{(g,x) \in G \times X \,:\, g \cdot x = x\}| &= \sum_{x \in X} |G_x| = \\ &= |G| \sum_{x \in X} \frac{1}{|G \cdot x|} = \\ &= |G| \sum_{\alpha \in X/G} \sum_{x \in \alpha} \frac{1}{|\alpha|} = \\ &= |G| \sum_{\alpha \in X/G} 1 = |G| \cdot |X/G|. \end{aligned}$$

como pretendido. □

Exemplo 10.11. O número de órbitas da acção de rotação num octaedro colocado na vertical é 3. Verifiquemos que este número é obtido pela fórmula acima.

Proposição 10.12. *Se X é um G-conjunto finito, então o conjunto das funções de X em $Y = [m]$ é também um G-conjunto, com a acção:*

$$(g \cdot f)(x) = f(g^{-1} \cdot x) \quad \forall x \in X.$$

Demonstração. ... □

Teorema 10.13. *Seja $c = c_\sigma$ o número de ciclos da permutação $\sigma : [n] \to [n]$, e $F^\sigma \subset Func([n], Y)$ o conjunto das funções fixas por σ. Então:*

$$|F^\sigma| = |Y|^c.$$

Demonstração. Vamos escrever

$$\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_c,$$

onde cada σ_i é um ciclo ($i = 1, \cdots, c$). Então $f \in F^\sigma$ (ie, f é uma função invariante por σ) se e só se para quaisquer $x, x' \in [n]$ que estejam no mesmo ciclo σ_i, temos $f(x) = f(x')$. Isto corresponde a escolher um valor de Y para cada um dos ciclos de σ. Como estas escolhas são independentes e há c ciclos, o número destas escolhas é $|Y|^c$. □

Exemplo 10.14. Quantas são as maneiras de colorir as faces de um cubo com 3 cores?
Resposta: 57.

Parte 3. **GRAFOS**

11. Grafos e Matrizes

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 redes sociais baseadas na internet.

Existem vários tipos de grafos, consoante a natureza das ligações entre vértices. Se as ligações são orientadas, falamos de grafos dirigidos, ou orientados. Caso contrário falamos de grafos não dirigidos.

Alguns exemplos de grafos são:

... colocar imagens ...

11.1. **Grafos e as matrizes correspondentes.**

Definição 11.1. Um grafo (finito) é um par $G = (V_G, A_G)$ dado por um conjunto de vértices V_G e um conjunto de arestas (ou ligações) A_G (que são conjuntos finitos), e em que A_G é formado por pares (não ordenados) de elementos distintos de V_G. Assim, cada aresta $a \in A_G$ é composta por **dois vértices** $a = \{v, w\}$, com $v \neq w \in V_G$, e não há duas arestas com os mesmos dois elementos.

Terminologia: Quando G está implícito, escrevemos simplesmente V e A para os conjuntos de vértices e arestas de G. Quando $a = \{v, w\} \in A$ dizemos que v e w são *vértices incidentes* em a, ou que v e w são *os extremos de* a; da mesma forma, dizemos que a *incide em* v e em w. Sempre que $v, w \in V$ são dois vértices unidos por uma aresta (ou seja, $v, w \in a$ para certo $a \in A$) dizemos também que v e w são *adjacentes*.

Exemplo 11.2. Vejamos alguns exemplos de grafos. Seja $n \in \mathbb{N}$.

- Se G tem n vértices, e não tem arestas (ou seja $|V| = n$ e $E = \varnothing$) temos um grafo *totalmente desconexo* em n vértices. Assim, um destes grafos é simplesmente um conjunto finito.
- Se G tem n vértices, e tem uma aresta entre cada par de vértices distintos, então G chama-se o *grafo completo* de n vértices, e denota-se por K_n. Este é um grafo simples com $\binom{n}{2}$ arestas.
- O grafo P_n com n vértices, numerados de 1 a n, e com arestas $a_1, \cdots, a_{n-1}$ de tal forma que $\psi(a_i) = \{i, i+1\}$ é chamado o *grafo caminho* de n vértices (ou de tamanho $n-1$), uma vez que a_i liga o vértice i ao vértice $i+1$ e não há mais arestas.
- O grafo C_n com n vértices, numerados de 1 a n, e com arestas $a_1, \cdots, a_n$ de tal forma que a_i liga o vértice i ao vértice $i+1$, para $i = 1, \cdots, n-1$ e a_n liga o vértice n ao vértice 1, chama-se o *grafo ciclo* de tamanho n.

Há várias quantidades importantes a reter quando temos um grafo.

Definição 11.3. Sendo $G = (V, A)$, a ordem de G é o número de vértices $|V|$, e o tamanho de G é o número de arestas $|A|$.

Como mencionado acima, há bastantes variações na definição de grafo. Em particular, podemos considerar grafos com arestas que incidem apenas num vértice.

Definição 11.4. Um pseudo-grafo (finito) é um par $G = (V, A)$ sendo V o conjunto de vértices V e A o de arestas (conjuntos finitos), mas onde os elementos $a \in A$ ou são arestas,

como anteriormente, ou são *lacetes*. Um lacete é um elemento $a \in A$ da forma $a = \{v\}$, para algum $v \in V$. Assim, o lacete é um tipo de ligação do vértice v consigo próprio. Neste caso, dizemos que a incide duplamente em v, ou que v é um extremo duplo de $a \in A$.

Observação 11.5. Nos pseudo-grafos admitimos apenas uma aresta entre cada par de vértices diferentes, ou um lacete, no máximo, para cada vértice. Podemos também permitir várias ligações diferentes entre os mesmos vértices ou vários lacetes num dado vértice, o que levaria a noções ainda mais gerais, que serão mencionadas no capítulo...

Naturalmente um grafo é um pseudo-grafo sem lacetes. Quando se trabalha com frequência com pseudo-grafos, os grafos da Definição 11.1 são chamados de grafos *simples*, para os distinguir. Como estudamos essencialmente os grafos da Definição 11.1, omitiremos, em geral, o adjectivo simples.

Para cada vértice $v \in V$ podemos considerar o número de arestas que nele incidem.

Definição 11.6. Seja G um grafo, e v um dos seus vértices. O grau de $v \in V$, denotado por d_v é o número de arestas que incidem nele:

$$d_v := |\{a \in A : v \in a\}|.$$

No caso de v ter um lacete $a \in A$ (apenas para um pseudo-grafo), este deve ser contado duas vezes. Se G tem todos os vértices do mesmo grau k, dizemos que G é k-regular.

Exemplo 11.7. Se $G = K_n$ o grafo completo de ordem n, temos que cada vértice é adjacente a todos os outros, pelo que $d_v = n - 1$ para todos os vértices $v \in K_n$. Desta forma K_n é $(n-1)$-regular. Um grafo ciclo é 2-regular para qualquer número de vértices.

Embora a representação gráfica dos grafos numa folha de papel ou num quadro seja extremamente útil para raciocinar sobre grafos, as seguintes ferramentas algébricas são também muito utilizadas.

Definição 11.8. Seja G um grafo (ou pseudo-grafo). A Matriz de Incidência de G é a matriz $M = M_G$ com $n = |V|$ linhas e $m = |A|$ colunas, cuja entrada na linha i e coluna j, correspondente ao vértice v_i e à aresta a_j, é dada por

$$M_{ij} = \begin{cases} 1, & a_j \text{ incide em } v_i \\ 0, & a_j \text{ não incide em } v_i, \\ 2, & a_j \text{ é lacete em } v_i \end{cases} \qquad i \in [n], \quad j \in [m]$$

(naturalmente, a terceira opção só ocorre em pseudo-grafos que não são grafos). A Matriz de Adjacência de G é uma matriz quadrada $Q = Q_G$, simétrica, com $n = |V|$ linhas e n colunas, cuja entrada i, j é dada por

$$Q_{ij} = \begin{cases} 1, & v_i \text{ e } v_j \text{ são adjacentes} \\ 0, & v_i \text{ e } v_j \text{ não são adjacentes} \end{cases}, \text{ para } i \neq j, \quad \text{e} \quad Q_{ii} = \begin{cases} 0, & v_i \text{ não tem lacete} \\ 2, & v_i \text{ tem lacete} \end{cases}$$

(como antes, a terceira opção só interessa em pseudo-grafos). Finalmente, a Matriz de Valência (ou Matriz de Grau) é a matriz quadrada diagonal $D = D_G$, com n linhas e colunas, dada por

$$D_{ii} = d_{v_i} \quad (\text{e } D_{ij} = 0, \text{ se } i \neq j).$$

Designamos por A^{t} a transposta da matriz A.

Proposição 11.9. *As matrizes de incidência, adjacência e valência verificam a igualdade matricial*

$$M \cdot M^{\mathsf{t}} = Q + D$$

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 incidentes, 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 $Q_{ij} + D_{ij}$ como queriamos provar.

Deixamos o caso de pseudo-grafos como exercício. □

Teorema 11.10. *Seja G um grafo (ou pseudo-grafo). A soma dos graus de todos os vértices é igual ao dobro do tamanho de G. Ou seja*

$$\sum_{v \in V} d_v = 2\,|A| \tag{11.1}$$

Demonstração. Novamente, consideremos o caso dos grafos (simples). Vamos somar todas as entradas da matriz M. Cada coluna tem 2 entradas iguais a 1, e todas as outras são zero. Cada linha tem tantos valores 1 quantos o grau do vértice correspondente. Por um lado, somando coluna a coluna, obtemos $2|A|$, uma vez que as colunas correspondem às arestas. Por outro lado, somando linha a linha, obtemos $\sum_{v \in V} d_v$ uma vez que cada linha corresponde a um vértice. O caso de pseudo-grafos é semelhante. □

Corolário 11.11. *Em qualquer grafo (ou pseudo-grafo) o número de vértices de grau ímpar é par.*

Demonstração. Basta considerar a igualdade (11.1) 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 11.12. *Seja G 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.*

Como consequência, se tivermos um grupo de pessoas em número ímpar, há sempre pelo menos uma delas que conhece um número par das restantes.

11.2. **Isomorfismos e subgrafos.**

11.3. **Sequências gráficas.** Dado um grafo G com vértices $V = \{v_1, \cdots, v_n\}$ podemos naturalmente cosiderar a sequência de inteiros não negativos

$$d_1, d_2, \cdots, d_n,$$

onde d_i é o grau do vértice v_i, $i \in [n]$. Como não nos interessa a ordem dos índices dos vértices, podemos sempre assumir que esta sucessão é não-crescente:

$$d_1 \geq d_2 \geq \cdots \geq d_n.$$

Uma sequências destas, obtida a partir de um grafo, chama-se uma sequência gráfica. Naturalmente, se dois grafos são isomorfos, então têm a mesma sequência gráfica. Mas podemos perguntar-nos: dada uma sequência não-crescente de números inteiros, será que é uma sequência gráfica? Por outras palavras, será que existe um grafo G tal que os graus dos seus vértices sejam os números da sequência dada?

Proposição 11.13. *Seja $d_1 \geq d_2 \geq \cdots \geq d_n$ uma sequência gráfica. Então temos:*

(1) $\sum_{i=1}^{n} d_i$ *é par,*
(2) $d_1 < n$
(3) $\sum_{i=1}^{n} d_i < n(n-1)$.

Demonstração. Seja G um grafo com essa sequência de graus. (1) Já foi visto. Para ver (2) e (3) consideramos que G é subgrafo do grafo completo K_n. Como K_n é $(n-1)$-regular e tem $\binom{n}{2} = \frac{n(n-1)}{2}$ arestas, temos $d_v \leq n-1$ para qualquer $v \in V_G$ e $2|A_G| \leq n(n-1)$ pelo que (3) segue do Teorema 11.10. □

Observação 11.14. Se quisermos obter um multigrafo, nem todas as restrições acima se têm que verificar. De facto, para qualquer sequência que verifique a condição (1), existe um multigrafo que a realiza.

Proposição 11.15. *Considere a sequência*

$$d_0 = \Delta \geq d_1 \geq d_2 \geq \cdots \geq d_n.$$

Esta sequência é gráfica se e só se uma ordenação dos números

$$d_1 - 1,\, d_2 - 1, \cdots,\, d_\Delta - 1,\, d_{\Delta+1}, \cdots, d_n$$

também for gráfica.

Demonstração. Supondo que $d_1 - 1 \geq d_2 - 1 \geq \cdots \geq d_\Delta - 1 \geq d_{\Delta+1} \geq \cdots \geq d_n$ é gráfica, então juntamos o vértice v_0, com grau Δ e obtemos um grafo com $n+1$ vértices e a sequência gráfica de cima. Caso a de cima seja gráfica, aplicamos o processo inverso, removendo o primeiro vértice. □

11.4. **Problemas de Revisão.**

(1) Sejam M, Q e D as matrizes de incidência, adjacência e grau de um pesudo-grafo G. Mostre que $M \cdot M^{\mathtt{t}} = Q + D$ e que $\sum_{i,j} M_{ij} = 2|A_G|$.
(2) Desenhe o grafo que tem a seguinte matriz de incidência. Qual o seu número de componentes conexas?
(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.
(4) Determine todos os grafos conexos com 4 vértices, a menos de isomorfismo.
(5) 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.
(6) Seja K_n o grafo completo com n vértices e seja v_0 um deles. Quantos caminhos diferentes têm v_0 como caminho final?
(7) Mostre que, se G e $\bar{G}$ são isomorfos, então a ordem de G, $n = |V_G|$ verifica: $n \equiv 0$ ou $n \equiv 1$ módulo 4.
(8) Seja G um grafo conexo e regular com 22 arestas. Quantos vértices pode ter G? Construa um tal grafo, que não seja um ciclo.
(9) 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?

12. Caminhos e Conexidade

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.

Definição 12.1. Um passeio num grafo (simples) é uma sucessão de vértices $v_0 v_1 \cdots v_n$ em que v_i e v_{i+1} são adjacentes. Nesta sucessão, podemos repetir o mesmo vértice várias vezes. 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 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.

Exemplo 12.2. ...

Definição 12.3. Um grafo diz-se conexo se dados quaisquer dois vértices, existe um passeio que começa num deles e termina no outro.

13. Grafos Planares

14. Árvores

15. Colorações

16. Emparelhamentos

Apêndice A. Raízes e Factorização de Polinómios

No caso de coeficientes reais (e complexos, claro!), a forma mais útil de entender a factorização de polinómios em factores irredutíveis é usando o conceito de *raiz de um polinómio* $p(x)$.

A.1. **Raízes e Factorização de Polinómios Reais.**

Exemplo A.1. Consideremos o polinómio (biquadrático) $p(x) = \frac{1}{3} - \frac{5}{3}x^2 + 2x^4$. A bem conhecida fórmula resolvente para equações do segundo grau, permite-nos escrever

$$p(x) = 0 \quad \Leftrightarrow \quad \frac{1}{3} - \frac{5}{3}x^2 + 2x^4 = 0 \quad \Leftrightarrow \quad x^2 = \frac{1}{4}\left(\frac{5}{3} \pm \sqrt{\frac{25}{9} - \frac{8}{3}}\right) = \frac{1}{4}\left(\frac{5}{3} \pm \frac{1}{3}\right)$$

ou seja as *raizes*, ou soluções de $p(x) = 0$ são dadas por $x^2 = \frac{1}{2}$ ou $x^2 = \frac{1}{3}$. Assim, podemos escrever:

$$p(x) = 2x^4 - \frac{5}{3}x^2 + \frac{1}{3} = 2(x^2 - \frac{1}{2})(x^2 - \frac{1}{3}) = 2(x - \frac{1}{\sqrt{2}})(x + \frac{1}{\sqrt{2}})(x - \frac{1}{\sqrt{3}})(x + \frac{1}{\sqrt{3}}).$$

Este polinómio serve para exemplificar como a factorização em irredutíveis é diferente em $\mathbb{Q}[x]$ e em $\mathbb{R}[x]$. Em $\mathbb{R}[x]$ a última expressão é uma factorização em polinómios mónicos irredutíveis, uma vez que todos os factores têm grau 1 e são mónicos (pelo exercício 7.28(2)). No entanto, estes factores não pertencem a $\mathbb{Q}[x]$ (pois o coeficiente $\frac{1}{\sqrt{3}}$, por exemplo, não é racional), e assim, a factorização em irredutíveis mónicos, no anel $\mathbb{Q}[x]$, garantida pelo Teorema 7.29, é a anterior:

$$p(x) = 2(x^2 - \frac{1}{2})(x^2 - \frac{1}{3}).$$

Voltando à factorização em $\mathbb{R}[x]$, ela foi obtida determinando os zeros do polinómio $p(x)$. Estes zeros são chamados *as raízes* de $p(x)$, e a factorização de polinómios está intimamente ligada com esta noção.

Definição A.2. Uma raiz do polinómio $p(x) \in \mathbb{R}[x]$ é um número complexo z_0, tal que $p(z_0) = 0$. Uma raiz real do polinómio $p(x) \in \mathbb{R}[x]$ é um número real x_0, tal que $p(x_0) = 0$.

Observação A.3. Note-se a diferença entre raiz (possivelmente complexa) e raiz real de um polinómio de coeficientes reais. De facto, nem todos os polinómios em $\mathbb{R}[x]$ têm raízes reais.

Exemplo A.4. Considere $p(x) = x^2 + 1 \in \mathbb{R}[x]$. As raízes de p são os números complexos $z_1 = i$ e $z_2 = -i$ (onde i é a unidade imaginária). Este polinómio não tem raízes reais, e como veremos é irredutível em $\mathbb{R}[x]$. No entanto, se considerarmos que $p(x) = x^2 + 1$ está em $\mathbb{C}[x]$, temos a seguinte factorização em irredutíveis (de $\mathbb{C}[x]$): $x^2 + 1 = (x - i)(x + i)$.

Este exemplo ilustra o que se passa em $\mathbb{C}[x]$: todos os polinómios têm raizes e todos os polinómios irredutíveis têm grau 1. Este enunciado é precisamente o Teorema Fundamental da Álgebra (veja-se o Apêndice). Apesar do caso real não ser assim tão simples como o complexo, vamos continuar a tratar da irredutibilidade em $\mathbb{R}[x]$, pois será usada mais tarde.

Proposição A.5. *Se $\alpha \in \mathbb{R}$ é uma raiz de $p(x) \in \mathbb{R}[x]$, então $(x - \alpha) \mid p(x)$.*

Demonstração. Consideremos a divisão de $p(x)$ por $b(x) := x - \alpha$. Temos

$$p(x) = (x - \alpha)\, q(x) + r(x), \tag{A.1}$$

onde $q(x)$ é o quociente, e $r(x)$ o resto. Pelo algoritmo da divisão, temos $\delta r < 1 = \delta b$, ou seja $r(x) = r \in \mathbb{R}$ é uma constante! A equação (A.1) fica então $r = p(x) - (x - \alpha)\, q(x)$. Substituindo x pela raiz α, e usando a hipótese de que $p(\alpha) = 0$, conclui-se $r = p(\alpha) - 0 \cdot q(\alpha) = 0$. Isto mostra que $p(x) = b(x)q(x)$ e que p é divisível por $b(x) = x - \alpha$. □

O seguinte corolário é imediato.

Corolário A.6. *Se um polinómio $p \in \mathbb{R}[x]$, de grau superior a 1, tem uma raiz real, então não é irredutível.*

Desta forma, para testar a irredutibilidade, podemos começar por tentar encontrar raízes. Segundo este corolário, sabemos que, ao encontrarmos uma raiz real α de $p(x)$, podemos escrever $p(x) = q(x)(x - \alpha)$, o que nos leva a considerar a irredutibilidade, por intermédio das raizes, de $q(x)$, um polinómio real com grau menor que p, e assim sucessivamente. E o que acontece quando p não tem raizes reais?

Proposição A.7. *Seja $p \in \mathbb{R}[x]$ um polinómio. Então, a sua lista de raízes complexas é da forma*

$$\{\alpha_1, \cdots, \alpha_m, w_1, \bar{w_1}, \cdots, w_k, \bar{w_k}\}$$

onde $\alpha_i \in \mathbb{R}$ e $w_i \in \mathbb{C} \setminus \mathbb{R}$. Dito de outra forma, sempre que um número, não real, w_i aparece na lista das raízes, então também aparece o seu conjugado $\bar{w_i}$.

Demonstração. Seja $p(x) = a_0 + \cdots + a_n x^n \in \mathbb{R}[x]$, com $n = \delta p$ e $a_i \in \mathbb{R}$ para todo $i = 1, \cdots, n$ ($a_n \neq 0$). Então $p(x) \in \mathbb{C}[x]$. Usando o teorema fundamental da Álgebra podemos factorizar $p(x)$ como produto de factores irredutíveis, todos de grau 1, com coeficientes complexos. Sem perda de generalidade podemos escrever:

$$p(x) = a_0 + \cdots + a_n x^n \ = \ c \cdot (x - z_1) \cdots (z - z_n)$$

onde $c \in \mathbb{C} \setminus \{0\}$ e todos os z_i são números complexos (não necessariamente distintos). Obviamente $p(z_i) = 0$ para todo $i = 1, \cdots, n$. Sendo $\bar{z_1}$ o número complexo conjugado a z_1, vemos que

$$p(\bar{z_i}) = a_0 + a_1\bar{z_i} + \cdots + a_n\bar{z_i}^n = \bar{a_0} + \overline{a_1 z_i} + \cdots + \overline{a_n z_i^n} = \overline{p(z_i)} = \bar{0} = 0.$$

Assim, qualquer conjugado de uma raiz é uma raiz, como queriamos provar. □

Proposição A.8. *Seja $p \in \mathbb{R}[x]$ um polinómio irredutível mónico. Então, $p(x) = x - \alpha$ com $\alpha \in \mathbb{R}$, ou $p(x) = x^2 + bx + c$ com $b, c \in \mathbb{R}$ e $b^2 - 4c < 0$.*

Demonstração. Vamos supor que p tem grau superior a 2. □

No segundo caso, de acordo com a fórmula resolvente da equação do segundo grau, não há raizes reais.

Proposição A.9. *Sejam $p, q \in \mathbb{R}[x]$. Se as raizes de p e q são disjuntas (como números complexos), então p e q são polinómios primos entre si.*

Demonstração. Na hipótese da proposição, os factores irredutíveis de p e q são diferentes. Ou seja, nenhum factor irredutível de p é factor de q, e vice-versa. Assim, de acordo com o Teorema ..., o máximo divisor comum mónico entre p e q é 1. □

A demonstração do seguinte resultado é um pouco longa, e envolve a consideração de alguma análise complexa, pelo que não será aqui feita.

Teorema A.10. *Seja $p(x) \in \mathbb{R}[x]$. Sejam $x_1, \cdots, x_m$ as suas raizes reais distintas, e $z_1 = a_1 \pm ib_1, \cdots, z_n = a_n \pm ib_n$ as suas raizes complexas distintas (que ocorrem aos pares). Então $\delta p \geq m + 2n$ e a factorização de $p(x)$ em polinómios mónicos irredutíveis é dada por*

$$p(x) = c\,(x - x_1)^{k_1} \cdots (x - x_m)^{k_m} (x^2 - 2a_1 x + |z_1|^2)^{l_1} \cdots (x^2 - 2a_n x + |z_n|^2)^{l_n},$$

para certos naturais $k_1, \cdots, k_m, l_1, \cdots, l_n$.

Apêndice A. O Teorema fundamental da Álgebra

O resultado mais importante sobre polinómios de váriavel complexa é o chamado teorema fundamental da álgebra, que afirma que qualquer polinómio não constante possui uma raíz em $\mathbb{C}$.

Teorema A.1. *[Gauss] Qualquer polinómio complexo não constante tem uma raíz complexa. Por outras palavras, dado um polinómio de grau $n \geq 1$, $p(z) = a_0 + a_1 z + ... + a_n z^n$, existe $z_0 \in \mathbb{C}$ tal que $p(z_0) = 0$.*

Para provar este teorema vamos usar duas propriedades simples dos polinómios: o facto de serem ilimitados e verificarem os princípios do módulo máximo e mínimo.

A.1. **Polinómios não constantes são ilimitados.** É intuitivo que os polinómios não constantes são ilimitados, pois este facto verifica-se para os polinómios com coeficientes reais, com os quais o leitor poderá estar familiarizado.

Para mostrar esta propriedade de forma rigorosa, precisamos de usar os conceitos de limite e de continuidade. Seja $f : \mathbb{C} \to \mathbb{C}$ uma função complexa de variável complexa. Diz-se que $f(z)$ tende para zero (resp. ∞) quando z tende para ∞ se, para todo $\alpha > 0$ existe $R > 0$ tal que

$$|f(z)| < \alpha, \text{ (resp. } |f(z)| > \alpha) \quad \forall z \text{ tal que } |z| > R.$$

Para expressar o conceito de função (i)limitada usa-se o módulo de números complexos.

Lema A.2. *Se $p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$ é um polinómio de grau $n > 0$, então $|p(z)| \to \infty$ quando $|z| \to \infty$.*

Demonstração. Para mostrar que $|p(z)|$ é tão grande como se queira, usa-se a desigualdade triangular, e o facto de que a função $\frac{a_{n-1}}{z} + \cdots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n}$ tende para zero quando $z \to \infty$. Mais precisamente, existe um $R > 0$ tal que $|\frac{a_{n-1}}{z} + \cdots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n}| < \frac{|a_n|}{2}$, sempre que $|z| > R$ (note-se que $a_n \neq 0$). Assim, temos:

$$\begin{aligned} |p(z)| &= |z^n| \left| a_n + \frac{a_{n-1}}{z} + \cdots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n} \right| \geq |z^n| \left(|a_n| - \left| \frac{a_{n-1}}{z} + \cdots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n} \right| \right) \geq \\ &\geq |z^n| \left(|a_n| - \frac{1}{2}|a_n| \right) = \frac{1}{2}|a_n||z|^n \text{ para todo o } z \text{ tal que } |z| > R. \end{aligned}$$

Isto é suficiente para concluir o pretendido. □

Uma função $f : \mathbb{C} \to \mathbb{C}$ diz-se limitada se existir $M > 0$ tal que $|f(z)| \leq M$ para todo o $z \in \mathbb{C}$. A mesma função diz-se ilimitada se não for limitada. Assim, este lema pode ser reescrito na seguinte forma.

Corolário A.3. *Se $p(z)$ é um polinómio limitado então ele é constante.*

A.2. **Princípios do módulo máximo e mínimo para polinómios.** Os polinómios verificam também os princípios do módulo máximo e do módulo mínimo, outra propriedade que embora seja simples de demonstrar, já não é tão intuitiva, dado que não é válida para os polinómios reais.

Definição A.4. Seja Ω uma região. Dizemos que uma função $h : \Omega \to \mathbb{R}$, tem um máximo (resp. mínimo) local em $z_0 \in \Omega$, se existe uma vizinhança $V \subset \Omega$ de z_0 tal que $h(z_0) \geq h(z)$ (resp. $h(z_0) \leq h(z)$) para todo $z \in V$.

Proposição A.5. *Dado um polinómio não constante p, a função $h(z) := |p(z)|$, $h : \mathbb{C} \to \mathbb{R}$ não tem máximos locais, e não tem mínimos locais em pontos z_0 onde $p(z_0) \neq 0$.*

Demonstração. Podemos supor, sem perda de generalidade, que o máximo ou mínimo local é atingido em $z_0 = 0$ (porque se $|p(z)|$ tem máximo/mínimo em z_0 então $|p(z + z_0)|$ tem máximo/mínimo em 0). Assim, seja $p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_m z^m + a_0$, $a_k = |a_k| e^{i\alpha_k}$ (onde a_m, $0 < m \leq n$, é o primeiro coeficiente não nulo a seguir ao a_0) e $z = re^{i\theta}$. O caso $m = n$, sendo mais simples, é deixado ao leitor. Supondo $m < n$, dado que $a_{m+1} z + \cdots + a_n z^{n-m}$ tende para zero quando $z \to 0$, existe um certo $\varepsilon > 0$ tal que $|a_{m+1} z + \cdots + a_n z^{n-m}| < |a_m|$ para todo z com $|z| < \varepsilon$. Isto equivale a ter $|a_{m+1} z^{m+1} + \cdots + a_n z^n| < |a_m z^m|$ sempre que $0 < |z| < \varepsilon$.

Esta desigualdade permite provar ambos os princípios, pelo que vamos somente deduzir o princípio do mínimo. Assim, para $0 < |z| < \varepsilon$, e assumindo $a_0 \neq 0$,

$$\begin{aligned}
&|a_0 + a_m z^m + a_{m+1} z^{m+1} + \cdots + a_n z^n| \leq |a_0 + a_m z^m| + |a_{m+1} z^{m+1} + \cdots + a_n z^n| < \\
&< |a_0 + a_m z^m| + |a_m z^m| = \left| |a_0| e^{i\alpha_0} + |a_m| r^m e^{i\alpha_m} e^{mi\theta} \right| + |a_m z^m| = \\
&= |a_0| - |a_m| r^m + |a_m| r^m = |a_0| = |p(z_0)|
\end{aligned}$$

desde que agora tomemos θ de tal modo a que $\alpha_0 = \alpha_m + m\theta + \pi$. Assim, em qualquer vizinhança de 0, $|p(z)|$ não atinge um mínimo, a menos que $a_0 = 0$. Neste último caso o ponto $z_0 = 0$ é uma raíz de $p(z)$. Assim, a função $|p(z)|$ não tem mínimos locais, excepto nas raízes de $p(z)$. □

Como consequência destes princípios, vemos que, para qualquer polinómio não constante, a função $h(z) = |p(z)|$ não apresenta nenhum máximo em nenhuma região $\Omega \subset \mathbb{C}$, e só apresenta mínimos quando essa região contém uma ou mais raízes de $p(z)$. Por outro lado, o importante teorema de Weierstrass diz-nos que funções contínuas têm máximos e mínimos em conjuntos compactos.

Teorema A.6. *(Weierstrass) Seja $h : \mathbb{C} \to \mathbb{R}$ uma função contínua e $D \subset \mathbb{C}$ um disco fechado. Então f atinge máximo e mínimo em D.*

Demonstração. Vamos provar primeiro que a imagem $h(D)$ é um conjunto limitado em $\mathbb{R}$.

Note-se que eualquer função contínua $h : \mathbb{C} \to \mathbb{R}$ é *localmente limitada*. Ou seja, dado $z_0 \in \mathbb{C}$, e um real positivo ε, existe uma vizinhança U de z_0 na qual temos:

$$|h(z) - h(z_0)| < \varepsilon \quad \Rightarrow |h(z)| < |h(z_0)| + \varepsilon, \quad \forall z \in U.$$

Vamos supor que f não é (globalmente) limitada em D, ou seja que $\forall M > 0$ existe $z \in D$ tal que $|h(z)| > M$. Vamos dividir sucessivamente o conjunto D em conjuntos fechados, cada vez menores, utilizando rectas horizontais ou verticais que passam no interior de D. No primeiro passo, escrevemos $D = A_1 \cup B_1$ onde A_1 e B_1 são subconjuntos fechados não vazios de D separados por uma recta vertical. Como $h(D)$ não é limitada, h não é limitada num dos conjuntos A_1 ou B_1, pelo que podemos assumir que $h(A_1)$ não é limitada, existindo um ponto $z_1 \in A_1$. Dividimos então $A_1 = A_2 \cup B_2$ por outra recta, desta vez horizontal, passando pelo interior de A_1 e supomos, sem perda de generalidade que $h(A_2)$ é ilimitada, pelo que existe $z_2 \in A_2$. Procedendo desta forma, construimos uma sucessão $\{z_n\}_{n\in\mathbb{N}}$ com $z_n \in A_n$.

A sucessão z_n forçosamente converge para um ponto z_∞ em $\mathbb{C}$, porque tanto as partes reais como as partes imaginárias de z_n pertencem a intervalos sucessivamente menores de $\mathbb{R}$. Por outro lado, como D é um conjunto fechado, D contém os pontos limite de sucessões em D, pelo que $z_n \to z_\infty \in D$. Por construção, para qualquer vizinhança U de z_∞, temos $A_N \subset U$ para N suficientemente grande. Como f é ilimitada em A_N, mas é limitada em U pelo argumento anterior de limitação local, obtemos uma contradição.

Agora mostramos que $f(D)$ tem máximo e mínimo. Vamos supor que não tem mínimo. Pelo axima do ínfimo, sabemos que existe $m = \inf_{z\in D}\{f(z)\}$. Vamos supor que este

mínimo não é atingido, ou seja $f(z) > m$ para todo o $z \in D$. Assim, a função

$$g(z) = \frac{1}{f(z) - m}$$

é contínua, e pelo argumento anterior, estando definida em todo o D, ela é limitada em D. Temos então $|g(z)| < M$ para certo $M > 0$. Ou seja,

$$|f(z) - m| > \frac{1}{M},$$

o que nos diz que os valores de $f(z)$ não se aproximam do ínfimo m, o que contradiz a definição de ínfimo. Assim, f tem mínimo em D, e a demonstração para o máximo é semelhante. □

Observação A.7. O teorema de Weierstrass é válido para qualquer conjunto compacto (ou seja, limitado e fechado, não apenas discos) contido em qualquer espaço euclideano $\mathbb{R}^n$ ou $\mathbb{C}^n$.

Este teorema tem o seguinte corolário, cuja demonstração se deixa ao leitor (note-se que um polinómio é uma função contínua).

Corolário A.8. *Se $p(z)$ é um polinómio não constante, e $K \subset \mathbb{C}$ é um subconjunto compacto, então os máximos da função $h(z) = |p(z)|$ (restringida a K) encontram-se na fronteira ∂K de K; os mínimos de h encontram-se também em ∂K quando $p(z)$ não tem raízes no interior de K.*

A.3. **Demonstração do Teorema Fundamental da Álgebra.** Podemos agora provar o teorema fundamental da álgebra, que foi demonstrado por primeira vez por Gauss:

Teorema A.9. *Qualquer polinómio não constante possui pelo menos uma raíz em $\mathbb{C}$.*

Demonstração. De acordo com o Lema A.2, seja R tal que $|p(z)| > |a_0|$, sempre que $|z| \geq R$. Assim, se por exemplo considerarmos o disco fechado $\overline{\mathbb{D}(R)}$, sabemos, pelo teorema de Weierstrass que a função *contínua* $h(z) = |p(z)| : \mathbb{C} \to \mathbb{R}$, tem um mínimo em $\overline{\mathbb{D}(R)}$. Este mínimo não está na circunferência fronteira, porque $|p(z)| > |a_0| = |p(0)|$, sempre que $z \in C(R)$. Assim, o mínimo estará no interior do disco, o que pelo princípio do mínimo (Proposição A.5), implica que existe um z_0, tal que $p(z_0) = 0$. □

Referências