INTRODUÇÃO À TEORIA DOS NÚMEROS

Vítor Neves

****

Departamento de Matemática

Universidade de Aveiro

2001

Introdução

O presente texto resulta da evolução de um conjunto de notas de apoio à disciplina **Introdução à Teoria dos Números** do segundo semestre do terceiro ano da licenciatura em *Ensino de Matemática*da Universidade de Aveiro.

Parafraseando um mestre, não pretendemos "escrever para autodidatas, mas sim para alunos com professor", pelo que deixámos para o leitor demonstrar – por vezes explicitamente como exercício – o que é manifestamente rotineiro (não necessariamente trivial...) ou nos parece estar fora do âmbito de um primeiro curso sobre Teoria dos Números.

Não sendo especialistas, limitamo-nos a aspectos clássicos e elementares da Teoria, de carácter mais formativo e menos técnico: a orientação foi de facto muito forte no sentido de preparar docentes para o ensino secundário.

O capítulo sobre extensões do corpo dos números reais (Cap. 8) pretende recuperar o estudo das construções do corpo real e suas extensões mais importantes, que deixou de se fazer sistematicamente nas licenciaturas, mas continua a ser importante se se pretende aprofundar o conceito de Número. As extensões não arquimedianas são afloradas de modo a alertar para a sua existência e onde podem ser estudadas.

A finalidade principal do texto – apoiar uma disciplina semestral – obrigou a escolhas não muito agradáveis: por questões de tempo não se tem mostrado razoável tratar cuidadosamente a equação de Pell, aspectos de Teoria Analítica, aproximação por fracções contínuas, raízes primitivas, critérios de primalidade ou Teoria Combinatória. Tais assuntos poderiam ser abordados se a filosofia subjacente a este texto se modificasse; mesmo assim, nem toda a matéria aqui descrita tem sido trabalhada durante o semestre nas aulas teóricas ou teórico-práticas.

Utilizamos um mínimo de Álgebra, de modo a construir um texto tão independente quanto possível.

Os saltos na numeração das páginas são um expediente de organização tipográfica incompleta: podem incluir-se sempre mais páginas alterando muito pouco as referências de edição para edição.

Agradecemos aos Mestres Paulo Almeida e Rui Duarte e à Doutora Ana Foulquié a leitura cuidada das várias versões preliminares destas notas bem como as sugestões que apresentaram.

NOTAÇÃO

Salvo referência em contrário, variáveis representadas por letras minúsculas designam números inteiros.

Aveiro

Maio de 2001

Vítor Neves

Índice

Parte I

Introdução à Teoria dos Números

Capítulo 1

Teorema Fundamental da Aritmética

1.1 Números Naturais

Se bem que se suponham conhecidas as propriedades algébricas elementares dos conjuntos de números naturais, inteiros, racionais, reais e complexos, vamos enunciar propriedades básicas dos números naturais que serão demonstradas e utilizadas mais tarde numa construção de outros conjuntos de números.

1.1.1 Axiomática de Peano

Uma *estrutura de números naturais* é um terno $\mathcal{N} =\prec \mathbf{N}, S, \mathbf{1} \succ$ satisfazendo as seguintes condições:

N1) $\mathbf{N}$ é um conjunto não vazio

N2) S é uma função injectiva de $\mathbf{N}$ em $\mathbf{N}$.

N3) Existe um elemento de $\mathbf{N}$, designado por $\mathbf{1}$, que não é imagem por S, isto é, $S : \mathbf{N} \to \mathbf{N}\backslash\{\mathbf{1}\}$.

N4) Princípio de Indução.

Se $\mathbf{1} \in A \subseteq \mathbf{N}$ e $S(n) \in A$ sempre que $n \in A$, então $A = \mathbf{N}$.

Um elemento $S(n)$ designa-se por *sucessor de* n, a condição N3 estabelece que $\mathbf{1}$ *não é sucessor* e, de acordo com a condição N2, *dois elementos de* $\mathbf{N}$ *são iguais sse têm o mesmo sucessor.*

Explorando as propriedades das estruturas de números naturais:

Teorema 1.1.1 *Qualquer elemento de* $\mathbf{N}\backslash\{\mathbf{1}\}$ *é sucessor.*

Por outras palavras: $\mathbf{1}$ *é o único elemento de* $\mathbf{N}$ *que não é sucessor.*

Dem. Defina-se $A = \{\mathbf{1}\} \cup S(\mathbf{N}) = \{\mathbf{1}\} \cup \{S(n) : \ n \in \mathbf{N}\}$. Por definição de A, não só $\mathbf{1} \in A$ mas também $S(n) \in A$ seja qual for $n \in \mathbf{N}$, em particular o mesmo acontece se $n \in A$. Pelo Princípio de Indução, $A = \mathbf{N}$, ou seja, o contradomínio $S(\mathbf{N})$ de S é $\mathbf{N}\backslash\{\mathbf{1}\}$, em virtude de N3. □

Pode também demonstrar-se que

Teorema 1.1.2 *Todas as estruturas de números naturais são isomorfas*

Dem. As condições

$$\begin{cases} \mathbf{I}(\mathbf{1}_1) = \mathbf{1}_2 \\ \\ \mathbf{I}(S_1(x)) = S_2(\mathbf{I}(x)) \quad \textit{se } x \in \mathbf{N}_1 \end{cases}$$

definem uma função[1] $\mathbf{I} : \mathbf{N}_1 \to \mathbf{N}_2$. O **Princípio de Indução,** o teorema 1.1.1 e o facto de as funções sucessor serem injectivas garantem que $\mathbf{I}$ é um isomorfismo entre as estruturas. □

Em face deste teorema, passaremos a designar os elementos de $\mathbf{N}$ por *números naturais.* No entanto, ainda antes de nos fixarmos nos números naturais intuitivos, verificaremos que a axiomática **N1, N2, N3** é suficiente para definir a Aritmética e ordenar adequadamente a estrutura.

1.1.2 Soma, ordem e produto

Seja $\mathcal{N} =\prec \mathbf{N}, S, \mathbf{1} \succ$ uma estrutura de números naturais.

Definição 1.1.1 *A* **soma** *de dois números naturais* m *e* n *designa-se por* $m + n$ *e define-se recursivamente do seguinte modo*[2]*:*

$$\begin{cases} m + \mathbf{1} = S(m) & (m \in \mathbf{N}) \\ m + S(n) = S(m + n) & (m, n \in \mathbf{N}) \end{cases} \tag{1.1}$$

[1] Veja-se o **Teorema de Recursão** em [8, pp 39 e seg.]
[2] Idem nota 1

Tem-se então

Teorema 1.1.3 *Para quaisquer* $m, n \in \mathbf{N}$ *a soma* $m + n$ *está definida e* $\prec \mathbf{N}, + \succ$ *é um semigrupo comutativo que verifica a* **Lei do Corte***, isto é, a condição seguinte*

$$\forall m, n, p \in \mathbf{N} \quad m + p = n + p \Rightarrow m = n. \tag{1.2}$$

Dem. Esquematizamos apenas uma demonstração da Lei do Corte. Defina-se para cada $m, n \in \mathbf{N}$

$$A_{mn} = \{p \in \mathbf{N} : \ m + p = n + p \Rightarrow m = n\}$$

Tem-se $\mathbf{1} \in A_{mn}$ pela definição de soma e pelo axioma **N2**. Se $p \in A_{mn}$ tem-se

$$m + S(p) = n + S(p) \quad sse \quad S(m + p) = S(n + p) \quad sse \quad m + p = n + p \quad sse \quad m = n$$

respectivamente por (1.1), por S ser injectiva (N2) e porque $p \in A_{mn}$. Mas então

$$\mathbf{1} \in A_{mn} \quad \& \quad p \in A_{mn} \Rightarrow S(p) \in A_{mn} \quad (p \in \mathbf{N})$$

Pelo Princípio de Indução $A_{mn} = \mathbf{N}$. □

Há uma forma frequentemente mais conveniente de enunciar o **Princípio de Indução,** a saber:

Teorema 1.1.4 *Se* $A \subseteq \mathbf{N}$, $\mathbf{1} \in A$ *e* $n + 1 \in A$ *sempre que* $n \in A$*, então* $A = \mathbf{N}$*.*

A ordenação de $\mathbf{N}$ pode fazer-se à custa da soma.

O número natural m diz-se **menor que** o número natural n — escrevendo-se $m < n$ — se existir $p \in \mathbf{N}$ tal que $n = m + p$.

Teorema 1.1.5 *1.* $\mathbf{1} < n$*, seja qual for* $n \in \mathbf{N} \backslash \{\mathbf{1}\}$*.*

2. $\mathbf{N}$ *não tem máximo.*

3. A relação $<$ *é de ordem total estrita em* $\mathbf{N}$*, ou seja, é transitiva e para quaisquer* $m, n \in \mathbf{N}$*, dá-se uma e só uma das seguintes condições*

$$m = n \quad ou \quad m < n \quad ou \quad n < m.$$

4. Todo o subconjunto não vazio de $\mathbf{N}$ *tem mínimo para* $<$*.*

Em virtude das partes 3 e 4 deste teorema diz-se que $\mathbf{N}$ é **bem ordenado** por $<$.

A relação de ordem permite um novo enunciado do Princípio de Indução.

Teorema 1.1.6 Princípio de Indução Completa *Se* A *é um subconjunto de* $\mathbb{N}$ *tal que, seja qual for* $n \in \mathbb{N}$*,* $n \in A$ *sempre que* $\{k \in \mathbb{N} : \ k < n\} \subseteq A$*, então* $A = \mathbb{N}$*.*

Este enunciado é de facto equivalente ao axioma **N4** e ao teorema 1.1.4 em estruturas de números naturais, mas não em conjuntos bem ordenados quaisquer.

E passamos à definição do produto.

Definição 1.1.2 *O* **produto** *dos números naturais m e n, nota-se $m \cdot n$ e define-se recursivamente*[3] *por*

$$\begin{cases} m \cdot \mathbf{1} = m & (m \in \mathbf{N}) \\ m \cdot (n+1) = m \cdot n + m & (m, n \in \mathbf{N}) \end{cases} \tag{1.3}$$

Como habitualmente, a notação simplifica-se pondo

$$m \cdot n = mn \qquad (m, n \in \mathbf{N}).$$

Nestes termos vem

Teorema 1.1.7 *Para quaisquer $m, n \in \mathbf{N}$ o produto mn está bem definido e $\prec \mathbf{N}, \cdot \succ$ é um semigrupo comutativo com* elemento neutro **1** *que verifica a* **Lei do Corte**, *isto é, a condição seguinte*

$$\forall m, n, p \in \mathbf{N} \quad mp = np \Rightarrow m = n. \tag{1.4}$$

Retomando o teorema 1.1.2, pode acrescentar-se que

Teorema 1.1.8 *A aplicação* **I** *do teorema 1.1.2 respeita a soma, o produto e a ordem, isto é, se $+_i, \cdot_i, <_i$ designam respectivamente a soma, o produto e a ordem sobre $\mathbf{N}_i$ $(i = 1, 2)$, então, para quaiquer $m, n \in \mathbf{N}_1$,*

1. $\mathbf{I}(m +_1 n) = \mathbf{I}(m) +_2 \mathbf{I}(n)$
2. $\mathbf{I}(m \cdot_1 n) = \mathbf{I}(m) \cdot_2 \mathbf{I}(n)$
3. $\mathbf{I}(m) <_2 \mathbf{I}(n) \quad sse \quad m <_1 n$

Este teorema dá-nos mais uma razão para nos limitarmos a estudar como estrutura de números naturais o terno $\prec \mathbb{N}, S, 1 \succ$, onde $\mathbb{N}$ designa o conjunto dos **números naturais intuitivos** 1,2,3,... com a respectiva soma $+$, ordem $<$ e produto $\times$ usuais, sendo $S(n) = n + 1$.

Os teoremas de extensão de semigrupos (ordenados) que verificam a lei do corte por grupos (ordenados) e de domínios de integridade (ordenados) por corpos (ordenados) permitem várias construções de anéis de Números Inteiros e de corpos de Números Racionais a partir das estruturas de Números Naturais. Algumas destas construções, bem como o estudo do corpo dos Números Reais e suas extensões, serão tratadas mais tarde (parte II).

Terminamos esta secção com uma das propriedades mais importantes de $\mathbb{N}$. Recorde-se que $\leq$ designa a relação de ordem lata associada a $<$, i.e., $a \leq b$ se e só se $a < b$ ou $a = b$.

[3] Idem nota 1

Teorema 1.1.9 Propriedade Arquimediana *Para quaisquer $a, b \in \mathbb{N}$, existe $x \in \mathbb{N}$ tal que $a < xb$.*

Dem. Tome-se $a \in \mathbb{N}$. Seja

$$A = \{b \in \mathbb{N} |\ a \leq b \ ou\ [b < a\ \&\ \exists x \in \mathbb{N}\ a < xb]\}.$$

Em primeiro lugar $\mathbf{1} \in A$ pois, ou $a = \mathbf{1}$ ou $\mathbf{1} < a$, mas pelo teorema 1.1.5, existe $x \in \mathbb{N}$ tal que $a < x = x\mathbf{1}$.

Suponha-se agora que $b \in A$: se $a \leq b$ também $a \leq b + \mathbf{1}$ e $b + \mathbf{1} \in A$. Se $b < a$, ou $b + \mathbf{1} = a$ e, de novo $b + \mathbf{1} \in A$, ou $b + \mathbf{1} < a$; em qualquer caso, por hipótese, para certo $x \in \mathbb{N}$ tem-se $a < xb < xb + x = x(b + \mathbf{1})$ e consequentemente, $b + \mathbf{1} \in A$.

Pelo Princípio de Indução $A = \mathbb{N}$. □

1.2 Aritmética

1.2.1 O máximo divisor comum

Teorema 1.2.1 (Algoritmo de Euclides) *Para quaisquer a e b, se $a > 0$ existem números inteiros únicos d e r tais que*

$$b \ = \ da \ + \ r \quad \& \quad 0 \leq \ r \ < \ a \tag{1.5}$$

Dem.

Unicidade

Fixe-se $a > 0$. Suponha-se que $da + r = d'a + r' \ \ \& \ \ 0 \leq r, r' < a$. Tem-se

$$(d - d')a \ = \ r' - r \quad \& \quad |r' - r| \ < \ a$$

Se $d \neq d'$ então $1 \leq |d - d'|$ e vem

$$a \ \leq \ |d - d'|a \ = |r' - r| \ < \ a$$

o que é impossível. Portanto $d = d'$ e também $r = r'$.

Existência

Se $0 \leq b < a$ tem-se $b = 0a + b$ e pode fazer-se $d = 0$ & $r = b$. Se $a < b$, pelo teorema 1.1.9, existe $x \in \mathbb{N}$ tal que $b < xa$. Tome-se

$$d \ = \ min\{x \in \mathbb{N} |\ b < xa\} - 1 \quad \& \quad r \ = \ b - da$$

Se $b < 0$, pelo que acabámos de ver, existem $d_1 \in \mathbb{N}$ e $r_1 \in \mathbb{N}$, sendo $0 \leq r_1 < a$, tais que $-b = d_1 a + r_1$; tome-se $d = -d_1 - 1$ e $r = a - r_1$. □

Um corolário de fácil demonstração:

Corolário 1.2.1 *Para quaisquer números inteiros a, b, se $a \neq 0$ existem $d, r \in \mathbb{Z}$ únicos tais que*

$$b \;=\; da \;+r \qquad \& \qquad 0 \leq r < |a|$$

Dem. Aplique-se o teorema anterior 1.2.1 a $|b|$ e $|a|$ e ajuste-se adequadamente. □

Os números d e r das proposições anteriores designam-se respectivamente por *cociente* e *resto* da divisão de b por a.

Definição 1.2.1 *Dado $a \neq 0$, b é* **divisível por** *a (ou a* **divide** *b ou a é* **divisor** *de b ou b é* **múltiplo** *de a) se o resto da divisão de b por a é zero. Nota-se $a \mid b$ se a divide b.*

Repare-se que *zero é divisível por qualquer número inteiro,* no sentido em que *para qualquer $a \in \mathbb{Z}$, existe $d \in \mathbb{Z}$ tal que $0 = da$, nomeadamente $d = 0$;* não se define o cociente de zero por zero

Proposição 1.2.1 *A relação $\cdot|\cdot$ em $\mathbb{Z}$ é reflexiva e transitiva, mas não é anti-simétrica pois*

$$a \mid b \;\;\&\;\; b \mid a \quad \Leftrightarrow \quad |a| \;=\; |b| \tag{1.6}$$

Dem. Demonstramos apenas a equivalência 1.6, no caso em que $a \neq 0 \neq b$.

Suponha-se que $b = ad \;\&\; a = bd'$. Tem-se $a \;=\; add'$ donde $dd' = 1$. Segue-se que $d = d' = 1$, caso em que $a = b$, ou $d = d' = -1$, caso em que $a = -b$. □

Mais algumas propriedades importantes, cuja demonstração fica ao cuidado do leitor.

Teorema 1.2.2 *Para quaisquer $a, b, c \in \mathbb{Z}$,*

1. $[a \mid b \;\;\&\;\; a \mid c] \;\Rightarrow \forall x, y \;\; a \mid (bx + cy)$;
2. *em particular* $a \mid b \;\Rightarrow\; \forall x \;\; a \mid bx$.
3. $[0 < a \;\;\&\;\; 0 < b \;\&\; a \mid b] \;\Rightarrow a \leq b$.

A alínea 1. do teorema anterior é de facto equivalente a qualquer das alíneas do corolário seguinte.

Corolário 1.2.2 *Para quaisquer $a, b, c, x, y \in \mathbb{Z}$*

1. $[a \mid b \;\;\&\;\; a \not| (bx + cy)] \;\Rightarrow\; a \not| c$.
2. $[a \mid b \;\;\&\;\; a \mid (bx + c)] \;\Rightarrow\; a \mid c$.

Definição 1.2.2 *O número inteiro d é* **máximo divisor comum** de a e b e designa-se por $mdc(a,b)$, se satisfaz simultâneamente as seguintes condições:

1. $d > 0$
2. $d \mid a \ \ \& \ \ d \mid b$
3. $\forall c \ [[c \mid a \ \ \& \ \ c \mid b] \ \Rightarrow c \mid d]$

Se $mdc(a,b) = 1$ diz-se que *a e b são primos entre si.*

Teorema 1.2.3 *Se $a \neq 0$ ou $b \neq 0$, então*

$$mdc(a,b) \ = \ min\{z = ax + by |\ x, y \in \mathbb{Z} \ \ \& \ \ z > 0\}, \tag{1.7}$$

pelo que o máximo divisor comum de dois números inteiros não simultâneamente nulos existe e é único.

O que, em particular, tem como consequência

Corolário 1.2.3 *Se $d = mdc(a,b)$, então existem $x, y \in \mathbb{Z}$ tais que $d = ax + by$.*

Dem. (Teorema 1.2.3) Seja

$$S \ = \ \{z = ax + by |\ x, y \in \mathbb{Z} \ \ \& \ \ z > 0\}$$

Como $a \neq 0$ ou $b \neq 0$, $S \neq \emptyset$ pois $0 < a^2 + b^2 = aa + bb$; assim S tem mínimo (teorema 1.1.5), digamos $d = min\ S = ax_0 + by_0 > 0$, para certos x_0, y_0; d verifica então a condição 1 da definição.

Vamos ver que $d \mid a$. Ponha-se $a = qd + r$, de acordo com o teorema 1.2.1, sendo $0 \leq r < d$; repare-se que,

$$r \ = \ a - qd \ = \ a(1 - qx_0) + b(-qy_0) \ \in S,$$

portanto, se $r > 0$, r teria de ser maior ou igual ao mínimo de S, o que não é o caso. A troca de a por b neste racicínio, permitiria concluir que $d \mid b$ e a condição 2 da definição também está verificada.

Por outro lado, se $c \mid a \ \ \& \ \ c \mid b$, como $d = ax_0 + by_0$, pelo teorema 1.2.2, $c \mid d$, verificando-se a condição 3.

Quanto à unicidade: utilize-se o que acabámos de ver e a condição 1.6 para concluir que se d' verifica as mesmas condições que d, então $d = d'$. □

Algumas propriedades do máximo divisor comum.

Teorema 1.2.4 *Para quaisquer $a, b \in \mathbb{Z}$*

1. $mdc(a,b) = 1 \quad \Leftrightarrow \quad \exists x, y \; ax + by = 1$
2. $mdc(\frac{a}{mdc(a,b)}, \frac{b}{mdc(a,b)}) = 1$
3. $[a \mid bc \;\; \& \;\; mdc(a,b) = 1] \;\Rightarrow\; a \mid c$
4. $a \mid bc \;\Rightarrow\; \frac{a}{mdc(a,b)} \mid c$
5. $mdc(na, nb) \;=\; n \cdot mdc(a,b) \quad se \quad n > 0.$

Dem. Alínea 1.
($\Rightarrow$) é um caso particular do corolário 1.2.3.
($\Leftarrow$) Como 1 é o menor inteiro positivo, se $1 = ax + by$, necessariamente $1 = min\{z = ax + by |\; x, y \in \mathbb{Z} \;\; \& \;\; z > 0\}$ e consequentemente, $1 = mdc(a,b)$, pelo teorema 1.2.3.

Alínea 2. Observe-se que $d = ax + by$, para certos x, y e divida-se por d em, ambos os membros.

Alínea 3. Como $mdc(a,b) = 1$, para certos x, y, $\; 1 = ax + by$ de onde se segue que $c = acx + bcy$. Como $a \mid bc$, para certo q vem $c = acx + aqy = a(cx + qy)$ e $a \mid c$.

Alínea 4. Esquematicamente:

$$a \mid bc \;\Rightarrow\; bc = qa \;\Rightarrow\; cd = cax + cby = cax + qay = a(cx + qy);$$

ou ainda $c = \frac{a}{d}(cx + qy)$ e $\frac{a}{d} \mid c$.

Alínea 5. Observe-se que se $n > 0$ então $min\{nz |\; z \in A\} = n \cdot minA$. □

1.2.2 Teorema Fundamental da Aritmética

Definição 1.2.3 *Um número inteiro p diz-se* **primo** *se verificar simultâneamente as duas condições*

1. $p > 1$
2. $\forall a \in \mathbb{Z} \quad [a \mid p \;\Rightarrow\; [|a| = p \; ou \; |a| = 1]]$.

Um número que não seja primo nem 1 *diz-se composto.*

A propriedade mais importante dos números primos é talvez a seguinte:

Lema 1.2.1 (de Euclides) *Se p é número primo e $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Dem. Se $p \mid ab$, então, pelo teorema 1.2.4, $\frac{p}{mdc(p,a)} \mid b$; ora se $p \not| a$, como p é primo $mdc(p,a) = 1$, consequentemente $p \mid b$. □

Lema 1.2.2 *Se $n > 1$ e $p = min\{x > 1 |\ x \mid n\}$, então p é primo. Em particular, qualquer número natural maior que 1 tem divisores primos.*

Dem. Ou bem que n é primo e, nesse caso $p = n$, ou bem que não; neste caso n tem divisores maiores que 1 e distintos de si próprio, o mínimo dos quais é p; ora p não pode ter divisores distintos de si próprio e de 1, pois qualquer deles seria um divisor de n, maior que 1 e menor que p, que não existe por definição de p; logo p é primo. □

E passamos a demonstrar o

Teorema 1.2.5 (Fundamental da Aritmética)
Se $n > 1$, existem números primos distintos dois a dois $p_1, \cdots, p_k$ e números naturais $\alpha_1, \cdots, \alpha_k$ de modo que

$$n \ = \ \prod_{i=1}^{k} p_i^{\alpha_i}. \tag{1.8}$$

Esta representação de n é única a menos de uma permutação dos factores.

Dem. Tome-se um número natural n.

I. *Existem números primos $p_1, \cdots, p_m$ tais que $n = \prod_{i=1}^{m} p_i$.*

Dem. Seja $n > 1$. Do lema anterior concluimos que n *tem divisores primos.*

Defina-se uma sequência de números primos da seguinte forma

$$p_1 \ = \ min\{x > 1 |\ x \mid n\} \tag{1.9}$$

$$p_{i+1} \ = \ min\{x > 1 |\ x \left| \frac{n}{\prod_{j=1}^{i} p_j}\right.\} \quad \textit{se existir} \tag{1.10}$$

Repare-se que p_{i+1} só não existe se $\frac{n}{\prod_{j=1}^{i} p_j} = 1$, isto é, se $n = \prod_{j=1}^{i} p_j$, como se pretende verificar que acontece.

Por outro lado, $\prod_{j=1}^{m} p_j \mid n$ desde que existam os p_j definidos como acima (proposição 1.2.1) e, de facto, $\prod_{j=1}^{m} p_j \leq n$.

Observe-se ainda que, sendo os números primos maiores ou iguais a 2, vem

$$2^m \ \leq \ \prod_{j=1}^{m} p_j \leq n.$$

Como $2^m > n$, para m suficientemente grande, concluimos que os números primos p_i são em número finito, em particular, para certo i, p_i existe, mas p_{i+1} não. Como observámos acima, $n = \prod_{j=1}^{i} p_j$.

Não é difícil mostrar que $p_j \leq p_{j+1}$ $(1 \leq j < i)$, pelo que associando da esquerda para a direita primos iguais, se obtém

$$n \ = \ \prod_{i=1}^{k} p_i^{\alpha_i}$$

com bases p_i em ordem crescente.

Resta ver que todos os divisores primos de n foram encontrados. Suponha-se que p é primo e $p \mid n$. Pelo lema 1.2.1, p terá de dividir um dos p_i, sendo portanto um deles. □

Há muitos números primos.

Corolário 1.2.4 (de Euclides) *O conjunto dos números primos é infinito.*

Dem. Vamos ver que, seja qual for o conjunto de números primos $\{p_1, \cdots, p_k\}$ existe um número primo que lhe não pertence.

Dados primos $p_1, \cdots, p_k$, seja $n = p_1 \cdots p_k + 1$. De acordo com o Teorema Fundamental, n terá pelo menos um divisor primo. Ora como nenhum dos p_i divide n, pois $p_i \mid p_1 \cdots p_k$ mas $p_i \not| 1$, esse primo não pode ser um deles. □

Os números primos estão esparsamente distribuidos

Corolário 1.2.5 *Os intervalos entre números primos consecutivos são arbitrariamente grandes.*

Dem. Para qualquer $n \in \mathbb{N}$, a sequência

$$(n+1)! + 2,\ (n+1)! + 3,\ \cdots,\ (n+1)! + (n+1)$$

não contém números primos, pois $k \mid (n+1)! + k$ se $2 \leq k \leq n+1$. □

Onde parar na detecção dos divisores primos de um dado inteiro?

Teorema 1.2.6 *Todo o número composto $n > 0$ tem um divisor primo menor ou igual a $\sqrt{n}$.*

Dem. Se n é composto tem pelo menos dois divisores primos, possivelmente iguais, caso contrário seria primo pelo Teorema Fundamental; se p_1, p_2 são primos que dividem n, algum não é maior que $\sqrt{n}$, pois $p_1, p_2 > \sqrt{n} \Rightarrow n \geq p_1 p_2 > (\sqrt{n})^2 = n$, o que é impossível. □

Um resultado semelhante é o corolário seguinte do lema de Euclides (1.2.1) e do teorema 1.2.2

Teorema 1.2.7 (de Gauss) *O produto de dois números naturais menores que um número primo não é divisível por este último.*

Quanto à distribuição dos números primos, o seguinte teorema é um dos mais importantes de Dirichlet; a sua demonstração é muito difícil e está fora do âmbito do presente texto; o leitor interessado pode encontrar uma demonstração por exemplo em [3], onde todo o capítulo 7 lhe é dedicado.

Teorema 1.2.8 (de Dirichlet) *Se a e b são números naturais primos entre si, a progressão aritmética $(na+b)_{n\in\mathbb{N}}$ tem uma infinidade de termos que são números primos.*

Tendo-se observado que um número primo ímpar é de uma das formas $4k+1$ ou $4k-1$ ($k \in \mathbb{Z}$), uma ligeira adaptação da demonstração do corolário 1.2.4 permite no entanto demonstrar facilmente o seguinte:

Teorema 1.2.9 *Existe uma infinidade de números primos da forma $4k-1$ ($k \in \mathbb{Z}$).*

Dem. Consideremos um conjunto finito de números primos distintos da forma $4k-1$, digamos $C := \{p_1, \cdots, p_n\}$ e defina-se

$$N \;=\; 2^2 p_1 \cdots p_n - 1.$$

Em primeiro lugar observe-se que N é da forma $4k-1$ e maior que qualquer dos elementos de C, portanto se for primo não está em C, i.e., C não contém todos os números primos da forma em estudo; se N for composto e p for um seu divisor primo, então p também não pode ser qualquer dos elementos de C; deixa-se como exercício mostrar que *algum* divisor primo de N é da forma $4k-1$ e, como acabámos de ver, não está em C.

Em suma: C não contém todos os números primos da forma $4k-1$. □

Não é tão simples demonstrar que o teorema anterior vale com $4k+1$ em vez de $4k-1$; fá-lo-emos mais tarde (vide corolário 2.4.3).

1.3 Exercícios

1. Demonstre que a adição e a multiplicação em $\mathbb{N}$ são associativas, são comutativas e verificam a Lei do Corte.

2. Mostre que se $f : \mathbb{N} \to \mathbb{N}$ é estritamente crescente, então para qualquer $n \in \mathbb{N}$, $n \leq f(n)$.

3. Demonstre o seguinte teorema.

   > **Princípio de Indução Completa:** *Se A é um subconjunto de $\mathbb{N}$ tal que, seja qual for o $n \in \mathbb{N}$, $n \in A$ sempre que $\{k \in \mathbb{N} : \; k < n\} \subseteq A$, então $A = \mathbb{N}$.*

4. Suponha dadas duas funções $g : \mathbb{N} \to \mathbb{N}$ e $h : \mathbb{N}^3 \to \mathbb{N}$. Admita que existe uma funçÃo f que verifica as fórmulas de recorrência presentes nas alíneas seguintes e prove a sua unicidade.

   (a) **(Recorrência)** Defina $f : \mathbb{N}^2 \to \mathbb{N}$ tal que

   $$\begin{cases} f(1,n) = g(n) & (n \in \mathbb{N}) \\ f(m+1,n) = h(m,n,f(m,n)) & (m,n \in \mathbb{N}) \end{cases}$$

   (b) **(Recorrência elementar)**Suponha dados $a \in \mathbb{N}$ e $h : \mathbb{N}^2 \to \mathbb{N}$ defina uma função $f : \mathbb{N} \to \mathbb{N}$ por

   $$\begin{cases} f(1) = a \\ f(n+1) = h(n,f(n)) & (n \in \mathbb{N}) \end{cases}$$

5. Mostre que, para qualquer $n \in \mathbb{N}$,

   (a) $\displaystyle\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$;

   (b) $\displaystyle\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$;

   (c) $\displaystyle\sum_{i=1}^{n} i^3 = \left(\sum_{i=1}^{n} i\right)^2$.

6. Encontre uma fórmula de recorrência para $\sum_{i=1}^{n} i^p \quad (n,p \in \mathbb{N})$.

7. Mostre que, para quaisquer $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$,

   (a) $a^n - b^n = (a-b)\displaystyle\sum_{i=0}^{n-1} a^i b^{n-1-i}$;

   (b) $a^n + b^n = (a+b)\displaystyle\sum_{i=0}^{n-1} (-1)^i a^{n-1-i} b^i$, se n é ímpar;

   (c) $(a+b)^n = \displaystyle\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$;

   sendo o *coeficiente binomial* $\binom{n}{i}$ definido por

   $$\binom{n}{i} = \frac{n!}{i!(n-i)!} \quad (n \in \mathbb{N} \text{ e } 0 \leq i \leq n).$$

8. O *coeficiente multinomial* é o número $\binom{n}{i_1 i_2 \cdots i_k}$ definido por

$$\binom{n}{i_1 i_2 \cdots i_k} = \frac{n!}{i_1! i_2! \cdots i_k!},$$

com $i_1 + i_2 + \cdots + i_k = n$ ($k, n \in \mathbb{N}$, $i_1, \ldots, i_k \in \mathbb{Z}_0^+$).

   (a) Mostre que os coeficientes multinomiais são números inteiros.

   (b) Mostre que, para quaisquer $n, k \in \mathbb{N}$ e $a_1, \ldots, a_k \in \mathbb{Z}$,

$$\left(\sum_{i=1}^{k} a_i\right)^n = \sum_{i_1+i_2+\cdots+i_k=n} \binom{n}{i_1 i_2 \cdots i_k} a_1^{i_1} a_2^{i_2} \cdots a_k^{i_k}.$$

9. Mostre que $d \mid a$ se e só se $d \mid |a|$.

10. Mostre que se $a \mid c$, $b \mid c$ e a e b são primos entre si, então $ab \mid c$.

11. Sejam a, b, c e d inteiros tais que $b \neq 0$, $d \neq 0$, $mdc(a, b) = 1 = mdc(c, d)$ e $\frac{a}{b} + \frac{c}{d}$ também é inteiro. Mostre que $|b| = |d|$.

12. Um *mínimo múltiplo comum* de dois números inteiros positivos a e b é um número inteiro $mmc(a, b)$ que verifique as seguintes condições:

- $mmc(a, b) > 0$;
- $a \mid mmc(a, b)$ e $b \mid mmc(a, b)$;
- para todo $k \in \mathbb{Z}$, se $a \mid k$ e $b \mid k$, então $mmc(a, b) \mid k$.

   (a) Mostre que $mmc(a, b)$ existe e é único. De facto

$$ab = mdc(a, b) mmc(a, b)$$

   (b) Mostre que $\cdot \mid \cdot$ é uma relação de ordem parcial em $\mathbb{N}$ para a qual

$$mdc(a, b) = inf\{a, b\} \quad \& \quad mmc(a, b) = sup\{a, b\}$$

13. (a) Mostre que os factores de base prima da representação de $mdc(a, b)$ (Teorema Fundamental) são os factores de base prima comum a a e a b tomados com o menor expoente.

   (b) Mostre que os factores de base prima da representação de $mmc(a, b)$ (Teorema Fundamental) são todos os factores de base prima de a ou de b, sendo os factores de base comum tomados com o maior expoente.

14. **Algoritmo de Euclides.** Dados $a, b \in \mathbb{Z}$ com $b \geq a > 0$, mostre que o algoritmo definido pelas relações de recorrência seguintes termina com $r = mdc(a, b)$.

- $a = r_0$;
- $b = q_1 r_0 + r_1,\ 0 \leq r_1 < a$;
- se $r_i > 0$ $(i \geq 1)$, então $r_{i-1} = q_{i+1} r_i + r_{i+1},\ 0 \leq r_{i+1} < r_i$;
- se $r_i = 0$, então $r = r_{i-1}$ e o algoritmo termina.

15. **Comprimento do algoritmo de Euclides.** Considere o algoritmo descrito no exercício anterior e seja $r_n = mdc(a, b)$. Mostre que:

    (a) $b \geq 2r_1$ e $a \geq 2r_2$;
    (b) $r_i \geq 2r_{i+2}$ $(i \geq 1)$;
    (c) $b \geq 2^{n/2}$.

    Qual é o número máximo de passos se $b \leq 10^p$?

16. Determine $mdc(a, b)$ e escreva-o como combinação linear de a e b para os seguintes pares:

    (a) $(21, 77)$, $(12, 128)$, $(54, 640)$, $(28, 640)$; nesta alínea verifique a sua resposta utilizando a definição de máximo divisor comum.
    (b) $(22587, 534)$, $(9800, 180)$, $(1587645, 6755)$.

17. Determine o mínimo múltiplo comum de cada um dos pares de números considerados no exercício anterior.

18. Sejam a, b e c números inteiros não simultaneamente nulos.

    (a) Mostre que equação diofantina em x e y, $ax + by = c$ tem solução se e só se $mdc(a, b) \mid c$.
    (b) Mostre que se (x_0, y_0) é uma solução da equação da alínea anterior e $d = mdc(a, b)$, então todas as soluções são da forma

$$x = x_0 + \frac{b}{d}k \quad \& \quad y = y_0 - \frac{a}{d}k \qquad (k \in \mathbb{Z}).$$

19. Determine as soluções inteiras das equações Diofantinas seguintes:

    (a) $5x + 7y = 14$;
    (b) $4x + 6y = 24$;
    (c) $17x + 34y = 25$;
    (d) $56x + 634y = 168$;
    (e) $1521x + 1955y + 455z = 221$;
    (f) $2x + 3y + 5z = 7$.

20. Determine duas fracções cujos denominadores sejam 12 e 16 e cuja soma seja $\frac{10}{48}$.

21. Numa papelaria vendem-se dois tipos de canetas por 110 e 70 escudos respectivamente. Ao fim de um dia a importância total recebida pela venda dessas canetas foi 6570 escudos. Qual é o menor número possível de canetas vendidas? E qual o maior?

22. Determine todas as soluções inteiras dos sistemas de equações seguintes.

(a) $\begin{cases} 2x+3y-4z &= 9 \\ 6x+9y+3z &= 12 \end{cases}$

(b) $\begin{cases} 3x-2y+6z &= -3 \\ 14x+28y-21z &= 35 \end{cases}$

(c) $\begin{cases} 4x+5y+6z &= 11 \\ 7x+14y+21z &= 35 \end{cases}$

(d) $\begin{cases} 9x+3y+15z &= -3 \\ 5x-6y+z &= -2 \end{cases}$

(e) $\begin{cases} 3x+2y-5z &= 10 \\ 6x+12y+4z &= 14 \end{cases}$

23. **Números de Fermat.** Um número da forma $F_k = 2^{2^k}+1$ para algum $k \in \mathbb{N}_0$ diz-se um *número de Fermat*. F_0, F_1, F_2, F_3, F_4 são primos. Euler mostrou em 1732 que F_5 não é primo. ($F_5 = 4294967297 = 641 \times 6700417$.)

(a) Mostre que se 2^n+1 é primo, então n é potência de 2.
(**Sugestão:** comece por estudar o caso em que n é ímpar).

(b) Mostre que números de Fermat distintos são primos entre si.

(c) Deduza da alínea anterior que há uma infinidade de primos.

24. **Números de Mersenne.** Um número da forma $M_p = 2^p - 1$, com p primo, diz-se um *número de Mersenne*.

Mostre que se $n > 1$, $a > 1$ e $a^n - 1$ é primo, então $a = 2$ e n é primo.

25. Suponha que p é um número primo.

(a) Mostre que p é o máximo divisor comum dos coeficientes binomiais $\binom{p}{i}$, onde $1 \leq i \leq p-1$.

(b) Mostre que para quaisquer $a, b \in \mathbb{Z}$, $a^p - b^p$ e p são primos entre si ou $p^2 \mid (a^p - b^p)$.

26. Mostre todos os números inteiros exceptuando as potências de 2 são somas de inteiros consecutivos.

27. Mostre que só a primeira soma parcial da série harmónica é inteira.

Capítulo 2

Congruências

2.1 Propriedades básicas

Definição 2.1.1 *Seja n um número natural maior que 1. Dois números inteiros x, e y dizem-se* **congruentes módulo** *n se $n \mid (x-y)$. Se x é congruente com y módulo n, nota-se*

$$x \equiv y \ (mod\ n)$$

Repare-se que a definição também tem sentido com $n = 1$, neste caso todos os números inteiros são congruentes entre si e por isso eliminamo-lo de início.

Outra formulação

Teorema 2.1.1 *Dois números inteiros x, y são congruentes $(mod\ n)$ se e apenas se a divisão de cada um deles por n tem o mesmo resto.*

Dem. Pondo $x = dn + r$ e $y = qn + s$ com $0 \leq r, s < n$, se $n \mid (x-y)$ então $n \mid (r-s)$; como $|r-s| < n$ terá de ser $r - s = 0$. A recíproca verifica-se imediatamente. □

Demonstra-se sem dificuldade que

Corolário 2.1.1 *A relação de congruência $\cdot \equiv \cdot$ é de equivalência em $\mathbb{Z}$ e compatível com a soma e o produto, ou seja se $a \equiv b\ (mod\ n)$ e $c \equiv d\ (mod\ n)$, então $a + c \equiv b + d\ (mod\ n)$ e $ac \equiv bd\ (mod\ n)$.*

E daqui se deduz que, mais geralmente,

Corolário 2.1.2 *Se* $a_i \equiv b_i \pmod n$ $(1 \leq i \leq k)$, *então*

1. $\sum_{i=1}^{k} a_i \equiv \sum_{i=1}^{k} b_i \pmod n$
2. $\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \pmod n$
3. *Se* f *é um polinómio de coeficientes em* $\mathbb{Z}$ $(f \in \mathbb{Z}[x])$ *e* $a \equiv b \pmod n$, *então* $f(a) \equiv f(b) \pmod n$

Note-se que, $n \mid m$ *se e apenas se* $m \equiv 0 \pmod n$.

Exemplo 2.1.1 Dados dígitos $a_0, \cdots, a_p \in \{0, 1, \cdots, 9\}$, seja

$$\overline{a_p \cdots a_0} = a_p 10^p + \cdots + a_1 10 + a_0;$$

então

$$\overline{a_p \cdots a_0} \equiv \sum_{i=0}^{p} a_i \pmod 3.$$

pois, por um lado $10 \equiv 1 \pmod 3$, por outro, se $f(x) = a_p x^p + \cdots + a_1 x + a_0$ então

$$\overline{a_p \cdots a_0} = f(10) \equiv f(1) = \sum_{i=0}^{p} a_i \pmod 3.$$

Por outras palavras: um número inteiro representado na base 10 é divisível por 3 se e apenas se a soma dos seus algarismos o for.

Por exemplo $3 \not| 7523426$, pois $7+5+2+3+4+2+6 = 29 \equiv 2+9 = 11 \equiv 2 \pmod 3$ e $2 \not\equiv 0 \pmod 3$.

Observando um pouco melhor

$$7+5+2+3+4+2+6 = (7+5)+2+(4+2)+6 \equiv 2 \pmod 3$$

Teorema 2.1.2 *Qualquer número inteiro é congruente* $\pmod n$ *com um e só um dos elementos de* $\{0, 1, \cdots, n-1\}$.

Dem. Dados $n \in \mathbb{N}$ & $x \in \mathbb{Z}$, pelo teorema 1.2.1, existem q e r únicos tais que

$$x = qn + r \quad 0 \leq r < n;$$

portanto $x \equiv r \pmod n$ & $0 \leq r \leq n-1$. A unicidade resulta do teorema 2.1.1. □

Um conjunto $\{r_1, \cdots, r_n\}$ diz-se um **sistema completo de resíduos** módulo n, se para cada número inteiro x existe um e um só r_i tal que $x \equiv r_i \pmod n$

Exemplo 2.1.2 $\{-3, -2, -1, 0, 1, 2, 3\}$ e $\{-7, 8, -5, 10, -3, 19, 13\}$ são sistemas completos de resíduos módulo 7.

Teorema 2.1.3 *Todos os sistemas completos de resíduos para um mesmo módulo têm o mesmo número de elementos.*

Dem.

Consideremos um sistema completo de resíduos, digamos $R = \{r_1, r_2, \cdots, r_k\}$, para um módulo fixo $n > 1$; seja ainda $R_0 = \{1, 2, \cdots, n-1\}$. Como vimos acima, no teorema 2.1.2, para cada $j = 1, \cdots, k$, existe um e só um $i(j) \in R_0$ tal que $r_j \equiv i(j)\ (mod\ n)$, portanto R_0 tem pelo menos o mesmo número de elementos que R; por outro lado, R é também um sistema completo de resíduos e, por definição, para cada elemento de R_0 existe um e só um elemento de R com o qual aquele é congruente $(mod\ n)$, donde R tem pelo menos tantos elementos como R_0. Em suma: R e R_0 têm de facto o mesmo número n de elementos. □

2.2 Inversão I

A congruência em x $2x \equiv 1\ (mod\ 4)$ não tem solução, porque os múltiplos de 4 são pares e $2x - 1$ é sempre ímpar; mas $2x \equiv 1\ (mod\ 5)$ tem solução 3.

Definição 2.2.1 *Um* **inverso aritmético** *de a $(mod\ n)$ é um número inteiro a^* tal que*

$$a^*a \ \equiv\ aa^* \ \equiv\ 1 \ \ (mod\ n).$$

Teorema 2.2.1 *O número $a \in \mathbb{Z} \setminus \{0\}$ tem inverso aritmético $(mod\ n)$ se e apenas se $mdc(a, n) = 1$.*

Dem. O teorema 1.2.4 diz, em particular, que $mdc(a, n) = 1$ se e apenas se existem $x, y \in \mathbb{Z}$ tais que $ax + ny = 1$. Por um lado esta última equação indica que $ax \equiv 1\ (mod\ n)$ e consequentemente x é um inverso aritmético de $a\ (mod\ n)$, que existe se $mdc(a, n) = 1$;por outro lado, de $aa^* \equiv 1\ (mod\ n)$, deduz-se $aa^* = dn + 1$, para algum $d \in \mathbb{Z}$, pelo que $aa^* + (-d)n = 1$ e a e n são primos entre si. □

Veremos adiante que dois inversos aritméticos de um mesmo número para o mesmo módulo são congruentes entre si para esse módulo.

Teorema 2.2.2 *Se $mdc(a, n) = d$ & $a \neq 0$, então*

$$ax \equiv ay\ (mod\ n) \quad \Leftrightarrow \quad x \equiv y\ mod(\frac{n}{d})$$

Dem. ($\Leftarrow$) Se $x \equiv y\ mod(\frac{n}{d})$, então, para certo $q \in \mathbb{Z}$, $x - y = q\frac{n}{d}$, pelo que $ax - ay = q\frac{an}{d} = q\frac{a}{d}n$, ou seja $ax \equiv ay\ (mod\ n)$.

($\Rightarrow$) Se $ax \equiv ay \ (mod\ n)$, então $a(x-y) = qn$ para algum $q \in \mathbb{Z}$; segue-se que $\frac{a}{d}(x-y) = \frac{n}{d}q$; ora $\frac{a}{d}$ e $\frac{n}{d}$ são primos entre si (teorema 1.2.4), pelo que $\frac{a}{d} \mid q$, vindo $x - y = \frac{q}{a/d}n$, isto é $x \equiv y \ (mod\ n)$. □

Observando que, de acordo com o teorema 2.2.1, $a^* \ (mod\ n)$ existe se e apenas se $mdc(a,n) = 1$, deduz-se que

Corolário 2.2.1 *Se a tem inverso aritmético* $(mod\ n)$*, então*

$$ax \ \equiv \ ay \ (mod\ n) \quad \Leftrightarrow \quad x \ \equiv \ y \ (mod\ n).$$

E ainda

Corolário 2.2.2 *Se p é primo e* $a \not\equiv 0 \ (mod\ p)$*, então a tem inverso* $(mod\ p)$*.*

Dem. Note-se que $a \not\equiv 0 \ (mod\ n) \ \Rightarrow \ mdc(a,p) = 1$. □

2.3 Congruências lineares

Uma congruência diz-se **linear** se for da forma

$$ax \ \equiv \ b \ \ (mod\ n) \tag{2.1}$$

Se $a = 0$, esta congruência tem solução x se e apenas se $n \mid b$ e neste caso qualquer $x \in \mathbb{Z}$ é solução. Assim consideraremos apenas congruências

$$ax \equiv \ b \quad com \quad a \neq 0. \tag{2.2}$$

Teorema 2.3.1 *Se a tem inverso* $a^* \ (mod\ n)$*, então*

$$ax \ \equiv \ b \ (mod\ n) \quad \Leftrightarrow \quad x \ \equiv a^*b \ (mod\ n).$$

Dem. Suponha-se que $aa^* \equiv 1 \ (mod\ n)$.

($\Rightarrow$) Se $ax \equiv b \ (mod\ n)$, então $a^*ax \equiv a^*b \ (mod\ n)$. Ora $a^*ax \equiv x \ (mod\ n)$, portanto $x \equiv a^*b \ (mod\ n)$.

($\Leftarrow$) Se $x \equiv a^*b \ (mod\ n)$, analogamente se obtém

$$ax \equiv aa^*b \equiv b \ (mod\ n)$$

e daí $ax \equiv b \ (mod\ n)$. □

Teorema 2.3.2 *Suponha-se que* $a \not\equiv 0 \ (mod\ n)$*. A congruência (2.1) tem solução se e apenas se* $mdc(a,n) \mid b$*. Se* $d = mdc(a,n) \mid b$*, e* a_d^* *é um inverso de* $\frac{a}{d} \ (mod\ n)$*, então as seguintes condições são equivalentes*

1. A congruência (2.1)

2. $x \equiv a_d^* \left(\frac{b}{d}\right) \pmod{\frac{n}{d}}$

3. $x = a_d^* \left(\frac{b}{d}\right) + k\left(\frac{n}{d}\right) \quad 0 \leq k \leq d-1 \pmod{n}$

Dem. Seja $d = mdc(a, n)$.

I) Existência de solução

($\Rightarrow$) Se $ax \equiv b \pmod{n}$ então $n \mid (ax - b)$. Como $d \mid n$ & $d \mid a$, tem-se $d \mid (ax - b)$ e $d \mid a$, portanto $d \mid b$ (corolário 1.2.2).

($\Leftarrow$) Existem $x_0,\ y_0$ tais que $x_0 a + y_0 n = d$. Por outro lado, por hipótese existe k tal que $b = kd$, assim

$$a(x_0 k) + n(y_0 k) = kd = b$$

isto é $a(x_0 k) \equiv b \pmod{n}$. Faça-se $x = x_0 k$.

II) Determinação da solução.

HIPÓTESE: $a_d^* \left(\frac{a}{d}\right) \equiv 1 \pmod{\frac{n}{d}}$ & $d \mid b$.

Considere-se a seguinte sequência de congruências equivalentes, observando que *2* e *3* o são obviamente:

$$\begin{aligned} ax &\equiv b \pmod{n} \\ d\frac{a}{d}x &\equiv d\frac{b}{d} \pmod{n} \\ \frac{a}{d}x &\equiv \frac{b}{d} \pmod{\frac{n}{d}} \qquad (\textit{teorema } 2.2.2). \end{aligned}$$

2.3.1 Inversão II

Dados $a \neq 0$ e $n > 0$ tais que $mdc(a, n) = 1$, vimos na demonstração do teorema 2.2.1 que $a^* \pmod{n}$ é coordenada x da solução (x, y) da equação diofantina $ax + ny = 1$, pelo que, determinado um a^*, todos os outros são da forma $a^* + kn$ ($k \in \mathbb{Z}$), ou seja

Teorema 2.3.3 *Todos os inversos* $\pmod{n}$ *de um mesmo número inteiro não nulo são congruentes* $\pmod{n}$ *entre si.*

E ainda

Teorema 2.3.4 *Se* $a \neq 0$ & $mdc(a, n) = 1$ *então* $a^{**} \equiv a \pmod{n}$.

Dem. A equação $aa^* + ny = 1$ diz-nos que a é inverso $\pmod{n}$ de a^*, isto é, a é um a^{**}.

O teorema anterior diz-nos que todos os inversos $\pmod{n}$ de a^* são congruentes $\pmod{n}$. Consequentemente $a^{**} \equiv a \pmod{n}$. □

Uma outra forma de enunciar o teorema 2.2.1 é a seguinte:

Teorema 2.3.5 *O número $a \in \mathbb{Z}\backslash\{0\}$ tem inverso $(mod\ n)$ se e apenas se é congruente com algum dos resíduos $(mod\ n)$ que são primos com n.*

Este resultado obtém-se muito facilmente do seguinte

Lema 2.3.1 *Se $a \neq 0$ & $a \equiv a'\ (mod\ n)$ & $mdc(a,n) = 1$, então $mdc(a',n) = 1$.*

Dem. Tem-se $a - a' = kn$ & $ax + ny = 1$ para alguns $k, x, y \in \mathbb{Z}$. Assim $ax = a'x + kxn$ & $ax + ny = a'x + (kx + y)n$ ou seja $1 = a'x + ny'$ & $mdc(a',n) = 1$.

□

2.4 A função ϕ de Euler

Definição 2.4.1 *A função de Euler $\phi : \mathbb{N} \to \mathbb{N}$ é dada por*

$\phi(n)$ = *número de números naturais de 1 a n que são primos com n.*

Exemplo 2.4.1 *Seja $P_n = \{x \geq 0 |\ x < n$ & $mdc(x,n) = 1\}$. Designando o número de elementos de um conjunto C por $\#C$, tem-se então $\phi(n) = \#P_n$*

1. $\phi(1) = \#\{1\} = 1$
2. $\phi(n) = n - 1$ *se e apenas se n é primo.*
3. $\phi(2^{725}) = 2^{724}$ *(Porquê?)*

2.4.1 Sistemas reduzidos de resíduos

Definição 2.4.2 *Um* **sistema reduzido** *de resíduos $(mod\ n)$ é um conjunto de números inteiros $a_1, \cdots, a_k$ primos com n, tais que para qualquer $x \in \mathbb{Z}$, se $mdc(x,n) = 1$ então existe um e um só i tal que $x \equiv a_i\ (mod\ n)$.*

Teorema 2.4.1 *$\{1, 2, \cdots, n-1\}$ é um sistema reduzido de resíduos $(mod\ n)$ se e apenas se n é primo.*

Dem. (se) resulta da definição de número primo.

(apenas se) Se n é composto tem pelo menos um divisor próprio, digamos d_1, tal que $1 < d_1 < n$; mas então $1 \leq d_1 \leq n - 1$ & $mdc(d_1, n) = d_1 \neq 1$, portanto $\{1, 2, \cdots, n-1\}$ tem elementos que não são primos com n, consequentemente não é um sistema reduzido. □

Teorema 2.4.2 *Para cada n, todos os sistemas reduzidos de resíduos $(mod\ n)$ têm $\phi(n)$ elementos.*

Dem. Seja P_n definido como no exemplo 2.4.1.

1. P_n é um sistema reduzido $(mod\ n)$ porque

   (a) Qualquer inteiro é congruente $(mod\ n)$ com algum elemento de $S_n = \{0, 1, \cdots, n-1\}$, em particular um inteiro primo com n, cujo congruente em S_n é primo com n (teorema 2.3.5), logo está em P_n.

   (b) Dois elementos distintos de P_n não são congruentes entre si. Assim

   > **I.** *cada x primo com n é congruente com um e um só elemento de P_n.*

2. Dado um sistema reduzido de resíduos $(mod\ n)$, digamos P'_n, a proposição **I** acima afirma *a função que associa a cada resíduo em P_n o seu único congruente em P'_n é bijectiva.* □

2.4.2 Teoremas de Euler, de Fermat e de Wilson

Teorema 2.4.3 (de Euler) *Para qualquer $a \in \mathbb{Z} \setminus \{0\}$ e qualquer $n \in \mathbb{N} \setminus \{1\}$*

$$mdc(a, n) = 1 \quad \Rightarrow \quad a^{\phi(n)} \equiv 1\ (mod\ n).$$

O corolário seguinte é imediato:

Corolário 2.4.1 *Para qualquer $a \in \mathbb{Z} \setminus \{0\}$ e qualquer $n \in \mathbb{N} \setminus \{1\}$*

$$mdc(a, n) = 1 \quad \Rightarrow \quad a^* \equiv a^{\phi(n)-1}\ (mod\ n).$$

Dem. (do teorema 2.4.3) Suponha-se $a \neq 0$ & $mdc(a, n) = 1$.

I) Se $0 \neq r$ & $mdc(r, n) = 1$, então $mdc(ar, n) = 1$.

Dem. Seja $d = mdc(ar, n)$ nas condições da hipótese. Se $d > 1$, então existe um número primo p tal que $p \mid d$. Segue-se que $p \mid ar$ & $p \mid n$, logo $p \mid a$ & $p \mid n$ ou $p \mid r$ & $p \mid n$; no primeiro caso $mdc(a, n) \geq p > 1$, no segundo $mdc(r, n) \geq p > 1$, o que contradiz as hipóteses.

II) Seja $\{r_1, \cdots, r_{\phi(n)}\}$ um sistema reduzido de resíduos $(mod\ n)$, e defina-se $P = \{ar_1, \cdots, ar_{\phi(n)}\}$.

Todos os elementos de P são primos com n, pelo que vimos em I. Por outro lado, como os r_i nunca são congruentes entre si, o mesmo acontece com os ar_i (teorema 2.2.2). Segue-se que

> *cada ar_i é congruente com um e só um dos r_j, digamos $r_j \equiv ar_{\sigma(j)}$, em que σ é uma permutação de $\{1, \cdots, \phi(n)\}$.*

III) Tem-se então

$$\prod_{i=1}^{\phi(n)}(ar_{\sigma(i)}) \equiv \prod_{i=1}^{\phi(n)} r_i \quad (mod\ n)$$

ou seja

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} r_{\sigma(i)} \equiv \prod_{i=1}^{\phi(n)} r_i \quad (mod\ n)$$

ou

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} r_i \equiv \prod_{i=1}^{\phi(n)} r_i \quad (mod\ n)$$

Pelo teorema 2.2.2, já que $mdc(\prod_{i=1}^{\phi(n)} r_i, n) = 1$, conclui-se $a^{\phi(n)} \equiv 1\ (mod\ n)$. □

Teorema 2.4.4 (Pequeno Teorema de Fermat) *Se p é primo e $p \not| a$, então $a^{p-1} \equiv 1\ (mod\ p)$.*

Dem. Basta observar que $\phi(p) = p - 1$. □

Teorema 2.4.5 (de Wilson) *Se p é primo, então $(p-1)! \equiv -1\ (mod\ p)$*

Dem. Se $p = 2$, tem-se $(p-1)! = 1 \equiv -1\ (mod\ 2)$. Se $p = 3$, tem-se $(p-1)! = 2 \equiv -1\ (mod\ 3)$. Suponha-se que $p > 3$. Sabemos que $P_p = \{1, 2, \cdots, p-1\}$ é um sistema reduzido de resíduos $(mod\ p)$. Observando que qualquer número e o seu inverso $(mod\ n)$ são primos com n e finalmente considerando o teorema 2.3.4:

Cada $r \in P_p$ tem um inverso $(mod\ p)$ $r_p^* \in P_p$ e $(r_p^*)_p^* = r$. Por outro lado, se $r = r_p^*$, tem-se $r^2 = rr_p^* \equiv 1\ (mod\ p)$ e $p \mid (r^2 - 1) = (r+1)(r-1)$; logo $p \mid (r+1)$ ou $p \mid (r-1)$, isto é, $r \equiv -1\ (mod\ p)$ ou $r \equiv 1\ (mod\ p)$ ou ainda $r \equiv p-1\ (mod\ p)$ ou $r \equiv 1\ (mod\ p)$.

Concluimos que

$$r = r_p^* \ \Leftrightarrow\ (r = 1\ ou\ r = p-1) \quad (1 \le r \le p-1);$$

donde os pares $\{r, r^*\}$ são conjuntos não singulares e definem uma partição de $\{2, \cdots, p-2\}$, tendo-se

$$\prod_{i=2}^{p-2} i \ = \ \prod_{i=1}^{\frac{p-3}{2}} r_i r_i^* \equiv 1\ (mod\ p)$$

Segue-se que

$$(p-1)! \ = \ 1 \cdot \prod_{i=2}^{p-2} i \cdot (p-1) \equiv \ p-1 \quad (mod\ p)$$

isto é $(p-1)! \equiv -1\ (mod\ p)$. □

O lema seguinte é extremamente simples, mas tem uma consequência não trivial.

Lema 2.4.1 *Se p é um número primo ímpar e $(-1)^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$, então $p \equiv 1 \ (mod\ 4)$.*

Dem. Suponha-se então que p é um número primo ímpar e que $(-1)^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$; queremos mostrar que $\frac{p-1}{2}$ é par. Se $\frac{p-1}{2}$ fosse ímpar, viria $-1 \equiv 1 \ (mod\ p)$, pelo que p dividiria 2, o que não é o caso; portanto $\frac{p-1}{2}$ é par. □

A consequência:

Teorema 2.4.6 *Seja p um primo ímpar. A congruência $x^2 \equiv -1 \ (mod\ p)$ tem solução se e apenas se $p \equiv 1 \ (mod\ 4)$; neste caso $\left(\frac{p-1}{2}\right)!$ é uma solução.*

Dem. (apenas se) De $x^2 \equiv -1 \ (mod\ p)$ deduz-se

$$x^{p-1} = (x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \ (mod\ p)$$

e conclui-se $1 \equiv (-1)^{\frac{p-1}{2}} \ (mod\ p)$; pelo lema 2.4.1, $p \equiv 1 \ (mod\ 4)$.

(se) Se $p \equiv 1 \ (mod\ 4)$, então $\frac{p-1}{2}$ é par. Por outro lado

$$(p-1)! \ = \ \left(\frac{p-1}{2}\right)! \left(p - \frac{p-1}{2}\right) \cdots (p-2)(p-1).$$

Pelo Teorema de Wilson,

$$-1 \ \equiv \ (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \ \ (mod\ p)$$

Como $\frac{p-1}{2}$ é par,

$$-1 \ \equiv \ \left[\left(\frac{p-1}{2}\right)!\right]^2 \ \ (mod\ p)$$

como pretendíamos verificar. □

E consequentemente

Corolário 2.4.2 *Se p é primo ímpar e para algum número inteiro x $p \mid (x^2+1)$, então $p \equiv 1 \ (mod\ 4)$.*

E mais um corolário (compare-se com o teorema 1.2.9).

Corolário 2.4.3 *Há uma infinidade de números primos da forma $4k+1$ ($k \in \mathbb{Z}$), i.e., congruentes com 1 para o módulo 4.*

Dem. Vamos mostrar que seja qual for o número natural n, existe um número primo maior que n da forma pretendida. Seja então n um número natural – maior ou igual a 4 para evitar trivialidades – e defina-se

$$N \;=\; (n!)^2 \;+\; 1.$$

Seja p o menor divisor primo de N. Se N é primo, $N = p$, é já da forma pretendida e maior que n. Se N não é primo, $p > n$ pois N não é divisível por qualquer número menor que n; $p > 2$ – porque N é ímpar – e $p \mid (n!)^2 + 1$; pelo corolário anterior (2.4.2) $p \equiv 1 \pmod 4$. □

2.5 Congruências polinomiais

2.5.1 Introdução

Nesta secção estudamos a resolução de congruências da forma

$$f(x) \equiv 0 \pmod n \tag{2.3}$$

em que f é um polinómio de coeficientes inteiros e *grau m maior que 1* $(mod\ n)$*:*

$$f(x) = a_0 + a_1x^1 + \cdots + a_mx^m \quad \& \quad m > 1 \quad \& \quad a_m \not\equiv 0 \pmod n. \tag{2.4}$$

O *grau* de um polinómio $f \pmod n$ designa-se por $deg_n(f)$. Se $f(x) = \alpha \in \mathbb{Z}$, o grau de $f \pmod n$ é zero.

O Teorema 2.4.6 é obviamente um caso particular deste estudo.

Comecemos por observar que, *para qualquer* $n > 1$ *existem congruências (2.3) & (2.4) sem solução;* mais precisamente:

Exemplo 2.5.1 *Se p é primo e* $p|n$*, então a congruência* $x^p - x + 1 \equiv 0 \pmod n$ *não tem soluções.* Tal pode verificar-se do seguinte modo: quando $p|n$, se $x^p - x + 1 \equiv 0 \pmod n$ também $x^p - x + 1 \equiv 0 \pmod p$; mas $x^p - x + 1 \equiv 1 \not\equiv 0 \pmod p$, quando p é primo, em virtude do *Pequeno Teorema de Fermat;* portanto a congruência inicial não tem de facto solução.

Exemplo 2.5.2 *Dois polinómios* $f(x)$ *e* $g(x)$ *congruentes* $(mod\ n)$ *para todo o* $x \in \mathbb{Z}$ ***não têm necessariamente o mesmo grau*** $(mod\ n)$***:*** se p é primo, $x^{p^2} - x$ e $x^p - x$ são ambos identicamente nulos $(mod\ p)$.

A situação é assim algo complicada mas, tal como a propósito do problema da resolubilidade algébrica, há resultados parciais importantes e relativamente simples[1].

Repare-se que

[1] De facto, nem mesmo no caso em que n é primo, se conhecem fórmulas resolventes gerais para a congruência (2.3) & (2.4)

Teorema 2.5.1 *Se dois polinómios f e g têm coeficientes do mesmo grau congruentes $(mod\ n)$, as congruências $f(x) \equiv 0\ (mod\ n)$ e $g(x) \equiv 0\ (mod\ n)$ são equivalentes. Assim basta considerar polinómios cujos coeficientes estejam entre 0 e $n-1$.*

Dem. Suponha-se que $f(x) = \sum_{i=0}^{m} a_i x^i$ e $g(x) = \sum_{i=0}^{m} b_i x^i$, sendo $a_i \equiv b_i\ (mod\ n)$ para $0 \leq i \leq n$. Tomando $c_i = \frac{a_i - b_i}{n}$ vem

$$f(x) - g(x) = n \sum_{i=0}^{m} c_i x^i$$

ou seja, $f(x) \equiv g(x)\ (mod\, n)$ para qualquer $x \in \mathbb{Z}$, em particular $f(x) \equiv 0\ (mod\, n)$ *sse* $g(x) \equiv 0\ (mod\ n)$. □

De facto, uma aplicação da regra de Ruffini mostra que

Teorema 2.5.2 *Para qualquer polinómio $f(x)$ como em (2.3) e (2.4) e qualquer $a \in \mathbb{Z}$, existe um polinómio $q(x)$, de coeficientes inteiros e grau $m-1$, tal que*

$$f(x) = (x-a)q(x) + f(a) \quad (x \in \mathbb{Z}).$$

Daqui decorre

Corolário 2.5.1 *Se $f(x)$ é um polinómio como em (2.3) & (2.4) e $a \in \mathbb{Z}$, então $f(a) \equiv 0\ (mod\ n)$ sse existe um polinómio $q(x)$ de coeficientes inteiros, grau $m-1\ (mod\ n)$ e coeficiente de maior ordem igual ao de $f(x)$ tal que*

$$f(x) \equiv (x-a)q(x)\ (mod\ n) \quad (x \in \mathbb{Z}). \tag{2.5}$$

Dem. Se $f(a) \equiv 0\ (mod\ n)$, então $n | f(a)$ e (2.5) resulta imediatamente do teorema anterior, por definição de congruência. Reciprocamente, se vale (2.5),então como a é concerteza solução de $(x-a)q(x) \equiv 0\ (mod\ n)$ para qualquer $x \in \mathbb{Z}$, necessariamente $f(a) \equiv 0\ (mod\ n)$. □

2.5.2 Módulo primo

Convencionemos que p designa um número primo. O primeiro facto a registar é que basta considerar polinómios de grau menor ou igual a $p\ (mod\ p)$:

Teorema 2.5.3 *Qualquer congruência polinomial $f(x) \equiv 0\ (mod\ p)$ é equivalente a outra $g(x) \equiv 0\ (mod\ p)$ em que $g(x)$ é um polinómio nulo ou de grau menor ou igual a $p-1\ (mod\ p)$.*

Dem. A ideia é baixar tanto quanto possível o grau dos monómios envolvidos, utilizando o Pequeno Teorema de Fermat:

Repare-se que, se $n = pq + r$ com $0 \leq r < p$, então

$$x^n = (x^p)^q x^r \equiv x^q x^r = x^{q+r}\ (mod\ p)$$

Aplicando sucessivamente esta sequência de congruências a cada monómio de f, reduz-se o expoente de cada um deles a um número inferior a p. □

Tal como para equações, o teorema 2.5.2 tem a seguinte consequência.

Teorema 2.5.4 *Se $b_1, b_2, ..., b_k$ são soluções da congruência polinomial $f(x) \equiv 0 \pmod p$ não congruentes duas a duas, existe um polinómio $q(x)$, cujo coeficiente de maior ordem é o mesmo que o de f e tal que*

$$deg_p(q) \leq deg_p(f) - k \quad \& \quad f(x) \equiv (x - b_1)(x - b_2) \cdots (x - b_k)q(x) \pmod p$$

Dem. A demonstração é muito semelhante à correspondente para equações, por utilização recursiva da regra de Ruffini:

Primeiro obtem-se

$$f(x) \equiv (x - b_1)q_1(x) \pmod p$$

pelo corolário 2.5.1. Em seguida há que verificar se

$$q_1(b_2) \equiv 0 \pmod p \tag{2.6}$$

e reaplicar o mesmo corolário, tantas vezes quanto necessário. Repare-se então que, por hipótese

$$0 \equiv f(b_2) \equiv (b_2 - b_1)q_1(b_2) \pmod p,$$

isto é,

$$p|(b_2 - b_1)q_1(b_2)$$

e como, também por hipótese, p é primo e $p \not| (b_1 - b_2)$, necessariamente $p|q_1(b_2)$, ou seja vale a equação (2.6). □

Uma conclusão a retirar é

Corolário 2.5.2 *Quando p é primo e $f(x)$ é um polinómio cujos coeficientes não são todos nulos $\pmod p$, o número de soluções distintas $\pmod p$ de uma congruência polinomial $f(x) \equiv 0 \pmod p$ é quando muito $deg_p(f)$.*

Antes de apresentarmos uma demonstração atentemos no seguinte exemplo.

Exemplo 2.5.3 Se n não é primo, o número de soluções não mutuamente congruentes $(mod\ n)$ de uma equação como em (2.3) e (2.4) pode ser superior ao grau de f $(mod\ n)$: $x^2 - 1 \equiv 0\ (mod\ 8)$ tem soluções $1, 3, 5, 7$.

Dem. (Do corolário 2.5.2) Tomem-se f, q e os b_i, com $1 \leq i \leq k$, como no teorema. Como $q(x)$ tem o mesmo coeficiente de maior ordem que $f(x)$, necessariamente o seu grau é maior ou igual a zero, portanto

$$0 \leq deg_p(q) \leq deg_p f(x) - k \quad i.e. \quad k \leq \deg_p(f).$$

□

2.5.3 Módulo potência de base prima

Veremos como se podem obter as soluções de uma congruência

$$f(x) \equiv 0 \ (mod\ p^{\alpha+1}) \tag{2.7}$$

a partir das da congruência $f(x) \equiv 0 \ (mod\ p^{\alpha})$. De facto vamos provar o seguinte:

Teorema 2.5.5 *As soluções da congruência*

$$f(x) \equiv 0 \ (mod\ p^{\alpha+1})$$

são da forma

$$x = b + kp^{\alpha} \text{ com } k \in \mathbb{Z}, \tag{2.8}$$

sendo

$$f(b) \equiv 0 \ (mod\ p^{\alpha}) \quad \& \quad f'(b)k \equiv -\frac{f(b)}{p^{\alpha}} \ \ (mod\ p) \tag{2.9}$$

Comecemos com uma **Fórmula de Taylor.** Designando por f' a derivada do polinómio f, definimos também

$$\begin{cases} f^{(0)} = f \\ f^{(i+1)} = \left(f^{(i)}\right)' \quad i \in \mathbb{Z}_0^+ \end{cases}$$

Nestes termos tem-se

Lema 2.5.1 *Seja $f(x)$ um polinómio de grau m $(mod\ n)$ de coeficientes inteiros como em (2.3) & (2.4). Então*

$$f(x+y) = f(x) + \sum_{k=1}^{m} \frac{f^{(k)}(x)}{k!} y^k \quad (x, y \in \mathbb{Z}) \tag{2.10}$$

e os coeficientes $\frac{f^{(k)}(x)}{k!}$ $(1 \leq k \leq m)$ são números inteiros.

Dem. Como, para quaisquer polinómios f e g e qualquer $\alpha \in \mathbb{Z}$ se tem

$$(f+g)' = f' + g' \qquad \& \qquad (\alpha f)' = \alpha f,'$$

basta demonstrar o teorema quando $f(x) = x^m$ e neste caso (2.10) é nada mais nada menos que uma outra forma de apresentar o desenvolvimento de Newton para $(x+y)^m$, pois

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

Dem. (Do teorema 2.5.5)

Observe-se que, quando $f(x) \equiv 0 \ (mod\ p^{\alpha+1})$ também $f(x) \equiv 0 \ (mod\ p^{\alpha})$, pelo que as soluções da primeira congruência se encontram entre as da segunda; resumindo

$$f(x) \equiv 0 \ (mod\ p^{\alpha+1}) \ \Rightarrow f(x) \equiv 0 \ (mod\ p^{\alpha}) \Rightarrow x = b + kp^{\alpha}$$

para algum $k \in \mathbb{Z}$ e algum $b \in \mathbb{Z}$ tal que $f(b) \equiv 0 \ (mod\ p^{\alpha})$.

Ora, pelo lema 2.5.1, vem

$$f(b + kp^{\alpha}) = f(x) + \sum_{i=1}^{m} \frac{f^{(i)}(b)}{i!}(kp^{\alpha})^{i};$$

como $\alpha \geq 1$, os termos do segundo membro em que $i > 1$ são divisíveis por $p^{\alpha+1}$, pois $\alpha i > 2\alpha = \alpha + \alpha \geq \alpha + 1$. Assim

$$f(b + kp^{\alpha}) \equiv f(b) + \frac{f'(b)}{1}kp^{\alpha} \quad (mod\ p^{\alpha+1});$$

mas $f(b) \equiv 0 \ (mod\ p^{\alpha})$, pelo que $f(b) = tp^{\alpha}$, para algum $t \in \mathbb{Z}$. A situação a analisar é então a seguinte

$$p^{\alpha}\left(t + f'(b)k\right) \equiv 0 \ (mod\ p^{\alpha+1})$$

ou seja

$$\frac{f(b)}{p^{\alpha}} + f'(b)k \equiv 0 \ (mod\ p)$$

como se pretendia verificar. □

Segue-se uma verificação mais detalhada da validade da fórmula (2.9).

Caso $f'(b) \equiv 0 \ (mod\ p)$**.** Neste caso a congruência (2.9) é equivalente a

$$\frac{f(b)}{p^{\alpha}} \equiv 0 \ (mod\ p)$$

por sua vez equivalente a

$$f(b) \equiv 0 \ (mod\ p^{\alpha+1}); \tag{2.11}$$

se esta se não verifica, pura e simplesmente não há soluções; se (2.11) se dá, então, pelo lema 2.5.1, a equação (2.8) dá-nos soluções para a congruência (2.7) seja qual for $k \in \mathbb{Z}$.

Caso $f'(b) \not\equiv 0 \ (mod\ p)$**.** Neste caso a solução em k de (2.9) é dada por

$$k \equiv -f'(b)^{*}\frac{f(b)}{p^{\alpha}} \ (mod\ p)$$

A solução da congruência (2.7) é mesmo única e dada por

$$x \equiv b - f'(b)^{*}\frac{f(b)}{p^{\alpha}}p^{\alpha} \ (mod\ p^{\alpha+1}) \quad \text{com} \quad f'(b)^{*}f'(b) \equiv 1 \ (mod\ p)$$

ou ainda

$$x \equiv b - f'(b)^* f(b) \ (mod\ p^{\alpha+1}) \ \ \& \ \ f'(b)^* f'(b) \equiv 1 \ (mod\ p) \tag{2.12}$$

□

2.5.4 Teorema Chinês do Resto

A resolução de congruências polinomiais (2.3) & (2.4) pode reduzir-se aos casos que temos vindo a estudar, como vamos ver. Note-se que para a discussão que segue não importa se $f(x)$ é ou não um polinómio.

Suponhamos então que n é um número natural composto, digamos

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

para certos números primos p_i.

Generalizando o argumento apresentado no exemplo 2.5.1, observe-se que

$$f(x) \equiv 0 \ (mod\ n) \ \Rightarrow \ f(x) \equiv 0 \ (mod\ p_i^{\alpha_i}) \quad (1 \leq i \leq k),$$

pelo que as soluções da congruência

$$f(x) \equiv 0 \ (mod\ n) \tag{2.13}$$

se encontram entre as do sistema de congruências

$$\begin{cases} f(x) \equiv 0 \ (mod\ p_i^{\alpha_i}) \\ 1 \leq i \leq k \end{cases}$$

Acontece que este sistema é mesmo equivalente à congruência (2.13), pois potências de primos distintos são primas entre si e o seu produto divide qualquer número dividido simultaneamente por todas elas (se $a|c$, $b|c$ e a e b são primos entre si, então $ab|c$.) Provámos então o seguinte

Teorema 2.5.6 *Se n é um número composto de factores de base prima $p_i^{\alpha_i}$*

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

a congruência

$$f(x) \equiv 0 \ (mod\ n)$$

é equivalente ao sistema de congruências

$$\begin{cases} f(x) \equiv 0 \ (mod\ p_i^{\alpha_i}) \\ 1 \leq i \leq k \end{cases} \tag{2.14}$$

Vimos já que algumas congruências polinomiais $f(x) \equiv 0 \ (mod\ n)$ não têm solução, mas se todas as do sistema (2.14) tiverem, então há de facto solução e deverá ser possível determiná-la. Utilizaremos o seguinte lema

Lema 2.5.2 (Teorema Chinês do Resto) *Se $m_1, ..., m_k$ são números naturais primos entre si dois a dois e $b_1, ..., b_k$ são números inteiros quaisquer, o sistema de congruências*

$$\begin{cases} x \equiv b_i \ (mod\ m_i) \\ 1 \leq i \leq k \end{cases} \tag{2.15}$$

tem solução e quaisquer duas soluções são congruentes $(mod\ m_1 \cdots m_k)$.

Dem. Comecemos pela afirmação final.

Se x e y são soluções do sistema (2.15), então $x - y \equiv 0 \ (mod\ m_i)$ para qualquer dos m_i, ou seja, $x - y$ é divisível por qualquer dos m_i. Como os m_i são primos entre si, o seu produto divide $x - y$, como se pretendia concluir.

Quanto à existência de solução para o sistema: vamos procurá-la na forma

$$x = x_1 b_1 + \cdots + x_k b_k \tag{2.16}$$

de modo que, para cada i,

1. todas as parcelas com possível excepção da i-ésima sejam divisíveis por m_i,
2. a i-ésima parcela seja congruente com $b_i \ (mod\ m_i)$.

Para verificar a primeira condição basta que

$$m_i' = \prod_{\substack{j=1 \\ j \neq i}}^{k} m_j \ | x_i;$$

para verificar a segunda basta que

$$x_i \equiv 1 \ (mod\ m_i)$$

As duas condições são verificadas simultâneamente se

$$(m_i')^* m_i' \equiv 1 \ (mod\ m_i) \quad \& \quad x_i = (m_i')^* m_i' \tag{2.17}$$

Ora cada m_i' é primo com m_i, portanto os inversos aritméticos $(m_i')^*$ existem e as condições (2.16) e (2.17) definem uma solução para o sistema (2.15). □

Exemplo 2.5.4 Considere-se a congruência

$$x^2 - 1 \equiv 0 \ (mod\ 108). \tag{2.18}$$

Como $108 = 2^2 \cdot 3^3$, pelo teorema 2.5.6, (2.18) é equivalente ao sistema

$$\begin{cases} x^2 - 1 \equiv 0 \ (mod\ 2^2) & (i) \\ x^2 - 1 \equiv 0 \ (mod\ 3^3) & (ii) \end{cases} \tag{2.19}$$

Por simples inspecção conclui-se que as soluções da congruência (i) são dadas por

$$x \equiv 1, -1 \ (mod\ 2^2).$$

Quanto a (ii), vamos utilizar o teorema 2.5.5. O módulo 3^2 é ainda razoavelmente baixo e, também por inspecção, se podem obter as soluções

$$x \equiv 1, -1 \ (mod\ 3^2).$$

Ora $f'(x) = 2x$ donde

$$f'(1) = 2 \equiv -1 \not\equiv 0 \ (mod\ 3) \quad \& \quad f'(-1) = -2 \equiv 1 \not\equiv 0 \ (mod\ 3).$$

Ambas as derivadas são invertíveis $(mod\ 3)$ e nas congruências em (2.9) $k \equiv 0 (mod\ 3)$, portanto

$$x^2 - 1 \equiv 0 \ (mod\ 3^3) \quad \text{se e só se} \quad x \equiv \pm 1 \ (mod\ 3^3).$$

O sistema (2.19) dá então lugar aos sistemas seguintes, que podem ser resolvidos utilizando, por exemplo, o Teorema Chinês do Resto 2.5.2, como vimos atrás.

$$(S1) \begin{cases} x \equiv 1 & (mod\ 2^2) \\ x \equiv 1 & (mod\ 3^3) \end{cases} \quad (S2) \begin{cases} x \equiv 1 & (mod\ 2^2) \\ x \equiv -1 & (mod\ 3^3) \end{cases}$$

$$(S3) \begin{cases} x \equiv -1 & (mod\ 2^2) \\ x \equiv 1 & (mod\ 3^3) \end{cases} \quad (S4) \begin{cases} x \equiv -1 & (mod\ 2^2) \\ x \equiv -1 & (mod\ 3^3) \end{cases}$$

De um modo geral, as soluções da congruência (2.18) são dadas pela fórmula

$$x \equiv 3 \cdot \ 3^3 \cdot (\pm 1) + 7 \cdot \ 2^2 \cdot (\pm 1) \equiv \pm 81 \pm 28 \ (mod\ 108)$$

onde as combinações de sinal são todas as possíveis.

Resolvendo detalhadamente $(S1)$: de acordo com a demonstração de 2.5.2, com (2.16) e (2.17) tem-se $m_1 = 2^2$, $m_1' = 3^3$ e $(m_1')^* \equiv -1 \ (mod\ 2^2)$ e também $m_2 = 3^3$, $m_2' = 2^2$ e $(m_2')^* \equiv 7 \ (mod\ 3^3)$. Segue-se que as soluções de $(S1)$ são dadas por

$$x \equiv 3 \cdot 3^3 \cdot 1 + 7 \cdot 2^2 \cdot 1 \equiv 109 \equiv 1 \ (mod\ 2^2 \cdot 3^3).$$

2.6 Exercícios

1. Mostre que a congruência $y^2 - x^2 - 2 \equiv 0 \ (mod\ 4)$ não tem soluções e conclua que a equação Diofantina $y^2 - x^2 - 2 = 0$ também as não tem.

2. Utilize congruências módulo 4 para mostrar que se $y^2 = x^3 + 2$, então x e y são ambos ímpares.

3. Seja $f(x) = 11x^3 + 15x^2 + 9x - 2$. Determine o resto da divisão de $f(a)$ por b para os pares (a, b) seguintes: (2,7), (6,7), (97,11).

4. Mostre que se p é primo, qualquer sequência de $p-1$ números inteiros consecutivos que não inclui múltiplos de p é um sistema reduzido de resíduos $(mod\ p)$.

5. Calcule $\phi(n)$ para $n \leq 28$.

6. Mostre que se p é primo e $n \in \mathbb{N}$, então $\phi(p^n) = p^n - p^{n-1}$.

7. Resolva as congruências:

   (a) $3x \equiv 1 \ (mod\ 5)$;
   (b) $3x \equiv 9 \ (mod\ 5)$;
   (c) $3x \equiv 9 \ (mod\ 24)$;
   (d) $5x \equiv 15 \ (mod\ 12)$;
   (e) $x^2 + 1 \equiv 0 \ (mod\ 4)$;
   (f) $x^3 + 2x + 1 \equiv 0 \ (mod\ 7)$;
   (g) $x^5 + x^4 + x^3 + x^2 + x \equiv -1 \ (mod\ 5)$.

8. Determine os inversos $(mod\ 18)$ de todos os inteiros que os têm.

9. Qual o inverso de 1975 $(mod\ 2001)$?

10. Mostre que uma quarta potência é congruente com 0 ou 1 $(mod\ 5)$.

11. Resolva as congruências

    (a) $2x + 3y \equiv 5 \ (mod\ 7)$;
    (b) $x^2 + y^2 - 5y \equiv 2 \ (mod\ 9)$.

12. Seja $a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$ a expressão decimal do número natural $n = \overline{a_k a_{k-1} \cdots a_1 a_0}$ $(0 \leq a_i \leq 9,\ 0 \leq i \leq k,\ a_0 \neq 0)$.

    (a) Mostre que $11 \mid n$ se e só se $11 \mid \sum_{i=0}^{k} (-1)^i a_i$;
    (b) Verifique se 1234567890987654321 é divisível por 11.

13. Mostre que se k for ímpar, $11^{2k} + 19^{2k}$ é divisível por 241.

14. Resolva os sistemas de congruências

    (a) $\begin{cases} 2x + 7y & \equiv & 2 \ (mod\ 5) \\ 3x + 6y & \equiv & 2 \ (mod\ 7) \end{cases}$;

    (b) $\begin{cases} 9x + 3y & \equiv & 3 \ (mod\ 10) \\ 15x + 2y & \equiv & 4 \ (mod\ 15) \end{cases}$;

    (c) $\begin{cases} 2x + 7y & \equiv & 2 \ (mod\ 5) \\ 3x - y & \equiv & 11 \ (mod\ 5) \end{cases}$.

15. Verifique se as seguintes congruências têm ou não solução e, no caso afirmativo, resolva-as.

    (a) $x^2 \equiv -1 \ (mod\ 17)$;
    (b) $x^2 \equiv -1 \ (mod\ 43)$;
    (c) $x^2 \equiv -1 \ (mod\ 65)$.

16. Mostre o recíproco do **Teorema de Wilson**:

    Se $m \in \mathbb{N} \setminus \{1\}$ e $(m-1)! \equiv -1 \ (mod\ m)$, então m é primo.

    (**Sugestão:** Observe que se $m > 4$ e m não é primo então $(m-1)! \equiv 0 \ (mod\ m)$.)

17. Mostre que a equação Diofantina $x^2 + 1 = 23y$ não tem soluções inteiras.

18. Seja p um número primo. Mostre que $(a+b)^p \equiv a^p + b^p \ (mod\ p)$.

19. Suponha que p é um primo ímpar. Mostre que

    (a) $\prod_{i=1}^{(p-1)/2} (2i)^2 \equiv (-1)^{(p+1)/2} \ (mod\ p)$,

    (b) $\prod_{i=1}^{(p-1)/2} (2i-1)^2 \equiv \prod_{i=1}^{(p-1)/2} (2i)^2 \ (mod\ p)$.

20. Reduza o mais possível o grau dos polinómios nas seguintes congruências e resolva-as.

    (a) $2x^{17} + 3x^2 + 1 \equiv 0 \ (mod\ 5)$;
    (b) $x^{10} + 2x^5 + 1 \equiv 0 \ (mod\ 5)$;
    (c) $3x^{23} + 2x^{20} + 4x^{17} - x^6 + x^5 - 3x^3 + 2x + 1 \equiv 0 \ (mod\ 5)$.

21. Factorize $(mod\ 11)$ de duas maneiras distintas os polinómios $f(x)$ seguintes, observando que em cada caso $f(a) \equiv 0 \ (mod\ 11)$.

(a) $f(x) = x^2 + 10x + 3$, $a = 6$;

(b) $f(x) = x^3 - x^2 + x + 10$, $a = 1$;

(c) $f(x) = x^3 - 6x^2 - 2x + 20$, $a = -3$.

22. Factorize $(mod\ 13)$ o polinómio $f(x) = x^4 - 6x^3 - 3x^2 - 7x + 2$ com pelo menos dois factores de primeiro grau.

23. Mostre que o polinómio $x^3 + 3x^2 + 2x + 2$ não pode ser factorizado $(mod\ 5)$.

24. Resolva a congruência $x^{p^\alpha} \equiv b\ (mod\ p)$ sabendo que p é primo e $\alpha \geq 1$.

25. Resolva os seguintes sistemas de congruências

(a) $\begin{cases} x \equiv 3 & (mod\ 7) \\ x \equiv 2 & (mod\ 6) \\ x \equiv 1 & (mod\ 5) \end{cases}$

(b) $\begin{cases} x \equiv 5 & (mod\ 2) \\ x \equiv 1 & (mod\ 3) \\ x \equiv 2 & (mod\ 5) \end{cases}$

(c) $\begin{cases} 3x \equiv 1 & (mod\ 10) \\ 4x \equiv 2 & (mod\ 7) \end{cases}$

(d) $\begin{cases} 3x \equiv 2 & (mod\ 4) \\ 2x \equiv 7 & (mod\ 15) \\ 4x \equiv -1 & (mod\ 7) \end{cases}$

26. (a) Suponha que $m, n \in \mathbb{N}$ e que $d = mdc(m, n)$. Mostre que o sistema de congruências

$$\begin{cases} x \equiv a & (mod\ m) \\ x \equiv b & (mod\ n) \end{cases}$$

tem solução se e só se $a \equiv b\ (mod\ d)$ e que, nesse caso, a solução é única $(mod\ mmc(m, n))$.

(b) Determine se cada um dos seguintes sistemas de congruências tem solução e, em caso afirmativo, resolva-o.

i. $\begin{cases} x \equiv 5 & (mod\ 6) \\ x \equiv 7 & (mod\ 10) \end{cases}$

ii. $\begin{cases} x \equiv 1 & (mod\ 6) \\ x \equiv 8 & (mod\ 15) \end{cases}$

27. Resolva as congruências:

(a) $x^{13} \equiv x\ (mod\ 1365)$;

(b) $x^{17} \equiv x\ (mod\ 4080)$.

28. Resolva as seguintes congruências

    (a) $x^2 + x + 1 \equiv 0 \ (mod\ 8)$;

    (b) $x^3 + x^2 + 1 \equiv 0 \ (mod\ 24)$;

    (c) $x^4 + x^2 + 1 \equiv 0 \ (mod\ 250)$.

29. Resolva a congruência

$$4x^4 + 9x^3 - 5x^2 - 21x + 61 \equiv 0 \ (mod\ 1125).$$

    Nota: Pretende-se que este seja um exercício de revisão dos vários temas tratados sobre congruências polinomiais.

30. Resolva a congruência $x^{50} + x^{12} \equiv 2 \ (mod\ 75)$.

31. Mostre que $5n^3 + 7n^5 \equiv 0 \ (mod\ 12)$, para qualquer inteiro n.

32. Determine todos os números inteiros cuja divisão inteira por 8 e por 7 dá respectiva e simultâneamente resto 6 e resto 5.

33. Um Coronel após ter sido destacado para comandar um regimento do Exército quis saber por quantos efectivos esse regimento era formado, com esse objectivo mandou-os dispor sucessivamente em colunas de:

    37 indivíduos, tendo sobrado um indivíduo;
    32 indivíduos, tendo sobrado 4 indivíduos;
    27 indivíduos, tendo sobrado um indivíduo.

    Sabendo que um regimento tem menos de 10 000 efectivos, determine quantas pessoas constituíam esse regimento.

34. Um casal resolveu ir fazer uma viagem à volta do mundo. Sabendo que partiram no dia 1 de Março de um ano bissexto num domingo, que chegaram no dia 6 de Março, segunda-feira e que demoraram menos de 4 anos, determine quantos dias demorou a viagem usando o teorema chinês do resto.

Capítulo 3

Resíduos quadráticos

3.1 Introdução

Neste capítulo, vamos estudar a resolubilidade de congruências polinomiais de segundo grau

$$uy^2 \ + \ vy \ + \ w \ \equiv 0 \ (mod \ m) \quad (2 < m \not| u)$$

Repare-se que a condição $2 < m \not| u$ evita que o grau do polinómio no primeiro membro desça. Vamos ver como se pode reduzir este estudo a congruências da forma

$$x^2 \ \equiv a \ (mod \ p) \quad (p \text{ primo maior que } 2 \ \& \ p \not| a) \tag{3.1}$$

Comecemos por observar que, fazendo $a = v^2 - 4uw, \ x = 2uy + v$, as soluções da congruência inicial se encontram entre as da congruência

$$x^2 \equiv a \quad (mod \ 4um), \tag{3.2}$$

as quais são soluções do sistema

$$\begin{cases} x^2 \equiv a \qquad (mod \ p_i^{\alpha_i}) \\ 1 \leq i \leq k \end{cases}$$

se $4um = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ em representação canónica, resolvendo-se cada uma das congruências a partir da inicial $x^2 \equiv a \ (mod \ p)$. Na verdade, se $m \not| 4u^2$, as soluções pretendidas podem encontrar-se entre as da congruência

$$x^2 \equiv a \quad (mod \ m), \tag{3.3}$$

potencialmente com menos soluções.

Uma outra forma de considerar o problema consiste em observar que, se m é primo, o inverso $(2u)^*$ existe $(mod \ m)$, $\Delta := u^2 - vw$ e $z^2 \equiv \Delta \ (mod \ m)$, então

$$uy^2 \ + \ vy \ + \ w \ \equiv 0 \ (mod \ m) \ \Leftrightarrow \ u \equiv (-v \pm z)(2u)^* \quad (mod \ m).$$

Organizemos o estudo.

3.2 Preliminares

O número inteiro a diz-se **resíduo quadrático** $(mod\ n)$ se $mdc(a,n) = 1$ e a congruência $x^2 \equiv a\ (mod\ n)$ tem solução; caso contrário diz-se resíduo **não quadrático**.

Em primeiro lugar: se $a \in \mathbb{Z}$ é resíduo quadrático $(mod\ m)$, então é resíduo quadrático $(mod\ p)$, para qualquer número primo que divida m. Pelo que as soluções de $x^2 \equiv a\ (mod\ m)$ se encontram entre as do sistema

$$\begin{cases} x^2 \equiv a & (mod\ p) \\ p|m & p\ primo \end{cases}$$

Além disso *qualquer número inteiro ímpar é resíduo quadrático* $(mod\ 2)$; assim basta considerar primos ímpares. Mas podemos ser mais precisos.

Lema 3.2.1 *Se p é número primo ímpar e $p \not| a$, a congruência*

$$x^2 \equiv a\ (mod\ p^\alpha) \tag{3.4}$$

tem solução sse o mesmo acontece com

$$x^2 \equiv a\ (mod\ p^{\alpha+1}). \tag{3.5}$$

De facto, ambas as congruências têm o mesmo número de soluções.

Dem. (se) Qualquer solução da congruência (3.5)é solução de (3.4).

(só se) Se $x^2 \equiv a\ (mod\ p^\alpha)$ e $(2x)^*$ designa um inverso de $2x\ (mod\ p)$, então

$$(x + kp^\alpha)^2 \equiv a\ (mod\ p^{\alpha+1}) \quad se \quad k \equiv k(x) = -(2x)^* \frac{x^2 - a}{p^\alpha}\ (mod\ p), \tag{3.6}$$

pois a última expressão implica

$$2xkp^\alpha \ \equiv\ x^2 - a\ \ (mod\ p^{\alpha+1}).$$

Finalmente observe-se que duas soluções da forma (3.6) da congruência (3.5) que sejam congruentes $(mod\ p^{\alpha+1})$ provêm de soluções congruentes $(mod\ p^\alpha)$ da primeira. Resumindo: há uma injecção do conjunto das soluções de (3.4) no das soluções de (3.5) que, por sua vez está contido naquele, i.e., são equipotentes. □

Segue-se

Corolário 3.2.1 *Se p é um número primo ímpar e $p \not| a$, o número de soluções das congruências $x^2 \equiv a\ (mod\ p)$ & $x^2 \equiv a\ (mod\ p^{\alpha+1})$ é o mesmo.*

E podemos concluir

Teorema 3.2.1 *Se m é ímpar e maior que 2, a é resíduo quadrático $(mod\ m)$ sse é resíduo quadrático $(mod\ p)$, para todos os números primos p que dividem m.*

Um outro resultado que interessa ter em conta é:

Teorema 3.2.2 *Se p é número primo ímpar, há $\frac{p-1}{2}$ resíduos quadráticos $(mod\ p)$ que são os elementos de $\{i^2|\ 1 \leq i \leq \frac{p-1}{2}\}$.*

Dem. verifiquemos que os resíduos descritos não são congruentes $(mod\ p)$. Ora $i^2 \equiv j^2\ (mod\ p)$ sse $p|i-j$ ou $p|i+j$, isto é, sse $i \equiv j$ *ou* $i \equiv -j\ (mod\ p)$; mas, para valores de i e j entre 1 e $\frac{p-1}{2}$, estas condições são equivalentes a $i = j$. Como os resíduos entre $\frac{p+1}{2}$ e p são simétricos $(mod\ p)$ dos já considerados, têm os mesmos quadrados $(mod\ p)$ e descrevemos de facto todos os resíduos quadráticos $(mod\ p)$. □

É claro que 1 é sempre resíduo quadrático. Mais precisamente

Lema 3.2.2 *Se p é número primo,*

$$x^2 \equiv 1\ (mod\ p) \quad \Leftrightarrow \quad [x \equiv 1\ (mod\ p) \quad ou \quad x \equiv -1\ (mod\ p)]$$

3.3 Lei de Reciprocidade Quadrática

O **símbolo de Legendre** $\left(\frac{a}{p}\right)$ é um instrumento de determinação do carácter quadrático do número inteiro ou resíduo $a\ (mod\ p)$ e define-se do seguinte modo

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & a\ é\ quadrático\ (mod\ p) \\ -1 & caso\ contrário \end{cases} \qquad (p \text{ é primo}) \tag{3.7}$$

É bastante simples verificar que

Teorema 3.3.1 *Se $p \not| a$ & $p \not| b$ & $a \equiv b\ (mod\ p)$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$*

Desenvolvamos algumas técnicas de cálculo

Teorema 3.3.2 (Critério de Euler) *Se p é primo ímpar e $p \not| a$, então*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \qquad (mod\ p) \tag{3.8}$$

Dem.
I) a é resíduo quadrático.

Neste caso temos, por um lado $x^2 \equiv a \ (mod\ p)$, para algum x, pelo que $p \not| x$, e daí

$$\left(\frac{a}{p}\right) = 1 \equiv x^{p-1} \equiv (x^2)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \ (mod\ p).$$

II) a não é resíduo quadrático

Repare-se que, pelo Pequeno Teorema de Fermat,

$$(a^{\frac{p-1}{2}})^2 \equiv 1 \ (mod\ p);$$

pelo que (lema 3.2.2)

$$a^{\frac{p-1}{2}} \equiv \pm 1 \ (mod\ p).$$

Defina-se

$$Q_p := \{i^2 |\ 1 \leq i \leq \frac{p-1}{2}\};$$

Como $x^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$ para qualquer $x \in Q_p$ e Q_p tem precisamente $\frac{p-1}{2}$ elementos, pelo Teorema de Lagrange (2.5.2), $a \notin Q_p$; consequentemente

$$\left(\frac{a}{p}\right) \ = \ -1 \ \equiv \ a^{\frac{p-1}{2}} \ (mod\ p).$$

□

Obtém-se então

Corolário 3.3.1 *Se p é um número primo ímpar , então*

1. $\left(\frac{ab}{p}\right) \ = \ \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \quad (p \not| a \ \ \& \ \ p \not| b)$
2. $\left(\frac{-1}{p}\right) \ = \ (-1)^{\frac{p-1}{2}}$
3. -1 *é resíduo quadrático* $(mod\ p)$*, sse* $p = 2$ *ou* $p \equiv 1 \ (mod\ 4)$

A terceira asserção é já conhecida (teorema 2.4.6); a segunda e a primeira resultam de o símbolo de Legendre só tomar os valores $0, 1$ ou -1 e por aplicação do critério de Euler.

Dado $n \in \mathbb{N}\backslash\{1, 2\}$, seja

$$L_n \ = \ \begin{cases} \{i \in \mathbb{Z} |\ |i| \leq \frac{n}{2}\} & \text{se } n \text{ é ímpar} \\ \\ \{i \in \mathbb{Z} |\ |i| < \frac{n}{2}\} \cup \{\frac{n}{2}\} & \text{se } n \text{ é par.} \end{cases}$$

L_n é o sistema completo de resíduos $(mod\ n)$, de menor valor absoluto. Para cada $x \in \mathbb{Z}$ e cada $n \in \mathbb{N}$, designe-se por $\hat{x}$ o resíduo em L_n congruente com $x \ (mod\ n)$.

Teorema 3.3.3 (Lema de Gauss) *Se p é um número primo ímpar que não divide a e $l = \#\{j|\ 1 \leq j \leq \frac{p-1}{2}\ \ \&\ \ \hat{ja} < 0\}$, então*

$$\left(\frac{a}{p}\right) \ = \ (-1)^l.$$

Dem. Como $p \not| a$, a função $i \mapsto \hat{ia}$ é uma permutação de $\{i \in \mathbb{Z}|\ 1 \leq |i| \leq \frac{p-1}{2}\}$, em particular, $\#\{\hat{ia}|\ 1 \leq i \leq \frac{p-1}{2}\}$

$\{|\hat{ja}|:\ 1 \leq j \leq \frac{p-1}{2}\} = \{1, 2, \cdots, \frac{p-1}{2}\}$, pelo que, por um lado

$$\prod_{j=1}^{\frac{p-1}{2}} \hat{ja} \ = \ (-1)^l \left(\frac{p-1}{2}\right)!$$

e por outro

$$\prod_{j=1}^{\frac{p-1}{2}} \hat{ja} \ \equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \ \ (mod\ p);$$

considerando o critério de Euler (teorema 3.3.2)

$$\left(\frac{a}{p}\right) \ \equiv \ a^{\frac{p-1}{2}} \ \equiv \ (-1)^l$$

e $\left(\frac{a}{p}\right) = (-1)^l$. □

Corolário 3.3.2 *Quando p é um número primo ímpar,*

$$\left(\frac{2}{p}\right) \ = \ (-1)^{\frac{p^2-1}{8}}$$

e, consequentemente: 2 é resíduo quadrático $(mod\ p)$ sse $p \equiv \pm 1\ (mod\ 8)$.

Dem. Para $1 \leq j \leq \frac{p-1}{2}$ tem-se

$$\begin{cases} \hat{2j} = 2j & 1 \leq j \leq \frac{p-1}{4} \\ \hat{2j} = 2j - p & \frac{p-1}{4} < j \leq \frac{p-1}{2} \end{cases}$$

portanto o número l do lema de Gauss verifica

$$l \ = \ \frac{p-1}{2} \ - \ \left[\frac{p-1}{4}\right]$$

e o segundo membro tem a mesma paridade que $\frac{p^2-1}{8}$, como se pode ver observando que $p \equiv \pm 1 \ (mod\ 4)$, portanto para certos $k \in \mathbb{Z}$, vem

$$\begin{aligned} \frac{p-1}{2} - \left[\frac{p-1}{4}\right] &= k \ \ \& \ \ \frac{p^2-1}{8} = 2k^2 + k \\ &ou \\ \frac{p-1}{2} - \left[\frac{p-1}{4}\right] &= 2k-1 \ - \ [k - \frac{1}{2}] \ = \ k \ \ \& \ \ \frac{p^2-1}{8} = 2k^2 - k \end{aligned}$$

□

Teorema 3.3.4 (Lei de Reciprocidade Quadrática) *Se p e q são números primos ímpares então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \ = \ (-1)^{\frac{(p-1)(q-1)}{4}}$$

Por outras palavras: *se dois números primos ímpares são congruentes com* 3 $(mod\ 4)$*, então um e um só deles é resíduo quadrático mod o outro; caso contrário, qualquer deles é ou nenhum é resíduo quadrático mod o outro.*

Dem. Considere-se a figura 3.3.

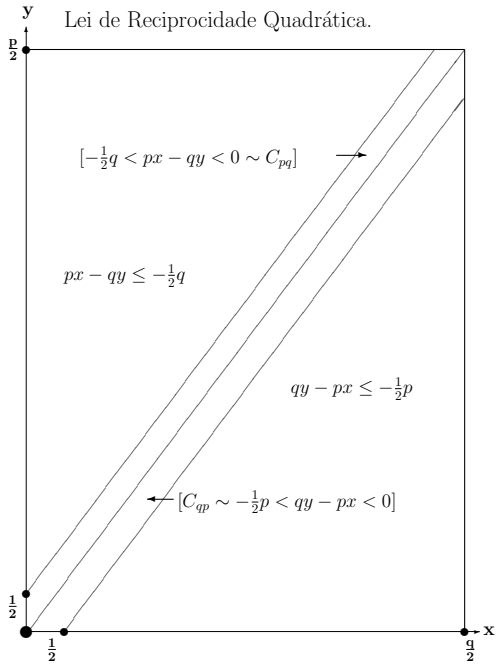

Figura 3.1: O rectângulo R.

Sejam

$$\begin{aligned} C_{pq} &= \{x \in \mathbb{Z} |\ 1 \leq x \leq \frac{q-1}{2} \ \ \& \ \ -\frac{q-1}{2} \leq px < 0 \pmod q\} \\ C_{qp} &= \{y \in \mathbb{Z} |\ 1 \leq y \leq \frac{p-1}{2} \ \ \& \ \ -\frac{p-1}{2} \leq qy < 0 \pmod p\} \\ l &= \#C_{pq} \\ m &= \#C_{qp} \end{aligned}$$

Pelo Lema de Gauss (teorema 3.3.3),

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \ = \ (-1)^{l+m}$$

Portanto basta mostrar que

$$l+m \ \ e \ \ \frac{(p-1)(q-1)}{4} \ \ têm \ \ a \ \ mesma \ \ paridade. \tag{3.9}$$

Ora, para cada $x \in C_{pq}$ existe um e só um $y \in \mathbb{Z}$ tal que $-\frac{q-1}{2} \leq px - qy < 0$ e simultâneamente $0 < y < \frac{p}{2}$ (repare-se que p é ímpar). Segue-se que

$$C_{pq} \ = \ \{(x,y) \in \mathbb{Z}^2 |\ 0 < x < \frac{1}{2}q \ \ \& \ \ 0 < y < \frac{1}{2}p \ \& \ \ -\frac{1}{2}q < px - qy < 0\}$$

Analogamente

$$C_{qp} \ = \ \{(x,y) \in \mathbb{Z}^2 |\ 0 < x < \frac{1}{2}q \ \ \& \ \ 0 < y < \frac{1}{2}p \ \ \& \ \ -\frac{1}{2}p < qy - px < 0\}$$

Se

$$R \ = \ \{(x,y) \in \mathbb{Z}^2 |\ 0 < x < \frac{1}{2}q \ \ \& \ \ 0 < y < \frac{1}{2}p\},$$

então $\#R = \frac{(q-1)(p-1)}{4}$ e $\#R - (l+m)$ é o número de pares $(x,y) \in R$ tais que

$$-\frac{1}{2}q < px - qy < 0 \quad ou \quad -\frac{1}{2}p < qy - px < 0;$$

estas condições definem dois conjuntos dijuntos equipotentes pois

$$(x,y) \mapsto \frac{1}{2}(q+1, p+1) - (x', y')$$

define uma bijecção entre eles. Conclui-se que vale a condição (3.9). □

3.4 Exercícios

1. Determine todos os números primos ímpares p para os quais -3 é resíduo quadrático $(mod\ p)$.

2. Determine todos os números primos ímpares p para os quais 7 é resíduo quadrático $(mod\ p)$.

3. Seja p um primo ímpar. Prove que 5 é um resíduo quadrático $(mod\ p)$ se $p \equiv \pm 1 (mod\ 10)$ e não é resíduo quadrático $(mod\ p)$ se $p \equiv \pm 3 (mod\ 10)$.

4. Encontre todos os resíduos quadráticos $(mod\ 29)$.

5. Calcule os seguintes símbolos de Legendre:

   (a) $\left(\frac{2}{29}\right), \left(\frac{-1}{29}\right), \left(\frac{5}{29}\right), \left(\frac{11}{29}\right)$;

   (b) $\left(\frac{2}{127}\right), \left(\frac{-1}{127}\right), \left(\frac{5}{127}\right), \left(\frac{11}{127}\right)$.

6. Determine, caso existam, as soluções das seguintes congruências quadráticas.

   (a) $5x^2 + 4x + 7 \equiv 0\ (mod\ 19)$.

   (b) $7x^2 + x + 11 \equiv 0\ (mod\ 17)$.

   (c) $2x^2 + 7x - 13 \equiv 0\ (mod\ 61)$.

7. Prove que 19 não divide $4n^2 + 4$ para qualquer número inteiro n.

8. Encontre os números primos $p < 100$ tais que a congruência quadrática

   $$x^2 + x - 3 \equiv 0\ (mod\ p)$$

   tem solução.

9. Resolva a congruência quadrática $x^2 + x - 10 \equiv 0\ (mod\ 2^4)$

10. Determine os valores de n para os quais -1 é resíduo quadrático $(mod\ n)$.

11. Procure as soluções da congruência quadrática $x^2 \equiv 7\ (mod\ 513)$

12. Verifique se 43 é um resíduo quadrático $(mod\ 923)$.

13. **Geradores de números primos.**

    (a) Mostre que $n^2 - n + 41$ é primo quando $1 \leq n \leq 40$, mas não para $n = 41$.

    (b) Mostre que $n^2 - 79n + 1061$ é primo quando $1 \leq n \leq 79$, mas não para $n = 80$.

(c) Mostre que $n^2 - 81n + 1681$ é primo quando $1 \leq n \leq 80$, mas não para $n = 81$.

Sugestão: Utilize o símbolo de Legendre para resíduos quadráticos.

14. (a) Mostre que para todos $\alpha \in \mathbb{N}$ e $n \in \mathbb{Z}$, $mdc(n, 2^\alpha) = 1$ se e só se $mdc(n, 2) = 1$.

    (b) Mostre que para todos $\alpha \in \mathbb{N}$ e $n \in \mathbb{Z}$, $(2^\alpha - n)^2 \equiv n^2 \ (mod\ 2^\alpha)$.

    (c) Mostre que para todos $\alpha \in \mathbb{N}$, $\alpha \geq 2$ e $n \in \mathbb{Z}$, $(2^{\alpha-1} - n)^2 \equiv n^2 \ (mod\ 2^\alpha)$.

    (d) Calcule todos os resíduos quadráticos módulo 2, 4 e 8.

    (e) Mostre que para todos $\alpha \in \mathbb{N}$, $\alpha \geq 3$ e $n \in \mathbb{Z}$, se $n \equiv 1 \ (mod\ 8)$, então $[n]_{2^\alpha} \in Q_{2^\alpha}$.

    (f) Mostre que para todos $\alpha \in \mathbb{N}$, $\alpha \geq 3$ e $n \in \mathbb{Z}$, se $[n]_{2^\alpha} \in Q_{2^\alpha}$, então $n \equiv 1 \ (mod\ 8)$.

15. Seja $f(x)$ um polinómio de coeficientes inteiros. Prove que

$$\sum_{x(mod\ p)} \left(\frac{f(ax+b)}{p}\right) = \sum_{x(mod\ p)} \left(\frac{f(x)}{p}\right), \quad \text{se } mdc(a,p) = 1$$

$$\sum_{x(mod\ p)} \left(\frac{af(x)}{p}\right) = \left(\frac{a}{p}\right) \sum_{x(mod\ p)} \left(\frac{f(x)}{p}\right), \quad \text{para todo } a.$$

16. Prove que se $\mathrm{mdc}(a, p) = 1$ então

$$\sum_{x=0}^{p-1} \left(\frac{ax+b}{p}\right) = 0.$$

17. Seja $f(x) = x(ax + b)$, onde $mdc(a, p) = mdc(b, p) = 1$. Prove que:

$$\sum_{x=1}^{p-1} \left(\frac{f(x)}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{a+bx}{p}\right) = -\left(\frac{a}{p}\right).$$

18. Sejam α, β números inteiros de valores possíveis ± 1. Seja $N(\alpha, \beta)$ o número de inteiros x no conjunto $\{1, 2, \ldots, p-2\}$ tais que

$$\left(\frac{x}{p}\right) = \alpha, \ \left(\frac{x+1}{p}\right) = \beta,$$

onde p é um primo ímpar. Prove que

$$4N(\alpha,\beta)=\sum_{x=1}^{p-2}\{1+\alpha\left(\frac{x}{p}\right)\}\{1+\beta\left(\frac{x+1}{p}\right)\}$$

e deduza

$$4N(\alpha,\beta)=p-2-\beta-\alpha\beta-\alpha\left(\frac{-1}{p}\right).$$

19. Use o exercício anterior para provar que para cada primo p existem inteiros x, y tais que $x^2+y^2+1\equiv 0\ (mod\ p)$.

Capítulo 4

Equações Diofantinas

Neste capítulo vamos estudar a resolução em $\mathbb{Z}$ de algumas equações **Diofantinas** da forma

$$ax^m + by^m = cz^k \quad m, n, k \in \mathbb{Z}$$

De um modo geral designaremos por **soluções triviais** as que têm pelo menos uma das coordenadas zero.

4.1 Ternos Pitagóricos

Um **terno pitagórico** é um terno ordenado (x, y, z) de números inteiros tal que

$$x^2 \ + \ y^2 \ = \ z^2. \tag{4.1}$$

É bastante simples verificar que os ternos pitagóricos triviais são os que têm pelo menos uma das primeiras coordenadas zero e as outras duas iguais ou simétricas. As soluções não triviais de (4.1) são caracterizadas pelo seguinte teorema.

Teorema 4.1.1 *O terno ordenado de números inteiros (x, y, z) é pitagórico sse é trivial ou existem $a, b, d \in \mathbb{N}$ verificando simultâneamente as seguintes condições.*

1. $b \ < \ a$
2. $mdc(a, b) = 1$
3. $|z| = (a^2 + b^2)d$
4. $\big[|x| = 2abd \quad \& \quad |y| = (a^2 - b^2)d\big] \quad ou \quad \big[|x| = (a^2 - b^2)d \ \ \& \ \ |y| = 2abd\big]$

Esta parte do texto é essencialmente dedicada à demonstração deste teorema.

Comecemos por notar que se tem o seguinte

Lema 4.1.1 *O terno (x, y, z) é pitagórico sse o mesmo acontece com $(|x|, |y|, |z|)$.*

Assim vamos limitar-nos a caracterizar as soluções não triviais da equação (4.1) em que todas as coordenadas sejam positivas, ou seja, vamos de facto passar a demonstrar

Teorema 4.1.2 *O terno ordenado de números naturais (x, y, z) é pitagórico sse existem $a, b, d \in \mathbb{N}$ verificando simultâneamente as seguintes condições.*

1. $b < a$
2. $mdc(a, b) = 1$
3. $z = (a^2 + b^2)d$
4. $\big[x = 2abd \quad \& \quad y = (a^2 - b^2)d\big] \quad ou \quad \big[x = (a^2 - b^2)d \quad \& \quad y = 2abd\big]$

Cálculos muito simples mostram que as quatro condições enunciadas no teorema são suficientes para que (x, y, z) seja um terno pitagórico não trivial. Veremos que são também necessárias.

Considere-se o seguinte lema.

Lema 4.1.2 *Para quaisquer números naturais m e n, $m^2|n^2$ sse $m|n$.*

Dem. É imediato que $m|n \Rightarrow m^2|n^2$, para quaisquer $m, n \in \mathbb{Z}$. A implicação recíproca, baseia-se em que um número primo divide um quadrado se e só se divide a base e no facto de todos os factores de base prima na decomposição canónica (Teorema Fundamental) de um quadrado perfeito terem expoente par. □

Como consequência tem-se

Lema 4.1.3 *Se (x, y, z) é um terno pitagórico de números naturais, então*

$$mdc(x, y, z) = mdc(x, y) = mdc(x, z) = mdc(y, z).$$

Dem. Sejam (x, y, z) um terno pitagórico de números naturais, $d = mdc(x, y, z)$ e, por exemplo $d_1 = mdc(x, z)$. Queremos mostrar que

$$d = d_1.$$

Comecemos por observar que

$$mdc(x, y, z) := mdc(mdc(x, y), z) = mdc(x, mdc(y, z)) = mdc(y, mdc(x, z)),$$

de onde se obtém, em particular, $d = mdc(y, d_1)$. Como $y^2 = z^2 - x^2$, também $d_1^2|y^2$ e, pelo lema 4.1.2, $d_1|y$; mas então $d_1 = d$. □

Digamos que um terno pitagórico (x, y, z) é **primitivo** se

$$x, y, z \in \mathbb{N} \quad \& \quad mdc(x, y, z) = 1.$$

Do lema anterior (lema 4.1.3), resulta imediatamente o seguinte teorema.

Teorema 4.1.3 *As condições seguintes são equivalentes para um terno pitagórico* (x, y, z)

1. (x, y, z) *é primitivo.*
2. *Duas das coordenadas do terno são primas entre si.*
3. *As coordenadas do terno são primas entre si duas a duas.*

E deste pode obter-se ainda:

Teorema 4.1.4 *Dado o terno pitagórico* $(x, y, z) \in \mathbb{N}^3$, *se*

$$d \in \mathbb{N} \quad \& \quad x = du \quad \& \quad y = dv \quad \& \quad z = dw \tag{4.2}$$

então $d = mdc(x, y, z)$ *sse* (u, v, w) *é terno pitagórico primitivo.*

Dem. Suponha-se que (x, y, z), (u, v, w) e d são dados como em (4.2).
(se) Por hipótese (u, v, w) é terno pitagórico primitivo e $d|x, y, z$. Vamos ver que $d = mdc(x, y)$, o que, pelo lema 4.1.3, arrasta $d = mdc(x, y, z)$. Ora, por hipótese e pelo lema 4.1.3, $mdc(u, v) = mdc(\frac{x}{d}, \frac{y}{d}) = 1$, pelo que $d = mdc(x, y)$, como se pretendia mostrar.
(só se) Tem-se

$$(du)^2 + (dv)^2 = (dw)^2;$$

dividindo por d^2 conclui-se que (u, v, w) é terno pitagórico; mais uma vez utilizando o lema 4.1.3, também se conclui que (u, v, w) é primitivo. □

Resumindo:

Teorema 4.1.5 *É condição necessária e suficiente para que o terno de números naturais* (x, y, z) *seja pitagórico que exista um terno pitagórico primitivo* (u, v, w) *e um número natural* d *tais que*

$$x = du \quad \& \quad y = dv \quad \& \quad z = dw \tag{4.3}$$

e neste caso $d = mdc(x, y, z)$.

Passamos então à caracterização dos ternos pitagóricos primitivos.

Teorema 4.1.6 *Para que o terno ordenado de números naturais* (x, y, z) *seja pitagórico primitivo é condição necessária e suficiente que existam* $a, b \in \mathbb{N}$ *verificando simultâneamente as seguintes condições.*

1. a *e* b *têm paridades distintas*
2. $b < a$

3. $mdc(a,b) = 1$

4. $z = a^2 + b^2$

5. $[x = 2ab \ \ \& \ y = a^2 - b^2] \quad ou \quad [x = a^2 - b^2 \ \ \& \ \ y = 2ab]$

Dem. Começamos com duas observações importantes. Uma cuja demonstração se deixa ao cuidado do leitor

Lema 4.1.4 *A soma de dois quadrados de números ímpares não é divisível por* 4.

e outra que demonstramos

Lema 4.1.5 *Se* (x, y, z) *é terno pitagórico primitivo, então* x *e* y *têm paridades diferentes.*

Dem. (do lema 4.1.5) Pelo lema 4.1.3, x e y não podem ser ambos pares e, pelo lema anterior (4.1.4), não podem ser ambos ímpares pois nesses casos z^2 seria par e consequentemente divisível por 4 e soma de dois quadrados de números ímpares. □

Lema 4.1.6 *Para quaisquer números naturais* a *e* b *primos entre si, tais que* $b < a$. *Tem-se uma das situações seguintes*

1. a *e* b *têm paridades distintas e nesse caso* $(2ab, a^2 - b^2, a^2 + b^2)$ *e* $(a^2 - b^2, 2ab, a^2 + b^2)$ *são ternos pitagóricos primitivos.*

2. a *e* b *são ambos ímpares e nesse caso* $(ab, \frac{a^2-b^2}{2}, \frac{a^2+b^2}{2})$ *e* $(\frac{a^2-b^2}{2}, ab, \frac{a^2+b^2}{2})$ *são ternos pitagóricos primitivos.*

Dem. Como a e b são primos entre si, não podem ser ambos pares, daí que as hipóteses apresentadas esgotam as possibilidades. Alguns cálculos simples mostram que os ternos em estudo são pitagóricos. Observe-se que no caso 2, como a e b são ambos ímpares, a diferença e a soma de quadrados são ambas pares.

Suponha-se então que

$$mdc(a,b) = 1 \quad \& \quad b < a \quad \& \quad d = mdc(2ab, a^2 - b^2, a^2 + b^2).$$

Vamos ver que no primeiro caso $d = 1$ e no segundo $d = 2$, o que, em vista do teorema 4.1.4, permite retirar as conclusões descritas.

1. Como a e b têm paridades diferentes, um é par e outro é ímpar de modo que $a^2 + b^2$ é ímpar, ou seja $2 \not| (a^2 + b^2)$ e consequentemente $2 \not| d$. Assim, se p for um número primo que divide d, ter-se-á

$$p \neq 2 \quad \& \quad p|ab \quad \& \quad p|(a+b)(a-b) \quad \& \quad p|a^2 + b^2.$$

Se $p|a$ e $p|a+b$, então $p|b$. Ora não há divisores primos comuns a a e b, donde d não tem divisores primos, isto é, $d = 1$. Analogamente se estudam os casos em que $p|a$ & $p|a-b$ ou $p|b$ & $p|a+b$ ou $p|b$ & $p|a-b$.

2. Vejamos que $d_1 = mdc(\frac{a^2-b^2}{2}, \frac{a^2+b^2}{2}) = 1$. Como $d_1 \in \mathbb{N}$, $d_1|\frac{a^2-b^2}{2}$ e $d_1|\frac{a^2+b^2}{2}$, somando ou subtraindo adequadamente, conclui-se que

$$d_1|a^2 \qquad \& \qquad d_1|b^2$$

pelo que se p fosse divisor primo de d_1, p seria divisor comum de a e de b, o que é impossível por estes serem números primos entre si; mas então $d_1 = 1$, por ser um número natural sem divisores primos; segue-se $mdc(a^2 - b^2, a^2 + b^2) = 2$ e, como $2|2ab$, $d = 2$. □

Continuando a demonstração do teorema 4.1.6:

Provámos no lema 4.1.6.1 que as condições do enunciado produzem ternos pitagóricos primitivos, ou seja formam uma condição suficiente como se pretende. Vejamos que formam também uma condição necessária.

Seja (x, y, z) um terno pitagórico primitivo. Pelo lema 4.1.5, x e y têm paridades diferentes. Digamos que x *é par* (e y é ímpar), por exemplo

$$x = 2k. \tag{4.4}$$

Tem-se

$$2|(2k)^2 = x^2 = z^2 - y^2 = (z - y)(z + y) \tag{4.5}$$

Pelo que $2|z - y$ ou $2|z + y$; em qualquer caso,

$$2|z - y \quad \& \quad 2|z + y$$

pois ambos os factores têm a mesma paridade. Segue-se que, para certos números naturais u e v se tem

$$z - y = 2u \quad \& \quad z + y = 2v \quad \& \quad u < v. \tag{4.6}$$

Resulta daqui, pela equação (4.5), que

$$k^2 = uv \tag{4.7}$$

Vejamos que

$$u \quad e \quad v \quad são \quad primos \quad entre \quad si: \tag{4.8}$$

Se p fosse um número primo divisor simultâneo de u e v, então ter-se-ia, pela condição (4.6)

$$p|u + v = z \quad \& \quad p|v - u = y;$$

mas então (x, y, z) não seria primitivo pelo lema 4.1.3, pois $p|mdc(y, z)$; assim necessariamente se dá (4.8). Mas então resulta da equação (4.7) que u, e v são por sua vez quadrados perfeitos e, para certos $a, b \in \mathbb{N}$ tem-se, ainda por (4.6),

$$u = b^2 \quad \& \quad v = a^2 \quad \& \quad b < a \quad \& \quad mdc(a, b) = 1$$

E concluimos com a equação (4.4)

$$x = 2ab \quad \& \quad y = a^2 - b^2 \quad \& \quad z = a^2 + b^2.$$

tendo-se ainda que *a e b têm paridades distintas* pois, caso contrário, x e y seriam ambos pares.

O caso em x é ímpar (e y é par) tratar-se-ia de modo análogo, dando lugar à outra possibilidade em 5 no lema 4.1.6. □

Resumindo: o teorema 4.1.2 caraceriza os ternos pitagóricos de números naturais como múltiplos naturais de ternos que se prova serem os únicos primitivos; os ternos pitagóricos em $\mathbb{Z}$ serão então obtidos de ternos em $\mathbb{N}$ por variações de sinal nas coordenadas (lema 4.1.1).

4.2 Somas de duas quartas potências

Demonstraremos o seguinte:

Teorema 4.2.1

$$x^4 + y^4 = z^2$$

só tem soluções triviais.

Entendendo *soluções triviais* como aquelas em que uma das coordenadas x ou y é nula.

Dem. Suponhamos que existem de facto soluções não triviais e, portanto existem números inteiros $u,\ v,\ w$ para os quais

$$u^4 + v^4 = w^2 \qquad \& \qquad u \neq 0 \quad \& \quad v \neq 0 \quad \& \quad w > 0.$$

De outro modo

$$C := \{z \in \mathbb{N} | \quad \exists x \in \mathbb{N}\ \exists y \in \mathbb{N} \quad x^4 + y^4 = z^2\} \neq \emptyset. \tag{4.9}$$

Assim sendo (u^2, v^2, w) é terno pitagórico; como, se $mdc(u, v) = d$, então $(\frac{u^2}{d^2}, \frac{v^2}{d^2}, \frac{w}{d^2})$ seria terno pitagórico primitivo e $(\frac{u}{d}, \frac{v}{d}, \frac{w}{d}) \in C$, podemos supor que (u^2, v^2, w)

é primitivo, pelo que, pelo teorema 4.1.6, possivelmente trocando u com v, existem números naturais $a,\ b$ tais que

$$\begin{aligned} a \text{ e } b \quad & \text{têm} \quad \text{paridades distintas}, && (4.10)\\ a \ &> \ b, && (4.11)\\ mdc(a,b) \quad &= \quad 1, && (4.12)\\ w \quad &= \quad a^2+b^2, && (4.13)\\ u^2 \quad &= \quad 2ab, && (4.14)\\ v^2 \quad &= \quad a^2-b^2; && (4.15) \end{aligned}$$

admitamos que valem estas mesmas condições. Em primeiro lugar, por (4.10),

$$a \text{ é ímpar e } b \text{ é par}, \tag{4.16}$$

porque se a fosse par, viria

$$v^2 \ = \ a^2-b^2 \ \equiv \ -b^2 \ \equiv \ -1 \pmod 4,$$

o que não pode acontecer porque v é ímpar e daí $v^2 \equiv 1 \pmod 4$. Ora $a^2 = v^2+b^2$, por (4.15), e (v,b,a) é terno pitagórico primitivo, por (4.12). Por (4.16) e pelo teorema 4.1.6, existem números naturais s e t tais que

$$s \text{ e } t \text{ têm paridades distintas},$$

$$s \ > \ t,$$

$$\begin{aligned} mdc(s,t) \ &= \ 1, && (4.17)\\ a \ &= \ s^2+t^2, && (4.18)\\ b \ &= \ 2st, && (4.19)\\ v \ &= \ s^2-t^2; && (4.20) \end{aligned}$$

mas então, por (4.14)

$$u^2 \ = \ 2ab \ = \ 4st(s^2+t^2) \tag{4.21}$$

e, como s e t são primos entre si, por (4.17), o mesmo acontece com s e s^2+t^2 e t e s^2+t^2, portanto $s,\ t$ e s^2+t^2 são quadrados perfeitos, digamos que, para certos números inteiros $x,\ y$ e z, que podemos supor não negativos,

$$s \ = \ x^2 \quad \& \quad t \ = \ y^2 \quad \& \quad s^2+t^2 \ = \ z^2 \tag{4.22}$$

e portanto

$$x^4 \ + \ y^4 \ = \ z^2,$$

ou seja

$$(x,y,z) \in C. \tag{4.23}$$

Vamos ver que

$$0 \ < \ z \ < \ w. \tag{4.24}$$

Se $s = 0 = t$, então $u = v = 0$, por (4.20) e (4.21), o que não acontece, portanto $0 < s^2 + t^2 = z^2$ e $z > 0$ porque estamos a supor que z não é negativo; por outro lado, por (4.22), (4.18) e (4.13)

$$z \ < \ z^2 \ = \ s^2 + t^2 \ = \ a \ < \ a^2 + b^2 \ = \ w.$$

Por (4.23) e (4.24), deduzimos que C não tem mínimo; tal não pode acontecer se se verifica (4.9), portanto $C = \emptyset$ e o teorema fica demonstrado. □

4.3 Somas de dois quadrados

Vamos caracterizar agora as soluções da equação

$$x^2 \ + \ y^2 \ = \ n \quad (0 \leq n \in \mathbb{Z}) \tag{4.25}$$

Comecemos por verificar que ela não tem sempre solução.

Exemplo 4.3.1 Pode verificar-se por tentativas que a equação $x^2 + y^2 = 7$ não tem solução em $\mathbb{Z}$: como 7 não é um quadrado perfeito,não há soluções triviais; por outro lado, as únicas expressões de 7 como soma de dois números naturais são 1+6, 2+5, 3+4 e suas comutadas e 2, 3, 5 e 6 também não são quadrados perfeitos.

Veremos de que maneira a existência de solução inteira para (4.25) depende da natureza de n.

Definição 4.3.1 *Um número natural n é* **simples** *se $n = 1$ ou n verifica a seguinte condição: Se p é um número primo*

$$p|n \ \Rightarrow \ \{p^2 \not| n \quad \& \quad [p = 2 \ ou \ p \equiv 1 \ (mod \ 4)]\}$$

Vamos demonstrar o seguinte:

Teorema 4.3.1 *A equação (4.25) tem solução sse existem $s, n_0 \in \mathbb{N}$ tais que n_0 é simples e $n = s^2 n_0$.*

Comecemos por observar que o exemplo 4.3.1 não é excepcional.

Lema 4.3.1 *Se $n \equiv 3 \ (mod \ 4)$, então n não é soma de dois quadrados.*

Dem. Um quadrado é congruente com 0 ou 1 (mod 4) consoante a base é par ou ímpar, pelo que uma soma de dois quadrados é congruente com 0, 1 ou 2 (mod 4). □

O exemplo seguinte também não é acidental

Exemplo 4.3.2 $5 = 1 + 4 = 1^2 + 2^2$

Lema 4.3.2 *Um número primo p é soma de dois quadrados sse $p = 2$ ou $p \equiv 1 \ (mod\ 4)$.*

Dem. (só se) Suponha-se que p é soma de dois quadrados, então pelo lema 4.3.1, $p \not\equiv 3 \ (mod\ 4)$. Ora os números congruentes com 0 ou 2 $(mod\ 4)$ são pares, pelo que p, sendo primo e par só pode ser 2, e se for ímpar, só resta $p \equiv 1 \ (mod\ 4)$.
(se) Se $p = 2$ então $p = 1^2 + 1^2$. Vejamos o caso

$$p \equiv 1 \ \ (mod\ 4). \tag{4.26}$$

Em primeiro lugar tem-se

$$\exists t \in \mathbb{N}\ \exists x \in \mathbb{Z}\ \left[x^2 + 1 = tp \quad \& \quad |x| \leq \frac{p-1}{2} < \frac{p}{2}\right] \tag{4.27}$$

pois a equação em (4.27) é equivalente à congruência $x^2 + 1 \equiv 0 \ (mod\ p)$, que tem solução por (4.26), podendo esta ser determinada pelo sistema *completo* de resíduos $(mod\ p)$

$$\{-\tfrac{p-1}{2} + i : \ 0 \leq i \leq p-1\}$$

onde os resíduos têm valor absoluto majorado como descrito em (4.27). Como $1 = 1^2$, tem-se que

$$C_p \ = \ \{t \in \mathbb{N} : \ tp \text{ é soma de dois quadrados}\} \neq \emptyset$$

De (4.27) deduz-se também

$$minC_p \ < \ p \tag{4.28}$$

pois se $t \in C_p$, então

$$t = \frac{x^2+1}{p} \leq \frac{\frac{p^2}{4}+1}{p} = \frac{p}{4} + \frac{1}{p} < \frac{p}{4} + \frac{p}{2} < p$$

Na verdade

$$minC_p \ = \ 1 \tag{4.29}$$

como se pode ver do seguinte modo: suponha-se que, pelo contrário,

$$1 < k = minC_p \quad \& \quad kp = a^2 + b^2 \tag{4.30}$$

Por um lado tem-se

$$\exists x, y \in \mathbb{Z}\ \exists m \in \mathbb{N}\ \{[x \neq 0 \ ou\ y \neq 0] \ \ \& \ \ |x|, |y| \leq \frac{k}{2} \ \ \& \ \ mk = x^2 + y^2\} \tag{4.31}$$

pois, por um lado, podemos tomar $x \equiv a \ (mod\ k)$ e $y \equiv b \ (mod\ k)$ no sistema completo de resíduos $(mod\ k)$ $\{-\frac{k}{2}+1+i : \ 0 \leq i \leq k-1\}$ se k é par, ou $\{-\frac{k-1}{2}+i : \ 0 \leq i \leq k-1\}$ se k é ímpar, verificando-se as inequações em (4.31); por outro lado, x e y não podem

ser nulos simultâneamente, já que, se $x = 0 = y$, então $a \equiv 0 \equiv b \ (mod\ k)$, pelo que $a^2 \equiv 0 \equiv b^2 \ (mod\ k^2)$; mas então ter-se-ia $kp = a^2 + b^2 \equiv 0 \ (mod\ k^2)$ ou seja $kp = \alpha k^2$ para algum $\alpha \in \mathbb{Z}$, de onde se concluiria $k|p$, o que é impossível por (4.28). Assim, sob a hipótese (4.30), também $0 \equiv kp = a^2 + b^2 \equiv x^2 + y^2 \ (mod\ k)$, isto é, $x^2 + y^2 = mk$ para algum $m \in \mathbb{N}$, ficando demonstrado (4.31) também sob a hipótese (4.30).

Mas podemos ser mais precisos ainda: nas condições (4.30)

$$m \ < \ k, \tag{4.32}$$

pois

$$m = \frac{x^2 + y^2}{k} \leq \frac{2k^2/4}{k} = \frac{k}{2} < k.$$

Vamos ainda poder concluir que

$$\exists u, v \in \mathbb{Z} \ u^2 + v^2 = mp, \tag{4.33}$$

o que, junto com (4.32) está em contradição com a definição de k em (4.30), seguindo-se que não pode ter-se $k > 1$, ou seja vale (4.29) como se pretendia provar. Deduzamos então (4.33):

$$k^2 mp = (kp)(mk) = (ay - bx)^2 + (ax + by)^2$$

Como x e y foram escolhidos de modo que $x \equiv a \ (mod\ k)$ e $y \equiv b \ (mod\ k)$, deduz-se que

$$ax + by \equiv a^2 + b^2 \equiv 0 \ (mod\ k) \quad \& \quad k|ax + by$$

e também

$$ay - bx \equiv ab - ba = 0 \ (mod\ k) \quad \& \quad k|ay - bx.$$

Segue-se que

$$mp = \left(\frac{ay - bx}{k}\right)^2 + \left(\frac{ax + by}{k}\right)^2$$

e as duas fracções do segundo membro são os u e v que procurávamos para deduzir (4.33).

O lema 4.3.2 está demonstrado. □

Para terminarmos a demonstração do teorema 4.3.1, interessa ter presente que

Lema 4.3.3 *Se dois números naturais são somas de dois quadrados, o seu produto também é.*

Dem. Basta lembrar a fórmula (do quadrado do valor absoluto) do produto dois números complexos [1] na forma algébrica: se $m = a^2 + b^2$ e $n = c^2 + d^2$, então $mn = (ac - bd)^2 + (ad + bc)^2$ □

[1] Veja-se a propósito (8.2)

Dem. (do teorema 4.3.1)
(se) Suponhamos então que $n = s^2 n_0$, em que n_0 é simples. Se $n_0 = 1$, imediatamente se tem $n = s^2 + 0^2$. Se, para números primos distintos p_i, $n_0 = p_1 \cdots p_k$, sendo possivelmente algum dos primos igual a 2 e os restantes congruentes com 1 $(mod\ 4)$, pelo lema anterior (lema 4.3.3) e pelo lema 4.3.2, tem-se

$$n \ = \ s^2(a^2 \ + \ b^2) \ = \ (sa)^2 \ + \ (sb)^2.$$

(só se) Suponha-se que n é soma de dois quadrados. Se $n = s^2 + 0^2$, o teorema vale com $n_0 = 1$. Se n não é um quadrado, escreva-se

$$n = a^2 + b^2 = \prod_{i=1}^{k} q_i^{\alpha_i} \cdot \prod_{i=1}^{r} q_{k+i}^{\alpha_{k+i}}$$

em que os q_i são primos distintos, os α_i são pares se $1 \leq i \leq k$ e ímpares se $k < i \leq k+r$, digamos

$$\alpha_{k+i} = 2\beta_i + 1 \quad (1 \leq i \leq r).$$

e faça-se

$$s^2 = \prod_{i=1}^{k} q_i^{\alpha_i} \cdot \prod_{i=1}^{r} q_{k+i}^{2\beta_i} \quad \& \quad n_0 = \prod_{i=1}^{r} q_{k+i}.$$

Falta verificar que os $q_{k+i} = p_i$ são 2 ou congruentes com 1 $(mod\ 4)$. Suponhamos que não e portanto, reordenando convenientemente,

$$p_1 \equiv 3\ (mod\ 4)$$

Repare-se que $n = a^2 + b^2 \equiv 0\ (mod\ p_1)$, portanto

$$p_1 | a,$$

já que, caso contrário, a teria inverso a^* $(mod\ p_1)$, e viria $1 + (a^* b)^2 \equiv 0\ (mod\ p_1)$, o que é impossível porque $p_1 \not\equiv 1\ (mod\ 4)$. Analogamente se conclui que

$$p_1 | b$$

e portanto

$$p_1^2 | a^2 + b^2 = n.$$

Como p_1 é distinto dos outros p_i, $p_1 | s$; segue-se que

$$\frac{n}{{p_1}^2} = \left(\frac{a}{p_1}\right)^2 + \left(\frac{b}{p_1}\right)^2 = \left(\frac{s}{p_1}\right)^2 p_1 \cdots p_r.$$

Por este processo eliminamos p_1 de s mas mantemos a forma

$$\bar{n} = \bar{s}^2 p_1 \cdots p_r$$

o que implica que $p_1 | \bar{s}$. Em suma, não podemos supor que $p_1 \equiv 3\ (mod\ 4)$ e o teorema fica demonstrado. □

4.4 Somas de quatro quadrados

Vamos demonstrar o seguinte

Teorema 4.4.1 *Qualquer número natural é soma de quatro quadrados de números inteiros.*

Convencionamos, para abreviar, que *soma de quatro quadrados* **deve entender-se como** *soma de quatro quadrados de números inteiros.*

Observando que vale

Lema 4.4.1 *O produto de dois números naturais que são somas de quatro quadrados é soma de quatro quadrados.*

bastará então provar

Lema 4.4.2 *Qualquer número primo é soma de quatro quadrados.*

Dem. (do lema 4.4.1)[2] Basta tomar em consideração a seguinte **Identidade de Lagrange**: para quaisquer $a, b, c, d, u, v, x, y \in \mathbb{R}$,

$$\begin{aligned}(a^2+b^2+c^2+d^2)(u^2+v^2+x^2+y^2) &= (au+bv+cx+dy)^2+(av-bu-cy+dx)^2\\ &+ (ax+by-cu-dv)^2+(ay-bx+cv-du)^2.\end{aligned}$$

□

A demonstração do lema 4.4.2 é essencialmemte semelhante à do lema 4.3.2, mas precisamos ainda de um outro lema.

Lema 4.4.3 *A congruência*

$$x^2+y^2 \equiv -1 \pmod p \tag{4.34}$$

tem solução para qualquer número primo p.

Dem. É claro que $1^2+0^2 = 1 \equiv -1 \pmod 2$. Portanto suporemos de ora em diante que p *designa um número primo ímpar.*

Relembrando a contagem de resíduos quadráticos sabemos que os x^2, para $0 \leq x \leq \frac{p-1}{2}$, são $\frac{p+1}{2}$ resíduos não congruentes $(mod\ p)$ dois a dois; o mesmo acontece com os $-1-y^2$, para $0 \leq y \leq \frac{p-1}{2}$. Como um sistema completo de resíduos tem p elementos, existem x^2 e $-1-y^2$ congruentes entre si $(mod\ p)$; mas então $x^2+1+y^2 \equiv 0 \pmod p$.

□

[2] Veja-se a propósito o teorema 8.2.3

Dem. (do lema 4.4.2) Queremos provar que, para qualquer número primo p, existem $x, y, z, w \in \mathbb{Z}$ tais que

$$p \;=\; x^2 + y^2 + z^2 + w^2. \tag{4.35}$$

De novo $2 = 1^2 + 1^2 + 0^2 + 0^2$, pelo que passaremos a supor que p *designa um primo ímpar*.

Em primeiro lugar, resulta do lema 4.4.3 que, para certos $m, x, y \in \mathbb{Z}$,

$$mp \;=\; x^2 + y^2 + 1^2 + 0^2 \quad \& \quad 0 \leq 0, 1, x, y \leq \frac{p-1}{2}. \tag{4.36}$$

Assim, definindo

$$k \;:=\; \min\{m \in \mathbb{N} |\; \exists x, y, z, w \; mp = x^2 + y^2 + z^2 + w^2\} \tag{4.37}$$

podemos concluir que

$$1 \;\leq k \;< p. \tag{4.38}$$

É claro que se $k = 1$ nada há mais a demonstrar. Vamos ver que $1 < k$ não pode acontecer. Suponhamos então que na verdade $1 < k$.

Se k é par, o mesmo acontece com $x + y + z + w$, portanto ou todos os x, y, z, w são pares ou todos são ímpares ou dois são pares e dois são ímpares; suponha-se que no último caso x e y têm a mesma paridade assim como z e w. Tem-se então

$$\frac{k}{2}p \;=\; \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2.$$

o que contradiz a minimalidade de k, dada em (4.37). Portanto k não é par, ou seja k *terá de ser ímpar*.

Se k dividisse todos os x, y, z, w então $k^2 | kp$ e daí $k|p$, o que também não pode acontecer. Assim $k \geq 3$. Por definição de k em (4.37),

$$x^2 + y^2 + z^2 + w^2 \; equiv \; 0 \; (mod \; k)$$

e podemos escolher resíduos positivos $(mod\ k)$, a, b, c, d de módulo não superior a $\frac{k}{2}$, e $s \in \mathbb{N}$ tais que

$$s < k \quad \& \quad x \equiv a \quad \& \quad y \equiv b \quad \& \quad z \equiv c \quad \& \quad w \equiv d \, (mod k) \quad \& \quad a^2 + b^2 + c^2 + d^2 = sk.$$

Pelo lema 4.4.1, existem $e, f, g, h \in \mathbb{Z}$ tais que

$$kpks \;=\; e^2 + f^2 + g^2 + h^2. \tag{4.39}$$

Como os e, f, g, h podem ser dados pela Identidade de Lagrange, pode supor-se que são todos divisíveis por k, pelo que, dividindo em (4.39) por k^2, representamos sp como soma de quatro quadrados e $s < k$, contradizendo a definição de k. Em qualquer caso concluimos que k não pode ser maior que 1. □

4.5 Exercícios

1. Resolva as seguintes equações Diofantinas:
   (a) $x^2 + y^2 = 51$;
   (b) $x^2 + y^2 + z^2 = 18$;
   (c) $x^2 + 2xy + 2y^2 = 17$;
   (d) $4x^2 + 12xy + 10y^2 = 26$.
2. Resolva a equação Diofantina em (x, y, z) $x^2 - y^2 = z$. e conclua que a equação Diofantina $x^2 - y^2 = m^k$ tem solução (x, y) quando $m, k \geq 3$.
3. Mostre que nem todos os números inteiros positivos são somas de, no máximo, três quadrados.
4. O **Teorema de Fermat** afirma:
   Quando $n > 2$, a equação Diofantina $x^n + y^n = z^n$ só tem soluções triviais.
   Verifique que vale quando $n = 4$, suponha-o demonstrado quando n é primo ímpar e apresente uma demonstração para os restantes casos baseada nestes dois.
5. Determine cinco ternos Pitagóricos primitivos distintos.
6. Mostre que para cada número inteiro $n \geq 3$ existe um terno Pitagórico em que uma das coordenadas é n.
7. Resolva a equação Diofantina $x^2 + 4y^2 = z^2$.
8. Determine todos os ângulos θ para os quais $sen\ \theta$ e $cos\ \theta$ são números racionais.
9. Mostre que a equação Diofantina $x^2 + y^4 = z^2$ tem um número infinito de soluções não triviais tais que $mdc(x, y) = 1$.
10. Resolva a equação Diofantina $x^2 + py^2 = z^2$ nos casos em que p é primo.
11. Resolva a equação Diofantina $(x^2 + y^2 - 2)^4 + 16 = z^2$.
12. Suponha que $mdc(a, b) = 1$. Mostre que se a não é soma de dois quadrados, então ab também não é.
13. Mostre que a equação $5x^2 + 14xy + 10y^2 = n$ tem soluções em inteiros se e só se n é soma de dois quadrados.
14. Mostre que a equação $(x^2 + 1)^4 + (y^2 + 2)^4 = (z + 4)^2$ não tem soluções inteiras.
15. Determine todas as soluções da equação diofantina
$$(x^4 + 1)^4 + y^{12} = (z^2 + 1)^4.$$

16. Considere a equação $x^2 - 6y^2 = 1$.

    (a) Mostre que se $(x_0, y_0) \in \mathbb{Z}^2$ é uma solução da equação, então $(5x_0+12y_0, 5y_0+2x_0)$ também é.

    (b) Use a alínea anterior para obter pelo menos cinco soluções distintas da equação.

    (c) Mostre que a equação tem infinitas soluções.

17. Mostre que se $\frac{n}{4^k} \equiv 7 \ (mod\ 8) \quad (k \in \mathbb{N})$, então n não é soma de três quadrados.

Capítulo 5

Funções aritméticas

5.1 Introdução

Uma função real de variável natural diz-se **aritmética.** Consideremos algumas funções aritméticas importantes.

Para cada $n \in \mathbb{N}$ define-se

$$\begin{aligned} d(n) &= \textit{número de divisores positivos de } n \\ \sigma(n) &= \textit{soma dos divisores positivos de } n \end{aligned}$$

Teorema 5.1.1 *Se $p_1, \cdots, p_k$ são os divisores primos de $n \in \mathbb{N}$ e para certos números naturais $\alpha_i \quad n = \prod_{i=1}^{k} p_i^{\alpha_i}$, então*

$$d(n) = \prod_{i=1}^{k}(1+\alpha_i) \tag{5.1}$$

$$\sigma(n) = \prod_{i=1}^{k}\sum_{j=0}^{\alpha_i} p_i^j \tag{5.2}$$

$$= \prod_{i=1}^{k}\frac{p_i^{\alpha_i+1}-1}{p_i-1} \tag{5.3}$$

A validade destes dois resultados conclui-se das observações seguintes

1. Os números primos que dividem os divisores de n não triviais também dividem n, isto é

$$1 \neq d \mid n \;\Rightarrow\; d = \prod_{j=1}^{r} p_{i_j}^{\beta_j}$$

com $1 \leq \beta_j \leq \alpha_{i_j}$.

2. Consequentemente os divisores positivos de n são **os monómios** do desenvolvimento de
$$f(n) \;=\; (1+p_1+\cdots+p_1^{\alpha_1})\cdots(1+p_k+\cdots+p_k^{\alpha_k})$$

3. Assim $d(n)$ é o **número de monómios** do desenvolvimento do mesmo $f(n)$ e $\sigma(n)=f(n)$

Uma argumentação de contagem análoga às anteriores permite estabelecer o teorema seguinte. Demonstrá-lo-emos também via das propriedades das funções multiplicativas (teorema 5.5.2)

Teorema 5.1.2 *Se $p_1,\cdots,p_k$ são os divisores primos de $n\in\mathbb{N}$ e para certos números naturais α_i $\quad n=\prod_{i=1}^k p_i^{\alpha_i}$, então*

$$\phi(n) \;=\; n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) \;=\; \prod_{i=1}^{k}\left[p_i^{\alpha_i-1}(p_i-1)\right]. \tag{5.4}$$

Utilizaremos o lema seguinte.

Lema 5.1.1 *Sejam d e n números naturais e suponha-se que $d|n$. O conjunto $\{i\in\mathbb{N}|\ d|i\leq n\}$ tem $\frac{n}{d}$ elementos.*

Dem. Se $n=kd$, os elementos do conjunto em questão são precisamente $1d,\ 2d,\ \cdots,\ kd$.

□

Dem. (do teorema 5.1.2) Seja n um número natural maior que 1, representado na forma canónica por $p_1^{\alpha_1}\cdots p_k^{\alpha_k}$. Se designarmos por C o conjunto dos números entre 1 e n que *não são* primos com n e definirmos

$$C_i \;:=\; \{k\in\mathbb{N}|\ 1\leq k\leq n \quad \& \quad p_i|k\},$$

tem-se, por um lado
$$C \;=\; \cup_{i=1}^k C_i$$

e, por outro lado

$$C_{i_1}\cap\cdots\cap C_{i_s} \;=\; \{k\in\mathbb{N}|\ 1\leq k\leq n \quad \& \quad p_{i_1}\cdots p_{i_s}|k\} \qquad (i_1<\cdots<i_s;\ 1\leq s\leq k).$$

Portanto

$$\begin{aligned}\#C \;=&\sum_{i=1}^{k}\#C_i-\sum_{1\leq i_1<i_2\leq k}\#(C_{i_1}\cap C_{i_2}) \;+\sum_{1\leq i_1<i_2<i_3\leq k}\#(C_{i_1}\cap C_{i_2}\cap C_{i_3})-\cdots\\ &+\;(-1)^{k+1}\#(C_1\cap\cdots\cap C_k)\end{aligned}$$

Como, pelo lema 5.1.1,

$$\#C_{i_1} \cap \cdots \cap C_{i_s} \;=\; \frac{n}{p_{i_1} \cdots p_{i_s}} \;=\; n\frac{1}{p_{i_1}} \cdots \frac{1}{p_{i_s}},$$

concluimos

$$\begin{aligned} \#C \;=\; \sum_{i=1}^{k} \frac{n}{p_i} - \sum_{1 \le i_1 < i_2 \le k} n\frac{1}{p_{i_1}}\frac{1}{p_{i_2}} \quad &+ \quad \sum_{1 \le i_1 < i_2 < i_3 \le k} n\frac{1}{p_{i_1}}\frac{1}{p_{i_2}}\frac{1}{p_{i_3}} - \cdots \\ &+ \quad (-1)^{k+1} n\frac{1}{p_1} \cdots \frac{1}{p_k}. \end{aligned}$$

e, pondo n em evidência nesta última fórmula, como

$$\phi(n) \;=\; n - \#C,$$

$$\begin{aligned} \frac{\phi(n)}{n} &= 1 - \frac{\#C}{n} \\ &= 1 - \sum_{i=1}^{k} \frac{1}{p_i} + \sum_{1 \le i_1 < i_2 \le k} \frac{1}{p_{i_1}}\frac{1}{p_{i_2}} - \sum_{1 \le i_1 < i_2 < i_3 \le k} \frac{1}{p_{i_1}}\frac{1}{p_{i_2}}\frac{1}{p_{i_3}} + \cdots \\ &\qquad + (-1)^k \frac{1}{p_1} \cdots \frac{1}{p_k} \\ &= \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right), \end{aligned}$$

ou seja

$$\phi(n) \;=\; n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

□

Outras funções aritméticas que virão a ser-nos úteis: defina-se para cada $n \in \mathbb{N}$

$$\mathbf{1}(n) \;:=\; 1 \tag{5.5}$$

$$\mathbf{e}(n) \;:=\; \left[\frac{1}{n}\right] \;=\; \begin{cases} 1 & \textit{se } n = 1 \\ 0 & \textit{se } n > 1 \end{cases}. \tag{5.6}$$

$$\tag{5.7}$$

E ainda a função μ **de Möbius**, definida, para cada número natural n, por

$$\mu(n) \;=\; \begin{cases} 1 & \textit{se } \; n = 1 \\ 0 & \textit{se } \; \exists p \; [p \textit{ é primo } \& \; p^2 \mid n] \\ (-1)^k & \textit{se } \; n = p_1 \cdots p_k \textit{ com os } p_i \textit{ primos distintos.} \end{cases} \tag{5.8}$$

5.2 Produto de Dirichlet

Designemos por $\mathcal{A}$ o conjunto de todas as funções aritméticas. Uma forma que se observou ser conveniente de algebrizar $\mathcal{A}$ foi o produto **de convolução** ou **de Dirichlet**, designado por $*$ e definido por

$$f * g(n) = \sum_{d|n} f(d)g(\frac{n}{d}) \qquad (n \in \mathbb{N}). \tag{5.9}$$

As propriedades básicas deste produto ficam descritas nos teoremas seguintes, cuja demonstração se deixa a cargo do leitor. Recordem-se as funções definidas na secção anterior (5.1).

Teorema 5.2.1 *$(\mathcal{A}, *)$ é um monóide comutativo. Mais precisamente:*

1. *$*$ é associativa e comutativa,*
2. *$\mathbf{e}$ é elemento neutro para $*$.*

Designe-se por $\mathcal{A}_1$ o conjunto das funções aritméticas *não nulas em* 1.

Teorema 5.2.2 *Se $f \in \mathcal{A}_1$ e g é definida recursivamente por*

$$\begin{aligned} g(1) &= \frac{1}{f(1)} \\ g(n) &= -\frac{1}{f(1)} \sum_{d|n} f(d) g\left(\frac{n}{d}\right), \quad \text{se } n > 1, \end{aligned}$$

então

1. *$g * f = f * g = \mathbf{e}$,*
2. *$(\mathcal{A}_1, *)$ é grupo abeliano.*

5.3 Funções multiplicativas

Uma função aritmética f diz-se **multiplicativa** se verificar

$$mdc(m,n) = 1 \quad \Rightarrow \quad f(mn) = f(m)f(n) \qquad (m,n \in \mathbb{N}) \tag{5.10}$$

Um resultado natural:

Teorema 5.3.1 *Uma função aritmética não identicamente nula f é multiplicativa se e apenas se*

$$f(1) = 1 \quad \& \quad f\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) = \prod_{i=1}^{k} f\left(p_i^{\alpha_i}\right) \tag{5.11}$$

sempre que os p_i são primos distintos dois a dois e os α_i são número naturais.

Dem. Suponha-se que f é multiplicativa. Como $mdc(1,n)=1$, tem-se $f(1)=f(1\times 1)=f(1)f(1)$, de onde se segue $f(1)=0$ ou $f(1)=1$; ora, se $f(1)=0$, resulta $f(m)=f(1\times m)=f(1)f(m)=0$, pois $mdc(1,m)=1 \ \ (m\in\mathbb{N})$ e f é identicamente nula; assim, se $f\not\equiv 0$, necessariamente $f(1)=1$. A segunda parte da condição (5.11) é também necessária, pois potências de base prima são primas entre si se as bases são distintas.

Concluimos que a condição (5.11) é necessária.

Suponha-se agora que vale a condição (5.11) e que $mdc(m,n)=1$. De $f(1)=1$ obtém-se, para m=1, $f(mn)=f(n)=f(1)f(n)=f(mn)$ e, para $n=1$, $f(mn)=f(m)=f(m)f(n)$. Se $m\neq 1\neq n$, então as representações canónicas de m e de n não têm factores primos comuns e a segunda parte da condição (5.11) garante que $f(mn)=f(m)f(n)$.

Concluimos que a condição (5.11) é suficiente. □

É um exercício fácil demonstrar agora o seguinte corolário.

Corolário 5.3.1 *Duas funções multiplicativas coincidem sse coincidirem nas potências de expoente inteiro não negativo dos números primos.*

Ilustremos a definição:

Teorema 5.3.2 *1. Todas as funções definidas na secção anterior (5.1) são multiplicativas.*

2. De facto, o produto de convolução de duas funções multiplicativas é também multiplicativo.

Dem. (*1*) Para verificar que d, σ e ϕ, basta observar que dois números naturais são primos entre si apenas quando não têm divisores primos comuns; consequentemente, se $n=\prod_{i=1}^{k} p_i^{\alpha_i}$ e $m=\prod_{i=1}^{r} q_i^{\beta_i}$, com primos p_i e q_j totalmente distintos dois a dois, e $mdc(m,n)=1$, tem-se

$$mn \ = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=1}^{r} q_i^{\beta_i}$$

e resta aplicar as equações em 5.1 e 5.4.

1 é obviamente multiplicativa, pois só toma o valor 1.

Quanto a **e**: dados números naturais m e n *quaisquer*, se são ambos 1

$$\mathbf{e}(mn) \ = \ 1 \ = \ 1\times 1 \ = \mathbf{e}(m)\mathbf{e}(n).$$

Se um deles é maior que 1, o mesmo acontece com o produto mn e tem-se

$$\left[\frac{1}{mn}\right] \ = \ 0;$$

por outro lado se, por exemplo $m > 1$, então

$$\left[\frac{1}{m}\right]\left[\frac{1}{n}\right] \;=\; 0 \times \left[\frac{1}{n}\right] \;=\; 0$$

e também $\mathbf{e}(mn) = \mathbf{e}(m)\mathbf{e}(n)$.

Para a função de Möbius vamos utilizar o Teorema 5.3.1.

Por definição $\mu(1) = 1$ e, se p é primo e $\alpha \in \mathbb{N}$, $\mu(p^\alpha)$ vale -1 ou 0, consoante $\alpha = 1$ ou $\alpha > 1$; assim, se algum dos expoentes em $\prod_{i=1}^k p_i^{\alpha_i}$ é maior que 1, por um lado $\mu\left(\prod_{i=1}^k p_i^{\alpha_i}\right) = 0$, por definição de μ e, por outro, $\prod_{i=1}^k \mu\left(p_i^{\alpha_i}\right) = 0$, pelo que observámos acima, pois um dos factores é zero; se todos os expoentes são 1, de novo $\mu\left(\prod_{i=1}^k p_i^{\alpha_i}\right) = (-1)^k$, por definição de μ e $\prod_{i=1}^k \mu\left(p_i^{\alpha_i}\right) = (-1)^k$, pelo que observámos acima. Em qualquer dos casos se verifica a condição (5.11) para μ.

(*2*) A demonstração não é conceptualmente difícil. Basta observar que, se $mdc(m,n) = 1$ e $d|mn$, então para certos k e t, $d = kt$, $mdc(k,t) = 1$ e $k|m$ e $t|n$ e desenvolver cálculos a partir das definições relevantes. □

Teorema 5.3.3 *Se g é uma função aritmética multiplicativa e*

$$f(n) \;=\; \sum_{d|n} g(d)$$

então f é multiplicativa.

Dem. Basta observar que, nas condições descritas $f = g * \mathbf{1}$, e aplicar o teorema 5.3.2. □

5.4 Fórmula de Inversão de Möbius

Lema 5.4.1 *Para qualquer $n \in \mathbb{N}$*

$$\sum_{d|n} \mu(d) \;=\; \begin{cases} 1 & se \;\; n = 1 \\ 0 & se \;\; n > 1 \end{cases} \tag{5.12}$$

Ou seja

$$\mu * \mathbf{1} \;=\; \mathbf{1} * \mu \;=\; \mathbf{e}. \tag{5.13}$$

Dem. Defina-se $f(n) = \sum_{d|n} \mu(d)$. Como vimos no teorema 5.3.2, μ é multiplicativa, pelo que f também é (teorema 5.3.3). Assim temos

$$f(1) \;=\; \sum_{d|1} \mu(d) \;= \mu(1) \;=\; 1.$$

Se p é primo e $\alpha \geq 1$,

$$f(p^\alpha) \;=\; \begin{cases} \mu(1)+\mu(p) = 1-1 = 0 & se \;\; \alpha = 1 \\ \sum_{i=0}^{\alpha} \mu(p^i) = 1-1+0 = 0 & \alpha > 1 \end{cases} \tag{5.14}$$

Portanto, se $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ for a decomposição canónica de n, tem-se que o valor (da função multiplicativa f) $f(n)$ é um produto de zeros, logo é zero. □

Teorema 5.4.1 *Seja g uma função aritmética qualquer. As duas condições seguintes são equivalentes*

$$\forall n \in \mathbb{N} \; f(n) \;=\; \sum_{d|n} g(d). \tag{5.15}$$

$$\forall n \in \mathbb{N} \;\; g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d}). \tag{5.16}$$

Dem. (5.15) pode reformular-se por $f = g * \mathbf{1}$, de onde se segue, pelo teorema 5.2.1 e pelo lema 5.4.1, $f*\mu = (g*\mathbf{1})*\mu = g*(\mathbf{1}*\mu) = g$, que reformula (5.16). Reciprocamente, (5.16) traduz-se por $g = f*\mu$ e segue-se analogamente $g*\mathbf{1} = f*\mu*\mathbf{1} = f$, que reformula (5.15). □

5.5 A função de Euler

Nesta secção apresentamos uma demonstração da fórmula (5.4) que põe em evidencia alguns resultados também importantes da teoria elementar dos números; em particular não se recorre ao produto de Dirichlet.

Lema 5.5.1 *Se $d \mid n \in \mathbb{N}$, então*

$$\phi(\frac{n}{d}) \;=\; \#\{k \in \mathbb{N} |\; k \leq n \;\&\; mdc(k,n) = d\} \tag{5.17}$$

Dem. Vamos ver que os dois seguintes conjuntos são equipotentes:

$$C_{nd} \;=\; \{k \in \mathbb{N} |\; k \leq n \;\&\; mdc(k,n) = d\} \tag{5.18}$$

$$C'_{nd} \;=\; \{k' \in \mathbb{N} |\; k' \leq \frac{n}{d} \;\&\; mdc(k', \frac{n}{d}) = 1\} \tag{5.19}$$

Defina-se $f(k) = \frac{k}{d} \quad (k \in C_{nd})$. Pelo teorema 1.2.4, $f(C_{nd}) \subseteq C'_{nd}$. Por outro lado, se $k' \in C'_{nd}$, tem-se $mdc(k', \frac{n}{d}) = 1$, logo

$$1 \;=\; min\{xk' + y\frac{n}{d} > 0 |\; x, y \in \mathbb{Z}\}$$

donde

$$\begin{aligned} d &= min\{d(xk' + y\frac{n}{d}) > 0 |\ x, y \in \mathbb{Z}\} \\ &= min\{xdk' + yn > 0 |\ x, y \in \mathbb{Z}\} \\ &= mdc(dk', n). \end{aligned}$$

Mas então f é bijectiva, pois de facto $f^{-1} = k' \mapsto dk'$.

Concluindo, os conjuntos em causa têm o mesmo cardinal, como queríamos provar. Repare-se que $\#C'_{nd}$ é precisamente $\phi(\frac{n}{d})$. □

Teorema 5.5.1

$$n \ = \ \sum_{d|n} \phi(d) \qquad (n \in \mathbb{N}) \tag{5.20}$$

Dem. Por um lado $d \mapsto \frac{n}{d}$ define uma permutação dos divisores de n, consequentemente

$$\sum_{d|n} \phi(d) \ = \ \sum_{d|n} \phi(\frac{n}{d});$$

por outro lado, os conjuntos C_{nd} definidos na demonstração do teorema anterior formam uma partição de $\{1, 2, \cdots, n\}$ e daí

$$n \ = \ \#\{1, \cdots, n\} \ = \ \sum_{d|n} \#C_{nd} \ = \ \sum_{d|n} \phi(\frac{n}{d}) \ = \ \sum_{d|n} \phi(d).$$

Como queríamos. □

Finalmente voltamos à fórmula de cálculo da função de Euler.

Teorema 5.5.2 *Se $p_1, \cdots, p_k$ são os divisores primos de $n \in \mathbb{N}$ e para certos números naturais α_i $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, então*

$$\phi(n) \ = \ n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \ = \ \prod_{i=1}^{k} \left[p_i^{\alpha_i - 1}(p_i - 1)\right]. \tag{5.21}$$

Em particular, ϕ é multiplicativa.

Dem. A segunda equação resulta obviamente da primeira. A primeira equação obtém-se com a fórmula de inversão de Möbius. Pelo teorema anterior e pela fórmula de inversão

$$\phi(n) \ = \ \sum_{d|n} \mu(d) \frac{n}{d} \ = \ n \sum_{d|n} \frac{\mu(d)}{d}$$

Por um lado os divisores positivos de n são da forma $p_1^{\beta_1}\cdots p_k^{\beta_k}$ com $0 \leq \beta_i \leq \alpha_i$; por outro $\mu(d) = 0$ se algum dos $\beta_i \geq 2$. Consequentemente $\frac{\mu(d)}{d} \neq 0$ apenas quando d é livre de quadrados; mas então os termos não nulos do segundo somatório acima são da forma

$$(-1)^l \frac{1}{p_{i_1}} \cdots \frac{1}{p_{i_l}}$$

As fórmulas de Van de Graaf para o desenvolvimento de $\prod_{i=1}^{l}(x - a_i)$ dão-nos a expressão final.

A multiplicatividade de ϕ é agora fácil de demonstrar: basta observar que, se m e n não têm divisores primos comuns, as comutatividade e associatividade do produto de números naturais permitem concluir $\phi(mn) = \phi(m)\phi(n)$. □

5.6 Números perfeitos

Um número natural diz-se **perfeito** se for a soma dos seus divisores próprios (nos quais se inclui 1); por exemplo 6 é o menor número perfeito. Vejamos alguns teoremas de classificação. Recorde-se que $\sigma(m)$ designa a soma dos divisores naturais do número natural m.

Teorema 5.6.1 *Para qualquer $n \in \mathbb{N}$, se $2^n - 1$ é primo, então $2^{n-1}(2^n - 1)$ é perfeito.*

Dem. Repare-se que n é perfeito sse $\sigma(m) = 2m$ e que, se $2^n - 1$ é primo, então $mdc(2^{n-1}, 2^n - 1) = 1$ $(n \in \mathbb{N})$. □

Teorema 5.6.2 *Os números perfeitos pares são da forma $2^{n-1}(2^n - 1)$ com $n \in \mathbb{N}$ e $2^n - 1$ primo.*

Dem. Em primeiro lugar observe-se que uma potência de dois não é perfeita pois

$$\sigma(2^n) = 2^{n+1} - 1 \ < \ 2^{n+1} \ = \ 2 \cdot 2^n. \tag{5.22}$$

Suponha-se então que m é perfeito e par. Pela equação anterior (5.22)

$$m \ = \ 2^\alpha \cdot k \quad com \quad k \ \acute{i}mpar \quad \& \quad k > 1.$$

Como σ é multiplicativa,

$$2m = \sigma(m) = \sigma(2^\alpha)\sigma(k) = \left(2^{\alpha+1} - 1\right)\sigma(k)$$

ou seja

$$2^{\alpha+1}k \ = \ \left(2^{\alpha+1} - 1\right)\sigma(k).$$

Como $2^{\alpha+1}$ e $2^{\alpha+1}-1$ são primos entre si

$$2^{\alpha+1}|\sigma(k) \quad isto\ é\ \sigma(k) \ = \ u2^{\alpha+1}; \tag{5.23}$$

mas então

$$2^{\alpha+1}k \ = \ (2^{\alpha+1}-1)u2^{\alpha+1} \quad \& \quad k \ = \ u(2^{\alpha+1}-1).$$

Assim, se $u > 1$,

$$\sigma(k) \geq 1 + u + u(2^{\alpha+1}-1) = u2^{\alpha+1} + 1,$$

o que contradiz (5.23); portanto só $u = 1$ é possível. Mas então

$$k \ = \ 2^{\alpha+1}-1 \quad \& \quad m \ = \ 2^{\alpha}(2^{\alpha+1}-1) \quad \& \quad \sigma(k) \ = \ 2^{\alpha+1}.$$

Em particular $\sigma(k) = k + 1$ e daí k é primo. □

5.7 Exercícios

1. Mostre que $d(n)$ é ímpar se e só se n é um quadrado perfeito.

2. Mostre que para cada número natural $m > 1$ existe um número infinito de números naturais n tais que $d(n) = m$.

3. Mostre que
$$\prod_{d|n} d = n^{\frac{d(n)}{2}}.$$

4. Mostre que para qualquer função aritmética f se tem
$$\sum_{d|n} f(d) = \sum_{d|n} f(\frac{n}{d}).$$

5. Nos problemas que se seguem supõe-se que para certos números primos distintos p_i e naturais α_i,
$$n = \prod_{i=1}^{k} p_i^{\alpha_i}.$$
Uma função aritmética f diz-se *totalmente multiplicativa* se para quaisquer $m, n \in \mathbb{N}$ se tem $f(mn) = f(m)f(n)$.

   (a) Defina $\lambda(n) = (-1)^{\sum_{i=1}^{k}\alpha_i}$ e $\lambda(1) = 1$. Mostre que

      i. λ é totalmente multiplicativa.

ii.
$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{se } n \text{ é quadrado perfeito} \\ 0 & \text{caso contrário.} \end{cases}$$

(b) Defina $\nu(n) = 2^{\sum_{i=1}^{k} \alpha_i}$ e $\nu(1) = 1$. Mostre que ν é totalmente multiplicativa e determine uma expressão para $\sum_{d|n} \nu(d)$.

(c) Para um dado $t \in \mathbb{Z}$ defina $\omega(k) = t^k$ e $\omega(1) = 1$. Mostre que

i. ω é multiplicativa;

ii.
$$\sum_{d|n} \omega(d) = \prod_{i=1}^{k} (1 + \alpha_i t).$$

6. Mostre que

(a) O produto de convolução é comutativo, associativo e distributivo relativamente à adição usual de funções.

(b) Se f e g são funções aitméticas multiplicativas, $f * g$ também é.

7. Defina
$$e(n) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } n > 1 \end{cases} \quad (n \in \mathbb{N})$$

(a) Mostre que e é multiplicativa.

(b) Mostre que para qualquer função aritmética f, $f * e = f$.

(c) Conclua que o conjunto das funções aritméticas f, $\mathcal{A}$, algebrizado por $*$ é um monóide comutativo.

8. Dada $f \in \mathcal{A}$ tal que $f(1) \neq 0$, seja g a função aritmética definida por
$$\begin{aligned} g(1) &= \frac{1}{f(1)} \\ g(n) &= -\frac{1}{f(1)} \sum_{d|n} f(d) g\left(\frac{n}{d}\right), \quad \text{se } n > 1 \end{aligned}$$

Mostre que

(a) $g * f = e$.

(b) Conclua da alínea anterior que o conjunto das funções aritméticas não nulas em 1 munido do produto de convolução é grupo abeliano.

(c) Seja $\mathcal{M}$ o conjunto das funções multiplicativas não identicamente nulas. Que pode dizer quanto à natureza algébrica de $(\mathcal{M}, *)$?

9. (a) Defina as funções aritméticas I_k e $\mathbf{1}$ por

$$I_k(n) = n^k \qquad \mathbf{1}(n) = 1$$

e mostre que

i. As funções I_k e $\mathbf{1}$ são multiplicativas.
ii. $d = \mathbf{1} * \mathbf{1}$;
iii. $\sigma = \mathbf{1} * I$;
iv. se $\sigma_k(n)$ é a soma das k-ésimas potências dos divisores positivos de n, então $\sigma_k = \mathbf{1} * I_k$;
v. se f é totalmente multiplicativa, então $f * f = fd$;
vi. $I_k * I_l(n) = n^l \sigma_{k-l}(n)$.

(b) Determine uma expressão para $\sigma * d$.

10. Suponha que f é uma função aritmética e defina

$$F(n) = \sum_{d|n} f(d) \quad (n \in \mathbb{N}).$$

Mostre que se F é multiplicativa, f também é.

11. Mostre que a única função aritmética f que verifica a condição

$$\sum_{d|n} f(d) = n$$

é a função ϕ.

12. A função Λ de von Mangoldt é definida por

$$\Lambda(n) = \begin{cases} \log p & \text{se } n = p^m \text{ para algum primo } p \text{ e algum } m \geq 1 \\ 0 & \text{caso contrário.} \end{cases}$$

Mostre que

(a) $\log n = \sum_{d|n} \Lambda(d)$;
(b) $\Lambda(n) = -\sum_{d|n} \mu(d) \log(d)$.

13. Mostre que, para cada $n \in \mathbb{N}$, o conjunto $\{x \in \mathbb{N} \mid \phi(x) = n\}$ é finito.

14. Mostre que se $n > 2$, $\phi(n)$ é par.

15. Mostre que $d(n) \leq 2\sqrt{n}$.

16. Seja $f(n)$ uma função multiplicativa não identicamente nula. Então

$$\sum_{d|n} \mu(d)f(d) = \prod_{p|n}(1 - f(p)),$$

onde p percorre todos os divisores primos de n.

17. Mostre que se n é um número perfeito, então $\sum_{d|n} \frac{1}{d} = 2$.

18. Determine todos os números perfeitos menores que 10^3.

19. Mostre que 28 é o único número perfeito par da forma

    (a) $a^n + 1$, com $n \geq 2$;

    (b) $a^n + b^n$, com $n \geq 2$ e $mdc(a, b) = 1$ $(28 = 3^3 + 1^3)$.

20. Mostre que não há números perfeitos pares da forma $a^{n^{n^{\cdot^{\cdot^{\cdot^{n}}}}}} + 1$, com $n \geq 2$ e pelo menos dois expoentes n.

21. Mostre que um número perfeito ímpar não é primo nem produto de dois primos.

22. Mostre que se n é um número perfeito ímpar então $n = p^e k^2$, onde p é um primo que não divide k e $p \equiv e \equiv 1 \ (mod\ 4)$.

23. Um par $(m, n) \in \mathbb{N}^2$ diz-se *amigável* se cada coordenada é a soma dos divisores próprios (incluindo 1) da outra. Mostre que

    (a) O par (m, n) é amigável se e só se $\sigma(m) = \sigma(n) = m + n$.

    (b) Verifique que $(220, 284)$, $(5020, 5564)$ e $(17296, 18416)$ são pares amigáveis.

24. Mostre que se $a = 3 \times 2^n - 1$, $b = 3 \times 2^{n-1} - 1$ e $c = 9 \times 2^{2n-1} - 1$ são primos ímpares, o par $(2^n ab, 2^n c)$ é amigável.

Parte II

Números reais

Capítulo 6

Fundamentação

Neste capítulo provamos que, a menos de um isomorfismo, o corpo $\mathbb{Q}$, dos números racionais, está contido em todos os corpos ordenados e todos os corpos ordenados completos são isomorfos e revemos algumas propriedades dos números reais.

Tomaremos um ponto de vista superestrutural: identificaremos subestruturas especiais dos corpos ordenados como estruturas de números naturais, de números inteiros e de números racionais. Na secção 6.2 abordaremos rapidamente uma visão mais construtiva (teorema 6.2.1).

OBS.: 1. Os termos *anel* e *domínio de integridade* entender-se-ão respectivamente como sinónimos de *anel associativo* e *domínio.*

2. Um *mergulho* de uma estrutura algébrica $\mathcal{A}$ noutra $\mathcal{B}$ é um morfismo injectivo de $\mathcal{A}$ em $\mathcal{B}$

6.1 Corpos ordenados e números racionais

Um **corpo** é um *anel de divisão comutativo.* Por outras palavras, uma estrutura algébrica $\mathcal{K} = (K, +, \cdot)$ com duas operações binárias $+$ e $\cdot$ diz-se um corpo se verificar as seguintes propriedades

1. $\mathcal{K}$ é um anel cujo zero designamos por $\mathbf{0}$.
2. $(K\backslash\{\mathbf{0}\}, \cdot)$ é um grupo comutativo cujo elemento neutro designamos por $\mathbf{1}$, ou por *unidade* do corpo.

Note-se que, em particular, $\mathbf{0} \neq \mathbf{1}$ pela segunda propriedade. Do modo usual, identificaremos $a \cdot b$ com ab quando $a, b \in K$.

Um corpo $\mathcal{K}$ é **ordenado** quando se distingue um subconjunto K^+ de K, dito **conjunto dos elementos positivos de** K, para o qual se verificam as condições seguintes

1. $\mathbf{0} \notin K^+ \neq \emptyset$

2. Para quaisquer $a, b \in K$, dá-se uma e só uma das condições seguintes

   (a) $a = b$

   (b) $a - b \in K^+$

   (c) $b - a \in K^+$

3. Para quaisquer $a, b \in K^+,\ a + b \in K^+$

4. Para quaisquer $a, b \in K^+,\ ab \in K^+$

É um exercício verificar que a condição

$$a \ < \ b \quad \textit{se e só se} \quad b - a \in K^+ \quad (a, b \in K^+)$$

define uma relação $<$ de ordem total estrita em K de modo que $K^+ = \{x \in K : \ \mathbf{0} < x\}$, e $\mathcal{K} = (K, +, \cdot, <)$ é uma estrutura algébrica em que $\mathcal{K} = (K, +, \cdot)$ é um corpo e $<$ é compatível com $+$ e semicompatível com $\cdot$, ou seja:

1. A relação $<$ é

   (a) *Anti-reflexiva* — $a \not< a$, seja qual for $a \in K$.

   (b) *Anti-simétrica* — $a < b \ \Rightarrow \ b \not< a$, sejam quais forem $a, b \in K$.

   (c) *Transitiva* — $a < b \ \& \ b < c \ \Rightarrow \ a < c$, sejam quais forem $a, b, c \in K$.

   (d) *Tricotómica* — para quaisquer $a, b \in K$, dá-se uma e só uma das condições seguintes: $a = b,\ a < b,\ b < a$.

2. Para quaisquer $a, b, c \in K, \quad a < b \ \Rightarrow \ a + c < b + c$.

3. Para quaisquer $a, b, c \in K, \quad [a < b \ \& \ \mathbf{0} < c] \ \Rightarrow \ ac < bc$

De facto, estas propriedades de $<$ podem ser tomadas como definidoras de corpo ordenado, deduzindo-se delas que o conjunto $\{x \in K : \ \mathbf{0} < x\}$ verifica as propriedades tomadas inicialmente como características de K^+, de tal modo que a relação de ordem obtida a partir de K^+ é precisamente $<$. De modo um pouco informal: há uma correspondência bijectiva natural entre ordens compatíveis com as operações do corpo e conjuntos de positivos.

Vamos ver que, a menos de um isomorfismo, todos os corpos ordenados, contêm o corpo dos números racionais, ou seja $\mathbb{Q}$ é o menor corpo ordenado.

Seja então $\mathcal{K}$ um corpo ordenado com relação de ordem $<$.

Lema 6.1.1 *Para qualquer $a \in K$,*

(i) $a < \mathbf{0}$ se e só se $\mathbf{0} < -a$

(ii) $-a < \mathbf{0}$ se e só se $\mathbf{0} < a$

(iii) Se $a \neq \mathbf{0}$ *então* $\mathbf{0} < a^2$

(iv) $\mathbf{0} < \mathbf{1}$

Dem. As condições (i) e (ii) são equivalentes, já que, em qualquer anel $a = -(-a)$. Assim limitar-nos-emos a provar (i), (iii) e (iv)

(i) Observe-se que vale a seguinte cadeia de implicações, pela compatibilidade de $<$ com $+$.

$$a < \mathbf{0} \ \Rightarrow \mathbf{0} = a + (-a) < \mathbf{0} + (-a) = -a \ \Rightarrow a = \mathbf{0} + a < -a + a = \mathbf{0}$$

(iii) Como $a^2 = (-a)^2$, por (i) e pela semicompatibilidade de $<$ com $\cdot$, quando $a \neq \mathbf{0}$, a^2 é sempre o produto de dois elementos positivos, portanto é positivo.

(iv) Observe-se que $\mathbf{0} \neq \mathbf{1} = \mathbf{1}^2$ e tome-se em conta (iii). □

Definição 6.1.1 *Um subconjunto* C *de* K *diz-se* **indutivo** se $\mathbf{1} \in C$ e $x + \mathbf{1} \in C$ sempre que $x \in C$.

Obviamente K e K^+ são indutivos, mas há concerteza subconjuntos indutivos mais pequenos. Designe-se por N a *intersecção de todos os subconjuntos indutivos de* K. Seja ainda S a restrição da função $x \mapsto x + \mathbf{1}$ a N.

Lema 6.1.2 N *é um subconjunto indutivo e* $(N, S, \mathbf{1})$ *é uma estrutura de números naturais.*

Dem. Em primeiro lugar, $\mathbf{1} \in N$ pois, por definição, $\mathbf{1}$ é elemento de todos os subconjuntos indutivos. Por outro lado, se $x \in N$ então x está em todos os subconjuntos indutivos e consequentemente $x+\mathbf{1}$ também, portanto $x+\mathbf{1} \in N$ se $x \in N$. E concluimos de facto duas coisas a saber:

1. N é indutivo
2. S é uma função de N em N.

Como $(K, +)$ é um grupo, S é injectiva. Além disso, $\mathbf{1} = S(x) \Rightarrow x = \mathbf{0}$, pelo que $\mathbf{1}$ só pode ser imagem por S de algum elemento de N se $\mathbf{0} \in N$. Ora K^+ é indutivo e $\mathbf{0} \notin K^+$, portanto $\mathbf{0} \notin N$ e $\mathbf{1} \notin S(N)$.

Finalmente, vejamos que se verifica o Princípio de Indução:

Se $\mathbf{1} \in A \subseteq N$ e $x + \mathbf{1} \in A$ sempre que $x \in A$, então A é um suconjunto indutivo de N; ora, por definição, $N \subseteq A$, portanto $A = N$. □

Assim $N = \{\mathbf{1}, \mathbf{1} + \mathbf{1}, \mathbf{1} + \mathbf{1} + \mathbf{1}, \cdots\}$ e como habitualmente fazemos a convenção notacional de designar a soma de n $\mathbf{1}s$ pelo número natural intuitivo n. Em suma

Corolário 6.1.1 *A menos de um isomorfismo de estruturas de números naturais, o conjunto* $\mathbb{N}$ *dos números naturais intuitivos é subconjunto de qualquer corpo ordenado.*

Deixamos ao cuidado do leitor a demonstração do seguinte resultado

Teorema 6.1.1 *A soma, o produto e a ordem definidas em* $\mathbb{N}$ *como universo da estrutura de números naturais* $(\mathbb{N}, S, \mathbf{1})$ *coincidem com as induzidas pelo corpo* $\mathcal{K}$.

Repare-se agora que, como $\mathcal{K}$ é um corpo, todos os elementos $n \in \mathbb{N}$ têm um inverso multiplicativo $n^{-1} \in K$, que é sempre um número positivo, e que os elementos da forma np^{-1} com $n, p \in \mathbb{N}$ formam um grupo para a multiplicação. Reunimos num lema algumas propriedades importantes:

Lema 6.1.3 *Sejam* K^+ *o subconjunto de elementos positivos de* K *e* $Q = \{np^{-1} : \ n, p \in \mathbb{N}\}$.

1. *Para qualquer* $a \in K\backslash\{\mathbf{0}\}$, a^{-1} *tem o mesmo sinal que* a.
2. $\mathbb{N} \subset Q \subseteq K^+$
3. $\left(np^{-1}\right)^{-1} = pn^{-1}$, *para quaisquer* $n, p \in \mathbb{N}$
4. $(np^{-1})(mq^{-1}) = (nm)(pq)^{-1} \quad (m, n, p, q \in \mathbb{N})$
5. $(Q, \cdot)$ *é um grupo comutativo*
6. $(mk)(pk)^{-1} = mp^{-1}$
7. $np^{-1} + mq^{-1} = (nq + mp)(pq)^{-1} \quad (m, n, p, q \in \mathbb{N})$, *e* $(Q, +)$ *é um semigrupo.*
8. $(Q, +, \cdot)$ *é uma estrutura algébrica onde* $\cdot$ *é distributiva relativamente a* $+$.

Dem. 1. Se $x < 0 < y$, então $xy < 0y = 0$, pela semi-compatibilidade do produto com a ordem; como $0 < 1 = aa^{-1}$, a e a^{-1} têm o mesmo sinal.

2. Por um lado, para todo o $n \in \mathbb{N}$, $n = n1 = n1^{-1}$; por outro, como K^+ é indutivo, $N \subseteq K^+$ e daí os elementos de Q são produtos de elementos positivos, logo também positivos.

3,4,6 deixam-se ao cuidado do leitor.

5. As partes 3 e 4 estabelecem que a estrutura é de grupóide (com identidade e) onde todos os elementos têm inverso; como a associatividade e a comutatividade são hereditárias, a estrutura é de facto de grupo comutativo.

7. $np^{-1} + mq^{-1} = nqq^{-1}p^{-1} + mpq^{-1}p^{-1} = (nq + mp)(pq)^{-1}$.

8. As distributividades são também hereditárias. □

Passando à identificação usual

$$ab^{-1} \;=\; \frac{a}{b} \quad se \quad b \neq 0,$$

as propriedades da estrutura $(Q, +, \cdot)$ que acabámos de descrever põem em evidência que ela se comporta como o conjunto dos números racionais positivos usuais ou intuitivos, em particular as propriedades 3, 4, 6 e 7 descrevem as propriedades essenciais das fracções:

$$\frac{1}{\frac{a}{b}} = \frac{b}{a}\ (a \neq 0) \quad \& \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \quad \& \quad \frac{ad}{bd} = \frac{a}{b} \quad \& \quad \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

Ora $\mathcal{K}$ é um corpo, consequentemente, fazendo $-X = \{-x :\ x \in X\}$,

$$-\mathbb{N} \;\subseteq\; -Q \;\subseteq K$$

e é fácil, se bem que porventura trabalhoso, demonstrar que

Teorema 6.1.2 *1.* $\mathbb{N} \cup \{0\} \cup -\mathbb{N} \quad \subseteq \quad Q \cup \{0\} \cup -Q \quad \subseteq \quad K.$

2. $(\mathbb{N} \cup \{0\} \cup -\mathbb{N}, +, \cdot)$ *é um subdomínio de integridade de* $\mathcal{K}$.

3. $(Q \cup \{0\} \cup -Q, +, \cdot, <)$ *é um subcorpo ordenado de* $\mathcal{K}$ *com conjunto de positivos* Q.

Para fixar ideias, defina-se

$$\mathbf{Z} = \mathbb{N} \cup \{0\} \cup -\mathbb{N} \quad \& \quad \mathbf{Q} = Q \cup \{0\} \cup -Q \quad \& \quad \mathcal{Z} = (\mathbf{Z}, +, \cdot) \quad \& \quad \mathcal{Q} = (\mathbf{Q}, +, \cdot).$$

Teorema 6.1.3 $\mathbf{Q} \;=\; \{\frac{m}{n} :\ m, n \in \mathbf{Z}\ \&\ n \neq 0\}$

Dem. Um aspecto fundamental da demonstração é que

$$\frac{-m}{-n} = \frac{m}{n} \quad \& \quad -\frac{m}{n} = \frac{-m}{n} = \frac{m}{-n}.$$

A verificação destas igualdades pode fazer-se por casos. □

Sistematizando o que temos vindo a descrever

Teorema 6.1.4 *A menos de isomorfismos de anéis*

1. *Qualquer corpo ordenado contém um subdomínio de integridade* $\mathcal{Z}$ *e um subcorpo* $\mathcal{Q}$ *como descritos no teorema 6.1.2.*

2. *Qualquer anel que contenha* $\mathbb{N}$ *também contém* $\mathcal{Z}$ *como subanel.*

3. *Qualquer corpo que contenha $\mathcal{Z}$ como subanel também contém $\mathcal{Q}$.*

4. *$\mathcal{Z}$ é o menor domínio de integridade que contém $\mathbb{N}$.*

5. *$\mathcal{Q}$ é o menor corpo ordenado que contém $\mathcal{Z}$ como subanel.*

Dem. (esquema) A proposição 1 tem vindo a ser demonstrada ao longo do texto. Na verdade é essencialmente para este resumo que se têm vindo a apresentar lemas, dos quais o terceiro (lema 6.1.3) tem por fim descrever os morfismo de anéis em causa:

A partir do momento em que se identificam os zeros $\mathbf{0}$ e $\mathbf{0}'$ e as unidades $\mathbf{1}$ e $\mathbf{1}'$ dos corpos ordenados $\mathcal{K}$ e $\mathcal{K}'$ os isomorfismos entre as várias subestruturas (de números naturais ou com universos em subconjuntos Q e Q' ou Z e Z') são restrições ou prolongamentos de um mesmo que fica definido pelas condições *necessárias* (de facto redundantes)

$$\begin{aligned}
\Phi(\mathbf{0}) &= \mathbf{0}' \\
\Phi(\mathbf{1}) &= \mathbf{1}' \\
\Phi(n\mathbf{1}) &= n\mathbf{1}' \\
\Phi(a+b) &= \Phi(a)+\Phi(b) \\
\Phi(ab) &= \Phi(a)\Phi(b) \\
\Phi(-x) &= -\Phi(x)
\end{aligned}$$

As proposições 2 e 3 resultam apenas de os anéis serem fechados para a passagem ao simétrico e os corpos serem fechados para a passagem ao inverso. As proposições 4 e 5 são meras reformulações de 2 e 3, respectivamente. □

Por estas razões passamos a identificar $\mathbf{Z}$ e $\mathbf{Q}$ respectivamente com os conjuntos $\mathbb{Z}$ dos inteiros intuitivos e $\mathbb{Q}$ dos racionais intuitivos, algebrizados e ordenados da maneira usual.

Repare-se também que as condições descritas nas equações acima não são suficientes para garantir que o mergulho Φ se prolongue a um isomorphismo entre os corpos $\mathcal{K}$ e $\mathcal{K}'$; até porque tal isomorfismo pode mesmo não existir. [1]

6.2 Uma visão construtiva

Na secção anterior tomámos o ponto de vista axiomático não nos preocupando com a existência de um modelo formal de corpo ordenado: aceitámos que os números racionais intuitivos constituem uma exemplificação suficiente de tal estrutura. No entanto *admitindo apenas a existência de alguma estrutura de números naturais (por exemplo a dos naturais intuitivos ...) é possível construir um corpo ordenado mínimo que a prolonga. Passamos a esquematizar tal construção.*

[1] Pode encontrar-se um tratamento deste tema em [16] ou [19].

Teorema 6.2.1 *Dada uma estrutura de números naturais com as operações de soma* $,+,$ *e produto* $,\cdot,$ *e a ordem* $<$ *canónicas* $\mathcal{N} = (\mathbb{N}, S, \mathbf{1}, +, \cdot, <)$*, existe um corpo ordenado* $\mathcal{Q} = (\mathbf{Q}, \mathbf{0}, \mathbf{1}, +, \cdot, <)$*, que a prolonga e, a menos de um isomorfismo de corpos ordenados, está contido em todos os possíveis prolongamentos de* $\mathcal{N}$ *por corpos ordenados.*

Dem. A demonstração da parte de unicidade a menos de um isomorfismo é obviamente o trabalho que desenvolvemos quase totalmente até aqui. Um esquema de demonstração deste teorema é o seguinte.

I. Defina-se em $\mathbb{N}^2$ a relação de *equivalência* $\equiv_\bullet$ por

$$(m,p) \equiv_\bullet (n,q) \quad sse \quad mq = np$$

II. Seja $Q = \mathbb{N}^2/\equiv_\bullet$ o respectivo conjunto cociente, designem-se as classes de equivalência por $[(m,p)]_\bullet$ e algebrize-se Q do seguinte modo

$$\begin{array}{lcl} [(m,p)]_\bullet \odot [(n,q)]_\bullet & = & [(mn,pq)]_\bullet \\ [(m,p)]_\bullet \lhd [(n,q)]_\bullet & sse & mq < np \\ [(m,p)]_\bullet \oplus [(n,q)]_\bullet & = & [(mq+np,pq)]_\bullet \end{array}$$

III. Verifique-se que $(Q, \oplus, \odot)$ é uma estrutura algébrica em que

1. $(Q, \odot)$ é um grupo comutativo com elemento neutro $\mathbf{1} = [(1,1)]_\bullet$.
2. $(Q, \oplus)$ é um semigrupo comutativo que verifica a Lei do Corte.
3. $\odot$ é distributiva em relação a $\oplus$
4. $\lhd$ é uma ordem total em Q
5. $\lhd$ é compatível com $\oplus$ e $\odot$, ou seja
   (a) $x \lhd y \quad sse \quad x \oplus z \lhd y \oplus z \quad x,y,z \in Q$
   (b) $x \lhd y \quad sse \quad xz \lhd yz \quad (x,y,z \in Q)$

IV. A função $\phi : \mathbb{N} \to Q$ dada por $\phi(n) = [(n,1)]_\bullet$ é um mergulho da estrutura algébrica ordenada $(\mathbb{N}, +, \cdot, <)$ para a estrutura algébrica ordenada $(Q, \oplus, \odot, \lhd)$; que identifica $(\mathbb{N}, +, \cdot, <)$ com uma subestrutura de $(Q, \oplus, \odot, \lhd)$, pelo que voltamos a designar as operações e a ordem pelos seus símbolos iniciais.

V. Defina em Q^2 a seguinte relação de equivalência

$$(a,b) \equiv_+ (c,d) \quad sse \quad a+d = b+c \quad ((a,b) \in Q^2)$$

e designe por $[(a,b)]_+$ as respectivas classes de equivalência e ainda por $\mathbf{Q}$ o correspondente conjunto cociente.

VI. Defina uma operação interna θ em $\mathbf{Q}$ por

$$[(a,b)]_+\theta[(c,d)]_+ = [(a+c,b+d)]$$

e verifique que $(\mathbf{Q},\theta)$ é um grupo comutativo, com elemento neutro $\mathbf{0} = [(a,a)]_+$ e no qual o simétrico (inverso para θ) de $x = [(a,b)]_+$, é $-x = [(b,a)]_+$.

OBS: Não é necessário utilizar a natureza dos elementos de Q, mas tão só que $(Q,+)$ é um semigrupo comutativo que verifica a Lei do Corte.

VII. A função $\psi : Q \to \mathbf{Q}$ dada por $\psi(x) = [(x+x,x)]_+$ é um mergulho da estrutura algébrica $(Q,+)$ em $(\mathbf{Q},\theta)$ e, identificando Q com $\psi(Q)$, tem-se com união disjunta

$$\mathbf{Q} = Q \cup \{\mathbf{0}\} \ \cup -Q$$

VIII. Passando a designar θ por $+$ e antecipando o facto de as novas operações estenderem as anteriores, complete-se a algebrização de $\mathbf{Q}$ do seguinte modo

1. $a < b \quad sse \quad b - a \in Q$
2. $|a| = \begin{cases} a & se \ \ a \in Q \cup \{\mathbf{0}\} \\ -a & se \ \ a \in -Q \end{cases}$
3. $a \cdot b = \begin{cases} |a||b| & se \ \ a,b \in Q \ ou \ \ -a,-b \in Q \\ -|a||b| & caso \ \ contrário \end{cases}$

IX. Verifique-se que $\mathcal{Q} = (\mathbf{Q},\mathbf{0},\mathbf{1},+,\cdot,<\ )$ é um corpo ordenado cujo conjunto de elementos positivos é Q.

OBS.: Também aqui não é necessário utilizar a natureza dos elementos de Q mas tão só as propriedades descrita em III.

X. Seja $\mathbf{Z} = \mathbb{N} \cup \{\mathbf{0}\} \cup -\mathbb{N}$. Verifique-se que, a menos de um isomorfismo de anéis, $\mathcal{Z} = (\mathbf{Z},+,\cdot)$ é o menor anel que prolonga $\mathcal{N}$

XI. Verifique-se que, a menos de um isomorfismo de corpos, $\mathcal{Q}$ é o menor corpo que prolonga $\mathcal{Z}$.

Fica terminado esquema de demonstração do teorema 6.2.1. □

6.3 Extensões próprias do corpo dos números racionais

Se o número natural n não é um quadrado perfeito, então $\sqrt{n} \notin \mathbb{Q}$; no entanto, se $\mathbb{Q}(\sqrt{n}) = \{a+b\sqrt{n} : \ a,b \in \mathbb{Q}\}$, então $(\mathbb{Q}(\sqrt{n}),+,.\mathbf{0},\mathbf{1})$ é um corpo (ordenado) do qual o corpo dos números racionais é subcorpo próprio pois

- $\mathbb{Q} \ = \ \mathbb{Q} + 0\sqrt{n} \ \subset \ \mathbb{Q}(\sqrt{n})$,

- $(a+b\sqrt{n})^{-1} = \frac{a}{a^2-nb^2} - \frac{b}{a^2-nb^2}\sqrt{n}$
- $(a+b\sqrt{n})(c+d\sqrt{n}) = (ac+nbd)+(ad+bc)\sqrt{n}$.

Lembrando que um número real α se diz **algébrico** se for raiz de um polinómio de coeficientes inteiros e se diz **transcendente** caso contrário, tem-se que, para $\alpha \in \mathbb{R}$, o menor corpo ordenado que contém $\mathbb{Q} \cup \{\alpha\}$, $\mathbb{Q}(\alpha)$,

- é uma extensão própria de $\mathbb{Q}$ sse $\alpha \notin \mathbb{Q}$
- é um espaço vectorial sobre $\mathbb{Q}$ que tem dimensão finita sse α é algébrico.

Informalmente: um número real é algébrico se e só se for representável por uma expressão onde figurem apenas números inteiros, somas, produtos, diferenças, cocientes e radiciações de índice natural em quantidade finita. Cálculos pacientes mostram que esta última condição é de facto suficiente para que a expressão represente um número algébrico; a demonstração de que é necessária não cabe no âmbito deste curso.

Exemplo 6.3.1 $\sqrt{3+\frac{\sqrt[3]{5}}{4}}$ é raiz do polinómio $64(x^2-3)^3-5$ e não é racional.

Na verdade não há "muitos"irracionais algébricos.

Teorema 6.3.1 *O conjunto dos números algébricos é numerável.*

Dem. Em primeiro lugar repare-se que

O conjunto $\mathbb{Z}[x]$ dos polinómios de coeficientes inteiros é numerável,

pois, para cada $n \in \mathbb{N}$, o conjunto dos polinómios de grau menor ou igual a n e coeficientes inteiros, $\mathbb{Z}_{(n)}[x]$, é equipotente a $\mathbb{Z}^{n+1}$; como $\mathbb{Z}$ é numerável, o mesmo acontece com qualquer das suas potências cartesianas de expoente finito e ainda

$$\mathbb{Z}[x] \;=\; \bigcup_{n=1}^{\infty} \mathbb{Z}_{(n)}[x].$$

Em segundo lugar, *cada polinómio em $\mathbb{Z}[x]$ tem um número finito* — eventualmente zero — *de raizes reais,* portanto o conjunto dos números reais algébricos é uma união numerável de conjuntos finitos e consequentemente é numerável. □

A construção de números transcendentes pode fazer-se como aplicação do seguinte teorema sobre números algébricos que, em parte, afirma: *os números irracionais algébricos são difíceis de aproximar com rapidez.*

Teorema 6.3.2 (de Liouville) *Seja α um número irracional algébrico, raiz do polinómio $P(x) = \sum_{i=0}^{n} a_i x^i$, de grau $n \geq 1$, e irredutível sobre $\mathbb{Q}[x]$. Então existe $M \in \mathbb{Q}^+$ tal que, para qualquer número racional $\frac{m}{k}$ $(m \in \mathbb{Z},\ k \in \mathbb{N})$ se tem*

$$|\alpha \;-\; \frac{m}{k}| \;<\; 1 \;\Rightarrow\; |\alpha \;-\; \frac{m}{k}| \;>\; \frac{M}{k^n}$$

Dem. $P(x)$ não tem raizes racionais, por ser irredutível sobre $\mathbb{Q}[x]$; consequentemente, para quaisquer $m \in \mathbb{Z}$ e $k \in \mathbb{N}$,

$$|P(\frac{m}{k})| = \frac{1}{k^n}|\sum_{i=0}^{n} a_i m^i k^{n-i}| \geq \frac{1}{k^n},$$

porque o polinómio do segundo membro só toma valores inteiros e não nulos, donde o seu valor absoluto só pode ser maior ou igual a 1. Faça-se

$$s = sup\{|P'(x)| : \ |x-\alpha| < 1\}$$

Dados então $m \in \mathbb{Z},\ k \in \mathbb{N}$ tais que $|\frac{m}{k} - \alpha| < 1$ tem-se, para algum c entre $\frac{m}{k}$ e α,

$$\begin{aligned} \frac{1}{k^n} &\leq |P(\frac{m}{k})| = |P(\frac{m}{k}) - 0| \\ &= |P(\frac{m}{k}) - P(\alpha)| = |P'(c)||\frac{m}{k} - \alpha| \\ &\leq s|\frac{m}{k} - \alpha|. \end{aligned}$$

pelo que podemos tomar $M \in]0, \frac{1}{s}]$. □

De um ponto de vista afirmativo: *se um número real α é aproximável por uma sucessão (r_n) de racionais que converge mais rapidamente para α que qualquer sucessão $\left(\frac{M}{k^n}\right)_{n\in\mathbb{N}}$, então α é transcendente.*

Exemplo 6.3.2 O número $\alpha = \sum_{i=1}^{\infty} 10^{-i!}$ é transcendente, pois

$$|\alpha \ - \ \sum_{i=1}^{n} 10^{-i!}| \ \leq \ 10^{-[(n+1)!-1]}.$$

Até Cantor ter demonstrado que *há mais números transcendentes que números algébricos* (teorema 6.6.2), na segunda metade do século XIX, o Teorema de Liouville era o único resultado que garantia a existência números transcendentes.

6.4 Corpos ordenados completos

ISOMORFISMO

Já os gregos do séc. V A.C. sabiam que $\sqrt{2}$ é irracional (*incomensurável* em linguagem da época). Na verdade interessa-nos observar um pouco mais: dados números naturais m e n, tem-se

$$\left(\frac{m}{n}\right)^2 < 2 \quad \Rightarrow \quad \left[\frac{m}{n} < \frac{3m+4n}{2m+3n} \quad \& \quad \left(\frac{3m+4n}{2m+3n}\right)^2 < 2\right].$$

Assim, $D = \{x \in \mathbb{Q} : \ x^2 < 2\}$ não tem supremo em $\mathbb{Q}$; no entanto 2 é claramente um majorante de D em $\mathbb{Q}$.

Definição 6.4.1 *Um corpo ordenado diz-se* **completo** *se qualquer dos seus subconjuntos não vazios e majorados tem supremo.*

Acabámos de ver que o corpo ordenado dos números racionais não é completo. Por outro lado, uma das propriedades do corpo ordenado dos números reais é precisamente ser completo. Na verdade esta propriedade caracteriza este último a menos de um isomorfismo, como se afirma no teorema 6.4.2.

Seja de ora em diante $\mathcal{K} = (K, +, \cdot, \mathbf{0}, \mathbf{1}, <)$ um corpo ordenado completo.

Um lema importante em si mesmo:

Lema 6.4.1 $\mathbb{N}$ *não é majorado em* K.

Dem. Se $\mathbb{N}$ fosse majorado teria supremo, digamos $s = sup\mathbb{N}$; se s pertencesse a $\mathbb{N}$, s não poderia ser supremo pois $s < s + 1 \in \mathbb{N}$; mas então existem $x, y \in \mathbb{N}$ tais que $s - \frac{1}{2} < x < y < s$, o que é impossível porque a diferença mínima entre elementos de $\mathbb{N}$ é 1. Segue-se que $\mathbb{N}$ não pode ser majorado. □

Uma consequência imediata deste lema:

Teorema 6.4.1 *Para quaisquer* $a, b \in K$ *tais que* $0 < a < b$, *existe* $n \in \mathbb{N}$ *tal que* $b < na$.

Em virtude deste teorema diz-se que os corpos ordenados completos são **Arquimedianos.** As várias extensões de $\mathbb{Q}$ a que aludimos na secção anterior são todas arquimedianas mas não necessariamente completas. E segue-se

Lema 6.4.2 *Entre dois elementos distintos quaisquer de um corpo ordenado completo existe um número racional.*

Dem. Comecemos por supor $0 < a < b$ em $\mathcal{K}$; pelo lema anterior, existem um número natural n tal que $n > \frac{1}{b-a}$ e $n > \frac{1}{a}$, ou seja, $\frac{1}{n} < a,\ b-a$. Seja $m = max\{k \in \mathbb{N} :\ \frac{k}{n} \leq a\}$. Tem-se que $\frac{m}{n} \in \mathbb{Q}$ e $a < \frac{m+1}{n} < b$. Os casos $a < 0 < b$ e $a < b < 0$ tratam-se analogamente ou por passagem ao simétrico. □

Teorema 6.4.2 *Todos os corpos ordenados completos são isomorfos.*

Dem. Sejam $\mathcal{K}_1 = (K_1, +, \cdot, \mathbf{0}, \mathbf{1}, <)$ e $\mathcal{K}_2 = (K_2, \oplus, \odot, \bar{\mathbf{0}}, \bar{\mathbf{1}}, \lhd)$ dois corpos ordenados completos. Tendo em vista o teorema 6.1.4, cada um destes corpos contém um corpo Q_i de números racionais $(i = 1, 2)$ e os Q_i são isomorfos, digamos que por um isomorfismo $\Phi : Q_1 \to Q_2$.

Definam-se *secções* Q_{ix} e uma função $\Psi : K_1 \to K_2$ por

$$Q_{ix} = \{v \in Q_i :\ v < (\lhd)x\}\ (x \in K_i;\ i = 1, 2) \quad \& \quad \Psi(x) = sup\Phi(Q_{1x})\ (x \in K_1).$$

Em primeiro lugar, pelo lema 6.4.2

$$x \;=\; sup Q_{ix} \quad (x \in K_i;\; i = 1, 2) \tag{6.1}$$

Em segundo lugar

$$\Psi \textit{ coincide com } \Phi \textit{ em } Q_1 \tag{6.2}$$

pois se $x \in Q_1$, por um lado $\Phi(x)$ majora $\Phi(Q_{1x})$ (por (6.1)) e, por outro, se $0 \lhd \varepsilon \in Q_2$ então, pelo lema 6.4.2 existe $u \in Q_1$ tal que $x - \Phi^{-1}(\varepsilon) < u < x$, donde $\Phi(x) - \varepsilon \lhd \Phi(u) \lhd \Phi(x)$ e $\Phi(x) = sup\phi Q_{1x} = \Psi(x)$. De seguida

$$x < y \;\Rightarrow\; \Psi(x) \lhd \Psi(y) \tag{6.3}$$

como se pode ver do seguinte modo: dados $x, y \in Q_1$ se $x < y$, de acordo com o lema 6.4.2, podemos escolher $u, v \in Q_1$ tais que $x < u < v < y$; por (6.2) e por definição de Ψ, $\Psi(u) = \Phi(u) \lhd \Phi(v) \leq \Psi(y)$; como para qualquer $z \in Q_1$, se $z < x$ então $z < u$ e daí $Q_{1x} \subseteq Q_{1u}$, temos $\Psi(x) \leq \Psi(u)$ e finalmente $\Psi(x) \lhd \Psi(y)$. Em particular

$$\Psi \textit{ é injectiva.} \tag{6.4}$$

$$\Psi \textit{ é sobrejectiva}: \tag{6.5}$$

Vamos ver que

$$\textit{Para qualquer } y \in K_2,\; y = \Psi\left(sup \Phi^{-1}(Q_{2y})\right). \tag{6.6}$$

Seja $x = sup\Phi^{-1}(Q_{2y})$. Se $u \in Q_{1x}$ então existe $v \in \Phi^{-1}(Q_{2y})$ tal que $u < v \leq x$; mas assim $\Phi(u) \lhd \Phi(v) \in Q_{2y}$, pelo que $\Psi(x) = sup\Phi(Q_{1x}) \leq supQ_{2y} = y$ (por (6.1)). Se $\Psi(x) \lhd y$, existe $v \in Q_{2y}$ tal que $\Psi(x) \lhd v \lhd y$; tomando $u \in Q_1$ tal que $\Phi(u) = v$ e, portanto, tal que $u \in \Phi^{-1}(Q_{2y})$, obtemos $\Psi(x) \lhd v \lhd \Psi(x)$ o que é impossível. Assim (6.6) e (6.5) ficam provadas.

Repare-se que (6.6) afirma ser Ψ^{-1} da mesma natureza que Ψ. Vejamos que

$$\Psi(x + y) \;=\; \Psi(x) \oplus \Psi(y) \quad (x, y \in K_1) \tag{6.7}$$

Como $sup(A \oplus B) \overset{\lhd}{=} supA \oplus supB \quad (A, B \subseteq K_2)$, também

$$\Psi(x + y) \overset{\lhd}{=} \Psi(x) \oplus \Psi(y) \quad (x, y \in K_1)$$

Dados $\delta \in Q_2$ tal que $\bar{0} \lhd \delta$ e $u \in Q_{1x},\; v \in Q_{1y},\; w, z \in Q_2$ tais que

$$\Psi(x) \ominus \frac{\delta}{2} \lhd w = \Phi(u) \lhd \Psi(x) \;\&\; \Psi(y) \ominus \frac{\delta}{2} \lhd z = \Phi(v) \lhd \Psi(y)$$

Segue-se, por (6.3), que $u < x$ e $v < y$; daí que $u + v < x + y$ e também, por (6.2),

$$(\Psi(x) \oplus \Psi(y)) \ominus \delta \lhd w \oplus z = \Phi(u + v) = \Psi(u + v) \lhd \Psi(x + y).$$

Como δ foi escolhido arbitrariamente, podemos concluir (6.7). Provemos agora que

$$\Psi(xy) \;=\; \Psi(x) \odot \Psi(y) \quad (x, y \in K_1) \tag{6.8}$$

Comecemos por observar que de (6.7) se conclui

$$\Psi(-x) \;=\; -\Psi(x) \quad (x \in K_1) \tag{6.9}$$

e portanto basta demonstrar (6.8) com $x, y > 0$; neste caso podemos usar que, para conjuntos de elementos positivos $A, B \subset K_2$, $sup(AB) \stackrel{\lhd}{=} supA \odot supB$ e raciocinar como para a soma, com as abreviaturas usuais:

Necessariamente $\Psi(xy) \stackrel{\lhd}{=} \Psi(x)\Psi(y)$; dado δ e escolhendo u, v, w, z como acima, obtemos

$$\begin{aligned} \Psi(x)\Psi(y) \ominus \frac{\delta}{2}\Psi(x+y) \oplus \left(\frac{\delta}{2}\right)^2 &\lhd wz \\ &= \Phi(uv) = \Psi(uv) \\ &\lhd \Psi(xy) \end{aligned}$$

de onde se concluirá (6.8). Resumindo: (6.4), (6.5), (6.7), (6.8) e (6.3) dizem-nos que Ψ é um isomorfismo entre os corpos ordenados $\mathcal{K}_1$ e $\mathcal{K}_2$. □

6.5 Existência

Também neste caso é possível tomar uma visão "da base para o topo" quanto à existência de um corpo ordenado completo, isto é de um corpo de números reais. Como vimos em 6.2, pode construir-se um corpo de números racionais $\mathcal{Q} = (\mathbb{Q}, +, \cdot, \mathbf{0}, \mathbf{1})$ a partir de um sistema intuitivo de números naturais. Na verdade podemos inspirar-nos na demonstração da isomorfia entre corpos ordenados completos para definir um desses corpos a partir do dos números racionais; é o que esquematizamos de seguida.

Uma construção

Definição 6.5.1 *Uma* **secção** *em $\mathbb{Q}$ é um conjunto S verificando as seguintes condições*

1. $\emptyset \neq S \subseteq \mathbb{Q}$.
2. *S tem majorante em $\mathbb{Q}$.*
3. *S é um* ideal de ordem*, isto é*

$$\forall a, b \in \mathbb{Q}\ [b < a \in S \;\Rightarrow\; b \in S]. \tag{6.10}$$

4. S não tem máximo.

O corpo ordenado completo cuja construção vamos esquematizar resultará da algebrização conveniente do *conjunto de todas as secções,* designado por $\mathbf{R}$.

Note-se que, mesmo quando uma secção tem supremo em $\mathbb{Q}$, este não é incluido nela.

A ordem $\lhd$
Dadas secções $S, T \in \mathbf{R}$,

$$S \lhd T \quad sse \quad S \subset T$$

entendendo-se, como temos vindo a fazer, que $\subset$ designa a inclusão estrita.

Teorema 6.5.1 *A relação $\lhd$ é de ordem total em $\mathbf{R}$.*

Dem. A anti-reflexividade e a anti-simetria resultam das propriedades da inclusão estrita $\subset$. Se $S \neq T$ & $S \not\lhd T$ & $T \not\lhd S$, então existem $s, t \in \mathbb{Q}$ tais que $s \in S \backslash T$ & $t \in T \backslash S$. Em particular $s \neq t$. Ora $<$ é uma relação de ordem total em $\mathbb{Q}$, portanto $s < t$ ou $t < s$; se $s < t$, pela condição (6.10) $s \in T$, o que não pode acontecer; se $t < s$, então $t \in S$, o que também não pode acontecer. Assim, ou $S = T$ ou $S \lhd T$ ou $T \lhd S$. □

A soma $\oplus$

Dadas secções $S, T \in \mathbf{R}$ defina-se

$$S \oplus T \;=\; \{s + t :\; s \in S \;\&\; t \in T\} \tag{6.11}$$

Há que verificar vários aspectos:

1. $S \oplus T$ é não vazio
2. $S \oplus T$ é majorado
3. $S \oplus T$ não tem máximo
4. $S \oplus T$ é ideal de ordem

Mostremos que vale 4, deixando a cargo do leitor a verificação do restante: se $a, b \in \mathbb{Q}$ e $b < a = s + t$ para alguns $s \in S$ e $t \in T$, então $b - t < a - t = s \in S$ pelo que $b - t = s' \in S$ e consequentemente $b = s' + t \in S \oplus T$.

Teorema 6.5.2 *Valem as seguintes proposições*

1. $(\mathbf{R}, \oplus)$ é um grupo comutativo.

2. A relação de ordem $\lhd$ é compatível com $\oplus$, isto é

$$\forall S, T, U \in \mathbf{R}\; [S \lhd T \Rightarrow S \oplus U \lhd T \oplus U]. \tag{6.12}$$

Dem. **(1)** Não é difícil mostrar que a estrutura é de semigrupo comutativo com elemento neutro $\mathbf{0} = \{x \in \mathbb{Q} : \ 0 < x\}$. Quanto à existência de simétricos $\ominus S$:

$$\ominus S \ = \begin{cases} \mathbb{Q}\setminus -(S \bigcup \{supS\}) & \text{se } supS \text{ existe em } \mathbb{Q} \\ \mathbb{Q}\setminus -S & \text{caso contrário} \end{cases}$$

As dificuldades na demonstração residem essencialmente em mostrar que, por exemplo no caso $S \lhd \mathbf{0}$, *se* $r \in \mathbb{Q}$ *e* $r < 0$, *então existem* $s \in S$, $s' \in \ominus S$ *tais que* $r = s + s'$*:* se $r \in S$, tome-se $r = r + 0$; se $r \notin S$, tome-se $k \in \mathbb{N}$ tal que $kr \in S \ \& \ (k-1)r \notin S$; se $supS \neq (k-1)r$, faça-se $r = kr + (1-k)r$; se $supS = (k-1)r$, tome-se $r = (k + \frac{1}{2})r + (1 - k - \frac{1}{2})r$; em qualquer dos casos se obtém a representação desejada para r.

Deixamos a prova das restantes afirmações a cargo do leitor. □

O produto $\odot$

Comece-se por verificar que vale o

Lema 6.5.1 $\mathbf{0} \stackrel{\lhd}{=} S$ *sse* $\ominus S \stackrel{\lhd}{=} \mathbf{0}$

Defina-se uma função **valor absoluto,** $\| \cdot \| : \mathbf{R} \to \mathbf{R}$ por

$$\|S\| \ = \begin{cases} S & se \ \ \mathbf{0} \stackrel{\lhd}{=} S \\ \ominus S & se \ \ S < \mathbf{0} \end{cases} \tag{6.13}$$

e defina-se o produto de duas secções maiores ou iguais a zero por

$$\mathbf{0} \stackrel{\lhd}{=} S, T \Rightarrow S \odot T = \mathbf{0} \cup \{st : \ s \in S \ \& \ t \in T \ \& \ s, t \geq 0\}.$$

Finalmente, defina-se o produto globalmente por

$$S \odot T \ = \begin{cases} \|S\|\|T\| & se \ \ \mathbf{0} \stackrel{\lhd}{=} S, T \ \ ou \ \ S, T \stackrel{\lhd}{=} \mathbf{0} \\ \ominus\|S\|\|T\| & se \ \ S \stackrel{\lhd}{=} \mathbf{0} \stackrel{\lhd}{=} T \ \ ou \ \ T \stackrel{\lhd}{=} \mathbf{0} \stackrel{\lhd}{=} S \end{cases} \tag{6.14}$$

Definindo ainda

$$\mathbf{1} \ = \ \{x \in \mathbb{Q} : \ x < 1\}$$

tem-se o seguinte

Teorema 6.5.3 $\mathcal{R} = (\mathbf{R}, \oplus, \odot, \mathbf{0}, \mathbf{1}, \lhd)$ *é um corpo ordenado completo.*

Dem. Tal como para a soma, é necessário verificar que a definição do produto $\odot$ é boa, no sentido em que o produto de secções ainda é uma secção, para o que basta estudar os casos em que as secções são ambas maiores ou iguais a zero. A demonstração correspondente para a soma fornece as linhas orientadoras.

Demonstrar que $\mathbf{1} = \{r \in \mathbb{Q} : \ r < 1\}$ é análogo ao que se fez para verificar que a secção $\mathbf{0}$ é neutra para a soma, transformando adequadamente os argumentos aditivos em argumentos multiplicativos. Também é simples mostrar que $\mathbf{0}$ é absorvente para o produto.

Um caso um pouco mais delicado:

$$S^{-1} = \begin{cases} \{r \in \mathbb{Q} : \ \forall s \in S \ \left(0 < s \Rightarrow r < \frac{1}{s}\right)\} \backslash \{\frac{1}{supS}\} & supS \in \mathbb{Q} \\ \{r \in \mathbb{Q} : \ \forall s \in S \ \left(0 < s \Rightarrow r < \frac{1}{s}\right)\} & supS \notin \mathbb{Q}; \end{cases} \quad (\mathbf{0} < S)$$

se $S < 0, \ S^{-1} = \ominus \|S\|^{-1}$.

As propriedades associativa do produto e distributiva deste em relação à soma têm demonstração também rotineira.

Finalmente, a verificação do axioma de completude:
Se $\mathcal{A}$ é um conjunto de secções não vazio e majorado, então $sup\mathcal{A} = \bigcup_{S \in \mathcal{A}} S$. □

6.6 Números transcendentes

A existência de números transcendentes está garantida pelo teorema de Liouville 6.3.2, mas também se pode demonstrar que

Teorema 6.6.1 *O número π e a base e dos logaritmos nepperianos são números transcendentes.*

A este propósito, veja-se [18] caps. 16 e 20; neste momento interessa-nos apenas mostrar que

Teorema 6.6.2 *O conjunto dos números transcendentes não é numerável.*

Dem. I. *O conjunto dos números reais não é numerável.*

Se $\mathbb{R}$ fosse numerável, o mesmo acontecia com o intervalo aberto $]0,1[$, digamos que

$$]0,1[\ = \ \{r_n : \ n \in \mathbb{N}\}$$

para alguma contagem fixada. Fixando também para cada $r_n \in]0,1[$ uma representação decimal

$$r_n \ = \ 0, r_1^n r_2^n r_3^n ... r_n^n ...$$

podemos definir um novo número real $s = s_1 s_2 ... s_n ... \in]0,1[$ do seguinte modo

$$s_n = \begin{cases} r_n^n + 1 & \text{se } 0 \leq r_n^n < 9 \\ 0 & \text{se } r_n^n = 9 \end{cases}$$

O número s é diferente de qualquer dos r_n porque difere de cada um deles na n-ésima casa decimal.

Resumindo: nenhuma enumeração esgota o intervalo $]0,1[$, ou seja, não há aplicações bijectivas de $\mathbb{N}$ em $]0,1[$, ou ainda, $]0,1[$ é infinito, não é numerável e, portanto, $\mathbb{R}$ também não.

II. *O conjunto dos números racionais é numerável.*

Cada número racional admite uma representação fraccionária irredutível única $\frac{m}{n}$ na qual $m \in \mathbb{Z}$ & $n \in \mathbb{N}$; a função $f : \mathbb{Q} \to \mathbb{Z}^2$ dada por $f(\frac{m}{n}) = (m, n)$ é então injectiva e, como $\mathbb{Z}^2$ é numerável, $\mathbb{Q}$ também é.

III. *O conjunto dos números irracionais não é numerável.*

Se fosse, $\mathbb{R}$ também seria pois seria união de $\mathbb{Q}$ com um conjunto numerável.

IV. *O conjunto dos números transcendentes não é numerável.*

Os números irracionais são algébricos ou transcendentes; como os algébricos formam um conjunto numerável (teorema 6.3.1), pelo que acabámos de ver, os transcendentes não podem constituir um conjunto numerável. □

6.7 Exercícios

1. Mostre que toda a ordem parcial lata gera uma ordem parcial estrita. Reciprocamente, mostre que toda a ordem parcial estrita gera uma ordem parcial lata.

2. Dê exemplos de ordens parciais densas, ordens parciais não densas e ordens parciais que não são completas.

3. Considere uma estrutura de números naturais, $\mathcal{N} = (N, S, \mathbf{1})$, e um corpo ordenado, $\mathcal{K} = (K, +, \cdot, \mathbf{0}, \mathbf{1}, <)$. Defina uma função $\Phi : \mathbb{N} \to K$ por $\Phi(\mathbf{1}) = \mathbf{1}$ & $\Phi(S(x)) = \Phi(x) + 1$. Mostre que Φ é um mergulho da estrutura de números naturais no corpo, quando na primeira se entendem definidas também a soma, o produto e a ordem canónicas.

4. Mostre que todo o corpo ordenado é infinito.

5. Suponha que $(K, +, \cdot, \mathbf{0}, \mathbf{1}, <)$ e $(K', +, \cdot, \mathbf{0}, \mathbf{1}, <)$ são dois corpos ordenados (o contexto determina o domínio onde as operações se realizam e a ordem se considera). Mostre que a função Φ do exercício 3 tem um e um só prolongamento ao subcorpo do números racionais de $\mathcal{K}$ que é por sua vez um isomorfismo para o subcorpo dos números racionais de $\mathcal{K}'$.

6. Se um corpo ordenado tem um elemento irracional, então entre cada dois quaisquer dos seus elementos existe um elemento irracional.

7. Suponha que $k \in \mathbb{N}$. Mostre que $\sqrt[k]{n} \in \mathbb{Q}$ se e só se n é uma k-ésima potência perfeita, isto é, se e só se existe $m \in \mathbb{N}$ tal que $n = m^k$.

8. Uma bijecção entre $\mathbb{N}$ e $\mathbb{N}^2$.

   (a) Mostre que a função $\nu : \mathbb{N}^2 \to \mathbb{N}$ dada por qualquer das equações

$$\begin{aligned}\nu(m,n) &= \frac{1}{2}\left((m+n)^2 - m - 3n + 2\right)\\ &= \frac{1}{2}\left((m+n)^2 - (m+n) - 2(n-1)\right)\\ &= \frac{1}{2}\left(m(m+n-1) + n(m+n-3) + 2\right)\end{aligned}$$

   é uma bijecção.

   Nota: Esta contagem resulta de ordenar $\mathbb{N}^2$ diagonalmente por

$$(1,1),\ (1,2),\ (2,1),\ (1,3),\ (2,2),\ (3,1),\ldots$$

   Sugestão de passos para a demonstração:

   1. $2\nu(m,n) \in \mathbb{N}$.

   2. 2ν é injectiva (Utilize $k = m + n$)

   3. ν é sobrejectiva, isto é, $\mathbb{N} = \nu(\mathbb{N}^2)$.

   (b) Designe por $[x]$ a *característica* de x, ou seja, o maior número inteiro não superior a x. e sejam $\alpha, \beta, f, g : \mathbb{N} \to \mathbb{N}$ as funções dadas por

$$\begin{aligned}&\alpha(m) = \left[\tfrac{-1+\sqrt{8m-7}}{2}\right] + 1 \quad \beta(m) = \tfrac{\alpha(m)(\alpha(m)-1)}{2}\\ &f(m) = m - \beta(m) \qquad\qquad g(m) = \alpha(m) + 1 - f(m)\end{aligned}$$

   Verifique que

$$\nu^{-1}(m) = (f(m), g(m)) \qquad (m \in \mathbb{N}).$$

9. Mostre que os números seguintes são transcendentes.

   (a) $\sum_{n=0}^{\infty} 10^{-n^n}$

   (b) $\sum_{n=0}^{\infty} 10^{-(2^{n^2}+p)}$, para cada $p \in \mathbb{Z}$.

10. Dê vários exemplos de números transcendentes obtidos por meio do Teorema de Liouville, além dos descritos acima e no restante texto.

11. Suponha que $f \in \mathbb{N}^{\mathbb{N}}$. Que pode dizer quanto à natureza dos números da forma $\sum_{n=0}^{\infty} 10^{f(n)}$, quando $\lim \frac{f(n)}{a^n} = +\infty$ e $a > 1$? E se este limite for finito?

Capítulo 7

Dízimas e Fracções contínuas

7.1 Dízimas

Recorde-se que $[x]$ designa a **característica** do número real x, isto é, *o maior número inteiro que é menor ou igual a* x.

Teorema 7.1.1 *A representação de qualquer número natural na base* 10 *é única, a menos de zeros à esquerda, isto é, para cada* $x \in \mathbb{N}$ *existe uma e uma só sequência* $(x_0, \cdots, x_m) \in \mathbb{Z}^{m+1}$ *tal que*

1. $0 \leq x_i \leq 9 \quad (0 \leq i \leq m \in \mathbb{N}_0)$
2. $x_m > 0 \ \ \& \ \ x = \sum_{i=0}^{m} x_{m-i} 10^{m-i}$
3. *Se* $x = \sum_{i=0}^{p} x_{p-i} 10^{p-i}$ *para algum* $p \in \mathbb{N}_0$, *então* $p \geq m$ *e* $p \geq j > m \ \Rightarrow \ x_j = 0$.

Dem. Tome-se $x \in \mathbb{N}$ e defina-se

$$\begin{cases} c_0 &= x \\ c_{n+1} &= \left[\frac{c_n}{10}\right] \\ x_n &= c_n - 10c_{n+1} \quad (n \in \mathbb{N}_0) \end{cases}$$

É fácil verificar que c_{n+1} e x_n são respectivamente o cociente e o resto da divisão de c_n por 10, pelo que, para

$$0 \ \leq \ x_n \ \leq 9 \quad \& \quad 10c_{n+1} \ \leq \ c_n \qquad (n \in \mathbb{N}_0)$$

e assim, para $n \in \mathbb{N}_0$

$$10^n c_n \ \leq \ c_0 = x \tag{7.1}$$

$$x \ = \ 10^n c_n + \sum_{i=1}^{n} 10^{n-i} x_{n-i} \tag{7.2}$$

entendendo-se $\sum_{i=1}^{0} \alpha_i = 0$.

Por (7.1), se $10^m \leq x < 10^{m+1}$, então $1 \leq x_m = c_m \leq 9$ e $x_{m+r} = c_{m+r} = 0$ ($r \in \mathbb{N}$). Em virtude da equação (7.2) o teorema fica demonstrado. □

Teorema 7.1.2 *Para cada número real $x \in [0, +\infty[$, existe uma e só uma sucessão $(a_n)_{n\in\mathbb{N}}$ tal que, para qualquer $n \in \mathbb{N}$, se verifica*

$$0 \leq a_n \leq 9 \tag{7.3}$$

$$0 \leq x - \left([x] + \sum_{i=1}^{n+1} \frac{a_i}{10^i}\right) < \frac{1}{10^{n+1}}. \tag{7.4}$$

Deste modo

$$x = [x] + \sum_{n=1}^{\infty} \frac{a_n}{10^n}$$

e também, para qualquer $n \in \mathbb{N}$, existe $k > n$ tal que $a_k < 9$.

A sucessão (a_n) referida neste teorema diz-se a **parte decimal** da **dízima** do número real $x \geq 0$; $[x]$ diz-se também a **parte inteira** da dízima; se $x_m \cdots x_0$ for a representação de $[x]$ dada pelo teorema 7.1.1, escreve-se

$$x = x_m \cdots x_0, a_1 a_2 \cdots a_n \cdots$$

O número 7.4 deste último teorema afirma que *a dízima (a_n) não é identicamente* 9, *seja a partir de que ordem for.*

Dem. Note-se que 0 é representável por $0,000\cdots$, verificando-se as asserções do teorema; assim, provado este, a parte de unicidade garante ser esta a única representação de zero nestas condições.

Defina-se

$$\begin{cases} x_1 = x - [x] \\ x_{n+1} = 10x_n - [10x_n] \quad (n \in \mathbb{N}) \end{cases} \qquad a_n = [10x_n] \ (n \in \mathbb{N})$$

1. É imediato que

$$0 \leq x_n < 1 \qquad (n \in \mathbb{N}) \tag{7.5}$$

de onde resulta que $0 \leq [10x_n] < 10$ e consequentemente, $0 \leq a_n \leq 9$.

2. Por outro lado, para cada $n \in \mathbb{N}$,

$$x_{n+1} = 10^n x_1 - \sum_{i=0}^{n} 10^{n-i} a_i$$

e portanto, considerando (7.5),

$$0 \leq x - \left([x] + \sum_{i=1}^{n} \frac{a_i}{10^i} \right) = \frac{x_{n+1}}{10^n} < \frac{1}{10^n}$$

3. Se $a_n = 9$ a partir da ordem $n+1$, ter-se-ia

$$x - \left([x] + \sum_{i=1}^{n} \frac{a_i}{10^i} \right) = \sum_{i=n+1}^{\infty} \frac{9}{10^i} = \frac{1}{10^n}$$

o que contradiz (7.4).

Resta ver que a dízima é única nas condições referidas e basta verificar esta unicidade quando $0 \leq x < 1$. Observe-se que

$$\begin{aligned} 0 \leq x - \sum_{i=1}^{n} \frac{a_i}{10^i} < \frac{1}{10^n} \quad &\Rightarrow \quad 0 \leq 10^n x - \sum_{i=1}^{n} a_i 10^{n-i} < 1 \\ &\Rightarrow \quad \sum_{i=1}^{n} a_i 10^{n-i} = [10^n x] \end{aligned}$$

portanto os a_i são univocamente determinados por x pelo teorema 7.1.1. □

Uma dízima diz-se **periódica** com período $b_1 \cdots b_p$ ($b_i \in \mathbb{N};\ 1 \leq i \leq p \in \mathbb{N}$), se a parte decimal tiver a forma

$$\cdots b_1 \cdots b_p b_1 \cdots b_p \cdots b_1 \cdots b_p \cdots$$

isto é, se existem $n_0, p \in \mathbb{N}$ tais que os termos da sucessão (a_n) do teorema 7.1.2 verificam

$$a_{n_0+i+kp} \ = \ b_i \quad (k \in \mathbb{N}; 1 \leq i \leq p),$$

representando-se

$$x \ = \ [x] + 0, a_1 \cdots a_{n_0} (b_1 \cdots b_p).$$

Se uma dízima é periódica de período $b_1 \cdots b_p$ e $a_1 = b_1$, dir-se-á **puramente periódica**, caso contrário diz-se que a dízima é **mista**. Uma dízima de período 0 também se diz **finita**.

Dados números naturais primos entre si a e $m > 1$, a **ordem** de a $(mod\ m)$ é o menor número natural h tal que $a^h \equiv 1\ (mod\ m)$.

Exercício 7.1.1 Suponha que $mdc(a, m) = 1$ e que h é a ordem de a $(mod\ m)$. Mostre que:

1. $h | \phi(n)$.
2. $h | m$.

Teorema 7.1.3 *Seja x um número real positivo*

1. *x é racional se e apenas se tem dízima periódica.*
2. *Se $x = \frac{a}{b}$ $(a, b \in \mathbb{N})$ e $mdc(a, b) = 1$ e $b = 2^\alpha 5^\beta n$ $(n \in \mathbb{N})$, então*
   (a) *Se $n = 1$, x tem dízima finita.*
   (b) *Se $\alpha = \beta = 0$ & $n > 1$, x tem dízima puramente periódica e o comprimento do período é a ordem de 10 $(mod\ n)$.*
   (c) *Se $\alpha > 0$ ou $\beta > 0$ e $n > 1$, x tem dízima mista, o comprimento do período é a ordem de 10 $(mod\ n)$ e o comprimento da parte não periódica é $max(\alpha, \beta)$.*

Dem. Vamos mostrar que *se x tem dízima periódica, então é racional*, ficando provada uma parte do número 1. De seguida provaremos as restantes alíneas do teorema, que obviamente esgotam os casos em que x é racional, ficando provado o restante de 1.

1. Suponhamos que a dízima de x tem período $a_{k+1} \cdots a_{k+p}$; segue-se que

$$\begin{aligned} x &= \sum_{n=1}^{k} \frac{a_n}{10^n} + \sum_{s=0}^{\infty} \sum_{i=1}^{p} \frac{a_{k+i}}{10^{k+sp+i}} \\ &= \frac{1}{10^k} \sum_{n=1}^{k} 10^{k-n} a_n + \sum_{i=1}^{p} \frac{a_{k+i}}{10^{k+i}} \sum_{s=0}^{\infty} \frac{1}{10^{sp}} \\ &= \frac{1}{10^k} \sum_{n=1}^{k} a_n 10^{k-n} + \frac{1}{10^{k+p}} \left(\sum_{i=1}^{p} a_{k+i} 10^{p-i} \right) \frac{10^p}{10^p - 1} \ \in \ \mathbb{Q} \end{aligned}$$

2. Suponha-se então que x é racional positivo, digamos

$$x = \frac{a}{2^\alpha 5^\beta n} \qquad mdc(a, 2^\alpha 5^\beta n) = mdc(10, n) = 1$$

e sejam

$$\mu = max\{\alpha, \beta\} \quad \& \quad \nu = ordem\ de\ 10\ (mod\ n).$$

a) $(n = 1)$ Neste caso

$$x = \frac{a 2^{\mu-\alpha} 5^{\mu-\beta}}{10^\mu}$$

e a dízima de x é claramente finita.

b) $(\alpha = \beta = 0;\ n > 1)$ Neste caso $10^\nu \equiv 1\ (mod\ n)$, ou seja, para algum $m \in \mathbb{N}$, $10^\nu = mn + 1$; mas então, para certos $q, r \in \mathbb{N}_0$, sendo $0 < r < 10^\nu - 1$,

$$\begin{aligned} 10^\nu x &= \frac{(mn+1)a}{n} = ma + \frac{a}{n} = ma + x \\ x &= \frac{ma}{10^\nu - 1} = q + \frac{r}{10^\nu - 1} \\ &= q + \frac{r}{10^\nu} \frac{1}{1 - \frac{1}{10^\nu}} \end{aligned}$$

Tomando $r = \sum_{i=1}^{\nu} 10^{\nu-i} a_i$ para certos $a_i \in \mathbb{N}_0$ com $a_\nu > 0$, segue-se que

$$\begin{aligned} x &= q + \left(\sum_{i=1}^{\nu} \frac{a_i}{10^i}\right) \sum_{n=0}^{\infty} \frac{1}{10^{n\nu}} \\ &= q + 0,(a_1 \cdots a_\nu) \end{aligned}$$

Conclui-se, por um lado, que a dízima é puramente periódica e, por outro, que o comprimento mínimo de um período, digamos λ, é menor ou igual a ν; mas de

$$\begin{aligned} x - [x] &= \left(\sum_{i=1}^{\lambda} \frac{a_i}{10^i}\right) \sum_{n=0}^{\infty} \frac{1}{10^{n\lambda}} \\ &= \frac{\sum_{n=1}^{\lambda} a_n 10^{\lambda-n}}{10^\lambda - 1} \\ &= \frac{r}{n} \in \mathbb{Q} \quad \& \quad mdc(r,n) = 1 \end{aligned}$$

deduz-se $n|10^\lambda - 1$, ou seja $10^\lambda \equiv 1 \ (mod\ n)$ pelo que $\lambda \geq \nu$. Segue-se que $\lambda = \nu$.

c) $(\alpha + \beta > 0 \ \& \ n > 1)$ Para estudar este caso, basta aplicar a alínea anterior a $10^\mu x$. □

7.2 Fracções contínuas simples

Notação

De modo a respeitar uma notação clássica para fracções contínuas e evitar ambiguidades *até ao fim deste capítulo a característica do número real x passa a ser designada por car(x).*

PROPRIEDADES BÁSICAS.

Por comodidade de exposição convirá utilizar com frequência $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ passando as sucessões de números reais a indiciar-se em $\mathbb{N}_0$.

Dados um número natural n, números reais *positivos* $r_1, r_2, ..., r_n$ e um número real qualquer r_0, o símbolo $[r_0; r_1, ..., r_n]$ define-se recursivamente do seguinte modo:

$$\begin{aligned} [r_0] &= r_0 \\ \forall n \in \mathbb{N}\ [r_0; r_1, ..., r_{n+1}] &= [r_0; r_1, ..., r_{n-1}, r_n + \frac{1}{r_{n+1}}] \end{aligned}$$

sendo fácil verificar o seguinte:

Teorema 7.2.1 *Se* $r_0 \in \mathbb{R} \quad \& \quad r_1, r_2, ..., r_n > 0$ *então*

1. *Para* $0 \leq i \leq n-1$, $[r_i; ..., r_n] = r_i + \frac{1}{[r_{i+1}; ..., r_n]}$

2. *Se todos os* $r_i \in \mathbb{N}$, *então*

   (a) $[r_i; ..., r_n] > 0 \quad (0 \leq i \leq n)$

   (b) $[r_i; ..., r_n] \in \mathbb{Q}$

Definição 7.2.1 *Uma sucessão* $(r_n)_{n\in\mathbb{N}_0}$ *de números* inteiros *diz-se* **simples** *se se verificarem ambas as seguintes condições*

1. $r_n \in \mathbb{N}_0$ *seja qual for* $n \in \mathbb{N}_0$.

2. $\forall n \in \mathbb{N}\ [r_n = 0 \ \Rightarrow\ \forall k \in \mathbb{N}_0\ r_{n+k} = 0]$.

Repare-se que *numa sucessão simples, se um termo de ordem positiva é positivo, o único termo de ordem menor que pode ser zero é o de ordem zero*

Definição 7.2.2 *Dada uma sucessão simples* (a_n), *a* **fracção contínua simples** $[a_0; a_1, ..., a_n, ...]$ *é a sucessão de números racionais* x_n *definida do seguinte modo*

1. *Se* $a_n = 0$ *para todo o* $n \in \mathbb{N}$, *então* $x_n = a_0\ (n \in \mathbb{N}_0)$

2. *Se* $a_n > 0$ *para todo o* $n \in \mathbb{N}$, *então*

$$x_n = [a_0; \cdots, a_n] \quad (n \in \mathbb{N}_0)$$

3. *Se* $a_1 > 0$ *e* $n_0 = min\{n : a_n = 0\} \in \mathbb{N}$ *então*

$$\begin{cases} x_n = [a_0; \cdots, a_n] & \text{se } n < n_0 \\ x_n = [a_0; \cdots, a_{n_0-1}] & \text{se } n \geq n_0 \end{cases}$$

As fracções $[a_0; \cdots, a_n]$ chamam-se **reduzidas** ou **convergentes** da fracção contínua. Uma fracção contínua diz-se **finita** se os termos a_n se anulam a partir de alguma ordem. Uma reduzida de ordem n pode identificar-se com a fracção contínua correspondente $[a_0; \cdots, a_n, 0, \cdots]$.

Observe-se que

$$a_n > 1 \ \Rightarrow\ [a_0; \cdots, a_n] = [a_0; \cdots, a_n - 1, 1] \tag{7.6}$$

no entanto

Teorema 7.2.2 *Se* $[a_0; \cdots, a_n]\ (n > 1)$ *é uma fracção contínua simples,* $0 < m \in \mathbb{Z},\ k \in \mathbb{N}$ *e*

$$\frac{m}{k} = [a_0; \cdots, a_n]\ \&\ a_n > 1\ \&\ mdc(k, m) = 1,$$

então os a_i *verificam as seguintes relações de recorrência:*

$$\begin{aligned} m &= a_0 k + r_0\ \&\ 0 \leq r_0 < k\ \ \&\ \ r_0 \in \mathbb{Z} \\ k &= a_1 r_0 + r_1\ \&\ 0 \leq r_1 < r_0\ \ \&\ \ r_1 \in \mathbb{Z} \\ r_{i-1} &= a_{i+1} r_i + r_{i+1}\ \&\ 0 \leq r_{i+1} < r_i\ \ \&\ \ r_{i+1} \in \mathbb{Z}\ \ \&\ \ 1 \leq i < n-1 \\ r_{n-2} &= a_n \end{aligned}$$

Repare-se que com $mdc(k,m)=1$, supondo $\frac{m}{k}=[a_0;a_1]=a_0+\frac{1}{a_1}$, vem $m=a_0k+r_0$ e $k=a_1r_0$, com $0\leq r<k$, pelo que $r_0|k$ e portanto $r_0|m$, ou seja, $r_0=1$ e $k=a_1$. Esta situação pode ser integrada no teorema considerando $m=r_{-2}$ e $k=r_{-1}$.

Dem. (do teorema 7.2.2) Comecemos por observar que os a_i são positivos e que as reduzidas $[a_i;\cdots,a_n]$ também, portanto

$$0 \;<\; \frac{1}{[a_i;\cdots,a_n]} \;=\; \frac{1}{a_i+\frac{1}{[a_{i+1};\cdots,a_n]}} \;<\; 1 \tag{7.7}$$

Definindo $x_i=[a_i;\cdots,a_n]$, vem

$$x_{i-1} \;=\; a_{i-1} \;+\; \frac{1}{x_i},$$

donde

$$a_i \;=\; [x_i] \;=\; car([a_i;\cdots,a_n]);$$

em particular,

$$a_0 \;=\; car(x_0) \;=\; car\left(\frac{m}{k}\right)$$

e a_0 é o cociente inteiro de m por k; portanto, se

$$m \;=\; a_0k+r_0 \quad \text{com} \quad 0\leq r_0<k \quad \& \quad r_0\in\mathbb{Z}$$

vem

$$\frac{r_0}{k}=\frac{1}{[a_1;\cdots,a_n]}$$

tendo-se também $r_0>0$ como seria de esperar. De novo

$$\frac{k}{r_0} \;=\; [a_1;\cdots,a_n] \;=\; a_1 \;+\; \frac{1}{[a_2;\cdots,a_n]}$$

e a_1 é o cociente inteiro de k por r_0, vindo

$$k \;=\; a_1r_0+r_1 \quad \text{com} \quad 0<r_1<r_0 \quad \& \quad r_1\in\mathbb{Z}$$

Convencionando $m=r_{-2}$ & $k=r_{-1}$ mostrámos

$$\begin{array}{rcl} r_{i-1} & = & a_{i+1}r_i+r_{i+1} \quad \text{com} \quad 0<r_{i+1}<r_i \quad \& \quad r_{i+1}\in\mathbb{Z} \\ \frac{r_{i-1}}{r_i} & = & [a_{i+1};\cdots,a_n] \quad \text{para} \quad i=-1,0 \end{array}$$

Suponhamos que estas relações se mantêm até $i\leq n-1$. Tem-se

$$a_{i+1} \;+\; \frac{1}{[a_{i+2};\cdots,a_n]} \;=\; \frac{r_{i-1}}{r_i} \;=\; a_{i+1} \;+\; \frac{r_{i+1}}{r_i}$$

donde

$$\frac{r_i}{r_{i+1}} = [a_{i+2};\cdots,a_n] = a_{i+2}+\alpha \quad (i+2\leq n) \tag{7.8}$$

$$a_{i+2} = car\left(\frac{r_i}{r_{i+1}}\right). \tag{7.9}$$

Ponhamos

$$r_i = a_{i+2}r_{i+1} + r_{i+2};$$

se $i+2<n$, então $[a_{i+2};\cdots,a_n]>a_{i+2}$ e a constante α em (7.8) é positiva, pelo que $r_{i+2}\geq 0$, como se pretendia verificar; se $i+2=n$, então $\alpha=0$ e $r_{n-2}=a_nr_{n-1}$.

Pelo que sabemos do algoritmo de Euclides para o cálculo de $mdc(m,k)$, a divisão de restos só é exacta quando o divisor é $mdc(m,k)$, neste caso 1; portanto $r_{n-1}=1$.

□

Uma consequência praticamente imediata deste teorema é

Teorema 7.2.3 *Duas fracções contínuas simples positivas* $[a_0;\cdots,a_n]$ *e* $[b_0;\cdots,b_n]$ *em que* $r_n,a_m>1$ *são iguais sse* $m=n$ & $a_i=b_i$ $(0\leq i\leq n)$.

Dem. Se as duas fracções são iguais, representam o mesmo número racional e o teorema anterior descreve a determinação das coordenadas univocamente. □

Repare-se que a condição imposta às últimas coordenadas das reduzidas em cada um dos teoremas anteriores é necessária em vista da equação (7.6).

Quanto à representação de números negativos por fracções contínuas: se $m\in\mathbb{Z}$ & $n\in\mathbb{N}$, independentemente do sinal de m tem-se sempre

$$\frac{m}{n} = car\left(\frac{m}{n}\right)+r \quad \text{com} \quad r\in\mathbb{Q}\cap[0,1[$$

Segue-se que

$$\frac{m}{n} = [car\left(\frac{m}{n}\right);a_1,\cdots,a_k] \quad \text{se} \quad r=[0;a_1,\cdots,a_k].$$

Adiantando-nos um pouco:*se soubéssemos que fracções contínuas simples diferentes têm limites diferentes* poderíamos concluir

Teorema 7.2.4 *Se* $[a_0;\cdots,a_n,\cdots]$ *é uma fracção contínua simples infinita e o* $\lim_n[a_0;\cdots,a_n]$ *existe, então este limite é um número irracional.*

A este propósito vejam-se os teoremas 7.2.9 e 7.2.10. Na próxima parte verificaremos que as fracções contínuas simples convergem sempre.

Fracções contínuas infinitas

De ora em diante (a_n) é uma sucessão simples para a qual $a_n\geq 1$ $(n\in\mathbb{N})$. Fixamos também a seguinte notação:

$$\begin{array}{lll} h_{-2}=0 & h_{-1}=1 & h_i = a_i h_{i-1} + h_{i-2} \ (i \geq 0) \\ k_{-2}=1 & k_{-1}=0 & k_i = a_i k_{i-1} + k_{i-2} \ (i \geq 0) \end{array}$$

Em particular

$$1 = k_0 \leq a_1 < k_n < k_{n+1} \ (n \geq 2) \quad \& \quad \lim_n k_n = +\infty. \tag{7.10}$$

Teorema 7.2.5 *Para qualquer número real $x \in]0, +\infty[$ e qualquer $n \in \mathbb{N}$,*

$$[a_0; \cdots, a_{n-1}, x] \ = \ \frac{x h_{n-1} + h_{n-2}}{x k_{n-1} + k_{n-2}} \tag{7.11}$$

Dem. $(n = 1)$

$$\begin{aligned} \frac{x h_0 + h_{-1}}{x k_0 + k_{-1}} &= \frac{x[a_0 \cdot 1 + 0] + 1}{x[a_0 \cdot 0 + 1] + 0} \\ &= \frac{a_0 x + 1}{x} = a_0 + \frac{1}{x} \\ &= [a_0; x] \end{aligned}$$

Supondo a igualdade **válida para** n

$$\begin{aligned} [a_0; \cdots, a_n, x] &= [a_0; \cdots, a_{n-1}, a_n + \frac{1}{x}] \\ &= \frac{\left(a_n + \frac{1}{x}\right) h_{n-1} + h_{n-2}}{\left(a_n + \frac{1}{x}\right) k_{n-1} + k_{n-2}} \\ &= \frac{x\left(a_n h_{n-1} + h_{n-2}\right) + h_{n-1}}{x\left(a_n k_{n-1} + k_{n-2}\right) + k_{n-1}} \\ &= \frac{x h_n + h_{n-1}}{x k_n + k_{n-1}} \end{aligned}$$

como se pretendia. Pelo Princípio de Indução, a equação (7.11) vale para qualquer $n \in \mathbb{N}$. □

Observação: Repare-se que $[x] = x = \frac{x h_{-1} + h_{-2}}{x k_{-1} + k_{-2}}$, pelo que a fórmula (7.11) vale mesmo se $n = 0$.

Corolário 7.2.1 $[a_0; \cdots, a_n] \ = \ \frac{h_n}{k_n} \quad (n \in \mathbb{N}_0)$.

Mais detalhadamente:

Teorema 7.2.6 *Seja $r_n = [a_0; \cdots, a_n]$ $(n \in \mathbb{N})$. Valem as seguintes proposições, para qualquer $n \in \mathbb{N}$:*

1. $h_n k_{n-1} - h_{n-1} k_n = (-1)^{n-1}$

2. $r_n - r_{n-1} = \frac{(-1)^{n-1}}{k_n k_{n-1}}$
3. $h_n k_{n-2} - h_{n-2} k_n = (-1)^n a_n$
4. $r_n - r_{n-2} = \frac{(-1)^n a_n}{k_n k_{n-2}}$
5. $mdc(h_n, k_n) = 1$

Dem. A primeira e a terceira equações podem ser demonstradas por indução; a segunda e a quarta equações obtêm-se dividindo respectivamente por $k_n k_{n-1}$ e $k_n k_{n-2}$; quanto à última equação, observe-se que $0 < d|h_n, k_n$ implica que $d|1$ e logo que $d = 1$. □

Um teorema sobre monotonia

Teorema 7.2.7 *Dada uma sucessão simples (a_n), seja $r_n = [a_0; \cdots, a_n]$. Para quaisquer $k, s \in \mathbb{N}$,*

1. $r_{2k} < r_{2k+2} < r_{2s+1} < r_{2s-1}$
2. (r_n) *converge.*

Dem. 2. A segunda afirmação é consequência da primeira: 1 implica que a subsucessão de índices pares e a subsucessão de índices ímpares convergem por serem monótonas e limitadas e também que

$$s \;=\; \lim_n r_{2n} \;\leq\; \lim_n r_{2n+1} \;=\; t$$

e, com (7.10), temos

$$0 \;\leq t - s \;\leq r_{2n+1} - r_{2n} \;=\; \frac{1}{k_{2n+1} k_{2n}} \to 0.$$

donde $t = s = \lim_n r_n$.

1. Do teorema 7.2.6.2 obtém-se $r_{2n+1} - r_{2n} > 0$; da asserção 4 do mesmo teorema obtém-se $r_{2n+1} - r_{2n-1} < 0$ & $r_{2n+2} - r_{2n} > 0$; agrupando:

$$r_{2k} < r_{2k+2} < r_{2s+1} < r_{2s-1} \quad (k, s \in \mathbb{N})$$

□

Defina-se $\theta_i \;=\; [a_i; a_{i+1}, \cdots]$ quando $a_{i+1} \geq 1$.

Lema 7.2.1 *Seja (a_n) uma sucessão simples na qual $a_1 > 0$.*

1. *Se $\theta_0 = [a_0; \cdots, a_n]$ & $a_n > 1$ ou se θ_0 é infinita, então $a_0 = [\theta_0]$.*

2. $\theta_0 = a_0 + \frac{1}{\theta_1}$

Dem. **(1)** O caso em que θ_0 é finita foi tratado na demonstração do teorema 7.2.2. O caso em que θ_0 é infinita obtém-se do seguinte modo: $r_0 < \theta_0 < r_1$ pelo teorema anterior, isto é, $a_0 < \theta_0 < a_0 + \frac{1}{a_1} \leq a_0 + 1$ & $a_0 < \theta_0 < a_0 + 1$, logo $a_0 = [\theta_0]$.

(2) Se θ_0 é finita, estamos perante a definição. Se θ_0 é infinita, tem-se

$$\begin{aligned} \theta_0 &= \lim_n [a_0; \cdots, a_n] = \lim_n \left(a_0 + \frac{1}{[a_1; \cdots, a_n]} \right) \\ &= a_0 + \frac{1}{\lim_n [a_1; \cdots, a_n]} \\ &= a_0 + \frac{1}{\theta_1} \end{aligned}$$

□

Teorema 7.2.8 *1. Duas fracções contínuas simples infinitas distintas têm limites distintos*

2. Duas fracções contínuas simples finitas distintas só têm o mesmo valor se forem da forma $[a_0; \cdots, a_n]$ *e* $[a_0; \cdots, a_n - 1, 1]$ *com* $a_n > 1$.

Veremos adiante que fracções contínuas simples infinitas têm limite irracional (teorema 7.2.9).

Dem. (do teorema 7.2.8) A proposição 2 foi de facto demonstrada no teorema 7.2.3.

(1) Se $\theta_0 = [a_0; \cdots] = [r_0, \cdots]$, pelo lema anterior concluimos $a_0 = [\theta] = r_0$ e também

$$\theta = a_0 + \frac{1}{\theta_1} = a_0 + \frac{1}{[r_1; \cdots, r_n]} = a_0 + \frac{1}{[r_1; \cdots, r_n]},$$

pelo que também $\theta_1 = [a_1; \cdots] = [r_1; \cdots]$. Por indução pode então mostrar-se que $a_n = r_n$ para qualquer $n \in \mathbb{N}$. □

Teorema 7.2.9 *Se* $\theta = [a_0; \cdots]$ *é uma fracção simples infinita, então* θ *é um número irracional.*

Dem. Pelos teoremas 7.2.6 e 7.2.7,

$$0 < |\theta - r_n| < |r_n - r_{n+1}| \quad \& \quad 0 < |k_n\theta - h_n| < \frac{1}{k_{n+1}};$$

se $\theta = \frac{a}{b}$ para alguns $a, b \in \mathbb{Z}$, ter-se-ia $0 < |k_n a - h_n b| < \frac{b}{k_{n+1}}$, o que, como $k_{n+1} \to +\infty$, implica $0 < |k_n a - h_n b| < 1$ para n grande, o que é impossível pois $k_n a - h_n b \in \mathbb{Z}$. Conclui-se que θ não pode ser racional. □

Completando

Teorema 7.2.10 *Todo o número irracional é limite de uma fracção contínua.*

Dem. Suponha-se que $r \notin \mathbb{Q}$ e defina-se

$$\begin{aligned} r &= x_0 \\ a_0 &= car(x_0) \quad \& \quad x_1 = \frac{1}{r - a_0} \\ a_n &= car(x_n) \quad \& \quad x_{n+1} = \frac{1}{x_n - a_n} \\ &= \frac{1}{x_n - car(x_n)} \qquad (n \in \mathbb{N}) \end{aligned}$$

Pode demonstrar-se por indução que todos os $a_n \in \mathbb{Z}$ e todos os $x_n \notin \mathbb{Q}$. Por construção

$$a_n \;=\; car(x_n) \;<\; x_n \;<\; a_n + 1, \quad \text{pois} \quad x_n \notin \mathbb{Z},$$

e daí $0 < x_n - a_n < 1$, pelo que

$$x_{n+1} \;=\; \frac{1}{x_n - a_n} \;>\; 1 \quad \& \quad a_{n+1} \;= car(x_{n+1}) \;\geq\; 1 \quad (n \geq 0);$$

por indução concluimos

$$a_n \geq 1 \quad (n \in \mathbb{N}),$$

observando que $x_n = a_n + \frac{1}{x_{n+1}}$; assim

$$\begin{aligned} r &= x_0 \;=\; a_0 + \frac{1}{x_1} = [a_0; x_1] \\ &= [a_0; a_1 + \frac{1}{x_2}] = [a_0; a_1, x_2] \\ &= \cdots \;=\; [a_0; a_1, \cdots, a_{n-1}, x_n]; \end{aligned}$$

Mas então, pelo teorema 7.2.5,

$$r \;=\; [a_0; \cdots, a_{n-1}, x_n] \;=\; \frac{x_n h_{n-1} + h_{n-2}}{x_n k_{n-1} + k_{n-2}}$$

seguindo-se

$$\begin{aligned} |r - r_{n-1}| &= |r - \frac{h_{n-1}}{k_{n-1}}| \\ &= |\frac{-(h_{n-1}k_{n-2} + h_{n-2}k_{n-1})}{k_{n-1}(x_n k_{n-1} + k_{n-2})}| \\ &= |\frac{(-1)^{n-1}}{k_{n-1}(x_n k_{n-1} + k_{n-2})}| \\ &= \frac{1}{k_{n-1}(x_n k_{n-1} + k_{n-2})} \leq \frac{1}{k_{n-1}} \end{aligned}$$

porque $x_n, k_m > 0$ & $\lim_n k_n = +\infty$. Em suma $r_{n-1} \to r$. □

E fica também demonstrado o teorema 7.2.4

7.3 Fracções periódicas

Nesta secção, abusaremos um pouco da notação identificando

$$[a_0; \cdots, a_n] \;=\; [a_0, \cdots, a_n]$$

Teorema 7.3.1 *Uma fracção contínua simples é periódica se e apenas se representa um irracional quadrático.*

Dem. Se a fracção é puramente periódica, digamos

$$\xi \;=\; [a_0; \cdots, a_n, \cdots] \;=\; [\overline{a_0, \cdots, a_n}],$$

observe-se que

$$\xi \;=\; [a_0; \cdots, a_n, \xi],$$

de onde se conclui

$$\xi \;=\; \frac{\xi h_n + h_{n-1}}{\xi k_n + k_{n-1}}, \tag{7.12}$$

que é uma equação quadrática de coeficientes inteiros.

Se a fracção é mista, digamos

$$\begin{aligned} \theta &= [b_0; \cdots, b_m, \overline{a_0, \cdots, a_n}] \\ \xi &= [\overline{a_0, \cdots, a_n}], \end{aligned}$$

então

$$\theta \;=\; \frac{\xi h'_m + h'_{m-1}}{\xi k'_m + k'_{m-1}}. \tag{7.13}$$

para certos $h', k' \in \mathbb{Z}$. E assim θ é também raiz de um polinómio do mesmo tipo; o que também pode ser visto do seguinte modo: ξ é irracional (a fracção é infinita), portanto, como raiz de polinómio do segundo grau de coeficientes inteiros, verifica

$$\xi = \alpha + \beta\sqrt{d} \quad \& \quad \alpha, \beta \in \mathbb{Q} \quad \& \quad d \in \mathbb{N};$$

pelo que, em virtude de (7.13), θ é da mesma forma, por também ser irracional.

Suponhamos agora que

$$a\xi^2 + b\xi + c = 0 \ \ \& \ \ a \neq 0 \quad \& \quad a, b, c \in \mathbb{Z} \tag{7.14}$$

$$\& \quad b^2 - 4ac \neq \quad \& \quad \xi = [a_0; \cdots, a_n, \cdots] \in \mathbb{R}\backslash\mathbb{Q}. \tag{7.15}$$

Tomando

$$s_n = [a_n; \cdots, a_{n+1}, \cdots]$$

tem-se

$$\xi = \frac{s_n h_{n-1} + h_{n-2}}{s_n k_{n-1} + k_{n-2}},$$

Substituindo em (7.14), obtém-se

$$A_n s_n^2 + B_n s_n + C_n = 0 \tag{7.16}$$

com

$$\begin{aligned} A_n &= a h_{n-1}^2 + b h_{n-1} k_{n-1} + c k_{n-1}^2 \\ B_n &= 2a h_{n-1} h_{n-2} + b(h_{n-1} kn - 2 + h_{n-2} k_{n-1}) + 2c k_{n-1} k_{n-2} \\ C_n &= a h_{n-2}^2 + b h_{n-2} k_{n-2} + c k_{n-2}^2 \end{aligned}$$

Vamos agora obter majorações de $|A_n|, |B_n|, |C_n|$ independentes de n.
$A_n \neq 0$ porque a equação (7.14) não tem raizes racionais.
A equação (7.16) mostra que

$$A_n x^2 + B_n x + C_n = 0 \tag{7.17}$$

tem raiz s_n. Além disso, alguns cálculos mostram que

$$B_n^2 - 4A_n C_n = (b^2 - 4ac)(h_{n-1} k_{n-2} - h_{n-2} k_{n-1})^2 = b^2 - 4ac \tag{7.18}$$

Ora

$$\left| \xi - \frac{h_n}{k_n} \right| < \frac{1}{k_n k_{n+1}} < \frac{1}{k_n^2}$$

pelo que

$$h_{n-1} = \xi k_{n-1} + \frac{\delta n - 1}{k_{n-1}} \quad \& \quad |\delta_{n-1}| < 1.$$

Daí

$$\begin{aligned} A_n &= a\left(\xi k_{n-1} + \frac{\delta n - 1}{k_{n-1}}\right)^2 + bk_{n-1}\left(\xi k_{n-1} + \frac{\delta n - 1}{k_{n-1}}\right) + ck_{n-1}^2 \\ &= (a\xi^2 + b\xi + c)k_{n-1}^2 + 2a\xi\delta_{n-1} + a\frac{\delta_{n-1}^2}{k_{n-1}^2} + b\delta_{n-1} \\ &= 2a\xi\delta_{n-1} + a\frac{\delta_{n-1}^2}{k_{n-1}^2} + b\delta_{n-1}, \end{aligned}$$

pelo que

$$|A_n| < 2|a\xi| + |a| + |b|$$

e, como $C_n = A_{n-1}$,

$$|C_n| < 2|a\xi| + |a| + |b|.$$

Por (7.18),

$$\begin{aligned} B_n^2 &\leq 4|A_n||C_n| + |b^2 - 4ac| \\ &< 4(2|a\xi| + |a| + |b|)^2 + |b^2 - 4ac|. \end{aligned}$$

Portanto os valores dos *números inteiros* A_n, B_n, C_n são limitados independentemente de n e o número de ternos (A_n, B_n, C_n) é finito; se (A, B, C) for um dos que ocorre pelo menos três vezes, os correspondentes $s_{n_1}, s_{n_2}, s_{n_3}$ têm pelo menos uma repetição, pois a equação (7.17) tem apenas duas soluções.

Se $s_{n_1} = s_{n_2}$ então

$$a_{n_1+i} = a_{n_2+i} \qquad (i \in \mathbb{N}_0)$$

e a fracção é periódica. □

7.4 Exercícios

1. Considere $n := \frac{4567890}{123456}$

   (a) Sem a calcular, determine a natureza da dízima de n e diga qual o comprimento do seu período.

   (b) Verifique que a resposta que deu à alínea anterior é correcta.

2. Prove os seguintes resultados

   (a) Suponha que $f \in \mathbb{Z}[x]$ e que f tem grau positivo. Mostre que *para qualquer* $m \in \mathbb{N}$, *existe* $n \in \mathbb{N}$ *tal que* $n > m$ & $f(n)$ *é composto.*

(b) A dízima $x := 0, a_1 \cdots a_n \cdots$ definida por

$$a_n \;=\; \begin{cases} 1 & \textit{se } n \textit{ é primo} \\ 0 & \textit{caso contrário.} \end{cases}$$

é irracional. (**SUG:** prove que *se a dízima é periódica, então existem* $a, b \in \mathbb{N}$ *tais que* $a \neq 0$ & $an + b$ *é primo quando* n *é suficientemente grande.*)

3. Seja x o número real em $]0, 1[$ cuja parte decimal é a sequência dos números primos, por exemplo, uma aproximação de x é $0,23571113171923 \cdots 89 \cdots 2161$ (2161 é um dos primeiros 1000 números primos). Prove que x é irracional. (**SUG:** Comece por deduzir do Teorema de Dirichlet sobre progressões aritméticas que há infinitos números primos congruentes com 1 para o módulo 10^s e conclua que há infinitos números primos cuja expressão decimal tem um número arbitrário de zeros consecutivos.)

4. Suponha que $b \in \mathbb{N}/\{1\}$.

   (a) Mostre que se $(a_n)_{n\in\mathbb{N}} \in \{0, 1, \cdots, b-1\}^{\mathbb{N}}$, então

   $$\sum_{i=1}^{\infty} \frac{a_n}{b^n} \;<\; +\infty \tag{7.19}$$

   (b) Mostre que qualquer número real em $]0, 1[$ tem uma *representação na base* b, i.e., é a soma de uma série como a descrita em (7.19).

   (c) Mostre que um número em $]0, 1[$ é racional sse a sua representação na base b é periódica.

5. Mostre que:

   (a) Se $a, b \in \mathbb{Z}$, $a < b$ e $r := [a; a_1, \cdots]$ e $s := [b; b_1, \cdots]$ são fracções contínuas simples, então $r < s$.

   (b) Se $r := [a_0; a_1, \cdots]$ e $s := [b_0; b_1, \cdots]$ são fracções contínuas simples e

   $$k \;:=\; \text{máx}\{j \in \mathbb{N} |\; \forall i \in \mathbb{N}\; [0 \leq i < j \Rightarrow a_i = b_i]\}$$

   então, convencionando que

   $$\text{máx}\, \emptyset \;:=\; 0,$$

   $$r \;<\; s \;\Leftrightarrow\; \begin{cases} k \textit{ é par} & e \quad a_k < b_k \\ k \textit{ é ímpar} & e \quad b_k < a_k. \end{cases}$$

6. Com a notação do texto mostre que

$$\forall n \in \mathbb{N} \ \left[n \geq 1 \Rightarrow \frac{k_n}{k_{n-1}} = [a_n; a_{n-1}, \cdots, a_1] \right]$$

e determine uma expressão semelhante para $\frac{h_n}{h_{n-1}}$, supondo que $a_0 \geq 0$.

7. Suponha que $r := \frac{m}{n}$ é uma fracção reduzida em $\mathbb{Q}$ e que $[a_0; \cdots, a_n]$ é a sua representação em fracção contínua. Com a notação do texto, mostre que

$$\forall i \in \mathbb{N} \ [0 \leq i \leq n-1 \Rightarrow \mid r_i - r \mid \leq \frac{1}{k_i k_{i+1}}]$$

e que a última desigualdade é igualdade apenas quando $i = n - 1$.

8. Mostre que se as primeiras n reduzidas de duas fracções contínuas simples são iguais duas a duas, então os primeiros n termos das fracções correspondentes também são iguais dois a dois.

9. Desenvolva os seguintes números em fracção contínua simples: 17/3, 3/17 e 8/1.

10. Converta em número racional as fracções contínuas $[2, 1, 4]$, $[-3, 2, 12]$ e $[0, 1, 1, 100]$.

11. Determine o valor das seguintes fracções contínuas:

    (a) $[\overline{1}]$;
    (b) $[2, \overline{1}]$;
    (c) $[2, 3, \overline{1}]$;
    (d) $[\overline{2}]$;
    (e) $[\overline{1, 2}]$;
    (f) $[\overline{2, 1}]$.

12. Para cada uma das dízimas $0, 12(4)$, $12, 23(465)$ e $1, (12345679)$, determine a fracção reduzida correspondente.

13. Determine o desenvolvimento em fracção contínua periódica dos seguintes números irracionais quadráticos

    (a) $\sqrt{29}$
    (b) $\sqrt{41}$
    (c) $\frac{\sqrt{37}+5}{3}$
    (d) $1 - \frac{2}{\sqrt{3}}$

14. Demostre que

a) $\sqrt{n^2+1} = [n, \overline{2n}]$ **b)** $\sqrt{n(n+1)} = [n, \overline{2, 2n}]$

15. Demonstre que se n é um inteiro positivo se tem

$$\frac{n+\sqrt{n^2+4}}{2} = [\overline{n}]$$

Capítulo 8

Extensões

De ora em diante supomos fixado um modelo de corpo ordenado completo, isto é, o corpo dos números reais; também nos referiremos indistintamente ao corpo enquanto estrutura algébrica $\mathcal{K} = (K, +, \cdot, 0, 1, <)$ ou ao seu suporte K; além disso, designaremos genericamente por $+$ e $\cdot$ (abreviando $a \cdot b$ por ab) as operações de soma e produto de qualquer corpo; finalmente: $\mathbf{0} = 0$ e $\mathbf{1} = 1$.

8.1 Os números complexos

O polinómio $x^2 + 1$ não tem raizes reais, pois $-1 < 0 \leq x^2$ em qualquer corpo ordenado (lema 6.1.1).

Esta secção consiste essencialmente na demonstração do seguinte

Teorema 8.1.1 *A menos de um isomorfismo de corpos, existe um corpo mínimo que prolonga o corpo $\mathbb{R}$ e onde o polinómio $x^2 + 1$ tem uma raiz.*

Admitamos a existência de um corpo K do qual o corpo $\mathbb{R}$ é subcorpo e onde existe um elemento designado por i tal que

$$i^2 \ + \ 1 \ = \ 0. \tag{8.1}$$

Repare-se que $\mathbb{R} \subseteq K$ e seja

$$\mathbb{C} \ = \ \{a + bi : a, b \in \mathbb{R}\}$$

Lema 8.1.1 *Para quaisquer números reais* $a,\ b,\ c$ *e* d

1. $a+bi = c+di$ *sse* $a=c$ *e* $b=d$.
2. $(a+bi)+(c+di) = (a+c)+(b+d)i$
3. $(a+bi)(c+di) = (ac-bd)+(ad+bc)i$
4. $(a+bi)^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$

Dem. (1) Se $a+bi = c+di$, então $a-c = (b-d)i$ portanto $(a-c)^2 = -(b-d)^2$; mas então

$$0 \ \leq \ (a-c)^2 \ = \ -(b-d)^2 \ \leq \ 0$$

pelo que $0 = a-c = b-d$.

As restantes propriedades são consequências do facto de K ser um corpo e a sua demonstração fica como exercício. □

Daqui resulta o seguinte teorema:

Teorema 8.1.2 $\mathcal{C} = (\mathbb{C}, +, \cdot, 0, 1)$ *é um corpo que prolonga* $\mathbb{R}$ *propriamente.*

Dem. Vejamos apenas que é extensão própria:

$$i \ = \ 0+1i \in \mathbb{C} \quad \& \quad \mathbb{R} = \mathbb{R}+0i \ \subseteq \ \mathbb{C} \quad \& \quad i \in \mathbb{C}\backslash\mathbb{R}$$

□

Por outro lado, o lema 8.1.1 só utiliza o facto de i ser uma raiz quadrada de -1, pelo que vale seja ela qual for, em particular se, por exemplo, substituirmos i por $-i$ no enunciado.

Por outro lado, também não interessou a natureza do corpo $\mathcal{K}$ para além do facto de conter uma raiz quadrada de -1.

Resumindo:

Teorema 8.1.3 *Qualquer corpo que contenha (um corpo ordenado isomorfo a)* $\mathbb{R}$ *e onde a equação* $x^2+1=0$ *tenha solução contém um corpo isomorfo a* $\mathcal{C}$*; um isomorfismo* Φ *pode ser descrito do seguinte modo: se* i *e* j *designam respectivamente raizes quadradas de* -1 *em cada um dos corpos extensão, então*

$$\Phi(a+bi) \ = \ a+bj \quad (a,b \in \mathbb{R}).$$

Fica assim cumprido o propósito anunciado no início da secção. Chamamos a esta extensão mínima o corpo dos números **complexos.**

Observe-se ainda que definindo **conjugado**, $\overline{z}$, do número complexo $z = a + bi$ $(a, b) \in \mathbb{R}^2$, por

$$\overline{a + ib} \;=\; a - ib$$

e uma função $N : \mathbb{C} \to \mathbb{R}$, designada também **norma**, por

$$N(a + bi) \;=\; a^2 + b^2 \qquad ((a, b \imath v t r^2)) \tag{8.2}$$

vem, para $z = a + bi,\ w = c + di \in \mathbb{C},\ a, b, c, d \in \mathbb{R}$,

$$\begin{aligned} N(z) &= z\overline{z} \\ z^{-1} &= \frac{\overline{z}}{N(z)} \\ N(zw) &= N(z)N(w). \end{aligned}$$

Em particular

$$(a^2 + b^2)(c^2 + d^2) \;=\; (ac - bd)^2 + (ad + bc)^2 \qquad (a, b, c, d \in \mathbb{R}).^1$$

Terminamos com as seguintes observações:

Observações.
1. O corpo $\mathcal{C}$ não é ordenável, pois $i^2 = -1$.

2. O corpo $\mathcal{C}$ é algebricamente fechado, isto é, vale o seguinte teorema, cuja demonstração não cabe no âmbito deste curso.

Teorema 8.1.4 (Fundamental da Álgebra)
Qualquer polinómio de coeficientes em $\mathbb{C}$ *e grau maior ou igual a 1 tem raizes em* $\mathbb{C}$.

8.2 Quaterniões

Seja $\mathbb{K} = \prec \mathbf{K}, + \succ$ um espaço vectorial sobre o corpo $\mathbb{R}$ dos números reais com dimensão 4. Vamos definir uma operação binária $\bullet$ de modo a que

K1. $\prec \mathbf{K}, +, \bullet \succ$ é anel de divisão.

K2. O corpo $\mathbb{C}$ dos números complexos é (isomorfo a um) subanel de $\mathbb{K}$.

Designemos por $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ uma base de $\mathbb{K}$. Como é habitual, simplificamos a notação $x \bullet y$ por xy e identificamos $\mathbb{K}$ com $\mathbf{K}$. Defina-se

1. $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}$
2. $\mathbf{ij} = k \quad \mathbf{jk} = \mathbf{i} \quad \mathbf{ki} = \mathbf{j}$

[1] Recorde-se a propósito o teorema 4.3.3.

3. Se $a,b,c,d,\alpha,\beta,\gamma,\delta \in \mathbb{R}$, $\quad x = a\mathbf{1}+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$, $\quad y = \alpha\mathbf{1}+\beta\mathbf{i}+\gamma\mathbf{j}+\delta\mathbf{k}$ então

$$\begin{aligned} xy &= (a\alpha - b\beta - c\gamma - d\delta)\mathbf{1} + (a\beta + b\alpha + c\delta - d\gamma)\mathbf{i} \\ &\quad (a\gamma + c\alpha + d\beta - b\delta)\mathbf{j} + (a\delta + d\alpha + b\gamma - c\beta)\mathbf{k} \end{aligned}$$

Três propriedades de demonstração particularmente rápida

Teorema 8.2.1 *Tem-se*

1. $\mathbf{1}$ *é elemento neutro de* $\bullet$.
2. $\mathbf{ji} = -k \quad \mathbf{kj} = -\mathbf{i} \quad \mathbf{ik} = -\mathbf{j}$
3. $\prec \mathbf{K}, \bullet \succ$ *não é comutativo.*
4. $\mathbb{C}$ *é isomorfo ao subanel de* $\mathbb{K}$ *cujos elementos são todos os da forma* $a\mathbf{1}+b\mathbf{i}$, *em que* $a,b \in \mathbb{R}$.

E vale **K2**. Quanto a **K1**

Teorema 8.2.2 $\mathbb{K}$ *é anel de divisão*

Dem. As propriedades da soma estão garantidas pelo facto de $\mathbb{K}$ ser espaço vectorial. A única propriedade que possivelmente exige mais que cálculos rotineiros é a existência de opostos multiplicativos. Na verdade, analogamente ao que se passa com $\mathbb{C}$, se $a\mathbf{1}+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} \neq 0 \quad a,b,c,d \in \mathbb{R}$

$$(a\mathbf{1}+b\mathbf{i}+c\mathbf{j}+d\mathbf{k})^{-1} = \frac{a\mathbf{1}-b\mathbf{i}-c\mathbf{j}-d\mathbf{k}}{a^2+b^2+c^2+d^2}$$

□

Parece-nos interessante observar que, analogamente ao que se faz em $\mathbb{C}$, definindo o **conjugado** do quaternião $\alpha = a\mathbf{1}+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$, $\overline{\alpha}$, por

$$\overline{a\mathbf{1}+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}} = a-b\mathbf{i}-c\mathbf{j}-d\mathbf{k} \qquad ((a,b,c,d) \in \mathbb{R}^4), \tag{8.3}$$

e definindo a **norma** do quaternião, N, por

$$N(\alpha) := a^2+b^2+c^2+d^2 \qquad ((a,b,c,d) \in \mathbb{R}^4),$$

então, para quaiquer $\alpha,\beta \in \mathbb{K}$,

$$\begin{aligned} N(\alpha) &= \alpha\overline{\alpha} \\ \alpha^{-1} &= \frac{\overline{\alpha}}{N(\alpha)} \\ N(\alpha\beta) &= N(\alpha)N(\beta). \end{aligned}$$

Em particular, vale uma **identidade de Lagrange** que enunciamos de seguida.

Teorema 8.2.3 *Se* $\alpha = a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ *e* $\beta = u\mathbf{1} + v\mathbf{i} + x\mathbf{j} + y\mathbf{k}$ *são quaterniões e* $(a,b,c,d),\ (u,v,x,y) \in \mathbb{R}^4$*, então*

$$\begin{aligned}(a^2+b^2+c^2+d^2)(u^2+v^2+x^2+y^2) &= (au+bv+cx+dy)^2 + (av-bu-cy+dx)^2 \\ &+ (ax+by-cu-dv)^2 + (ay-bx+cv-du)^2.\end{aligned}$$

8.3 Extensões ordenadas

8.3.1 (In)Completude

Leibniz utilizava (e Newton também) *números infinitesimais* , isto é, números não nulos, mas de valor absoluto menor que qualquer número real positivo, do mesmo modo que os números reais. Na verdade um grande número de matemáticos do século XVIII (e Fermat antes deles) obteve resultados fundamentais utilizando os primeiros, e mesmo Euler se socorreu de números infinitos para obter, por exemplo, o desenvolvimento da função *seno* em produto. Tal pode de facto ser feito no contexto adequado e tomando os devidos cuidados como se pode ver em [19]. Para já tratamos apenas de algumas propriedades puramente algébricas de extensões próprias do corpo dos números reais.

Teorema 8.3.1 *Se* K *é um corpo ordenado que prolonga propriamente o dos números reais, então existem em* K *elementos positivos menores que qualquer número real positivo.*

Dem. Suponhamos que K é uma extensão ordenada própria de $\mathbb{R}$ e que $\alpha \in K\backslash\mathbb{R}$. Podem dar-se três casos a saber

1. $\forall r \in \mathbb{R}\ r < \alpha$
2. $\forall r \in \mathbb{R}\ \alpha < r$
3. $\exists r, s \in \mathbb{R}\ r < \alpha < s$

No primeiro caso, como K é um corpo ordenado,

$$\forall s \in \mathbb{R}^+ \quad 0 < \frac{1}{\alpha} < \frac{1}{s}$$

ou, como se pretende,

$$\forall r \in \mathbb{R}^+ \quad 0 < \frac{1}{\alpha} < r$$

O segundo caso, pode tratar-se analogamente tomando $-\alpha$ em vez de α.

No terceiro caso defina-se

$$A \ = \ \{x \in \mathbb{R} :\ x < \alpha\}$$

O conjunto $A \subseteq \mathbb{R}$, não é vazio, pois $r \in A$, e é majorado em $\mathbb{R}$ por s, portanto tem um supremo também em $\mathbb{R}$, digamos $\sigma = sup A$. Vamos ver que $|\sigma - \alpha|$ é o número

pretendido. Tome-se $M \in \mathbb{R}^+$. Por um lado $\sigma - M < \sigma$ e assim existe $a \in A$ tal que $\sigma - M < a < \alpha$ e

$$\sigma \ - \ \alpha \ < \ M;$$

por outro lado, $\sigma < \sigma + M$ e portanto $\alpha \leq \sigma + M \in \mathbb{R}$; segue-se que de facto $\alpha < \sigma + M \in \mathbb{R}$, ou seja

$$\alpha \ - \ \sigma \ < \ M.$$

As duas desigualdades mostram o que se pretende. □

Os elementos $\alpha \in K$ cuja existência está garantida pelo teorema 8.3.1 dizem-se **infinitesimais.** Os outros elementos, ainda designados por α, podem ser **infinitos**, se

$$\forall r \in \mathbb{R}^+ \ r < |\alpha| \tag{8.4}$$

ou **finitos**, se

$$\exists r \in \mathbb{R}^+ \ |\alpha| < r. \tag{8.5}$$

A condição 8.4 é equivalente à disjunção das 1 ou 2 da demonstração acima; a condição 8.5 é equivalente a 3 da mesma demonstração.

8.3.2 Parte standard

Notemos $x \approx y$ se $x - y$ é infinitesimal, o que também se traduz por x está *infinitamente próximo de* y.

Com um pouco mais de precisão pode mostrar-se o seguinte

Teorema 8.3.2 *Seja K uma extensão própria ordenada do corpo dos números reais. Para cada elemento finito $\alpha \in K$, existe um e só um número real ${}^o\alpha$ tal que ${}^o\alpha \approx \alpha$.*

Dem. Releia-se a demonstração anterior e tome-se ${}^o\alpha = \sigma$. Mostrou-se que $\alpha \approx {}^o\alpha \in \mathbb{R}$. Quanto à unicidade, observe-se que outro número real infinitamente próximo de α estaria também infinitamente próximo de ${}^o\alpha$ e portanto o valor absoluto da diferença entre os dois seria um número *real* menor que qualquer número *real* positivo, pelo que só poderia ser zero. □

O número ${}^o\alpha$ cuja existência é garantida por este teorema diz-se **parte standard** de α.

Teorema 8.3.3 *Seja K uma extensão ordenada própria do corpo $\mathbb{R}$. Sejam respectivamente $\mathcal{O}$ e Θ os conjuntos dos números finitos e dos números infinitesimais em K. Para simplificar a notação, entendam-se as operações e ordem restringidas adequadamente.*

1. *$(\mathcal{O}, +, \cdot, \leq)$ é um domínio de Integridade ordenado.*

2. *$(\Theta, +, \cdot, \leq)$ é um domínio de Integridade ordenado e ideal em $(\mathcal{O}, +, \cdot, \leq)$; em particular*
$$\forall \varepsilon \in \Theta \ \forall \delta \in \mathcal{O} \ \ [0 \leq |\delta| \leq \varepsilon \ \Rightarrow \ \delta \in \Theta]. \tag{8.6}$$

3. *A função $st : (\mathcal{O}, +, \cdot) \to (\mathbb{R}, +, \cdot)$ é um epimorfismo de anéis, $\Theta = st^{-1}(0)$ e $\mathcal{O}_{/\Theta}$ é isomorfo a $\mathbb{R}$.*

Concluimos observando que

Corolário 8.3.1 *Os corpos ordenados que prolongam propriamente o corpo dos números reais não são completos.*

Dem. Vejamos o conjunto dos infinitesimais Θ não tem supremo, mesmo sendo majorado por qualquer número *real* positivo: se $s = \sup \Theta$ então $s \notin \Theta$, porque $0 < s < 2s \in \Theta$; mas então existe $r \in \mathbb{R}$ tal que $0 < r \leq s$, portanto (o supremo) s é menor ou igual a(o majorante) r, o que é absurdo. Em suma: Θ não tem supremo. □

8.4 Exercícios

1. Determine os seguintes produtos de quaterniões:
   (a) $(i + j)(i - j)$;
   (b) $(1 - i + 2j - 2k)(1 + 2i - 4j + 6k)$.

2. Mostre que os únicos quaterniões que comutam com i são da forma $a + bi$.

3. Determine todos os quaterniões que comutam simultaneamente com i e j.

4. Mostre que há um número infinito de soluções da equação $x^2 = -1$ no conjunto dos quaterniões.

5. Suponha que $a = a_1^2 + a_2^2 + a_3^2 + a_4^2$ e que $b = b_1^2 + b_2^2 + b_3^2 + b_4^2$, onde $a_i, b_i \in \mathbb{Z}$. Mostre que $ab = c_1^2 + c_2^2 + c_3^2 + c_4^2$, onde
$$(a_1 + a_2 i + a_3 j + a_4 k)(b_1 + b_2 i + b_3 j + b_4 k) = c_1 + c_2 i + c_3 j + c_4 k.$$

6. Seja $\mathcal{K} = (K, +, \cdot, \mathbf{0}, \mathbf{1}, <)$ um corpo ordenado que prolonga propriamente o dos números reais. Sejam respectivamente Θ e $\mathcal{O}$ os conjuntos de elementos infinitesimais e elementos finitos de $\mathcal{K}$. Mostre que, para quaisquer $a, b, x, y \in K$
   (a) Se $x \approx a \in \mathcal{O}$ então $x^2 \approx a^2$, mas pode acontecer $x \approx a$ & $x^2 \not\approx a^2$.
   (b) Se $a, b \in \mathcal{O}$ & $x \approx a$ & $y \approx b$, então $xy \approx ab$, mas pode acontecer $x \approx a$ & $y \approx b$ mas $xy \not\approx ab$.

(c) Se $x \approx a \not\approx 0$, então $\frac{1}{x} \approx \frac{1}{a}$, mas pode acontecer $x \approx a$ & $\frac{1}{x} \not\approx \frac{1}{a}$.

(d) Sendo a função $f(x)$ um polinómio em x de coeficientes em $\mathcal{O}$ e grau $n \in \mathbb{N}$ e $a \in \mathcal{O} \setminus \Theta$, para todo o $h \in \Theta$, existe $\varepsilon \in \Theta$ tal que

$$f(a+h) \;=\; f(a) \;+ f'(a)h \;+ \varepsilon h;$$

(e) Se $f(x) = \frac{1}{x},\ a \notin \Theta$ & $h \approx 0$, então existe $\varepsilon \in \Theta$ tal que

$$f(a+h) \;=\; f(a) \;-\; \frac{1}{a^2}h \;+\; \varepsilon h.$$

Parte III

Aplicações

Capítulo 9

Criptografia

9.1 Introdução

Um **alfabeto** é um conjunto finito de símbolos com os quais serão elaboradas sequências ou **unidades de texto**. Designaremos por $T(\mathcal{A})$ o conjunto das unidades de texto no alfabeto $\mathcal{A}$.

Uma **função de cifra** é uma aplicação injectiva de um conjunto de unidades de texto para outro; os elementos do contradomínio da função de cifra designam-se por **unidades de cifra**. Um **texto** é uma sequência de unidades de texto; um **texto cifrado** é uma sequência de unidades de cifra.

Vamos considerar apenas casos em as unidades de cifra e de texto são do mesmo tipo e construidas com o mesmo alfabeto.

Um **sistema de cifra** é um terno

$$T(\mathcal{A}) \xrightarrow{f} T(\mathcal{A}) \xrightarrow{f^{-1}} T(\mathcal{A})$$

em que f é uma função de cifra.

9.2 Sistemas afins

Seja $\mathcal{A}$ um alfabeto com n símbolos distintos ($n > 1$) e fixe-se uma enumeração $\nu : \mathcal{A} \to \{0, 1, \cdots, n-1\}$.

Uma k**-unidade de texto** é uma sequência de k elementos de $\mathcal{A}$. Como convencionámos na introdução, as unidades de cifra são também sequências de k elementos de $\mathcal{A}$. Cada texto é constituido por um número inteiro de unidades; se for necessário, completa-se a última unidade por repetição do último símbolo do alfabeto.

A função de cifra **afim de parâmetros** a e b é a função f construida do seguinte modo:

1. Fixam-se $a \in \mathbb{N}$ primo com n e $b \in \{1, \cdots, n-1\}$

2. Cada unidade de texto $u = A_0 \cdots A_{k-1}$ é codificada por um número $\phi(u)$ que se obtém por expressão na base n:
$$\phi(u) = \nu(A_0)n^{k-1} + \cdots + \nu(A_{k-2})n + \nu(A_{k-1})$$
3. Para cada unidade de texto u, $f(u) = \phi^{-1}\left(a\phi(u) + b \ (mod\ n^k)\right)$ $0 \leq \phi\left(f(u)\right) \leq n^k - 1$.

Os parâmetros a, b constituem a **chave** da cifra.

Teorema 9.2.1 *Se f é uma função de cifra afim de parâmetros a, b e a^* designa o inverso de a $(mod\ n^k)$ então, para cada unidade de cifra c*

$$f^{-1}(c) = \phi^{-1}\left(a^*\phi(c) - a^*b \ (mod\ n^k)\right).$$

Os sistemas afins mais simples ocorrem com $k = 1 = a$ e podem ser designados por **sistemas de deslocamento**.

9.3 Codificação Matricial

Outra forma de codificar resulta de se tomar uma k-unidade de texto como um elemento de $(\mathbb{Z}_n)^k$, como módulo sobre o anel $\mathbb{Z}$, e utilizar matrizes. Vejamos um caso menos complicado.

Designe-se o conjunto das matrizes 2×2 com coordenadas em $\mathbb{Z}_n$ por $\mathcal{M}_2$.

Teorema 9.3.1 *Se*

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathcal{M}_2 \qquad \& \qquad \Delta = ad - bc,$$

as seguintes condições são equivalentes.

1. $mdc(\Delta, n) = 1$
2. *A é invertível*
3. $ker(A) = \vec{0} \in (\mathbb{Z}_n)^2$
4. *A define um automorfismo de $(\mathbb{Z}_n)^2$*

Dem. $(1 \Rightarrow 2)$ Designando por Δ^* o inverso de Δ $(mod\ n)$, é fácil verificar que

$$A^{-1} = \Delta^* \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$(2 \Rightarrow 4)$ e $(4 \Rightarrow 3)$ são imediatas.
$(3 \Rightarrow 1)$ Suponha-se que $\delta = mdc(\Delta, n) > 1$ e ponha-se $n = m\delta$. Repare-se que $0 < m < n$ e portanto $n \not| m$; em particular

$$m \not\equiv 0 \ (mod\ n). \tag{9.1}$$

Se δ divide todas as coordenadas de A, então

$$A \begin{bmatrix} m \\ m \end{bmatrix} = \vec{0}$$

e, por (9.1), não vale 3.

Se δ não divide simultâneamente a e b então

$$\begin{bmatrix} -bm \\ am \end{bmatrix} \neq \vec{0} \tag{9.2}$$

mas

$$A \begin{bmatrix} -bm \\ am \end{bmatrix} = \begin{bmatrix} 0 \\ m\Delta \end{bmatrix} = \vec{0}.$$

e torna a não valer 3, em virtude de (9.2).

Se δ não divide simultâneamente c e d então

$$\begin{bmatrix} dm \\ -cm \end{bmatrix} \neq \vec{0} \tag{9.3}$$

mas

$$A \begin{bmatrix} dm \\ -cm \end{bmatrix} = \begin{bmatrix} m\Delta \\ 0 \end{bmatrix} = \vec{0}.$$

e, de novo, não vale 3, em virtude de (9.3). □

Neste contexto, os textos são estruturados em matrizes de duas linhas, correspondendo cada coluna a uma unidade de cifra. As funções de cifra afins f passam a entender-se do seguinte modo:

1. São dados um elemento $\vec{b} \in (\mathbb{Z}_n)^2$ e uma matriz invertível $A \in \mathcal{M}_2$.
2. A primeira transformação $\phi : T(\mathcal{A}) \to (\mathbb{Z}_n)^2$ toma a forma
$$\phi\left(\begin{bmatrix} A_1 \\ A_2 \end{bmatrix}\right) = \begin{bmatrix} \nu(A_1) \\ \nu(A_2) \end{bmatrix}$$
3. Módulo n, tem-se finalmente
$$f(u) \;=\; \phi^{-1}\left(A\phi(u) + \vec{b}\right).$$

9.4 Criptografia de chave pública

Recorde-se que um número natural se diz **livre de quadrados** se for 1 ou um produto de números primos *distintos.* Seja também ϕ a função de Euler. O teorema seguinte enuncia alguns lemas de que precisamos para esta secção.

Teorema 9.4.1 *1. Se m é livre de quadrados e $d = mcd(a, m)$ então a é primo com $\frac{m}{d}$.*

2. Se m é livre de quadrados e $d|m$ então d é primo com $\frac{m}{d}$.

3. Para qualquer $m \in \mathbb{N}$, se $d|m$ então $\phi(d)|\phi(m)$.

4. Se $n \equiv 1 \ (mod\ \phi(m))$ e a é primo com m, então $a^n \equiv a \ (mod\ m)$

5. Se m é livre de quadrados e $n \equiv 1 \ (mod\ \phi(m))$, então $\forall a \in \mathbb{N}\ a^n \equiv a \ (mod\ m)$.

Dem. Demonstraremos apenas a proposição 5. As proposições anteriores são essencialmente lemas para a última.

Para evitar trivialidades podemos supor que $a, m, n > 1$. Seja $d = mdc(a, m)$; tem-se para certos $r, s \in \mathbb{N}_0$

$$\begin{aligned} a^n &= a^{r\phi(m)+1} \\ &= a^{rs\phi(\frac{m}{d})+1} \\ &= \left[a^{\phi(\frac{m}{d})}\right]^{rs} \cdot a \\ &\equiv 1^{rs} \cdot a \quad (mod\ \frac{m}{d}) \\ &\equiv a \quad (mod\ \frac{m}{d}) \end{aligned}$$

Em particular, para algum $\alpha \in \mathbb{N}$,

$$d|a^n - a = \alpha \cdot \frac{m}{d}$$

e, pela proposição 1, $d|\alpha$, donde $a^n \equiv a \ (mod\ m)$. □

Segue-se como corolário:

Teorema 9.4.2 *Se m é simples, $k, k' \in \mathbb{N}$ e $kk' \equiv 1 \ (mod\ \phi(m))$, então $\forall a \in \mathbb{N}\ a^{kk'} \equiv a \ (mod\ m)$.*

UM EXEMPLO DE CODIFICAÇÃO

I. Fixe-se um código n_σ para cada símbolo σ da linguagem que vai ser utilizada.

Exemplo 9.4.1 Se σ designar uma letra do alfabeto latino, seja n_σ o seu número de ordem alfabética habitual com dois dígitos: $n_a = 01,\ n_b = 02,\ ...,\ n_j = 10, ...$

II. Traduza-se a mensagem para esse código.

Exemplo 9.4.2 De acordo com o exemplo anterior, supondo ainda que $n_o = 35$ a palavra *código* é traduzida por 033504090715.

III. Pode-se ficar por aqui ou dificultar um pouco mais a descodificação.

Exemplo 9.4.3 Digamos que o maior n_σ é 50 e seja $m = 5 \cdot 17$, pelo que $\phi(m) = 64$; tome-se também $k = 5$ & $k' = 13$. Em vez de se codificar como no exemplo 9.4.1, recodifique-se

$$n'_\sigma \ = \ (n_\sigma)^5$$

com as letras em blocos separados: a palavra *código* passa a ser traduzida por

$$243\ 52521875\ 1024\ 59049\ 16807\ 759375$$

IV. A descodificação pode ser feita utilizando o teorema 9.4.2 por quem saiba que $k' = 13$ e $m = 85$.

Exemplo 9.4.4 $(mod\ 85)$ tem-se

$$\begin{aligned} 243^{13} &\equiv 73^{13} \equiv (-12)^{13} \\ &\equiv -(12^3)^4 \cdot 12 \equiv -28^4 \cdot 12 \\ &\equiv -21 \cdot 12 \equiv -82 \equiv 3 \\ &= 03 \end{aligned}$$

Mais um caracter

$$\begin{aligned} 52521875^{13} &\equiv 35^{13} \equiv (35^4)^3 \cdot 35 \\ &\equiv (35^3) \cdot 35 = 35^4 \\ &\equiv 35 \end{aligned}$$

Repare-se que os exemplos que temos vindo a descrever podem ser tratados com uma calculadora científica não particularmente sofisticada. Codificações mais seguras podem fazer-se utilizando números primos muito grandes para compor o módulo m.

9.5 Assinaturas; ISBN

Num sistema de chave pública uma **assinatura** do detentor da chave (m, k) pode ser $\alpha \equiv k^{k'}\ (mod\ n)$: o receptor, que conhece (m, k), deverá obter $k \equiv \alpha^k\ (mod\ m)$.

O *International Standard Book Number*, ISBN, é um instrumento de detecção de eventual existência de erro de referência.

Cada livro tem um ISBN que consiste numa sequência $a_1 \cdots a_{10}$ de dez símbolos: os primeiros nove são algarismos de 0 a 9, o décimo pode ser um desses algarismos ou a letra X, para representar dez na base 11, de acordo com a seguinte congruência

$$a_{10} \ \equiv \sum_{i=1}^{9} a_i i \quad (mod\ 11)$$

Esta representação é sensível a trocas de quaisquer dois símbolos, indicando uma probabilidade alta de designar o livro correctamente caso a congruência se verifique.

9.6 Exercícios

1. (a) Suponha que $m = pq$ e $\phi = (p-1)(q-1)$ onde p e q são números reais. Encontre uma fórmula para p e para q em função de m e de ϕ;

   (b) Suponha que $m = 39247771$ é o produto de dois primos, p e q, distintos. Determine p e q sabendo que $\phi(m) = 39233944$

2. Sejam $T = \{\bigcirc, A, B, C, D, \ldots, W, X, Y, Z\}$, onde $\bigcirc$ representa o espaço em branco e σ a correspondência que a cada letra faz corresponder o seu número de ordem alfabética habitual com dois dígitos:

   $\sigma(A) = 01, \sigma(B) = 02, \ldots, \sigma(Z) = 26$ e $\sigma(\bigcirc) = 00$.

   Consideremos o conjunto $T^2 = \{xy \ : \ x, y \in T\}$, a correspondência $\tau : T^2 \to \{0, 1, \ldots, m-1\}$ definida por $\tau(xy) = \sigma(x)\sigma(y) \ (mod\ 1333)$ (ab representa a concatenação de a com b), o módulo=1333 ($1333 = 31 \times 43$) e o expoente codificador $s = 13$.

   (a) Prove que a correspondência τ é uma aplicação injectiva;

   (b) Prove que τ não é sobrejectiva;

   (c) Codifique e descodifique as palavras SIM e EULER;

   (d) Descodifique 084404430682 e 084405821121.

Bibliografia

[1] **George E. Andrews:** *Number Theory,* Dover 1971.

[2] **William W. Adams e Larry J. Goldstein:** *Introduction to Number Theory,*Prentice-Hall, Inc., 1976.

[3] **Tom M. Apostol:** *Introduction to Analytic Number Theory* Spriger UTM 1976.

[4] **A. Baker:** *A Concise Introduction to the Theory of Numbers,* CUP 1984.

[5] **Owen Brison:** *Teoria Elementar dos Números I e II:* Bol. da SPM 33, Dezembro de 1995 & 37, Outubro de 1997.

[6] **John H. Conway & Richard K. Guy:** *O Livro dos Números*, (Trad. de José Sousa Pinto) Univ. de Aveiro/Gradiva 2000.

[7] **H. Davenport:** *The Higher Arithmetic,* CUP 1995.

[8] **Herbert B. Enderton:** *A Mathematical Introduction to Logic*, Harcourt/Acad. Press 2001.

[9] **A. Gonçalves:** *Introdução à Álgebra*, IMPA 1979.

[10] **G. H. Hardy e E. M. Wright:** *An Introduction to the Theory of Numbers,* Oxford, 1985.

[11] **I. N. Herstein:** *Topics in Algebra*, John Wiley & Sons 1975.

[12] **K. Ireland:** *A Classical Introduction to Modern Number Theory,* Springer GTM 84, 1990.

[13] **Neil Koblitz:** *A course in Number Theory and Criptography* Springer GTM 114, 1994.

[14] **I. Niven, H. Zuckerman e H. Montgomery:** *An Introduction to the Theory of Numbers,* John Wiley & Sons, Inc., 1991.

[15] **J. Rey Pastor e P. Pi Calleja & C. A. Trejo:** *Análisis Matemático*, I Vol., Kapeluz, 1969.

[16] **J. S. Pinto:** *Métodos Infinitesimais de Análise Matemática*, Fund. Calouste Gulbenkian 2000.

[17] **J. S. Pinto e A. M. Caetano:** *Conjuntos Numéricos, Estudo I,* Cadernos de Matemática, Universidade de Aveiro, 1996.

[18] **Michael Spivak:** *Calculus*,W. A. Benjamin, Inc., Reverté 1975. (tradução espanhola Reverté S.A.)

[19] **K. D. Stroyan, W. A. J. Luxemburg:** *Introduction to the Theory of Infinitesimals,* Acad. Press, 1976.

Índice remissivo