Tópicos de Matemática Elementar

Ano lectivo 2002–03

António Machiavelo

Departamento de Matemática Pura

da

Universidade do Porto

Part I
Os Números

1 Os Inteiros: a Teoria dos Números

1.1 O mistério mais antigo

Grécia clássica: divisores = “partes que *medem* o número” [1]

Exemplo: $\rightsquigarrow$ “2 mede 6”.

Número Perfeito = aquele que é igual à $\underbrace{\text{soma das suas partes}}_{\text{soma dos seus divisores, excluindo o próprio (mas incluindo 1)}}$ [2].

Exemplos: $6 = 1 + 2 + 3$;

$28 = 1 + 2 + 4 + 7 + 14.$

Notação: $\sigma(n)$ = soma de *todos* os divisores de n $\big($i.e. 1 e n incluídos$\big)$ $= \sum_{d|n} d.$

(σ lê-se “sigma” e $d \mid n$ significa “d divide n”.)

É claro que: $\boxed{n \text{ perfeito} \Leftrightarrow \sigma(n) = 2n}$

Exemplo: $\sigma(60) = 1{+}2{+}3{+}4{+}5{+}6{+}10{+}12{+}15{+}20{+}30{+}60 = 168(> 2{\cdot}60...)$

Dado o inteiro n, considere-se a sua decomposição em factores primos:

$$n = p_1^{\alpha_1} \cdots p_t^{\alpha_t};\ p_i \text{ primo}, \alpha_i \geq 0.$$

(tal decomposição existe sempre e é única, a menos de uma permuta dos p_i’s...)

Exemplo: $60 = 2^2 \cdot 3 \cdot 5$.

Tem-se então que:

$$\begin{aligned} \sigma(n) &= \sum_{0 \leq ?_i \leq \alpha_i} \underbrace{p_1^{?_1} \cdots p_t^{?_t}}_{\text{(esta é a forma genérica de um divisor de } n)} = \qquad (*) \\ &= \big(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}\big) \cdots \big(1 + p_t + p_t^2 + \cdots + p_t^{\alpha_t}\big) \end{aligned}$$

[1] Veja as definições do livro VII dos Elementos de Euclides.

[2] Definição XXII, loc. cit.

A validade desta última igualdade pode ser vista do seguinte modo: as parcelas do último produto, quando expandido, correspondem exactamente a todas as maneiras possíveis de multiplicar uma das parcelas do 1º factor por uma das parcelas do 2º factor, ...etc...

Exemplo: $\sigma(60) = (1+2+2^2)\,(1+3)(1+5)$.

Lema 1.1.1 $1 + x + x^2 + \cdots + x^t = \dfrac{x^{t+1}-1}{x-1}$, *para todo o número* $x \neq 1$ *e para todo o inteiro positivo* t.

Verificação:

$$\begin{array}{rl} (x-1)\,(1+x+x^2+\cdots+x^t) = & \quad\; x + x^2 + \cdots + x^t + x^{t+1} \\ & -1 - x - x^2 - \cdots - x^t \\ \hline = -1+ & \qquad\qquad\qquad\quad +x^{t+1} \end{array} \qquad \square$$[3]

Resulta assim que: $\boxed{\sigma(n) = \dfrac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\dfrac{p_t^{\alpha_t+1}-1}{p_t-1}}$ $(**)$

Exemplo: $\sigma(60) = \dfrac{2^3-1}{2-1}\dfrac{3^2-1}{3-1}\dfrac{5^2-1}{5-1} = (2^3-1)(1+3)(1+5) = 7\cdot 4\cdot 6 = 168.$

Observação: De $(*)$ resulta facilmente que o número de divisores de n, normalmente denotado por $\nu(n)$, é igual a $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_t+1)$ (*porquê*?).

Da fórmula $(**)$ resulta a seguinte:

Proposição 1.1.2 *Se* a *e* b *são dois números sem factores comuns (= primos entre si), então* $\sigma(ab) = \sigma(a)\sigma(b)$.

Razão: Neste caso, os primos de a não se "misturam" com os de b no produto ab... (Tente perceber através de alguns exemplos. O que acontece se a e b tiverem factores comuns?).

[3] Este símbolo será usado para indicar o fim de uma demonstração ou de uma verificação.

Teorema 1.1.3 (Euclides, $\sim$ 300 A.C.) *Se m é tal que $2^m - 1$ é primo, então $2^{m-1}(2^m - 1)$ é um número perfeito.*

Demonstração: Como por hipótese o número $2^m - 1$ é primo, resulta que o número $2^{m-1}(2^m - 1)$ está já decomposto em primos. Pelo que acima se viu, tem-se então que: $\sigma(2^{m-1}(2^m - 1)) = \dfrac{2^m - 1}{2 - 1}(1 + (2^m - 1)) = (2^m - 1)2^m$. Fica assim verificado que a soma de todos os divisores de $2^{m-1}(2^m - 1)$ é duas vezes ele próprio. $\square$

Exemplo: $2^5 - 1 = 31$ é primo, logo $2^4\,(2^5 - 1) = 16 \cdot 31 = 496$ é perfeito.

(Observe-se que este resultado nada diz sobre o caso em que $2^m - 1$ é composto.)

Este resultado de Euclides levanta o problema de saber para que m's é que $2^m - 1$ é composto. Usando o lema 1.1.1 é fácil concluir que:

Proposição 1.1.4 *m composto $\Rightarrow 2^m - 1$ composto.*

Razão: $m = ab$, com $a > 1$ e $b > 1 \Rightarrow 2^m - 1 = (2^a)^b - 1 =$ (pelo lema 1.1.1) $= \underbrace{(2^a - 1)}_{>1}\underbrace{\left(1 + 2^a + (2^a)^2 + \cdots + (2^a)^{b-1}\right)}_{>1}$. $\square$

Por conseguinte, $2^m - 1$ só pode ser primo quando m o for.

<u>No entanto</u>: $2^{11} - 1 = 23 \cdot 89$, o que mostra que a implicação contrária na proposição anterior é falsa.

Os primos da forma $2^m - 1$ são denominados "*primos de Mersenne*", em homenagem a Marin Mersenne (1588-1648), que se interessou pelo seu estudo.

Cerca de 2000 anos após o resultado de Euclides, o matemático suiço Leonhard Euler (1707-1783) obteve o seguinte resultado:

Teorema 1.1.5 (Euler, in artigo póstumo de 1849) *O resultado de Euclides fornece todos os perfeitos pares. Isto é, se n é um número par que é perfeito, então $n = 2^{m-1}(2^m - 1)$, para algum m tal que $2^m - 1$ é primo.*

Demonstração: Seja n um número perfeito par. Escreva-se $n = 2^{t-1}a$ com a ímpar e, necessariamente, $t \geq 2$.

Tem-se: $2^t a = 2n =$ (por hipótese) $= \sigma(n) =$ (2^{t-1} e a não têm factores comuns) $= \sigma(2^{t-1})\,\sigma(a) = (2^t - 1)(a + x) =$ (onde x é a soma dos divisores de a que são $\neq$ de a) $= 2^t a - a + (2^t - 1)\,x \Rightarrow a = (2^t - 1)\,x \Rightarrow x \mid a$ e $x \neq a$ (pois $2^t - 1 > 1$). Mas, como $x = \sum_{d|a;d\neq a} d = \cdots + x + \cdots$, resulta que $x = 1$ e $a = 2^t - 1$ é primo. □

Este resultado levanta naturalmente a seguinte questão:

$\boxed{\textit{Quais os perfeitos ímpares?}}$

Esta é uma questão levantada há mais de 2500 anos e à qual ainda hoje não se sabe a resposta! Ou seja, não se conhece nenhum exemplo de um número perfeito ímpar, nem nunca ninguém consegui provar que tal exemplo não existe. É o problema matemático mais antigo que ainda continua em aberto!

Há, no entanto, algumas propriedades que se provou que um tal número, se existir, terá de satisfazer. Por exemplo, se n for um perfeito ímpar, então:

- n tem a forma $p^a m^2$, para algum p primo, sendo p e a da forma $4x + 1$ (i.e. dão resto 1 quando divididos por 4) [Euler, 17??];
- n tem pelo menos 8 factores primos distintos [P. Hagis, 1975];
- $n > 10^{300}$, i.e. n tem pelo menos 300 algarismos [R. P. Brent, G. L. Cohen, H. J. J. Riele, 1989].

Do que acima se viu, surge também a questão:

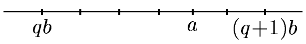
$\boxed{\textit{Para que primos } p \textit{ é } 2^p - 1 \textit{ primo?}}$

O estudo deste problema levou Pierre de Fermat (1601-1665) a uma importante descoberta de que falaremos adiante.

1.2 Alguns resultados básicos

Seja b um inteiro positivo.

Dado um inteiro arbitrário a, considere-se o múltiplo de b, menor ou igual a a, mais perto de a. Designe-se-o por qb.



(A que é igual b nesta figura?)

Então $qb \leq a < (q+1)b$ e $r = a - qb$ satisfaz $0 \leq r < b$.

Daqui resulta que:

Algoritmo de Divisão: *Dados dois inteiros a e b, com $b > 0$, existem inteiros q e r tais que:*

$$a = bq + r \text{ e } 0 \leq r < b.$$

Os inteiros q e r nessas condições são únicos e designam-se, respectivamente, por o quociente e o resto da divisão de a por b.

O máximo divisor comum de dois inteiros a e b é, como o nome o indica, o maior dos inteiros (positivos) que dividem simultaneamente a e b.
Notação: $(a, b) = \text{m.d.c.}(a, b)$.

Do livro VII dos Elementos de Euclides vem o famoso:

Algoritmo de Euclides: *Sejam a e b dois inteiros positivos. Usando o* *algoritmo da divisão, obtêm-se* $r_1, \ldots, r_n$ *satisfazendo:*

$$\begin{array}{lcll} a & = & b\,q_1 + r_1 & ,\ 0 < r_1 < b \\ b & = & r_1\,q_2 + r_2 & ,\ 0 < r_2 < r_1 \\ r_1 & = & r_2\,q_3 + r_3 & ,\ 0 < r_3 < r_2 \\ & \vdots & & \\ r_{n-2} & = & r_{n-1}\,q_n + r_n & ,\ 0 < r_n < r_{n-1} \\ r_{n-1} & = & r_n\,q_{n+1} & \end{array}$$

(i.e. r_n *é o primeiro* r_i *que divide* r_{i-1} *sem deixar resto.)*
Então $r_n = (a, b)$.

Demonstração: Em primeiro lugar, observe-se que a sequência $r_1, r_2, r_3, \ldots$ tem de "parar" pois $b > r_1 > r_2 > r_3 > \cdots \geq 0$, e que termina com zero.

Em seguida, procedendo da última das equações para a primeira, observe--se que: $r_n \mid r_{n-1} \Rightarrow r_n \mid r_{n-2} \Rightarrow \cdots \Rightarrow r_n \mid r_2 \Rightarrow r_n \mid r_1 \Rightarrow r_n \mid b \Rightarrow r_n \mid a$. Logo, r_n é um divisor comum de a e b.

Finalmente, e procedendo agora da primeira para a última das equações, note-se que, se c é um divisor comum de a e b, então: $c \mid a$ e $c \mid b \Rightarrow c \mid r_1 \Rightarrow c \mid r_2 \Rightarrow \cdots \Rightarrow c \mid r_n$. Ou seja, todo o divisor comum de a e b divide r_n. Em particular, r_n é o maior dos divisores comuns. $\square$

Corolário 1.2.1 *Todos os divisores comuns de* a *e* b *dividem* (a, b).
Isto é: $c \mid a,\ c \mid b \Rightarrow c \mid (a, b)$.

(Corolário é o mesmo que "consequência".)

Demonstração: Resulta da prova anterior. $\square$

Corolário 1.2.2 *O máximo divisor comum de dois números é a soma de um múltiplo de um dos números com um múltiplo do outro. Isto é,* $(a, b) =$

$ax+by$, para alguns inteiros x, y. Existe uma infinidade de pares de tal inteiros, um dos quais pode ser calculado a partir dos r_i's e dos q_i's.

Demonstração: Usando as notações da descrição do algoritmo de Euclides, tem-se:

$$\left.\begin{array}{r} r_n = r_{n-2} - r_{n-1}q_n \\ r_{n-1} = r_{n-3} - r_{n-2}q_{n-1} \end{array}\right\} \Rightarrow \left(\begin{array}{c} \text{eliminando} \\ r_{n-1} \text{ da } 1^{\underline{a}}, \\ \text{usando a } 2^{\underline{a}} \end{array}\right) \Rightarrow r_n = \boxed{?}\, r_{n-3} + \boxed{?}\, r_{n-2}.$$ Em seguida,

$$\left.\begin{array}{r} r_n = \boxed{?}\, r_{n-3} + \boxed{?}\, r_{n-2} \\ r_{n-2} = r_{n-4} - r_{n-3}q_{n-2} \end{array}\right\} \underset{\text{(analogamente)}}{\Longrightarrow} r_n = \boxed{?}\, r_{n-4} + \boxed{?}\, r_{n-3} \; ... \text{ etc.}$$

... até que se obtém $r_n = \boxed{?}\, a + \boxed{?}\, b$.

Finalmente, se x e y é um par de inteiros nas condições referidas, então também o são $x - bt$ e $y + at$, para todo o inteiro t (porquê?). $\square$

Exemplo: $a = 105, b = 22$ (Qual a diferença se tomar $a = 22, b = 105$?)

$$\begin{array}{rcll} 105 & = & 22 \cdot 4 + 17 & \\ 22 & = & 17 \cdot 1 + 5 & \\ 17 & = & 5 \cdot 3 + 2 & \\ 5 & = & 2 \cdot 2 + 1 & \rightsquigarrow \; 1 = 5 - 2 \cdot 2 = 5 - (17 - 3 \cdot 5) \cdot 2 = \\ 2 & = & 2 \cdot 1 & \qquad = 7 \cdot 5 - 2 \cdot 17 = 7 \cdot (22 - 17) - 2 \cdot 17 = \\ & & & \qquad = 7 \cdot 22 - 9 \cdot 17 = 7 \cdot 22 - 9 \cdot (105 - 4 \cdot 22) = \\ & & & \qquad = 43 \cdot 22 - 9 \cdot 105 \end{array}$$

Resulta que $x = -9, y = 43$ é uma solução de $1 = 105x + 22y$.

Um exemplo do uso do corolário anterior para dar demonstrações concisas e elegantes:

Proposição 1.2.3 *$(a, b) = 1$ e $a \mid bc \Rightarrow a \mid c$.*

Demonstração: $(a, b) = 1 \Rightarrow$ existem inteiros x, y tais que $1 = ax + by$. Resulta que $c = acx + bcy$. Agora, $a \mid bc \Rightarrow a \mid acx + bcy$, e portanto $a \mid c$. $\square$

O Triângulo de Pascal

Matemáticos chineses do século XI usavam já o triângulo que muito depois se veio a chamar “triângulo de Pascal”, para gerar os coeficientes binomiais:

$$
\begin{array}{lccccccccccccc}
(a+b)^0 = & & & & & & & 1 & & & & & & \\
 & & & & & & \overset{a}{\swarrow} & & \overset{b}{\searrow} & & & & & \\
(a+b)^1 = & & & & & a & & + & & b & & & & \\
 & & & & \overset{a}{\swarrow} & & \overset{b}{\searrow} & & \overset{a}{\swarrow} & & \overset{b}{\searrow} & & & \\
(a+b)^2 = & & & a^2 & & + & & 2ab & & + & & b^2 & & \\
 & & \overset{a}{\swarrow} & & \overset{b}{\searrow} & & \overset{a}{\swarrow} & & \overset{b}{\searrow} & & \overset{a}{\swarrow} & & \overset{b}{\searrow} & \\
(a+b)^3 = & a^3 & & + & & 3a^2b & & + & & 3ab^2 & & + & & b^3 \\
\vdots & & & \vdots & & & & \vdots & & & & \vdots & &
\end{array}
$$

ou, escrevendo apenas os coeficientes:

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

obtemos um “triângulo” de números onde cada elemento é a soma dos dois acima.

Este triângulo aparece com “profundidade” 6 em Yang Hui, em 1261, e com “profundidade” 8 em Chu Shih Chieh, em 1303 [4]. Yiang Hui atribui o triângulo a Chia Hsien (c. 1050)[5]. O triângulo parece também ter sido conhecido pelo matemático árabe Omar Khayyam (∼1050-1122)[6].

O triângulo de Pascal fornece um método rápido de cálculo dos coeficientes de $(a+b)^n$, usualmente denominados coeficientes binomiais. Tem no

[4]Stillwell, p. 135 e G. G. Joseph, p. 179.
[5]loc.cit.
[6]Boyer, p. 228.

entanto a desvantagem de ser preciso, caso queiramos calcular os coeficientes do desenvolvimento de $(a+b)^n$, de se ter de calcular todos os coeficientes de $(a+b)^k$ para todo o $k \leq n$. Há, porém, uma maneira de calcular directamente um dado coeficiente, que passamos a descrever.

Comecemos por observar que o coeficiente de $a^{n-i}b^i$ em $(a+b)^n$ é igual ao número de maneiras diferentes de ir buscar i b's de entre os n factores de $(a+b)^n$, uma vez que quando este produto é expandido obtemos todas as parcelas da forma $\boxed{?_1} \cdot \boxed{?_2} \cdots \boxed{?_n}$ onde $?_i \in \{a, b\}$. Mas:

$$\left\{ \begin{array}{c} \text{número de maneiras} \\ \text{diferentes de ir buscar} \\ i\ b\text{'s aos } n \text{ factores} \end{array} \right\} = \left\{ \begin{array}{c} \text{número de maneiras} \\ \text{diferentes de escolher } i \\ \text{sítios (para os } b\text{'s), de} \\ \text{entre } n \end{array} \right\} =$$

$$\left\{ \begin{array}{c} \text{número de maneiras} \\ \text{diferentes de escolher } i \\ \text{objectos de entre } n \\ \text{objectos distintos} \end{array} \right\}$$

Notação: $\binom{n}{i}$ = número de maneiras diferentes de escolher i objectos de entre n objectos distintos, e que se lê: "combinações de n, i a i".

Este número pode ser calculado usando o seguinte processo, composto de duas etapas: em primeiro lugar, imaginemos que temos i "caixas" onde iremos colocar i objectos escolhidos de entre os n existentes. Na primeira caixa podemos colocar um qualquer dos n objectos. *Para cada uma* dessas n possíveis escolhas, ficamos com $n-1$ objectos para colocar na segunda caixa. Temos assim $n(n-1)$ maneiras de preencher as duas primeiras caixas. *Para cada uma* dessas escolhas, ficamos com $n-2$ objectos para colocar na terceira caixa, etc...

$$\begin{array}{cccc} \multicolumn{4}{c}{\overbrace{\hspace{4cm}}^{i}} \\ \boxed{} & \boxed{} & \cdots & \boxed{} \\ \uparrow & \uparrow & \cdots & \uparrow \\ \text{n} & \text{n-1} & \cdots & \text{n-(i-1)} \end{array}$$

Temos pois $n(n-1)\cdots(n-(i-1))$ maneiras de colocar i dos n objectos nas caixas. Em segundo lugar, colocamos os i objectos seleccionados todos juntos numa só caixa:

$$\boxed{\text{E}}\quad \boxed{\text{X}}\quad \boxed{\text{M}}\quad \boxed{\text{P}}\quad \boxed{\text{L}}\quad \boxed{\text{O}} \rightsquigarrow \boxed{\begin{array}{cc} \text{X} & \text{E} \\ \text{M} & \text{P} \\ \text{O} & \text{L} \end{array}}$$

Falta agora saber quantos arranjos de um dado subconjunto fixo de i elementos nas i caixas resultam numa mesma combinação na "caixa final". Mas isto corresponde a calcular de quantas maneiras se podem distribuir i objectos distintos por i caixas, o que é um caso particular do que foi feito no primeiro passo deste raciocínio. Esse número é, por conseguinte, igual a $i(i-1)(i-2)\cdots 2\cdot 1$.

Concluimos assim que as $n(n-1)\cdots(n-(i-1))$ maneiras de escolher i objectos, de entre n, para as i caixas, se dividem em grupos com $i(i-1)(i-2)\cdots 2\cdot 1$ elementos cada, correspondendo a uma mesma selecção de i objectos. Resulta que:

$$\binom{n}{i} = \frac{n(n-1)\cdots(n-(i-1))}{i(i-1)(i-2)\cdots 2\cdot 1}$$

Exemplo: Sejam $n = 4, i = 2$ e sejam A, B, C, D os 4 objectos. Procedendo como na explicação dada atrás, obteriamos:

$$\left.\begin{array}{c}\boxed{\text{A}}\boxed{\text{B}}\\[1ex] \boxed{\text{B}}\boxed{\text{A}}\end{array}\right\} \rightsquigarrow \boxed{\begin{array}{c}A\\B\end{array}} \qquad \left.\begin{array}{c}\boxed{\text{A}}\boxed{\text{C}}\\[1ex] \boxed{\text{C}}\boxed{\text{A}}\end{array}\right\} \rightsquigarrow \boxed{\begin{array}{c}A\\C\end{array}} \qquad \left.\begin{array}{c}\boxed{\text{A}}\boxed{\text{D}}\\[1ex] \boxed{\text{D}}\boxed{\text{A}}\end{array}\right\} \rightsquigarrow \boxed{\begin{array}{c}A\\D\end{array}}$$

$$\left.\begin{array}{c}\boxed{\text{B}}\boxed{\text{C}}\\[1ex] \boxed{\text{C}}\boxed{\text{B}}\end{array}\right\} \rightsquigarrow \boxed{\begin{array}{c}B\\C\end{array}} \qquad \left.\begin{array}{c}\boxed{\text{B}}\boxed{\text{D}}\\[1ex] \boxed{\text{D}}\boxed{\text{B}}\end{array}\right\} \rightsquigarrow \boxed{\begin{array}{c}B\\D\end{array}} \qquad \left.\begin{array}{c}\boxed{\text{C}}\boxed{\text{D}}\\[1ex] \boxed{\text{D}}\boxed{\text{C}}\end{array}\right\} \rightsquigarrow \boxed{\begin{array}{c}C\\D\end{array}}$$

Notação: $n! =$ (lê-se "n factorial") produto de todos os inteiros positivos de 1 a n. (Convenciona-se que $0! = 1$).

Usando esta notação, tem-se: $\binom{n}{i} = \dfrac{n!}{(n-i)!i!}$.

Esta fórmula para o número de combinaçõesde n objectos i a i aparece num texto de 1321 do matemático hebraico Levi ben Gershon[7]. Blaise Pascal (1623-1662) provou que este número é também o coeficiente binómial do monómio $a^{n-i}b^i$.

De tudo isto se conclui:

Expansão Binomial:

$$\boxed{(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i}b^i, \text{ onde } \binom{n}{i} = \frac{n!}{(n-i)!i!}}$$

De um modo mais geral tem-se:

Expansão Multinomial:

$$\boxed{(a_1 + a_2 + \cdots + a_k)^n = \sum_{i_1+i_2+\cdots+i_k=n} \frac{n!}{i_1!i_2!\cdots i_k!} a_1^{i_1}a_2^{i_2}\cdots a_k^{i_k}}$$

Demonstração: O coeficiente de $a_1^{i_1}a_2^{i_2}\cdots a_k^{i_k}$ pode ser calculado do seguinte modo: há $\binom{n}{i_1}$ maneiras diferentes de escolher os i_1 sítios, de entre os n possíveis, de onde provêm os a_1's; *para cada uma* dessas maneiras, há $\binom{n-i_1}{i_2}$ diferentes escolhas de i_2 sítios, de entre os restantes $n-i_1$, de onde escolher os a_2's; *para cada uma* destas, há agora $\binom{n-i_1-i_2}{i_3}$ escolhas para

[7] Stillwell, p. 136.

os a_3's; etc...

Resulta assim que o coeficiente procurado é igual a:

$$\binom{n}{i_1}\binom{n-i_1}{i_2}\binom{n-i_1-i_2}{i_3}\cdots\binom{n-i_1-i_2-\cdots-i_{k-2}}{i_{k-1}}\binom{n-i_1-i_2-\cdots-i_{k-1}}{i_k}=\frac{n!}{(n-i_1)!i_1!}\cdot$$

$$\cdot\frac{(n-i_1)!}{(n-i_1-i_2)!i_2!}\frac{(n-i_1-i_2)!}{(n-i_1-i_2-i_3)!i_3!}\cdots\frac{(n-i_1-\cdots-i_{k-2})!}{(n-i_1-\cdots-i_{k-2}-i_{k-1})!i_{k-1}!}\frac{(n-i_1-\cdots-i_{k-1})!}{(n-i_1-\cdots-i_{k-1}-i_k)!i_k!}=$$

$$=\frac{n!}{i_1!i_2!\cdots i_k!}$$ □

1.3 Números Primos.

Os números primos (= sem factores próprios): 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, etc..., são uma espécie de "átomos" a partir dos quais todos os números são multiplicativamente construídos. Um considerável esforço tem sido dispendido por diversos matemáticos, desde tempos imemoriais, no estudo desses números. Um dos primeiros resultados ficou eternizado como a Proposição XX do livro IX dos Elementos de Euclides:

Teorema 1.3.1 *Existe uma infinidade de números primos.*

Demonstração: Dada qualquer família $p_1, p_2, \ldots, p_t$ de números primos, o número $p_1p_2\cdots p_t+1$, não sendo divisível por nenhum dos primos dessa família, tem necessariamente um factor primo diferente de $p_1, p_2, \ldots, p_t$. Fica assim mostrado que existe um primo que não pertence à família dada. □

Alternativamente: O número $n!+1$ tem um factor primo, como todos os números, que é necessariamente maior que n. □

Mas como determinar se um número é ou não primo? Em príncipio é necessário, de um forma ou outra, verificar que não tem nenhum divisor próprio. Há maneiras muito eficientes de indirectamente fazer essa verificação[8], limitamo-nos aqui a fazer a seguinte observação muito simples:

Proposição 1.3.2 *Todo o número composto n admite um divisor primo menor ou igual a $\sqrt{n}$.*

Razão: Seja $n = a \cdot b$, com $a > 1, b > 1$. Como não se pode ter simultaneamente $a > \sqrt{n}$ e $b > \sqrt{n}$ (pois tal implicaria $ab > n$), terá de ser $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$. Se, por exemplo, $a \leq \sqrt{n}$, então um factor primo de a satisfaz a condição requerida. □

Alternativamente: Seja p o menor número primo que divide n. Então $n = a \cdot p$ para algum $a > 1$. Necessariamente $a \geq p$ e portanto $p^2 \leq p \cdot a = n$, o que mostra que $p \leq \sqrt{n}$. □

Daqui resulta imediatamente:

Se um número n não for divisível por nenhum primo $\leq \sqrt{n}$, então ele é primo.

Uma pequena amostra do que se sabe e do que se desconhece sobre os números primos:

Sabe-se que:

- $\displaystyle\sum_{p \text{ primo}} \frac{1}{p}$ diverge (Euler, 17??).
- Se $(a, b) = 1$, então a progressão aritmética $a, a + b, a + 2b, a + 3b, \ldots$ contém uma infinidade de primos (Dirichlet, 1837).

[8]Recentemente (8/2002) houve um espectacular avanço nesta área: três matemáticos indianos, M. Agrawal, N. Kayal e N. Saxena, descobriram um algoritmo em tempo polinomial para decidir se um número é ou não primo, resolvendo assim um importantíssimo problema em Teoria da Complexidade intensivamente estudado nas últimas décadas.

Nota: $a = b = 1$ é o resultado de Euclides.

Exercício: Mostre a validade deste resultado para $a = 3, b = 4$; $a = 5, b = 6$ e tente o caso $a = 1, b = 4$.

- Designe-se por $\pi(x)$ o número de primos $\leq x$, onde x é um número real positivo. Gauss conjecturou em 1793, quando tinha 15 anos, que $\pi(x)$ é assimptoticamente igual a $\displaystyle\int_2^x \frac{dt}{\log t}$, baseado em evidência numérica (isto de acordo com uma carta que ele escreveu 50 anos mais tarde...). Mostra-se que isto é equivalente a $\displaystyle\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1$. Este resultado, conhecido como o "Teorema dos Números Primos" foi provado por Hadamard e, independentemente, por de la Vallée Poussin, em 1896.

Gostar-se-ia de saber se:

- Existe uma infinidade de primos da forma $n^2 + 1$?

- Existe uma infinidade de primos de Mersenne (i.e. da forma $2^p - 1$)?

  Nota[9]: O maior primo de Mersenne conhecido em Setembro de 2002 era $2^{13466917} - 1$, um número com 4 053 946 algarismos!

- Existe mais algum primo de Fermat, $F_n = 2^{2^n} + 1$, com $n > 4$?

  Nota[10]: Em 2002 sabia-se que F_n é composto para $5 \leq n \leq 32$ e eram conhecidos mais 206 números desta forma que são compostos, o maior dos quais sendo F_{382449}, um verdadeiro gigante com mais do que 10^{115128} algarismos!

- Existe uma infinidade de pares de primos gémeos?

  Nota: $p, p+2$ dizem-se "primos gémeos" se ambos forem números primos. Exemplos:

[9]Este é mais um feito do grupo GIMPS, the *Great Internet Mersenne Prime Search*. A glória da descoberta do primo mencionado, feita em 12/7/2001 coube ao canadiano Michael Cameron, na altura com 20 anos. Ver, na internet, *The Prime Pages* de Chris Caldwell.

[10]Para mais detalhes, consultar: http://www.prothsearch.net/fermat.html#Summary

3, 5; 11, 13; 59, 61. Sabe-se que $\displaystyle\sum_{p,p+2 \text{ gémeos}} \frac{1}{p}$ é convergente! (Brun, 1919).

1.4 O "pequeno" teorema de Fermat e o teorema de Euler.

O resultado de Euclides sobre os números perfeitos conduz naturalmente à questão de determinar quando é que $2^p - 1$ é primo, o que por sua vez leva a considerar o problema de saber quando é que um primo q divide um número da forma $2^p - 1$ (p primo).

Suponha-se que se quer determinar se $2^{13} - 1$ é primo e, em particular, se quer saber se este número é divisível por 7. Isto pode ser rapidamente averiguado do seguinte modo:

Potências de 2	1	2	2^2	2^3	2^4	2^5	2^6	2^7	$\cdots$	2^{12}	2^{13}
Resto da divisão por 7	1	2	4	1	2	4	1	$\cdots$	$\cdots$	$\cdots$	2

Observação: Como $2^a = 7q + r \Rightarrow 2^{a+1} = 7(2q) + 2r$, conclui-se que, para achar o resto da divisão de 2^{a+1} por 7, basta achar o resto da divisão de $2r$ por 7 (sendo r conhecido): $2r = 7q' + r' \Rightarrow 2^{a+1} = 7(2q + q') + r'$.
Vê-se assim que $2^{13} - 1$ dá resto $2 - 1 = 1$ quando dividido por 7(!).

Antes de prosseguirmos, é conveniente introduzir uma noção e uma notação, introduzidas por K. F. Gauss (1777-1855) na sua monumental obra "Disquisitiones Arithmeticae", de 1801, e cuja utilidade é difícil sobrevalorizar.

Definição 1.4.1 *Dois inteiros a e b dizem-se* **congruentes modulo** m *se deixam o mesmo resto quando divididos por m.*

Notação: $a \equiv b \pmod{m}$ significa "a congruente com b modulo m"[11].
Exemplos: $23 \equiv 9 \pmod 7$, já que tanto 23 como 9 deixam resto 2 quando divididos por 7; $5 \equiv -11 \pmod 8$, uma vez que $-11 = 8 \cdot (-2) + 5$.

[11] "Congruentes" deriva do latim e significa "concordantes", "correspondentes"; "modulo" significa "pequena medida".

Proposição 1.4.2 *$a \equiv b \pmod{m} \Leftrightarrow m \mid a-b \Leftrightarrow a = b+tm$, para algum inteiro t.*

Demonstração: $a \equiv b \pmod{m}$ significa que $a = mq_1 + r$ e $b = mq_2 + r$ (para alguns q_1, q_2, r). Mas então, $a - b = m(q_1 - q_2)$. Isto mostra a primeira "$\Rightarrow$". De facto, podemos mostrar a primeira "$\Leftrightarrow$" duma só vez, observando que se $a = mq_1 + r_1$ e $b = mq_2 + r_2$, com $0 \leq r_1, r_2 < m$, então $a - b = m(q_1 - q_2) + r_1 - r_2$, e como $0 \leq r_1 - r_2 < m$, vê-se imediatamente que $m \mid a - b \Leftrightarrow r_1 = r_2$, i.e. $a \equiv b \pmod{m}$.

A segunda "$\Leftrightarrow$" é fácil e a sua prova é deixada como exercício. □

Exemplos: Nos dois exemplos dados acima tem-se: $7 \mid 23 - 9$ e $8 \mid 5 - (-11)$. Também: $23 = 9 + 2 \cdot 7$ e $5 = -11 + 2 \cdot 8$.

Propriedades da relação de congruência:

(i) $a \equiv a \pmod{m}$;

(ii) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$;

(iii) $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$;

(iv) $\left.\begin{array}{r} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array}\right\} \Rightarrow \left\{\begin{array}{c} a + c \equiv b + d \pmod{m} \\ ac \equiv bd \pmod{m} \end{array}\right.$;

(As propriedades (i), (ii) e (iii), conhecidas por *reflexividade*, *simetria* e *transitividade*, respectivamente mostram que "$\equiv$" é uma "relação de equivalência".)

Demonstração: (da 2ª parte de (iv)) $\left.\begin{array}{r} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array}\right\} \Rightarrow \left\{\begin{array}{l} a = b + tm \\ c = d + sm \end{array}\right.$, para alguns inteiros $t, s \Rightarrow ac = bd + bsm + dtm + tsm^2 = bd + (bs + dt + tsm)m \Rightarrow ac \equiv bd \pmod{m}$.

As outras são fáceis e são deixadas como exercício. □

Exemplo: O resultado anterior justifica os seguintes cálculos, que mostram como verificar que $23 \mid 2^{11}-1$ sem muitas contas: $2^5 = 32 \equiv 9 \pmod{23} \Rightarrow 2^{10} = (2^5)^2 \equiv 9^2 = 81 \equiv 12 \pmod{23} \Rightarrow 2^{11} = 2 \cdot 2^{10} \equiv 2 \cdot 12 = 24 \equiv 1 \pmod{23} \Rightarrow 23 \mid 2^{11}-1$.
Alternativamente: $2^4 = 16 \equiv -7 \pmod{23} \Rightarrow 2^8 = (2^4)^2 \equiv (-7)^2 = 49 \equiv 3 \pmod{23} \Rightarrow 2^{11} = 2^3 \cdot 2^8 \equiv 8 \cdot 3 = 24 \equiv 1 \pmod{23} \Rightarrow 23 \mid 2^{11}-1$.

Regressando agora ao nosso problema de estudar quando é que um primo q divide $2^p - 1$, depois de construir várias tabelas como a da página 14 poderiamos resumir a informação obtida na seguinte tabela:

Primo p	3	5	7	11	13	17	19	23	29	31	37	...
Primeiro expoente $d \geq 1$ tal que $2^d \equiv 1 \pmod{p}$	2	4	$3^{(*)}$	10	12	8	18	11	28	5	36	...

[(*) resulta da tabela da página 14.]

Nota algum padrão?

Numa carta dirigida a Frénicle de Bessey, datada de 18 de Outubro de 1640, P. Fermat escreve o seguinte[12]:

Parece-me que depois disto lhe devo dizer qual a fundação na qual assento todas as demonstrações que dizem respeito a progressões geométricas, nomeadamente:

Todo o número primo mede [divide] *infalivelmente uma das potências menos a unidade em qualquer progressão, e o expoente dessa potência é um divisor do dado número primo menos um; e depois de encontrada a primeira potência que satisfaz esta condição, todos aqueles cujos expoentes são múltiplos do primeiro satisfazem essa mesma condição.*

[12] ver O. Ore, *Number Theory and Its History.*

Vamos ver que assim é, começando com:

Teorema 1.4.3 ("Pequeno" teorema de Fermat): *Se p é um número primo e a um inteiro não divisível por p, então:*

$$a^{p-1} \equiv 1 \pmod{p}$$

(equivalentemente: $a^p \equiv a \pmod{p}$, para todo o inteiro a.)

1ª Demonstração: (Os argumentos usados nesta prova são muito possivelmente próximos das divagações originais que levaram à descoberta deste resultado[13].)

1ª etapa: $a^t \equiv 1 \pmod{p}$, para algum $t > 0$.

Razão: Como $p \nmid a$, os restos módulo p dos p números $1, a, a^2, \ldots, a^{p-1}$ estão entre os $p-1$ números $1, 2, \ldots, p-1$. Pelo "princípio das meias e das gavetas"[14], há dois desses números com o mesmo resto. Ou seja, existem i, j com $0 \leq j < i \leq p-1$ tais que $a^i \equiv a^j \pmod{p}$. Tem-se então que $i - j > 0$ e $p \mid a^i - a^j = a^j\,(a^{i-j} - 1)$. Como $(p, a^j) = 1$, resulta da Proposição 1.2.3. que $a^{i-j} \equiv 1 \pmod{p}$. $\square$

Como este último cálculo (de "$a^i \equiv a^j \pmod{p}$" a "$a^{i-j} \equiv 1 \pmod{p}$") reaparece em diversas situações, aproveitamos a oportunidade para dar a sua formulação mais geral, que nos será útil por várias vezes:

Lema 1.4.4 *Se $(a, n) = 1$ e $ax \equiv ay \pmod{n}$, então $x \equiv y \pmod{n}$.*

Demonstração: $ax \equiv ay \pmod{n} \Rightarrow n \mid ax - ay = a(x-y) \Rightarrow$ (usando Prop. 1.2.3., uma vez que $(a, n) = 1$) $n \mid x - y \Leftrightarrow x \equiv y \pmod{n}$. $\square$

Seja agora d o menor dos inteiros $t \geq 1$ tal que $a^t \equiv 1 \pmod{p}$.

---

[13] cf. Edwards.

[14] Se tivermos $m > n$ meias e as colocarmos em n gavetas, haverá necessariamente uma gaveta com pelo menos duas meias!

<u>*2ª etapa*: $d \mid p-1$</u>

Razão: Considerem-se os números $1, a, a^2, \ldots, a^{d-1}$. Estes números dão restos distintos quando divididos por p, pois que se dois tivessem o mesmo resto, então pelo raciocínio feito acima obter-se-ia um expoente $1 \leq t < d$ tal que $a^t \equiv 1 \pmod p$, o que não pode ser pois d é o menor destes.

Se agora todos os restos $1, 2, 3, \ldots, p-1$ aparecerem como restos de $1, a, a^2, \ldots, a^{d-1}$, então $d = p-1$ e a prova acaba aqui. Senão, seja b um inteiro não divisível por p, que dê um resto, módulo p, distinto dos de $1, a, a^2, \ldots, a^{d-1}$. Então os restos de $b, ba, ba^2, \ldots, ba^{d-1}$ são distintos entre si e distintos dos de $1, a, a^2, \ldots, a^{d-1}$, pois:

$$ba^i \equiv ba^j \pmod p \underset{(\text{lema } 1.2.3.;(\text{b},\text{p})=1)}{\Longrightarrow} a^i \equiv a^j \pmod p,$$

e:

$$ba^i \equiv a^j \pmod p \underset{(\text{lema } 1.2.3.;(\text{a}^{\text{i}},\text{p})=1)}{\Longrightarrow} b \equiv a^{j-i} \pmod p.$$

[Observe que esta última congruência não faz sentido caso $j < i$. Uma maneira de resolver este problema é notar que podemos substituir j por $j+$(*um múltiplo de d*) (porquê?), e portanto fazer com que j seja maior do que i.]

Se ainda não esgotamos todos os restos $1, 2, \cdots, p-1$, seja c não divisível por p um número cujo resto é distinto dos de $1, a, a^2, \ldots, a^{d-1}$ e dos de $1, ba, ba^2, \ldots, ba^{d-1}$... etc...

Obtem-se assim:

$$\left.\begin{array}{cccc} \boxed{\begin{array}{c}1\\a\\a^2\\\vdots\\a^{d-1}\end{array}} & \boxed{\begin{array}{c}b\\ba\\ba^2\\\vdots\\ba^{d-1}\end{array}} & \boxed{\begin{array}{c}c\\ca\\ca^2\\\vdots\\ca^{d-1}\end{array}} & \begin{array}{c}\cdots\\\cdots\\\cdots\\\vdots\\\cdots\end{array}\\ d\ \text{n}^{\underline{\text{os}}} & d\ \text{n}^{\underline{\text{os}}} & d\ \text{n}^{\underline{\text{os}}} & \end{array}\right\}$$

aqui vão estar representados, ao fim de um número finito de escolhas, todos os restos $1, 2, 3, \cdots, p-1$, uma e uma só vez (*porquê?*).
<u>*Exercício*</u>: Construa explicitamente um quadro como este para $a = 2, p = 31$.

Os números $1, 2, 3, \cdots, p-1$ ficam assim divididos em grupos de d, o que mostra que $d \mid p-1$. $\square$

3ª e última etapa:

Seja então $p-1 = ds$. Tem-se $a^{p-1} = \left(a^d\right)^s \equiv 1^s \equiv 1 \pmod{p}$. $\square$

2ª Demonstração: Os números $a, 2a, 3a, \cdots, (p-1)a$ têm restos distintos módulo p, pois $p \nmid ia - ja = (i-j)a$ para $0 \leq j < i \leq p-1$, uma vez que p é primo e por hipótese não divide a, enquanto que $i - j < p$. Mas então os restos dos números $a, 2a, 3a, \cdots, (p-1)a$ são necessariamente os números $1, 2, 3, \cdots, p-1$ (numa outra ordem, possivelmente...). Donde resulta que:

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1) \equiv a \cdot 2a \cdot 3a \cdots (p-1)a = (p-1)!\, a^{p-1} \pmod{p}.$$

Como p é primo, tem-se que $(p, (p-1)!) = 1$ e, usando o lema 1.4.4., resulta que $1 \equiv a^{p-1} \pmod{p}$. $\square$

3ª Demonstração: Vamos mostrar por indução que $a^p \equiv a \pmod{p}$, para todo o natural a.

É claro que $1^p \equiv 1 \pmod{p}$.

Agora: suponhamos que, para um determinado número natural (fixo) a, é verdade que $a^p \equiv a \pmod{p}$. Então:

$$(a+1)^p = a^p + \underbrace{\binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-2} a^2 + \binom{p}{p-1} a}_{\equiv 0 \pmod{p}} + 1 \equiv$$

$\equiv a+1 \pmod{p}$, uma vez que $p \mid \dfrac{p!}{(p-i)!\, i!}$ para todo $0 < i < p$, pois nestes casos p não figura no denominador. $\square$

4ª Demonstração:

$$a^p = (\underbrace{1+1+\cdots+1}_{a})^p = \sum_{i_1+i_2+\cdots+i_a=p} \frac{p!}{i_1!\, i_2!\, \cdots i_a!} 1^{i_1} \cdot 1^{i_2} \cdots 1^{i_a} \equiv$$

$\equiv \underbrace{1^p + 1^p + \cdots + 1^p}_{a} = a \pmod p$, pois $p \mid \dfrac{p!}{i_1!\, i_2!\, \cdots i_a!}$, excepto quando um dos i_j's é igual a p e todos os outros são, necessariamente, iguais a 0. $\square$

Tem-se ainda o seguinte resultado:

Proposição 1.4.5 *Seja p primo e a não divisível por p. Se d é o menor expoente positivo tal que $a^d \equiv 1 \pmod p$, e se $a^t \equiv 1 \pmod p$, então $d \mid t$.*

Demonstração: Divida-se t por d: $t = dq + r$. Então $1 \equiv a^t \equiv \left(a^d\right)^q \cdot a^r \equiv$ $\equiv a^r \pmod p$. Mas $0 \leq r < d$. Pela minimalidade de d, resulta que r é necessariamente igual a 0, ou seja, $d \mid t$. $\square$

Destes resultados podemos retirar informações importantes sobre os divisores primos dos números de Mersenne e dos de Fermat, como veremos de seguida.

Corolário 1.4.6 *Seja $p \neq 2$ um primo. Os factores primos de $2^p - 1$ são da forma $2kp + 1, k \in \mathbb{N}$.*

Demonstração: Seja q um primo que divide $2^p - 1$. Então $2^p \equiv 1 \pmod q$. Como p é primo, resulta de proposição anterior que p é necessariamente o menor expoente d tal que $2^d \equiv 1 \pmod q$ (já que $d \mid p \Rightarrow d = 1$ ou $d = p$, e $d \neq 1$ pois $2 \not\equiv 1 \pmod q$). Por outro lado, $2^{q-1} \equiv 1 \pmod q$, pelo teorema de Fermat (porque é que $q \neq 2$?). Usando novamente o resultado anterior, conclui-se que $p \mid q - 1$. Logo, $q = pt + 1$ para algum inteiro t. Finalmente p, q ímpares $\Rightarrow t$ par. Donde, $t = 2k$ para algum k e portanto $q = 2kp + 1$. $\square$

Exemplos:

- Os factores primos de $2^{11}-1$ estão entre os números primos da forma $22k+1 (k=1,2,\ldots)$. O factor 23 (ver pp. 4 e 17) corresponde a $k=1$.
- Os factores primos de $2^{13}-1$ são da forma $26k+1 (k=1,2,\ldots)$. Os únicos primos desta forma $\leq \sqrt{2^{13}-1} < 2^6\sqrt{2} < 64 \cdot 1,5 = 96$ são: 53 e 79. Resulta que se $2^{13}-1$ não fôr divisível por 53 nem por 79 (o que de facto é verdade - verifique-o!), então é primo.

Corolário 1.4.7 *Os factores primos de* $2^{2^n}+1$ ($n \geq 0$) *são da forma* $2^{n+1}k+1$ *para algum* $k \in \mathbb{N}$.

Demonstração: Seja p um primo tal que $p \mid 2^{2^n}+1$, ou, equivalentemente, $2^{2^n} \equiv -1 \pmod{p}$. Então $2^{2^{n+1}} \equiv \left(2^{2^n}\right)^2 \equiv (-1)^2 \equiv 1 \pmod{p}$. Se designarmos por d o menor inteiro positivo tal que $2^d \equiv 1 \pmod{p}$, como acima, resulta então da proposição anterior que $d \mid 2^{n+1}$. Mas então $d = 2^t$ para algum $0 \leq t \leq n+1$. Mas se t fosse $\leq n$, então ter-se-ia que $d \mid 2^n$, e portanto $-1 \equiv 2^{2^n} \equiv 1 \pmod{p}$. Isto implicaria $p=2$, o que é falso (*porquê* ?). Resulta assim que $t = n+1$, ou seja, $d = 2^{n+1}$. Pelo teorema de Fermat, sabe-se que $2^{p-1} \equiv 1 \pmod{p}$, resultando da proposição anterior que $2^{n+1} \mid p-1$, isto é: $p = 2^{n+1}k+1$ para algum k. □

Exemplos:

- Os factores primos de $F_3 = 2^{2^3}+1 = 257$ são da forma $2^4k+1 = 16k+1 (k=1,2,3,\cdots)$. Mas $\sqrt{2^8+1} < 2^4+1 = 17$ (porquê ?). Resulta que 257 é primo sem ser necessário efectuar qualquer divisão !!!
- Os factores primos de $F_4 = 2^{2^4}+1 = 65.537$ são da forma $32k+1 (k = 1,2,3,\cdots)$. Os únicos primos desta forma $\leq \sqrt{2^{16}+1} < 2^8+1 = 257$ (porquê ?) são: 97 e 193.

97 não divide F_4:

$2^6 \equiv 64 \equiv -33 \pmod{97} \Rightarrow 2^6 + 2^5 \equiv -1 \pmod{97} \Rightarrow 3 \cdot 2^5 \equiv -1 \pmod{97} \Rightarrow 9 \cdot 2^{10} \equiv 1 \pmod{97} \Rightarrow 9 \cdot 2^{16} \equiv 2^6 \equiv 64 \pmod{97}$. Agora, se $2^{16} \equiv -1 \pmod{97}$, então $-9 \equiv 64 \pmod{97}$, o que é falso. Donde $2^{16} \not\equiv -1 \pmod{97}$

193 não divide F_4:

$2^8 \equiv 256 \equiv 63 \pmod{193} \Rightarrow 2^8 - 2^6 \equiv -1 \pmod{193} \Rightarrow 3 \cdot 2^6 \equiv -1 \pmod{193} \Rightarrow 9 \cdot 2^{12} \equiv 1 \pmod{193} \Rightarrow 9 \cdot 2^{16} \equiv 2^4 \equiv 16 \pmod{193}$. Agora, se $2^{16} \equiv -1 \pmod{193}$, então $-9 \equiv 16 \pmod{193}$, o que é falso. Portanto, $2^{16} \not\equiv -1 \pmod{193}$.

Conclui-se que $F_4 = 2^{16} + 1$ é primo !

- Os factores primos de $F_5 = 2^{2^5} + 1 = 4.294.967.297$ são da forma $64k + 1 (k = 1, 2, 3, \cdots)$. $k = 10$ fornece o factor primo, 641, descoberto por Euler, mostrando assim que é falsa a conjectura de Fermat de que $2^{2^n} + 1$ é primo para todo $n \geq 0$.

A generalização de Euler

Seja n um inteiro positivo. Claro que se $(a, n) > 1$, então não existe nenhum inteiro d tal que $a^d \equiv 1 \pmod{n}$ (*porquê*?). Mas e se $(a, n) = 1$? Vamos ver que que neste caso existem tais expoentes, à semelhança do que acontece módulo números primos.

Sejam $m_1, m_2, \cdots, m_k$ *todos* os números de 1 a n que são primos com n (*exemplo*: para $n = 9$ esses números s ão: 1, 2, 4, 5, 7 e 8). Agora, se a é tal que $(a, n) = 1$, então os números $a \cdot m_1, a \cdot m_2, \cdots, a \cdot m_k$ são primos com n (*porquê*?) e portanto também o são os seus restos (já que: se $(b, n) = 1$ e $b = nq + r$, então $(n, r) = 1$. (*porquê*?)). Mas, $am_i \not\equiv am_j \pmod{n}$ para $i \neq j$, pois $am_i \equiv am_j \pmod{n} \Rightarrow m_i \equiv m_j \pmod{n} \Rightarrow i = j$. Resulta que os números $am_1, am_2, \cdots, am_k$ deixam restos $m_1, m_2, \cdots, m_k$ (em geral numa outra ordem) módulo n, isto é:

$$\{\text{restos de } am_1, am_2, \cdots, am_k\} = \{m_1, m_2, \cdots, m_k\}.$$

(*exemplo*: para $n = 9, a = 4$ tem-se que os restos, módulo 9, dos números $4 \cdot 1, 4 \cdot 2, 4 \cdot 4, 4 \cdot 5, 4 \cdot 7, 4 \cdot 8$ são: 4, 8, 7, 2, 1, 5, respectivamente).

Então: $m_1 m_2 \cdots m_k \equiv am_1 am_2 \cdots am_k \equiv a^k m_1 m_2 \cdots m_k \pmod{n}$. Como $(m_1 m_2 \cdots m_k, n) = 1$ (*porquê?*), pode-se aplicar o lema 1.4.4. para concluir que: $a^k \equiv 1 \pmod{n}$

Vê-se assim que k é um dos expoentes procurados, e justifica-se que se lhe dê um nome:

Notação: $\varphi(n)$ = número de inteiros positivos menores ou iguais a n que são primos com n. A φ chama-se *o indicador de Euler.*

Observação: $\varphi(1) = 1$.

De tudo o que acima se viu, resulta:

Teorema 1.4.8 (Euler): *Se n é um número inteiro positivo e $a \in \mathbb{Z}$ é tal que $(a, n) = 1$, então $a^{\varphi(n)} \equiv 1 \pmod{n}$.* $\square$

Observe-se que no caso particular em que n é um número primo, então $\varphi(n) = n - 1$ (*porquê?*). O teorema de Euler contém assim o resultado de Fermat como um caso particular.

Surge agora o seguinte problema: como calcular $\varphi(n)$ rapidamente?

Se, por exemplo, quisermos calcular $\varphi(10.000)$, seria impracticável enumerar todos os números de 1 a 10.000 que são primos com 10.000. Pode-se, alternativamente, começar por observar que $10.000 = 10^4 = 2^4 \cdot 5^4$, e que por conseguinte um número é primo com 10.000 *se e só se* não fôr múltiplo nem de 2, nem de 5. Donde:

$\varphi(10.000) = 10.000 - \#\{$múltiplos de 2, entre 1 e 10.000$\} - \#\{$múltiplos de 5, entre 1 e 10.000$\} + \#\{$múltiplos de 10, entre 1 e 10.000$\}$[15] $= 10.000 - \dfrac{10.000}{2} - \dfrac{10.000}{5} + \dfrac{10.000}{10} = 4.000$

[*Notação*: $\# =$ "cardinal de".]

Em geral, seja $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ a factorização de n em números primos. Tem-se:

$$\begin{aligned}
\varphi(n) &= n - \#\{\text{múltiplos de } p_1,\ \text{de 1 a } n\} - \cdots - \#\{\text{múltiplos de } p_t,\ \text{de 1 a } n\} + \\
&+ \#\{\text{múltiplos de } p_1p_2,\ \text{de 1 a } n\} + \cdots + \#\{\text{múltiplos de } p_{t-1}p_t,\ \text{de 1 a } n\} - \\
&- \#\{\text{múltiplos de } p_1p_2p_3,\ \text{de 1 a } n\} - \cdots etc \cdots , \qquad (*)
\end{aligned}$$

onde na 2ª fila são consideradas todas as combinações possíveis de dois primos; na 3ª fila todas as de três primos; etc ...

Exemplo: $\varphi(12) = \varphi(2^2 \cdot 3) = 12 - \#\{2,4,6,8,10,12\} - \#\{3,6,9,12\} + \#\{6,12\}$.

Exercício: Escreva $(*)$ explicitamente para $n = 420$.

Note-se que em $(*)$ um número da forma $cp_{i_1}^{\beta_1}p_{i_2}^{\beta_2}\cdots p_{i_k}^{\beta_k} < n$, com $(c,n) = 1$, $k \geq 1$, $\beta_j \leq \alpha_{i_j}$ (observe-se que estes são precisamente os números compreendidos entre 1 e n e que *não* são primos com n) é contado: $1 - k - \binom{k}{2} - \binom{k}{3} + \cdots + (-1)^k\binom{k}{k} = (1-1)^k = 0$ vezes ! Isto é, só os números entre 1 e n que são primos com n é que são contados em $(*)$ (uma vez).

[15] Esta última parcela é necessária uma vez que os múltiplos de 10 foram descontados duas vezes: uma como múltiplos de 2 e outra como múltiplos de 5.

Resulta que:

$$\begin{aligned}
\varphi(n) &= n - \frac{n}{p_1} - \cdots - \frac{n}{p_t} + \frac{n}{p_1p_2} + \frac{n}{p_1p_3} + \cdots + \frac{n}{p_1p_t} + \cdots + \\
&\quad + \cdots + \frac{n}{p_{t-1}p_t} - \frac{n}{p_1p_2p_3} - \cdots = \\
&= n\left(1 - \sum_i \frac{1}{p_i} + \sum_{i<j} \frac{1}{p_ip_j} - \sum_{i<j<k} \frac{1}{p_ip_jp_k} + \cdots\right) \underset{(**)}{=} \\
&\underset{(**)}{=} n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_t}\right) = \\
&= p_1^{\alpha_1}\cdots p_t^{\alpha_t}\left(\frac{p_1-1}{p_1}\right)\left(\frac{p_2-1}{p_2}\right)\cdots\left(1 - \frac{1}{p_t}\right) = \\
&= p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_t^{\alpha_t-1}(p_1-1)(p_2-1)\cdots(p_t-1).
\end{aligned}$$

A igualdade $(**)$ justifica-se pelo facto de o produto de vários factores, cada um dos quais contendo várias parcelas, ser igual à soma de todas as parcelas constituídas por produtos formados por um membro de cada um desses factores.

Em conclusão:

$$\boxed{\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}) = p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_t^{\alpha_t-1}(p_1-1)(p_2-1)\cdots(p_t-1)}$$

onde p_i é um número primo $(i = 1, 2, \ldots n)$ e $\alpha_i \in \mathbb{N}$.

Exemplo: $\varphi(10.000) = \varphi(2^4 \cdot 5^4) = 2^3 \cdot 5^3(2-1)(5-1) = 1000 \cdot 4 = 4.000$.

Inversos módulo n

Sejam $(a, n) = 1$. Pelo algoritmo de Euclides, existem $x, y \in \mathbb{Z}$ tais que $ax + ny = 1$. Resulta que $ax \equiv 1 \pmod{n}$, para algum $x \in \mathbb{Z}$. Por analogia com o facto de se chamar inverso de um número ao que por ele multiplicado dá 1, tem-se:

Definição 1.4.9 *Dados dois inteiros a e n com $(a, n) = 1$, chama-se* **inverso de a módulo** *n a qualquer um dos inteiros x tais que $a \cdot x \equiv 1$* $\pmod{n}$.

Ficou visto que se $(a, n) = 1$, então existem inversos de a módulo n, um dos quais pode ser calculado usando o algoritmo de Euclides. É claro que se a e n tiverem factores comuns, então a não tem nenhum inverso módulo n (*porquê*?).

Exemplo: $a = 5$, $n = 17$.

$$\begin{aligned} 17 &= 3 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \quad \rightsquigarrow \quad 1 = 5 - 2 \cdot 2 = 5 - (17 - 3 \cdot 5) \cdot 2 = \\ & \qquad\qquad\qquad\quad = 7 \cdot 5 - 2 \cdot 17. \end{aligned}$$

Conclui-se assim que 7 é um inverso de 5 módulo 17 (observe-se que -10 e 24 são também inversos de 5 módulo 7, assim como qualquer número da forma $7 + 17k$, $k \in \mathbb{Z}$).

1.5 O código RSA.

A criptografia, "a ciência de manter os segredos secretos"[16], é uma actividade bem antiga, assim como o envolvimento de matemáticos na invenção e quebra de códigos secretos[17]. François Viéte (1540-1603), famoso pelo seu tratamento da teoria das equações, tendo sido um dos primeiros a tratar casos gerais usando letras para representar números genéricos[18], é também famoso por ter decifrado mensagens secretas espanholas, a serviço do rei Henri IV de França, durante a guerra com Espanha. Filipe II de Espanha, incapaz de acreditar que tal era humanamente possível, apresentou queixa junto do Papa de que os franceses estavam a usar magia negra. O Papa bem pode ter ficado impressionado, mas não o suficiente para acreditar que magia negra estivesse envolvida, já que os próprios especialistas do Vaticano haviam

[16] H. Delfs e H. Knebl, *Introduction to Cryptography*, Springer 2002.

[17] cf. D. Kahn, *The Codebreakers: The Story of Secret Writing*, Scribner 1996, a segunda edição, revista e actualizada, do grande clássico da história da criptologia originalmente escrito em 1967.

[18] cf. D. J. Struik, *História Concisa das Matemáticas*, Gradiva 1987.

decifrado um dos códigos de Filipe II uns 30 anos antes![19]

Outro famoso matemático, um dos "pais" dos computadores, desempenhou um papel fundamental no deciframento do supostamente indecifrável código Enigma, o código secreto usado pelas tropas de Hitler na 2ª guerra mundial: Alan Turing (1912-1954)[20].

Todos os códigos "clássicos" são "simétricos". Isto é, conhecendo a chave de codificação sabe-se também como descodificar. A descoberta de algoritmos muito rápidos de primalidade, isto é algoritmos que decidem se um número é ou não primo, enquanto o problema de factorizar um número (ou simplesmente descobrir um factor) continua a ser computacionalmente muito demorado, levou à invenção de códigos assimétricos: os códigos de "chave pública".

Para dar uma ideia da diferença de complexidade entre determinar a primalidade de um número e factorizá-lo, pode-se hoje (2002) decidir, num computador "decente", se um número com 600 algarismos é ou não primo em menos de 1 minuto, enquanto que descobrir um factor de muitos dos números de 600 algarismos pode levar, na mesma máquina, mais de um século![21]

Um desses códigos de "chave pública" é o código RSA, assim chamado em honra aos seus inventores: Rivest, Shamir e Adleman.

Descrição do código RSA

Sejam p e q dois primos distintos e "grandes" (300 algarismos é suficiente nos dias de hoje (2002)...). Seja $n = p \cdot q$, escolha-se um número c (de

[19] cf. J. Stillwell, *Mathematics and Its History*, Springer 1989, pp. 63-64.

[20] Ver a excelente biografia *Alan Turing: the enigma* de Andrew Hodges (Simon & Schuster, Inc., 1984)

[21] Por exemplo, o teorema de Fermat pode ser usado, em certos casos, para mostrar que um número é composto sem que se determine qualquer factor: se n for ímpar e verificando-se que $2^{n-1} \not\equiv 1 \pmod{n}$ (o que é muito rápido), conclui-se imediatamente que n é composto. (O recíproco é falso: existem números compostos ímpares n tais que $2^{n-1} \equiv 1 \pmod{n}$, por exemplo 341...)

codificar...) tal que $(c, \varphi(n)) = 1$ [$\Leftrightarrow (c, p-1) = (c, q-1) = 1$] e determine-se d (de **d**escodificar...) de modo que $dc \equiv 1 \pmod{\varphi(n)}$ (isto é d é um inverso de c módulo $\varphi(n)$).

$n, c \longrightarrow$ públicos (toda a gente os pode conhecer...)
$d \longrightarrow$ secreto (p, q e $\varphi(n)$ devem ser deitados ao lixo...)

Seja agora M a mensagem, ou parte da mensagem, numa forma númerica, a ser codificada. M deve satisfazer as seguintes condições: $(M, n) = 1$ e $M < n$ (o que certamente acontece se $M < \max\{p, q\}$).

Para "traduzir" mensagens em mensagens numéricas podemos (por exemplo) utilizar o seguinte "dicionário":

$\nearrow$	0	1	2	3	4	5	6	7	8	9
1	A	B	C	D	E	F	G	H	I	J
2	K	L	M	N	O	P	Q	R	S	T
3	U	V	W	X	Y	Z	,	.	!	

(isto é, A $\leftrightarrow$ 10, N $\leftrightarrow$ 23, "," $\leftrightarrow$ 36, "espaço" $\leftrightarrow$ 39, etc...)

Exemplo: "O exame final vai ser fácil" $\longmapsto$ "249914331022149915182310219931101899281427991510121821"

A mensagem M é então codificada achando o resto, E, da divisão de M^c por n. Ou seja, E, a mensagem que será enviada, é o único número E tal que $E \equiv M^c \pmod{n}$ e $0 \leq E < n$.

Para descodificar E basta calcular o resto da divisão de E^d por n, pois: $E^d \equiv M^{cd} \pmod{n}$, e como $cd \equiv 1 \pmod{\varphi(n)}$, tem-se que $cd = 1 + \varphi(n)q$ para algum $q \in \mathbb{Z}$ e portanto $M^{cd} \equiv M \cdot \left(M^{\varphi(n)}\right)^q \equiv M \pmod{n}$, pelo teorema de Euler, uma vez que $(M, n) = 1$. Como $M < n$, M é assim o resto de E^d módulo n, como afirmado.

Exemplo: Sejam $p = 1117$ e $q = 4789$ (p e q pequenos só para exemplificar). Então $n = 5349313$ e $\varphi(n) = 1116 \cdot 4788 = 5343408$. É fácil verificar que $(11, \varphi(n)) = 1$, ou seja, podemos tomar $c = 11$.

Cálculo de d:

$$\begin{array}{rcll} 5343408 & = & 11 \cdot 485764 + 4 & \\ 11 & = & 4 \cdot 2 + 3 & \\ 4 & = & 3 \cdot 1 + 1 & \rightsquigarrow \ 1 = 4 - 3 = 4 - (11 - 2 \cdot 4) = \\ & & & \quad = 3 \cdot 4 - 11 = 3 \cdot (\varphi(n) - 485764 \cdot 11) = \\ & & & \quad = 3 \cdot \varphi(n) - 1457293 \cdot 11. \end{array}$$

Resulta que: $1 \equiv 11 \cdot (-1457293) \pmod{\varphi(n)}$, isto é, -1457293 é um inverso de c módulo $\varphi(n)$. Como é conveniente obter um número positivo, uma vez que serão calculados restos de potências elevadas a esse expoente, podemos tomar $d = -1457293 + \varphi(n) = 3886115$ (*porquê?*). Os números p, q e $\varphi(n)$ podem agora ser esquecidos.

Fica assim construído um código RSA com $n = 5349313$ e $c = 11$, sendo $d = 3886115$ o número secreto necessário à descodificação. A mensagem "*O exame final vai ser fácil*" pode agora ser codificada, dividindo-se-a, por exemplo, em blocos de três algarismos cada (o que assegura que $(M, n) = 1$ (*porquê?*)) e executando os seguintes cálculos:

$$\begin{array}{ccccc} M_1 = 249 & \rightsquigarrow & E_1 \equiv {M_1}^c \equiv 249^{11} \equiv 2042845 & \pmod{5349313} \\ M_2 = 914 & \rightsquigarrow & E_2 \equiv {M_2}^c \equiv 914^{11} \equiv 4793058 & \pmod{5349313} \\ \vdots & \vdots & \vdots & \\ \textit{etc...} & \textit{etc...} & \textit{etc...} & \\ \vdots & \vdots & \vdots & \end{array}$$

A mensagem "*O exame final vai ser fácil*" quando codificada com o código RSA considerado neste exemplo terá pois o seguinte aspecto: 2042845; 4793058; etc...[22]

O receptor da mensagem teria, para a descodificar, de calcular o resto da divisão de $2042845^{3886115}$ por 5349313, o de $4793058^{3886115}$ por 5349313

[22] A mensagem completa é: 2042845; 4793058; 217181; 4070128; 1182283; 1849985; 2973626; 2065925; 3988179; 3364889; 200779; 4320621; 2582542; 4965112; 2539593; 4510145; 114931; 4861614

etc... Em qualquer pequeno e modesto computador, com o algoritmo apropriado, usando as propriedades básicas das congruências, é relativamente rápido verificar que:

$$\begin{aligned} &2042845^{3886115} \equiv 249 \pmod{5349313}, \\ &4793058^{3886115} \equiv 914 \pmod{5349313}, \\ &\text{etc...}, \end{aligned}$$

recuperando-se assim a mensagem original.

O código RSA é considerado hoje um dos códigos mais seguro, sendo actualmente indecifrável. É claro que se alguém descobrir métodos "rápidos" de factorização, ou algoritmos "eficientes" de determinar $\varphi(n)$ sem ser necessário conhecer a factorização em primos de n, o código RSA deixaria de ter qualquer valor... Há porém quem conjecture, e com algumas razões para isso, que tal nunca acontecerá: de algum modo, factorizar um número pode ser "intrinsecamente" muito mais difícil do que determinar se ele é ou não primo.

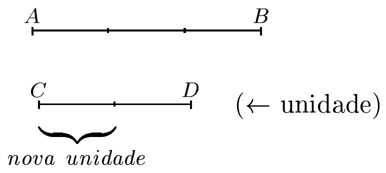
O código RSA tem também a vantagem de não ser necessário compartilhar segredos. A codificação é pública: n e c são conhecidos por todos, enquanto d é apenas conhecido por *uma* das partes. É claro que isto aumenta a segurança do código. Como Benjamin Franklin uma vez disse: "*Três pessoas conseguem guardar um segredo se duas delas estiverem mortas*".

2 Dos Racionais aos Reais

2.1 Generalidades sobre os números racionais

Os números racionais surgem naturalmente da necessidade de considerar submúltiplos de uma dada unidade.

Exemplo:



$AB = \frac{3}{2}CD$ significa que AB é 3 vezes metade da unidade CD. Mas também $AB = \frac{6}{4}CD = \frac{9}{6}CD = \ldots = \frac{3k}{2k}CD$ (correspondente a subdividir $\frac{1}{2}CD$ em k partes...).

Há pois muitas representações de um número racional como fracção de dois inteiros. Tem-se:

$$\frac{a}{b} = \frac{c}{d} \quad sse \quad ad = bc \quad \text{(verificar...)}$$

Um pequena reflexão conduz à introdução da soma e o produto de números racionais através das seguintes expressões:

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad+bc}{bd} \\ \frac{a}{b} \cdot \frac{c}{d} &= \frac{ac}{bd} \end{aligned}$$

(onde $a, b, c, d \in \mathbb{Z}$, com $b \neq 0$ e $d \neq 0$).

<u>Exercício:</u> Verificar que o resultado destas operações não depende dos representantes escolhidos. Verificar também que estas duas operações são associativas, comutativas, têm elemento neutro e cada elemento tem um inverso, com excepção do zero na multiplicação.

Do mesmo modo se pode motivar a introdução da relação de ordem usual no conjunto dos números racionais através de:

$$\frac{a}{b} < \frac{c}{d} \quad sse \quad ad < bc,$$

onde $a, b, c, d \in \mathbb{Z}$ com $b > 0$ e $d > 0$ (observer que é sempre possível escolher uma representação de um dado número racional com denominador positivo).

Notação: $\mathbb{Q}$ designa o conjunto de todos os números racionais.

Tem-se:

Proposição 2.1.1 *Sejam $a, b, c, d \in \mathbb{Z}$ com $b > 0$ e $d > 0$. Então*

$$\frac{a}{b} < \frac{c}{d} \Rightarrow \frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}.$$

Em particular, entre dois quaisquer números racionais distintos existe um outro.

Demonstração: $\frac{a}{b} < \frac{a+c}{b+d} \Leftrightarrow ab + ad < ba + bc \Leftrightarrow ad < bc \Leftrightarrow \frac{a}{b} < \frac{c}{d}$.

Analogamente $\frac{a+c}{b+d} < \frac{c}{d} \Leftrightarrow ad + cd < bc + dc \Leftrightarrow ad < bc \Leftrightarrow \frac{a}{b} < \frac{c}{d}$. □

2.2 Dízimas periódicas

Os três desenvolvimentos decimais: $\frac{1}{6} = 0,16666...$

$$\frac{1}{7} = 0,142857\,142857...$$

$$\frac{1}{8} = 0,125$$

são de tipos diferentes. As duas primeiras dízimas são infinitas, a terceira é finita. Ambas as infinitas são periódicas: na primeira o período não começa logo após a vírgula, o que acontece na segunda. Estes dois tipos de dízimas designam-se, respectivamente, por **periódica mista** e **periódica pura**.

Notação: O período de uma dízima é usualmente indicado colocando-o entre parêntesis.

Exemplos:

$\frac{1}{7} = 0,(142857)$ $\frac{39}{44} = 0,88(63)$

$\frac{19}{27} = 0,(703)$ $\frac{19}{20} = 0,95$

$\frac{1}{11} = 0,(09)$ $\frac{1}{13} = 0,(076923)$

$\frac{1}{17} = 0,(0588235294117647)$

Veremos que todas as dízimas correspondentes a números racionais são de um dos três tipos indicados, e estudaremos como o tipo de dízima depende do numerador e do denominador.

Em primeiro lugar temos:

Proposição 2.2.1 *Toda a dízima correspondente ao desenvolvimento decimal de um número racional é periódica.*

Razão: Isto é evidente quando se utiliza o algoritmo da divisão.

Exemplo:

Para estudar as dízimas correspondestes aos números racionais é necessário perceber exactamente o que é feito no algoritmo que usualmente se usa para fazer divisões. Para tal, sejam $a \in \mathbb{Z}$ e $b \in \mathbb{N}$ tais que $(a, b) = 1$ (esta condição, que será essencial adiante, em nada restringe o nosso estudo, uma vez que todo o número racional admite sempre uma (e uma só) representação da forma $\frac{a}{b}$ com $a \in \mathbb{Z}, b \in \mathbb{N}$ e $(a, b) = 1$). Vejamos que determinar a dízima de $\frac{a}{b}$ correponde a determinar

$q, q_1, q_2, q_3, \ldots$ tais que:

$$\begin{array}{rcl} a & = & bq + r_0 \\ 10r_0 & = & bq_1 + r_1 \\ 10r_1 & = & bq_2 + r_2 \\ \vdots & \vdots & \vdots \\ 10r_n & = & bq_{n+1} + r_{n+1} \\ \vdots & \vdots & \vdots \end{array} \qquad (*)$$

com $0 \leq r_n < b$ para todo $n = 0, 1, 2, \ldots$ [A multiplicação por 10 corresponde a "baixar um zero"...]

Como $0 \leq r_n < b$, tem-se que $0 \leq 10r_n < 10b$ e por conseguinte $0 \leq q_{n+1} < 10$. Ou seja, q_n é um dígito (um número de 0 a 9) para todo $n \geq 1$. De (*) resulta, sucessivamente, que:

$$\begin{array}{lllllllll} \frac{a}{b} & = & q & + & \frac{r_0}{b} & & & & \\ & & & & \frac{r_0}{b} & = & \frac{q_1}{10} & + & \frac{r_1}{10b} \\ & & & & & & & & \frac{r_1}{10b} = \frac{q_2}{10^2} + \frac{r_2}{10^2 b}, \\ & & & & & & & & \qquad\qquad\vdots \end{array}$$

o que mostra que

$$\frac{a}{b} = q + \frac{q_1}{10} + \frac{q_2}{10^2} + \frac{q_3}{10^3} + \cdots = q, q_1 q_2 q_3 \ldots$$

Ou seja, (*) realmente determina a dízima de $\frac{a}{b}$, como afirmado. Note-se ainda que $(a, b) = 1 \Rightarrow (b, r_0) = 1$ (porquê?).

De (*) resulta também que:

$$\begin{aligned}
10r_0 &\equiv r_1 \pmod{b}\\
10r_1 &\equiv r_2 \pmod{b}\\
&\vdots\\
10r_n &\equiv r_{n+1} \pmod{b}\\
&\vdots
\end{aligned}$$

Donde resulta, para todo $t, n \geq 0$:

$$r_{n+t} \equiv 10r_{n+t-1} \equiv 10^2 r_{n+t-2} \equiv \cdots \equiv 10^t r_n \pmod{b}.$$

O nosso estudo divide-se agora em 3 casos: b primo com 10, b divide uma potência de 10, e o restante caso.

1º caso: $(b, 10) = 1$

Neste caso tem-se $(b, r_n) = 1$ para todo $n \in \mathbb{N}$ (*porquê?*) Em particular a dízima não é finita.

Seja r_n o primeiro resto a repetir-se (o que tem de acontecer pois só há um número finito de restos possíveis). Isto é, $r_{n+t} = r_n$ para algum $t \geq 1$. Pelo que acima ficou visto, resulta daqui que $r_n = r_{n+t} \equiv 10^t r_n \pmod{b}$. Como $(r_n, b) = 1$, deduz-se que $10^t \equiv 1 \pmod{b}$ e portanto $r_0 \equiv 10^t r_0 \equiv r_t \pmod{b}$. Mas como r_0 e r_n são números positivos menores que b, conclui-se que $r_0 = r_t$, ou seja, o primeiro resto a aparecer repetido é r_0!

Resulta também que o comprimento do período é igual a d, onde d é o menor inteiro positivo com $10^d \equiv 1 \pmod{b}$. Sabemos que $d \mid \varphi(b)$ (ver...). Vemos ainda que o comprimento do período não depende, neste caso, do numerador!

Resumindo, ficou provado que:

Proposição 2.2.2 *Seja $b \in \mathbb{N}$ um número primo com 10. Seja $a \in \mathbb{Z}$ tal que $(a, b) = 1$. Então a dízima de $\frac{a}{b}$ é puramente periódica, de período igual ao menor expoente positivo d tal que $10^d \equiv 1 \pmod{b}$.*
Em particular, o período é um divisor de $\varphi(b)$ e não depende do numerador.

<u>2º caso</u>: $b = 2^\alpha \cdot 5^\beta$, para alguns $\alpha, \beta \geq 0$.

Seja $n = \max\{\alpha, \beta\}$. Então $b \mid 10^n$. Como $r_n \equiv 10^n r_0 \pmod{b}$, resulta que $r_n = 0$, ou seja a dízima é finita.

<u>3º caso</u>: $b = 2^\alpha \cdot 5^\beta \cdot c$, com $\alpha, \beta \geq 0$, $\max\{\alpha, \beta\} > 0$, $(c, 10) = 1$ e $c > 1$.

Seja $n = \max\{\alpha, \beta\} \geq 1$. Tem-se $\frac{a}{b} = \frac{2^{n-\alpha}5^{n-\beta}a}{10^n c}$. Pelo 1º caso, sabemos que $\frac{2^{n-\alpha}5^{n-\beta}a}{c}$ é puramente periódica e que o comprimento do período é independente de a (e igual ao menor inteiro positivo d tal que $10^d \equiv 1 \pmod{c}$). Como dividir por 10^n correponde a deslocar a vírgula n casas para a esquerda, resulta que temos neste caso uma dízima periódica mista (que não é pura resulta de que se tem $(b, r_1) > 1$ (*porquê?*)).

Resumindo alguns dos resultados obtidos, temos:

Proposição 2.2.3 *Seja $b \in \mathbb{N}$ e $a \in \mathbb{Z}$ tal que $(a, b) = 1$. Então a dízima de $\frac{a}{b}$ é puramente periódica, mista ou finita consoante se tenha, respectivamente, $(b, 10) = 1$, $(b, 10) \neq 1$ e b tem um factor primo $\neq 2, 5$, ou b não tem nenhum factor primo $\neq 2, 5$.*

Ficou visto, em particular, que um número racional tem uma dízima periódica. O recíproco é também verdadeiro, como se pode ver através do seguinte exemplo que ilustra como converter uma dízima periódica numa fracção:

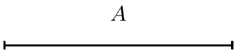
Seja $\alpha := 1,(317)$. Multiplicando α pela potência de 10 necessária para fazer avançar um período para a esquerda da vírgula, obtem-se:

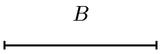
$$\begin{array}{rcrcccl} \alpha & = & 1, & 317 & 317 & 317 & ... \\ 10^3\alpha & = & 1317, & 317 & 317 & 317 & ..., \end{array}$$

donde resulta: $10^3\alpha - \alpha = 1316 \Rightarrow (10^3 - 1)\alpha = 1316 \Rightarrow \alpha = \frac{1316}{999}$.

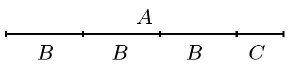
É claro que o que foi feito neste exemplo pode ser feito com qualquer dízima periódica (há uma pequena adaptação a fazer se a dízima fôr mista, qual?).

2.3 Os irracionais

Dados dois segmentos, 

e 

, como encontrar uma "medida comum" aos dois? Euclides, nos *Elementos*, refere o seguinte processo: meça-se A usando B. Se B não medir A exactamente, seja C (que é menor que B...) o segmento que resta:



Use-se agora C para medir B, e seja D o segmento que resta... etc... Quando obtivermos um segmento que divida exactamente o anterior, esse segmento é a medida comum pretendida. Repare que isto não é mais do que o algoritmo de Euclides visto atrás numa versão geométrica (a original).

Inicialmente os Pitagóricos (585 A. C. - 400 A. C.) acreditavam que era sempre possível arranjar uma medida comum a dois segmentos dados, em particular, que algo como o algoritmo de Euclides necessariamente termina ao fim de um número finito de etapas. Esta crença, sem dúvida baseada na intuição, estava associada à doutrina dos Pitagóricos de que "os números são a base do universo". A descoberta da existência de segmentos incomensuráveis (i. e. sem medida comum) causou pois sérios problemas filosóficos. Não se sabe ao certo quem descobriu este facto e como[23], mas uma possibilidade é

[23]Ver Boyer, cap. V, §9, p. 79.

através do:

Teorema de Pitágoras: [24]

Figure 1: Uma prova do Teorema de Pitágoras.

Neste contexto surge muito naturalmente a seguinte questão: qual a medida comum entre o lado e a diagonal do triângulo rectângulo cujos catetos são ambos iguais a 1, por exemplo?

Resolver esta questão é equivalente a encontrar dois números naturais a, b tais que $\sqrt{2} = \dfrac{b}{a}$ ($\frac{1}{a}$ seria a tal medida comum...). Tentemos determiná-los. Para tal procuremos retirar o máximo de informação possível do facto de que esses números têm de ser tais que $b^2 = 2a^2$. Mas daqui resulta que b tem se ser par (*porquê?*). Tentemos então utilizar esta pequena informação sobre b, escrevendo $b = 2c$ ($c \in \mathbb{N}$). Introduzindo isto na igualdade anterior, vem que $2c^2 = a^2$, de onde se conclui que a teria também de ser par. Mas isto é muito estranho, pois é claro que poderiamos ter partido de um par a, b formado por números primos entre si (*porquê?*). Que significa tudo isto? Só pode significar uma coisa: não existem números naturais a e b tais que $\sqrt{2} = \dfrac{b}{a}$!!

[24]Este resultado era já conhecido pelo menos desde 1800 A. C. por matemáticos babilónios.

Ou seja, se representarmos os números racionais numa recta (depois de escolhida uma unidade), e apesar de entre dois quaisquer haver sempre um outro, como vimos acima, essa recta teria "buracos"! Outra conclusão que resulta do que se acaba de ver é que os números racionais não são adequados para todas as medições de distâncias. Isto levou naturalmente a uma extensão do conceito de número. No entanto o estatuto de número (real) permaneceu confuso durante um longo período. Foi apenas nos finais do século XIX que se assentaram ideais, de um modo claro e preciso sobre os números reais, como resultado do trabalho de várias pessoas, essencialmente: H. Méray (1835-1911), Karl Weierstrass (1815-1897), H. Heine (1821-1881), G. Cantor (1845-1918) e Richard Dedekind (1831-1916)[25]. Veremos mais adiante qual a original solução dada por Dedekind ao problema de definir exactamente o que é um número real.

A prova dada acima de que $\sqrt{2}$ é um número irracional pode ser facilmente adaptada para mostrar a irracionalidade de outros números, como a de $\sqrt{p}$, para todo o primo p. Mas provar que números como $\sqrt{2}+\sqrt{3}$ são irracionais já não é assim tão fácil (repare que não é verdade que a soma de dois irracionais seja sempre irracional, por exemplo $\sqrt{2}$ e $(2-\sqrt{2})$ sço ambos irracionais mas a sua soma é racional!). O seguinte resultado é uma importante ferramenta para provar a irracionalidade destes e outros números.

Proposição 2.3.1 *Seja* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *um polinómio de coeficientes inteiros (ou seja,* $a_i \in \mathbb{Z}$*, para* $i = 1, \ldots, n$*). Se* r, s *são dois inteiros primos entre si tais que* $f(\frac{r}{s}) = 0$*, então:* $r \mid a_0$ *e* $s \mid a_n$*.*

[25] Boyer, pp. 604-608.

Demonstração:

$$\begin{aligned} f\left(\frac{r}{s}\right) = 0 \quad &\Leftrightarrow \quad a_n \frac{r^n}{s^n} + a_{n-1}\frac{r^{n-1}}{s^{n-1}} + \cdots + a_1 \frac{r}{s} + a_0 = 0 \Leftrightarrow \\ &\Leftrightarrow \quad a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s = 0 \Rightarrow \\ &\Rightarrow \quad s \mid a_n r^n, r \mid a_0 s^n. \end{aligned}$$

Como $(r, s) = 1$, resulta que $s \mid a_n$ e $r \mid a_0$, como queríamos provar. □

Este resultado é usado para mostrar a irracionalidade de certos números que são raízes de polinómios de coeficientes inteiros, uma vez que limita a verificação de que tais polinómios não têm raízes racionais a um número finito de cálculos.

Exemplos:

1. *Nova prova que* $\sqrt{2}$ *é irracional.*

   Se $\frac{r}{s}$ fosse uma raiz racional de $x^2 - 2$, com $(r, s) = 1$, ter-se-ia, pela proposição acabada de provar, que $s \mid 1$ e $r \mid 2$, o que implica $\frac{r}{s} = \pm 1, \pm 2$. Mas nenhum dos quatro números $\pm 1, \pm 2$ é raiz de $x^2 - 2$, logo $\sqrt{2}$ é irracional.

2. *Prova da irracionalidade de* $\sqrt{2} + \sqrt{3}$.

   Ponha-se $\alpha := \sqrt{2} + \sqrt{3}$. Tem-se: $\alpha^2 = 5 + 2\sqrt{6}$, de onde se deduz que $(\alpha^2 - 5)^2 = 24$, e de onde resulta que $\alpha^4 - 10\alpha^2 + 1 = 0$. Isto mostra que $\sqrt{2} + \sqrt{3}$ é uma das raízes do polinómio $X^4 - 10X^2 + 1 = 0$. Pela proposição anterior as únicas possíveis raízes racionais deste polinómio são ± 1. Mas $(\pm 1)^4 - 10 \cdot (\pm 1)^2 + 1 \neq 0$, de modo que se conclui que este polinómio **não** tem raízes racionais. Em particular, $\sqrt{2} + \sqrt{3}$ não é racional!

Corolário 2.3.2 *Se $a \in \mathbb{N}$ não é uma potência n-ésima, então $\sqrt[n]{a} \notin \mathbb{Q}$.*

Demonstração: Pela proposição anterior, as raízes racionais do polinómio $X^n - a$, se existirem, têm de ser de facto inteiras (*porquê?*). Isto mostra o que se queria provar (*porquê?*). $\square$

Pensou-se durante muito tempo que o processo de radiciação conduzia a todos os números irracionais. Veio-se a descobrir no século XIX (embora já se desconfiasse antes), e depois de um longo processo histórico, que não se obtinham todos os números desse modo. Tais descobertas levaram à seguinte distinção:

Definição 2.3.3 *Um número real α diz-se* **algébrico** *se existir um polinómio de coeficientes racionais do qual α seja raiz. Caso contrário, isto é, se tal polinómio não existir, α diz-se um número* **transcendente**.

Exemplos:

- $\sqrt{2}$ é algébrico: é raiz de $x^2 - 2$.
- $\sqrt{2} + \sqrt{3}$ é algébrico: vimos acima que é raiz de $x^4 - 10x^2 + 1$.
- $e = \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n = \sum_{n\geq 1} \frac{1}{n!}$ é transcendente: resultado obtido em 1873 por Hermite (1822-1901).
- $\pi = \frac{\textit{perímetro de um círculo}}{\textit{diâmetro desse mesmo círculo}}$ é transcendente: resultado obtido em 1882 por F. Lindemann (1852-1931).

Questões em aberto: $e + \pi$ é transcendente? e e^π, π^e?...

Seja $\gamma = \lim_{n\to\infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right) - \log n$, número entre 0 e 1 a que se dá o nome de *constante de Euler*. Não se sabe se γ é racional ou não!

Um resultado um pouco inesperado

Considerem-se todos os racionais entre 0 e 1, 0 excluído e 1 incluído, ou seja todos os números de $]0,1]\cap\mathbb{Q}$. Cada um desses números pode ser escrito de maneira única na forma $\dfrac{a}{b}$ com $a,b\in\mathbb{N}$ e $(a,b)=1$. Agora, "cubra-se" o número $\dfrac{a}{b}$ com um "lençol" de comprimento $\dfrac{1}{2b^2}$ centrado nesse número (i.e. o intervalo $\left[\frac{a}{b}-\frac{1}{4b^2},\frac{a}{b}+\frac{1}{4b^2}\right]$). Imagine-se cada racional "coberto" pelo seu "lençol". Será que todos estes "lençois" cobrem todo o intervalo $]0,1[$? A resposta é não!! De facto:

$$\frac{1}{\sqrt{2}}\notin\bigcup_{\substack{0<\frac{a}{b}\leq 1\\(a,b)=1,b>0}}\left[\frac{a}{b}-\frac{1}{4b^2},\frac{a}{b}+\frac{1}{4b^2}\right]$$

Demonstração: Como não há nenhum racional que multiplicado por ele próprio dê 2, tem-se que $b^2-2a^2\in\mathbb{Z}-\{0\},\forall a,b\in\mathbb{Z}$. Mas então: $|b^2-2a^2|\geq 1,\forall a,b\in\mathbb{Z}$ e portanto, para todo $a,b\in\mathbb{Z}$ com $b>0, 0<\dfrac{a}{b}\leq 1$, tem-se:

$$\frac{|b^2-2a^2|}{2b^2}\geq\frac{1}{2b^2}\Rightarrow\left|\frac{1}{2}-\frac{a^2}{b^2}\right|\geq\frac{1}{2b^2}\Rightarrow\left|\frac{1}{\sqrt{2}}-\frac{a}{b}\right|\cdot\left|\frac{1}{\sqrt{2}}+\frac{a}{b}\right|\geq\frac{1}{2b^2}\Rightarrow$$

$$\left|\frac{1}{\sqrt{2}}-\frac{a}{b}\right|\geq\frac{1}{2b^2\left(\frac{1}{\sqrt{2}}+\frac{a}{b}\right)}>\frac{1}{2b^2(1+1)}=\frac{1}{4b^2}.\qquad\square$$

2.4 Os Primeiros Transcendentes

Seja α um número algébrico e $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ um polinómio de coeficientes inteiros do qual α é raiz.

[*Obs*: dizer que α é raiz de um polinómio $x^n+c_{n-1}x^{n-1}+\cdots+c_1x+c_0$ de coeficientes racionais é equivalente a dizer que α é raiz de um polinómio $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$

de coeficientes inteiros (*porquê* ?). Exemplo iluminador: as raízes de $x^3 + \frac{3}{2}x + \frac{1}{3}$ são as mesmas de $6x^3 + 9x + 2$...].

Suponha-se que $f(x)$ tem grau mínimo de entre os polinómios nessas condições. Então $f(r) \neq 0 \; \forall r \in \mathbb{Q}$ (*porquê* ?).

A derivada de f, f', é limitada em $[\alpha - 1, \alpha + 1]$, pois é contínua. Isto é, existe $c > 0$ tal que $|f'(x)| \leq c$, para todo $x \in [\alpha - 1, \alpha + 1]$. Por outro lado, tem-se que $\left| f\left(\frac{r}{s}\right) \right| = \frac{|a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n|}{s^n} \geq \frac{1}{s^n}$ (para todo o racional $\frac{r}{s}$ com s positivo), uma vez que o numerador é um número inteiro positivo não nulo. Para cada racional $\frac{r}{s} \in [\alpha - 1, \alpha + 1]$ tem-se ainda, por um resultado do Cálculo Infinitesimal (que é geométricamente óbvio), que $-f\left(\frac{r}{s}\right) = f(\alpha) - f\left(\frac{r}{s}\right) = \left(\alpha - \frac{r}{s}\right) f'(z)$, para algum $z \in [\alpha - 1, \alpha + 1]$.

Reunindo toda esta informação, como peças de um puzzle, temos que: $\frac{1}{s^n} \leq \left| f\left(\frac{r}{s}\right) \right| = \left| f(\alpha) - f\left(\frac{r}{s}\right) \right| = \left| \alpha - \frac{r}{s} \right| \; |f'(z)| \leq c \; \left| \alpha - \frac{r}{s} \right|$, donde resulta que $\left| \alpha - \frac{r}{s} \right| \geq \frac{1}{cs^n}$, para todo $\frac{r}{s} \in [\alpha - 1, \alpha + 1] \cap \mathbb{Q}$ (com s positivo). Se fizermos $M = \min\left\{1, \frac{1}{c}\right\}$, tem-se que $\left| \alpha - \frac{r}{s} \right| \geq \frac{M}{s^n}$, para *todo o racional* $\frac{r}{s}$ com $s \geq 1$ (*porquê* ?). Ficou assim mostrado o seguinte resultado importante:

Teorema 2.4.1 (Liouville, 1844) *Se α é um número algébrico e se n é o mínimo dos graus dos polinómios dos quais α é raiz, então existe $M > 0$ tal que $\left| \alpha - \frac{r}{s} \right| \geq \frac{M}{s^n}$, para todo $\frac{r}{s} \in \mathbb{Q}$, com r, s inteiros e $s \geq 1$.* □

Definição 2.4.2 *Um número real α é chamado um* **número de Liouville** *se, para todo o inteiro positivo m, existe um número racional $\frac{r_m}{s_m}$, com $s_m >$*

1, tal que $\left|\alpha - \frac{r_m}{s_m}\right| < \frac{1}{s_m^m}$.

Corolário 2.4.3 *Os números de Liouville são transcendentes.*

Demonstração: Seja α um número de Liouville. Suponha-se que α é algébrico e que os polinómios de grau mínimo do qual α é raiz têm grau n. Então, pelo teorema de Liouville, existiria $M > 0$ tal que $\frac{1}{s_m^m} > \left|\alpha - \frac{r_m}{s_m}\right| \geq \frac{M}{s_m^n}$, para *todo* m. Resultaria que $s_m^n \geq s_m^m M$, e portanto $1 \geq s_m^{m-n} M \geq 2^{m-n} M$, para *todo* m, o que é absurdo. Por conseguinte α não pode ser algébrico $\square$

Impoẽ-se um exemplo de um número de Liouville:

Exemplo: O número $\alpha = \sum_{k \geq 1} \frac{1}{10^{k!}} = \frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^6} + \frac{1}{10^{24}} + \frac{1}{10^{120}} + \frac{1}{10^{720}} + \frac{1}{10^{5040}} + \cdots = 0,110001000000000000000001\underbrace{0\ldots0}_{95\ zeros}1\underbrace{0\ldots0}_{599\ zeros}1\underbrace{0\ldots0}_{4319\ zeros}1\ldots$ é um número de Liouville, logo transcendente.

Razão: Faça-se $\frac{1}{10} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \ldots + \frac{1}{10^{m!}} = \frac{r_m}{10^{m!}}$, e $s_m = 10^{m!}$. Tem-se então que: $\left|\alpha - \frac{r_m}{s_m}\right| = \frac{1}{10^{(m+1)!}} + \frac{1}{10^{(m+2)!}} + \cdots \leq$ (porquê?) $\frac{2}{10^{(m+1)!}} = \frac{2}{(10^{m!})^{m+1}} = \frac{2}{s_m^{m+1}} = \frac{1}{s_m^m}\frac{2}{s_m} \Rightarrow \left|\alpha - \frac{r_m}{s_m}\right| < \frac{1}{s_m^m}$ $\square$

Como se pode verificar pelo exemplo dado, o resultado de Liouville fornece facilmente exemplos, se bem que aparentemente não muito interessantes, de transcendentes. Existem vários outros resultados interessantes de transcendência, sendo um dos mais profundos e poderosos o famoso:

Teorema 2.4.4 (Gelfond-Schneider, 1934-35) *Se* α, β $(\in \mathbb{C})$ *são números algébricos, com* $\alpha \neq 0, 1$ *e* $\beta \notin \mathbb{Q}$*, então* α^β *é trancendente.*

Demonstração: Omitida por ultrapassar (em muito) o nível deste curso. $\square$

Exemplos: $2^{\sqrt{2}}, \sqrt{2}^{\sqrt{2}}$ são transcendentes.

Exercício: Utilize este resultado para concluir que $\log_{10}(2)$ é transcendente.

2.5 Os Infinitos de G. Cantor

Uma longa história, que se inicia com a equação diferencial que traduz o comportamento de uma corda vibrante, que passa pelo estudo de séries trignométricas, pela própria formulação da ideia moderna de função, levou G. Cantor (1845-1918), matemático russo de ascendência dinamarquesa-judaica, a ponderar de um modo profundo sobre os diferentes "tamanhos" de conjuntos infinitos. Essas reflecções, refinadas desde então, deram lugar aos conceitos e resultados que a seguir se apresentam. Uma das consequências mais curiosas é que há muito mais transcendentes do que algébricos, num sentido da palavra "muitos" que será brevemente explicitado.

Definição 2.5.1 *Dois conjuntos S, T dizem-se* **equipotentes** *se existir uma bijecção entre eles, em cujo caso utilizaremos a notação $S \simeq T$.*

Exemplos: $\{1, 2, 5\} \simeq \{3, 17, 2\} \simeq \{A, B, C\}$

$\mathbb{N} \simeq \{\text{números pares}\} \simeq \{\text{números impares}\}$.

Observe-se que a ideia de equipotência é uma ideia bem natural, que está na base do processo de contagem. De facto, para comparar dois conjuntos de objectos nem sempre é necessário contá-los. Por exemplo, se numa sala de aula todos os alunos estiverem sentados e houver cadeiras vazias, ninguém precisa contar as cadeiras e os alunos para concluir que há mais cadeiras que alunos. Aliás, quando contamos o que fazemos é estabelecer uma correspondência entre os objectos cuja quantidade pretendemos determinar, e um certo conjunto de objectos abstractos que trazemos sempre connosco: os números (naturais)! Os números são uma utilíssima ferramenta que nos permite estabelecer correspondências entre objectos que não estão fisicamente lado a lado.

O que Cantor fez não foi mais que estender este conceito básico de correspondência a conjuntos infinitos.

Definição 2.5.2 *Um conjunto diz-se* **numerável** *se for finito ou se for equipotente ao conjunto dos números naturais.*

Exemplos:

1. $\mathbb{Z}$ é numerável: $0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots$ é uma "enumeração" dos números inteiros.

2. $\mathbb{Q}^+$ é numerável (!)

   Razão: Os números racionais positivos podem ser "enumerados" de acordo com o esquema seguinte, prosseguindo no sentido indicado e saltando os números que tenham já sido levados em conta (isto porque cada racional positivo aparece aí repetido uma infinidade de vezes...):

$$\begin{array}{cccccccccccc}
\frac{1}{1} & \rightarrow & \frac{2}{1} & & \frac{3}{1} & \rightarrow & \frac{4}{1} & & \frac{5}{1} & \rightarrow & \frac{6}{1} & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \\
\frac{1}{2} & & \frac{2}{2} & & \frac{3}{2} & & \frac{4}{2} & & \frac{5}{2} & & \cdots & \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & & & & \\
\frac{1}{3} & & \frac{2}{3} & & \frac{3}{3} & & \frac{4}{3} & & \cdots & & & \\
 & \swarrow & & \nearrow & & \swarrow & & & & & & \\
\frac{1}{4} & & \frac{2}{4} & & \frac{3}{4} & & \cdots & & & & & \\
\downarrow & \nearrow & & \swarrow & & & & & & & & \\
\frac{1}{5} & & \frac{2}{5} & & \cdots & & & & & & & \\
 & \swarrow & & & & & & & & & & \\
\frac{1}{6} & & \cdots & & & & & & & & &
\end{array}$$

3. S, T numeráveis $\Rightarrow S \cup T$ numerável.

Razão: Por hipótese, podemos escrever $S = \{s_1, s_2, s_3, s_4, \ldots\}$ e $T = \{t_1, t_2, t_3, t_4, \ldots\}$. Mas então, $\{s_1, t_1, s_2, t_2, s_3, t_3, s_4, t_4 \ldots\}$ é uma "enumeração" de $S \cup T$, depois de removidas as eventuais repetições...

4. I numerável, S_i numerável para todo $i \in I \Rightarrow \bigcup_{i\in I} S_i$ numerável (!)

   Razão: Por hipótese, podemos supôr $I = \mathbb{N}$ e, para cada $i \in I$, escrever $S_i = \{s_{i1}, s_{i2}, s_{i3}, s_{i4}, \ldots\}$. Então

$$
\begin{array}{cccccccccccc}
s_{11} & \rightarrow & s_{12} & & s_{13} & \rightarrow & s_{14} & & s_{15} & \rightarrow & s_{16} & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \\
s_{21} & & s_{22} & & s_{23} & & s_{24} & & s_{25} & & \cdots & \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & & & & \\
s_{31} & & s_{32} & & s_{33} & & s_{34} & & \cdots & & & \\
 & \swarrow & & \nearrow & & \swarrow & & & & & & \\
s_{41} & & s_{42} & & s_{43} & & \cdots & & & & & \\
\downarrow & \nearrow & & \swarrow & & & & & & & & \\
s_{51} & & s_{52} & & \cdots & & & & & & & \\
 & \swarrow & & & & & & & & & & \\
s_{61} & & \cdots & & & & & & & & &
\end{array}
$$

   fornece uma enumeração de $\bigcup_{i\in I} S_i$, "saltando" por cima dos elementos eventualmente repetidos.

5. $\mathbb{Q}$ é numerável.

   Razão: Resulta de $\mathbb{Q} = \mathbb{Q}^+ \cup \{0\} \cup \mathbb{Q}^-$, por (2) e (4).

6. S, T numeráveis $\Rightarrow S \times T = \{(s,t) \mid s \in S, t \in T\}$ numerável.

   Razão: Por hipótese, podemos escrever $S = \{s_1, s_2, s_3, s_4, \ldots\}$ e $T = \{t_1, t_2, t_3, t_4, \ldots\}$. Então:

$$
\begin{array}{cccccccccccc}
(s_1,t_1) & \rightarrow & (s_1,t_2) & & (s_1,t_3) & \rightarrow & (s_1,t_4) & & (s_1,t_5) & \rightarrow & (s_1,t_6) & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \\
(s_2,t_1) & & (s_2,t_2) & & (s_2,t_3) & & (s_2,t_4) & & (s_2,t_5) & & \cdots & \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & & & & \\
(s_3,t_1) & & (s_3,t_2) & & (s_3,t_3) & & (s_3,t_4) & & \cdots & & & \\
 & \swarrow & & \nearrow & & \swarrow & & & & & & \\
(s_4,t_1) & & (s_4,t_2) & & (s_4,t_3) & & \cdots & & & & & \\
\downarrow & \nearrow & & \swarrow & & & & & & & & \\
(s_5,t_1) & & (s_5,t_2) & & \cdots & & & & & & & \\
 & \swarrow & & & & & & & & & & \\
(s_6,t_1) & & \cdots & & & & & & & & &
\end{array}
$$

fornece uma enumeração de $S \times T$.

7. $S_1, S_2, \ldots, S_n$ numeráveis $\Rightarrow S_1 \times S_2 \times \cdots \times S_n$ numerável.

   Razão: Resulta, por simples indução, do exemplo anterior.

8. $\mathcal{A} = \{$números algébricos$\}$ é numerável.

   Razão: A ideia básica é que os números algébricos são raízes de polinómios de coeficientes racionais; por (5), (7) e (4) o conjunto desses polinómios é numerável; como cada polinómio tem um número finito de raízes, o resultado em questão segue agora de (7).

   Mais precisamente, seja $\mathcal{P}_n = \{X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0 \,|\, c_i \in \mathbb{Q}\}$. Como $\mathcal{P}_n \simeq \mathbb{Q}^n$, resulta de (5) e (7) que $\mathcal{P}_n$ é numerável, para todo $n \geq 1$. Agora, de (4) resulta que $\mathcal{P} = \bigcup_{n \geq 1} \mathcal{P}_n$ é numerável. Dado $f \in \mathcal{P}$, designe-se por $\mathcal{R}_f$ o conjunto das raízes de f, i.e. $R_f = \{\alpha \mid f(\alpha) = 0\}$, que é um conjunto finito. Como $\mathcal{A} = \bigcup_{f \in \mathcal{P}} \mathcal{R}_f$, a sua numerabilidade resulta finalmente de (4).

Depois desta sequência de exemplos e resultados começa a parecer que todos os conjuntos são numeráveis. Porém uma das mais espectaculares descobertas de Cantor é que:

Proposição 2.5.3 $\mathbb{R}$ *não é numerável (!!)*

Razão: Mostremos que o intervalo $[0,1[$ não é numerável, o que implica o resultado em questão (*porquê?)*. Para isso procedemos por redução ao absurdo, ou seja, começamos por supôr que $[0,1[$ é numerável. Resultaria daí que poderiamos incluir *todos* os números de $[0,1[$ numa lista da forma:

$$\begin{array}{l} 0,a_{11}a_{12}a_{13}a_{14}a_{15}\ldots \\ 0,a_{21}a_{22}a_{23}a_{24}a_{25}\ldots \\ 0,a_{31}a_{32}a_{33}a_{34}a_{35}\ldots \\ 0,a_{41}a_{42}a_{43}a_{44}a_{45}\ldots \\ 0,a_{51}a_{52}a_{53}a_{54}a_{55}\ldots \\ \vdots \end{array}$$

(onde os a_{ij} são dígitos, i.e. números de 0 a 9).

Mostremos agora que esta lista não pode ser completa. Para isso construa-se o número $0,b_1b_2b_3b_4b_5\ldots$ do seguinte modo: escolha-se $b_1 \neq a_{11}, b_2 \neq a_{22}, b_3 \neq a_{33}$, etc... (por exemplo, seja $b_i = 1$ se $a_{ii} \neq 1$, e $b_i = 0$ se $a_{ii} = 1$). Bom, este número não está na lista dada, pois difere de todos os números que dela constam em pelo menos um algarismo, nomeadamente, difere do i-ésimo número da lista no i-ésimo algarismo após a vírgula. Isto contradiz as nossas suposições, o que conclui a prova $\square$

Corolário 2.5.4 *O conjunto dos números transcendentes não é numerável*

Razão: Resulta imediatamente do resultado acabado de provar, juntamente com (8) e (4). $\square$

Por conseguinte, há muitos mais transcendentes que algébricos !!!... Isto, no seguinte sentido, natural depois de tudo o que ficou visto: um conjunto

B é "maior" que o conjunto A se não houver nenhuma bijecção entre A e B, mas houver uma bijecção de A numa parte de B (o que é o mesmo que dizer que há uma injecção de A em B). Para descrever esta situação, é por vezes usada a notação: $A \prec B$, e diz-se que B tem cardinalidade superior à de A.

É possível mostrar (o que não vai ser feito aqui) que dados dois conjuntos A e B, então acontece uma de três coisas: $A \prec B$ ou $B \prec A$ ou $A \simeq B$. Isto é, ou há uma injecção de A em B, ou uma injecção de B em A, ou então uma bijecção de A em B. Que $A \prec B$ e $B \prec A$ não podem ocorrer simultaneamente é o conteúdo do seguinte resultado:

Teorema 2.5.5 (Schröder-Bernstein) *Se existem funções $A \to B$ e $B \to A$ injectivas, então $A \simeq B$.*

Demonstração: Ver P. Halmos, *Naïve Set Theory* (Springer-Verlag 1974). $\square$

Do que ficou visto, não é difícil concluir que:

$$\mathbb{Q} \simeq \{\text{ algébricos }\} \prec \{\text{ transcendentes }\} \simeq \mathbb{R}.$$

[De facto todas estas relações resultam imediatamente do que se mostrou, excepto a última $\simeq$, isto é que: $\{$ transcendentes $\} \simeq \mathbb{R}$, cuja prova é um interessante exercício.]

Uma outra espectacular descoberta de G. Cantor é que dado um conjunto, há sempre um outro de cardinalidade superior.

Teorema 2.5.6 (G. Cantor) *Seja A um conjunto e $\mathcal{P}(A) = \{S : S \subseteq A\}$ o conjunto dos subconjuntos ("partes") de A. Tem-se que $A \prec \mathcal{P}(A)$.*

Demonstração: É claro que a aplicação $A \to \mathcal{P}(A)$ dada por $a \mapsto \{a\}$ é injectiva. Falta pois mostrar que $A \not\simeq \mathcal{P}(A)$. Suponha-se, por redução ao absurdo, que existe uma bijecção $\phi : A \to \mathcal{P}(A)$. Seja $\mathcal{C} = \{a \in A : a \notin \phi(a)\} \in \mathcal{P}(A)$. Por hipótese, existe $c \in A$ tal que $\phi(c) = \mathcal{C}$. Mas:

$$c \in \mathcal{C} \underset{[\text{pois } \mathcal{C} = \phi(c)]}{\Longleftrightarrow} c \in \phi(c) \underset{[\text{por definição de } \mathcal{C}]}{\Longleftrightarrow} c \notin \mathcal{C} \qquad (!!!)$$

Resulta que tal bijecção não existe. □

Observação: A demostração anterior mostra que não existe nenhuma aplicação sobrejectiva $\phi : A \to \mathcal{P}(A)$, exibindo um conjunto que não pertence a $Im(\phi)$, nomeadamente: $\{a \in A : a \notin \phi(a)\}$.

Este resultado de G. Cantor esteve na base de um profundo e sistemático estudo dos fundamentos da Matemática, pois conduz imediatamente a um paradoxo:

Paradoxo de Cantor: Seja Ω o conjunto cujos elementos são *todos* os conjuntos. Em particular, $\mathcal{P}(\Omega) \subseteq \Omega$, uma vez que os subconjuntos de Ω, sendo conjuntos, são elementos de Ω. Mas isto contradiz o resultado anterior!

Um dos primeiros a notar a existência de paradoxos decorrentes do trabalho de Cantor em teoria dos conjuntos, foi Burali-Forti (1861-1931) num artigo de 1897. Poucos anos depois, Bertrand Russel (1872-1970) introduz, numa linguagem despida de gíria matemática, mais uns paradoxos em torno da ideia de um conjunto de todos os conjuntos. Um dos seus exemplos mais famosos é o:

Paradoxo de Russel: Dado um conjunto há duas possibilidades: ou ele é um elemento de ele próprio ou não. Por exemplo, o conjunto de todos os objectos que não são pêras, é um elemento de si próprio (pois não é uma pêra!), enquanto o conjunto dos números naturais não é um dos seus elementos. Considere-se agora o conjunto de todos os conjuntos que não são elementos de si próprios. Será que este conjunto é um elemento de si próprio? Bom, ele pertence a si próprio se e só se for um dos conjuntos que não pretencem a si próprios. Mas isto é contraditório!!!

Tudo isto conduziu a uma reflecção crítica do conceito de conjunto, cujo uso indiscriminado conduz a vários paradoxos. Uma axiomatização da teoria dos conjuntos que elimina estes paradoxos foi introduzida por Zermelo em 1908, tendo sido posteriormente refinada por Fraenkel em 1921.

Finalizamos esta secção com dois divertidos paradoxos inspirados nesta análise crítica sobre o conceito de conjunto, que foram introduzidos por Bertrand Russel (1872-1970) e Jules Richard (1892-1956), respectivamente. Desafia-se o leitor a resolvê-los:

Paradoxo do Barbeiro (1918): O barbeiro de uma certa cidade afirma barbear *exactamente* aqueles que não se barbeiam a si próprios. Quem barbeia o barbeiro?

Paradoxo de Richard: Considere o conjunto $\mathcal{C}$ dos números naturais que são definidos por frases com menos de 100 letras [26]. Por exemplo: "trinta e seis" e "dezanove vezes quarenta e sete" mostram, respectivamente, que 36 e 893 $\in \mathcal{C}$. Agora, o complementar de $\mathcal{C}$ tem um mínimo, e esse mínimo pode ser descrito como "*o menor número natural que não pode ser descrito com menos de cem letras*". Mas esta frase contém menos de 100 letras (!), e portanto o menor número que não está em $\mathcal{C}$, estaria em $\mathcal{C}$ ...!!!

2.6 O que é um número real?

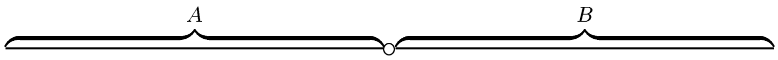
Vimos acima que a "recta racional" contém "buracos", por exemplo: $\sqrt{2}$. Depois vimos que contém de facto uma infinidade deles. Vimos de seguida que há uma infinidade não numerável de números que não são sequer raízes de polinómios de coeficientes racionais: os transcendentes. Em Álgebra II (do 2º ano do curso) será visto que um número transcendente não pode ser

[26] Mostre que não há mais do que 27^{100} frases com um número de letras inferior a 100.

obtido como combinação de números racionais usando adições, subtracções, multiplicações, divisões e radiciação. Isto não pode deixar de fazer surgir a pergunta: o que é um número real? Como se pode caracterizar o conjunto dos números reais, e como ter a certeza que foram "tapados" todos os "buracos" da recta?

Estas questões, relativas à estrutura lógica dos números reais, foram enfrentadas por diversos matemáticos durante a segunda metade do século XIX. As construções dos números reais a partir dos números racionais de G. Cantor, via sucessões de Cauchy, e R. Dedekind (1831-1916), via "cortes" de racionais, são aquelas que hoje é mais comum apresentar. Limitar-nos-emos a dar aqui uma ideia da construção a partir dos chamados "cortes" de Dedekind.

A ideia de Dedekind é, grosso modo, considerar os reais como os "buracos" da recta racional. Mais precisamente, ele começa por observar que em cada divisão da recta em duas classes de pontos, tais que cada ponto da primeira classe está à esquerda de cada ponto da segunda classe, existe um e um só



ponto que produz a divisão. Dedekind transporta esta ideia para os números e define um número real como um "corte" de números racionais, em que um "corte" significa exactamente um par de conjuntos (A, B) de números racionais tais que $A \cup B = \mathbb{Q}$ e nenhum elemento de A é maior que algum elemento de B. Observando que B é determinado por A, temos:

Definição 2.6.1 *Um* **número real** *é um* <u>*conjunto*</u> *S de números racionais tal que:*

(i) $S \neq \emptyset, \mathbb{Q}$;

(ii) $x < y \ \wedge \ y \in S \Rightarrow x \in S$;

(iii) *não existe* $x \in S$ *tal que* $y \leq x \ \forall y \in S$.

[*Observações:* A condição (ii) significa que se S contém um dado número, então contém todos os números menores que esse. A condição (iii) diz que S não tem um máximo, e é importante porque não queremos que, por exemplo, $\{r \in \mathbb{Q} \mid r < 1\}$ e $\{r \in \mathbb{Q} \mid r \leq 1\}$ sejam ambos números reais, pois são conjuntos distintos.]

Notação: $\mathbb{R} = \{S \subset \mathbb{Q} \mid S$ é um número real $\}$.

Exemplos: $\sqrt{2} = \{r \in \mathbb{Q} \mid r < 0 \vee r^2 < 2\}$;

$1 = \{r \in \mathbb{Q} \mid r < 1\}$;

$-\sqrt[3]{5} = \{r \in \mathbb{Q} \mid r^3 < -5\}$.

A soma e o produto de dois números reais S e T são definidos à custa das respectivas operações dos números racionais, através de:

$$S + T = \{r \in \mathbb{Q} \mid r = s + t \text{ para alguns } s \in S, t \in T\},$$

$$S \times T = \{r \in \mathbb{Q} \mid r < 0 \text{ ou } r = s \cdot t \text{ para alguns } s \in S, t \in T, s \geq 0, t \geq 0\}.$$

A relação de ordem é definida da maneira óbvia:

$$S \leq T \Leftrightarrow S \subseteq T$$

Pode-se mostrar[27] que $\mathbb{R}$ munido destas operações tem as propriedades esperadas e é **completo**, isto é "não tem buracos", o que se pode ser formulado do seguinte modo: se $\emptyset \neq A \subseteq \mathbb{R}$ tem a propriedade (ii) considerada na definição de número real, i. e. $x < y \ \wedge \ y \in A \Rightarrow x \in A$, então existe $\alpha \in \mathbb{R}$ tal que $x \leq \alpha \ \forall x \in A$ e $\alpha \leq y \ \forall y \notin A$. Isto significa que se construírmos "cortes" de números reais, como acima fizemos para os racionais, não obteremos novos números.

[27] Para uma descrição mais detalhada e demonstrações das afirmações feitas, consultar M. Spivak, *Calculus*, Cap. 28.

3 Equações polinomiais e números complexos

3.1 A equação do segundo grau

A resolução de equações do 2º grau era já conhecida pelos matemáticos Babilónios cerca de 1700A.C. Estes foram aparentemente conduzidos a estas equações via problemas do tipo: encontrar dois números cuja soma e produto é conhecido. De facto, os dois números cuja soma é s e cujo produto é p são exactamente as duas soluções de $x^2 - sx + p = 0$. Isto porque, se α e β são tais que $\alpha + \beta = s, \alpha\beta = p$, então $x^2 - sx + p = (x-\alpha)(x-\beta)$.

As equações mais simples do 2º grau são as das forma $x^2 = c$. No caso de c ser um número negativo, não há soluções visto o quadrado de qualquer número real ser não negativo. Se $c = 0$, há uma única solução: $x = 0$. No caso em que $c > 0$, há duas soluções: uma positiva e uma negativa. A solução positiva denota-se por $\sqrt{c}$[28] e a outra solução é pois $-\sqrt{c}$.

A resolução algébrica destas equações faz-se por redução do caso geral a equações do tipo $x^2 = c$, via a relação $(x+a)^2 = x^2 + 2ax + a^2$ que, quando vista da direita para a esquerda, serve para eliminar o termo de grau 1 do seguinte modo:

$$ax^2 + bx + c = 0 \Leftrightarrow x^2 + \frac{b}{a}x + \frac{c}{a} = 0 \Leftrightarrow$$

$$\Leftrightarrow \left(x + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a} = 0 \Leftrightarrow \left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}$$

[28]Em particular, $\sqrt{2}$ é apenas um *nome* dado à raiz positiva de $x^2 = 2$. Uma maneira interessante de calcular aproximações racionais de $\sqrt{2}$ é a seguinte: $x^2 = 2 \Leftrightarrow x^2 - 1 = 1 \Leftrightarrow (x-1)(x+1) = 1 \Leftrightarrow x = 1 + \frac{1}{1+x} \Leftrightarrow x = 1 + \frac{1}{1+\frac{1}{1+x}}$, etc... Isto sugere que os números racionais $1 + \frac{1}{2}, 1 + \frac{1}{1+\frac{1}{2}}, 1 + \frac{1}{1+\frac{1}{1+\frac{1}{2}}}$, etc... se aproximam de $\sqrt{2}$, o que não é difícil mostrar.

De onde se conclui que as soluções de $ax^2 + bx + c = 0$ são:

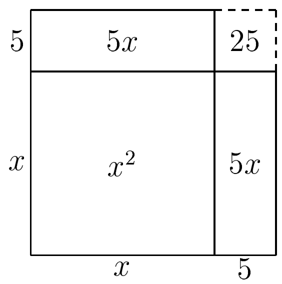
$$x = -\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2|a|} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

[*Nota*: O símbolo "$\pm$" é aqui utilizado apenas para escrever as duas soluções numa só fórmula. Assim a segunda igualdade significa que os dois números da esquerda são os dois da direita, embora o '$+$' corresponda ao '$-$' no caso de a ser negativo...]

O processo de eliminação do termo de grau 1 acima usado é por vezes designado por "completar o quadrado". Essa terminologia deriva da resolução geométrica da equação do 2º grau, resolução essa descrita por Euclides (livro VI) e usada pelos matemáticos árabes como al-Khwârizmi (c.780-c.850), onde se "completa" mesmo um quadrado, como no seguinte exemplo:

Problema: Resolver $x^2 + 10x = 39$.

Solução: Considere-se o quadrado de lado x. Adicione-se-lhe dois rectângulos de lados 5 e x como na figura seguinte:



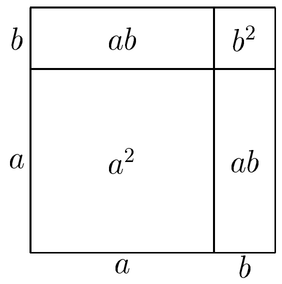
Como a zona sombreada tem área 39, o quadrado de lado $x + 5$ tem área 64, e portanto $x + 5 = 8$, donde resulta que $x = 3$. $\square$

Observe-se que este método permite apenas encontrar a solução positiva da equação dada...

Note-se que 25 é aquilo que é preciso adicionar para completar a figura sombreada de modo a formar um quadrado, ou seja o quadrado de lado

5 "completa" o quadrado grande. 25 é exactamente aquilo que é preciso adicionar a $x^2 + 10x$ para termos o quadrado $(x + 5)^2$.

A terminar esta secção fica aqui a prova geométrica da relação $(a+b)^2 = a^2 + 2ab + b^2$ (cf. Prop. 28 do livro VI dos Elementos de Euclides):



3.2 A resolução da cúbica

O interesse pelas equações cúbicas parece ter-se iniciado com Arquimedes (c.287-212A.C.), que no seu trabalho "Da Esfera e do Cilindro" considera o problema de cortar uma esfera por um plano de tal modo que a razão dos volumes dos dois pedaços na qual ela fica dividida seja um dado número, e mostra que a solução deste problema passa pela resolução de uma equação cúbica da forma $x^3 + m = nx^2$. Arquimedes resolve então esta equação usando a intersecção de uma parábola com uma hipérbole rectangular.

O interesse por equações cúbicas parece desaparecer logo após Arquimedes, tendo sido ressuscitado por Eutocius (c.480- ?), um comentador de obras de Apolónio e Arquimedes, para voltar a desaparecer passado pouco tempo, sendo mais uma vez ressuscitado, já no seio da civilização islâmica, por uma análise do mesmo resultado de Arquimedes feita por Abū 'Abdallāh al-Māhānī (825-888). Tipos particulares de equações cúbicas são então considerados e resolvidos por alguns matemáticos islâmicos, como Thābit ibn Qurra (836-901), al-Hasan ibn al-Haitham (c.965-c.1039) (conhecido por Alhazen), entre outros. É porém o matemático e poeta persa 'Umar al-Khayyāmī (c.1048-1131), também conhecido por Omar Khayyam, um dos maiores génios do seu tempo, o primeiro a tratar de modo sistemático as equações do 3º grau. No seu livro "Al-jabr wa'l muqabalah" (c.1079), Khayyam classifica as equações cúbicas em 19 tipos (quando expressas apenas com coeficientes positivos), mostrando que 5 destes tipos se reduzem a equações do 2º grau e, usando secções cónicas, resolve os restantes 14 tipos.

Vamos exemplificar o trabalho de Khayyam com a sua solução das equações da forma "cubo e lados igual a um número", ou seja, da forma $x^3 + mx = n$ $(m, n > 0)$, utilizando porém linguagem e notações modernas.

Khayyam começa por determinar a raiz quadrada de m, do seguinte modo, bem conhecido desde (pelo menos) Euclides[29]: sejam A e B dois pontos tais que $AB = m$; considere-se o ponto C no segmento [30] AB, situado de tal modo que B fique entre A e C, e $BC = 1$; determine-se o ponto médio M de AC e considere uma semicircunferência de diâmetro AC (ver figura); levante-se uma perpendicular a AC em B; seja D o ponto de intersecção dessa perpendicular com a circunferência;

então $a = BD$ é a raiz quadrada de m (prove-o! Sugestão: utilize o facto de o triângulo ADC ser um triângulo rectângulo em D (porquê?) e, por conseguinte, ADC é semelhante a BCD...).

[29]Como todos os matemáticos islâmicos, Khayyam conhecia muito bem os trabalhos mais importantes dos matemáticos gregos, entretanto traduzidos para o árabe.

[30]Por comodidade, usamos aqui a mesma notação tanto para o nome de um segmento como para o seu comprimento, sendo claro do contexto, em cada instância, a qual nos referimos.

Em seguida, Khayyam constrói o número b de tal modo que $n = a^2b$. Isso é feito geometricamente (como tudo o resto) de um modo bem simples. Considere-se a seguinte figura, onde $AB = 1$, $AD = a^2 = m$, $DE = n$, $DE \perp AD$, e C é a intersecção da perpendicular a AD por B com o segmento AE:

então $b = BC$ satisfaz a condição requerida (prove-o!).

Não podemos prosseguir sem deixar de referir que para os matemáticos gregos, assim como para Khayyam, dado um segmento AB, *a parábola de vértice B e parâmetro AB* era vista como a curva $\mathcal{P}$ constituida pelos pontos D tais que o rectângulo $BCDE$ é tal que se tem $(BE)^2 = BC \cdot AB$ (se colocarmos um referencial Cartesiano centrado em B de tal modo que A se situe na parte negativa do eixo dos 'x', então a equação desta parábola assume uma forma familiar: $y^2 = px$, onde $p = AB$).

Exercício: mostre que nesta figura, os pontos situados nos cantos superioresdireitos dos rectângulos representados estão todos numa mesma parábola, a de vértice B e parâmetro AB.

A solução de Khayyam da cúbica considerada, que foi entretanto reescrita na forma $x^3 + a^2x = a^2b$ $(a, b > 0)$, é a seguinte: sejam A e B tais que $AB = a$ e considere-se a parábola de vértice B e parâmetro AB; seja C tal que $BC \perp AB$ e $BC = b$; desenhe-se a circunferência de diâmetro BC (desenhe a figura!). Seja Z o ponto de intersecção dessa circunferência com a parábola. Finalmente, seja E a intersecção da perpendicular a BC que passa em Z com BC. Tem-se então que BE é a solução procurada de $x^3 + mx = n$.

No seu livro, Omar Khayyam faz ainda a discussão do número de raízes para cada tipo de cúbica. É de notar também que, apesar de todas as suas construcções serem de índole geométrica, sem dúvida sob influência da tradição grega, e de exprimir as soluções das cúbicas como segmentos e não como números dependendo dos coeficientes da equação, sabemos que Khayyam procurava encontrar esses números[31], pois logo no seu primeiro capítulo escreve:

> "*Quando, porém, o objectivo do problema é um número absoluto, nem eu, nem nenhum daqueles que se dedicam à álgebra, conseguiram resolver esta equação - talvez outros que se seguirão sejam capazes de preencher esta lacuna - excepto quando contém os três primeiros graus, nomeadamente, número, coisa e o quadrado.*"

Por "número absoluto", Khayyam refere-se a o que nós chamariamos de uma solução algébrica, por oposição a uma solução geométrica. Iriam passar-se mais de 4 séculos antes que "os que se seguirão" serem capazes dessa resolução algébrica desejada por Omar Khayyam. Não que não tivessem havido tentativas entretanto. Em 1494 Luca Pacioli (c.1445-c.1514), um

[31] A álgebra, como manipulação não geométrica de quantidades numéricas, conhecidas ou não, é acima de tudo uma das maiores contribuições dos matemáticos árabes.

monge italiano que foi aluno de Piero della Francesca e amigo e professor de Leonardo da Vinci, escrevia na sua *Summa de Arithmetica, Geometria, Proportione et Proportionalitá*[32], que a resolução de equações do 3º grau é tão difícil quanto a quadratura do círculo[33]. No entanto, a resolução daquelas equações estava para breve e iria desencadear um notável desenvolvimento da Matemática.

A realização do sonho de Omar Khayyam coube a Scipione del Ferro (1465-1526), professor de matemática da Universidade de Bolonha, uma das mais antigas universidades medievais, com uma forte tradição em Matemática. Este descobriu, não se sabe como[34] nem exactamente quando, apenas que deve ter sido algures por volta de 1515, como resolver cúbicas da forma $x^3 + px = q$.

Durante os séculos XVI e XVII era usual manterem-se secretas estas descobertas, desafiando os rivais a resolver o mesmo problema, e del Ferro não divulga o seu método. No entanto, antes de morrer, este confidencia o seu método a António Maria Fior (primeira metade do séc. XVI), e ao seu cunhado e sucessor Annibale della Nave (1500?-58).

Nada mais aconteceu até Niccolò Fontana di Brescia (1499-1557) entrar em cena. Este, ainda rapaz, tinha recebido um golpe de sabre na cara, aquando do saque de Brescia pelos franceses em 1512, o que o fazia gaguejar; por essa razão era conhecido por Tartaglia, o que em italiano sig-

[32]O primeiro livro de álgebra a ser impresso e uma das obras mais influentes do início do Renascimento

[33]A quadratura do círculo é um dos grandes problemas que os geómetras gregos formularam e a que não conseguiram dar resposta. O problema consiste em, dado um círculo, determinar, usando sómente régua (não graduada) e compasso, um quadrado de (exactamente) igual área. Com a prova da transcendência de π, por Lindemann em 1882, ficou mostrado que tal construcção é impossível.

[34]Mesmo sem qualquer fundamento histórico, uma vez que quase nada se sabe da vida de Scipione del Ferro, é bem possível que este fosse familiar com a obra de Khayyam, dado que muitas das obras dos matemáticos árabes foram traduzidas para o latim, e não deixa de ser tentador especular sobre a possível inspiração que o trabalho de Khayyam terá tido sobre o de del Ferro.

nifica "Gago". Nascido num meio bastante pobre, aprendeu latim, grego e matemática por ele próprio e ganhava a sua vida ensinando ciência em diversas cidades italianas.

Tartaglia de algum modo teve conhecimento da resolução algébrica da cúbica e, o facto de o saber possível motiva-o a dedicar-se a trabalhar na questão e o seu empreendimento é, ao fim de algum tempo, bem sucedido. Ouvindo que Tartaglia se vangloria de saber resolver cúbicas, Fior desafia-o, em 1535, a um "duelo" matemático, como era típico da época. Cada um propõe 30 cúbicas para o outro resolver num certo intervalo de tempo. O resultado é inesperado: Tartaglia resolve todas as 30 de Fior, sem que este tenha conseguido resolver sequer uma das questões propostas por Tartaglia! Esta humilhante derrota de Fior tem uma explicação simples: enquanto Fior sabia resolver apenas equações do tipo $x^3 + px = q$, Tartaglia era também capaz de resolver as do tipo $x^3 + px^2 = q$, e as 30 cúbicas que este propôs a Fior eram todas deste tipo...

A notícia do triunfo de Tartaglia chega ao conhecimento do médico e matemático italiano Girolamo Cardano (1501-76), que o convida a ir a sua casa. Pressionado por Cardano, Tartaglia revela-lhe, a 25 de Março de 1539, o seu método, em verso e de um modo um tanto obscuro, mas não antes de Cardano prometer solenemente mantê-lo secreto. Em 1542, Cardano e o seu aluno Ludovico Ferrari (1522-65) recebem uma visita de della Nave, e ficam a saber que o método de Tartaglia é o mesmo de del Ferro. Apesar da sua promessa, Cardano decide publicar a sua própria versão do método num livro intitulado *Ars Magna*, publicado em 1545.

A solução das equações cúbicas foi o primeiro claro avanço da Matemática renascentista sobre a Matemática dos gregos, dos hindus e dos árabes. Esse avanço revelava o poder da álgebra e do simbolismo literal que os matemáticos começavam agora a dominar. É pois perfeitamente justificável o entusiasmo de Cardano ao escrever no seu livro:

> "*Como esta arte* [da resolução da cúbica] *ultrapassa toda a subtileza e perspicácia do talento mortal, e é uma verdadeira prenda celestial e um teste muito claro da capacidade da mente humana, aquele que a ela se aplique sentirá que nada há que não possa compreender.* "

Vejamos pois a resolução de del Ferro-Tartaglia-Cardano. Comecemos por observar que a equação cúbica geral pode, após divisão pelo coeficiente do termo de maior grau, ser posta na forma:

$$x^3 + ax^2 + bx + c = 0 \ (a, b, c \in \mathbb{R}). \tag{1}$$

Em seguida, e em perfeita analogia com o que foi feito com as do 2º grau, a relação $\left(x + \frac{a}{3}\right)^3 = x^3 + ax^2 + \frac{a^2}{3}x + \frac{a^3}{27}$ pode ser usada para eliminar o termo de grau 2 e reduzir a cúbica inicial à forma:

$$y^3 + py + q = 0 \ (p, q \in \mathbb{R}). \tag{2}$$

(*Exercício*: Mostre que quando (1) é transformado em (2), se tem $y = x + \frac{a}{3}$, $p = b - \frac{a^2}{3}$, $q = \frac{2a^3}{27} - \frac{ab}{3} + c$.)

A ideia de del Ferro foi introduzir duas novas variáveis u e v, a determinar, tais que $y = u + v$. Como

$$(u+v)^3 + p(u+v) + q = u^3 + v^3 + (3uv + p)(u+v) + q,$$

isto é zero se u e v forem escolhidos de tal modo que $\begin{cases} u^3 + v^3 = -q \\ 3uv = -p \end{cases}$, o que é equivalente a $\begin{cases} u^3 + v^3 = -q \\ u^3v^3 = -\left(\frac{p}{3}\right)^3. \end{cases}$ Mas, pelo que se disse na secção (3.1), isto é equivalente a dizer que u^3, v^3 são as raízes do polinómio $z^2+qz-\left(\frac{p}{3}\right)^3$ (O problema reduz-se assim a uma equaçãodo 2º grau!). Por conseguinte,

$$u^3=\frac{-q+\sqrt{q^2+4\left(\frac{p}{3}\right)^3}}{2}, \quad v^3=\frac{-q-\sqrt{q^2+4\left(\frac{p}{3}\right)^3}}{2}. \tag{3}$$

Portanto:

$$y=\sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}. \tag{4}$$

3.3 Os problemas da fórmula resolvente do terceiro grau

A descoberta da fórmula resolvente para as equações cúbicas é um exemplo típico do que muitas vezes acontece em Matemática, em que a resolução de um problema levanta de imediato novas questões, dando assim origem a novas linhas de investigação. O exemplo em causa é talvez um dos mais profícuos de toda a história da Matemática.

Cardano é o primeiro a apontar uma dificuldade com o seu método, que ele não resolve, e que é a seguinte: a fórmula resolvente não fornece soluções quando $\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3$ é negativo, mas isto acontece para equações que se sabe à priori terem soluções! Cardano dá dois exemplos: $x^3=20x+25$ e $x^3=30x+36$, que têm 5 e 6 como raízes, respectivamente (de facto estes exemplos são obtidos da igualdade $x^3=(x^2-x)x+x^2$ para $x=5,6$, respectivamente), e para as quais $\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3=-\frac{15125}{108}, -676$, respectivamente.

O que é que se passa aqui? Será que este método de resolução da cúbica não é o melhor e é necessário procurar métodos alternativos? Bom, depois de milénios de esforço, a comunidade matemática não podia desistir assim tão facilmente de tão precioso achado. E é mais um dos algebristas italianos do século XVI, Rafael Bombelli (1526-72), que dá o passo seguinte.

Considere-se a equação $x^3 = 15x + 4$, um exemplo do próprio Bombelli, que tem a solução $x = 4$, como facilmente se verifica[35]. A fórmula (4), p. 66, dá, no entanto, $x = \sqrt[3]{2+\sqrt{-121}} + \sqrt[3]{2-\sqrt{-121}}$. Bombelli tem a ideia de que, trabalhando com raízes de números negativos formalmente, submetendo-as às mesmas regras operatórias usuais, talvez as expressões que aparecem na fórmula resolvente sejam da forma $2 + m\sqrt{-1}$ e $2 - m\sqrt{-1}$, respectivamente, de modo que a sua soma é realmente 4. Calculando o cubo destas expressões, Bombelli descobre que de facto: $\sqrt[3]{2+\sqrt{-121}} = 2+\sqrt{-1}$ e $\sqrt[3]{2-\sqrt{-121}} = 2-\sqrt{-1}$.

É assim que se começam a manipular raízes de números negativos: para "encontrar" a raiz "real" de uma equação cúbica na expressão da fórmula resolvente de del Ferro-Tartaglia-Cardano, quando nesta aparecem raízes quadradas de números negativos. Lentamente estas manipulações tornam-se mais comuns e nascem assim os "números complexos".

Definição 3.3.1 *Seja i um símbolo abstracto e considerem-se as expressões abstractas $a + bi$ com $a, b \in \mathbb{R}$. Estipule-se que:*

1. $a + bi = c + di \Leftrightarrow a = c, b = d$;

2. $i^2 = -1$;

3. $(a + bi)+(c + di) = (a + c) + (b + d)i$;

4. $(a + bi)\cdot(c + di) = (ac - bd) + (ad + bc)i$.

[35] $15 \times 4 + 4 = 16 \times 4 = 4^3$.

A estas expressões dá-se o nome de **números complexos** *e denota-se por* $\mathbb{C}$ *o conjunto dessas expressões munido da soma e produto assim definidos.*

Pode-se verificar (o que é deixado como exercício) que:

- A adição de números complexos tem as seguintes propriedades:
  - associativa: $(x+y)+z = x+(y+z)\ \forall x, y, z \in \mathbb{C}$;
  - comutativa: $x+y = y+x\ \forall x, y \in \mathbb{C}$;
  - tem elemento neutro: $0+0i$;
  - todo o complexo tem um simétrico: $-(a+bi) = (-a)+(-b)i$.
- A multiplicação de números complexos tem as seguintes propriedades:
  - associativa: $(x \cdot y) \cdot z = x \cdot (y \cdot z)\ \forall x, y, z \in \mathbb{C}$;
  - comutativa: $x \cdot y = y \cdot x\ \forall x, y \in \mathbb{C}$;
  - tem elemento neutro: $1+0i$;
  - todo o complexo *não nulo* tem um inverso:
    $$(a+bi)^{-1} = \left(\frac{a}{a^2+b^2}\right) + \left(\frac{-b}{a^2+b^2}\right) i.$$
- A adição e a multiplicação estão relacionadas através da seguinte propriedade:
  - distributividade: $(x+y) \cdot z = x \cdot z + y \cdot z\ \forall x, y, z \in \mathbb{C}$.

Um conjunto munido de duas operações que satisfazem as propriedades acabadas de descrever diz-se um **corpo**. Por exemplo $\mathbb{Q}$ e $\mathbb{R}$, munidos das operações de adição e multiplicação usuais são corpos. Observe-se que as definições de soma e produto de números complexos são inteiramente forçadas se queremos que elas tenham essas propriedades e sejam uma extensão das operações usuais de números reais. Por exemplo: $(a+bi)(c+di) = ac+adi+bic+bidi = ac+adi+bci+bdi^2 = ac+(ad+bc)i-bd = (ac-bd)+(ad+bc)i$.

Antes de prosseguirmos, poder-se-ia perguntar que relação de ordem se pode introduzir em $\mathbb{C}$. Vejamos que *não existe* nenhuma relação de ordem de tal modo que "> 0" tenha as seguintes *propriedades*:

(1) Dado $z \in \mathbb{C}$, $z > 0$ ou $z = 0$ ou $-z > 0$, sendo apenas uma destas condições satifeita;

(2) $z, w > 0 \Rightarrow z + w > 0, zw > 0$.

(Ou seja, não existe em $\mathbb{C}$ nenhum subconjunto análogo ao dos números positivos em $\mathbb{R}$.)

Razão: Se tal fosse possível, ter-se-ia $z^2 > 0$, para todo $z \in \mathbb{C} - \{0\}$ (*porquê?*). Mas então $1 = 1^2 > 0$ e, simultaneamente, $-1 = i^2 > 0$, o que implicaria, por (2), que $0 = 1 + (-1) > 0$, o que é absurdo. O disparate resultou de se ter assumido que existia uma relação de ordem em $\mathbb{C}$ com as propriedades mencionadas. Resulta que tal ordem não existe $\square$

É claro que se podem definir relações de ordem em $\mathbb{C}$, por exemplo, poder-se-ia pôr: $a + bi \leq c + di \Leftrightarrow \{a \leq c$ ou $(a = c$ e $b \leq d)\}$ (chamada ordem *lexicográfica*, por ser análoga à que usamos para ordenar as palavras (i.e. o nosso léxico)) Outro exemplo: $a + bi \leq c + di \Leftrightarrow \{a \leq d$ ou $(a = d$ e $b \leq c)\}$. O que acabamos de provar mostra, no entanto, que estas relações de ordem, ou outras quaisquer em $\mathbb{C}$, relativamente à soma e ao produto, não gozam das propriedades a que estamos habituados em $\mathbb{R}$. Isto limita em muito a utilidade dessas relações de ordem. Por estas razões, nenhuma ordem em $\mathbb{C}$ tem um papel priveligiado relativamente às outras, não fazendo por conseguinte sentido escrever $z \leq w$ para $z, w \in \mathbb{C}$, a não ser que se especifique o que "$\leq$" significa.

Um outro problema com a fórmula resolvente de del Ferro-Tartaglia-Cardano é que, aparentemente, fornece apenas *uma* solução para as equações do 3ºgrau. Onde estão as outras?

Exemplo (Cardano, *Ars Magna*): Considere-se a equação: $x^3 + 16 = 12x$. É fácil ver que 2 é solução: $2^3 + 16 = 4 \times (2 + 4) = 4 \times 6 = 12 \times 2$. Por outro lado, tem-se neste caso que: $\frac{q}{2} = 8$ e $\frac{p}{3} = -4$. Substituindo na fórmula (4), p. 66, vem:

$$x = \sqrt[3]{-8 + \sqrt{8^2 + (-4)^3}} + \sqrt[3]{-8 - \sqrt{8^2 + (-4)^3}} = \sqrt[3]{-8} + \sqrt[3]{-8} = -4$$

Onde está a raiz $x = 2$?

Outro exemplo: Considere-se a equação$(x-1)(x-2)(x+3) = x^3 - 7x + 6$. Neste caso, $\frac{q}{2} = 3$ e $\frac{p}{3} = -\frac{7}{3}$, e a fórmula resolvente dá:

$$\begin{aligned} x &= \sqrt[3]{-3 + \sqrt{9 - \left(\frac{7}{3}\right)^3}} + \sqrt[3]{-3 - \sqrt{9 - \left(\frac{7}{3}\right)^3}} \\ &= \sqrt[3]{-3 + \frac{10}{3\sqrt{3}}i} + \sqrt[3]{-3 - \frac{10}{3\sqrt{3}}i} \qquad (5) \end{aligned}$$

Qual das raízes $x = 1, 2, -3$ é esta? Para vermos qual, tentemos resolver $(a + \frac{b}{\sqrt{3}}i)^3 = -3 + \frac{10}{3\sqrt{3}}i$ (*porquê?*). Isto conduz, após alguns cálculos que deixamos como exercício, a:

$$\begin{cases} a(a^2 - b^2) = -3 \\ b(9a^2 - b^2) = 10. \end{cases} \qquad (6)$$

Escrevendo este sistema na forma $\begin{cases} a^2 - b^2 = -\frac{3}{a} \\ \\ 9a^2 - b^2 = \frac{10}{b} \end{cases}$ e subtraindo a primeira destas equações à segunda obtém-se: $8a^2 = \dfrac{3}{a}+\dfrac{10}{b}$; daqui tiramos b em função de a, o que substituído na primeira das equações do sistema considerado dá: $64a^9 + 144a^6 - 235a^3 + 27 = 0$. Esta equação de grau 9 é uma equação em a^3 de grau 3, a qual tem 3 raízes racionais, o que pode ser visto usando a Proposição da pág. 33. Daqui é fácil deduzir que o sistema (6) tem 3 soluções: $a = \dfrac{1}{2}, b = -\dfrac{5}{2}; a = 1, b = 2; a = -\dfrac{3}{2}, b = \dfrac{1}{2}$.

Por conseguinte, o que acontece é que as equações (3), p. 66, não têm apenas uma solução no novo corpo de números $\mathbb{C}$, como acontece nos reais, mas sim três!

Para vermos que assim é em geral, comecemos por resolver $x^3 = 1$ em $\mathbb{C}$. Como $x^3 - 1 = (x - 1)(x^2 + x + 1)$, e como $x^2 + x + 1 = 0$ tem as raízes $x = \dfrac{-1 \pm\sqrt{1-4}}{2} = -\dfrac{1}{2}\pm\dfrac{\sqrt{3}}{2}i$ (*porque é que se pode usar a fórmula resolvente do segundo grau em* $\mathbb{C}$*?*), resulta que a equação $x^3 = 1$ tem 3 soluções em $\mathbb{C}$: $1, -\dfrac{1}{2} + \dfrac{\sqrt{3}}{2}i, -\dfrac{1}{2} - \dfrac{\sqrt{3}}{2}i$.

Seja $\omega = -\dfrac{1}{2} + \dfrac{\sqrt{3}}{2}i$ e $\bar{\omega} = -\dfrac{1}{2} - \dfrac{\sqrt{3}}{2}i$. Observe-se que, como ω e $\bar{\omega}$ são as duas raízes do polinómio $X^2 + X + 1$, resulta que $\omega + \bar{\omega} = -1$ e $\omega\bar{\omega} = 1$.

Agora, se z é uma raiz cúbica do número complexo x, então as duas outras raízes cúbicas de x são: $z\omega$, $z\bar{\omega}$. Vemos assim que, se no método descrito de resolução das equações do 3º grau (ver p. 65) u for uma das raízes cúbicas de $-\dfrac{q}{2}+\sqrt{\left(\dfrac{q}{2}\right)^2 + \left(\dfrac{p}{3}\right)^3}$ (depois de escolhida e fixada uma raiz quadrada de $\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3$), então u, $u\omega$, $u\bar{\omega}$ são as as soluções da equação da esquerda em (3), p. 66. Por outro lado, fazendo $v = -\dfrac{p}{3u}$ (de modo a ter que $3uv = -p$, ver p. 66), resulta que: $-\dfrac{p}{3u\omega} = v\bar{\omega}$ e $-\dfrac{p}{3u\bar{\omega}} = v\omega$. De tudo isto se deduz:

Proposição 3.3.2 *Dados $p, q \in \mathbb{C}$, seja u uma das raízes cúbicas de $-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$. Faça-se $v = -\frac{p}{3u}$. Então as raízes de $X^3 + pX + q$ são: $u + v, u\omega + v\bar{\omega}$ e $u\bar{\omega} + v\omega$.*

Demonstração: O resultado resulta de tudo o que ficou dito, excepto alguns detalhes que não ficaram explicitados e que são deixados como exercício (note-se que, em particular, fica também como exercício perceber quais são esses detalhes). $\square$

Observação: A primeira discussão completa da solução de Cardano aparece apenas em 1732, num artigo de L. Euler, onde é realçado o facto de haver sempre três soluções e descrito como são obtidas.

Exemplo: Na resolução da equação $x^3 + 16 = 12x$, acima considerada (p. 70), tem-se que $-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} = -8$. Pode-se pois tomar $u = -2$, obtendo-
-se $v = -\frac{-12}{3(-2)} = -2$. As raízes da equação dada são pois: $u + v = -4$, $u\omega + v\bar{\omega} = -2(\omega + \bar{\omega}) = 2$ e $u\bar{\omega} + v\omega = 2$.

Os números complexos aparecem assim como um instrumento que resolve os problemas levantados pela fórmula resolvente do 3º grau, e que explica porque é que a fórmula de del Ferro-Tartaglia-Cardano não fornece, em certos casos, a solução esperada.

3.4 Digressão trigonométrica

Lema 3.4.1 *A soma dos ângulos internos de um triângulo é π radianos.*

Demonstração: $\square$

Lema 3.4.2 *O ângulo inscrito é metade do ângulo ao centro.*

Demonstração: Considerando, em primeiro lugar, o caso onde um dos lados do ângulo é um diâmetro do círculo, é fácil concluir o que se pretende se observarmos que o triângulo representado na figura da esquerda é isósceles. O caso geral reduz-se ao anterior, como se ilustra na figura da direita:

□

Lema 3.4.3 *Todo o triângulo se inscreve num círculo.*

Demonstração: Considere a segunte figura, relembrando que a mediatriz de AC, por exemplo, é o conjunto dos pontos cuja distância a A é igual à distância a C:

Sendo X o ponto de intersecção das mediatrizes representadas, tem-se então que: $dist(A,X) = dist(C,X)$ e $dist(B,X) = dist(C,X)$. Resulta daqui que $dist(A,X) = dist(B,X)$. O círculo pretendido é pois o de centro X e raio $r = dist(A,X) = dist(B,X) = dist(C,X)$. □

Proposição 3.4.4 $\begin{cases} \operatorname{sen}(x+y) = \operatorname{sen} x \ \cos y + \cos x \ \operatorname{sen} y \\ \cos(x+y) = \cos x \ \cos y - \operatorname{sen} x \ \operatorname{sen} y \end{cases} \qquad (\forall x, y \in \mathbb{R}).$

Demonstração[36]:

1º caso: $x > 0, y > 0$ e $x + y < \pi$.

Seja $z = \pi - (x+y)$ e considere-se a seguinte figura (utilize os lemas anteriores para mostrar que é possível desenhá-la e que os dois ângulos z são de facto iguais):

Tem-se: $\operatorname{sen} z = c$. Analogamente, $a = \operatorname{sen} x$, $b = \operatorname{sen} y$. Por conseguinte, $c = a \cos y + b \cos x \Rightarrow \operatorname{sen}(x+y) = \operatorname{sen}(\pi - (x+y)) = \operatorname{sen} z = \operatorname{sen} x \cos y + \operatorname{sen} y \cos x$.

Os outros casos: A fórmula que acabamos de provar (no caso indicado) é também verdadeira quando $x = 0$ ou $y = 0$, como é imediato verificar. Resulta que ela é válida para: $0 \leq x$, $0 \leq y$ e $x + y \leq \pi$.

[36] cf. S. Kung, *Amer. Math. Monthly*, vol. 64, nº 2, April 1991, p.97.

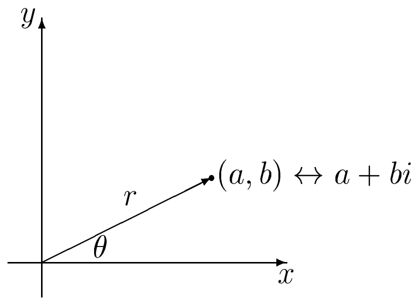
Figure 2: $\operatorname{sen}(x+y) = \operatorname{sen} x \cos y + \cos x \operatorname{sen} y$

Usando que $\operatorname{sen}(x+y) = \operatorname{sen}((\pi - x) + (-y)) = -\operatorname{sen}((x-\pi)+y) = -\operatorname{sen}((2\pi - x) + (-y)) =$ etc..., consegue-se reduzir qualquer outro caso ao primeiro (*exercício*: verificar que assim é!). Conclui-se pois que $\operatorname{sen}(x+y) = \operatorname{sen} x \cos y + \cos x \operatorname{sen} y$, $\forall x, y \in \mathbb{R}$.

Finalmente, $\cos(x+y) = \operatorname{sen}\left(\frac{\pi}{2} - (x+y)\right) = \operatorname{sen}\left(\left(\frac{\pi}{2} - x\right) + (-y)\right) =$
$= \operatorname{sen}\left(\frac{\pi}{2} - x\right)\cos(-y) + \cos\left(\frac{\pi}{2} - x\right)\operatorname{sen}(-y) = \cos x \cos y - \operatorname{sen} x \operatorname{sen} y,$
para todos $x, y \in \mathbb{R}$. □

3.5 Representação geométrica e raízes de números complexos

Cada número complexo sendo determinado por um par de números reais, podemos identificar cada complexo a um ponto (ou vector) do plano (no que se segue, supomos o plano munido dum referencial Cartesiano fixado duma vez por todas, e identificaremos cada ponto do plano ao vector com base na origem e extremidade nesse ponto).



Sejam r e θ, respectivamente, a distância do ponto à origem e o ângulo, contado no sentido oposto ao do movimento dos ponteiros de um relógio, desde a parte positiva do eixo dos 'x' ao vector determinado por esse ponto. Tem-se então que: $r = \sqrt{a^2 + b^2}$ (pelo teorema de Pitágoras), $a = r\cos\theta$ e $b = r\,\mathrm{sen}\,\theta$. Isto mostra que é possível escrever qualquer complexo na forma, dita trigonométrica:

$$r(\cos\theta + i\,\mathrm{sen}\,\theta) \text{ com } r \geq 0, \theta \in \mathbb{R}. \tag{7}$$

Vê-se também que $r(\cos x + i\,\mathrm{sen}\,x) = s(\cos y + i\,\mathrm{sen}\,y) \Leftrightarrow r = s$ e $x - y = 2\pi k$, para algum inteiro k.

A importância desta representação geométrica resulta essencialmente de que:

$$\begin{aligned} (\cos x + i\,\mathrm{sen}\,x)(\cos y + i\,\mathrm{sen}\,y) &= (\cos x\,\cos y - \mathrm{sen}\,x\,\mathrm{sen}\,y) + \\ &\quad + i\,(\cos x\,\mathrm{sen}\,y + \mathrm{sen}\,x\,\cos y) \\ &= \cos(x+y) + i\,\mathrm{sen}\,(x+y). \end{aligned} \tag{8}$$

Daqui resulta facilmente que a multiplicação pelo complexo $r(\cos\theta + i\,\mathrm{sen}\,\theta)$ corresponde, no plano, a compôr uma rotação de um ângulo θ com uma homotetia de razão r. Tem-se pois a seguinte correpondência entre as operações algébricas dos números complexos e as transformações do plano:

- somar um complexo $\leftrightarrow$ translacção;

- multiplicar por um complexo $\leftrightarrow$ composta de uma rotação com uma homotetia.

Não é pois de admirar que a estrutura algébrica dos complexos capture muita da geometria do plano.

De (8) resulta facilmente por indução que:

$$(r(\cos\theta + i\,\mathrm{sen}\,\theta))^n = r^n(\cos(n\theta) + i\,\mathrm{sen}\,(n\theta)). \tag{9}$$

E a partir daqui não é difícil chegar ao seguinte resultado:

Proposição 3.5.1 *As raízes n-ésimas de $z = r(\cos\theta + i\,\mathrm{sen}\,\theta)$ $(r \geq 0)$ são os números distintos $\sqrt[n]{r}\left(\cos\left(\frac{\theta+2\pi k}{n}\right) + i\,\mathrm{sen}\left(\frac{\theta+2\pi k}{n}\right)\right)$, para $k = 0, 1, \ldots, n-1$ (ou outros quaisquer n valores, dois a dois não congruentes modulo n), onde $\sqrt[n]{r}$ denota o único número real positivo x tal que $x^n = r$.*

Demonstração: De (9) resulta imediatamente que estes números são de facto raízes n-ésimas de z. Resta pois mostrar que eles são distintos e que não há outras raízes.

Tem-se que: $w = s(\cos y + i\,\mathrm{sen}\,y)$ é uma raiz n-ésima de $z \Leftrightarrow$

$$\Leftrightarrow r(\cos\theta + i\,\mathrm{sen}\,\theta) = w^n = s^n(\cos ny + i\,\mathrm{sen}\,ny) \Leftrightarrow \begin{cases} r = s^n \\ \cos\theta = \cos ny \\ \mathrm{sen}\,\theta = \mathrm{sen}\,ny \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} s = \sqrt[n]{r} \\ \theta = ny + 2\pi k, \text{para algum inteiro k} \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} s = \sqrt[n]{r} \\ \\ y = \dfrac{\theta - 2\pi k}{n}, \text{para algum inteiro k.} \end{cases}$$

Isto mostra que todas as raízes n-ésimas de z têm a forma exibida, restando eliminar valores de k diferentes dos indicados, e mostrar que estes dão raízes distintas. Mas:

$$\sqrt[n]{r}\left(\cos\left(\frac{\theta+2\pi k}{n}\right)+i\,\mathrm{sen}\left(\frac{\theta+2\pi k}{n}\right)\right)=\sqrt[n]{r}\left(\cos\left(\frac{\theta+2\pi k'}{n}\right)+i\,\mathrm{sen}\left(\frac{\theta+2\pi k'}{n}\right)\right)$$

$\Leftrightarrow \dfrac{\theta+2\pi k}{n}=\dfrac{\theta+2\pi k'}{n}+2\pi t$, para algum inteiro $t \Leftrightarrow k=k'+nt$, para algum inteiro $t \Leftrightarrow k\equiv k' \pmod{n}$. $\square$

Este resultado tem uma consequência interessante:

Corolário 3.5.2 *Todo o número complexo não nulo tem exactamente n raízes n-ésimas.* $\square$

Exemplo: raízes cúbicas da unidade. Como $1=\cos 0+i\,\mathrm{sen}\,0$, tem-se que as raízes cúbicas da unidade são as seguintes:

- $\cos\left(\dfrac{2\pi 0}{3}\right)+i\,\mathrm{sen}\left(\dfrac{2\pi 0}{3}\right)=1$;
- $\cos\left(\dfrac{2\pi}{3}\right)+i\,\mathrm{sen}\left(\dfrac{2\pi}{3}\right)=-\cos\left(\dfrac{\pi}{3}\right)+i\,\mathrm{sen}\left(\dfrac{\pi}{3}\right)=-\dfrac{1}{2}+\dfrac{\sqrt{3}}{2}i$;
- $\cos\left(\dfrac{4\pi}{3}\right)+i\,\mathrm{sen}\left(\dfrac{4\pi}{3}\right)=-\cos\left(\dfrac{\pi}{3}\right)-i\,\mathrm{sen}\left(\dfrac{\pi}{3}\right)=-\dfrac{1}{2}-\dfrac{\sqrt{3}}{2}i$.

Da Proposição anterior resulta ainda que as raízes n-ésimas da unidade são os n números $\cos\left(\dfrac{2\pi k}{n}\right)+i\,\mathrm{sen}\left(\dfrac{2\pi k}{n}\right)$, $k=0,1,\ldots,n-1$, que estão equidistribuidos na circunferência unitária, formando os vértices de um polígono regular de n lados. Por exemplo, para $n=7$ obtem-se a seguinte figura:

Figure 3: Raízes sétimas da unidade

3.6 O módulo e o conjugado de um número complexo

Definição 3.6.1 *Dado um número complexo $z = a+bi$, chama-se conjugado de z, ao número $a - bi$, o qual se denota por $\overline{z}$. Chama-se módulo de z ao número real não negativo $\sqrt{a^2 + b^2}$, denotando-o por $|z|$.*

Geometricamente, o conjugado é o número que se obtém quando se reflecte z relativamente ao eixo dos 'x', enquanto o módulo é a sua distância à origem. A importância do conceito de conjugado e de módulo resulta das seguintes propriedades:

- $|w \cdot z| = |w| \cdot |z| \, \forall w, z \in \mathbb{C}$ (como resulta de (8), ou por cálculo directo).
- $\overline{w+z} = \overline{w} + \overline{z}$ e $\overline{w \cdot z} = \overline{w} \cdot \overline{z}$, para todos $w, z \in \mathbb{C}$ (prove isto como exercício).
- $z = \overline{z} \Leftrightarrow z \in \mathbb{R}$.

Tem-se também que $|z|^2 = z \cdot \overline{z}$ (prove-o!).

Duas aplicações geométricas:

(1) Do facto de a conjugação preservar o produto, resulta que $\overline{z^n} = \bar{z}^n$ (porquê?). Em particular, se α é uma raiz n-ésima da unidade, então $\bar{\alpha}^n =$

$\overline{\alpha^n} = \overline{1} = 1$. Donde se conclui que o conjugado de uma raiz n-ésima da unidade é ainda uma raiz n-ésima da unidade. Resulta que o polígono regular cujos vértices são as raízes n-ésimas da unidade, como na Figura 2, é simétrico relativamente ao eixo dos 'x'.

(2) Observe que, dados dois números complexos w e z, $w+z$ e $w-z$ "são" as duas diagonais do paralelogramo formado por w e z (exercício: explique o que se quer aqui dizer, assim como o porquê das aspas). Tem-se que: $|w+z|^2+|w-z|^2 = (w+z)(\overline{w}+\overline{z})+(w-z)(\overline{w}-\overline{z}) = |w|^2+w\overline{z}+z\overline{w}+|z|^2+|w|^2 - w\overline{z} - z\overline{w} + |z|^2 = 2|w|^2 + 2|z|^2$. Fica assim mostrado que a soma dos quadrados das diagonais de um paralelogramo é igual à soma dos quadrados dos seus lados!

BIBLIOGRAFIA

[Ber90] J. L. Berggren, *Episodes in the Mathematics of Medieval Islam*, Springer-Verlag, 1990.

[BJC78] Bento de Jesus Caraça, *Conceitos Fundamentais da Matemática*, Sá da Costa, 1978 (9ª edição) [original de 1941/42].

[Cro87] J. N. Crossley, *The Emergence of Number*, World Scientific, 1987.

[KeU92] M. Kac & S. Ulam, *Mathematics and Logic*, Dover 1992 [original de 1968].

[Esta foi uma obra que teve grande influência na abordagem aqui feita...]