M Gazeta de Matemática

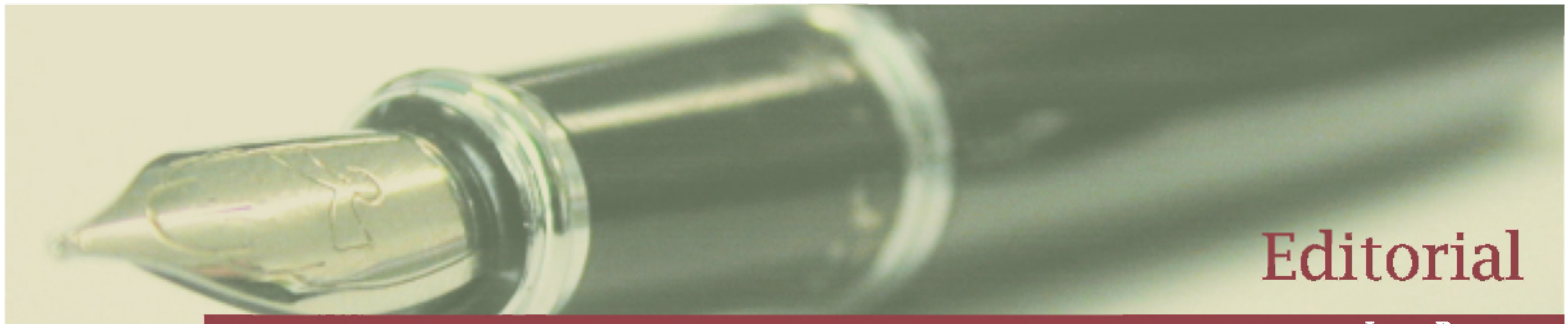
Nº 0154

Publicação quadrimestral
da Sociedade Portuguesa de Matemática
Ano LXIX | Março 2008
4,20€

2007: o ano de Euler

4 | Superstições académicas e Educação Matemática: o caso do Brasil
[Daniel Tausk]

14 | Augusto d'Arzilla Fonseca
[Teresa de Jesus Costa]



Editorial

por **Jorge Buescu**
[Universidade de Lisboa]

"Em poucas palavras: é necessário recolocar a Matemática na posição central... do ensino da Matemática. É urgente a Matemática!"

A *Gazeta de Matemática* tem uma história ilustre, de que nos orgulhamos de ser herdeiros. Foi fundada em 1939 por António Aniceto Monteiro, Bento de Jesus Caraça, Hugo Ribeiro, Silva Paulo e Zaluar Nunes, homens de cultura e visão a quem devemos a fundação da Sociedade Portuguesa de Matemática e também da *Portugaliae Mathematica* – a única revista portuguesa de investigação em matemática.

Infelizmente, por razões históricas bem conhecidas, essa geração que prometia um renascimento científico em Portugal não foi aproveitada pelo país. A *Gazeta* continuou a publicar-se até 1976, tendo sido editados 136 números.

Em 2000, Ano Mundial da Matemática, a *Gazeta de Matemática* renasceu, e desde então se manteve como publicação bianual, em grande parte devido ao esforço titânico e enorme empenhamento pessoal de Graciano de Oliveira. A ele, e a toda a equipa que desde então o acompanhou, em particular Carlota Simões e Maria do Céu Pinto, deve a comunidade matemática o seu reconhecimento por esta ressurreição.

É assim com o peso acrescido da responsabilidade desta herança que a *Gazeta de Matemática* entra numa nova fase da sua vida – com uma nova Direcção, uma nova equipa editorial, e um rumo que tentará honrar dignamente, na semelhança e na diferença, os seus antecessores.

Na semelhança porque, como sempre, o objectivo da *Gazeta de Matemática* é falar de matemática.

Na diferença porque na nossa opinião, hoje mais do que nunca, a *Gazeta* deve conter mais matemática e ser menos *sobre matemática*.

O nosso sistema de ensino, nos últimos trinta anos, foi deslizando por um plano inclinado de facilitismo, de pobreza intelectual, de esvaziamento de conteúdos, de impreparação científica, e o nível de aprendizagem pelos alunos foi consequentemente "caindo, caindo, caindo sempre, na razão directa dos quadrados dos tempos" – para citar um poeta, por sinal extraordinário professor de Ciências: António Gedeão/Rómulo de Carvalho.

Há dez anos os nossos governantes pura e simplesmente negavam, de forma autista, a existência de problemas. Os nossos alunos eram diferentes dos outros – fim de discussão. Entretanto, com as avaliações internacionais independentes como o TIMMS e o PISA e a divulgação dos rankings das escolas, os problemas tornaram-se indisfarçáveis. Estão penosamente visíveis. E não, não têm nada a ver com genética! Têm apenas a ver com o desastre documentado em que o sistema de ensino da matemática se tornou.

Existem hoje, em 2008, diagnósticos realizados. É necessário enriquecer os nossos *curricula* escolares, enriquecer a componente científica da formação de professores, aumentar a exigência com alunos e professores, enriquecer os manuais, ter critérios objectivos de aferição do progresso.

Em poucas palavras: é necessário recolocar a matemática na posição central... do ensino da matemática. É urgente a matemática!

Com a pobreza de conteúdos matemáticos com que vemos os nossos jovens confrontados na escola, e com a tremenda inércia governamental em atacar os problemas, é quase uma obrigação moral levar mais matemática a mais pessoas. Pela nossa parte, esperamos que mais matemática na *Gazeta* possa ajudar a um novo renascimento da matemática em Portugal, desta vez no ensino e na cultura científica.

Como dizia Dias Agudo no artigo inaugural do relançamento, em 2000, da *Gazeta de Matemática*, "Sejamos dignos dos matemáticos portugueses da década de 40"! Os tempos são diferentes, os desafios diferentes. O objectivo é o mesmo.

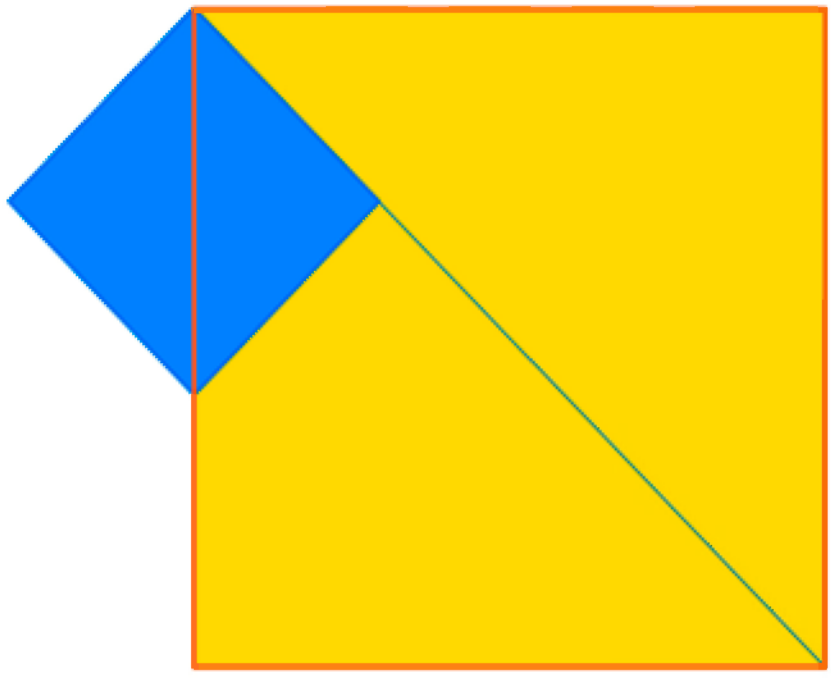
No âmbito de uma colaboração acordada entre a Gazeta e o Atractor, passa a haver com regularidade um espaço da responsabilidade do Atractor sem um formato fixo. Pode, como é o caso deste primeiro número, ser um texto sucinto que remete para algo mais desenvolvido existente no *site* do Atractor (www.atractor.pt), com conteúdos interactivos, pode ser um resumo de vários conteúdos interactivos criados pelo Atractor, eventualmente com uma indicação da sua possível utilização didáctica, etc. Quaisquer reacções ou sugestões serão bem-vindas para atractor@atractor.pt.

Incomensurabilidade

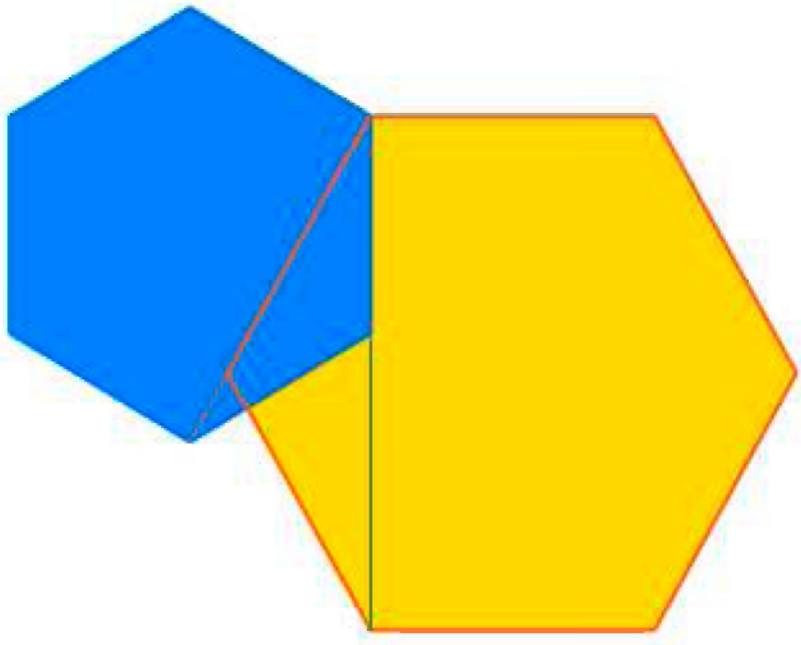
"Pois todos os homens começam por se admirar que as coisas sejam como são, como, por exemplo, com os autómatos, ou os solstícios, ou a incomensurabilidade da diagonal do quadrado com o lado; porque parece espantoso, aos que não conhecem a razão, que exista uma coisa que não possa ser medida mesmo pela unidade mais pequena. Mas acabamos por adoptar a posição oposta que é, como diz o provérbio, a melhor, como é o caso nestes outros exemplos quando se aprende a causa; pois nada surpreenderia mais um geómetra que a diagonal fosse afinal comensurável."

Aristóteles, *Metafísica*

Para medir um segmento usando outro mais pequeno como unidade, a operação a fazer é simples se, ao contarmos quantas vezes a unidade cabe no maior, não sobrar resto. Se sobrar, podemos tomar essa sobra como unidade mais pequena e depois, se necessário, repetir o processo. Se, ao fim de um número finito de passos, não houver sobra, encontrámos uma unidade comum na qual os segmentos iniciais se medem por números inteiros e esses segmentos dizem-se *comensuráveis*. No caso da diagonal de um quadrado e do seu lado, o processo não termina: somos levados a segmentos cada vez mais pequenos, sem encontrar um que sirva. As demonstrações mais divulgadas desta incomensurabilidade são a *geométrica*, no espírito da escola grega, que se atribui aos Pitagóricos e que consta da obra de Platão (e do Livro X de Euclides); e a *aritmética*, que se pensa ser posterior e que, na descrição de Aristóteles (An. Pr. I. 23. 41ª23-7), se resume a um raciocínio por absurdo: *"(…) para deduzir que a diagonal do quadrado é incomensurável com o lado mostra-se, supondo que são quantidades comensuráveis, que há números ímpares iguais a pares"*. A apresentação[1] destes dois argumentos sem o uso de fracções irredutíveis realça um aspecto menos conhecido: que a demonstração



[1] http://www.atractor.pt/mat/mcomensurabilidade

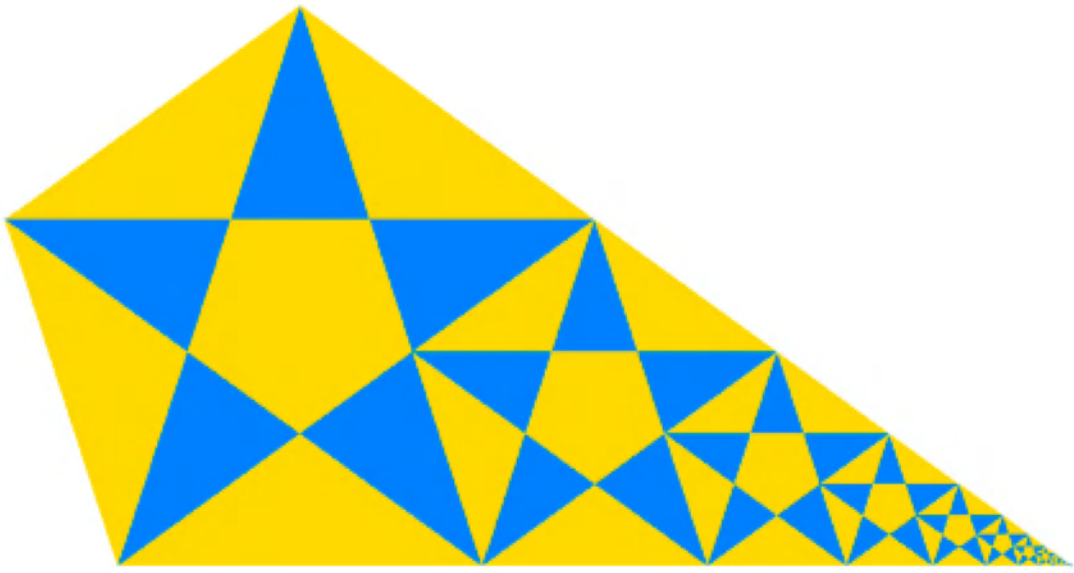


aritmética é exactamente a formulação nesse contexto da estratégia geométrica de prova, sendo o essencial em ambas que uma sucessão decrescente de números naturais é constante a partir de certa ordem.

Se quisermos tentar aplicar o mesmo processo a outros polígonos regulares, como nos de mais de 5 lados, as diagonais não têm todas o mesmo comprimento, há que fazer uma escolha: consideraremos nesse caso as diagonais mais curtas. Então, no caso do pentágono e do hexágono regulares, existem demonstrações geométricas análogas à mencionada para o quadrado, que estabelecem a incomensurabilidade entre a diagonal e o lado.

No entanto, por razões algébricas explicadas no *site*[2], um tal argumento geométrico não pode estender-se a polígonos regulares com mais de 6 lados, apesar de as grandezas serem, também nesse caso, incomensuráveis.

As páginas do *Atractor* que aqui se mencionam contêm uma apresentação interactiva deste assunto e ainda uma interpretação com sistemas dinâmicos do processo de construção de novos polígonos regulares utilizado nas demonstrações de incomensurabilidade por subtracção recíproca. M



[2] http://www.atractor.pt/mat/incomensurabilidade/diagonal.pdf

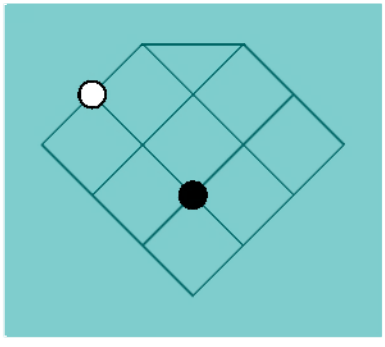
por Jorge Nuno Silva
[Universidade de Lisboa]

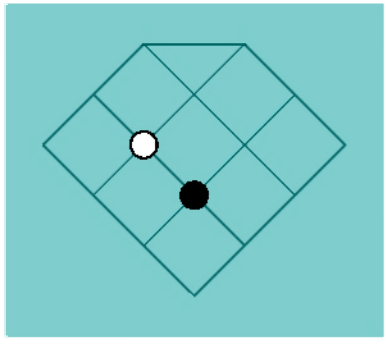
Emoções em Grafópolis

Um grafo é um grafo é um grafo. Mas, em certos mundos, ainda que virtuais, um grafo pode ser outra coisa. Uma caça ao ladrão num recticulado simples pode ter as suas subtilezas e um concurso de dança pode ser muito intelectual...

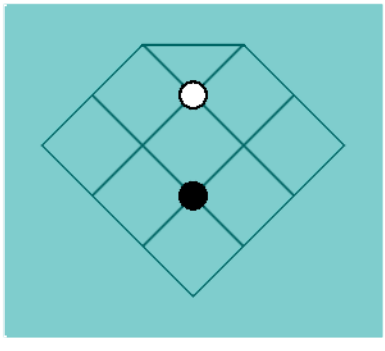
Há muito, muito tempo, numa terra distante, vivia um povo estranho, que construía cidades bizarras. Num bairro de uma delas, um polícia (Ponto Branco) persegue um ladrão (Ponto Negro). As condições locais obrigam a que cada um dê um passo, alternadamente, deslocando-se de uma intersecção para uma outra vizinha.

Vejamos um exemplo de movimentação do agente na sua perseguição do meliante:



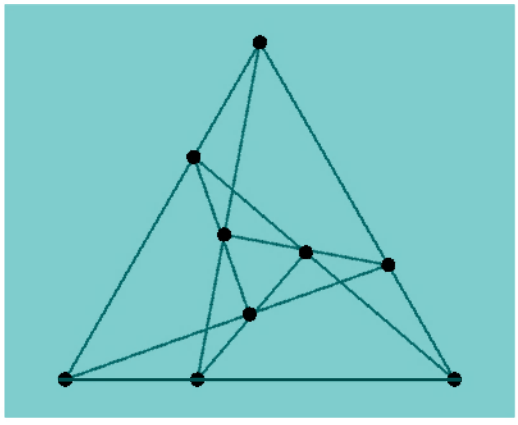


Acontece que, na vida real, a posição inicial, sendo o polícia o próximo a mover-se, é a seguinte:



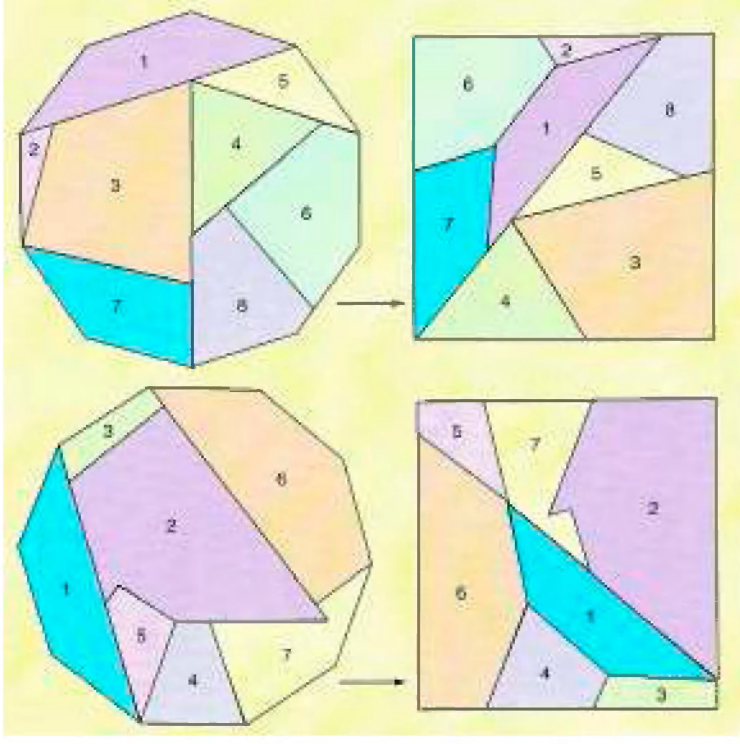
Será que o polícia apanha o ladrão em, no máximo, sete movimentos? Se sim, como? Se não, porquê?

Outra actividade muito popular em Grafópolis é a dança das quadras.
Eis como se processa: cada uma de duas equipas de quatro pessoas coloca um dos seus elementos, alternando a vez, num ponto do seguinte recinto:



A equipa que conseguir colocar três elementos em linha recta ganha a taça em disputa.
Este jogo parece muito complicado, mas há uma equipa que ganha consistentemente todos os jogos em que participa, desde que seja a primeira a jogar. Será que existe mesmo uma estratégia vencedora para a primeira equipa a jogar?

Nota sobre o problema do último número: Eis como transformar um dodecágono regular num quadrado, usando respectivamente oito e sete regiões.



por Pedro Quaresma [Departamento de Matemática, Universidade de Coimbra]
Elsa Lopes [Núcleo de Estágio Pedagógico, Lic. Matemática, F.C.T.U.C., Escola B. 2, 3 c/ Sec. José Falcão, Miranda do Corvo]

Criptografia

Saiba como transmitir informação de forma segura: dos sistemas de chave secreta usados na antiguidade aos actuais sistemas de chave pública.

1 Introdução

A necessidade de proteger os canais de comunicação entre pessoas de uma mesma comunidade vem desde os primórdios da civilização. A ideia de não só proteger os meios de comunicação mas também proteger o próprio conteúdo da mensagem através da cifração é também muito antiga. O imperador romano Júlio César (100 - 44 a.C.) desenvolveu uma cifra simples para poder comunicar com os seus generais: na mensagem original cada letra é *deslocada* três posições para a direita, considerando-se que o alfabeto se fecha sobre si próprio, isto é, que após a última letra vem a primeira; o receptor da mensagem só tem que *deslocar* cada letra três posições para a esquerda para obter a mensagem original.

A cifração de mensagens foi-se tornando um processo cada vez mais sofisticado, passando pelas máquinas Enigma [5] usadas pelo exército alemão aquando da Segunda Guerra Mundial, até aos nossos dias com as transacções electrónicas na Internet. Na actual *Sociedade da Informação*, em que cada vez mais as pessoas comunicam através da Internet, um meio de comunicação muito exposto, a importância da criptografia é enorme. Só através da cifração das comunicações é que podemos garantir a confidencialidade da informação que queremos transmitir.

2 O Surgimento da Criptografia

O surgimento da criptografia (do Grego: kryptós, oculto + graph, r. de graphein, escrever) deve ter sido quase que simultâneo com o da escrita [8]. Os Espartanos, em 400 a.C., desenvolveram um sistema muito curioso: enrolava-se uma tira de couro num bastão, onde se escrevia a mensagem. O acto de desenrolar a tira do bastão cifrava a mensagem, que só poderia ser decifrada tornando a enrolar a tira num bastão de diâmetro semelhante.

Em contraponto com este método puramente mecânico, a cifra de Júlio César implicava um algoritmo de cifração. Um sistema criptográfico é então um conjunto de técnicas que nos permitem tornar incompreensível uma dada mensagem, de modo que só o verdadeiro destinatário da mesma a consiga decifrar, obtendo dessa forma o texto original.

2.1 Sistemas Criptográficos Simétricos

Os primeiros sistemas criptográficos inventados eram do tipo *criptografia simétrica*, ou de *chave secreta*. Sistemas em que existe uma só *chave de cifração*, e em que os processos de cifração e de decifração são simétricos.

No caso do algoritmo de Júlio César estamos perante um algoritmo monoalfabético aditivo, isto é, no processo de cifração só é utilizado um alfabeto, e basta somar ou subtrair três ao código numérico de cada letra do alfabeto.

Qual será o significado da frase?

D FKDYH WHP GH VHU PDQWLGD VHFUHWD

Embora se possam desenvolver sistemas mais sofisticados [8], nomeadamente os métodos polialfabéticos multiplicativos, este tipo de sistema tem sempre dois problemas de base que limitam a sua capacidade de proteger a informação:

a chave de cifração tem de ser do conhecimento de toda a organização *amiga*, e tem de ser mantida secreta de todas as organizações inimigas. Quanto maior for a complexidade da organização *amiga* mais difícil será verificar esta condição;

a despeito de algoritmos mais sofisticados, o estudo das línguas naturais, a sua construção frásica, a frequência relativa das diferentes letras do alfabeto, entre outras características, permitem obter muita informação que pode depois ser usada para quebrar o código de cifração.

2.2 Sistemas Criptográficos Assimétricos

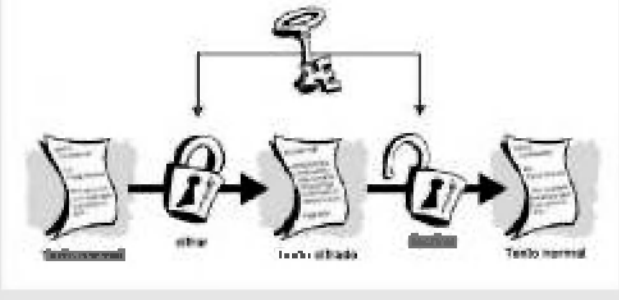
Surgem então em cena os sistemas de *criptografia assimétrica* ou de *chave pública*. Sistemas em que o processo de cifração usa uma *chave pública*, mas em que o processo de decifração usa uma chave diferente, dita *chave privada*.

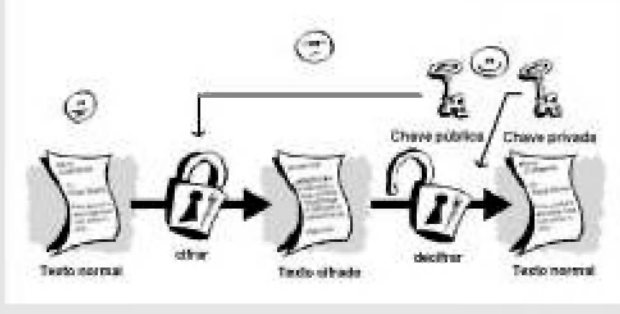
Este tipo de sistema resolve os dois problemas acima expostos:

a chave privada é do conhecimento de uma única entidade, o receptor da mensagem. Mantê-la secreta é assim muito mais fácil;

os algoritmos desenvolvidos são bastante mais complicados de quebrar do que os anteriores.

No que se segue, vamos descrever um dos algoritmos actualmente usados. Esperamos conseguir convencer o leitor da maior dificuldade existente em quebrar um código deste tipo quando em contraponto com os anteriores métodos. Queremos no entanto referir dois pontos: primeiro, as implementações apresentadas usam estruturas de dados simples, comummente encontradas nas linguagens de programação, o que leva a que não seja possível dificultar muito a tarefa do *inimigo*; por outro lado, no exemplo que iremos apresentar mais à frente, a cifração é feita carácter a carácter, o que não é o caso das implementações em uso na Internet, que usam blocos de caracteres como forma de evitar o estudo linguístico da mensagem cifrada.





Esta imagem e a seguinte (adaptadas) foram retiradas do texto (disponível na Internet) *Segurança da Informação: Estratégias para Neutralizar o Inimigo*, de **Francisco Gomes Milagres,** Universidade do Estado de Minas Gerais, Faculdade de Informática de Passos, 21 de Maio de 2003.

3. O Algoritmo RSA

Um sistema assimétrico muito usado na actualidade é o assim designado *sistema de criptografia RSA* [2, 3, 4, 6] que obtém o seu nome das iniciais dos seus três autores. Vamos de seguida descrevê-lo, apresentando uma das suas implementações desenvolvida no sistema de programação numérica *Octave*[1].

Num sistema de criptografia assimétrica é então necessário possuir programas para:

gerar as chaves públicas e privadas (secretas), C_p e C_s;

cifrar as mensagens $A_{C_p} : M \longrightarrow A_{C_p}(M)$;

decifrar as mensagens $A_{C_s} : M \longrightarrow A_{C_s}(M)$;

Para que estejamos perante um sistema de criptografia e não perante um simples sistema de baralhação de mensagens, os programas de cifração e decifração têm de ser funções inversas, isto é, tem de se verificar que:

$$A_{C_s}(A_{C_p}(M)) = M \qquad A_{C_p}(A_{C_s}(M)) = M$$

O sistema RSA vai usar resultados conhecidos da Teoria dos Números para poder assegurar uma grande segurança no processo de decifração, não será de estranhar portanto que surja a necessidade de trabalhar com números primos.

3.1 Geração das Chaves

As chaves pública e privada vão ser constituídas, cada uma delas, por um par de números inteiros, os quais vão depois constituir o âmago dos processos de cifração e decifração.

Começa-se por escolher dois números primos p e q, deles obtêm-se $n = pq$.

De seguida determina-se a função φ de Euler para n, $\varphi(n)$ dá-nos o número de naturais inferiores ou iguais a n e que são primos com n. A função de Euler é uma função de inteiros em inteiros que, entre outras, tem as seguintes propriedades [2,3,4].

Teorema 1 *Se m e n forem dois números naturais, primos entre si, tem-se* $\varphi(mn) = \varphi(m)\varphi(n)$.

Teorema 2 *Um número natural p é primo se e só se* $\varphi(p) = p - 1$

Temos então que $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$, ou seja, o cálculo de $\varphi(n)$ é, dado a escolha de p e q, muito fácil de efectuar.

O próximo passo é o de escolher um natural e, tal que $1 < e < \varphi(n)$ e que seja primo relativo com $\varphi(n)$. O par (e, n) é a chave pública do código RSA.

Para a determinação da chave privada do código RSA é necessário apresentar previamente o conceito de congruência módulo n.

Definição 1 (Congruência módulo *n*) Seja $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}$, então *a e b dizem-se* congruentes módulo n *se tiverem o mesmo resto na divisão por n, denota-se tal facto por* $a = b \pmod{n}$.

Decorre da definição que se $a = b \pmod{n}$ então $a = b + kn$, para um dado $k \in \mathbb{Z}$.

Temos então que, para obter a chave privada da cifra RSA, começar por determinar um natural d que seja o inverso multiplicativo de e, módulo $\varphi(n)$, ou seja, deve-se verificar a seguinte igualdade.

$$d\,e = 1 \pmod{\varphi(n)}$$

O par (d, n) é a chave privada da cifra RSA.

A obtenção dos números primos p e q pode ser feita recorrendo a um dos muitos algoritmos para a obtenção de números primos, por exemplo o *Crivo de Eratóstenes* [7, pag. 278].

O algoritmo para a criação das chaves é o seguinte:

```
##Determinação das Chaves Pública e Privada:
##
## -> p,q dois números primos.
## <- (e,n) e (d,n), as chaves públicas e privadas.
function chaves(p, q)
  n = p*q;
  fi = (p-1)*(q-1);
  e = 2;
  k = 0;
  do
    e = e+1;
  until (gcd(fi,e) == 1)
  achou = false;
  while (!achou)
    d = (1 + (k * fi))/e;
    if ( d == round(d))
      achou = true;
    else
      k = k+1;
    endif
  endwhile
  printf("\n A chave pública é (%d,%d).\n", e, n);
  printf("\n A chave privada é (%d,%d).\n\n", d, n);
endfunction
```

[1] Octave, www.octave.org, é um sistema de programação numérica de distribuição gratuita, compatível com o *MatLab*.

Para os valores de $p = 11$ e $q = 23$ ter-se-ia:

octave > chaves (11,23).
A chave pública (3, 253).
A chave privada (147, 253).

O Algoritmo de cifração RSA é:

$$C = A_{C_p}(M) = M^e \pmod{n}$$

e o algoritmo de decifração é:

$$M = A_{C_s}(C) = C^d \pmod{n}$$

Nesta nossa implementação simplificada do algoritmo RSA, em Octave, tanto a função de cifração como a função de decifração lidam com inteiros. A mensagem é primeiro convertida de um vector de caracteres num vector de naturais, de seguida cifrada ou decifrada consoante os casos e, finalmente, convertida de novo num vector de caracteres[2].

```
##Cifrar a Mensagem Digital Original:
##
## -> (e,n), chave pública
##    m, mensagem a cifrar (vector de inteiros)
## <- x, mensagem cifrada (vector de inteiros)
function x=cifrar(e, n, m)
  t=columns(m);
  for i=1:t
    x(i) = mod((m(i))^e, n);
  endfor
endfunction

##Decifrar a Mensagem Cifrada:
##
## -> (d,n), chave pública
##    c, mensagem a decifrar (vector de inteiros)
## <- modl, mensagem decifrada (vector de inteiros)
function modl = decifrar(d, n, c)
  t=columns(c);
  for i=1:t
    modl(i) = 1;
    j=1;
    while (j <= d)
      modl(i) = mod((c(i))*modl(i), n);
      j = j+1;
    endwhile
  endfor
endfunction
```

3.2 Validação do Sistema RSA

Como já dissemos antes é necessário verificar se estamos perante um sistema de criptografia válido, isto é, temos que verificar que:

$$A_{C_s}(A_{C_p}(M)) = A_{C_p}(A_{C_s}(M)) = M^{ed} \pmod{n} = M$$

Para o desenvolvimento da demonstração são necessários alguns resultados auxiliares [2, 3, 4].

Teorema 3 (Pequeno Teorema de Fermat) *Se n é um número primo, então $a^{n-1} = 1 \pmod{n}$, para todo o $a \in Z$ tal que mdc (a, n)=1*

Teorema 4 (Teorema chinês dos restos)
Sejam $m_1, m_2, \ldots, m_k \in \mathbb{N}$ primos dois a dois e $a_1, a_2, \ldots, a_k \in \mathbb{Z}$. O sistema:

$$\begin{cases} x = a_1 \pmod{m_1} \\ \vdots \\ x = a_k \pmod{m_k} \end{cases}$$

Tem uma solução simultânea x para todas as congruências, e cada duas soluções são congruentes módulos $m = m_1 m_2 \ldots m_k$.

Teorema 5 (Sistema de Criptografia RSA) *Sendo (e,n) e (d,n) as chaves pública e privada respectivamente do sistema de criptográfia RSA verifica-se então que:*

$$(m^e)^d \pmod{n} = m$$

para qualquer inteiro m, com $0 < m < n$

Demonstração
Da definição de e e d tira-se que $ed = 1 \pmod{\varphi(n)}$ existe então um $k \in Z$ tal que $ed = 1 + k\varphi(n)$, ou seja:
$ed = 1 + k(p-1)(q-1)$, $k \in Z$
donde:

$$(m^e)^d = m^{ed} = m^{1+k(p-1)(q-1)} = mm^{(p-1)(q-1)k}$$

segue-se que:

$$(m^e)^d = m(m^{(p-1)})^{(q-1)k} = m(\text{mod } p)$$

Se p não é um divisor de m esta congruência é uma consequência do Pequeno Teorema de Fermat. Caso contrário a asserção é trivial dado que ambos os membros da equação são congruentes com 0 mod p.
De forma análoga ter-se-ia que:

$$(m^e)^d = m \pmod{q}$$

Dado que p e q são números primos distintos podemos aplicar o Teorema chinês dos restos, e dado que se assume que $0 < m < n$, obtém-se

$$(m^e)^d = m(\text{mod } pq) = m(\text{mod } n) = m$$

q.e.d.

[2] O programa Octave contendo todas as funções referidas no texto pode ser obtido em http://www.mat.uc.pt/~pedro/cientificos/Cripto/

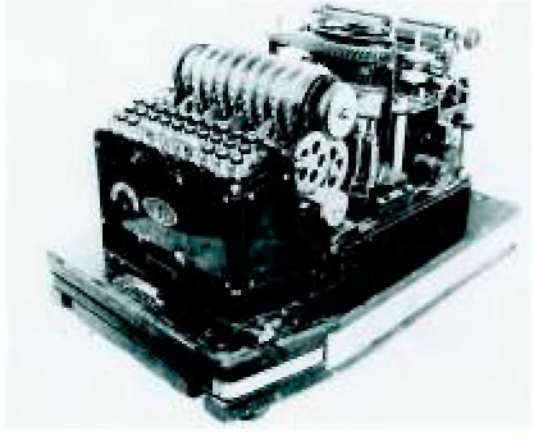
3.3 Como «Quebrar» o Código RSA

Por quebrar um código entende-se o acto de conseguir decifrar a mensagem sem que se tenha um prévio conhecimento da chave secreta. Para quebrar o código RSA basta descobrir o d, que poderá ser obtido de e, de p e de q. O e pertence à chave pública, o p, e o q são factores primos de n, que é o outro elemento da chave pública. Ou seja, para quebrar um sistema deste tipo basta factorizar n.
O problema reside então na factorização em números primos de um dado número natural n. Para valores de n suficientemente grandes esta tarefa é impraticável, mas isso é tema para um outro artigo, até lá deixamos ao leitor da *Gazeta de Matemática* algumas pistas [1, 2, 3, 4] e um pequeno desafio.

```
359394 185904 0 231105 382481 474195 382481 10935 75745 382481
185904 0 201637 382481 302441 522545 270765 382481 185904 0 185904
382481 265174 79985 0 365807 292080 66056 261188 75745 382481 371293
60839 185904 185904 265174 185904 0 90175 75745 75745 382481 185904
270765 522545 10935 66056 474195
```

Sabendo que se usaram os algoritmos descritos acima, com uma cifração letra a letra (caracteres *ASCII* entre ' ' e '~' que correspondem a, ' ' =0, '!'=1, ...) e a nossa chave pública é (5,561971).

Sistema com encriptação RSA.



Máquina Enigma.

Referências

[1] **D. Atkins, M. Graff, A. Lenstra, e P. Leyland**. The magic words are squeamish ossifrage. In *ASIACRYPT: 1994*, pages 263–277, 1994.

[2] **Douglas R. Stinson**, *Cryptography, Theory and Practice*, 3rd Ed., Chapman & Hall/CRC, Boca Raton, 2006.

[3] **Johannes Buchmann**. *Introduction to Cryptography*. Springer-Verlag, New York, 2000.

[4] **Neal Koblitz**, *A Course in Number Theory and Cryptography*, 2nd Ed., Springer, New York, 1994.

[5] **António Machiavelo**. *O que vem à rede... Gazeta de Matemática*, (147): 14-15, Julho 2004.

[6] **R. Rivest, A. Shamir, e L. Adleman**. *A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM*, 21(2): 120-126, 1978.

[7] **Pimenta Rodrigues, Pedro Pereira, e Manuela Sousa**. *Programação em C++*. FCA Editora de Informática Lda, 2ª edição, 1998.

[8] **Richard Spillman**. *Classical and Contemporary Cryptology*. Prentice-Hall, 2005.

por Fabio Chalub
[Universidade Nova de Lisboa]

O Atlas da Matemática

Um computador pode ajudar a compreendermos a matemática? A classificação do grupo de Lie simples $E(8)$ mostra que sim! Mas para chegar a esta conclusão foi necessário o desenvolvimento de novos algoritmos para resolver um problema antigo. Conheça um pouco desta história.

Atlas é o nome de um dos Titãs, que ao perder a batalha contra os deuses do Olímpio foi condenado pelo próprio Zeus a carregar os céus sobre os seus ombros. Isto deu-lhe tanto conhecimento sobre a Terra que o seu nome hoje é mais associado às artes da Cartografia (ou seja, do desenho de mapas) do que à própria deidade grega.

Em matemática, a palavra atlas também tem o seu significado. Afinal, as estruturas geométricas são compreendidas a partir de "cartas", pequenos mapas que fazem corresponder a estrutura euclidiana aos espaços não euclidianos. O conjunto destas cartas constitui um atlas, que descreve completamente as superfícies, ou de forma mais geral, as "variedades riemannianas".

Portanto, quando um grupo de matemáticos resolveu mapear todos os grupos de Lie simples, não foi nenhuma surpresa chamar ao projecto "Atlas dos grupos de Lie e de suas representações"[1]. Mas o que é isto?

Um grupo é um conjunto de elementos com uma operação (chamada "produto") tal que, dados dois elementos, o seu produto esteja no conjunto e exista um elemento ("identidade") cujo produto com qualquer outro elemento dê como resultado o outro elemento. Além disto esta operação é associativa (ou seja, podemos colocar parêntesis em qualquer lugar, de forma indistinta) e para cada elemento existe um "inverso", ou seja, alguém que multiplicado pelo elemento original tem como resultado a identidade.

Estas quatro hipóteses são chamadas "axiomas de grupo". Alguns exemplos de grupo são os números naturais (ou racionais, ou reais) com a operação de soma; os números reais, excepto o zero, com a multiplicação; ou ainda as matrizes invertíveis com a multiplicação. Veja que aquilo a que chamamos "produto" no parágrafo acima pode ser qualquer operação matemática que transforme dois elementos num único, e que tem que ser dita explicitamente sempre que queremos definir um grupo.

Para termos um grupo de Lie (em homenagem ao matemático Norueguês do século XIX, Sophus Lie)

Sophus Lie.

[1] http://www.liegroups.org

devemos além disto considerar que estas operações são contínuas (ou seja, pequenas variações dos elementos de quem tomamos o produto terão um pequeno efeito no resultado da operação; o mesmo para a inversão). Um grupo de Lie é um objecto matemático, em geral fácil de ser estudado. Isto decorre pelo facto de estes (bom, pelo menos os "conexos", mas não entraremos neste detalhe) serem totalmente determinados pela sua álgebra de Lie.

Uma álgebra é um objecto muito mais simples do que um grupo pois tem muito mais operações permitidas. Mais exactamente, uma álgebra é um conjunto com duas operações que normalmente chamamos de "soma" e "multiplicação", pois são muito similares à soma e multiplicação usuais das matrizes. Aliás, as matrizes são o melhor exemplo das álgebras de Lie. Portanto basta estudarmos as matrizes para bem compreendermos os grupos de Lie.

E assim foi feito. Em 1887, Wilhelm Killing, um matemático alemão, completou a classificação dos grupos de Lie simples (um grupo é simples quando não possui subgrupos de um tipo chamado "normal"). Encontrou quatro famílias infinitas, chamadas grupos de Lie clássicos: $A(n)$, as matrizes complexas n por n de determinante 1; $B(n)$, as matrizes reais $2n+1$ por $2n+1$ com determinante 1; $C(n)$ as matrizes quaterniónicas n por n que preservam o produto interno simpléctico e $D(n)$ as matrizes reais $2n$ por $2n$ com determinante 1. Com a excepção do grupo $C(n)$, todos os outros exemplos aparecem no dia-a-dia. No entanto, o caso $C(n)$ é tratado da mesma forma que todos os outros. Apenas não é um objecto ao qual estejamos habituados.

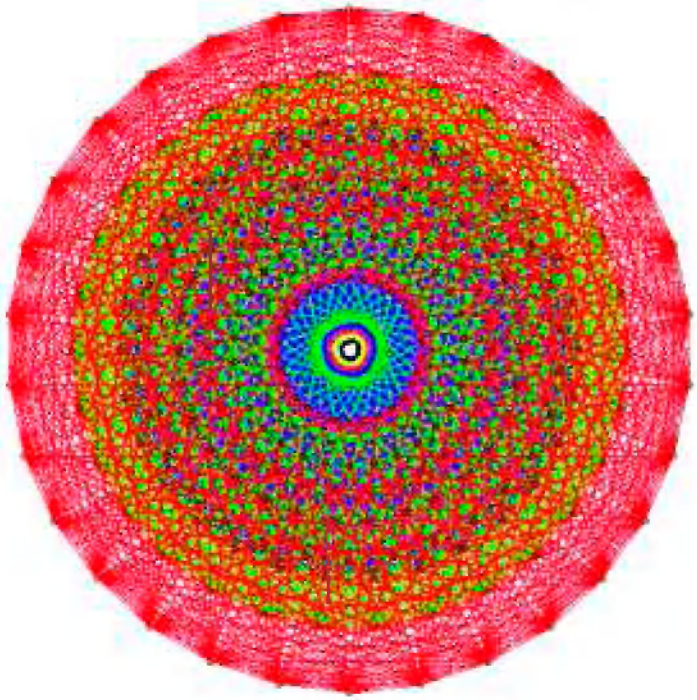
Killing também encontrou alguns exemplos que não encaixavam nesta classificação. São os chamados grupos de Lie excepcionais, $G(2)$, $F(4)$, $E(6)$, $E(7)$ e $E(8)$. Apesar do nome, não há nada de realmente excepcional nestes. Apenas a classificação usual (que leva em consideração as simetrias do espaço euclidiano) coloca-os à parte, sem formar toda uma família de dimensões crescentes. No entanto, nada há de diferente entre estes e qualquer um daqueles do parágrafo anterior tomados isoladamente.

Como cada um destes grupos é determinado por uma álgebra e dado que uma álgebra é um objecto simples, então é possível compreendê-los (mesmos os excepcionais) a partir do estudo de matrizes. Aliás, de um número finito de matrizes (para cada caso). Estas matrizes, por sua vez, são obtidas a partir de um polinómio. Desta forma o objectivo do projecto Atlas é obter o polinómio mais simples possível que permita compreender cada grupo de Lie.

Finalmente, a 8 de Janeiro de 2007, o grupo Atlas, usando computadores, obteve o polinómio de grau 22 que caracteriza o grupo $E(8)$.

Mas porquê isto tudo? Os grupos de Lie sempre tiveram muitas aplicações, sobretudo em Física. O grupo de Heisenberg da mecânica quântica, assim como os grupos de Lorentz e Poincaré da relatividade são exemplos de grupos de Lie. E para quem tem conhecimentos de mecânica clássica não é difícil ver a importância dos grupos clássicos obtidos acima. Mesmo os grupos excepcionais têm importância crescente na física teórica (sobretudo partículas e altas energias).

Uma visão mais técnica do projecto Atlas, não contemplando todos os níveis de detalhe, pode ser obtida na referência[2]. M



Representação do grupo $E(8)$, projectado de 8 para 2 dimensões.
Imagem de John Stembridge, baseada num desenho de Peter McMullen.

[2]David Vogan, "The Character Table for *E8*", *Notices of the Amer. Math. Soc.* volume 54(9), p 1022-1034 (2007).

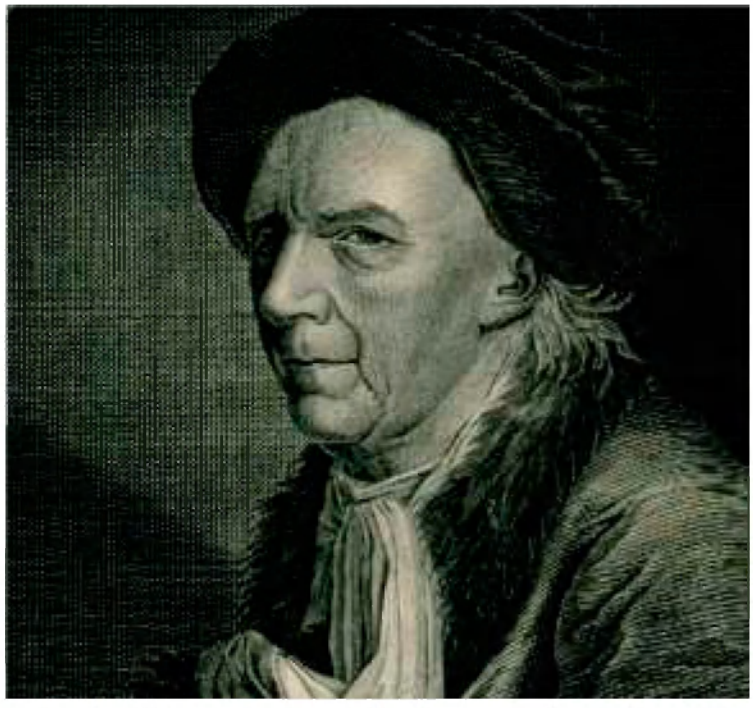
por António Machiavelo
[Departamento de Matemática Pura da Faculdade de Ciências da Universidade do Porto]

Celebrando Euler

Na sua adolescência, Leonhard Euler desfrutou de condições excepcionais. As influências do pai, do tutor e do grande matemático Johan Bernoulli foram fundamentais para que se tornasse um dos maiores matemáticos de sempre.

No ano que há pouco terminou, celebrou-se o tricentésimo aniversário de um dos mais fecundos e criativos matemáticos de todos os tempos: Leonardo Euler (1707-1783). A quantidade e diversidade absolutamente espantosa de trabalhos que escreveu, ultrapassando os 850 artigos e mais de uma vintena de livros, fazem de Euler um dos mais produtivos matemáticos de todos os tempos. De tal modo que a edição da sua obra completa não tem sido tarefa fácil. Foi iniciada em 1907 e, resultado de várias vicissitudes e da complexidade do trabalho, ainda não foi terminada! Duas das pessoas actualmente envolvidas nessa tarefa, Andreas Kleinert e Martin Mattmüller, relatam a história desse esforço hercúleo, os actuais obstáculos e o que esperar num futuro próximo, no artigo "Leonhardi Euleri Opera Omnia: a centenary project", publicado na Newsletter da EMS (European Mathematical Society) de Setembro de 2007, e disponível em: *http://www.ems-ph.org/newsletter/news.php* e também em: *www.euler-2007.ch/doc/EMS70965.pdf*.

É muito fácil encontrar biografias de Euler na Internet, embora nem todas, obviamente, tenham a mesma qualidade. Em 2006, a editora Birkhauser publicou uma tradução inglesa da excelente biografia *Leonhard Euler*, originalmente escrita em alemão em 1995, da autoria de Emil Fellmann, historiador de ciência. O primeiro capítulo pode ser encontrado na Internet, em[1]: *http://www.springerlink.com/content/t22713u184507u6p/* e inclui, logo no início, uma autobiografia (necessariamente incompleta) que Euler ditou, a 1 de Dezembro de 1767, a um dos seus filhos. É uma biografia cuidada, das poucas que deixa claro que o facto deste ter entrado para a universidade com 13 anos não tem nada de extraordinário em si mesmo, sendo o habitual da época (para quem tinha essa sorte). Fica também clara a influência do pai, que teve aulas com o grande matemático Jacob Bernoulli nos seus anos de universidade, antes de se dedicar à teologia; de Johannes

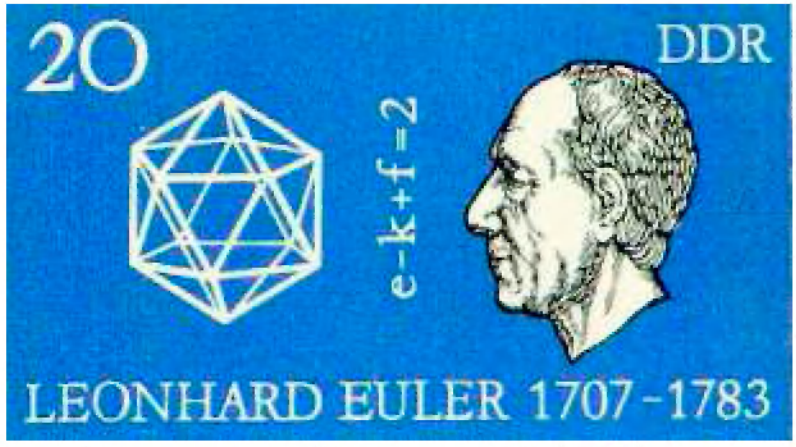


Leonhard Euler aos 71 anos, pintado pelo dinamarquês nascido na Alemanha Joseph Friedrich August Darbes (1747 – 1810).

[1] Que possivelmente pode apenas ser acedido numa universidade com acesso especial à base de dados SpringerLink.

Burckhardt, um tutor privado que o pai contratou para ensinar o jovem Euler, e que era um entusiasta da matemática; assim como o papel crucial de Johann Bernoulli na educação matemática deste. Sem dúvida um conjunto de condições excepcionais de que Euler soube tirar todo o proveito.

A Mathematical Association of America tem há já algum tempo uma rubrica intitulada "How Euler Did It", da autoria de Ed Sandifer, da Western Connecticut State University, onde, como o título indica, são expostos alguns dos resultados de Euler e o modo como este os obteve. São artigos bem interessantes e estão disponíveis em: *http://www.maa.org/news/howeulerdidit.html*



Selo comemorativo dos 200 anos da morte de Leonhard Euler. República Democrática da Alemanha, 1983.

De entre os muitos resultados de Euler (qualquer tentativa de sumariar as contribuições de Euler necessitaria de muitas páginas), limito-me aqui a apresentar um dos meus favoritos. É sem dúvida um dos seus resultados mais curiosos, e demonstra bem a criatividade e o domínio magistral sobre somas e produtos formais infinitos do seu autor. Trata-se do resultado principal dos artigos[2] "Découverte d'une loi tout extraordinaire des nombres, par rapport à la somme de leurs diviseurs", publicado em 1747, "Observatio de summis divisorum" e "Demonstratio theorematis circa ordinem in summis divisorum observatum", ambos publicados em 1760. Nestes trabalhos, Euler expõe uma relação de recorrência que encontrou entre a sequência formada pelas somas dos divisores dos números naturais, cujos primeiros elementos são:

$$1,3,4,7,6,12,8,15,13,18,12,28,14,24,24,31,18,\ldots$$

Consegue o leitor discernir aqui algum padrão?... Bom, designando a soma de todos os divisores de n por $\int n$, por exemplo $\int 10 = 1+2+5+10 = 18$, Euler mostra que:

$$\int n = \int (n-1) + \int (n-2) - \int (n-5) - \int (n-7) + \int (n-12) + \int (n-15) - \int (n-22) - \int (n-26), + \cdots$$

sendo $\int (n-k) = 0$ se $k > n$ e $\int (n-n) = n$, e onde a sequência dos números que nela aparecem,

$$1,2,5,7,2,15,22,26,35,40,51,57,70,77,92,100,117,126,145,155,\ldots$$

é tal que, acrescentado um zero no início, a sequência das suas diferenças:

$$1,1,3,2,5,3,7,4,9,5,11,6,13,7,15,8,17,9,19,10,\ldots$$

é formada alternando a sequência dos números ímpares com a dos números naturais.

Como é que Euler descobriu esta relação profunda? De um modo verdadeiramente genial! Por um lado, brincando com produtos infinitos Euler observou que se tem:

$$(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)(1-x^7)\cdots =$$
$$= 1-x-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-x^{35}-x^{40}+\cdots.$$

[2] Descoberta de uma lei extraordinária dos números, relativamente à soma dos seus divisores; Uma observação sobre a soma dos divisores; Demonstração de um teorema sobre a ordem observada nas somas dos divisores; os artigos E175, E243 e E244, respectivamente, do índice de Enestrom, um inventário dos trabalhos de Euler feito no início do século XX pelo matemático sueco Gustav Enestrom.

Por outro lado, Euler observa que a série (como expressão formal):

$$z = \int 1 \cdot x + \int 2 \cdot x^2 + \int 3 \cdot x^3 + \int 4 \cdot x^4 + \int 5 \cdot x^5 + \cdots$$

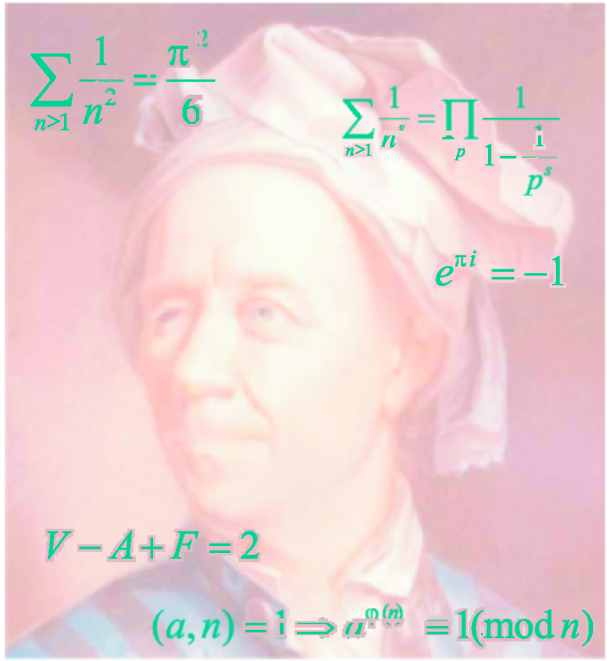
se pode escrever do seguinte modo:

$$\begin{aligned} z = {} & 1\left(x + x^2 + x^3 + x^4 + x^5 + \cdots\right) + 2\left(x^2 + x^4 + x^6 + x^8 + x^{10} + \cdots\right) \\ & + 3\left(x^3 + x^6 + x^9 + x^{12} + x^{15} + \cdots\right) + 4\left(x^4 + x^8 + x^{12} + x^{16} + x^{20} + \cdots\right) \\ & + 5\left(x^5 + x^{10} + x^{15} + x^{20} + x^{25} + \cdots\right) + \cdots \end{aligned}$$

Soma então as séries geométricas entre parêntesis e executa a seguinte sequência de manipulações (para quem sabe o que os termos seguintes significam): primitiva, o que faz aparecer a função logaritmo; usando o facto de esta converter somas em produtos, observa que aparece o produto infinito atrás referido (talvez tenha sido isto que o levou a estudá-lo); usa o resultado que obteve para esse produto e deriva; uma multiplicação formal final com as expressões que obtém conduz ao resultado anunciado[3].

Para mais detalhes não há nada como seguir o preceito do famoso matemático norueguês Niels Abel (1802-1829), de "estudar os mestres, e não os seus alunos", e ler os originais. Uma tradução destes artigos do latim para a língua inglesa, assim como de vários outros, pode ser encontrada no *Euler Archive* em: *http://www.eulerarchive.org* e são ainda hoje, mais de dois séculos passados, fascinantes de ler! Polya, que dedica o capítulo VI do seu livro *Mathematics and Plausible Reasoning*[4] a este resultado de Euler, aí incluindo uma tradução para inglês do artigo E175, explica porquê: "[...] Euler parece-me quase único num aspecto: o seu esforço para apresentar cuidadosamente fundamentos indutivos relevantes, em detalhe e ordenadamente. Apresenta-a de um modo convincente mas honestamente, como um cientista genuíno o deve fazer. A sua apresentação é a «exposição honesta das ideias que o conduziram a essas descobertas» e tem um charme distinto".

No último parágrafo do artigo da Newsletter da EMS acima mencionado, é anunciado que o Comité Euler está presentemente a trabalhar num projecto que visa disponibilizar toda a obra de Euler na Internet. O *Euler Archive* contém já[5], digitalizados, 96.3% dos trabalhos publicados de Euler e traduções de 85 artigos. Não há melhor forma de celebrar este mestre intemporal! Esperemos que no presente século toda a obra deste impressionante e fértil trabalhador intelectual fique disponível na Internet, acessível a todos os que queiram penetrar no mundo fascinante deste notável matemático a quem Johann Bernoulli, que, diga-se, não era nada dado a elogios, se referiu como "de longe o mais astuto dos matemáticos" e "o incomparável Leonardo Euler, o príncipe entre os matemáticos". M



Alguns resultados descobertos por Euler, sobre um seu retrato feito por Emanuel Handmann.

[3] Para os entendidos, todas estas manipulações são justificáveis por o conjunto das séries formais com coeficientes racionais, Q[[x]], ter uma estrutura natural de anel topológico comutativo, com $\lim_{n\to\infty} x^n = 0$, com operadores de diferenciação e primitivação que são contínuos. Obviamente, Euler não trabalha neste contexto, mas o que faz está absolutamente correcto!

[4] Princeton University Press, 1954.

[5] Em 7/11/2007.

Apologia de um Matemático - G. H. Hardy

Recensão por **José Carlos Santos**
[Universidade do Porto]

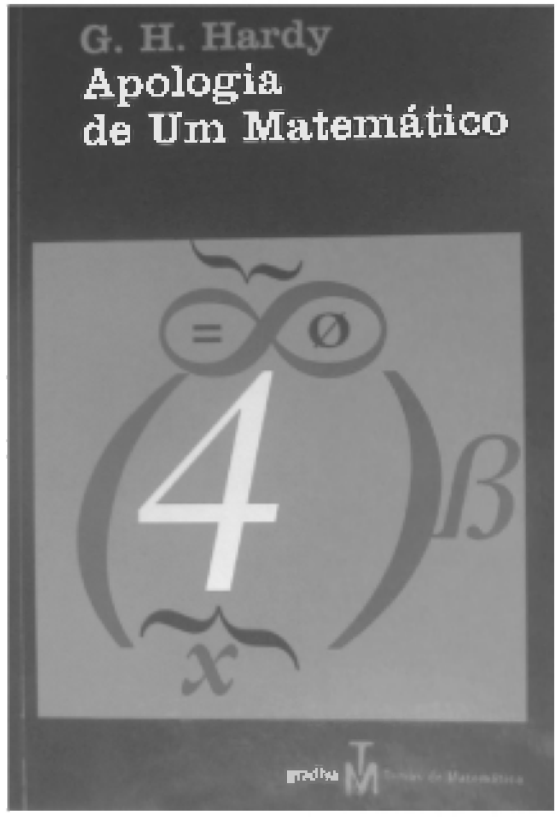
Escrito há quase setenta anos, a *Apologia de um Matemático* de G. H. Hardy ainda hoje merece ser lida. Trata-se de um livro de divulgação Matemática que retrata, sobretudo, a actividade de um matemático. Hardy encara a estética como um valor fulcral e traça uma panorâmica muito interessante da comunidade matemática britânica do período entre as duas guerras mundiais. Os pontos de vista idiossincráticos do autor não deixam ninguém indiferente.

A *Apologia de um Matemático* é a tradução para português do livro *A Mathematician's Apology*, de Godfrey Harold Hardy (1877–1947), originalmente publicado em 1940. Não é vulgar que se traduzam livros sobre matemática com mais de meio século, mas a opção de o fazer justifica-se plenamente neste caso.

G. H. Hardy foi um matemático notável e muito influente na comunidade matemática britânica do seu tempo. Esta estava, no fim do século XIX, bastante isolada do continente europeu, apesar de ter produzido matemáticos de renome, tais como, por exemplo, Arthur Cayley (1821–1895) ou James Joseph Sylvester (1814–1897). Um evento que mostra até que ponto ia tal isolamento foi o prémio proposto pela Academia das Ciências de Paris em 1881 para a determinação do número de maneiras de representar um número inteiro como soma de cinco quadrados. Acontece que tal problema já fora resolvido em 1867 pelo matemático inglês Henry Smith (1826–1883)! Hardy dedicou-se sobretudo à Análise, que era um ramo da Matemática particularmente pouco cultivado em Cambridge, onde se licenciou e foi professor no início e no fim da sua carreira (foi professor em Oxford de 1919 a 1931). Daí ter escrito um livro de Análise, com o título não ortodoxo *A Course in Pure Mathematics*, num estilo que o seu colega e colaborador J. E. Littlewood (1885–1977) descreveria mais tarde como sendo *como um missionário a falar aos canibais*.

Hardy foi um matemático bastante activo e também notavelmente gregário, o que se reflecte no facto de uma grande proporção dos seus artigos ter sido escrita em colaboração. Parte da sua actividade consistiu em tentar elevar o nível da pesquisa matemática no Reino Unido.

A *Apologia de um Matemático* foi publicada quando a criatividade do seu autor já diminuíra bastante e ele começara a ter problemas de saúde (sofrera uma trombose coronária no ano anterior). Neste livro, Hardy explica aos seus leitores qual é a



natureza da matemática e em que consiste a actividade de um matemático. Não se trata de maneira nenhuma de uma abordagem sociológica ou histórica destes assuntos. Hardy dá a sua visão pessoal destes tópicos e não o ponto de vista da comunidade matemática do seu tempo ou a evolução histórica de tais pontos de vista.

E qual é a visão pessoal de Hardy? Vejamos alguns aspectos dela. A defesa da *matemática pura* é talvez o aspecto deste livro que é mais frequentemente referido. Para Hardy, todo o valor de um resultado matemático é interno à própria matemática, ou seja, é independente das suas eventuais aplicações. Ou, nas palavras de Hardy, "*não é possível justificar a vida de qualquer matemático profissional genuíno com base na 'utilidade' do seu trabalho.*" E como se determina o valor de um trabalho matemático? Parte da resposta está contida numa das frases mais citadas do livro:

"*A beleza é o primeiro teste: não há lugar perene no mundo para matemática feia.*"

Hardy deixa claro que é bastante difícil quer definir exactamente o que torna um teorema importante, quer definir a beleza matemática da citação anterior, mas tenta, através de exemplos concretos, transmitir ao leitor a sua percepção relativa a estes tópicos. Os exemplos (a irracionalidade da raiz quadrada de 2, por exemplo) são escolhidos de maneira a poderem ser compreendidos pelo maior número possível de leitores. Um dos pontos fortes do livro reside precisamente no modo cuidadoso, mas também apaixonado, como Hardy transmite o valor estético dos teoremas que aborda.

É muitas vezes referida esta visão de Hardy da inutilidade da matemática pura e do baixo apreço que tem pelas suas aplicações. No entanto deve realçar-se que Hardy tem esta visão não só da matemática mas, mais geralmente, da actividade científica em geral. Por exemplo, ele escreve:

"*É [...] espantoso verificar o escasso valor prático que o conhecimento científico tem para as pessoas comuns, o carácter enfadonho e banal do que o tem, e como o seu valor parece variar em proporção inversa à da sua suposta utilidade.*"

E, relativamente ao seu próprio trabalho, afirma:

"*Nunca fiz nada de «útil». Nenhuma descoberta minha fez, ou é susceptível de vir a fazer, directa ou indirectamente, para o bem ou para o mal, a menor diferença para a amenidade do mundo.*"

Esta visão da utilidade da ciência, centrada na sua aplicabilidade a questões práticas da vida corrente, é bastante restritiva, para além de ser bastante menos defensável hoje em dia do que no tempo de Hardy. De facto, muitos ramos da ciência que pareciam, antes da Segunda Guerra Mundial, serem exemplos de ciência pura desligada de

quaisquer aplicações, têm muitas aplicações hoje em dia. Um exemplo, entre muitos, é a teoria geral de relatividade. Ainda é vista geralmente, mesmo por pessoas cultas e interessadas por assuntos científicos, como sendo algo totalmente desligado da

realidade do dia-a-dia. Mas o facto é que o sistema de posicionamento GPS exige, na sua planificação, que se entre em conta com aquela teoria embora, obviamente, o utilizador comum daquele sistema não tenha, nem precise de ter, conhecimento desse facto. Ora, ironicamente, Hardy descreve a relatividade e a mecânica quântica como "*disciplinas [que] são presentemente [...] quase tão inúteis como a teoria dos números* (acrescentando que *[o] tempo poderá vir a alterar tudo isto)*" e escreve também que "*até hoje ninguém descobriu qualquer propósito bélico que pudesse ser satisfeito por intermédio da teoria dos números ou da relatividade.*" Mas ainda antes da morte de Hardy o mundo pôde ver que a teoria da relatividade podia servir para propósitos bélicos; as primeiras bombas atómicas explodiram em 1945. A propósito disto, convém notar que Hardy era um pacifista radical e que escreveu este livro em plena Segunda Guerra Mundial, algo que se reflecte em várias passagens.

É interessante contrastar a visão que Hardy tinha da utilidade das suas descobertas com o facto de ter feito uma contribuição para a genética: a lei de Hardy-Winberg, sobre a distribuição de alelos (que são as formas que um mesmo gene pode apresentar) numa população. Tudo indica que ele não a considerava útil. Tal como muitas outras descobertas científicas, não é útil para a vida corrente da generalidade das pessoas, mas é certamente útil para o estudo genético de populações. Além disso, Hardy trabalhou em teoria dos números (é co-autor de um dos livros mais conhecidos sobre esta área, *An Introduction to the Theory of Numbers*) que, como foi visto acima, Hardy considerava particularmente «*inútil.*» Mas hoje em dia a teoria dos números está na base da criptografia.

Outro aspecto marcante do livro é a melancolia suscitada pelo declínio das capacidades mentais do autor. Isto manifesta-se logo desde o início do livro, quando Hardy declara que a função de um matemático consiste em criar novos teoremas e não em falar daquilo que faz ou do que outros matemáticos têm feito. E explica porque é que o faz:

"*Escrevo sobre matemática porque, como qualquer matemático que passou a casa dos sessenta, já não disponho da frescura de espírito nem da energia ou paciência para me dedicar efectivamente ao meu verdadeiro trabalho.*"

É naturalmente discutível se o trabalho de um matemático deve ou não consistir somente (ou principalmente) na criação de teoremas. Certamente que poucos hoje concordarão com Hardy quando este afirma que "*[a] exposição, a crítica, a apreciação são obra para espíritos de segunda categoria.*" Mas é precisamente pelo facto de ser esta a opinião de Hardy que o texto é particularmente pungente na sua descrição da consciência da perda de capacidades mentais do seu autor.

Um aspecto da actividade de um matemático sobre o qual Hardy discorre é o da colaboração com outros matemáticos. Não poderia deixar de o fazer, pois a sua carreira foi marcada pelas extraordinárias colaborações com Littlewood e com Srinivasa Ramanujan (1887–1920). A primeira é talvez a mais extensa e produtiva da história da matemática, pois começou em 1911 e durou trinta e cinco anos. Nesse período, Hardy e Littlewood dominaram a Análise britânica e escreveram muitas dezenas de artigos e um livro (*Inequalities*, em colaboração com George Pólya (1887–1985)). Quanto ao relacionamento de Hardy com Ramanujan, este foi descrito por Hardy (no seu livro *Ramanujan: Twelve Lectures on Subjects Suggested by His Life and Work*) como tendo sido o único evento romântico da sua vida. A

história é bastante conhecida e, além disso, é descrita com algum detalhe no prefácio do livro, mas será dado aqui um breve resumo. Em 1913, Hardy recebeu uma carta de Ramanujan da Índia (então uma colónia britânica) onde o autor, então um funcionário público de 27 anos, lhe descrevia uma série de resultados matemáticos que obtivera. Seria um génio ou uma fraude? Ao fim de algumas horas, Hardy e Littlewood chegaram a um veredicto: génio! Hardy conseguiu, com dificuldade, fazer com que Ramanujan fosse para Inglaterra no ano seguinte para completar a sua fraca educação formal. Trabalharam juntos durante cinco anos mas, infelizmente, Littlewood teve pouca oportunidade para trabalhar com eles, pois passou grande parte desse período a fazer estudos de balística (foi segundo tenente de artilharia durante a Primeira Guerra Mundial). Ramanujan regressou à Índia em 1919 e faleceu no ano seguinte. O relacionamento entre Hardy e Ramanujan é daqueles de que se poderia dizer que "*dava um romance*." E deu! Em 2007, o escritor norte-americano David Leavitt (n. 1961) publicou o romance *The Indian Clerk*, que consiste no retrato ficcionado do convívio entre os dois e onde surgem personagens como Bertrand Russell (1872–1970), D. H. Lawrence (1885–1930) e Ludwig Wittgenstein (1889–1951).

Estas duas colaborações de Hardy (haveria outras) marcaram decididamente a sua carreira. Na *Apologia* ele conta que, dos artigos científicos que publicou nos dez primeiros anos da sua carreira, não havia mais de quatro ou cinco de que se conseguia recordar com satisfação e que a associação com Littlewood e Ramanujan foi o evento decisivo da sua vida. E acrescenta:

"*Ainda hoje digo para mim, quando me sinto deprimido e me vejo forçado a ouvir gente pomposa e maçadora, «Bem, fiz uma coisa que você jamais poderia ter feito: colaborar com Littlewood e Ramanujan de igual para igual.*"

É usual descrever-se a actividade de um matemático como sendo solitária. Este livro, pelas suas referências à faceta de trabalho colectivo, dá uma visão diferente e complementar do que é fazer pesquisa em matemática.

O prefácio é da autoria do físico e escritor C. P. Snow (1905–1980), que foi colega e amigo de Hardy. O termo *prefácio* é enganador, pois transmite a impressão de ser um texto de tamanho bastante reduzido comparado com o texto de Hardy. De facto, é quase do mesmo tamanho! Snow enriquece bastante o livro ao narrar a vida de Hardy e ao descrever a sua personalidade, para além de, como já foi dito, contar também como foi o relacionamento entre Hardy e Ramanujan. Convém notar que Snow reproduz o erro bastante comum que consiste em dizer que Ramanujan foi o primeiro indiano a ser eleito para a *Royal Society*. De facto, foi o segundo, tendo o primeiro sido o engenheiro naval Ardaseer Cursetjee (1808–1877), a quem tal honra fora atribuída em 1841, 77 anos antes de Ramanujan! Snow também lastima que o texto de Hardy *Bertrand Russell & Trinity*, escrito em 1942, "*nunca foi tornado acessível ao público.*" Isto era verdade quando o prefácio foi escrito (em 1967), mas o texto acabaria por ser publicado em livro dez anos mais tarde.

A tradutora enriqueceu o livro com algumas notas de rodapé contendo informações relativas a expressões correntes em Cambridge mas pouco conhecidas fora daquele meio, bem como com curtas descrições de pessoas que, sendo bastante conhecidas no Reino Unido quando o livro foi escrito, serão provavelmente desconhecidas da generalidade dos leitores portugueses actuais. Além disso, consegue preservar o estilo elegante da prosa de Hardy. Finalmente, saliente-se que a escolha de *Apologia de um Matemático* para o título em

Hardy com John Edensor Littlewood no Trinity College, Universidade de Cambridge.

português desta obra, em vez de *Justificação de um Matemático*, que seria uma escolha talvez considerada mais natural por bastantes pessoas, se justifica plenamente por o título ser uma referência clara à *Apologia de Sócrates*.

Matemática – Origens e Aplicações - Gueorgui Smirnov, Isabel Maria de Oliveira Rodrigues | Escolar Editora, 2006

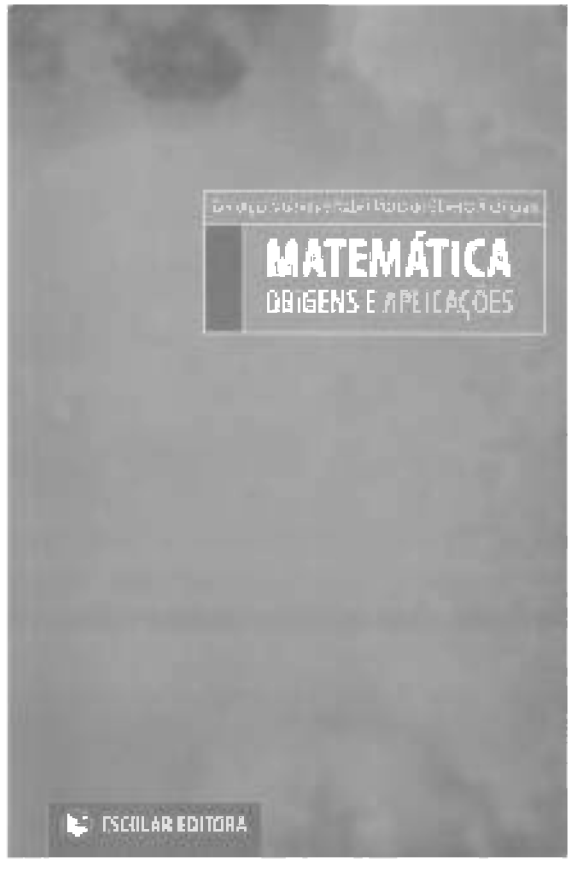
Recensão por **Maria Pires de Carvalho**
[Departamento de Matemática Pura da Faculdade de Ciências do Porto]

"(...) este livro é muito bem-vindo. Alunos curiosos e docentes que queiram despertar o interesse sobre o que ensinam têm aqui ampla escolha de temas de matemática aplicada, introduzidos de modo leve e encadeado em conversa amena, por vezes até bem-humorada, com o leitor"

A maioria dos livros de divulgação matemática elege como objectivo a apresentação de uma amostra especialmente apelativa de contributos matemáticos, sublinhando o valor intrínseco das suas ideias essenciais e não a sua aplicabilidade em outros domínios mais ou menos tecnológicos. Ainda que possam ter muita qualidade científica e literária – e já passaram alguns desses por esta secção –, omitem por vezes aspectos relevantes do edifício matemático: a motivação exterior à matemática que está na origem de inúmeros conceitos e descobertas, as conexões surpreendentes da matemática com outras ciências, o uso da linguagem matemática e dos seus teoremas na resolução de problemas em contextos reais – que aliás muitos vêem como profanadores do espírito da ciência pura.

Nesse sentido, este livro é muito bem-vindo. Alunos curiosos e docentes que queiram despertar o interesse sobre o que ensinam têm aqui ampla escolha de temas de matemática aplicada, introduzidos de modo leve e encadeado em conversa amena, por vezes até bem-humorada, com o leitor. Cada capítulo é (mais ou menos) autónomo, começando por delinear um problema, particularizando parâmetros se conveniente, testando hipóteses na companhia de uma calculadora e terminando em apoteose com uma resolução elegante. Assuntos como o controlo de um satélite, o processamento de imagens, a dinâmica de populações, a difusão do calor ou o problema isoperimétrico são uma oportunidade bem aproveitada para introduzir métodos poderosos de aproximação e optimização, numa exibição aprazível e de invulgar qualidade do uso da matemática noutras áreas.

Cada exemplo prático é analisado cuidadosamente quanto à robustez do modelo e do conteúdo matemático que o valida; nenhum exige mais de uma hora a entender. Mas há um pressuposto para este sucesso: o leitor tem de dominar conteúdos de matemática e física que não são



frequentes no percurso académico dos alunos do nível secundário ou do 1º ano da universidade, aqueles para quem os autores declaradamente escreveram esta obra. Vejamos alguns exemplos que substanciam esta crítica.

– Depois de várias páginas sobre polinómios e séries de Taylor motivadas pela necessidade de "*calcular a função exponencial e outras funções*" (p. 26), lê-se que este é "*um método universal*" para mais adiante (p. 33) se afirmar que "*claro que as calculadoras não utilizam os polinómios de Taylor.*" Porquê? – indagará o leitor desapontado, sem encontrar resposta no que se segue.

– Na página 40 os autores avisam que irão procurar uma fórmula geral para a sucessão de Fibonacci e, para isso, sem mais explicações, buscarão progressões geométricas que satisfaçam esse tipo de relação de recorrência. Há boas razões para esta estratégia, mas não acredito que alguma delas seja conhecida dos alunos do secundário, que lerão aqui infelizmente apenas um (magro) rasgo de génio.

– Na página 48 diz-se que: "*Entre os valores de Arg z existe um que pertence ao intervalo] – π, π].*" Não creio que se possa esperar que um aluno do secundário deduza com rigor esta afirmação.

– Na página 50 lê-se: "*Por indução obtemos a fórmula de Moivre.*" Ora, não só não é usual pedir-se aos alunos do secundário que entendam demonstrações, como o método de indução está ausente dos programas desse nível.

– Na página 84 é prometida ao leitor "*uma resolução elementar do Problema Isoperimétrico (…).*" Mas, como se sabe, o argumento de Steiner aqui reproduzido é insuficiente e disso o leitor não é avisado, recebendo como tarefa completar detalhes que não estão ao seu alcance. Senão vejamos:

(a) Na página 85 lê-se: "*Sejam A e B dois pontos da fronteira do conjunto que dividem a curva em duas partes de perímetros iguais.*" Que aluno do secundário saberá justificar com clareza esta afirmação?

(b) Logo de seguida os autores escrevem: "*Mostremos que um diâmetro do conjunto que tem área máxima, de entre todos os conjuntos de perímetro P, divide a área em duas partes iguais.*" Afinal, onde foi provado que existe uma curva que engloba uma área máxima? Não pode esperar-se que um aluno do secundário ou sequer do 1º ano da universidade complete este dado da demonstração.

Mais adiante no livro (p. 104) os autores alertam para a questão da existência ou não de mínimos ou máximos, mas não vão além de uma analogia pouco inspirada, e até enganadora, com o teorema de Weierstrass sobre a existência de máximos de funções contínuas em intervalos compactos.

(c) O argumento usa (p. 87) a caracterização da circunferência que é descrita pelo Teorema do Arco Capaz. Ora, se é verdade que os alunos do secundário aprendem que a circunferência tem a propriedade aqui mencionada, poucos saberão que o recíproco também é válido e que, sendo "*a fronteira do conjunto de área máxima é formada pelos vértices dos triângulos rectângulos que têm como hipotenusa o mesmo segmento AB*", ela é necessariamente uma circunferência.

Todas estas imperfeições seriam de somenos importância se este livro apresentasse referências bibliográficas que o complementassem (e são inúmeras as boas obras disponíveis sobre os assuntos que compõem este livro), oferecendo ao leitor menos orientado um percurso mais firme através destes capítulos essenciais da matemática e suas aplicações.

Há ainda a assinalar alguns deslizes, dos que se costumam desculpar em textos de divulgação matemática apelando-se ao princípio de que aos leitores iniciantes na área é melhor não revelar as dificuldades para que não desanimem (ou, então, devem tentar deslindar sozinhos os aspectos mais delicados das questões). São de facto defeitos evitáveis, como estes dos primeiros capítulos:

– Em todas as instâncias em que se apela ao facto de uma função derivável num intervalo ter derivada nula nos pontos de mínimo ou máximo (como na pág. 89), esquece-se de mencionar que o ponto tem de ser interior para esta afirmação ser segura.

– Na página 22, a propósito da tangente ao gráfico de uma função, diz-se: "*É fácil ver que o declive desta recta é a derivada [da função] no ponto (…).*" Há alguma coisa a verificar? Não é apenas a

definição de tangente? Ou está-se aqui a apelar à noção intuitiva (errada) que uma recta tangente a um gráfico num ponto é a que intersecta o gráfico apenas nesse ponto?

– Na página 25, sobre o método de Newton, os autores escrevem: "*Este método pode ser aplicado à resolução de equações do tipo* $f(x)=0$. *Basta que no ponto que resolve a equação, isto é, que verifica a condição* $f(x)=0$, *a derivada da função seja diferente de zero. Então para os valores de* x *que estão perto do ponto* x *é possível calcular o valor* $x-\frac{f(x)}{f'(x)}$ *e construir a sucessão*

$$x_{k+1} - x_k \quad \frac{f(x_k)}{f'(x_k)}, \quad k = 0,1,2,..."$$

Esta afirmação é falsa; e mesmo que os autores tivessem em mente apenas funções com derivada contínua, não é esse o universo de funções que qualquer aluno do secundário ou do 1º ano da universidade já domina.

– A apresentação da resolução do problema da braquistócrona, por Johann Bernoulli, peca desde o seu início (p. 99) por supor que a curva mais rápida que se procura é o gráfico de uma função $y = y(x)$. Além disso, não são dadas razões válidas para a existência de uma tal curva, embora se aprecie o esforço de relacionar este problema com o da trajectória da luz em meio não homogéneo. Não fica assim claro que a curva encontrada seja a mais rápida entre todas as possíveis unindo os dois pontos considerados.

Dois últimos reparos de menor importância. Há aqui e acolá uma escolha menos avisada de notação (como nas páginas 28-29 ou no fim da 147), e o deselegante uso de $f(x)$ para referir a função f e o valor dela em x. Lamenta-se ainda a ausência nesta obra de um índice remissivo, coisa actualmente muito fácil de fazer mesmo com os mais modestos processadores de texto.

Que não se conclua daqui que este é um livro dispensável: a apresentação original e o conteúdo interessante por que os autores optaram fazem deste um dos melhores livros de divulgação matemática em português, cuja leitura e uso se recomendam. ■

por Graciano de Oliveira
[Universidade de Coimbra]

Governo das Universidades e Politécnicos e empréstimos a estudantes

O sistema de empréstimos a estudantes do ensino superior já é praticado há muito noutros países, mas entre nós é inovador.

Dois diplomas mobilizaram, nos últimos tempos, a atenção dos interessados no nosso sistema escolar: o que ficou conhecido como RJIES (Regime Jurídico das Instituições de Ensino Superior) e o que dispõe sobre os empréstimos a conceder a estudantes.

O primeiro altera profundamente um regime que contava já com muitos anos e que fora aprovado na Assembleia da República por unanimidade. O RJIES não terá sido suficientemente discutido mas tem pontos muito controversos. Um deles é o novo método para a escolha dos reitores das Universidades e dos presidentes dos Politécnicos. Segundo o nº 1 do Artigo 86º, o reitor ou presidente é eleito pelo Conselho Geral depois da abertura de candidaturas e audição pública dos candidatos. O Conselho Geral (Artigo 81º) tem entre 15 e 35 membros, sendo mais de metade professores e investigadores e os restantes estudantes e personalidades externas de reconhecido mérito.

Quanto ao sistema de empréstimos a estudantes do ensino superior, ele já é praticado desde há muito noutros países mas, entre nós, é inovador.

Eis as nossas perguntas:

1. Que pensa, na generalidade, do RJIES? Foi suficientemente discutido e divulgado?

2. Qual a sua opinião sobre o processo de designação dos reitores e dos presidentes?

3. A representação estudantil no governo dos estabelecimentos de ensino superior foi drasticamente reduzida. Que acha disso?

4. E sobre o regime de empréstimos aos estudantes? Diz-se que virá reforçar a autonomia dos estudantes face aos pais...

5. O diploma prevê um prazo de carência de 1 ano, isto é, um lapso de tempo de 1 ano após a conclusão dos estudos, em que se admite que o estudante não poderá pagar. Muitos comentadores, dada a dificuldade em conseguir um emprego, consideram 1 ano muito pouco. Que lhe parece?

A. Gomes Martins, Vice-Reitor da Universidade de Coimbra

1. Acho que, dado o ritmo das mudanças de contexto, era necessário rever muitos dos aspectos do enquadramento legal do ensino superior (ou pelo menos das universidades, sobre as quais me sinto mais à vontade para emitir opinião). O próprio CRUP [Conselho de Reitores das Universidades Portuguesas] tinha já feito diversas propostas que o MCTES [Ministério da Ciência, Tecnologia e Ensino Superior] sempre ignorou, entre as quais a de uma

nova lei de autonomia. A experiência que fui acumulando em quatro anos de mandato diz-me que havia (há) muito processos de decisão muito ineficientes e que isso não é compatível com a agilidade que se tornou quase imperativa no governo das universidades. Mas o que a experiência também diz é que as decisões mais participadas são mais robustas porque são menos contestáveis. Ora, o RJIES reduz muito a capacidade de participação da comunidade universitária nas decisões. E, recursivamente, a sociedade não teve oportunidade de o debater e de lhe incorporar alguma sabedoria. A votação isolada do grupo parlamentar que suporta o governo é bem ilustrativa disso. Os unilateralismos têm uma enorme probabilidade de não serem produto de espíritos especialmente iluminados porque estes não têm tendência para o unilateralismo. Por isso raramente uma imposição unilateral corresponde a um rasgo de génio.

2. Em abstracto, o processo definido pode parecer virtuoso. Na minha opinião peca por retirar à figura do reitor a capacidade de congregação de vontades. Passa a constituir uma figura distante, em que os membros da comunidade universitária dificilmente se reverão. E os tempos presentes e futuros próximos vão requerer uma grande capacidade de mobilização de vontades que não se faz só com prescrições, admoestações ou castigos.

3. A representação estudantil poderia ser não tão expressiva quanto era até aqui. Acho que o equilíbrio entre a participação útil e importante para a universidade por um lado e o ónus de responsabilidade para os estudantes (pessoal mas também político) por outro, poderia passar por uma representação qualitativamente diferente e possivelmente com menos peso relativo. Mas o nível em que ficou é, em minha opinião, muito obviamente desviado de uma visão equilibrada deste compromisso.

4. Não digo que não, em abstracto. Mas se olharmos para o actual nível de endividamento das famílias portuguesas tenho as maiores dúvidas sobre quem poderá beneficiar deste sistema. O facto de existirem sistemas de empréstimos em vários outros países não lhe confere virtudes por si só. Significa apenas que o paradigma dominante é o de uma concepção de ensino superior como um sistema de prestação de serviços, cuja relação com os estudantes é uma relação comercial com clientes. A própria UNESCO [Organização das Nações Unidas para a Educação, Ciência e Cultura] reconhece, apesar de fazer coro com o Banco Mundial e com a OCDE [Organização para a Cooperação e Desenvolvimento Económico] na necessidade de "partilhar os custos" do ensino superior com as famílias, que o retorno do investimento no graduado pelo ensino superior, só em termos monetários, sem contar com inúmeras externalidades sociais positivas, se situa

Cidade de Coimbra e a sua Universidade.

entre 6 e 15. Qualquer investidor fica com os olhos em cifrões quando vê um ROI [Return Of Investment] com estes valores! Um sistema de ensino superior é, por muito que se queira reduzir esta concepção a uma velharia inútil, uma ferramenta estratégica de desenvolvimento de qualquer sociedade. Reduzir a relação do estudante com o sistema a uma relação mercantil é errado e pernicioso. Pode conduzir a garrotar partes importantes de gerações e a estreitar ainda mais a base social do acesso ao sistema (o que não dizer então do subfinanciamento?!).

5. Por mim até pode ser um mês. Se se redefinirem os indecorosos limites de rendimento que hoje balizam os escalões de acesso a bolsas de estudo, se se aumentar significativamente o número de bolsas e se se garantir financiamento aos serviços de acção social que lhes permita oferecer serviços de qualidade e baixo custo, um mês é suficiente porque é indiferente.

António Brotas, Secretário de Estado do Ensino Superior e Investigação Científica do VI Governo provisório (1975/76)

1. Não. Mas, sobretudo, não houve um clima propício à apresentação e discussão de propostas alternativas.

2. A lei existente podia ter alguns correctivos, mas não muito grandes.

3. Nunca me preocupou a percentagem da "representação estudantil", mas sempre considerei totalmente errada a imposição vincadamente corporativa "de os estudantes só se poderem fazer representar nas assembleias por estudantes" (e os funcionários e os docentes idem). Sempre considerei os estudantes inteligentes e capazes de compreender que, para defender os seus próprios interesses e os da escola numa assembleia, professores da sua confiança podiam ser preferíveis a outros estudantes. Este carácter corporativo, que a meu ver foi a grande pecha que inferiorizou a gestão democrática portuguesa, parece manter-se nas versões actuais.

4. Os empréstimos darão autonomia a alguns estudantes. Na generalidade dos casos, permitirão os aumentos das propinas e de outros custos e farão com que os estudantes terminem os estudos endividados. Preferiria que, em vez de propinas, os estudantes pudessem prestar serviços às escolas. Penso que seria bom para eles, para as escolas e o Estado pouparia dinheiro.

5. É obvio que os desempregados não poderão pagar as dívidas.

Pedro Barros, Presidente da Associação Académica da Universidade do Algarve

1. No meu entender, penso que era urgente haver uma reforma nas instituições de Ensino Superior.

O RJIES aparece desta forma para combater certas e determinadas lacunas que durante vários anos são detectadas. É importante também referir que são, muitas vezes, os alunos dirigentes associativos que focam determinadas situações que não correm conforme o previsto, de modo a serem alteradas.

Assim, e muito bem, o Ministério da Ciência, Tecnologia e Ensino Superior, escutou e discutiu com diversas Associações Académicas e de Estudantes de institutos de Ensino Superior o RJIES antes deste ser apresentado em Conselho de Ministros e antes de ser apresentado na Assembleia da República.

Orgulhosamente, pensámos que muitas das nossas sugestões seriam analisadas cuidadosamente, e que muitas delas seriam contempladas no RJIES. No entanto, e para nosso grande espanto, o RJIES foi apresentado e aprovado não mencionando quaisquer sugestões que os estudantes, e muito bem, apresentaram ao Ministério que tutela o Ensino Superior em Portugal.

Quanto à divulgação, penso que um assunto desta dimensão foi devidamente anunciado e todas as entidades competentes tiveram conhecimento do RJIES.

2. No que respeita ao processo de designação dos reitores e dos presidentes, penso que, em ambos os

casos, deveriam ser eleitos democraticamente por toda a comunidade académica a que se candidatam, mas, acima de tudo, deveriam ser professores ou investigadores de carreira da própria instituição.

Quem melhor do que eles conhece a instituição de ensino de modo a representá-la da melhor maneira, interna e externamente? Quem melhor do que eles conhece a instituição de ensino de modo a presidir ao Conselho de Gestão?

3. Apesar de sermos intitulados como uma "geração rebelde", os jovens de hoje em dia são mais do que aquilo que nos apelidam.

A representação estudantil foi, nos últimos anos, a melhor maneira de se combater lacunas emergentes de diversas instituições de ensino portuguesas, porque os "estudantes rebeldes" enfrentam os problemas que vivem, marcando sempre as suas posições, convictos e conscientes.

Verdade seja dita que muitos professores e investigadores reconhecem o valor dos estudantes, e dão-nos apoio nas decisões e reivindicações levadas em curso. No entanto, sou apologista que por detrás de uma boa negociação estará sempre um bom diálogo.

Neste momento, resta-me perguntar: tendo em conta o corte drástico sofrido na representação estudantil nos diversos órgãos de gestão de cada instituição de ensino, que diálogo será possível?

Penso que retirar a voz activa aos estudantes representativos da grande massa estudantil é uma atitude que vai, a longo prazo, ter repercussões inerentes. Por exemplo, o não permitir a detecção atempada de problemas por não terem a participação de quem recai neles directamente.

4. O regime de empréstimos aos estudantes é algo batalhado por muitas Associações Académicas e de Estudantes no nosso país.

Felizmente surge uma maneira de não condenar um estudante que não tenha recursos financeiros que lhe permitam tirar um curso superior, prosseguir os seus estudos da maneira mais digna e correcta, dado que o sistema de ensino está cada vez mais caro.

Infelizmente, o que se tem vindo a constatar é que as propinas pagas pelos estudantes estão a ser mal aplicadas.

Para bem das instituições, estas verbas estão a fazer face aos cortes sucessivos por parte do MCTES, pois caso contrário já teriam fechado as portas.

Agora, interrogo-me se os Institutos Superiores PÚBLICOS poderão ter os dias contados porque, mais dia, menos dia, as propinas dos alunos terão que ser aplicadas para o acréscimo de qualidade, assim como está previsto, surgindo então problemas económicos que deveriam ser combatidos pelo Ministério, como prática normal, mas pouco ou nada frequente.

Gostava também de ver o regime de empréstimos aos estudantes como uma bênção e não como uma autonomia dos estudantes face aos pais, pois julgo que qualquer pai gosta de dar aos seus filhos as melhores condições de vida para estes prosseguirem os estudos até onde possível. Assim sendo, é uma maneira através da qual se potencia o aumento da procura de estudantes de classe baixa ao Ensino Superior.

5. Concordo plenamente, não só com os comentadores mas com todos os meus colegas dirigentes associativos. Sem dúvida é um problema inerente ao regime de empréstimos aos estudantes que nos preocupa bastante.

Penso que tal situação poderia ser revista e analisada pelas entidades competentes. Quando é considerado o prazo de um ano, deveria ser para motivar o estudante recém-licenciado a procurar um emprego, mas, devido ao panorama nacional, nem sempre tal situação é possível.

Logo, acho que deveriam ser analisadas cuidadosamente e salvaguardadas situações como as que prevemos que aconteçam.

Saudações Académicas.

por Teresa de Jesus Costa
[Escola Secundária de Montejunto - Grupo de História da Matemática da Universidade de Aveiro]

Alguns aspectos da vida e da obra de Augusto d'Arzilla Fonseca (1853-1912)

O calculo dos quaterniões (...) tem sido objecto de muitas memorias e mesmo livros especiaes publicados nas differentes línguas da Europa. Em Portugal pessoa alguma se havia occupado d'elle, e por isso o sr. Arzilla fez um bom serviço tomando-o para assumpto da sua Dissertação inaugural.

Francisco Gomes Teixeira – Coimbra 1884

GRUPO DE PROFESSORES DE PRINCÍPIOS DO SEC. XX

1º PLANO – GRUPO DA ESQUERDA: Costa Lobo, Basílio Freire, Assis Teixeira, Daniel de Matos, Guimarães Pedrosa, Afonso Costa. — GRUPO DA DIREITA: Alberto dos Reis, Bernardo Aires, Joaquim Tavares, Serras e Silva.

2º PLANO – GRUPO DA ESQUERDA: Sidónio Pais, Bernardino Machado, Bernardo Madureira, Rocha Peixoto, Avelino Calisto. - GRUPO DA DIREITA: Raimundo Mola, Marnoco e Sousa, Silva Basto, Arzilla Fonseca, Francisco Basto, Lopes Vieira.

3º PLANO – GRUPO DA ESQUERDA: Sousa Pinto, Henrique de Figueiredo, Almeida Garrett, Paiva Pita, Dias da Silva. - GRUPO DA DIREITA: Sousa Refoios, António de Vasconcelos, António de Pádua.

4º PLANO – GRUPO DA ESQUERDA: Mendes dos Remédios, Alves da Hora, Henriques da Silva. - GRUPO DA DIREITA: Frederico Laranjo, Jesus Lino, Alves Moreira, Sousa Gomes.

GRUPO CENTRAL – 1º PLANO - VICE-REITOR E DECANOS: Júlio Augusto Henriques (Filosofia), Costa Alemão (Medicina), Silva Ramos (Teologia), Gonçalves Guimarães (Vice-Reitor), Fernandes Vaz (Direito), Cosia e Almeida (Matemática).

> Sir William Rowan Hamilton começou em 1844 a tractar nos *Philosophical Magazine, Irish Academy Transactions* e *Irish Academy Proceedings*, um novo calculo, a que deu o nome de *Methodo* ou *Calculo de quaterniões*.
>
> [Fo, 1884]

É com estas palavras que Arzilla Fonseca começa por referir a descoberta dos quaterniões por Hamilton, que motivado pelo trabalho então desenvolvido no âmbito dos Números Complexos estabeleceu as regras da multiplicação

$$i^2 = j^2 = k^2 = ijk = -1$$

para os símbolos i, j, k.

Na verdade, a descoberta dos quaterniões está na origem da álgebra moderna e marcou o aparecimento da Análise Vectorial.

Toda a história que decorreu entre a descoberta dos quaterniões até à sua aceitação e reconhecimento é longa, e carregada de polémicas e discussões sobre os trabalhos realizados por Hamilton de 1843 até à data da sua morte em 1865.

É uma agradável surpresa constatar que Portugal também participou na história dos quaterniões. Augusto d'Arzilla Fonseca, professor da Faculdade de Matemática da Universidade de Coimbra, escreveu dois livros sobre o assunto, *Principios Elementares do Calculo de Quaterniões* e *Applicações dos Quaterniões à Mecanica*.

Todo este entusiasmo do professor de Coimbra, relativamente aos quaterniões, levar-nos-ia a pensar que a Universidade a que pertencia, aproveitando os ventos de modernidade, motivaria Fonseca a leccionar o assunto por que tanto se interessou, como além de mais estava previsto nos estatutos. Contudo, esta história não teve propriamente um final feliz.

Os trabalhos de Augusto d'Arzilla Fonseca, *Principios Elementares do Calculo de Quaterniões* (1884) e *Applicação dos Quaterniões á Mecanica* (1885), encontram-se na lista de Alexander Macfarlane[1] e são referidos por Michael Crowe[2] entre as publicações de livros sobre quaterniões no período de 1841 a 1900.

Apesar de considerarmos ser um hábito português reconhecer postumamente as obras notáveis, Arzilla Fonseca teve o privilégio de ver os seus trabalhos reconhecidos. Gomes Teixeira não deixa de os elogiar no *Jornal de Sciencias Mathematicas e Astronomicas* com a publicação de duas notícias em1884 e em 1885[3].

Sobre Augusto d'Arzilla Fonseca sabemos que nasceu no Funchal, no dia 21 de Outubro de 1853[4]. Matriculou-se no curso de Matemática em Julho de

[1] **A. Macfarlane** – *Bibliography of Quaternions and allied systems of Mathematics* – Dublin, Uni. Press, 1904.

[2] **Michael J. Crowe** – *A History of Vector Analysis* – Dover, 1993.

[3] Gomes Teixeira não deixa de referir, ainda no seu jornal, um outro trabalho sobre quaterniões, desta vez realizado por Valentin Balbin em 1887 (matemático argentino), o que vem reforçar a importância dada ao assunto.

[4] Arzilla Fonseca faleceu no Porto em 17 de Fevereiro de 1912.

A. d'Arzilla Fonseca – Principios elementares do calculo de quaterniões – Coimbra 1884.

O calculo dos quaterniões, cuja descoberta data de 1843, tem sido objecto de muitas memorias e mesmo livros especiaes publicados nas differentes linguas da Europa. Em Portugal pessoa alguma se havia occupado d'elle, e por isso o sr. Arzilla fez um bom serviço tomando-o para assumpto de sua Dissertação inaugural. N'ella apresenta a parte elementar d'esta doutrina, isto é, a composição dos vectores, a multiplicação e divisão dos vectores, a resolução das equações do primeiro gráo de quaterniões, a differenciação de quaterniões, etc.

A. d'Arzilla Fonseca – Applicação dos quaterniões á Mecanica – Coimbra 1885.

No volume V deste jornal demos notícia de um trabalho, em que o sr. Arzilla expõe com todo o rigor e clareza e theoria dos quaterniões.
No presente trabalho faz applicação dos principios expostos no anterior á Mecanica racional, para fazer ver a importancia d'estes principios.
Principia pela Statica onde considera o equilibrio do ponto e dos systemas rigidos, e passa depois á Dinamica onde considera o movimento do ponto e o movimento do corpo solido independentemente das forças que o produzem, e em seguida o movimento do ponto, produzido por quaesquer forças.

1880, e no curso de Filosofia em Junho de 1882. Concluiu a formação de bacharel naqueles cursos no ano de 1883. Obteve a licenciatura em Matemática a 3 de Março de 1884 e o grau de doutor em Matemática a 27 de Julho de 1884 (*Principios Elementares do Calculo de Quaterniões* vem a propósito da obtenção deste grau).

Arzilla Fonseca foi segundo lente da Faculdade de Matemática, em Coimbra, onde leccionou a cadeira de Geometria Descritiva de 1885 a 1887 e de 1888 a 1911. Os períodos de interrupção correspondem a ausências para o cumprimento de tarefas militares, dado que além de professor era também militar. Obteve os postos de alferes (12 de Janeiro de 1875), tenente (20 de Julho de 1881), capitão (10 de Junho de 1886) e major (4 de Novembro de 1897).

Sobre uma avaliação realizada no início da sua vida académica, podemos ler no seu dossier pessoal que o seu estado físico era bom, tinha óptimas qualidades morais, uma capacidade intelectual muito boa, uma instrução variada e uma instrução profissional excelente. O dossier atesta também que executava muito bem os serviços que lhe eram atribuídos.

Arzilla Fonseca merece ser recordado como o divulgador dos trabalhos de Hamilton em Portugal. A propósito do cálculo elementar de quaterniões, recorde-se o tema da sua dissertação inaugural, *Principios Elementares do Calculo de Quaterniões* (1884).

Mas como foi recebida esta nova teoria no seio da Universidade de Coimbra?

Desde a sua criação que a Faculdade contou com um número insuficiente de doutores. A realização dos primeiros doutoramentos permitiu aumentar o quadro de professores.

Em 1853 fundou-se a revista *O Instituto* (revista científica e literária), associada ao Instituto de Coimbra[5]. Eram ali publicados trabalhos em Matemática, alguns dos quais serviam de textos de apoio aos alunos.

A partir de 1857, iniciou-se a publicação de dissertações. Considera-se que a produção de trabalhos dos matemáticos de Coimbra visava sobretudo o ensino e, em muitos casos, os trabalhos publicados eram traduções adaptadas de trabalhos estrangeiros (é o caso da tese de Henrique Manuel de Figueiredo, *Superficies de Riemann*, publicada em 1887).

Não existia uma revista periódica com maior exclusividade na publicação de trabalhos em Matemática até a fundação por Francisco Gomes Teixeira do *Jornal de Sciencias Mathematicas e Astronomicas*, em 1877. Este jornal veio motivar uma maior abertura na comunidade matemática portuguesa. Ao consultá-lo, podemos constatar que

[5]Foi fundado em 1852 em Coimbra e tinha como órgão oficial *O Instituto, Jornal Scientifico e Litterário*. Cultivou as Ciências e as Artes e teve como meios de acção bibliotecas, gabinetes de leitura e museus, entre outros. No século XIX teve grande importancia para o desenvolvimento científico e literário, devendo-se-lhe o núcleo arqueológico que constituiu o ponto de partida do actual Museu Machado de Castro e das escavações em Conimbriga.

Gomes Teixeira mantinha uma correspondência assídua com matemáticos internacionais de renome.

Numa tentativa de justificar a baixa produção de artigos sobre Matemática em Portugal, Luís da Costa e Almeida, director da Faculdade de Matemática, entre 1888 e 1911, escreveu [Al, 1892]:

"São geralmente reconhecidas as causas que determinam serem entre nós relativamente pouco numerosas as publicações sobre assumptos mathematicos. A maior difficuldade da composição typographica de tais escriptos, e o consumo limitadissimo que para elles se póde esperar no mercado, são as principais dessas causas."

E possível que nas afirmações de Luís da Costa e Almeida estivesse implícita a ideia de que a necessidade da formação de um corpo docente mais estável e uma enorme exclusividade ao ensino deixavam pouco espaço à investigação.

Na revista da Faculdade de Matemática da Universidade de Coimbra, Luís da Costa e Almeida apresenta uma lista de doutores, indicando os temas das dissertações elaboradas entre 1872 e 1892. Aparecem com as teses respectivas: Francisco Gomes Teixeira, *Integração das Equações ás derivadas parciaes de segunda ordem* (1875), Augusto d'Arzilla Fonseca, *Principios Elementares do Calculo de Quaterniões* (1884), Francisco Miranda da Costa Lobo, *Resolução das Equações Indeterminadas* (1885), Henrique Manuel de Figueiredo, *Superfícies de Riemann* (1887), entre outros. Dos quatro Matemáticos indicados, Gomes Teixeira foi o que gozou de um enorme reconhecimento, quer em Portugal, quer no estrangeiro. Francisco Costa Lobo notabilizou-se por proporcionar à comunidade matemática de Coimbra uma maior abertura, demonstrando um enorme interesse em convidar matemáticos estrangeiros de renome a visitarem o nosso país e mesmo a trabalharem em Portugal[6].

Augusto d'Arzilla Fonseca é contemporâneo de Gomes Teixeira, de Henrique Manuel de Figueiredo e de Costa Lobo, partilhando o clima de dinamismo proporcionado à Faculdade de Matemática por influência de Gomes Teixeira e com os contributos de Costa Lobo[7].

Podemos concluir que os professores de Coimbra estavam informados sobre os trabalhos produzidos no estrangeiro e que a Faculdade de Matemática era conhecida a nível internacional sobretudo através de actos individuais. Por exemplo, Costa Lobo chegava a convidar matemáticos estrangeiros e hospedava-os em sua casa, ficando algumas despesas destas estadias a seu cargo.

Nesta época, o tão comentado isolamento científico português parecia não existir. Contudo, se pensarmos na História da Matemática em Portugal ao longo de oito séculos, é habitual depararmo-nos com uma ou outra personalidade interessada em Matemática e não com a criação de uma escola de investigadores, à semelhança do que acontecia noutros países.

Fotografia tirada a vários professores da Faculdade de Matemática da Universidade de Coimbra, em 1900, no antigo Observatório Astronómico da Universidade de Coimbra. Da esquerda para a direita: Sidónio Pais, Almeida Garrett, Rocha Peixoto, Costa Lobo e Henrique de Figueiredo.

[6] Recordemos que Rudolf Fueter (1880-1950) que viria a trabalhar em Análise de Quaterniões, foi convidado para sócio correspondente estrangeiro do Instituto de Coimbra e, a convite de Costa Lobo, visitou Portugal em 1932 e proferiu uma palestra sobre *Quelques Résultats de L'Algèbre Moderne*, na Universidade de Coimbra.

[7] F. M. Costa Lobo, para além de exercer as funções de lente da Faculdade de Matemática da Universidade de Coimbra, foi director do Observatório Astronómico de Coimbra, Governador Civil substituto daquela cidade em 1889-1890 e Deputado às Cortes por Coimbra em 1905-1909.

O livro *Principios Elementares do Calculo de Quaterniões*

O trabalho de Arzilla Fonseca divide-se em seis partes com os seguintes títulos:

I – Propriedades das Operações;
II – Vectores e sua composição;
III – Producto e quociente de Vectores. Quaterniões;
IV – Interpretação e transformação de expressões;
V – Equações do primeiro grau. Biquaterniões;
VI – Diferenciação de Quaterniões;

Na introdução, Fonseca faz uma breve referência à História da descoberta dos quaterniões por Hamilton e refere a boa aceitação daquela teoria na Inglaterra, na Alemanha e na América. Estabelece um paralelo entre o cálculo das equipolências de Bellavitis no plano e o trabalho de Hamilton no espaço com o cálculo de quaterniões, com excepção da não aplicabilidade das regras usuais do cálculo nesta teoria (referimo-nos à perda da comutatividade ao passar da segunda à terceira dimensão).

Sobre a Teoria dos Quaterniões o autor escreve [Fo, 1884]:

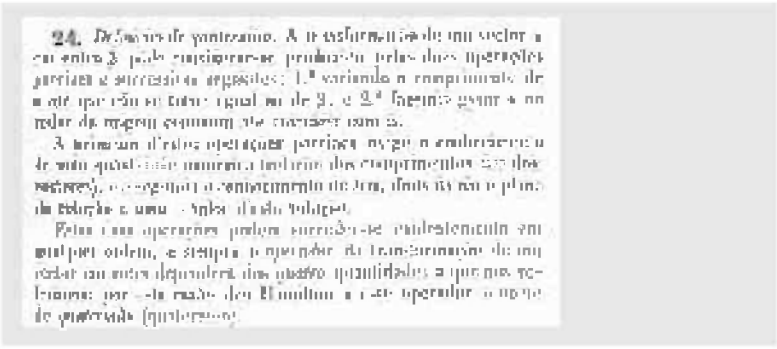
"Ainda que os quaterniões não se appliquem vantajosamente a todos os ramos das Mathematicas, introduzem porém em alguns d'elles uma grande concisão e dão ás suas soluções um manifesto caracter intuitivo."

E ainda:

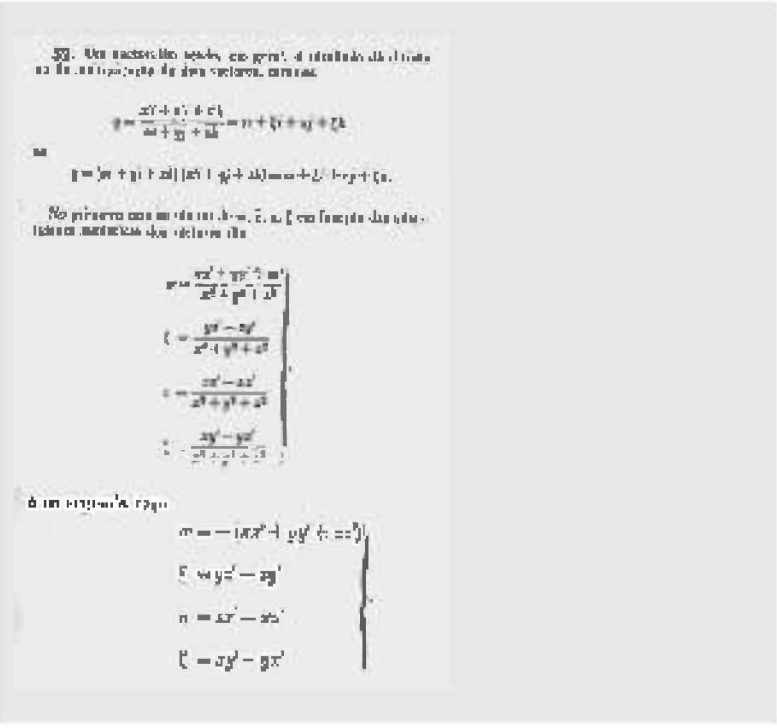
"Attendendo á novidade (entre nós) do assumpto e á sua importância, resolvemos escolher para dissertação inaugural, a que por lei somos obrigados, a exposição elementar dos principios do calculo de quaterniões, reservando para mais tarde o fazer a sua applicação á Mecanica."

Arzilla Fonseca não deixa de referir o atraso com que os quaterniões chegaram até ao nosso país. Na época, a cultura francesa tinha uma forte influência em Portugal, e também naquele país os quaterniões não só apareceram tardiamente[8] como gozaram de uma recepção pouco calorosa.

Nas partes I, II e III do seu livro, Arzilla Fonseca estabelece os pré-requisitos, até chegar à definição de quaternião.



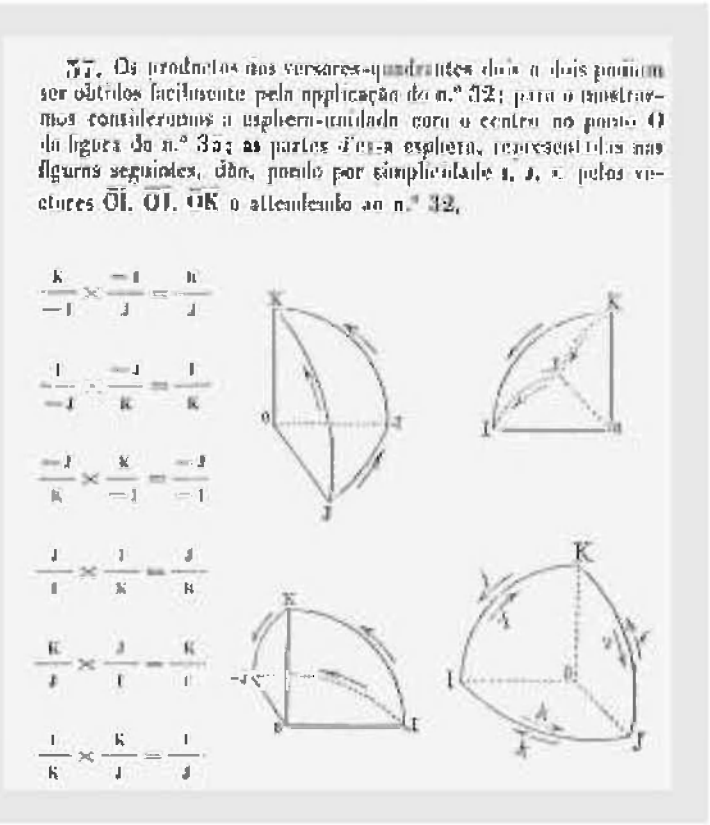
Sempre fiel a Hamilton, que é referido com frequência ao longo da sua obra, Fonseca define quaternião como o resultado da divisão ou da multiplicação de dois vectores.



O autor prossegue a apresentação do cálculo elementar de quaterniões com a exposição da resolução de equações do 1º grau e a diferenciação de quaterniões.

[8] A Teoria dos Quaterniões foi discutida com maior detalhe em França, a pa tir da publicação dos trabalhos de Allégret (A. Allégret, *Essai sur le Calcul des Quaternions de M. W. Hamilton*, Thèse de doctorat en Sciences de la Faculte de Paris, l'aris, 1862).

Podemos mesmo pensar que seria um sonho de Fonseca adaptar o seu trabalho ao ensino pelo modo como expõe os assuntos, utilizando metodologias que facilitavam uma maior compreensão dos temas expostos[9]. Vejamos, por exemplo, como o autor apresenta o *produto dos versores quadrantes*:



37. Os productos dos versores-quadrantes dois a dois podem ser obtidos facilmente pela applicação do n.º 32; para o mostrarmos consideremos a esphera-unidade com o centro no ponto O da figura do n.º 30; as partes d'esta esphera, representadas nas figuras seguintes, dão, ponto por simplicidade i, j, k pelos vectores $\overline{OI}$, $\overline{OJ}$, $\overline{OK}$ o attendendo ao n.º 32,

$$\frac{k}{-1}\times\frac{-i}{j}=\frac{k}{j} \qquad \frac{i}{-j}\times\frac{-j}{k}=\frac{i}{k}$$

$$\frac{-j}{k}\times\frac{k}{-i}=\frac{-j}{-i} \qquad \frac{j}{i}\times\frac{i}{k}=\frac{j}{k}$$

$$\frac{k}{j}\times\frac{j}{i}=\frac{k}{i} \qquad \frac{i}{k}\times\frac{k}{j}=\frac{i}{j}$$

Esta ideia pode ser reforçada se pensarmos que o autor escreveu a segunda obra tendo em vista a aplicação dos quaterniões à Mecânica. Recordemos alguns comentários de Arzilla Fonseca [Fo,1884]:

"N'esta exposição, em vez de seguirmos exclusivamente o caminho analytico ou o geometrico, adoptamo-los conjunctamente, por nos parecer que damos assim mais simplicidade e clareza á interpretação dos resultados."

Desconhecemos as razões que levaram o professor Arzilla Fonseca a escrever sobre quaterniões. Contudo, ao longo do seu primeiro livro, defende a importância do uso daquela teoria, e é sensível às suas aplicações à Física – Matemática.

A inspecção d'estas formulas mostra a largura com a extensão dos quaterniões tem com a Physica mathematica. Assim, se r representa a temperatura de um corpo solido no ponto, cujas coordenadas rectangulares são x, y, z, o symbolo $-\nabla r$ representará o fluxo de calor n'este ponto. Se v é o potencial de um systema de corpos, que se attrahem, ou a somma dos seus massas divididas respectivamente pelas suas distancias a um ponto variavel (x, y, z), então ∇v será um vector representando em grandeza e direcção a força acceleratriz n'esse ponto, produzida pela acção dos corpos do systema. E, se v é uma funcção similar das tres coordenadas rectangulares x, y, z, o symbolo $\pm\nabla v$ representará um vector normal á superficie, que tem por equação v = const.

Saliente-se ainda a sensibilidade do autor relativamente às dificuldades em criar um cálculo não comutativo:

"...não tractamos do calculo das variações de quaterniões, dos integraes de funcções de quaterniões e das funcções exponenciaes, em que os expoentes são quaterniões, e por meio das quaes Hamilton definiu os logarithmos de quaterniões, por exigirem uma grande extensão que nem sempre pode ser feita elementarmente, e mesmo porque são assumptos que ainda não estão completamente assentes."

Os momentos amargos da vida académica de Arzilla Fonseca

Ao fim de doze anos a ensinar Geometria Descritiva, Arzilla Fonseca, alegando problemas de visão, propôs à Congregação uma mudança na disciplina a leccionar, o que nunca conseguiu (informação retirada das actas da Congregação da Faculdade de Matemática da Universidade de Coimbra)[10]. Na verdade, Arzilla Fonseca teve conhecimento da existência de uma vaga, pela saída do professor José Falcão, e associado a esta vaga estava o lugar de astrónomo que, segundo Arzilla

[9] O autor utiliza com frequência figuras que, ao mesmo tempo, proporcionam uma maior clareza dos assuntos expostos.

[10] Fonseca mostrou a sua indignação face à decisão da Faculdade de Matemática relativamente ao seu pedido e escreveu *Recurso para a Opinião Pública* de uma decisão da Faculdade de Matemática contra um dos seus membros, em 1900, seguido de um *Novo Recurso para a Opinião Pública*, escrito em 1902.

Fonseca, exigia um grande esforço visual, mas era também um motivo para quebrar a rotina do ensino da Geometria Descritiva.

Arzilla Fonseca concorreu à vaga existente apresentando as razões que o próprio descreve:[11]

« A regencia ha perto de 12 annos da cadeira de geometria descriptiva tem-me prejudicado muito a vista, porque a minha reconhecida miopia se tem aggravado com a necessidade de acompanhar e fazer trabalhos practicos, que outros deveres imperiosos me forçam a executar [illegible] de noite.

« em vista do estado da minha vista, que se aggrava com os trabalhos praticos, que sou obrigado a acompanhar e executar na cadeira de Geometria em que me conservo ha muitos annos, peço à Illustre Faculdade me permitta a transferencia para a primeira cadeira que vagar, salvos os direitos, que a praxe tem estabelecido e eu respeitosamente acato, de escolha por um collega mais antigo ».

Infelizmente a resposta da faculdade não foi favorável[12].

« ... desejando dar ao seu illustre collega o dr. Arzilla Fonseca uma prova de alta (1) consideração que constantemente lhe tem testemunhado; [illegible] seu illustre collega [illegible] que haja [illegible] deste requerimento; [illegible] o Dr. Arzilla Fonseca tem professado [illegible] da faculdade; ....

que não póde ser attendido o requerimento do seu illustre collega o Dr. Arzilla Fonseca, apresentado [illegible] congregação de 12 do mez corrente. »

E ainda:

« O conselho [illegible] que esta deliberação não [illegible] por fórma alguma [illegible] do sr. dr. Arzilla que opportunamente poderá ser attendido. »

Mais tarde, quando se procedeu à distribuição de cadeiras, Arzilla Fonseca, apresentou um novo pedido de mudança de cadeira, o que lhe foi mais uma vez negado.

O conselho da faculdade resolveu que fosse [illegible] a deliberação [illegible], tendo em attenção as necessidades da disciplina do primeiro anno, que exige [illegible] com facilidade e promptidão; [illegible] não poder acceder aos desejos [illegible] pelo requerente [1] ».

Foi decretada em 24 de Dezembro de 1901 uma nova cadeira, criada pela reforma da Universidade de Coimbra. Arzilla Fonseca apresentou um novo requerimento ao Director da Faculdade dias antes da realização da Congregação, concorrendo para essa cadeira ou outra que vagasse pelo preenchimento daquela.

Nessa congregação, presidida pelo vice-reitor da Universidade, estavam presentes os professores Luís da Costa, Rocha Peixoto, Sousa Pinto, Luciano da Silva, Arzilla Fonseca, Francisco Costa Lobo, Henrique Figueiredo e Sidónio Pais.

Relativamente à distribuição de serviço na Faculdade de Matemática, sempre que existia uma vaga os professores mais velhos tinham prioridade de escolha, e as cadeiras consideradas *menos agradáveis*[13] eram distribuídas pelos mais novos.

Acontece que, naquela congregação, o professor Henrique Figueiredo apresentou duas propostas:

- Transferência do Doutor José Bruno para a cadeira vaga.

- O Doutor Luciano deveria ocupar a cadeira do Doutor José Bruno.

As duas propostas foram unanimemente aprovadas e, mais uma vez, Arzilla Fonseca viu o seu requerimento indeferido por quatro votos contra três .

Indignado, Arzilla Fonseca declarou que, pelos meios ao seu dispor, protestaria contra a deliberação da Faculdade.

[11]Este pedido foi apresentado em 12 de Fevereiro de 1900.
[12]A resposta ao pedido de Fonseca foi dada em 16 de Fevereiro de 1900.
[13]Esta expressão é utilizada por Arzilla Fonseca.

Na verdade, Arzilla Fonseca tinha tornado pública toda a sua história no concurso a uma vaga com a publicação de um *Recurso* em 1900, e reforçou a sua desilusão com o *Novo Recurso*, em 1902.


RECURSO

PARA A OPINIÃO PUBLICA


NOVO RECURSO

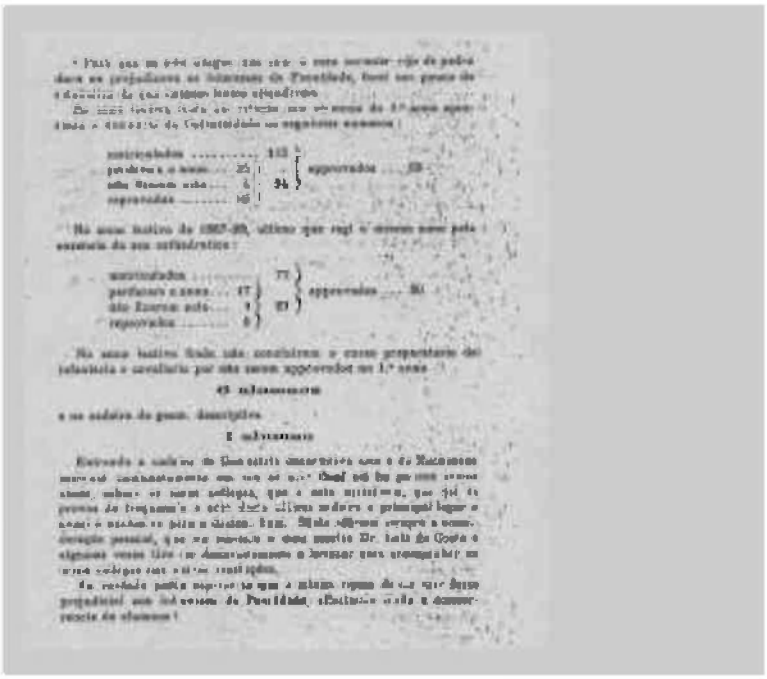
Nos anos que se seguiram, a vida na Universidade não parece ter sido fácil para Arzilla Fonseca, que chega a demonstrar uma relação pouco amigável com Henrique de Figueiredo, entre outros colegas. Contudo, mantém uma enorme estima pelo professor Sousa Pinto e aprecia as qualidades científicas e humanas de Gomes Teixeira.

"Conheço na minha Faculdade duas excepções: as que se deram com os Ex.mos Drs. Gomes Teixeira e Rocha Peixoto. A primeira só seria para admirar que se não tivesse dado e que a Faculdade possuindo a honra de ter S. Ex.a como membro lhe não abrisse immediatamente a cadeira de Analyse, ainda mesmo provida já, para que S. Ex.a tivesse occasião de com a sua excepcionalisssima competencia augmentar o brilho e a honra d'ella, do primeiro estabelecimento scientifico e do paiz." [Fo, 1900]

Se recordarmos a avaliação de Arzilla Fonseca ficamos um pouco surpresos. Na verdade, um homem de qualidades *morais óptimas* põe em causa e desafia a *moral* da sua própria Faculdade:

"Lamento, pelo muito que venero a Universidade, digna de muita consideração e respeito de todos, apezar dos isolados casos menos correctos e prudentes de alguns dos seus membros, o ver - me obrigado a quebrar o silencio, que perante o publico deveria ter, para assim procurar obter o único desforço de um insulto feito á minha qualidade de professor." [Fo, 1900]

Está patente nas palavras de Fonseca a sua indignação relativamente à decisão da sua Faculdade. Decisão que veio a marcar profundamente a sua vida e que o levou a recorrer a todos os meios para justificar o seu mérito científico e pedagógico. O próprio apresenta um relatório sobre o sucesso dos alunos na sua cadeira e refere: *"Para que se não allegue que com o meu caracter rijo de pedra dura eu prejudicava os interesses da Faculdade..."* [Fo, 1902]



Talvez o *carácter rijo* de Arzilla Fonseca não fosse o único responsável por toda esta história. Na época, eram conhecidos alguns actos isolados, menos agradáveis na Universidade de Coimbra. Rafael Bordalo Pinheiro (1846-1905) fundador da caricatura nacional, representa a Universidade de Coimbra[14], como uma nobre e antipática dama, conhecida também por mãe dos bacharéis, dado que era fecunda em formar bacharéis.

Embora exagerada, a visão de Bordalo Pinheiro vem chamar a nossa atenção para um ambiente universitário hostil aos mais sensíveis, como seria possivelmente o caso do professor Arzilla Fonseca.

O impacto da introdução da teoria dos quaterniões por Arzilla Fonseca no Portugal de 1900

A história da introdução dos quaterniões em Portugal, por Arzilla Fonseca, é um dos exemplos das tentativas de abertura do nosso país ao mundo científico internacional. Em Coimbra, grande centro intelectual daquela época, encontravam alguma expressão em actos individuais e na política do *Instituto* que incluía, entre os seus membros, sócios correspondentes estrangeiros. Estas tentativas de certo modo falharam, vítimas de um certo pavor à inovação tão conhecido e comentado em certos sectores da sociedade portuguesa da época.

Arzilla Fonseca *trouxe-nos* um assunto *novo*. Contudo, mais uma vez se evidencia que o contributo dos matemáticos portugueses da época no desenvolvimento da Matemática ligou-se essencialmente ao ensino e à adaptação de livros clássicos ao ensino, que provinham de traduções baseadas numa ou várias fontes. É natural que nem todos os seus colegas aceitassem a teoria dos quaterniões, o que não era inédito na época, e que a posição de Gomes Teixeira fosse isolada ao considerar a grande importância daquela teoria.

Arzilla Fonseca traduz a teoria dos quaterniões de Hamilton acrescentando notas pessoais e citações a outros autores, como por exemplo Bellavitis e Hermann Grassmann. Não apresenta referências bibliográficas, o que nos leva a pensar que as normas de exigência para trabalhos daquela natureza, no fim do século XIX, são muito diferentes das actuais.

Podemos pensar que Arzilla Fonseca foi vítima de uma atmosfera científica geral que não incentivou, ou até desmotivou, o espírito criativo necessário para uma investigação que se impunha num contexto internacional. Mas recordemos que, naquela época, Gomes Teixeira conheceu glória e reconhecimento nacional e internacional, lamentavelmente não acompanhado por outros matemáticos portugueses da época.

Arzilla Fonseca, *asfixiado* com alguns aspectos do meio universitário de Coimbra, apresentou recursos contra um sistema que considerava obsoleto e, em certos aspectos, corrupto. Infelizmente, ficamos sem saber quais seriam as suas intenções relativamente à investigação na teoria dos quaterniões e à divulgação dos seus trabalhos.

A Universidade de Coimbra (Novembro de 1882)

[14] No Álbum de Glórias de Rafael Bordalo Pinheiro, podemos encontrar um texto de Ramalho Ortigão onde é referida a presença do sino (ao lado da dama) que tange para tudo e o modo negativo como a Universidade procedeu com dois dos seus mais tenros filhos (não são referidos nomes). O autor refere ainda a existência de uma mentalidade pouco aberta ao progresso, afirmando, em pleno final do século XIX, que aquela instituição é contemporânea do Marquês de Pombal e do seu regime opressivo.

Agradecimento

Ao Professor José Vitória por me ter facultado os trabalhos de Augusto d'Arzilla Fonseca.
Ao Professor Manuel Costa Lobo pelas informações sobre alguns aspectos da vida do seu avô, Francisco Miranda da Costa Lobo.
Ao Professor Jaime Carvalho e Silva que gentilmente me cedeu alguns documentos sobre Arzilla Fonseca e a História da Universidade de Coimbra.

Referências Bibliográficas

Almeida, Luís da Costa – *A Faculdade de Matemática da Universidade de Coimbra*: 1872-1892, Coimbra 1892, Al, 1892

Crowe, Michael J. – *A history of vector Analysis*, Dover, 1993, Cr, 1993

Fonseca, A. d'Arzilla – *Principios Elementares do Calculo de Quaterniões* - Coimbra, 1884, Fo, 1884

Fonseca, A. d'Arzilla – *Applicação dos Quaterniões á Mecanica* - Coimbra, 1885, Fo, 1885

Fonseca, A. d'Arzilla – *Recurso para a opinião publica* - Coimbra, 1900, Fo, 1900

Fonseca, A. d'Arzilla – *Novo Recurso para a opinião publica* - Coimbra, 1902, Fo, 1902

Fueter, R.- *Quelques résultats de l'algèbre moderne* - Revista da Faculdade de Ciências, vol.II, nº4, Coimbra,1932, Fu, 1932

Macfarlane, A. – *Bibliography of quaternions and allied systems of Mathematics, Dublin*, Uni. Press, 1904, Ma,1904

Kuipers, Jack B. – *Quaternions and rotations sequences* – Princeton Uni. Press, 1999, Ku, 1999

Ortiz, Eduardo L. – *Proyectos de cambio científico e proyectos de cambio político en la tercera República: el caso de la teoría de los cuaterniones* – Revista Brasileira de História da Matemática, vol. 1, 2, Or, 2000

Silva, Jaime C. – *História da Universidade em Portugal* (A Faculdade de Matemática da Universidade de Coimbra (1772-1911)), a publicar, Si

Rafael Bordalo Pinheiro, *Álbum de glórias* – Edição comemorativa do centenário da morte de Rafael Bordalo Pinheiro (1846-1905), Clássicos Expresso, 2005

Memoria professorum Universitatis Conimbrigensis – dir. **Manuel Augusto**; colab. **Abílio Ferreira Marques de Queirós**;...et al., Coimbra: Arquivo da Universidade, 1992

por António Saraiva[1]
[Centro de Matemática do Porto]

Algoritmo de Potenciação

Para potências elevadas, são claros os ganhos computacionais de usar algoritmos de potenciação em etapas. Desenvolve-se aqui um desses algoritmos.

Dado um real x e um natural n, para calcular x^n podemos usar o método seguinte: escreva-se n na base 2; na representação binária de n, substitua-se cada 0 pela letra Q e cada 1, com excepção do primeiro que é ignorado nesta transcrição, por QX; na palavra que daqui resulta, cada Q significa *elevar ao quadrado* e cada X representa a operação de *multiplicação por* x.

Por exemplo, se $n = 21$, n representa-se na base 2 por $10101_{(2)}$; desta representação binária obtemos a palavra $QQXQQX$, que indica que, para calcular x^{21}, devemos "quadrar, quadrar, multiplicar por x, quadrar, quadrar e multiplicar por x"; ou seja, devemos calcular sucessivamente x^2, x^4, x^5, x^{10}, x^{20} e x^{21}.

O procedimento delineado acima tem semelhanças com o algoritmo de Horner para determinar uma dízima de um natural de que se conhece a representação binária finita. De facto, se $N = a_r a_{r-1} \cdots a_1 a_{0(2)}$, onde $r \geq 0$, $a_r = 1$ e $a_i \in \{0, 1\}$ para todo o i, então este algoritmo traduz-se pelo esquema

	a_r	a_{r-1}	$\cdots$	a_1	a_0
2					

tabela que é completada do seguinte modo:

	a_r	a_{r-1}	a_{r-2}	$\cdots$	a_1	a_0
2	a_r	b_{r-1}	b_{r-2}	$\cdots$	b_1	b_0

onde

$b_{r-1} = 2 \times a_r + a_{r-1}$

$b_{r-2} = 2 \times b_{r-1} + a_{r-2} = 2^2 \times a_r + 2 \times a_{r-1} + a_{r-2}$

$\vdots$

$b_0 = 2^r \times a_r + 2^{r-1} \times a_{r-1} + \cdots + 2 \times a_1 + a_0$

Ora, se associarmos a N a palavra

$$X^{a_r} QX^{a_{r-1}} Q \cdots QX^{a_1} QX^{a_0}$$

e tivermos em conta que $a_r = 1$, podemos lê-la como

$$(x)\,(QX^{a_{r-1}} Q \cdots QX^{a_1} QX^{a_0})$$

[1]Trabalho realizado com a orientação de Maria Carvalho (FCUP) no âmbito de uma bolsa da Fundação para a Ciência e a Tecnologia de iniciação à investigação.

e interpretar a sua aplicação a x como a composição em sequência das operações $Q, X^{a_{r-1}}, Q, \ldots, Q, X^{a_0}$:

$$x = x^{a_r} \to x^{2a_r} \to x^{2a_r+a_{r-1}} \to x^{2^2a_r+2a_{r-1}} \cdots \to x^{2^r a_{r+2}^{\cdots-1}a_{r-1}+\cdots+2a_1+a_0} = x^N.$$

1. Notação

Se F é um símbolo funcional, escreveremos $(\alpha)F$ para designar a aplicação de F a α. Sempre que a notação se simplificar sem prejuízo da clareza do argumento, omitiremos os parênteses, escrevendo apenas αF. E, ao contrário do que é usual, descreveremos a composição de funções pela direita: assim $(\alpha)(FG)$ representa a acção de F seguida da de G na variável α.

Consideremos o operador $Q: \mathbb{R} \to \mathbb{R}$, $(\alpha)Q = \alpha^2$ e, para cada real x, a aplicação de multiplicação por x, $X: \mathbb{R} \to \mathbb{R}$, $(\alpha)X = \alpha \times x$. Por convenção, para cada x real, $x^0 = 1$. Dado um natural m e qualquer operador $T: \mathbb{R} \to \mathbb{R}$, a composta de T consigo mesmo m vezes, $T \circ T \circ \cdots \circ T$, será denotada por T^m. Como usualmente, $T^0 = Identidade$. Note-se que, no algoritmo de potenciação, quando, para calcular x^N, se usa uma palavra formada com as letras Q e QX, estamos de facto a determinar a imagem de x pelo operador composição de certos iterados de Q e de X. Por convenção, a palavra vazia I será interpretada como a *Identidade* de $\mathbb{R}$.

Finalmente relembremos que todo o número natural n pode ser representado numa base b, onde b é um inteiro maior ou igual a dois. Mais precisamente, existe um único $m \in \mathbb{Z}^+$ e existem (dígitos únicos) $a_0, a_1, \cdots, a_m$ de $\{0, 1, \cdots, b-1\}$ com $a_m \neq 0$, tais que

$$n = a_m \times b^m + a_{m-1} \times b^{m-1} + \cdots + a_1 \times b + a_0;$$

a representação de n na base b é então $a_m a_{m-1} \cdots a_1 a_{0(b)}$. Assim, na base tradicional (a decimal), os dígitos podem ser um dos dez algarismos habituais 0, 1, 2, $\cdots$, 9; neste caso é usual omitir o índice na representação, escrevendo-se apenas $n = a_m a_{m-1} \cdots a_1 a_0$. Já na base $b = 2$, a representação (binária) de n consiste numa sequência finita de 0's e 1's, sendo o dígito mais à esquerda um 1. Por exemplo, se n é representado na base 10 por 27, então, na base 2, $n = 11011_{(2)}$ pois

$$27 = 16 + 8 + 2 + 1 = 1 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1.$$

2. Justificação do algoritmo

Sejam x um real e N um natural. Mostraremos, por indução em N, que o algoritmo produz efectivamente x^N. O caso $N = 1$ é imediato: $1 = 1_{(2)}$ e, como na transcrição desta representação binária numa palavra o primeiro dígito 1 é ignorado, obtemos a palavra vazia I; logo, o resultado do algoritmo é $(x)\,Id$, que é x^1.

Fixemos agora um real x e suponha-se que, para um dado $N \in \mathbb{Z}^+$, o algoritmo dá como resultado x^N. Seja $a_r a_{r-1} \cdots a_1 a_{0(2)}$ a representação finita de N na base 2, onde $r > 0$, $a_r = 1$ e $a_i \in \{0, 1\}$ para todo o i. Temos as duas alternativas seguintes:

(I) $a_r = a_{r-1} = \cdots = a_1 = a_0 = 1$, isto é, $N = 111 \cdots 1_{(2)} = 2^{r+1} - 1$.

Neste caso $N+1 = 2^{\overbrace{\cdots}^{r}} = 1\,0\,0\cdots 0_{(2)}$, representação que tem $r+1$ zeros; a primeira e segunda etapas do algoritmo aplicadas a esta escrita binária conduzem à palavra Q^{r+1}; e portanto o algoritmo produz $(x)Q^{r+1}$. Ora, mostra-se facilmente por indução finita que

Lema 1. $\forall \alpha \in \mathbb{R} \forall m \in \mathbb{Z}_0^+ \ (\alpha)Q^m = \alpha^{2^m}$.

Prova: Fixemos um real α. Para $m=0$, a igualdade é imediata uma vez que, por convenção, $(\alpha)Q^0 = (\alpha)\,Id = \alpha = \alpha^1 = \alpha^{2^0}$. Suponhamos que a igualdade é válida para um natural m fixado. Então

$$(\alpha)Q^{m+1} = [(\alpha)Q^m]Q = (\alpha^{2^m})Q = (\alpha^{2^m})^2 = \alpha^{2^{m+1}}.\blacksquare$$

Resulta deste Lema que $(x)Q^{r+1} = x^{2^{r+1}}$, ou seja, $(x)Q^{r+1} = x^{N+1}$.

(II) *Pelo menos um dos a_i's é zero, para algum $i \in \{0,1,\cdots,r-1\}$.*

Neste caso, seja $m \in \{0,1,\cdots,r-1\}$ o menor índice tal que $a_m = 0$. Assim, na representação binária de N, há um dígito nulo na m-ésima casa seguido por m dígitos iguais a 1:

$$N = a_r \cdots a_{m+1}\,0\,1\,1\,1\cdots 1_{(2)}.$$

E portanto,

$$N+1 = a_r \cdots a_{m+1} 1\,0\,0\,0\cdots 0_{(2)}$$

onde o dígito 1 assinalado é seguido por m zeros. A transcrição de $a_r \cdots a_{m+1}$, como dita o algoritmo, dá-nos uma palavra (eventualmente vazia) que corresponde a um operador P (eventualmente a *Identidade*). Além disso, aplicando o algoritmo a N obtemos a palavra $PQ(QX)^m$; analogamente, a $N+1$ corresponde a palavra $PQXQ^m$. Ora,

$$(x)\,[PQXQ^m] = (xP)(QXQ^m)$$

e

Proposição 1. $\forall m \in \mathbb{Z}_0^+ \ QXQ^m = Q(QX)^m X$.

Prova: Fixemos um real α e um inteiro não-negativo m. Temos

$$(\alpha)QXQ^m = [(\alpha)Q]XQ^m = (\alpha^2)XQ^m = (\alpha^2 . x)Q^m$$

e, pelo Lema 1,

$$(\alpha^2 . x)Q^m = (\alpha^2 . x)^{2^m}$$

ou seja, $(\alpha)QXQ^m = \alpha^{2^{m+1}} . x^{2^m}$. Além disso,

$$(\alpha)Q(QX)^m X = [\alpha^2 (QX)^m] . x$$

e

Lema 2. $\forall\beta\in\mathbb{R}\,\forall m\in\mathbb{Z}_0^+\ (\beta)(QX)^m=\beta^{2^m}.\,x^{2^m-1}$.
Prova: Consideremos um real β. Se $m=0$, a igualdade é imediata:

$$(\beta)(QX)^0=\beta=\beta^{2^0}.\,x^{2^0-1}.$$

Suponhamos agora, por indução, que a igualdade é válida para um natural m fixado. Então

$$(\beta)(QX)^{m+1}=[(\beta)(QX)^m]\,(QX)=(\beta^{2^m}x^{2^m-1})^2.\,x=\beta^{2^{m+1}}.\,x^{2^{m+1}-1}.\blacksquare$$

Retomemos a prova da Proposição. Deduzimos já que, para todo o natural m e todo o real α,

$$(\alpha)QXQ^m=\alpha^{2^{m+1}}.\,x^{2^m}$$

e

$$(\alpha)Q(QX)^mX=[\alpha^2(QX)^m].\,x.$$

Pelo Lema 2, o segundo membro desta última igualdade pode reescrever-se como

$$[\alpha^2(QX)^m].\,x=[(\alpha^2)^{2^m}.\,x^{2^m-1}].\,x$$

logo

$$(\alpha)Q(QX)^mX=\alpha^{2^{m+1}}.\,x^{2^m}$$

e portanto

$$(\alpha)QXQ^m=(\alpha)Q(QX)^mX.\blacksquare$$

Voltemos ao caso (II) do algoritmo. Já sabemos que

$$(x)\,[PQXQ^m]=(xP)(QXQ^m);$$

resulta agora da Proposição que

$$(xP)(QXQ^m)=(xP)\,[Q(QX)^mX];$$

além disso, uma vez que a composição é operação associativa,

$$(xP)\,[Q(QX)^mX]=[(x)(PQ(QX)^m)]X;$$

e, por hipótese de indução, $(x)(PQ(QX)^m)=x^N$; logo

$$[(x)(PQ(QX)^m)]X=(x^N).\,x=x^{N+1}.$$

3. Vantagens computacionais

O algoritmo de potenciação aqui analisado é naturalmente mais vantajoso, numa perspectiva computacional, se a potência é elevada. A economia nos cálculos deve-se ao uso eficiente de potências já calculadas. Por exemplo, o modo menos rápido de se determinar 13^{53} é o de multiplicar 13 por si mesmo 52 vezes. Mas, tendo em conta que $53 = 32 + 16 + 4 + 1$, temos

$$13^{53} = 13 \times 13^4 \times 13^{16} \times 13^{32} = (((((13^2)\,13)^2)^2\,13)^2)^2\,13 = 13\,(QXQQXQQX)$$

o que requer o uso da operação de *elevar ao quadrado* cinco vezes (para se obterem 13^2, 13^4, 13^8, 13^{16} e 13^{32}) além de três *multiplicações por* 13 (ou seja, 13×13^4, $13 \times 13^4 \times 13^{16}$ e $13 \times 13^4 \times 13^{16} \times 13^{32}$), num total de 8 multiplicações em vez das 52 acima.

O algoritmo é mais eficiente quando os expoentes têm representações binárias com mais dígitos iguais a zero. Por exemplo, no cálculo de x^{256} precisamos de 8 multiplicações, uma vez que $256 = 2^8 = 100000000_{(2)}$, e portanto

$$x^{256} = x^{2^8} = (((((((x^2)^2)^2)^2)^2)^2)^2)^2$$

o que corresponde a 8 operações de elevar ao quadrado. Mas, para determinar x^{255}, precisamos de 14 multiplicações, das quais 7 são operações de elevar ao quadrado e as restantes 7 são multiplicações finais:

$$255 = 2^8 - 1 = 11111111_{(2)}$$
$$x^{255} = x \times x^2 \times x^4 \times x^8 \times x^{16} \times x^{32} \times x^{64} \times x^{128} = (((((((x^2)\,x)^2\,x)^2\,x)^2\,x)^2\,x)^2\,x)^2\,x.$$

No que se segue iremos comprovar que, dados $x \neq 0$ e $N \in \mathbb{Z}^+$, no cálculo de x^N, usando o algoritmo de potenciação, o número $\mathfrak{m}$ de multiplicações efectuadas é sempre menor ou igual a $N-1$. Note-se que $N-1$ é o número de multiplicações utilizadas para obter x^N se fizermos o produto de x por si mesmo até se chegar à potência N.

Comecemos por observar a seguinte tabela:

N	$N_{(2)}$	*Palavra*	$\mathfrak{m}$	$N-1$
1	1	I	0	0
2	10	Q	1	1
3	11	QX	2	2
4	100	Q^2	2	3
5	101	Q^2X	3	4
6	110	QXQ	3	5
7	111	$(QX)^2$	4	6

Quando $N = 1, 2$ ou 3, o valor de $\mathfrak{m}$ é $N-1$, enquanto que, para $4 \leq N \leq 7 = 2^3 - 1$, $\mathfrak{m}$ é estritamente menor que $N-1$. Na verdade esta vantagem é válida para $N \geq 4$. Verifiquemos esta afirmação para os casos não inscritos na

tabela ($N \geq 8 = 2^3 = 1000_{(2)}$).

Suponha-se que $N = a_r a_{r-1} \cdots a_1 a_{0(2)}$, onde $r > 3$, $a_r = 1$ e $a_i \in \{0, 1\}$ para $i = 0, 1, \cdots, r$. Claramente $\mathfrak{m}$ é menor ou igual ao número de multiplicações efectuadas quando aplicamos o algoritmo ao natural $11 \cdots 1_{(2)}$ que tem $r+1$ dígitos iguais a 1. Ora a palavra que resulta da transcrição desta representação binária é $(QX)^*$, e portanto o correspondente número de multiplicações é $2r$. Ou seja, em geral, $\mathfrak{m} \leq 2r$.

Por outro lado, é fácil verificar por indução que, para todo o inteiro r maior ou igual a 3, se tem $r \leq 2^{r-1} - 1$ ou, equivalentemente, $2r < 2^r - 2$. Ora, como $N > 2^r$, temos $N - 1 > 2^r - 1$, e portanto

$$\mathfrak{m} \leq 2r \leq 2^r - 2 < 2^r - 1 \leq N - 1.$$

Podemos acrescentar que, dado $N = a_r a_{r-1} \cdots a_1 a_{0(2)}$, onde $r \geq 0$, $a_r = 1$ e $a_i \in \{0, 1\}$ para $i = 0, 1, \cdots, r$, se tem

$$\mathfrak{m} = r + \sum_{i=0}^{r-1} a_i.$$

4. Generalização

O uso da base 2 nas secções anteriores não é essencial; podem estabelecer-se, por argumento idêntico, algoritmos de potenciação que utilizam a representação dos naturais noutras bases. Como anteriormente, o processo pode ser descrito pelas três etapas seguintes: dados $b \in \mathbb{Z}$, $b \geq 2$, $x \in \mathbb{R}$ e $N \in \mathbb{Z}$,

(1) escreva-se N na base b, digamos $N = c_r c_{r-1} \cdots c_1 c_{0(b)}$, onde $r > 0$, $c_r > 0$ e $c_i \in \{0, 1, \cdots, b-1\}$ para todo o i;

(2) na representação anterior, substitua-se cada c_i por X^{c_i}, sendo $X^0 = Id$, e coloque-se entre X^{c_i+1} e X^{c_i} a letra E: obtemos assim a transcrição

$$X^{c_r} E X^{c_{r-1}} E \cdots E X^{c_1} E X^{c_0};$$

(3) a palavra de (2) é agora interpretada do seguinte modo: cada E significa elevar à potência b; cada X^{c_i} corresponde a multiplicar por x^{c_i};

(4) finalmente aplique-se esta leitura ao número 1, da esquerda para a direita, fazendo actuar sucessivamente X^{c_r}, E, $X^{c_{r-1}}$, E, ..., X^{c_0}:

$$1 \to x^{c_r} \to x^{bc_r} \to x^{bc_r + c_{r-1}} \to x^{b^2 c_r + b c_{r-1}} \cdots \to x^{b^r c_r + b^{r-1} c_{r-1} + \ldots + b c_1 + c_0} = x^N.$$

Exemplos:

(a) $102 = 10210_{(3)} + XEX^0EX^2EXEX^0 \rightleftharpoons XE^2X^2EXE$

$$1 \to x \to x^3 \to x^9 \to x^{11} \to x^{33} \to x^{34} \to x^{102}.$$

(b) $102 = 204_{(7)} + X^2EX^0EX^4 \rightleftharpoons X^2E^2X^4$

$$1 \to x^2 \to x^{14} \to x^{98} \to x^{102}.$$

Referências

[1] **Robert M. Young**, *Excursions in Calculus*, Dolciani Mathematical Expositions, 13 (1992) MAA.