Proposta: Que Matemática para a Sociedade da Informação?

DI-CCTC, *Universidade do Minho*

Sumário

*Este é um texto escrito por **informáticos** preocupados com a crescente iliteracia matemática numa sociedade que, paradoxalmente, da Matemática depende cada vez mais. Mas é também um texto sobre o significado que tem "pensar matematicamente". Não o fazemos a partir do vazio, mas de um corpo de princípios e métodos que nos parece possível destilar de vários anos de investigação em Ciências da Computação e que poderá ter interesse partilhar com as comunidades mais vastas da Educação e da Matemática.*

Por isso, o texto termina com um convite para um encontro. Um desafio para um diálogo urgente.

1 Motivação

A Sociedade da Informação requer profissionais altamente qualificados que possam conceber sistemas complexos com níveis cada vez maiores de fiabilidade e segurança. Mas requer também do conjunto da sociedade um grau elevado de "fluência matemática", entendendo-se por esta a capacidade de recorrer à linguagem e ao método matemático para modelar problemas e situações e raciocinar produtivamente no interior desses modelos. Tal capacidade e literacia tornou-se um elemento fundamental da cidadania democrática.

De facto, nas Sociedades da Informação o uso efectivo da Matemática tem já, e terá cada vez mais no futuro, um enorme potencial económico. Muitos se admirariam, por exemplo, que a noção de *prova*, não raro remetida para pequenos cantos do curriculum, tivesse hoje um papel fundamental na garantia de segurança de uma compra on-line, via Internet. Ou então na certificação de que os sistemas informáticos que mantém em rota os aviões não entram em colapso. A verdade é que, como notou Dijkstra[1] , "high technology so celebrated today is essentially a mathematical technology".

Como informáticos temos consciência destes desafios e do papel insubstituível que uma educação matemática sólida e efectiva tem no desenvolvimento de um país que se queira actor, e não espectador, da progressiva globalização da Sociedade da Informação.

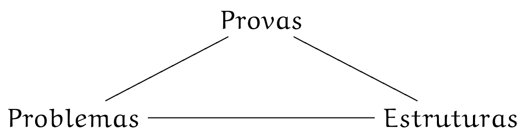
Como professores partilhamos com outros colegas de todos os níveis de ensino, a preocupação pelo facto de muitos alunos, em diferentes idades, acharem a Matemática difícil de compreender e aplicar, assim como com a relativa diminuição da atractividade de carreiras profissionais ligadas às Ciências e à Matemática. Preocupam-nos, ainda, os diversos indicadores e estatísticas que assinalam uma situação difícil no ensino da Matemática no nosso país, quando comparada com padrões internacionais. Pior que tudo, a chamada *matemático-fobia*, que parece atingir todas as camadas do tecido social, tornou-se um 'hot spot' nos meios de comunicação social.

É consensual reconhecer a necessidade de novas aproximações ao ensino/aprendizagem que facilitem a apropriação efectiva pelos alunos dos conteúdos e, sobretudo, dos métodos da Matemática e conduzam a uma maior efectividade na resolução de problemas em e com a Matemática.

[1]E. W. Dijkstra (1930-2002, prémio Turing em 1972), considerado um dos nomes mais influentes no desenvolvimento das Ciências da Computação (`www.cs.utexas.edu/users/EWD/`).

2 Um ponto de partida

A Matemática, nos seus múltiplos domínios, percorre constantemente os três vértices de um triângulo:



I.e., parte dos *problemas*, modela-os, abstrai-os e generaliza-os em *estruturas* conceptuais simples, explora-os através de métodos precisos que tornam possível raciocinar sobre problemas e estruturas e certificar formalmente a correcção desse raciocínio. A essa certificação, ou explicação objectiva, damos o nome de *prova*. Nela reside o poder da Matemática.

O foco da experiência matemática é a *resolução de problemas*. O cerne do seu método é a noção de *prova*, *i.e.*, de certificação formal de um argumento. Reparamos, porém, que uma e outra são consideradas usualmente actividades difíceis, relegadas para segundo plano na prática escolar, usadas de forma ad-hoc e largamente informal, *i.e.*, pouco capaz de ajudar os alunos a se apropriarem das ferramentas mentais e metodológicas que tornem o seu modo de raciocinar mais efectivo e produtivo.

Preocupa-nos, por exemplo, que o próprio recurso sistemático e organizado à Lógica, como ferramenta elementar de resolução de problemas, não seja treinado nem ensinado de forma explícita e sistemática em contexto escolar.

Mas que contribuição poderão dar as Ciências da Computação a este estado de coisas? Gostaríamos de sublinhar aqui, tentativamente, três aspectos: a *centralidade da Lógica*, o poder do *raciocínio formal* ou *por cálculo* e a exploração do *carácter algorítmico* de boa parte do edifício matemático. Detalhando,

- Em primeiro lugar a consciência de que a principal competência matemática requerida por quem tem de desenvolver ou utilizar produtivamente a Informática, é a do uso judicioso e *explícito* da Lógica na organização do raciocínio. Pensamos que também no processo de ensino/aprendizagem da Matemática o recurso explícito à Lógica permite aos alunos analisarem criticamente as suas construções, extraí-las construtivamente do próprio processo argumentativo e construirem explicações claras das decisões que tomam.

- Por outro lado, e ao longo dos últimos 20 anos, foram desenvolvidos métodos de construção de programas que exploram o poder da *manipulação simbólica* no raciocínio matemático. De facto, o *fazer da Matemática* baseia-se num equilíbrio dinâmico entre os processos de abstracção e construção de conceitos, por um lado, e a capacidade de manipular as expressões que constituem as suas representações simbólicas, por outro. Estes dois pólos não podem ser separados. Os símbolos exprimem ideias de forma precisa e concisa. Possuem uma dinâmica própria que guia o raciocínio rigoroso e é fonte de abstracção e generalização de problemas, conceitos e argumentos.

  Em muitas áreas da Ciência as propriedades e comportamentos de sistemas (naturais ou artificiais) são descritas por equações (ou inequações). Estas não constituem apenas uma linguagem simbólica de representação de fenómenos, mas são também objecto de regras de cálculo que, uma vez correctamente entendidas, assistem e complementam o raciocínio intuitivo na construção matemática.

  Em Matemática são muitos os exemplos onde a formalização de tópicos emergentes em diferentes contextos conduzem a fórmulas muito semelhantes que podem ser manipuladas a partir das mesmas regras lógicas, sem referência às suas interpretações específicas. Esta é a essência do raciocínio formal que permite a descoberta de generalizações e novas aplicações, a concentração no essencial e o descarte do que é contingente. Recorde-se, por exemplo, que foi através da manipulação formal das equações de Maxwell que se conjecturou a existência de ondas electromagnéticas.

O raciocínio formal, ou *por cálculo*[2], permite substituir argumentos longos e verbosos (plenos de reticências, passos não justificados e explicações fornecidas como ”óbvias”) por derivações formais curtas, fáceis de seguir, apresentadas em formato standard que facilita a reutilização, compreensão, comparação e adaptação de argumentos e estratégias.

Trata-se de um procedimento comum em Álgebra e Análise, embora seguido muitas vezes de forma implícita e não sistemática. A tomada de consciência de que pode ser igualmente aplicado à Lógica, com enorme vantagem, é uma contribuição das Ciências da Computação que têm na Lógica o seu *calculus* básico.

- Em Ciências da Computação valorizamos, ainda, um estilo de prova, dito *construtivo*, que procede pela *derivação* estrutural do resultado, por contra-posição ao estilo mais clássico baseado na enunciação de um teorema seguida da sua *verificação*. Na sub-secção 3.2 ilustramos este modo de raciocinar numa aplicação à Matemática escolar.

  Este estilo é sobretudo útil para explorar o carácter *algorítmico* comum a boa parte do edifício matemático. Característica que poderá ser explorada na resolução de problemas e na construção de conhecimento matemático. Note-se que, apesar dos algoritmos serem estudados desde o início das civilizações, o advento da era digital revolucionou a sua natureza e importância. A prática de várias décadas no desenvolvimento sistemático de algoritmos a partir de descrições mais ou menos informais de problemas, poderá ter repercussões interessantes para o ensino da Matemática.

Na secção seguinte ilustramos através de pequenos exemplos, a aplicação de alguns destes princípios. Parece-nos ser essa a maneira mais directa de comunicarmos aquilo que nos move: a consciência de que o *método* da Matemática, mais até que os seus *conteúdos*, é essencialmente uma ferramenta para a descoberta e a argumentação rigorosa que constitui, ao fim e ao cabo, a essência de cultura científica.

Antes, porém uma pequena nota para dizer que, no âmbito de dois projectos de doutoramento conjunto entre a Universidade do Minho (DI-CCTC) e a University of Nottingham, está a ser desenvolvida uma ferramenta para registo e manipulação de fórmulas matemáticas manuscritas. Resumidamente, o eventual utilizador será capaz de escrever manualmente expressões matemáticas no ecrã de um Tablet PC (ou de outro dispositivo que aceite input através de uma caneta) que serão reconhecidas por software, possibilitando uma manipulação automática e confiável da sua estrutura. Esta ferramenta, apesar de ainda se encontrar numa fase inicial, irá facilitar a escrita de texto matemático, como se manuscrito numa folha de papel, assistir no ensino das técnicas calculacionais em Lógica e na resolução de problemas, aumentando, deste modo, a capacidade de cada aluno se exprimir e raciocinar em Matemática.

3 Alguns exemplos

3.1 O pastor, a ovelha, o lobo e a couve

O primeiro exemplo, retomando um enunciado bem conhecido, põe em relevo um aspecto que é muito caro aos informáticos: a importância de uma correcta *modelação do problema* para evitar o recurso à “força bruta”. Ilustra-se aqui um princípio importante para a resolução eficaz de problemas, a saber, *evitar distinções desnecessárias.*

> *Um pastor tem que atravessar um rio, levando consigo uma ovelha, uma couve e um lobo. Porém, o seu barco só lhe permite levar um acompanhante de cada vez, fazendo com que várias viagens sejam necessárias. Além disso, a ovelha não pode ficar sozinha com a couve, nem o lobo pode ficar sozinho com a ovelha.*
>
> *Como é que o pastor pode concretizar a sua tarefa?*

[2] A expressão *cálculo* não tem aqui, obviamente, qualquer conotação com *repetição exaustiva de “exercícios de aplicação”* tão ao gosto de certos manuais escolares.

Normalmente, as soluções para este problema consideram os quatro indivíduos e, como cada um deles pode estar numa das duas margens, o número de estados possíveis (incluindo estados inválidos) é de 16 (2^4). Note-se que se o problema lidasse com 10 indivíduos, o número total de estados aumentaria para 1024 (2^{10}).

Este rápido aumento do número de estados é frequentemente causado por uma má análise do problema e pela existência de distinções desnecessárias. De facto, analisando o enunciado do problema com cuidado, notamos que existe uma simetria entre o lobo e a couve, pois nenhum deles pode ser deixado com a ovelha. Esta simples observação permite-nos reescrever o enunciado sem distinguir esses dois indivíduos. Sendo assim, se designarmos a ovelha por "alfa"e o lobo e a couve por "betas", temos o seguinte problema equivalente:

> *Um pastor tem que atravessar um rio, levando consigo um alfa e dois betas. Porém, o seu barco só lhe permite levar um acompanhante de cada vez, fazendo com que várias viagens sejam necessárias. Além disso, o alfa não pode ficar sozinho com um beta.*
>
> *Como é que o pastor pode concretizar a sua tarefa?*

Não é difícil ver que a solução deste segundo problema é única e muito mais simples: o pastor atravessa o alfa e volta sozinho; atravessa um beta e volta com o alfa; atravessa o segundo beta e volta sozinho; finalmente, atravessa o alfa.

Assim, há duas soluções para o problema original que correspondem às duas possíveis escolhas para o primeiro beta a ser atravessado: o lobo ou a couve.

3.2 Bagatela com logaritmos

Este segundo exemplo visa ilustrar o estilo de prova *construtiva* que referimos acima. Introduz, também, a notação que usamos para apresentar os nossos cálculos. O problema é um exercício muito simples:

> *Será* $\ln(2) + \ln(7)$ *superior ou inferior a* $\ln(3) + \ln(5)$*?*

Um modo de atacar esta questão consiste em formular a hipótese $\ln(2) + \ln(7) \leq \ln(3) + \ln(5)$ e verificá-la do seguinte modo:

(1)	A função $\ln$ é estritamente crescente	
(2)	$\ln(x \times y) = \ln(x) + \ln(y)$	
(3)	$14 < 15$	
(4)	$14 = 2 \times 7$ e $15 = 3 \times 5$	
(5)	$\ln(14) < \ln(15)$	por (1) e (3)
(6)	$\ln(2) + \ln(7) < \ln(3) + \ln(5)$	por (2), (4) e (5)

O argumento é fácil de seguir e verificar, mas fornece pouca intuição sobre o problema. Além disso não é simples de recordar nem de reproduzir. Note-se, ainda, que, muito provavelmente, a prova não foi feita pela ordem em que é apresentada. Talvez por isso suscite reduzida adesão dos alunos.

Vejamos, agora, o que seria uma abordagem *construtiva* ao problema. Note-se, em primeiro lugar, que não se parte de uma hipótese (mais ou menos diligentemente enunciada) mas da própria questão a que se pretende responder.

A prova inicia-se pela identificação da incógnita $\Box$ (que não representa um número, como os alunos estão habituados na matemática escolar, mas uma relação de ordem) e desenvolve-se pela identificação e aplicação de propriedades que permitam determiná-la. Note-se, ainda, que toda a prova, evoluindo por manipulação sintáctica, é construtora de intuição e significado.

$$
\begin{array}{ll}
 & \mathrm{ln}(2) + \mathrm{ln}(7) \;\square\; \mathrm{ln}(3) + \mathrm{ln}(5) \\
= & \quad \{ \text{ a função } \mathrm{ln} \text{ distribui pela multiplicação } \} \\
 & \mathrm{ln}(2 \times 7) \;\square\; \mathrm{ln}(3 \times 5) \\
= & \quad \{ \text{ aritmética } \} \\
 & \mathrm{ln}(14) \;\square\; \mathrm{ln}(15) \\
= & \quad \{ \text{ } 14 < 15 \text{ e a função } \mathrm{ln} \text{ é estritamente crescente } \} \\
 & \square \;\text{ é }\; <
\end{array}
$$

3.3 Um bispo no tabuleiro do xadrez

Consideremos um novo exemplo de raciocínio por cálculo na resolução de um problema sobre o jogo do xadrez.

> *No jogo do xadrez, o bispo move-se ao longo das diagonais. Mostre que, se mover um bispo, a casa para onde ele se desloca tem a mesma cor da casa inicial.*

Toda a resolução do problema parte de uma adequada *modelação* e da explicitação de uma propriedade *invariante*:

> *Propriedade*: Se usarmos coordenadas cartesianas para as casas do tabuleiro e se ao canto inferior esquerdo corresponder a coordenada $(0,0)$, então podemos dizer que uma casa (i,j) é preta se as paridades de i e de j forem as mesmas (ou são ambos pares, ou são ambos ímpares).

Consideremos, então, o problema: provar que a cor da casa para onde o bispo se desloca é a mesma da casa inicial. Não é difícil ver que se um bispo se encontra na casa (i,j), então pode-se deslocar uma distância k (positiva ou negativa) para a posição $(i+k, j+k)$ ou para a posição $(i+k, j-k)$ — desde que fique dentro do tabuleiro. Assim, o objectivo é provar que as casas (i,j), $(i+k, j+k)$ e $(i+k, j-k)$ têm todas a mesma cor. Para isso, usamos a propriedade acima para definir a função preta que, dada uma casa, devolve $\mathrm{verdadeiro}$ se ela é preta e falso se ela é branca[3]. Formalmente,

$$\mathrm{preta}(i,j) = (\mathrm{par}(i) \equiv \mathrm{par}(j))$$

Esta função permite a formalização do nosso objectivo de uma forma muito compacta.

Provemos primeiro que as casas (i,j) e $(i+k, j+k)$ têm a mesma cor, i.e.,

$$\mathrm{preta}(i,j) = \mathrm{preta}(i+k, j+k)$$

Assim

$$
\begin{array}{ll}
 & \mathrm{preta}(i+k, j+k) \\
= & \quad \{ \quad \text{definição da função } \mathrm{preta} \quad \} \\
 & \mathrm{par}(i+k) \equiv \mathrm{par}(j+k)
\end{array}
$$

[3] Assumimos a existência de uma função par que, dado um número, devolve $\mathrm{verdadeiro}$ se esse número é par e falso se é ímpar. O símbolo $\equiv$ denota igualdade booleana (i.e., $a \equiv b$ só é verdadeiro se a e b forem ambos verdadeiros ou ambos falsos)

$$
\begin{array}{cll}
= & \{ & \text{a função } par \text{ distribui pela adição, i.e., para todo o } i \text{ e } k\text{:} \\
  &   & par(i+k) \equiv par(i) \equiv par(k) \quad \} \\
  & \multicolumn{2}{l}{par(i) \equiv par(k) \equiv par(j) \equiv par(k)} \\
= & \{ & \text{a equivalência é associativa, simétrica, e reflexiva } \} \\
  & \multicolumn{2}{l}{par(i) \equiv par(j)} \\
= & \{ & \text{definição da função } preta \ \} \\
  & \multicolumn{2}{l}{preta(i,j)}
\end{array}
$$

Provámos em quatro passos que as casas (i,j) e $(i+k, j+k)$ têm a mesma cor. Cada passo é uma equivalência e a justificação é dada entre chavetas. Por exemplo, o primeiro passo diz que a expressão $preta(i+k, j+k)$ é equivalente à expressão $par(i+k) \equiv par(j+k)$, por definição da função $preta$. Por outro lado, no terceiro passo utilizamos propriedades da relação de igualdade booleana para remover a sub-expressão $par(k)$. Finalmente, por transitividade da relação de igualdade booleana concluimos que a primeira expressão — $preta(i+k, j+k)$ — é equivalente à última — $preta(i,j)$ (i.e., as casas (i,j) e $(i+k, j+k)$ são ambas pretas ou são ambas brancas).

Sugerimos ao leitor que, de modo similar, verifique que (i,j) e $(i+k, j-k)$ têm a mesma cor, e que cada jogada de um cavalo é para uma casa de cor diferente da original.

3.4 Um problema sobre divisibilidade

O exemplo seguinte mostra que um formato de prova conciso, juntamente com o uso da lógica equacional, permite construir argumentos mais concisos, informativos e rigorosos. Veremos, em particular, de que forma permite evitar o recurso a argumentos por *dupla implicação* que, apesar de usados recorrentemente, dificultam a compreensão da prova.

Consideremos, pois, o seguinte lema e respectiva prova, extraídos da página 39 do livro "Elementary Number Theory" de Gareth A. Jones e J. Mary Jones (Springer, 1998). No que se segue a expressão $a = b \pmod{n}$ significa que a e b são congruentes módulo n, i.e., a e b têm o mesmo resto na divisão inteira por n. Também usamos a barra \ para denotar a relação de divisão. Assim, $n \backslash (a-b)$ significa que n divide o inteiro $a-b$, i.e., existe um inteiro k tal que $n \times k = a - b$.

Lema 3.1
Para qualquer $n \geq 1$ *temos que* $a = b \pmod{n}$ *se e só se* $n \backslash (a-b)$.

Prova
Escrevendo $a = q \times n + r$ *e* $b = q' \times n + r'$, *temos que* $a - b = (q - q') \times n + (r - r')$ *com* $-n < r - r' < n$. *Se* $a = b \pmod{n}$, *então* $r = r'$, *i.e.,* $r - r' = 0$. *Temos então* $a - b = (q - q') \times n$, *que é divisível por* n. *Conversamente, se* n *divide* $a - b$, *então divide* $(a - b) - (q - q') \times n = r - r'$; *como* 0 *é o único inteiro estritamente entre* $-n$ *e* n *que é divisível por* n, *temos que* $r - r' = 0$. *Então,* $a = b \pmod{n}$.

Vejamos agora como podemos reescrever esta prova, utilizando um formato mais conciso e evitando a dupla implicação:

Prova
Escrevendo $a = q \times n + r$ e $b = q' \times n + r'$, temos que $a - b = (q - q') \times n + (r - r')$ com $-n < r - r' < n$. Então,

$$
\begin{array}{cll}
& n \backslash (a-b) & \\
= & \{ & \text{porque } a-b=(q-q')\times n+(r-r') \quad \} \\
& n \backslash ((q-q')\times n+(r-r')) & \\
= & \{ & \text{propriedade da divisão inteira} \quad \} \\
& n \backslash (r-r') & \\
= & \{ & \text{temos que } -n<r-r'<n \text{ e } 0 \text{ é o único inteiro estritamente} \\
& & \text{entre } -n \text{ e } n \text{ que é divisível por } n \quad \} \\
& r-r'=0 & \\
= & \{ & r-r'=0 \equiv r=r' \text{ e definição de congruência} \quad \} \\
& a=b \pmod{n} &
\end{array}
$$

Em apenas quatro passos provámos o lema, utilizando as mesmas propriedades da prova original. Além disso, concluímos imediatamente que quaisquer duas expressões das cinco apresentadas são equivalentes.

3.5 Tetraminós e invariantes

O nosso último exemplo recorre a uma técnica muito importante na concepção de algoritmos e que acaba por ter um espectro de utilização muito vasto na resolução de problemas em Matemática. Trata-se do recurso a propriedades *invariantes*. Um invariante é uma propriedade que se mantém constante. O exemplo ilustra como é que invariantes, aliados com o nosso formato de prova, são úteis na resolução de problemas.

> *Um tetraminó é uma figura geométrica composta por 4 quadrados do mesmo tamanho. Supondo que um tabuleiro rectangular é coberto por tetraminós, mostre que pelo menos um dos lados do tabuleiro tem um número par de quadrados.*

É fácil ver que quando se coloca um tetraminó no tabuleiro, o número de quadrados cobertos aumenta 4. Assim, um invariante deste problema é que o número de quadrados cobertos é um múltiplo de 4.

Usando este invariante, a solução do problema é imediata:

$$
\begin{array}{cll}
& \text{um tabuleiro } m\times n \text{ está coberto por tetraminós} & \\
\Rightarrow & \{ & \text{invariante: o número de quadrados cobertos é um múltiplo de 4;} \\
& & \text{há } m\times n \text{ quadrados cobertos} \quad \} \\
& m\times n \text{ é múltiplo de 4} & \\
\Rightarrow & \{ & \text{propriedade de múltiplos} \quad \} \\
& m \text{ é múltiplo de 2} \quad \vee \quad n \text{ é múltiplo de 2} &
\end{array}
$$

Note-se, de passagem, que o formato de cálculo que utilizamos permite escrever implicações da mesma forma que escrevemos equivalências.

4 Uma proposta

Esperamos ter conseguido nas secções acima dar uma ideia de uma abordagem à resolução de problemas que, cultivada nas Ciências da Computação, nos parece ter algum potencial para o Ensino da Matemática nos anos terminais do Ensino Básico e no Ensino Secundário.

As preocupações e as linhas deste texto são comuns a outros grupos de investigação em departamentos de Ciências da Computação em diversas universidades europeias com quem temos contacto. Mas serão elas relevantes para quem tem no dia-a-dia a missão de ensinar Matemática e, sobretudo, de estimular a capacidade de *pensar matematicamente*?

Estamos convencidos ser essa capacidade, mais que qualquer pretensa literacia informática ou tecnológica, a pedra de toque do sucesso pessoal e social na complexidade da Sociedade da Informação.

Gostaríamos, pois, de iniciar um diálogo com alguns professores de diferentes níveis de ensino. Por isso lançamos o convite para uma *workshop* informal onde nos propomos

- apresentar e ilustrar este tipo de abordagem,
- aplicá-la a um conjunto de problemas,
- situá-la numa breve incursão na História da Matemática,
- apresentar algumas ideias de ferramentas computacionais capazes de a apoiarem.

Aqui fica o convite:

Workshop: Que Matemática para a Sociedade da Informação?

Sábado, 29 de Março, 2008 (9.30h — 18.00h)
Departamento de Informática

Campus de Gualtar (Braga) da Universidade do Minho

(confirmar para Luís S. Barbosa: `lsb@di.uminho.pt`)