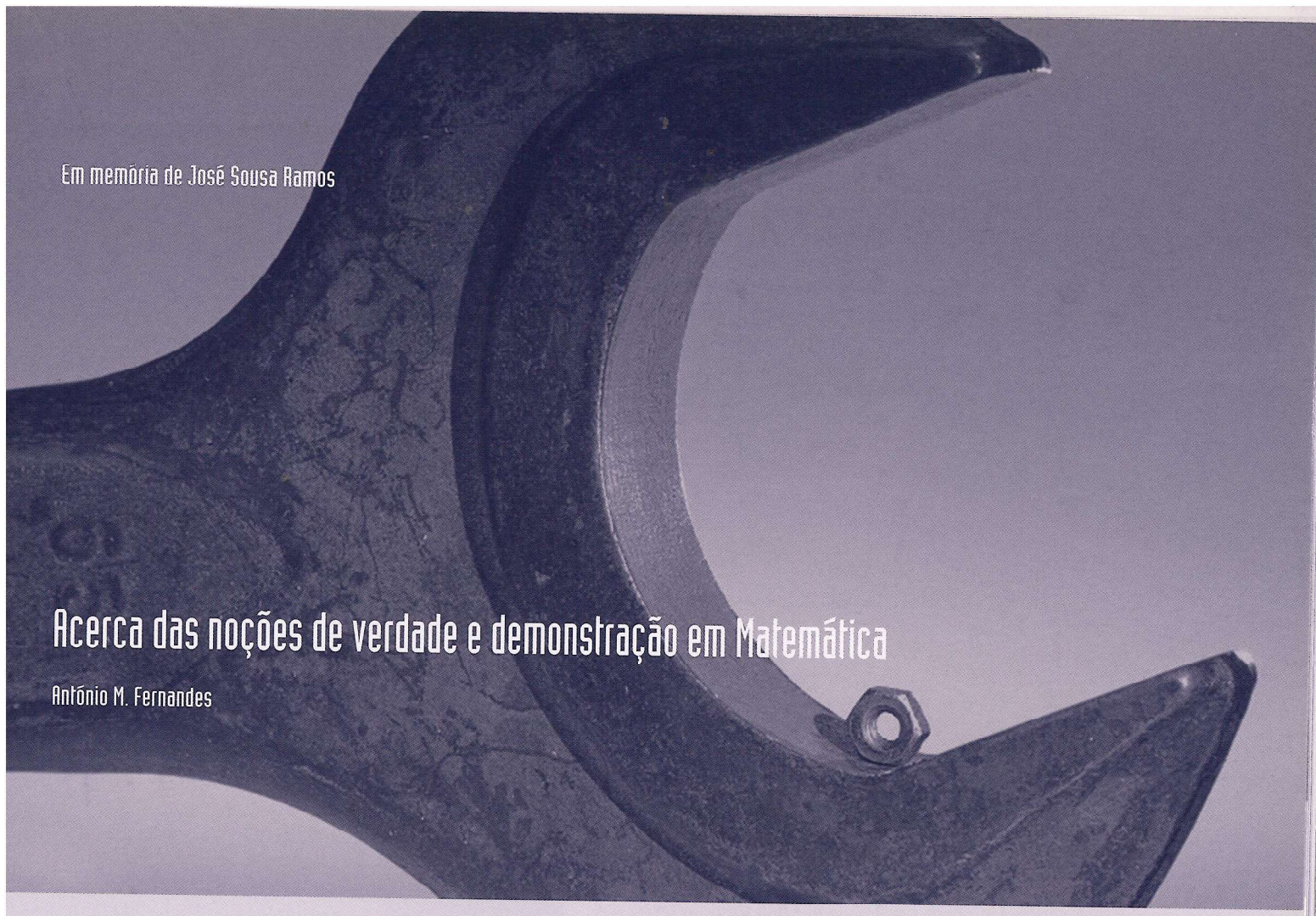

Em memória de José Sousa Ramos

Acerca das noções de verdade e demonstração em Matemática

António M. Fernandes

A matemática contemporânea tem lugar num grande sistema fundacional originalmente idealizado por Georg Cantor (1845–1918) que, à semelhança da geometria euclidiana (em certa medida, o primeiro sistema fundacional), também é descrito através de axiomas. Inicialmente proposto por Ernest Zermelo (1871–1953) em 1904, o conjunto de axiomas foi mais tarde completado e reformulado por Zermelo e Fraenkel, em 1908. Falamos da teoria de conjuntos de Zermelo-Fraenkel e podemos, de forma razoavelmente aproximada, dizer que a Matemática consiste no estudo das propriedades das *estruturas* que se podem descrever nesta teoria. Este artigo tem duas personagens centrais, uma *teoria* e uma *estrutura*, que conjuntamente trarão, assim se espera, alguma luz sobre as noções de *verdade* e *demonstração*.

Consideremos a estrutura privilegiada para o desenvolvimento da aritmética, que é precisamente a estrutura dos números naturais $(\mathbb{N}, S, +, \times, \leq, 0)$ que, abreviadamente, representaremos apenas por $\mathbb{N}$. Aqui $+$ e $\times$ são as operações binárias de adição e multiplicação. A relação binária $\leq$ é a relação de ordem em $\mathbb{N}$ e S é a operação de sucessor, que a cada natural faz corresponder o natural que imediatamente lhe sucede na ordem dos naturais. Finalmente 0 é o número natural *zero*. Apesar de parecer muito simples, a estrutura é muito rica, como o atesta a complexidade da teoria dos números.

À estrutura $\mathbb{N}$, como a qualquer outra (com diferentes operações e relações), corresponde uma *linguagem* na qual se formulam todas as asserções que, uma vez demonstradas constituem os teoremas acerca dos números naturais. Esta linguagem, no caso em apreço, é também designada por *linguagem da aritmética* e consiste numa combinação de *símbolos lógicos* $(\forall, \exists, \wedge, \vee, \neg, \Rightarrow, \Leftrightarrow)$, de variáveis $(x, y, z, \ldots)$ e dos símbolos $+$, $\times$, $\leq$ e 0. As combinações de símbolos que são relevantes na descrição de aspectos da estrutura $\mathbb{N}$ designam-se *termos* e *fórmulas*.

Os termos podem descrever-se indutivamente de acordo com o seguinte: (1) as variáveis são termos; (2) o símbolo 0 é um termo; (3) se t_1 e t_2 são termos, então $t_1 + t_2$, $t_1 \times t_2$ e $S(t_1)$ são termos. Todos os termos são obtidos através de (1)–(3), acima. (Note-se que, quando substituímos as variáveis por elementos de $\mathbb{N}$, obtemos depois de executar as operações indicadas pelo termo, um elemento de $\mathbb{N}$, que é a sua *interpretação*, relativamente à atribuição de valores às variáveis que foi considerada.) As fórmulas, por sua vez, são descritas pelas seguintes cláusulas: (1) se t_1 e t_2 são termos, então $t_1 < t_2$ e $t_1 = t_2$ são fórmulas; (2) se φ e ψ são fórmulas, então $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \Leftrightarrow \psi$, $\varphi \Rightarrow \psi$ e $\neg\varphi$ são fórmulas; (3) se φ é uma fórmula e x é uma variável, então $(\forall x)\varphi$ e $(\exists x)\varphi$ são fórmulas.

Detenhamo-nos por breves instantes na descrição mais detalhada do significado dos diferentes símbolos lógicos envolvidos na *construção* das fórmulas. As variáveis representam elementos genéricos do domínio em causa, neste caso, representam números naturais. Os símbolos $\wedge$ e $\vee$ representam a conjunção e a disjunção, respectivamente. Assim, $\varphi \wedge \psi$ *significa* "φ e ψ", enquanto que $\varphi \vee \psi$ *significa* "φ ou ψ". Continuando, $\varphi \Rightarrow \psi$ *significa* "se φ então ψ" e $\varphi \Leftrightarrow \psi$ *significa* "φ se e só se ψ". O símbolo $\neg$ representa a *negação*, pelo que $\neg\varphi$ *significa* "não φ". Os símbolos $\forall$ e $\exists$ designam-se de *quantificadores*. Uma fórmula como $(\exists x)\varphi$ *significa* "existe pelo menos um x tal que φ", enquanto que $(\forall x)\varphi$ *significa* "para todo o x tem-se φ".

Se considerarmos uma fórmula como por exemplo $(\exists x)S(x) = y$ ela não parece dizer nada acerca de $\mathbb{N}$. Em certo sentido parece *incompleta*, como se não fosse possível dizer nada acerca do seu valor semântico, sem que se saiba antes quem é y. De facto não pode mas, para cada concretização de y já é possível dizer se estamos perante uma asserção verdadeira ou falsa. Por exemplo, quando atribuímos à variável y o valor 0, a fórmula é falsa já que nenhum número natural tem 0 como sucessor.

A variável y na fórmula acima, que não aparece quantificada, diz-se uma *variável livre*. O fenómeno anterior generaliza-se e se $\phi(x_1, \ldots, x_n)$ é uma fórmula em que as variáveis livres são $x_1, \ldots, x_n$ então, escrevemos $\mathbb{N} \vDash \phi(x_1, \ldots, x_n)[a_1, \ldots, a_n]$ para indicar que a fórmula $\phi(x_1, \ldots, x_n)$ é verdadeira em $\mathbb{N}$ quando se atribui o valor a_i à variável x_i, com $i = 1, \ldots, n$. Uma fórmula como por exemplo $(\exists x)(\forall y)x \leq y$ não tem variáveis livres. Uma tal fórmula diz-se uma *sentença*. A verdade de uma sentença numa estrutura não depende de nenhuma atribuição de valores às variáveis. Voltando ao exemplo anterior, a sentença $(\exists x)(\forall y)x \leq y$ que afirma a existência de um elemento menor que todos os outros, é claramente verdadeira em $\mathbb{N}$, e não tem sequer cabimento qualquer atribuição de valores às variáveis já que, nenhuma delas é livre. Neste caso se φ é uma sentença verdadeira em $\mathbb{N}$ escrevemos $\mathbb{N} \vDash \varphi$.

Na estrutura $\mathbb{N}$ são verdadeiros todos os axiomas de uma teoria muito simples, designada por *aritmética de Robinson* que denotamos abreviadamente por Q. Os axiomas são:

(1) $(\forall x)S(x) \neq 0$
(2) $(\forall x)(\forall y)[S(x) = S(y) \Rightarrow x = y]$
(3) $(\forall x)[x \neq 0 \Rightarrow (\exists y)x = S(y)]$
(4) $(\forall x)x + 0 = x$
(5) $(\forall x)(\forall y)[x + S(y) = S(x + y)]$
(6) $(\forall x)x \times 0 = 0$
(7) $(\forall x)(\forall y)[x \times S(y) = x \times y + x]$
(8) $(\forall x)(\forall y)[x \leq y \Leftrightarrow (\exists z)z + x = y]$.

A teoria Q é muito fraca, de facto os seus axiomas não são suficientes para demonstrar a associatividade da operação de multiplicação, ou seja, usando os axiomas (1)–(8) acima, não se pode demonstrar a sentença $(\forall x)(\forall y)(\forall z)[(x \times y) \times z = x \times (y \times z)]$. Assim sendo, não permitem demonstrar todas as *verdades* do modelo $\mathbb{N}$ (por exemplo a associatividade de $\times$).

Gottfried Wilhelm von Leibniz

Poderíamos ser levados a pensar que os axiomas da aritmética de Robinson são simplesmente uma má escolha, e que é possível encontrar uma axiomática que permita demonstrar todas as verdades da estrutura $\mathbb{N}$. Como veremos isso não é assim.

Os resultados limitativos de Tarski e Gödel

Gottfried Wilhelm von Leibniz (1646–1716) pode ser considerado um génio universal. De facto, ele desenvolveu trabalho notório em áreas tão distintas como a História, o Direito, a Filosofia Especulativa, a Metafísica e a Matemática. Leibniz imaginou todo um programa que permitiria, de acordo com as suas próprias expectativas, aceder à *verdade*. De certo modo, o *programa* Leibnitziano é uma antevisão do que se passaria no início do Séc. XX em torno dos fundamentos da Matemática. Tal como Frege, muitos anos depois, Leibniz vislumbrou a necessidade de uma linguagem, diferente da língua natural, onde as proposições pudessem ser descritas— a *characteristica universalis*. Esta linguagem deveria constituir um meio para descrever factos através de símbolos. Esses símbolos seriam *manipulados* combinatorialmente através de um cálculo—o *calculus raticinator*—, cálculo esse cujo propósito final seria o de obter todas as proposições verdadeiras. Alguns anos mais tarde George Boole (1815–1864)

Alfred Tarski

Kurt Gödel

cumpriria parcialmente as aspirações de Leibniz e conseguiu algebrizar as leis básicas da lógica, fundado aquilo que hoje se conhece sob a designação de *álgebras de Boole*.

A lógica e matemática modernas de certo modo adaptaram a visão de Leibniz, através da formalização da noção de demonstração e da possibilidade de verificar efectivamente se uma dada sequência de sentenças de uma determinada linguagem formal (por exemplo da linguagem da aritmética, que entretanto descrevemos) é ou não uma demonstração. Evitando entrar em demasiados detalhes, uma demonstração de uma sentença φ é uma sequência finita de sentenças $(\psi_1, \psi_2, \ldots, \psi_n)$, onde φ é ψ_n (a última sentença da sequência). A sequência não pode ser arbitrária (como é de esperar), efectivamente, cada sentença ψ_i que surge na sequência ou é um axioma, ou então, resulta da aplicação de alguma *regra dedutiva* a sentenças que ocorrem antes de ψ_i na sequência. Não querendo entrar em grandes explicações sobre a natureza das regras dedutivas, diremos apenas que se tratam de formas muito básicas de concluir factos a partir de premissas, por exemplo, a regra *modus ponens*, que está relacionada com o silogismo aristotélico, permite concluir φ, a partir das hipóteses θ e $\theta \Rightarrow \varphi$. De uma maneira geral, se de uma lista de axiomas Γ se pode demonstrar uma sentença φ, escrevemos $\Gamma \vdash \varphi$.

Retomemos a nossa discussão acerca da estrutura $\mathbb{N}$ e da teoria Q de Robinson. É, talvez, surpreendente que uma teoria que não consegue demonstrar a associatividade da operação de multiplicação, possa servir para representar as funções computáveis. Podemos aqui entender por função *computável* uma função $f : \mathbb{N} \to \mathbb{N}$ para a qual existe um programa de computador tal que, uma vez dado o valor n o programa é executado e *devolve* o valor $f(n)$. A suficiência de Q para interpretar as funções computáveis pode então exprimir-se do seguinte modo: considerada uma função computável f, existe um termo da linguagem $\mathcal{L}$, digamos $t(x)$ tal que $f(n) = m$ se e só se, é possível demonstrar na teoria de Robinson que $t(\mathbf{n}) = \mathbf{m}$ onde, para cada natural $n \in \mathbb{N}$, estamos a denotar por $\mathbf{n}$ o termo que é interpretado por n em $\mathbb{N}$, isto é, $\mathbf{0} = 0$, $\mathbf{1} = S(0)$, $\mathbf{2} = S(S(0))$, e assim sucessivamente.

Usando este facto, é possível codificar em Q, as noções sintácticas, como termos e fórmulas. Ou seja, podem representar-se esses objectos através de números. De uma maneira geral dada uma fórmula φ ou um termo t, denotam-se por $\ulcorner \varphi \urcorner$ e por $\ulcorner t \urcorner$ os respectivos códigos (ou números de Gödel, como também se diz). A própria noção de *demonstração* pode ser formalizada e interpretada Q, o que corresponde a dizer que podem descrever-se fórmulas $\mathrm{Term}(x)$, $\mathrm{Form}(x)$

e $\mathrm{Dem}(x, y)$ tais que $Q \vdash \mathrm{Term}(\mathbf{n})$ se e só se n é o código de um termo; $Q \vdash \mathrm{Form}(\mathbf{n})$ se e só se n é o código de uma fórmula e, $Q \vdash \mathrm{Dem}(\mathbf{m}, \mathbf{n})$ se e só m codifica uma demonstração (a partir dos axiomas de Q) da sentença cujo código é n. O resultado que se menciona a seguir foi frutuosamente explorado por Gödel que dele soube extrair consequências significativas. Ele corresponde, de certo modo, a uma formalização do conhecido *paradoxo do mentiroso*.

Lema diagonal. *Se T é uma teoria que contém Q então para qualquer fórmula $\varphi(x)$ da linguagem de T existe uma sentença θ* tal que $T \vdash \theta \Leftrightarrow \varphi(\ulcorner \theta \urcorner)$.

Quando escrevemos $\varphi(\ulcorner \theta \urcorner)$ estamos de facto a escrever $\varphi(\mathbf{n})$, que é o resultado de substituir todas as ocorrências da variável x em φ pelo termo $\mathbf{n}$, sendo que $n = \ulcorner \theta \urcorner$.

Este resultado permite concluir o seguinte,

Se T *é uma teoria consistente que estende* Q, *então o conjunto dos teoremas de* T *não se pode definir em* T. *Mais precisamente o conjunto* $\Gamma = \{\ulcorner \theta \urcorner : \mathrm{T} \vdash \theta\}$ *não é definível em* T.

Isto significa que não existe uma fórmula $\Psi(x)$ da linguagem de T tal que dado n se tem $n \in \Gamma$ se e só se $T \vdash \Psi(\mathbf{n})$ e $n \notin \Gamma$ se e só se $T \vdash \neg\Psi(\mathbf{n})$.

Os resultados limitativos sucedem-se, a partir daqui, em catadupa.

O conjunto de todas as proposições verdadeiras em $\mathbb{N}$ *não se pode definir em* T, *seja qual for a extensão* T *de* Q.

Em particular, o conjunto de todas as proposições verdadeiras na estrutura $\mathbb{N}$ não pode ser determinado por um programa de computador, ou seja, não é decidível (o que destrói o sonho de Leibniz).

É neste momento possível estabelecer um distinção essencial entre as noções de *verdade* e *demonstração*. Já vimos que a teoria Q não é suficiente para que, a partir dos seus axiomas se possam demonstrar todas as *verdades* da estrutura $\mathbb{N}$. Os resultados anteriores, porém, revelam que não é possível completar esse conjunto de axiomas de modo a que todas as verdades da estrutura $\mathbb{N}$ possam ser capturadas por demonstração. A razão é simples: para que uma axiomática T possa capturar a verdade numa estrutura ela tem que ser *completa*, ou seja, dada uma sentença φ, tem-se uma de duas alternativas, ou $\mathrm{T} \vdash \varphi$ ou $\mathrm{T} \vdash \neg\varphi$. Isto deve-se ao simples facto de que numa estrutura ou uma proposição ou a sua negação são verdadeiras (mas não ambas, é claro!). Ora, é possível demonstrar que se uma axiomática é completa então o conjuntos dos seu teoremas é decidível e, consequentemente definível mas, já se viu que o conjunto das verdades de $\mathbb{N}$ (ou de qualquer outra estrutura mais complexa) não é definível.

Este resultado é um dos *teoremas da incompletude de Gödel*. Em última análise revela que a matemática não é axiomatizável num sentido que permita, para qualquer sentença φ, demonstrar φ ou a respectiva negação. Ou seja, a decisão acerca da verdade de certas proposições permanecerá sempre inacessível a qualquer sistema axiomático que venha a ser proposto.

Conclusão

Os resultados enunciados anteriormente parecem configurar uma insuficiência do sistema axiomático. Curiosamente, a axiomática proposta por Euclides é completa e, consequentemente, decidível. Isto significa que podemos colocar um computador a funcionar e esperar que ele determine todos os teoremas da geometria Euclidiana. Isto não significa que essa seria a melhor atitude a tomar, o computador seguiria uma estratégia pré-estabelecida e certamente aconteceria que os teoremas interessantes não surgissem em tempo útil. De qualquer modo, a geometria euclidiana é claramente insuficiente para as necessidades da matemática actual, de facto, insuficiente para a matemática depois de Newton. Qualquer sistema fundacional moderno será sempre incompleto. Os axiomas da teoria de conjuntos são, por exemplo, insuficientes para determinar a estrutura dos números reais. Por outro lado, é ainda um problema em aberto, o de saber se os axiomas da teoria de conjuntos são suficientes para determinar a verdade em $\mathbb{N}$.

Pode então perguntar-se porque é a matemática tão atraída por sistemas axiomáticos, sendo que, como se sabe, eles são essencialmente incompletos. Bom, existem duas razões uma mais empírica, outra mais metodológica. De facto foram tentadas fundamentações não axiomáticas. A mais notável, levada a cabo por Georg Cantor, que tentou fundar a teoria de conjuntos sobre uma definição directa da noção de conjunto. A tentativa não resistiu ao famoso paradoxo de Russell e ficou claro que não seria fácil remediar essa definição, cujo propósito era o de caracterizar a *essência* da noção de conjunto.

Sabemos, depois de Gödel, que não é possível estabelecer matematicamente a consistência lógica da própria matemática, ou seja, demonstrar que uma contradição não pode ser deduzida dos axiomas da teoria de conjuntos. Mesmo assim, o conhecimento organizado em torno de uma estrutura axiomática é certamente aquele que melhor pode contornar a descoberta de algum tipo de inconsistência. De facto, analisando a estrutura da prova de inconsistência e analisando a estrutura dos axiomas, seria certamente possível determinar a origem da inconsistência e remediá-la. Pelo menos, será mais fácil alcançar este propósito, por esta via.

Em suma, o método axiomático é o método mais seguro para estabelecer conhecimento válido, por outro lado, pela sua natureza incompleta, obriga-nos a aperfeiçoar os nossos sistemas de forma continuada, numa tarefa que nunca estará acabada.

Deste modo a Matemática constitui certamente a forma mais *segura* de conhecimento mas, longe de ser uma estrutura cristalizada, é uma estrutura *viva* em crescimento, não apenas no que diz respeito aos seus resultados, mas igualmente em relação às suas fundações.

António M. Fernandes
Departamento de Matemática, IST