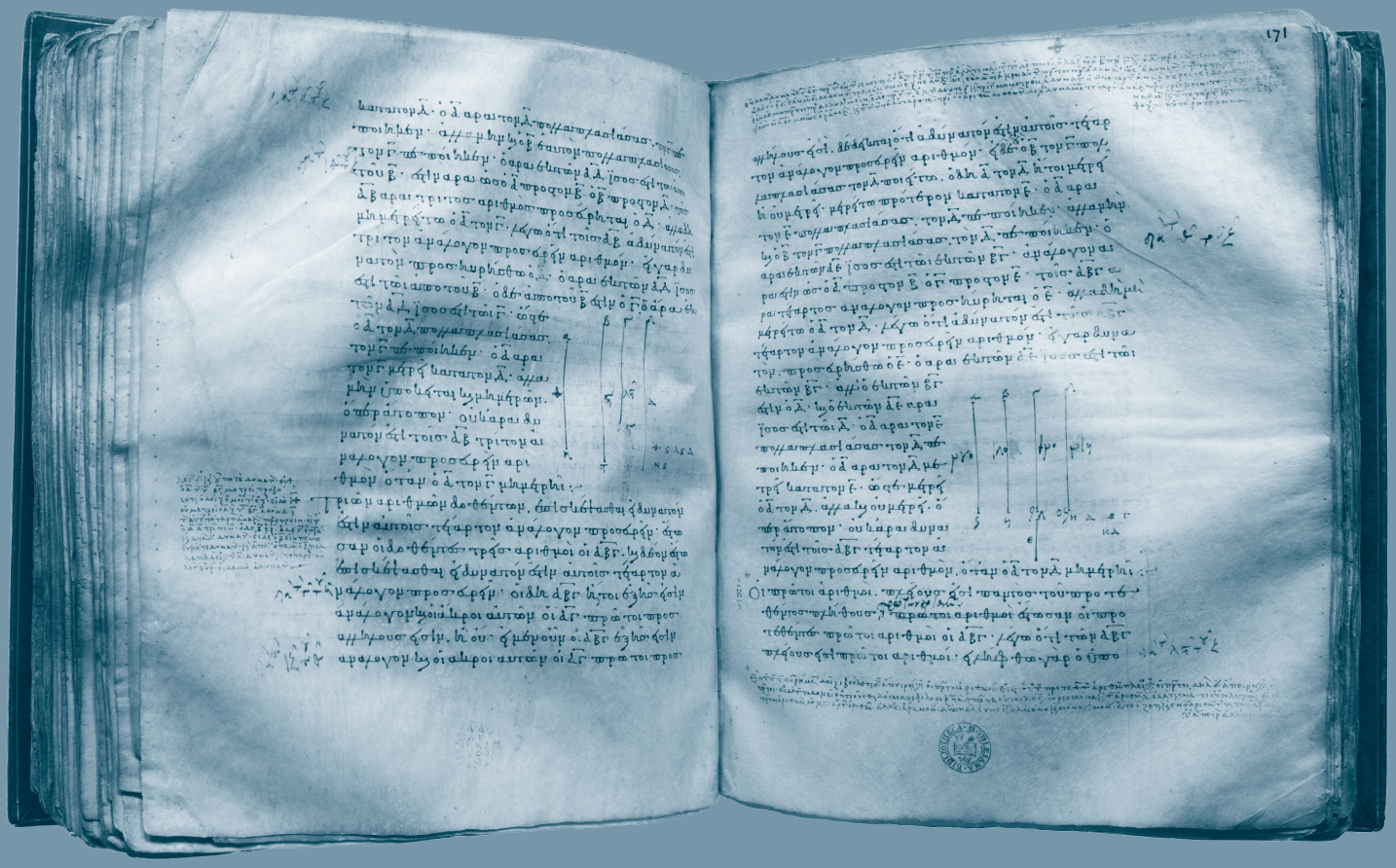

"Proposição 20 do livro 9 dos Elementos de Euclides"

O computador enquanto tecnologia ao serviço da investigação matemática*

Reinhard Kahle e Isabel Oitavem

Quando, nos anos 1980s e 1990s as universidades foram equipadas com computadores, e estes ficaram acessíveis a estudantes e docentes, para serem usados na docência e também na investigação, a receptividade ao uso do computador nas actividades de investigação em matemática foi reduzida. Houve professores de matemática que recusaram esta tecnologia com o argumento de ela não ser uma mais-valia para a sua investigação. A verdade é que, apesar da grande evolução dos computadores desde então até aos nossos dias, continua a não ser claro como é que a capacidade computacional actual pode ser posta ao serviço da investigação matemática em geral.

Por exemplo, sabe-se, desde Euclides, que existe um número infinito de números primos. A demonstração original foi, obviamente, feita sem recurso a qualquer tecnologia. Hoje em dia, o poder computacional disponível é usado para calcular mais e mais números primos – o recorde atual[1] é $2^{74207281}-1$. Os números primos têm aplicações importantes, por exemplo na criptografia, pelo que é essencial dispormos de ferramentas para os calcularmos. Porém, se a capacidade de cálculo permite alimentar as aplicações, não permite, por si só, responder à questão teórica de base: provar que os números primos são infinitos. Neste sentido, do ponto de vista da investigação matemática, o recurso à tecnologia não constitui uma mais-valia.

Tal pode ser ilustrado pelo problema dos números primos gémeos. Dois números primos dizem-se gémeos se a sua diferença for 2. Os pares (3, 5), (5, 7), (11, 13), mas tam-

bém (107, 109) são exemplos de números primos gémeos. É uma questão em aberto saber se existe um número infinito de números primos gémeos. Uma curta reflexão mostra que os computadores não podem ajudar a resolver esta questão, pelo menos não a podem resolver por "força-bruta": podemos tentar encontrar mais e mais exemplos de números primos gémeos, mas uma tal procura, mesmo que tenhamos mais e mais "sucessos", não vai permitir concluir que existe um número infinito de tais números; e, no caso de existir só um número finito, vamos procurar sem fim – mas sem saber que não há um fim.

Dito isto, há obviamente áreas de investigação matemática, onde o computador tem um elevado valor heurístico. Ele permite/facilita o cálculo de exemplos que satisfazem conjecturas, ou – em casos particulares – permite mesmo fornecer contra-exemplos. A área da combinatória é, por exemplo, uma área da matemática onde combinações em conjuntos finitos, mas algumas vezes muito grandes, são sistematicamente estudadas. Neste contexto pode-se querer verificar uma certa propriedade para um conjunto grande de casos particulares, e o computador pode fazer este trabalho por nós. Porém, regra geral, a parte matematicamente mais interessante, não é a verificação destes casos, mas sim o argumento matemático que os especifica. Vamos regressar a isto mais à frente, quando discutirmos a demonstração controversa do teorema das quatro cores.

Uma outra área que pode tirar proveito do recurso aos computadores é a investigação operacional. Nesta área procuram-se algoritmos que forneçam soluções óptimas para problemas como o do caixeiro-viajante (determinar a menor rota para percorrer uma série de cidades). De certa forma, aqui o computador (ou mais exatamente os algoritmos a implementar no computador) é o objeto de estudo matemático e, por isso, não deve constituir surpresa que ele seja usado. Adicionalmente, "verificamos'' (i.e. testamos) a eficiência dos algoritmos encontrados deixando o computador calcular um grande número de exemplos (este procedimento designa-se em inglês por benchmarking).

O mesmo se aplica em criptografia, onde se investiga os algoritmos de encriptação. Tais algoritmos permitem às pessoas autorizadas uma decifração fácil, e às restantes, mesmo quando usando grandes poderes computacionais, não permitem quebrar a encriptação.

No entanto, recentemente, o computador entrou numa outra zona da investigação matemática: a verificação de demonstrações.

Já mencionamos a demonstração do teorema das quatro cores: baseado em trabalho de Heinrich Heesch os matemáticos Kenneth Appel e Wolfgang Haken demonstraram este teorema em 1976, usando programas de computadores para a verificação de que 1936 "casos problemáticos" têm uma certa propriedade que é suficiente para assegurar o teorema. Esta demonstração iniciou uma discussão profunda sobre o uso de computadores em demonstrações matemáticas. Note-se que a demonstração teve duas partes: uma primeira que consiste na redução aos 1936 casos – esta parte não envolve o computador e é considerada puramente "matemática" no sentido tradicional – e uma segunda parte que consiste na verificação por "força-bruta" (i.e. exaustiva) dos 1936 casos, efetuada pelo computador. Aqui "o problema" reside apenas no número de casos a considerar que, de tão grande, inviabiliza a sua verificação por um matemático (apesar da verificação de cada caso, por si só e isoladamente, não ser problemática)[2]. Pelo menos quando, em 1996, Neil Robertson, Daniel Sanders, Paul Seymour e Robin Thomas apresentaram uma nova demonstração ainda com recurso a computadores, mas desta vez com "apenas" 633 casos, a comunidade matemática aceitou esta forma de demonstração.

A discussão reiniciou-se só quando, em 1998, Thomas Hales deu uma demonstração da conjetura de Kepler. Segundo a conjetura de Kepler se empilharmos esferas iguais, a densidade máxima é alcançada com um empilhamento piramidal de faces centradas. De resto, esta é a forma como se empilham laranjas numa banca de venda.

Como no caso do teorema das quatro cores, a demonstração de Hales baseia-se na redução a uma série de casos (apesar da matemática envolvida para chegar a estes casos ser mais complicada do que no caso do teorema das quatro cores). E estes casos são verificados por programas implementados em computadores. Hales foi convidado a publicar o seu trabalho no Annals of Mathematics, uma das revistas mais prestigiadas do mundo; mas o grupo de doze matemáticos, que teve de fazer a revisão chegou a um resultado estranho: estavam "99% seguros" de que o resultado estava correto. Para assegurar o 1% em falta, Hales iniciou um projeto quase revolucionário a que chamou Flyspeck, e consistia na verificação formal da sua demonstração por um outro programa de computador. Sobre o Flyspeck, Hales e muitos colaboradores trabalharam onze anos, de 2001 até 2014, para formalizar a demonstração original num sistema computacional (HOL Light) e verificar todos os passos desta demonstração.

Qual é o significado duma tal verificação de demonstrações por computadores? Poder-se-ia pôr a questão de ter que verificar a correcção da verificação da demonstração, e assim por diante, o que conduziria a uma sequência sem fim de verificações. Mas o que se passa é que, em geral, é

bem mais fácil verificar a correcção de uma demonstração do que encontrá-la. Da mesma forma, os programas computacionais para efetuar uma tal verificação são suficientemente simples para, hoje em dia, serem aceites sem necessidade de recorrer a mais uma "auto-verificação". Com os programas de verificação (como o HOL Light) ganhamos, de facto, mais confiança na demonstração verificada. Eles constituem uma ferramenta de "validação" de demonstrações. Nessa medida, a verificação formal de demonstrações complexas tornou-se uma nova "indústria" de investigação matemática que aproveita essencialmente os novos recursos tecnológicos.

Não substituindo o raciocínio humano, os recursos tecnológicos têm hoje um espaço incontestável na investigação matemática.

Notas:

* Investigação apoiada pelo projeto Hilbert's 24th Problem, PTDC/MHC-FIL/2583/2014, e pelo Centro de Matemática e Aplicações, UID/MAT/00297/2013, financiados pela FCT/MCTES.

[1] Ver https://pt.wikipedia.org/wiki/N%C3%BAmero_primo#Maior_n.C3.BAmero_primo_j.C3.A1_calculado

[2] Existiram também críticas relativamente à elegância, expressa pela frase anónima: "Uma boa demonstração lê-se como um poema, esta parece ser uma lista telefónica."

Reinhard Kahle
CMA e DM, FCT, Universidade NOVA de Lisboa
Isabel Oitavem
CMA e DM, FCT, Universidade NOVA de Lisboa

MATERIAIS PARA A AULA DE MATEMÁTICA

Esta atividade destina-se a alunos do 3.º ou 4.º anos de escolaridade, de preferência com alguns conhecimentos prévios de Scratch. Alguns destes alunos estão já envolvidos no projeto de "Iniciação à Programação no 1.º Ciclo do Ensino Básico" pelo que faz sentido propor-lhes desafios que promovam a aplicação de conhecimentos na área da matemática. A atividade proposta toma a forma de jogo onde, por entrar a imprevisibilidade dos números sorteados, o próprio construtor do jogo poderá jogar. Depois de criado e testado o jogo, o professor pode promover um debate onde os alunos discutam estratégias que permitam adivinhar os números em menos tentativas. Será também possível aumentar o número máximo sorteado e verificar se há relação entre este número e o número de tentativas necessárias para acertar. Com esta tarefa os alunos podem:

- Compreender o que são números aleatórios
- Compreender o que é um algoritmo
- Utilizar estruturas de decisão e ciclos
- Implementar uma solução programada em *Scratch*
- Discutir estratégias para acertar no número, usando o menor número possível de tentativas

Possível resolução em *Scratch*

João Torres
(CCTIC-ESE/IPS)
Projeto EduScratch 2016

ADIVINHA O NÚMERO EM QUE ESTOU A PENSAR...

Utilizando o *Scratch* cria um programa onde uma personagem vai ter de fazer o seguinte:

– Escolher um número inteiro ao acaso entre 1 e 100.

– Pedir ao jogador para tentar adivinhar o número, entre um e 100, que ele escolheu e esperar a sua resposta.

– Dizer ao jogador se o número indicado é maior ou menor do que o que ele escolheu e dizer que acertou quando o número for descoberto.

Depois de construíres o jogo, joga com os teus amigos e discutam se há alguma estratégia para adivinhar o número com menos tentativas.

Sugestões:

Podes criar uma variável que conte o número de tentativas utilizadas.

Podes, no final, enviar uma mensagem de acordo com o número de tentativas.

Podes dificultar o jogo escolhendo números entre 1 e 1000 ou até 10000 se quiseres.