ANTÓNIO MACHIAVELO
Universidade do Porto
ajmachia@fc.up.pt

PRIMOS DE OUTROS MUNDOS

A noção de número primo, número natural maior do que um que não pode aparecer num produto sem estar presente nalgum dos respetivos fatores, pode ser estendida a outros universos numéricos. Encontram-se aí outros primos, ainda mais enigmáticos do que os usuais, constituindo toda uma fauna exótica habitando mundos recheados de aventuras empolgantes para os mais corajosos e destemidos.

Como muitas outras coisas subtis sobre números, tudo começou com Fermat e Euler. Num comentário[1] a um problema de Diofanto, escrito na sua cópia pessoal da edição da *Aritmética* publicada por Bachet de Méziriac, Fermat escreveu:

Poderá haver, nos números inteiros, um outro quadrado, para além de 25, que aumentado de 2 faça um cubo? Isto certamente parece, à primeira vista, difícil de decidir; no entanto, eu posso mostrar, por uma demonstração rigorosa, que 25 é o único quadrado inteiro que é inferior a um cubo por duas unidades.

Por outras palavras, o que Fermat aqui afirma é que a única solução em números naturais da equação $y^3 = x^2 + 2$ é dada por $x = 5$, em cujo caso $y = 3$.

Na sua obra *Elementos de Álgebra*[2], Euler dá conta de uma sua ideia para lidar com o problema descrito no comentário acima citado, cuja solução Fermat não deixou escrita. É uma ideia arrojada: usar números complexos para resolver um problema sobre os números naturais!

Os números complexos não são mais do que uma estrutura algébrica que pode ser sobreposta ao plano euclidiano, uma maneira de somar e multiplicar pontos de uma forma que captura alguns aspetos da geometria desse mesmo plano. Enquanto que a adição de complexos corresponde à soma de vetores, a multiplicação por um complexo corresponde a uma rotação composta com uma homotetia. Estas operações têm todas as propriedades da adição e produto usuais, sendo neste contexto o número correspondente ao ponto (a, b) designado por $a + bi$, onde i representa pois o ponto $(0, 1)$. As operações são completamente determinadas pela preservação das propriedades da adição e multiplicação reais, e pela relação $i^2 = -1$ (a multiplicação por i corresponde a uma rotação de 90º no sentido direto).

A ideia revolucionária de Euler aparece descrita no capítulo XII da parte II da sua *Álgebra*. Consiste em considerar o subconjunto $\mathcal{A} = \{a + b\sqrt{2}\,i : a, b \in \mathbb{Z}\}$ dos números complexos, que é fechado para a adição e a multiplicação, ou seja, a soma e o produto de dois quaisquer elementos de $\mathcal{A}$ é ainda um elemento deste conjunto. $\mathcal{A}$ é um exemplo daquilo a que se chama um *anel* — um conjunto munido de duas operações com as propriedades usuais, com a possível exceção da existência de inversos multiplicativos. O anel dos inteiros, $\mathbb{Z}$, é o protótipo, o arquétipo, de um anel.

A relevância aqui do anel $\mathcal{A}$ é que nele se tem

$$x^2 + 2 = \left(x + \sqrt{2}\,i\right)\left(x - \sqrt{2}\,i\right).$$

Euler raciocina então por analogia. Nos números inteiros, se dois números não tiverem fatores em comum, para além de 1, então só quando ambos são cubos é que o seu produto é um cubo. Isto é uma consequência da unicidade da fatorização em primos, que advém justamente do facto de os números primos não poderem surgir em produtos sem estarem presentes nos respetivos fatores. Assim, se em $\mathcal{A}$ houver fatorização única em primos – que seriam elementos atómicos, no sentido de não se poderem escrever como produto de outros mais pequenos, ou seja, mais próximo da

origem — e se os números $x+\sqrt{2}\,i$ e $x-\sqrt{2}\,i$ não tiverem divisores primos comuns, então cada um teria de ser um cubo. Portanto,

$$\left(x+\sqrt{2}\,i\right)=\left(a+b\sqrt{2}\,i\right)^3,$$

para alguns $a,b\in\mathbb{Z}$. Daqui resulta que

$$\begin{aligned} x &= a\left(a^2-6b^2\right)\\ 1 &= b\left(3a^2-2b^2\right), \end{aligned}$$

de onde se conclui, uma vez que 1 só pode ser escrito de duas maneiras como produto de dois inteiros, que $x=\pm 5$, o que mostra o resultado descoberto por Fermat.

Este argumento só mais tarde seria tornado rigoroso, como resultado de trabalhos de Gauss, Kummer, Kronecker e Dedekind, entre outros, trabalhos esses diretamente influenciados pelas ideias de Euler. Gauss, em particular, usou o anel $\mathbb{Z}[i]$ para deduzir algumas propriedades bem subtis dos números inteiros (para quem sabe o que é: a lei de reciprocidade biquadrática), pelo que é hoje denominado *anel dos inteiros Gaussianos*.

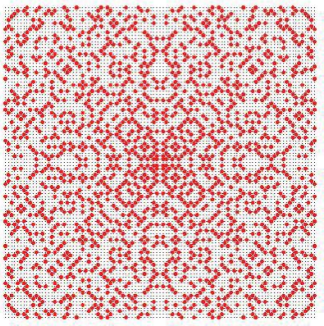
O estudo destes anéis mais gerais, que contêm o anel dos inteiros, conduziu à descoberta da existência de três noções aritméticas distintas: 1) *unidade*: número que tem um inverso multiplicativo ou, equivalentemente, que divide todos os outros; 2) *irredutível*: número que, não sendo uma unidade, não se pode decompor como produto de dois números que não sejam unidades; 3) *primo:* número que não pode aparecer num produto sem que apareça num dos fatores. Por exemplo, i é uma unidade de $\mathbb{Z}[i]$, enquanto que se mostra que 2 é irredutível em $\mathbb{Z}[i\sqrt{5}]$ mas não é primo, pois divide $\left(1+i\sqrt{5}\right)\left(1-i\sqrt{5}\right)$, sem dividir nenhum dos fatores.

Há assim toda uma panóplia de anéis aritméticos, que colocam problemas interessantes, muitos dos quais por resolver, em particular o de saber quando é que os irredutíveis são primos. Uma outra questão, bem curiosa, é designada por "o problema do fosso Gaussiano", e é a seguinte: na reta real, não se pode caminhar desde a origem até um primo arbitrariamente longe, colocando os pés apenas nos primos e dando passos de comprimento limitado. Isto porque, para qualquer $n\in\mathbb{N}$, os números $(n+1)!+2,(n+1)!+3,\ldots,(n+1)!+n,(n+1)!+(n+1)$ são n números compostos consecutivos. Será que no plano euclidiano é ou não possível caminhar desde a origem até um primo Gaussiano arbitrariamente longe, com passos de comprimento limitado e usando apenas os primos Gaussianos? Não se sabe! Para mais informações sobre este intrigante problema, ver o artigo de Gethner, Wagon, and Wick, "A Stroll Through the Gaussian Primes"[3], e pesquisar "Gaussian moat problem".

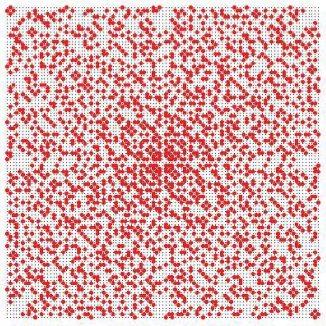
Para saber mais sobre estes anéis exóticos e a sua aritmética, aconselha-se um breve passeio pela página *http://www.cut-the-knot.org/arithmetic/int_domain.shtml* e páginas subsequentes, seguido de um mergulho no excelente texto da autoria de Keith Conrad disponível em *http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/Zinotes.pdf*. Para relaxar um pouco, nada como brincar com uma calculadora que fatoriza um elemento de $\mathbb{Z}[i]$ em primos Gaussianos: *http://www.had2know.com/academics/gaussian-integer-factorization.html*

Para os mais corajosos, que queiram penetrar mais fundo nas densas e deslumbrantes florestas tropicais de novos mundos numéricos, recomendamos o livro sobre Teoria Algébrica dos Números de Franz Lemmermeyer, inteiramente disponível em: *http: //www.fen.bilkent.edu.tr/~franz/ant06/ant.pdf*

A terminar, deixamos aqui duas imagens de dois desses universos novos, prontinhos a explorar pelos leitores mais audazes. Boas aventuras!



Primos de $\mathbb{Z}[i]$ com coordenadas em $[-50,50]$.



Primos de $\mathbb{Z}[\omega]$ com coordenadas em $[-50,50]$, onde $\omega=\frac{-1+i\sqrt{3}}{2}$, uma raiz cúbica de 1.

[1] Ver *Oeuvres de Fermat*, vol. 3, pp. 269. Disponível na biblioteca digital Gallica, em *http://gallica. bnf.fr* e no Internet Archive, em *http://archive.org.*

[2] Disponível em várias versões na Google Books, em *http://books.google.pt/*, assim como no Internet Archive, em *http://archive.org.*

[3] Publicado no *American Mathematical Monthly*, vol. 105 (1998), pp. 327–337, e disponível em: *http: //mathdl.maa.org/images/upload_library/22/Chauvenet/GethnerWagonWick.pdf*