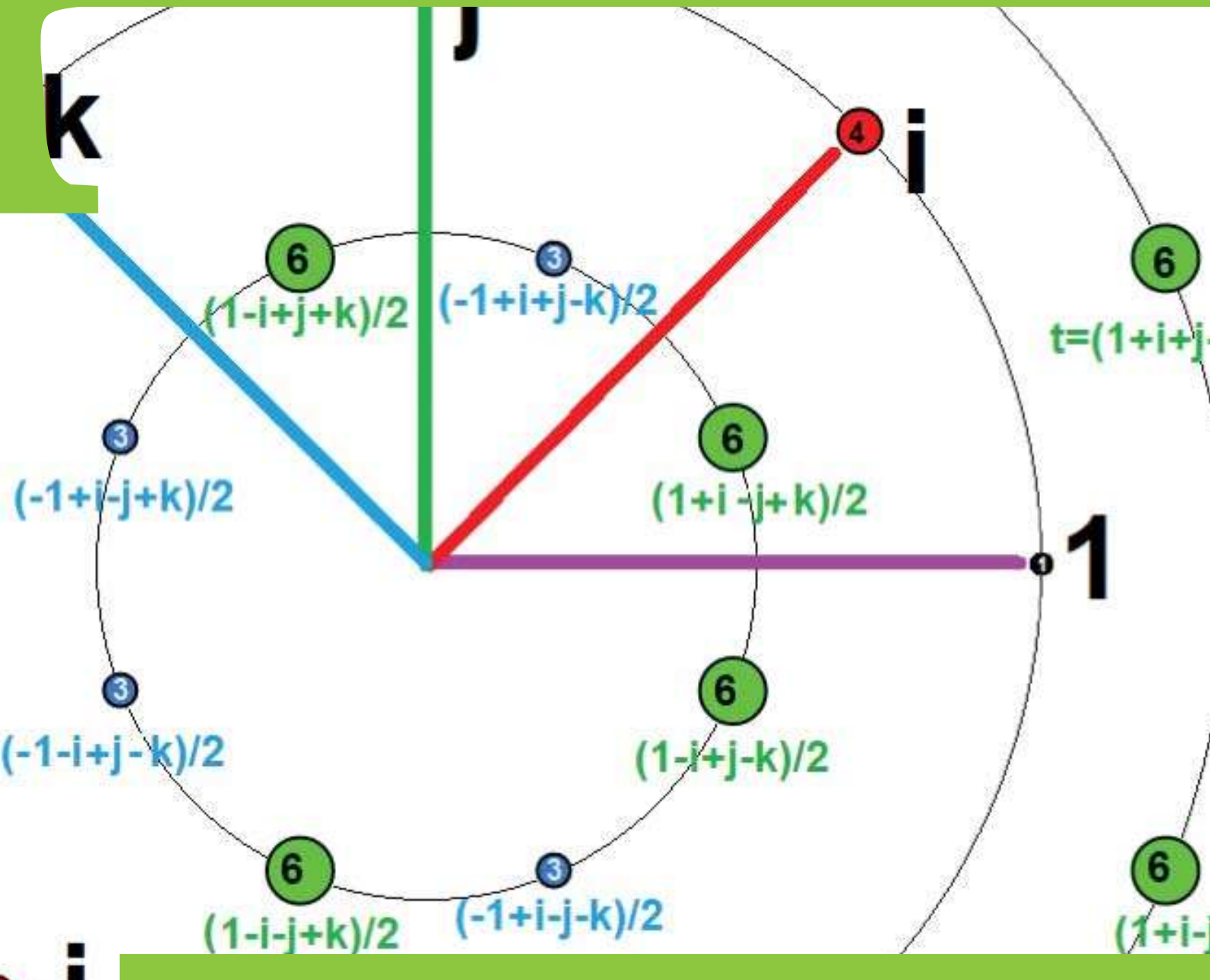

OS QUATERNIÕES E A CONJETURA 1-3-5

António Machiavelo
Faculdade de Ciências da Universidade do Porto
ajmachia@fc.up.pt

Dá-se aqui uma súmula das ideias subjacentes à demonstração recentemente publicada pelo autor e por Nikolaos Tsopanidis, completada com a ajuda de Rogério Reis, da conjetura 1-3-5, anunciada em 2016 por Zhi-Wei Sun, demonstração essa que usa uma aritmética um pouco exótica em subconjuntos speciais dos quaterniões, que se expõe aqui assumindo que o leitor nada sabe destes assuntos.

1. HISTÓRIA DO PROBLEMA

A *Aritmética* de Diofanto de Alexandria, matemático grego do século III, é uma obra que teve uma enorme influência no desenvolvimento da Teoria de Números a partir do século XVII. Consistindo numa sequência de problemas sobre números racionais e respetivas soluções, sabe-se que era formada originalmente por 13 "livros" – usualmente assim chamados, mas que seria mais apropriado apelidar de capítulos –, mas só seis desses "livros" eram conhecidos[1] quando, em 1621, Claude Gaspard Bachet de Méziriac (1581--1638), matemático, poeta e tradutor francês, edita e publica esses "livros" da *Aritmética*. A edição de Bachet continha o texto grego original, uma tradução para latim e extensos comentários feitos pelo próprio Bachet. Num desses comentários faz notar que na resolução dos problemas 29 e 30 do livro IV, Diofanto parece pressupor que qualquer número natural (de facto, qualquer número racional positivo) pode ser escrito como uma soma de quatro ou menos quadrados, i.e. números da forma n^2 para algum $n \in \mathbb{N} = \{1, 2, 3, \ldots\}$. Bachet refere que verificou que assim é, de facto, para todos os números até 325 e que gostaria de ver uma demonstração de que é sempre verdade (cf. [20, p.30] e [5, p.188]).

Não se sabe exatamente quando Pierre de Fermat, o famoso magistrado e matemático francês do século XVII, adquiriu uma cópia dessa edição de Bachet, mas é claro da sua correspondência que em 1636 Fermat não só a tinha estudado cuidadosamente, como tinha feito algumas descobertas em Teoria de Números inspiradas nos problemas de Diofanto e nos comentários de Bachet (ver o volume 2 de [17], em particular a carta de Fermat a Mersenne datada de 2 de setembro de 1636, na p. 57). E pouco depois, ainda em 1636, numa carta a Marin Mersenne escrita em setembro ou outubro desse mesmo ano [17, Vol. 2, p. 65], Fermat escreve que descobriu uma proposição pulquérrima: que todo o número é a soma de um, dois ou três números triangulares[2]; de um, dois ou quatro números quadrados; de um, dois, três, quatro ou cinco números pentagonais, *et eo continuo in infinitu progressu*, ou seja, e assim sucessivamente.

Fermat irá repetir esta mesma afirmação, e que está na posse de uma sua demonstração, em cartas a Blaise Pascal, em 1654 [17, vol. 2, pp. 312-313], e a Kenelm Digby, em 1658 [17, vol. 2, pp. 404]. A Pierre de Carcavi, em 1659 [17, vol. 2, pp. 433], menciona apenas que tem uma prova por "descida infinita" de que todo o número natural é uma soma de não mais de quatro quadrados. Fermat menciona algures que pensa escrever um tratado de Teoria de Números em que expõe os seus métodos e este resultado em particular, mas infelizmente nunca o chegou a fazer, desconhecendo-se a demonstração que Fermat teria deste seu belíssimo resultado.

Leonhard Euler, por volta de 1730, toma conhecimento dos trabalhos de Fermat em Teoria de Números e, em particular, fica impressionado com a afirmação de que todo o número é uma soma de, no máximo, k números k-gonais ($k \geq 3$), nomeadamente, que todo o número natural é uma soma de, no máximo, quatro quadrados (ver [20, p. 173]). Aceitando o número 0 como um número k-gonal, para todo $k \geq 3$, podemos remover a frase "no máximo" das proposições anteriores, tornando o seu enunciado mais curto, o que faremos daqui em diante.

Euler irá tentar obter uma demonstração do caso dos quadrados, descobrindo pelo caminho alguns resultados parciais, por si só interessantes, como o produto de duas somas de quatro quadrados ser ainda uma soma de quatro quadrados; todo o número primo divide uma soma da quatro quadrados; que é suficiente mostrar que todo o primo é uma soma de quatro quadrados de números racionais para deduzir o resultado pretendido. Mas Euler não consegue chegar a uma demonstração, tendo esta sido obtida, em 1772, por Lagrange, com base no trabalho de Euler sobre somas de dois quadrados. Num artigo apre-

[1] Entretanto foram descobertos mais quatro "livros" em 1968, por Fuat Sezgin, numa biblioteca do Irão.

[2] Ver [13] para uma descrição do que são os números poligonais.

sentado à Academia de Petersburgo a 21 de setembro de 1772 e publicada na *Nova Acta Eruditorum* em 1773, Euler, depois de congratular Lagrange pelo seu sucesso, fornece uma demonstração mais simples (ver [20, p. 228] e [11] para mais detalhes).

O caso dos números triangulares viria a ser demonstrado por Gauss, a 10 de julho de 1796. A data precisa é aqui conhecida, pois Gauss escreveu nesse dia num seu pequeno diário a seguinte frase, curta mas expressiva: EYPHKA! $num = \Delta + \Delta + \Delta$. A demonstração viria a ser incluída na sua obra seminal *Disquisitiones Arithmeticae*, publicada em 1801. Em 1798 Legendre publica, em [8], uma demonstração de que um número natural é uma soma de três quadrados se e só se não for da forma $4^a(8b+7)$.

Finalmente, em 1813, Cauchy observa que este resultado de Legendre é equivalente à proposição de que todo o natural é uma soma de três triangulares e demonstra o caso geral do teorema dos números poligonais [1, pp. 320-353]. No seu artigo, Cauchy mostra um pequeno refinamento do teorema dos quatro quadrados, nomeadamente que se k é um número par qualquer e s um outro número par tal que $\sqrt{3k}-1 < s < \sqrt{4k}$, então é sempre possível encontrar $t, u, v, w \in \mathbb{Z}$ tais que se tem, simultaneamente:

$$\begin{cases} k &= t^2+u^2+v^2+w^2 \\ s &= t+u+v+w, \end{cases} \qquad (1)$$

a menos que $k-\left(\frac{s}{2}\right)^2$ seja da forma $4^a(8b+7)$ [1, Théorème III, p. 326]. Um pouco mais à frente Cauchy mostra que se k é um número ímpar arbitrário e $\sqrt{3k-2}-1 < s < \sqrt{4k}$, então o sistema (1) tem solução [1, Théorème IV, p. 329]. Estes resultados foram depois refinados e as demonstrações um pouco simplificadas por Legendre (ver [9, pp. 331-356]) e ainda dão origem a artigos de investigação – ver [16].

Em 2016, o matemático chinês Zhi-Wei Sun (孙智伟) considera vários refinamentos do resultado de Fermat-Lagrange sobre somas de quatro quadrados e, a 9 de abril de 2016, conjetura que todo o número inteiro não-negativo $n \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ pode ser escrito com uma soma de quatro quadrados $x^2+y^2+z^2+w^2$ $(x, y, z, w \in \mathbb{N}_0)$ de tal forma que $x+3y+5z$ é ainda um quadrado perfeito (ver *http://maths.nju.edu.cn/~zwsun/1-3-5-Conj.pdf*). Sun dá a esta conjetura o nome de *Conjetura 1-3-5*, por estes serem os coeficientes da forma linear que se exige ser um quadrado. A 4 de dezembro de 2016, Sun anuncia na *The On-Line Encyclopedia of Integer Sequences* (OEIS, *https://oeis.org*), na entrada relativa à sequência com a etiqueta A271518, que Qing-Hu Hou (侯 庆虎), da Universidade de Tianjin, verificou a validade da conjetura 1-3-5 para todos os números até 10^9. A 17 de fevereiro de 2017 é anunciado, na mesma página, que Qing-Hu Hou terminou a verificação da validade da conjetura até 10^{10}.

A conjetura 1-3-5 viria a ser publicada em [18] (Conjecture 4.3i, p. 184), juntamente com várias outras do mesmo género. Nesse mesmo artigo, Sun oferece uma recompensa de US$1350 pela primeira demonstração completa desta sua conjetura (ver Remark 4.3, pp.184-185).

Em agosto de 2018, eu e Nikolaos Tsopanidis, na altura meu aluno de doutoramento, iniciámos um ataque à conjetura 1-3-5 usando aritmética de quaterniões, uma abordagem que viria a ser eventualmente bem-sucedida no final de 2019, em grande parte graças à grande persistência do Nikolaos. A nossa demonstração tem duas partes: na primeira, [14], mostrámos que a conjetura é válida para números suficientemente grandes, mais precisamente maiores do que $10^4/(\sqrt[4]{35}-\sqrt[4]{34})^4 \simeq 1.051 \times 10^{11}$; a segunda, [15], consiste numa série de estratagemas, alguns sugeridos pelo próprio Zhi-Wei Sun, que conduziram à verificação de que é verdadeira para todos os números naturais até aí, o que foi feito com a imprescindível ajuda do meu colega Rogério Reis, do Departamento de Ciência de Computadores da Faculdade de Ciências do Porto.

Dar-se-á aqui uma ideia do que são os quaterniões e de algumas das suas propriedades aritméticas, dando-se depois um esboço da demonstração da conjetura 1-3-5.

2. OS QUATERNIÕES

Os quaterniões foram introduzidos pelo matemático irlandês William Rowan Hamilton em 1843, e posteriomente descritos em [4], após uma longa busca de uma estrutura algébrica no espaço tridimensional $\mathbb{R}^3$ que fosse análoga à estrutura algébrica no plano $\mathbb{R}^2$ fornecida pelos números complexos. Na altura era já bem percebida a relação profunda e profícua entre propriedades algébricas dos números complexos e a geometria do plano, e Hamilton ambicionava descobrir uma estrutura análoga em $\mathbb{R}^3$ que capturasse a geometria do espaço, e que pudesse até ser útil para facilitar a resolução de problemas de mecânica. Vir-se-ia a descobrir que tal estrutura em $\mathbb{R}^3$ simplesmente não existe, e Hamilton eventualmente apercebeu-se de que é necessária uma quarta dimensão, ou seja, existe uma estrutura algébrica em $\mathbb{R}^4$ que tem em si embutida alguma da geometria do espaço quadridimensional. Os pontos de $\mathbb{R}^4$, quando este está munido dessa estrutura, são apelidados de *quaterniões* e, na realidade, estes vieram a ser úteis

para efetuar cálculos envolvendo rotações tridimensionais, tendo sido, mais recentemente, amplamente usados em computação gráfica tridimensional.

Recordemos que os números complexos constituem uma estrutura algébrica em $\mathbb{R}^2$ em que se identifica o ponto (1,0) com o número 1 e se denota o ponto (0,1) pelo símbolo i, o que conduz à identificação do ponto (a, b) com a expressão $a + bi$, sendo a estrutura algébrica destas expressões dada por uma soma que corresponde diretamente à soma de vetores e por uma multiplicação que prolonga a multiplicação de números reais e que é completamente determinada pela relação $i^2 = -1$ e pela exigência de se manterem válidas as propriedades usuais, como a associatividade, a comutatividade e a distributividade relativamente à soma. O conjunto $\mathbb{R}^2$ munido destas duas operações denota-se por $\mathbb{C}$, *o corpo dos números complexos*, e é fácil ver que a multiplicação por i corresponde à rotação em torno da origem de um ângulo de $\frac{\pi}{2}$ radianos no sentido direto.

Analogamente, os quaterniões fornecem uma estrutura algébrica a $\mathbb{R}^4$ em que o ponto (a, b, c, d) é identificado com a expressão $a + bi + cj + dk$, sendo a soma dada pela soma usual de vetores e a multiplicação fica completamente determinada pelas relações

$$i^2 = j^2 = k^2 = -1$$
$$ij = k = -ji$$

e pelas exigências de ser: associativa; distributiva relativamente à soma; os números reais, identificados com os pontos com as três últimas coordenadas nulas, comutarem com todos os quaterniões. Ao conjunto $\mathbb{R}^4$ munido destas duas operações chama-se *o anel de divisão dos quaterniões*, que se denota por $\mathbb{H}$. A diferença entre um "corpo" e um "anel de divisão" é que, nestes últimos, a multiplicação não necessita de ser comutativa. E no caso dos quaterniões não o é, pois $ij \neq ji$, por exemplo. De facto, mostra-se que não é possível munir $\mathbb{R}^4$ de uma estrutura de corpo, sendo, em certo sentido os quaterniões o melhor que se pode obter em dimensão quatro (ver [3], Cap. 8, §2).

Dado um quaternião

$$\alpha = a_0 + a_1 i + a_2 j + a_3 k \quad (a_0, a_1, a_2, a_3 \in \mathbb{R}),$$

o seu *conjugado* é o quaternião

$$\bar{\alpha} = a_0 - a_1 i - a_2 j - a_3 k;$$

a sua *parte real*, denotada $\Re(\alpha)$, é o número $a_0 = \frac{1}{2}(\alpha + \bar{\alpha})$; a sua *parte vetorial*, $\mathcal{V}(\alpha)$, o quaternião $a_1 i + a_2 j + a_3 k = \frac{1}{2}(\alpha - \bar{\alpha})$. Um quaternião é apelidado de *puro* quando a sua parte real é nula.

É fácil verificar que se tem:

$$\begin{aligned}(a_0 + a_1 i + a_2 j + a_3 k)(b_0 + b_1 i + b_2 j + b_3 k) = \\ = (a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3) + \\ + (a_0 b_1 + a_1 b_0 + a_2 b_3 - a_3 b_2)\, i \\ + (a_0 b_2 - a_1 b_3 + a_2 b_0 + a_3 b_1)\, j \\ + (a_0 b_3 + a_1 b_2 - a_2 b_1 + a_3 b_0)\, k. \quad (2)\end{aligned}$$

Se designarmos por $\alpha \cdot \beta$ o produto interno dos quaterniões α e β vistos como elementos de $\mathbb{R}^4$, resulta de (2) que

$$\Re(\alpha\beta) = \alpha \cdot \bar{\beta}. \quad (3)$$

É também fácil de ver que

$$\overline{\alpha\beta} = \bar{\beta}\bar{\alpha}. \quad (4)$$

(Note-se a troca na ordem dos fatores).

Finalmente, neste rol de definições, há ainda que mencionar a noção de *norma* de um quaternião α, que é o número real não-negativo $\mathrm{N}(\alpha) = \alpha\bar{\alpha}$ (a razão de não termos aqui a usual raiz quadrada é porque é muito útil, no contexto aritmético, que este número seja um inteiro quando as coordenadas do quaternião são todas números inteiros). Grande parte da relevância aritmética desta aplicação $\mathrm{N} : \mathbb{H} \to \mathbb{R}_0^+$ advém do facto de ser multiplicativa, i.e. $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$, para todos os $\alpha, \beta \in \mathbb{H}$, algo de que se deduz facilmente de (4). Note-se ainda que se tem (algo que o leitor poderá verificar como exercício):

$$\mathrm{N}(\alpha) = a_0^2 + a_1^2 + a_2^2 + a_3^2,$$

uma soma de quatro quadrados!

3. ARITMÉTICA NOS QUATERNIÕES E SOMAS DE QUATRO QUADRADOS

Um subconjunto dos quaterniões que é natural esperar que tenha algum interesse estudar do ponto de vista aritmético é o conjunto dos chamados *inteiros de Lipschitz*, constituído pelos quaterniões de coordenadas inteiras, ou seja:

$$\mathcal{L} = \{a + bi + cj + dk \in \mathbb{H} : a, b, c, d \in \mathbb{Z}\}.$$

Este conjunto é fechado para a soma e para o produto, ou seja a soma e o produto de dois quaisquer seus elementos ainda é um seu elemento, dando origem ao que se designa por *anel*, que é, grosso modo, um conjunto munido de duas operações satisfazendo as propriedades usuais exceto a existência de inversos multiplicativos para todos os seus elementos não-nulos. Este anel foi extensamente estudado por Rudolf Lipschitz, tendo este publicado em 1886 um longo artigo, [12], onde, a propósito do estudo das transformações lineares que deixam a forma quadráti-

ca $x^2+y^2+z^2$ invariante, exibe várias propriedades aritmeticamente interessantes deste anel.
Em 1896, Hurwitz publica um artigo, [6], posteriormente expandido numa monografia, [7], publicada em 1919, onde mostra que há um anel dentro dos quaterniões que é um pouco mais interessante em termos aritméticos, a que agora se chama o *anel dos inteiros de Hurwitz*, nomeadamente:

$$\mathcal{H} = \mathcal{L} \cup \left\{ \frac{a}{2} + \frac{b}{2}i + \frac{c}{2}j + \frac{d}{2}k \in \mathbb{H} : a,b,c,d \in \mathbb{Z} \text{ e são todos ímpares} \right\}.$$

Ou seja, os elementos de $\mathcal{H}$ são os quaterniões cujas coordenadas ou são todas inteiras, ou todas metades de números inteiros ímpares. Observe-se que a norma de um inteiro de Hurwitz é um inteiro não-negativo, pois o quadrado de um número ímpar tem a forma $4n+1$, o que implica que a soma dos quadrados de quatro números ímpares é um número divisível por 4.

Em ambos os anéis $\mathcal{L}$ e $\mathcal{H}$ define-se a noção de quaternião *primo* como sendo um quaternião cuja norma é um número primo de $\mathbb{N}$. Neste contexto, e para desfazer qualquer possível confusão, é usual apelidar de *primo racional* um número primo de $\mathbb{N}$. Por exemplo, $1+i+j+2k$ é um quaternião primo, pois a sua norma é o primo racional 7. Num qualquer anel A (pense em $A=\mathbb{Z}$, $\mathcal{L}$, $\mathcal{H}$, por exemplo) define-se a noção de *divisibilidade* estipulando que $a \in A$ divide $b \in A$ (à esquerda, por exemplo) se existir algum elemento $q \in A$ tal que $b = aq$; define-se *unidade* como sendo um elemento com inverso multiplicativo, ou seja, $u \in A$ é uma unidade se existir $v \in A$ tal que $uv = vu = 1$, o elemento neutro da multiplicação. O conjunto de todas as unidades de um anel A é denotado por A^*. As unidades são os elementos "aritmeticamente neutros", pois dividem todos os elementos do anel (tanto à esquerda como à direita), como é fácil ver. No caso dos inteiros de Lipschitz e de Hurwitz não é difícil ver que u é uma unidade se e só se $\mathrm{N}(u) = 1$, e que se tem:

$$\mathcal{L}^* = \{\pm 1, \pm i, \pm j, \pm k\},$$

$$\mathcal{H}^* = \mathcal{L}^* \cup \left\{ \frac{\pm 1 \pm i \pm j \pm k}{2} \right\}.$$

Em particular, $\mathcal{L}$ tem oito unidades, enquanto que $\mathcal{H}$ tem 24.

Dois elementos de um anel dizem-se *associados* se um for igual ao outro vezes uma unidade. Isto implica que têm exatamente os mesmos múltiplos, o que os torna aritmeticamente equivalentes. Um facto importante é que todo o quaternião de Hurwitz tem um associado à esquerda e um outro à direita que é um inteiro de Lipschitz. Isto torna possível, muitas vezes, mostrar a existência de um quaternião de coordenadas inteiras tendo uma certa propriedade aritmética deduzindo primeiro que há um quaternião de Hurwitz nas mesmas condições, o que é mais fácil por $\mathcal{H}$ ser mais "bem-comportado", como veremos já de seguida.

A razão de o anel dos inteiros de Hurwitz ser um pouco mais interessante e mais bem "comportado" do que o de Lipschitz reside no facto de em $\mathcal{H}$ haver uma divisão com resto, ou melhor, duas, uma à esquerda e outra à direita – uma pequena excentricidade que advém de a multiplicação de quaterniões não ser comutativa. Isto significa o seguinte. Dados $\alpha, \beta \in \mathcal{H}$, existem $\gamma, \rho \in \mathcal{H}$ tais que $\alpha = \beta\gamma + \rho$ com $\mathrm{N}(\rho) < \mathrm{N}(\beta)$, ou seja, um quociente (neste caso à direita) e um resto que é menor, em termos da norma, do que o divisor. Há também, claro, um quociente à esquerda e um resto correspondente. Estes quocientes e restos não são, em geral, únicos e os esquerdos podem ser completamente distintos dos direitos, mas a existência destas divisões com resto permite mostrar que o conjunto das combinações lineares (esquerdas ou direitas), com coeficientes em $\mathcal{H}$, de um número finito de elementos de $\mathcal{H}$ é igual ao conjunto dos múltiplos (esquerdos ou direitos) de um único elemento. Ou seja, por exemplo,

Proposição 1. *Dados $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathcal{H}$, existe $\gamma \in \mathcal{H}$ tal que*

$$\{z_1\alpha_1 + z_2\alpha_2 + \cdots + z_n\alpha_n : z_1, z_2, \ldots, z_n \in \mathcal{H}\} = \{z\gamma : z \in \mathcal{H}\}.$$

Um tal quaternião γ é, de certo modo, um máximo divisor comum dos α_i.

Este resultado permite dar uma demonstração relativamente simples e conceptual do teorema de Fermat-Lagrange de que todo o número natural é uma soma de quatro quadrados, de que damos aqui um esboço, deixando os detalhes como exercícios para o leitor interessado. Pela multiplicatividade da norma referida no último parágrafo da secção anterior, basta mostrar que todo o número primo é uma tal soma. Seja, pois, p um qualquer número primo racional e seja S o conjunto dos quadrados módulo p (i.e. dos restos dos quadrados quando divididos por p). Como a aplicação $x \mapsto x^2$ dos restos módulo p neles próprios é tal que um qualquer resto não-nulo módulo p tem zero ou duas pré-imagens, resulta que $|S| = 1 + \frac{p-1}{2} = \frac{p+1}{2}$. Seja S' o conjunto dos restos[3] dos elementos da forma $-1-x$ com $x \in S$. É claro que $|S'| = \frac{p+1}{2}$. Ora, como há apenas p restos distintos, resulta que S e S' não podem ser disjuntos. Isto implica que existem $a, b \in \mathbb{N}_0$, com $a, b \leq \frac{p-1}{2}$, tais

que a^2 e $-1-b^2$ dão o mesmo resto quando divididos por p, ou seja, p divide a^2+b^2+1, número este que é menor do que p^2.

Considere-se agora o quaternião $\alpha = a+bi+j$. Como foi mencionado acima, existe algum $\gamma \in \mathcal{H}$ tal que $\{z_1 p + z_2\alpha : z_1, z_2 \in \mathcal{H}\} = \{z\gamma : z \in \mathcal{H}\}$. Mas então, em particular, $p = \delta\gamma$ e $\alpha = \epsilon\gamma$, para alguns $\delta, \epsilon \in \mathcal{H}$, de onde se deduz que $\mathrm{N}(\gamma)$ divide p^2 e divide $\mathrm{N}(\alpha)$. Daqui resulta que $\mathrm{N}(\gamma)$ é igual a 1 ou p. Mas, $\gamma = \zeta p + \eta\alpha$, para alguns $\zeta, \eta \in \mathcal{H}$, donde é relativamente fácil deduzir que γ não pode ser uma unidade e, portanto, $\mathrm{N}(\gamma) = p$. Substituindo, se necessário, γ por um seu associando em $\mathcal{L}$, concluímos que p é uma soma de quatro quadrados, como queríamos mostrar.

A Proposição 1 pode também ser usada de um modo muito eficaz para deduzir uma espécie de fatorização única para inteiros de Hurwitz *primitivos*, i.e., que não são múltiplos de um inteiro racional:

Teorema 1 (Lipschitz-Hurwitz). *Seja $\alpha \in \mathcal{H} \setminus \mathcal{H}^*$ primitivo. Para cada fatorização de $\mathrm{N}(\alpha)$ num produto de primos racionais, $\mathrm{N}(\alpha) = p_1 p_2 \cdots p_{\ell-1} p_\ell$, há uma fatorização*

$$\alpha = \pi_1 \pi_2 \cdots \pi_{\ell-1} \pi_\ell$$

num produto de primos de Hurwitz de tal modo que $\mathrm{N}(\pi_t) = p_t$, para $t = 1, 2, \ldots, \ell$. Diz-se que esta fatorização de α é modelada na fatorização correspondente de $\mathrm{N}(\alpha)$.

Além disso, qualquer outra fatorização de α modelada na mesma fatorização de $\mathrm{N}(\alpha)$ tem necessariamente a forma

$$\alpha = \pi_1 u_1 \cdot u_1^{-1} \pi_2 u_2 \cdot u_2^{-1} \pi_3 u_3 \cdot \cdots \cdot u_{\ell-2}^{-1} \pi_{\ell-1} u_{\ell-1} \cdot u_{\ell-1}^{-1} \pi_\ell,$$

onde $u_t \in^*$ para $t = 1, 2, \ldots, \ell-1$.

Este resultado pode ser resumido dizendo-se que a fatorização modelada numa dada fatorização da norma de um inteiro de Hurwitz primitivo é única a menos de *migração de unidades* [2, Cap. 5]. Para o que se segue é importante observar que a parte da existência de fatorizações modeladas em fatorizações da norma se aplica a inteiros de Hurwitz arbitrários, e não apenas aos primitivos, e que se aplica ainda a inteiros de Lipschitz, obtendo-se fatorizações destes em primos de Lipschitz.

4. A ESTRATÉGIA DA DEMONSTRAÇÃO DA CONJETURA 1-3-5

Recorde-se que a conjetura 1-3-5 preconiza a existência, para cada $m \in \mathbb{N}$, de quatro inteiros não-negativos $x, y, z, t \in \mathbb{N}_0$ tais que:

$$\begin{cases} x^2+y^2+z^2+t^2 &= m \\ x+3y+5z &= \text{quadrado perfeito.} \end{cases}$$

A primeira ideia subjacente ao ataque à conjetura 1-3-5 consiste em procurar descrever as soluções inteiras (i.e. em $\mathbb{Z}$) do sistema acima, do seguinte modo. Pondo $\gamma = x+yi+zj+tk \in \mathcal{L}$ e $\zeta = a+bi+cj+dk \in \mathcal{L}$, tem-se que o sistema

$$\begin{cases} x^2+y^2+z^2+t^2 &= m \\ ax+by+cz+dt &= n^2, \end{cases}$$

com $m, n \in \mathbb{N}$, é equivalente a

$$\begin{cases} \mathrm{N}(\gamma) &= m \\ \zeta \cdot \gamma &= n^2, \end{cases} \tag{5}$$

que, por (3), é o mesmo que

$$\begin{cases} \mathrm{N}(\gamma) &= m \\ \Re(\zeta\bar{\gamma}) &= n^2. \end{cases} \tag{6}$$

Agora, se pusermos $\delta = \zeta\bar{\gamma}$, a última igualdade é equivalente a dizer que $\delta = n^2 + Ai + Bj + Ck$, para alguns $A, B, C \in \mathbb{Z}$, enquanto a penúltima igualdade, dada a última, é equivalente a $\mathrm{N}(\zeta)m - n^4 = A^2+B^2+C^2$.

Portanto, para o sistema (5) ter solução é necessário que se tenha

$$n \leq \sqrt[4]{m\,\mathrm{N}(\zeta)}, \tag{7}$$

assim como, pelo teorema de Gauss-Legendre sobre somas de três quadrados, que

$$m\,\mathrm{N}(\zeta) - n^4 \text{ não seja da forma } 4^r(8s+7), \text{ com r,s}\in \mathbb{N}_0. \tag{8}$$

Reciprocamente, se estas duas condições, (7) e (8), forem satisfeitas, então existem $A, B, C \in \mathbb{Z}$ tais que $m\,\mathrm{N}(\zeta) - n^4 = A^2+B^2+C^2$. Pondo $\delta = n^2 + Ai + Bj + Ck$, e uma vez que $\mathrm{N}(\delta) = \mathrm{N}(\zeta)m$, da existência de fatorizações modeladas em fatorizações da norma (Teorema 1 e parágrafo seguinte), vem que existem $\xi, \gamma \in \mathcal{L}$ tais que $\delta = \xi\bar{\gamma}$, $\mathrm{N}(\xi) = \mathrm{N}(\zeta)$ e $\mathrm{N}(\gamma) = m$. Resulta daqui que γ é uma solução do sistema (6) onde em vez de ζ está um quaternião, ξ, que tem a mesma norma que ζ. Isto mostra o resultado seguinte.

[3] Dados $a, b \in \mathbb{Z}$ com $b \neq 0$, o quociente e o resto da divisão de a por b são, respetivamente, os únicos números $q \in \mathbb{Z}$ e $r \in \mathbb{N}_0$ tais que $a = bq + r$ e $r < b$. Isto faz com que, por exemplo, o resto da divisão de -7 por 3 seja 2, sendo o quociente -3.

Proposição 2. *Sejam $m, n, \ell \in \mathbb{N}$ tais que $n \leq \sqrt[4]{m\ell}$ e $m\ell - n^4$ não é da forma $4^r(8s+7)$. Então, para alguns $a, b, c, d \in \mathbb{N}_0$ tais que $a^2+b^2+c^2+d^2 = \ell$, o sistema*

$$\begin{cases} x^2+y^2+z^2+t^2 &= m \\ ax+by+cz+dt &= n^2 \end{cases}$$

tem soluções inteiras.

Como se sabe que os números que têm exatamente uma decomposição como soma de quatro quadrados, a menos de troca de parcelas, são: 1, 3, 5, 7, 11, 15, 23, $4^s r$ com $s \geq 0$ e $r \in \{2, 6, 14\}$ [10], resulta que se $a^2+b^2+c^2+d^2 = \ell$ for um destes números, então o sistema (5) tem soluções inteiras desde que m e n satisfaçam as hipóteses desta última proposição.

A dificuldade com a conjetura 1-3-5 reside no facto de $35 = 1^2+3^2+5^2$ ter uma outra decomposição como soma de quatro quadrados, nomeadamente $1+3^2+3^2+4^2$, sendo estas as únicas duas decomposições a menos da ordem das parcelas. Os argumentos apresentados acima permitem pois concluir apenas o seguinte.

Proposição 3. *Sejam $n, m \in \mathbb{N}$ tais que $n \leq \sqrt[4]{35\,m}$ e $35m - n^4$ não é da forma $4^r(8s+7)$. Então, pelo menos um dos dois sistemas seguintes tem soluções em números inteiros:*

$$\begin{cases} x^2+y^2+z^2+t^2 &= m \\ x+3y+5z &= n^2, \end{cases} \qquad \text{(1-3-5)}$$

$$\begin{cases} x^2+y^2+z^2+t^2 &= m \\ x+3y+3z+4t &= n^2. \end{cases} \qquad \text{(1-3-3-4)}$$

A segunda ideia é tentar encontrar uma solução do sistema (1-3-5) a partir de uma solução do sistema (1-3-3-4) usando as observações seguintes.

Fixemos, de agora em diante, $\alpha = 1+3i+5j$ e $\beta = 1+3i+3j+4k$. Dados dois quaterniões ζ e ξ, vamos usar a notação $\zeta \sim \xi$ quando estes dois quaterniões têm as mesmas coordenadas a menos de sinal e permutação das coordenadas. Por exemplo, $3-5j+k \sim \alpha$ e $4-3i-j+3k \sim \beta$. Repare-se que se tivermos uma solução γ de (6) com $\zeta \sim \alpha$, então trocando convenientemente a ordem e os sinais das coordenadas de γ, obtém-se uma solução, em inteiros, do sistema (1-3-5).

Suponhamos agora que temos uma solução do sistema (1-3-3-4) dada por $\gamma \in \mathcal{L}$ com $\mathrm{N}(\gamma) = m$ e $\Re(\beta\bar{\gamma}) = n^2$. Não é difícil ver que, para um qualquer $\rho \in \mathcal{L} \setminus \{0\}$, se tem:

$$\Re(\rho^{-1}\beta\bar{\gamma}\rho) = \Re(\beta\bar{\gamma}) \quad \text{e} \quad \mathrm{N}(\rho^{-1}\gamma\rho) = \mathrm{N}(\gamma).$$

Como, para um qualquer $\sigma \in \mathcal{L} \setminus \{0\}$,

$$\rho^{-1}\beta\bar{\gamma}\rho = (\rho^{-1}\beta\sigma)\,(\sigma^{-1}\bar{\gamma}\rho),$$

vê-se assim que se conseguirmos encontrar $\rho, \sigma \in \mathcal{L} \setminus \{0\}$ com $\mathrm{N}(\rho) = \mathrm{N}(\sigma)$ e tais que $\rho^{-1}\beta\sigma \sim \alpha$ e $\sigma^{-1}\bar{\gamma}\rho \in \mathcal{L}$, então de uma solução γ do sistema (1-3-3-4) consegue-se derivar uma solução do sistema (1-3-5).

Foi esta parte da demonstração da conjetura 1-3-5, mostrar a existência de tais inteiros de Lipschitz, ρ e σ, que deu mais trabalho. O que se fez foi considerar para ρ todos os quatro primos não-associados de norma 3, os seis primos não-associados de norma 5 e os oito primos não-associados de norma 7. Para cada um desses quaterniões ρ determina-se σ com $\mathrm{N}(\sigma) = \mathrm{N}(\rho)$ e tal que

$$\beta\rho = \sigma\delta, \text{ para algum } \rho \text{ com } \mathrm{N}(\delta) = \mathrm{N}(\beta) = \mathrm{N}(\alpha) = 35.$$

Isto é feito usando as técnicas que estão na base da demonstração do teorema da fatorização de Lipschitz-Hurwitz acima mencionado.

Quando acontece que se tem $\delta \sim \alpha$, obtém-se assim uma solução do sistema (1-3-5) à custa de uma solução do sistema (1-3-3-4), desde que a condição $\rho^{-1}\bar{\gamma}\sigma \in \mathcal{L}$ seja satisfeita, o que corresponde, como mostrámos em [14], a ser satisfeita uma certa congruência módulo $\mathrm{N}(\rho)$; quando $\delta \sim \beta$, obtém-se uma outra solução do sistema (1-3-3-4) que, viemos a descobrir, vem a dar uma solução do sistema (1-3-5) quando se usa, a partir dela, um ρ novo para um outro primo. Mais especificamente, quando não se obtém uma solução do sistema (1-3-5) usando um primo de norma 3, a solução do sistema (1-3-3-4) que se obtém pode dar uma solução do sistema (1-3-5) quando se usa agora um primo de norma 5, e se ainda não der, então um primo de norma 7 consegue finalmente resolver o problema. Quem quiser poderá ver os detalhes em [14].

Com tudo isto conseguiu-se mostrar um resultado que é mais preciso do que a conjetura 1-3-5, mas para soluções inteiras, nomeadamente:

Teorema 2. Sejam $m, n \in \mathbb{N}$ tais que $35m - n^4$ é não-negativo e não é da forma $4^r(8s+7)$ $(r, s \in \mathbb{N}_0)$. Então o sistema (1-3-5) tem soluções inteiras sempre que:

i) m é um múltiplo por 3 e $\mathrm{mdc}(n, 15) = 1$.

ii) m é da forma $3\ell+1$ e n é um múltiplo de 3 não divisível por 5.

iii) m é da forma $3\ell+2$ e $\mathrm{mdc}(n,105)=1$.

Para mostrar a existência de uma solução em inteiros do sistema (1-3-5) há agora que, para um dado $m\in\mathbb{N}$, mostrar que existe um $n\in\mathbb{N}$ com $n\leq\sqrt[4]{35m}$ tal que: $35m-n^4$ não é da forma $4^r(8s+7)$ $(r,s\in\mathbb{N}_0)$ e uma das condições i), ii) ou iii) do resultado anterior é satisfeita. Isto foi feito mostrando que se tivermos dez números consecutivos, então um deles satisfaz as condições pretendidas.

Para resolver o problema inicial, que requere soluções não-negativas, mostrou-se que é suficiente garantir que o intervalo $[\sqrt[4]{34m},\sqrt[4]{35m}]$ tenha, pelo menos, dez naturais consecutivos. É fácil ver que isto é equivalente a exigir que se tenha

$$m\geq\left(\frac{10}{\sqrt[4]{35}-\sqrt[4]{34}}\right)^4\simeq 105103560126,8026.$$

Na altura, a conjetura estava verificada até ao número 10^{10}. Precisávamos, pois, de ir "um pouco" mais além: até $1,051\times10^{11}$, o que corresponde a verificar mais de dez vezes a quantidade de números previamente verificados!

Zhi-Wei Sun incentivou-nos a levar a cabo a verificação numérica, tendo dado várias ideias para o fazer de um modo eficaz. Em primeiro lugar mostrou que o nosso limite inicial, que era de cerca de $1,3\times10^{13}$, podia ser reduzido a algo como $2,18\times10^{11}$, tendo nós posteriormente reduzido um pouco mais, até ao número acima mencionado. Adicionalmente, Sun sugeriu que usássemos uma outra sua conjetura, 4.9(ii) de [19], que é mais forte do que a conjetura 1-3-5 e consiste no seguinte:

Conjetura (Zhi-Wei Sun). *Todo o número natural pode ser escrito na forma $x^2+y^2+z^2+t^2$ com $x,y,z,t\in\mathbb{N}_0$ tais que $x+3y+5z$ é um quadrado e, adicionalmente, verifica-se pelo menos uma das três condições seguintes: x é três vezes um quadrado, ou y é um quadrado, ou z é um quadrado.*

O uso desta conjetura, e o facto de ser verdadeira, como viemos a comprovar, até $1,051\times10^{11}$, foi instrumental no sucesso do ataque computacional, pois reduz, em muito, a procura de uma representação de um número na soma de quatro quadrados com a característica pretendida.

Rogério Reis escreveu um programa em *C*, muito eficiente e que pode ser fatiado em pedaços a serem distribuídos por vários computadores, que foi, então, usado para verificar esta conjetura de Sun para todos os números até ao limite pretendido. Pelo caminho foram também usadas outras observações que foram sendo descobertas quando se testou o programa. O leitor interessado poderá ver todos os detalhes, assim como o código de próprio programa, em [15].

Várias experiências feitas durante a verificação da conjetura até $1,051\times10^{11}$ conduziram a uma forma mais precisa da conjetura de Sun que acabamos de referir, nomeadamente:

Conjetura. *Todo o número $m\in\mathbb{N}$ que não é um múltiplo de 16, com a exceção de 31, 43, 111, 151, 168, 200, 248, 263, 319, 456, 479, 871, 1752, 1864, 3544, pode ser representado como uma soma de quatro quadrados, $x^2+y^2+z^2+t^2$, com $x,y,z,t\in\mathbb{N}$ tais que $x+3y+5z$ é um quadrado e x é três vezes um quadrado ou y é um quadrado. Além disso, para $m>14\,485\,001\,848$, há uma representação com $x\in\{0,3\}$ ou $y\in\{0,1\}$. Adicionalmente, após este limite e ignorando os múltiplos de 16, a densidade dos números que têm uma representação com $x=0$ ou $y=0$ é $\frac{5}{6}$.*

Até ao momento, não fazemos ideia de como abordar esta conjetura.

5. CONSIDERAÇÕES FINAIS

A demonstração que foi feita da conjetura 1-3-5 levanta algumas questões que vale a pena considerar.

Em primeiro lugar, é um pouco surpreendente que a "proposição 1-3-3-4", nomeadamente que todo o natural se possa escrever na forma $x^2+y^2+z^2+t^2$ com $x,y,z,t\in\mathbb{N}_0$ tais que $x+3y+3z+4t$ seja um quadrado perfeito, não é verdadeira: os números 3, 4, 7, 8, 22, 23, 31, 42, 61, 95, 148, 157 e 376 não admitem uma tal representação. Cálculos que fizemos parecem sugerir que, exceto estes 13 números e os seus múltiplos obtidos por multiplicação por potências de 16, todos os outros números naturais admitem uma representação desse tipo. Seria interessante perceber o que está por detrás desta diferença entre o caso 1-3-5 e o caso 1-3-3-4.

Em segundo lugar, seria muito interessante fornecer uma abordagem mais conceptual à parte da demonstração onde se usam primos quaterniónicos de norma 3, 5 e 7, onde tudo acabou por funcionar muito bem, mas sem que se perceba a razão profunda, que estou convencido de existir, para tudo dar certo. Parece-me que deve haver uma série de propriedades escondidas por detrás do método que utilizámos e a sua descoberta poderia permitir atacar outras conjeturas análogas, nomeadamente a "conjetura 24" de Sun (ver OEIS A281976 e [19, Conjecture 4.7(i)]):

todo $m \in \mathbb{N}$ pode ser escrito na forma $x^2+y^2+z^2+t^2$ com $x, y, z, t \in \mathbb{N}_0$ de modo a que x e $x+24y$ sejam ambos quadrados perfeitos. Sun oferece US$2400 pela primeira demonstração. Será que esta conjetura pode ser atacada por um método semelhante ao que usámos para a conjetura 1-3-5? Aqui $\mathrm{N}(1+24i) = 577$ e há, a menos de ordem e sinais, 21 quaterniões de Lipschitz de norma 577, o que torna a nossa abordagem impraticável, a menos que se encontrem as tais propriedades escondidas que acabo de mencionar.

REFERÊNCIAS

[1] *Œuvres Complètes D'Augustin Cauchy*, II^{e} Série, Tome VI, Gauthiers-Villars, 1887.

[2] J. H. Conway, D. A. Smith, *On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry*, A K Peters/CRC Press, 2003.

[3] H.-D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel, R. Remmert, *Numbers*, Springer, 1991.

[4] William R. Hamilton, *On Quaternions; or on a new System of Imaginaries in Algebra*, Philosophical Magazine, 1844-1850 (em várias partes). Disponível em linha no endereço: *https://www.maths.tcd.ie/pub/HistMath/People/Hamilton/OnQuat*.

[5] Thomas Heath, *Diophantus of Alexandria: a Study in the History of Greek Algebra*, Cambridge at the University Press, 2nd edition, 1910.

[6] Adolf Hurwitz, "Uber die Zahlentheorie der Quaternionen", *Nachrichten von der Gesellschaft der Wissenschaften zu G öttingen, Mathematisch-Physikalische Klasse*, (1896) 313-340.

[7] Adolf Hurwitz, *Vorlesungen Űber die Zahlentheorie der Quaternionen*, Springer-Verlag, 1919.

[8] Adrien-Marie Legendre, *Essai sur la Théorie des Nombres*, Duprat, 1798.

[9] Adrien-Marie Legendre, *Théorie des Nombres*, Troisième Édition, Tome II, Firmin Didot Frères, 1830.

[10] D. H. Lehmer, "On the Partition of Numbers into Squares", *American Mathematical Monthly* 55 (1948) 476-481.

[11] Franz Lemmermeyer, "Euler, Goldbach, and 'Fermat's Theorem'", *Elemente der Mathematik* 65 (2010) 144-153.

[12] Rudolf Lipschitz, "Recherches sur la Transformation par des Substitutions Réelles d'une Somme de Deux ou de Trois Carrés en Elle-même", *Journal de Mathématiques Pures et Appliquées*, 4e série, tome 2 (1886) 373-440.

[13] António Machiavelo, "A Forma dos Números", *Gazeta de Matemática* 152 (2007) 38-39.

[14] António Machiavelo, Nikolaos Tsopanidis, "Zhi-Wei Sun's 1-3-5 Conjecture and Variations", *Journal of Number Theory* 22 (2021) 1-20.

[15] António Machiavelo, Rogério Reis, Nikolaos Tsopanidis, "Report on Zhi-Wei Sun's 1-3-5 Conjecture and Some of Its Refinements", *Journal of Number Theory* 22 (2021) 21-29.

[16] Melvyn B. Nathanson, "A Short Proof of Cauchy's Polygonal Number Theorem", *Proceedings of the American Mathematical Society* 99(1) (1987) 22-24.

[17] Paul Tennery e Charles Henri (editores), *Œuvres de Fermat*, Gauthiers-Villars et Fils, 1891, 1894, 1896 e 1912 (quatro volumes e um suplemento).

[18] Zhi-Wei Sun, "Refining Lagrange's Four-Square Theorem", *Journal of Number Theory* 175 (2017) 167-190.

[19] Zhi-Wei Sun, "Restricted Sums of Four-Squares", *International Journal of Number Theory* 15(9) (2019) 1863-1893.

[20] André Weil, *Number Theory: An approach through History from Hammurapi to Legendre*, Springer Science+Business Media, 2001.

SOBRE O AUTOR

António Machiavelo é professor auxiliar do Departamento de Matemática da Faculdade de Ciências do Porto e membro do Centro de Matemática da Universidade do Porto. Trabalha em Teoria de Números, Combinatória Analítica e Criptografia, tendo também fortes interesses em História e Filosofia da Matemática. Gosta de praticar malabarismo, jogar xadrez, aprender línguas e escabichar bons livros.