ALFREDO COSTA
Universidade
de Coimbra
amgc@mat.uc.pt

# DESCIDA INFINITA E CRIMINOSOS MINIMAIS

Introduzimos brevemente o método da descida infinita, revestindo-o a certo ponto com as vestes do método do "criminoso minimal". Fazemo-lo na perspetiva da iniciação à resolução de problemas olímpicos de natureza técnica.

## 1. O MÉTODO DA DESCIDA INFINITA

A experiência pessoal do autor destas linhas leva-o a concordar com o *cliché* segundo o qual os iniciados no gosto pela matemática desenvolvem facilmente um especial fascínio pelas equações ditas *diofantinas*, isto é, equações no domínio dos números naturais, ou, mais geralmente, dos números inteiros. O método da *descida infinita* pode, com sucesso, ser aplicado na resolução de algumas de tais equações. De aprendizagem obrigatória num curso de formação olímpica, tem o duplo atrativo de ser acessível a iniciados e de ter bastante *pedigree*. Tal *pedigree* decorre não só da frequência com que é usado em problemas relevantes, mas também do facto de ter sido promovido por Pierre de Fermat (1607-1665), um dos poucos matemáticos que não surpreendem que um vulgar transeunte da rua os reconheça pelo nome.

Parafraseemos a explicação informal que Oysten Ore nos dá sobre o método, no seu livro sobre a História da Teoria dos Números [5]: assumimos que um problema pode ser resolvido no domínio dos números naturais, e de uma sua solução deduzimos uma nova solução no mesmo domínio, definida por números de menor valor; como os inteiros positivos não podem decrescer indefinidamente, chegamos a um absurdo, pelo que o problema não tem solução. Sucintamente: o método assenta na observação de que não podemos fazer uma "descida infinita" na "escada infinita dos número naturais". O nome do método, traduzido do original em francês *descente infinie*, deve-se a Fermat [5].

Figura 1. Pierre de Fermat (1607-1665).[1]

A demonstração da seguinte proposição constitui um exemplo simples de aplicação do método da descida infinita na resolução de equações diofantinas. Neste texto estamos a considerar o conjunto $\mathbb{N}$ dos números naturais como sendo o dos números inteiros positivos.

**Proposição 1.** A equação $x^2 + y^2 = 3z^2$ não tem soluções naturais.

*Demonstração.* Suponhamos que a equação tem soluções naturais. Podemos então tomar naturais $x_0$, $y_0$ e $z_0$ tais que

$$x_0^2 + y_0^2 = 3z_0^2. \tag{1}$$

Suponhamos que $x_0$ não é múltiplo de 3. Como $y_0^2 = 3z_0^2 - x_0^2$, então $y_0$ também não é múltiplo de 3. A divisão de $x_0$ por 3 dá resto 1 ou 2, isto é, temos $x_0 = 3k+1$ ou $x_0 = 3k+2$ para algum número inteiro $k$. Como $(3k+1)^2 = 3(3k^2+2k)+1$ e $(3k+2)^2 = 3(3k^2+4k+1)+1$, em qualquer dos casos vemos que $x_0^2 = 3s+1$ para algum inteiro $s$. Do mesmo modo, temos $y_0^2 = 3t+1$ para algum inteiro $t$. Deduzimos então a igualdade $x_0^2 + y_0^2 = 3(s+t)+2$, que nos diz que o inteiro $x_0^2 + y_0^2$ dá resto 2 quando dividido por 3. Mas a igualdade $x_0^2 + y_0^2 = 3z_0^2$ garante-nos que esse inteiro é múltiplo de 3. Logo, para evitarmos uma contradição, $x_0$ tem de ser múltiplo de 3. Pela mesma razão, $y_0$ tem de ser múltiplo de 3.

Portanto, existem números naturais $x_1$ e $y_1$ tais que $x_0 = 3x_1$ e $y_0 = 3y_1$. Substituindo na equação inicial, obtemos

$$9x_1^2 + 9y_1^2 = 3z_0^2$$

ou seja,

$$3(x_1^2 + y_1^2) = z_0^2.$$

Decorre desta última igualdade que podemos substituir $z_0$ por $3z_1$ para algum número natural $z_1$, obtendo-se então

$$x_1^2 + y_1^2 = 3z_1^2.$$

Logo $(x_1, y_1, z_1)$ também é uma solução da equação $x^2 + y^2 = 3z^2$ formada por números naturais, tendo-se $x_1 < x_0$, $y_1 < y_0$ e $z_1 < z_0$.

Repetindo o argumento, a partir da solução $(x_1, y_1, z_1)$ obteremos uma outra solução $(x_2, y_2, z_2)$ da mesma equação $x^2 + y^2 = 3z^2$, formada por números naturais $x_2, y_2, z_2$ tais que $x_2 < x_1$, $y_2 < y_1$ e $z_2 < z_1$. Continuando indefinidamente este processo, obtemos uma sequência infinita

$$(x_0, y_0, z_0),\ (x_1, y_1, z_1),\ (x_2, y_2, z_2),\ \cdots$$

de soluções naturais da equação $x^2 + y^2 = 3z^2$ tais que

$$x_0 > x_1 > x_2 > x_3 > \cdots$$

Mas isto é impossível, visto que apenas existe um número finito de números naturais menores do que $x_0$.

Chegamos assim a um absurdo. O absurdo surgiu de supormos que a equação $x^2 + y^2 = 3z^2$ tem soluções naturais. Portanto, no domínio dos números naturais, tal equação não tem soluções. $\square$

Os conhecedores da teoria elementar das congruências [4] poderão achar o segundo parágrafo desta demonstração particularmente entediante, mas é de esperar alguma tolerância se tiverem em conta o objetivo de tornar a prova imediatamente acessível a todos os leitores que são alunos do ensino secundário.

## 2. CRIMINOSOS MINIMAIS

O autor deste artigo fez a sua formação em Teoria dos Grupos recorrendo ao livro de Joseph Rotman [6]. Um comentário aí feito, que capta a atenção, é sobre o uso frequente do método do "criminoso minimal" em diversas demonstrações de teoremas sobre grupos finitos. Tomando de empréstimo a descrição feita por Rotman, quando se quer provar que uma estrutura finita de um certo tipo (e.g., um grupo finito) com a propriedade $P$ tem de também ter a propriedade $Q$, frequentemente assume-se que existe uma estrutura $G$ desse tipo que é de tamanho mínimo de entre todas as que têm a propriedade $P$ e não têm a propriedade $Q$. Depois, explorando a minimalidade de $G$, deduz-se uma contradição. Nesta narrativa, a estrutura $G$ é o nosso "criminoso minimal", sendo o seu "crime" a violação de um teorema que queremos provar que é verdadeiro. O uso da sugestiva expressão "criminoso minimal" (tradução de *least criminal*) no contexto dos grupos finitos é atribuído por Rotman a Reinhold Baer; pode-se ver um exemplo do seu uso por Baer num artigo da nossa lista de referências [2].

Mais geralmente, para se provar que um determinado problema não tem soluções, o método consiste em: começar por verificar que se o conjunto de soluções é não vazio,

[1] Imagem do domínio público, via Wikimedia Commons, *https://commons.wikimedia.org/wiki/File:Pierre_de_Fermat3.jpg*

Figura 2. Reinhold Baer (1902-1979).[2]

então é (parcialmente) pré-ordenado de alguma forma, e de tal modo que existem elementos minimais; e em seguida, explora-se a minimalidade de um tal elemento (o "criminoso minimal") para se chegar a um absurdo.

Por exemplo, a demonstração da proposição 1 poderia ter sido adaptada ao método do criminoso minimal, atribuindo ao conjunto $S$ das soluções $(x_0, y_0, z_0)$ da equação $x^3 + y^3 = 3z^3$, no domínio dos números naturais, a pré-ordem $\preceq$ definida por $(a, b, c) \preceq (a', b', c')$ se e só se $a \leq a'$. Como todo o subconjunto não vazio de $\mathbb{N}$ tem um elemento mínimo, se $S$ for não vazio, então tem elementos minimais. A prova de que $S$ é vazio é feita assumindo que $S$ não é vazio e extraindo uma contradição a partir de um elemento minimal de $S$, apelando de algum modo ao carácter minimal de tal elemento.

O método da descida infinita pode ser sempre revestido com as roupagens do princípio do "criminoso minimal". Estas roupagens têm em geral a vantagem de permitirem um texto mais elegante, na opinião do autor.

Vejamos a aplicação do princípio do "criminoso minimal" na resolução do seguinte exercício, incluído num teste feito durante um estágio do Projeto Delfos.

**Problema 1.** *Determine todos os ternos $(x, y, z)$ de inteiros que satisfazem a igualdade*

$$x^3 + 3y^3 + 9z^3 = 3xyz.$$

*Resolução.* Observemos que o terno $(0, 0, 0)$ é uma solução da equação $x^3 + 3y^3 + 9z^3 = 3xyz$. Provemos que é a única.

Suponhamos que $(0, 0, 0)$ não é a única solução da equação. De entre as soluções diferentes de $(0, 0, 0)$, tomemos uma solução $(x_0, y_0, z_0)$ tal que o valor de $|x_0| + |y_0| + |z_0|$ é o menor possível. Uma vez que temos

$$x_0^3 = 3x_0y_0z_0 - 3y_0^3 - 9z_0^3,$$

sabemos que $x_0^3$ é múltiplo de 3. Sendo 3 um número primo, daqui decorre que existe um número inteiro $x_1$ tal que $x_0 = 3x_1$. Substituindo $x_0$ por $3x_1$, obtemos a igualdade

$$9x_1^3 + y_0^3 + 3z_0^3 = 3x_1y_0z_0,$$

pelo que $y_0^3$ é múltiplo de 3. Assim, temos $y_0 = 3y_1$ para algum inteiro $y_1$, donde

$$3x_1^3 + 9y_1^3 + z_0^3 = 3x_1y_1z_0.$$

Continuando com este argumento, obtemos $z_0 = 3z_1$ para algum inteiro $z_1$, e portanto

$$x_1^3 + 3y_1^3 + 9z_1^3 = 3x_1y_1z_1.$$

Logo $(x_1, y_1, z_1)$ também é solução da equação em análise. Reparemos que

$$|x_0| \geq |x_1|, \quad |y_0| \geq |y_1|, \quad |z_0| \geq |z_1|,$$

e que

$$|x_0| = |x_1| \Leftrightarrow x_0 = 0, \quad |y_0| = |y_1| \Leftrightarrow y_0 = 0 \quad \text{e} \quad |z_0| = |z_1| \Leftrightarrow z_0 = 0.$$

Como, pelo menos, uma das componentes de $(x_0, y_0, z_0)$ é não nula, daqui decorre que

$$0 < |x_1| + |y_1| + |z_1| < |x_0| + |y_0| + |z_0|.$$

Mas isto contradiz o carácter minimal da solução $(x_0, y_0, z_0)$.

Assim, por redução ao absurdo, concluímos que, no domínio dos inteiros, a única solução da equação $x^3 + 3y^3 + 9z^3 = 3xyz$ é $(0, 0, 0)$. □

## 3. SOB OS AUSPÍCIOS DE PITÁGORAS E FERMAT

Um triângulo retângulo diz-se *pitagórico* se os comprimentos dos seus lados forem números inteiros. Recordemos que um *quadrado perfeito* é um inteiro não negativo cuja raiz quadrada é um inteiro. O método da descida infinita foi introduzido por Pierre de Fermat para demonstrar que a área de um triângulo pitagórico nunca pode ser um quadrado perfeito [5]. Nesta secção revisitamos essa demonstração, revestindo-a com o princípio do "criminoso minimal".

Dizemos que um terno $(a, b, c)$ de inteiros positivos é um *terno pitagórico* se $a, b, c$ forem os comprimentos dos lados de um triângulo retângulo em que $c$ é o comprimento da hipotenusa. Portanto, pelo Teorema de Pitágoras e pelo seu recíproco, um terno $(a, b, c)$ de inteiros positivos é um terno pitagórico se e só se é uma solução da equação diofantina $x^2 + y^2 = z^2$.

Um terno pitagórico $(a, b, c)$ diz-se *primitivo* quando os inteiros $a, b, c$ são dois a dois primos entre si; o que, em virtude da igualdade $a^2 + b^2 = c^2$, facilmente se vê ser equivalente a que não exista um número primo simultaneamente dividindo $a$, $b$ e $c$. Naturalmente, um triângulo retângulo cujos comprimentos dos lados formam um terno pitagórico primitivo diz-se um *triângulo pitagórico primitivo.*

O teorema seguinte é a bem conhecida caracterização dos ternos pitagóricos primitivos, cuja demonstração apareceu nesta coluna num número recente da *Gazeta de Matemática* [3]. Nessa caracterização usa-se o seguinte facto, fácil de estabelecer usando restos da divisão por 4: num triângulo pitagórico, pelo menos, um dos catetos tem comprimento par; portanto, num triângulo pitagórico primitivo, exatamente um dos catetos é par.

**Teorema 1**. *Seja $(a, b, c)$ um terno de inteiros positivos em que a é par. O terno $(a, b, c)$ é um terno pitagórico primitivo se e só se $a = 2mn$, $b = m^2 - n^2$ e $c = m^2 + n^2$, para alguns inteiros positivos $m$, $n$ primos entre si e tais que $m - n$ é ímpar.*

O Teorema Fundamental da Aritmética, que afirma a existência e a unicidade da fatorização de um inteiro em números primos, permite-nos provar facilmente o seguinte facto.

**Lema 1**. *Seja $n$ um quadrado perfeito. Se $u$ e $v$ são inteiros positivos primos entre si tais que $n = uv$, então $u$ e $v$ são quadrados perfeitos.*

Este lema tem um papel importante na demonstração do teorema sobre o qual esta secção se ocupa, que agora formalmente enunciamos.

Figura 3. Busto de Pitágoras no Museu do Vaticano.[3]

**Teorema 2.** *A área de um triângulo pitagórico não pode ser um quadrado perfeito.*

*Demonstração.* Suponhamos que existe um triângulo pitagórico cuja área é um quadrado perfeito. Então existe um tal triângulo $T$ de área mínima, de entre todos os triângulos pitagóricos cuja área é um quadrado perfeito. Seja $k$ o inteiro positivo tal que a área de $T$ é $k^2$. Seja $\lambda$ o máximo divisor comum dos comprimentos dos lados de $T$, e sejam $a, b, c$ os inteiros tais que $\lambda a$ e $\lambda b$ são os comprimentos dos catetos de $T$, e $\lambda c$ é o comprimento da sua hipotenusa. Observemos que

$$k^2 = \frac{\lambda^2 ab}{2}.$$

Consideremos agora o triângulo pitagórico $T'$, seme-

[2] George M. Bergman, CC BY-SA 4.0 *https://commons.wikimedia.org/wiki/File:Reinhold_Baer_1972_(headshot_enlarged,_as-is).jpg,* via Wikimedia Commons.

[3] Andargor at English Wikipedia, Public domain, via Wikimedia Commons, *https://upload.wikimedia.org/wikipedia/commons/c/c1/Pythagoras_Bust_Vatican_Museum.jpg*

lhante a $T$, cujos catetos e hipotenusa medem $a, b, c$, respetivamente. Note-se que $(a, b, c)$ é um terno pitagórico primitivo. A sua área é $\frac{ab}{2}$, que é um inteiro, uma vez que $a$ ou $b$ é par. Sem perda de generalidade, vamos supor que $a$ é par. Ora, temos

$$\frac{ab}{2} = \frac{k^2}{\lambda^2} = \left(\frac{k}{\lambda}\right)^2.$$

Como $\frac{k}{\lambda}$ é racional, o inteiro $\frac{ab}{2}$ é um quadrado perfeito. Pela minimalidade de $T$, temos então de ter $\lambda = 1$. Ou seja, $T$ é um triângulo pitagórico primitivo.

Pelo teorema 1, existem inteiros positivos $m$ e $n$, primos entre si, com $m - n$ ímpar, tais que

$$a = 2mn, \quad b = m^2 - n^2, \quad c = m^2 + n^2.$$

Portanto, temos

$$k^2 = mn(m^2 - n^2) = mn(m-n)(m+n). \tag{2}$$

Verifiquemos que os números $m, n, m-n$ e $m+n$ são dois a dois primos entre si. Já sabemos que $m$ e $n$ são primos entre si. Suponhamos que existe um número primo $r$ que divide os números $m+n$ e $m-n$. Como $m-n$ é ímpar, temos $r \neq 2$. Além disso, $r$ divide a soma $(m+n)+(m-n) = 2m$ e a diferença $(m+n)-(m-n) = 2n$. Portanto, o primo $r$ é um divisor comum de $m$ e $n$, o que contradiz o facto de $m$ e $n$ serem primos entre si. Verifica-se, pois, que $m+n$ e $m-n$ são de facto primos entre si. Como $\mathrm{mdc}(x, y) = \mathrm{mdc}(x-y, y)$ para quaisquer inteiros $x, y$, vemos que os pares $(m+n, n)$, $(m+n, m)$, $(m-n, m)$ e $(m+n, n)$ também são pares de números primos entre si.

Pela igualdade (2) e pelo lema 1, existem inteiros positivos $u, v$ tais que

$$m = u^2, \qquad n = v^2 \tag{3}$$

e inteiros positivos $p$ e $q$ tais que

$$u^2 - v^2 = p^2, \qquad u^2 + v^2 = q^2. \tag{4}$$

O facto de $m$, $n$, $m-n$ e $m+n$ serem dois a dois primos entre si também implica que $u$, $v$, $p$, $q$ são dois a dois primos entre si, como facilmente se verifica. Como m e n têm paridades distintas, também $u$ e $v$ têm paridades distintas, e portanto $p$ e $q$ têm de ser números ímpares. Somando e subtraindo as igualdades (4), obtemos respetivamente

$$2u^2 = p^2 + q^2, \tag{5}$$

e

$$2v^2 = q^2 - p^2 = (q-p)(q+p). \tag{6}$$

Como $p, q$ são ímpares, sabemos que $q-p$ e $q+p$ são pares. Portanto, de (6) deduzimos que $2v^2$ é múltiplo de 4, pelo que $v$ é par. Seja $v_1 = \frac{v}{2}$. Substituindo $v$ por $2v_1$ em (6), somos levados à igualdade

$$2v_1^2 = \frac{q-p}{2} \cdot \frac{q+p}{2}. \tag{7}$$

Se algum número primo dividisse ambos os inteiros $\frac{q+p}{2}$ e $\frac{q-p}{2}$, então dividiria a sua soma, que é $q$, e a sua diferença, que é $p$, contradizendo o facto de que $p$ e q são primos entre si. Portanto, os inteiros $\frac{q-p}{2}$ e $\frac{q+p}{2}$ são primos entre si, decorrendo então da igualdade (7) que exatamente um deles é par.

Comecemos por supor que $\frac{q-p}{2}$ é par. Então, $q-p$ e $\frac{q+p}{2}$ também são primos entre si, e uma vez que

$$(2v_1)^2 = (q-p) \cdot \frac{q+p}{2}$$

resulta do lema 1 que $q - p = (2d)^2$ e $\frac{q+p}{2} = s^2$ para alguns inteiros positivos $d$ e $s$. Logo, temos

$$q = \frac{q-p}{2} + \frac{q+p}{2} = 2d^2 + s^2$$

e

$$p = \frac{q+p}{2} - \frac{q-p}{2} = s^2 - 2d^2.$$

Substituindo em (5) obtemos

$$u^2 = (s^2)^2 + (2d^2)^2.$$

Pelo recíproco do Teorema de Pitágoras, existe um triângulo retângulo $T_1$ com catetos de comprimento $s^2$ e $2d^2$, e hipotenusa de comprimento $u$. A área do triângulo $T_1$ é

$$s^2 d^2 = \frac{q+p}{2} \cdot \frac{q-p}{4} = v_1^2.$$

De modo análogo, prova-se que se $\frac{q+p}{2}$ é par então obtemos também um triângulo pitagórico $T_1$ cuja área é $v_1^2$.

Portanto, em qualquer dos casos, $T_1$ é um triângulo pitagórico cuja área é um quadrado perfeito. Reparemos ainda que essa área é

$$v_1^2 = \left(\frac{v}{2}\right)^2 = \frac{n}{4}.$$

Logo, $T_1$ tem área menor do que a área de $T$:

$$\frac{n}{4} < n^2 < n(m+n) \leq k^2.$$

Mas isto contradiz a hipótese de que $T$ é o triângulo pitagórico de área mínima de entre todos aqueles cuja área é um quadrado perfeito.

Tendo a contradição nascido da hipótese de que existia algum triângulo pitagórico cuja área é um quadrado perfeito, fica assim demonstrado o teorema. □

## 4. UM CASO ESPECIAL DO GRANDE TEOREMA DE FERMAT

Há o Pequeno e o Grande Teorema de Fermat, do mesmo Pierre de Fermat do qual temos falado. O "Pequeno Teorema de Fermat" [4] diz-nos que se $p$ é um número primo, então $a^p - a$ é um múltiplo de $p$, qualquer seja o inteiro $a$. A sua demonstração é feita nas aulas do Projeto Delfos. O "Grande Teorema de Fermat", também conhecido como "Último Teorema de Fermat", diz-nos que, no domínio dos números naturais, a equação $x^n + y^n = z^n$ é impossível se $n$ for um inteiro maior do que 2. A sua demonstração não é feita nas aulas do Projeto Delfos... De facto, a sua prova, extremamente difícil, só foi alcançada na última década do século XX. Isto após árduo labor de muitos matemáticos, ao longo de séculos, culminando no trabalho épico de Andrew Wiles [1]. No entanto, para o caso especial $n = 4$, a demonstração decorre do teorema 2 de forma simples, como vemos de seguida.

Figura 4. Andrew Wiles (1953-).[4]

Comecemos por observar que se $(u, v, w)$ é uma solução da equação $x^4 + y^4 = z^4$, então $(w, v, u^2)$ é uma solução da equação $x^4 - y^4 = z^2$. Assim, para provar a impossibilidade de soluções naturais para a equação $x^4 + y^4 = z^4$, basta provar o teorema seguinte.

**Teorema 3.** *A equação $x^4 - y^4 = z^2$ não tem soluções naturais.*

*Demonstração.* Para quaisquer números naturais $x, y, z$, sejam

$$a = 2x^2y^2, \quad b = x^4 - y^4, \quad c = x^4 + y^4.$$

Observemos que $a^2 + b^2 = c^2$. Portanto, pelo recíproco do Teorema de Pitágoras, existe um triângulo retângulo com catetos de comprimentos $a, b$ e hipotenusa de comprimento $c$. A sua área é $x^2y^2(x^4 - y^4)$. Logo, se existirem números naturais $x, y, z$ tais que $x^4 - y^4 = z^2$, então existe um triângulo pitagórico cuja área é o quadrado perfeito $(xyz)^2$. Mas isso é impossível, pelo teorema 2. □

## REFERÊNCIAS


[1] Amir D. Aczel. *O Último Teorema de Fermat*. Ciência Aberta. Gradiva, 1997. Traduzido do original em inglês.

[2] Reinhold Baer. "The Hypercenter of Functorially Defined Subgroups". *Illinois J. Math.*, 8:177-230, 1964.

[3] Alfredo Costa. "Ternos Pitagóricos e Tijolos de Euler". *Gazeta de Matemática*, (200):13-17, 2023.

[4] José Plínio Oliveira Santos. *Introdução à Teoria dos Números*. Coleção Matemática Universitária. IMPA, 4ª edição, 2024.

[5] Oystein Ore. *Number Theory and Its History*. Dover Publications, Inc., New York, 1988. Reprint of the 1948 original, With a supplement.

[6] Joseph J. Rotman. *An Introduction to the Theory of Groups*. Number 148 in Grad. Texts in Math. Springer, New York, 4th edition, 1995.


[4] Foto retirada da página webdo prémio Abel, *https://abelprize.no/abel-prize-laureates/2016* Photo: Peter Badge. Copyright holder: Peter Badge/Typos1