SOMAS DE DOIS QUADRADOS

FERNANDO FERREIRA

Nesta secção vamos demonstrar o seguinte resultado:

Teorema. *Seja p um número primo, congruente com 1 módulo 4. Então p é soma de dois quadrados inteiros.*

O primo 2 também é soma de dois quadrados, pois $2 = 1^2 + 1^2$. Porém, os restantes primos – aqueles que são congruentes com 3 módulo 4 – nunca podem ser soma de dois quadrados inteiros. De facto, tem-se algo mais geral: um número natural congruente com 3 módulo 4 nunca é soma de dois quadrados inteiros. Com efeito, se $n \equiv 3 \pmod 4$ e $n = x^2 + y^2$ (onde $x, y \in \mathbb{Z}$) tem-se, por maioria de razão, que $n = x^2 + y^2 \pmod 4$, ou seja, que $3 = x^2 + y^2 \pmod 4$. Ora, os únicos quadrados módulo 4 são o 0 e o 1 e uma soma de dois destes números nunca dá 3.

Em geral, quando é que um número natural é soma de dois quadrados inteiros? Em primeiro lugar, o número 1 é soma de dois quadrados inteiros, pois $1 = 1^2 + 0^2$ (um quadrado inteiro é sempre soma de dois quadrados inteiros, um dos quais 0). No que diz respeito aos naturais $n > 1$, a seguinte igualdade nos inteiros é clarificadora:

$$(x^2 + y^2)(z^2 + w^2) = (xz + yw)^2 + (xw - yz)^2$$

Esta igualdade permite concluir que o produto de dois números, cada qual soma de dois quadrados inteiros, ainda é uma soma de dois quadrados inteiros. Em particular, se na fatorização dum número natural n em primos *não* aparecem primos congruentes com 3 módulo 4, conclui-se que n é soma de dois quadrados inteiros. Por exemplo, 130 é soma de dois quadrados. De facto, $130 = 7^2 + 9^2$ (note-se que $130 = 2 \cdot 5 \cdot 13$). Se na fatorização de n aparecem primos p congruentes com 3 módulo 4, isto pode impedir que se possa escrever n como soma de dois quadrados inteiros. É claro que se esses primos p aparecem exatamente um número par de vezes (isto é, se o expoente r de p na fatorização de n é par), então os próprios factores p^r são quadrados e conclui-se que n é soma de dois quadrados inteiros. Por exemplo, dado que 45 é $3^2 \cdot 5$ daqui sai que 45 é soma de dois quadrados (é $3^2 + 6^2$). Pode demonstrar-se, o que faremos na parte final desta secção, que se na fatorização de n aparecer um primo p congruente com 3 módulo 4 exatamente um número ímpar de vezes, então n *não* é soma de dois quadrados inteiros. É o caso de $n = 15$.

Demonstração do teorema. O resultado segue-se dos dois seguintes factos:

(a) Existe um natural k com $1 \leqslant k < p$ tal que kp é soma de dois quadrados inteiros.
(b) Se kp é soma de dois quadrados inteiros, onde $1 < k < p$, então existe um inteiro k' com $1 \leqslant k' < k$ tal que $k'p$ é soma de dois quadrados inteiros.

O *método de desmonstração descendente de Fermat* permite concluir que p é soma de dois quadrados inteiros. Com efeito, por (a), kp é soma de dois quadrados inteiros. Se $k = 1$, já se tem o que se quer. Caso contrário, por (b), existe $k' < k$ tal que $k'p$ é soma de dois quadrados inteiros. Se $k' = 1$, temos o que se quer. Caso contrário, novamente por (b), existe $k'' < k'$ tal que $k''p$ é soma de dois quadrados inteiros. Se $k'' = 1$, temos o que se quer. Caso contrário, existe $k''' < k''$ tal que ..., etc. Este processo descendente tem que terminar ao fim dum número finito de passos, concluindo-se o resultado.

Que método é este? É uma versão do princípio do mínimo. O que (a) e (b) mostram é que o menor inteiro positivo k tal que kp é soma de dois quadrados inteiros é o inteiro 1.

Argumentemos (a). Dado que $p \equiv 1 \pmod 4$, sai $\left(\frac{-1}{p}\right) = 1$, i.e., -1 é resíduo quadrático módulo p. Logo, existe $x \in \mathbb{Z}$ tal que $x^2 \equiv -1 \pmod p$. Tomando o resíduo menor, posso supor que $-\frac{p}{2} < x < \frac{p}{2}$. Seja k inteiro tal que $x^2 + 1 = kp$. Vem $1 \leqslant k$ e

$$kp = x^2 + 1 < \frac{p^2}{4} + 1 < p^2$$

Logo $kp = x^2 + 1^2$, com $k < p$. Como se queria.

Argumentemos (b). Suponhamos que $x^2 + y^2 = kp$, com $x, y \in \mathbb{Z}$ e $1 < k < p$. Tomem-se resíduos menores $z, w \in \mathbb{Z}$ tais que $x \equiv z \pmod k$ e $y \equiv w \pmod k$ e $-\frac{k}{2} < z, w \leqslant \frac{k}{2}$. Vem $z^2 + w^2 \equiv x^2 + y^2 \pmod k$. Logo, existe um inteiro não negativo k' tal que $z^2 + w^2 = k'k$.

Tem-se que $1 \leqslant k'$, ou seja, que $k' \neq 0$. Se fosse 0, viria $z = w = 0$. Sairia $k \mid x$ e $k \mid y$. Logo $k^2 \mid (x^2 + y^2)$, i.e., $k^2 \mid kp$. Concluir-se-ia que $k \mid p$, o que contradiz a primalidade de p.

Também é fácil de ver que $k' < k$. Com efeito:

$$k'k = z^2 + w^2 \leqslant \frac{k^2}{4} + \frac{k^2}{4} = \frac{k^2}{2}$$

Logo $k' \leqslant \frac{k}{2}$ e, portanto, $k' < k$.

Como já se referiu, tem-se:

$$(*) \qquad (xz + yw)^2 + (xw - yz)^2 = (x^2 + y^2)(z^2 + w^2) = k'k^2p$$

Ora,

$$xz + yw \equiv x^2 + y^2 \equiv 0 \pmod k$$

e

$$xz - yz \equiv xy - yx \equiv 0 \pmod k$$

Sejam x' e y' os inteiros $x' := \frac{xz+yw}{k}$ e $y' := \frac{xw-yz}{k}$. Dividindo ambos os membros da igualdade $(*)$ por k^2, obtém-se

$$x'^2 + y'^2 = k'p$$

Tem-se, pois, que $k'p$, com $1 \leqslant k' < k$, é soma de dois quadrados inteiros. □

Proposição 1. *É condição necessária e suficiente para que número natural n seja soma de dois quadrados inteiros que os primos p congruentes com 3 módulo 4 apareçam exatamente um número par de vezes na fatorização de n.*

Demonstração. Podemos supor que $n \neq 1$. No início desta secção já argumentámos a condição suficiente. Para argumentar a condição necessária, suponhamos que $n = x^2 + y^2$, com $x, y \in \mathbb{Z}$, e que o número primo p aparece exatamente um número ímpar de vezes na fatorização de n. Temos que ver que p é 2 ou que p é congruente com 1 módulo 4. Seja $d = \mathrm{mdc}(x, y)$. Vem $x = dx'$ e $y = dy'$, para certos $x', y' \in \mathbb{Z}$. Note-se que $\mathrm{mdc}(x', y') = 1$. Dado que $n = d^2x'^2 + d^2y'^2$, vem $n' = x'^2 + y'^2$, onde $n = n'd^2$. Por hipótese, p aparece um número ímpar de vezes na fatorização de n. Sai imediatamente que $p \mid n'$. Logo, $x'^2 + y'^2 \equiv 0 \pmod p$. É claro que nem p divide x', nem p divide y' (p. ex., se $p \mid y'$, sai $p|y'^2$; logo, $p \mid x'^2$ e, portanto, $p \mid x'$, o que contradiz $x' \perp y'$). Seja, então, $u \in \mathbb{Z}$ tal que $y'u \equiv 1 \pmod p$. Vem $(x'u)^2 + 1 \equiv 0 \pmod p$. Logo, -1 é resíduo quadrático módulo p. Como sabemos (caso p não seja 2), isto é equivalente a dizer que $p \equiv 1 \pmod 4$. □