O TEOREMA DOS QUATRO QUADRADOS DE LAGRANGE

FERNANDO FERREIRA

O teorema dos quatro quadrados de Lagrange diz que todo o número natural é soma de quatro quadrados inteiros. Isto é verdade para 1 e para 2, pois $1 = 1^2 + 0^2 + 0^2 + 0^2$ e $2 = 1^2 + 1^2 + 0^2 + 0^2$. Tem-se a seguinte igualdade nos inteiros:

$$(*) \qquad (x^2 + y^2 + z^2 + w^2)(x'^2 + y'^2 + z'^2 + w'^2) = (xx' + yy' + zz' + ww')^2 +$$

$$(xy' - yx' + wz' - zw')^2 + (xz' - zx' + yw' - wy')^2 + (xw' - wx' + zy' - yz')^2$$

Esta igualdade mostra que o produto de dois números, cada qual soma de quatro quadrados inteiros, ainda é uma soma de quatro quadrados inteiros. Logo, para demonstrar o teorema de Lagrange, basta mostrar que todo o primo ímpar é soma de quatro quadrados inteiros. Seja p um primo ímpar. Vamos ver o seguinte:

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

O teorema dos quatro quadrados de Lagrange sai agora por uma aplicação do método descendente de Fermat.

Argumentemos (a). Seja $r = \frac{p-1}{2}$. As $r+1$ entradas da lista $0^2, 1^2, 2^2, \ldots, r^2$ são todas distintos módulo p. O mesmo se passa com as entradas da lista $-1-0^2, -1-1^2, -1-2^2, \ldots, -1-r^2$. A concatenação destas duas listas tem $(r+1)+(r+1) = p+1$ entradas. Logo, uma entrada da primeira lista tem de ser igual, módulo p, a uma entrada da segunda lista. Sejam então $x, y \in \mathbb{Z}$ com $0 \leqslant x, y \leqslant r$ e tais que $x^2 \equiv -1 - y^2 \pmod{p}$. Vem $x^2 + y^2 + 1 \equiv 0 \pmod{p}$. Podemos, é claro, tomar resíduos menores x e y tais que $-\frac{p}{2} < x, y < \frac{p}{2}$. Tem-se $x^2 + y^2 + 1^2 + 0^2 = kp$, para um certo inteiro positivo k e, além disso

$$kp = x^2 + y^2 + 1^2 + 0^2 < \frac{p^2}{4} + \frac{p^2}{4} + 1 = \frac{p^2}{2} + 1 < p^2$$

Conclui-se que $k < p$, como se queria.

Argumentemos (b). Por hipótese, kp é soma de quatro quadrados inteiros (onde $1 < k < p$): $kp = x^2 + y^2 + z^2 + w^2$, com $x, y, z, w \in \mathbb{Z}$. Distinguimos dois casos.

Suponhamos que k é par. Então, ou x, y, z, w são todos pares, ou são todos ímpares, ou dois são pares e dois são ímpares. Em todo caso, sem perda de generalidade, podemos supor que x e y têm a mesma paridade e que z e w também têm a mesma paridade. Vem

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 = \frac{k}{2}\, p$$

pois a soma dos dois primeiros quadrados dá $\frac{x^2+y^2}{2}$ e a soma dos dois últimos quadrados dá $\frac{z^2+w^2}{2}$. Note-se que os quatro quadrados acima são quadrados de números inteiros e que $1 \leqslant \frac{k}{2} < k < p$. Como se queria.

Suponhamos agora que k é ímpar. Tem-se $x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{k}$. Tomem-se resíduos menores $x', y', z', w' \in \mathbb{Z}$ tais que $x \equiv x' \pmod{k}$, $y \equiv y' \pmod{k}$, $z \equiv z' \pmod{k}$, $w \equiv w' \pmod{k}$

e $-\frac{k}{2} < x', y', z', w' < \frac{k}{2}$. Vem $x'^2 + y'^2 + z'^2 + w'^2 \equiv 0 \pmod{k}$, ou seja $x'^2 + y'^2 + z'^2 + w'^2 = k'k$ para certo inteiro não negativo k'.

Tem-se que $1 \leqslant k'$, ou seja $k' \neq 0$. Se fosse 0, viria $x' = y' = z' = w' = 0$ e, portanto, $k \mid x$, $k \mid y$, $k \mid z$ e $k \mid w$ o que, atendendo à igualdade $x^2 + y^2 + z^2 + w^2 = kp$, permitiria concluir $k \mid p$. Isto contradiz a primalidade de p.

Também se tem $k' < k$. Com efeito

$$k'k = x'^2 + y'^2 + z'^2 + w'^2 < \frac{k^2}{4} + \frac{k^2}{4} + \frac{k^2}{4} + \frac{k^2}{4} = k^2$$

e, portanto, $k' < k$.

Recapitulando, tem-se $x^2 + y^2 + z^2 + w^2 = kp$ e $x'^2 + y'^2 + z'^2 + w'^2 = k'k$. Pela igualdade $(*)$, vem:

$$(**) \qquad \begin{aligned} k'k^2p = {} & (xx' + yy' + zz' + ww')^2 + (xy' - yz' + wz' - zw')^2 + \\ & (xz' - zx' + yw' - wy')^2 + (xw' - wx' + zy' - yz')^2 \end{aligned}$$

Ora,

$$\begin{aligned} xx' + yy' + zz' + ww' &\equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{k} \\ xy' - yz' + wz' - zw' &\equiv xy - yz + wz - zw \equiv 0 \pmod{k} \\ xz' - zx' + yw' - wy' &\equiv xz - zx + yw - wy \equiv 0 \pmod{k} \\ xw' - wx' + zy' - yz' &\equiv xw - wx + zy - yz \equiv 0 \pmod{k} \end{aligned}$$

Tomem-se então os inteiros

$$\begin{aligned} a &:= \frac{xx' + yy' + zz' + ww'}{k} \\ b &:= \frac{xy' - yz' + wz' - zw'}{k} \\ c &:= \frac{xz' - zx' + yw' - wy'}{k} \\ d &:= \frac{xw' - wx' + zy' - yz'}{k} \end{aligned}$$

Dividindo ambos os membros da igualdade $(**)$ por k^2 obtém-se $a^2 + b^2 + c^2 + d^2 = k'p$. Como se queria demonstrar.