EQUAÇÕES DE THUE

FERNANDO FERREIRA

Mais tarde iremos demonstrar o seguinte resultado importante:

Proposição. *Para todo o número irracional α, a desigualdade*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}$$

tem um número infinito de soluções racionais $\frac{a}{b}$.

E se α for racional? Neste caso tem-se:

Proposição. *Se α é um número racional, então a desiguldade*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}$$

tem apenas um número finito de soluções racionais $\frac{a}{b}$.

Demonstração. Seja α um número racional da forma $\frac{c}{d}$, com $c \in \mathbb{Z}$ e $d \in \mathbb{N}$. Seja $\frac{a}{b} \neq \alpha$ ($a \in \mathbb{Z}$ e $b \in \mathbb{N}$) tal que $\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}$. Então

$$0 < \left|\frac{c}{d} - \frac{a}{b}\right| < \frac{1}{b^2}$$

Daqui sai $0 < |cb - ad| < \frac{d}{b}$. Como $|cd - ad|$ é um número natural, vem $1 \leqslant |cd - ad|$. Vem imediatamente $b < d$. Logo, os denominadores duma aproximação de $\frac{a}{b}$ a α (diferente do próprio α) como na proposição só podem tomar um número finito de valores. Ora, para cada denominador b há no máximo três (dois, de facto) numeradores possíveis que verificam a aproximação. Com efeito se temos uma tal aproximação $\frac{a}{b}$, isto é, se $\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}$ então, se $\frac{a'}{b}$ é também uma aproximação com o mesmo denominador (portanto, também se tem $\left|\alpha - \frac{a'}{b}\right| < \frac{1}{b^2}$), vem

$$\left|\frac{a'}{b} - \frac{a}{b}\right| \leqslant \left|\frac{a'}{b} - \alpha\right| + \left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2} + \frac{1}{b^2} = \frac{2}{b^2} \leqslant \frac{2}{b}$$

Daqui sai que $|a' - a| < 2$. Logo a' só pode ser um dos valores $a - 1$, a ou $a + 1$. □

Se formos um só nada mais exigentes na aproximação racional, a situação da proposição anterior também se aplica aos números algébricos, como mostrou Klaus Roth em 1955:

Teorema de Roth. *Seja α um número real algébrico e seja dado $\varepsilon > 0$. Então a desigualdade*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^{2+\varepsilon}}$$

tem apenas um número finito de soluções racionais $\frac{a}{b}$.

Este teorema valeu a Roth a medalha Fields em Matemática. A demonstração do teorema é muito complicada e não cabe neste curso. Trata-se de um teorema de aproximação diofantina que diz que um número real algébrico só pode ter um número finito de aproximações racionais de um certo tipo. O resultado ainda não é totalmente bem compreendido pois a sua demonstração não é construtiva. Mais concretamente, a demonstração não nos diz como é que se obtém uma majoração em valor absoluto para os possíveis valores de a e b (com $a \perp b$) em termos da forma como são

dados α e ε. Usa, de modo essencial, um raciocínio por redução ao absurdo. Será possível uma demonstração construtiva? Esta é uma questão importante da matemática de hoje.

Mais tarde iremos enunciar e demonstrar um teorema da aproximação diofantina devido a Joseph Liouville em 1844. Recordemos que um número algébrico α diz-se que tem ordem n se for raíz dum polinómio irredutível de $\mathbb{Q}[X]$ de grau n. Uma consequência do teorema de Liouville é a seguinte proposição:

Proposição. *Seja α um real número algébrico de ordem $n \geqslant 2$ e seja dado $\varepsilon > 0$. Então a desigualdade*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^{n+\varepsilon}}$$

tem apenas um número finito de soluções racionais $\frac{a}{b}$.

O teorema de Roth é um extraordinário refinamento deste resultado de Liouville (no teorema de Roth nem sequer há dependência na ordem do número algébrico). Nesta secção iremos falar um pouco da história que decorreu entre os teoremas de Liouville e de Roth, e na conexão entre teoremas deste tipo e a finitude do número de soluções de certas equações diofantinas.

Seja $P(Z) = c_n Z^n + c_{n-1} Z^{n-1} + \cdots + c_1 Z + c_0$ um polinómio irredutível de $\mathbb{Q}[Z]$ de grau n. Podemos associar a este polinómio o seguinte polinómio homogéneo $F(X,Y) \in \mathbb{Q}[X,Y]$ a duas variáveis:

$$F(X,Y) := c_n X^n + c_{n-1} X^{n-1} Y + \cdots + c_1 X Y^{n-1} + c_0 Y^n$$

Uma *equação de Thue* é uma equação da forma $F(x,y) = d$, onde $d \in \mathbb{Z}$ e $F(X,Y)$ é um polinómio de grau $\geqslant 3$ como acima, mas de *coeficientes inteiros*. Tem-se:

Teorema (Thue)**.** *Uma equação de Thue tem apenas um número finito de soluções inteiras.*

Observação. A hipótese do grau do polinómio ser maior ou igual a 3 é essencial. Para grau 2, uma equação da forma $x^2 - ny^2 = 1$, onde n é um inteiro positivo que não é um quadrado, tem (como veremos) um número infinito de soluções inteiras. Note-se que o polinómio $Z^2 - n$ é irredutível em $\mathbb{Q}[Z]$ (porque n não é um quadrado). Estas equações chamam-se *equações de Pell* e estudá-las-emos mais tarde.

Demonstração. Vamos adotar a seguinte terminologia. Dada uma propriedade $R(a,b)$ de pares de inteiros $a, b \in \mathbb{Z}$, dizemos que um inteiro b é *bom* para R se $\exists a \in \mathbb{Z}\, R(a,b)$.

A demonstração é por contradição. Suponhamos que a equação de Thue $F(x,y) = d$ tem um números infinito de soluções inteiras. Dado que para cada $b \in \mathbb{Z}$ existe no máximo um número finito de inteiros a tais que $F(a,b) = d$, podemos concluir que existe um número infinito de inteiros b bons para $F(a,b) = d$. Existe, então, um número infinito de inteiros b diferentes de 0 bons para

$$c_n a^n + c_{n-1} a^{n-1} b + \cdots + c_1 a b^{n-1} + c_0 b^n = d$$

ou seja (dividindo ambos os membros por b^n), bons para

$$c_n \left(\frac{a}{b}\right)^n + c_{n-1} \left(\frac{a}{b}\right)^{n-1} + \cdots + c_1 \frac{a}{b} + c_0 = \frac{d}{b^n}$$

Seja $P(Z) = c_n (Z - \alpha_1) \cdots (Z - \alpha_n)$ a fatorização linear de $P(Z)$ em $\mathbb{C}[Z]$. Portanto, existe um número infinito de inteiros b diferentes de 0 bons para

$$c_n \left(\frac{a}{b} - \alpha_1\right) \cdots \left(\frac{a}{b} - \alpha_n\right) = \frac{d}{b^n}$$

e, por consequência, existe um número infinito de inteiros *positivos* b bons para

$$(\star) \qquad \left|\alpha_1 - \frac{a}{b}\right| \cdots \left|\alpha_n - \frac{a}{b}\right| = \left|\frac{d}{c_n}\right| \frac{1}{b^n}$$

(porque simplesmente se pode mudar o sinal dos numeradores a).

Seja $\gamma := \min_{1 \leqslant i < j \leqslant n} |\alpha_i - \alpha_j|$. Note-se que $\gamma > 0$, dado que as raízes do polinómio $P(Z)$ são diferentes duas a duas (pois $P(Z)$ é irredutível em $\mathbb{Q}[Z]$). Para b suficientemente grande, tem-se

$$\left|\frac{d}{c_n}\right| \frac{1}{b^n} < \left(\frac{\gamma}{2}\right)^n$$

Logo, existe um número infinito de inteiros positivos b bons para

$$\left|\alpha_1 - \frac{a}{b}\right| \cdots \left|\alpha_n - \frac{a}{b}\right| < \left(\frac{\gamma}{2}\right)^n$$

É claro que para cada um desses inteiros positivos b se tem

$$\exists i \left(1 \leqslant i \leqslant n \wedge \left|\alpha_i - \frac{a}{b}\right| < \frac{\gamma}{2}\right)$$

Visto que o número de índices i é finito, podemos tomar i_0 ($1 \leqslant i_0 \leqslant n$) tal que existe um número infinito de inteiros positivos b bons para

$$\left|\alpha_{i_0} - \frac{a}{b}\right| < \frac{\gamma}{2}$$

Sai, para $i \neq i_0$ com $1 \leqslant i \leqslant n$,

$$\left|\alpha_i - \frac{a}{b}\right| \geqslant |\alpha_i - \alpha_{i_0}| - \left|\alpha_{i_0} - \frac{a}{b}\right| > \gamma - \frac{\gamma}{2} = \frac{\gamma}{2}$$

Por ($\star$) e pelas desigualdades acima, vem

$$\left|\alpha_{i_0} - \frac{a}{b}\right| = \frac{1}{b^n}\left|\frac{d}{c_n}\right| \prod_{\substack{1 \leqslant i \leqslant n \\ i \neq i_0}} \left|\alpha_i - \frac{a}{b}\right|^{-1} < \frac{1}{b^n}\left|\frac{d}{c_n}\right| \left(\frac{2}{\gamma}\right)^{n-1}$$

Assim, há um número infinito de inteiros positivos b bons para

$$\left|\alpha_{i_0} - \frac{a}{b}\right| < \frac{c}{b^n}$$

onde c é a constante positiva $|\frac{d}{c_n}|(\frac{2}{\gamma})^{n-1}$. Como $n \geqslant 3$, tome-se $\varepsilon > 0$ tal que $2 + \varepsilon < n$ (podemos tomar $\varepsilon = \frac{1}{2}$, por exemplo). Seja $\delta := n - (2 + \varepsilon) > 0$. Para b suficientemente grande, tem-se $c < b^\delta$. Portanto, pelo que vimos, existe um número infinito de inteiros positivos b bons para

$$\left|\alpha_{i_0} - \frac{a}{b}\right| < \frac{1}{b^{n-\delta}} = \frac{1}{b^{2+\varepsilon}}$$

Vê-se facilmente que esta situação contradiz o teorema de Roth. □

Na parte final da demonstração usámos o teorema de Roth. Não é necessário tanto para concluir o argumento: como se viu, basta ter a finitude de aproximações racionais com $|\alpha - \frac{a}{b}| < \frac{1}{b^{n-\delta}}$, para certo $\delta > 0$ (infelizmente, o teorema de Liouville não é suficiente para justificar isto). Na demonstração de Axel Thue de 1909, mostrou-se algo mais: para números algébricos irracionais α (i.e., de ordem $n \geqslant 2$) e para cada $\varepsilon > 0$, há apenas um número finito de soluções racionais da inequação $|\alpha - \frac{a}{b}| < \frac{1}{b^{\frac{n}{2}+1+\varepsilon}}$.

Entre o resultado de Thue e o resultado de Roth, vários matemáticos melhoraram sucessivamente as estimativas (Carl Ludwig Siegel, Freeman Dyson e Alexander Gelfond). Todas estas estimativas foram obtidas de forma não construtiva.