Aproximações Diofantinas e o Problema 6 da IMO 1991

1. Aproximações Diofantinas

Uma das áreas de interesse da Teoria dos Números é encontrar aproximações racionais de números reais. Essa área é normalmente chamada *Teoria das Aproximações Diofantinas*.

Vejamos um exemplo: você deve saber que $\sqrt{2} \approx 1,41 = \frac{141}{100}$. Será que podemos encontrar uma aproximação melhor? A aproximação $\sqrt{2} \approx \frac{17}{12} = 1,14$ é um pouquinho mais melhor, apesar de ter um denominador menor. Mas se quisermos aproximações $\pi \approx \frac{p}{q}$ melhores, devemos aumentar o denominador q. Mas quanto devemos aumentar? Será que podemos garantir a existência de uma aproximação boa com denominador pequeno? É claro que, dado um irracional α, sempre podemos encontrar uma aproximação racional $\frac{p}{q}$ tal que

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q}$$

De fato, basta tomar q qualquer e p de modo que p/q é mais próximo possível de α. Se p/q não estiver a uma distância menor que $1/q$ de α então $(p-1)/q$ ou $(p+1)/q$ está mais próximo de α, o que não é possível.

Mas será que não conseguimos algum resultado melhor? Para isso, provaremos

1.1. Um resultado de Dirichlet

Teorema. *Seja α um número irracional qualquer. Então existem infinitos racionais $\frac{p}{q}$, $q > 0$, tais que*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$$

Demonstração

Observe que

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2} \iff |q\alpha - p| < \frac{1}{q}$$

Assim, basta provar que, dentre os números $n\alpha$, existem infinitos "próximos" de um inteiro. Para facilitar um pouco, usaremos a seguinte notação: $\lfloor x \rfloor$ é chamada *piso de* x e é o maior inteiro menor que ou igual a x; $\{x\} = x - \lfloor x \rfloor$ é a parte fracionária de x e é um número entre 0 e 1.

Seja N um inteiro positivo. Divida o intervalo $[0;1]$ em N intervalos: $[0;1/N[$, $[1/N;2/N[$, $\ldots$, $[(N-1)/N;1[$. Considere os $N+1$ números

$$\{\alpha\};\{2\alpha\};\{3\alpha\};\ldots;\{(N+1)\alpha\}$$

Dentre esses $N+1$ números existem dois, digamos $\{i\alpha\}$ e $\{j\alpha\}$, $i > j$, pertencentes a um mesmo intervalo. Logo

$$|\{i\alpha\} - \{j\alpha\}| < \frac{1}{N} \iff |i\alpha - \lfloor i\alpha \rfloor - (j\alpha - \lfloor j\alpha \rfloor)| < \frac{1}{N} \iff |(i-j)\alpha - (\lfloor i \rfloor - \lfloor j \rfloor)| < \frac{1}{N}$$

Observe que $i - j \leq N$. Logo, sendo $q = i - j$ e $p = \lfloor i \rfloor - \lfloor j \rfloor$,

$$|q\alpha - p| < \frac{1}{N} < \frac{1}{q}$$

e o resultado segue. ∎

Na verdade, pode-se provar o seguinte

Teorema'. *Seja α um irracional qualquer. Então o conjunto dos números $\{n\alpha\}$ é denso em $[0;1[$. Em outras palavras, para cada $x \in [0;1[$ existem infinitos números da forma $\{n\alpha\}$ tão próximos de x quanto queiramos.*

Mas não podemos melhorar tanto assim.

Exemplo 1.1.

(Prova de Seleção Cone Sul 2003) Sendo a e b inteiros positivos, prove que

$$|a\sqrt{2} - b| > \frac{1}{2a+b}$$

Resolução

Como $\sqrt{2}$ é irracional, $2a^2 \neq b^2$. Logo

$$|2a^2 - b^2| \geq 1 \iff |(a\sqrt{2} - b)(a\sqrt{2} + b)| \geq 1 \iff |a\sqrt{2} - b| \geq \frac{1}{a\sqrt{2}+b} > \frac{1}{2a+b}$$

∎

Este último exemplo nos ajuda no problema 6 da IMO 1991:

Exemplo 1.2.

Um seqüência infinita $x_0, x_1, x_2, \ldots$ de números reais é dita *limitada* quando existe uma constante C tal que $|x_i| \leq C$ para todo $i \geq 0$. Dado um real $a > 1$, construa uma seqüência infinita limitada $x_0, x_1, x_2, \ldots$ tal que

$$|x_i - x_j||i - j|^a \geq 1$$

para todo i, j inteiros não negativos distintos.

Resolução

O que a ver esse problema com aproximações diofantinas? Na verdade, há várias construções. Uma dela usa aproximações diofantinas. Lembra do resultado de Dirichlet? Vamos pensar em um número irracional α. O mais simples é $\sqrt{2}$ (é claro que você pode escolher algum outro). Considere $x_i = k\{i\sqrt{2}\}$, k constante real positiva. Note que $0 \leq x_i \leq k$ e, portanto, $(x_i)_{i\geq 0}$ é limitada.

Então

$$x_i - x_j = k(\{i\sqrt{2}\} - \{j\sqrt{2}\}) = k((i-j)\sqrt{2} - (\lfloor i\sqrt{2} \rfloor - \lfloor j\sqrt{2} \rfloor))$$

Provaremos algo mais forte: encontraremos um k tal que valha

$$|x_i - x_j||i - j| \geq 1$$

(veja que $|i - j|^a \leq |i - j|$)

Temos

$$|k((i-j)\sqrt{2} - (\lfloor i\sqrt{2} \rfloor - \lfloor j\sqrt{2} \rfloor))||i - j| \geq 1$$

Veja que obtemos uma expressão do tipo $|m\sqrt{2} - n|$, m, n inteiros. Do exemplo anterior, $|m\sqrt{2} - n| \geq \frac{1}{m\sqrt{2}+n}$. Assim, sendo $m = i - j$ (podemos supor $i > j$) e $n = \lfloor i\sqrt{2} \rfloor - \lfloor j\sqrt{2} \rfloor$,

$$k|m\sqrt{2} - n|m > \frac{km}{m\sqrt{2}+n}$$

Para terminar, precisamos estimar n em função de m. Mas veja que, como $x \le \lfloor x \rfloor < x + 1$,

$$n = \lfloor i\sqrt{2} \rfloor - \lfloor j\sqrt{2} \rfloor < i\sqrt{2} - j\sqrt{2} + 1 = m + 1 \le 2m$$

Logo

$$k|m\sqrt{2} - n|m > \frac{km}{m\sqrt{2} + 2m} = \frac{k}{\sqrt{2} + 2}$$

e basta tomarmos $k = \sqrt{2} + 2$.

2. A existência de soluções da equação de Pell

Chamaremos de *equação de Pell* a equação diofantina

$$x^2 - Dy^2 = 1,$$

D inteiro positivo não quadrado perfeito. Um exemplo de equação de Pell é

$$x^2 - 3y^2 = 1$$

Vamos supor x e y positivos. Digamos que encontrarmos uma solução inicial $(x_0; y_0)$. No nosso exemplo, podemos tomar $(2; 1)$. Observe que, sendo n inteiro positivo,

$$2^2 - 3 \cdot 1^2 = 1 \iff (2 + 1 \cdot \sqrt{3}) \cdot (2 - 1 \cdot \sqrt{3}) = 1 \implies (2 + 1 \cdot \sqrt{3})^n \cdot (2 - 1 \cdot \sqrt{3})^n = 1 \qquad (*)$$

Com o auxílio do binômio de Newton, você pode provar que se $(x + y\sqrt{D})^n = x_n + y_n\sqrt{D}$ então $(x - y\sqrt{D})^n = x_n - y_n\sqrt{D}$. Assim, se $(2 + 1 \cdot 3)^n = x_n + y_n\sqrt{3}$,

$$(*) \iff (x_n + y_n\sqrt{3}) \cdot (x_n - y_n\sqrt{3}) = 1 \iff x^2 - 3y_n^2 = 1,$$

ou seja, $(x_n; y_n)$ é uma solução. Com isso, conseguimos infinitas soluções (é claro que isso é generalizável para qualquer equação de Pell). De fato, essas são as únicas quando $x_0 + y_0\sqrt{D}$ é mínimo: se existe uma outra raiz $(x; y)$, existe m tal que

$$(x_0 + y_0\sqrt{D})^m < x + y\sqrt{D} < (x_0 + y_0\sqrt{D})^{m+1} \iff 1 < \frac{x + y\sqrt{D}}{x_m + y_m\sqrt{D}} < x_0 + y_0\sqrt{D}$$

Mas

$$\frac{x + y\sqrt{D}}{x_m + y_m\sqrt{D}} = \frac{x + y\sqrt{D}}{x_m + y_m\sqrt{D}} \cdot \frac{x_m - y_m\sqrt{D}}{x_m - y_m\sqrt{D}} = \frac{(x + y\sqrt{D})(x_m - y_m\sqrt{D})}{x_m^2 - Dy_m^2} = (xx_m - Dyy_m) + (x_m y - xy_m)\sqrt{D}$$

e, sendo $x > y$ e $x_m > y_m$,

$$x^2x_m^2 - D^2y^2y_m^2 = (Dy^2 + 1)(Dy_m^2 + 1) - D^2y^2y_m^2 > 0 \implies xx_m - Dyy_m > 0$$

e, como $x + y\sqrt{D} > x_m + y_m\sqrt{D} \implies y > y_m$,

$$x_m^2y^2 - x^2y_m^2 = (y_m^2 + 1)y^2 - (y^2 + 1)y_m^2 = y^2 - y_m^2 > 0 \implies x_m y - xy_m > 0,$$

logo $(xx_m - Dyy_m; x_m y - xy_m)$ é uma outra solução menor que a solução mínima, absurdo!!

Fica somente uma pergunta para acabarmos: quem garante a existência de uma solução inicial $(x_0; y_0)$? Isso é demonstrado com o uso do resultado de Dirichlet. Os lemas a seguir são retirados da referência [1].

Lema 1. *Se* $|x - \sqrt{D}y| < 1/y$ *(lembre-se: existem infinitos desses* (x, y)*!!) então*

$$|x^2 - Dy^2| < 1 + 2\sqrt{D}$$

Demonstração

É só fazer umas contas:

$$|x^2 - Dy^2| = |(x - y\sqrt{D})(x + y\sqrt{D})| < \frac{1}{y}(x + y\sqrt{D}$$

Basta então

$$x + y\sqrt{D} < y(1 + 2\sqrt{D}) \iff x - y\sqrt{D} < y,$$

o que é verdadeiro, já que $|x - \sqrt{D}y| < 1/y < y$. ∎

Lema 2. *Para algum inteiro positivo* k *há infinitos pares de inteiros* $(x; y)$, $y > 0$, *tais que* $x^2 - Dy^2 = k$.

Demonstração

Mais uma vez os pombos atacam! Do Lema 1 e do resultado de Dirichlet, existem infinitos pares $(x; y)$ tais que

$$|x^2 - Dy^2| < 1 + 2\sqrt{D}$$

Mas $1 + 2\sqrt{D}$ é uma valor constante, ou seja, para todos esses pares $|x^2 - Dy^2|$ é limitado, sendo que há um número finito de valores inteiros que esse valor pode assumir. Como são infinitos pares, para algum k existem infinitos pares $(x; y)$ tais que $x^2 - Dy^2 = k$ (os valores são as casas e os pares, os pombos!). ∎

Lema 3. *Existem dois pares distintos* $(x_1; y_1)$ *e* $(x_2; y_2)$ *satisfazendo as condições do Lema 2 tais que* $x_1 \equiv x_2 \pmod{k}$ *e* $y_1 \equiv y_2 \pmod{k}$.

Demonstração

Mais casa de pombos! Há $k \cdot k = k^2$ pares possíveis de restos $(r_1; r_2)$ da divisão de cada termo do par por k. Considere então $k^2 + 1$ pares $(x; y)$ que satisfazem o Lema 2 (são infinitos, portanto existem $k^2 + 1$ deles). Existem dois pares $(x_1; y_1)$ e $(x_2; y_2)$ com o mesmo par de restos, ou seja, $x_1 \equiv x_2 \pmod{k}$ e $y_1 \equiv y_2 \pmod{k}$. ∎

Lema 4. *Se* $(x_1; y_1)$ *e* $(x_2; y_2)$ *satisfazem o Lema 3 e* x_3 *e* y_3 *são inteiros tais que* $x_3 + y_3\sqrt{D} = (x_1 + y_1\sqrt{D})(x_2 - y_2\sqrt{D})$ *então* k *divide* x_3 *e* y_3; $y_3 \neq 0$ *e* $x_3^2 - Dy_3^2 = k^2$ *(*k *é aquele definido no Lema 2).*

Demonstração

Visto que

$$(x_1 + y_1\sqrt{D})(x_2 - y_2\sqrt{D}) = (x_1x_2 - y_1y_2D) + (x_2y_1 - x_1y_2)\sqrt{D},$$

temos

$$x_3 = x_1x_2 - y_1y_2D \equiv x_1 \cdot x_1 - y_1 \cdot y_1D = x_1^2 - Dy_1^2 = k \equiv 0 \pmod{k}$$

e

$$y_3 = x_2y_1 - x_1y_2 \equiv x_1y_1 - x_1y_1 = 0 \pmod{k}$$

Além disso,

$$y_3 \neq 0 \iff x_2y_1 \neq x_1y_2 \iff x_2^2y_1^2 \neq x_1^2y_2^2 \iff (Dy_2^2 + k)y_1^2 \neq (Dy_1^2 + k)y_2^2 \iff y_1^2 \neq y_2^2,$$

o que é verdadeiro.

Por fim, visto que $x_3 - y_3\sqrt{D} = (x_1 - y_1\sqrt{D})(x_2 + y_2\sqrt{D})$ (verifique!!),

$$\begin{aligned} x_3^2 - Dy_3^2 = (x_3 + y_3\sqrt{D})(x_3 - y_3\sqrt{D}) &= (x_1 + y_1\sqrt{D})(x_2 - y_2\sqrt{D}) \cdot (x_1 - y_1\sqrt{D})(x_2 + y_2\sqrt{D}) \\ &= (x_1^2 - Dy_1^2)(x_2 - Dy_2^2) = k \cdot k = k^2 \end{aligned}$$

∎

Teorema. *Toda equação de Pell admite pelo menos uma solução não trivial.*

Demonstração

Por não trivial entendemos $(x; y)$ tal que $xy \neq 0$. Tome $(x_3; y_3)$ como no Lema 4. Como k divide x_3 e y_3, $x_3 = kx_0$ e $y_3 = ky_0$ com x_0, y_0 inteiros. Assim,

$$(kx_0)^2 - D(ky_0)^2 = k^2 \iff x_0^2 - Dy_0^2 = 1,$$

ou seja, $(x_0; y_0)$ é uma solução. ∎