

# Aula 2 - POT - Teoria dos Números - Nível III - Princípios

Fabio E. Brochero Martinez  
Carlos Gustavo T. de A. Moreira      Nicolau C. Saldanha  
Eduardo Tengan

2 de Julho de 2012

# Princípios

Nesta aula apresentaremos alguns princípios fundamentais: o *Princípio da Indução Finita* e o *Princípio da Casa dos Pombos*. Esta é uma versão do capítulo 0 de [1].

## 0.1 Princípio da Indução Finita

Seja  $P(n)$  uma propriedade do número natural  $n$ , por exemplo:

- $n$  pode ser fatorado em um produto de números primos;
- $1 + 2 + \dots + n = \frac{n(n+1)}{2}$ ;
- a equação  $2x + 3y = n$  admite solução com  $x$  e  $y$  inteiros positivos.

Uma maneira de provar que  $P(n)$  é verdadeira para todo natural  $n \geq n_0$  é utilizar o chamado *Princípio da Indução Finita* (PIF), que é um dos axiomas que caracterizam o conjunto dos números naturais. O PIF consiste em verificar duas coisas:

1. (Base da Indução)  $P(n_0)$  é verdadeira e
2. (Passo Indutivo) Se  $P(n)$  é verdadeira para algum número natural  $n \geq n_0$ , então  $P(n + 1)$  também é verdadeira.

Na base da indução, verificamos que a propriedade é válida para um valor inicial  $n = n_0$ . O passo indutivo consiste em mostrar como utilizar a validade da propriedade para um dado  $n$  (a chamada *hipótese de indução*) para provar a validade da mesma propriedade para o inteiro seguinte  $n + 1$ . Uma vez verificados a base e o passo indutivo, temos uma “cadeia de implicações”

$$\begin{array}{l} P(n_0) \text{ é verdadeira (base)} \xrightarrow{\text{passo indutivo}} P(n_0 + 1) \text{ é verdadeira} \\ \xrightarrow{\text{passo indutivo}} P(n_0 + 2) \text{ é verdadeira} \\ \xrightarrow{\text{passo indutivo}} P(n_0 + 3) \text{ é verdadeira} \\ \vdots \end{array}$$

de modo que  $P(n)$  é verdadeira para todo natural  $n \geq n_0$ .

Vejamos alguns exemplos.

**Exemplo 0.1.** *Demonstrar que, para todo inteiro positivo  $n$ ,*

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

SOLUÇÃO: Observemos que  $1 = \frac{1 \cdot 2}{2}$  donde a igualdade vale para  $n = 1$  (base da indução). Agora suponha que a igualdade valha para  $n = k$  (hipótese de indução):

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}$$

Somando  $k + 1$  a ambos lados da igualdade, obtemos

$$1 + 2 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$$

de modo que a igualdade também vale para  $n = k + 1$ . Pelo PIF, a igualdade vale para todo número natural  $n \geq 1$ .  $\square$

**Exemplo 0.2.** *Demonstrar que, para todo número natural  $n$ ,*

$$M_n = n(n^2 - 1)(3n + 2)$$

*é múltiplo de 24.*

SOLUÇÃO: Veja que se  $n = 0$  então  $M_0 = 0$ , que é um múltiplo de 24 (base da indução).

Agora, suponhamos que para certo inteiro  $k$  o número  $M_k$  é divisível por 24 (hipótese de indução) e vamos mostrar que  $M_{k+1}$  também é divisível por 24 (passo indutivo). Calculamos primeiramente a diferença

$$\begin{aligned} M_{k+1} - M_k &= (k+1)((k+1)^2 - 1)(3(k+1) + 2) - k(k^2 - 1)(3k + 2) \\ &= k(k+1)[(k+2)(3k+5) - (k-1)(3k+2)] \\ &= 12k(k+1)^2. \end{aligned}$$

Um dos números naturais consecutivos  $k$  e  $k + 1$  é par donde  $k(k+1)^2$  é sempre par e  $12k(k+1)^2$  é divisível por 24. Por hipótese de indução,  $M_k$  é divisível por 24 e temos portanto que  $M_{k+1} = M_k + 12k(k+1)^2$  também é divisível por 24, como se queria demonstrar.  $\square$

Uma variante do PIF é a seguinte versão (às vezes apelidada de *princípio de indução forte* ou *princípio de indução completa*), em que se deve mostrar

1. (Base da Indução)  $P(n_0)$  é verdadeira e
2. (Passo Indutivo) Se  $P(k)$  é verdadeira para todo natural  $k$  tal que  $n_0 \leq k \leq n$ , então  $P(n+1)$  também é verdadeira.

**Exemplo 0.3.** *A sequência de Fibonacci  $F_n$  é a sequência definida recursivamente por*

$$F_0 = 0, \quad F_1 = 1 \quad e \quad F_n = F_{n-1} + F_{n-2} \quad \text{para } n \geq 2$$

Assim, seus primeiros termos são

$$F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5, F_6 = 8, \dots$$

Mostre que

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

onde  $\alpha = \frac{1+\sqrt{5}}{2}$  e  $\beta = \frac{1-\sqrt{5}}{2}$  são as raízes de  $x^2 = x + 1$ .

SOLUÇÃO: Temos que  $F_0 = \frac{\alpha^0 - \beta^0}{\alpha - \beta} = 0$  e  $F_1 = \frac{\alpha^1 - \beta^1}{\alpha - \beta} = 1$  (base de indução). Agora seja  $n \geq 1$  e suponha que  $F_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}$  para todo  $k$  com  $0 \leq k \leq n$  (hipótese de indução). Assim,

$$\begin{aligned} F_{n+1} &= F_n + F_{n-1} \\ &= \frac{\alpha^n - \beta^n}{\alpha - \beta} + \frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} \\ &= \frac{(\alpha^n + \alpha^{n-1}) - (\beta^n + \beta^{n-1})}{\alpha - \beta} = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} \end{aligned}$$

pois  $\alpha^2 = \alpha + 1 \implies \alpha^{n+1} = \alpha^n + \alpha^{n-1}$  e analogamente  $\beta^{n+1} = \beta^n + \beta^{n-1}$ .

Observe que, neste exemplo, como o passo indutivo utiliza os valores de dois termos anteriores da sequência de Fibonacci, a base requer verificar a fórmula para os dois termos iniciais  $F_0$  e  $F_1$  e não apenas para o primeiro termo.  $\square$

**Exemplo 0.4.** Prove usando o princípio da indução matemática que

$$\frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdots 2n} \leq \frac{1}{\sqrt{2n+1}}.$$

SOLUÇÃO: Vejamos que se  $n = 1$  temos que  $\frac{1}{2} < \frac{1}{\sqrt{3}}$ . Suponhamos que para um certo  $n$  temos

$$\frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdots 2n} \leq \frac{1}{\sqrt{2n+1}}.$$

Para o caso seguinte temos que

$$\frac{1 \cdot 3 \cdot 5 \cdots (2n-1) \cdot (2n+1)}{2 \cdot 4 \cdots 2n \cdot (2n+2)} \stackrel{H.I.}{<} \frac{1}{\sqrt{2n+1}} \cdot \frac{2n+1}{2n+2},$$

e assim basta mostrar que  $\frac{1}{\sqrt{2n+1}} \cdot \frac{2n+1}{2n+2} \leq \frac{1}{\sqrt{2n+3}}$ . Isso sua vez é equiva-

lente a mostrar que  $\frac{\sqrt{2n+1}}{2n+2} \leq \frac{1}{\sqrt{2n+3}}$ , mas, elevando ao quadrado, também vai ser equivalente a mostrar  $(2n+1)(2n+3) \leq (2n+2)^2$ , o que (expandindo os dois lados) é claramente verdadeiro, o que conclui a prova.  $\square$

**Exemplo 0.5.** Demonstrar que, para quaisquer naturais  $n \geq m$ , o coeficiente binomial

$$\binom{n}{m} \stackrel{\text{def}}{=} \frac{n!}{m!(n-m)!}$$

é inteiro.

SOLUÇÃO: Procederemos por indução sobre a soma  $m + n$ . Se  $m + n = 0$  então  $m = n = 0$  e  $\binom{0}{0} = 1$  é inteiro (base de indução). Para o passo indutivo, observe primeiramente que para  $0 < m < n$  temos a seguinte identidade de binomiais

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$$

que segue diretamente das definições:

$$\begin{aligned} \binom{n-1}{m} + \binom{n-1}{m-1} &= \frac{(n-1)!}{m!(n-m-1)!} + \frac{(n-1)!}{(m-1)!(n-m)!} \\ &= \frac{((n-m)+m)(n-1)!}{m!(n-m)!} = \binom{n}{m}. \end{aligned}$$

Agora suponhamos que  $\binom{n}{m}$  é inteiro para  $m+n \leq k$  (hipótese de indução). Note que podemos supor também que  $0 < m < n$ , já que se  $m = n$  ou  $m = 0$  temos  $\binom{n}{m} = 1$  e o resultado vale trivialmente. Assim, se  $m+n = k+1$ , temos que  $\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$  é inteiro também pois cada somando da direita é inteiro pela hipótese de indução.  $\square$

**Exemplo 0.6.** *Sejam  $x_1, \dots, x_n$  números reais positivos. Neste exercício vamos provar que*

$$\frac{x_1 + \dots + x_n}{n} \geq \sqrt[n]{x_1 \dots x_n}.$$

Tal desigualdade é conhecida como desigualdade das médias aritmética e geométrica.

- (a) *Utilize o PIF para mostrar a desigualdade das médias para  $n = 2^k$ .*
- (b) *Sejam  $x_1, \dots, x_n$  reais positivos fixados e  $A = \frac{x_1 + \dots + x_n}{n}$  a média aritmética destes números. Suponha que a desigualdade valha para  $n+1$  números reais positivos quaisquer; aplicando-a para  $x_1, \dots, x_n, A$ , conclua que a desigualdade vale também para quaisquer  $n$  números reais positivos.*
- (c) *Combinando os itens anteriores, prove a desigualdade para todo  $n$  natural.*

SOLUÇÃO: Primeiro observemos que se  $a, b > 0$  então

$$0 \leq (a-b)^2 = a^2 - 2ab + b^2 = (a+b)^2 - 4ab,$$

logo  $\sqrt{ab} \leq \frac{a+b}{2}$ , assim a desigualdade vale para  $n = 2$ . Agora mostremos que se a desigualdade vale para  $k$  então a desigualdade vale para  $2k$ . De fato

$$\begin{aligned} \frac{x_1 + \dots + x_{2k}}{2k} &= \frac{\frac{x_1 + \dots + x_k}{k} + \frac{x_{k+1} + \dots + x_{2k}}{k}}{2} \\ &\geq \frac{\sqrt[k]{x_1 \dots x_k} + \sqrt[k]{x_{k+1} \dots x_{2k}}}{2} \\ &\geq \sqrt{\sqrt[k]{x_1 \dots x_k} \sqrt[k]{x_{k+1} \dots x_{2k}}} = \sqrt[2k]{x_1 \dots x_{2k}}. \end{aligned}$$

Assim a desigualdade é verdadeira para  $2, 4, 8, \dots, 2^n, \dots$ . Suponhamos que a desigualdade é verdadeira para  $n+1$ , e sejam  $x_1, \dots, x_n$  reais positivos,

definamos  $A = \frac{x_1 + \dots + x_n}{n}$  e  $G = \sqrt[n]{x_1 \cdots x_n}$ , temos que mostrar que  $A \geq G$ , mas de fato sabemos que

$$A = \frac{x_1 + \dots + x_n + A}{n+1} \geq \sqrt[n+1]{x_1 \cdots x_n A} = G^{\frac{n}{n+1}} A^{\frac{1}{n+1}}.$$

Daqui facilmente concluímos o que queríamos demonstrar.  $\square$

Um terceiro disfarce do PIF é o chamado *princípio da boa ordenação* (PBO) dos números naturais, que afirma que todo subconjunto  $A$  não vazio de  $\mathbb{N}$  tem um elemento mínimo. (Você sabe dizer por que o princípio da boa ordem não vale para o conjunto  $\mathbb{Z}$  de todos os inteiros?)

Vejam os a equivalência entre os dois princípios. Assuma primeiramente o PBO e seja  $P(n)$  uma propriedade para a qual  $P(0)$  é verdadeira e  $P(n)$  verdadeira implica  $P(n+1)$  verdadeira. Seja  $B$  o conjunto dos  $n$  tais que  $P(n)$  é falsa; devemos mostrar que  $B = \emptyset$ . Suponha que não; pelo PBO o conjunto  $B$  possui um menor elemento  $b$ . Como  $0 \notin B$  (pois  $P(0)$  é verdadeira por hipótese) temos que  $b \geq 1$  e assim  $b-1 \in \mathbb{N}$  e pela minimalidade de  $b$  temos que  $b-1 \notin B$ , ou seja,  $P(b-1)$  é verdadeira. Mas por hipótese temos então que  $P(b)$  também é verdadeira, o que é um absurdo, logo  $B = \emptyset$ .

Assuma agora o PIF e seja  $A \subset \mathbb{N}$  um subconjunto não vazio. Defina agora o conjunto  $B = \{b \in \mathbb{N} \mid a \notin A \text{ para todo } a < b\}$ . Trivialmente  $0 \in B$ . Afirmamos que existe  $k \in B$  tal que  $k+1 \notin B$  e nesse caso  $k$  será o menor elemento de  $A$ . De fato, se isto não acontecer, teremos que  $0 \in B$  e  $k \in B$  implica que  $k+1 \in B$ . Logo, pelo PIF,  $B = \mathbb{N}$  e  $A = \emptyset$ , o que é absurdo.

**Exemplo 0.7.** *Demonstrar que toda função  $f : \mathbb{N} \rightarrow \mathbb{N}$  monótona não-crescente (isto é,  $n \leq m \implies f(n) \geq f(m)$ ) é constante a partir de um certo número natural.*

SOLUÇÃO: Seja  $A \subset \mathbb{N}$  a imagem de  $f$ . Pelo PBO, tal conjunto possui elemento mínimo  $a_0$ . Seja  $n_0$  um natural tal que  $f(n_0) = a_0$ . Como a função é monótona não-crescente então para todo  $n \geq n_0$  temos que  $f(n) \leq f(n_0)$ , mas pela definição de  $a_0$  temos  $f(n) \geq a_0$ . Logo  $f(n) = a_0$  para todo  $n \geq n_0$ , como queríamos demonstrar.  $\square$

**Observação 0.8.** *Dado um conjunto  $S$ , uma relação  $\prec$  em  $S$  é chamada de ordem parcial em  $S$  se ela satisfaz os seguintes axiomas:*

1. (Reflexividade)  $a \prec a$  para todo  $a \in S$ .
2. (Anti-simetria) se  $a \prec b$  e  $b \prec a$  então  $a = b$ .
3. (Transitividade) se  $a \prec b$  e  $b \prec c$  então  $a \prec c$ .

*Dizemos que  $\prec$  é uma ordem total se, dados quaisquer  $a, b \in S$ , ou  $a \prec b$  ou  $b \prec a$ . Uma ordem total  $\prec$  em  $S$  é uma boa ordem se todo subconjunto  $A$  de  $S$  possui um elemento mínimo, isto é, um elemento  $a \in A$  tal que  $a \prec b$  para todo  $b \in A$ . É possível demonstrar que para todo conjunto  $S$  podemos definir uma ordem total em  $S$  que é uma boa ordem. Este fato usa o axioma da escolha (e na verdade é equivalente a ele) e está fora do propósito deste livro. Veja por exemplo [3].*

## Problemas Propostos

**0.1.** *Demonstrar por indução que para  $n \geq 1$  natural*

$$(a) 1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

$$(b) 1^3 + 2^3 + \dots + n^3 = (1 + 2 + \dots + n)^2.$$

$$(c) (1^5 + 2^5 + \dots + n^5) + (1^7 + 2^7 + \dots + n^7) = 2(1 + 2 + \dots + n)^4.$$

$$(d) \operatorname{sen} x + \operatorname{sen} 2x + \dots + \operatorname{sen} nx = \frac{\operatorname{sen} \frac{(n+1)x}{2} \cdot \operatorname{sen} \frac{nx}{2}}{\operatorname{sen} \frac{x}{2}}.$$

**0.2.** *Seja  $F_n$  o  $n$ -ésimo termo da sequência de Fibonacci. Demonstrar que para todo natural  $n \geq 1$  temos*

$$(a) F_1 + F_2 + \dots + F_n = F_{n+2} - 1.$$

$$(b) F_{n+1} \cdot F_{n-1} - F_n^2 = (-1)^n.$$

$$(c) \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}.$$

$$(d) \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \binom{n-3}{3} + \dots = F_{n+1}, \text{ onde na soma interpretamos } \binom{m}{k} = 0 \text{ se } k > m.$$

**0.3.** *Demonstrar que*

$$(a) n^3 - n \text{ é um múltiplo de } 6 \text{ para todo natural } n.$$

$$(b) 5^n - 1 \text{ é múltiplo de } 24 \text{ para todo número natural } n \text{ par.}$$

$$(c) 2^n + 1 \text{ é múltiplo de } 3 \text{ para todo natural ímpar } n.$$

**0.4.** *Mostre que para todo natural  $n \geq 4$*

$$(a) 2^n < n!.$$

$$(b) 2n^3 > 3n^2 + 3n + 1.$$

**0.5.** *Dado um inteiro positivo  $n$ , definimos  $T(n, 1) = n$  e, para todo  $k \geq 1$ ,  $T(n, k+1) = n^{T(n, k)}$ . Prove que existe  $c \in \mathbb{N}$  tal que, para todo  $k \geq 1$ ,  $T(2010, k) < T(2, k+c)$ . Determine o menor inteiro positivo  $c$  com essa propriedade.*

**0.6.** *Mostre que para todo  $n$  e  $k$  inteiros positivos*

$$\binom{n}{n} + \binom{n+1}{n} + \binom{n+2}{n} + \dots + \binom{n+k}{n} = \binom{n+k+1}{n+1}.$$

**0.7.** *Demonstre a fórmula do binômio de Newton para  $n$  natural:*

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \dots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n.$$

**0.8.** Encontrar com demonstração uma expressão para o multinômio

$$(x_1 + x_2 + \cdots + x_k)^n$$

em termos dos coeficientes multinomiais

$$\binom{n}{i_1, \dots, i_k} \stackrel{\text{def}}{=} \frac{n!}{i_1! \cdots i_k!}$$

onde  $i_1 + \cdots + i_k = n$ .

**0.9.** Considere  $n$  retas em posição geral em um plano, isto é, sem que haja duas retas paralelas ou três retas concorrentes em um mesmo ponto.

(a) Determine em função de  $n$  o número de regiões em que as retas dividem o plano.

(b) Demonstre que é possível colorir essas regiões com duas cores sem que duas regiões vizinhas tenham a mesma cor (duas regiões são vizinhas se elas possuem um segmento de reta em comum).

**0.10.** Demonstrar que para cada número natural  $n$  existe um número natural  $M$  satisfazendo simultaneamente as seguintes duas condições:

(i)  $M$  possui  $n$  dígitos pertencentes ao conjunto  $\{1, 2\}$ .

(ii)  $M$  é divisível por  $2^n$ .

**0.11** (IMO1987). Mostre que não existe uma função  $f: \mathbb{N} \rightarrow \mathbb{N}$  tal que  $f(f(n)) = n + 1987$  para todo  $n \in \mathbb{N}$ .

## 0.2 Princípio da Casa dos Pombos

É intuitivamente claro que se colocamos  $n + 1$  objetos em  $n$  gavetas então haverá ao menos uma gaveta com mais de um objeto. Isto é exatamente o que afirma o chamado *Princípio da Casa dos Pombos* (PCP) ou *Princípio das Gavetas de Dirichlet*: se temos  $kn + 1$  pombos e  $n$  casinhas, então existirá uma casinha onde haverá pelo menos  $k + 1$  pombos. De fato, se em todas as casas houvesse no máximo  $k$  pombos, então o número de pombos não poderia ultrapassar  $kn$ .

O PCP parece bastante inocente, mas tem muitas aplicações interessantes, especialmente em argumentos de *existência* em que não se determina o objeto procurado explicitamente. Como exemplos falamos mais do que  $10^3$  palavras, vejamos alguns.

**Exemplo 0.9.** Do conjunto  $A = \{1, 2, \dots, 99, 100\}$ , escolhamos ao acaso 51 números. Demonstrar que entre os números escolhidos sempre existem dois que são consecutivos.

SOLUÇÃO: Para provar isto, primeiro escolhamos gavetas adequadas ao problema. Distribuímos os números de  $A$  em 50 “gavetas” assim construídas:

$$\{1, 2\} \quad \{3, 4\} \quad \{5, 6\} \quad \cdots \quad \{99, 100\}$$



Como há 50 gavetas das quais retiramos 51 números, sempre existirá uma gaveta da qual escolhermos dois números e estes, graças à nossa construção, serão consecutivos. Podemos generalizar este resultado considerando os números  $\{1, 2, \dots, 2n\}$  e escolhendo dentre eles  $n + 1$  números ao acaso.  $\square$

**Exemplo 0.10.** *Do conjunto  $A = \{1, 2, \dots, 99, 100\}$ , escolhamos ao acaso 55 números. Demonstrar que entre os números escolhidos sempre existem dois tais que sua diferença é 9.*

SOLUÇÃO: Como no exemplo anterior o problema é descobrir como formar as gavetas. Consideremos as gavetas numeradas  $0, 1, 2, \dots, 8$ , onde o número  $n$  é colocado na gaveta  $i$  se, e só se, o resto na divisão de  $n$  por 9 é  $i$ . Como escolhamos  $55 = 9 \times 6 + 1$  números, pelo PCP existirá uma gaveta  $j$  na qual há 7 ou mais números escolhidos. Mas em cada gaveta há no máximo 12 números (por exemplo, o conjunto  $\{1, 10, 19, 28, 37, 46, 55, 64, 73, 82, 91, 100\}$  possui exatamente 12 elementos). Segue, como no problema anterior, que existirão dois números que serão “consecutivos” em tal conjunto, isto é, dois números cuja diferença é 9.  $\square$

**Exemplo 0.11.** *Demonstrar que qualquer conjunto de  $n$  inteiros possui um subconjunto não vazio cuja soma dos elementos é divisível por  $n$ .*

SOLUÇÃO: Sejam  $a_1, a_2, \dots, a_n$  os elementos do conjunto, e definamos as “sommas parciais”  $s_j = a_1 + \dots + a_j$  para  $j = 1, \dots, n$ . Se algum dos  $s_j$  é divisível por  $n$  o problema fica resolvido. Se nenhum é divisível por  $n$ , então os possíveis restos na divisão por  $n$  são  $1, 2, \dots, n - 1$  e como há  $n$  somas parciais pelo PCP existem duas  $s_j$  e  $s_k$  com  $j < k$  que deixam o mesmo. Portanto  $s_k - s_j = a_{j+1} + \dots + a_k$  é divisível por  $n$  e  $\{a_{j+1}, a_{j+2}, \dots, a_k\}$  é o subconjunto procurado.

Por outro lado, observemos que  $n$  é a quantidade mínima de elementos para que se verifique tal condição, no sentido em que existem conjuntos  $A$  com  $n - 1$  elementos tais que a soma dos elementos de todo subconjunto não vazio de  $A$  não é divisível por  $n$ . Por exemplo,  $A = \{1, n + 1, 2n + 1, \dots, (n - 1)n + 1\}$  é um destes conjuntos (verifique!).  $\square$

**Exemplo 0.12.** *Seja  $\alpha$  um número real. Demonstrar que, para todo inteiro  $n \geq 2$ , existe um inteiro  $0 < k < n$  tal que o módulo da diferença entre  $k\alpha$  e seu inteiro mais próximo é menor ou igual a  $\frac{1}{n}$ .*

SOLUÇÃO: Vamos denotar por  $\{x\}$  a parte fracionária do número real  $x$ , isto é, o único real que satisfaz  $0 \leq \{x\} < 1$  e  $x = m + \{x\}$  para algum  $m \in \mathbb{Z}$ .

Considere  $\{k\alpha\}$  para  $k = 1, 2, \dots, n$ . Particione o intervalo  $[0, 1)$  em  $n$  partes de tamanho  $\frac{1}{n}$ :

$$[0, 1) = \left[0, \frac{1}{n}\right) \cup \left[\frac{1}{n}, \frac{2}{n}\right) \cup \left[\frac{2}{n}, \frac{3}{n}\right) \cup \dots \cup \left[\frac{n-1}{n}, 1\right)$$

Se  $\{k\alpha\} \in [0, \frac{1}{n})$  ou  $\{k\alpha\} \in [\frac{n-1}{n}, 1)$  para algum  $k = 1, \dots, n - 1$ , o problema acabou. Caso contrário, pelo PCP haverá duas partes fracionárias  $\{j\alpha\}$  e  $\{k\alpha\}$

com  $1 \leq j < k \leq n - 1$  pertencentes a um mesmo intervalinho dentre os  $n - 2$  restantes. Sendo  $x = (k - j)\alpha$ , teremos

$$\{x\} = \begin{cases} \{k\alpha\} - \{j\alpha\} & \text{se } \{k\alpha\} \geq \{j\alpha\} \\ 1 + \{k\alpha\} - \{j\alpha\} & \text{se } \{k\alpha\} < \{j\alpha\} \end{cases}$$

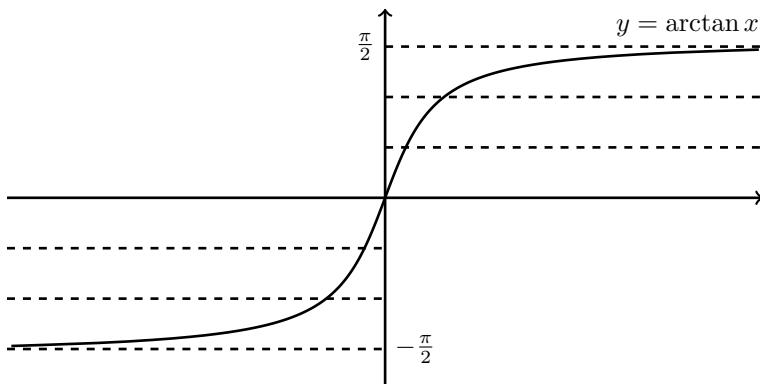
e portanto  $\{x\} \in [0, \frac{1}{n})$  ou  $\{x\} \in [\frac{n-1}{n}, 1)$ , assim  $k - j$  satisfaz as condições do problema.  $\square$

**Exemplo 0.13.** *Demonstrar que dados 7 números reais sempre é possível escolher 2 deles, digamos  $a$  e  $b$ , tais que*

$$\left| \frac{a - b}{1 + ab} \right| < \frac{1}{\sqrt{3}}.$$

**SOLUÇÃO:** Vejamos inicialmente que a função  $y = \tan x$  é crescente entre  $(-\frac{\pi}{2}, \frac{\pi}{2})$ , e além disso, para cada real  $r$  existe um único ângulo  $\theta$  neste intervalo com  $r = \tan \theta$ .

Portanto, dados os 7 números reais, a cada um deles podemos fazer corresponder um ângulo no intervalo  $(-\frac{\pi}{2}, \frac{\pi}{2})$ , e dividindo tal intervalo em 6 partes iguais, i.e., em 6 intervalos de comprimento  $\frac{\pi}{6}$ , abertos à esquerda, existirão 2 ângulos  $\theta$  e  $\gamma$  que estejam no mesmo intervalo, e portanto,  $|\theta - \gamma| < \frac{\pi}{6}$ .



Podemos supor sem perda de generalidade que  $a = \tan \theta > \tan \gamma = b$  e como a função tangente é crescente,

$$\frac{a - b}{1 + ab} = \frac{\tan \theta - \tan \gamma}{1 + \tan \theta \tan \gamma} = \tan(\theta - \gamma) < \tan \frac{\pi}{6} = \frac{1}{\sqrt{3}},$$

como queríamos demonstrar.  $\square$

## Problemas Propostos

**0.12.** *Escolhem-se 7 pontos no interior de um retângulo de dimensões  $2 \times 3$ . Demonstrar que sempre é possível encontrar dois pontos tal que sua distância é menor ou igual a  $\sqrt{2}$ .*

**0.13.** Escolhem-se 9 pontos no interior de um quadrado de lado 1. Demonstrar que é possível escolher 3 deles de tal forma que a área do triângulo que formam é menor ou igual a  $\frac{1}{8}$ .

**0.14.** Dadas 6 pessoas numa festa, demonstrar que necessariamente existem 3 pessoas que se conhecem mutuamente ou 3 pessoas que não se conhecem mutuamente. Suponha que a relação de conhecer é simétrica. Este é um caso particular do teorema de Ramsey, veja por exemplo [2].

**0.15.** Do conjunto  $A = \{1, 2, \dots, 99, 100\}$  escolhemos 51 números. Demonstrar que, entre os 51 números escolhidos, existem dois tais que um é múltiplo do outro.

**0.16.** Dado um número irracional  $u$ , demonstrar que sempre é possível encontrar infinitos números racionais  $\frac{p}{q}$ ,  $p, q \in \mathbb{Z}$ , de tal forma que

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

**0.17** (IMO1985). Dado um conjunto  $M$  com 1985 inteiros positivos distintos, nenhum dos quais tem divisores primos maiores do que 23, mostre que há 4 elementos em  $M$  cujo produto é uma quarta potência.

**0.18** (OIbM1998). Determinar o mínimo valor de  $n$  para o qual, de todo subconjunto de  $\{1, 2, \dots, 999\}$  com  $n$  elementos, é possível selecionar quatro inteiros diferentes  $a, b, c, d$  tais que  $a + 2b + 3c = d$ .

**0.19.** Demonstrar que de qualquer conjunto de  $2^{n+1} - 1$  números inteiros positivos é possível escolher  $2^n$  elementos de tal forma que sua soma é divisível por  $2^n$ .

**0.20** (IMO2001). Sejam  $n_1, n_2, \dots, n_m$  inteiros com  $m$  ímpar. Denotemos por  $x = (x_1, \dots, x_m)$  uma permutação dos inteiros  $1, 2, \dots, m$ , e definamos  $f(x) = x_1 n_1 + \dots + x_m n_m$ . Demonstre que existem duas permutações  $a$  e  $b$  tais que  $f(a) - f(b)$  é divisível por  $m!$ .

**0.21** (IMO1991). Seja  $S = \{1, 2, \dots, 280\}$ . Encontrar o menor inteiro  $n$  para o qual todo subconjunto de  $S$  com  $n$  elementos contém cinco números que são dois a dois primos entre si.

**0.22** (Erdős). Mostrar que toda a sequência com  $n^2 + 1$  números reais contém ou uma subsequência crescente com  $n + 1$  termos ou uma subsequência decrescente com  $n + 1$  termos.

**0.23.** Pintamos todos os pontos do plano de azul, verde ou preto. Mostrar que existe no plano um retângulo cujos vértices têm todos a mesma cor.

# Bibliografia

- [1] F. E. Brochero Martinez, C. G. Moreira, N. C. Saldanha, E. Tengan - Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro - Projeto Euclides, IMPA, 2010.
- [2] C. G. Moreira, *O teorema de Ramsey*, Revista Eureka! 6, 23–29.
- [3] A. Shen e N. K. Vereshchagin, *Basic Set Theory*, AMS, 2002.

## Dicas e Soluções

0.2 (d) Use a identidade  $\binom{n-k}{k} + \binom{n-k}{k+1} = \binom{n+1-k}{k+1}$ .

0.3 (b) Use a igualdade  $5^{n+2} - 1 = 25 \cdot 5^n - 1 = 24 \cdot 5^n + 5^n - 1$ .

0.5 Vamos ver que  $c = 3$  funciona. Para isso, vamos mostrar por indução algo ligeiramente mais forte que o pedido: para todo  $k \geq 1$ , temos  $12 \cdot T(2010, k) < T(2, k + 3)$ . De fato, para  $k = 1$ , temos  $24120 = 12 \cdot T(2010, 1) < 65536 = T(2, 4)$ , e, se vale  $12 \cdot T(2010, k) < T(2, k+3)$  para um certo  $k \geq 1$ , teremos

$$\begin{aligned} T(2, k + 4) &= 2^{T(2, k+3)} > 2^{12 \cdot T(2010, k)} = 4096^{T(2010, k)} = \\ &= 2^{T(2010, k)} \cdot 2048^{T(2010, k)} > 12 \cdot 2010^{T(2010, k)} = 12 \cdot T(2010, k + 1), \end{aligned}$$

como queríamos.

Note que  $T(2010, 1) = 2010 > 16 = T(2, 3)$ , donde necessariamente  $c > 2$ .

0.8 Podemos provar por indução em  $n$  que

$$(x_1 + x_2 + \dots + x_k)^n = \sum_{\substack{i_j \geq 0, \forall j \leq k \\ i_1 + \dots + i_k = n}} \binom{n}{i_1, \dots, i_k} x_1^{i_1} x_2^{i_2} \dots x_k^{i_k},$$

usando a identidade

$$\binom{n}{i_1, i_2, \dots, i_{k-1}, i_k} = \sum_{j=1}^k \binom{n-1}{i_1, \dots, i_{j-1}, i_j - 1, i_{j+1}, \dots, i_k},$$

para  $i_1 + \dots + i_k = n$ .

- 0.10 Denotando um tal  $M$  por  $M_n$ , tome  $M_{n+1} = 2 \cdot 10^n + M_n$ , caso  $M_n$  seja divisível por  $2^{n+1}$ , e  $M_{n+1} = 10^n + M_n$ , caso contrário.
- 0.11 Considere a função  $g : \{0, 1, \dots, 1986\} \rightarrow \{0, 1, \dots, 1986\}$  em que  $g(k)$  é o resto da divisão de  $f(k)$  por 1987. Mostre que  $g(g(k)) = k$  para todo  $k$ , e conclua que existe  $a \in \{0, 1, \dots, 1986\}$  tal que  $g(a) = a$ . Use isso para chegar a uma contradição, considerando a restrição de  $f$  aos naturais que deixam resto  $a$  quando divididos por 1987.
- 0.12 Divida o retângulo como a união de 6 quadrados de lado 1, e observe que dois dos 7 pontos devem estar num mesmo quadrado.
- 0.14 Considere uma das pessoas, que chamaremos de  $P$ . Como há 5 outras pessoas na festa, ou há 3 outras pessoas que  $P$  conhece ou há 3 outras pessoas que  $P$  não conhece. Suponha a primeira alternativa, sem perda de generalidade. Se há duas dessas 3 pessoas que  $P$  conhece que se conhecem, junto com  $P$  teríamos 3 pessoas que se conhecem mutuamente. Caso contrário, essas 3 pessoas que  $P$  conhece são 3 pessoas que se desconhecem mutuamente.
- 0.15 Escreva cada um desses 51 números como  $2^k \cdot b$ , com  $b$  ímpar. Há apenas 50 possibilidades para  $b$ , de modo que a dois desses 51 números será associado um mesmo  $b$  e portanto um será múltiplo do outro.
- 0.16 Use o resultado do Exemplo 0.12.
- 0.17 Os possíveis fatores primos dos elementos de  $M$  são os seguintes 9 primos: 2, 3, 5, 7, 11, 13, 17, 19, 23. Dado um subconjunto de  $M$  com mais de  $512 = 2^9$  elementos, haverá dois deles em cuja fatoração prima as paridades dos expoentes de cada primo coincidem, e portanto seu produto será um quadrado perfeito. Usando repetidamente esse argumento, obtemos 737 pares disjuntos de elementos de  $M$  tais que o produto dos elementos de cada par é um quadrado perfeito (de fato, se retirarmos de  $M$  menos de 737 pares de elementos distintos, sobram pelo menos  $1985 - 2 \cdot 736 = 513$  elementos, dos quais podemos obter um novo par). Agora, como há mais de 512 pares em que o produto dos elementos é um quadrado perfeito, e os primos que dividem cada um desses produtos estão entre os 9 primos listados acima, haverá dois desses pares para os quais, se tomarmos os expoentes de cada um desses primos no produto dos termos do par e os dividirmos por 2, as paridades dos resultados coincidirão, e portanto o produto dos 4 termos desses dois pares será uma quarta potência.
- 0.18 Note que, se  $X = \{166, 167, \dots, 999\}$ , então  $X$  tem 834 elementos e  $a + 2b + 3c \geq 168 + 2 \cdot 167 + 3 \cdot 166 > 999$  para quaisquer elementos distintos  $a, b, c$  de  $X$ . A resposta é 835 - de fato, se o conjunto tem pelo menos 835 elementos e  $c$  e  $b$  são o menor e o segundo menor elementos do conjunto, então  $3c + 2b \leq 3 \cdot 165 + 2 \cdot 166 = 827$  e, se  $1 \leq m \leq 999 - (3c + 2b)$ ,  $m \notin \{b, c\}$ , caso o conjunto não satisfizesse as condições do enunciado, teríamos  $m$  ou  $3c + 2b + m$  fora do conjunto, o qual teria então pelo menos  $999 - 827 - 2 = 170$  elementos de  $\{1, 2, \dots, 999\}$  fora dele, absurdo.
- 0.20 Consideremos os restos das divisões de  $f(x)$  por  $m!$ . Se  $f(a)$  e  $f(b)$  deixam restos iguais, então  $f(a) - f(b)$  será múltiplo de  $m!$ . Caso

os restos sejam todos diferentes, como há  $m!$  permutações  $x$  e  $m!$  possíveis restos, todos os restos são atingidos uma vez, e a soma de todos os restos é  $0 + 1 + \dots + (m-1) = m!(m-1)/2$ , que deixa resto  $m!/2$  quando dividida por  $m!$ . Mas a soma de todos os  $f(x)$  é  $(1+2+\dots+m) \cdot (m-1)! \cdot (n_1 + \dots + n_m) = ((n+1+\dots+n_m) \cdot m! \cdot (m+1)/2)$ , que é múltiplo de  $m!$ , pois  $(m+1)/2$  é inteiro, absurdo.

- 0.21 A resposta é 217. Considere o conjunto dos inteiros positivos entre 1 e 280 que são múltiplos de 2, 3, 5 ou 7. Este conjunto tem 216 membros, e, dados 5 de seus elementos, dois deles terão um fator comum pertencente a  $\{2, 3, 5, 7\}$ .

Sejam agora  $A_1 = \{1\} \cup \{p \text{ primo} | 2 \leq p < 280\}$ ,  $A_2 = \{2 \cdot 41, 3 \cdot 37, 5 \cdot 31, 7 \cdot 29, 11 \cdot 23, 13 \cdot 19\}$ ,  $A_3 = \{2 \cdot 37, 3 \cdot 31, 5 \cdot 29, 7 \cdot 23, 11 \cdot 19, 13 \cdot 17\}$ ,  $A_4 = \{2 \cdot 31, 3 \cdot 29, 5 \cdot 23, 7 \cdot 19, 11 \cdot 17, 13^2\}$ ,  $A_5 = \{2 \cdot 29, 3 \cdot 23, 5 \cdot 19, 7 \cdot 17, 11 \cdot 13\}$ , e  $A_6 = \{2 \cdot 23, 3 \cdot 19, 5 \cdot 17, 7 \cdot 13, 11^2\}$ . Os elementos de cada conjunto  $A_i$  são primos entre si dois a dois.  $A_1$  tem 60 elementos,  $A_2, A_3$ , e  $A_4$  têm 6 elementos cada e  $A_5$  e  $A_6$  têm 5 elementos cada. Assim, os conjuntos  $A_i$  têm, no total, 88 elementos. Se um subconjunto  $X$  de  $\{1, 2, \dots, 280\}$  tem 217 elementos, terá pelo menos 25 elementos em comum com a união dos 6 conjuntos  $A_i$ , e, como  $25 > 4 \cdot 6$ , existe  $i \leq 6$  tal que  $X$  tem pelo menos 5 elementos em comum com  $A_i$ , os quais, por construção dos  $A_i$ , são necessariamente primos entre si dois a dois.

- 0.22 Considere, para cada  $k$  com  $1 \leq k \leq n^2 + 1$ , o tamanho  $f(k)$  da maior subsequência monótona não-crescente da sequência dada cujo primeiro termo é o  $k$ -ésimo termo da sequência. Se, para algum  $k$ ,  $f(k) \geq n + 1$ , o problema está resolvido. Senão,  $f(k)$  pode assumir apenas os valores  $1, 2, \dots, n$ , e portanto existem  $n + 1$  valores  $k_1 < k_2 < \dots < k_{n+1}$  com  $f(k_1) = f(k_2) = \dots = f(k_{n+1})$ . Nesse caso, os termos da sequência de índices  $k_1, k_2, \dots, k_{n+1}$  formarão uma subsequência crescente.