Resolução da Lista 2 da disciplina de Matemática Discreta

Feita por Guilherme de Abreu Barreto[1]

Estratégias de demonstração

Exercício 1

Proposição

Sejam n e k dois números naturais onde $n > k$. Se tentarmos distribuir n objetos em k urnas (P), então pelo menos uma das urnas conterá mais de um objeto (Q). $P \implies Q$.

Contrapositiva

Sejam n e k dois números naturais onde $n > k$. Pelo menos uma urna restará vazia ($\neg Q$) se tentarmos distribuir k objetos em n urnas ($\neg P$). $\neg Q \implies \neg P$.

Exercício 2

Consideremos N um número de n dígitos $\{a_1, a_2, \dots, a_n\}$ cuja soma $a_1 + a_2 + \cdots + a_n = \sum_{i=1}^{n} a_i = k$. Sabemos que o critério de divisibilidade de N por 9 é $N|9 \iff N = 9q$, $\forall N, n, a, k, q \in \mathbb{N}$. Podemos descrever N da seguinte maneira:

$$N = a_1 \cdot 10^{n-1} + a_2 \cdot 10^{n-2} + \cdots + a_n \cdot 10^{n-n} = \sum_{i=1}^{n} a_i 10^{n-i}$$

Por vez, 10^n pode ser escrito da seguinte forma:

$$10^n = 99\dots9(\text{n - 1 vezes}) + 1 = \underbrace{\sum_{i=1}^{n-1} 9 \cdot 10^i}_{\equiv 9q} + 1$$

Logo, para cada dígito de N teremos:

$$N = a_1[(10^{n-1} - 1) + 1] + a_2((10^{n-2} - 1) + 1] + \cdots + a_n[(10^{n-n} - 1) + 1] = \sum_{i=1}^{n} a_i(9q + 1) = k9q + k$$

Finalmente, $9kq|9$ e, se $k|9$ o for, então também é $N|9$. ∎

Exercício 3

Prova direta

Se um número n^2 é par, ou seja, $n^2 = 2k$ para algum $k \in \mathbb{R}$, n também é par.

$$n^2 = 2k \implies n = \pm\sqrt{2k} \cdot \frac{\sqrt{2}}{\sqrt{2}} = 2 \cdot \underbrace{\left(\pm\frac{\sqrt{k}}{\sqrt{2}}\right)}_{k_2} = 2k_2 \blacksquare$$

Prova por contrapositiva

Retomemos o enunciado:

> Se n^2 é par (P), então n é par (Q, $P \implies Q$).

A contrapositiva disso seria:

> Se n é ímpar ($\neg Q$), n^2 é ímpar ($\neg P$, $\neg Q \implies \neg P$).

Se n é ímpar, ou seja, $n = 2k + 1$ para qualquer $k \in \mathbb{R}$, n^2 também é impar.

$$n^2 = n \cdot n = (2k+1)(2k+1) = 4k^2 + 2k + 2k + 1 = 2\underbrace{(2k^2 + 2k)}_{k_2} + 1 = 2k_2 + 1 \blacksquare$$

A primeira demonstração é mais objetiva: foram menores os números de passos requeridos. Mas em termos de compreensibilidade a alternativa possui seu valor.

Exercício 4

Um número primo inteiro, $p \in \mathbb{Z}$ é aquele que tem **somente** quatro divisores distintos, ± 1 e $\pm p$. Já um número primo natural, $p \in \mathbb{N}$ tem **unicamente** dois divisores naturais distintos: o número um e ele mesmo. Por estarmos tratando aqui de valores para p tais que $p > 3$, estamos tratando de números primos **naturais**. Seria a fórmula $3k \pm 1$, $k \in \mathbb{N}$, capaz de representá-los?

- Todo número $p > 2$ é **ímpar**, doutra forma seria divisível por dois e não primo. Se segue que todo número p ímpar maior que 3 **não é divisível** por 3.
- Múltiplos de três são ora ímpar, ora par:
  - $3(2k) = 2(3k) \equiv 0 (\mathrm{mod}\ 2)$, par;
  - $3(2k \pm 1) = 6n \pm 3 = 6k \pm 2 \pm 1 = 2(3k \pm 1) \pm 1 \equiv 0 (\mathrm{mod}\ 2) \pm 1$, ímpar.

Assim, proponho que esta fórmula seja capaz de representar todos os números naturais impares n_i não múltiplos de 3 para todo valor $2k$.

$n_i = 2k \pm 1 \equiv 0 (\text{mod } 2) \pm 1$
$3(2k) \pm 1 = 2(3k) \pm 1 \equiv 0 (\text{mod } 2) \pm 1$
$\therefore n_i \equiv 3(2k) \pm 1 \blacksquare$

Exercício 5

Sempre que qualquer um dos lados de uma inequação sofre uma multiplicação por um valor menor que 0, o sinal de desigualdade assume sua forma dual, de tal sorte que $-2 < 1$ ao ser elevado ao quadrado fica:

$$(-2)\underbrace{(-2)}_{<0} > 1 \cdot 1 \implies 4 > 1 \blacksquare$$

Exercício 6

a. Conforme exposto anteriormente, qualquer número ímpar pode ser representado pela forma $2k \pm 1 \equiv 0 (\text{mod } 2) \pm 1$, utilizaremo-nos aqui da forma $n = 2k + 1$:

$n^2 + 4n = (2k+1)^2 + 4(2k+1) = 4k^2 + 4k + 1 + 8k + 4 =$
$2(2k^2 + 2k + 2) + 1 \equiv 0 (\text{mod } 2) + 1; \text{é ímpar.} \blacksquare$

b. A contrapositiva dessa afirmação é: se r é racional então r^2 é racional. Por definição um número racional é aquele que pode ser representado na forma

$$\frac{n}{d}, n \in \mathbb{Z}, d \in \mathbb{Z}^*$$

Então,

$$r = \frac{n}{d} \implies r^2 = \frac{n^2}{d^2} = \frac{n_2}{d_2}, n_2 \in \mathbb{Z}, d_2 \in \mathbb{Z}^* \blacksquare$$

c. Falso. Por exemplo, para $n = 2$ este não é o caso:

$$2^5 < 5^n \implies 32 < 25 \equiv F$$

Enquanto para $n = 1$ é:

$$1^5 < 5^1$$

Então seria correto dizer que $(\exists n \in \mathbb{N})(n^5 < 5^n)$. $\blacksquare$

d. Na matemática, considera-se triviais soluções ou exemplos ridiculamente simples e de pouco interesse. Muitas vezes, as soluções ou exemplos triviais que envolvem o número 0 são considerados triviais. Este não é o caso com a desigualdade de Bernoulli, que tem implicações importantes para a análise combinatória necessita ser demonstrada por indução finita. Isto é, admite-se 0 enquanto base de indução, mas então procede-se a demonstrar que tal hipótese vale para qualquer número natural n. Tal demonstração se dá da seguinte maneira:

1. $(1+r)^n \geq 1+nr$ é válido para $n=0$: $(1+r)^0 = 1; 1 \geq 1+0r$.

2. Agora, veremos se isso é válido para $n+1$:

$$(1+r)^n \geq 1+nr \implies (1+r)(1+r)^n \geq (1+r)(1+nr) \implies$$
$$(1+r)^{n+1} \geq 1+nr+r+\underbrace{nr^2}_{\geq 0}$$

Repare que em $(1+r)^{n+1} \geq 1+nr+r+nr^2$, nr^2 é sempre maior ou igual à 0, então

$$(1+r)^{n+1} \geq 1+nr+r \implies (1+r)^{n+1} \geq 1+r(n+1) \blacksquare$$

Fica demonstrado que tal igualdade é válida para qualquer $n \in \mathbb{N}$.

Exercício 7

a. Considerando a progressão aritmética $1, \ldots, n$, a soma de todos os termos desta progressão (S_n)pode ser escrita das seguintes formas:

$$S_n = 1 + \cdots + n$$
$$S_n = n + \cdots + 1$$

Somando estas formulações membro a membro, obtemos:

$$2S_n = (1+n) + (2+(n-1)) + \cdots + ((n-1)+2) + (n+1)$$

Nesta formulação, notemos que

- Todos os pares entre parênteses têm o mesmo valor, por serem simétricos em relação às extremidades da progressão;

- existem n pares.

Logo,

$$2S_n = n(1+n) \implies S_n = \frac{n(n+1)}{2}$$

Consideremos agora a soma dos cubos $1^3, \ldots, n^3$. O produto notável cubo da soma pode ser descrito da seguinte forma:

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Então, enquanto $k^3 = k^3$ para qualquer número $k \in \mathbb{Z}$, temos que

$$(k+1)^3 = k^3 + 3k^2 + 3k + 1$$

Então, $1^3 + \cdots + n^3$ equivale à

$$+\begin{cases} \cancel{1^3} = 1^3 \\ \cancel{2^3} = 1^3 + 3(1)^2 + 3(1) + \cancel{1} \\ \cancel{3^3} = \cancel{2^3} + 3(2)^2 + 3(2) + 1 \\ \cancel{4^3} = \cancel{3^3} + 3(3)^2 + 3(3) + 1 \\ \vdots \\ \cancel{n^3} = \cancel{(n-1)^3} + 3(n-1)^2 + 3(n-1) + 1 \\ (n+1)^3 = \cancel{n^3} + 3n^2 + 3n + 1 \end{cases}$$
$$\implies (n+1)^3 = 1^3 + 3S_{n^2} + 3S_n + (n+1)$$

Onde S_{n^2} é o valor da soma dos quadrados de $1, \ldots, n$, ou seja, o valor que buscamos. Resolvendo essa equação, temos:

$$\begin{aligned} &(n+1)^3 = 1 + 3S_{n^2} + 3\frac{n(n+1)}{2} + (n+1) \\ &\implies 6S_{n^2} = 2(n+1)^3 - 3n(n+1) - 2(n+1) \\ &= (n+1)[2(n+1)^2 - 3n - 2] \\ &= (n+1)[2(n^2 + 2n + 1) - 3n - 2] \\ &= (n+1)(2n^2 + 4n + \cancel{2} - 3n - \cancel{2}) \\ &= n(n+1)(2n+1) \\ &\implies S_{n^2} = \frac{n(n+1)(2n+1)}{6} \;\blacksquare \end{aligned}$$

b.

1. A hipótese se conforma na base de indução: $1^3 = 1^2$.

2. Se assumirmos que

$$1^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2$$

é verdadeiro, então

$$1^3 + \cdots + (n+1)^3 = \left[\frac{(n+1)(n+2)}{2}\right]^2$$

também o é.

3. Testemos esta hipótese de indução:

$$1^3 + \cdots + n^3 + (n+1)^3 = \left[\frac{n(n+1)}{2}\right]^2 + (n+1)^3 = (n+1)^2\left(\frac{n^2}{4} + n + 1\right)$$
$$= \frac{(n+1)^2(n^2+4n+4)}{4} = \frac{(n+1)^2(n+2)^2}{4} = \left[\frac{(n+1)(n+2)}{2}\right]^2 \blacksquare$$

c.

- Base de indução ($n = 2$):

$$\frac{a_1}{1+a_1} + \frac{a_2}{(1+a_1)(1+a_1+a_2)} = \frac{a_1(1+a_1+a_2)+a_2}{(1+a_1)(1+a_1+a_2)}$$

$$= \frac{a_1 + a_1^2 + a_1a_2 + a_2}{(1+a_1)(1+a_1+a_2)} = \frac{a_1\,\cancel{(1+a_1)} + a_2\,\cancel{(1+a_1)}}{\cancel{(1+a_1)}(1+a_1+a_2)} = \frac{a_1+a_2}{1+a_1+a_2}$$

- Hipótese de indução: se

$$\frac{a_1+\cdots+a_n}{1+a_1+\ldots a_n} = \frac{a_1}{1+a_1} + \cdots + \frac{a_n}{(1+a_1+\cdots+a_{n-1})(1+a_1+\cdots+a_n)}$$

para todo $n \in \mathbb{N}$, então

$$\frac{a_1+\cdots+a_{n+1}}{1+a_1+\ldots a_{n+1}} = \frac{a_1}{1+a_1} + \cdots + \frac{a_{n+1}}{(1+a_1+\cdots+a_n)(1+a_1+\cdots+a_{n+1})}$$

- Passo de indução:

$$\frac{a_1}{1+a_1} + \cdots + \frac{a_{n+1}}{(1+a_1+\cdots+a_n)(1+a_1+\cdots+a_{n+1})} =$$

$$\underbrace{\frac{a_1+\cdots+a_n}{1+a_1+\ldots a_n}}_{\text{Por hipótese}} + \frac{a_{n+1}}{(1+a_1+\cdots+a_n)(1+a_1+\cdots+a_{n+1})}$$

Prosseguimos com a substituição de variáveis $a_1 + \cdots + a_n = A$:

$$\frac{A}{1+A} + \frac{a_{n+1}}{(1+A)(1+A+a_{n+1})} = \frac{A(1+A+a_{n+1})+a_{n+1}}{(1+A)(1+A+a_{n+1})}$$

$$= \frac{A + A^2 + Aa_{n+1} + a_{n+1}}{(1+A)(1+A+a_{n+1})} = \frac{A\,\cancel{(1+A)} + a_{n+1}\,\cancel{(1+A)}}{\cancel{(1+A)}(1+A+a_{n+1})} = \frac{a_1+\cdots+a_{n+1}}{1+a_1+\ldots a_{n+1}} \blacksquare$$

Exercício 8

a. Três é um número ímpar e, portanto, pode ser escrito na forma $(2k+1)$. Logo,

$$(2k+1)^n - 1 = (2^n k^n + 2^{n-1}k^{n-1} + \cdots + 2k + \cancel{1}) - \cancel{1}$$
$$= 2(2^{n-1}k^n + 2^{n-2}k^{n-1} + \cdots + k) \equiv 0 (\text{mod } 2)$$

Ou seja, um número par. ■

b. Se n é par, então

$$5^n - 2^n = 5^{2k} - 2^{2k} = (5^k - 2^k)(5^k + 2^k)$$
$$= (5-2)(5^{k-1} + 5^{k-2} \cdot 2 + \cdots + 5 \cdot 2^{k-2} + 2^{k-1})(5^k + 2^k)$$
$$= 3(5^{k-1} + 5^{k-2} \cdot 2 + \cdots + 5 \cdot 2^{k-2} + 2^{k-1})(5^k + 2^k) \equiv 0 (\text{mod } 3)$$

Senão,

$$5^{2k+1} - 2^{2k+1} = (5-2)(5^{2k} + 5^{2k-1} \cdot 2 + \cdots + 5 \cdot 2^{2k-1} + 2^{2k}) =$$
$$3(5^{2k} + 5^{2k-1} \cdot 2 + \cdots + 5 \cdot 2^{2k-1} + 2^k) \equiv 0 (\text{mod } 3)$$ ■

c. $2^n + 3^n$ é múltiplo de 5 quando $n = 2k+1$ (ida):

$$2^{2k+1} - 3^{2k+1} = (2+3)(2^{2k} + 2^{2k-1} \cdot 3 + \cdots + 2 \cdot 3^{2k-1} + 3^k) =$$
$$5(2^{2k} + 2^{2k-1} \cdot 3 + \cdots + 2 \cdot 3^{2k-1} + 3^k) \equiv 0 (\text{mod } 5)$$

o número 5, ao ser multiplicado, **não** produz um número da forma $2^n + 3^n$, quando $n = 2k$ (volta):

- Toda potência de 5 tem como último algarismo 5, pois o resultado da multiplicação de 5 por 5 é 25.
- Toda potência $2^{2k} = 4^k, 4 \times 4 = 1\mathbf{6}; 16 \times 4 = 2\mathbf{4}; 24 \times 4 = 9\mathbf{6}$, e assim por diante. Ou seja, ora se produz final 6, ora se produz final 4.
- Toda potência $3^{2k} = 9^k, 9 \times 9 = 8\mathbf{1}; 81 \times 9 = 72\mathbf{9}; 729 \times 9 = 656\mathbf{1}$, e assim por diante. Ou seja, ora se produz final 1, ora se produz final 9.

Como 1 + 6 = 7 produz final 7 e 9 + 4 = 13 produz final 3, não é possível que o número resultante desta soma seja múltiplo de 5. ■

d.

- Base da indução $(k = 1)$:

$$0^3 + 1^3 + 2^3 = 9 \equiv 0 (\text{mod } 9);$$

- Hipótese de indução: Se

$$(k-1)^3 + k^3 + (k+1)^3 = k^3 - \cancel{3k^2} + 3k - \cancel{1} + k^3 + k^3 + \cancel{3k^2} + 3k - \cancel{1}$$
$= 3k^3 + 6k \equiv 0 (\text{mod } 9)$para qualquer $k \in \mathbb{N}$, então também

$$3(k+1)^3 + 6(k+1) \equiv 0 (\text{mod } 9)$$

- Passo de indução:

$$k^3+(k+1)^3+(k+2)^3 = k^3+k^3+3k^2+3k+1+k^3+6k^2+12k+8$$
$$= 3k^3+9k^2+9k+3+6k+6 = 3(k^3+3k^2+3k+1)+6k+6$$
$$= 3(k+1)^3+6(k+1) \equiv 0 (\text{mod } 9) \blacksquare$$

Logo, conclui-se que a soma de três cubos consecutivos de fato produz um número divisível por 9.

Exercício 9

- Base da indução $(n=1)$:

$$(\cos\theta + i\sin\theta)^1 = \cos\theta + i\sin\theta$$

- Hipótese de indução: se

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$$

para todo $n \geq 1$, então também

$$(\cos\theta + i\sin\theta)^{n+1} = \cos[(n+1)\theta] + i\sin[(n+1)\theta]$$

- Passo de indução:

$$(\cos\theta + i\sin\theta)^{n+1} = (\cos\theta + i\sin\theta)^n(\cos\theta + i\sin\theta)$$
$$= \underbrace{[\cos(n\theta) + i\sin(n\theta)]}_{\text{Por hipótese}}(\cos\theta + i\sin\theta)$$
$$= \cos(n\theta)\cos\theta - \sin(n\theta)\sin\theta + i[\cos(n\theta)\sin(\theta) + \sin(n\theta)\cos\theta]$$
$$= \underbrace{\cos[(n+1)\theta] + i\sin[(n+1)\theta]}_{\text{Por identidade trigonométrica}}$$

Fazendo uso da identidade de Euler

- Base da indução $(n=1)$:

$$e^{1i\theta} = \cos\theta + i\sin\theta$$

- Hipótese de indução: se

$$e^{ni\theta} = \cos(n\theta) + i\sin(n\theta)$$

para todo $n \geq 1$, então também

$$e^{(n+1)i\theta} = \cos[(n+1)\theta] + i\sin[(n+1)\theta]$$

- Passo de indução:

$$e^{(n+1)i\theta} = e^{ni\theta}e^{1i\theta} = (\cos\theta + i\sin\theta)^n(\cos\theta + i\sin\theta)$$

$$
\begin{aligned}
&= \underbrace{[\cos(n\theta) + i\sin(n\theta)]}_{\text{Por hipótese}}(\cos\theta + i\sin\theta) \\
&= \cos(n\theta)\cos\theta - \sin(n\theta)\sin\theta + i[\cos(n\theta)\sin(\theta) + \sin(n\theta)\cos\theta] \\
&= \underbrace{\cos[(n+1)\theta] + i\sin[(n+1)\theta]}_{\text{Por identidade trigonométrica}} \blacksquare
\end{aligned}
$$

Exercício 10

- Base da indução $(n = 1)$

$$H_1(x) = e^{x^2}\left(-\frac{d}{dx}\right)^1 e^{-x^2} = e^{x^2}\cdot 2xe^{-x^2} = 2x$$

- Hipótese de indução: se

$$H_n(x) = e^{x^2}\left(-\frac{d}{dx}\right)^n e^{-x^2}$$

para todo $n \geq 1$, então também

$$H_{n+1}(x) = e^{x^2}\left(-\frac{d}{dx}\right)^{n+1} e^{-x^2}$$

- Passo de indução:

$$
\begin{aligned}
&H_n(x) = e^{x^2}\left(-\frac{d}{dx}\right)^n e^{-x^2} \implies \left(\frac{d}{dx}\right)^n e^{-x^2} = (-1)^n H_n(x)e^{-x^2} \\
&\left(\frac{d}{dx}\right)^{n+1} e^{-x^2} = (-1)^n \underbrace{\left[\left(\frac{d}{dx}H_n(x)\right)e^{-x^2} + H_n(x)(-2x)e^{-x^2}\right]}_{\text{Aplicação da regra da cadeia}} \\
&= (-1)^{n+1}e^{-x^2}\left[\left(2x - \frac{d}{dx}\right)H_n(x)\right] = (-1)^{n+1}e^{x^2}\left(\frac{d}{dx}\right)^{n+1} e^{-x^2} = H_{n+1}(x) \blacksquare
\end{aligned}
$$

Quanto a paridade do polinômio de Hermite, vemos que ele possui grau n, de tal sorte que, como demonstra o gráfico abaixo

Este produz uma função ímpar quando n é ímpar e uma função par quando não.

Exercício 11

- Base de indução $(n = 1)$:

$$\frac{[f(x)]'}{f(x)} = \frac{f'(x)}{f(x)}$$

Para demonstrar a propriedade das derivadas subjacente a este cálculo, vale a pena explicitar o passo seguinte também. Considerando que

$$f(x) = g(x)h(x) \implies f'(x) = g(x)h'(x) + g'(x)h(x)$$

Então

$$\frac{[f_1(x)f_2(x)]'}{f_1(x)f_2(x)} = \frac{\cancel{f_1(x)}f_2'(x)}{\cancel{f_1(x)}f_2(x)} + \frac{\cancel{f_2(x)}f_1'(x)}{f_1(x)\cancel{f_2(x)}} = \frac{f_1'(x)}{f_1(x)} + \frac{f_2'(x)}{f_2(x)}$$

- Hipótese de indução: se

$$\frac{[f_1(x)\dots f_n(x)]'}{f_1(x)\dots f_n(x)} = \frac{f_1'(x)}{f_1(x)} + \dots + \frac{f_n'(x)}{f_n(x)}$$

então, para $n \geq 1, n \in \mathbb{N}$,

$$\frac{[f_1(x)\dots f_{n+1}(x)]'}{f_1(x)\dots f_{n+1}(x)} = \frac{f_1'(x)}{f_1(x)} + \dots + \frac{f_{n+1}'(x)}{f_{n+1}(x)}$$

- Passo de indução: considerando $g(x) = f_1(x)\dots f_n$

$$\frac{[g(x)f_{n+1}]'}{g(x)f_{n+1}} = \frac{\cancel{g(x)}f_{n+1}'(x)}{\cancel{g(x)}f_{n+1}(x)} + \frac{g'(x)\cancel{f_{n+1}(x)}}{g(x)\cancel{f_{n+1}(x)}} = \underbrace{\frac{f_1'(x)}{f_1(x)} + \dots + \frac{f_n'(x)}{f_n(x)}}_{\text{Por hipotése}} + \frac{f_{n+1}'(x)}{f_{n+1}(x)} \blacksquare$$

Exercício 12

Prosseguiremos nessa demonstração por absurdo. Assumiremos que $\sqrt{2} \in \mathbb{Q}$, portanto, $\sqrt{2} = \frac{a}{b}$, uma fração irredutível onde $a, b \in \mathbb{Z}$ e $b \neq 0$.

Lema: Todo quadrado de um número inteiro não nulo tem 1 como resto da divisão inteira por três se não for divisível por 3.

- Todo número inteiro quando dividido por três produz resto 0, 1 ou 2. Considerando que este não produza resto 0, temos:

$$\begin{cases} (3k+1)^2 = 9k^2 + 6k + 1 = 3\underbrace{(3k^2 + 2k)}_{k_2} + 1 \\ (3k+2)^2 = 9k^2 + 12k + 4 = 3\underbrace{(3k^2 + 4k + 1)}_{k_2} + 1 \end{cases}, k \in \mathbb{Z}$$

Temos que $\left(\frac{a}{b}\right)^2 = 2$, 2 não é múltiplo de 3 e portanto

$2 = 3k + 1 \implies 3k = 1 \implies k = \frac{1}{3}, k \notin \mathbb{Z}$

O que é absurdo. **Teorema:** $\sqrt{2}$ e irracional. ■

Exercício 13 [2]

$(\sqrt{2}^{1+\sqrt{2}})^{1+\sqrt{2}} = 2^{\frac{(1+\sqrt{2})^2}{2}} = \underbrace{2^{\frac{3+2\sqrt{2}}{2}}}_{\text{irracional}}$ ■

Exercício 14

a. Prova por indução finita comum

- Base de indução$(n = 2)$: 2 é primo: $2 = 2 \times 1$, então números primos existem.
- Hipótese de indução: se um número $n > 1, n \in \mathbb{N}$ é primo ou múltiplo de primos, $n - 1$ também é.
- Se $n + 1$ for primo, então não resta nada a provar. Senão, devemos concluir que existem pelo menos dois números inteiros a e b, $1 < a \leq b \leq n$ tais que $ab = n$. Por vez estes também ou são primos ou múltiplos de primos, e assim por diante. Assim, percorremos todos os valores de n à 1 e concluímos que a mesma condição se sustenta. ■

b. Prova por indução forte

- Base de indução$(n = 2)$: 2 é primo: $2 = 2 \times 1$, então números primos existem.
- Hipótese de indução: todos os números entre 1 e n ou são primos ou, senão, múltiplos de primos.
- Passo de indução: Se n for primo, então não resta nada a provar. Senão, devemos concluir que existem pelo menos dois números inteiros a e b, $1 < a \leq b \leq n$ tais que $ab = n$. Pela hipótese de indução, $a = p_1 p_2 \ldots p_n$ e $b = q_1 q_2 \ldots q_n$, sendo p e q números primos. Ora, então n também é múltiplo de números primos: $n = p_1 p_2 \ldots p_3 q_1 q_2 \ldots q_3$ ■

Exercício 15

Exemplo de desenho feito seguindo esse método para $n = 3$.

Propriedade 1: Por não ser paralela a qualquer outra reta ou interceptá-las em um ponto comum, uma reta em posição geral intercepta demais retas no plano em n pontos distintos, sendo n o número de demais retas.

Propriedade 2: Por interceptar as n retas, temos $n + 1$ subdivisões do plano em faces opostas, somadas ao número de faces anterior. Ou seja,

$$F_{n+1} = F_n + n + 1$$

1. Base de indução $(n = 0)$:

$$\frac{n^2 + n + 2}{2} = 1$$

De fato, um plano sem subdivisões tem uma única face.

2. Hipótese de indução: se o número de faces de um plano dividido por retas de maneira a gerar o maior número de subdivisões é dado por

$$F_n = \frac{n^2 + n + 2}{2}$$

Para qualquer número de retas n, então:

$$F_{n+1} = \frac{(n+1)^2(n+1) + 2}{2}$$

Passo de indução: Retomando a fórmula dada pela propriedade 2:

$$F_{n+1} = F_n + n + 1 = \frac{n^2 + n + 2}{2} + n + 1 = \frac{n^2 + n + 2 + 2n + 2}{2} =$$
$$= \frac{(n^2 + 2n + 1) + (n + 1) + 2}{2} = \frac{(n+1)^2 + (n+1) + 2}{2} \blacksquare$$

Exercício 16

- Base de indução: $0^p \equiv 0(\text{mod p})$;
- Hipótese de indução: se $n^p \equiv n(\text{mod } p)$ para qualquer $n \in \mathbb{N}$ então também $(n+1)^p \equiv (n+1)(\text{mod } p)$.
- Passo de indução: para concluirmos, faremos uso do seguinte lema (o qual será por vez demonstrado ao final desta demonstração):

$$(a+b)^p \equiv a^p + b^p(\text{mod } p), \forall a, b \in \mathbb{N}, p \in \mathbb{P}$$

Ou seja,

$$(n+1)^p \equiv n^p + 1^p(\text{mod } p) \equiv n^p + 1(\text{mod } p)$$

Pela hipótese de indução $n^p \equiv n(\text{mod } p)$, então

$$(n+1)^p \equiv n + 1(\text{mod } p) \blacksquare$$

Demonstração do lema *Freshman's Dream* (o sonho do calouro):

Para $\forall a, b \in \mathbb{N}, p \in \mathbb{P}$, tem-se:

$$(a+b)^p = a^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + \binom{p}{p-1}xy^{p-1} + y^p$$

Isolando-se os coeficientes binomiais, tem-se que cada um deles pode ser escrito na forma:

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} = p\frac{(p-1)!}{i!(p-i)!} \in \mathbb{N}$$

Como tanto $i < p$ e $(p-i) < p$, e p não é divisível senão por p, cada $\binom{p}{i}$ é um coeficiente múltiplo de p. Assim, o módulo de $(a+b)^p$ por p é tal que:

$$(a+b)^p \equiv a^p + b^p \pmod p \blacksquare$$

Exercício 17

Para analisar o tempo de processamento deste algoritmo, consideraremos a linha 1 que se repete $(n-1)$ vezes. A operação executada nessa linha, porém, não é atômica: ela toma tempo proporcional ao tamanho da entrada que varia em cada iteração. Na primeira iteração a comparação na linha 4 é feita $(n-1)$ vezes, na segunda $(n-2)$, e assim por diante. Assim, o tempo de processamento em função do tamanho n da entrada, então, é:

$$\sum_{i=1}^{n-1}(n-i) = \sum_{i=1}^{n-1} n - \sum_{i=1}^{n-1} i = n(n-1) - \frac{(n-1)[(n-1)+1]}{2}$$
$$= (n-1)\left(n - \frac{n}{2}\right) = \frac{n(n-1)}{2} = \frac{n^2-n}{2} \in \Theta(n^2) \blacksquare$$

---

1. nUSP: 12543033; Turma 04. ↩
2. $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (2^{\frac{1}{2}\cdot 2^{\frac{1}{2}}})^{2^{\frac{1}{2}}} = 2^{\frac{1}{2}\cancel{\cdot 2^{\frac{1}{2}}\cdot 2^{\frac{1}{2}}}} = 2$ ↩