

Aula 1

(1)

① Os numeros inteiros

$$\mathbb{Z} = \{ \dots -3, -2, -1, 0, 1, 2, 3, \dots \}$$

$\mathbb{Z}$ é conjunto que tem 2 operações
 $+$ (soma) e $\cdot$ (produto) ~~que~~ e
~~satisfazem~~ relação de ordem $\leq$ que

Satisfazem os seguintes axiomas.

Axiomas Sejam $x, y, z \in \mathbb{Z}$
01: $(x+y)+z = x+(y+z) \rightarrow$ associatividade da soma

02: $x+y = y+x \rightarrow$ comutatividade da soma

03: Existe elemento unico denotado por 0,
-i.e. $x+0 = 0+x = x$ para todos $x \in \mathbb{Z}$

04: Existe elemento oposto $(-x)$ para todos
 $x \in \mathbb{Z}$, t.q. $x+(-x) = (-x)+x = 0$

05: $(x \cdot y) \cdot z = x \cdot (y \cdot z) \rightarrow$ associatividade do produto

06: $x \cdot y = y \cdot x \rightarrow$ comutatividade do produto

07: Existe unico elemento neutro para produto
denotado por $1 \in \mathbb{Z}$ t.q.

$$1 \cdot x = x \cdot 1 = x$$

P8 Se $y \neq 0$ e $xy = yz \Rightarrow x = z$.

(lei de cancelamento).

P9. $x \cdot (y+z) = xy + xz \rightarrow$ distributividade
do produto em relação ao soma.

R1 $x \leq x, \forall x \in \mathbb{Z} \rightarrow$ (reflexiva)

R2. $x \leq y$ e $y \leq z \Rightarrow x \leq z$ (transitiva)

R3. $x \leq y$ e $y \leq x \Rightarrow x = y$ (anti-simetria)

R4. Temos que
 $x < y$ ou $y < x$ ou $x = y$ (tricotomia).

R5. $x \leq y \Rightarrow x + z \leq y + z$.

R6 $x \leq y \Rightarrow x \cdot z \leq y \cdot z, \forall z \geq 0$.

Princípio do Boa Ordem (PBO).

Todo subconjunto não-vazio S de $\mathbb{Z}$
de elementos não-negativos possui um
elemento mínimo, isto é elemento $x \in \mathbb{Z}$, t.q.
 $x \leq y$ para todos $y \in S$.

Propriedade 1. Não existe inteiro m tal que $0 < m < 1$. 13

Prova Suponhamos absurdo que existe tal $m \in \mathbb{Z}$. Assim o conjunto $S = \{m \in \mathbb{Z} \mid 0 < m < 1\}$ não vazio e pelo (PBO) tem elemento mínimo $x_0 \in S$.
 $x_0 \in S \Rightarrow 0 < x_0 < 1 \Rightarrow 0 < x_0^2 < x_0 < 1$
 $\Rightarrow x_0^2 \in S$ e $x_0^2 < x_0$. Contradição.

Propriedade 2. (arquitimediana).

Sejam $a, b \in \mathbb{Z}$ positivos.

Existe $n \in \mathbb{Z}$ positivo tal que $n \cdot a \geq b$.

Prova. Suponhamos que $n \cdot a < b$ para todos $n \in \mathbb{Z}$.
Então $b - n \cdot a > 0, \forall n \in \mathbb{Z}$. Logo

$S = \{b - n \cdot a \mid n \in \mathbb{Z}\}$ - não-vazio e formado pelos inteiros não-negativos.

Pelo (PBO) S tem elemento mínimo, isto é, existe $r \in S$ t.q. $b - r \cdot a$ é mínimo de S .

$b - (r+1)a = b - r \cdot a - a < b - r \cdot a$. Contradição.

Princípio da indução finita

Muito usável para os problemas tipo
"mostrar para todos n ".

Exemplos:

a) Mostre que $1+2+\dots+n = \frac{n \cdot (n+1)}{2}$, $\forall n \geq 1$

b) Mostre que $1+3+\dots+(2n-1) = n^2$, $\forall n \geq 1$

(PIF): Suponhamos que seja dada
afirmação $a(n)$ dependendo de $n \in \mathbb{N}$ t.q.

(i) $a(0)$ é verdadeiro

(ii) Para $k \in \mathbb{N}$, $a(k+1)$ é verdadeira
sempre que $a(k)$ for verdadeira.

$\Rightarrow a(n)$ é verdadeira para todos $n \in \mathbb{N}$.

Demonstração. Seja S o conjunto dos
inteiros $m \in \mathbb{N}$ tais que $a(m)$ seja falsa.

e suponhamos que S não é vazio.
Pelo (PBO) existe $x_0 \in S$ t.q. $x_0 \leq m$, $\forall m \in S$.

$a(0)$ é verdadeiro por (i) $\Rightarrow 0 \notin S$ e $x_0 \geq 1$.

Como $x_0 - 1 \notin S$ (x_0 é mínimo) $\Rightarrow a(x_0 - 1)$
é verdadeira. Agora pela (ii) segue

$a(x_0) = a((x_0 - 1) + 1)$ é verdadeira e contradiz
 $\Rightarrow S = \emptyset$ e (PIF) vale.

Obs.

(5)

- Verificar $a(0)$ é verdadeiro chama-se base de indução
- Assumir que $a(k)$ verdadeira chama-se hipótese da indução
- ... Provar $a(k)$ verdadeira $\Rightarrow a(k+1)$ verdadeiro passo de indução

Exemplos

- (1) $1+2+\dots+n = \frac{n \cdot (n+1)}{2} \quad \forall n \geq 1.$
- (2) $1+3+\dots+2n-1 = n^2, \quad \forall n \geq 1$
- (3) Mostre que $2n^3 > 3n^2+3n+1, \quad \forall n \geq 3.$

$(PBO) \Rightarrow (PIF)$

Exercício (pr casa) mostre que $(PIF) \Rightarrow (PBO)$

"tudo subconj não vazio tem mínimo" usando indução.

Aula 2 (2ª - versão).

(1)

Lembra-se:

Princípio de Boa ordem (PBO)

— Todo subconjunto S não-vazio em $\mathbb{Z}$ dos números não-negativos, possui elemento mínimo, isto é elemento $x \in S$, t.q. $x \leq y$ para todo $y \in S$.

Princípio da Indução Finita (PIF)

Suponha mos que seja dada uma afirmação $a(n)$ dependendo de $n \in \mathbb{Z}$, $n \geq 0$, t.q.

(i) $a(0)$ verdadeira.

(ii) para todo $k \in \mathbb{N}$, $a(k+1)$ é verdadeira sempre que for $a(k)$ verdadeira.

$\Rightarrow a(n)$ é verdadeira para todo $n \geq 0$

Exemplo. Considere sequência

$$a_1 = 1, a_2 = 3, a_n = a_{n-1} + a_{n-2}, \quad \forall n \geq 3.$$

Mostre que $a_n < \left(\frac{7}{4}\right)^n, \quad \forall n \geq 1.$

Base: ($n=1$) $a_1 = 1 < \frac{7}{4}$ vale.

Hipótese: Vale para todo $1 \leq k < m$
 $a_k < \left(\frac{7}{4}\right)^k$

Passo: Mostramos para m
$$a_m = a_{m-1} + a_{m-2} < \left(\frac{7}{4}\right)^{m-1} + \left(\frac{7}{4}\right)^{m-2}$$
$$= \left(\frac{7}{4}\right)^{m-2} \cdot \left(\frac{7}{4} + 1\right) = \left(\frac{7}{4}\right)^{m-2} \cdot \left(\frac{11}{4}\right)$$
$$< \left(\frac{7}{4}\right)^{m-2} \cdot \frac{49}{16} = \left(\frac{7}{4}\right)^m$$

$\Rightarrow$ Teo (PII^2) des. sempre vale.

Números Binomiais.

Def. Seja $n \in \mathbb{Z}, n \geq 0$.

Definimos

- 1) $0! = 1$
- 2) $n! = n \cdot (n-1)! \text{ para } n \geq 1$.

Logo $n! = n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1$.

Proposição Seja A conjunto com n elementos
Existem $n!$ maneiras de ordenar os elementos em A .

Exemplo $A = \{ "a", "b", "c" \}$

abc	} $6 = 3!$ maneiras.
acb	
bac	
bca	
cab	
cba	

Demonstração. (Por indução em n)

(3)

Base: (se $n=1$) Se $n=1 \Rightarrow A$ tem apenas 1 elemento. Apenas uma ordenação é possível $\Rightarrow 1=1!$

Hipótese: Se A tem k -elementos $\Rightarrow$ existem $(k+1)!$ ordenações possíveis.

Passo: Provamos para $k+1$. Seja $A = \{a_1, \dots, a_k, a_{k+1}\}$

ordenação
— — — — —
 $k+1$ lugares

Existem $k+1$ opções de colocar a_{k+1} em ordenação

Existem $k!$ opções de ordenar $\{a_1, \dots, a_k\}$ (pelo Hip.).

Assim em total temos $(k+1) \cdot k! = (k+1)!$ ordenações.

Logo pelo (FIP) há $n!$ para $A = \{a_1, \dots, a_n\}$

Def. Seja A conjunto com $n \in \mathbb{Z}$ elementos.

O número de subconjuntos de A com k elementos é denotado por $\binom{n}{k}$ e chamado coeficiente binomial.

Exemplos Seja $A = \{a_1, a_2, a_3\}$ ($n=3$) (4)

$$\binom{3}{0} = 1 \text{ pois temos somente conjunto vazio}$$

$$\binom{3}{1} = 3 \text{ pois temos } \{a_1\}, \{a_2\}, \{a_3\}$$

$$\binom{3}{2} = 3, \text{ pois temos } \{a_1, a_2\}, \{a_1, a_3\}, \{a_2, a_3\}.$$

$$\binom{3}{3} = 1 \text{ ——— } \{a_1, a_2, a_3\}.$$

Teorema $\binom{n}{k} = \frac{n!}{k!(n-k)!}, \forall n \geq 0 \text{ e } 0 \leq k \leq n.$

Demonstração Por indução em n .

Base: $n=0: \binom{0}{0} = 1 = \frac{0!}{0!0!} = 1.$

$$n=1: \binom{1}{0} = 1 = \frac{1!}{0!1!} = 1.$$

$$\binom{1}{1} = 1 = \frac{1!}{1!0!} = 1.$$

Hipótese: Vale para $n-1$ isto é $\binom{n-1}{k} = \frac{(n-1)!}{k!(n-1-k)!}$

Passo: Provamos para n . Seja $0 \leq k \leq n$

$$\binom{n}{k} = ?$$

$$\text{Se } n=k: \binom{n}{n} = 1 = \frac{n!}{n!(n-n)!} = 1.$$

Assim seja $0 \leq k \leq n-1$

Sejam r - número dos subconjuntos
de k elementos de A que
contem a_1



$$r = \binom{n-1}{k-1} \text{ e } s = \binom{n-1}{k}$$

$r+s$ = número de todos subconjuntos.

$$\binom{n}{k} = r+s = \binom{n-1}{k-1} + \binom{n-1}{k} =$$

$$\binom{n}{k} = \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-1-k)!} = \frac{(n-1)! \cdot k + (n-1)! \cdot (n-k)}{k!(n-k)!}$$

$$= \frac{(n-1)! \cdot k + (n-1)! \cdot n - (n-1)! \cdot k}{k!(n-k)!} = \frac{n!}{k!(n-k)!}$$

Assim por (PIF) $\Rightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!}, \forall n \geq 0$
 $0 \leq k \leq n.$ $\square$

Exemplo Um comitê de 3 pessoas deve ser
formado a partir de 20 pessoas.
Quantes comitês diferentes são possíveis?

Sol. Há $\binom{20}{3} = \frac{20!}{3! \cdot 17!} = \frac{20 \cdot 19 \cdot 18}{3 \cdot 2 \cdot 1} = 1140$ - comitês

Formula de Newton

(6)

$$\begin{array}{ccccccc} & & \binom{0}{0} & & & & 1 \\ & & & & & & & 1 & 1 \\ & \binom{1}{0} & \binom{1}{1} & & & & & & & \\ & \binom{2}{0} & \binom{2}{1} & \binom{2}{2} & & & & 1 & 2 & 1 \\ & \binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} & & & 1 & 3 & 3 & 1 \\ & & & \vdots & & & & 1 & 4 & 6 & 4 & 1 \\ & & & & & & & 1 & 5 & 10 & 10 & 5 & 1 \end{array}$$

Segue pois $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.

$$(x+y)^0 = 1$$

$$(x+y)^1 = x + y$$

$$(x+y)^2 = x^2 + 2xy + y^2$$

$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$$

$$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$$

$$(x+y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5$$

Teorema (Formula do Binômio de Newton).

Sejam $x, y \in \mathbb{R}$ e n inteiro positivo

$$(x+y)^n = \sum_{i=0}^n \binom{n}{i} x^i y^{n-i}$$

Demonstração Indução por n. (7)

Base: $n=0$. $(x+y)^0 = 1 = \binom{0}{0} x^0 y^0 = 1$

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

Hipótese: Vale para k isto é

$$(x+y)^k = \sum_{i=0}^k \binom{k}{i} x^i y^{k-i}$$

Passo: Provemos para $k+1$.

$$\begin{aligned}(x+y)^{k+1} &= (x+y)^k \cdot (x+y) = x \cdot (x+y)^k + y \cdot (x+y)^k \quad \underline{\text{HI}} \\&= \binom{k}{0} x^k y^0 + \binom{k}{1} x^{k-1} y^1 + \dots + \binom{k}{k-1} x^1 y^{k-1} + \binom{k}{k} x^0 y^k + \\&\quad + \binom{k}{0} y^{k+1} + \binom{k}{1} x y^k + \dots + \binom{k}{k-1} x^k y^2 + \binom{k}{k} x^k y = \\&= x^{k+1} + \left(\binom{k}{0} + \binom{k}{1} \right) x^k y + \left(\binom{k}{1} + \binom{k}{2} \right) x^{k-1} y^2 + \dots + \left(\binom{k}{k-1} + \binom{k}{k} \right) x^k y + y^{k+1} \\&= x^{k+1} + \binom{k+1}{1} x^k y + \binom{k+1}{2} x^{k-1} y^2 + \dots + \binom{k+1}{k} x y^k + y^{k+1} \\&= \sum_{i=0}^{k+1} \binom{k+1}{i} x^i y^{k+1-i}\end{aligned}$$

Pelo (PIT) $\Rightarrow$ fórmula válido.

Corolário. $\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} = 2^n$.

Dem. Tomamos $x=y=1$ em fórmula de Newton.

$$2^n = (1+1)^n = \sum_{i=0}^n \binom{n}{i} x^i y^{n-i} = \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n}.$$

Exercício Mostre que $n^3 < 2^n$, para todas $n \geq 10$ (8)

Solução

Base: $n=10$. Temos $10^3 = 1000$. Claro que $2^{10} = 1028$. $10^3 < 2^{10}$.

Hipótese $k^3 \leq 2^k$.

Passo: $(k+1)^3 \stackrel{?}{\leq} 2^{k+1}$.

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

$$3k^2 + 3k + 1 \leq 3k^2 + 3k^2 + k^2 = 7k^2 \leq k^3, \quad k \geq 10$$

Assim

$$(k+1)^3 < 2^k + k^3 < 2 \cdot 2^k = 2^{k+1}$$

Ex. 2 Mostre que $n! > 2^n$, $\forall n \geq 4$.

Solução Base $n=4$. $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$
 $2^4 = 16$. Logo $4! > 2^4$.

Hipótese Vale para $n=k$, isto é $k! = 2^k$.

$$(k+1)! = k! \cdot k > 2^k \cdot k > 2 \cdot 2^k = 2^{k+1}, \text{ se } k \geq 2.$$

Aula 3

1

Números binomiais

Def. Seja $n \in \mathbb{Z}$, $n \geq 0$.

Definimos 1) $0! = 1$

2) $n! = n \cdot (n-1)!$, para $n \geq 1$.

Logo $n! = n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1$ é chamado

número binomial

Proposição [Interpretação combinatória de $n!$]

Seja A um conjunto não-vazio com n elementos.

Assim existem $n!$ maneiras de ordenar os elementos de A .

Prova (Usando Princípio da Indução Finita).

Base: $\boxed{n=1}$

Se $|A|=1 \Rightarrow$ há apenas uma ordenação possível. Logo a afirmação vale pois $1! = 1$.

Hipótese: $\boxed{n=k}$

Suponha que há $k!$ ordenações possíveis para todo conjunto com k elementos.

Passo: $\boxed{n=k+1}$ Provamos para caso $|A|=k+1$.

Seja $A = \{a_1, a_2, \dots, a_k, a_{k+1}\}$

$(k+1)$ -elementos

Se $\underline{\hspace{1cm}} \dots \underline{\hspace{1cm}}$, assim há $(k+1)$ -lugares de colocar a_1 em ordenação: $\underline{\hspace{1cm}} \underline{\hspace{1cm}} \dots \underline{\hspace{1cm}}$

de colocar a_1 em ordenação: $\underline{\hspace{1cm}} \underline{\hspace{1cm}} \dots \underline{\hspace{1cm}}$

Além disso há $k!$ opções de ordenar o resto $\{a_2, a_3, \dots, a_{k+1}\}$. Portanto no total tem

$(k+1) \cdot k! = (k+1)!$ ordenações.

Logo pelo (PIF) a afirmação segue $\square$

Def. Seja A um conjunto com n elementos e seja $k \in \mathbb{Z}$ com $0 \leq k \leq n$. O número dos subconjuntos de A com k -elementos será denotado por $\binom{n}{k}$.

Exemplo:

$\boxed{n=2}, A=\{a_1, a_2\}$ $\binom{2}{0} = 1$, só conj. vazio $\binom{2}{1} = 2$: $\{a_1\}, \{a_2\}$ $\binom{2}{2} = 1$: $\{a_1, a_2\}$	}	$\boxed{n=3}, A=\{a_1, a_2, a_3\}$ $\binom{3}{0} = 1$, só subconj. vazio $\binom{3}{1} = 3$: $\{a_1\}, \{a_2\}, \{a_3\}$ $\binom{3}{2} = 3$: $\{a_1, a_2\}, \{a_1, a_3\}, \{a_2, a_3\}$ $\binom{3}{3} = 1$: $\{a_1, a_2, a_3\}$
--	---	---

Teorema Vale a fórmula.

$$\textcircled{*} \binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}, \quad \forall n \geq 0, 0 \leq k \leq n.$$

Prova [por indução]

Base: $\boxed{n=0}$: $\binom{0}{0} = 1 = \frac{0!}{0! \cdot 0!} = 1$

↑
pois único subconj do conj vazio é vazio

$\boxed{n=1}$: $\binom{1}{0} = 1 = \frac{1!}{0! \cdot 1!}$

subconj com 0 elementos é só vazio

$\binom{1}{1} = 1 = \frac{1!}{1! \cdot 0!}$

subconj de $\{a\}$ com 1 elemento é próprio $\{a\}$

Hipótese Vale em caso $n-1$, para todo $0 \leq k \leq n-1$

isto é $\binom{n-1}{k} = \frac{(n-1)!}{k! \cdot (n-1-k)!}$, para $0 \leq k \leq n-1$.

Passo Vamos provar para caso n . Seja $k \in \mathbb{Z}$, $0 \leq k \leq n$

Se $n=k$, assim $\binom{n}{n} = 1$ pois há único subconj.

com n -elementos em conjunto de n -elementos.

Por outro lado:

$$\binom{n}{n} = \frac{n!}{n! \cdot (n-n)!} = 1$$

Considere $A = \{a_1, \dots, a_n\}$.

Seja $0 \leq k \leq n-1$. Considere:

(4)

t = numero dos subconjuntos de k -elementos que contem a_1

s = numero dos subconjuntos de k -elementos que não contem a_1

Assim: $t = \binom{n-1}{k-1}$ e $s = \binom{n-1}{k}$

Por outro lado $t + s$ = numero de todos subconj.

Com k -elementos em A

$$\Rightarrow \binom{n}{k} = t + s = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Usando hipotese temos:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(k-1)!(n-1-k+1)!} + \frac{(n-1)!}{k!(n-1-k)!} =$$

$$\frac{(n-1)! \cdot k + (n-k) \cdot (n-1)!}{k! \cdot (n-k)!} = \frac{(n-1)! \cdot (k+n-k)}{k! \cdot (n-k)!} = \frac{n!}{k! \cdot (n-k)!}$$

Usando (PIF) $\Rightarrow$

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} \text{ para todo } n \geq 0 \text{ e } 0 \leq k \leq n.$$

Exemplo:

$$a) \binom{3}{1} = \frac{3!}{1! \cdot (3-1)!} = \frac{3!}{2!} = \frac{1 \cdot 2 \cdot 3}{1 \cdot 2} = 3$$

$$b) \binom{7}{4} = \frac{7!}{4! \cdot (7-4)!} = \frac{7!}{4! \cdot 3!} = \frac{5 \cdot 6 \cdot 7}{1 \cdot 2 \cdot 3} = 35 //$$

Exercício Um comitê de 3 pessoas deve ser formado a partir de 20 candidatos. Quantos comitês diferentes são possíveis — ?

Solução há $\binom{20}{3} = \frac{20 \cdot 19 \cdot 18}{3 \cdot 2 \cdot 1} = 1140$

Comitês diferentes

Formula de Newton

Considere

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} \\ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ \begin{pmatrix} 2 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 2 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 2 \\ 2 \end{pmatrix} \\ \begin{pmatrix} 3 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 3 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 3 \\ 2 \end{pmatrix} \quad \begin{pmatrix} 3 \\ 3 \end{pmatrix} \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots$$

Aplicando (*) temos [ou aplicando $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$]

$C + X = C \binom{1}{1} + 1 \times \binom{1}{0} + 1 = (C+X)$

Triângulo de Pascal

$$\begin{array}{ccccccc} & & & & 1 & & \\ & & & 1 & & 2 & & 1 \\ & & 1 & & 3 & & 3 & & 1 \\ & 1 & & 4 & & 6 & & 4 & & 1 \\ & & & & & & & & & & \end{array}$$

Por outro lado considere:

$$\sum_{k=0}^{n-1} C \cdot X \cdot \binom{n-1}{k} = C \cdot X \cdot \sum_{k=0}^{n-1} \binom{n-1}{k} = C \cdot X \cdot (C+X)$$

$$\begin{aligned}
 (x+y)^0 &= 1 \\
 (x+y)^1 &= x + y \\
 (x+y)^2 &= x^2 + 2xy + y^2 \\
 (x+y)^3 &= x^3 + 3x^2y + 3xy^2 + y^3 \\
 (x+y)^4 &= x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4 \\
 (x+y)^5 &= x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5 \\
 &\vdots
 \end{aligned}$$

Teorema [Formula Binomial de Newton]

Sejam $x, y \in \mathbb{R}$ (números reais) e n - inteiro não-negativo.

Então: $(x+y)^n = \sum_{i=0}^n \binom{n}{i} x^i \cdot y^{n-i}$ **

Prova [Indução por n]

Base: $n=0$ $(x+y)^0 = 1 = \binom{0}{0} \cdot x^0 \cdot y^0 = 1$

$n=1$ $(x+y)^1 = \binom{1}{0}x + \binom{1}{1}y = x+y$

Hipótese: $n=k$ Suponha que

$$(x+y)^k = \sum_{i=0}^k \binom{k}{i} \cdot x^i \cdot y^{k-i}$$

Passo: Provarmos para: $n=k+1$, isto é

$$(x+y)^{k+1} = \sum_{i=0}^{k+1} \binom{k+1}{i} \cdot x^i \cdot y^{k+1-i} //$$

Temos:

(7)

$$(x+y)^{k+1} = (x+y)^k \cdot (x+y) = x \cdot (x+y)^k + y(x+y)^k =$$

$$\underline{\text{hipótese}} \quad \binom{k}{0} x y^k + \binom{k}{1} x^2 y^{k-1} + \dots + \binom{k}{k-1} x^k y + \binom{k}{k} x^{k+1} +$$

$$+ \binom{k}{0} y^{k+1} + \binom{k}{1} x y^k + \binom{k}{2} x^2 y^{k-1} + \dots + \binom{k}{k} x^k y =$$

$$= x^{k+1} + \left[\binom{k}{0} + \binom{k}{1} \right] x y^k + \left[\binom{k}{1} + \binom{k}{2} \right] x^2 y^{k-1} + \dots +$$

$$+ \left[\binom{k}{k-1} + \binom{k}{k} \right] x^k y + y^{k+1} \quad \underline{\text{Relações}}$$

$$= \binom{k+1}{0} y^{k+1} + \binom{k+1}{1} x y^k + \binom{k+1}{2} x^2 y^{k-1} + \dots + \binom{k+1}{k} x^k y + \binom{k+1}{k+1} x^{k+1}$$

$$= \sum_{i=0}^{k+1} \binom{k+1}{i} x^i \cdot y^{k+1-i}$$

Pelo (PIF) $\textcircled{**}$ vale.

Corolário: $\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} = 2^n$

Prova: Sejam $x=y=1$ em $\textcircled{**}$, assim

$$2^n = (1+1)^n = \sum_{i=0}^n \binom{n}{i} \underset{1}{x^i} \underset{1}{y^{n-i}} = \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n}.$$

Álgebra

Revisão

① Axiomática dos inteiros

$\mathbb{Z}$ um conjunto dos inteiros que tem duas operações: soma e produto que satisfazem as seguintes axiomas:

$$1) (a+b)+c = a+(b+c),$$

$$2) \exists 0 \in \mathbb{Z}, \text{ t.q. } a+0=0+a=a,$$

$$3) \exists -a \in \mathbb{Z}, \text{ t.q. } a+(-a)=0$$

$$4) a+b=b+a$$

$$5) (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

$$6) \exists 1 \in \mathbb{Z}, \text{ t.q. } a \cdot 1 = 1 \cdot a = a.$$

$$7) \cancel{a} \cdot y = \cancel{z} \cdot y \Rightarrow a=z, y \neq 0$$

$$8) a \cdot b = b \cdot a$$

$$9) a(b+c) = ab+ac.$$

Exercício 1. Mostre as seguintes consequências dos axiomas:

$$a) a+b=a+c \Rightarrow b=c, \forall a, b, c \in \mathbb{Z}.$$

$$b) a \cdot 0 = 0, \forall a \in \mathbb{Z}, \quad c) a \cdot b = 0 \Rightarrow a=0 \text{ ou } b=0$$

$$d) -(-a)=a, \quad e)$$

Solução

$$\begin{aligned} a+b &= (a+b)+0 = (a+b)+(\cancel{b}+(-\cancel{b})) \\ &\stackrel{\Delta \times 2}{=} \cancel{a} + (\cancel{b} + (-\cancel{b})) \\ &\stackrel{\Delta \times 3}{=} \cancel{a} + \cancel{b} + (-\cancel{b}) \\ &= a+b = a+c \Rightarrow \\ (a+b)+(-a) &= (a+c)+(-a) \\ (a+(-a))+b &= (a+(-a))+c \\ 0+b &= 0+c \\ b &= c \end{aligned}$$

b) Temos que $0 + b = b \quad \forall b \in \mathbb{Z}$

(2)³

Assim $0 + 1 = 1 \Rightarrow a \cdot (0 + 1) = a \cdot 1$

$$\Rightarrow a \cdot 0 + a \cdot 1 = a \cdot 1 \Rightarrow a \cdot 1 = a$$

Prop. 9 Prop. 6

$$\Rightarrow a \cdot 0 + (a + (-a)) = a + (-a), \quad a + (-a) = 0, \quad \forall a \in \mathbb{Z}$$

Prop. 3

$$\Rightarrow a \cdot 0 = 0$$

c) $a \cdot b = 0$

Suponha que $b \neq 0$. Assim escrevemos

$$a \cdot b = 0 \text{ como } a \cdot b = 0 \cdot b \Rightarrow a = 0$$

Prop. 8

Suponhamos que $a \neq 0$. Assim escrevemos

$$a \cdot b = 0 \text{ como } a \cdot b = a \cdot 0 \Rightarrow b \cdot a = 0 \cdot a \Rightarrow b = 0$$

d) $a + (-a) = 0$ também $(-a) + (-(-a)) = 0$

Prop. 3 Prop. 3

Assim $a + (-a) = (-a) + (-(-a))$ ou

$$(a + (-a)) + a = ((-a) + (-(-a))) + a$$

$$\boxed{a = (-(-a))} //$$

Princípios

Princípio de Boa Ordem

Todo subconjunto não-vazio S em $\mathbb{Z}$ dos não-negativos tem elemento mínimo.

Princípio da Indução Finita

Suponha-se que seja dada uma afirmação $a(n)$ dependendo do $n \in \mathbb{N}^0$ t.q.

(i) $a(0)$ é verdadeira

(ii) $a(k)$ é verdadeiro $\Rightarrow a(k+1)$ é verdadeiro

Assim $a(n)$ é sempre verdadeiro.

$(\text{PBO}) \Rightarrow (\text{PIF})$ — mostramos na 2ª aula.

$(\text{PIF}) \stackrel{?}{\Rightarrow} (\text{PBO})$ — trabalho p/ casa

Exercício 2 $(\text{PIF}) \Rightarrow (\text{PBO})$ é equivalente

mostrar que todo conjunto não-vazio dos números inteiros não-negativos tem elemento mínimo, usando indução.

Solução Seja $a(n)$ — afirmação: "todo conjunto com n -elementos tem elemento mínimo".

Base $a(1)$: — $S = \{x_0\}$. Claro que x_0 é mínimo em S .

Hip: $a(k)$: — $S = \{x_1, \dots, x_k\}$, $x_1, \dots, x_k \in \mathbb{N}$ tem elemento mínimo.

Passo: $a(k+1)$ — $S = \{x_1, \dots, x_k, x_{k+1}\} = \{x_1, \dots, x_k\} \cup \{x_{k+1}\}$

Seja x_0 é mínimo em $\{x_1, \dots, x_k\}$. Se

$x_0 < x_{k+1} \Rightarrow x_0$ é mínimo em S

$x_0 > x_{k+1} \Rightarrow x_{k+1}$ é mínimo em S .

No qualque caso S tem elemento minimo.
Assim pelo (PIF) $a(n)$ é verdadeira ou seja
(pfo) é verdadeira //

Exercício 3 (Lista 1).

Mostre que não há inteiros entre 4 e 5.

Solução Considere o conjunto $S = \{x-4 \mid x \in \mathbb{Z}, 4 \leq x \leq 5\}$.

Suponhamos que S não é vazio.

Assim existe elemento $m \in S$ t.q. $m \leq y, \forall y \in S$

Todos elementos de S são entre 0 e 1 assim
 $0 < m^2 < 1$, m^2 é inteiro assim $0 < m^2 + 4 < 5 \Rightarrow m^2 \in S$

ou Contradição //

(3) Princípio do Indução finita.

Exercício 4 Mostre que $n^3 \leq 2^n$ para todos $n \geq 10$.

Solução Base: $n=10$. Temos $10^3 = 1000$
 $2^{10} = 1028$

Claro que $10^3 < 2^{10}$

Hipótese $k^3 \leq 2^k$

Passo $(k+1)^3 \leq 2^{k+1}$

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

$$3k^2 + 3k + 1 \leq 3k^2 + 3k^2 + k^2 = 7k^2 < k^3, \text{ se } k \geq 10$$

$$\text{Assim } k^3 + k^3 \leq 2^k + 2^k = 2 \cdot 2^k = 2^{k+1} //$$

Exercício 5

(5)

Mostre que

$$-1^2 + 2^2 - 3^2 + 4^2 - \dots - (-1)^n \cdot n^2 = (-1)^n \cdot \frac{n(n+1)}{2}, \quad n \geq 1 (*)$$

Solução Quando $n=1$.

Base: $n=1$. $(-1) \cdot 1^2 = (-1) \cdot \frac{1 \cdot (1+1)}{2}$ ou
 $-1 = -1$ - vale

Hipótese Seja $k \in \mathbb{Z}$ é dado e (*) é válido para $n=k$.

$$-1^2 + 2^2 - 3^2 + 4^2 - \dots - (-1)^k \cdot k^2 = (-1)^k \cdot \frac{k(k+1)}{2}.$$

Passo:

$$\begin{aligned} & \underbrace{-1^2 + 2^2 - 3^2 + 4^2 - \dots + (-1)^k \cdot k^2}_{= (-1)^k \cdot \frac{k(k+1)}{2}} + (-1)^{k+1} \cdot k^2 = \\ & = (-1)^k \cdot \frac{k(k+1)}{2} + (-1)^{k+1} \cdot k^2 = (-1)^{k+1} \left((k+1) \left(\frac{k}{2} - k \right) \right) = \\ & = (-1)^{k+1} \cdot (k+1) \left(\frac{2k+2-k}{2} \right) = (-1)^{k+1} \cdot \frac{(k+1)(k+2)}{2}. \end{aligned}$$

Fez (PIF) (*) é válido.

Exercício 6 Busca a fórmula da expressão.

$$\prod_{i=2}^n \left(1 - \frac{1}{i^2}\right) = \left(1 - \frac{1}{4}\right) \left(1 - \frac{1}{9}\right) \left(1 - \frac{1}{16}\right) \dots \left(1 - \frac{1}{n^2}\right)$$

Vamos calcular para n pequenos

$$n=2 \quad \left(1 - \frac{1}{4}\right) = \frac{3}{4}, \quad n=3 \quad \left(1 - \frac{1}{4}\right) \left(1 - \frac{1}{9}\right) = \frac{3}{4} \cdot \frac{8}{9} = \frac{2}{3}$$

$$n=4: \left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{8}\right)\left(1 - \frac{1}{16}\right) \cdot \frac{2}{3} \cdot \frac{15}{16} = \frac{5}{8}$$

$$n=5: \left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{8}\right)\left(1 - \frac{1}{16}\right)\left(1 - \frac{1}{32}\right) \cdot \frac{5}{8} \cdot \frac{21}{32} = \frac{7}{8}$$

Assim

n	2	3	4	5
valor	$3/4$	$2/3$	$5/8$	$7/8$

n	2	3	4	5
valor	$3/4$	$4/6$	$5/8$	$6/10$

Hip: $\prod_{i=2}^n \left(1 - \frac{1}{i}\right) = \frac{n+1}{2n}$

Mostremos pelo (PIP).

Baze: já mostrado

Hip: Vale para $n=k$, isto é $\prod_{i=2}^k \left(1 - \frac{1}{i}\right) = \frac{k+1}{2k}$

Passo: $\prod_{i=2}^{k+1} \left(1 - \frac{1}{i}\right) = \prod_{i=2}^k \left(1 - \frac{1}{i}\right) \cdot \left(1 - \frac{1}{k+1}\right) = \frac{k+1}{2k} \cdot \left(\frac{(k+1)^2 - 1}{(k+1)^2}\right) =$

$$= \frac{k^2 + 2k + 1 - 1}{2k \cdot (k+1)} = \frac{k+2}{2(k+1)}$$

Pelo (PIP) fórmula vale para todos n .

Exercício 7 Seja Li a sequência dos números Fibonacci.

Mostre que $\sum_{i=1}^n Li^2 = Li \cdot L_{n+1}$.

Solução

Base: $n=1$. $1 \neq \sum_{i=1}^1 f_i^2 = 1$. $f_1 \cdot f_2 = 1$.

Hipótese vale para $n=k$, isto é $\sum_{i=1}^k f_i^2 = f_k \cdot f_{k+1}$

Passo

$$\sum_{i=1}^{k+1} f_i^2 = \sum_{i=1}^k f_i^2 + f_{k+1}^2 = f_k \cdot f_{k+1} + f_{k+1}^2 = f_{k+1} (f_k + f_{k+1}) = f_{k+1} \cdot f_{k+2}.$$

Pelo (PIF) fórmula vale para todos n .

Exercício 8. Mostre que $n! > 2^n$, $\forall n \geq 4$.

Solução Base $n=4$. $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$

$$2^4 = 16$$

$$\text{Logo } 4! > 2^4.$$

Hipótese Vale para $n=k$, isto é $k! > 2^k$.

Passo: $(k+1)! = k! \cdot k > 2^k \cdot k > 2 \cdot 2^k = 2^{k+1}$, se $k > 2$.

Exercício 9 Quantas diagonais tem um polígono convexo.

Solução



Vimos os casos mais fácil.

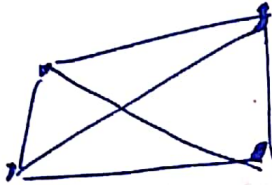
✓

$$n=3$$



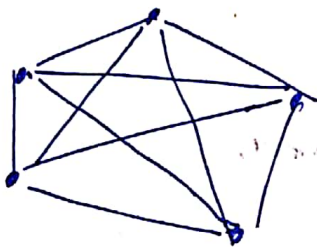
0 - diagonais

$$n=4$$



2 - diagonais

$$n=5$$



5 - diagonais

Cada diagonal é um par de pontos
que não ficam no mesmo lado

Assim N° dos diagonais = $\frac{\text{N}^{\circ} \text{ de pares dos pontos diferentes}}{\text{N}^{\circ} \text{ dos lados}}$

$$N^{\circ} \text{ dos lados} = n$$

$$N^{\circ} \text{ dos pares dos pontos diff} = \frac{\text{N}^{\circ} \text{ de maneiras de porm 2 vertices em pteiz de } n}{1} = \binom{n}{2}$$

$$\binom{n}{2} - n = \frac{n!}{2!(n-2)!} - n = \frac{(n-2)!(n-1) \cdot n}{2! \cdot (n-2)!} - n =$$

$$= n \left(\frac{n-1}{2} - 1 \right) = \frac{n \cdot (n-3)}{2}$$

$$\text{Por exemplo } n=5 \Rightarrow \frac{5 \cdot (5-3)}{2} = 5 \text{ - diagonais.}$$

Aula 5

Divisibilidade (continuação)

⑦ Lembra-se

a) Sejam $a, b \in \mathbb{Z}$. Dizemos que

$a \xrightarrow{\text{divide}} b$ ou

b é múltiplo de a ou

a é divisor de b se existir $c \in \mathbb{Z}$, t.q. $b = a \cdot c$.

b) Notação: $a \mid b$ se a divide b
 $a \nmid b$ se a não-divide b .

c) Algoritmo de divisão

Sejam $a, b \in \mathbb{Z}$, com $b > 0$. Existem:

$q \in \mathbb{Z}$, quociente e

$r \in \mathbb{Z}$, o resto de divisão de a por b , t.q.

$$a = b \cdot q + r, \text{ com } 0 \leq r < b.$$

⑧ Observação sobre Algoritmo de divisão:

q e r do Teorema (Algoritmo) são únicos(!):

Demonstração Se $a = b \cdot q_1 + r_1$ e $a = b \cdot q_2 + r_2$ assim

$$r_1 = a - b q_1 \text{ e } r_2 = a - b q_2 \text{ ou}$$

$$\Rightarrow r_1 - r_2 = a - b q_1 - a + b q_2$$

$$\Rightarrow r_1 - r_2 = b(q_2 - q_1) \text{ assim } b \mid (r_1 - r_2).$$

Lembra-se Se $a \mid b$, $b \neq 0 \Rightarrow |a| \leq |b|$.

Logo $b | z_1 - z_2$ e $|b| \leq |z_1 - z_2|$.

Por outro lado $\begin{cases} 0 \leq z_1 < b \\ 0 \leq z_2 < b \end{cases}$ ou $\begin{cases} 0 \leq z_1 < b \\ b \leq -z_2 \leq 0 \end{cases}$

$$-b \leq z_1 - z_2 \leq b \Rightarrow |z_1 - z_2| \leq b$$

Assim $z_1 - z_2 = 0 \Rightarrow z_1 = z_2$.

Logo $a - bq_1 = a - bq_2 \Rightarrow bq_1 = bq_2 \Rightarrow q_1 = q_2$. $\square$

Exemplo Mostre que dados 3 inteiros consecutivos um deles é múltiplo de 3.

Solução Seja $a, a+1, a+2 \in \mathbb{Z}$, para a .

Temos 3 possibilidades (pelo A.I. de Div.).

1) $a = 3k \rightarrow a$ é múltiplo de 3 (aqui $a+1$ e $a+2$ não)

2) $a = 3k+1 \rightarrow a+2 = 3k+3$ é múltiplo de 3

3) $a = 3k+2 \rightarrow a+1 = 3k+3$ é múltiplo de 3.

Exemplo 2, Mostre que $3 | n^3 - n$, para $\forall n \in \mathbb{Z}$.

Solução Escrevemos $n^3 - n = n \cdot (n^2 - 1) = (n-1) \cdot n \cdot (n+1)$.

Assim $n^3 - n$ é o produto dos 3 inteiros positivos.

ou seja é múltiplo de 3. //

② Máximo divisor Comum!

Def. Sejam $a, b \in \mathbb{Z}$. Dizemos que um inteiro c é divisor comum de a e b se $c | a$ e $c | b$.

Def. Sejam $a, b \in \mathbb{Z}$. Um inteiro (positivo) d é chamado máximo divisor comum se:

- i) $d|a$ e $d|b$.
- ii) se $c \in \mathbb{Z}$ é t.q. $c|a$ e $c|b$, então $c|d$.

Perguntas naturais:

- Máximo divisor comum existe?
- — // — // —, é único?

Lema. Sejam $a, b \in \mathbb{Z}$. Se d e d' são máximos divisores comuns de a e b assim, $d = d'$.

Demonstração d é divisor comum de a e $b \Rightarrow$

$$d|d' \xRightarrow{d' \neq 0} |d| \leq |d'|$$

$$d' \text{ satisfaz (ii)} \Rightarrow d'|d \xRightarrow{d \neq 0} \begin{cases} |d| \leq |d'| \\ |d'| \leq |d| \end{cases} \Rightarrow |d| = |d'| \Rightarrow d = d'. \quad \square$$

Obs. Pelo lema anterior, se existir o máximo div. comum de a e b , ele é único. Denotaremos esse número por $\text{mdc}(a, b)$.

Teorema (de Bézout). Sejam $a, b \in \mathbb{Z}$, $a \neq 0$ e $b \neq 0$. Então existem $x, s \in \mathbb{Z}$ t.q.

$$\text{mdc}(a, b) = ax + bs \quad (\text{logo mdc existe})$$

Demonstração Considere $S = \{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\}$.

S é não vazio pois se $x=a, y=b$, assim

$$a \cdot a + b \cdot b = a^2 + b^2 > 0$$

Além disso S é formado pelos inteiros positivos

Pelo (PBO), $\exists d \in S$ elemento mínimo.

Vamos mostrar que $\text{mdc}(a, b) = d$.

Pelo Algo da divisão $a = dq + r$, com $0 \leq r < d$

Se $r > 0$. Assim $r_1 = a - dq = a - (ar + bs) \cdot q =$

$$= a - arq - bsq = a(1 - rq) + b(-sq) \in S$$

Mas $r_1 < d$. Contradição. Logo $r_1 = 0$ e $d | a$.

Analogamente $d | b$.

Assim d cumpre i).

Seja $c | a$ e $c | b$. Vimos que $c | ar + bs$. Logo $c | d$.

— $\therefore d$ cumpre ii). $\square$.

③ Divisores

Def. Seja $a \in \mathbb{Z}$ não nulo e defina

$$\text{Div}(a) = \{c \in \mathbb{Z} \mid c | a\}.$$

Observe que $\text{Div}(a)$ é um conjunto finito pois $c | a \Rightarrow |c| \leq |a|$ $a \neq 0$

$$\text{Logo } \text{Div}(a) \subseteq \{-|a|, -|a|+1, \dots, |a|-1, |a|\}.$$

Dados a, b não nulos em $\mathbb{Z}$, define

$$\text{Div}(a, b) = \text{Div}(a) \cap \text{Div}(b).$$

$$\text{Logo } \mathcal{D}(a,b) = \mathcal{D}(a) \cap \mathcal{D}(b) = \{c \in \mathbb{Z} \mid c|a \text{ e } c|b\}$$

Conjunto de divisores comuns de a e b .

Proposição Sejam $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$.

$$\text{Então } \text{mdc}(a,b) = \max \mathcal{D}(a,b).$$

Demonstração Observe inicialmente que

$$\mathcal{D}(a,b) \neq \emptyset, \text{ pois } 1 \in \mathcal{D}(a) \text{ e } 1 \in \mathcal{D}(b).$$

$$\text{Sejam } d = \text{mdc}(a,b), d' = \max \mathcal{D}(a,b).$$

$$d = \text{mdc}(a,b) \xrightarrow{(i)} d|a \text{ e } d|b \Rightarrow d \in \mathcal{D}(a,b) \Rightarrow d \leq d'.$$

Por outro lado como $d' \in \mathcal{D}(a,b)$ temos $d'|a$ e $d'|b$.

Como $d = \text{mdc}(a,b)$, por ii) devemos ter $d'|d$.

Como $d \neq 0$ isso implica $|d'| \leq |d|$.

Mas ambos são > 0 . Logo $d' \leq d$.

Portanto: $d = d'$. $\square$.

Exemplo Calcular $\text{mdc}(30,36)$.

$$\text{Solução } \mathcal{D}(30) = \{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30\}$$

$$\mathcal{D}(36) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 9, \pm 12, \pm 18, \pm 36\}$$

$$\mathcal{D}(30,36) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$$

$$\text{Logo } \text{mdc}(30,36) = \max \mathcal{D}(30,36) = 6.$$

④ 1º algoritmo do Euclides

(5)

Lema Sejam a e b inteiros positivos. Seja z o resto de divisão de a por b . Então

$$\text{mdc}(a, b) = \text{mdc}(b, z).$$

Demonstração Mostremos que $\mathcal{D}(a, b) = \mathcal{D}(b, z)$

Escreva $a = bq + z$, com $q, z \in \mathbb{Z}$, $0 \leq z < b$.

Logo, $z = a - bq$.

Seja $c \in \mathcal{D}(a, b)$. Assim $c|a$ e $c|b$. Portanto $c|a - bq$.

Logo $c|z$. Assim $c \in \mathcal{D}(b, z)$. $\mathcal{D}(a, b) \subset \mathcal{D}(b, z)$

Por outro lado, se $c \in \mathcal{D}(b, z)$ então $c|b$ e $c|z$

Portanto $c|\underbrace{bq + z}_a$, logo $c \in \mathcal{D}(a, b)$ e $\mathcal{D}(b, z) \subset \mathcal{D}(a, b)$

$$\mathcal{D}(a, b) = \mathcal{D}(b, z).$$

$$\text{mdc}(a, b) = \max \mathcal{D}(a, b) = \max \mathcal{D}(b, z) = \text{mdc}(b, z)$$

1º algoritmo Aplicar o lema sucessivas até obter resto 0 (zero).

Exemplo

i) Calcule $\text{mdc}(30, 36)$

$$30 = 0 \cdot 36 + 30, \text{ isto é}$$

$$\text{mdc}(30, 36) = \text{mdc}(36, 30) = \text{mdc}(30, 6) = \text{mdc}(6, 0) = 6$$

$$36 = 1 \cdot 30 + 6$$

$$30 = 5 \cdot 6 + 0$$

$$\text{Logo } \text{mdc}(30, 36) = 6$$

b) Calcule $\text{mdc}(1128, 336) = ?$

$$\begin{array}{r} 1128 \\ 1008 \\ \hline 120 \end{array} \quad \begin{array}{r} 336 \\ 3 \\ \hline 120 \end{array}$$

$$\begin{aligned} \text{mdc}(1128, 336) &= \text{mdc}(336, 120) = \\ &= \text{mdc}(120, 96) = \text{mdc}(96, 24) = \\ &= \text{mdc}(24, 0) = 24. \end{aligned}$$

c) Calcule $\text{mdc}(42823, 6409) = \text{mdc}(6409, 4369) =$

$$\begin{aligned} &= \text{mdc}(4369, 2040) = \text{mdc}(2040, 289) \\ &= \text{mdc}(289, 17) = \text{mdc}(17, 0) = 17. \end{aligned}$$

$$\begin{array}{r} 42823 \\ 38454 \\ \hline 4369 \end{array} \quad \begin{array}{r} 6409 \\ 6 \\ \hline 6409 \\ 4369 \\ \hline 2040 \end{array}$$

Efficiencia do Algoritmo

$$\text{mdc}(159037, 92263)$$

A) Método dos divisores. Testamos divisores ímpares.
Depois de 127 divisões encontramos 257 e
 $92263 = 257 \times 359$ é divisor de 159037.

Ex 128 divisões.

B) Mostre em caso que precisamos 10 divisões só pelo Algoritmo de Euclides.

(7)

Teorema (de Lame, 1844)

O número das divisões em aplicação do Algoritmo de Euclides ≤ 5 vezes número de dígitos em menor número.

Por exemplo

O número de divisões para buscar

$\text{mcd}(117035, 35688479)$

será $\leq 5 \cdot 6 = 30$.
