TEMA 3: Teoria Elemental de Números

Divisibilidade em Z. Algoritmo de Euclides, básico e extendido. Números primos. Teorema fundamental da aritmética. Princípio de induçom. Equaçons diofânticas. Congruências: teorema chinês dos restos, critérios de divisibilidade, sistemas de numeraçom.

➢ Divisibilidade em Z e Algoritmo de Euclides

- **Teorema da divisom**

$$\boxed{\text{Dados } a,\ b \in N,\ b\neq 0,\ \exists^{o}\ q,\ r \in Z \ /\ a=b\cdot q+r \quad 0\leq r<b}$$

dem.

1º) existência por induçom em $a \in N$

- base: $\underline{0}$ para $a=0$, $a=b\cdot 0+0$ $0\leq 0<b$ queda demostrado.
- hipótese: $\underline{n}$ para $n<a$, supomos certo o enunciado.
- paso: $\underline{a}$ para a, hai dous casos possíveis:

▪se $\underline{a<b} \Rightarrow a=0\cdot b+a$ $0\leq a<b$ queda demostrado.

▪se $\underline{a\geq b} \Rightarrow \left.\begin{array}{l} 0\leq a-b<a \\ \underbrace{a-b=q\cdot b+r \quad 0\leq r<b}_{\text{hipótese induçom}} \end{array}\right\} \Rightarrow a=(q+1)\cdot b+r$ $0\leq r<b$ queda demostrado.

(porque $a-b<a$)

2º) unicidade por reducçom ao absurdo

Dados $a,\ b \in N,\ b\neq 0,\ \exists \begin{cases} q,\ r \in Z \ /\ a=b\cdot q+r \quad 0\leq r<b \\ q',\ r' \in Z \ /\ a=b\cdot q'+r' \quad 0\leq r'<b \end{cases}$

Hai dous casos:

▪se $\underline{q<q'} \Rightarrow (q-q')\cdot b+(r-r')=0 \Leftrightarrow (q'-q)\cdot b=r-r'$

$0\leq r-r'<b$ $\qquad q'-q\geq 1$ (por hipótese $q<q'$)

contradicçom $\Rightarrow q\geq q'$

▪se $\underline{q'<q} \Rightarrow (q'-q)\cdot b+(r'-r)=0 \Leftrightarrow (q-q')\cdot b=r'-r$

$0\leq r'-r<b$ $\qquad q-q'\geq 1$ (por hipótese $q'<q$)

contradicçom $\Rightarrow q'\geq q$

entom $q=q' \Rightarrow (q'-q)\cdot b+(r'-r)=0 \Rightarrow 0\cdot b+(r'-r)=0 \Rightarrow r'=r$

O teorema da divisom geraliza-se para números enteiros:

$$\boxed{\text{Dados } a,\ b \in Z,\ b\neq 0,\ \exists^{o}\ q,\ r \in Z \ /\ a=b\cdot q+r \quad 0\leq r<|b|}$$

Def.- Dados a, b $\in$ Z, b$\neq$0, a é <u>múltiplo</u> de b se $\exists$ q $\in$ Z / a=q·b (r=0).

Def.- d é o máximo comum divisor (M.C.D.) de a e de b, d=MCD(a,b) se:
1º) d|a e d|b (d é "divisor comum")
2º) se d'|a e d'|b $\Rightarrow$ d'|d (d é "máximo divisor")

- **Teorema**

O máximo comum divisor é único.

dem. (por reducçom ao absurdo)

$$\left.\begin{array}{l} d'=mcd(a,b) \Rightarrow d|a \text{ e } d|b \Rightarrow d|d' \\ d=mcd(a,b) \Rightarrow d'|a \text{ e } d'|b \Rightarrow d'|d \end{array}\right\} \Rightarrow d=d'$$

- **Teorema de Bezout**

$$\boxed{\text{Dados } a, b \in N, \exists\ MCD(a,b) \text{ e é } \alpha a+\beta b;\ \alpha, \beta \in Z}$$

Consideramos $\left\{\begin{array}{l} S = \{xa+yb/x,y\in Z\} \\ d = \text{menor enteiro positivo} \in S \end{array}\right\}$

$$S \overset{?}{=} \{\lambda d/\lambda\in Z\}$$

1º)

"$\supset$"

$\lambda d=\lambda(\alpha a+\beta b)=\lambda\alpha a+\lambda\beta b \in S$

$d\in S$

"$\subset$"

$s\in S \Rightarrow s=xa+yb;\ s=q\cdot d+r;\ 0\leq r<d$

$r=s-q\cdot d=xa+yb-q(\alpha a+\beta b)=(x-q\alpha)a+(y-q\beta)b \in S \Rightarrow$

$\Rightarrow r=0 \Rightarrow s=q\cdot d$

$\uparrow$

$r\in S;\ r<d$

2º)

$$d \overset{?}{=} MCD(a,b)$$

$$\left.\begin{array}{l} a\in S \Rightarrow d|a\ (a=1\cdot a+0\cdot b) \\ \quad\uparrow \\ \quad S=\{\text{múltiplos de } d\} \\ \quad\downarrow \\ b\in S \Rightarrow d|b\ (b=0\cdot a+1\cdot b) \end{array}\right\} \text{ se } d'|a \text{ e } d'|b \Rightarrow d'|d$$

Algoritmo de Euclides

Dados n_1, $n_2 \in N$, $n_2\neq 0$

$n_1=n_2q_2+n_3 \quad 0\leq n_3<n_2$

$n_2=n_3q_3+n_4 \quad 0\leq n_4<n_3$

...

$MCD(n_1,n_2)$ = derradeiro resto nom nulo

(despexando os restos desde o derradeiro ao primeiro).

- **Teorema**

Se $p|a\cdot b$ e p é primo $\Rightarrow$ $p|a$ ou $p|b$

dem.

Suponhamos p a (nom divide) $\Rightarrow$ $MCD(p,a)=1=\alpha a+\beta p$ $\Leftrightarrow$ $b=\alpha ab+\beta pb$ $\Leftrightarrow$ $b=\alpha\lambda p+\beta pb=p(\alpha\lambda+\beta b)$ $\Rightarrow$ $p|b$ (suponhemos p b $\Rightarrow$ $p|a$)

- **Teorema**

Se a, b som primos entre si: $a|m$ e $b|m \Rightarrow a\cdot b|m$

dem.

$MCD(a,b)=1=\alpha a+\beta b$ $\Leftrightarrow$ $m=m\alpha a+m\beta b$ $\Leftrightarrow$ $m=b\mu\alpha a+\lambda a\beta b$ $\Leftrightarrow$ $m=(\mu\alpha+\lambda\beta)ab$ $\Leftrightarrow$ $m|ab$

➢ Números primos

➢ Princípio de induçom

Princípio de Induçom Finita

Seja P(n) umha proposiçom sobre enteiros positivos (N):

1º) Comprova-se para o primeiro enteiro positivo, P(1).
2º) Sendo $n \geq 1$, supom-se certo para P(n).
3º) Demostra-se para P(n+1).

Entom cumpre-se para todos os enteiros positivos.

Umha variaçom possível é que a propriedade se dé dum enteiro positivo k em adiante, sendo esse enteiro $k > 1$. Este câmbio nom afecta à validez do razonamento e porém o procedimento segue sendo o mesmo:

1º) Comprova-se P(k) certo.
2º) Sendo $n \geq k$, supom-se certo para P(n).
3º) Demostra-se para P(n+1).

Exercício 3.1

Comprovar a seguinte afirmaçom:

$$3^n-2n^2-1 = \dot{8} \ \forall \ n \in N$$

1º) $P(1)\equiv 3^1-2\cdot 1^2-1=3-2-1=0=8\cdot 0 \Rightarrow$ múltiplo de 8 c.q.d.
2º) Supomos certo $P(n)\equiv 3^n-2n^2-1=8k$ para algum $k\in N$.
3º) $P(n+1)\equiv 3^{n+1}-2(n+1)^2-1=3^{n+1}-2(n^2+2n+1)-1=3^{n+1}-2n^2+4n-3=$
$=3(3^n-2n^2-1)+4n^2+4n=\underline{3\cdot 8k}+4n^2+4n$ sendo $k\in N$

$\uparrow$ por hipótese de induçom

Agora o que resta por demostrar é que $4n^2+4n=\dot{8}$

1º) $P'(1)\equiv 4\cdot 1^2+4\cdot 1=8 \Rightarrow$ múltiplo de 8 c.q.d.
2º) Supomos certo $P'(n)\equiv 4n^2+4n=8k'$ para algum $k'\in N$.
3º) $P'(n+1)\equiv 4\cdot(n+1)^2+4\cdot(n+1)=4\cdot(n^2+2n+1)+4n+4=$
$=\underline{4n^2}+8n+4+\underline{4n}+4=8k'+8n+8=8(k^o+n+1) \Rightarrow$ múltiplo de 8.

$\uparrow$ por hipótese de induçom

Exercício 3.2

Comprovar a seguinte afirmaçom:

$$1^2+2^2+...+n^2=[n\cdot(n+1)\cdot(2n+1)]/6 \ \forall \ n \in N$$

1º) $P(1)\equiv 1^2=[1\cdot(1+1)\cdot(2\cdot 1+1)]/6 \Leftrightarrow 1=6/6$, é certo.
2º) Supomos certo $P(n)\equiv 1^2+2^2+...+n^2=[n\cdot(n+1)\cdot(2n+1)]/6$
3º) Temos que demostrar que:

$$P(n+1)\equiv 1^2+2^2+...+(n+1)^2=[(n+1)\cdot(n+2)\cdot(2n+3)]/6$$

$$1^2+2^2+...+n^2+(n+1)^2=\underset{\substack{\uparrow\\ \text{por hipótese de induçom}}}{[n\cdot(n+1)\cdot(2n+1)]/6}+(n+1)^2=$$

$$\frac{n\cdot(n+1)\cdot(2n+1)+6\cdot(n+1)^2}{6}=\frac{(n+1)[n\cdot(2n+1)+6\cdot(n+1)]}{6}$$

$$=\mathbf{[}(n+1)(2n^2+n+6n+6)\mathbf{]}/6=\mathbf{[}(n+1)(2n^2+7n+6)\mathbf{]}/6$$

e este último resultado é igual a $[(n+1)\cdot(n+2)\cdot(2n+3)]/6$ c.q.d. já que $(2n+3)\cdot(n+2)$ val o mesmo que $(2n^2+7n+6)$.

Exercício 3.3

Comprovar a seguinte afirmaçom:

$$1(1!)+2(2!)+...n(n!)=(n+1)!-1 \ \forall\ n \in N$$

1º) $P(1)\equiv 1(1!)=(1+1)!-1$ certo.
2º) Supom-se certo $1(1!)+2(2!)+...n(n!)=(n+1)!-1$ para um $n \in N$.
3º) Temos que demostrar que se cumpre:

$$1(1!)+2(2!)+...(n+1)[(n+1)!]=(n+2)!-1$$

$$1(1!)+2(2!)+...(n+1)[(n+1)!]=(n+1)!-1+(n+1)[(n+1)!]=$$
$$=(n+1)!(n+1+1)-1=(n+2)!-1 \text{ c.q.d.}$$

Exercício 3.4

Comprovar a seguinte afirmaçom:

$$1+3+5+...+(2n-1)=n^2 \ \forall\ n \in N$$

1º) $P(1)\equiv 1+(2\cdot 1-1)=1^2$
2º) Supom-se certo $1+3+5+...+(2n-1)=n^2$
3º) Temos que demostrar que se cumpre:

$$1+3+5+...+(2n-1)+(2n+1)=(n+1)^2$$

$$1+3+5+...+(2n-1)+(2n+1)=n^2+(2n+1)=(n+1)^2 \text{ c.q.d.}$$

Definiçons recursivas para definir um conceito sobre N.

Exemplos:

- potências: $x^1=x$; $x^{n+1}=x^n\cdot x$
- factorial: $1!=1$; $(n+1)!=(n+1)\cdot n!$
- nºs de Fibonacci: $x_1=0$; $x_2=1$; $x_{n+1}=x_n+x_{n-1}$

1º) Define-se um caso base.
2º) Mediante a recursom define-se o conceito para um paso qualquera supondo-o já definido para o paso anterior (suposto o conceito definido para n, definí-lo para n+1).

A validez do pricípio de induçom basea-se na definiçom axiomática dos números naturais:

Def.- O conjunto N define-se axiomaticamente como:

- um conjunto nom vazio.
- dotado dumha aplicaçom sucessor $S:N\rightarrow N$ que verifica:
  - i) S é injectiva.
  - ii) 1 nom é sucessor de nengum elemento, e recebe o nome de "primeiro elemento".
  - iii) Se $A \subseteq N$ é tal que $1 \in A$, e se se cumpre a implicaçom "$n \in N \Rightarrow S(n) \in A$", entom A = N.

O princípio de induçom basea-se no apartado iii) desta definiçom axiomática dos naturais:

$A=\{n\in N/P(n)\}$

base de induçom i) $1\in A \Leftrightarrow P(1)$

hipótese de induçom ii) Se $n\in A\Leftrightarrow P(n) \underset{\substack{\uparrow \\ \text{paso inductivo}}}{\Rightarrow} n+1\in A\Leftrightarrow P(n+1)$

Exercício 3.5

Demostrar $n^3+2n=\dot{3}\ \forall\ n \in N$

i) $n=1 \Rightarrow P(1)\equiv 1^3+2\cdot 1=3 \Rightarrow$ múltiplo de 3 c.q.d.

ii) $P(n)\equiv n^3+2n=3k$ para algum $k\in N$.

iii) $(n+1)^3+2(n+1)=3k'$ para algum $k'\in N$?

$$n^3+3n^2+3n+1+2n+2=n^3+3n^2+5n+3=\underbrace{3(n^2+1)}_{\text{Trivialmente }\dot{3}}+\underbrace{3n}_{\dot{3}}+\underbrace{2n+n^3}_{\text{Por hipótese }\dot{3}}$$

Exercício 3.6

Demostrar a Lei de DeMorgan $(A\cap B)'=A'\cup B'$ sobre n conjuntos:

i) $n=2 \Rightarrow P(2)$ certo. Ver Tema 1 Aptdo "Propriedades das operaçons sobre conjuntos".

ii) $(A_1\cap A_2\cap...A_n)'=A_1'\cup A_2'\cup...A_n'$ por hipótese.

iii) Demostrar $(A_1\cap A_2\cap...A_n\cap A_{n+1})'=A_1'\cup A_2'\cup...A_n'\cup A_{n+1}'$

$A_1'\cup A_2'\cup...A_n'\cup A_{n+1}'$

$=$ pola associatividade da intersecçom

$(A_1'\cup A_2'\cup...A_n')\cup A_{n+1}'$

$=$ pola hipótese de induçom ii)

$(A_1\cap A_2\cap...A_n)'\cup A_{n+1}'$

$=$ pola base de induçom i)

$(A_1\cap A_2\cap...A_n\cap A_{n+1})'$

➢Equaçons diofânticas

Dados a, b, c $\in$ Z, Q, procuramos a existência de x, y $\in$ Z na expressom seguinte:

$$\mathbf{a \cdot x + b \cdot y = c}$$

$x^2 - y^2 = n \in N$
$x^2 + y^2 = z^2$

- **Teorema**

Sejam a, b, n números enteiros; a equaçom lineal $ax+by=n$ tem soluçom enteira x_0, y_0

se e só se

$mcd(a,b) \mid n$.

dem. "$\Leftarrow$"

Chamamos d = mcd(a,b)

$$d|n \Rightarrow \begin{cases} \text{se } n=0 \Rightarrow x_0=y_0=0 \\ \text{se } n\neq 0 \Rightarrow d\lambda=n;\ d=mcd(a,b) \Rightarrow d=ax_1+by_1 \Rightarrow \end{cases}$$

$$\Rightarrow d\lambda=n=a\lambda x_1+b\lambda y_1 \Rightarrow x_0=\lambda x_1,\ y_0=\lambda y_1 \Leftrightarrow x_0=(n/d)x_1,\ y_0=(n/d)y_1$$

Dado que x_1, y_1 som enteiros e que d divide a n, x_0, y_0 som enteiros c.q.d.

"$\Rightarrow$"

$ax_0+by_0=n$ onde x_0, y_0 som enteiros.

Sendo d=mcd(a,b), d|a e d|b $\Rightarrow$ $d\lambda=a$, $d\mu=b$ onde λ, μ enteiros $\Rightarrow$ $d\lambda x_0+d\mu y_0=n \Rightarrow d(\lambda x_0+\mu y_0)=n \Rightarrow d|n$ c.q.d.

➢Congruências

Definiçom: Seja m > 0, dados a, b $\in$ Z diremos que a e b som congruentes módulo m se e só se a-b é divisível por m.

Notaçom:

$$a \equiv b \bmod (m) \Leftrightarrow m \mid a-b$$

$$a \equiv b\ (m)$$

$$a \equiv_m b$$

$a \equiv b \bmod (m) \Leftrightarrow a-b = m\cdot k$ para algum enteiro k $\Leftrightarrow$ $a = b+m\cdot k$ para algum k $\in$ Z.

- **Teorema**

Fixado $m > 0$, cada $a \in Z$ é congruente com um dos enteiros 0, 1, 2, ..., m-1 e só um.

demostraçom (algoritmo da divisom):

$a = q \cdot m + r \qquad 0 \leq r < m$

$a-r = q \cdot m \Rightarrow m \mid a-r \Rightarrow a \equiv r \bmod m$

r é o menor resíduo nom negativo de a módulo m, o que nom é mais que a módulo m.

Definiçom: O conjunto dos enteiros 0, 1, 2, ..., m-1 chama-se conjunto de números resíduos nom negativos módulo m.

Seja $\{a_1, a_2, ..., a_n\}$ colecçom completa de resíduos módulo m, se cada enteiro é congruente com um só dos valores a_i $1 \leq i \leq m$ módulo m, equival a dizer que cada a_i é congruente módulo m com um valor distinto do conjunto {0, 1, 2, ..., m-1}.

Exemplo: {49, -24, 18, -19, 28, 46, -5, -15} é colecçom completa de resíduos módulo 8 (ao dividi-los por 8 obtêm-se restos distintos entre 0 e 7).

- **Teorema**

Sejam a e $b \in Z$. Daquela $a \equiv b \bmod m \Leftrightarrow$ ao dividir a e b por m se obtém o mesmo resto.

dem.

"$\Rightarrow$" $\quad a = q_1 \cdot m+r \quad 0 \leq r < m$

$\qquad b = q_2 \cdot m+r \quad 0 \leq r < m$

$a-b = (q_1-q_2) \cdot m+r-r \Leftrightarrow m \mid (a-b) \Leftrightarrow a \equiv b \bmod m$

"$\Leftarrow$" $\quad a = q_1 \cdot m+r_1 \quad 0 \leq r_1 < m$

$\qquad b = q_2 \cdot m+r_2 \quad 0 \leq r_2 < m$

$$\left.\begin{array}{l} a \equiv r_1 \bmod m \\ b \equiv r_2 \bmod m \\ a \equiv b \bmod m \end{array}\right\} r_1 = r_2$$

Sistemas de numeraçom

$341_{10}=\underline{3}\cdot 10^2+\underline{4}\cdot 10^1+\underline{1}\cdot 10^0$

$28_{10}=\underline{1}\cdot 2^4+\underline{1}\cdot 2^3+\underline{1}\cdot 2^2+\underline{0}\cdot 2^1+\underline{0}\cdot 2^0=11100_2$

$28_{10}=\underline{4}\cdot 7^1+\underline{0}\cdot 7^0=40_7$

- **Teorema**

Seja b um número natural $b\geq 2$ que chamaremos *base*. Entom todo número $m\in N$ (i.e. expressado em base dez) pode-se escrever de maneira única em base b do jeito seguinte:

$$m_b = a_k\cdot b^k+a_{k-1}\cdot b^{k-1}+...+a_1\cdot b+a_0$$

para algum $k\geq 0$ com $0\leq a_i<b$ $\forall i=0,1,...,k$ (os dígitos usados na base b vam de 0 a b-1)

demostraçom

existência

$n = m_1\cdot b+a_0 \quad 0\leq a_0<b$
$m_1 = m_2\cdot b+a_1 \quad 0\leq a_1<b$
$m_2 = m_3\cdot b+a_2 \quad 0\leq a_2<b$
...
$n>m_1>m_2>...$

Polo princípio de boa ordenaçom, esta cadeia de naturais tem um primeiro elemento (aqui derradeiro, o menor).

Seja m_k o derradeiro elemento da lista.

$m_k = 0\cdot b+a_k \quad 0\leq a_k<b$

$a_k\neq 0$ porque senom m_k seria cero

se nom fora cero poderiamos dividir de novo

$n = m_1\cdot b+a_0 = (m_2\cdot b+a_1)\cdot b+a_0 = m_2\cdot b^2+a_1\cdot b+a_0 = (m_3\cdot b+a_2)\cdot b^2+a_1\cdot b+a_0$
$= m_3\cdot b^3+a_2\cdot b^2+a_1\cdot b+a_0 = ... = a_k\cdot b^k+a_{k-1}\cdot b^{k-1}+...+a_2\cdot b^2+a_1\cdot b+a_0$

unicidade

Supomos que se pode expressar de duas formas:

$n = a_k\cdot b^k+a_{k-1}\cdot b^{k-1}+...+a_2\cdot b^2+a_1\cdot b+a_0 \qquad 0\leq a_i<b$
$n = c_k\cdot b^k+c_{k-1}\cdot b^{k-1}+...+c_2\cdot b^2+c_1\cdot b+c_0 \qquad 0\leq c_i<b$

$0 = (a_k-c_k)\cdot b^k+(a_{k-1}-c_{k-1})\cdot b^{k-1}+...+(a_1-c_1)\cdot b+(a_0-c_0)$

onde

$$\left.\begin{array}{l} b|0 \\ b|(a_k-c_k)\cdot b^k+(a_{k-1}-c_{k-1})\cdot b^{k-1}+...+(a_1-c_1)\cdot b \end{array}\right\} \Rightarrow$$

$$\left.\begin{array}{l} \Rightarrow b|(a_0-c_0) \\ 0\leq a_0,c_0<b \end{array}\right\} \Rightarrow a_0-c_0=0 \Leftrightarrow a_0=c_0$$

entom

$a_k\cdot b^k+a_{k-1}\cdot b^{k-1}+...+a_2\cdot b^2+a_1\cdot b$
$=$
$c_k\cdot b^k+c_{k-1}\cdot b^{k-1}+...+c_2\cdot b^2+c_1\cdot b$

de onde se tem que

$$a_k \cdot b^{k-1}+a_{k-1} \cdot b^{k-2}+...+a_2 \cdot b+a_1$$
$$=$$
$$c_k \cdot b^{k-1}+c_{k-1} \cdot b^{k-2}+...+c_2 \cdot b+c_1$$

repite-se o razoamento e deduz-se que $a_1=c_1$

em k+1 iteraçons demostra-se que $a_i=c_i$ $\forall$ 0,1,...k e conseqüentemente a unicidade da expressom.

Observaçons

Algoritmo cálculo ordenador

$n \equiv a_0 \bmod (b)$
$(n-a_0) \equiv a_1 \bmod (b^2)$
$(n-a_0-a_1 \cdot b) \equiv a_2 \bmod (b^3)$
...

Notaçom

$n_{10}=(a_k,a_{k-1},...,a_2,a_1,a_0)_b$

ou simplesmente

$n_{10}=(a_k a_{k-1}...a_2 a_1 a_0)_b$

Para bases superiores a dez b>10, usam-se letras para significar os dígitos; e.g. na base hexadecimal (b=16) os dígitos som 1,2,3,...,9,A,B,...,E,F

Nota

Nom sempre os números que manejamos som sumatórios de potências da mesma base. Por exemplo nas mediçons de tempos as agrupaçons som em 60 segundos, 60 minutos, 24 horas, 7 dias, 52 semanas.

- **Teorema**

Seja $\{b_0,b_1,b_2,...,b_m\}$ onde $\forall$ $b_i \geq 2$, ao conjunto chamamos-lhe ***base múltiple***. Todo natural n se pode escrever de forma única como:

$$n = a_0+a_1 \cdot b_0+a_2 \cdot (b_1 \cdot b_0)+...+a_{m+1}(b_0 \cdot b_1 \cdot ... \cdot b_m)$$

com $0 \leq a_i < b_i$ i=0,1,...,m
e algum $a_j \neq 0$ j=0,1,...,m+1

exemplo para tempos:

s = s+m·60+h·(60·60)

Exemplo:

expressar 5.427 segundos em unidades máximas

5.427 |60·60 $=b_1 \cdot b_0$=minutos,segundos

1.827 15 $=a_2$=horas

27 |60 $=b_0$=segundos

27 0 $=a_1$=minutos

$=a_0$=segundos

5.427[s] = 27[s] + 0·60[m] + 15·(60·60)[h]

Exercícios

a) Escrever o número 1.302_7 em forma decimal.
b) Escrever o número 34.350 em base 13.
c) Resolver a ecuaçom $(7.210)_8=x_5$
d) Demostrar que $121_m=[m+1]^2_{10}$ [$m\geq 3$ por guarismos]
e) Expressar 169_m em base 10 [$m\geq 10$ por guarismos]

a) Escrever o número 1.302_7 em forma decimal.

$1.302_7=1\cdot 7^3+3\cdot 7^2+0\cdot 7^1+2\cdot 7^0=343+147+0+2=492_{10}$

b) Escrever o número 34.350 em base 13.

```
34.350   |13
    4   2642  |13
           3  203   |13
                8    15   |13
                      2   1
```

$34.350_{10}=12.834_{13}$

c) Resolver a ecuaçom $(7.210)_8=x_5$

$7.210_8=7\cdot 8^3+2\cdot 8^2+1\cdot 8=3.720_{10}$

```
3.720    |5
    0    744   |5
           4   148   |5
                 3   29    |5
                       4    5     |5
                            0     1
```

$7.210_8=104.340_5$

d) Demostrar que $121_m=[m+1]^2_{10}$ [$m\geq 3$ por guarismos]

"$m\geq 3$ por guarismos" quer dizer que como em 121 como máximo guarismo que aparece é o 2 a base há de ser polo menos 3.

$1\cdot m^2+2\cdot m+1=m^2+2m+1=[m+1]^2$

e) Expressar 169_m em base 10 [$m\geq 10$ por guarismos]

"$m\geq 10$ por guarismos" quer dizer que como em 169 aparece como máximo guarismo o 9 a base há de ser polo menos 10.

$1\cdot m^2+6\cdot m+9=[m+1]^2$

CÂMBIOS DE BASE ENTRE b E b^r

De b a b^r fam-se agrupando de r em r dígitos (empeçando pola direita, claro!)

Por exemplo, para passar 11101110110110001_2 a base 8, hai que agrupar e 3 em 3 cifras já que $8=2^3$

$11101110110110001_2=11,101,110,110,110,001_8=356661_8$

Por exemplo, para passar 11101110110110001_2 a base 16, hai que agrupar de 4 em 4 cifras já que $16=2^4$

$11101110110110001_2=1,1101,1101,1011,0001_{16}=1DDB1_{16}$

De b^r a b fam-se substituíndo cada guarismo pola sua representaçom na base b

Por exemplo, para passar $CD10A2_{16}$ a base 2, substitui-se cada guarismo pola sua representaçom em base 2

$CD10A2_{16}=1100,1101,0001,0000,1010,0010_2=110011010001000010100010_2$

➢Critérios de divisibilidade

Seja n um número natural $n=\sum_{i=0}^{t} a_i \cdot 10^i$ (a_i som as t+1 cifras de n_{10})

Estudaremos a divisibilidade de n por um número natural $k \geq 2$

Consideremos <u>os restos obtidos ao dividir as sucesivas potências de 10 por um número natural $k \geq 2$</u>. Os restos denotamo-los por r_i $0 \leq i \leq t$

$$10^0 = 1 \bmod(k) \equiv r_0 \qquad (r_0 \text{ será sempre } 1)$$
$$10^1 = 10 \bmod(k) \equiv r_1$$
$$10^2 = 100 \bmod(k) \equiv r_2$$
$$\ldots$$
$$10^i = 10\ldots0 \bmod(k) \equiv r_i$$

$$\text{dado } n=\sum_{i=0}^{t} a_i \cdot 10^i \equiv \left(\sum_{i=0}^{t} a_i \cdot r_i\right) \bmod(k)$$

propriedade das congruências

n é divisível por k $\Leftrightarrow \left(\sum_{i=0}^{t} a_i \cdot r_i\right) \bmod(k) \equiv 0$

$\Leftrightarrow \boldsymbol{\sum_{i=0}^{t} a_i \cdot r_i}$ **é divisível por k**

Exemplo:

$n=119=1\cdot 10^2+1\cdot 10+9$ 119 é 7x17

k=5

$$10^0 = 1 \bmod(5) \equiv r_0=1$$
$$10^1 = 10 \bmod(5) \equiv r_1=0$$
$$10^2 = 100 \bmod(5) \equiv r_2=0$$

$\sum_{i=0}^{t} a_i \cdot r_i = \underline{1}\cdot 0+\underline{1}\cdot 0+\underline{9}\cdot 1=9$ $\bmod(5) \neq 0 \Rightarrow$ 119 nom é divisível por 5

k=6

$$10^0 = 1 \bmod(6) \equiv r_0=1$$
$$10^1 = 10 \bmod(6) \equiv r_1=4$$
$$10^2 = 100 \bmod(6) \equiv r_2=4$$

$\sum_{i=0}^{t} a_i \cdot r_i = \underline{1}\cdot 4+\underline{1}\cdot 4+\underline{9}\cdot 1=17$ $\bmod(6) \neq 0 \Rightarrow$ 119 nom é divisível por 6

k=7

$$10^0 = 1 \bmod(7) \equiv r_0=1$$
$$10^1 = 10 \bmod(7) \equiv r_1=3$$
$$10^2 = 100 \bmod(7) \equiv r_2=2$$

$\sum_{i=0}^{t} a_i \cdot r_i = \underline{1}\cdot 2+\underline{1}\cdot 3+\underline{9}\cdot 1=14$ $\bmod(7) = 0 \Rightarrow$ 119 sim é divisível por 7

Casos particulares de divisibilidade

- **Divisibilidade por 3**

n é divisível por 3 ⇔ a suma das suas cifras é múltiplo de 3

$10^0 = 1 \bmod(3) \equiv r_0=1$
$10^1 = 10 \bmod(3) \equiv r_1=1$
$10^2 = 100 \bmod(3) \equiv r_2=1$
...
$10^i = 10...0 \bmod(3) \equiv r_i=1$

$$\forall\, n,\ n=\sum_{i=0}^{t} a_i\cdot 10^i \equiv \left(\sum_{i=0}^{t} a_i\cdot r_i\right) \bmod(3) = \left(\sum_{i=0}^{t} a_i\right) \bmod(3)$$

Ex. É 51 divisível por 3?

5+1=6, é múltiplo de 3 ⇒ 51 é divisível por 3

É 86 divisível por 3?

8+6=14, nom é múltiplo de 3 ⇒ 86 nom é divisível por 3

- **Divisibilidade por 4**

$10^0 = 1 \bmod(4) \equiv r_0=1$
$10^1 = 10 \bmod(4) \equiv r_1=2$
$10^2 = 100 \bmod(4) \equiv r_2=0$
$10^3 = 1000 \bmod(4) \equiv r_2=0$
...
$10^i = 10...0 \bmod(4) \equiv r_i=0\ \forall\ i\geq 2$

$$\forall\, n,\ n=\sum_{i=0}^{t} a_i\cdot 10^i \equiv a_0\cdot 1+a_1\cdot 2 \bmod 4$$

n é múltiplo de 4

⇔ a cifra das unidades sumada con duas vezes a das dezenas é múltiplo de 4

⇔ **o número formado polas suas duas derradeiras cifras (à direita) é múltiplo de 4*

*$a_0\cdot 1+a_1\cdot 2 \equiv a_0+a_1\cdot 10$

- **Divisibilidade por 7**

$10^0 \bmod(7) \equiv r_0=1$
$10^1 \bmod(7) \equiv r_1=3$
$10^2 \bmod(7) \equiv r_2=2$
$10^3 \bmod(7) \equiv r_3=6 \equiv_{mod\ 7} -1$
$10^4 \bmod(7) \equiv r_4=4 \equiv_{mod\ 7} -3$
$10^5 \bmod(7) \equiv r_5=5 \equiv_{mod\ 7} -2$
$10^6 \bmod(7) \equiv r_6=1$
$10^7 \bmod(7) \equiv r_7=3$

$10^8 \bmod(7) \equiv r_8=2$

...

$$n=\sum_{i=0}^{t} a_i\cdot 10^i \text{ é divisível por } 7$$

$$\Leftrightarrow a_0+3\cdot a_1+2\cdot a_2-a_3-3\cdot a_4-2\cdot a_5... \text{ é divisível por } 7$$

Exemplo:

é 38.024 divisível por 7?

$\underline{1}\cdot 4+\underline{3}\cdot 2+\underline{2}\cdot 0\underline{-1}\cdot 8\underline{-3}\cdot 3=-7$ é divisível por 7 $\Rightarrow$ 38.024 tamém

$$n=\sum_{i=0}^{t} a_i\cdot 10^i \text{ é divisível por } 7$$

$$\Leftrightarrow n-2\cdot a_0 \text{ é divisível por } 7$$

$$\Leftrightarrow \sum_{i=0}^{t} a_i\cdot 10^{i-1} \text{ é divisível por } 7$$

(aplíca-se recursivamente)

Exemplo:

é 38.024 divisível por 7?

3.802 –8 $\rightarrow$ 3.794 $\rightarrow$ 379 –8 $\rightarrow$ 371 $\rightarrow$ 37 –2 $\rightarrow$ 35 $=7\cdot 5$

$\Rightarrow$ sim é divisível 38.024 por 7

Exercicios

Problema 1. Escrevam-se em base 10 os seguintes números:

3.541_7

58.321_{12}

101.111_2

Resposta 1.

$3.541_7=3\cdot 7^3+5\cdot 7^2+4\cdot 7+1=1.303_{10}$

$58.321_{12}=5\cdot 12^4+8\cdot 12^3+3\cdot 12^2+2\cdot 12+1=117.961_{10}$

$101.111_2=2^5+2^3+2^2+2+1=47_{10}$

Problema 2. Resólvam-se as seguintes ecuaçons:

a) $124_5=x_9$

b) $132_x=330_5$

Resposta 2.

a) $124_5=5^2+2\cdot 5+4=39_{10}$

$$\begin{array}{l|l} 39 & 9 \\ \hline 3 & 4 \end{array}$$

$124_5=43_9$

b) $330_5=3\cdot 5^2+3\cdot 5=90_{10}$

$$x^2+3x+2=90 \Leftrightarrow x^2+3x-88=0 \Leftrightarrow x=\frac{-3\pm\sqrt{9-4\cdot(-88)}}{2}=\frac{-3\pm 19}{2}=\begin{cases}8\\-11\end{cases}$$

$330_5=132_8$

Problema 3. Calcúle-se:

a) 13+23+33
b) 43·21
onde todos os números estám expressados em base 5.

Resposta 3.

a) unidades: 3+3+3=9, em base 5 ≡ 14, 4 unidades e levamos 1
dezenas: 1+2+3=6, em base 5 ≡ 11, mais 1 que levamos das unidades → 12

resposta: $13_5+23_5+33_5=124_5$

comprovaçom: $(5+3)+(2\cdot5+3)+(3\cdot5+3)=8_{10}+13_{10}+18_{10}=39_{10}=5^2+2\cdot5+4$

b)
```
  1     ← levamos no produto
  43
 x21
-----
11      ← levamos na suma
  43
141
-----
2003
```

Problema 4. Demostre-se que um enteiro em base 7 é par se e só se a suma das suas cifras é par.

Resposta 4.

$n_{10}=a_i\cdot7^i+...+a_2\cdot7^2+a_1\cdot7+a_0$

$7 \bmod(2)\equiv1 \Rightarrow 7^2 \bmod(2)\equiv1, ..., 7^i \bmod(2)\equiv1$

$n_{10} \bmod(2)\equiv a_i+...+a_2+a_1+a_0$ ⇒ a paridade de n é a paridade da suma das cifras

Problema 5. Prove-se que todo número natural se pode escrever de jeito único da forma:

$$n=a_0+3\cdot a_1+3^2\cdot a_2+...+3^k\cdot a_k$$

para algum k, onde a_i=-1,0,1 para i=0,1,...,k

Resposta 5.

Todo natural se pode expressar em base 3:

$$n=c_0+3\cdot c_1+3^2\cdot c_2+...+3^{k'}\cdot c_{k'}$$

Consideremos o primeiro c_j=2, para i=0,1,...,j-1 consideramos $a_i=b_i$ e como c_j=3-1 temos que

$$3^j\cdot c_j+3^{j+1}\cdot c_{j+1}=(-1)\cdot3^j+(c_j+1)\cdot3^{j+1}$$

polo tanto tomamos c_j=-1

Segundo os valores que tome $c_{j+1}+1$ distinguimos diferentes casos:

-se é 3 daquela $(c_j+1)\cdot 3^{j+1}=3^{j+2} \Rightarrow$ tomamos $a_{j+1}=0$

-se é 2 daquela procéde-se como antes se fiz

-se é 1 daquela $a_{j+1}=c_{j+1}+1$

A continuaçom procede-se do mesmo modo co coeficiente $c_{j+2}+1$ ou b_{j+2} segundo os casos e assi sucessivamente se chega a expressar n na forma desejada onde k é k′ ou k′+1 segundo se o termo que aparez con $3^{k'}$ seja 0, 1 ou 2.

Problema 6.

a) Achem-se os critérios de divisibilidade por 14 e por 9
b) Apliquem-se estes critérios para obter a cifra designada por x tal que o número 68x062 seja divisível por 126

a) $n=10^i a_i+...+10^2 a_2+10a_1+a_0$ é divisível por 9
$\Leftrightarrow$
$r_i a_i+...+r_2 a_2+r_1 a_1+r_0 a_0$ é divisível por 9

onde os r_i som

$1 \bmod(9)=1=r_0$
$10 \bmod(9)=1=r_1$
$100 \bmod(9)=1=r_2$
$1000 \bmod(9)=1=r_3$
...

conclusom

$n=10^i a_i+...+10^2 a_2+10a_1+a_0$ é divisível por 9
$\Leftrightarrow$
a suma das suas cifras é divisível por 9

$n=10^i a_i+...+10^2 a_2+10a_1+a_0$ é divisível por 14
$\Leftrightarrow$
$r_i a_i+...+r_2 a_2+r_1 a_1+r_0 a_0$ é divisível por 14

onde os r_i som

$1 \bmod(14)= 1=r_0$

$10 \bmod(14)=10=r_1$
$100 \bmod(14)= 2=r_2$
$1.000 \bmod(14)= 6=r_3$
$10.000 \bmod(14)= 4=r_4$
$100.000 \bmod(14)=12=r_5$
$1.000.000 \bmod(14)= 8=r_6$

$10.000.000 \bmod(14)=10=r_7$
$100.000.000 \bmod(14)= 2=r_8$
$1.000.000.000 \bmod(14)= 6=r_9$
$10.000.000.000 \bmod(14)= 4=r_{10}$
...

$n=10^i a_i+...+10^2 a_2+10a_1+a_0$ é divisível por 14
$\Leftrightarrow$
$a_0+10a_1+2a_2+6a_3+4a_4+12a_5+8a_6+...$ é divisível por 14

b) $126=14\cdot 9$

126 é divisível por 9 daquela:

$6+8+x+0+6+2=9y \Rightarrow 22+x=9y$

como x há de ser um número de umha soa cifra provamos
22+0 nom é múltiplo de 9
22+1 nom é múltiplo de 9
22+2 nom é múltiplo de 9
22+3 nom é múltiplo de 9
22+4 nom é múltiplo de 9
22+6 nom é múltiplo de 9
22+7 nom é múltiplo de 9
22+8 nom é múltiplo de 9
22+9 nom é múltiplo de 9
22+5 sim é múltiplo de 9

entom x=5

126 é divisível por 14 daquela:

$2+10\cdot 6+2\cdot 0+6\cdot x+4\cdot 8+12\cdot 6=14z \Rightarrow 166+6x=14z$

comprovaçom: $196=14\cdot 14$

Problema 7.

a) Achem-se os critérios de divisibilidade por 4 e por 13.
b) Apliquem-se estes critérios para determinar o maior número de seis cifras divisível por 4 e por 13.

Resposta 7.

a) $n=10^i a_i+...+10^2 a_2+10a_1+a_0$ é divisível por 4
$\Leftrightarrow$
$r_i a_i+...+r_2 a_2+r_1 a_1+r_0 a_0$ é divisível por 4

onde os r_i som

1 mod(4)=1=r_0
10 mod(4)=2=r_1
100 mod(4)=0=r_2
1.000 mod(4)=0=r_3
10.000 mod(4)=0=r_4
...

conclusom: um número é divisível por 4 se e só se o é o número resultado de sumar as unidades e o dobre das dezenas.

$n=10^i a_i+...+10^2 a_2+10a_1+a_0$ é divisível por 13
$\Leftrightarrow$
$r_i a_i+...+r_2 a_2+r_1 a_1+r_0 a_0$ é divisível por 13

onde os r_i som

$$
\begin{aligned}
1 \bmod(13) &= 1=r_0\\
10 \bmod(13) &= 10=r_1\\
100 \bmod(13) &= 9=r_2\\
1.000 \bmod(13) &= 12=r_3\\
10.000 \bmod(13) &= 3=r_4\\
100.000 \bmod(13) &= 4=r_5
\end{aligned}
$$

$$
\begin{aligned}
1.000.000 \bmod(13) &= 1=r_6\\
10.000.000 \bmod(13) &= 10=r_7\\
100.000.000 \bmod(13) &= 9=r_8\\
1.000.000.000 \bmod(13) &= 12=r_9\\
10.000.000.000 \bmod(13) &= 3=r_{10}
\end{aligned}
$$

...

c) $n=10^5a+10^4b+10^3c+10^2d+10e+f=(\text{“abcdef”})_{10}$

$2e+f=4k$

$f+10e+9d+12c+3b+4a=13k'$

supomos $n=9999ef \Rightarrow f+10e+5=13k'$

imos provando as dezenas e=9,8,7,... até que se cumpran as duas condiçons:

$e=9 \Rightarrow 2\cdot9+f=4k \Rightarrow f=5-4k=5-4=1 \Rightarrow 1+90+5=13k'$ nom
$e=8 \Rightarrow 2\cdot8+f=4k \Rightarrow f=3-4k=...$ nom
$e=7 \Rightarrow 2\cdot7+f=4k \Rightarrow f=14-4k=$
$e=6 \Rightarrow 2\cdot6+f=4k \Rightarrow f=12-4k=12-4\cdot3=0 \Rightarrow 60+5=13k'=13\cdot5$ sim

$n=999960$

Problema 8. Considere-se o número 1234567891011...100, onde os números escritos som os naturais do 1 ao 100 sem espaços entre eles. Estude-se se n é divisível por 9.

Resposta 8.

$n=10^ia_i+...+10^2a_2+10a_1+a_0$ é divisível por 9
$\Leftrightarrow$
a suma das suas cifras é divisível por 9

1,2,3,...100 é umha progressom aritmética do seguinte jeito:

1	1	1	1x1
2	3	12	1x3
3	6	123	2x3
4	10	1234	2x5
5	15	12345	3x5
6	21	123456	3x7
7	28	1234567	4x7
8	36	12345678	4x9
9	45	123456789	5x9
10	55	123456789010	5x11
...	...		...
i	s_i	1234...i	$s_i=(i \text{ DIV } 2) \times \begin{cases} i & \text{se } i \text{ é impar} \\ i+1 & \text{se } i \text{ é par} \end{cases}$
...	...		...
100	$s_{100}=(100 \text{ DIV } 2)\text{x}(101)=50\text{x}101=5.050$		

entom:

1234...100 é divisível por 9
se e só se
5.050 é divisível por 9
se e só se ← recursivamente
10 é divisível por 9

resposta: 1234...100 nom é divisível por 9

Problema 9. Dado um número natural $n=a_t a_{t-1}...a_1 a_0$ demostre-se:
a) n é divisível por 2 se e só se a_0 é par.
b) n é divisível por 4 se e só se o número a_1a_0 o é.
c) n é divisível por 5 se e só se a_0 é 0 ou 5.

Resposta 9.
a) $n=10^i a_i+...+10^2 a_2+10a_1+a_0$ é divisível por 2
$\Leftrightarrow$
$r_i a_i+...+r_2 a_2+r_1 a_1+r_0 a_0$ é divisível por 2

onde os r_i som

1 mod(2)=1=r_0
10 mod(2)=0=r_1
100 mod(2)=0=r_2
1.000 mod(2)=0=r_3
10.000 mod(2)=0=r_4
...

entom

$n=10^i a_i+...+10^2 a_2+10a_1+a_0$ é divisível por 2
$\Leftrightarrow$
a_0 é divisível por 2
$\Leftrightarrow$
a_0 é par

b) $n=10^i a_i+...+10^2 a_2+10a_1+a_0$ é divisível por 4
$\Leftrightarrow$
$r_i a_i+...+r_2 a_2+r_1 a_1+r_0 a_0$ é divisível por 4

onde os r_i som

1 mod(4)=1=r_0
10 mod(4)=2=r_1
100 mod(4)=0=r_2
1.000 mod(4)=0=r_3
10.000 mod(4)=0=r_4
...

entom

$n=10^i a_i+...+10^2 a_2+10a_1+a_0$ é divisível por 4
$\Leftrightarrow$
$2a_1+a_0$ é divisível por 4
$\Leftrightarrow$ ← 10 mod(4)≡2
$10a_1+a_0$ é divisível por 4
$\Leftrightarrow$
a_1a_0 é divisível por 4

c) $n=10^i a_i+...+10^2 a_2+10a_1+a_0$ é divisível por 5
$\Leftrightarrow$
$r_i a_i+...+r_2 a_2+r_1 a_1+r_0 a_0$ é divisível por 5

onde os r_i som

$1 \bmod(5)=1=r_0$
$10 \bmod(5)=0=r_1$
$100 \bmod(5)=0=r_2$
$1.000 \bmod(5)=0=r_3$
$10.000 \bmod(5)=0=r_4$
...

entom

$n=10^i a_i+...+10^2 a_2+10a_1+a_0$ é divisível por 5
$\Leftrightarrow$
a_0 é divisível por 5
$\Leftrightarrow$
a_0 é 0 ou 5

Problema 10.
a) Obtenha-se umha geralizaçom do critério de divisibilidade por k dum número enteiro n escrito em base b, e como conseqüência:
b) Obtenha-se um critério de divisibilidade de n_9 por 8.
c) Estude-se se 53.286_9 é divisível por 8.

Resposta 10.
a) $n=b^i a_i+...+b^2 a_2+ba_1+a_0$ é divisível por k
$\Leftrightarrow$
$r_i a_i+...+r_2 a_2+r_1 a_1+r_0 a_0$ é divisível por k

onde os r_i som $r_i=\mathbf{b}^i \bmod(k)$

b) $n=9^i a_i+...+9^2 a_2+9a_1+a_0$ é divisível por 8
$\Leftrightarrow$
$r_i a_i+...+r_2 a_2+r_1 a_1+r_0 a_0$ é divisível por 8

onde os r_i som

$1_9 \bmod(8)=1=r_0$ $\quad 1_9=(9^0)_{10}$
$10_9 \bmod(8)=1=r_1$ $\quad 10_9=(9^1)_{10}$
$100_9 \bmod(8)=1=r_2$ $\quad 100_9=(9^2)_{10}$
...

entom

$n=9^i a_i+...+9^2 a_2+9a_1+a_0$ é divisível por 8
$\Leftrightarrow$
a suma das suas cifras é divisível por 8

c) $5+3+2+8+6=24$, $24 \bmod(8)=0 \Rightarrow 53.286_9$ é divisível por 8