CAPÍTULO II

OS NÚMEROS NATURAIS

1. Introdução

O objetivo deste capítulo é fazer um estudo aritmético do conjunto $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ dos números naturais. Um pré-requisito para este assunto seria, num enfoque mais formal e completo, a própria construção lógica de $\mathbb{N}$. Mas isto só será feito, e mesmo assim omitindo-se alguns detalhes, no Apêndice I, ao fim do capítulo. Obviamente esta abordagem significa que, embora a ênfase seja a aritmética propriamente dita, não queremos deixar de chamar a atenção para seus princípios básicos — algo cuja necessidade passa muitas vezes totalmente despercebida.

Enquanto a geometria, 300 anos antes de Cristo, nos *Elementos* de Euclides, já recebia um tratamento lógico-dedutivo, com seus postulados e axiomas, definições e teoremas, para a teoria dos números (e mesmo para as demais partes da matemática) demorou muito um tratamento semelhante.

A primeira tentativa nesse sentido se deve a Giovanni Campano (viveu por volta de 1260). Este capelão do Papa Urbano IV procurou fundamentar os números naturais em 4 postulados, o último dos quais afirmava que "um número não pode diminuir indefinidamente", o que significa, no fundo, a existência do mínimo de qualquer coleção de números naturais. Posteriormente Gottfried W. Leibniz (1646-1716) assinalou que "verdades" tão evidentes como $2 + 2 = 4$ devem ser objeto de demonstração a partir do conceito de número, o mesmo devendo acontecer também com propriedades aparentemente tão óbvias como a comutativa da adição e a comutativa da multiplicação. Mas Leibniz não se alongou no assunto.

Mas ao se chegar ao século XIX já não era possível à Matemática, no estágio que atingira e no ritmo em que se desenvolvia, continuar se apoiando quase que inteiramente na intuição. E seus alicerces passaram a ser investigados amplamente e a receber a fundamentação lógica necessária.

No que se refere aos números, parece que a primeira tentativa séria nesse sentido foi feita por Hermann G. Grassmann (1809-1877) que, em 1861, definiu adição e multiplicação de inteiros e demonstrou as propriedades fundamentais dessas operações, usando apenas a função sucessor $x \to x + 1$ e implicitamente o princípio de indução. O primeiro sistema completo de axiomas para a aritmética foi apresentado por Richard Dedekind (1831-1916) em 1888. A axiomática que formularemos no Apêndice I se deve a Giuseppe Peano (1858-1932) e data de 1891.

2. Operações — relação de ordem

Não faremos aqui, como já foi dito, a construção lógica de $\mathbb{N} = \{0, 1, 2, \ldots\}$. Tampouco serão dadas agora as definições formais de adição e multiplicação de números naturais. O leitor interessado encontrará tudo isso no já citado Apêndice I. Neste parágrafo nos limitaremos a citar as propriedades dessas duas operações que servem de embasamento teórico à aritmética dos números naturais. Antes disso registremos que o conjunto $\mathbb{N} - \{0\}$ será indicado pela notação $\mathbb{N}^*$. Ou seja: $\mathbb{N}^* = \{1, 2, 3, \ldots\}$.

2.1 Adição

$\mathbf{a}_1$ $a + (b + c) = (a + b) + c$, $\forall a, b, c \in \mathbb{N}$ (associativa)
$\mathbf{a}_2$ $a + b = b + a$, $\forall a, b \in \mathbb{N}$ (comutativa)
$\mathbf{a}_3$ $a + 0 = a$, $\forall a \in \mathbb{N}$ (0 é o elemento neutro da adição em $\mathbb{N}$)
$\mathbf{a}_4$ $a + b = a + c \Rightarrow b = c$ (lei do cancelamento da adição)

2.2 Multiplicação

$\mathbf{m}_1$ $a(bc) = (ab)c$, $\forall a, b, c \in \mathbb{N}$ (associativa)
$\mathbf{m}_2$ $ab = ba$, $\forall a, b \in \mathbb{N}$ (comutativa)
$\mathbf{m}_3$ $a \cdot 1 = a$, $\forall a \in \mathbb{N}$ (1 é o elemento neutro da multiplicação)
$\mathbf{m}_4$ $ab = 0 \Rightarrow a = 0$ ou $b = 0$ (lei do anulamento do produto)
$\mathbf{m}_5$ $(ac = bc$ e $c \neq 0) \Rightarrow a = b$ (lei do cancelamento da multiplicação)
$\mathbf{m}_6$ $ab = 1 \Rightarrow a = 1$ e $b = 1$
$\mathbf{m}_7$ $a(b + c) = ab + ac$, $\forall a, b, c \in \mathbb{N}$ (a multiplicação é distributiva em relação à adição)

Nota: O símbolo $\Rightarrow$ será sempre usado neste texto com o significado de "se..., então...". Por exemplo a propriedade $\mathbf{m}_6$ deve ser interpretada da maneira condicional seguinte: "Se a e b são números naturais e $ab = 1$, então $a = 1$ e $b = 1$". E o símbolo $\Leftrightarrow$ será empregado com o sentido de "se, e somente se".

2.3 Relação de ordem

Define-se a relação $\leqslant$ (menor que ou igual) em $\mathbb{N}$ do seguinte modo: se $a, b \in \mathbb{N}$, diz-se que $a \leqslant b$ se $b = a + u$, para algum $u \in \mathbb{N}$. O número u nessas condições chama-se *diferença* entre b e a e é indicado por $u = b - a$, onde b é o *minuendo* e a o *subtraendo*.

Assim a *subtração* $(a, b) \to a - b$ só está definida neste caso para os pares ordenados (a, b) em que $a \geqslant b$. Valem as seguintes propriedades:

- $(b - a) + a = b$, sempre que $a \leqslant b$
  De fato, se $b - a = u$, então $b = a + u = a + (b - a)$
- Se $c \leqslant a$, então $(a + b) - c = (a - c) + b$
  Seja $a - c = u$. Então $a = c + u$ e portanto $a + b = c + (u + b)$. Donde $(a + b) - c = u + b = (a - c) + b$
  Do mesmo modo se provam:
- $b + c \leqslant a \Rightarrow a - (b + c) = (a - b) - c$
  Neste caso simplifica-se a notação assim:
  $(a - b) - c = a - b - c$
- Se $b \leqslant a$ e $d \leqslant c$, então $(a - b) + (c - d) = (a + c) - (b + d)$.

Mas vejamos agora as principais propriedades da relação $\leqslant$. Observemos antes que algumas delas poderiam ser provadas a partir dos resultados que já temos, ao passo que a demonstração de outras depende de pré-requisitos que figuram no Apêndice I.

$\mathbf{O}_1$ $a \leqslant a$, $\forall a \in \mathbb{N}$ (reflexiva)
$\mathbf{O}_2$ $a \leqslant b$ e $b \leqslant a \Rightarrow a = b$ (anti-simétrica)
$\mathbf{O}_3$ $a \leqslant b$ e $b \leqslant c \Rightarrow a \leqslant c$ (transitiva)
$\mathbf{O}_4$ $a \leqslant b$ ou $b \leqslant a$ (a relação $\leqslant$ é total)
$\mathbf{O}_5$ $a \leqslant b \Rightarrow a + c \leqslant b + c$, $\forall c \in \mathbb{N}$ ($\leqslant$ é compatível com a adição)
$\mathbf{O}_6$ $a \leqslant b \Rightarrow ac \leqslant bc$, $\forall c \in \mathbb{N}$ ($\leqslant$ é compatível com a multiplicação)

Por valerem as seis propriedades anteriores diz-se que $\leqslant$ é uma relação de ordem total sobre $\mathbb{N}$ compatível com a adição e a multiplicação de $\mathbb{N}$.

Diz-se que a é *menor que* b e escreve-se $a < b$ se $b = a + v$, para algum $v \neq 0$. É claro então que: $a < b \Leftrightarrow a \leqslant b$ e $a \neq b$

$\mathbf{O}_7$ $a < b \Rightarrow a + 1 \leqslant b$

$\mathbf{O}_8$ Se L é um subconjunto não vazio de $\mathbb{N}$, então L possui um elemento m tal que $m \leqslant x$ para todo $x \in L$ (*princípio do menor número natural*).

O elemento m que aparece em O_8 é chamado *mínimo* de L e será indicado por $m = \min L$. É fácil provar que m é único. De fato, se $m_1 = \min L$, então $m \leqslant m_1$ (pois $m_1 \in L$) e $m_1 \leqslant m$ (pois $m_1 = \min L$ e $m \in L$). Logo $m = m_1$. Por exemplo, o mínimo do conjunto $\{1, 3, 5, 7, \ldots\}$ é 1

Dado $L \subset \mathbb{N}$, $L \neq \emptyset$, um elemento $M \in L$ (caso exista) tal que $x \leqslant M$, $\forall x \in L$, chama-se *máximo* de L. Notação: $M = \max L$. Se L possui máximo, este é único (demonstração análoga à que se fez para o mínimo). Há subconjuntos não vazios de $\mathbb{N}$ que não têm máximo: é o caso de $\{1, 3, 5, \ldots\}$ e $\{0, 2, 4, 6, \ldots\}$, por exemplo.

Alternativamente poderemos usar $b \geqslant a$ com o significado de $a \leqslant b$ e $b > a$ com o de $a < b$.

As propriedades a seguir decorrem do que já vimos e, vez por outra, são necessárias:

- $a \leqslant b$ e $b < c \Rightarrow a < c$
- $a < b \Rightarrow a + c < b + c$
- $a + c \leqslant b + c \Rightarrow a \leqslant b$
- $(a \leqslant b$ e $c \leqslant d) \Rightarrow a + c \leqslant b + d$
- $(a < b$ e $c \neq 0) \Rightarrow ac < bc$
- $(a < b$ e $c \leqslant d) \Rightarrow a + c < b + d$
- $c \leqslant b \Rightarrow a(b - c) = ab - ac$

3. Indução

3.1 Primeiro princípio de indução

Apesar da designação clássica, trata-se de uma proposição relativamente fácil de provar a partir dos resultados que já temos. Eis o seu enunciado:

"Seja $a \in \mathbb{N}$ e suponhamos que a cada número natural $n \geqslant a$ esteja associada uma afirmação $P_{(n)}$. Admitamos ainda que seja possível provar o seguinte:

i $P_{(a)}$ é verdadeira

ii Para todo $r \geqslant a$, se $P_{(r)}$ é verdadeira, então $P_{(r+1)}$ também é verdadeira.

Então $P_{(n)}$ é verdadeira para todo $n \geqslant a$."

A idéia da demonstração é simples. Devido a **i** $P_{(a)}$ é verdadeira. De **ii** segue então que $P_{(a+1)}$ é verdadeira. Ainda por **ii** decorre que $P_{(a+2)}$ é verdadeira. E assim por diante.

Vejamos como formalizar esse raciocínio.

Demonstração: Seja $L = \{x \in \mathbb{N} | x \geqslant a$ e $P_{(x)}$ é falsa$\}$. Basta provar então que $L = \emptyset$. Suponhamos $L \neq \emptyset$ e seja $m = \min L$. Logo $P_{(m)}$ é falsa e como, por hipótese, $P_{(a)}$ é verdadeira, então $m > a$. Desta última relação segue que $m > 0$; portanto $m = 1 + u$, para algum $u \in \mathbb{N}$, e daí $u < m$.

Mas $m > a$ implica que $m \geqslant a + 1$. Assim $m = 1 + u \geqslant a + 1$, do que resulta $u \geqslant a$.

Em resumo: $m > u \geqslant a$. Mas isto obriga $P_{(u)}$ a ser verdadeira (se fosse falsa, u estaria em L, o que não é possível pois $u < m = \min L$). Então, devido a **ii**: $P_{(u+1)} = P_{(m)}$ é verdadeira. Absurdo. ■

A afirmação $P_{(r)}$ que figura em **ii**, no enunciado do princípio, é chamada *hipótese de indução*.

3.2 Somatórios e produtórios em $\mathbb{N}$

São comuns em Matemática as *definições por recorrência* (*recursão*). Na verdade trata-se de definições por indução.

Examinemos o caso da adição e o da multiplicação em $\mathbb{N}$. Sendo ambas operações binárias sobre $\mathbb{N}$, a soma e o produto de dois números naturais estão naturalmente definidos. Admitindo que também o estejam para $n - 1 \geqslant 2$ números quaisquer de $\mathbb{N}$ e pondo, por definição

$$a_1 + a_2 + \ldots + a_n = (a_1 + \ldots + a_{n-1}) + a_n$$

e

$$a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_{n-1}) a_n$$

então passa a ter sentido falar em soma ou produto de $m \geqslant 2$ naturais quaisquer.

Assim, por exemplo:

$$a_1 + a_2 + a_3 = (a_1 + a_2) + a_3$$
$$a_1 + a_2 + a_3 + a_4 = (a_1 + a_2 + a_3) + a_4$$

Faremos uso, como é praxe, das seguintes notações:

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \ldots + a_n$$

onde o primeiro membro deve ser lido "somatório dos a_i, para i de 1 a n" e

$$\prod_{i=1}^{n} a_i = a_1 a_2 \ldots a_n$$

cujo primeiro membro se lê "produtório dos a_i, para i de 1 a n".

Quando n = 1 faz-se, por extensão:

$$\sum_{i=1}^{n} a_i = a_1 \qquad \text{e} \qquad \prod_{i=1}^{n} a_i = a_1$$

Outro conceito que pode ser introduzido por recorrência é o de *potência n-ésima de a*, onde a, n ∈ IN, a ≠ 0. Por definição:

$a^0 = 1$
$a^{n+1} = a^n \cdot a$, sempre que $n \geqslant 0$.

Isto significa que $a^1 = a^0 \cdot a = 1 \cdot a = a$, $a^2 = a^1 \cdot a = a \cdot a$, $a^3 = a^2 \cdot a = (a \cdot a) \cdot a$, e assim por diante.

Exemplo 1: Provemos por indução sobre n que $a^m \cdot a^n = a^{m+n}$, para quaisquer m, n ∈ IN, sempre que a ≠ 0.

$$n = 0 : a^m \cdot a^0 = a^m \cdot 1 = a^m = a^{m+0}$$

Logo, a propriedade vale para n = 0.
Hipótese de indução: $a^m \cdot a^r = a^{m+r}$, $\forall r \geqslant 0$.

$$n = r + 1 : a^m \cdot a^{r+1} = a^m \cdot (a^r \cdot a) \overset{(*)}{=} (a^m \cdot a^r) \cdot a \overset{(*)}{=} a^{m+r} \cdot a = a^{(m+r)+1} = a^{m+(r+1)}.$$

Note-se que a hipótese de indução foi usada na passagem (*).

A definição de potência pode ser estendida a a = 0 do seguinte modo: $0^n = 0$, para todo n ∈ IN, n ≠ 0.

Se a é um número natural e existe b ∈ IN de modo que $a = b^2$, então se diz que a é um *quadrado perfeito*. Os números naturais quadrados perfeitos são: 0, 1, 4, 9, 16, ..., n^2, ... E se $a = b^3$ para algum b ∈ IN, então a é chamado *cubo perfeito*. Os cubos perfeitos são: 0, 1, 8, 27, ..., n^3, ...

Exercício: Se a ∈ IN, a ≠ 0, prove que $(a^m)^n = a^{mn}$, ∀m, n ∈ IN (use indução sobre n).

PROPRIEDADES Vejamos agora algumas propriedades básicas envolvendo somatórios e produtórios:

i $$\sum_{i=1}^{n} a_i = \left(\sum_{i=1}^{n-1} a_i\right) + a_n \qquad \text{e}$$

$$\prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) a_n \qquad (\forall n \geqslant 2)$$

A validade destas propriedades é decorrência imediata dos conceitos e notações nelas envolvidos.

ii $$\sum_{i=1}^{n} (a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i \qquad \text{e}$$

$$\prod_{i=1}^{n} (a_i b_i) = \left(\prod_{i=1}^{n} a_i\right)\left(\prod_{i=1}^{n} b_i\right)$$

Provemos por indução a primeira dessas relações (indução sobre n).

$$n = 1 : \sum_{i=1}^{n} (a_i + b_i) = a_1 + b_1; \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i = a_1 + b_1$$

Vamos supor a propriedade válida para $r \geqslant 1$. Então:

$$\sum_{i=1}^{r+1} (a_i + b_i) = \left[\sum_{i=1}^{r} (a_i + b_i)\right] + (a_{r+1} + b_{r+1}) =$$
$$= \left(\sum_{i=1}^{r} a_i + \sum_{i=1}^{r} b_i\right) + (a_{r+1} + b_{r+1}) =$$
$$= \left[\left(\sum_{i=1}^{r} a_i\right) + a_{r+1}\right] + \left[\left(\sum_{i=1}^{r} b_i\right) + b_{r+1}\right] =$$
$$= \sum_{i=1}^{r+1} a_i + \sum_{i=1}^{r+1} b_i$$

iii Para todo k ∈ IN: $$\sum_{i=1}^{n} (ka_i) = k \sum_{i=1}^{n} a_i \qquad \text{e} \qquad \prod_{i=1}^{n} (ka_i) = k^n \prod_{i=1}^{n} a_i.$$

A demonstração fica como exercício (indução sobre n).

iv Se $a_i = a$ (i = 1, 2, ..., n), então:

$$\sum_{i=1}^{n} a_i = na \qquad \text{e} \qquad \prod_{i=1}^{n} a_i = a^n$$

Provemos a segunda dessas propriedades por indução sobre n.

$$n = 1 : \prod_{i=1}^{n} a_i = a_1 = a \qquad \text{e} \qquad a^n = a^1 = a$$

Seja $r \geqslant 1$ e suponhamos $\prod_{i=1}^{r} a_i = a^r$

Então $\prod_{i=1}^{r+1} a_i = \left(\prod_{i=1}^{r} a_i\right) a_{r+1} = a^r \cdot a = a^{r+1}$

v Se $a_i = i$ $(i = 1, 2, \ldots, n)$, então:

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Vamos também por indução sobre n.

$n = 1$: $\sum_{i=1}^{n} a_i = a_1 = 1$ e $\frac{n(n+1)}{2} = \frac{1(1+1)}{2} = 1$

Admitamos $r \geqslant 1$ e $\sum_{i=1}^{r} i = \frac{r(r+1)}{2}$

Então:

$$\sum_{i=1}^{r+1} a_i = \left(\sum_{i=1}^{r} a_i\right) + a_{r+1} = \frac{r(r+1)}{2} + (r+1) = \frac{r(r+1) + 2(r+1)}{2} =$$

$$= \frac{(r+1)(r+2)}{2}$$

Por exemplo:

$$\sum_{i=1}^{5} (3i + 2) = 3 \sum_{i=1}^{5} i + \sum_{i=1}^{5} 2 = 3 \cdot \frac{5(5+1)}{2} + 5 \cdot 2 = 55$$

$$\prod_{i=1}^{4} (i+2)^2 = \left[\prod_{i=1}^{4} (i+2)\right]^2 = (3 \cdot 4 \cdot 5 \cdot 6)^2 = 129\,600$$

vi Somatórios duplos

Sejam $a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n \in \mathbb{N}$ $(m \geqslant 1, n \geqslant 1)$. Às vezes há necessidade de considerar a soma de todos os produtos possíveis $a_i b_j$ $(1 \leqslant i \leqslant m;\ 1 \leqslant j \leqslant n)$. Mas esses produtos são exatamente as parcelas de:

$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = (a_1 + \ldots + a_i + \ldots + a_m)(b_1 + \ldots + b_j + \ldots + b_n)$$

Assim, em virtude de iii, deste item,

$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_i\right) b_j = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_i b_j\right)$$

e, analogamente:

$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_i b_j\right)$$

Em vista desse resultado a soma de todos os $a_i b_j$ é usualmente indicada por:

$$\sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j \quad \text{ou} \quad \sum_{j=1}^{n} \sum_{i=1}^{m} a_i b_j$$

Estas expressões recebem o nome de *somatórios duplos*. Das considerações feitas resulta que:

$$\sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j = \left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right)$$

Por exemplo:

a) $\sum_{i=1}^{2} \sum_{j=1}^{3} (2i)(3+j) = \left(\sum_{i=1}^{2} 2i\right)\left(\sum_{j=1}^{3} (3+j)\right) =$

$$= \left(2 \sum_{i=1}^{2} i\right)\left(\sum_{j=1}^{3} 3 + \sum_{j=1}^{3} j\right) =$$

$$= 2 \cdot \frac{2 \cdot 3}{2} \cdot \left(3 \cdot 3 + \frac{3 \cdot 4}{2}\right) = 6 \cdot (9 + 6) = 90$$

b) $\sum_{i=1}^{3} \sum_{j=1}^{2} i^2 \cdot 2^j = \left(\sum_{i=1}^{3} i^2\right)\left(\sum_{j=1}^{2} 2^j\right) =$

$$= (1 + 4 + 9) \cdot (2 + 4 + 8) = 14 \cdot 14 = 196$$

c) Se $m = n$, então:

$$\sum_{i=1}^{n} \sum_{j=1}^{n} ij = \left(\sum_{i=1}^{n} i\right)\left(\sum_{j=1}^{n} j\right) = \left(\sum_{i=1}^{n} i\right)^2 = \left[\frac{n(n+1)}{2}\right]^2$$

Nota: Se $a_1, a_2, \ldots, a_n \in \mathbb{N}$ $(n \geqslant 1)$ e $1 \leqslant r \leqslant n$, pomos, por definição:

$$\sum_{i=r}^{n} a_i = a_r + a_{r+1} + \ldots + a_n$$

$$\prod_{i=r}^{n} a_i = a_r\, a_{r+1} \ldots a_n$$

Assim, para $n \geqslant 2$ e $1 \leqslant r < n$:

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{r} a_i + \sum_{i=r+1}^{n} a_i$$

e

$$\prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{r} a_i\right)\left(\prod_{i=r+1}^{n} a_i\right)$$

3.3 Segundo princípio de indução

Seja $a \in \mathbb{N}$ e suponhamos que a cada natural $n \geqslant a$ esteja associada uma afirmação $P_{(n)}$. Admitamos ainda que seja possível provar as duas condições seguintes:

i $P_{(a)}$ é verdadeira.
ii Para todo $r > a$, se $P_{(k)}$ é verdadeira sempre que $a \leqslant k < r$, então $P_{(r)}$ também é verdadeira.

Então $P_{(n)}$ é verdadeira para todo $n \geqslant a$.

A demonstração deste princípio, aliás muito parecida com a do anterior, fica como exercício. Teremos ocasião, ainda neste capítulo, de usar algumas vezes este princípio.

EXERCÍCIOS

21. Calcule:

a) $\sum_{i=1}^{4} (2i + 3)$

b) $\sum_{i=2}^{4} i(i + 2)$

c) $\sum_{i=1}^{r+2} 3i$

d) $\sum_{i=1}^{3} 2^i$

22. Calcule:

a) $\prod_{i=1}^{4} 5$

b) $\prod_{i=1}^{3} i^2$

c) $\prod_{i=2}^{5} (i + 2)(i + 3)$

d) $\prod_{i=2}^{4} 3^i$

23. Escreva, usando o símbolo de somatório ou produtório:

a) $(a_1 + 2) + (a_2 + 4) + (a_3 + 4)$

b) $2^3 + 3^4 + 4^5 + \ldots + n^{n+1}$

c) $7 \cdot 8 \cdot 9 \cdot 10 \ldots 25$

d) $a_1b_2 + a_2b_3 + \ldots + a_nb_{n+1}$

e) $1^2 + 2^2 + \ldots + n^2$

f) $2^1 + 2^2 + 2^3 + \ldots + 2^p$

24. (Fuvest-81) P é uma propriedade relativa aos números naturais. Sabe-se que: 1) P é verdadeira para o natural $n = 10$; 2) Se P é verdadeira para n, então P é verdadeira para $2n$; 3) Se P é verdadeira para n, $n \geqslant 2$, então P é verdadeira para $n - 2$. Pode-se concluir que:

a) P é verdadeira para todo natural n.
b) P é verdadeira somente para os números naturais n, $n \geqslant 10$
c) P é verdadeira para todos os números naturais pares.
d) P é verdadeira somente para as potências de 2.
e) P não é verdadeira para os números ímpares.

25. Prove por indução:

a) $1^2 + 2^2 + \ldots + n^2 = \dfrac{n(n + 1)(2n + 1)}{6}$ $(n \geqslant 1)$

b) $1^3 + 2^3 + \ldots + n^3 = (1 + 2 + \ldots + n)^2$ $(n \geqslant 1)$

c) $1 \cdot 2 + 2 \cdot 3 + \ldots + n \cdot (n + 1) = \dfrac{n(n + 1)(n + 2)}{3}$ $(n \geqslant 1)$

d) $a \geqslant 1 \Rightarrow a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \ldots + a + 1)$ $(n \geqslant 1)$

e) $2n \leqslant n^2$ $(n \geqslant 2)$

f) $a \geqslant 2 \Rightarrow 2a^n \leqslant a^{n+1}$ $(n \geqslant 1)$

g) $a \geqslant 1 \Rightarrow a^{n+1} \leqslant a^{2n}$ $(n \geqslant 1)$

h) $a \geqslant 2 \Rightarrow 1 + a + \ldots + a^n < a^{n+1}$ $(n \geqslant 1)$

i) $n^3 < n!$ $(n \geqslant 6)$

j) $n! > n^2$ $(n \geqslant 4)$

Resolução de h):

Para $n = 1$ a relação é $1 + a < a^2$ que obviamente é verdadeira para $a = 2$. Supondo $1 + k < k^2$ $(k \geqslant 2)$, então $1 + (k + 1) = (1 + k) + 1 < k^2 + 1 < k^2 + 2k + 1 = (k + 1)^2$. Logo $1 + a < a^2$, para todo $a \geqslant 2$. Seja $r \geqslant 1$ e façamos a hipótese

$$1 + a + \ldots + a^r < a^{r+1}$$

Daí

$$1 + a + \ldots + a^r + a^{r+1} < a^{r+1} + a^{r+1} = 2a^{r+1} \leqslant a^{r+2}$$

o que conclui a resolução. Note-se que na última passagem usamos o resultado proposto em f).

26. Prove que:

$$1 + 3 + \ldots + (2n - 1) = n^2$$

ou seja, que a soma dos n primeiros números ímpares é n^2.

27. Prove por indução sobre n que o número de subconjuntos de um conjunto finito com n elementos é 2^n.

28. Prove por indução sobre n que:

$$(a^m)^n = a^{mn}$$

para quaisquer a, m, n $\in$ IN, $a \neq 0$.

29. Se $b + c \leqslant a$, mostre que:

$$a - (b + c) = (a - b) - c$$

30. Sejam x, y $\in$ IN. Se $3 < x < 6$ e $6 < y < 10$, mostre que $2 \leqslant y - x \leqslant 5$. De um modo geral, prove que se $a < x < b$ e $b < y < c$, então $2 \leqslant y - x \leqslant c - a - 2$.

31. Prove que o produto de quatro *números naturais consecutivos*, acrescido de 1, é um quadrado perfeito.

Resolução: Se a indica o menor dos números, então os outros são a + 1, a + 2 e a + 3.
Como

$$a(a + 1)(a + 2)(a + 3) = a^4 + 6a^3 + 11a^2 + 6a$$

deve-se procurar m $\in$ IN de modo que:

$$a^4 + 6a^3 + 11a^2 + 6a + 1 = (a^2 + ma + 1)^2$$

Desenvolvendo o segundo membro e identificando o resultado com o primeiro, obtém-se m = 3. Logo:

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

Por exemplo, se a = 4, então:

$$1 + 4 \cdot 5 \cdot 6 \cdot 7 = (4^2 + 12 + 1)^2 = 29^2$$

4. Divisibilidade em IN

4.1 Múltiplos e divisores

DEFINIÇÃO 1 Diz-se que um número natural a *divide* um número natural b se b = ac, para algum c $\in$ IN. Neste caso diz-se também que a é *divisor* de b e que b é *múltiplo* de a. Ou ainda que b é *divisível* por a. Indicaremos por a | b o fato de a dividir b; e se a não divide b, escrevemos a $\nmid$ b.

O elemento c $\in$ IN tal que b = ac, onde $a \neq 0$, é indicado por $c = \frac{b}{a}$ ou, eventualmente, por c = b : a e é chamado quociente de b por a.

Por exemplo, 2 | 6 pois $6 = 2 \cdot 3$, 5 | 10 pois $10 = 5 \cdot 2$, 1 | a ($\forall a \in$ IN) pois $a = 1 \cdot a$ e 0 | 0 uma vez que $0 = 0 \cdot a$, para todo a $\in$ IN. Mas, se $b \neq 0$, então 0 $\nmid$ b pois $0 \cdot c = 0 \neq b$, $\forall c \in$ IN.

Atenção: Não se deve confundir o símbolo | com o traço de fração ——. Assim, 2 | 6 (p. ex.) não deve ser confundido com $\frac{2}{6}$ ou $\frac{6}{2}$. Enquanto estes dois últimos símbolos indicam numerais, 2 | 6 expressa uma relação particular entre 2 e 6. O que ocorre é que, conforme notação já introduzida, 2 | 6 equivale a $6 = 2 \cdot \frac{6}{2}$. Assim, 0 | 0 é uma relação verdadeira, ao passo que $\frac{0}{0}$ é uma expressão indeterminada.

Para a relação x | y em IN valem as seguintes propriedades:

d_1 a | a, $\forall a \in$ IN, pois $a = a \cdot 1$ (reflexiva)

d_2 a | b e b | a $\Rightarrow$ a = b (anti-simétrica)
De fato, por hipótese, b = ac e a = bd. Daí: a = a(cd). Se a = 0, como b = ac, então b = 0. Se $a \neq 0$, então cd = 1 e portanto c = d = 1. Logo a = b também neste caso.

d_3 a | b e b | c $\Rightarrow$ a | c (transitiva)
Como b = ar e c = bs, então c = a(rs)

d_4 Se a | b e a | c, então a | (bx + cy), $\forall x, y \in$ IN
Em particular: a | b $\Rightarrow$ a | bx, $\forall x \in$ IN
De b = ar e c = as (hipóteses) decorre que bx = arx e cy = asy. Donde bx + cy = arx + asy = a(rx + sy).

Nota: Do que vimos segue que: a | b e a | c $\Rightarrow$ a | (b + c). Além disso,

$$\frac{b + c}{a} = \frac{b}{a} + \frac{c}{a}$$

pois:

$$\left(\frac{b}{a} + \frac{c}{a}\right)a = \frac{b}{a} \cdot a + \frac{c}{a} \cdot a = b + c$$

$\mathbf{d}_5$ Se $c|a$, $c|b$ e $a \leqslant b$, então $c|(b-a)$.
Por hipótese $a = cr$ e $b = cs$. Fazendo $b = a + u$, então $cs = cr + u$ e daí $u = cs - cr = c(s - r)$. Logo $c|u$ e como $u = b - a$ a propriedade está provada. Neste caso:

$$\frac{b-a}{c} = \frac{b}{c} - \frac{a}{c}$$

$\mathbf{d}_6$ Seja $a = b + c$ e suponhamos $d|b$. Então: $d|a \iff d|c$. ($c = a - b$)
($\Rightarrow$) é $\mathbf{d}_5$ e ($\Leftarrow$) é $\mathbf{d}_4$ para $x = y = 1$.

$\mathbf{d}_7$ Se $a|b$ e $b \neq 0$, então $a \leqslant b$.
Das hipóteses segue que existe $q \in \mathbb{N}^*$ de modo que $b = aq$. Como $q > 0$, então, devido a $\mathbf{O}_7$, $1 = 0 + 1 \leqslant q$ e portanto $q = 1 + u$, para algum $u \in \mathbb{N}$. Daí $b = aq = a(1 + u) = a + au$, o que implica $a \leqslant b$.

Notação: Indicaremos por M_a o conjunto dos múltiplos de a. Assim $M_a = \{0, a, 2a, 3a, \ldots\}$. Em particular $M_0 = \{0\}$ e $M_1 = \mathbb{N}$. Os elementos de $M_2 = \{0, 2, 4, \ldots\}$ são chamados *números naturais pares* e os de $\mathbb{N} - M_2 = \{1, 3, 5, \ldots\}$ de *naturais ímpares*.

4.2 O algoritmo da divisão (ou de Euclides)

Seja b um número natural não nulo. Se $a \in \mathbb{N}$, então ou a é múltiplo de b ou está entre dois *múltiplos consecutivos* de b, isto é: $bq \leqslant a < b(q + 1)$. Isto significa que $q + 1$ é o mínimo de $\{n \in \mathbb{N} \mid bn > a\}$, subconjunto não vazio de $\mathbb{N}$ pois contém o elemento $a + 1$. (De fato: $b \geqslant 1 \Rightarrow ab \geqslant a \Rightarrow ab + b \geqslant a + b \Rightarrow b(a + 1) \geqslant a + b > a$.)

De $bq \leqslant a$ resulta que existe $r \in \mathbb{N}$ tal que $a = bq + r$. Mostremos que $r < b$. Se $r = a - bq \geqslant b$, então $(a - bq) + bq \geqslant b + bq$ e daí $a \geqslant b(q + 1)$, o que não é possível. Assim:

$$a = bq + r \ (r < b)$$

As considerações que acabamos de fazer podem assim ser sintetizadas:
"Dados $a, b \in \mathbb{N}$, $b \neq 0$, existem $q, r \in \mathbb{N}$ de maneira que $a = bq + r$ $(r < b)$".

Obviamente, se $r = 0$, então a é múltiplo de b.

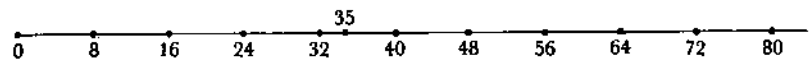
Suponhamos $a = bq + r = bq_1 + r_1$, onde $r < b$ e $r_1 < b$. Admitamos que se pudesse ter $r \neq r_1$, digamos $0 < r - r_1 < b$ (já levando em conta que tanto r como r_1 são menores que b). Mas então da igualdade $bq + r = bq_1 + r_1$ decorre que $bq + (r - r_1) = bq_1$ e portanto $b|(r - r_1)$. Donde $b \leqslant r - r_1$, o que é absurdo. Logo $r = r_1$ e portanto $q = q_1$.

Provamos pois o

TEOREMA 1 *(algoritmo da divisão ou de Euclides)*: "Para quaisquer a, $b \in \mathbb{N}$, $b \neq 0$, existe um único par de números q e r, de maneira que $a = bq + r$ $(r < b)$".

Os elementos a, b, q e r são chamados, respectivamente, *divisor*, *dividendo*, *quociente* e *resto* da divisão de a por b.

Exemplo 2: Vamos aplicar o algoritmo aos números $a = 35$ e $b = 8$. Observemos que 35 está entre os múltiplos 32 e 40 de 8:



$8 \cdot 4 < 35 < 8 \cdot (4 + 1)$. Logo $q = 4$ e $r = 35 - 8 \cdot 4 = 3$. Isso explica o algoritmo

$$\begin{array}{r|l} 35 & 8 \\ \hline -\ 32 & 4 \\ \hline 3 & \end{array}$$

Exemplo 3: Procuraremos explicar agora o algoritmo usual prático da divisão, calculando o quociente e o resto quando $a = 351$ e $b = 8$. Numa primeira etapa, quando se faz

$$\begin{array}{r|l} 351 & 8 \\ \hline 31 & \end{array}$$

na verdade o 4 que aparece sob a chave não passa do algarismo das dezenas do quociente procurado, como se pode verificar a seguir:

$35 = 8 \cdot 4 + 3$ (algoritmo da divisão para 35 e 8) $\Rightarrow$
$\Rightarrow 350 = 8 \cdot 40 + 30$
$\Rightarrow 351 = 8 \cdot 40 + 31$

Usando agora o algoritmo com os números 31 e 8:

$$31 = 8 \cdot 3 + 7$$

Logo

$$351 = 8 \cdot 40 + 8 \cdot 3 + 7 = 8 \cdot 43 + 7$$

Voltando ao dispositivo prático:

$$\begin{array}{r|l} 351 & 8 \\ \hline 31 & 43 \\ \hline 7 & \end{array}$$

5. Sistemas de numeração posicionais — base

Em nosso sistema de numeração todo número n é um polinômio

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_r \cdot 10^r$$

onde $r \geqslant 0$ e os $a_i \in \{0, 1, 2, \ldots, 9\}$ $(i = 1, 2, \ldots, r)$ estão univocamente determinados. O numeral que representa n é escrito assim:

$$a_r a_{r-1} \ldots a_1 a_0$$

Por exemplo:

$$641 = 1 + 4 \cdot 10 + 6 \cdot 10^2$$

Mas o papel desempenhado pelo 10 em nosso sistema de numeração é apenas uma opção ou uma circunstância, como mostra o resultado a seguir.

TEOREMA 2 Seja b um número natural maior que 1 e seja $M = \{0, 1, 2, \ldots, b - 1\}$. Então todo número n pode ser representado univocamente da seguinte maneira:

$$n = a_0 + a_1 \cdot b + a_2 \cdot b^2 + \ldots + a_r \cdot b^r$$

onde $r \geqslant 0$, $a_i \in M$ $(i = 1, 2, \ldots, r)$ e $a_r \neq 0$.

Demonstração:

i A existência será provada por indução (segundo princípio) sobre n. Se $n < b$, então $n = n$ é a representação pretendida. Vamos tomar $n \geqslant b$ e admitir como hipótese que para todo q, $1 \leqslant q < n$, essa representação seja possível. Aplicando o algoritmo da divisão para n e b se obtém

$$n = bq + a_0 \ (a_0 \in M)$$

Note-se que não pode ocorrer $q \geqslant n$. De fato, como $b > 1$, então $bq > q$ e essa hipótese levaria a $bq > n$ e portanto a $bq + a_0 = n > n$. Logo $1 \leqslant q < n$ e pela hipótese de indução:

$$q = a_1 + a_2 b + \ldots + a_r b^{r-1} \ (a_i \in M;\ a_r \neq 0)$$

Conseqüentemente,

$$n = b(a_1 + a_2 b + \ldots + a_r b^{r-1}) + a_0 = a_0 + a_1 b + a_2 b^2 + \ldots + a_r b^r$$

conforme o enunciado.

ii A unicidade também será provada por indução sobre n e é trivial para $n < b$. Seja $n \geqslant b$ e suponhamos que a unicidade se verifique para todo q, $1 \leqslant q < n$. Suponhamos ainda que:

$$n = a_0 + a_1 b + \ldots + a_r b^r = a'_0 + a'_1 b + \ldots + a'_s b^s$$

onde, também, $a'_0, a'_1, \ldots, a'_s \in M$. Então:

$$n = b(a_1 + a_2 b + \ldots + a_r b^{r-1}) + a_0 =$$
$$b(a'_1 + a'_2 b + \ldots + a'_s b^{s-1}) + a'_0$$

Como $b > a_0$ e $b > a'_0$, o algoritmo de Euclides (unicidade) garante que $a_0 = a'_0$ e $a_1 + a_2 b + \ldots + a_r b^{r-1} = a'_1 + a'_2 b + \ldots + a'_s b^s = q$. Como $q < n$, então, pela hipótese de indução, $r - 1 = s - 1$ (do que segue $r = s$) e $a_1 = a'_1, a_2 = a'_2, \ldots, a_r = a'_r$. ■

Se cada um dos elementos do conjunto $M = \{0, 1, \ldots, b - 1\}$ é representado por um símbolo especial, então cada um desses símbolos é chamado *algarismo* do *sistema posicional de base b*. A proposição demonstrada torna válido representar cada número $n = a_0 + a_1 b + \ldots + a_r b^r$ pela seqüência dos algarismos que nele figuram da seguinte maneira:

$$n = (a_r a_{r-1} \ldots a_2 a_1)_b$$

No caso $b = 10$ omitem-se os parênteses e o índice.

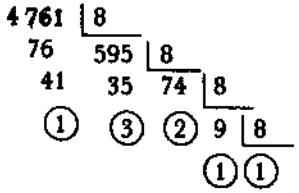
Quando $1 < b \leqslant 10$ é praxe usar os próprios algarismos indo-arábicos que sejam necessários para indicar os dígitos de 0 a $b - 1$. **Por exemplo:**

$$(2102)_3 = 2 + 0 \cdot 3 + 1 \cdot 3^2 + 2 \cdot 3^3 = 65$$
$$(10001)_2 = 1 + 0 \cdot 2 + 0 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4 = 17$$

Exemplo 4: Dado um número n escrito na base 10, a demonstração da proposição anterior (primeira parte) mostra como passá-lo para uma base b qualquer. Por exemplo, consideremos $n = 4\,761$ e $b = 8$. Apliquemos o algoritmo da divisão a 4 761 e 8:

$$4\,761 = 8 \cdot 595 + 1$$

Assim, na representação pretendida, o último algarismo (o das unidades) será o 1. A seguir a demonstração manda que se use a hipótese de indução. Isto equivale a repetir o raciocínio com o 595 e, se for o caso, fazer o mesmo com o quociente obtido. E assim por diante. Na prática pode-se proceder assim:



Portanto:

$$4\,761 = (11231)_8$$

Exemplo 5: Dado o número $(2102)_3$, para passá-lo à base 5, por exemplo, pode-se primeiro encontrar sua representação decimal e depois proceder como no exemplo anterior.

$$(2102)_3 = 2 + 0 \cdot 3 + 1 \cdot 3^2 + 2 \cdot 3^2 = 65$$

Então

$$\begin{array}{r|l} 65 & 5 \\ 15 & 13 \quad 5 \\ 0 & 3 \quad 2 \end{array}$$

Logo: $(2102)_3 = (230)_5$

5.1 Operações

O procedimento usado em nosso sistema de numeração para efetuar adições e subtrações, ou seja, somando em coluna as unidades, depois as dezenas acrescidas de algum eventual transporte da coluna anterior e assim por diante é muito fácil de justificar. Examinemos, por exemplo, a adição 47 + 24:

$$\begin{array}{r} {\scriptstyle 1} \\ 47 \\ +\ 24 \\ \hline 71 \end{array}$$

A soma das 7 unidades do primeiro número com as 4 do segundo é $11 = 1 + 1 \cdot 10$, uma unidade e uma dezena. Esta é então juntada às 4 dezenas de 47 e às duas de 24, obtendo-se as *7* dezenas da soma. Mas, embutidas nesse processo, estão as propriedades da adição em IN e, ainda, a propriedade distributiva. De fato:

$$\begin{aligned} 47 + 24 &= (4 \cdot 10 + 7) + (2 \cdot 10 + 4) = \\ &= (4 \cdot 10 + 2 \cdot 10) + (7 + 4) = (4 \cdot 10 + 2 \cdot 10) + (1 \cdot 10 + 1) = \\ &= (4 \cdot 10 + 2 \cdot 10 + 1 \cdot 10) + 1 = 7 \cdot 10 + 1 \end{aligned}$$

É claro que num sistema de base b posicional qualquer adição ou subtração pode ser efetuada da mesma maneira que o fazemos na base 10. Calculemos, por exemplo, $(4125)_6 + (1302)_6$:

$$\begin{array}{r} {\scriptstyle 1} \\ (4125)_6 \\ +\ (1302)_6 \\ \hline (5431)_6 \end{array}$$

Note-se que levamos em conta, na adição das unidades simples, que $5 + 2 = 7 = 1 \cdot 6 + 1 = (11)_6$ e por isso o resultado da coluna correspondente é 1, tendo sido transportado ainda, para a coluna seguinte, o algarismo 1.

Efetuemos agora a subtração $(2103)_4 - (1302)_4$:

$$\begin{array}{r} {\scriptstyle 1\,(11)_4} \\ (2\ 1\ 0\ 3)_4 \\ -\ (1\ 3\ 0\ 2)_4 \\ \hline (2\ 0\ 1)_4 \end{array}$$

Neste caso, como o número de unidades da terceira casa do minuendo é menor que o do subtraendo, foi preciso tomar emprestada uma unidade da casa seguinte. Como $(11)_4 = 1 \cdot 4^2 + 1 \cdot 4^3 = (1 + 1 \cdot 4) \cdot 4^2 = (3 + 2) \cdot 4^2 = 3 \cdot 4^2 + 2 \cdot 4^2$, o resultado na terceira coluna deve ser 2. Na prática o que se procura é o número que somado a 3 resulta $(11)_4 = 1 + 1 \cdot 4 = 5$

A multiplicação num sistema de numeração posicional de base b também pode ser efetuada segundo o procedimento usual da numeração decimal. E, assim como neste caso é preciso conhecer as tabuadas até a do 9, num sistema de base b tem que se partir de uma tábua de multiplicação (que pode estar na memória) para os números de 0 a b − 1. Calculemos por exemplo $(201)_3 \cdot (112)_3$. A tábua no caso é:

•	0	1	2
0	0	0	0
1	0	1	2
2	0	2	11

Assim, na base 3:

$$\begin{array}{r} 201 \\ 112 \\ \hline 1102 \\ 201+ \\ 201++ \\ \hline (100212)_3 \end{array}$$

uma vez que nesse caso $1 + 2 = 3 = 1 \cdot 3 + 0 = (10)_3$.

5.2 Critérios de divisibilidade

São bem conhecidos os critérios de divisibilidade da aritmética elementar. Mas, como justificá-los? De que maneira dependem eles de nosso sistema de numeração? Daremos resposta agora a essas perguntas em alguns casos. No capítulo III voltaremos ao assunto com uma ferramenta matemática mais potente para abordar a questão: a teoria das congruências.

Critério de divisibilidade por 2: Dado um número $n = a_0 + a_1 \cdot 10 + \ldots + a_r \cdot 10^r$, observando que toda potência 10^k ($k \geqslant 1$) é um número par, então:

$$n = a_0 + a_1(2q_1) + \ldots + a_r(2q_r) = a_0 + 2(a_1q_1 + \ldots + a_rq_r)$$

Ou seja

$$n = a_0 + 2q \ (q \in \mathbb{N})$$

Como 2q é divisível por 2, então n é divisível por 2 se, e somente se, a_0 é também divisível por 2. Ou seja, se e somente se $a_0 \in \{0, 2, 4, \ldots, 8\}$.

Critério de divisibilidade por 3: Primeiro observemos que o resto da divisão de 10^k por 3 é sempre 1, para todo $k \geqslant 0$. De fato, $10^0 = 1 = 3 \cdot 0 + 1$. Vamos supor $10^r = 3s + 1$, onde $r \geqslant 0$. Então $10^{r+1} = 10^r \cdot 10 = (3s + 1) \cdot (3 \cdot 3 + 1) = 3(9s) + 3s + 3 \cdot 3 + 1 = 3(9s + s + 3) + 1 = 3(10s + 3) + 1$.

Assim, para todo $n \in \mathbb{N}$:

$$\begin{aligned} n &= a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_r \cdot 10^r = \\ &= a_0 + a_1(3q_1 + 1) + a_2(3q_2 + 1) + \ldots + a_r(3q_r + 1) = \\ &= (a_0 + a_1 + \ldots + a_r) + 3(a_1q_1 + a_2q_2 + \ldots + a_rq_r) \end{aligned}$$

Em resumo:

$$n = (a_0 + a_1 + \ldots + a_r) + 3q$$

Portanto n é divisível por 3 se, e somente se, $a_0 + a_1 + \ldots + a_r$ é divisível por 3 (propriedade d_6).

Por exemplo: 1 761 é divisível por 3 já que 1 + 7 + 6 + 1 = 15 o é. Já o número 226 não é divisível por 3 posto que 2 + 2 + 6 = 10 não é múltiplo de 3.

A condição de divisibilidade de um número $n = a_0 + a_1 \cdot 10 + \ldots + a_r \cdot 10^r$ por 9 é semelhante à anterior: $9 \mid n \iff 9 \mid (a_0 + a_1 + \ldots + a_r)$. O motivo é que, também neste caso, $10^k = 9 \cdot s + 1$, para todo $k \in \mathbb{N}$.

Exemplo 6: Mostremos que um número $n = (a_ra_{r-1} \ldots a_1a_0)_{12}$ é divisível por 8 se, e somente se, o número $(a_1a_0)_{12}$ formado pelos dois últimos algarismos de n é divisível por 8.

Primeiro notemos que:

$$n = (a_1a_0)_{12} + a_2 \cdot 12^2 + a_3 \cdot 12^3 + \ldots + a_r \cdot 12^r$$

Mas, para $k \geqslant 2$, 12^k é divisível por 8. De fato, $12^2 = 144$ é múltiplo de 8. E se $12^s = 8 \cdot q_s$ ($s \geqslant 2$), então

$$12^{s+1} = 12^s \cdot 12 = (8q_s)12 = 8(12q_s)$$

Assim:

$$\begin{aligned} n &= (a_1a_0)_{12} + a_2(8q_2) + \ldots + a_r(8q_r) \\ &= (a_1a_2)_{12} + 8q \end{aligned}$$

Novamente a propriedade d_6 garante nossa afirmação.

EXERCÍCIOS

32. (Fuvest-77) Calcule quantos múltiplos de três, de quatro algarismos distintos, podem ser formados com 2, 3, 4, 6 e 9.

Resolução: Com os cinco algarismos dados podem ser formados apenas três subconjuntos de quatro algarismos cuja soma dos elementos é divisível por 3: {2, 3, 4, 6}, {2, 3, 4, 9} e {2, 4, 6, 9}. Cada um deles dá origem a 24 múltiplos de 3. Logo, a resposta é 3 × 24 = 72.

33. (UFMG-89) Seja n = ab000 um número não nulo, cujos cinco algarismos são a, b e três zeros. Se n é um quadrado perfeito e é divisível por 3, pode-se afirmar que a + b é igual a:

a) 1 b) 6 c) 8 d) 9 e) 12

34. (Cesgranrio-88) Se cdu é o maior número de três algarismos divisível por 11, então a soma c + d + u vale:

a) 22 b) 18 c) 20 d) 17 e) 16

Resolução: O maior número de três algarismos é 999, cuja divisão por 11 fornece resto 9. O número procurado é, então: 999 − 9 = 990. Resposta: 18.

35. Quantos números naturais entre 1 e 1 000 são divisíveis por 9? E quantos, entre 250 e 25 000, são divisíveis por 11?

Sugestão (1ª parte): O primeiro desses números é 9 e o último 999. Conte o número de termos da P.A. em que o primeiro termo é 9, o último é 999 e a razão é 9.

36. (Cesgranrio-89) Se n é o número de múltiplos de 6 compreendidos entre 92 e 196, então n é:

a) 14 b) 15 c) 16 d) 17 e) 18

37. Se n e a são naturais não nulos, quantos números naturais entre 1 e n são divisíveis por a?

38. Prove que:

a) a soma de dois números pares é par e que a soma de dois números ímpares também é par.

b) o produto de dois números naturais é ímpar se, e somente se, ambos são ímpares.

39. Prove que o quadrado de um número natural a é par se, e somente se, a é par.

Resolução: Se a é par, então $a = 2t$, para algum $t \in \mathbb{N}$; daí $a^2 = (2t)^2 = 4t^2 = 2(2t^2)$ é par. Para a recíproca suponhamos que a fosse ímpar, digamos $a = 2r + 1$; então $a^2 = 4r^2 + 4r + 1 = 2(2r^2 + 2r) + 1$ é ímpar, o que não é possível.

40. Mostre que $a + b + a^2 + b^2$ é par, para quaisquer $a, b \in \mathbb{N}$.

41. Se a, b e c são números naturais não nulos, prove que: $a|b \iff ac|bc$.

42. Prove que: $(1 + 2 + \ldots + n)|3(1^2 + 2^2 + \ldots + n^2)$, para todo $n \geqslant 1$.

Sugestão: Lembrar que $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$ e usar o exercício 25-a.

43. Prove por indução que:

a) $7|(3^{2n+1} + 2^{n+2})$, $\forall n \geqslant 0$

b) $9|(10^n + 3 \cdot 4^{n+2} + 5)$, $\forall n \geqslant 0$

c) $11|(2^{2n-1} \cdot 3^{n+2} + 1)$, $\forall n \geqslant 1$

d) $17|(3^{4n+2} + 2 \cdot 4^{3n+1})$, $\forall n \geqslant 0$

Resolução de d): Seja $a(n) = 3^{4n+2} + 2 \cdot 4^{3n+1}$

$n = 0 : a(0) = 3^2 + 2 \cdot 4 = 17$.

Logo $17|a(0)$.

Seja $r \geqslant 0$ e suponhamos que $17|a(r)$, ou seja: $3^{4r+2} + 2 \cdot 4^{3r+1} = 17q$ para algum $q \in \mathbb{N}$.

Daí $2 \cdot 4^{3r+1} = 17q - 3^{4r+2}$.

$n = r + 1$: $a(r+1) = 3^{4(r+1)+2} + 2 \cdot 4^{3(r+1)+1} =$

$= 3^{4r+6} + 2 \cdot 4^{3r+1} \cdot 4^3 = 3^{4r+6} + (17q - 3^{4r+2}) \cdot 64 =$

$= 17(64q) + 3^{4r+2} \cdot (3^4 - 64) = 17(64q + 3^{4r+2})$

44. Demonstre que de dois números pares consecutivos um é sempre divisível por 4.

45. (Unicamp-89) É possível encontrar dois números, ambos divisíveis por 7, tais que a divisão de um pelo outro deixe resto 39? Justifique a resposta.

46. Escreva o número 182 respectivamente nas bases 2, 8 e 12.

Obs.: No caso da base 12 use os algarismos indo-arábicos de 0 a 9 e as letras a e b para indicar, respectivamente, 10 e 11, se for preciso.

47. Efetue:

a) $(1034)_5 + (243)_5$

b) $(54302)_6 - (2134)_6$

c) $(1002)_4 \cdot (204)_4$

d) $(1025)_7 \cdot (1102)_7 + (21543)_7$

Resolução de d):

$$\begin{array}{r} (1025)_7 \\ (1102)_7 \\ \hline 2053 \\ 1025 \\ 1025 \\ \hline (1132553)_7 \\ + \quad (1132553)_7 \\ \quad (21543)_7 \\ \hline (1154426)_7 \end{array}$$

Notar que:

- $2 \cdot 5 = 10 = 1 \cdot 7 + 3 = (13)_7$
- $2 + 2 + 5 = 9 = 1 \cdot 7 + 2 = (12)_7$

onde levamos em conta que $1 + 5 + 5 = 11 = 1 \cdot 7 + 4 = (14)_7$.

48. Passe para o nosso sistema de numeração: $(10121)_3$, $(1042)_5$ e $(10\ ab)_{12}$, onde a representa "dez" e b "onze".

49. Construa a tábua de multiplicação referente à base 7.

50. Determine b em cada um dos seguintes casos:

a) $(104)_b = 8\,285$ b) $12\,551 = (30407)_b$.

51. Na divisão euclidiana de 802 por b o quociente é 14 e o resto r. Determine b e r.

Resolução: Por hipótese, $802 = b \cdot 14 + r$ $(r < b)$. Daí: $0 \leqslant$ $\leqslant 802 - 14 \cdot b = r < b$. Assim $14b \leqslant 802$ e $802 < 15b$. Os valores possíveis para esse sistema de desigualdades são $b = 54, 55, 56$ ou 57. Logo, respectivamente: $r = 46, 32, 18$ ou 4.

52. Mostre que para todo $n \in \mathbb{N}$ o número $\frac{n(n+1)}{2}$ está em $\mathbb{N}$ e que seu algarismo das unidades não pode ser 2, nem 4, nem 7 e nem 9.

Sugestão: Se o algarismo das unidades de $\frac{n(n+1)}{2}$ fosse um desses, o de $n(n+1)$ seria 4 ou 8. Mostre que isso não é possível.

53. Mostre que $(111)_b | (10101)_b$, para todo $b > 1$. Escreva o quociente da divisão em termos da base b.

54. Prove que: a) em todo sistema de numeração de base $b > 2$ o número $(121)_b$ é um quadrado perfeito; b) em todo sistema de numeração de base $b > 3$, o número $(1\ 331)_b$ é um cubo perfeito.

Resolução de a): $(121)_b = 1 + 2 - b + 1 - b^2 = (1 + b)^2$

55. Determinar as condições sobre os naturais b e d, $b > 1$ e $d > 1$, a fim de que: $(14)_b = (22)_d$.

56. Seja n um número natural e $n = (a_r a_{r-1} \ldots a_2 a_1)_5$ sua representação na base 5. Prove que: $4 | n \iff 4 | (a_0 + a_1 + \ldots + a_n)$. Generalize este resultado para uma base qualquer $b > 2$.

Sugestão: Veja como foi justificado o critério de divisibilidade por 9 no nosso sistema de numeração.

57. (Fuvest-88)

$$\begin{array}{cccc} 1 & a & b & c \\ & \times & & 3 \\ \hline a & b & c & 4 \end{array}$$

Acima está representada uma multiplicação, onde os algarismos a, b e c são desconhecidos. Qual o valor da soma a + b + c?

a) 5 c) 11 e) 17
b) 8 d) 14

58. O produto de um número de três algarismos por 7 termina à direita em 638. Ache esse número.

59. a) Na divisão euclidiana de a por b, o quociente é 106 e o resto 304. Qual o maior número de que se pode aumentar dividendo e divisor sem que o quociente se altere?
b) E se $q = 356$ e $r = 4\ 623$?

Resolução de a): Por hipótese $a = b \cdot 106 + 304$ $(304 < b)$. Acrescentando x ao dividendo e ao divisor, se 106 é o quociente da divisão de $a + x$ por $b + x$, então (segundo $4 \cdot 2$):

$$(b + x) \cdot 106 \leqslant a + x < (b + x) \cdot 107$$

Subtraindo $106b + x$ de cada um dos termos:

$$105x \leqslant 304 < b + 106x$$

A última desigualdade se verifica para todo x pois $304 < b$. Assim basta estudar $105x \leqslant 304$ que fornece as soluções $x = 0, 1$ ou 2. A resposta é então o número 2.

60. Se o algarismo das centenas do produto $a5 \cdot 164$ é 9, determine a (a representa um algarismo de nosso sistema de numeração).

61. Quantos números há num sistema de numeração de base b, formados de n algarismos? Qual o menor deles? (Escreva-o em função de b.)

6. Máximo divisor comum

DEFINIÇÃO 2 Sejam $a, b \in \mathbb{N}$. Um número $d \in \mathbb{N}$ se diz *máximo divisor comum* de a e b se: **i** $d | a$ e $d | b$; **ii** se c é um número natural tal que $c | a$ e $c | b$, então $c | d$.

Por exemplo, sejam $a = 6$ e $b = 8$. Indicando por D_x o conjunto dos divisores de $x \in \mathbb{N}$, então

$$D_6 = \{1, 2, 3, 6\} \quad \text{e} \quad D_8 = \{1, 2, 4, 8\}$$

do que segue:

$$D_6 \cap D_8 = \{1, 2\}$$

Observemos que: **i** $2 | 6$, $2 | 8$; **ii** se $c | 6$ e $c | 8$, então $c = 1$ ou $c = 2$ e portanto $c | 2$. Donde 2 é máximo divisor comum de 6 e 8.