1

INTRODUÇÃO

POR QUE ESTUDAR OS INTEIROS?

Para a maioria das pessoas, "número" quer dizer número inteiro positivo. Os inteiros relativos, os racionais, os reais e os complexos foram concebidos, aos poucos, à medida que as necessidades práticas ou teóricas o exigiam. Ainda hoje, os algoritmos usados para somar, multiplicar e dividir números racionais estão baseados nos algoritmos correspondentes para a soma, multiplicação e divisão de inteiros. Assim, as necessidades do dia-a-dia exigem o domínio das regras operacionais dos inteiros. Por isso, todo professor deve compreendê-las, a fim de poder ensiná-las.

Do ponto de vista histórico, é interessante observar que os racionais antecedem de muito a aceitação dos inteiros relativos. Os egípcios e os babilônios trabalhavam livremente com frações; os primeiros de maneira pesada e inconveniente, pois só admitiam frações do tipo $\frac{1}{n}$ (aceitavam também a fração 2/3). Os segundos, graças a sua notação posicional, com base 60, usavam livremente as frações sexagesimais, análogas às nossas frações decimais; estas frações sexagesimais foram utilizadas também pelos cientistas e matemáticos gregos sempre que necessitavam efetuar cálculos com números racionais. Já na Matemática pura, os gregos só reconheciam a existência de inteiros positivos, substituindo as frações por razões entre inteiros.

A história fascinante dos vários sistemas numéricos pode ser lida no livro de George Ifrah, "Números, a História de uma Grande Invenção". Em particular, a aceitação dos números negativos e complexos é interessante, pois mostra como idéias matemáticas importantes por vezes demoram até serem totalmente aceitas.

Os matemáticos, na tarefa de tornarem rigorosa a Matemática, a partir do século XIX, mostraram como os números relativos, racionais, reais e complexos podem todos ser construídos a partir dos números naturais. Nas palavras do matemático alemão Leopold Kronecker (1823, 1891), "Deus fez os números naturais. Todo o resto é trabalho do homem". Nesta generalização progressiva do conceito de número, a qual não seguiu a ordem histórica da utilização deles, a passagem realmente difícil é a de número racional para número real.

Isso pode ser feito pelo método dos cortes de Dedekind[1] ou usando as chamadas sucessões de Cauchy[2] de números racionais, como fez Peano[3].

Outra razão para estudarmos os inteiros é que eles são o protótipo de uma estrutura algébrica muito importante: a de anel comutativo com identidade (mais precisamente, de domínio de integridade). As generalizações sucessivas do conceito de número (racionais, reais e complexos) sempre preservaram esta estrutura. A crença de que ela deveria ser sempre mantida para qualquer tipo de "número" criado pelos matemáticos só foi rompida com o descobrimento dos quaternions pelo irlandês William Rowan Hamilton (1805, 1865), a partir de quem a Álgebra passou a ser encarada como o estudo das estruturas algébricas.

Ainda outra razão para o estudo dos inteiros é simplesmente estética. O estudo das propriedadas dos números primos tem se revelado fonte de belos e profundos resultados, cujo estudo algumas vezes muito contribuiu para o desenvolvimento da Matemática.

Além disso, o estudo dos inteiros é uma ótima maneira de exercitar o hábito de fazer conjecturas e demonstrações. A possibilidade de "experimentação" com os inteiros é muito grande, pelo menos tão grande, se não maior, do que com geometria. Recentemente, tem-se dado muita ênfase à necessidade de um ensino mais criativo em Matemática, que fuja ao modelo "definição, teorema, corolários", o qual é um dos responsáveis pela falta de interesse dos alunos pela Matemática. Neste sentido, os inteiros são um ótimo campo para experiências e exploração, a fim de desenvolver a criatividade dos alunos.

---

[1] Julius W. Richard Dedekind (1831, 1916), matemático alemão.

[2] Augustin-Louis Cauchy (1789, 1857), matemático francês, desenvolveu o rigor na Análise Matemática e no cálculo das séries. Tratou também das funções de uma variável complexa e criou a teoria dos grupos finitos. Também enunciou teoremas fundamentais sobre os determinantes e sobre equações diferenciais.

[3] Giuseppe Peano (1858, 1932), matemático italiano, professor da Universidade de Turim, fez trabalhos sobre a Análise Matemática e sobre os fundamentos da Matemática. Descobriu uma curva que passa por todos os pontos de um quadrado e axiomatizou os números naturais. Criou também uma língua universal.

CAPÍTULO 1

O Princípio da Indução Finita

Antes de abordarmos o estudo dos números naturais, estudaremos o **princípio da indução matemática**, ou **método da indução finita** [4]. Ele é uma técnica poderosa para demonstrar afirmações relativas aos números naturais. É particularmente útil quando suspeitamos que uma afirmação relativa aos números naturais é verdadeira e desejamos demonstrá-la.

Daremos, neste capítulo, o enunciado do princípio da indução, ilustraremos seu uso com alguns exemplos e proporemos exercícios para serem resolvidos empregando-o. No capítulo seguinte, mostraremos como esse princípio se insere na fundamentação da Aritmética e como as propriedades básicas das operações com números naturais dependem dele.

Seja $P(n)$ uma proposição relativa ao número natural n; por exemplo, $P(n)$ pode ser uma das afirmações:

a) $P(n)$: "Um conjunto A com n elementos tem exatamente 2^n subconjuntos distintos".

b) $P(n)$: "$\frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30}$ é um inteiro".

c) $P(n)$: "$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$ ".

d) $P(n)$: "O inteiro n, maior do que 1, pode ser escrito como um produto de números primos".

---

[4] A palavra "indução", em Matemática, tem significado diferente do que possui nas ciências experimentais. Nestas, baseando-se em casos conhecidos, o cientista "induz" resultados gerais, isto é, passa do particular ao geral. Em Matemática, "indução" é uma técnica que permite demonstrar resultados gerais.

e) $P(n)$: "A soma dos ângulos internos de um polígono convexo de n lados é igual a $2(n-2)$ retos".

É fácil dar muitos outros exemplos de afirmações verdadeiras relativas a números naturais. Em muitos casos, o princípio da indução finita, também chamado de princípio da indução matemática, permite demonstrá-las. Seu enunciado é o seguinte:

Princípio da indução finita. Dado o número inteiro positivo a, seja $P(n)$ uma asserção relativa aos inteiros $n = a, a+1, a+2, \ldots$

Se

a) $P(a)$ *é verdadeira*

e

b) *Supondo* $P(k)$ *verdadeira pudermos demonstrar que* $P(k+1)$ *é verdadeira*

então,

$P(n)$ *será verdadeira para todo* $n = a, a+1, a+2\ldots$

As demonstrações por indução finita ocorrem em todos os níveis da Matemática, do mais elementar aos mais avançados. Variam de extremamente simples a muito difíceis. Aqui, obviamente, trataremos de problemas de Matemática elementar, a nível do segundo grau.

Exemplo 1.1. *Demonstre, por indução em* n*, que a desigualdade de Bernoulli* [5]*:* $(1+x)^n \geq 1+nx$ *vale para todo* $n = 1, 2, \ldots$*, desde que se tenha* $1 + x > 0$*. (Aqui,* x *é um número real qualquer, inteiro ou não.)*

Com efeito, se $n = 1$, temos que $1 + x = 1 + x$, portanto a desigualdade é válida para $n = 1$.

Suponha agora que a desigualdade seja válida para um certo número natural n. Temos então $(1+x)^n \geq 1+nx$. Multiplicando ambos os membros desta desigualdade pelo número $1 + x$ (o qual é positivo, por hipótese) vem

$$(1+x)^n(1+x) \geq (1+nx)(1+x).$$

[5] Jacques Bernoulli (1654-1705), matemático suiço.

Lembrando que $(1+x)^n(1+x) = (1+x)^{n+1}$ e desenvolvendo o produto $(1+nx)(1+x)$, obtemos

$$(1+x)^{n+1} \geq 1 + (n+1)x + nx^2.$$

Como nx^2 não pode ser negativo, concluímos que

$$(1+x)^{n+1} \geq 1 + (n+1)x.$$

□

Exemplo 1.2. *Mostre que, para* $n = 1, 2, \ldots$, *vale*

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Seja $P(n)$ a asserção "a soma dos naturais $1 + 2 + \cdots + n$ é igual a $\frac{n(n+1)}{2}$ ". Temos:

1- $P(1)$ é válida, pois a soma dos naturais de 1 até 1 vale 1 e é claro que $1 = \frac{1\cdot(1+1)}{2}$.

2- Suponha agora que $P(k)$ seja válida, isto é, que a soma dos naturais de 1 a k seja igual a $\frac{k(k+1)}{2}$. Então a soma dos naturais de 1 a $k+1$ é

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

pois estamos aceitando a hipótese de indução, ou seja, que

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

Mas,

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

Logo a validez de $P(k)$ implica a de $P(k+1)$, o que conclui a demonstração. □

Exemplo 1.3. *Um conjunto* A *com* n *elementos possui* 2^n *subconjuntos distintos.*

Para provar esta afirmação, definamos $P(n)$: 'Úm conjunto A com n elementos tem exatamente 2^n subconjuntos distintos". (Aqui, n é um inteiro não-negativo.)

a) Se $n = 0$, então $A = \emptyset$, e o conjunto das partes de A é $P(A) = \{\emptyset\}$, donde o número de elementos de $P(A)$ é 1, ou seja, 2^0.

b) Suponha agora verdadeiro que qualquer conjunto com k elementos tem 2^k subconjuntos distintos. A partir disso, demonstraremos que qualquer conjunto com $k + 1$ elementos tem 2^{k+1} subconjuntos distintos.

Com efeito, seja $A = \{a_1, a_2, \ldots, a_k, a_{k+1}\}$ um conjunto com $(k + 1)$ elementos. Os subconjuntos de A dividem-se em dois tipos: os que contêm a_{k+1} e os que não contêm a_{k+1}. Contaremos:

1- O número de subconjuntos de A que não contêm a_{k+1}.

2- O número de subconjuntos de A que contêm a_{k+1}.

1- Seja $B = \{a_1, a_2, \ldots, a_k\}$. O número de subconjuntos de A que não contêm a_{k+1} é obviamente igual ao número de subconjuntos de B.

Ora, como B tem k elementos e estamos aceitando a hipótese de indução para conjuntos com k elementos, o número de subconjuntos de B é 2^k.

2- Um subconjunto de A que contém a_{k+1} é da forma $X \cup \{a_{k+1}\}$, onde X é um subconjunto de B. Então, o número dos subconjuntos de A que contêm a_{k+1} é igual ao número dos subconjuntos de B. Como B tem k elementos, vemos que o número de subconjuntos de A que contêm a_{k+1} é 2^k.

Assim, o número total de subconjuntos de A será $2^k + 2^k = 2^k(1+1) = 2^k \cdot 2 = 2^{k+1}$.

Portanto, admitindo a validez de $P(k)$, demonstramos que vale $P(k+1)$, isto é, que o número de subconjuntos de um conjunto com $k + 1$ elementos é 2^{k+1}. Isto conclui a demonstração por indução. □

Exemplo 1.4. *Demonstre que* $2^n < n!$, *para* $n \geq 4$.

Vamos usar o princípio da indução com $a = 4$.

Com efeito, se $n = 4$, então $2^4 = 16 < 4! = 24$.

Suponha agora que, para um inteiro $n \geq 4$, se tenha $2^n < n!$ Mostremos que daí decorre que $2^{n+1} < (n + 1)!$ Ora, como $2 < n + 1$, (lembre-se que $n \geq 4$) segue-se,

multiplicando membro a membro esta desigualdade pela desigualdade $2^n < n!$, que $2.2^n < (n+1)n!$, ou seja, $2^{n+1} < (n+1)!$, o que conclui a demonstração. □

O princípio da indução finita é particularmente útil quando, baseando-nos em experiências, acreditamos que um resultado é verdadeiro e desejamos prová-lo.

Exemplo 1.5. *Ache uma fórmula para a soma*

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

Como a soma dos n primeiros números naturais é dada por um polinômio do segundo grau em n, tentaremos ver se a soma dos quadrados dos n primeiros números ímpares é dada por um polinômio do grau 3. Por enquanto, isso não passa de uma experiência que estamos fazendo.

Suponhamos portanto que, exitem constantes A, B, C e D tais que a igualdade

$$1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = An^3 + Bn^2 + Cn + D$$

valha para todo número natural n e tentemos determinar os coeficientes A, B, C e D. Então,

para $n = 1$, temos

$$1 = A + B + C + D;$$

para $n = 2$, temos

$$10 = 8A + 4B + 2C + D;$$

para $n = 3$, temos

$$35 = 27A + 9B + 3C + D;$$

para $n = 4$, temos

$$84 = 64A + 16B + 4C + D.$$

Obtemos assim o sistema linear

$$A + B + C + D = 1$$

$$8A + 4B + 2C + D = 10$$

$$27A + 9B + 3C + D = 35$$

$$64A + 16B + 4C + D = 84,$$

cujas incógnitas são A, B, C e D.

Vemos facilmente que as soluções deste sistema são

$$A = \frac{4}{3}, \quad B = 0, \quad C = -\frac{1}{3}, \quad D = 0.$$

Isto nos leva a conjeturar que, para todo número natural n, vale

$$1^2 + 3^2 + \cdots + (2n-1)^2 = \frac{4}{3}n^3 - \frac{1}{3}n = \frac{1}{3}n(2n-1)(2n+1).$$

É importante perceber que *não* fizemos uma demonstração de que a fórmula acima é válida para todo n. Com efeito, o que provamos foi que a expressão da direita coincide com a da esquerda para $n = 1, 2, 3$ e 4. Tentaremos mostrar que isso é verdade para n qualquer. Para fazê-lo, usaremos indução finita.

Como já vimos que $P(1)$ é válida, começamos a indução supondo que a fórmula seja verdadeira para um inteiro positivo k:

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

Desejamos então mostrar que

$$1^2 + 3^2 + \cdots + (2(k+1)-1)^2 = \frac{1}{3} \cdot (k+1) \cdot (2(k+1)-1) \cdot (2(k+1)+1),$$

ou seja, que

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

Mas

$$\begin{aligned} 1^2 + 3^2 + \cdots + (2k+1)^2 &= (1^2 + 3^2 + \cdots + (2k-1)^2) + (2k+1)^2 = \\ &= \frac{1}{3} \cdot k \cdot (2k-1) \cdot (2k+1) + (2k+1)^2, \end{aligned}$$

pois estamos supondo que

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

Temos então

$$\frac{1}{3}\cdot k\cdot(2k-1)\cdot(2k+1)+(2k+1)^2=$$
$$=(2k+1)[\frac{1}{3}k(2k-1)+2k+1]=$$
$$=\frac{(2k+1)}{3}(2k^2+5k+3)=\frac{(2k+1)}{3}(2k+3)(k+1),$$

como queríamos demonstrar.

Podemos então afirmar que

$$1^2+3^2+\cdots+(2n-1)^2=\frac{4}{3}n^3-\frac{1}{3}n=\frac{1}{3}n(2n-1)(2n+1)$$

vale para qualquer n inteiro positivo. □

O perigo de fazer generalizações apressadas relativamente a asserções sobre inteiros fica evidenciado com o seguinte exemplo:

Exemplo 1.6. *Considere o polinômio* $p(n)=n^2-n+41$ *e a afirmação "o valor de* $p(n)$ *é sempre um primo para* $n=0,1,2,3,\ldots$".

Embora isso seja verdadeiro para $n=0,1,2,\ldots,40$, $p(41)=41^2-41+41=41^2$ não é primo, logo a afirmação não é verdadeira. □

Semelhantemente, a expressão $q(n)=n^2-79n+1601$ fornece primos para $n=1,2,\ldots,79$, mas $q(80)=80^2-79\cdot 80+1601=1681$ não é primo, pois é divisível por 41.

A moral da história é: Só aceite que uma afirmação sobre os inteiros é realmente verdadeira para todos os inteiros se isso houver de fato sido demonstrado!

O método da indução matemática como técnica de demonstração foi usado explicitamente pela primeira vez pelo italiano Francesco Maurolycus $(1494-1575)$. Pascal [6] o empregou para deduzir relações sobre os coeficientes binomiais no Triângulo de Pascal.

Na prática, usamos frequentemente o princípio da indução finita quando dizemos "... e assim sucessivamente". Ao fazermos isso, estamos reconhecendo, geralmente mentalmente ou após alguns cálculos, que o fenômeno estudado é bem regular, que a validade do

[6] Blaise Pascal (1623, 1662), matemático, místico e filósofo francês. Aos 17 anos escreveu um trabalho de Geometria Projetiva, o "Ensaio sobre as Cônicas". Pascal construíu uma máquina de calcular, fez a famosa experiência sobre o vácuo, em Paris, e desenvolveu o Cálculo das Probabilidades, explorando as propriedades do "Triângulo de Pascal". Usando os "indivisíveis" demonstrou vários resultados de cálculo integral. Abandonou a Matemática, dedicando-se à Filosofia e à defesa do Cristianismo.

resultado enunciado independe dos valores particulares de $\mathfrak{n}$ dados como exemplo. Isso é exatamente o princípio da indução finita.

Observações

1. Para habituar-se com o método de demonstração por indução é preciso praticá-lo muitas vezes, a fim de perder aquela vaga sensação de desonestidade que o principiante tem quando admite que o fato a ser provado é verdadeiro para $\mathfrak{n}$, antes de demonstrá-lo para $\mathfrak{n}+1$.

2. O método de indução é também usado para definir *indutivamente* ou *por recorrência* funções de $\mathbf{N}$ em um conjunto Y. Isso será visto no próximo capítulo.

3. Pratique também (com moderação) o exercício de descobrir o erro em paradoxos que resultam do uso inadequado do método de indução. Vejamos três desses sofismas:

Exemplo 1.7. *Seja* $\mathsf{P}(\mathfrak{n})$ *a afirmação: Se um conjunto de* $\mathfrak{n}$ *bolas contém uma bola preta, então todas as bolas do conjunto são pretas.*

Demonstraremos a verdade desta afirmação, usando o princípio da indução finita. Como no mundo certamente existe uma bola preta, teremos então demonstrado que todas as bolas do mundo são pretas!

1- $\mathsf{P}(1)$ certamente é verdadeira, pois se um conjunto de uma bola contém uma bola preta, todas as bolas do conjunto são pretas.

2- Aceitemos agora que $\mathsf{P}(\mathsf{k})$ seja verdadeira para um número natural k arbitrário, e mostremos que $\mathsf{P}(\mathsf{k}+1)$ é verdadeira.

Seja um conjunto $\{\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_{k+1}\}$ de $\mathsf{k}+1$ bolas, que contém alguma bola preta. Sem perda de generalidade, podemos supor que ela seja $\mathfrak{b}_1$. Considere agora o conjunto $\{\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_k\}$. Ele contém k bolas e uma delas ($\mathfrak{b}_1$) é preta. Então, pela hipótese de indução, todas as bolas do conjunto são pretas, ou seja, as bolas $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_k$ são todas pretas; em particular, $\mathfrak{b}_2$ é preta.

Consideremos agora o conjunto $\{\mathfrak{b}_2, \ldots, \mathfrak{b}_{k+1}\}$, que contém k elementos. Já demonstramos que $\mathfrak{b}_2$ é preta, logo este conjunto contém uma bola preta. Então, pela hipótese de indução, todas suas bolas são pretas. Isto é, $\mathfrak{b}_2, \ldots, \mathfrak{b}_{k+1}$ são pretas. Mas então *todas* as bolas $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_{k+1}$ são pretas.

Mostramos assim que todas as bolas do mundo são pretas! Mas isso é obviamente falso. Onde está nosso erro? Ele não é devido a termos suposto que a bola preta era b_1. Isso não traz nenhum problema. □

O exemplo seguinte é uma reformulação abstrata do anterior:

Exemplo 1.8. *Toda função* $f : X \to Y$*, cujo domínio é um conjunto finito,* X *é constante.*

Demonstração: Isto é obviamente verdadeiro se X tem apenas 1 elemento. Supondo a afirmação verdadeira para todos os conjuntos com n elementos, seja $f : X \to Y$ definida num conjunto X com $n+1$ elementos. Considere um elemento $a \in X$. Como $X' = X - \{a\}$ tem n elementos, f assume o mesmo valor $c \in Y$ em todos os elementos de X'. Agora troque a por um outro elemento $b \in X'$. Obtém-se $X'' = X - \{b\}$ um conjunto com n elementos (entre os quais a). Novamente pela hipótese de indução, f é constante e igual a c em X''. Logo $f(a) = c$ e daí $f : X \to Y$ é constante. (Aqui o erro reside no uso inadequado da hipótese de indução. O raciocínio empregado supõe implicitamente que X tem pelo menos 3 elementos. Na realidade, não vale a implicação $P(1) \Rightarrow P(2)$.) □

Vejamos outro exemplo de "demonstração" falsa usando o princípio da indução finita.

Exemplo 1.9. *Dois inteiros positivos quaisquer são iguais.*

Com efeito, seja $P(n)$ a proposição "se a e b são inteiros positivos tais que $max(a, b) = n$, então $a = b$ ".

Obviamente $P(1)$ é correta, pois se $max(a, b) = 1$, então $a = b = 1$.

Suponha agora que $P(r)$ seja verdadeira e sejam a e b inteiros quaisquer tais que $max(a, b) = r + 1$.

Considere então os inteiros $\alpha = a - 1$ e $\beta = b - 1$. Então, $max(\alpha, \beta) = r$, donde $\alpha = \beta$, logo $a = b$, e $P(r + 1)$ é verdadeira, o que conclui a demonstração por indução! □

Em geral, pseudo-demonstrações usando o princípio da indução finita, como os três exemplos acima, têm seus problemas nos casos em que n é pequeno, normalmente na passagem de $n = 1$ para $n = 2$, ou de $n = 2$ para $n = 3$. Você conhece outras "demonstrações" falsas por indução?

Em algumas situaçSes (como a do Teorema 1.1 que veremos a seguir), ao tentarmos provar um fato por meio do princípio da indução, sentimos que, usando apenas a validez

de $P(k)$, não parece possível provar a de $P(k+1)$. Em vez disso, para estabelecer $P(k+1)$ precisamos supor $P(1)$, $P(2)$, ..., $P(k)$ simultaneamente. Isto nos conduz ao **segundo princípio da indução**, que apresentaremos e usaremos agora, e cuja justificativa será dada no capítulo seguinte.

Segundo princípio da indução. Dado um inteiro a, seja $P(n)$ uma afirmação relativa aos inteiros n, $n = a, a+1, a+2, \ldots$

Se

1) $P(a)$ *é verdadeira*

e

2) *Para cada inteiro* $k \geq a$, *a validade de* $P(a), P(a+1), \ldots, P(k)$ *acarreta a validade de* $P(k+1)$,

então,

$P(n)$ *é válida para todos os inteiros* $n \geq a$.

Usaremos o segundo princípio da indução para demonstrar o seguinte resultado fundamental da Aritmética dos inteiros, o qual será muito usado no restante deste texto.

Teorema 1.1**.** *Qualquer inteiro* n *maior do que* 1 *pode ser escrito como um produto de primos.*

Demonstração: Considere a afirmação "o inteiro n ou é primo ou pode ser escrito como um produto de primos", para $n = 2,\ 3,\ 4,\ \ldots$ Usaremos a segunda forma do princípio da indução, tomando $a = 2$.

1- O número 2 é primo, logo vale $P(2)$.

2-Seja k um inteiro, $k \geq 2$. Suponha que a afirmação seja válida para todos os inteiros maiores que ou iguais a 2 e menores que ou iguais a k. Mostraremos que ela é válida para o inteiro $k+1$.

Se o inteiro $k+1$ é primo, nada há a demonstrar. Suponha portanto que $k+1 = a \cdot b$, onde a e b são inteiros maiores do que 1. Então obviamente $a < k+1$ e $b < k+1$. Logo, pela hipótese de indução, a se escreve como um produto de primos

$$a = p_1 \cdot p_2 \cdot \cdots \cdot p_s.$$

Analogamente, pela hipótese de indução, b se escreve como um produto de primos

$$b = q_1 \cdot q_2 \cdots q_t.$$

Então,

$$a \cdot b = p_1 \cdot p_2 \cdots p_s \cdot q_1 \cdot q_2 \cdots q_t,$$

um produto de primos, como queríamos demonstrar. □

Apresentamos mais um exemplo de utilização desta forma do princípio da indução: Sabe-se que, traçando diagonais internas que não se cortam, pode-se decompor qualquer polígono em triângulos justapostos. Isto é evidente quando o polígono é convexo: basta fixar um vértice e traçar as diagonais a partir dele. Se o polígono não é convexo, a prova requer mais cuidados [7].

O leitor pode experimentar com um polígono não-convexo e verificar que há muitas maneiras diferentes de decompô-lo em triângulos justapostos mediante diagonais internas. Mas vale o resultado seguinte, no qual usaremos o segundo princípio da indução [8].

Exemplo 1.10. *Qualquer que seja a maneira de decompor um polígono* P*, de* n *lados, em triângulos justapostos por meio de diagonais internas que não se intersectam, o número de diagonais utilizadas é sempre* $n - 3$.

Demonstração: Com efeito, dado n, suponhamos que a proposição acima seja verdadeira para todo polígono com menos de n lados. Seja então dada uma decomposição do polígono P, de n lados, em triângulos justapostos, mediante diagonais internas. Fixemos uma dessas diagonais. Ela decompõe P como reunião de dois polígonos justapostos P_1, de n_1 lados, e P_2, de n_2 lados, onde $n_1 < n$ e $n_2 < n$, logo a proposição vale para os polígonos P_1 e P_2. Evidentemente, $n_1 + n_2 = n + 2$.

---

[7] Vide LIMA, Elon Lages- "Meu Professor de Matemática e Outras Histórias", IMPA/VITAE, Rio de Janeiro, pag. 109.

[8] Para uma demonstração do mesmo fato usando boa-ordenação, veja "Revista do Professor de Matemática", vol. 19, pag. 31.

ENTRA A FIGURA V

As $\mathtt{d}$ diagonais que efetuam a decomposição de $\mathtt{P}$ se agrupam assim: $\mathtt{n}_1 - 3$ delas decompõem $\mathtt{P}_1$, $\mathtt{n}_2 - 3$ decompõem $\mathtt{P}_2$ e uma foi usada para separar $\mathtt{P}_1$de $\mathtt{P}_2$. Portanto

$$\mathtt{d} = \mathtt{n}_1 - 3 + \mathtt{n}_2 - 3 + 1 = \mathtt{n}_1 + \mathtt{n}_2 - 5.$$

Como $\mathtt{n}_1 + \mathtt{n}_2 = \mathtt{n} + 2$, resulta que $\mathtt{d} = \mathtt{n} - 3$. Isto completa a demonstração. □

Você certamente terá notado algo estranho em nossa apresentação do princípio da indução finita: Nós o enunciamos e o empregamos mas nada foi dito sobre como chegamos a ele. É um teorema? Se isso acontece, qual sua demonstração? É simplesmente uma regra empírica que a experiência mostrou funcionar? Enfim, o que é o princípio da indução finita? A resposta depende de como você encara os números naturais.

É possível construir os números naturais a partir da teoria dos conjuntos, como fez Richard Dedekind, que definiu conjunto finito como aquele que não admite bijeção sobre uma parte própria e número natural como o número cardinal de um conjunto finito. Outro ponto de vista, de maior simplicidade conceitual (e por isso quase universalmente adotado hoje em dia) é o de Giuseppe Peano, onde o princípio da indução aparece como um axioma, isto é, como uma das propriedades definidoras dos números naturais. Este é o ponto de vista que adotaremos no capítulo seguinte.

EXERCÍCIOS

1.1. Prove, por indução, que $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

1.2. Num polígono com $n \geq 6$ lados, o número de diagonais é maior do que n.

1.3. Prove, por indução, que $[(n+1)/n]^n < n$, para todo $n \geq 3$. (Sugestão: Observe que $(n+2)/(n+1) < (n+1)/n$ e eleve ambos os membros desta desigualdade à potência $n+1$.) Conclua daí que a seqüência $1, \sqrt{2}, \sqrt[3]{3}, \sqrt[4]{4}, \sqrt[5]{5}, \ldots$ é decrescente a partir do terceiro termo.

1.4. Para todo $n \in \mathbf{N}$, ponha $x_n = \left[\frac{(n+1)^2}{n(n+2)}\right]^n$ e prove, por indução, que se tem $x_n < \frac{n+2}{n+1}$. Conclua, a partir daí, que a seqüência de termo geral $(\frac{n+1}{n})^n$ é crescente. (Sugestão: observe que $x_{n+1} = (\frac{n+2}{n+1})^3 \cdot \frac{n}{n+3} \cdot x_n$ e use a hipótese de indução.)

1.5. Demonstre que a soma dos n primeiros números ímpares é n^2, ou seja, que $1 + 3 + 5 + \cdots + (2n-1) = n^2$.

1.6. Determine A^n se $A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$.

1.7. [A Torre de Hanói] São dados três suportes A, B e C. No suporte A estão encaixados n discos, cujos diâmetros, de baixo para cima, estão em ordem estritamente decrescente. Mostre que é possível, com $2^n - 1$ movimentos, transferir todos os discos para o suporte B, usando o suporte C como auxiliar, de modo que jamais, durante a operação, um disco maior fique sobre um disco menor.

ENTRA A FIGURA A

1.8. Demonstre que $2n^3 > 3n^2 + 3n + 1$ para $n \geq 3$.

1.9. Considere n retas em um plano. Mostre que o "mapa" determinado por elas pode ser colorido com apenas duas cores sem que duas regiões vizinhas tenham a mesma cor.

1.10. Mostre que, se $n \geq 2$, então $n^n > n!$

1.11. Ache uma expressão para $1^3 + 2^3 + 3^3 + \cdots + n^3$.

1.12. Mostre que $1\cdot2\cdot3+2\cdot3\cdot4+3\cdot4\cdot5+\cdots+n(n+1)(n+2) = n(n+1)(n+2)(n+3)/4$.

1.13. Mostre que $\frac{1}{1\cdot3} + \frac{1}{3\cdot5} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$.

1.14. Ache uma expressão para $1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n!$

1.15. Demonstre que $\frac{4^n}{n+1} < \frac{(2n)!}{(n!)^2}$, para todo número natural $n > 1$.

1.16. São dadas n retas "em posição geral" em um plano, isto é, tais que não há entre elas duas que sejam paralelas nem três que possuam um ponto comum. Ache uma expressão, em função de n, para o número de regiões que as n retas dadas determinam no plano.

1.17. Demonstre que se n é ímpar, então $x^n + a^n$ é divisível por $x + a$.

1.18. [Pequeno Teorema de Fermat] Demonstre que se p é um número primo, então $n^p - n$ é múltiplo de p.

1.19. Quantas são as sequências de n termos, todos pertencentes ao conjunto $\{0, 1\}$ e que não possuem dois zeros consecutivos?

1.20. Marcam-se n ($n > 1$) pontos distintos sobre uma circunferência. Demonstre que há $(k-1)(-1)^n + (k-1)^n$ modos de colorí-los, usando k cores distintas, de modo que não haja dois pontos consecutivos com a mesma cor.

1.21. Mostre que para cada número natural p maior ou igual a 3, existem naturais distintos n_1, n_2, ..., n_p, tais que $\frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_p} = 1$.

1.22. Seja A uma matriz quadrada tal que $A^2 = A$. Mostre que $A^n = A$.

1.23. Em um torneio disputado por n pessoas, cada uma delas joga com todas as outras. Não havendo empates, mostre que é possível rotular os jogadores como P_1, P_2, ..., P_n, de modo que P_1 venceu P_2, P_2 venceu P_3,..., P_{n-1} venceu P_n.

1.24. [A sequência de Fibonacci[9]] Um casal de coelhos adultos gera um casal de filhotes por mês, o qual, por sua vez, se reproduzirá, gerando também um casal de filhotes por mês, a partir de dois meses de idade. Tem-se, no mês 0, um casal de coelhos adultos. Supondo todos os coelhos imortais, determine

a) quantos casais de coelhos nascerão no mês 12;

b) quantos casais de coelhos nascerão no mês n;

c) qual a quantidade total de casais de coelhos existentes no mês n.

1.25. A sequência de Fibonacci, $F_1, F_2, \ldots, F_n, \ldots$ é definida por $F_1 = F_2 = 1$ e por $F_{n+2} = F_{n+1} + F_n$. Mostre que:

$F_n = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$.

1.26. Em um corredor há 1000 armários fechados, numerados sucessivamente de 1 a 1000. Um gaiato percorre o corredor e reverte a posição das portas de todos os armários. Em seguida, outro gaito reverte a posição das portas dos armários cujos números são múltiplos de 2. Um terceiro gaiato reverte em seguida a posição das portas dos armários cujos números são múltiplos de 3, e assim sucessivamente, para os múltiplos de 4, 5, 6, $\ldots$, 999 e 1000. Quais os números dos armários cujas portas estarão abertas ao fim do processo? Quantos são estes armários?

1.27. Dado um conjunto finito, mostre que é possível ordenar seus subconjuntos, por inclusão, de modo que cada subconjunto seja obtido a partir do anterior pelo acréscimo ou pela supressão de um único elemento.

---

[9] Leonardo de Pisa (1175(?), 1240(?)), matemático italiano, publicou em 1202 o Liber Abaci.

CAPÍTULO 2

NÚMEROS NATURAIS

A finalidade deste capítulo é abordar, de forma sucinta, a sequência dos números naturais, sobre a qual pode ser construído todo o edifício da Matemática como ciência dedutiva. Esta última frase já nos dá idéia da importância do assunto. Sua enorme relevância, entretanto, não decorre de complexas concepções filosóficas nem repousa sobre intricadas construções matemáticas. Pelo contrário, a compreensão do que são e do que significam os números naturais se faz a partir de idéias extremamente simples e espontâneas, como mostraremos a seguir. Esse entendimento, essa forma final bem-acabada de apresentar os números naturais, surgiu no final do século XIX e encontrou sua expressão mais límpida nos trabalhos de Richard Dedekind e Giuseppe Peano.

2.1 A SEQÜÊNCIA DOS NÚMEROS NATURAIS

Os números naturais constituem um modelo matemático, uma escala padrão, que nos permite a operação de contagem. A seqüência desses números é uma livre e antiga criação do espírito humano. Comparar conjuntos de objetos com essa escala abstrata ideal é o processo que torna mais precisa a noção de quantidade; esse processo (a contagem) pressupõe portanto o conhecimento da seqüência numérica. Familiarizarmo-nos com tal seqüência é nosso objetivo imediato.

Sabemos que os números naturais são

$$1, 2, 3, 4, 5, \ldots$$

A totalidade desses números constitui um conjunto, que indicaremos com o símbolo $\mathbf{N}$ e que chamaremos de *conjunto dos números naturais.* Portanto

$$\mathbf{N} = \{1, 2, 3, 4, 5, \ldots\}.$$

Evidentemente, o que acabamos de dizer só faz sentido quando já se sabe o que é um número natural. Nos parágrafos seguintes, vamos fazer de conta que esse conceito nos é desconhecido e procuraremos investigar o que há de essencial na seqüência $1, 2, 3, 4, 5, \ldots$

Deve-se a Peano a constatação de que se pode elaborar toda a teoria dos números naturais a partir de quatro fatos básicos, conhecidos atualmente como os *axiomas de Peano.* Noutras palavras, o conjunto $\mathbf{N}$ dos números naturais possui quatro propriedades fundamentais, das quais resultam, como conseqüências lógicas, todas as afirmações verdadeiras que se podem fazer sobre esses números.

Começaremos nosso estudo com o enunciado e a apreciação do significado dessas quatro proposições fundamentais a respeito dos números naturais.

2.2 OS AXIOMAS DE PEANO

Um matemático profissional, em sua linguagem direta e objetiva, diria que o conjunto $\mathbf{N}$ dos números naturais é caracterizado pelas seguintes propriedades:

A. Existe uma função $\mathsf{s} : \mathbf{N} \to \mathbf{N}$, que associa a cada $\mathtt{n} \in \mathbf{N}$ um elemento $\mathsf{s}(\mathtt{n}) \in \mathbf{N}$, chamado o *sucessor* de $\mathtt{n}$;

B. A função $\mathsf{s} : \mathbf{N} \to \mathbf{N}$ é injetiva;

C. Existe um único elemento 1 no conjunto $\mathbf{N}$ tal que $1 \neq \mathsf{s}(\mathtt{n})$ para todo $\mathtt{n} \in \mathbf{N}$;

D. Se um subconjunto $\mathsf{X} \subset \mathbf{N}$ é tal que $1 \in \mathsf{X}$ e $\mathsf{s}(\mathsf{X}) \subset \mathsf{X}$ (isto é, $\mathtt{n} \in \mathsf{X} \Rightarrow \mathsf{s}(\mathtt{n}) \in \mathsf{X}$), então $\mathsf{X} = \mathbf{N}$.

(Observe que, como estamos chamando de $\mathbf{N}$ o conjunto dos números naturais, a notação $\mathtt{n} \in \mathbf{N}$ significa que $\mathtt{n}$ é um número natural.)

As afirmações **A, B, C** e **D** são os **axiomas de Peano.** A notação $\mathsf{s}(\mathtt{n})$ é provisória. Depois de definirmos adição, escreveremos $\mathtt{n} + 1$ em vez de $\mathsf{s}(\mathtt{n})$.

Como concessão à fraqueza humana, nosso matemático nos faria a gentileza de reformular os axiomas de Peano em linguagem corrente, livre de notação matemática. E nos diria então que as afirmações acima significam exatamente o mesmo que essas outras:

A'. Todo número natural possui um único sucessor, que também é um número natural;

B'. Números naturais diferentes possuem sucessores diferentes; (Ou ainda: números que têm o mesmo sucessor são iguais.)

C'. Existe um único número natural que não é sucessor de nenhum outro. Este número é representado pelo símbolo 1 e chamado de "número um";

D'. Se um conjunto de números naturais contém o número 1 e, além disso, contém o sucessor de cada um de seus elementos, então esse conjunto coincide com $\mathbf{N}$, isto é, contém todos os números naturais.

A partir daí, retomamos a palavra para dizer que o sucessor de 1 chama-se "dois", o sucessor de dois chama-se "três", etc. Nossa civilização progrediu ao ponto em que temos um sistema de numeração, o qual nos permite representar, mediante o uso apropriado dos símbolos $0, 1, 2, 3, 4, 5, 6, 7, 8$ e 9, *todos* os números naturais. Além disso, nossa linguagem também fornece nomes para os primeiros termos da seqüência dos números

naturais. (Números muito grandes não têm nomes específicos, ao contrário dos menores, como "mil novecentos e noventa e quatro". Quem sabe, por exemplo, o nome do número de átomos do universo?)

Voltando a usar a notação $\mathtt{s}(\mathtt{n})$ para o sucessor do número natural $\mathtt{n}$, teremos então $2 = \mathtt{s}(1)$, $3 = \mathtt{s}(2)$, $4 = \mathtt{s}(3)$, $5 = \mathtt{s}(4)$, etc. Assim, por exemplo, a igualdade $2 = \mathtt{s}(1)$ significa apenas que estamos usando o símbolo 2 para representar o sucessor de 1.

A seqüência dos números naturais pode então ser indicada assim:

$$1 \xrightarrow{s} 2 \xrightarrow{s} 3 \xrightarrow{s} 4 \xrightarrow{s} 5 \ldots$$

As flechas ligam cada número ao seu sucessor.

Nenhuma flecha aponta para 1, pois este número não é sucessor de nenhum outro.

O diagrama acima diz muito sobre a estrutura do conjunto $\mathbf{N}$ dos números naturais. Mediante uma análise crítica, veremos agora qual o significado dos axiomas de Peano. Para melhor entendê-los buscaremos situações em que eles não valem.

O axioma A contém a idéia de que o conjunto dos números naturais é *discreto*. (Em oposição a *contínuo*, como o conjunto dos pontos de uma reta.)

Exemplo 2.1. *Uma situação em que não vale o axioma B é indicada no diagrama abaixo. Nele, tem-se o conjunto* $\mathsf{X} = \{1, 2, 3, 4\}$ *e a função* $\mathtt{s} : \mathsf{X} \to \mathsf{X}$*, com* $\mathtt{s}(1) = 2, \mathtt{s}(2) = 3, \mathtt{s}(3) = 4, \mathtt{s}(4) = 2$.

ENTRA FIGURA I

A função $\mathtt{s}$ não é injetiva, pois $\mathtt{s}(1) = \mathtt{s}(4)$, embora $1 \neq 4$.

Já o diagrama seguinte exibe um caso em que valem os axiomas A e B mas não vale C:

ENTRA FIGURA II

Aqui, temos $\mathsf{X} = \{1, 2, 3\}$ e a função $\mathsf{s} : \mathsf{X} \to \mathsf{X}$, dada por $\mathsf{s}(1) = 2$, $\mathsf{s}(2) = 3$, $\mathsf{s}(3) = 1$, é injetiva mas todo elemento $\mathfrak{n} \in \mathsf{X}$ é "sucessor" de algum outro elemento de X pois s é sobrejetora. □

Exemplo 2.2. *Neste exemplo, valem os axiomas* A *e* B *mas não valem* C *nem* D. *Ele se exprime pelo diagrama*:

ENTRA FIGURA III

Aqui, $\mathbf{N}$ é o conjunto dos números naturais mas a função $\mathsf{s} : \mathbf{N} \to \mathbf{N}$ é definida por $\mathsf{s}(\mathfrak{n}) = \mathfrak{n} + 2$. Então não vale o axioma C porque os elementos 1 e 2 gozam ambos da propriedade de não serem da forma $\mathsf{s}(\mathfrak{n})$ para nenhum $\mathfrak{n} \in \mathbf{N}$.

Tampouco vale o axioma D porque se considerarmos o conjunto $\mathsf{X} = \{1, 3, 5, \ldots\}$ formado pelos números ímpares, veremos que vale $1 \in \mathsf{X}$ e, além disso, $\mathfrak{n} \in \mathsf{X} \Rightarrow \mathsf{s}(\mathfrak{n}) = \mathfrak{n} + 2 \in \mathsf{X}$ mas não se tem $\mathsf{X} = \mathbf{N}$. □

Um exemplo em que valem os axiomas A, B e C mas falha o axioma D é proposto no Exercício 2.1.

Evidentemente, ao apresentarmos estes contra-exemplos estamos violando o trato de não admitir conhecimento algum sobre os números naturais. Note-se porém que as considerações acima não fazem parte da teoria. Elas servem apenas para ajudar a compreensão e delimitar o alcance dos axiomas.

2.3 O AXIOMA DA INDUÇÃO

Um dos axiomas de Peano, o último, possui claramente uma natureza mais elaborada do que os demais. Ele é conhecido como o *axioma da indução*. Dado o seu maior grau de complexidade, e dada também sua grande importância, faremos dele uma análise mais detida, acompanhada de comentários.

O significado informal do axioma D é que todo número natural pode ser obtido a partir de 1 por meio de repetidas aplicações da operação de tomar o sucessor. Assim, por exemplo, 3 é o sucessor do sucessor de 1, 4 é o sucessor do sucessor do sucessor de 1, etc.

Para se estudar melhor o axioma da indução é útil reexaminar o Exemplo 2.2, no qual $\mathbf{N} = \{1, 2, 3, \ldots\}$ mas a função $\mathsf{s} : \mathbf{N} \to \mathbf{N}$ foi modificada, pondo-se $\mathsf{s}(\mathfrak{n}) = \mathfrak{n} + 2$. Então, se começarmos com 1 e a este número aplicarmos repetidamente a operação de tomar o "sucessor" (nesta nova acepção) obteremos $\mathsf{s}(1) = 3,\ \mathsf{s}(3) = 5,\ \mathsf{s}(5) = 7$, etc., e nunca chegaremos a qualquer número par. Portanto, o diagrama

ENTRA FIGURA IV

exibe uma função injetiva $\mathsf{s} : \mathbf{N} \to \mathbf{N}$ para a qual não é verdade que todo número natural $\mathfrak{n}$ pode ser obtido, a partir de 1, mediante repetidas aplicações da operação de passar de k para $\mathsf{s}(\mathsf{k})$. □

Dentro de um ponto de vista estritamente matemático, podemos reformular o axioma da indução do seguinte modo. Um subconjunto $\mathsf{X} \subset \mathbf{N}$ chama-se *indutivo* quando $\mathsf{s}(\mathsf{X}) \subset \mathsf{X}$, ou seja, quando $\mathfrak{n} \in \mathsf{X} \Rightarrow \mathsf{s}(\mathfrak{n}) \in \mathsf{X}$, ou ainda, quando o sucessor de qualquer elemento de X também pertence a X.

Dito isto, o axioma da indução afirma que o único subconjunto indutivo de $\mathbf{N}$ que contém o número 1 é o próprio $\mathbf{N}$.

No Exemplo 2.2, os números ímpares $1, 3, 5, \ldots$ formam um conjunto indutivo que contém o elemento 1 mas não é igual a $\mathbf{N}$.

O papel fundamental do axioma da indução na teoria dos números naturais e, mais geralmente, em toda a Matemática, resulta do fato de que ele pode ser visto como um método de demonstração, chamado o *método de indução matemática*, ou *princípio da indução finita*, ou *princípio da indução*, conforme explicaremos agora.

Seja P uma propriedade que se refere a números naturais. Um dado número natural pode gozar ou não da propriedade P.

Por exemplo, seja P a propriedade de um número natural $\mathtt{n}$ ser sucessor de outro número natural. Então 1 não goza da propriedade P, mas todos os demais números gozam de P.

O princípio da indução diz o seguinte:

Princípio da indução. *Seja* P *uma propriedade referente a números naturais. Se* 1 *goza de* P *e se, além disso, o fato de o número natural* $\mathtt{n}$ *gozar de* P *implicar que seu sucessor* $\mathtt{s}(\mathtt{n})$ *também goza de* P*, então todos os números naturais gozam da propriedade* P.

Para ver que o princípio da indução é verdadeiro (uma vez admitidos os axiomas de Peano) basta observar que, dada a propriedade P cumprindo as condições estipuladas no enunciado do princípio da indução, o conjunto X dos números naturais que gozam da propriedade P contém o número 1 e é indutivo. Logo $\mathsf{X} = \mathbf{N}$, isto é, todo número natural goza da propriedade P.

No que se segue, veremos diversos exemplos de demonstrações por indução. (Chama-se assim uma demonstração baseada no princípio da indução.) Pode-se mesmo dizer que todas as propriedades básicas dos números naturais são demonstradas por indução. Como não dispomos ainda dos instrumentos de trabalho para lidar com esses números (as operações fundamentais e a noção de ordem: "menor do que" e "maior do que") vamos ilustrar o método de prova por indução com um exemplo bem simples.

Exemplo 2.3. *Entre os axiomas de Peano não consta explicitamente a afirmação de que todo número é diferente do seu sucessor, a qual provaremos agora.*

Demonstração: Seja P esta propriedade. Mais precisamente, dado o número natural n, escrevamos $\mathsf{P}(\mathsf{n})$ para significar, abreviadamente, a afirmação $\mathsf{n} \neq \mathsf{s}(\mathsf{n})$. Então $\mathsf{P}(1)$ é verdadeira, pois $1 \neq \mathsf{s}(1)$, já que 1 não é sucessor de número algum; em particular, 1 não é sucessor de si próprio. Além disso, se supusermos $\mathsf{P}(\mathsf{n})$ verdadeira, isto é, se admitirmos que $\mathsf{n} \neq \mathsf{s}(\mathsf{n})$, então $\mathsf{s}(\mathsf{n}) \neq \mathsf{s}(\mathsf{s}(\mathsf{n}))$, pois a função $\mathsf{s} : \mathbf{N} \to \mathbf{N}$ é injetiva. Mas a afirmação $\mathsf{s}(\mathsf{n}) \neq \mathsf{s}(\mathsf{s}(\mathsf{n}))$ significa que $\mathsf{P}(\mathsf{s}(\mathsf{n}))$ é verdadeira. Assim, a verdade de $\mathsf{P}(\mathsf{n})$ acarreta a verdade de $\mathsf{P}(\mathsf{s}(\mathsf{n}))$. Pelo princípio da indução, todos os números naturais gozam da propriedade P, ou seja, são diferentes de seus sucessores. □

Nas demonstrações por indução, a hipótese de que a propriedade P é válida para o número natural n (da qual deve decorrer que P vale também para $\mathsf{s}(\mathsf{n})$) chama-se *hipótese de indução.*

Exemplo 2.4. *O princípio da indução não é utilizado somente como método de demonstração. Ele serve também para definir funções* $\mathsf{f} : \mathbf{N} \to \mathsf{Y}$ *que têm como domínio o conjunto* $\mathbf{N}$ *dos números naturais.*

Em geral, para se definir uma função $\mathsf{f} : \mathsf{X} \to \mathsf{Y}$ requer-se que seja dada uma regra bem determinada, a qual mostre como se deve associar a cada elemento $\mathsf{x} \in \mathsf{X}$ um único elemento $\mathsf{y} = \mathsf{f}(\mathsf{x}) \in \mathsf{Y}$.

Entretanto, no caso particular em que o domínio da função é o conjunto $\mathbf{N}$ dos números naturais, a fim de definir uma função $\mathsf{f} : \mathbf{N} \to \mathsf{Y}$ não é necessário dizer, de uma só vez, qual a receita que dá o valor $\mathsf{f}(\mathsf{n})$ para todo $\mathsf{n} \in \mathbf{N}$. Basta que se tenha conhecimento dos seguintes dados:

(1) O valor $\mathsf{f}(1)$;

(2) Uma regra que permita calcular $\mathsf{f}(\mathsf{s}(\mathsf{n}))$ quando se conhece $\mathsf{f}(\mathsf{n})$.

Esses dois dados permitem que se conheça $\mathsf{f}(\mathsf{n})$ para todo número natural n. (Diz-se então que a função f foi definida *por recorrência*.) Com efeito, se chamarmos de X o conjunto dos números naturais n para os quais se pode determinar $\mathsf{f}(\mathsf{n})$ o dado (1) acima nos mostra que $1 \in \mathsf{X}$ e o dado (2) assegura que $\mathsf{n} \in \mathsf{X} \Rightarrow \mathsf{s}(\mathsf{n}) \in \mathsf{X}$. Logo, pelo axioma da indução, tem-se $\mathsf{X} = \mathbf{N}$. □

Observação: Uma função $f : \mathbf{N} \to Y$ cujo domínio é o conjunto dos números naturais chama-se uma *seqüência* ou *sucessão* de elementos de Y. A notação usada para uma tal seqüência é $(y_1, y_2, \ldots, y_n, \ldots)$, onde se usa y_n em vez de $f(n)$ para indicar o valor da função f no número n. O elemento y_n chama-se n-*ésimo termo* da seqüência.

2.4 ADIÇÃO DE NÚMEROS NATURAIS

Nosso primeiro exemplo de uma função definida por recorrência é a *adição* de números naturais.

Para definir a adição, fixaremos um número natural arbitrário k e definiremos a soma $k + n$ para todo $n \in \mathbf{N}$.

Fixado $k \in \mathbf{N}$, a correspondência $n \mapsto k+n$ será uma função $f : \mathbf{N} \to \mathbf{N}$, $f(n) = k+n$, chamada "somar k". Ela se define por recorrência, a partir dos seguintes dados:

$$(1) \quad k + 1 = s(k),$$

$$(2) \quad k + s(n) = s(k + n).$$

Portanto, $k + 1$ é, por definição, o sucessor de k. E se conhecermos $k + n$ saberemos o valor de $k + s(n)$; por definição tem-se $k + s(n) = s(k + n)$. Isto nos permite conhecer $k + n$ para todo $n \in \mathbf{N}$.

A partir de agora, usaremos a notação definitiva $n + 1$ em vez de $s(n)$.

Usando as notações definitivas $n + 1$ em vez de $s(n)$ e $(k + n) + 1$ em vez de $s(k + n)$, a igualdade (2) se escreve então assim:

$$(2') \quad k + (n + 1) = (k + n) + 1.$$

Portanto as igualdades (1) e (2) ou, equivalentemente, (1) e (2') definem, por recorrência, a soma $k + n$ de dois números naturais quaisquer k e n.

As propriedades da adição de números naturais são provadas por indução. Vejamos dois exemplos:

Teorema 2.1. [Associatividade da adição] $k + (n + p) = (k + n) + p$, *para quaisquer* $k, n, p \in \mathbf{N}$.

Demonstração: Fixados arbitrariamente $k, n \in \mathbf{N}$, a associatividade $k + (n + p) = (k + n) + p$ é verdadeira quando $p = 1$, por definição. (Vide (2')) Supondo-a verdadeira para p, tem-se sucessivamente:

$$\begin{aligned} k + [n + (p + 1)] &= k + [(n + p) + 1] \quad \text{por (2')} \\ &= [k + (n + p)] + 1 \quad \text{novamente por (2')} \\ &= [(k + n) + p] + 1 \quad \text{pela hipótese de indução} \\ &= (k + n) + (p + 1) \quad \text{outra vez por (2')}. \end{aligned}$$

Segue-se então que a lei associativa $k + (n + p) = (k + n) + p$ é válida para quaisquer números naturais k, n, p. □

Teorema 2.2. [Comutatividade da adição] $k + n = n + k$ *para quaisquer* $k, n \in \mathbf{N}$.

Demonstração: A comutatividade $n + p = p + n$ se prova usando duas vezes o princípio da indução.

Primeiro consideramos o caso $p = 1$. A igualdade $n + 1 = 1 + n$ é obviamente verdadeira quando $n = 1$. Supondo-a válida para um certo valor de n, tem-se a hipótese de indução $n + 1 = 1 + n$. Somando 1 a ambos os membros desta igualdade e usando a associatividade, vem

$$(n + 1) + 1 = (1 + n) + 1 = 1 + (n + 1).$$

Segue-se que $n + 1 = 1 + n$ para todo $n \in \mathbf{N}$.

Vemos, portanto, que a comutatividade $n + p = p + n$ é verdadeira quando $p = 1$. Admitamos agora (hipótese de indução) que ela valha para um certo p e mostremos que isto acarreta sua validez para $p + 1$. Com efeito, temos sucessivamente

$$\begin{aligned} n + p &= p + n \quad \text{hipótese de indução} \\ (n + p) + 1 &= (p + n) + 1 \quad \text{somando 1 a ambos os membros} \\ n + (p + 1) &= (p + n) + 1 \quad \text{associatividade} \\ &= 1 + (p + n) \quad \text{comutatividade da soma com 1} \\ &= (1 + p) + n \quad \text{associatividade} \\ &= (p + 1) + n \quad \text{comutatividade da soma com 1.} \end{aligned}$$

Segue-se que $n + p = p + n$ para quaisquer $n, p \in \mathbf{N}$. □

Outra propriedade importante da adição é a demonstrada a seguir:

Teorema 2.3. [Lei do corte] *Para quaisquer números naturais* m, n, p, *se* $m + p = n + p$, *então* $m = n$.

Demonstração: Com efeito, de $m + 1 = n + 1$ segue-se que $m = n$ em virtude do axioma B de Peano. Logo a lei do corte vale para $p = 1$. Supondo-a válida para um certo número natural p (hipótese de indução), mostremos que se pode também cortar $p + 1$. Admitamos então que se tenha

$$m + (p + 1) = n + (p + 1).$$

Pela associatividade, esta igualdade equivale a

$$(m + p) + 1 = (n + p) + 1.$$

Cortando 1 de ambos os membros, vem

$$m + p = n + p.$$

Pela hipótese de indução, concluímos que

$$m = n.$$

Assim $m + (p + 1) = n + (p + 1) \Rightarrow m = n$ portanto a Lei do Corte é válida em geral. □

A lei do corte equivale à afirmação de que, para todo $k \in \mathbf{N}$, a aplicação $f_k : \mathbf{N} \to \mathbf{N}$, dada por $f_k(n) = n + k$, é injetiva.

2.5 ORDEM

A adição de números naturais permite introduzir uma relação de ordem em $\mathbf{N}$.

Definição: Dados os números naturais $\mathfrak{m}, \mathfrak{n}$ diremos que $\mathfrak{m}$ *é menor do que* $\mathfrak{n}$, e escreveremos

$$\mathfrak{m} < \mathfrak{n},$$

para significar que existe $\mathfrak{p} \in \mathbf{N}$ tal que $\mathfrak{n} = \mathfrak{m} + \mathfrak{p}$. Neste caso, diz-se também que $\mathfrak{n}$ *é maior do que* $\mathfrak{m}$ e escreve-se $\mathfrak{n} > \mathfrak{m}$ para exprimir que se tem $\mathfrak{m} < \mathfrak{n}$.

A notação $\mathfrak{m} \leq \mathfrak{n}$ significa que $\mathfrak{m} < \mathfrak{n}$ ou $\mathfrak{m} = \mathfrak{n}$.

Por definição tem-se portanto $\mathfrak{m} < \mathfrak{m} + \mathfrak{p}$ para quaisquer $\mathfrak{m}, \mathfrak{p} \in \mathbf{N}$. Em particular, $\mathfrak{m} < \mathfrak{m} + 1$. Segue-se também da definição da relação $<$ que $1 < \mathfrak{n}$ para todo número natural $\mathfrak{n} \neq 1$, pois, pelo axioma C, $\mathfrak{n} \neq 1$ implica que $\mathfrak{n}$ é sucessor de algum número natural $\mathfrak{m}$, ou seja, $\mathfrak{n} = \mathfrak{m} + 1 = 1 + \mathfrak{m}$, logo $\mathfrak{n} > 1$. Assim, 1 é o menor dos números naturais.

Provaremos a seguir as propriedades básicas da relação de ordem $\mathfrak{m} < \mathfrak{n}$ que definimos. A primeira delas é a *transitividade*.

Teorema 2.4. [Transitividade] *Se* $\mathfrak{m} < \mathfrak{n}$ *e* $\mathfrak{n} < \mathfrak{p}$*, então* $\mathfrak{m} < \mathfrak{p}$.

Demonstração: $\mathfrak{m} < \mathfrak{n},\ \mathfrak{n} < \mathfrak{p} \Rightarrow \mathfrak{n} = \mathfrak{m} + \mathfrak{k},\ \mathfrak{p} = \mathfrak{n} + \mathfrak{r} \Rightarrow \mathfrak{p} = (\mathfrak{m} + \mathfrak{k}) + \mathfrak{r} = \mathfrak{m} + (\mathfrak{k} + \mathfrak{r}) \Rightarrow \mathfrak{m} < \mathfrak{p}$. □

Outra importante propriedade da relação de ordem é que, dados dois números naturais diferentes $\mathfrak{m}$ e $\mathfrak{n}$, ou se tem $\mathfrak{m} < \mathfrak{n}$ ou então $\mathfrak{n} < \mathfrak{m}$. Esta propriedade pode ser reformulada de outra maneira, como segue.

Diremos que os números naturais $\mathfrak{m}$ e $\mathfrak{n}$ são *comparáveis* quando se tem $\mathfrak{m} = \mathfrak{n}$, ou $\mathfrak{m} < \mathfrak{n}$ ou $\mathfrak{n} < \mathfrak{m}$.

Podemos então enunciar o seguinte teorema.

Teorema 2.5. [Comparabilidade] *Todo número natural* $\mathfrak{n}$ *é comparável com qualquer número natural* $\mathfrak{m}$.

Demonstração: Isto se prova por indução. O número 1 é comparável com qualquer outro número natural pois já sabemos que que $1 < \mathfrak{m}$ para todo $\mathfrak{m} \neq 1$.

Suponhamos agora que o número $\mathfrak{n}$ seja comparável com todos os números naturais. Mostremos, a partir daí, que $\mathfrak{n}+1$ também tem essa propriedade. Com efeito, seja $\mathfrak{m} \in \mathbf{N}$ tomado arbitrariamente. Sabemos que se tem $\mathfrak{m} < \mathfrak{n}$, ou $\mathfrak{m} = \mathfrak{n}$ ou $\mathfrak{n} < \mathfrak{m}$. Examinemos cada uma dessas possibilidades:
Se for $\mathfrak{m} < \mathfrak{n}$ então $\mathfrak{m} < \mathfrak{n} + 1$.
Se for $\mathfrak{m} = \mathfrak{n}$, então $\mathfrak{m} < \mathfrak{n} + 1$.
Se for $\mathfrak{n} < \mathfrak{m}$ então $\mathfrak{m} = \mathfrak{n} + \mathfrak{p}$. Neste caso, há duas possibilidades. Ou se tem $\mathfrak{p} = 1$, donde $\mathfrak{m} = \mathfrak{n} + 1$, ou então $\mathfrak{p} > 1$, logo $\mathfrak{p} = 1 + \mathfrak{p}'$, e portanto $\mathfrak{m} = (\mathfrak{n} + 1) + \mathfrak{p}'$ e concluímos que $\mathfrak{n} + 1 < \mathfrak{m}$. Em qualquer hipótese, vemos que $\mathfrak{n} + 1$ é comparável com qualquer número natural $\mathfrak{m}$. Por indução, fica provada a comparabilidade de dois números naturais quaisquer $\mathfrak{m}, \mathfrak{n}$. □

A comparabilidade dos números naturais é complementada pela proposição abaixo.

Teorema 2.6. [Tricotomia] *Dados* $\mathfrak{m}, \mathfrak{n} \in \mathbf{N}$, *qualquer das afirmações* $\mathfrak{m} < \mathfrak{n}$, $\mathfrak{m} = \mathfrak{n}$, $\mathfrak{n} < \mathfrak{m}$ *exclui as outras duas.*

Demonstração: Se tivéssemos $\mathfrak{m} < \mathfrak{n}$ e $\mathfrak{m} = \mathfrak{n}$, então seria $\mathfrak{m} = \mathfrak{m} + \mathfrak{p}$, donde $\mathfrak{m} + 1 = \mathfrak{m} + \mathfrak{p} + 1$ e, cortando $\mathfrak{m}$, concluiríamos que $1 = \mathfrak{p} + 1$, um absurdo, pois 1 não é sucessor de $\mathfrak{p}$. Portanto $\mathfrak{m} < \mathfrak{n}$ (e, analogamente, $\mathfrak{n} < \mathfrak{m}$) é incompatível com $\mathfrak{m} = \mathfrak{n}$.

Do mesmo modo, se tivéssemos $\mathfrak{m} < \mathfrak{n}$ e $\mathfrak{n} < \mathfrak{m}$, então teríamos $\mathfrak{n} = \mathfrak{m} + \mathfrak{p}$ e $\mathfrak{m} = \mathfrak{n} + \mathfrak{k}$, do que resultaria $\mathfrak{n} = \mathfrak{n} + \mathfrak{k} + \mathfrak{p}$, logo $\mathfrak{n} + 1 = \mathfrak{n} + \mathfrak{k} + \mathfrak{p} + 1$, e cortando $\mathfrak{n}$ concluiríamos que $1 = \mathfrak{k} + \mathfrak{p} + 1$, um absurdo. □

O teorema seguinte mostra que $\mathfrak{n}$ e $\mathfrak{n} + 1$ são números consecutivos.

Teorema 2.7. *Não existem números naturais entre* $\mathfrak{n}$ *e* $\mathfrak{n} + 1$.

Demonstração: Se fosse possível ter $\mathfrak{n} < \mathfrak{p} < \mathfrak{n}+1$, teríamos $\mathfrak{p} = \mathfrak{n}+\mathfrak{k}$ e $\mathfrak{n}+1 = \mathfrak{p}+\mathfrak{r}$, logo $\mathfrak{n} + 1 = \mathfrak{n} + \mathfrak{k} + \mathfrak{r}$. Cortando $\mathfrak{n}$, obteríamos $1 = \mathfrak{k} + \mathfrak{r}$. Por definição, isto significaria $\mathfrak{k} < 1$, o que é absurdo, pois já vimos que $\mathfrak{k} \neq 1 \Rightarrow \mathfrak{k} > 1$. □

A conexão entre a relação de ordem e a operação de adição é dada pelo seguinte teorema:

Teorema 2.8. [Monotonicidade da Adição] *Se* $m < n$, *então* $m + p < n + p$.

Demonstração: Usando a definição de $<$, temos que $m < n \Rightarrow n = m + k \rightarrow n + p = (m + k) + p \Rightarrow m + p < n + p$. □

A recíproca da monotonicidade é a *lei do corte para desigualdades*: $m + p < n + p \Rightarrow m < n$. O leitor poderá prová-la por absurdo, usando a tricotomia e a própria monotonicidade.

2.6 BOA ORDENAÇÃO

Definição: Dado o subconjunto $A \subset \mathbf{N}$, diz-se que o número natural a é o *menor* (ou *primeiro*) *elemento* de A quando $a \in A$ e, além disso, $a \leq x$, para todos os elementos $x \in A$.

Por exemplo, 1 é o menor elemento de $\mathbf{N}$.

De agora em diante, dado $n \in \mathbf{N}$, indicaremos com I_n o conjunto dos números naturais p tais que $1 \leq p \leq n$. Assim, $I_1 = \{1\}$, $I_2 = \{1, 2\}$, $I_3 = \{1, 2, 3\}$, etc.

As propriedades da relação de ordem $m < n$ demonstradas na seção anterior para os números naturais (exceto o Teorema 1.4) são igualmente válidas para os números inteiros, racionais e, mais geralmente, para números reais quaisquer. Existe, porém, uma propriedade de suma importância que é válida para a ordem entre os números naturais, mas sem equivalente para números inteiros, racionais ou reais. Trata-se do

Teorema 2.9. **[Princípio da boa ordenação]** *Todo subconjunto não-vazio* $A \subset \mathbf{N}$ *possui um menor elemento.*

Demonstração: Sem perda de generalidade, podemos admitir que $1 \notin A$, pois caso contrário 1 seria evidentemente o menor elemento de A. O menor elemento de A, cuja existência queremos provar, deverá ser da forma $n + 1$, para um certo número natural n. Devemos pois encontrar um número natural n tal que $n + 1 \in A$ e, além disso, todos os elementos de A sejam maiores do que n, logo maiores do que $1, 2, \ldots, n$. Noutras palavras, procuramos um número natural n tal que $I_n \subset \mathbf{N} - A$ e $n + 1 \in A$. Com esse objetivo, consideramos o conjunto

$$X = \{n \in \mathbf{N}; I_n \subset \mathbf{N} - A\}.$$

Portanto, X é o conjunto dos números naturais n tais que todos os elementos de A são maiores do que n. Como estamos supondo que $1 \notin A$, sabemos que $1 \in X$. Por outro lado, como A não é vazio, nem todos os números naturais pertencem a X, ou seja, temos $X \neq \mathbf{N}$. Pelo axioma D, vemos que o conjunto X não é indutivo, isto é, deve existir algum $n \in X$ tal que $n+1 \notin X$. Isto significa que todos os elementos de A são maiores do que n mas nem todos são maiores do que $n+1$. Como não há números naturais entre n e $n+1$, concluímos que $n+1$ pertence a A e é o menor elemento de A. □

O teorema abaixo contém uma aplicação do princípio da boa ordenação.

Teorema 2.10**.** *Toda função monótona não-crescente* $f : \mathbf{N} \to \mathbf{N}$ *é constante a partir de um certo ponto. (Isto e, existe* $n_0 \in \mathbf{N}$ *tal que* $f(n) = f(n_0)$*, para todo* $n \geq n_0$*.)*

Demonstração: Seja $f(n_0)$ o menor elemento do conjunto $X = \{f(1), \ldots, f(n), \ldots\}$. Então $n > n_0 \Rightarrow f(n) \leq f(n_0)$ (porque a função f é monótona não-crescente) o que acarreta que $f(n) = f(n_0)$ (porque $f(n_0)$ é o menor elemento de X). □

Corolário. Não existem seqüências decrescentes $n_1 > n_2 > \ldots$ de números naturais.

Com efeito, do contrário, pondo $f(k) = n_k$, obteríamos uma função estritamente decrescente $f : \mathbf{N} \to \mathbf{N}$. □

O princípio da boa ordenação pode muitas vezes ser usado em demonstrações, substituindo o princípio da indução. Vejamos um exemplo desse uso.

Dissemos anteriormente que um subconjunto $X \subset \mathbf{N}$ chama-se *indutivo* quando $n \in X \Rightarrow n+1 \in X$, ou seja, quando X contém o sucessor de cada um dos seus elementos. O princípio da indução afirma que se um conjunto indutivo X contém o número 1 então X contém todos os números naturais.

Vamos usar o princípio da boa ordenação para provar que se um conjunto indutivo X contém o número a, então X contém todos os números naturais maiores do que a.

A prova desta afirmação se faz por absurdo, como ocorre em geral quando se usa a boa ordenação. Suponhamos, então, que existam números naturais maiores do que a não pertencentes ao conjunto indutivo X. Seja b o menor desses números. Como $b > a$, podemos escrever $b = c+1$, onde, pela definição de b, tem-se necessariamente $c \in X$. Mas, como X é indutivo, isto obriga que $b = c+1 \in X$, uma contradição. □

A proposição que acabamos de demonstrar pode ser reenunciada da seguinte forma:

Teorema 2.11**. [Princípio da indução generalizado]** *Seja* P *uma propriedadereferente a números naturais, cumprindo as seguintes condições*:

(1) O número natural $\mathfrak{a}$ goza da propriedade P;

(2) Se um número natural $\mathfrak{n}$ goza da propriedade P então seu sucessor $\mathfrak{n}+1$ também goza de P.

Então todos os números naturais maiores do que ou iguais a $\mathfrak{a}$ *gozam da propriedade* P.

□

Observação: No Capítulo 1, este teorema foi chamado de princípio da indução.

Exemplo 2.5. *Para exibir uma situação simples onde se emprega o princípio da indução generalizado, usaremos a multiplicação de números naturais, que será definida na seção 9.*

Trata-se de provar que $2\mathfrak{n}+1 < 2^{\mathfrak{n}}$, para todo $\mathfrak{n} \geq 3$. Esta afirmação, (que é falsa para $\mathfrak{n} = 1, 2$), vale quando $\mathfrak{n} = 3$. Supondo-a válida para um certo $\mathfrak{n}$, mostremos que daí decorre sua validez para $\mathfrak{n}+1$. Com efeito,

$$\begin{aligned} 2(\mathfrak{n}+1)+1 &= 2\mathfrak{n}+1+2 \\ &< 2^{\mathfrak{n}}+2 \quad \text{pela hipótese de indução} \\ &< 2^{\mathfrak{n}}+2^{\mathfrak{n}} \quad \text{pois} \quad 2^{\mathfrak{n}} = 2.2.\ldots.2 > 2.1.1\ldots.1 \\ &= 2^{\mathfrak{n}+1}. \end{aligned}$$

□

Exemplo 2.6. *Usando a desigualdade* $2\mathfrak{n}+1 < 2^{\mathfrak{n}}$*, que acabamos de provar para* $\mathfrak{n} \geq 3$*, podemos demonstrar que* $\mathfrak{n}^2 < 2^{\mathfrak{n}}$ *para todo* $\mathfrak{n} \geq 5$*, empregando novamente o princípio da indução generalizado.*

Demonstração: Com efeito, vale $5^2 < 2^5$ pois $25 < 32$. Supondo válida a desigualdade $n^2 < 2^n$ para um certo valor de n, daí segue-se que

$$\begin{aligned}(n+1)^2 &= n^2 + 2n + 1 \\ &< 2^n + 2n + 1 \quad \text{pela hipótese de indução} \\ &< 2^n + 2^n \quad \text{pelo exemplo anterior} \\ &= 2^{n+1}.\end{aligned}$$

Portanto $P(n) \Rightarrow P(n+1)$. Pelo princípio da indução generalizado, segue-se que $P(n)$ vale para todo $n \geq 5$. Evidentemente, a desigualdade $n^2 < 2^n$ é falsa para $n = 1, 2, 3, 4$. □

2.7 SEGUNDO PRINCÍPIO DA INDUÇÃO

Em algumas situações, ao tentarmos fazer uma demonstração por indução, na passagem de n para $n+1$, sentimos necessidade de admitir que a proposição valha não apenas para n e sim para todos os números naturais menores do que ou iguais a n. A justificativa de um raciocínio desse tipo se encontra no

Teorema 2.12**. [Segundo princípio da indução]** *Seja* $X \subset \mathbf{N}$ *um conjunto com a seguinte propriedade:*

Dado $n \in \mathbf{N}$*, se todos os números naturais menores do que* n *pertencem a* X*, então* $n \in X$*. Nestas condiçSes, o conjunto* X *é necessariamente igual a* $\mathbf{N}$*.*

Então $X = \mathbf{N}$*.*

Demonstração: Com efeito, supondo, por absurdo, que $X \neq \mathbf{N}$, isto é, que $\mathbf{N} - X \neq \emptyset$, seja n o menor elemento do conjunto $\mathbf{N} - X$, ou seja, o menor número natural que não pertence a X. Isto quer dizer que todos os números naturais menores do que n pertencem a X. Mas então, pela propriedade (I), n pertence a X, uma contradição. Segue-se que $\mathbf{N} - X = \emptyset$ e $X = \mathbf{N}$. □

Observação. Se um conjunto $X \subset \mathbf{N}$ goza da propriedade (I), para que um número natural n não pertencesse a X seria necessário que existisse algum número natural $r < n$ tal que $r \notin X$. Em particular, se $n = 1$, como não existe número natural menor do que 1, a hipótese $1 \notin X$ não pode ser cumprida. Noutras palavras, (I) já contém implicitamente

a afirmação de que $1 \in \mathsf{X}$. Assim, ao utilizar o segundo princípio da indução, não é preciso estipular que X contém o número 1.

Toda propriedade P que se refira a números naturais define um subconjunto $\mathsf{X} \subset \mathbf{N}$, a saber, o conjunto dos números naturais que gozam da propriedade P. (E reciprocamente, todo conjunto $\mathsf{X} \subset \mathbf{N}$ define uma propriedade referente a números naturais, a saber, a propriedade de pertencer a X.) Deste modo, "propriedade" e "conjunto" são noções equivalentes.

Por isso, é natural que o segundo princípio da indução possua a formulação seguinte, onde ele aparece como o

Teorema 2.13**. [Segundo método de demonstração por indução]** *Seja* P *uma propriedade referente a números naturais. Dado* $\mathfrak{n} \in \mathbf{N}$*, se a validade de* P *para todo número natural menor do que* $\mathfrak{n}$ *implicar que* P *é verdadeira para* $\mathfrak{n}$*, então* P *é verdadeira para todos os números naturais.*

Demonstração: Com efeito, nas condições do enunciado, o conjunto X dos números naturais que gozam da propriedade P satisfaz a condição (I) do segundo princípio da indução, logo $\mathsf{X} = \mathbf{N}$ e P vale para todos os números naturais. □

2.8 NÚMEROS CARDINAIS

Até agora, não há nenhuma relação entre o processo de contar e os números naturais. No entanto, historicamente, estes números surgiram da contagem de objetos discretos. Como recuperar, em um contexto matemático, esta relação básica entre os números naturais e a contagem?

Lembremos que, dado $n \in \mathbf{N}$, escrevemos $I_n = \{p \in \mathbf{N}; p \leq n\}$, portanto $I_n = \{1, 2, \ldots, n\}$.

Uma *contagem* dos elementos de um conjunto não-vazio X é uma bijeção $f : I_n \to X$. O número natural n chama-se então o *número cardinal*, ou a *cardinalidade*, ou o *número de elementos* do conjunto X. Diz-se também que X *possui* n *elementos*.

Dada uma contagem $f : I_n \to X$, podemos por $x_1 = f(1), x_2 = f(2), \ldots, x_n = f(n)$ e escrever $X = \{x_1, x_2, ..., x_n\}$. O conjunto X chama-se um *conjunto finito* quando existe $n \in \mathbf{N}$ tal que X possui n elementos.

Um exemplo óbvio de conjunto finito é I_n. Evidentemente, a função identidade $f : I_n \to I_n$ é uma contagem, logo I_n possui n elementos.

Um conjunto X diz-se *infinito* quando não é finito. Isto significa que para nenhum $n \in \mathbf{N}$ pode existir uma bijeção $f : I_n \to X$.

Um exemplo de conjunto infinito é o próprio conjunto $\mathbf{N}$ dos números naturais, pois nenhuma função $f : I_n \to \mathbf{N}$ pode ser sobrejetiva, não importa qual n se tome. De fato, dada f, tomamos $k = f(1) + f(2) + \cdots + f(n)$ e vemos que $k > f(x)$ para todo $x \in I_n$, logo $k \notin f(I_n)$, e f não é sobrejetiva.

A fim de que não haja ambigüidade quando se falar do número de elementos de um conjunto finito X, é necessário provar que todas as contagens de X fornecem o mesmo resultado.

Noutras palavras, dado o conjunto X, os números naturais m, n e as bijeções $f : I_m \to X$, $g : I_n \to X$, devemos mostrar que se tem $m = n$.

Começamos observando que se f e g são bijeções, então $\phi = g^{-1} \circ f : I_m \to I_n$ também é uma bijeção. Basta portanto provar o seguinte:

Teorema 2.14**.** *Dados* $m, n \in \mathbf{N}$*, se* $\phi : I_m \to I_n$ *é uma bijeção, então* $m = n$*.*

Demonstração: Com efeito, chamemos de X o conjunto dos números naturais n que têm a seguinte propriedade: só existe uma bijeção $\phi : I_m \to I_n$ quando $m = n$. Evidentemente, $1 \in X$. Suponhamos agora que $n \in X$. Dada uma bijeção $\phi : I_{m+1} \to I_{n+1}$, duas coisas podem acontecer. Primeira: $\phi(m+1) = n+1$. Neste caso, a restrição $\phi : I_m \to I_n$ é uma bijeção, logo $m = n$, donde $m+1 = n+1$. Segunda: $\phi(m+1) = b$, com $b < n+1$. Neste caso, consideramos $a = \phi^{-1}(n+1)$ e definimos uma nova bijeção $\psi : I_{m+1} \to I_{n+1}$, pondo $\psi(m+1) = n+1$, $\psi(a) = b$ e $\psi(x) = \phi(x)$ para os demais elementos $x \in I_{m+1}$. Então recaímos no caso anterior e novamente concluímos que $m+1 = n+1$. Isto mostra que $n \in X \Rightarrow n+1 \in X$, logo $X = \mathbf{N}$ e a unicidade do número cardinal de um conjunto finito fica demonstrada. □

Agora os números naturais não são apenas elementos do conjunto-padrão $\mathbf{N}$, mas servem também para responder perguntas do tipo "quantos elementos tem o conjunto X?", ou seja, podem ser usados tanbém como números cardinais.

A adição de números naturais se relaciona com a cardinalidade dos conjuntos por meio da seguinte proposição.

Teorema 2.15**.** *Sejam X, Y conjuntos finitos disjuntos. Se X tem m elementos e Y tem n elementos, então $X \cup Y$ tem $m+n$ elementos.*

Demonstração: Com efeito, se $f : I_m \to X$ e $g : I_n \to Y$ são bijeções, definimos uma bijeção $h : I_{m+n} \to X \cup Y$ por $h(x) = f(x)$ se $1 \leq x \leq m$ e $h(m+x) = g(x)$ se $1 \leq x \leq n$, o que conclui a demonstração. □

Prova-se, por indução, que todo subconjunto de um conjunto finito X é também finito e seu número de elementos é menor do que ou igual ao de X [10].

Um subconjunto $X \subset \mathbf{N}$ chama-se *limitado* quando existe algum $k \in \mathbf{N}$ tal que $n \in \mathbf{N} \Rightarrow n \leq k$ (ou seja, todo elemento de X é menor do que ou igual a k).

Teorema 2.16**.** *Todo subconjunto finito $X = \{n_1, n_2, \ldots, n_r\} \subset \mathbf{N}$ é limitado.*

[10] Veja E. L. LIMA, "Análise Real", IMPA, Rio de Janeiro, vol 1, pag. 5.

Demonstração: Com efeito, tomando $k = n_1 + \cdots + n_r$ vemos imediatamente que k é maior do que qualquer elemento de X. □

Usando o fato de que todo subconjunto de um conjunto finito também é finito, podemos provar que, reciprocamente, todo subconjunto limitado $X \subset \mathbf{N}$ é finito. Com efeito, se X é limitado, então existe $k \in \mathbf{N}$ tal que $n \in X \to n \leq k$. Isto significa que todo número n pertencente a X pertence também ao conjunto finito $I_k\{1, 2, \ldots, k\}$, ou seja, que $X \subset I_k$, logo X é finito. □

Dado o conjunto $X \subset \mathbf{N}$, se o número natural k é maior do que ou igual a qualquer elemento de X, diz-se que k é uma *cota superior* do conjunto X. Assim, os conjuntos limitados $X \subset \mathbf{N}$ (ou seja, os finitos) são aqueles que possuem cotas superiores.

Se $X \subset \mathbf{N}$ é um conjunto limitado (isto é, finito), o princípio da boa ordenação assegura que entre os números naturais k que são cotas superiores de X existe um menor de todos. Esta menor cota superior de X pertence necessariamente ao conjunto X e é, portanto, o maior elemento de X. Assim, todo conjunto limitado (isto é, finito) de números naturais possui um elemento máximo.

É conveniente incluir, por definição, o conjunto vazio entre os conjuntos finitos e dizer que o seu número de elementos é *zero*. Embora zero não seja um número natural, ele passa a ser o número cardinal do conjunto vazio.

2.9 MULTIPLICAÇÃO DE NÚMEROS NATURAIS

Fixado um número natural $\mathtt{k}$, a *multiplicação* por $\mathtt{k}$ associa a todo número natural $\mathtt{n}$ o produto $\mathtt{nk}$ definido por indução, da seguinte maneira:

(1) $1 \cdot \mathtt{k} = \mathtt{k}$;

(2) $(\mathtt{n}+1) \cdot \mathtt{k} = \mathtt{n} \cdot \mathtt{k} + \mathtt{k}$.

O produto $\mathtt{n} \cdot \mathtt{k}$ escreve-se também $\mathtt{nk}$ e lê-se "$\mathtt{n}$ vezes $\mathtt{k}$". A definição acima diz portanto que uma vez $\mathtt{k}$ é igual a $\mathtt{k}$ e $\mathtt{n}+1$ vezes $\mathtt{k}$ é igual a $\mathtt{n}$ vezes $\mathtt{k}$ mais (uma vez) $\mathtt{k}$. Assim, por definição, $2 \cdot \mathtt{k} = \mathtt{k} + \mathtt{k}$, $3 \cdot \mathtt{k} = \mathtt{k} + \mathtt{k} + \mathtt{k}$, etc. Noutras palavras, $\mathtt{n} \cdot \mathtt{k}$ ($\mathtt{n}$ vezes $\mathtt{k}$) é a soma de $\mathtt{n}$ parcelas iguais a $\mathtt{k}$.

Como no caso da adição, prova-se que a multiplicação de números naturais goza das propriedades abaixo:

Associatividade: $(\mathtt{m} \cdot \mathtt{n}) \cdot \mathtt{k} = \mathtt{m} \cdot (\mathtt{n} \cdot \mathtt{k})$;

Comutatividade: $\mathtt{m} \cdot \mathtt{k} = \mathtt{k} \cdot \mathtt{m}$;

Distributividade: $\mathtt{m} \cdot (\mathtt{n} + \mathtt{k}) = \mathtt{m} \cdot \mathtt{n} + \mathtt{m} \cdot \mathtt{k}$;

Lei do Corte: $\mathtt{m} \cdot \mathtt{k} = \mathtt{n} \cdot \mathtt{k} \Rightarrow \mathtt{m} = \mathtt{n}$;

Monotonicidade: $\mathtt{m} < \mathtt{n} \Rightarrow \mathtt{m} \cdot \mathtt{k} < \mathtt{n} \cdot \mathtt{k}$.

Exemplo 2.7. *Segue-se da monotonicidade que só se pode ter* $\mathtt{m} \cdot \mathtt{n} = 1$ *quando* $\mathtt{m}$ *e* $\mathtt{n}$ *forem ambos iguais a* 1.

Demonstração: Com efeito, se tivermos, por exemplo, $\mathtt{m} > 1$, a monotonicidade implicará $\mathtt{m} \cdot \mathtt{n} > \mathtt{n}$ e, como $\mathtt{n} \geq 1$, daí se seguirá que $\mathtt{m} \cdot \mathtt{n} > 1$. □

Exemplo 2.8. *Decorre também da monotonicidade que se* $\mathtt{a} < \mathtt{b}$ *e* $\mathtt{c} < \mathtt{d}$ *então* $\mathtt{ac} < \mathtt{bd}$.

Demonstração: Com efeito, $\mathtt{a} < \mathtt{b} \Rightarrow \mathtt{ac} < \mathtt{bc}$ e $\mathtt{c} < \mathtt{d} \Rightarrow \mathtt{bc} < \mathtt{bd}$. Então, pela transitividade, $\mathtt{ac} < \mathtt{bd}$. □

EXERCÍCIOS

2.1. Construa um esquema de setas começando com os números ímpares, seguidos dos números pares divisíveis por 4 em ordem decrescente e, por fim, os pares não divisíveis por 4 em ordem crescente. Noutras palavras, tome $X = \mathbf{N}$ e defina $s : X \to X$ pondo $s(n) = n + 2$ se n não é divisível por 4, $s(n) = n - 4$ se n for múltiplo de 4. Mostre que $s : X \to X$ cumpre os axiomas A, B, C mas não D.

2.2. Defina, por recorrência, uma função $f : \mathbf{N} \to \mathbf{N}$ estipulando que $f(1) = 3$ e $f(n+1) = 5.f(n) + 1$. Dê uma fórmula explícita para $f(n)$.

2.3. Dê uma fórmula explícita para $f : \mathbf{N} \to \mathbf{N}$ sabendo que $f(1) = 1$, $f(2) = 5$ e $f(n + 2) = 3f(n + 1) - 2f(n)$.

2.4. Seja $X \subset \mathbf{N}$ um conjunto indutivo não-vazio. Mostre que existe $a \in \mathbf{N}$ tal que $X = \{n \in \mathbf{N}; n \geq a\}$.

2.5. Demonstre a lei do corte para desigualdades: $m + p < n + p \Rightarrow m < n$.

2.6. Demonstre as propriedades multiplicativa, associativa e comutativa da multiplicação de números naturais.

2.7. Mostre que vale a distributividade: $m.(n + k) = m.n + m.k$.

2.8. Mostre que vale a lei do corte: $m.k = n.k \to m = n$.

2.9. Mostre que vale a monotonicidade: $m < n \Rightarrow m.k < n.k$.

2.10. Use a distributividade de duas maneiras diferentes para calcular $(m + n)(1 + 1)$ e aplique em seguida a lei do corte para obter uma nova prova de que $m + n = n + m$.

2.11. Um conjunto $S \subset \mathbf{N}$, não-vazio, é limitado superiormente, se existe um natural k tal que para todo natural $x \in S$, então $x \leq k$. Mostre que todo conjunto S limitado superiormente possui um maior elemento. (Isto é, existe $m \in S$ tal que $x \leq m$, para todo $x \in S$).

2.12. Dado um conjunto finito, mostre que é possível ordenar seus subconjuntos, por inclusão, de modo que cada subconjunto seja obtido a partir do anterior pelo acréscimo ou pela supressão de um único elemento.

2.13. Demonstre, usando boa ordenação, o Exemplo 1.10.

CAPÍTULO 3

DIVISIBILIDADE E O TEOREMA FUNDAMENTAL DA ARITMÉTICA

Apresentaremos inicialmente algumas definições e resultados básicos da Aritmética dos números naturais que levam à definição fundamental de *número primo*. Todas estas idéias são usadas desde a escola elementar. Nosso objetivo é revê-las, sistematizá-las e explorá-las em exemplos e problemas interessantes.

3.1 DIVISIBILIDADE

Dizemos que o número natural $\mathtt{a}$ *divide* o número natural $\mathtt{b}$, o que representamos por $\mathtt{a}|\mathtt{b}$, se existe um número natural $\mathtt{c}$ tal que $\mathtt{b} = \mathtt{a} \cdot \mathtt{c}$. Dizemos então que $\mathtt{b}$ é um *múltiplo* de $\mathtt{a}$, ou que $\mathtt{a}$ *divide* $\mathtt{b}$, ou que $\mathtt{a}$ é um *fator* de $\mathtt{b}$ ou ainda que $\mathtt{a}$ é *divisor* de $\mathtt{b}$, e escrevemos $\mathtt{a}|\mathtt{b}$. Dizemos também que a *divisão* de $\mathtt{b}$ por $\mathtt{a}$ é *exata*. Na matemática grega, dizia-se que $\mathtt{a}$ "mede" $\mathtt{b}$, uma alusão clara ao fato de que então se trabalhava com grandezas (em nosso caso, o segmento de reta de comprimento $\mathtt{a}$ está contido exatamente $\mathtt{c}$ vezes no segmento de reta de comprimento $\mathtt{b}$).

Todo este capítulo está centrado em torno da noção de divisibilidade. O primeiro resultado que apresentamos é um critério, útil em demonstrações e problemas, que usa divisibilidade para decidir se dois números naturais são iguais.

Embora o *zero* não seja um número natural, nós o empregaremos por vezes, para simplificar enunciados e demonstraçSes.

Teorema 3.1**.** *Sejam* $\mathtt{a}$*, e* $\mathtt{b}$ *números naturais. Se* $\mathtt{a}$ *divide* $\mathtt{b}$ *e* $\mathtt{b}$ *divide* $\mathtt{a}$*, então* $\mathtt{a} = \mathtt{b}$*.*

Demonstração: Com efeito, se $a|b$, então existe um número natural c tal que $b = a \cdot c$. Se $b|a$, existe então um número natural d tal que $a = b \cdot d$.

Segue-se que $b = (bd)c = bdc$. Cortando d, vem $1 = dc$. Pelo Exemplo 2.7 concluímos que $d = 1$ e $c = 1$, donde $a = b$. □

Teorema 3.2. *Se* a, b *e* c *são números naturais e* $a|b$ *e* $a|c$, *então* $a|(b + c)$.

Demonstração: Com efeito, se $a|b$, então existe k_1 tal que $b = k_1 a$. Se $a|c$, existe k_2 tal que $c = k_2 a$. Assim, $b + c = k_1 a + k_2 a = (k_1 + k_2)a$, donde $a|(b + c)$, como queríamos demonstrar. □

A recíproca deste teorema nem sempre é verdadeira. É fácil achar números naturais a, b e c tais $a|(b + c)$ mas a não divide b e a não divide c; por exemplo, $4|(9 + 3)$, mas 4 não divide 9 ($4 \not| 9$) e 4 não divide 3 ($4 \not| 3$).

Pedimos que o leitor demonstre, como exercício, o seguinte teorema

Teorema 3.3. *Se* a, b *e* c *são números naturais tais que* $a|b$ *e* $b|c$, *então* $a|c$.

Um número natural chama-se *par* se é múltiplo de 2 e *ímpar* se não é múltiplo de 2.

3.2 OS PRIMOS E O TEOREMA FUNDAMENTAL DA ARITMÉTICA

Dizemos que um número natural é *primo* se ele é diferente de 1 e se os únicos divisores de $\mathtt{p}$ são 1 e $\mathtt{p}$. O menor primo é 2, pois seus únicos divisores são 1 e 2.

O conceito de número primo é fundamental em Teoria dos Números, a parte da Matemática que estuda as propriedades dos números inteiros. Alguns teoremas profundos e poderosos dizem respeito a números primos. Alguns dos problemas relativos aos primos têm enunciados enganosamente fáceis, mas cujas soluções se revelam diabolicamente difíceis.

Um fato importante, já conhecido dos matemáticos gregos, cuja demonstração se encontra nos *Elementos* de Euclides (Proposição XX, do Livro IX) é que *existe uma infinidade de primos*. Apresentaremos a demonstração deste fato após termos introduzido a divisão de números naturais.

O resultado a seguir, já demonstrado no Capítulo 1, (Teorema 1.1), é fundamental pois mostra o papel importante desempenhado pelos primos no estudo dos números naturais: qualquer número natural pode ser obtido como o produto de números primos. Além disso, a demonstração deste fato mostra a utilização do segundo princípio da indução. Devido a sua importância, repetimos a demonstração.

Exemplo 3.1. *Qualquer número natural* $\mathtt{n}$ *maior do que* 1 *pode ser escrito como um produto de primos.*

Demonstração: Considere a afirmação "$\mathtt{P}(\mathtt{n})$: o número natural $\mathtt{n}$ é primo ou então pode ser escrito como um produto de primos", para $\mathtt{n} = 2,\ 3,\ 4,\ \ldots$ Usaremos a segunda forma do princípio da indução, tomando $\mathtt{n} = 2$.

1- Como 2 é primo, $\mathtt{P}(2)$ é verdadeira.

2-Seja $\mathtt{k}$ um número natural com $\mathtt{k} \geq 2$. Suponha que a afirmação $\mathtt{P}(\mathtt{n})$ seja válida para todos os números naturais maiores que ou iguais a 2 e menores que ou iguais a $\mathtt{k}$. Mostraremos que ela é válida para o número natural $\mathtt{k}+1$.

Se $\mathtt{k}+1$ é primo, nada há a demonstrar. Se $\mathtt{k}+1$ não pe primo, então $\mathtt{k}+1 = \mathtt{a} \cdot \mathtt{b}$, onde $\mathtt{a}$ e $\mathtt{b}$ são números naturais maiores do que ou iguais a 2. É claro que , $\mathtt{a} < \mathtt{k}+1$ e

$b < k + 1$. Pela hipótese de indução, $P(a)$ e $P(b)$ são verdadeiras. Noutras palavras,

$$a = p_1 \cdot p_2 \cdot \cdots \cdot p_s$$

e

$$b = q_1 \cdot q_2 \cdots q_t$$

se escrevem ambos como produtos de primos. Então

$$k + 1 = a \cdot b = p_1 \cdot p_2 \cdots p_s \cdot q_1 \cdot q_2 \cdots q_t,$$

é um produto de primos, como queríamos demonstrar. □

Mostraremos a seguir que esta decomposição de um número natural em produto de números primos é "essencialmente única". Com isso, queremos dizer que se escrevermos

$$n = p_1^{\alpha_1}.p_2^{\alpha_2} \ldots p_k^{\alpha_k},$$

com os p_i distintos entre si, então qualquer outra decomposição do número natural n em um produto de potências de primos distintos entre si fornecerá exatamente os mesmos primos p_i elevados às potências α_i, com possíveis mudanças de ordem entre os p_i. Este resultado é conhecido como **teorema fundamental da Aritmética** e merece seu nome.

Para completar a demonstração do teorema fundamental da Aritmética, necessitamos de um resultado prévio:

Teorema 3.4**.** *Seja n um número natural cuja decomposição em fatores primos é essencialmente única. Suponha que $n = ab$ e que o primo p divide o produto ab (ou seja, divide n). Então ou p divide a ou p divide b. (Observe que a e b não são necessariamente primos.)*

Demonstração: Com efeito, se p não for fator primo nem de a nem de b, existem decomposições de a e de b que não contêm o fator primo p. Obtemos então uma decomposição de ab em fatores primos que não contém o primo p. Por outro lado, como $p|ab$, p comparece em alguma decomposição de ab em fatores primos. Assim, n admite duas decomposições em fatores primos essencialmente distintas, o que é uma contradição. □

Podemos agora demonstrar o teorema fundamental da Aritmética.

Teorema 3.5. *Todo número natural admite, de maneira essencialmente única, uma decomposição em produto de números primos.*

Demonstração: Com efeito, já mostramos, usando o segundo princípio da indução matemática, que existe uma tal decomposição. Resta mostrar que ela é única, a menos da ordem em que nela comparecem os fatores primos. Para fazer isso, usaremos o princípio da boa ordenação.

Suponha que existam números naturais que possam ser decompostos em produtos de primos segundo duas maneiras essencialmente distintas. Então, pelo princípio da boa ordenação, existe o *menor* destes, o qual chamaremos de $\mathfrak{m}$. Assim, $\mathfrak{m}$ pode ser escrito como

$$\mathfrak{m} = p_1 p_2 \cdots p_r$$

e como

$$\mathfrak{m} = q_1 q_2 \cdots q_s,$$

duas decomposições em fatores primos essencialmente distintas; além disso, qualquer número natural menor do que $\mathfrak{m}$ admite uma única decomposição em fatores primos, a menos da ordem destes fatores.

Podemos supor, sem perda de generalidade, que

$$p_1 \leq p_2 \leq \ldots \leq p_r,$$

$$q_1 \leq q_2 \leq \ldots \leq q_s.$$

Afirmamos que $p_1 \neq q_1$. Com efeito, suponha que $p_1 = q_1$. Então, como

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

usando a lei do cancelamento, segue-se que

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s.$$

O número natural acima, $p_2p_3\cdots p_r$, é menor do que m e tem duas decomposições em primos essencialmente distintas, o que é uma contradição. Assim, $p_1 \neq q_1$. Suponha, sem perda de generalidade, que $p_1 < q_1$ e considere o número natural

$$m' = m - p_1q_2q_3\cdots q_s.$$

Temos então que

$$m' = q_1q_2\cdots q_s - p_1q_2\cdots q_s = (q_1 - p_1)(q_2q_3\cdots q_s).$$

Como $q_1 > p_1$, vemos que m' é realmente um número natural. Além disso, segue-se da definição de m' que $m' < m$.

Assim, pela definição de m, vemos que m' se decompõe em produto de fatores primos de maneira essencialmente única.

Ora, como $m' = p_1p_2\cdots p_r - p_1q_2\cdots q_s = p_1(p_2p_3\cdots p_r - q_2q_3\cdots q_s)$, vemos que p_1 é fator primo de m' e então, como m' *se decompõe em produto de fatores primos de maneira essencialmente única*, segue-se que p_1 divide $(q_1 - p_1)$ ou p_1 divide $q_2q_3\cdots q_s$.

Como $p_1 < q_1 \leq q_2 \leq q_3 \leq \ldots \leq q_s$, todos os q_i são estritamente maiores do que p_1. Assim, p_1 não pode ser um dos fatores primos q_2, q_3,...,q_s. Ou seja, p_1 não é fator primo de $q_2q_3\ldots q_s$, que possui decomposição única por ser menor do que m. Como p_1 não divide $q_2q_3\cdots q_s$, p_1 é obrigatoriamente fator primo de $(q_1 - p_1)$. Ou seja, existe s tal que $q_1 - p_1 = p_1s$, o que acarreta $q_1 = p_1(s+1)$. Assim, p_1 é fator primo de q_1. Como $p_1 \neq q_1$ e $p_1 \neq 1$, chegamos a uma contradição, o que conclui a demonstração. □

Podemos aplicar imediatamente este teorema para enunciar o seguinte resultado, que fortalece o teorema 3.4:

Teorema 3.6**.** *Se o número primo* p *divide um produto* ab*, então ou* $p|a$ *ou* $p|b$.

Demonstração: Com efeito, o teorema 3.4 afirmava que este resultado é válido para números cuja decomposição em fatores primos é essencialmente única. Como já mostramos que isso é verdadeiro para qualquer número natural, temos o resultado desejado. □

Se p não é primo, e $p|ab$, não é necessário que p divida um dos fatores. Por exemplo, $4|2 \times 6$, mas 4 não divide 2 e 4 não divide 6.

O número 12 tem os divisores 1, 2, 3, 4, 6 e 12, que podem ser achados por simples inspeção. No entanto, dado um número natural bem grande, é na prática impossível determinar ou contar, por tentativas, todos seus divisores. O teorema fundamental da Aritmética nos permite resolver estes dois problemas, desde que conheçamos a decomposição em fatores primos do número dado.

Exemplo 3.2. *Usando o teorema fundamental da Aritmética, mostre que todos os divisores do número natural* $b = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$ *são da forma*

$$a = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s},$$

onde $0 \leq t_i \leq r_i$ *e* $i = 1, 2, \ldots s$.

Demonstração: Com efeito, se $a|b$, então,

$$b = ak.$$

Então, pelo teorema fundamental da Aritmética, na decomposição em fatores primos de a, só podem aparecer os primos $p_1, p_2, \ldots, p_s$.

De fato, se um primo $q \neq p_i$, para $i = 1, 2, \ldots, s$ for fator de a,

$$a = qr,$$

e assim $b = qrk$, ou seja, q é fator primo de b, o que é uma contradição, pelo teorema fundamental da Aritmética.

Certamente, se $0 \leq t_i \leq r_i$, para $i = 1, \ldots, s$,

$$a = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$$

divide b, pois

$$b = p_1^{(r_1 - t_1)} p_2^{(r_2 - t_2)} \cdots p_s^{r_s - t_s} (p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}).$$

E, também pelo teorema fundamental da Aritmética, não podemos ter, para algum i, $t_i > r_i$, o que conclui a demonstração. □

Exemplo 3.3. *Quantos divisores tem o número natural*

$$b = p_1^{r_1} \cdot p_2^{r_2} \cdots p_s^{r_s}?$$

Seja k um divisor de b. A decomposição de k como um produto de potências de primos distintos será da forma

$$k = p_1^{t_1} \cdot p_2^{t_2} \cdots p_s^{t_s},$$

onde $0 \leq t_i \leq r_i$, $i \leq s$. Assim, temos

$$(r_1 + 1) \text{ escolhas possíveis para o expoente de } p_1$$
$$(r_2 + 1) \text{ escolhas possíveis para o expoente de } p_2$$
$$\cdots$$
$$(r_s + 1) \text{ escolhas possíveis para o expoente de } p_s.$$

Ou seja, o número total de divisores de a é

$$(r_1 + 1)(r_2 + 1) \cdots (r_s + 1).$$

□

O maior primo conhecido, quando este livro foi escrito em 1993, era $2^{756839} - 1$. Este número é um dos *primos de Mersenne*[11], mais precisamente o número M_{756839}. Ele foi descoberto em 1989 e, escrito na base 10, tem 227.832 algarismos. Os números $M_n = 2^n - 1$ são chamados *números de Mersenne*. Mersenne conjecturou que M_n era primo para $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ e composto para todos os outros valores primos de $n < 257$. Na realidade, a lista de primos de Mersenne continha três omissões (para $n = 61$, $n = 89$ e $n = 107$) e dois erros (M_{67} e M_{257} são compostos).

O primeiro método para verificar se um número natural é primo foi o chamado *Crivo de Eratóstenes*, que na prática funciona somente para números pequenos. Ele consiste em cancelar, sucessivamente, na sequência dos números naturais, os múltiplos de 2, 3, 5, 7, 11, 13, etc. Os números não cancelados são primos.

---

[11] Marin Mersenne (1588, 1648) padre francês, fundou a Academia de Ciências de Paris, determinou as frequências das notas musicais e a velocidade do som.

Os matemáticos desenvolveram métodos e algoritmos engenhosos que permitem reduzir enormemente o tempo necessário para a fatoração de números grandes, mas mesmo assim este continua sendo um problema difícil de resolver, na prática. Devido à importância da criptografia, esta é uma área de pesquisa em Teoria dos Números que muito se desenvolveu nos últimos anos.

O interesse em calcular números primos muito grandes deve-se ao fato de que os métodos modernos de criptografia encifram mensagens usando como "chave" um número muito grande, obtido multiplicando primos também muito grandes. Para decifrar a mensagem, é necessário conhecer os fatores primos da "chave". Não importa que o "inimigo" conheça a "chave": Não há maneira prática de se achar os fatores primos de um número realmente grande, por exemplo um número com 200 algarismos em base 10, mesmo usando os computadores mais rápidos e modernos que existem. O limite para achar a decomposição em fatores primos de um número é atualmente da ordem de 60 a 70 algarismos. Para dar uma idéia da magnitude da tarefa envolvida, mencionamos que a tentativa ingênua de fatorar um número n de 100 algarismos usando o processo de divisão pelos números menores do que $\sqrt{n}$ gastaria 10^{36} anos nos mais modernos computadores! Mesmo usando os algoritmos mais eficientes e os computadores mais rápidos existentes hoje, a fatoração deste número exigiria muitos anos de cálculos. Com a velocidade dos computadores cada vez maior e com a engenhosidade dos matemáticos para criar algoritmos de fatoração de números inteiros cada vez mais eficientes, é necessário procurar primos cada vez maiores para obter códigos seguros.

Durante muito tempo, foram procuradas fórmulas que gerassem números primos. Um exemplo é $n^2 - 79n + 1601$, que é primo para $n = 1, 2, \ldots, 79$. Em verdade, pode-se demonstrar que nenhum polinômio de uma variável, com coeficientes inteiros, assume somente valores primos, para valores inteiros da variável.

Exemplo 3.4. *Não existe nenhum polinômio de uma variável,* $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, *com coeficientes inteiros, tal que* $f(n)$ *seja primo, para todo* n *inteiro*[12].

[12] Estamos usando aqui o conceito de número inteiro, que ainda não definimos. No entanto, como o resultado deste exemplo não é necessário para a teoria, isso não nos causará problemas.

Demonstração: Com efeito, suponha que $f(a) = p$ seja primo, para um certo número natural a, e considere os números inteiros

$$f(a + kp), \qquad k = 0, 1, 2, \ldots$$

Mostraremos inicialmente que $f(a + kp)$ é divisível por p, para $k = 0, 1, 2, \ldots$. Com efeito,

$$f(a + kp) - f(a) = \sum_{i=0}^{n} a_i\{(a + kp)^i - a^i\}.$$

Mas, pela expressão do Binômio de Newton, temos, para $i = 1, 2, \ldots, n$,

$$(a + kp)^i - a^i = \sum_{j=1}^{i} \binom{i}{j} a^{i-j}(kp)^j,$$

e este número é sempre divisível por p.

Assim, $f(a+kp)-f(a)$ é sempre divisível por p, para $k = 0, 1, \ldots$ Como $f(a)$ é divisível por p (é igual a p), então forçosamente $f(a + kp)$ é divisível por p, $\quad k = 0, 1, 2, \ldots$

Então, os números $f(a + kp)$ para $k = 0, 1, 2, \ldots$ ou não são primos, o que resolve o problema, ou então $f(a + kp) = p$, ou $f(a + kp) = -p$, ou $f(a + kp) = 0$.

Ora, um polinômio de grau n só pode ter o mesmo valor no máximo para n valores da variável. Assim, o polinômio $f(x)$ só pode ter os três valores acima (p, $-p$, 0) no máximo para $3n$ valores de x. Então, se fizermos $k = 0, 1, 2, \ldots, 3n$, teremos certeza de que um dos valores de $f(a + kp)$ não será primo. □

No entanto, sabe-se hoje que existe um polinômio de grau 25, com 26 variáveis, cujos valores positivos, para valores inteiros das variáveis x_1, x_2, ..., x_{26}, são primos! É possível mesmo exibir este polinômio.

Este resultado, como muitos outros de Matemática, envolve idéias que à primeira vista nada têm a ver com o problema resolvido. Ele é consequência de trabalhos de vários matemáticos sobre o chamado *Décimo Problema de Hilbert*, que pergunta se existe um algoritmo para resolver uma equação diofantina dada. A solução negativa do problema de Hilbert foi iniciada por Martin Davis em 1950, continuada por Davis, Julia Robinson e H. Putnam em 1960 e concluida em 1970, por Yuri Matyasevitch, que usou em seu

trabalho os números de Fibonacci. A partir do trabalho de Matyasevitch, que garantia a existência de um polinômio em várias variáveis e cujos valores positivos, para valores naturais das variáveis são primos, James Jones, Daihachiro Sato, Hideo Wada e Douglas Wiens finalmente em 1977 acharam um polinômio com as propriedades pedidas.

Um resultado profundo sobre números primos, cuja demonstração foge totalmente ao escopo deste livro, é a chamada "lei de distribuição dos primos".

Dado um número natural n, chame de A_n o número de primos entre $1, 2, 3, \ldots, n$. Por exemplo, $A_2 = 1$, $A_3 = A_4 = 2, \ldots, A_{19} = 8$, etc. Durante algum tempo, os matemáticos tentaram encontrar uma expressão explícita que lhes permitisse calcular A_n, para todo número natural n. Obviamente $\lim_{x\to\infty} A_n$ é infinito, pois existem infinitos números primos. Gauss, baseando-se na observação das tabelas de primos, chegou à convicção de que $\lim_{n\to\infty} \frac{A_n/n}{1/\log n} = 1$, a chamada *lei de distribuição dos primos.* Este resultado só foi demonstrado no fim do século XIX. Mesmo hoje, após simplificações introduzidas em sua prova, trata-se de um teorema difícil.

Apresentamos a seguir alguns resultados que decorrem imediatamente do teorema fundamental da Aritmética.

3.3 APLICAÇÕES DO TEOREMA FUNDAMENTAL DA ARITMÉTICA

Exemplo 3.5. *Mostre que todo número natural* n *pode ser escrito como* $n = 2^k r$, *onde* r *é um número ímpar e* k *é um inteiro não-negativo.*

Demonstração: De fato, usando a decomposição de um inteiro em potências de primos, escreva $n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$. Se algum dos p_i for igual a 2, podemos supor, sem perda de generalidade, que $p_1 = 2$. Então

$$n = 2^{r_1} p_2^{r_2} \cdots p_s^{r_s},$$

com $p_2^{r_2} \cdots p_s^{r_s}$ ímpar. Se nenhum dos p_i for igual a 2, escreva

$$n = 2^0 p_1^{r_1} \cdots p_s^{r_s}.$$

Como $p_1^{r_1} \cdots p_s^{r_s}$ é ímpar (por quê?), isso demonstra nosso resultado. □

Exemplo 3.6. *Seja* n *um número natural. Então* n *é um quadrado perfeito se e somente se todos os expoentes dos fatores primos que comparecem na decomposição de* n *são pares.*

Demonstração: Com efeito. Suponha que

$$n = p_1^{2s_1} p_2^{2s_2} \cdots p_k^{2s_k}.$$

Considere então o número natural

$$a = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}.$$

É imediato verificar que

$$\begin{aligned} a^2 &= (p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k})(p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}) \\ &= p_1^{2s_1} p_2^{2s_2} \cdots p_k^{2s_k} = n, \end{aligned}$$

ou seja, n é um quadrado perfeito.

Suponha agora que n é um quadrado perfeito e que

$$n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}.$$

Por hipótese, $n = a^2$ para algum número natural a. Se

$$a = q_1^{s_1} q_2^{s_2} \cdots q_r^{s_r},$$

então

$$a^2 = q_1^{2s_1} q_2^{2s_2} \cdots q_r^{2s_r},$$

e temos que

$$n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k} = q_1^{2s_1} q_2^{2s_2} \cdots q_r^{2s_r}.$$

Pela unicidade da decomposição em potências de primos, e se necessário modificando a ordem dos p_i, segue-se que $k = r$, $p_i = q_i$, para $1 \leq i \leq k$, e que $t_i = 2s_i$, o que conclui a demonstração. □

Semelhantemente, se n é uma potência q-ésima, cada expoente s_i na decomposição de n em potências de primos será um múltiplo de q (demonstre isso!).

Exemplo 3.7. *Ache o menor número natural* n *tal que* $\frac{n}{2}$ *é um quadrado,* $\frac{n}{3}$ *é um cubo, e* $\frac{n}{5}$ *é uma quinta potência.*

Solução: Claramente a decomposição em fatores primos de n conterá os primos 2, 3 e 5. Como estamos interessados no *menor* n que satisfaz as condições pedidas, podemos também supor que somente os primos acima comparecem na decomposição de n em fatores primos. Ou seja, podemos supor que

$$n = 2^a \cdot 3^b \cdot 5^c.$$

Então

$$\frac{n}{2} = 2^{a-1} \cdot 3^b \cdot 5^c, \tag{A}$$
$$\frac{n}{3} = 2^a \cdot 3^{b-1} \cdot 5^c, \tag{B}$$
$$\frac{n}{5} = 2^a \cdot 3^b \cdot 5^{c-1}. \tag{C}$$

Observando as potências do fator primo 2 em (A), (B) e (C), vemos que $a-1$ é par, $3|a$ e $5|a$. O menor número natural a que satisfaz estas condições é 15.

Semelhantemente, examinando as potências de 3 em (A), (B) e (C), vemos que b é par, $b-1$ é múltiplo de 3 e b é múltiplo de 5; assim, o menor valor de b para que isso ocorra é 10.

Da mesma maneira, como c é par, c é múltiplo de 3 e $c-1$ é múltiplo de 5, vem que $c = 6$. Logo

$$n = 2^{15}3^{10}5^6.$$

□

Exemplo 3.8. *Mostre que existe um único número natural* n *tal que*

$$2^8 + 2^{11} + 2^n$$

é um quadrado.

Demonstração: Seja

$$m^2 = 2^8 + 2^{11} + 2^n.$$

Então

$$2^n = m^2 - 2^8(1 + 2^3),$$

donde

$$2^n = m^2 - (3 \cdot 2^4)^2 = (m + 3 \cdot 2^4)(m - 3 \cdot 2^4) =$$

$$= (m + 48)(m - 48).$$

Pelo teorema da fatoração única, $m+48$ e $m-48$ devem ser potências de 2. Assim, existem t e s, com $t > s$, tais que

$$m - 48 = 2^s, \qquad m + 48 = 2^t, \qquad \text{com} \quad s + t = n,$$

donde

$$m = 2^s + 48, \quad m = 2^t - 48,$$

e assim

$$2^s - 2^t = 96.$$

Como $t > s$, temos que

$$2^s(2^{t-s} - 1) = 2^5 \cdot 3.$$

Ora, como $2^{t-s} - 1$ é ímpar, vem que $s = 5$, $2^{t-s} - 1 = 3$, logo $2^{t-s} = 4$, donde $t - s = 2$, e vemos então que $t = 7$, e daí decorre que $n = 12$. □

Exemplo 3.9. *Dado um número natural* n*, quantos pares* (x, y) *de números naturais satisfazem a equação*

$$\frac{xy}{x + y} = n?$$

Solução: Vemos que

$$xy = n(x + y),$$

donde

$$xy - nx - ny = 0,$$

que é equivalente a

$$(x - n)(y - n) = n^2.$$

Assim, as soluções da equação são determinadas pelos divisores de n^2. Para contá-los, suponha que

$$n = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}.$$

Então

$$n^2 = p_1^{2r_1} p_2^{2r_2} \cdots p_t^{2r_t},$$

Aplicando o Exemplo 2.2, vemos que o número dos divisores de n^2 será

$$(2r_1 + 1)(2r_2 + 1) \cdots (2r_t + 1).$$

□

Exemplo 3.10. *Em quantos zeros termina o número* 1000!?

Solução: Decompondo 1000! em um produto de potências de fatores primos distintos, podemos escrever

$$1000! = 2^a 5^b r,$$

onde r é primo com 2 e com 5.

É óbvio que $a > b$. Assim, o número de zeros finais em 1000! será igual a b, pois

$$1000! = 2^{a-b} \cdot r \cdot (2 \cdot 5)^b = (2^{a-b} \cdot r) \cdot 10^b,$$

onde em $2^{a-b} \cdot r$ não comparece o fator 5, logo não pode comparecer o fator 10. Nosso problema reduz-se portanto a achar b, ou seja, o número de potências de 5 que comparecem na decomposição de 1000! em potências de fatores primos distintos.

Como $1000! = 1 \times 2 \times 3 \times 4 \times \cdots \times 99 \times 1000$, e 5 é primo, se $5|1000!$, então 5 divide um dos números $1, 2, 3, 4, \ldots, 1000$. Assim, devemos contar os múltiplos de 5 entre 1 e 1000.

Observe que para cada um destes $[\frac{1000}{5}]$ múltiplos de 5 entre 1 e 1000, podemos associar um fator 2, de maneira a obter um fator 2×5 de 1000!

Considere, contudo, por exemplo, o número $75 = 5 \times 15$. O processo descrito acima nos fornece $[\frac{75}{5}]$ fatores 2×5. No entanto, como em 75 o número 5 comparece com expoente

2, podemos associar a 75 mais um fator 2, obtendo assim um fator 10 extra. Ou seja, em geral, para cada múltiplo de $25(=5^2)$, associamos mais um fator 2; obtemos desta maneira outros $[\frac{1000}{25}]$ fatores 10.

Este raciocínio pode ser generalizado para as outras potências de 5.

Fazendo isso, vemos que os $[\frac{1000}{125}]$ múltiplos de 5^3 geram $[\frac{1000}{125}]$ fatores 10 ainda não contados.

Os $[\frac{1000}{625}]$ múltiplos de 5^4 geram $[\frac{1000}{625}]$ fatores de 10 ainda não contados, etc.

Somando o número total de fatores 10 contados acima obtemos

$$\left[\frac{1000}{5}\right] + \left[\frac{1000}{5^2}\right] + \left[\frac{1000}{5^3}\right] + \left[\frac{1000}{5^4}\right] + \cdots =$$

$$200 + 40 + 8 + 1 = 249.$$

O raciocínio acima pode ser sintetizado como segue:

Considere o conjunto A_1 dos múltiplos de 5 de 1 a 1000,

$$A = \{5, 10, 15, \ldots, 1000\}.$$

O número de elementos de A_1 é $[\frac{1000}{5}]$.

Dividindo cada elemento de A_1 por 5, obtemos o conjunto

$$A_1' = \{1, 2, \ldots, 200\}.$$

O número de múltiplos de 5 em A_1' é $[\frac{200}{5}] = [\frac{1000}{25}]$. Seja A_2 o conjunto dos múltiplos de 5 em A_1',

$$A_2 = \{5, 10, \ldots, 40\}.$$

O número de múltiplos de 5 deste conjunto é $[\frac{40}{5}]$.

Dividindo cada elemento de A_2 por 5, obtemos o conjunto

$$A_2' = \{1, 2, \ldots, 8\}.$$

O número dos múltiplos de 5 de A_2' é $[\frac{8}{5}]$. Seja A_3 o conjunto dos múltiplos de 5 de A_2'.

$$A_3 = \{5\}.$$

Obviamente podemos parar o processo neste ponto. O número total de múltiplos de 10 em 1000! será

$$\left[\frac{1000}{5}\right] + \left[\frac{1000}{5^2}\right] + \left[\frac{1000}{5^3}\right] + \left[\frac{1000}{5^4}\right] + \cdots =$$

$$200 + 40 + 8 + 1 = 249,$$

o que coincide com o resultado achado anteriormente.

Este processo é inteiramente geral; ele nos permite determinar o número de zeros com que termina $\mathfrak{n}!$, onde $\mathfrak{n}$ é um número natural qualquer:

$$[\frac{\mathfrak{n}}{5}] + [\frac{\mathfrak{n}}{5^2}] + \cdots + [\frac{\mathfrak{n}}{5^s}] + \cdots$$

□

EXERCÍCIOS

3.1. Se a, b e c são números naturais, demonstre que se a divide b, então a divide bc.

3.2. Ache números naturais a, b e c tais que a divide bc mas a não divide b e a não divide c.

3.3. Ache números naturais a, b e c tais que $a|(b+c)$ mas a não divide b e a não divide c.

3.4. Demonstre que se a é um número natural ímpar, então o número natural $a(a^2-1)$ é um múltiplo de 24.

3.5. Demonstre que se a e b são números naturais consecutivos, com $a > b$, então $a^3 - b^3$ não é par.

3.6. Demonstre que o cubo de qualquer número natural tem uma das formas $9k$, $9k+1$ ou $9k+8$ (Na linguagem das *congruências*, que estudaremos mais tarde, isso quer dizer que o cubo de qualquer número natural é congruente a 0, a 1 ou a 8 módulo 9).

3.7. Demonstre que, para todo número natural n, $n^5 - n$ é múltiplo de 30.

3.8. Ache todos os primos da forma $n^2 - 1$, n número natural.

3.9. Ache todos os primos da forma $n^3 - 1$, n número natural.

3.10. Ache todos os primos da forma $n^4 + 4$, n número natural.

3.11. Demonstre que, se $k \geq 1$, a soma de k números naturais ímpares e consecutivos não pode ser um número primo.

3.12. Mostre que se p é um primo maior do que 3, então ele é da forma $6k-1$ ou da forma $6k+1$ (Na linguagem das congruências, isso quer dizer que p é côngruo a 1 ou a -1 módulo 6.)

3.13. Mostre que se a é um número natural e $a|1$, então $a = 1$.

3.14. Sejam a, b e c números naturais. Demonstre que se $a|b$ e $b|c$, então $a|c$ (a relação "divide" é transitiva.

3.15. Seja a um número natural. Mostre que um dos números $a, a+2, a+4$ é divisível por 3.

3.16. Se n é um número natural, então $n(n+1)(2n+1)$ é um múltiplo de 6.

3.17. Sejam a, b e c números naturais tais que $a|(2b-3c)$ e $a|(4b-5c)$. Então $a|c$.

3.18. Mostre que se a e b são números naturais, então os números naturais a e $a+2b$ têm a mesma paridade (isto é, são ambos pares ou ambos ímpares).

3.19. Ache o maior número natural de 4 algarismos divisível por 17.

3.20. Ache o menor número natural de 6 algarismos divisível por 15.

3.21. Ache um número natural de 4 algarismos, quadrado perfeito, divisível por 27 e cujo algarismo das unidades é 6.

3.22. Um número natural é composto se não é primo. Seja n um número natural.

a) *Mostre que se um dos números* $2^n - 1$ *e* $2^n + 1$ *é primo, então o outro é composto.*

b) *Mostre que se* n *e* $8n - 1$ *são primos, então* $8n + 1$ *é composto.*

c) *Mostre que se* n *e* $8n^2 + 1$ *são primos, então* $8n^2 - 1$ *é primo.*

d) *Mostre que os números* $1\,0001, 1\,0001\,0001, \ldots$ *são compostos.*

3.23. Considere os números naturais do intervalo [100, 1000]

a) *Quantos desses números naturais são múltiplos de* 3 *e de* 7*?*

b) *Quantos desses números naturais são múltiplos de* 3 *mas não de* 7*?*

c) *Quantos desses números naturais são múltiplos de* 3 *ou de* 7*?*

d) *Quantos desses números naturais são múltiplos de* 3 *ou de* 7 *mas não de* 5*?*

3.24. Mostre que existe um múltiplo de 7 que começa com 1000 algarismos iguais a 1.

3.25. Mostre que se um número natural n não é divisível nem por 2 e nem por 5, então ele tem múltiplos cujos algarismos são todos iguais a k ($k = 1, 2, 3, \ldots$.)

3.26. Determine todos os primos que são somas ou diferenças de dois primos.

3.27. Um número natural é perfeito se e só se ele é igual à metade da soma de seus divisores positivos. Demonstre que se p é um número natural tal que $2^p - 1$ é primo, então $(2^p - 1)2^{p-1}$ é perfeito. (Euler provou que todo número perfeito par é dessa forma. Ainda não se sabe, até hoje, se exitem números perfeitos ímpares nem tão pouco se existem infinitos números perfeitos).

3.28. Seja n um número perfeito. Determine a soma dos inversos dos seus divisores.

3.29. Determine n número natural para que $(n + 3)$ divida $(n^2 + 4n + 9)$.

3.30. Considere as funções $h, f : \mathbf{N}\times\mathbf{N} \to \mathbf{N}$, dada por $h(m, n) = [m(n+1)-(n!+1)]^2-1$, $f(m, n) = \frac{1}{2}(n - 1)\{|h(m, n)| - h(m, n)\} + 2$.

Demonstre que

a) $f(m, n)$ é sempre primo;

b) $f(m, n)$ é sobre o conjunto dos primos.

CAPÍTULO 4

DIVISÃO, MÁXIMO DIVISOR COMUM E ALGORITMO DE EUCLIDES

4.1 O ALGORITMO DA DIVISÃO

O número natural 3 divide o número natural 12. Ou seja, 3 "mede" 12 exatamente. Isso quer dizer que 3 "está contido um número exato de vezes em 12". Por outro lado, 3 *não* está contido em 17 um número exato de vezes, pois $3 \times 1 = 3$, $3 \times 2 = 6$,..., $3 \times 5 = 15$, $3 \times 6 = 18$. Ou seja, $17 = 3 \times 5 + \mathfrak{n}$, onde $\mathfrak{n}$ é o número natural que indica o fato de que 3 não está contido um número exato de vezes em 17. É claro que $\mathfrak{n} = 2$. Dizemos que ao dividirmos 17 por 3 obtemos o "resto" 2. Ou seja, este resto indica quanto o número natural 3 não está contido exatamente em 15. Este processo, para "medir" quanto um número natural não divide exatamente outro, é inteiramente geral, como mostramos a seguir.

Teorema 4.1**.** *Sejam* $\mathfrak{a}$ *e* $\mathfrak{b}$ *números naturais, com* $\mathfrak{a} > \mathfrak{b}$*. Suponha que* $\mathfrak{b}$ *não divide* $\mathfrak{a}$*. Existem então números naturais* $\mathfrak{q}$ *e* $\mathfrak{r}$ *tais que*

$$\mathfrak{a} = \mathfrak{b}\mathfrak{q} + \mathfrak{r}, \qquad \mathfrak{r} < \mathfrak{b}.$$

Além disso, $\mathfrak{q}$ *e* $\mathfrak{r}$ *ficam unicamente determinados por* $\mathfrak{a}$ *e* $\mathfrak{b}$ *(dizemos que* $\mathfrak{q}$ *e* $\mathfrak{r}$ *são únicos para* $\mathfrak{a}$ *e* $\mathfrak{b}$ *dados).*

A demonstração usa o fato de que todo conjunto limitado (isto é, finito) de números naturais possui um maior elemento (Veja o final da Capítulo 2.) da boa ordenação.

Considere o conjunto S dos múltiplos de b que são menores do que a. Como este conjunto é limitado superiormente por a, ele possui um maior elemento k; como k é um múltiplo de b, existe um número natural q tal que $k = qb$. Seja $r = a - qb$.

Afirmamos que $r < b$. Com efeito, se $r = b$,então $a = qb + b = b(q + 1)$, o que é uma contradição, pois a não é um múltiplo de b. Se $r > b$, então $r = b + s$ e assim $b + s = a - qb \Rightarrow s = a - (q + 1)b$ e isso mostra que $(q + 1)b$ é um elemento de S maior do que $k = qb$, uma contradição.

Suponha agora que

$$a = bq + r, \qquad r < b,$$

$$a = bq' + r', \qquad r' < b;$$

em primeiro lugar, podemos supor que $r \leq r'$. Se $r = r'$, como $bq + r = bq' + r'$, segue-se imediatamente que $bq = bq' \Rightarrow b = b'$ (Semelhantemente, se $q = q'$, vemos também que $r = r'$.)

Se $r < r'$, então,

$$r' - r = b \cdot (q' - q)$$

é um número natural menor do que b e um múltiplo de b, o que é impossível. □

A idéia usada na demonstração acima dá realmente uma maneira para determinar q e r. Considere sucessivamente os múltiplos de b, $(b, 2b, 3b, \ldots)$, até chegar ao maior deles que seja menor do que a, qb. Então a diferença $a - qb$ é exatamente o resto procurado.

Ao efetuarmos a divisão de a por b, chamamos a de *dividendo*, b de *divisor* e r de *resto*.

Quando $b|a$, ou seja, b divide a, dizemos que temos uma *divisão exata* ou que *o resto da divisão é nulo*, ou ainda que a divisão *não deixa resto.*

Mais tarde, quando estudarmos o sistema de numeração decimal, apresentaremos um processo mais eficiente para a determinação do quociente e do resto de uma divisão. O processo indicado acima, que funciona para dividendo e divisor pequenos, é realmente empregado no ensino elementar, no primeiro contacto das crianças com a divisão de números naturais.

Como no capítulo anterior, utilizaremos por vezes o *zero*, embora ele não seja um número natural, a fim de simplificar enunciados e demonstrações.

Exemplo 4.1. *Sejam* $\mathtt{a} = 11$ *e* $\mathtt{b} = 3$. *Ache o quociente e o resto da divisão de* $\mathtt{a}$ *por* $\mathtt{b}$.

Solução: Tomando os múltiplos sucessivos de 3, vemos que $3 \times 1 = 3, 3 \times 2 = 6, 3 \times 3 = 9, 3 \times 4 = 12$. Assim, 9 é o maior múltiplo de 3 menor do que 11, e então o resto é $11 - 9 = 2$, ou seja, $11 = 3 \times 3 + 2$. Assim, o quociente é 3 e o resto é 2. □

Exemplo 4.2. *Dividiu-se* 392 *por* 45. *Determine o maior número natural que se pode somar a* 392 (*o dividendo*), *sem alterar o quociente.*

Solução: Vemos que $392 = 8 \times 45 + 32$, ou seja, o quociente é 8. Os números naturais que divididos por 45 têm quociente 8 são da forma $\mathtt{N} = 8 \times 45 + \mathtt{r}$, em que $\mathtt{r} < 45$, ou da forma $\mathtt{N} = 8 \times 45$. Assim, o maior destes números será aquele para o qual $\mathtt{r}$ é máximo, ou seja, $8 \times 45 + 44 = 404$. □

Exemplo 4.3. *Sabendo que* $53 = 4 \times 12 + 5$, *qual o resto e o quociente da divisão de* 53 *por* 12?

Pela unicidade do resto e do quociente no algoritmo da divisão, como $5 < 12$, vemos, de $53 = 4 \times 12 + 5$, que 12 é o quociente e 5 o resto da divisão de 53 por 12. □

A conclusão a que chegamos no exemplo acima, aparentemente trivial, será usada por nós. Sempre que $\mathtt{a} = \mathtt{bt} + \mathtt{s}$, $\mathtt{a}$, $\mathtt{b}$, $\mathtt{t}$ e $\mathtt{s}$ naturais e $\mathtt{s} < \mathtt{t}$, podemos dizer afirmar que $\mathtt{t}$ é o quociente e $\mathtt{s}$ o resto da divisão de $\mathtt{a}$ por $\mathtt{b}$.

Uma aplicação imediata do algoritmo da divisão é a demonstração de que existem infinitos números primos.

Teorema 4.2**.** *Existe uma infinidade de números primos.*

Demonstração. Suponhamos, por absurdo, que só existem $\mathtt{n}$ primos distintos, que chamaremos de $\mathtt{p}_1,\ \mathtt{p}_2, \ldots,\ \mathtt{p}_\mathtt{n}$ e considere o número natural

$$\mathtt{N} = \mathtt{p}_1 \cdot \mathtt{p}_2 \cdot \ldots \cdot \mathtt{p}_\mathtt{n} + 1.$$

Obviamente $\mathtt{N}$ é maior do que qualquer dos primos $\mathtt{p}_1, \ldots, \mathtt{p}_\mathtt{n}$. Se $\mathtt{N}$ for primo, achamos um primo distinto dos $\mathtt{n}$ primos $\mathtt{p}_1, \ldots, \mathtt{p}_\mathtt{n}$, o que é uma contradição. Suponha portanto que $\mathtt{N}$ não é primo. Já sabemos que $\mathtt{N}$ se escreve como um produto de primos. Ou seja, pelo menos um dos $\mathtt{p}_\mathtt{i}$, $\mathtt{com}\ 1 \leq \mathtt{i} \leq \mathtt{n}$, divide $\mathtt{N}$.

Mas como

$$N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1,$$

vemos que N, ao ser dividido por cada um dos primos p_i deixa resto 1. Ou seja, N não pode ser múltiplo de nenhum dos p_i, uma contradição! □

Acabamos de ver que existe uma quantidade infinita de números primos. Como você observou, a demonstração desse fato é bem simples. Por outro lado, demonstrar que existem infinitos primos em uma progressão aritmética

$$a_1,\ a_1 + r,\ a_1 + 2r, \ldots,$$

em que a_1 e r são números inteiros é um problema muito difícil. Somente no século passado, Lejeune-Dirichlet [13] conseguiu mostrar, usando técnicas sofisticadas, que em toda progressão aritmética em que o primeiro termo e a razão são primos entre si existe uma infinidade de números primos.

No entanto, em alguns casos especiais, é fácil mostrar que uma progressão arimética contém infinitos primos.

Exemplo 4.4. *Há uma infinidade de primos na progressão aritmética*

$$3,\ 7,\ 11,\ 15, \ldots$$

Demonstração: Os elementos desta progressão aritmética são da forma $4n + 3$, $n = 0, 1, 2, \ldots$ Assim, desejamos mostrar que existem infinitos primos da forma $4n + 3$.

Em primeiro lugar, pelo algoritmo da divisão, qualquer número natural se escreve em uma das formas $4n$, $4n+1$ $4n+2$, $4n+3$ (divida o número por 4 e veja quais os restos possíveis). Se o número é primo, então ele será forçosamente da forma $4n + 1$ ou $4n + 3$, pois $4n + 2$ e $4n$ são pares.

Observe também que se dois números são da forma $4n + 1$, então seu produto é da mesma forma, pois

$$(4n_1 + 1)(4n_2 + 1) = 4(4n_1n_2 + n_1 + n_2) + 1.$$

[13] Peter Gustav Lejeune Dirichlet (1805-1859), matemático alemão, trabalhou em teoria dos números, séries de Fourier e equações a derivadas parciais. Caracterizou-se por seu cuidado com o rigor matemático.

Suponha que o número de primos da forma $4n+3$ é finito e represente-os por $p_1, \ldots, p_s$; considere o número

$$N = 4(p_1 p_2 \cdots p_s) - 1 = 4(p_1 p_2 \cdots p_s - 1) + 3,$$

que é da forma $4n+3$. Certamente N é diferente de todos os números $p_1,\ p_2, \ldots,\ p_s$ (por quê?). Se N for primo, chegamos a uma contradição, que se originou da suposição de só termos um número finito de primos da forma $4n+3$. Suponha portanto que N não é primo. Então, na decomposição de N em fatores primos não comparecem os primos $p_1, \ldots, p_s$, pois N não é divisível por nenhum destes números.

Observe também que os fatores primos de N não podem ser todos da forma $4n+1$, pois já vimos que o produto de números deste tipo é também deste tipo. Assim, um dos fatores de N é obrigatoriamente da forma $4n+3$. Então, como estamos supondo que só existe um número finito de primos desta forma, este fator é um dos $p_i,\ \ i = 1,\ 2, \ldots, s$. Mas já vimos que nenhum destes p_i divide N, e chegamos a uma contradição. Assim, N é primo e distinto de $p_1, \ldots, p_s$, o que conclui nossa demonstração. □

4.2 O MÁXIMO DIVISOR COMUM

Sejam $\mathtt{a}$ e $\mathtt{b}$ dois números naturais. Chame de $\mathtt{A}$ o conjunto dos divisores de $\mathtt{a}$. Certamente o conjunto $\mathtt{A}$ é não-vazio, pois $1 \in \mathtt{A}$. Analogamente, chame de $\mathtt{B}$ o conjunto dos divisores de $\mathtt{b}$. É claro que $1 \in \mathtt{A} \cap \mathtt{B}$, ou seja, a intersecção destes dois conjuntos é não-vazia. Como os divisores de $\mathtt{a}$ não são maiores do que $\mathtt{a}$ e os de $\mathtt{b}$ não são maiores do que $\mathtt{b}$, o conjunto $\mathtt{A} \cap \mathtt{B}$ é um conjunto não-vazio de números naturais limitado superiormente. Assim, $\mathtt{A} \cap \mathtt{B}$ possui um maior elemento. O *máximo divisor comum de* $\mathtt{a}$ e de $\mathtt{b}$, representado por m.d.c.($\mathtt{a}$, $\mathtt{b}$) é o maior divisor comum de $\mathtt{a}$ e de $\mathtt{b}$.

Exemplo 4.5. *Ache o* m.d.c.(48, 60).

Solução: Em primeiro lugar, $48 = 2^4 \times 3$. Assim, seus divisores são 1, 2, 2^2, 2^3, 2^4, 3×2, 3×2^2, 3×2^3, 3×2^4, ou seja, 1, 2, 4, 8, 16, 3, 6, 12, 24 e 48. (Você já sabe que o número dos divisores de 48 é exatamente 10. Assim, a lista acima contém todos eles). Chamando de $\mathtt{A}$ o conjunto desses divisores podemos escrever:

$$\mathtt{A} = \{1, 2, 4, 8, 16, 3, 6, 12, 24, 48\}.$$

Analogamente, usando o fato de que $60 = 2^2 \times 3 \times 5$, achamos facilmente que o conjunto $\mathtt{B}$ dos divisores de 60 é:

$$\mathtt{B} = \{1, 2, 2^2, 3, 5, 6, 10, 12, 15, 20, 30, 60\}.$$

Mas

$$\mathtt{A} \cap \mathtt{B} = \{1, 2, 3, 4, 6, 12\},$$

donde, pela definição de máximo divisor comum, m.d.c.(48, 60) = 12. □

As observações acima mostram que sempre existe o máximo divisor comum de dois inteiros não-nulos. Resta o problema de calculá-lo. O cálculo direto baseado na definição, ou seja, achar os conjuntos $\mathtt{A}$, $\mathtt{B}$ e $\mathtt{A} \cap \mathtt{B}$, é impraticável para números grandes. Daremos duas maneiras para calcular o máximo divisor comum de dois números naturais. A primeira, baseada no teorema fundamental da Aritmética, e a segunda no algoritmo da divisão.

Uma observação trivial é que se $a|b$, então m.d.c.$(a, b) = a$, pois a é certamente o maior divisor comum de a e de b, pois é o maior divisor de a. Assim, ao procurarmos achar o máximo divisor comum de dois números naturais, o único caso interessante é quando nenhum deles é múltiplo do outro.

Exemplo 4.6. *Sejam* a *e* b *números naturais cujas decomposições em produto de fatores primos são*

$$\begin{aligned} a &= p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}, \\ b &= q_1^{s_1} q_2^{s_2} \cdots q_t^{s_t}. \end{aligned}$$

Então,

$$\text{m.d.c.}(a, b) = z_1^{c_1} \cdot z_2^{c_2} \cdots z_k^{c_k},$$

onde os z_i são os fatores primos comuns a a e a b, e c_i é o menor expoente de z_i nas duas decomposiçSes.

Demonstração: Observe, em primeiro lugar que, como $n^0 = 1$ para qualquer número natural, podemos escrever que $a = p_1^{r_1} p_2^{r_2} \cdot \ldots \cdot p_n^{r_n} \cdot q_1^0 q_2^0 \cdot \ldots \cdot q_t^0$, e que $b = p_1^0 p_2^0 \cdots p_n^0 \cdot q_1^{s_1} q_2^{s_2} \cdot \ldots \cdot q_t^{s_t}$.

Ou seja, unificando a notação para evitarmos primos p_i e q_j e expoentes r_i e s_j, podemos escrever

$$a = z_1^{n_1} z_2^{n_2} \cdots z_k^{n_k}$$

onde $n_i = 0$ se $z_i \neq p_1, p_2, \ldots, p_n$, e

$$b = z_1^{m_1} z_2^{m_2} \cdots z_k^{m_k},$$

onde $m_i = 0$ se $z_i \neq q_1, q_2, \ldots, q_k$. Observe que os expoentes m_i e n_i são não-negativos.

Defina agora c_i =mínimo de n_i e m_i, $\quad 1 \leq i \leq k$. Afirmamos que

$$\text{m.d.c.}(a, b) = z_1^{c_1} \cdot z_2^{c_2} \cdots z_k^{c_k}.$$

É claro que, como $c_1 \leq n_1,\ m_1, \quad c_2 \leq n_2,\ m_2$, ..., $c_k \leq n_k,\ m_k$, temos que

$$z_1^{c_1} z_2^{c_2} \cdots z_k^{c_k} | z_1^{n_1} z_2^{n_2} \cdots z_k^{n_k},$$

e que

$$z_1^{c_1} z_2^{c_2} \cdots z_k^{c_k} | z_1^{m_1} z_2^{m_2} \cdots z_k^{m_k}.$$

Fazendo $t = z_1^{c_1} z_2^{c_2} \cdots z_k^{c_k}$, acabamos de mostrar que $t|a$ e $t|b$. Ou seja, t é um divisor comum de a e b.

Considere agora um divisor comum qualquer, d, de a e de b. Afirmamos então que na decomposição em fatores primos de d só podem aparecer os primos $z_1, \ldots, z_k$. Com efeito, se na decomposição em primos de d comparecer um primo z_s, distinto de $z_1, \ldots, z_k$, este primo teria que dividir um dos z_i, $i = 1, 2 \ldots k$, o que é um absurdo.

Além disso, na decomposição em primos de d, qualquer um dos z_i, $i = 1, 2 \ldots k$, não pode ter expoente maior do que minimo $\{n_i, m_i\} = n_i$. De fato, se minimo $\{n_i, m_i\} = n_i$ e se o expoente de z_i na decomposição de d for maior do que n_i, d não divide a. Se minimo $\{n_i, m_i\} = m_i$, e o expoente de z_i na decomposiçsao de d for maior do que m_i, então d não divide b. Mas então t é o máximo divisor comum de a e de b.

Pela definição de c_i como o mínimo de n_i e m_i, vemos que $c_i = 0$ se z_i não é um fator comum de a e de b. Quando z_i é um fator comum, então $c_i = \min\{r_1, s_i\}$. □

Exemplo 4.7. *Calcule, pelo processo descrito no exemplo anterior, o máximo divisor comum de* 48 *e* 60.

Solução: Sabemos que

$$48 = 2^4.3;$$

$$60 = 2^2.3.5.$$

Como

$$\min\{2, 4\} = 2;$$

$$\min\{1, 1\} = 1;$$

$$\min\{0, 1\} = 0,$$

segue-se que o máximo divisor comum será $2^2.3^1.5^0 = 12$. □

Para calcular o máximo divisor comum de dois números, baseando-nos em suas decomposições em fatores primos, usamos na prática o seguinte dispositivo:

$$\begin{array}{rrl} 60, & 48 & 2 \\ 30 & 24 & 2 \\ 15 & 12 & 3 \\ 5 & 4 & \end{array}$$

$$2 \times \times 2 \times 3 = 12$$

em que se dividem sucessivamente os dois números por seus fatores primos comuns.

4.3 O ALGORITMO DE EUCLIDES

Apresentaremos agora o *algoritmo de Euclides*, uma maneira bem mais eficiente de calcular máximos divisores comuns. Demonstraremos, em primeiro lugar, que:

Teorema 4.3. *Sejam* $\mathtt{a}$ *e* $\mathtt{b}$ *números naturais, com* $\mathtt{a} > \mathtt{b}$ *e tais que* $\mathtt{b}$ *não divide* $\mathtt{a}$. *Se*

$$\mathtt{a} = \mathtt{bq} + \mathtt{r}, \qquad \mathtt{r} < \mathtt{b},$$

Então m.d.c.($\mathtt{a}$, $\mathtt{b}$) = m.d.c.($\mathtt{b}$, $\mathtt{r}$).

Demonstração: Pelo algoritmo da divisão, $\mathtt{a} = \mathtt{bq} + \mathtt{r}$, donde $\mathtt{r} = \mathtt{a} - \mathtt{bq}$. Se o número natural $\mathtt{d}$ divide $\mathtt{a}$ e $\mathtt{b}$, então $\mathtt{d}|\mathtt{r}$. Como já sabemos que $\mathtt{d}|\mathtt{b}$, segue-se que $\mathtt{d}|\mathtt{b}$ e $\mathtt{d}|\mathtt{r}$. Assim, mostramos que todo divisor de $\mathtt{a}$ e de $\mathtt{b}$ é um divisor de $\mathtt{b}$ e de $\mathtt{r}$. Por outro lado, se $\mathtt{d}$ divide $\mathtt{b}$ e $\mathtt{r}$, como $\mathtt{a} = \mathtt{bq} + \mathtt{r}$, segue-se imediatamente que $\mathtt{d}|\mathtt{a}$. Como $\mathtt{d}|\mathtt{b}$, então vemos que $\mathtt{d}|\mathtt{a}$ e $\mathtt{d}|\mathtt{b}$. Ou seja, todo divisor de $\mathtt{b}$ e de $\mathtt{r}$ é um divisor de $\mathtt{a}$ e de $\mathtt{b}$. Ora, se o conjunto dos divisores de $\mathtt{a}$ e de $\mathtt{b}$ coincide com o conjunto dos divisores de $\mathtt{b}$ e de $\mathtt{r}$, então m.d.c.($\mathtt{a}$, $\mathtt{b}$) = m.d.c.($\mathtt{b}$, $\mathtt{r}$), como queríamos demonstrar. □

A aplicação sucessiva deste resultado permite achar, rapidamente, o m.d.c. de dois inteiros.

Exemplo 4.8. *Calcule o* m.d.c.(178, 39).

Solução:

$$178 = 39 \times 4 + 22, \tag{1}$$

$$39 = 22 \times 1 + 17, \tag{2}$$

$$22 = 17 \times 1 + 5, \tag{3}$$

$$17 = 5 \times 3 + 2, \tag{4}$$

$$5 = 2 \times 2 + 1, \tag{5}$$

logo

$$\text{m.d.c.}(178,\, 39) = \text{m.d.c.}(39,\, 22) = \text{m.d.c.}(22,\, 17)$$

$$= \text{m.d.c.}(17,\, 5) = \text{m.d.c.}(5,\, 2) = \text{m.d.c.}(2,\, 1) = 1.$$

Na prática, dispomos as operações deste processo no seguinte dispositivo:

Apresentaremos agora uma demonstração geral do *algoritmo de Euclides*.

Teorema 4.4. *Sejam* a, b *números naturais, com* $a > b$*, e tais que* b *não divide* a*.*

Se

$$a = bq_1 + r_1, \qquad r_1 < b. \tag{A}$$

$$b = r_1 q_2 + r_2, \qquad r_2 < r_1, \tag{B}$$

$$r_1 = r_2 q_3 + r_3, \qquad r_3 < r_2, \tag{C}$$

$$\dots$$

$$r_{n-2} = r_{n-1} q_n + r_n, \qquad r_n < r_{n-1}, \tag{D}$$

$$\dots$$

$$r_{s-3} = r_{s-2}q_{s-1} + r_{s-1} \tag{E}$$

$$r_{s-2} = r_{s-1}q_s. \tag{F}$$

Então m.d.c.$(a, b) = r_{r-1}$.

Demonstração: Pela unicidade do quociente e do resto na algoritmo da divisão, vemos que as igualdades A, B, C, D, E e F acima são obtidas aplicando sucessivamente este algoritmo a a e b, b e r_1, ..., r_{n-2} e ..., r_{s-3} e r_{s-2}, e a r_{s-2} e r_{s-1}.

Certamente chegamos, por aplicaçSes sucessivas do algoritmo da divisão, a um estágio em que o resto é nulo, pois a sucessão dos restos, $r_1, r_2, r_3, \ldots$ é uma sucessão estritamente decrescente de números naturais.

Pelo Teorema 4.3, temos então

$$\text{m.d.c.}(a, b) = \text{m.d.c.}(b, r_1) = \text{m.d.c.}(r_1, r_2) = \ldots = \text{m.d.c.}(r_{s-2}r_{s-1}, =)r_{s-1}.$$

Ou seja, o último resto não-nulo nesta sequência de divisões sucessivas é o m.d.c.(a, b).

□

Dois números naturais a e b são *relativamente primos* se m.d.c.$(a, b) = 1$. Dizemos também que a é *primo com* b, ou que a e b são *primos entre si*. Observe que, em termos das decomposições de a e de b em fatores primos, dizer que a e b são relativamente primos quer dizer que eles não têm fatores primos comuns. Isso é uma consequência imediata da primeira maneira dada acima para calcular o máximo divisor comum de dois números.

O Teorema 3.6 pode ser generalizado como segue:

Exemplo 4.9. *Se* $p|ab$, *e* m.d.c.$(p, a) = 1$, *então* $p|b$.

Demonstração: A demonstração é imediata. Pelo teorema fundamental da Aritmética, p é fator primo de ab. Ora, na decomposição em fatores primos de a não comparece o primo p, pois a e p são relativamente primos. Então, p deve forçosamente comparecer na decomposição de b em fatores primos. □

A função estudada no exemplo a seguir é importante em Teoria dos Números.

Exemplo 4.10. *Seja* n *um número natural. Quantos números naturais menores que ou iguais a* n *são relativamente primos com* n?

Solução: Uma aplicação direta do princípio da inclusão-exclusão da Análise Combinatória [14] mostra que se

$$\mathfrak{n} = \mathfrak{p}_1^{\mathfrak{r}_1} \cdot \mathfrak{p}_2^{\mathfrak{r}_2} \cdots \mathfrak{p}_s^{\mathfrak{r}_s},$$

então

$$\phi(\mathfrak{n}) = \mathfrak{n}(1 - \frac{1}{\mathfrak{p}_1})(1 - \frac{1}{\mathfrak{p}_2}) \cdots (1 - \frac{1}{\mathfrak{p}_s}).$$

□

O número de naturais menores do que $\mathfrak{n}$ e primos com $\mathfrak{n}$ é claramente uma função de $\mathbf{N}$ em $\mathbf{N}$. Ela é chamada *função* ϕ *de Euler*[15], ou *função tociente.*

4.4 O MÍNIMO MÚLTIPLO COMUM

Sejam $\mathfrak{a}$ e $\mathfrak{b}$ dois números naturais. Considere os conjuntos dos múltiplos de $\mathfrak{a}$ e de $\mathfrak{b}$ respectivamente. A intersecção destes dois conjuntos é não vazia, pois o número natural $\mathfrak{a} \cdot \mathfrak{b}$ pertence a ambos. Pelo princípio da boa ordenação, esta intersecção possuirá então um menor elemento, que será chamado de *mínimo múltiplo comum de* $\mathfrak{a}$ *e de* $\mathfrak{b}$ e representado por m.m.c.($\mathfrak{a}$, $\mathfrak{b}$) ou por $[\mathfrak{a}, \mathfrak{b}]$.

Exemplo 4.11. *Ache o mínimo múltiplo comum de* 48 *e* 30.

Solução: O conjunto A dos múltiplos de 48 é:

$$\{48, 96, 144, 192, 240, 288, 336, \ldots\}.$$

O conjunto B dos múltiplos de 50 é:

$$\{30, 60, 90, 120, 150, 180, 210, 240, 270, 300, 330, 360, \ldots\}.$$

Assim, $A \cap B = \{240, \ldots\}$, e seu menor elemento é 240, que será o mínimo múltiplo comum de 48 e 30.

---

[14] Veja o livro Análise Combinatória e Probabilidade nesta coleção.

[15] Matemático suiço (1707-1783), deixou trabalhos importantes em Análise Matemática, Teoria dos Números, Astronomia, Combinatória e outras áreas. Trabalhou nas Academias de Berlim e de São Peterburgo.

Na prática, usamos o seguinte dispositivo para calcular o mínimo múltiplo comum utilizando a decomposição em fatores primos dos dois números:

Exemplo 4.12. *Sejam* a *e* b *números naturais cujas decomposições em produto de fatores primos são, como no Exemplo 3.4,*

$$a = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n},$$
$$b = q_1^{s_1} q_2^{s_2} \cdots q_t^{s_t}.$$

Então

$$\text{m.m.c.}(a, b) = z_1^{d_1} \cdot z_2^{d_2} \cdots z_k^{d_k},$$

onde os z_i são os primos que aparecem na decomposição de a ou de b, e d_i é o maior dos expoentes com que z_i comparece (obviamente, quando zi só comparecer na decomposição de um dos números a ou b, então d_i será o expoente de z_i naquela decomposição).

Demonstração: Observe, em primeiro lugar que, como $n^0 = 1$ para qualquer número natural, podemos escrever que $a = p_1^{r_1} p_2^{r_2} \cdot \ldots \cdot p_n^{r_n} \cdot q_1^0 q_2^0 \cdot \ldots \cdot q_t^0$, e que $b = p_1^0 p_2^0 \cdots p_n^0 \cdot q_1^{s_1} q_2^{s_2} \cdot \ldots \cdot q_t^{s_t}$.

Ou seja, unificando a notação para evitarmos primos p_i e q_j e expoentes r_i e s_j, podemos escrever

$$a = z_1^{n_1} z_2^{n_2} \cdots z_k^{n_k}$$

e

$$b = z_1^{m_1} z_2^{m_2} \cdots z_k^{m_k},$$

onde os expoentes m_i e n_i são não-negativos.

Defina agora d_i =máximo de n_i e m_i, $\quad 1 \leq i \leq k$. Afirmamos que

$$\text{m.m.c.}\,(a,\, b) = z_1^{d_1} \cdot z_2^{d_2} \cdots z_k^{d_k}.$$

É claro que, como $d_1 \geq n_1,\ m_1, \quad d_2 \geq n_2,\ m_2, \ldots, d_k \geq n_k,\ m_k$, temos que

$$z_1^{n_1} z_2^{n_2} \cdots z_k^{n_k} | z_1^{d_1} z_2^{d_2} \cdots z_k^{d_k},$$

e que

$$z_1^{m_1} z_2^{m_2} \cdots z_k^{m_k} | z_1^{d_1} z_2^{d_2} \cdots z_k^{d_k}.$$

Fazendo $t = z_1^{d_1} z_2^{d_2} \cdots z_k^{d_k}$, acabamos de mostrar que $a|t$ e $b|t$. Ou seja, t é um múltiplo comum de a e b.

É claro que t é o *menor* múltiplo comum de a e de b. Com efeito, seja m um múltiplo qualquer de a. Ele deve ter, em sua decomposição em fatores primos, todos os primos que comparecem na decomposição em fatores primos de a com expoentes maiores ou iguais aos respectivos expoentes na decomposição de a. Como m também é múltiplo de b, podemos dizer o mesmo em relação aos expoentes da decomposição em primos de b. Assim, cada primo z_i comparece na decomposição em primos de m e seu expoente é maior ou igual a d_i. Como $t = z_1^{d_1} z_2^{d_2} \cdots z_k^{d_k}$, ele é o menor dos múltiplos de a e de b. □

Existe, entre o máximo divisor comum e o mínimo múltiplo comum de dois números naturais, a relação demonstrada abaixo, resultado dos exemplos 4.5 e 4.11:

Exemplo 4.13. *Sejam* a *e* b *dois números naturais. Então* $\text{m.m.c.}\,(a,\, b) \cdot \text{m.d.c}\,(a,\, b) = a \cdot b$.

Demonstração: Com efeito, dados dois números naturais r e s, mostremos que vale sempre que $\min\{r,\, s\} + \max\{r,\, s\} = r + s$. Se $r < s$, então $\min\{r,\, s\} = r$, $\max\{r,\, s\} = s$, e temos o resultado desejado. A demonstração para o caso em que $r > s$ é inteiramente análoga.

Agora, usando a notação dos exemplos 4.5 e 4.11, temos: $p_i^{c_i} \cdot p_i^{d_i} = p_i^{c_i + d_i} = p_i^{n_i + m_i} = p_i^{n_i} \cdot p_i^{m_i}$, e segue-se o resultado desejado. □

EXERCÍCIOS

4.1. Ache o m.d.c.(256, 48) diretamente a partir da definição, isto é, achando o conjunto dos divisores de 256, de 48 e sua intersecção.

4.2. Ache o m.d.c.(256, 48) usando a decomposição em fatores primos.

4.3. Ache o m.d.c.(256, 48) usando o algoritmo de Euclides.

4.4. Reveja a definição da seqüência de Fibonacci (Capítulo 1, Exercício 27). Calcule a máximo divisor comum entre o décimo quinto e o décimo sexto termos da seqüência.

4.5. Ache o m.d.c.(14, 128) usando o algoritmo de Euclides.

4.6. Calcule m.d.c.(n, $n+1$), onde n é um número natural.

4.7. Calcule m.d.c.(n, $n+2$), onde n é um número natural.

4.8. Se $b|c$, então m.d.c.(a, b) = m.d.c.($a+c$, b).

4.9. Se m.d.c.(a, b) = 1, demonstre que m.d.c.(a^m, b^n) = 1, para m e n inteiros positivos.

4.10. Se m.d.c.(m_i, m) = 1, para $i = 1, 2, \ldots, k$, mostre que m.d.c.($m_1 m_2 \cdots m_k$, m) = 1.

4.11. Para cercar um terreno de forma retangular e de dimensões 48 e 36 metros respectivamente, deseja-se fixar o menor número possível de estacas, de modo que as distâncias entre duas estacas consecutivas sejam iguais e que haja uma estaca em cada um dos vértices do terreno. Determine o número de estacas.

4.12. Cinco pessoas, uma das quais tinha um macaco, compraram um saco de cocos, e combinaram dividí-los no dia seguinte. Um dos homens levantou-se durante a noite e decidiu retirar logo sua parte. Abriu o saco, dividiu os cocos por 5, obtendo um coco de resto, que foi dado ao macaco. O homem retirou sua parte, recolocou os cocos restantes no saco e deitou-se. Mais tarde, outro homem levantou-se, decidiu também retirar sua parte, e para isso dividiu os cocos por 5, obtendo um coco de resto, que foi dado ao macaco. Após ficar com sua parte e recolocar os cocos no saco, o homem deitou-se. Os três homens restantes agiram de mesma maneira, obtendo cada um deles resto um, que foi dado ao macaco. Na manhã seguinte, os 5 homens se reuniram, dividiram os cocos por 5, e obtiveram um de resto, que foi dado ao macaco. Determinar o menor número de cocos para que o processo descrito acima possa ocorrer.

4.13. Demonstre que $5x + 13y$ e $x + 6y$ são múltiplos de 17 para os mesmos valores naturais de x e y.

4.14. Qual o maior valor que pode ter a razão de uma progressão aritmética que admita 32, 227 e 942 como termos da progressão.

4.15. Determine números naturais a e b tais que $a + b = 168$ e m.d.c.$(a, b) = 24$.

4.16. Determine números naturais a e b tais que $a + b = 35$ e m.m.c.$(a, b) = 60$.

4.17. Os números naturais a e b são tais que m.d.c.$(a, b) = d$. Prove que exatamente d elementos do conjunto $\{a, 2a, 3a, \ldots, ba\}$ são divisíveis por b.

4.18. Sejam m e n números naturais, $p =$ m.d.c.(m, n) e $A_m = \{z \in \mathbb{C} \text{ tais que } z^m = 1\}$. A_n e A_p são definidos analogamente. Demonstre que $A_m \cap A_n = A_p$.

4.19. Em um tabuleiro $m \times n$, as bordas são espelhadas. Um raio de luz parte de um dos vértices do tabuleiro, na direção da diagonal da casa que contém este vértice. Quantas casas o raio de luz atravessa?

4.20. Você tem um pedaço de papel que pode ser cortado em 8 ou 12 pedaços. Cada um desses pedaços pode ser novamente cortado em 8 ou 12 pedaços e assim sucessivamente. Como fazer para obter 70 pedaços?

4.21. O máximo divisor comum de mais de dois números naturais é definido recursivamente por m.d.c.$(a_1, a_2, \ldots, a_n)$ = m.d.c.{m.d.c.$(a_1, a_2, \ldots, a_{n-1}), a_n\}$.

a) Prove que m.d.c.$(a_1, a_2, \ldots a_n)$ é um divisor comum de $a_1, a_2, \ldots, a_n$.

b) Demonstre que se t é um divisor comum dos números naturais $a_1, a_2, \ldots a_n$, então t divide m.d.c. $(a_1, a_2, \ldots a_n)$.

c) Se t é um divisor comum de $a_1, a_2, \ldots a_n$, então $|t| \leq$ m.d.c.$(a_1, a_2, \ldots a_n)$.

4.22. O mínimo múltiplo comum de mais de dois números naturais é definido recursivamente por m.m.c.$(a_1, a_2, \ldots a_n)$ = m.m.c.(m.m.c.$(a_1, a_2, \ldots a_{n-1}), a_n)$.

a) Prove que m.m.c.$(a_1, a_2, \ldots a_n)$ é um múltiplo comum de $a_1, a_2, \ldots a_n$.

b) Demonstre que se t é um múltiplo comum de $a_1, a_2, \ldots a_n$, então t é múltiplo do m.m.c.$(a_1, a_2, \ldots a_n)$.

c) Prove que se t é um múltiplo comum de $a_1, \ldots a_n$, então, $t \geq$ m.m.c.$(a_1, \ldots a_n)$.

4.23. Determine o menor número natural positivo que dividido por 2 deixa resto 1, dividido por 3 deixa resto 2, dividido por 4 deixa resto 3, dividido por 5 deixa resto 4 e dividido por 6 deixa resto 5.

4.24. Determine todos os números naturais que divididos por 3 deixam resto 1, divididos por 4 deixam resto 2 e divididos por 5 deixam resto 3.

4.25. Suponha que os planetas descrevem órbitas circulares, com centro no Sol, e os períodos de Júpiter, Saturno e Urano são, respectivamente, 12 anos, 30 anos e 84 anos.

a) Daqui a quanto tempo estes três planetas estarão, pela primeira vez, simultaneamente, novamente nas mesmas posições, em relação ao Sol, em que se encontram agora?

b) Daqui a quanto tempo estes três planetas estarão simultaneamente nas posições diametralmente opostas em relação ao Sol às posições que ocupam atualmente?

4.26. Determine m.d.c.(a, b) onde a é o número que tem m algarismos, todos iguais a 1, e b é o número que tem n algarismos, todos iguais a 1.

4.27. Mostre que o m.d.c. d de dois números naturais a e b tem as seguintes propriedades:

a) $\mathtt{d}$ é um divisor comum de $\mathtt{a}$ e de $\mathtt{b}$.

b) Se $\mathtt{h}$ é um divisor comum de $\mathtt{a}$ e de $\mathtt{b}$, então $\mathtt{h}$ é divisor de $\mathtt{d}$.

4.28. Reciprocamente, mostre que se o número natural $\mathtt{d}$ goza das duas propriedades do exercício anterior, então $\mathtt{d}$ = m.d.c.($\mathtt{a}$, $\mathtt{b}$).

4.29. Sejam $\mathtt{f}_n$ e $\mathtt{f}_{n+1}$ dois termos consecutivos quaisquer da seqüência de Fibonacci. Mostre que m.d.c.($\mathtt{f}_n$, $\mathtt{f}_{n+1}$)=1.

CAPÍTULO 5

CONGRUÊNCIAS, O TEOREMA CHINÊS DO RESTO E DIVISIBILIDADE

5.1 CONGRUÊNCIAS

O alemão Karl Friedrich Gauss (1777, 1855), um dos maiores matemáticos que já viveram, introduziu o conceito de *congruência*, fundamental em Teoria dos Números, a parte da Matemática que investiga as propriedades dos números inteiros.

Seja $\mathfrak{m}$ um inteiro positivo. Dois inteiros $\mathfrak{a}$ e $\mathfrak{b}$ são *congruentes (ou côngruos) módulo* $\mathfrak{m}$ se e somente se $\mathfrak{m}$ divide $\mathfrak{a} - \mathfrak{b}$. Quando isso acontece, escrevemos

$$\mathfrak{a} \equiv \mathfrak{b} \pmod{\mathfrak{m}}.$$

Temos, por exemplo,

$$7 \equiv 2 \pmod{5},$$

pois $7 - 2 = 5 = 5 \cdot 1$;

$$4 \equiv -2 \pmod{3},$$

pois $4 - (-2) = 6 = 3.2$;

$$-1 \equiv 14 \pmod{5},$$

pois $-1 - 14 = -15 = (-3) \cdot 5$.

Por outro lado, $5 \not\equiv 11 \pmod{7}$, pois $5 - 11 = 6$, que não é um múltiplo de 7.

É freqüentemente mais fácil verificar se dois inteiros $\mathfrak{a}$ e $\mathfrak{b}$ são congruentes módulo $\mathfrak{m}$ examinando os restos de suas divisões por $\mathfrak{m}$.

Teorema 5.1. *Dois inteiros* a *e* b *são côngruos* $\pmod{m}$ *se e somente se os restos de suas divisões por* m *são iguais.*

Demonstração: De fato, suponha que $a \equiv b \pmod{m}$ e que r_1 e r_2 sejam os restos da divisão de a e b, respectivamente, por m. Então,

$$a = mq_1 + r_1, \quad b = mq_2 + r_2, \ \ 0 \leq r_1,\ r_2 < m.$$

Podemos supor, sem perda de generalidade, que $r_2 \leq r_1$. Então

$$a - b = m(q_1 - q_2) + (r_1 - r_2),$$

com $0 \leq r_1 - r_2 < m$. Se $a \equiv b \pmod{m}$, $a - b$ é múltiplo de m ou seja, o resto $(r_1 - r_2)$ da divisão de $a - b$ por m é nulo, e assim $r_1 = r_2$, isto é, a e b deixam o mesmo resto quando divididos por m.

Reciprocamente, se a e b deixam o mesmo resto quando divididos por m, isto é, se $r_1 = r_2$, então $a - b = m(q_1 - q_2)$, ou seja, $a - b$ é múltiplo de m. Logo, por definição, $a \equiv b \pmod{m}$. □

Conseqüências imediatas deste teorema são os seguintes resultados

Exemplo 5.1. *Sejam* a *um inteiro e* m *um inteiro positivo. Se* $a = qm + r$, *então* $a \equiv r \pmod{m}$. □

Exemplo 5.2. *Um número inteiro* a *é par se e somente se* $a \equiv 0 \pmod{2}$*; ele é ímpar se e somente se* $a \equiv 1 \pmod{2}$.

Demonstração: Com efeito, se a é par, então existe b tal que $a = 2b$; ou seja, o resto da divisão de a por 2 é 0. Por outro lado, se a é ímpar, o resto da divisão de a por 2 é 1. Estas duas possibilidades são as únicas, visto que os restos possíveis na divisão por 2 são 0 e 1. □

Em geral, temos o seguinte resultado:

Teorema 5.2. *Seja* a *um inteiro e* m *um número natural. Então* a *é côngruo, módulo* m*, a um dos inteiros* $0, 1, 2, \cdots, m-2, m-1$.

Demonstração: De fato, estes são todos os restos possíveis na divisão de a por m. □

(Obs: Na definição de congruência, poderíamos aceitar módulos negativos. Mas isso não representa nenhum ganho em generalidade, visto que se m é negativo e $a \equiv b \pmod{m}$, então certamente $a \equiv b \pmod{-m}$, pois se $a - b = km$, então $a - b = (-k)(-m)$, onde $-m$ é positivo.

A congruência se assemelha muito com a igualdade de inteiros.

Exemplo 5.3. *Mostre que a relação de congruência é uma relação de equivalência.*

Demonstração: Em primeiro lugar, $a \equiv a \pmod{m}$, pois $a - a = 0 \cdot m$. Assim, ser côngruo é uma relação reflexiva.

Em segundo lugar, se $a \equiv b \pmod{m}$, então existe k inteiro tal que $a - b = k \cdot m$. Mas então $b - a = (-k) \cdot m$, logo b é côngruo a $a \pmod{m}$. Assim, a congruência é uma relação simétrica.

Em terceiro lugar, suponha que $a \equiv b \pmod{m}$ e que $b \equiv c \pmod{m}$. Existem então inteiros k_1 e k_2 tais que

$$a - b = k_1 m,$$

$$b - c = k_2 m.$$

Mas então $a - c = (k_1 + k_2) \cdot m$, ou seja, $a \equiv c \pmod{m}$, como queríamos demonstrar. □

Teorema 5.3. *Se x é um inteiro qualquer e $a \equiv b \pmod{m}$, então—?*:

a) $a + x \equiv b + x \pmod{m}$;

b) $ax \equiv bx \pmod{m}$.

Demonstração:

a) Se $a \equiv b \pmod{m}$, existe então um número inteiro k tal que $a - b = km$, donde $a + (x - x) - b = km$, donde $a + x + (b + m) = km$, ou seja, $a + x = b + x \pmod{m}$.

b) Se $a \equiv b \pmod{m}$, então $a - b = km$, donde $ax - bx = (kx)m$, donde $ax \equiv bx \pmod{m}$. □

Uma consequência fácil destas duas propriedades e da transitividade da congruência é o teorema a seguir.

Teorema 5.4. *Se* $a \equiv b \pmod{m}$, *e* $c \equiv d \pmod{m}$, *então a)* $a + c \equiv b + d \pmod{m}$ *b)* $a \cdot c \equiv b \cdot d \pmod{m}$.

Demonstração:

a) Como $a \equiv b \pmod{m}$, segue-se que $a + c \equiv b + c \pmod{m}$. Como $c \equiv d \pmod{m}$, vem que $c + d \equiv b + c \pmod{m}$. Daí segue-se que $a + c \equiv b + c \equiv b + d \pmod{m}$, ou seja, $a + c \; equivb + d \pmod{m}$, como queríamos demonstrar.

b) A demonstração deste item é análoga: Se $a \equiv b \pmod{m}$, então $a \cdot c \equiv b \cdot c \pmod{m}$; se $c \equiv d \pmod{m}$, então $b \cdot c \equiv b \cdot d \pmod{m}$. Vem assim que $a \cdot b \equiv c \cdot d \pmod{m}$. □

Há contudo diferenças importantes entre a relação de igualdade e a de congruência. Por exemplo, um fato muito importante na Aritmética dos inteiros é que se $ab = ac$ e $a \neq 0$, então $b = c$ (é a chamada lei do cancelamento). Para congruências isso em geral não é válido. Por exemplo, embora $2 \cdot 5 \equiv 2 \cdot 2 \pmod{6}$, não é verdade que $5 \equiv 2 \pmod{6}$. No entanto, vale o seguinte resultado:

Teorema 5.5. *Sejam* a, b *e* c *números inteiros com* m.d.c.$(c, m) = 1$*; se* $ca \equiv cb \pmod{m}$, *então* $a \equiv b \pmod{m}$.

Demonstração: Com efeito, dizer que $ca \equiv cb \pmod{m}$ significa que existe um inteiro q tal que $(ca - cb) = qm$. Ou seja, $qm = c(a - b)$. Assim, m divide $c(a - b)$. Como m não divide c, pois são relativamente primos, então $m|(a - b)$, isto é, $a \equiv b \pmod{m}$. □

Podemos também trabalhar com equações lineares módulo um inteiro m.

Teorema 5.6. *Sejam* a, b *e* m *números inteiros. Se* m.d.c.$(a, m) = 1$, *então a equação* $ax \equiv b \pmod{m}$ *tem soluções inteiras. Duas soluções quaisquer são congruentes* $\pmod{m}$. *Além disso, se* x_0 *é solução e* $y \equiv x_0 \pmod{m}$, *então* y *também é solução.*

Demonstração: Com efeito, se m.d.c.$(a, m) = 1$, sabemos que existem inteiros r e s tais que

$$ar + sm = 1.$$

Então

$$arb + smb = b,$$

donde

$$a(rb) - b = -(sb)m,$$

isto é,

$$a(rb) \equiv b \pmod{m},$$

e $x = rb$ é solução da equação dada.

Por outro lado, se

$$ar_1 \equiv b \pmod{m},$$

$$ar_2 \equiv b \pmod{m},$$

segue-se que $ar_1 \equiv ar_2 \pmod{m}$ (por quê?), e como m.d.c.$(a, m) = 1$, decorre que $r_1 \equiv r_2 \pmod{m}$, pelo Exemplo 5.4. Além disso, se x_0 é solução e $y \equiv x_0 \pmod{m}$, temos $ay \equiv ax_0 \equiv b \pmod{m}$, e y também é solução. □

Assim, por exemplo a equação $3x \equiv 1 \pmod{5}$ tem solução, pois m.d.c.$(3, 5) = 1$. Uma solução é $x = 7$. As outras soluções são da forma $x = 7 + k \cdot 5$, k um inteiro arbitrário. Já a equação $6x \equiv 1 \pmod{8}$ não tem solução, visto que $6x - 1$ é sempre um número ímpar, para x qualquer, e portanto não pode ser um múltiplo de 8. Observe que m.d.c.$(6, 8) = 2$.

Exemplo 5.4. *Ache as soluções de* $3x \equiv 5 \pmod{7}$.

Solução: Se x é solução da congruência acima, então existe um inteiro k tal que $3x = 5 + 7k$, donde $3x - 7k = 5$. Ou seja, verificar se a congruência $3x \equiv 5 \pmod{7}$ é equivalente a resolver a equação diofantina $3x - 7k = 5$, a qual obviamente tem solução pois m.d.c.$(3, 7)$ é divisor de 5. □

Exemplo 5.5. *Ache todas as soluções (se elas existirem!) da congruência* $6x \equiv 4 \pmod{8}$.

Solução: Resolver esta congruência é equivalente a resolver a equação diofantina $6x - 8k = 4$. Como m.d.c.(6, 8) divide 4, vemos que a equação diofantina tem solução, e o mesmo acontecerá com a congruência. Uma solução da equação diofantina é $k = 2$, $x = 2$. Todas as outras soluções da congruência serão côngruas a essa, módulo 8. □

Em verdade, a observação abaixo melhora este resultado.

Observação: Voltando às soluções apresentadas para a equação diofantina $ax+by = c$, $x = x_0 + (b/d)k$, $y = y_0 - (a/d)k$, onde k é um inteiro qualquer, e d é o m.d.c.(a, b) e (x_0, y_0) é uma solução particular, vemos que, na linguagem das congruências, $x \equiv x_0 \pmod{b/d}$ e $y \equiv y_0 \pmod{a/d}$ Assim, no exemplo precedente, podemos mesmo afirmar que todas as soluções da congruência $6x \equiv 4 \pmod 8$ são côngruas a 2 módulo 4, pois neste caso $d = 2$.

Exemplo 5.6. *Se p é um número primo, mostre que as únicas soluções de $x^2 \equiv 1 \pmod p$ são 1 e -1.*

Demonstração: Com efeito, $x^2 \equiv 1 \pmod p \iff x^2 - 1 \equiv 0 \pmod p \iff (x - 1)(x + 1) \equiv 0 \pmod p \iff p|(x - 1)(x + 1)$. Como p é primo, então ou p divide $x - 1$, ou p divide $x + 1$. No primeiro caso, $x \equiv 1 \pmod p$; no segundo, $x \equiv -1 \pmod p$. □

Vejamos agora algumas aplicações das congruências.

Exemplo 5.7. *Mostraremos, em primeiro lugar, que $10^k \equiv 1 \pmod 9$, para todo inteiro k não-negativo.*

Demonstração: A demonstração é feita por indução. Com efeito, se $k = 0$, $10^k = 10^0 = 1 \equiv 1 \pmod 9$.

Suponha portanto que $10^k \equiv 1 \pmod 9$. Como $10 \equiv 1 \pmod 9$, segue-se imediatamente que $10^{k+1} \equiv a0^k \times 10 \equiv 1 \times 1 = 1 \pmod 9$. □

Exemplo 5.8. *Seja $N = 22 \times 31 + 11 \times 17 + 13 \times 19$. Sem efetuar as operações,*

a) *Determine se N é par ou ímpar;*

b) *Ache o algarismo das unidades de N;*

c) *Ache o resto da divisão de N por 7.*

Solução:

a) Como

$$22 \equiv 0 \pmod 2,$$

$$31 \equiv 1 \pmod 2,$$

$$11 \equiv 1 \pmod 2,$$

$$17 \equiv 1 \pmod 2,$$

$$13 \equiv 1 \pmod 2,$$

$$19 \equiv 1 \pmod 2,$$

segue-se

$$\mathfrak{n} \equiv 0.1 + 1.1 + 1.1 \equiv 2 \equiv 0 \pmod 2,$$

e portanto $\mathfrak{n}$ é par.

b) Como $22 \equiv 2 \pmod{10}$, e $31 \equiv 1 \pmod{10}$, segue-se que $22 \times 31 \equiv 2 \pmod{10}$. De $11 \equiv 1 \pmod{10}$, $17 \equiv 7 \pmod{10}$, segue-se que $11 \times 17 \equiv 7 \pmod{10}$. Além disso, $13 \equiv 3 \pmod{10}$ e $19 \equiv 9 \pmod{10}$ acarretam que $13 \times 19 \equiv 27 \equiv 7 \pmod{10}$. Então $\mathsf{N} \equiv 2 + 7 + 7 \equiv 6 \pmod{10}$.

Ora se

$$\mathsf{N} = \mathfrak{a}_k 10^k + \mathfrak{a}_{k-1} 10^{k-1} + ... + \mathfrak{a}_1 10 + \mathfrak{a}_0,$$

como

$$10^{\mathfrak{i}} \equiv 0 \pmod{10},\ \mathfrak{i} \geq 1,$$

vemos que $\mathsf{N} \equiv \mathfrak{a}_0 \pmod{10}$. Ou seja, N *é congruo a seu algarismo das unidades* (mod 10). Assim, o algarismo das unidades de N é côngruo a 6 e como $0 \leq \mathfrak{a}_0 \leq 9$, $\mathfrak{a}_0 = 6$.

c) Temos

$$22 \equiv 1 \pmod 7,$$

$$31 \equiv 3 \pmod 7,$$

donde

$$22 \times 31 \equiv 3 \pmod 7.$$

Como

$$11 \equiv 4 \pmod 7,$$

$$17 \equiv 3 \pmod 7;$$

portanto

$$11 \times 17 \equiv 12 \equiv 5 \pmod 7.$$

De

$$13 \equiv 6 \pmod 7$$

$$19 \equiv 5 \pmod 7;$$

segue-se

$$13 \times 19 \equiv 30 \equiv 2 \pmod 7.$$

Assim,

$$\mathsf{N} \equiv 3 + 5 + 2 \equiv 10 \equiv 3 \pmod 7,$$

ou seja, N deixa resto 3 quando dividido por 7. □

Exemplo 5.9. *Sejam* $\mathfrak{a}_1$ *e* $\mathfrak{a}_0$ *os algarismos respectivamente das dezenas e das unidades de um inteiro* N. *Mostre que* $\mathsf{N} \equiv 10\mathfrak{a}_1 + \mathfrak{a}_0 \pmod{100}$.

Demonstração: Com efeito, mais uma vez escreva

$$\mathsf{N} = \mathfrak{a}_k 10^k + \mathfrak{a}_{k-1} 10^{k-1} + ... + \mathfrak{a}_1 10 + \mathfrak{a}_0.$$

Vemos então que

$$\mathfrak{a}_i 10^i \equiv 0 \pmod{100},$$

se $i \geq 2$. Então

$$\mathsf{N} \equiv \mathfrak{a}_1 10 + \mathfrak{a}_0 \pmod{100}.$$

□

Exemplo 5.10. *Ache os dois últimos algarismos de* 3^{1234}.

Solução: Observe que

$$\begin{aligned} 3^2 &\equiv 9 \pmod{100}, \\ 3^4 &\equiv 81 \pmod{100}, \\ 3^8 \equiv 81 \times 81 &\equiv 61 \pmod{100}, \\ 3^{10} \equiv 61 \times 9 &\equiv 49 \pmod{100}, \\ 3^{20} \equiv 49 \times 49 \equiv 2401 &\equiv 1 \pmod{100}. \end{aligned}$$

Uma vez chegados a este ponto, nossas contas se tornam mais eficientes:

$$1234 = 20 \times 61 + 14,$$

donde

$$3^{1234} = (3^{20})^{61} \cdot 3^{14}.$$

Como $3^{20} \equiv 1 \pmod{100}$, vemos que

$$(3^{20})^{61} \equiv 1 \pmod{100}.$$

Então

$$3^{1234} \equiv 3^{14} \pmod{100}.$$

Mas

$$3^{14} = 3^{10} \cdot 3^4 \equiv 49 \times 81 \equiv 69 \pmod{100},$$

e achamos assim a resposta desejada. □

Exemplo 5.11. *Seja* $\mathfrak{m}$ *um inteiro. Mostre que* $\mathfrak{m}^2$ *é côngruo a* 0, *ou a* 1, *ou a* 4 (mod 8).

Demonstração: Com efeito, se $\mathfrak{m}$ é um inteiro, então $\mathfrak{m}$ é côngruo ou a 0, ou a 1, ou a 2, ou a 3 (mod 4) (estes são os restos possíveis na divisão de $\mathfrak{m}$ por 4).

Se $\mathfrak{m} \equiv 0 \pmod{4}$, então $\mathfrak{m} = 4\mathfrak{k}$, donde $\mathfrak{m}^2 = 16\mathfrak{k}^2 = 8 \cdot (2\mathfrak{k}^2) \equiv 0 \pmod{8}$.

Se $\mathfrak{m} \equiv 1 \pmod{4}$, então $\mathfrak{m} = 4\mathfrak{k}+1$, donde $\mathfrak{m}^2 = 16\mathfrak{k}^2+8\mathfrak{k}+1 = 8\cdot(2\mathfrak{k}^2+\mathfrak{k})+1 \equiv 1 \pmod{8}$.

Se $m \equiv 2 \pmod 4$, então $m = 4k+2$, donde $m^2 = 16k^2+16k+4 = 8\cdot(2k^2+2k)+4 \equiv 4 \pmod 8$.

Se $m \equiv 3 \pmod 4$, então $m = 4k+3$, donde $m^2 = 16k^2+24k+9 = 8\cdot(2k^2+3k)+9 \equiv 1 \pmod 8$.

E vemos assim que m^2 realmente é côngruo ou a 0, ou a 1 ou a 4 (mod 8). □

Assim, por exemplo 515 *não* é um quadrado perfeito, pois $515 = 8 \times 64 + 3$, ou seja, $515 = 3 \pmod 8$. Por outro lado, $68 \equiv 4 \pmod 8$, mas 68 não é um quadrado perfeito. Ou seja, a condição é necessária mas não é suficiente.

O resultado acima pode às vezes ser usado de maneira dramática para mostrar, quase que magicamente, que certos números não são quadrados perfeitos.

Exemplo 5.12. *O número* 894378 *é um quadrado perfeito*?

Solução: Como $894378 = 111797 \times 8 + 2$, segue-se que $894378 \equiv 2 \pmod 8$, e portanto não pode ser um quadrado perfeito! □

Exemplo 5.13. *Mostre que* $2^{70} + 3^{70}$ *é divisível por* 13.

Solução: Tomando todas as congruências módulo 13, temos

$$2^4 \equiv 3 \Rightarrow 2^8 \equiv 9 \Rightarrow 2^{16} \equiv 81 \equiv 3 \Rightarrow 2^{20} \equiv 2^{16} \cdot 2^4 \equiv 9 \Rightarrow$$
$$\Rightarrow 2^{60} \equiv 27 \equiv 1 \Rightarrow 2^{68} \equiv 2^{60} \cdot 2^8 \equiv 9 \Rightarrow$$
$$\Rightarrow 2^{70} \equiv 2^{68} \cdot 2^2 \equiv 36 \equiv -3.$$

$$3^3 \equiv 1 \Rightarrow 3^6 \equiv 1 \Rightarrow 3^{12} \equiv 1 \Rightarrow 3^{24} \equiv 1 \Rightarrow$$
$$\Rightarrow 3^{30} \equiv 1 \Rightarrow 3^{60} \equiv 1 \Rightarrow e^{66} \equiv 1 \Rightarrow 3^{69} \equiv 1 \Rightarrow 3^{70} \equiv 3.$$

Temos então

$$2^{70} + 3^{70} \equiv -3 + 3 \equiv 0 \pmod{13},$$

ou seja, $2^{70} + 3^{70}$ é múltiplo de 13, como queríamos demonstrar. □

Exemplo 5.14. *Defina a sucessão* $\{t_n\}$ *por* $t_1 = 7$, $t_2 = 7^{t_1} = 7^7$, $t_n = 7^{t_{n-1}}$. *Ache o algarismo das unidades de* t_n.

Solução: Tomemos congruências módulo 100:

$$7 \equiv 7,$$
$$7^2 \equiv 49,$$
$$7^3 \equiv 43,$$
$$7^4 \equiv 1,$$

e vemos assim que $7^{4q+r} \equiv 7^r \pmod{100}$.

Temos agora, tomando ainda congruências módulo 100,

$$t_1 \equiv 07$$
$$t_2 = 7^7 = 7^{4+3} \equiv 7^3 \equiv 43.$$

Afirmamos, que para $n \geq 2$, $t_n \equiv 43 \pmod{100}$. A demonstração é feita por indução. Com efeito, para $n = 2$, o resultado acabou de ser demonstrado. Suponhamos que ele seja válido para t_n e mostremos que então será válido para t_{n+1}. Ora

$$t_{n+1} = 7^{t_n} = 7^{100k+43} \equiv 7^{4\times 25\times k} \times 7^{40+3} \equiv 1 \times 7^3 \equiv 43,$$

como queríamos demonstrar. □

5.2 O TEOREMA CHINÊS DO RESTO

Já vimos critérios para decidir se a equação $ax \equiv b \pmod{m}$ tem solução. O teorema abaixo trata de sistemas de congruências lineares.

Teorema 5.7. [Teorema Chinês do Resto[16]] *Sejam* $m_1, \ldots, m_s$ *inteiros positivos relativamente primos dois a dois* (*ou seja,* m.d.c.$(m_i, m_j) = 1$, *se* $i \neq j$). *Então, o sistema de congruências lineares*

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\ldots$$
$$x \equiv a_s \pmod{m_s}$$

possui uma única solução módulo $m_1 m_2 \cdots m_s$.

Demonstração: Para $k = 1, 2, \ldots, s$, seja $t_k = m_1 m_2 \cdots m_{k-1} m_{k+1} \cdots m_s$. Segue-se então da hipótese que m.d.c.$(t_k, m_k) = 1$.

Já sabemos que a congruência $t_k x \equiv 1 \pmod{m_k}$ tem uma solução única módulo m_k. Chamemos esta solução de x_k e consideremos o inteiro

$$b = a_1 t_1 x_1 + a_2 t_2 x_2 + \cdots + a_s t_s x_s.$$

Mostraremos que b é solução (única módulo $m_1 m_2 \cdots m_s$) do sistema de congruências dado.

De fato, se $i \neq k$, vemos que m_k divide t_i donde $t_i \equiv 0 \pmod{m_k}$. Então, $b \equiv a_k t_k x_k \pmod{m_k}$.

Mas x_k é solução da congruência $t_k x \equiv 1 \pmod{m_k}$, logo $t_k x_k \equiv 1 \pmod{m_k}$. Assim, $b \equiv a_k \cdot 1 \equiv a_k \pmod{m_k}$, e mostramos portanto que b é uma solução do sistema dado.

---

[16] Este teorema encontra-se em um texto matemático chinês escrito entre 280 e 473 de nossa era, o Sun Tzu Suan Ching, um dos mais antigos textos aritméticos chineses existentes.

Resta mostrar que esta solução é única módulo $m_1 m_2 \cdots m_s$. Ou seja, mostrar que duas soluções quaisquer do sistema são côngruas módulo $m_1 m_2 \cdots m_s$.

Seja portanto b' uma outra solução do sistema. Assim,

$$\begin{aligned} b &\equiv a_1 \equiv b' \pmod{m_1} \\ b &\equiv a_2 \equiv b' \pmod{m_2} \\ &\cdots \\ b &\equiv a_s \equiv b' \pmod{m_s}. \end{aligned}$$

Então $b - b'$ é um múltiplo de m_k, para todos os valores de k. Como temos, por hipótese, que m.d.c.$(m_i, m_j) = 1$, se $i \neq j$, segue-se portanto $m_1 m_2 \cdots m_s$ divide $b - b'$, donde $b \equiv b' \pmod{m_1 m_2 \cdots m_s}$, como queríamos demonstrar. □

Exemplo 5.15. *Resolva o sistema de congruências lineares*

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7. \end{aligned}$$

Solução: Observe, em primeiro lugar, que m.d.c.(3, 5) = m.d.c.(3, 7) = m.d.c.(5, 7) = 1. Assim, o sistema terá uma solução módulo $3 \cdot 5 \cdot 7 = 105$.

Temos que $t_1 = 35$, $t_2 = 21$, $t_3 = 15$ e consideremos as seguintes congruências lineares:

$$\begin{aligned} 35x &\equiv 1 \pmod 3, \\ 21x &\equiv 1 \pmod 5, \\ 15x &\equiv 1 \pmod 7. \end{aligned}$$

Suas soluções são, respectivamente, $x_1 = 2$, $x_2 = 1$, $x_3 = 1$.

Então o inteiro

$$b = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23$$

é a única solução (módulo 105) do sistema de congruências lineares dado. □

Uma consequência imediata do Teorema Chinês do Resto é o seguinte:

Exemplo 5.16. *Sejam* $m_1, \ldots, m_s$ *inteiros positivos relativamente primos dois a dois* (*ou seja),* m.d.c.$(m_i,\ m_j) = 1$, *se* $i \neq j$). *Sejam* $a_1, \ldots, a_s$ *inteiros tais que* m.d.c.$(a_k,\ m_k) = 1$, *para* $k = 1,\ \ldots, s$. *Então, o sistema de congruências lineares*

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2} \\ &\cdots \\ a_s x &\equiv b_s \pmod{m_s} \end{aligned}$$

possui uma única solução módulo $m_1 m_2 \cdots m_r$.

Demonstração: Como m.d.c.$(a_k,\ m_k) = 1$, para $k = 1, 2, \ldots, s$, já sabemos que a congruência linear $a_k x \equiv 1 \pmod{m_k}$ possui uma solução única módulo m_k. Seja a'_k esta solução. Ou seja, para cada k, $k = 1,\ 2,\ \ldots, s$, temos que $a_k a'_k \equiv 1 \pmod{m_k}$.

Assim, podemos substituir o sistema dado de congruências lineares pelo sistema *equivalente*

$$\begin{aligned} x &\equiv b_1 a'_1 \pmod{m_1} \\ x &\equiv b_2 a'_2 \pmod{m_2} \\ &\cdots \\ x &\equiv b_r a'_r \pmod{m_r}. \end{aligned}$$

Ora, pelo Teorema Chinês do Resto, este sistema tem uma solução única, o que conclui a demonstração. □

Exemplo 5.17. *Resolva o sistema de congruências*

Solução:

$$\begin{aligned} 2x &\equiv 1 \pmod{5} \\ 3x &\equiv 2 \pmod{7} \\ 4x &\equiv 3 \pmod{11}. \end{aligned}$$

Em primeiro lugar, os módulos das congruências são relativamente primos dois a dois. Além disso, temos que m.d.c.$(2,\ 5)$ = m.d.c.$(3,\ 7)$ = m.d.c.$(4,\ 11) = 1$. Assim, pelo exemplo anterior, o sistema de congruências terá uma solução única módulo $5 \times 7 \times 11 = 385$.

Achemos, em primeiro lugar, as soluções das congruências lineares $2x \equiv 1 \pmod 5$, $3x \equiv 1 \pmod 7$ e $4x \equiv 1 \pmod{11}$. As soluções são, respectivamente, 3, 5, 3.

Devemos então resolver o sistema de congruências

$$x \equiv 3 \pmod 5$$

$$x \equiv 10 \pmod 7$$

$$x \equiv 9 \pmod{11}.$$

Usando a notação do Exemplo 5.16, temos que $t_1 = 77$, $t_2 = 55$ e $t_3 = 35$. As congruências $77x \equiv 1 \pmod 5$, $55x \equiv 1 \pmod 7$ e $35x \equiv 1 \pmod{11}$ têm as soluções 3, 6, e 6 respectivamente.

Então, $b = 3 \times 77 \times 3 + 10 \times 55 \times 6 + 9 \times 35 \times 6 = 5883 \equiv 108 \pmod{385}$ é a solução pedida. □

O Teorema Chinês do Resto pode ser utilizado para achar a solução de uma congruência decompondo seu módulo em um produto de fatores primos.

Exemplo 5.18. *Resolva a congruência* $13x \equiv 17 \pmod{42}$.

Solução: Como $42 = 2 \times 3 \times 7$, a congruência dada é equivalente ao sistema de congruências

$$13x \equiv 17 \pmod 2$$

$$13x \equiv 17 \pmod 3$$

$$13x \equiv 17 \pmod 7,$$

que, por sua vez, como vimos nos exemplos anteriores, é equivalente ao sistema

$$x \equiv 1 \pmod 2$$

$$x \equiv 2 \pmod 3$$

$$x \equiv 4 \pmod 7.$$

Utilizando a notação da demonstração do Teorema Chinês do Resto vemos que $t_1 = 21$, $t_2 = 14$ e $t_3 = 6$, $a_1 = 1$, $a_2 = 2$, $a_3 = 4$, $x_1 = 0$, $x_2 = 5$, $x_3 = 11$. Assim, a solução será

$$1 \times 0 \times 21 = 2 \times 14 \times 2 + 4 \times 6 \times 11 = 320$$

. □

O método que apresentamos neste exemplo é bem útil quando se deseja resolver uma congruência módulo um inteiro grande, pois ele transforma a congruência em um sistema de congruências módulo inteiros menores.

Exemplo 5.19. *Uma solução direta da congruência* $13x \equiv 17 \pmod{42}$ *é a seguinte:*

Solução: Como no exemplo anterior, podemos montar o seguinte sistema de congruências:

$$13x \equiv 17 \pmod{2}$$

$$13x \equiv 17 \pmod{3}$$

$$13x \equiv 17 \pmod{7},$$

Da primeira congruência deste sistema, vemos que x é da forma $1 + 2k$. Substituindo este valor de x na segunda congruência, vemos que $1 + 2k \equiv 2 \pmod{3}$, donde $k \equiv 2 \pmod{3}$, ou seja $k = 2+3t$, donde finalmente $x = 5+6t$. Da terceira congruência obtemos então que $5 + 6t \equiv 4 \pmod{7}$, donde $t \equiv 1 \pmod{7}$. Assim, $t = 1 + 7r$, e portanto $x = 11 + 42r$, ou seja, $x \equiv 11 \pmod{42}$ é a única solução módulo 42 da congruência dada. (Observação: Como m.d.c.$(13, 42) = 1$, sabemos que a congruência dada, $13x \equiv 17 \pmod{42}$ tem solução. Poderíamos tê-la achado diretamente aplicando o algoritmo de Euclides, a fim de determinar r e s tais que $13r + 42s = 1$.

Exemplo 5.20. [O Pequeno Teorema de Fermat] *Se* a *é um número inteiro e* p *é um número primo, então* $a^p \equiv a \pmod{p}$.

Demonstração: A demonstração deste teorema já foi pedida nos exercícios do capítulo sobre indução finita. Ela é uma aplicação direta do princípio da indução.

Com efeito, seja $P(n)$ a afirmação "$n^p \equiv n \pmod{p}$". É claro então que $P(0)$ é verdadeira. Suponha agora que $P(k)$ seja verdadeira. Sabemos que $(k+1)^p = k^p + \binom{p}{1}k^{p-1} + \binom{p}{2}k^{p-2} + \cdots \binom{p}{p-1}k + 1$; para $1 < j < p$, o inteiro $\binom{p}{j} = \frac{p(p-1)\cdots(p-j+1)}{1\cdot 2\cdots j}$ é um múltiplo de p, visto que p é primo, e portanto seus únicos divisores são ± 1 e $\pm p$. Neste desenvolvimento binomial cada coeficiente, exceto o primeiro e o último, é divisível por p, e vemos que $(k+1)^p \equiv k^p + 1 \equiv k + 1 \pmod{p}$, que é exatamente a afirmação $P(k+1)$. Desta maneira, concluimos a demonstração do teorema pedido. □

Exemplo 5.21. [Teorema de Wilson] *Se* p *é um número primo, então* $(p-1)! \equiv -1 \pmod{p}$.

Demonstração: Em primeiro lugar, o teorema é verdadeiro para $p = 2$ e $p = 3$, por verificação direta. Podemos pois supor que o primo p é maior ou igual a 5.

A congruência $kx \equiv 1 \pmod{p}$, onde k é um dos inteiros $1, 2, 3, \ldots, p-1$, admite exatamente uma solução $\pmod{p}$, pois m.d.c.$(k, p) = 1$. Pelo Exercício 5.8, se $k = 2, 3, \ldots, p-2$, então $x \neq k$.

O número de pares não-ordenados $\{k, x\}$ tais que $kx \equiv 1 \pmod{p}$ é $(p-3)/2$, pois se $kx \equiv 1 \pmod{p}$, então $xk \equiv 1 \pmod{p}$, e $x \neq k$, pelo exercício citado.

Cada inteiro do conjunto $\{2, 3, \ldots, p-2\}$ pertence a um desses pares. Assim, se tomarmos os $(p-3)/2$ pares, que são soluçSes de $ax \equiv 1 \pmod{p}$, obteremos todos os inteiros $\{2, 3, \ldots, p-2\}$.

Multiplicando essas $(p-3)/2$ congruências, obtemos

$$2 \cdot 3 \cdot 4 \cdot \cdots \cdot (p-2) \equiv 1 \pmod{p},$$

ou seja

$$(p-2)! \equiv 1 \pmod{p}.$$

Como $p - 1 \equiv -1 \pmod{p}$, obtemos enfim que

$$(p-1)! \equiv -1 \pmod{p},$$

como queríamos demonstrar. □

5.3 OS CRITÉRIOS DE DIVISIBILIDADE

A noção de congruência pode ser utilizada para justificar os *critérios de divisibilidade* normalmente empregados no sistema de numeração decimal. Critérios análogos podem ser demonstrados em um sistema de numeração com uma base b qualquer.

Demonstraremos inicialmente um critério de divisibilidade por 9 bem conhecido.

Exemplo 5.22. *Ache um critério de divisibilidade de um inteiro* N *por* 9.

Solução: Escreva a representação decimal de N

$$N = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0.$$

Já sabemos que

$$\begin{aligned} 10 &\equiv 1 \pmod 9; \\ 100 &\equiv 1 \pmod 9; \\ 1000 &\equiv 1 \pmod 9; \\ &\cdots \\ 10^k &\equiv 1 \pmod 9. \end{aligned}$$

Segue-se daí que

$$\begin{aligned} a_k 10^k &\equiv a_k \pmod 9; \\ a_{k-1} 10^{k-1} &\equiv a_{k-1} \pmod 9; \\ &\cdots \\ a_1 10 &\equiv a_1 \pmod 9; \\ a_0 &\equiv a_0 \pmod 9. \end{aligned}$$

Logo

$$a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0 \equiv (a_k + a_{k-1} + \cdots + a_1 + a_0) \pmod 9.$$

Como N é divisível por 9 se e somente se N é côngruo a $0 \pmod 9$, vemos que N é divisível por 9 se e somente se $\sum_{i=0}^{k} a_i \equiv 0 \pmod 9$. Isto é, se e somente se a soma dos algarismos de N for um número divisível por 9. □

Exemplo 5.23. *Ache um critério de divisibilidade de um número* N *por* 11.

Solução: Mais uma vez, escreva

$$N = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0.$$

Temos então

$$10 \equiv -1 \pmod{11};$$

$$100 \equiv 1 \pmod{11};$$

$$1000 \equiv -1 \pmod{11};$$

$$\cdots$$

$$10^k \equiv (-1)^k \pmod{11};$$

e assim

$$a_k 10^k \equiv (-1)^k \pmod{11};$$

$$\cdots$$

$$a_2 10^2 \equiv a_2 \pmod{11};$$

$$a_1 10 \equiv -a_1 \pmod{11};$$

$$a_0 \equiv a_0 \pmod{11}.$$

Então

$$\begin{aligned} N &= a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0 \\ &\equiv (-1)^k a_k + \cdots + a_2 - a_1 + a_0 \pmod{11}, \end{aligned}$$

ou seja,

$$N \equiv \sum_{i=0}^{k} (-1)^i a_i \pmod{11}.$$

Daí decorre imediatamente que N é divisível por 11 se e somente se a soma alternada $a_0 - a_1 + a_2 - \cdots + (-1)^k a_k$ é um múltiplo de 11. □

Observação: por vezes, a procura de critérios de divisibilidade é facilitada devido ao fato de que se m.d.c.$(a, b) = 1$, então um inteiro N é divisível por $a \cdot b$ se e somente se ele é divisível por a e por b.

Outra utilização semelhante das congruências é na justificação da chamada "prova dos nove" das operações elementares.

Por exemplo, multiplicou-se o inteiro a pelo inteiro b, e encontrou-se c. Se $a \equiv a_1 \pmod 9$, $b \equiv b_1 \pmod 9$ e $c \equiv c_1 \pmod 9$, estando correta a multiplicação, ter-se-á $c_1 \equiv c \equiv ab \equiv a_1 b_1 \pmod 9$. Logo, se $c_1 \not\equiv a_1 b_1 \pmod 9$, houve erro na

multiplicação. Assim, por exemplo, $4357 \times 3412 = 14865084$ é uma multiplicação na qual algum engano foi cometido, pois $14865084 \equiv 1 + 4 + 8 + 6 + 5 + 0 + 8 + 4 \equiv 36 \equiv 0 \pmod 9$, $3412 \equiv 3 + 4 + 1 + 2 \equiv 1 \pmod 9$, $4357 \equiv 4 + 3 + 5 + 7 \equiv 1 \pmod 9$ e $0 \not\equiv 1 \cdot 1 \pmod 9$.

Observe que a prova dos noves é uma condição necessária porém não suficiente para a correção da operação, pois é possível se ter $\mathtt{c} \equiv \mathtt{ab} \pmod 9$ com $\mathtt{c} \neq \mathtt{ab}$ (Você será capaz de achar um exemplo desta situação?).

EXERCÍCIOS

5.1. Prove que se $a \equiv b \pmod{m}$ e x é um inteiro, então $a + x \equiv b + x \pmod{m}$.

5.2. Ache um exemplo de inteiros a, b e c tais que $c \equiv ab \pmod{9}$, mas $c \neq ab$.

5.3. Prove que se $a \equiv b \pmod{m}$ e x é um inteiro, então $ax \equiv bx \pmod{m}$.

5.4. Prove que se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$ e $ac \equiv bd \pmod{m}$.

5.5. Prove que se m.d.c.$(a, b) = 1$, então o inteiro n é divisível pelo produto ab se e só se ele é divisível por a e por b.

5.6. Prove que $2222^{5555} + 5555^{2222}$ é divisível por 7.

5.7. Resolva a equação $3x \equiv 11 \pmod{2275}$.

5.8. Se $2^n - 1$ é primo, prove que n é primo.

5.9. Sejam a, b e m inteiros, com m positivo. Suponha que $ax \equiv b \pmod{m}$ tem solução. O que é possível concluir sobre a, b e m?

5.10. Se $ac \equiv bc \pmod{m}$ e m.d.c.$(c, m) = d$, então $a \equiv b \pmod{m/d}$.

5.11. Mostre que se a e b são inteiros e p é um número primo, então $(a + b)^p \equiv a^p + b^p \pmod{p}$ [Veja o Exemplo 5.22].

5.12. Mostre que qualquer quadrado perfeito é côngruo a 0 ou a 1 $\pmod{4}$.

5.13. Mostre que um número da forma $4n + 3$ não pode ser escrito como soma de dois quadrados.

5.14. Mostre que se m.d.c.$(a, 35) = 1$, então $a^{12} \equiv 1 \pmod{35}$.

5.15. Demonstrre que se $(p-1)! \equiv -1 \pmod{p}$, então p é um número primo.

5.16. Qual o último algarismo de 777^{777}?

5.17. Mostre que entre os números

$$11$$

$$111$$

$$1111$$

$$\ldots$$

$$11\ldots11$$

não podem figurar quadrados.

5.18. Mostre que se m.d.c.$(a, b) = 1$, então $x \equiv k \pmod{ab}$ se e somente se $x \equiv k \pmod{a}$ e $x \equiv k \pmod{b}$.

5.19. Ache o resto da divisão de 15! por 17.

5.20. Mostre que se $k \geq 0$, então $10^k \equiv 1 \pmod{3}$.

5.21. Demonstre que se $k \geq 0$, então $10^k \equiv (-1)^k \pmod{11}$.

5.22. Sejam a, b e d inteiros, com b positivo. É verdade que se $ab \equiv 0 \pmod{d}$ então $a \equiv 0 \pmod{d}$ ou $b \equiv 0 \pmod{d}$? Ache uma condição suficiente para que isso seja verdade.

5.23. Sejam p um primo positivo, a, b e c inteiros. Mostre que se $ab \equiv ac \pmod{p}$, $a \not\equiv 0 \pmod{p}$, então $b \equiv c \pmod{p}$. A condição de p ser primo é necessária?

5.24. Sejam p um primo positivo e a um inteiro. O menor inteiro positivo h tal que $a^h \equiv 1 \pmod{p}$ divide necessariamente $p-1$.

5.25. Sejam a e n inteiros positivos tais que m.d.c.$(a, n) = 1$. Então $a^{\phi(n)} \equiv 1 \pmod{n}$, onde ϕ é a função tociente de Euler.

5.26. Mostre que se p e q são primos diferentes,e se $a^p \equiv a \pmod{q}$, $a^q \equiv a \pmod{p}$, então $a^{pq} \equiv a \pmod{pq}$.

5.27. Mostre que $2^{340} \equiv 1 \pmod{341}$ e que $2^{341} \equiv 2 \pmod{341}$

5.28. Resolva o sistema de congruências

$$\begin{aligned} x &\equiv 3 \pmod{10} \\ x &\equiv 11 \pmod{13}\,. \\ x &\equiv 15 \pmod{17} \end{aligned}$$

5.29. Resolva o sistema de congruências

$$\begin{aligned} 5x &\equiv 11 \pmod{17} \\ 3x &\equiv 19 \pmod{32} \\ 11x &\equiv 6 \pmod{37}. \end{aligned}$$

5.30. Prove que se $k \equiv 1 \pmod{4}$, então $6k + 5 \equiv 3 \pmod{4}$.

5.31. Se $a^2 \equiv b^2 \pmod{m}$ é verdade que $a \equiv b \pmod{m}$?

5.32. Um banco numera as contas-correntes com números de 6 dígitos, seguidos por um dígito verificador, $ABCDEF-G$. O dígito verificador é o resto da divisão de $A+2B+4C+3D-5E+7F$ por 10. A conta de DÁrtagnan é $154383X-5$. Qual o dígito representado por X?

5.33. Mostre que para todo n natural, $7^{2n} - 2352n - 1$ é divisível por 2304.

5.34. Prove que se x, y e z são inteiros tais que $x^2 + y^2 = z^2$, então x e y não são ambos ímpares e xy é múltiplo de 6.

5.35. Os números a, b e c são inteiros e $a \neq 0$. Prove que se a equação $ax^2 + bx + c = 0$ possui raízes racionais, então pelo menos um dos números a, b e c é par.

5.36. Prove que se p é um primo e $a \not\equiv 0 \pmod{p}$, então os números $a \cdot 1, a \cdot 2, a \cdot 3, \ldots, a \cdot p$ são todos distintos módulo p.

5.37. Mostre que se k é ímpar, então $1^k + 2^k + \cdots + n^k$ é divisível por $1 + 2 + \cdots + n$.

5.38. Ache um critério de divisibilidade por 7.

5.39. Ache um critério de divisibilidade por 4.

5.40. Ache um critério de divisibilidade por 8.

5.41. Ache um critério de divisibilidade por 3.

5.42. Ache um critério de divisibilidade por 6.

5.43. Ache um critério de divisibilidade por 13.

5.44. Sejam $p_1, \ldots, p_k$ números primos, com $p_1 < p_2 < \cdots < p_k$. Então qualquer número natural N menor do que $p_{1\cdot 2} \cdot \ldots \cdot p_k$ se escreve de maneira única como $(a_1, \ldots, a_k)$, onde

$$N \equiv a_i \qquad (\text{mod } p_i).$$

5.45. Outro critério de divisibilidade por 7 é o seguinte: Para verificar se um número é divisível por 7, destacamos os dois últimos algarismos do número e somamos o quádruplo do número formado por esses dois últimos algarismos ao número formado pelos restantes algarismos. O número original será divisível por 7 se e sómente se essa soma for divisível por 7. Assim, por exemplo, para verificar se 435769 é divisível por 7, calculamos $4357+4\times79 = 4673$; $46 + 4 \times 73 = 338$; $3 + 4 \times 38 = 155$. Como 155 não é divisível por 7, 435769 também não é. Demonstre a validade desse processo.

5.46. Prove a validade do seguinte critério de divisibilidade por 13: Um número é divisível por 13 se e sómente se a soma do triplo do número formado pelos dois últimos algarismos com o número formado pelos algarismos restantes for divisível por 13.

5.47. Deduza critérios análogos para as divisibilidades por 19 e por 23.

5.48. Uma pilha tem 1000 moedas. É permitido retirar uma moeda da pilha e dividí-la em duas outras, de tamanhos não necessariamente iguais. A mesma operação pode ser feita em cada uma das novas pilhas e assim sucessivamente. É possível terminar com todas as pilhas contendo 3 moedas cada? E contendo 7 moedas cada?

CAPÍTULO 6

A REPRESENTAÇÃO DECIMAL DOS NÚMEROS NATURAIS

6.1 O SISTEMA DECIMAL DE NUMERAÇÃO

Seja $\mathtt{b}$ um número natural maior do que 1. Então, dado um número natural $\mathtt{N}$ arbitrário, é sempre possível escrever $\mathtt{N}$ como

$$\mathtt{N} = \mathtt{a}_k\mathtt{b}^k + \mathtt{a}_{k-1}\mathtt{b}^{k-1} + \cdots + \mathtt{a}_1\mathtt{b} + \mathtt{a}_0,$$

onde $0 \leq \mathtt{a}_i < \mathtt{b}$, para $\mathtt{i} = 0,\ 1, \ldots, \mathtt{k}$. É a chamada *representação de* $\mathtt{N}$ *na base* $\mathtt{b}$.

Exemplo 6.1. *Ache a representação de* 39 *na base* 3.

Solução: Em primeiro lugar, temos que

$$39 > 3^0$$

$$39 > 3^1$$

$$39 > 3^2$$

$$39 > 3^3,$$

mas $39 < 3^4 = 81$. Então, pelo algoritmo da divisão, $39 = 1 \times 3^3 + 12$. Além disso, pelo mesmo algoritmo, $12 = 1 \times 9 + 3$. Assim

$$39 = 1 \times 3^3 + 1 \times 3^2 + 3 \times 1.$$

□

Claramente, o procedimento adotado no exemplo acima para achar a representação de 39 na base 3 funciona para um número natural N qualquer e para qualquer base b.

Se a representação de N na base b é

$$N = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

escrevemos que $N = (a_k a_{k-1} \ldots a_1 a_0)_b$. Quando não há possibilidade de confusão, omitimos b na notação acima e escrevemos simplesmente $N = a_k a_{k-1} \ldots a_1 a_0$.

Exemplo 6.2. *Escreva o número* 29 *na base* 2.

Solução: Observe que $29 = a_k 2^k + \cdots a_1 2^1 + a_0 2^0$, para algum k. Assim, $29 = 2q_1 + a_0$, onde $q_1 = a_k 2^{k-1} + \cdots + a_1$. Ou seja, a_0 é o resto da divisão de 29 por 2. Para acharmos a_1, observe que $q_1 = 2q_2 + a_1$. Assim, a_1 é o resto da divisão de q_1 por 2. Este processo pode ser continuado, e achamos facilmente $a_2, a_3, \ldots, a_k$. Em nosso exemplo:

$$29 = 14 \times 2 + 1 \Rightarrow a_0 = 1;$$

$$14 = 7 \times 2 + 0 \Rightarrow a_1 = 0;$$

$$7 = 3 \times 2 + 1 \Rightarrow a_2 = 1;$$

$$7 = 3 \times 2 + 1 \Rightarrow a_3 = 1$$

$$3 = 2 \times 1 + 1 \rightarrow a_4 = 1.$$

Assim, $(29)_2 = 11101$. □

Obviamente este processo é inteiramente geral e fornece **uma maneira prática para calcular a representação de um número em qualquer base**: Divida o número pela base. O resto será o algarismo das "unidades" da representação do número na base dada. Divida em seguida o quociente obtido pela base. O resto obtido será o segundo algarismo (da direita para a esquerda) da representação do número na base. Divida o quociente pela base. O resto obtido será o terceiro algarismo (da direita para a esquerda) da representação do número na base. E assim sucessivamente.

Exemplo 6.3. *É claro que a representação de um número natural em uma base* b *é única. Seja, por exemplo,* $b = 10$ *e suponha que o número natural* N *tenha duas representações decimais distintas*

$$N = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$$

e

$$N = c_s 10^s + c_{s-1} 10^{s-1} + \cdots + c_1 10 + c_0,$$

e suponha que $k \leq s$.

Afirmamos então que $10^k \leq N < 10^{k+1}$. Com efeito,

$$\begin{aligned} N \leq & 9 \times 10^k + 9 \times 10^{k-1} + \cdots + 9 \times 10 + 9 \\ = & 9(10^k + \cdots + 10 + 1) = \frac{9(10^{k+1} - 1)}{10 - 1} \\ = & 10^{k+1} - 1 \leq 10^{k+1}. \end{aligned}$$

Por outro lado, claramente $N \geq a_k 10^k \geq 10^k$, donde, enfim,

$$10^k \leq N < 10^{k+1}.$$

Então, como $k \leq s$, vemos que $c_s = c_{s-1} = \ldots = c_{k+1} = 0$.

Observe também que de

$$N = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$$

vemos que a_k é o quociente e $a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$ o resto da divisão de N por 10^k, pois $0 \leq a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 < 10^k$ pelo raciocínio usado acima. Pela mesma razão, c_k será o quociente e $c_{k-1} 10^{k-1} + \cdots + c_1 10 + c_0$ o resto da divisão de N por 10^k. Pela unicidade do quociente e do resto da divisão, vemos que $a_k = c_k$ e portanto

$$a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 = c_{k-1} 10^{k-1} + \cdots + c_1 10 + c_0.$$

Um raciocínio indutivo mostra agora facilmente que $a_i = c_i$, para $i = 0, 1, 2, \ldots, k$, o que conclui a demonstração. □

O raciocínio usado acima é inteiramente geral. Funciona para qualquer base b.

O sistema de representação mais utilizado é o *decimal*, ou seja, aquele cuja base é o número 10. Neste sistema, qualquer número natural $\mathtt{N}$ se escreve como

$$\mathtt{N} = \mathtt{a}_\mathtt{k} 10^\mathtt{k} + \mathtt{a}_{\mathtt{k}-1} 10^{\mathtt{k}-1} + \cdots + \mathtt{a}_1 10 + \mathtt{a}_0,$$

com $0 \leq \mathtt{a}_\mathtt{i} < 9$ para $0 \leq \mathtt{i} \leq \mathtt{k}$. Assim, qualquer número natural se escreve como soma de múltiplos de potências de 10.

Observe que, ao escrevermos por exemplo o número 777 na base 10, o algarismo 7 tem 3 valores distintos, dependendo de sua posição. Com efeito, 777 na base 10 quer dizer $7 \times 10^2 + 7 \times 10 + 7 \times 1$; isto é, o primeiro 7 à esquerda significa em realidade 700 (está na "casa das centenas")o segundo 70 (está na casa das dezenas) e o terceiro 7 (está na casa das unidades). Dizemos que o sistema de representação na base 10 (mais geralmente na base $\mathtt{b}$), é um "sistema posicional". Nele, o valor dos algarismos depende de sua posição no número. Este fato se expressa, na escola elementar, dizendo que um algarismo tem dois valores: seu "valor absoluto", independente de sua posição no número, e seu "valor relativo", que depende de sua posição no número. No exemplo acima, o valor absoluto dos algarismos do número 777 é 7. Seus valores relativos são, respectivamente, da esquerda para a direita, 700, 70 e 7.

A criação de um sistema posicional foi essencial para o desenvolvimento da Matemática. Em primeiro lugar, um tal sistema permite representar qualquer número, por maior que seja, usando somente os $\mathtt{b}$ algarismos $0,\ 1, \ldots, \mathtt{b}-1$, quando a base do sistema for $\mathtt{b}$. Em segundo lugar, permite desenvolver algoritmos sistemáticos e eficientes para as operações com números naturais.

Os babilônios desenvolveram, uns 2000 anos antes de Cristo, um sistema posicional com base 60, que era contudo prejudicado pela não existência do *número* zero. Ao contrário do que se poderia supor, poucas civilizações descobriram sistemas de numeração posicionais: os babilônios, já citados, os maias, os chineses e os hindus, a quem devemos nosso sistema atual, que nos chegou por intermédio dos árabes. Os hindus foram os criadores do número zero, também descoberto pelos maias.

Hoje, adota-se universalmente o "sistema de numeração de base 10". Devido à utilização dos computadores digitais, usam-se também os sistemas de numeração de base 16 "o sistema hexadecimal" e de base 2, o "sistema binário".

A escolha do número 10 como base de nosso sistema de numeração parece decorrer do fato de que temos dez dedos. Em algumas línguas há vestígios de contagem usando a base 20, que corresponderia a 20 dedos (os dos pés e os das mãos): o francês *quatre-vingts*, 80, o inglês *score*, 20. Em alguns sistemas, como o romano, o número 5 (os dedos de uma mão), tinha um papel destacado.

Do ponto de vista matemático, para trabalharmos com frações, quanto mais divisores primos tivermos na base $\mathfrak{b}$ do sistema melhor, pois a representação da fração $\frac{\mathfrak{m}}{\mathfrak{n}}$ na base $\mathfrak{b}$ é finita se e somente se os divisores primos do denominador $\mathfrak{n}$ forem divisores da base $\mathfrak{b}$ (demonstre isso!). Deste ponto de vista, a base 60 usada pelos babilônios é melhor do que a nossa base 10, pois $10 = 2 \times 5$ e $60 = 2^2 \times 3 \times 5$. Por outro lado, quanto maior a base, maiores as tabelas de soma e de multiplicação que deverão ser memorizadas, ou pelo menos usadas. Nossas tabelas para essas operações são 9×9. Na base 60 usaríamos tabelas 59×59!

Outro fato que deve ser pesado é que quanto maior a base $\mathfrak{b}$, menor o comprimento da representação de um número natural $\mathfrak{n}$. Assim, o número 9 é representado na base 10 por um algarismo. Na base 2, ele será representado por 101, ou seja, por três algarismos.

Levando em conta todas estas considerações, vemos que a base 10 é uma escolha razoável.

Mostraremos agora como um sistema de numeração posicional permite o desenvolvimento de algoritmos simples para as operações com números naturais. Para facilitar a exposição, daremos sempre exemplos numéricos, que no entanto são inteiramente gerais.

6.2 O ALGORITMO DA ADIÇÃO NO SISTEMA DECIMAL

Exemplo 6.4. *Efetue a soma* $\mathsf{N}_1 + \mathsf{N}_2$, *se* $\mathsf{N}_1 = 1235$ *e* $\mathsf{N}_2 = 324$ *em base* 10.

Solução: Temos que

$$\mathsf{N}_1 = 1 \times 10^3 + 2 \times 10^2 + 3 \times 10 + 5 \times 1$$
$$\mathsf{N}_2 = 3 \times 10^2 + 2 \times 10 + 4 \times 1.$$

Então, somando os dois lados destas igualdades e grupando os coeficientes das potências de 10, temos

$$\mathsf{N}_1 + \mathsf{N}_2 = 1 \times 10^3 + (2+3) \times 10^2 + (3+2) \times 10 + (5+4) \times 1.$$

Assim, $\mathsf{N}_1 + \mathsf{N}_2 = (1559)_{10}$. Observe que, para chegar a este resultado, simplesmente somamos os algarismos que são, nos dois números, coeficientes de uma mesma potência de 10. O algoritmo usual da soma faz isso automaticamente para nós:

FIGURA 1

A Coluna A corresponde à "casa das unidades" (coeficientes de 10^0), a B à casa das dezenas (coeficientes de 10^1), a C à casa das centenas (coeficientes de 10^2) e a D à casa dos milhares (coeficientes de 10^3).

Exemplo 6.5. *Efetue a soma* $754 + 678$.

Solução: Sejam $\mathsf{N}_1 = 754 = 7\times10^2+5\times10+4\times10^0$ e $\mathsf{N}_2 = 678 = 6\times10^2+7\times10+8\times10^0$. Então $\mathsf{N}_1+\mathsf{N}_2 = (7+6)\times10^2+(5+7)\times10+(4+8)\times10^0$. Mas $4+8=10+2$, $5+7=10+2$. Assim

$$\begin{aligned}
\mathsf{N}_1+\mathsf{N}_2 &= (7+6)\times10^2+(5+7)\times10+(4+8)\times10^0 \\
&= (7+6)\times10^2+(5+7)\times10+(2+10)\times10^0 \\
&= (7+6)\times10^2+(5+7)\times10+10\times10^0+2\times10^0 && \text{vai um} \\
&= (7+6)\times10^2+(5+7+1)\times10+2\times10^0 \\
&= (7+6)\times10^2+(10+3)\times10+2\times10^0 \\
&= (7+6)\times10^2+10\times10+3\times10+2\times10^0 \\
&= (7+6+1)\times10^2+3\times10+2\times10^0 && \text{vai um} \\
&= (10+4)\times10^2+3\times10+2\times10^0 \\
&= 10\times10^2+4\times10^2+3\times10+2\times10^0 && \text{vai um} \\
&= 10^3+4\times10^2+3\times10+2\times10^0,
\end{aligned}$$

e portanto $\mathsf{N}_1+\mathsf{N}_2 = (1432)_{10}$.

O algoritmo da soma faz estas operações automaticamente para nós, encarregando-se de transformar $10\times10^{\mathsf{k}}$ em $10^{\mathsf{k}+1}$, pelo processo conhecido de "vai um":

FIGURA 2

Vejamos agora como a representação decimal permite efetuar facilmente a multiplicação de dois números naturais.

6.3 ALGORITMO DA MULTIPLICAÇÃO NO SISTEMA DECIMAL

Exemplo 6.6. *Efetue o produto* 23×14.

Solução: Sejam $\mathsf{N}_1 = 23 = 2 \times 10^1 + 3 \times 10^0$ e $\mathsf{N}_2 = 14 = 1 \times 10^1 + 4 \times 10^0$. Então, pela lei distributiva,

$$\begin{aligned} \mathsf{N}_1 \times \mathsf{N}_2 = 23 \times 14 &= (2 \times 10 + 3 \times 10^0) \times (1 \times 10 + 4 \times 10^0) = \\ &= (2 \times 10^1 + 3 \times 10^0) \times 4 \times 10^0 + \qquad (\mathsf{A}) \\ &+ (2 \times 10^1 + 3 \times 10^0) \times 1 \times 10. \qquad (\mathsf{B}) \end{aligned}$$

A linha (A) acima corresponde a multiplicar 23 por 4, que é exatamente a primeira operação efetuada no algoritmo usual da multiplicação. Semelhantemente, a linha (B) corresponde a multiplicar 23 por 1×10^1.

Procedendo como no algoritmo da multiplicação, efetuaremos sucessivamente estas multiplicaçSes. Para 23×4 temos:

$$\begin{aligned} &(2 \times 10^1 + 3 \times 10^0) \times 4 \times 10^0 = \\ &= 2 \times 4 \times 10^1 + 3 \times 4 \times 10^0 = \\ &= 2 \times 4 \times 10^1 + (10 + 2) \times 10^0 = \\ &= 2 \times 4 \times 10^1 + 10^1 + 2 \times 10^0 = \qquad \text{vai um!} \\ &= (8 + 1) \times 10^1 + 2 \times 10^0 = \\ &= 9 \times 10^1 + 2 \times 10^0 = 92. \qquad (\mathsf{C}) \end{aligned}$$

Semelhantemente, para $23 \times (1 \times 10^1)$ temos:

$$\begin{aligned}
&(2 \times 10^1 + 3 \times 10^0) \times 1 \times 10^1 = \\
&= 2 \times 1 \times 10^2 + 3 \times 1 \times 10^1 = \\
&= 2 \times 10^2 + 3 \times 10^1 = 230. \qquad \text{(D)}
\end{aligned}$$

Somando agora os resultados destas multiplicaçSes, (C) e (D), temos:

$$\begin{aligned}
\mathsf{N}_1 \times \mathsf{N}_2 &= (2 \times 10^1 + 3 \times 10^0) \times (1 \times 10^1 + 4 \times 10^0) = \\
&= (9 \times 10^1 + 2 \times 10^0) + (2 \times 10^2 + 3 \times 10^1) = \\
&= 2 \times 10^2 + (9 + 3) \times 10^1 + 2 \times 10^0 = \\
&= (2 + 1) \times 10^2 + 2 \times 10^1 + 2 \times 10^0 = \qquad \text{vai um!} \\
&= 3 \times 10^2 + 2 \times 10^1 + 2 \times 10^0 = 322.
\end{aligned}$$

O algoritmo da multiplicação faz tudo isso automaticamente para nós, como você poderá verificar comparando os passos efetuados acima com os feitos no algoritmo.

6.4 ALGORITMO DA DIVISÃO NO SISTEMA DECIMAL

Mostraremos agora como funciona o algoritmo para a divisão de dois números naturais. Ou seja, dados dois números naturais $\mathtt{a}$ e $\mathtt{b}$ por suas representações decimais, como achar o quociente $\mathtt{q}$ e o resto $\mathtt{r}$ da divisão de $\mathtt{a}$ por $\mathtt{b}$?

Trabalharemos com exemplos numérico, que são contudo inteiramente gerais, a fim de ilustrar o funcionamento do algoritmo da divisão.

Exemplo 6.7. *Efetue a divisão de* 24 *por* 7.

Solução: O conhecimento da "taboada de multiplicação" por 7 resolve o problema. Com efeito

$$7 \times 1 = 7 < 24$$

$$7 \times 2 = 14 < 24$$

$$7 \times 3 = 21 < 24$$

$$7 \times 4 = 28 > 24,$$

e podemos interromper o processo. Assim, o quociente da divisão de 24 por 7 é 3 e o resto é 3.

Exemplo 6.8. *Divida* 983 *por* 4.

Solução: O algoritmo que vamos apresentar reduz o problema de dividir 983 por 4 à realização sucessiva de divisões simples, que exigem somente o conhecimento da tabela de multiplicação do divisor, como no exemplo anterior.

Ora, $983 = 900 + 80 + 3$, donde $983 \div 4 = 900 \div 4 + 80 \div 4 + 3 \div 4$.

Mas

$$900 \div 4 = (9 \div 4) \times 100 = (2 + 1 \div 4) \times 100 = 2 \times 100 + (1 \div 4) \times 100;$$

$$2 \times 100 + (1 \div 4) \times 100 + 80 \div 4 = 2 \times 100 + (18 \div 4) \times 10$$

$$= 2 \times 100 + (4 + 2 \div 4) \times 10 = 2 \times 100 + 4 \times 10 + (2 \div 4) \times 10;$$

$$2 \times 100 + 4 \times 10 + (2 \div 4) \times 10 + 3 \div 4 = 2 \times 100 + 4 \times 10 + (23 \div 4) = 2 \times 100 + 4 \times 10 + 5 + 3 \div 4.$$

O algoritmo da divisão efetua tudo isso automaticamente para nós:

FIGURA 5

Exemplo 6.9. *Ache o quociente e o resto da divisão* $243 \div 7$.

Solução: Mais uma vez, reduziremos o problema de dividir $243 \div 7$ ao de efetuar divisões sucessivas por 7, envolvendo, em cada caso, a multiplicação de no máximo 9×7.

Ora, $243 = 200 + 40 + 3$, donde $243 \div 7 = 200 \div 7 + 40 \div 7 + 3 \div 7$. Ora, como $200 > 7 \times 9$, procedemos como segue:

$$200 \div 7 + 40 \div 7 + 3 \div 7 = (20 \div 7) \times 10 + (4 \div 7) \times 10 + 3 \div 7.$$

Ou seja, na linguagem do algoritmo da divisão, "baixamos o 4". Então

$$= [(20 + 4) \div 7] \times 10 + 3 \div 7 = (24 \div 7) \times 10 + 3 \div 7$$

$$= [3 + (3 \div 7)] \times 10 + 3 \div 7 = 3 \times 10 + (3 \div 7) \times 10 + 3 \div 7$$

$$= 3 \times 10 + (33 \div 7) = 3 \times 10 + 4 + (5 \div 7).$$

Além da representação decimal, existem outras, úteis para aplicações particulares, e que apresentamos simplesmente no exemplo abaixo, ou nos exercícios, sem nos determos em seu estudo.

6.5 A REPRESENTAÇÃO FATORIAL DOS INTEIROS

Exemplo 6.10. *Mostre que qualquer número natural* N *se escreve de maneira única como*

$$N = a_1 \cdot 1 + a_2 \cdot 2! + \cdots + a_k \cdot k!, \qquad 0 \leq a_i \leq i,$$

para $i = 1, 2, \ldots, k$. *É a chamada* representação fatorial *dos números naturais.*

Podemos então representar N por $(a_1, a_2, \ldots, a_k)$. Os coeficientes a_i são chamados de *algarismos fatoriais* de N.

Há duas maneiras fáceis de achar a representação fatorial de um número natural N. Podemos dividir N por 2, e o resto será a_1. Dividindo então o quociente obtido por 3, o resto será a_2, e assim sucessivamente. A unicidade do resto e do quociente no algoritmo da divisão, juntamente com o fato de que cada a_i é menor ou igual a i, mostra que a representação obtida é única.

Outra maneira de obter a representação é a seguinte: suponha que $p! \leq N < (p+1)!$. Dividindo N por $p!$ o quociente é a_p. Dividindo o resto obtido por $(p-1)!$, o quociente será a_{p-1}, e assim sucessivamente.

O maior número possível com p algarismos é, em representação fatorial, $(1, 2, 3, \ldots, p)$. Pela unicidade da representação, este número é $(p+1)! - 1$, ou seja

$$1 \cdot 1 + 2 \cdot 2! + \cdots + p \cdot p! = (p+1)! - 1.$$

EXERCÍCIOS

6.1. Ache a representação de 73 na base 2.

6.2. Ache a representação de 97 na base 4.

6.3. Ache a representação de 172 na base 3.

6.4. Escreva o número b na base b.

6.5. Escreva os números b^2, b^3, ..., b^k na base b.

6.6. Seja o número $N = (a_k a_{k-1} \dots a_0)_b$. Ache a representação na base b dos números $N \times b$, $N \times b^2$, ..., $N \times b^k$.

6.7. Construa as tabelas de adição e de multiplicação para o sistema de base 2.

6.8. Efetue, em base 2, as seguintes operações

a)$1101011 + 11001101$;

b) 111×110101;

c) $11011011 \div 111$;

d)$111111 - 1011$.

6.9. Desenvolva algoritmos para efetuar somas, subtrações, multiplicações e divisões na base 2.

6.10. Construa as tabelas de adição e de multiplicação para o sistema de base 7.

6.11. Efetue, no sistema de numeração de base 7, as seguintes operações

a) $5647 + 32141$;

b) 346×4321;

c) $654325 \div 635$;

d) $645345 - 555$.

6.12. O sistema de base 16, "hexadecimal", muito utilizado em microcomputadores, tem os seguintes algarismos

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \mathsf{A}, \mathsf{B}, \mathsf{C}, \mathsf{D}, \mathsf{E}, \mathsf{F}.$$

6.13. Represente, no sistema "hexadecimal", os números 16, 17, 64, 73, 256.

6.14. Construa, no sistema "hexadecimal", as tabelas de adição e multiplicação.

6.15. Efetue, no sistema "hexadecimal", as seguintes operações:

a)$7\mathsf{A}59\mathsf{B} + \mathsf{F}3\mathsf{C}21$;

b)$\mathsf{CDAEF} \times 9\mathsf{A}4\mathsf{E}3\mathsf{F}$;

c)$\mathsf{FE}4321 \div 34\mathsf{A}$.

6.16. Ache a representação fatorial de 984.

6.17. Seja $\mathtt{k}$ um número natural fixo.Então, dado um número natural $\mathfrak{n}$ qualquer, podemos escrevê-lo de maneira única como

$$\mathfrak{n} = \binom{\mathfrak{a}_1}{1} + \binom{\mathfrak{a}_2}{2} + \cdots + \binom{\mathfrak{a}_\mathtt{k}}{\mathtt{k}},$$

com $0 \leq \mathfrak{a}_1 < \mathfrak{a}_2 < \cdots < \mathfrak{a}_\mathtt{k}$.

Obs: A representação obtida acima é chamada de *representação combinatória* de N.

6.18. Ache a representação combinatória de 759.

6.19. Ache o dígito $\mathtt{k}$ que torna o número natural $5\mathtt{k}9$ divisível por 9.

6.20. Ache o dígito $\mathtt{k}$ que torna o número natural $50\mathtt{k}2\mathtt{k}$ divisível por 2, por 3 e por 11.

6.21. Ache os dígitos $\mathtt{k}$ e $\mathtt{t}$ que tornam o número natural $56\mathtt{k}21\mathtt{t}$ divisível por 9 e por 10.

6.22. Ache os dígitos k e t que tornam o número natural $7k36t5$ divisível por 1375.

6.23. Mostre que todo número natural de seis algarismos,todos eles iguais, é divisível por 7, 11, 13 e 37.

6.24. Demonstre que um número natural é divisível por 8 se e somente se a soma do algarismo das unidades com o dobro do algarismo das dezenas com o quádruplo do algarismo das centenas é divisível por 8.

6.25. Considere uma balança de dois pratos e pesos $P_0, P_1, \ldots, P_k$, que podem ser colocados no prato da esquerda. Mostre que uma condição necessária e suficiente para podermos pesar, no prato da direita, qualquer objeto com peso P um número inteiro de quilogramas e $P \leq 2^{k+1} - 1$ é que $P_i = 2^i$, para $i = 0, 1, \ldots, k$.

6.26. Temos uma balança de dois pratos e uma coleção de $k+1$ pesos, com $1, 3, 3^2, \ldots 3^k$ quilogramas respectivamente e que podem ser colocados em qualquer dos pratos da balança. Qual o valor de P, inteiro, em quilogramas, para o qual é possível pesar qualquer objeto com peso inteiro, em quilogramas, menor ou igual a P?

6.27. Se $m = 14641$ na base b, $b \geq 7$, prove que m é quadrado perfeito e determine a representação de $\sqrt{m}$ na base $b + 1$.

6.28. Determine a representação de $(14654)_b$ na base $b + 1$.

6.29. Mostre que a representação de m/n é finita, isto é, contém somente um número finito de algarismos não-nulos, se e somente se n é da forma $2^r 5^s$, com r e s inteiros não-negativos.

CAPÍTULO 7

OS NÚMEROS INTEIROS

É muito grande a importância do conjunto **N** dos números naturais. Em primeiro lugar, os naturais servem para "contar" objetos. São o padrão de contagem, como vimos no Capítulo 2.

Além disso, e não menos importante, é possível, começando com eles, construir grande parte da Matemática, como também foi dito no Capítulo 2.

Um passo decisivo neste sentido é ampliar, sucessivamente o conjunto dos números naturais para obtermos um conjunto no qual seja possível efetuar sem problemas as operaçSes da Aritmética: a adição, a subtração, a multiplicação e a divisão por divisor não-nulo.

A primeira etapa deste programa é a criação do conjunto dos números inteiros, $\mathbb{Z}$.

As dificuldades da aceitação do zero e dos números negativos são psicologicamente válidas. Inicialmente, para o homem, a noção de número estava associada à contagem de objetos concretos, e portanto qualquer "número" era necessariamente um número natural, um inteiro positivo.

A criação do zero, feita pelos hindus, em época não bem determinada, em torno do século 10 de nossa era, foi um grande progresso no sentido da abstração do conceito de "número". Mentes especulativas sugerem que esta concepção do zero pelos hindus pode estar relacionada com sua religião, com o conceito de nirvana.

A concepção dos números negativos constituiu um problema ainda maior. Como contar "coisas" negativas? Com a aceitação destes números e das operaçSes que podem ser feitas com eles, temos a libertação definitiva da associação dos números com objetos concretos, visíveis.

7.1 O CONJUNTO Z.

O conjunto $\mathbb{Z}$ dos *números inteiros* (às vezes chamados também *inteiros relativos*) é uma extensão do conjunto dos números naturais, obtida acrescentando a $\mathbf{N}$ o zero e os números negativos, a fim de que qualquer equação do tipo $a + x = b$ tenha sempre uma solução x, quaisquer que sejam $a, b \in \mathbb{Z}$ dados. Os elementos de $\mathbb{Z}$ são chamados de *números inteiros, inteiros relativos,* ou *simplesmente inteiros.*

Tudo o que se pode afirmar a respeito dos números inteiros resulta dos seguintes **Axiomas dos números inteiros.**

1. Estão definidas em $\mathbb{Z}$ duas operações chamadas *adição* e *multiplicação*, representadas respectivamente por $x+y$ e $x \cdot y$. Essas operações são comutativas e associativas, isto é, $x + y = y + x$, $x \cdot y = y \cdot x$, $(x + y) + z = x + (y + z)$ e $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, para quaisquer $x, y, z \in \mathbb{Z}$.
2. Existe em $\mathbb{Z}$ um elemento 0, chamado *zero*, tal que $x + 0 = x$ para todo $x \in \mathbb{Z}$.
3. para todo $x \in \mathbb{Z}$, existe $-x \in \mathbb{Z}$, chamado *o inverso aditivo*, ou o *negativo* de x, tal que $-x + x = 0$.
4. Para quaisquer $x, y, z \in \mathbb{Z}$, vale $x(y + z) = xy + xz$ (distributividade).
5. Tem-se $\mathbf{N} \subset \mathbb{Z}$ e as operações de $\mathbb{Z}$, quando aplicadas a elementos de $\mathbf{N}$, coincidem com a adição e a multiplicação de números naturais. Além disso, $1 \cdot x = x$ não apenas quando $x \in \mathbf{N}$, mas para todo $x \in \mathbb{Z}$.
6. Para todo $x \in \mathbb{Z}$ tem-se uma e somente uma das alternativas seguintes: ou $x \in \mathbf{N}$, ou $x = 0$, ou $-x \in \mathbf{N}$.

Os axiomas acima formam um conjunto básico de propriedades a partir das quais se podem demonstrar todos os teoremas relativos aos números inteiros. Vejamos uma amostra.

Teorema 7.1**.** *Para quaisquer* $x, y \in \mathbb{Z}$*, tem-se*

(a) $x + y = x \Rightarrow y = 0$.

(b) $x + y = 0 \Rightarrow y = -x$.

(c) $x \cdot 0 = 0$.

(d) $(-x)(-y) = x \cdot y$.

Demonstração: Provaremos cada um dos itens (a), (b), (c) e (d).

(a) Partindo da hipótese $x + y = x$, somamos $-x$ a ambos os membros da igualdade e obtemos sucessivamente (aplicando os axiomas)

$$\begin{aligned} -x + (x + y) &= -x + x, \\ (-x + x) + y &= 0, \\ 0 + y &= 0, \\ y &= 0. \end{aligned}$$

(b) De modo análogo, somando $-x$ a ambos os membros da igualdade $x + y = 0$ obtemos $y = -x$.

(c) Temos $x + x \cdot 0 = x \cdot 1 + x \cdot 0 = x(1 + 0) = x \cdot 1 = x$. Segue-se então de (a) que $x \cdot 0 = 0$.

(d) Observe que $(-x)(-y)+(-x)y = (-x)(-y+y) = (-x)\cdot 0 = 0$. De modo análogo se vê que $x\cdot y+(-x)\cdot y = 0$. Segue-se de (b) que $(-x)(-y) = -[(-x)y]$ e que $xy = -[(-x)y]$, logo $(-x)(-y) = xy$. □

Um caso particular de (d) é a intrigante igualdade $(-1)(-1) = 1$, misteriosa durante muito tempo; só no Século XIX ficou claro que ela é uma consequência das "leis da Aritmética", que são exatamente nossos axiomas. Da prova de (d) resulta que $(-x)y = -(xy)$.

Se $x, y \in \mathbb{Z}$, escreveremos $x - y$ para representar o inteiro $x + (-y)$. A operação que associa a cada par ordenado de inteiros (x, y) o inteiro $x - y$ chama-se *subtração* e o número $x - y$ é chamado a *diferença* entre x e y.

Dados $a, b \in \mathbb{Z}$ quaisquer, existe um único inteiro x tal que $a + x = b$. Basta tomar $x = b - a$. Assim, no conjunto $\mathbb{Z}$, a equação $a+x = b$ possui uma e somente uma solução.

7.2 A ORDENAÇÃO DOS INTEIROS.

A relação de ordem em $\mathbb{Z}$ é definida de modo análogo ao que foi feito em $\mathbf{N}$. Dados os inteiros x, y, escreve-se $x < y$ e diz-se que "x é menor do que y", quando $y - x \in \mathbf{N}$, isto é, quando existir $n \in \mathbf{N}$ tal que $y = x + n$.

Quando se tem $x < y$, escreve-se também (com o mesmo significado) que $y > x$ e diz-se que "y é maior do que x".

Em particular, $x > 0$ significa que $x \in \mathbf{N}$. Diz-se então que os números naturais são os inteiros *positivos*. Analogamente, quando $x < 0$, diz-se que x é um inteiro *negativo*.

Escreve-se ainda $x \geq y$ para significar que $x > 0$ ou $x = 0$.

Teorema 7.2. *A relação de ordem entre os inteiros goza das seguintes propriedades:*

(a) *Transitividade*: Se $x < y$ e $y < z$, então $x < z$.

(b) *Tricotomia*: Dados os inteiros x e y, vale uma, e somente uma, das alternativas $x < y$, $x = y$ ou $x > y$.

(c) *Monotonicidade da adição*: se $x < y$ então $x+z < y+z$, sejam quais forem $x, y, z \in \mathbb{Z}$.

(d) *Monotonicidade da multiplicação:* Se $x < y$ e $z \in \mathbf{N}$, então $zx < yz$.

Demonstração: (a) Se $x < y$ e $y < z$, então $y = x + m$ e $z = y + n$, com $m, n \in \mathbf{N}$. Segue-se que $z = x + (m + n)$, logo $x < z$.

(b) Pelo axioma 6, dados $x, y \in \mathbb{Z}$, vale exatamente uma das alternativas $y - x \in \mathbf{N}$, $y - x = 0$, $-(y - x) \in \mathbf{N}$. A primeira significa $x < y$, a segunda $x = y$ e a terceira $x > y$.

(c) Se $x < y$, então $y = x+n$, com $n \in \mathbf{N}$, logo $y+z = (x+z)+n$, e assim $x+z < y+z$.

(d) Se $x < y$, e $z \in \mathbf{N}$, então $y = x + n$, com $n \in \mathbf{N}$, logo $yz = xz + nz$, com $nz \in \mathbf{N}$, portanto $xz < yz$. □

Corolário: [Lei do corte para a multiplicação] *Se* $xz = yz$ *e* $z \neq 0$, *então* $x = y$.

Com efeito, suponhamos inicialmente $z > 0$. Então de $x < y$, resultaria $xz < yz$ e de $x > y$ resultaria $xz > yz$. Portanto a única conclusão compatível com a hipótese $xz = yz$ é que se tenha $x = y$. O caso $z < 0$ se reduz a este pois $xz = yz$ é o mesmo que $x(-z) = y(-z)$. □

Uma importante conseqüência da lei do corte para a multiplicação é o

Teorema 7.3. [Anulamento do produto] *O produto de dois inteiros só é igual a zero quando ao menos um dos fatores é zero.*

Demonstração: Seja $xy = 0$. Se $y = 0$, o teorema está demonstrado. Se $y \neq 0$, escreveremos $xy = 0 \cdot y$ e, cortando o fator não-nulo y, obteremos $x = 0$. □

Na realidade, o teorema que acabamos de demonstrar é equivalente à lei do corte para a multiplicação, ou seja, essa lei pode ser provada a partir do teorema. Com efeito, se temos $xz = yz$ com $z \neq 0$, concluímos que $x - y = 0$, logo $x = y$.

Outra forma de enunciar o Teorema 7.3 é dizer que o produto de dois inteiros diferentes de zero é diferente de zero.

Exemplo 7.1. *Como aplicação do Teorema 5.3, vamos mostrar que se* $x^2 = y^2$ *então* $x = \pm y$.

Demonstração: Com efeito, $x^2 = y^2 \Rightarrow x^2 - y^2 = 0 \Rightarrow (x+y)(x-y) = 0 \Rightarrow x+y = 0$ ou $x - y = 0 \Rightarrow x = y$ ou $x = -y$. □

Observação: A lei do corte para a adição, $x+z = y+z \Rightarrow x = y$, se prova simplesmente somando $-z$ a ambos os membros da igualdade.

A relação de ordem em $\mathbb{Z}$ permite que se defina a noção de *valor absoluto* (ou *módulo*) de um número inteiro.

Se $x \in \mathbb{Z}$ é um número inteiro, seu *valor absoluto* $|x|$ é o número inteiro não-negativo definido por:

Se $x \in \mathbf{N}$ ou $x = 0$, então $|x| = x$.

Se $x < 0$ então $|x| = -x$.

Atenção: Quando $x < 0$, o número $-x$ é positivo!

Outra maneira de definir o valor absoluto é

$$|x| = \max\{x, -x\}.$$

Ou seja, $|x|$ é o maior dos dois números x e $-x$. Evidentemente, quando $x = 0$, tem-se $x = -x = 0$. Se $x \neq 0$, um dos dois números x, $-x$ é positivo e o outro é negativo. O maior deles é o positivo. Ele é $|x|$.

Para todo número inteiro x, tem-se $|x| = x$ ou $|x| = -x$. Em qualquer hipótese, tem-se $|x|^2 = x^2$, pois x e $-x$ têm o mesmo quadrado.

O valor absoluto se relaciona com as operações de adição e multiplicação na forma do teorema abaixo.

Teorema 7.4. *Para quaisquer inteiros* x, y *tem-se:*

(a) $|x + y| \leq |x| + |y|$,

(b) $|x \cdot y| = |x| \cdot |y|$.

Demonstração: (a) Como $|x| \geq x$ e $|y| \geq y$, segue-se que $|x| + |y| \geq x + y$. Analogamente, sabemos que $|x| \geq -x$ e $|y| \geq -y$, logo $|x| + |y| \geq -(x + y)$. Assim, o número $|x|+|y|$ é maior do que ou igual ao maior dos números $(x+y)$ e $-(x+y)$, que é precisamente $|x + y|$. Portanto $|x| + |y| \geq |x + y|$.

(b) Como $|xy|$ e $|x||y|$ são ambos não-negativos, basta provarmos que têm o mesmo quadrado para concluir que são iguais . (Vide o Exemplo 7.1 acima.) Ora, $|xy|^2 = (xy)^2 = x^2y^2$ e, por sua vez, $(|x||y|)^2 = |x|^2|y|^2 = x^2y^2$. Isto completa a demonstração. □

7.3 DIVISIBILIDADE EM Z

Praticamente todos os resultados sobre divisibilidade demonstrados nos capítulos anteriores para os números naturais se generalizam, quase sem modificações, para os números inteiros. Repetiremos rapidamente essa parte, assinalando as diferenças.

Dizemos que o inteiro a *divide* o inteiro b, o que representamos por $a|b$, se existe um inteiro c tal que $b = a \cdot c$. Dizemos então que b é um *múltiplo* de a, ou que a *divide* b, ou que a é um *fator* de b.

Um fato por vezes esquecido é que, por exemplo, -6 é múltiplo de 2, pois $-6 = (-3) \times 2$, ou que 15 é múltiplo de -5, pois $15 = (-3) \times (-5)$. Deve-se evitar erros como os exemplificados.

Observe que 0 é múltiplo de qualquer inteiro n, pois $0 = 0 \cdot n$. Por outro lado, 0 não pode ser divisor de nenhum número inteiro. Ou seja, **a divisão por** 0 **não está definida, não faz sentido.**

Teorema 7.5. *Sejam* a *e* b *inteiros não-nulos. Se* a *divide* b *e* b *divide* a*, então* $a = \pm b$.

Demonstração: Com efeito, se $a|b$, então existe um inteiro c tal que $b = a \cdot c$. Se $b|a$, existe então um inteiro d tal que $a = b \cdot d$.

Temos então $b = (bd)c = bdc$, donde $1 = dc$. Mas então $d = \pm 1$, $c = \pm 1$, (Vide Capítulo 2, Seção 9. exemplo 2.7) e assim $a = \pm b$. □

Teorema 7.6. *Se* a, b *e* c *são inteiros e* $a|b$ *e* $a|c$*, então* $a|(b + c)$.

Demonstração: Com efeito, se $a|b$, então existe k_1 inteiro tal que $b = k_1 a$. Se $a|c$, existe k_2 inteiro tal que $c = k_2 a$. Assim, $b + c = k_1 a + k_2 a = (k_1 + k_2)a$, donde $a|(b + c)$, o que queríamos demonstrar. □

A recíproca deste teorema nem sempre é verdadeira. É fácil achar inteiros a, b e c tais $a|(b + c)$ mas a não divide b e a não divide c.

Seja dado um número natural a e considere o conjunto

$$M_a = \{n \in \mathbb{Z} \quad \hbox{taisque } n \text{ é múltiplo de } \quad a\}.$$

Observe que se $r, s \in M_a$, então

a) $r + s \in M_a$ e

b) $r - s \in M_a$,

como é imediato verificar.

De a) segue-se trivialmente que se $r \in M_a$ e $m \in \mathbb{Z}$, então $mr = r + r + \cdots + r \in M_a$. Ou seja, o conjunto M_a é fechado em relação à soma, e à diferença de elementos de M_a e ao produto de um elemento de M_a por um inteiro qualquer. Este fato é extremamente importante. A notação clássica para M_a é (a); este conjunto é chamado, em Álgebra, o *ideal gerado por* (a).

Mostra-se, reciprocamente, (veja a digressão teórica deste capítulo) que se um conjunto $S \subset \mathbb{Z}$ é fechado em relação à soma e à subtração, então existe $a \in \mathbf{N}$ tal que $S = (a)$, ou seja, S é formado pelos múltiplos de um certo inteiro a, que podemos supor positivo.

O algoritmo da divisão, que já demonstramos para números naturais, é um dos resultados fundamentais da Aritmética dos inteiros. Ele está subjacente a muitos dos resultados importantes que podemos demonstrar sobre os números inteiros. Seu enunciado é o seguinte:

Teorema 7.7. *Sejam* a *e* b *inteiros, com* $b > 0$. *Existem então inteiros* q *e* r *tais que*

$$a = bq + r, \qquad 0 \leq r < b.$$

Além disso, q *e* r *ficam unicamente determinados por* a *e* b (dizemos que q e r são únicos para a e b dados).

Demonstração: A prova que apresentaremos, também utilizando o princípio da boa ordenação, é mais simples do que a que apresentamos para os números naturais, pois agora não precisamos nos preocupar em saber se os números envolvidos são números naturais, isto é, inteiros positivos ou se o resto é nulo ou não-nulo.

Como b é positivo, temos que

$$(-|a|) \cdot b \leq -|a| \leq a.$$

Isso mostra que há um múltiplo de b que não é maior do que a (o número $(-|a|) \cdot b$).

Considere o conjunto de *todos* os inteiros da forma $a - bx$, para x inteiro qualquer. Pelo exposto acima, este conjunto contém um elemento não-negativo. De fato, $a - (|a|)b \geq 0$. Defina agora S como sendo o conjunto de todos os números não-negativos da forma $a - bx$. Pela observação acima, S é não-vazio. Pelo princípio da boa ordenação, existe então em S um menor elemento, r, que será um número não-negativo. Como r é um elemento de S, ele é da forma

$$r = a - qb,$$

para algum inteiro q,

donde

$$a = qb + r.$$

Já sabemos que r é não-negativo. Afirmamos que r é estritamente menor do que b.

Com efeito, se $r \geq b$, então

$$a - b(q + 1) = a - bq - b = r - b \geq 0,$$

pertence a S e é menor do que r $(r = a - bq)$, uma contradição. Assim, $0 \leq r < b$.

Suponha agora que

$$a = bq + r, \qquad 0 \leq r < b,$$

$$a = bq' + r', \qquad 0 \leq r' < b,$$

e suponha que $r \leq r'$ (isso não é nenhuma perda de generalidade). Mas então

$$r' - r = b \cdot (q' - q)$$

é não-negativo, menor do que b e um múltiplo de b. A única possibilidade é $r' - r = 0$, donde $r' = r$ e $q' = q$. □

Dizemos que um inteiro não-nulo é *primo* se ele é diferente de ± 1 e se os únicos divisores de p são ± 1 e $\pm p$. De modo inteiramente análogo ao que já foi feito, demonstra-se que qualquer inteiro pode ser decomposto, de maneira essencialmente única, em um produto de números primos.

A definição de máximo divisor comum de dois inteiros é análoga à do máximo divisor comum de dois números naturais. O máximo divisor comum de dois números inteiros é sempre positivo. Demonstra-se então, como antes, que o m.d.c. de dois números inteiros pode ser calculado usando suas decomposições em fatores primos ou o algoritmo de Euclides.

Um fato novo, que não é verdadeiro para os números naturais, é que o algoritmo de Euclides nos permite escrever o m.d.c.(a, b) como uma *combinação linear* de a e de b, resultado importante que utilizaremos várias vezes.

Teorema 7.8**.** *Sejam* a *e* b *inteiros não-nulos e* $d = \text{m.d.c.}(a, b)$*. Existem então inteiros* u *e* t *tais que* $d = ua + tb$*.*

Antes de fazermos a demonstração geral, mostremos como podemos achar os inteiros u e t em um caso concreto: escrevamos o m.d.c.$(754, 221)$ como combinação linear de 754 e de 221:

Temos, aplicando o algoritmo de Euclides a 754 e 221,

$$754 = 3 \cdot 221 + 91 \qquad \text{(A)}$$

$$221 = 2 \cdot 91 + 39 \qquad \text{(B)}$$

$$91 = 2 \cdot 39 + 13 \qquad \text{(C)}$$

$$39 = 3 \cdot 13. \qquad \text{(D)}$$

E assim m.d.c.(754, 221) = 13.

De (C) vemos que

$$13 = 91 - 2 \cdot 39.$$

Mas usando (B) temos $39 = 221 - 2 \cdot 91$, logo $13 = 91 - 2 \cdot (221 - 2 \cdot 91) = 5 \cdot 91 - 2 \cdot 221$. De (A) decorre que $91 = 754 - 3 \cdot 221$, donde, finalmente,

$$13 = 5 \cdot 754 - 17 \cdot 221.$$

A demonstração geral é inteiramente análoga ao exemplo dado. Relembremos o algoritmo de Euclides: se a e b, são números inteiros positivos, aplicando sucessivamente o algoritmo da divisão

$$a = bq_1 + r_1, \qquad 0 \leq r_1 < b. \tag{E}$$

$$b = r_1 q_2 + r_2, \qquad 0 \leq r_2 < r_1, \tag{F}$$

$$r_1 = r_2 q_3 + r_3, \qquad 0 \leq r_3 < r_2, \tag{G}$$

$$\dots$$

$$r_{n-2} = r_{n-1} q_n + r_n, \qquad 0 \leq r_n < r_{n-1}, \tag{H}$$

$$\dots$$

Vemos que os restos $r_1, \dots, r_n$ formam uma sucessão estritamente decrescente de números inteiros não-negativos. Então, para algum índice s, devemos obter resto nulo, pois do contrário o processo poderia continuar sempre. Ou seja

$$r_{s-3} = r_{s-2} q_{s-1} + r_{s-1} \tag{I}$$

$$r_{s-2} = r_{s-1} q_s \tag{J}$$

e $\text{mdc}\,(a, b) = r_{s-1}$.

Para escrever o $\text{mdc}\,(a, b)$ como combinação linear de a e de b, temos, de (I), que $r_{s-3} - r_{s-2} q_{s-1} = r_{s-1}$. Como $r_{s-4} = r_{s-3} q_{s-2} + r_{s-2}$, vem que

$$\begin{aligned} r_{s-1} &= r_{s-3} - (r_{s-4} - r_{s-3} q_{s-2}) q_{s-1} \\ &= r_{s-3}(1 + q_{s-2} q_{s-1}) - r_{s-4} q_{s-1}. \end{aligned}$$

Podemos obviamente continuar desta maneira, substituindo agora o valor de r_{s-3}, etc. até chegarmos enfim a uma expressão que será da forma $ua + tb$, como queríamos demonstrar.

□

Uma aplicação imediata deste teorema é a seguinte propriedade do máximo divisor comum.

Teorema 7.9. *Sejam* a *e* b *inteiros não nulos. Se* m.d.c.$(a, b) = d$ *e* k *é um divisor comum de* a *e de* b*, então* $k|d$.

Com efeito, sabemos que existem inteiros u e t tais que $d = au + bt$. Como k é um divisor comum de a e de b, existem q_1 e q_2 tais que $a = q_1k$ e $b = q_2k$. Então,

$$d = q_1ku + q_2kt = (q_1u + q_2t)k,$$

ou seja, k é um divisor de d, como desejávamos mostrar. □

Exemplo 7.2. *Uma pessoa possui dois recipientes, um de 9 litros e outro de 16 litros. Como poderá, usando-os, obter um litro de água em um deles?*

Solução: Como

$$16 = 1 \times 9 + 7$$

$$9 = 1 \times 7 + 2$$

$$7 = 3 \times 2 + 1$$

$$2 = 1 \times 2,$$

vemos que

$$16 \times 4 - 7 \times 9 = 1.$$

Este resultado pode ser interpretado da seguinte maneira:

Chamando de P_1 e de P_2 os recipientes de 16 e de 9 litros respectivamente, proceda como segue: Encha P_1 com 16 litros de água e verta 9 litros desta água em P_2. Esvazie P_2. Tente encher novamente P_2 com a água que resta em P_1. Teremos então 7 litros de água em, P_2 e 0 litros em P_1. Encha agora P_1 com 16 litros d'água. Com esta água, complete P_2. Esvazie P_2. Com a água restante em P_1, tente encher P_2, e continue como feito até agora: enchendo P_1, transferindo toda ou parte de sua água para P_2, esvaziando P_2 quando

este estiver cheio, voltando a encher P_1 quando este estiver vazio, etc. Afirmamos então que após ter enchido P_1 4 vezes e completado P_2 7 vezes com a água de P_1, restará em P_1 exatamente 1 litro d'água, pois $16 \times 4 - 7 \times 9 = 1$! □

Dois inteiros não-nulos a e b são *relativamente primos* se m.d.c.$(a, b) = 1$. Dizemos também que a é *primo com* b, ou que a e b são *primos entre si*. Observe que a é primo com b, se e somente se existem inteiros u e t tais que $au + bt = 1$. Como aplicação imediata desta observação redemonstramos o seguinte resultado:

Exemplo 7.3. *Se* $p|ab$, *e* m.d.c.$(p, a) = 1$, *então* $p|b$.

Como m.d.c.$(p, a) = 1$, existem inteiros u e t tais que $pu+at = 1$. Daí $pbu+abt = b$. Como $p|pbu$ e $p|abt$, (pois $p|ab$), então $p|(pbu + abt)$, isto é, $b|b$. □

7.4 UMA DIGRESSÃO TEÓRICA

O estudo que apresentamos do máximo divisor comum, embora satisfatório para a Aritmética dos inteiros, pode ser modificado. Isso é feito para obtermos um tratamento que possa ser aplicado a outras situações. Por exemplo, o conjunto $R[t]$ dos polinômios com coeficientes reais, com as operações usuais de soma e de produto de polinômios constitui uma estrutura algébrica que goza de muitas das propriedades dos inteiros. Em verdade, ambos são exemplos dos chamados *domínios euclidianos*. Em $R[t]$ existe um algoritmo de divisão inteiramente análogo ao dos inteiros, e dois polinômios não-nulos têm um máximo divisor comum (que será um polinômio). O tratamento que apresentamos a seguir para o máximo divisor comum pode ser utilizado em situações em que não existe a noção de "menor do que", a qual foi utilizada em nossa apresentação. Além disso, ele enfatiza o emprego das combinações lineares de dois elementos, e usa, mesmo sem explicitá-la, uma noção central em Álgebra, a de *ideal*.

Seja S um subconjunto não-vazio do conjunto dos números inteiros. Dizemos que S é *fechado em relação à soma* se a soma de dois elementos quaisquer de S é um elemento de S. Dizemos que S é *fechado em relação à subtração* se a diferença de dois elementos quaisquer de S é um elemento de S. Por exemplo, o conjunto de todos os múltiplos de 2 é fechado em relação à soma e à subtração, pois a soma de dois múltiplos de 2 é um múltiplo de 2 e a

diferença de dois múltiplos de 2 é um múltiplo de 2, visto que se $\mathfrak{a} = 2 \cdot \mathfrak{b}$ $\mathfrak{a}' = 2 \cdot \mathfrak{b}'$, então $\mathfrak{a} \pm \mathfrak{a}' = 2 \cdot (\mathfrak{b} \pm \mathfrak{b}')$. De maneira análoga, poderíamos ver que o conjunto dos múltiplos de qualquer inteiro $\mathfrak{m}$ é fechado em relação à soma e à subtração. Em verdade, estes são os únicos subconjuntos dos inteiros fechados em relação a estas duas operações, como mostraremos agora:

Teorema 7.10**.** *Seja* S *um subconjunto não-vazio dos inteiros, fechado em relação à soma e à subtração. Então, ou* $\mathsf{S} = \{0\}$, (*conjunto formado pelo número* 0), *ou* S *é formado por todos os múltiplos de um inteiro positivo.*

Demonstração: Obviamente o conjunto $\{0\}$ é fechado em relação à soma e à subtração, pois $0 + 0 = 0$ e $0 - 0 = 0$. Suponha então que $\mathsf{S} \neq \{0\}$. Existe então em S um elemento não nulo, $\mathfrak{a}$. Afirmamos, além disso, que S contém um inteiro *positivo*. Com efeito, $0 \in \mathsf{S}$, pois $0 = \mathfrak{a} - \mathfrak{a}$. Então, $-\mathfrak{a} \in \mathsf{S}$, pois $-\mathfrak{a} = 0 - \mathfrak{a}$. Como ou $\mathfrak{a}$ ou $-\mathfrak{a}$ é positivo, S contém um elemento positivo.

Considere agora o conjunto de todos os elementos de S que são positivos. Pelas observações acima, este conjunto é não-vazio. Então, pelo princípio da boa ordenação, ele possui um menor elemento, $\mathfrak{b}$.

Todo múltiplo de $\mathfrak{b}$ pertence a S. Com efeito, se $\mathfrak{t} > 0$, $\mathfrak{t}\mathfrak{b} = \mathfrak{b} + \mathfrak{b} + \cdots + \mathfrak{b}$ ($\mathfrak{t}$ vezes) pertence a S pois S é é fechado em relação à adição; como $-\mathfrak{t}\mathfrak{b} = 0 - \mathfrak{t}\mathfrak{b} = -\mathfrak{t}\mathfrak{b}$, $-\mathfrak{t}\mathfrak{b}$ pertence a S, pois S é fechado em relação à subtração (lembramos que $0 \in \mathsf{S}$).

Além disso, o conjunto S é formado pelos múltiplos deste menor elemento positivo $\mathfrak{b}$. Com efeito, se $\mathfrak{n} \in \mathsf{S}$, então, pelo algoritmo da divisão, existem $\mathfrak{q}$ e $\mathfrak{r}$, $0 \leq \mathfrak{r} < \mathfrak{b}$, tais que

$$\mathfrak{n} = \mathfrak{b}\mathfrak{q} + \mathfrak{r}.$$

Ora, $\mathfrak{b}\mathfrak{q} = \mathfrak{b} + \mathfrak{b} + \cdots + \mathfrak{b}$ certamente pertence a S. Então $\mathfrak{r} = \mathfrak{n} - \mathfrak{b}\mathfrak{q}$ pertence a S, como diferença de dois elementos de S. Mas $\mathfrak{r} < \mathfrak{b}$. Ou seja, se $\mathfrak{r} > 0$, achamos em S um elemento positivo menor do que $\mathfrak{b}$, uma contradição. Então $\mathfrak{r} = 0$, ou seja, $\mathfrak{n} = \mathfrak{b}\mathfrak{q}$. □

Sejam $\mathfrak{a}$ e $\mathfrak{b}$ inteiros. Dizemos que o inteiro $\mathfrak{d}$ é um *máximo divisor comum de* $\mathfrak{a}$ *e* $\mathfrak{b}$ se

1) $\mathfrak{d}$ divide $\mathfrak{a}$ e $\mathfrak{d}$ divide $\mathfrak{b}$ (ou seja, $\mathfrak{d}$ é um divisor comum de $\mathfrak{a}$ e de $\mathfrak{b}$);

2) $\mathtt{d}$ é um múltiplo de qualquer divisor comum de $\mathtt{a}$ e de $\mathtt{b}$.

Uma observação imediata é que se $\mathtt{d}_1$ e $\mathtt{d}_2$ são dois máximos divisores comuns de $\mathtt{a}$ e de $\mathtt{b}$, então $\mathtt{d}_1 = \pm\mathtt{d}_2$. Com efeito, uma aplicação imediata de 2) mostra que $\mathtt{d}_1|\mathtt{d}_2$ e $\mathtt{d}_2|\mathtt{d}_1$, logo $\mathtt{d}_1 = \pm\mathtt{d}_2$.

Dois inteiros não-nulos $\mathtt{a}$ e $\mathtt{b}$ têm sempre um máximo divisor comum:

Teorema 7.11**.** *Sejam* $\mathtt{a}$ *e* $\mathtt{b}$ *inteiros não-nulos. Existem então um máximo divisor comum* $\mathtt{d}$ *de* $\mathtt{a}$ *e* $\mathtt{b}$ *e inteiros* $\mathtt{u}$ *e* $\mathtt{t}$ *tais que*

$$\mathtt{d} = \mathtt{u}\cdot\mathtt{a} + \mathtt{t}\cdot\mathtt{b}.$$

Demonstração: Considere o conjunto $\mathtt{S}$ dos inteiros da forma $\mathtt{x}\mathtt{a} + \mathtt{y}\mathtt{b}$, com $\mathtt{x}$ e $\mathtt{y}$ inteiros arbitrários. $\mathtt{S}$ é não-vazio, pois $0 = 0\mathtt{a} + 0\mathtt{b}$ é um elemento de $\mathtt{S}$. Além disso, $\mathtt{S}$ é fechado em relação à soma e à subtração: se $\mathtt{s}_1 = \mathtt{x}_1\mathtt{a}+\mathtt{y}_1\mathtt{b}$ e $\mathtt{s}_2 = \mathtt{x}_2\mathtt{a}+\mathtt{y}_2\mathtt{b}$ são elementos de $\mathtt{S}$, então $\mathtt{s}_1 \pm \mathtt{s}_2 = (\mathtt{x}_1 \pm \mathtt{x}_2)\mathtt{a} + (\mathtt{y}_1 \pm \mathtt{y}_2)\mathtt{b}$. Já provamos que então $\mathtt{S}$ é formado pelos múltiplos de um menor elemento positivo, que chamaremos de $\mathtt{d}$. Como $\mathtt{d} \in \mathtt{S}$, existem inteiros $\mathtt{u}$ e $\mathtt{t}$ tais que

$$\mathtt{d} = \mathtt{u}\mathtt{a} + \mathtt{t}\mathtt{b}.$$

Observe que $\mathtt{a} = 1\cdot\mathtt{a} + 0\cdot\mathtt{b}$, $\mathtt{b} = 0\cdot 1 + 1\cdot\mathtt{b}$, logo $\mathtt{a}$ e $\mathtt{b}$ são elementos de $\mathtt{S}$. Segue-se que $\mathtt{a}$ e $\mathtt{b}$ são múltiplos de $\mathtt{d}$, isto é, que $\mathtt{d}$ é um divisor comum de $\mathtt{a}$ e de $\mathtt{b}$.

Por outro lado, se $\mathtt{c}$ é um divisor comum qualquer de $\mathtt{a}$ e de $\mathtt{b}$, temos que $\mathtt{a} = \mathtt{k}_1\mathtt{c}$, $\mathtt{b} = \mathtt{k}_2\mathtt{c}$, e daí vemos que

$$\mathtt{d} = \mathtt{u}\mathtt{k}_1\mathtt{c} + \mathtt{t}\mathtt{k}_2\mathtt{c} = \mathtt{c}(\mathtt{u}\mathtt{k}_1 + \mathtt{t}\mathtt{k}_2),$$

logo $\mathtt{c}$ é divisor de $\mathtt{d}$. Isso conclui a demonstração de que $\mathtt{d}$ é um máximo divisor comum de $\mathtt{a}$ e de $\mathtt{b}$. □

Se $\mathtt{d}$ é um máximo divisor comum de $\mathtt{a}$ e de $\mathtt{b}$, então o mesmo acontece com $-\mathtt{d}$ (verifique isso!). Assim, $\mathtt{a}$ e $\mathtt{b}$ têm sempre um máximo divisor comum positivo. Ele será chamado de *máximo divisor comum de* $\mathtt{a}$ *e de* $\mathtt{b}$, e representado por m.d.c.($\mathtt{a}$, $\mathtt{b}$) .

É claro que o máximo divisor comum obtido agora coincide com o máximo divisor que já tínhamos achado em nosso tratamento inicial (demonstre isso!). Podemos então

escrevê-lo como combinação linear dos dois inteiros a e b, usando o algoritmo de Euclides, como feito anteriormente.

7.5 AS EQUAÇÕES DIOFANTINAS

Uma aplicação significante do máximo divisor comum de dois números é à determinação das soluções inteiras das equações do tipo $ax + by = c$, onde a, b e c são números inteiros, a e b não-nulos [17]. Equações desta forma são exemplos das chamadas *equações diofantinas*. Resolver uma equação diofantina é achar suas soluções inteiras.

Exemplo 7.4. *Ache as soluções inteiras da equação diofantina* $ax + by = c$ [18].

Seja portanto a equação diofantina

$$ax + by = c,$$

isto é, nela a, b e c são números inteiros, a e b não-nulos, e procuramos soluções (x, y) que sejam pares ordenados de números inteiros. Este problema admite solução completa, como mostrado pelo teorema a seguir:

Teorema 7.12. *A equação diofantina* $ax + by = c$ *tem soluções inteiras se e somente se o máximo divisor comum,* d*, de* a *e* b *divide* c*. Se isso acontecer, todas as soluções da equação são da forma* $x = x_0 + (b/d)k$, $y = y_0 - (a/d)k$, k *um inteiro qualquer.*

Demonstração: Suponha, em primeiro lugar, que a equação tem uma solução inteira (x_0, y_0), ou seja, que $ax_0 + by_0 = c$, com x_0 e y_0 inteiros. Seja d o máximo divisor comum de a e b. Então, $a = da_1$ e $b = db_1$, com a_1 e b_1 inteiros. Logo, $c = (a_1x_0 + b_1y_0) \cdot d$, isto é, d divide c, pois $a_1x_0 + b_1y_0$ será um inteiro.

---

[17] Agradecemos à Revista do Professor de Matemática a permissão para usar este material, que foi publicado originalmente como o artigo 'Úma Equação Diofantina e suas resoluções", de Gilda da la ROCQUE e João Bosco PITOMBEIRA, no número 19 (1991), pags. 39-47.

[18] O matemático grego Diofanto (325?, 410?) mostrou como achar uma solução desta equação. O matemático hindu Aryabata (476, ?) estudou sistemáticamente este tipo de equação, determinando a forma geral das soluções.

Suponha, agora, que o máximo divisor comum d, de a e b, divide c. Então, $c = dc_1$, e a equação pode ser escrita como

$$ax + by = dc_1.$$

Ora, se d é o máximo divisor comum de a e b, sabemos que existem inteiros r e s tais que

$$ar + bs = d,$$

donde, multiplicando ambos os membros pelo número inteiro c_1, vem que

$$a(rc_1) + b(sc_1) = dc_1 = c,$$

ou seja, mostramos que o par (rc_1, sc_1) é solução de $ax + by = c$.

Antes de concluirmos a demonstração, achando todas as soluções inteiras da equação dada, observe que este teorema tem o seguinte corolário imediato:

Corolário. *Se* m.d.c.$(a, b) = 1$ (*isto é, se* a *e* b *são relativamente primos*), *então a equação* $ax + by = c$ *sempre tem soluções inteiras, qualquer que seja o inteiro* c.

Já sabemos como encontrar uma solução da equação diofantina $ax + by = c$. Perguntamos se, a partir dela, é possível encontrar *todas* as demais. É disto que trataremos agora.

Consideremos mais uma vez a equação diofantina $ax + by = c$e seja $d =$ m.d.c.(a, b). Supondo que d divide c (para que exista solução inteira), podemos escrever $a = a_1 d,\ b = b_1 d,\ c = c_1 d$, com m.d.c.$(a_1, b_1) = 1$.

Assim, a equação

$$ax + by = c \tag{A}$$

se transforma na equação

$$a_1 dx + b_1 dy = dc_1 \tag{B}$$

ou ainda, como $d \neq 0$,

$$a_1 x + b_1 y = c_1, \tag{C}$$

com a_1 e b_1 relativamente primos. Vemos portanto que as soluções de (A) são as mesmas que as de (C). Assim, para achar todas as soluções de (A), é suficiente achar todas as soluções de (C).

Seja portanto (x_0, y_0) uma solução inteira de $a_1x+b_1y = c_1$, com a_1 e b_1 relativamente primos. Então $a_1x_0+b_1y_0 = c_1$. Ora, se ao primeiro membro acrescentarmos e subtraírmos o mesmo número, a igualdade continuará valendo. Consideremos portanto a equação

$$a_1x_0 + b_1y_0 + a_1b_1k - a_1b_1k = c_1,$$

com k um inteiro arbitrário. Reagrupando convenientemente os termos desta equação obtemos

$$a_1(x_0 + b_1k) + b_1(y_0 - a_1k) = c_1,$$

o que mostra que o par $(x_0 + b_1k, y_0 - a_1k) = (x_0 + (b/d)k, y_0 - (a/d)k)$ é ainda uma solução da equação diofantina considerada. (Observe que, até este ponto, a hipótese de que m.d.c.$(a_1, b_1) = 1$ não foi utilizada!).

Será que este método fornece *todas* as soluções inteiras? Existirão outras? Para buscarmos uma resposta desta pergunta, suponhamos que (x_0, y_0) e (x_1, y_1) são soluções inteiras de $a_1x + b_1y = c_1$, com m.d.c.$(a_1, b_1) = 1$. Temos então $a_1x_0 + b_1y_0 = c_1$ e $a_1x_1 + b_1y_1 = c_1$. Logo,

$$a_1(x_1 - x_0) = b_1(y_0 - y_1).$$

Portanto, $a_1|b_1(y_0 - y_1)$. Como m.d.c.$(a_1, b_1) = 1$, $a_1|(y_0 - y_1)$ (veja o Exemplo 4.9). Logo, existe um inteiro k tal que $y_0 - y_1 = ka_1$, isto é, $y_1 = y_0 - ka_1$. Mas então $a_1(x_1 - x_0) = b_1(y_0 - y_1) = b_1ka_1$, e como $a_1 \neq 0$, $xx_1 - x_0 = b_1k$, isto é, $x_1 = x_0 + b_1k$. Logo qualquer solução (x_1, y_1) será da forma $(x_0 + b_1k, y_0 - a_1k) = (x_0 + (b/d)k, y_0 - (a/d)k)$, com k inteiro. □

Observe que a condição de a_1 e b_1 serem relativamente primos só é necessária para garantir que, deste modo, foram encontradas todas as soluções.

Exemplo 7.5. *Mostre que a equação diofantina* $4x + 6y = 9$ *não tem solução* (*inteira*!).

Solução: Como m.d.c.(4, 6) = 2, e 2 não divide 9, vemos imediatamente que a equação não pode ter soluções inteiras. De resto, é claro que o número $4x + 6y$, com x e y inteiros, será sempre par, logo não pode ser igual a 9. □

Exemplo 7.6. *Determine todas as soluções inteiras da equação* $8x + 12y = 36$.

Solução: É claro que esta equação tem solução, pois m.d.c.(8, 12) = 4 e 4|36.

É fácil ver que $x_0 = 0$, $y_0 = 3$ é uma solução da equação. Então as soluções são os pares (x, y) da forma

$$\begin{aligned} x &= x_0 + (b/d)k = 0 + (12/4)k = 3k \\ y &= y_0 - (a/d)k = 3 - (8/4)k = 3 - 2k, \end{aligned}$$

com k inteiro. □

Observe que se a equação $ax + by = c$ tem soluções, uma delas pode ser encontrada usando o algoritmo de Euclides, que nos permite escrever o m.d.c.(a, b) na forma $ar+bs = d$.

Exemplo 7.7. *Ache uma solução inteira da equação*

$$143x + 17y = 132.$$

Solução: Em primeiro lugar, m.d.c.(143, 17) = 1, logo a equação tem soluções inteiras. Para achar uma delas, apliquemos o algoritmo de Euclides a 143 e 17.

$$\begin{aligned} 143 &= 8 \cdot 17 + 7 \\ 17 &= 2 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1. \end{aligned}$$

Logo,

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 = 7 - 2 \cdot [17 - 2 \cdot 7] = \\ &= 5 \cdot 7 - 2 \cdot 17 = 5 \cdot [143 - 8 \cdot 17] - 2 \cdot 17 = \\ &= 5 \cdot 143 - 42 \cdot 17. \end{aligned}$$

Donde

$$143 \cdot (5 \cdot 132) + 17 \cdot (-42 \cdot 132) = 132,$$

ou seja, $(x_0, y_0) = (660, -5544)$ é solução da equação dada. □

Exemplo 7.8. *Determine todas as soluções da equação diofantina*

$$143x + 17y = 132.$$

Já sabemos que uma das soluções desta equação é:

$$(x_0, y_0) = (660, -5544).$$

Então, *todas* as soluções são da forma

$$x = 660 + 17k,$$
$$y = -5544 - 143k,$$

onde k é um inteiro arbitrário. Dando a k os valores $0, \pm 1, \ \pm 2, \ldots$, obtemos todas as soluções inteiras da equação. □

7.6 POTÊNCIAS E RADICAIS

No Capítulo 2, dissemos que uma das aplicaçSes importantes do Princípio da Indução Matemática é para definir funçSes $f : \mathbf{N} \to \mathbf{N}$. Foi assim que definimos a *adição* e o *produto* de dois números naturais. Apresentamos agora um outro exemplo de função definida indutivamente.

Exemplo 7.9. *Seja* a *um número natural. Defina* a elevado à potência n, que será representado por a^n, da seguinte maneira:

$$a^1 = a$$
$$a^n = a \cdot a^n.$$

Desta maneira, definimos a potência n-ésima de a, para todo natural n. De fato, seja $f_a : \mathbf{N} \to \mathbf{N}$ definida indutivamente por $f_a(1) = a$, $f_a(n) = a \cdot f_a(n-1)$. Então, como já sabemos, a função f está perfeitamente bem definida. Ou seja, podemos calcular f_a para um número natural qualquer.

O número a é chamado de *base* e o natural n é chamado de *expoente*.

Observe que $f_a(2) = a \cdot f_a(1) = a \cdot a =$, $f_a(3) = a \cdot f_a(2) = a \cdot (a \cdot a) = a \cdot a \cdot a$, $f_a(4) = a \cdot f_a(3) = a \cdot (a \cdot a \cdot a) = a \cdot a \cdot a \cdot a$, e assim sucessivamente. Tradicionalmente, escrevemos $f_a(n) = a^n$. As designaçSes "a ao quadrado" e "a ao cubo" para a^2 e a^3 respectivamente se originaram com os gregos, para os quais os fatos algébricos tinham que ser tratados geometricamente.

É fácil verificar que

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

$$(ab)^m = a^m b^m \tag{2}$$

$$(a^n)^m = a^{nm}. \tag{3}$$

Estas são as chamadas "leis dos expoentes".

Observe a vantagem da notação tradicional de "potências", em relação à notação funcional $f_a(n)$ introduzida acima. Usando esta última, as três igualdades acima se escreveriam como $f_a(n+m) = f_a(n) \cdot f_a(m)$, $f_{ab}(m) = f_a(m) f_b(m)$ e $f_{f_a(m)}(n) = f_a(mn)$! No entanto, para demonstrar as "leis dos expoentes" acima usaremos a notação funcional.

Demonstraremos sucessivamente (1), (2) e (3):

(1) Mostremos em primeiro lugar que $a^{n+m} = a^n \cdot a^m$; isto é, para todo n natural, $f_a(k + n) = f_a(k) \cdot f_a(n)$. Seja k um número natural fixo. Temos que $f_a(k + 1) = f_a(1 + k) = f_a(1) \cdot f_a(k) = f_a(a) \cdot a = f_a(k) \cdot f_a(1)$.

Suponha agora que $f_a(k+s) = f_a(k) \cdot f_a(s)$ e mostremos que então $f_a(k+(s+1)) = f_a(k) \cdot f_a(s+1)$.

Ora, $f_a(k + (s + 1)) = f_a((k + s) + 1) = f_a(k + s) \cdot f_a(1) = (f_a((k) \cdot f_a(s)) \cdot f_a(1) = f_a(s) \cdot (f_a(s) \cdot f_a(1)) = f_a(k) \cdot f_a(s+1)$. Então, pelo princípio da Indução Finita, qualquer que seja o n natural, $f_a(k + n) = f_a(k) \cdot f_a(n)$.

(2) Mostremos agora que $(ab)^m = a^m b^m$, ou seja, que $f_{ab}(m) = f_a(m) f_b(m)$, para todo natural m.

Em primeiro lugar, $f_{ab}(1) = ab = f_a(1) f_b(1)$.

Suponha agora que $f_{ab}(k) = f_a(k) f_b(k)$, e mostremos que então $f_{ab}(k+1) = f_a(k+1) f_b(k+1)$

Ora, $f_a(k+1)f_b(k+1) = (f_a(k)f_a(1))(f_b(k)f_b(1)) = (f_a(k)f_a(1))(f_b(k)f_b(1)) = f_a(k+1)f_b(k+1)$.

Então, pelo Princípio da Indução Finita, $f_{ab}(n) = f_a(n)f_b(n)$ para todo natural n.

(3) Resta agora demonstrar que $(a^n)^m = a^{nm}$, ou seja, que $f_{f_a(m))}(n) = f_a(mn)$.

Em primeiro lugar, $f_{(f_a(1))}(n) = f_a(n)$.

Suponha agora que $f_{(f_a(k))}(n) = f_a(kn)$.

Mostraremos então que

$f_{(f_a(k))}(n+1) = f_a(k(n+1))$. Ora $f_{(f_a(k))}(n+1) = f_{f_a(k)}(n)f_{f_a(k)}(1)f_{(f_a(k)}(n) = f_a(k)f_{f_a(k)}(n) = f_a(k)f_a(kn) = f_a(k+kn) = f_a(k(n+1))$.

Assim, pelo Princípio da Indução Finita, $f_{f_a(m))}(n) = f_a(mn)$, para todo n natural. Um processo de indução análogo sobre m completa a demonstração. □

Com a notação de potência, uma expressão como a^{b^c} é ambígua. Significa $(a^b)^c$ ou $a^{(b^c)}$? No primeiro caso, teríamos imediatamente que $(a^b)^c = a^{bc}$. Assim, *convenciona-se* que a expressão a^{b^c} significa $a^{(b^c)}$, ou seja, primeiro eleva-se b à potência c, e em seguida eleva-se a a este resultado.

Exemplo 7.10. *O cálculo com expoentes inteiros é uma generalização imediata do cálculo com expoentes naturais, já estudado no exemplo precedente.*

O que são expoentes negativos e nulos? Em primeiro lugar, como estas operaçSes com expoentes estão definidas no conjunto $\mathbb{Z}$ dos números inteiros, é importante que elas coincidam com as operaçSes correspondentes quando os expoentes forem números naturais. Ou seja, desejamos que as propriedades já demonstradas para as operaçSes com expoentes para os números naturais

$$a^{n+m} = a^n \cdot a^m$$

$$(ab)^m = a^m b^m$$

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

continuem válidas quando m e n forem inteiros quaisquer.

Qual a definição de a^{-m}, para m um inteiro positivo? Se quisermos que $a^{m-n} = a^n \cdot a^{-m}$, como a^{n-m} é o produto de $n-m$ fatores iguais a a e a^n é o produto de n

fatores iguais a a, então forçosamente, para que esta igualdade se verifique, em seu lado direito temos que dividir a^n pelo produto de m fatores iguais a a. Isto é, $a^{-m} = 1/a^m$!

Além disso, se quisermos mais uma vez preservar a propriedade de que $a^{m+n} = a^m \cdot a^n$, como $a^{m-m} = a^0 = a^m \cdot \frac{1}{a^m} = 1$, devemos ter que $a^0 = 1$.

Percebido isso, é fácil definir expoentes inteiros.

Seja a um inteiro positivo. Mais uma vez **defina** $a^1 = a$. **Defina** também $a^0 = 1$. Se n é um número inteiro qualquer positivo, defina, como antes, $a^{n+1} = a \cdot a^n$. Se n é um inteiro positivo, defina $a^{-n} = 1/a^n$. Verifica-se então que continuam valendo as igualdades

$$a^{n+m} = a^n \cdot a^m \tag{4}$$

$$(ab)^m = a^m b^m \tag{5}$$

$$(a^n)^m = a^{nm}, \tag{6}$$

onde n e m são inteiros quaisquer. □

Utilizamos neste exemplo a noção de *número racional*, pois estamos tomando inversos de inteiros, que em geral não são inteiros. No entanto, a importância de se compreender que as definiçSes de a^0 e de $a^{-n} = 1/a^n$ são "naturais", para que as leis das operaçSes com os expoentes válidas para expoentes naturais continuem válidas, sem exceção, para expoentes inteiros justifica o uso que fizemos aqui dos números racionais. Em verdade, as propriedades (4), (5) e (6) continuam válidas para expoentes *racionais*.

Em primeiro lugar, o que é uma potência racional? Como definiríamos $a^{\frac{m}{n}}$? Se quisermos que (6) continue valendo, como $\frac{m}{n} = m \times \frac{1}{n}$, então $a^{\frac{m}{n}} = (a^{\frac{1}{n}})^m$, e é portanto suficiente sabermos definir $a^{\frac{1}{n}}$.

O que é então $a^{\frac{1}{n}}$? Ora, para que (6) continue valendo, $(a^{\frac{1}{n}})^n = a^{n \cdot \frac{1}{n}} = a^1 = a$, ou seja $a^{\frac{1}{n}}$ é a n-ésima raiz de a!

Definimos portanto $a^{\frac{1}{n}}$ como sendo a n-ésima raiz de a, para a um inteiro *positivo*.

Uma vez feito isso, mostra-se sem problemas que

$$a^{p+q} = a^p \cdot a^q$$

$$(ab)^p = a^p b^p$$

$$(a^p)^q = a^{pq},$$

para $\mathtt{p}$ e $\mathtt{q}$ números racionais quaisquer.

Observe que exigimos, ao lidarmos com potências, que a *base*, o número $\mathtt{a}$, seja sempre positivo. Além disso, não atribuiremos significado à expressão 0^0. Ou seja, 0^0 **não está definido**.

EXERCÍCIOS

7.1. Usando somente os axiomas dos inteiros $(1-6)$, mostre que se $\mathfrak{a}$ e $\mathfrak{b}$ são inteiros tais que $\mathfrak{a} \cdot \mathfrak{b} = 0$, então ou $\mathfrak{a} = 0$ ou $\mathfrak{b} = 0$.

7.2. Na divisão de dois inteiros $\mathfrak{a}$ e $\mathfrak{b}$, o quociente é 16 e o resto 165. Ache o maior inteiro que pode ser somado ao dividendo e ao divisor sem alterar o quociente.

7.3. Uma discoteca tem lâmpadas vermelhas, verdes e amarelas. Todos os dias, às 21 horas, essas lâmpadas são acesas simultaneamente. A partir daí, a cada 45 segundos, as lâmpadas vermelhas são apagadas se estiverem acesas, e são acesas se estiverem apagadas. O mesmo se dá com as lâmpadas verdes a cada 140 segundos e com as amarelas, a cada 36 segundos. Às 21 horas e 50 minutos, que lâmpadas estarão acesas?

7.4. A programação da Rádio MPB é formada por módulos musicais de 17 minutos, intercalados com 6 minutos de anúncios. Todos os dias a programação se inicia à 6 horas, com música. Um incauto ouvinte que sintonizar seu rádio nessa emissora às 21 horas ouvirá ainda quantos minutos de música antes da interrupção para anúncios?

7.5. Dividindo o inteiro $\mathfrak{a}$ pelo inteiro $\mathfrak{b}$, o quociente é 16 e o resto é o maior possível. Ache $\mathfrak{a}$ e $\mathfrak{b}$, sabendo que sua soma é 341.

7.6. Ache os inteiros positivos menores do que 150 e que divididos por 39 deixam resto igual ao quociente.

7.7. Dividem-se 4933 e 4435 por um inteiro positivo $\mathfrak{n}$, obtendo os restos 37 e 19 respectivamente. Ache $\mathfrak{n}$.

7.8. Determine o maior inteiro positivo $\mathfrak{n}$ para o qual são iguais os restos das divisões, por $\mathfrak{n}$, de 1166, 1558 e 2244.

7.9. Determine um inteiro que, dividido por 39, deixa resto 16 e dividido por 56 deixa resto 27.

7.10. Determine dois múltiplos de 7 tais que o resto da divisão de um deles pelo outro seja 39.

7.11. Prove que, para todo inteiro positivo n, existem n inteiros consecutivos, todos compostos.

7.12. Se n é um inteiro positivo, mostre que existe um múltiplo de n que se escreve somente com os algarismos 0 e 1.

7.13. Em um mês de abril com 5 domingos, em que dia da semana cai o dia 23 de abril, dia de São Jorge e aniversário de Pixinguinha, de Shakespeare e de Jorge de Lima?

7.14. Anos bissextos são os divisíveis por 4 mas não por 100 e também os divisíveis por 400. Sabendo que 1º de janeiro de 1993 foi uma sexta-feira, pergunta-se:

a) Qual o próximo ano cujo primeiro de janeiro será também uma sexta-feira?

b) Qual o próximo ano cujo primeiro de janeiro será uma terça feira?

c) Em que dia da semana cairá primeiro de janeiro de 2050?

7.15. Qual é o número máximo de sextas-feiras 13 que pode haver em um ano?

7.16. Dividindo o inteiro a pelo inteiro b ($b > 0$) o quociente é q e o resto é r. Mostre que $q = [a/b]$, onde $[x]$, parte inteira de x, é o maior inteiro que é menor ou igual a x.

7.17. Demonstre as seguintes propriedades da função parte inteira definida no exercício anterior

a) para todo real x, $[x] \leq x < [x] + 1$;

b) $[x + y] \geq [x] + [y]$, para quaisquer reais x e y;

c) $[[x]/n] = [x/n]$, para quaisquer real x e qualquer inteiro n;

d) $[x] + [x + \frac{1}{n}] + \cdots + [x + \frac{(n-1)}{n}] = [nx]$.

7.18. Determine o menor inteiro positivo cujo primeiro algarismo é 1 e que tem a propriedade de se transformar no seu triplo quando o primeiro algarismo é transferido para o último lugar. Que outros inteiros positivos têm essas propriedades?

7.19. Escreva 1993 como uma soma de inteiros positivos cujo produto seja máximo.

APÊNDICE I

O JOGO DE EUCLIDES [19]

São dados dois jogadores e cada um escolhe, secretamente, um número natural não-nulo. Suponhamos que um dos jogadores escolheu o número $\mathtt{a}$ e o outro o número $\mathtt{b}$, com $\mathtt{a} \geq \mathtt{b} > 0$. Um dos jogadores é então sorteado para começar o jogo, e recebe o par (não-ordenado) $\{\mathtt{a}, \mathtt{b}\}$. Ele deverá subtrair do maior número, $\mathtt{a}$, um múltiplo não-nulo do menor, $\mathtt{kb}$, de modo que $\mathtt{a} - \mathtt{kb}$ ainda seja um número natural. O segundo jogador receberá o novo par (não-ordenado) $\{\mathtt{a}-\mathtt{kb}, \mathtt{b}\}$, e repetirá o processo, subtraindo do maior número do par um múltiplo do menor, e assim por diante. Ganhará o jogo quem primeiro obtiver o par $\{\mathtt{n}, 0\}$.

Suponhamos, por exemplo, que os números escolhidos tenham sido 31 e 7. O primeiro jogador terá várias opções de jogo: $\{24, 7\}, \{17, 7\}, \{10, 7\}, \{3, 7\}$. Suponhamos que escolheu $\{10, 7\}$. Neste caso, o segundo jogador só terá uma alternativa: escolher $\{3, 7\}$. Será novamente a vez do primeiro jogador, que poderá agora escolher $\{4, 3\}$ ou $\{1, 3\}$. Se jogar $\{1, 3\}$, o segundo jogador jogará $\{1, 0\}$, e será o vencedor. Se jogar $\{4, 3\}$, o segundo jogador será obrigado a jogar $\{1, 3\}$ e, na jogada seguinte, o primeiro jogador ganhará o jogo.

Não é difícil de ver que o jogo termina com o par $\{\mathtt{n}, 0\}$, onde $\mathtt{n}$ é o m.d.c.$(\mathtt{a}, \mathtt{b})$. De fato, por um raciocínio análogo ao do Teorema 4.3, os divisores comuns de $\mathtt{a}$ e $\mathtt{b}$ são iguais aos divisores comuns de $\mathtt{a}-\mathtt{kb}$ e $\mathtt{b}$. Assim, m.d.c.$(\mathtt{a}, \mathtt{b})$ = m.d.c.$(\mathtt{a}-\mathtt{kb}, \mathtt{b}) = \ldots =$ m.d.c.$(\mathtt{n}, 0) = \mathtt{n}$.

Dado um par $\{\mathtt{a}, \mathtt{b}\}$, com $\mathtt{a} > \mathtt{b}$, os pares $\{\mathtt{a}-\mathtt{b}, \mathtt{b}\}, \ldots, \{\mathtt{a}-\mathtt{qb}, \mathtt{b}\}$, com $\mathtt{a}-\mathtt{qb} \geq 0$, são chamados de *pares derivados* de $\{\mathtt{a}, \mathtt{b}\}$. Assim, $\{24, 7\}$, $\{17, 7\}$, $\{10, 7\}$, $\{3, 7\}$ são os pares derivados de $\{31, 7\}$.

Se $\mathtt{a} - \mathtt{qb} \geq 0$ e $\mathtt{a} - (\mathtt{q}+1)\mathtt{b} < 0$, $\{\mathtt{a} - \mathtt{qb}, \mathtt{b}\}$ chama-se *par derivado mínimo* de $\{\mathtt{a}, \mathtt{b}\}$. No exemplo, $\{3, 7\}$ é o par derivado mínimo de $\{31, 7\}$. Observe que, dentre todos

---

[19] Agradecemos à Revista do Professor de Matemática a permissão para usar este material, que foi publicado, pela primeira vez, como o artigo "O jogo de Euclides", no número 14 (1989), pags. 24-28, por João Bosco Pitombeira.

os pares derivados de um par $\{a, b\}$, com $a > b$, os números do par derivado mínimo são b e o resto da divisão de a por b. Se $\{a - qb, b\}$ for o par derivado mínimo, diremos que o par $\{a - (q-1)b, b\}$ é o *par anterior ao par derivado mínimo*.

Antes de prosseguirmos, observe mais uma vez o exemplo. Dado o par $\{31, 7\}$, o primeiro jogador tem apenas duas opções significativas: ele escolhe o par derivado mínimo $\{3, 7\}$, ou ele escolhe o par anterior ao par derivado mínimo, isto é, $\{10, 7\}$, obrigando o adversário a jogar $\{3, 7\}$. Qualquer outra escolha daria estas mesmas duas opções ao adversário.

Qual das duas é a melhor?

Suponhamos que o primeiro jogador receba o par $\{n, m\}$, com $m < n$. Se $\frac{n}{m}$ for um número inteiro k, o primeiro jogador ganhará o jogo com a jogada $\{n - km, m\}$=$\{0, m\}$.

Suponhamos portanto que $n = qm + r$, com $0 < r < m$.

O jogador deverá optar pelo par derivado mínimo ou pelo par anterior a este, ou seja, deverá optar entre $\{n - qm, m\}$=$\{r, m\}$, com $0 < r < m$, ou $\{n - (q-1)m, m\}$=$\{qm + r - qm + m, m\}$=$\{m + r, m\}$, com $m < m + r$.

Como o adversário prosseguirá subtraindo de m um múltiplo de r ou de $m + r$ um múltiplo de m, estudemos as razões $\frac{m}{r}$ e $\frac{m+r}{m}$. Fazendo $\frac{m}{r} = x$, teremos $\frac{m+r}{m} = 1 + \frac{r}{m} = 1 + \frac{1}{x}$. A pergunta então se tansforma na seguinte: qual das duas razões $x = \frac{m}{r}$ ou $1 + \frac{1}{x} = \frac{m+r}{m}$ é vantajosa para o jogador?

Observemos, inicialmente, que as razões seriam iguais se $x = 1 + \frac{1}{x}$, ou seja, se $x^2 - x - 1 = 0$, ou ainda, dado que $x > 0$, se $x = \frac{1+\sqrt{5}}{2}$. Este número, que representaremos por τ, é aproximadamente igual a $1,618$ e terá um papel importante na discussão do problema.

Cálculos simples mostram que se $x < \tau$, então $1 + \frac{1}{x} > \tau$ e que se $x > \tau$, então $1 + \frac{1}{x} < \tau$.

Podemos então reformular nossa pergunta: o primeiro jogador pode optar entre um par cuja razão é maior do que τ ou um par cuja razão é menor do que τ. Qual sua melhor opção?

Observe que se um jogador receber um par $\{a, b\}$ com $1 < \frac{a}{b} < \tau$, naquela jogada ele não poderá ganhar o jogo e terá como única opção o par $\{a - b, b\}$ com razão $\frac{b}{a-b} > \tau$. De fato, se $1 < \frac{a}{b} < \tau < 2$, então $\frac{a}{b}$ não é inteiro e $a - 2b$ é negativo. Portanto, a única

opção será $\{a - b,\, b\}$, e assim $\frac{b}{a-b} = \frac{1}{(a/b)-1} > \frac{1}{\tau-1} = \tau$. Portanto, é sempre vantajoso para um jogador escolher aquele par cuja razão é menor do que 2 e passá-lo ao adversário. Este, na sua vez, não ganhará o jogo e será obrigado a devolver um par com razão maior do que 2.

Apresentamos agora o fato decisivo: se um jogador receber um par $\{a,\, b\}$ com $\frac{a}{b} > \tau$, ele terá uma estratégia que lhe garantirá a vitória.

Com efeito, se $\frac{a}{b} > 2$, de duas uma, ou a é múltiplo de b e o jogador vencerá naquele lance, ou ele terá duas opções: escolher o par derivado mínimo ou o anterior ao mínimo. Já vimos que ele deve escolher o par com razão menor do que τ, o que impedirá a vitória do adversário no lance seguinte.

Se $\tau < \frac{a}{b} < 2$, o jogador não terá escolha, terá que jogar $\{a-b,\, b\}$. Mas como $a < 2b$, segue-se que $a-b < b$, e portanto $\frac{b}{a-b} = \frac{1}{(a/b)-1} < \frac{1}{\tau-1} = \tau$, e assim, novamente, passará ao adversário um par com razão menor do que τ.

Portanto, o jogador que receber um par $\{a,\, b\}$ com $\frac{a}{b} > \tau$ poderá sempre impedir que seu adversário ganhe o jogo no lance seguinte. Como o jogo é finito, pois os sucessivos pares contêm números naturais cada vez menores, necessariamente haverá uma vez em que o jogador receberá um par $\{a,\, b\}$ com a múltiplo de b, o que lhe dará a vitória.

Resumindo, temos o seguinte: Se o jogo começar com $\{a,\, b\}$, com $a \geq b > 0$, o primeiro jogador terá uma estratégia que lhe garantirá a vitória se e somente se $\frac{a}{b} > \tau$, ou $\frac{a}{b} = 1$. Nos casos restantes, o segundo jogador terá uma estratégia que lhe garantirá a vitória. □

APÊNDICE II

CALENDÁRIO PERMANENTE

O nosso calendário, dito gregoriano, foi adotado, nos países cristãos, em 1582, em substituição ao calendário juliano, durante o papado de Gregório XIII. Nele, os anos têm 365 dias e os anos bissextos têm um dia a mais, o 29 de fevereiro. Os anos bissextos são os múltiplos de 4 que não são múltiplos de 100 e também os múltiplos de 400. Isso é devido ao fato de a Terra efetuar uma revolução em torno do Sol em um tempo um pouco menor do que 365,25 dias. Assim, a cada 4 anos acrescentamos um dia além dos 365 dias usuais. Tal correção é excessiva e, a cada 100 anos, um ano que deveria ser bissexto deixa de sê-lo; por sua vez, essa correção da correção também é excessiva e, a cada 400 anos, um ano que não deveria ser bissexto volta a sê-lo.

Uma fórmula que permite determinar em que dia da semana caiu ou cairá qualquer data posterior a 1582 pode ser obtida do modo que se segue.

Numeremos os meses a partir de março. Assim, março=1, abril=2,..., dezembro=10, janeiro=11 e fevereiro=12. Seja então o ano xyzt. Chamemos de A o número formado pelos dois últimos algarismos do ano, ou seja, $\mathsf{A} = \mathsf{zt}$ e chamemos de C o número formado pelos demais algarismos, isto é, $\mathsf{C} = \mathsf{xy}$. Assim, por exemplo, para o ano de 1947 temos $\mathsf{C} = 19$ e $\mathsf{A} = 47$. É claro que o ano é igual a $100\mathsf{C} + \mathsf{A}$. Defina B como 1 se o ano for bissexto e como 0, caso contrário.

Numeremos agora os dias da semana, pondo sábado=0, domingo=1, segunda-feira=2,..., sexta-feira=6. Provaremos que o dia da semana, em que cai o dia N do mês M do ano $100\mathsf{C} + \mathsf{A}$ satisfaz

$$\mathsf{d} \equiv \mathsf{N} + 1 - 2\mathsf{C} + \mathsf{A} + \lfloor \mathsf{A}/4 \rfloor + \lfloor \mathsf{C}/4 \rfloor \times \lfloor 2,6\mathsf{M} - 0,2 \rfloor - (1 + \mathsf{B}) \times \lfloor \mathsf{M}/11 \rfloor \pmod{\mathfrak{m}}.$$

Assim, por exemplo, para o dia 15 de novembro de 1889 temos C = 18, A = 89, N = 15, M = 9 e B = 0. Daí,

$$\begin{aligned} \mathsf{d} &\equiv 15 + 1 - 36 + 89 + \lfloor 89/4 \rfloor + \lfloor 18/4\times \rfloor \lfloor 2,6 \cdot 9 - 0,2 \rfloor - (1 + 0) \times \lfloor 9/11 \rfloor \\ &\equiv 15 + 1 - 36 + 89 + 22 + 4 + 23 - 0 \equiv 118 \equiv 16 \pmod 7, \end{aligned}$$

e a república foi proclamada em uma sexta-feira.

A demonstração da fórmula será feita em etapas, do modo que se segue:

A) A FÓRMULA PARA O DIA 1º DE MARÇO DO ANO 100 C + A.

Como os anos não-bissextos têm 365 dias e $365 = 7\mathrm{x}52+1$, o 1º de março de $100\mathsf{C}+\mathsf{A}$ cai um dia da semana após o dia da semana em que caiu o 1º de março do ano anterior, a não ser que $100\mathsf{C}+\mathsf{A}$ seja bissexto, caso em que cairá dois dias após o 1º de março do ano anterior. Seja d_{1600} o dia da semana em que caiu o 1º de março de 1600. Se não existissem anos bissextos, o 1º de março de $100\mathsf{C}+\mathsf{A}$ cairia $100\mathsf{C}+\mathsf{A}-1600$ dias após d_{1600}. Havendo x anos bissextos entre 1600 (exclusive) e $100\mathsf{C}+\mathsf{A}$ (inclusive), ele cairá $100\mathsf{C}+\mathsf{A}-1600+\mathrm{x}$ dias após d_{1600} e teremos $\mathsf{d} \equiv 100\mathsf{C}+\mathsf{A}-1600+\mathrm{x} \pmod 7$.

Calculemos x, o número de anos bissextos entre $1600 e 100\mathsf{C}+\mathsf{A}$. Temos

$\mathrm{x} = \lfloor(100\mathsf{C}+\mathsf{A}-1600)/4\rfloor - \lfloor(100\mathsf{C}+\mathsf{A}-1600)/100\rfloor + \lfloor(100\mathsf{C}+\mathsf{A}-1600)/400\rfloor$.

Lembrando que $\lfloor z+\mathrm{n}\rfloor = \lfloor z\rfloor + \mathrm{n}$, se n é inteiro, obtemos

$$\begin{aligned}\mathrm{x} &= \lfloor 25\mathsf{C}+(\mathsf{A}/4)-400\rfloor - \lfloor \mathsf{C}+(\mathsf{A}/100)-16\rfloor + \lfloor(\mathsf{C}/4)+(\mathsf{A}/400)-4\rfloor \\ &= 25\mathsf{C}+\lfloor\mathsf{A}/4\rfloor - 400 - \mathsf{C} - \lfloor\mathsf{A}/100\rfloor + 16 + \lfloor\mathsf{C}/4\rfloor + \lfloor\mathsf{A}/400\rfloor - 4 \\ &= 24\mathsf{C} - 388 + \lfloor\mathsf{A}/4\rfloor + \lfloor\mathsf{C}/4\rfloor - \lfloor\mathsf{A}/100\rfloor + \lfloor\mathsf{A}/400\rfloor.\end{aligned}$$

Como $0 \le \mathsf{A} \le 99$, temos $\lfloor\mathsf{A}/100\rfloor + \lfloor\mathsf{A}/400\rfloor = 0$. Daí, $\mathrm{x} = 24\mathsf{C} - 388 + \lfloor\mathsf{A}/4\rfloor + \lfloor\mathsf{C}/4\rfloor$.

Logo, o dia da semana, em que cai o dia 1º de março do ano 100 C + A, satisfaz, módulo 7,

$$\begin{aligned}\mathsf{d} &\equiv \mathsf{d}_{1600} + 100\mathsf{C}+\mathsf{A}-1600+24\mathsf{C}-388+\lfloor\mathsf{A}/4\rfloor \times \lfloor\mathsf{C}/4\rfloor \\ &\equiv \mathsf{d}_{1600} + 124\mathsf{C}+\mathsf{A}-1988+\lfloor\mathsf{A}/4\rfloor+\lfloor\mathsf{C}/4\rfloor \\ &\equiv \mathsf{d}_{1600} - 2\mathsf{C}+\mathsf{A}+\lfloor\mathsf{A}/4\rfloor+\lfloor\mathsf{C}/4\rfloor,\end{aligned}$$

pois $24 \equiv -2$ e $1988 \equiv 0 \pmod 7$.

B) A FÓRMULA PARA O DIA 1º DO MÊS M DO ANO 100 C + A.

Como março tem 31 dias, o 1º de abril cairá 3 dias após o dia da semana em que caiu o 1º de março. Analogamente, como abril tem 30 dias, o 1º de maio cairá 2 dias após o 1º de abril, 5 dias após o 1º de março, etc...

Portanto, para aplicar a fórmula para o 1º de abril, basta somar 3 ao segundo membro; para maio, somar 5, etc... Para fevereiro, se o ano não é bissexto, a correção é $0 \equiv 28 \pmod 7$, e se for bissexto, a correção será $-1 \equiv 27 \pmod 7$. Para janeiro, as correções são $-3 \equiv 125$ e $-4 \equiv 24$.

A tabela a seguir mostra as correções que devem ser somadas ao segundo membro da fórmula, no caso de ano não-bissexto, bem como os valores de $\lfloor 2,6\mathsf{M} - 2,2 \rfloor$.

MÊS	M	CORREÇÃO	$\lfloor 2,6\mathsf{M} - 2,2 \rfloor$
MARÇO	1	0	0
ABRIL	2	3	3
MAIO	3	5	5
JUNHO	4	8	8
JULHO	5	10	10
AGOSTO	6	13	13
SETEMBRO	7	16	16
OUTUBRO	8	18	18
NOVEMBRO	9	21	21
DEZEMBRO	10	23	23
JANEIRO	11	25	26
FEVEREIRO	12	28	29

Observe que a correção é igual a $\lfloor 2,6\mathsf{M} - 2,2 \rfloor$ exceto para os meses de janeiro e fevereiro, casos em que ainda devemos subtrair 1. Ora, $\lfloor \mathsf{M}/11 \rfloor$ é igual a 1 para os meses de janeiro e fevereiro e é igual a 0 para os demais meses. Então, a correção para o mês M de um ano não-bissexto é igual a $\lfloor 2,6\mathsf{M} - 2,2 \rfloor - \lfloor \mathsf{M}/11 \rfloor$.

Para anos bissextos, devemos ainda subtrair mais uma unidade para os meses de janeiro e fevereiro. Para isso, basta subtrair do segundo membro da fórmula $\mathsf{B} \times \lfloor \mathsf{M}/11 \rfloor$.

Então, a fórmula para o dia 1º do mês M é $\mathsf{d} \equiv \mathsf{d}_{1600} - 2\mathsf{C} + \mathsf{A} + \lfloor \mathsf{A}/4 \rfloor + \lfloor \mathsf{C}/4 \rfloor + \lfloor 2,6\mathsf{M} - 2,2 \rfloor - (1 + \mathsf{B}) \times \lfloor \mathsf{M}/11 \rfloor \pmod 7$. (mod 7).

C) A FÓRMULA PARA O DIA N DO MÊS M DO ANO 100 C + A.

Evidentemente, agora basta somar N-1 ao segundo membro. Obtemos

$$\mathsf{d} \equiv \mathsf{d}_{1600} - 2\mathsf{C} + \mathsf{A} + \lfloor \mathsf{A}/4 \rfloor + \lfloor \mathsf{C}/4 \rfloor + \lfloor 2,6\mathsf{M} - 0,2 - 2 \rfloor + (1 + \mathsf{B})\mathsf{M}/11 + \mathsf{N} - 1.$$

Para determinar d_{1600}, olhamos a folhinha e vemos que hoje, 15 de novembro de 1993 é segunda-feira. Logo, temos d = 2, C = 19, A = 93, M = 9, B = 0 e N = 15. Daí,

$$2 \equiv \mathsf{d}_{1600} - 38 + 93 + 23 + 4 + 23 - 2 + 0 + 15 - 1 \pmod 7.$$

Portanto, $\mathsf{d}_{1600} \equiv -115 \equiv 4 \pmod 7$.

PROBLEMAS

1) Em que dia da semana caiu:

a) 21 de abril de 1792? (sábado)

b) 13 de maio de 1888? (domingo)

c) 7 de setembro de 1822? (sábado)

d) 29 de setembro de 1992? (terça)

2) Em que dia da semana cairá:

a) 1 de janeiro de 2001? (segunda)

b) 29 de fevereiro de 2400? (terça)

3) Há muitos anos atrás comecei a colecionar calendários. Passados muitos anos, observei que os calendários se repetiam e que minha coleção já estava completa. Joguei fora, então, as duplicatas. Com quantos calendários ficou minha coleção? (14)

4) Salvador começou a colecionar calendários em 1975, guardando a cada ano o calendário do ano. Hoje, sua coleção já tem várias duplicatas (por exemplo, o calendário de 1975 é igual ao de 1986), mas ainda não está completa. Em que ano Salvador completará sua coleção? (2000)

5) Qual o próximo ano no qual o Natal será domingo? (2005)

6) Prove que, se z é real e n é inteiro, então $\lfloor z + \mathfrak{n} \rfloor = \lfloor z \rfloor + \mathfrak{n}$.

APÊNDICE III

O TEOREMA DE LAMÉ [20]

Relembremos o algoritmo de Euclides, já demonstrado (Teorema XXXX): Dados dois inteiros $\mathfrak{a}$ e $\mathfrak{b}$ não nulos, aplicando sucessivamente o algoritmo da divisão, temos:

$$\mathfrak{a} = \mathfrak{b}q_1 + \mathfrak{b}_1, \quad 0 < \mathfrak{b}_1 < \mathfrak{b},$$

$$\mathfrak{b} = \mathfrak{b}_1 q_2 + \mathfrak{b}_2, \quad 0 < \mathfrak{b}_2 < \mathfrak{b}_1,$$

$$\mathfrak{b}_1 = \mathfrak{b}_2 q_3 + \mathfrak{b}_3, \quad 0 < \mathfrak{b}_3 < \mathfrak{b}_2,$$

$$\ldots$$

$$\mathfrak{b}_{n-2} = \mathfrak{b}_{n-1} q_n + \mathfrak{b}_n, \quad 0 < \mathfrak{b}_n < \mathfrak{b}_{n-1},$$

$$\mathfrak{b}_{n-1} = \mathfrak{b}_n q_{n+1}.$$

Então m.d.c.$(\mathfrak{a}, \mathfrak{b}) = \mathfrak{b}_n$.

Usando o algoritmo de Euclides, são necessárias $n + 1$ divisões para vermos que m.d.c.$(\mathfrak{a}, \mathfrak{b}) = \mathfrak{b}_n$, pois só chegamos a uma conclusão quando verificarmos que $\mathfrak{b}_{n-1} = \mathfrak{b}_n q_{n+1} + \mathfrak{b}_{n+1} = \mathfrak{b}_n q_{n+1} + 0 = \mathfrak{b}_n q_{n+1}$.

Chamaremos de *Comprimento* do algoritmo de Euclides o número de divisões necessárias para calcular o m.d.c.$(\mathfrak{a}, \mathfrak{b})$. Usando a notação do algoritmo, seu comprimento é $n + 1$.

O algoritmo de Euclides é bem eficiente. Por exemplo, se quisermos verificar que m.d.c.$(97, 24) = 1$ são necessários apenas dois passos:

$$97 = 4 \times 24 + 1$$

$$24 = 24 \times 1.$$

Agora, se quisermos calcular m.d.c.$(21479, 24)$, temos

$$21479 = 894 \times 24 + 23,$$

$$24 = 1 \times 23 + 1,$$

$$23 = 1 \times 23.$$

[20] Agradecemos à redação da Revista do Professor de Matemática a permissão para usar este material, que foi originalmente publicado, na revista, como "Euclides, Fibonacci e Lamé", número 23 (1993), por João Bosco Pitombeira.

Ou seja, em 3 passos vemos que m.d.c.(21479, 24) = 1. Por fim, como último exemplo, para calcular m.d.c.(49745692, 24), temos

$$49745692 = 2072737 \times 24 + 4,$$

$$24 = 6 \times 4;$$

isto é, em apenas 2 passos chegamos ao resultado desejado.

Dados dois números inteiros e positivos $\mathtt{a}$ e $\mathtt{b}$, uma pergunta natural é a de saber qual o comprimento do algoritmo de Euclides aplicado a eles. Em outras palavras, quantas divisões são necessárias para calcular o máximo divisor comum de $\mathtt{a}$ e de $\mathtt{b}$.

É imediato verificar que se mantivermos $\mathtt{b}$ fixo, mesmo que $\mathtt{a}$ seja muito grande em relação a $\mathtt{b}$, o número de divisões no algoritmo de Euclides não pode crescer. Em verdade, este número depende apenas de $\mathtt{b}$.

Teorema: *Suponha que* $\mathtt{a}$ *e* $\mathtt{b}$ *são inteiros positivos, com* $\mathtt{a} \geq \mathtt{b}$. *Então, o comprimento do algoritmo de Euclides para achar* m.d.c.($\mathtt{a}$, $\mathtt{b}$) *depende somente de* $\mathtt{b}$ *e é no máximo igual a* $\mathtt{b}$.

Com efeito, usando mais uma vez a notação do Teorema 1, sabemos que, no algoritmo, m.d.c.($\mathtt{a}$, $\mathtt{b}$) = $\mathtt{b}_\mathtt{n}$ e que $0 < \mathtt{b}_\mathtt{n} < \mathtt{b}_{\mathtt{n}-1} < \cdots < \mathtt{b}_1 < \mathtt{b}$. Como há no máximo $\mathtt{b} - 1$ inteiros distintos não-negativos entre 0 e $\mathtt{b}$, vemos que $\mathtt{n} < \mathtt{b} - 1$, donde $\mathtt{n} + 1 \leq \mathtt{b}$. Ora, como já vimos, são necessárias $\mathtt{n} + 1$ divisões para determinar o máximo divisor comum. Assim, são necessárias no máximo $\mathtt{b}$ divisões para achar m.d.c.($\mathtt{a}$, $\mathtt{b}$).

No entanto, este resultado não é muito bom. Por exemplo, se $\mathtt{b} = 99$, devemos ter que $\mathtt{n} + 1 \leq 99$ e chegamos à conclusão de que talvez tenhamos que efetuar 99 divisões para calcular o máximo divisor comum!

O Teorema de Lamé melhora muito esta situação:

Teorema: (*Lamé*) *Sejam* $\mathtt{a}$ *e* $\mathtt{b}$ *inteiros positivos. Então, o comprimento do algoritmo de Euclides aplicado a* $\mathtt{a}$ *e a* $\mathtt{b}$ *é menor ou igual a* 5 *vezes o número de dígitos na representação decimal de* $\mathtt{b}$.

Segundo o teorema, se $\mathtt{b}$ é igual a 99, então o número de divisões no algoritmo de Euclides é no máximo 10, não sendo influenciado por $\mathtt{a}$. Isso representa um progresso notável em relação à estimativa anterior.

Este teorema é devido a Lamé [21]. Embora não tenha se dedicado sistematicamente à teoria dos números, ele deixou algumas jóias sobre o assuunto, uma das quais é o teorema acima.

A demonstração do Teorema de Lamé é um exemplo de utilização inteligente dos números de Fibonacci.

Como sabemos, estes números foram introduzidos por Leonardo de Pisa (1170?, 1250), também chamado de Fibonacci, em seu livro "Liber Abbaci", de 1202, onde encontramos, como um exercício sobre multiplicação, o famoso "problema dos coelhos": Começando com um casal de coelhos, supondo que nenhum coelho morre, que cada casal gera um novo casal por mês, e que um casal de coelhos começa a ter filhotes com um mês de idade, quantos casais de coelhos teremos após 12 meses?

É fácil ver que a solução do problema é dada pela sequência

$$1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233,$$

em que cada termo dá o número de coelhos no primeiro, segundo, ..., décimo segundo mês.

A lei de formação dos termos desta sequência é

$$f_n = f_{n-1} + f_{n-2}$$

e ela tem se revelado muito importante, atualmente, no estudo dos algoritmos usados em computação (teórica ou prática).

Embora isso não seja muito conhecido, em 1611 Johann Kepler (1571-1630) também considerou a mesma sequência, ao estudar a disposição de folhas e flores nas plantas ("filotaxia").

A primeira aplicação dos números de Fibonacci ao estudo dos algoritmos foi dada por Lamé, em 1844, no teorema enunciado acima. Em verdade, esta foi a primeira aplicação "significativa" destes números.

---

[21] Gabriel Lamé (1795-1870), engenheiro e matemático francês, conhecido por seus trabalhos sobre a equação do calor e criador das coordenadas curvilíneas.

Para efetuarmos a demonstração, voltemos ao algoritmo de Euclides. Em primeiro lugar, $b_n \geq 1$, pois b_n é um número inteiro. De $b_{n-1} = b_n q_{n+1}$, vemos que $b_{n-1} \geq 2$, pois $b_{n-1} > b_n$. Assim, $b_n \geq f_1$ e $b_{n-1} \geq f_2$. Então,

$$b_{n-2} = b_{n-1} q_n + b_n \geq f_2 + f_1 = f_3,$$

pois $q_n \geq 1$. Analogamente, de

$$b_{n-3} = b_{n-2} q_{n-1} + b_{n-1},$$

obtemos, pois $q_{n-1} \geq 1$,

$$b_{n-3} \geq f_3 + f_2 = f_4.$$

Continuando desta maneira, vemos, de maneira geral, que

$$b_{n-k} \geq f_{k+1} \quad \text{para} \quad k = 0, 1, 2, \ldots, n-1,$$

e enfim, de $b \geq b_1 + b_2$, vem que

$$b \geq f_n + f_{n-1} = f_{n+1},$$

ou seja, fazendo $b_0 = b$, temos que

$$b_{n-k} \geq f_{k+1}, \quad \text{para} \quad k = 0, 1, 2, \ldots, n.$$

Este resultado nos mostra que o comprimento do algoritmo de Euclides é **menor ou igual ao número de ordem do maior número de Fibonacci menor ou igual a** b.

Podemos ver que este resultado é o melhor possível achando o máximo divisor comum entre dois números de Fibonacci consecutivos. Calculemos, por exemplo m.d.c.(21, 13) = m.d.c.(f_7, f_6):

$$21 = 13 + 8$$

$$13 = 8 + 5$$

$$8 = 5 + 3$$

$$5 = 3 + 2$$

$$3 = 2 + 1$$

$$2 = 1 \times 2 + 0.$$

Neste exemplo, f_7 e f_6 não desempenham nenhum papel essencial; ele funciona igualmente no caso geral, para achar m.d.c.(f_{n+1}, f_n).

Consideremos agora a raíz positiva de $x^2 - x - 1 = 0$, que é $\alpha = (1 + \sqrt{5})/2$. Temos então que

$$\alpha^2 = \alpha + 1 < 2 + 1 \leq f_2 + f_1 = f_3.$$

Mas

$$\alpha^3 = \alpha^2 + \alpha < f_3 + 2 \leq f_3 + f_2 = f_4,$$

$$\alpha^4 = \alpha^3 + \alpha^2 \leq f_4 + f_3 = f_5,$$

e assim sucessivamente, chegando enfim a

$$\alpha^j < f_{j+1} \leq b, \quad j = 2, 3, 4, \ldots$$

Em particular,

$$\alpha^n < b.$$

Como a função $\log_{10} x$ é estritamente crescente, temos que

$$n \log_{10} \alpha < \log_{10} b,$$

ou, equivalentemente,

$$n < \frac{\log_{10} b}{\log_{10} \alpha}.$$

Ora, calcula-se facilmente, usando uma tábua de logaritmos ou uma máquina de calcular, que $\log_{10} \alpha = \log_{10} \frac{(1+\sqrt{5})}{2} = 0,20898 > 0,20 = \frac{1}{5}$; ou seja, $\frac{1}{\log_{10}} < 5$. Assim

$$n < \frac{\log_{10} b}{\log_{10} \alpha} < 5 \times \log_{10} b.$$

Se o número de algarismos na representação decimal de b é s, então

$$b = t_{s-1} 10^{s-1} + t_{s-2} 10^{s-2} + \cdots + t_1 10 + t_0,$$

e portanto $b < 10^s$, donde $\log_{10} b < s$, e vemos que $n < 5s$. Como n é um inteiro estritamente menor do que $5s$, temos que $n + 1 \leq 5s$, o resultado procurado.

APÊNDICE IV

AS SOLUÇÕES INTEIRAS E POSITIVAS DA EQUAÇÃO $x^2 + y^2 = z^2$

A equação $x^2 + y^2 = z^2$ é homogênea, isto é, todos os seus termos têm o mesmo grau. Isso implica que, se (x_0, y_0, z_0) é uma solução inteira e positiva, então (tx_0, ty_0, tz_0) também é solução inteira e positiva, qualquer que seja t inteiro e positivo. Reciprocamente, se (x_0, y_0, z_0) é solução inteira e positiva e t é um inteiro positivo que divide x_0, y_0 e z_0, então $(x_0/t, y_0/t, z_0/t)$ também é solução inteira e positiva.

Basta, portanto, concentrar nossa atenção nas soluções (x_0, y_0, z_0) tais que o máximo divisor comum de x_0, y_0 e z_0 seja igual a 1. Tais soluções são ditas *primitivas*.

Além disso, se (x, y, z) é solução primitiva, então x e y não podem ser ambos pares, pois isso acarretaria z também par e a solução não seria primitiva. Por outro lado, x e y não podem ser ambos ímpares, pois se x e y fossem ímpares, teríamos $x \equiv \pm 1$ e $y \equiv \pm 1 \pmod 4$; daí, $z^2 = x^2 + y^2 = 1 + 1 \equiv 2 \pmod 4$, o que é absurdo pois nenhum quadrado é côngruo a 2, módulo 4.

Portanto, basta considerar as soluções primitivas nas quais x é par e y é ímpar, as demais soluções primitivas sendo obtidas pela troca de x com y. É claro que, nessas soluções, z é ímpar.

Teorema: *Se a e b são inteiros positivos, primos entre si e de paridades diferentes, com* $a > b$, *então* $x = 2ab, y = a^2 - b^2, z = a^2 + b^2$ *é solução primitiva de* $x^2 + y^2 = z^2$, *com* x *par e* y *ímpar.*

Demonstração: Temos que

$$x^2 + y^2 = (2ab)^2 + (a^2 - b^2)^2 = 4a^2b^2 + a^4 - 2a^2b^2 + b^4 = (a^2 + b^2)^2 = z^2.$$

Como a e b têm paridades diferentes, y é ímpar. Além disso, como $x = 2ab$, x é par. Se d é um primo que divide x e y, $d \neq 2$, pois y é ímpar. Como d divide x e não divide 2, d divide a ou d divide b. Como d divide também $a^2 - b^2$, d divide a e d divide b. Como a e b são primos entre si, $d = 1$ e a solução é primitiva.

Teorema recíproco: *Se* x, y, z *são inteiros positivos primos entre si tais que* $x^2 + y^2 = z^2$, *com* x *par, então existem inteiros positivos*a *e* b, $a > b$, *primos entre si e de paridades diferentes, tais que* $x = 2ab$, $y = a^2 - b^2$, $z = a^2 + b^2$.

Demonstração: Já sabemos que $\mathtt{y}$, e $\mathtt{z}$, são ímpares, o que acarreta $\mathtt{z}-\mathtt{y}$ e $\mathtt{z}+\mathtt{y}$ pares. Daí,

$$[\frac{\mathtt{x}}{2}]^2 = \frac{\mathtt{z}^2-\mathtt{y}^2}{4} = \frac{\mathtt{z}+\mathtt{y}}{2}\cdot\frac{\mathtt{z}-\mathtt{y}}{2}.$$

Seja $\mathtt{d}$ o máximo divisor comum de $\frac{\mathtt{z}+\mathtt{y}}{2}$ e $\frac{\mathtt{z}-\mathtt{y}}{2}$. Então, $\mathtt{d}$ divide $\frac{\mathtt{z}+\mathtt{y}}{2}+\frac{\mathtt{z}-\mathtt{y}}{2}=\mathtt{z}$ e $\mathtt{d}$ divide $\frac{\mathtt{z}+\mathtt{y}}{2}-\frac{\mathtt{z}-\mathtt{y}}{2}=\mathtt{y}$. Como $\mathtt{z}$ e $\mathtt{y}$ são primos entre si, $\mathtt{d}=1$, isto é, $\frac{\mathtt{z}+\mathtt{y}}{2}$ e $\frac{\mathtt{z}-\mathtt{y}}{2}$ também são primos entre si. Mas, se $\frac{\mathtt{z}+\mathtt{y}}{2}$ e $\frac{\mathtt{z}-\mathtt{y}}{2}$ são primos entre si e o produto deles é um quadrado perfeito, cada um deles é também um quadrado perfeito, ou seja, existem inteiros positivos $\mathtt{a}$ e $\mathtt{b}$ tais que $\frac{\mathtt{z}+\mathtt{y}}{2}=\mathtt{a}^2$ e $\frac{\mathtt{z}-\mathtt{y}}{2}=\mathtt{b}^2$.

É claro que $\mathtt{z}=\mathtt{a}^2+\mathtt{b}^2$, $\mathtt{y}=\mathtt{a}^2-\mathtt{b}^2$, $\mathtt{x}=2\mathtt{a}\mathtt{b}$, $\mathtt{a}>\mathtt{b}$, $\mathtt{a}$ e $\mathtt{b}$ têm paridades diferentes (pois $\mathtt{y}$ é ímpar) e $\mathrm{mdc}(\mathtt{a},\mathtt{b})=1$, pois $\mathtt{a}^2$ e $\mathtt{b}^2$ são primos entre si.

As soluções inteiras e positivas de $\mathtt{x}^2+\mathtt{y}^2=\mathtt{z}^2$ são chamadas de ternas pitagóricas, pois são os lados de um triângulo retângulo de lados inteiros.

O quadro abaixo mostra todas as ternas pitagóricas primitivas com a e b menores que 7.

a	b	x	y	z
2	1	4	3	5
4	1	8	15	17
6	1	12	35	37
3	2	12	13	25
5	2	20	21	29
4	3	24	7	25
5	4	40	9	41
6	5	60	11	61

PROBLEMAS

1) Prove que em toda terna pitagórica um dos catetos é múltiplo de 3 e um dos lados é múltiplo de 5.

2) Determine todas as ternas pitagóricas que constituem uma progresssão geométrica ou uma progresssão aritmética.

3) Mostre que, em todo triângulo retângulo de lados inteiros, o raio do círculo inscrito é inteiro e a área é um múltiplo de 6.

4) Prove que, se a e b são primos entre si e ab é um quadrado perfeito, então a e b são quadrados perfeitos.

5) Prove que não há ternas pitagóricas nas quais os catetos sejam iguais.

6) Determine todas as ternas pitagóricas nas quais um dos elementos é igual a 12.

7) Prove que, se n é um inteiro e $n \geq 3$, existe alguma terna pitagórica à qual n pertence.

8) Determine todas as soluções inteiras e positivas de $x^2 + y^2 = z^4$.

9) Considere as soluções inteiras e positivas da equação $x^2 + 2y^2 = z^2$, nas quais mdc(x,y,z) = 1.

a) Prove que y deve ser par.

b) Prove que x e z devem ser ímpares.

c) Determine todas as soluções.

APÊNDICE V

O BINÔMIO DE NEWTON

Teorema: *Para quaisquer números reais* a *e* b*, e qualquer número inteiro positivo* n*, tem-se*

$$(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^{n-j} b^j.$$

Este resultado é geralmente conhecido como *Binômio de Newton* [22].

Demonstração: Usaremos indução sobre n, o expoente de $(a+b)^n$.

1- Se $n = 1$, então $(a+b)^1 = \sum_{j=0}^{1} \binom{1}{j} a^{1-j} b^j = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = a + b$, visto que $\binom{1}{0} = \binom{1}{1} = 1$, $a^0 = b^0 = 1$.

Assim, o resultado é válido para o inteiro 1.

2- Aceitemos agora que, se k é um inteiro maior ou igual a 1,

$$(a+b)^k = \sum_{j=0}^{k} \binom{k}{j} a^{k-j} b^j =$$

$$= \binom{k}{0} a^k b^0 + \binom{k}{1} a^{k-1} b^1 + \binom{k}{2} a^{k-2} b^2 + \cdots + \binom{k}{k} a^0 b^k.$$

Desejamos mostrar que

$$(a+b)^{k+1} = \sum_{j=0}^{k+1} \binom{k+1}{j} a^{k+1-j} b^j.$$

Ora,

$$(a+b)^{k+1} = (a+b)^k (a+b) =$$

$$= \Big[\sum_{j=0}^{k} \binom{k}{j} a^{k-j} b^j\Big](a+b) =$$

$$= \sum_{j=0}^{k} \binom{k}{j} a^{k-j+1} b^j + \sum_{j=0}^{k} \binom{k}{j} a^{k-j} b^{j+1} =$$

---

[22] Em verdade, este resultado é muito anterior a Newton, pois era conhecido na China, em torno de 1300 d. C. Mais tarde, no Ocidente, em torno de 1540, Michael Stifel, alemão, (1487?, 1567) certamente conhecia a fórmula do binômio. Newton estendeu esta fórmula para o caso de n fracionário, o qual é muito mais difícil, pois o segundo membro torna-se então uma série infinita. Daí o seu nome.

$$= \binom{k}{0} a^k b^1 + \binom{k}{1} a^{k-1} b^2 + \binom{k}{2} a^{k-2} b^3 + \cdots + \binom{k}{k-1} a^1 b^k + \binom{k}{k} a^0 b^{k+1} +$$
$$+ \binom{k}{0} a^{k+1} b^0 + \binom{k}{1} a^k b^1 + \binom{k}{2} a^{k-1} b^2 + \cdots + \binom{k}{k-1} a^2 b^{k-1} + \binom{k}{k} a^1 b^k =$$
$$= \binom{k}{0} a^{k+1} b^0 + \left[\binom{k}{0} + \binom{k}{1}\right] a^k b^1 + \cdots + \left[\binom{k}{k+1} + \binom{k}{k}\right] a^1 b^k + \binom{k}{k} a^0 b^{k+1}.$$

É bem conhecido que

$$\binom{k}{j} + \binom{k}{j+1} = \binom{k+1}{j+1},$$

donde,

$$(a+b)^{k+1} = \binom{k}{0} a^{k+1} b^0 + \binom{k+1}{1} a^k b^1 +$$
$$+ \binom{k+1}{2} a^{k-1} b^2 + \cdots + \binom{k+1}{k} a^k b^1 + \binom{k}{k} a^0 b^{k+1}.$$

Mas

$$\binom{k}{0} = \binom{k+1}{0} = 1$$

e

$$\binom{k}{k} = \binom{k+1}{k+1} = 1,$$

logo

$$(a+b)^{k+1} = \binom{k+1}{0} a^{k+1} b^0 + \binom{k+1}{1} a^k b^1 + \cdots + \binom{k+1}{k} a^1 b^k + \binom{k+1}{k+1} a^0 b^{k+1},$$

ou ainda,

$$(a+b)^{k+1} = \sum_{j=0}^{k+1} \binom{k+1}{j} a^{k+1-j} b^j,$$

como queríamos demonstrar.

Ou seja, mostramos que se

$$(a+b)^k = \sum_{j=0}^{k} \binom{k}{j} a^{k-j} b^j,$$

então

$$(a+b)^{k+1} = \sum_{j=0}^{k+1} \binom{k+1}{j} a^{k+1-j} b^j.$$

Podemos assim afirmar, pelo princípio da indução finita, que

$$(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^{n-j} b^j,$$

para qualquer inteiro positivo n. □