Elementos da Teoria dos Números

Mauri Cunha do Nascimento
Hércules de Araujo Feitosa

2013

Sumário

Introdução

O interesse pelos números e suas propriedades acompanham o desenvolvimento das mais diversas civilizações de que temos informações, desde os momentos iniciais de seus desenvolvimentos. Na obra "Os Elementos", de Euclides (360 a.C. - 295 a.C.), já aparecem os conceitos de números pares, ímpares, primos e compostos. Como a Matemática grega era essencialmente geométrica, os números eram representados por segmentos de retas. O Livro VII de "Os Elementos" inicia com a regra para a determinação do máximo divisor comum de dois números. Vários outros resultados aparecem nestes livros, inclusive a demonstração da existência de uma quantidade infinita de números primos.

Talvez, o mais ilustre matemático amador tenha sido Pierre de Fermat (1601-1665), que é considerado o fundador da moderna teoria dos números. Fermat estudou direito em Toulouse, onde trabalhou como advogado e conselheiro do parlamento local. Seu mais famoso enunciado, conhecido como o "Último Teorema de Fermat", só foi demonstrado recentemente, em 1995, por Andrew Wiles. O enunciado desse teorema afirma que não existem números inteiros não nulos, a, b, c tais que $a^n + b^n = c^n$, para $n > 2$. Fermat escreveu na margem de um livro que tinha uma demonstração simples para esta afirmação, mas que o espaço da margem era insuficiente para escrevê-la. Provavelmente, a prova que Fermat dispunha não estaria correta, dado que este problema ficou longo período sem resposta. Entretanto, graças às tentativas de resolvê-lo, muitos elementos teóricos da Matemática foram desenvolvidos.

Números da forma $2^{2^n} + 1$ ficaram conhecidos como números de Fermat, pois Fermat conjecturou que tais números

seriam sempre primos, depois de ter verificado que o resultado era válido para $n = 0, 1, 2, 3, 4$. Um século depois, Leonhard Euler (1707-1783) mostrou que para $n = 5$, a conjectura não valia, pois $2^{2^5} + 1 = 4.294.967.297 = 641 \cdot 6.700.417$. Não sabemos até o momento se existe algum número $n > 5$ tal que $2^{2^n} + 1$ é um número primo. Fermat demonstrou resultados interessantes, como o teorema que diz que 'um número primo p é soma de dois quadrados se, e somente se, $p = 2$' ou 'se o resto da divisão de p por 4 é igual a 1. Por exemplo, $5 = 2^2 + 1^2, 13 = 3^2 + 2^2$, porém 3, 7 e 11 não se escrevem como soma de dois quadrados. Existem inúmeras conjecturas que envolvem os números inteiros, muitas delas com enunciados bastante simples, como por exemplo, a que afirma que 'todo número par maior que 2 é soma de dois números primos', enunciada por Christian Goldbach (1690-1764), a qual permanece um problema aberto e intrigante.

Estes Elementos da Teoria dos Números são constituídos da seguinte maneira.

No Capítulo 1 apresentamos as noções de conjuntos, relações e funções, de modo breve, apenas como suporte para resultados usados em momentos posteriores. Algo semelhante ocorre no Capítulo 2, em que apresentamos as propriedades dos números inteiros. É usual o tratamento da teoria dos números sobre os inteiros, embora também possa ser arquitetada sobre os números naturais. O Capítulo 3 inicia propriamente a teoria, quando são introduzidos os princípios de indução em duas versões e são mostradas as equivalências dessas duas versões com o princípio da boa ordem dos números naturais.

O Capítulo 4 define o conceito de divisão de inteiros e introduz o famoso algoritmo da divisão de Euclides. No capítulo seguinte, investigamos as bases de numeração. Embora tradicio-

nalmente usamos a base dez, isto não foi sempre unânime nas civilizações passadas. Também o advento das linguagens artificiais e a teoria da computação mostrou o interesse em aplicações de outras bases, particularmente, a base dois. No Capítulo 6 tratamos dos critérios de divisibilidade, ou mais especificamente, procuramos mostrar algumas características que um dado número deve ter para, ao ser dividido por um outro número, dar resto zero.

As lições escolares tradicionais de estabelecer o máximo divisor comum e o mínimo múltiplo comum são justificadas no Capítulo 7. O capítulo seguinte é destinado aos famosos primos, que comparecem como fatores em todos os números inteiros positivos maiores ou iguais a dois. Esta afirmação pode e deve ser estendida para todos os inteiros, incluindo aí os negativos. O Capítulo 9 desenvolve as congruências e uma pequena álgebra sobre classes de números. O capítulo seguinte traz as equações diofantinas lineares, uma parte das equações que estiveram nos interesses do matemático grego antigo Diofanto. No Capítulo 11 discorremos sobre as ternas pitagóricas com o intuito de apresentar o famoso Último Teorema de Fermat e algumas contribuições em torno do teorema. O penúltimo capítulo mostra os números quadrados e triangulares, que têm motivação visual e geométrica. Finalmente, no último capítulo apresentamos algumas particularidades e curiosidades sobre números.

1 Conjuntos, relações e funções

Nesse capítulo apresentamos algumas noções gerais, mas fundamentais para desenvolvimentos posteriores, sobre conjuntos, relações entre conjuntos, particularmente as relações de equivalência e de ordem. Mais detalhes sobre os elementos teóricos desenvolvidos neste ínterim podem ser encontrados em (Feitosa, Paulovich, 2005) e (Feitosa, Nascimento, Alfonso, 2008).

1.1 A noção de conjunto

O ponto de partida para a elaboração de uma teoria é dado pela introdução dos seus conceitos primitivos, que são conceitos não definidos.

Assim, para esses elementos de Teoria dos Conjuntos, não apresentamos definições para os conceitos de conjunto, elemento e relação de pertinência.

A idéia intuitiva de conjunto é a de coleção, classe de objetos, agrupamento, etc. Um conjunto é determinado pelos seus *elementos* ou *membros*.

Os conjuntos são, em geral, denotados por letras latinas maiúsculas $A, B, C, ...$ e os elementos de um conjunto são geralmente representados por letras latinas minúsculas $a, b, c, ..., x, y, z$.

Usamos chaves para indicar os elementos do conjunto considerado. Quando conhecidos os elementos de um conjunto, a maneira usual de representá-lo é a seguinte:

$A = \{a, b, c\}$.

1.1.1 Relação de pertinência e a determinação de um conjunto

A relação de pertinência é fundamental para a teoria dos conjuntos.

Para indicar-se que um elemento *a pertence* a um conjunto A utilizamos o símbolo $\in$ e escrevemos $a \in A$; quando b não pertence ao conjunto A, utilizamos o símbolo $\notin$ e escrevemos $b \notin A$.

Exemplo 1.1 *Dado o conjunto* $A = \{1, 2, 3\}$ *podemos escrever:* $1 \in A, 2 \in A, 3 \in A, 4 \notin A, 5 \notin A, ...$

Ao mudarmos a ordem dos elementos num conjunto, continuamos tendo o mesmo conjunto, isto é, $\{1, 2, 3\}, \{1, 3, 2\}$ e $\{3, 2, 1\}$ representam o mesmo conjunto.

Um conjunto pode ser determinado de duas maneiras: *extencionalmente*, pela listagem de seus elementos, ou *intencionalmente*, através de alguma propriedade comum de seus elementos.

- extencionalmente:

Exemplo 1.2 $A = \{a, b, c, d, e\}$.

Exemplo 1.3 $B = \{-1, 0, 1, 2, 3\}$.

Exemplo 1.4 $\mathbb{Z} = \{... - 3, -2, -1, 0, 1, 2, 3, ...\}$.

- intencionalmente:

Exemplo 1.5 $A = \{x \in \mathbb{N} : x > 4\}$.

Exemplo 1.6 $B = \{x \in \mathbb{Z} : -4 \leq x < 6\}$.

Exemplo 1.7 $C = \{x \in \mathbb{R} : x \leq 10\}$.

1.1.2 Tipos de conjuntos

Alguns conjuntos são os que aparecem naturalmente na teoria dos conjuntos. Dentre eles, destacamos:

(i) *Conjunto vazio*: é o único conjunto que não tem elementos. Denotamos o conjunto vazio por { } ou, simplesmente, pelo símbolo $\emptyset$.

Exemplo 1.8 $A = \{x \in \mathbb{R} : x^2 + 1 = 0\}$.

Exemplo 1.9 $D = \{x \in \mathbb{N} : 4 < x < 5\}$.

(ii) *Conjunto unitário*: é um conjunto que possui apenas um elemento.

Exemplo 1.10 $A = \{8\}$.

Exemplo 1.11 $B = \{x : x \text{ é número primo par}\}$.

(iii) *Conjuntos finitos e infinitos*: um conjunto é finito quando tem uma quantidade de elementos igual a algum número natural. Um conjunto é infinito quando não é finito.

Exemplo 1.12 $A = \{x \in \mathbb{N} : x \text{ é número primo e } x < 100\}$ *é finito.*

Exemplo 1.13 $E = \mathbb{N}$ *é infinito.*

(iv) *Conjunto universo*: denominamos conjunto universo (domínio ou campo) ao conjunto de todos os elementos que estão sob verificação. Denotamos o conjunto universo por U.

1.1.3 Inclusão e igualdade de conjuntos

Esta seção trata da inclusão e igualdade de conjuntos.

Um conjunto A é *subconjunto* de um conjunto B quando todos os elementos que pertencem a A, também pertencem a B. Indicamos isto por: $A \subseteq B \Leftrightarrow (\forall x)(x \in A \rightarrow x \in B)$.

A expressão $A \subseteq B$ tem o significado de 'A está contido em B' ou 'A é parte de B' ou, ainda, 'B contém A'. Para todo conjunto A, são seus subconjuntos o próprio conjunto A e o conjunto vazio $\emptyset$. Estes dois subconjuntos são denominados de subconjuntos *triviais*.

O conjunto A é um *subconjunto próprio* de B se $A \subseteq B$ e algum elemento de B não pertence a A. Indicamos a inclusão própria por $A \subset B$.

Exemplo 1.14 *Dados os conjuntos* $A = \{-1, 0, 1\}$ *e* $B = \{-3, -2, -1, 0, 1, 2\}$*, como todos os elementos de* A *também são elementos de* B *e* $-2 \in B$*, mas* $-2 \notin A$*, podemos escrever:* $A \subset B$*.*

Exemplo 1.15 *Se* $A = \{2, 3\}$ *e* $B = \{x \in \mathbb{R} : x^2 - 5x + 6 = 0\}$*, então* $A \subseteq B$ *e* $B \subseteq A$*.*

Dois conjuntos A e B são *iguais* quando têm exatamente os mesmos elementos. A igualdade de conjuntos é denotada por $A = B$. Assim:

$A = B \Leftrightarrow (\forall x)((x \in A \rightarrow x \in B)\ e\ (x \in B \rightarrow x \in A))$ $\Leftrightarrow (\forall x)(x \in A \leftrightarrow x \in B)$.

A sentença $(\forall x)(x \in A \leftrightarrow x \in B)$ também é conhecida como o princípio da extensionalidade dos conjuntos.

Desta maneira, podemos também definir a igualdade de conjuntos da seguinte maneira: $A = B \Leftrightarrow A \subseteq B \; e \; B \subseteq A$ e a inclusão própria por: $A \subset B \Leftrightarrow A \subseteq B \; e \; A \neq B$.

Exemplo 1.16 *Dados os conjuntos* $A = \{0, 1, 2\}$ *e* $B = \{x \in \mathbb{N} : x \leq 2\}$*, podemos verificar que* A *e* B *possuem os mesmos elementos. Logo, indicamos isto por* $A = B$*.*

1.1.4 Conjunto das partes de um conjunto

Dado um conjunto A, o *conjunto das partes* de A é o conjunto $\mathcal{P}(A)$, cujos elementos são todos os subconjuntos de A.

Exemplo 1.17 *Dado o conjunto* $A = \{1, 2, 3\}$*, o conjunto das partes de* A *é o conjunto:* $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

Exemplo 1.18 *Se* $D = \{\alpha, \beta\}$*, então* $\mathcal{P}(D) = \{\emptyset, \{\alpha\}, \{\beta\}, \{\alpha, \beta\}\}$.

1.1.5 Operações com conjuntos e a álgebra dos conjuntos

Agora, veremos como compor com os conjuntos de forma a obtermos novos conjuntos. Isto é feito a partir das operações sobre conjuntos. Quatro importantes operações serão tratadas: a união, a intersecção, a complementação e a diferença entre conjuntos.

• A união de conjuntos: a *união* de dois conjuntos A e B é o conjunto $A \cup B$ cujos elementos pertencem a A ou a B. Assim: $A \cup B = \{x \in U : x \in A \vee x \in B\}$.

Em geral, indicamos quem é o nosso universo de discurso U. Isto é importante para evitarmos certos problemas que esta abordagem intuitiva pode causar.

Exemplo 1.19 *Dados os conjuntos* $A = \{-1, 0, 1\}$ *e* $B = \{1, 2, 3\}$*, então a união de* A *e* B *é o conjunto:* $A \cup B = \{-1, 0, 1, 2, 3\}$.

Exemplo 1.20 *Se* $A = \mathbb{Z}$ *e* B *é o conjunto dos inteiros pares, isto é,* $B = \{x \in \mathbb{Z} : x = 2.q \wedge q \in \mathbb{Z}\}$*, então* $A \cup B = \mathbb{Z}$.

• A intersecção de conjuntos: a *intersecção* de dois conjuntos A e B é o conjunto $A \cap B$ cujos elementos pertencem a A e a B simultaneamente. Assim, $A \cap B = \{x \in U : x \in A \; e \; x \in B\}$.

Exemplo 1.21 *Dados os conjuntos* $A = \{-1, 0, 1, 2, 3\}$ *e* $B = \{2, 3, 4, 5\}$*, temos que* $A \cap B = \{2, 3\}$.

Exemplo 1.22 *Se* $A = \mathbb{Z}$ *e* $B = \{x \in \mathbb{R} : x^2 = 2\}$*, então* $A \cap B = \emptyset$.

Dois conjuntos A e B são *disjuntos* ou *mutuamente exclusivos* quando $A \cap B = \emptyset$.

• A diferença de dois conjuntos: dados dois conjuntos A e B, a *diferença* entre A e B é o conjunto $A - B$ formado pelos elementos que pertencem a A, mas não pertencem a B. Assim: $A - B = \{x \in U : x \in A \; e \; x \notin B\}$.

Exemplo 1.23 *Dados os conjuntos* $A = \{-2, -1, 0, 1, 2\}$ *e* $B = \{0, 1, 2, 3\}$*, a diferença entre* A *e* B *é o conjunto* $A - B = \{-2, -1\}$.

Exemplo 1.24 *Se $A = \mathbb{R}$ e $B = \mathbb{Q}$, então $A - B$ é o conjunto $\mathbb{R} - \mathbb{Q}$ dos números irracionais.*

• A complementação: dados dois conjuntos A e B de maneira que $B \subseteq A$, o *complementar* de B com relação a A é o conjunto $\complement_B^A$ formado pelos elementos de A que não pertencem a B. Ou seja: $\complement_B^A = \{x \in U : x \in A \text{ e } x \notin B\}$.

De acordo com a definição de complementar, podemos observar que $\complement_B^A = A - B$. Além disso, o complementar de um conjunto A em relação ao universo U é representado por A^C ou A'.

De forma geral, uma estrutura algébrica é determinada por um conjunto não vazio munido de uma ou mais operações. O número de operações definidas e as propriedades verificadas pelas operações caracterizam abstratamente as álgebras. Dotaremos os conjuntos de uma estrutura algébrica, que chamamos a álgebra dos conjuntos.

Dado um conjunto qualquer U, o conjunto das partes de U é não vazio. Assim, consideremos $A, B, C \in \mathcal{P}(U)$. Com relação às operações de união, intersecção e complementação de conjuntos determinamos uma álgebra $(\mathcal{P}(U), \cup, \cap, \ ', \emptyset, U)$, em que valem as seguintes propriedades:
Propriedades da união:

$A \cup A = A$ [Idempotência]
$A \cup B = B \cup A$ [Comutatividade]
$(A \cup B) \cup C = A \cup (B \cup C)$ [Associatividade]
$A \cup \emptyset = A$ [Elemento neutro]
$A \cup U = U$ [Elemento absorvente]

Propriedades da intersecção:

$A \cap A = A$ [Idempotência]

$A \cap B = B \cap A$ [Comutatividade]

$(A \cap B) \cap C = A \cap (B \cap C)$ [Associatividade]

$A \cap U = A$ [Elemento neutro]

$A \cap \emptyset = \emptyset$ [Elemento absorvente]

Propriedades distributivas:

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Propriedades da complementação:

$A' \cap A = \emptyset$

$A' \cup A = U$

$\emptyset' = U$

$U' = \emptyset$

$(A')' = A$

Propriedades de dualidade ou leis de De Morgan:

$(A \cup B)' = A' \cap B'$

$(A \cap B)' = A' \cup B'$

Propriedades de absorção e diferença:

$A \cap (A \cup B) = A$

$A \cup (A \cap B) = A$

$A - B = A \cap B'$.

Exercício 1.1 *Verificar as propriedades das operações com conjuntos.*

1.2 Relações

Agora apresentamos as relações entre conjuntos.

O *produto cartesiano* do conjunto A pelo conjunto B é o conjunto de todos os pares ordenados (a, b) tais que $a \in A$ e $b \in B$. Assim, $A \times B = \{(a, b) : a \in A \ e \ b \in B\}$.

Uma *relação binária* é um subconjunto de $A \times B$.

Assim $R \subseteq A \times B$ é uma relação binária. Em geral, quando tratamos de uma relação binária, dizemos apenas relação. Para uma relação R, algumas vezes escrevemos xRy no lugar de $(x, y) \in R$. Por exemplo, no caso da relação de ordem $\leq$ sobre o conjunto dos números reais $\mathbb{R}$, temos que $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x \text{ é menor ou igual a } y\}$, contudo, usualmente denotamos esta relação por '$x \leq y$' e não por '$(x, y) \in R$'.

Seja R uma relação em $A \times B$. O *domínio* de R, denotado por $Dom(R)$, é definido por: $Dom(R) = \{x \in A : (x, y) \in R \text{ para algum } y \in B\}$. A *imagem* de R, indicada por $Im(R)$, é definida por: $Im(R) = \{y \in B : (x, y) \in R \text{ para algum } x \in A\}$.

Uma relação *sobre* um conjunto A é um subconjunto R do produto cartesiano $A \times A$. A relação R é:

(i) *reflexiva* quando, para todo $a \in A, aRa$;

(ii) *simétrica* quando, para todos $a, b \in A$, se aRb, então bRa;

(iii) *transitiva* quando, para todos $a, b, c \in A$, se aRb e bRc, então aRc;

(iv) *anti-simétrica* quando, para todos $a, b \in A$, se aRb e bRa, então $a = b$.

Exemplo 1.25 *A relação $R = \{(a, b) \in \mathbb{R} : a \leq b\}$, usualmente denotada por $a \leq b$, é reflexiva, transitiva e anti-simétrica.*

Exemplo 1.26 *Seja T o conjunto de todos os triângulos de um dado plano. A relação S definida por '$t \sim u \Leftrightarrow t$ é congruente a u' é uma relação reflexiva, simétrica e transitiva em T.*

1.2.1 Relações de equivalência

A relação de equivalência desempenha um papel importante na Matemática, como um modo de generalizar a relação de igualdade em situação em que indivíduos embora distintos possam executar um papel equivalente.

Uma *relação de equivalência* sobre um conjunto A é uma relação que é reflexiva, simétrica e transitiva.

Exemplo 1.27 *A relação $R = \{(a,a),(b,b),(c,c),(a,c),(c,a)\}$, é uma relação de equivalência sobre $A = \{a,b,c\}$.*

Exemplo 1.28 *A relação de igualdade em qualquer conjunto é sempre uma relação de equivalência.*

Exemplo 1.29 *A semelhança de triângulos é uma relação de equivalência.*

Exemplo 1.30 *A relação '$<$' em $\mathbb{R}$ não é uma relação de equivalência, pois não é simétrica: $1 < 2$ mas não ocorre $2 < 1$.*

Quando R é uma relação de equivalência em um conjunto A e $a \in A$, o conjunto $[a] = \{x \in A : xRa\}$ é a *classe de equivalência* de a.

Também é usual denotar-se a classe de equivalência $[a]$ por $\bar{a}$.

Exemplo 1.31 *Se* $A = \{1, 2, 3\}$ *e* $R = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$*, então* R *é uma relação de equivalência e as suas classes de equivalência são dadas por:* $[1] = \{1, 2\}$*,* $[2] = \{1, 2\}$ *e* $[3] = \{3\}$*.*

Teorema 1.1 *Seja* R *uma relação de equivalência em um conjunto* A*. Então:*

(i) duas classes de equivalência são iguais ou disjuntas;

(ii) o conjunto A *é a união de todas as classes de equivalência.*

Demonstração: *Ver (Feitosa, Nascimento, Alfonso, 2008).* ∎

Quando R é uma relação de equivalência em um conjunto A, o *conjunto quociente* de A pela relação R é o conjunto das classes de equivalência de R: $A|_R = \{[a] : a \in A\} = \{B \in \mathcal{P}(A) : B = [a], \text{ para algum } a \in A\}$.

Uma *partição* $\mathbf{P}$ de um conjunto não vazio A é uma coleção de subconjuntos não vazios de A, dois a dois disjuntos e cuja união é igual a A.

Assim, cada membro X de $\mathbf{P}$ é não vazio, ou seja, $X \neq \emptyset$. Se $X, Y \in \mathbf{P}$ e $X \neq Y$, então $X \cap Y = \emptyset$ e, $\cup\{X : X \in \mathbf{P}\} = A$.

Exemplo 1.32 *Se* $A = \{1, 2, 3, 4\}$*, são partições de* A*:* $\mathbf{P}_1 = \{\{1\}, \{2\}, \{3\}, \{4\}\}$ *e* $\mathbf{P}_2 = \{\{1, 2\}, \{3, 4\}\}$*, etc.*

Exemplo 1.33 *O conjunto* $\mathbf{P} = \{(-\infty, -3], (-3, 7], (7, \infty)\}$ *é uma partição de* $\mathbb{R}$*.*

1.2.2 Relações de ordem

A definição de relação de ordem procura formalizar algumas concepções intuitivas da ordenação e são fundamentais no contexto matemático.

Seja R uma relação em um conjunto A. A relação R é uma *relação de ordem* sobre A quando é reflexiva, anti-simétrica e transitiva. Nestas condições, dizemos que o par (A, R) é uma *estrutura de ordem* e o conjunto A é *ordenado* por R.

Uma relação de ordem é muitas vezes chamada de ordem parcial.

Exemplo 1.34 *A relação 'x é menor ou igual a y', denotada por $x \leq y$, no conjunto dos números reais é uma ordem.*

Exemplo 1.35 *Dado um conjunto E, consideremos o conjunto $\mathcal{P}(E)$. A relação 'A é subconjunto de B' é uma relação de ordem em $\mathcal{P}(E)$.*

Como é usual, a menos que precisemos indicar de outro modo, denotaremos uma estrutura de ordem por $(A, \leq)$.

A ordem $\leq$ em A é uma *ordem total* (ou *ordem linear*) quando para todo par de elementos $x, y \in A$, tem-se que $x \leq y$ ou $y \leq x$.

Nesse caso, temos uma estrutura de ordem total $(A, \leq)$ e dizemos que A é um conjunto totalmente ordenado por $\leq$. Devemos observar que cada ordem total é ainda uma ordem parcial.

Exemplo 1.36 *A relação 'x é menor ou igual a y' é uma ordem total em* $\mathbb{N}$ *(ou em* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$*).*

Seja $(A, \leq)$ uma ordem parcial e $x, y \in A$. O elemento x é *estritamente menor* que y, o que é denotado por $x < y$, quando $x \leq y$ e $x \neq y$.

Nesse caso dizemos que $<$ é uma *ordem estrita*. Essa ordem estrita é anti-simétrica e transitiva, mas não é reflexiva.

Um par $(A, \leq)$ é uma ordem total se, e somente se, vale a lei da tricotomia, isto é, para quaisquer $x, y \in A$, vale exatamente uma das condições seguintes: $x < y$ ou $x = y$ ou $y < x$.

Sejam $(E, \leq)$ uma ordem e $\emptyset \neq A \subseteq E$. Um elemento M de A é um *máximo* de A quando: $\forall x(x \in A \rightarrow x \leq M)$. Um elemento m de A é um *mínimo* de A quando: $\forall x(x \in A \rightarrow m \leq x)$.

Seja $(A, \leq)$ uma ordem parcial. O conjunto A é *bem ordenado* quando todo subconjunto não vazio B de A tem elemento mínimo. Nesse caso, o par $(A, \leq)$ é uma *boa ordem*.

Exemplo 1.37 $(\mathbb{N}, \leq)$ *é uma boa ordem, mas* $(\mathbb{Z}, \leq)$ *não é.*

Exemplo 1.38 $(\mathbb{Z}\times\mathbb{Z}, \preceq)$ *em que* $(x, y) \preceq (z, w) \Leftrightarrow x < z \vee (x = z \text{ e } y \leq w)$ *é uma ordem total. Esta ordem é conhecida como ordem lexicográfica, a ordem dos dicionários.*

Segue da definição, que todo conjunto bem ordenado determina uma ordem total, pois dados $x, y \in A$, o conjunto $\{x, y\} \subseteq A$ tem um mínimo.

1.3 Funções

Cada função é um caso particular de uma relação.

Uma *função* de A em B é uma relação $h \subseteq A \times B$ tal que para cada $x \in A$ existe um único y de modo que $(x, y) \in h$.

Em geral, denotamos uma função h de A em B por $h : A \longrightarrow B$. Esta notação indica que h é uma função com $Dom(h) = A$ e $Im(h) \subseteq B$. O conjunto B é o *contradomínio* de h.

Assim, uma função h de A em B é uma relação que satisfaz:

(i) $h \subseteq A \times B$;

(ii) $(\forall x \in A)(\exists y \in B)((x, y) \in h)$;

(iii) $(x, y) \in h$ e $(x, z) \in h \Rightarrow y = z$.

Para uma função h e um ponto (elemento) $x \in Dom(h)$, o único y tal que $(x, y) \in h$ é chamado o *valor* de h em x ou a *imagem* de x por h, e é denotado por $h(x)$. O elemento x é o *argumento* de $h(x)$.

Assim, $(x, y) \in h \Leftrightarrow y = h(x)$ e, desse modo, $(x, h(x)) \in h$.

Exemplo 1.39 *Para um conjunto A, $i_A : A \to A$ é a função identidade em A e $i_A(x) = x$, para todo $x \in A$.*

Uma função é *sobrejetiva* quando $Im(h) = B$. Uma função é *injetiva* quando, para $x, z \in A$, se $x \neq z$, então $h(x) \neq h(z)$. Uma função é *bijetiva* quando é injetiva e sobrejetiva.

Uma função sobrejetiva aplica A sobre o todo de B, não deixando qualquer elemento de B sem um correspondente em A.

Uma função injetiva conduz elementos distintos em imagens distintas, ou de acordo com a sua contra-positiva, '$h(x) = h(z) \Rightarrow x = z$', imagens idênticas exigem argumentos idênticos. Numa função bijetiva, para cada $y \in B$, existe um único $x \in A$ tal que $(x, y) \in h$.

Exemplo 1.40 *Dado um conjunto não vazio A e uma relação de equivalência $\sim$ em A, seja $A|_\sim = \{[a] : a \in A\}$ o conjunto quociente de A por $\sim$. A função projeção $\pi : A \longrightarrow A_\sim$ é uma função sobrejetiva que leva cada membro $a \in A$ em $\pi(a) = [a]$.*

É usual denotarmos uma seqüência por $(a)_n = (a_1, a_2, a_3, ..., a_n, ...)$. Poderíamos iniciar uma seqüência do 0, mas não seria natural dizer que o primeiro elemento de $(a)_n$ é a_0. Devido a isto, em temas da Matemática que usam com muita freqüência as seqüências, como no cálculo e análise matemática, assume-se que 0 não é número natural, enquanto que em contexto algébricos é bom que o elemento neutro da adição de naturais seja ele um número natural e, daí, considerar-se 0 como número natural. Contudo, cada contexto deve explicitar suas escolhas e manter a coerência e consistência interna, independente da escolha feita.

Exercício 1.2 *Descrever os seguintes conjuntos através de uma propriedade característica de seus elementos:*
(a) $A = \{0, 2, 4, 6, ...\}$*;*
(b) $B = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$*;*
(c) $C = \{0, 1, 4, 9, 16, 25, 36, ...\}$*;*
(d) $D = \{1, -1, 2, -2, 3, -3\}$.

Exercício 1.3 *Descrever por meio da listagem dos seus elementos os conjuntos:*
(a) conjunto dos múltiplos de 3 entre -11 e 8;

(b) conjunto dos divisores de 36;
(c) conjunto dos múltiplos de 0.

Exercício 1.4 *Determinar se é verdadeira ou falsa cada uma das seguintes sentenças:*
(a) $\{0,1\} \in \{0,1,2,3\}$*;* *(b)* $\{a\} \in \{a,b\}$*;* *(c)* $\emptyset \in \{0\}$*;*
(d) $0 \in \emptyset$*;* *(e)* $\{a\} \subseteq \emptyset$*;* *(f)* $a \in \{a,\{a\}\}$*;*
(g) $\{a\} \subseteq \{a,\{a\}\}$*;* *(h)* $\emptyset \subseteq \{\emptyset,\{a\}\}$*;* *(i)* $\emptyset \in \{\emptyset,\{a\}\}$*.*

Exercício 1.5 *Dados os conjuntos* $A = \{1,2,3,4\}$ *e* $B = \{2,4\}$*, escrever com a simbologia da teoria dos conjuntos as sentenças abaixo e determinar quais são verdadeiras e quais são falsas:*
(a) 3 é elemento de A*;* *(b)* B *é parte de* A*;*
(c) 4 pertence a B*;* *(d) 1 não está em* B*;*
(e) B *é igual a* A*;* *(f)* B *não é subconjunto de* A*.*

Exercício 1.6 *Demonstrar que para todo conjunto* A*, vale* $\emptyset \subseteq A$*.*

Exercício 1.7 *Mostrar que existe um único conjunto vazio.*

Exercício 1.8 *Construir o conjunto das partes de* $B = \{a,b,c\}$*.*

Exercício 1.9 *Justificar a igualdade* $A \cup (A \cap B) = A$*.*

Exercício 1.10 *Dar exemplos de conjuntos* A, B *e* C *tais que* $(A \cup B) \cap C \neq A \cup (B \cap C)$*.*

Exercício 1.11 *Verificar quais propriedades são satisfeitas, sobre o conjunto* $\mathbb{R}$*, para cada uma das relações abaixo:*
(a) $aRb \Leftrightarrow a^2 = b^2$*;* *(b)* $aRb \Leftrightarrow a - b < 1$*;*
(c) $aRb \Leftrightarrow a < b$*;* *(d)* $aRb \Leftrightarrow a = b^2$*;*

Exercício 1.12 *Para as seguintes relações de* $\mathbb{R}$ *em* $\mathbb{R}$*, dizer se são, ou não, funções e justificar:*
(a) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 = y^2\}$*;*
(b) $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 10\}$*;*
(c) $T = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = x^2\}$*;*
(d) $T = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x = y^2\}$*.*

2 Propriedades dos inteiros

Neste capítulo apresentamos os números inteiros e algumas propriedades elementares que caracterizam a estrutura algébrica dos inteiros com a adição, a multiplicação, o zero, o um e a relação de ordem usuais. Estes elementos teóricos serão usados nos desenvolvimentos posteriores.

Embora já tenhamos utilizadas algumas notações, vamos explicitá-las a seguir.

O conjunto dos *números inteiros*, denotado por $\mathbb{Z}$, é o conjunto determinado por:

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

e o conjunto dos *números naturais*, denotado por $\mathbb{N}$, é o conjunto

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, ...\}$$

Como usualmente, se desejamos indicar que 0 não pertence ao um conjunto, denotamos o conjunto seguido de um asterisco, por exemplo,

$$\mathbb{N}^* = \{1, 2, 3, 4, 5, ...\}.$$

Os conjuntos dos números reais, dos racionais (ou fracionários), e dos complexos são denotados, respectivamente, por $\mathbb{R}, \mathbb{Q}$ e $\mathbb{C}$.

2.1 Operações elementares com inteiros

Interessa-nos não apenas o conjunto $\mathbb{Z}$, mas também alguns aspectos algébricos determinados sobre $\mathbb{Z}$. Assim, destacamos duas operações sobre os inteiros, uma *adição* $+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, que para dois inteiros a e b associa um outro inteiro indicado

por $a + b$, a *soma* de a e b; e uma *multiplicação* $\cdot : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, que para dois inteiros a e b associa um outro inteiro indicado por $a \cdot b$, o *produto* de a e b.

Como é usual, desde que não haja problemas de notação e entendimento, indicamos uma multiplicação de a por b apenas por ab. Também, a multiplicação tem prioridade sobre a adição: $a + bc$ significa $a + (bc)$.

Exemplo 2.1 $2n = 14$.

Exemplo 2.2 $2 \cdot 7 = 14$.

Exemplo 2.3 $a(b + c) = ab + ac$.

Destacamos em $\mathbb{Z}$ dois elementos que desempenham papel especial quanto a estas duas operações de adição e multiplicação, o 0 (zero) e o 1 (um), conforme veremos logo a seguir.

Consideramos a ordem usual em $\mathbb{Z}$: $a \leq b \Leftrightarrow a - b \leq 0$. A ordem estrita é dada por $a < b \Leftrightarrow a - b < 0$.

Dizemos que um inteiro a é positivo ou negativo caso $a > 0$ ou $a < 0$, respectivamente.

As propriedades, indicadas a seguir, para as operações de adição e multiplicação de números inteiros, serão assumidas como válidas. Detalhes sobre as validades de tais propriedades podem ser encontradas em textos que versam sobre a construção dos inteiros, como em (Feitosa, Nascimento, Alfonso, 2009).

Dados $a, b, c \in \mathbb{Z}$, em $(\mathbb{Z}, 0, 1, +, ., <)$ valem as propriedades:

1. Fechamento: $a + b \in \mathbb{Z}$ e $ab \in \mathbb{Z}$
2. Comutatividade: $a + b = b + a$ e $ab = ba$

3. Associatividade: $a + (b + c) = (a + b) + c$ e $a(bc) = (ab)c$
4. Elemento neutro da adição (zero): existe $0 \in \mathbb{Z}$ tal que $a + 0 = 0 + a = a$
5. Elemento neutro da multiplicação (um): existe $1 \in \mathbb{Z}$ tal que $1.a = a.1 = a$
6. Distributividade: $a(b + c) = ab + ac$
7. Multiplicação por zero: $0a = 0$
8. Inverso aditivo (oposto): Para cada $a \in \mathbb{Z}$, existe $-a \in \mathbb{Z}$ tal que $a + (-a) = 0$
9. Integridade: Se $ab = 0$, então $a = 0$ ou $b = 0$
10. Regra do sinal: $(-a)b = a(-b) = -(ab)$ e $(-a)(-b) = ab$
11. Tricotomia: Dados os inteiros a e b, então $a < b$ ou $a = b$ ou $b < a$
12. Desigualdades:
    (i) $a < b \Leftrightarrow a + c < b + c$
    (ii) Se $0 < c$, então $a < b \Leftrightarrow ac < bc$
    (iii) Se $c < 0$, então $a < b \Leftrightarrow ac > bc$
13. Cancelamento:
    (i) $a + c = b + c \Leftrightarrow a = b$
    (ii) Se $a \neq 0$, então $ab = ac \Leftrightarrow b = c$

    Para a inteiro, denotamos $a^2 = aa$.

Exercício 2.1 *Dados $a, b, c, d \in \mathbb{Z}$, mostrar que:*
(a) $(a + b)(c + d) = ac + ad + bc + bd$;
(b) $(a + b)^2 = a^2 + 2ab + b^2$;
(c) $(a - b)^2 = a^2 - 2ab + b^2$;
(d) $(a + b)(a - b) = a^2 - b^2$;
(e) $(b + c)d = bd + cd$;
(f) $a(b + c)d = abd + acd$.

Exercício 2.2 *Dados $a, b, c, d \in \mathbb{Z}$, mostrar a validade ou dar um contra-exemplo para:*
(a) $a^2 > ab \Rightarrow a > b$;
(b) $a < b \ e \ c < d \Rightarrow a + c < b + d$;
(c) $a < b \ e \ c < d \Rightarrow ac < bd$;
(d) $a + c < b + d \Rightarrow a < b \ e \ c < d$;
(e) $ab = a \Rightarrow b = 1$.

3 Indução matemática

Neste capítulo tratamos da indução matemática. A indução matemática é um princípio postulado por Peano para os números naturais que afirma que se uma propriedade é verificada para o zero, e sempre que verificada para um natural n, também pode ser verificada para o seu sucessor n+1, então a propriedade é verificada para todos os números naturais.

Mostraremos que a indução, como no enunciado acima, é equivalente a outros resultados, no sentido que, tomando um deles como princípio (ou axioma), os demais, inclusive o princípio de indução, são demonstrados a partir dele.

3.1 A boa ordem e os princípios de indução

Princípio da boa ordem (PBO): Todo subconjunto não vazio do conjunto dos números naturais tem um menor elemento (elemento mínimo).

Este princípio indica que se $S \subseteq \mathbb{N}$ e $S \neq \emptyset$, então existe $s \in S$ tal que $s \leq n$, para todo $n \in S$.

Princípio da indução (PI): Dado $m \in \mathbb{N}$, seja $S = \{x \in \mathbb{N} : m \leq x\}$. Se $P(n)$ é uma propriedade sobre $n \in \mathbb{N}$ tal que:
(i) $P(m)$ é verdadeira e
(ii) se $n \in S$ e $P(n)$ é verdadeira, então $P(n+1)$ é verdadeira;
então $P(n)$ é verdadeira para todo $n \in S$, isto é, $P(n)$ é verdadeira para todo $n \in \mathbb{N}$, $n \geq m$.

Princípio forte da indução (PFI): Dado $m \in \mathbb{N}$, seja $S = \{x \in \mathbb{N} : m \leq x\}$. Se $P(n)$ é uma propriedade sobre $n \in \mathbb{N}$ tal que:

(i) $P(m)$ é verdadeira e

(ii) para todos $n, r \in S$, com $m \leq r < n$, sempre que $P(r)$ é verdadeira tem-se que $P(n)$ é verdadeira;

então $P(n)$ é verdadeira para todo $n \in S$, isto é, $P(n)$ é verdadeira para todo $n \in \mathbb{N}$, $n \geq m$.

Se no conjunto S acima temos $m = 0$, então $S = \mathbb{N}$. A seguir mostramos a equivalência entre os três princípios mencionados.

Lema 3.1 *PBO* $\Rightarrow$ *PFI.*

Demonstração: *Seja $P(n)$ uma propriedade que satisfaz as hipóteses do PFI, isto é, valem: (i) $P(m)$ é verdadeira e (ii) para todos $n, r \in S$, com $m \leq r < n$, se $P(r)$ é verdadeira, então $P(n)$ é verdadeira.*

Seja $K = \{n \in \mathbb{N} : m \leq n \text{ e } P(n) \text{ é } falsa\}$. Suponhamos que $K \neq \emptyset$. Pelo PBO, existe o menor elemento k de K e, desde que, por hipótese, $P(m)$ é verdadeira, então $m < k$ Agora, pela minimalidade de k, para todo r tal que $m \leq r < k$, tem-se que $P(r)$ é verdadeira. Mas, então, por (ii), $P(k)$ é verdadeira e, portanto, $k \notin K$, o que contradiz a escolha de k. Logo, $K = \emptyset$ e, desse modo, $P(n)$ é verdadeira para todo $n \in S = \{n \in \mathbb{N} : m \leq n\}$. ∎

Lema 3.2 *PFI* $\Rightarrow$ *PI.*

Demonstração: *Seja $P(n)$ uma propriedade que satisfaz as hipóteses do PI, isto é, valem: (i) $P(m)$ é verdadeira e (ii) se $n \in S$ e $P(n)$ é verdadeira, então $P(n+1)$ é verdadeira.*

Sejam $n, r \in S$ tais que para $m \leq r < n$, tem-se $P(r)$ verdadeira. Como $m < n$, então $m \leq n-1 < n$ e, daí, $P(n-1)$ é verdadeira. Por (ii), $P(n) = P((n-1)+1)$ é verdadeira e, pelo PFI, $P(n)$ é verdadeira, para todo $n \in S$. ∎

Lema 3.3 *PI $\Rightarrow$ PBO.*
Demonstração: *Seja $S \subseteq \mathbb{N}$, tal que $S \neq \emptyset$. Se $0 \in S$, então 0 é o menor elemento de S. Se $0 \notin S$, consideremos a propriedade $P(n)$: $n < s$, para todo $s \in S$. Desse modo $P(0)$ é verdadeira.*
Afirmação 1: Existe $r \in \mathbb{N}$ tal que $P(r)$ é verdadeira, mas $P(r+1)$ é falsa.
Suponhamos que para todo $r \in \mathbb{N}$, $P(r)$ verdadeira implica $P(r+1)$ verdadeira. Como $P(0)$ é verdadeira, pelo PI, $P(n)$ é verdadeira para todo $n \in \mathbb{N}$ e, portanto, $S = \emptyset$, o que contradiz a asserção $S \neq \emptyset$. Logo, existe r que satisfaz a afirmação 1.
Afirmação 2: $r+1$ é o menor elemento de S.
Consideremos que r satisfaz a afirmação 1. Como $P(r)$ é verdadeira, então $r < s$ para todo $s \in S$. Logo, $r+1 \leq s$ para todo $s \in S$. Se $r+1 \notin S$, então $r+1 < s$ para todo $s \in S$, ou seja, $P(r+1)$ é verdadeira, o que é uma contradição, pois estamos considerando que r satisfaz a afirmação 1. Assim, $r+1 \in S$ e, além disso, $r+1$ é o menor elemento de S, pois $r+1 \leq s$ para todo $s \in S$. ∎

Teorema 3.4 *Os três princípios acima são equivalentes.*
Demonstração: *Segue dos lemas anteriores.* ∎

Mostrar que uma proposição $P(n)$ é válida para todo $n \geq m$ é mostrar que $P(n)$ é válida para todo $n \in \{k \in \mathbb{N} : k \geq m\}$. Assim, para aplicar o PI, deve-se mostrar:
(i) $P(m)$ é válida;
(ii) Supor $k \geq m$ e $P(k)$ válida (hipótese de indução) e

demonstrar $P(k+1)$ válida
Concluir que, pelo PI, $P(n)$ é válida para todo $n \in \mathbb{N},\ n \geq m$.

A aplicação do PIF é análoga, mantendo (i) e mudando (ii) para:
(ii) Supor $m < n$ e $P(k)$ válida para todo k tal que $m \leq k < n$ (hipótese de indução) e demonstrar $P(n+1)$ válida.
Concluir que, pelo PIF, $P(n)$ é válida para todo $n \in \mathbb{N},\ n \geq m$.

3.2 Aplicações dos princípios de indução na Matemática

O princípio de indução tem inúmeras aplicações na Matemática, naturalmente na teoria dos números, mas em muitas outras sub-áreas da Matemática, como veremos a seguir.

Iniciemos com uma aplicação que envolve os números inteiros e suas propriedades.

Veremos que dados dois inteiros a e b, com $a \neq 0$, então algum múltiplo de a é maior que b. Embora este resultado receba o nome em homenagem a Arquimedes, ele foi enunciado anteriormente por Eudoxo.

Um conjunto ordenado $(A, \leq)$ admite a *propriedade arquimediana* se para todos $a,\ b\ \in\ A$, com $a \neq 0$, existe $d \in A$, tal que $d.a > b$.

Teorema 3.5 *O conjunto $\mathbb{Z}$ admite a propriedade arquimediana, ou mais especificamente, para $a, b \in \mathbb{Z}$, com $a \neq 0$, segue que:*

(i) existe $d \in \mathbb{Z}$ tal que $da > b$;

(ii) existe $e \in \mathbb{Z}$ tal que $ea < b$.

Demonstração: *(i) Podemos verificar somente o caso* $a > 0$, *pois se* $a < 0$ *então* $-a > 0$ *e* $(-d)a = d(-a)$.
Se $a > b$, *basta tomarmos* $d = 1$. *Agora, se* $a \leq b$, *então* $b - a \geq 0$. *Seja* $K = \{b - na : n \in \mathbb{Z} \text{ e } b - na \geq 0\}$. *Como* $b - a \in K$, *então* $K \neq \emptyset$. *Pelo princípio da boa ordem (PBO), o conjunto* K *tem um menor elemento, digamos* $b - ma$. *Desde que* $a > 0$, *então* $b - ma > b - ma - a = b - (m + 1)a$. *Como* $b - ma$ *é o menor elemento de* K, *então* $b - (m + 1)a \notin K$, *ou seja,* $b-(m+1)a < 0$ *e, portanto,* $b < (m+1)a$. *Assim, se* $d = m+1$, *temos* $da = (m + 1)a > b$.
(ii) De (i), considerando a *e* $-b$, *existe* $d \in \mathbb{Z}$ *tal que* $da > -b$. *Agora, multiplicando esta desigualdade por* -1, *temos* $(-d)a < b$. *Logo, basta tomarmos* $e = -d$. ∎

Exemplo 3.1 *Verificar que* $1+2+3+...+n = \frac{n}{2} \cdot (n+1)$, *para todo* $n \in \mathbb{N}^*$.

Como $n \in \mathbb{N}^*$, *iniciamos com o caso em que* $n = 1$. *Assim, para* $n = 1$, *temos* $1 = \frac{1}{2}(1 + 1)$, *que é válido.*

Como hipótese de indução, assumimos que a igualdade vale para $k \geq 1$ *e, daí, mostramos que vale para* $k + 1$.

Desde que $1 + 2 + 3 + ... + k = \frac{k}{2} \cdot (k + 1)$, *então* $1 + 2 + 3 + ... + k + (k + 1) = \frac{k}{2} \cdot (k + 1) + (k + 1) = (\frac{k}{2} + 1) \cdot (k + 1) = \frac{k+2}{2} \cdot (k + 1) = \frac{k+1}{2} \cdot (k + 2)$.

Assim, o resultado vale para $k + 1$ *e, pelo PI, vale para todo* $n \in \mathbb{N}^*$.

Os princípios de indução servem para justificar definições dadas por recursão, como no seguinte caso.

Para $n \in \mathbb{Z}^*$ e $r \in \mathbb{N}$, a *potência* de n é definida por: $n^0 = 1$ e $n^{r+1} = n^r \cdot n$, desde que n^r esteja definido. Define-se também $0^r = 0$ para $r > 0$.

Exercício 3.1 *Mostrar, por indução sobre p, que $n^p \in \mathbb{Z}$, quaisquer que sejam $n, p \in \mathbb{Z}$, com $p \geq 0$ e $n \neq 0$.*

Exercício 3.2 *Para $m, n, r, s \in \mathbb{Z}$, com $m \neq 0, n \neq 0, r \geq 0$ e $s \geq 0$, mostrar que:*
(a) $n^r \cdot n^s = n^{r+s}$ *(b)* $n^r \cdot m^r = (nm)^r$ *(c)* $(n^r)^s = n^{rs}$

Exercício 3.3 *Comprovar, por indução, as seguintes igualdades:*
(a) $2^0 + 2^1 + 2^2 + ... + 2^{n-1} = 2^n - 1$, *para todo* $n \in \mathbb{N}$, *com* $n \geq 1$;
(b) $1^2 + 2^2 + 3^2 + ... + n^2 = n(n+1)(2n+1)/6$, *para todo* $n \in \mathbb{N}$, *com* $n \geq 1$;
(c) $1^3 + 2^3 + 3^3 + ... + n^3 = n^2(n+1)^2/4$, *para todo* $n \in \mathbb{N}$, *com* $n \geq 1$;
(d) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + ... + n \cdot (n+1) = n(n+1)(n+2)/3$, *para todo* $n \in \mathbb{N}$, *com* $n \geq 1$.

O fato de algumas afirmações valerem para uma boa quantidade inicial de números naturais não garante que valha para todos os números naturais. Por exemplo, a fórmula $n^2 + n + 41$ fornece números primos para $n = 1, 2, ..., 39$, porém para $n = 40$ podemos verificar que $n^2 + n + 41$ não é um número primo.

Apesar da simplicidade de aplicação dos princípios de indução, precisamos tomar cuidado ao Demonstrar resultados, verificando se estamos aplicando de forma correta os conceitos e teoremas envolvidos.

Procurar o erro na 'dedução' a seguir.

Exemplo 3.2 ***(Teorema Feminista):*** *Todos os homens são iguais.*

Demonstração: *por indução sobre o conjuntos com n homens. Para $n = 1$ o enunciado vale, pois num conjunto unitário de homens todos são iguais.*

Hipótese de indução: Em cada conjunto com n homens todos eles são iguais.

Seja A um conjunto com $n + 1$ homens, digamos $A = \{h_1, h_2, ..., h_n, h_{n+1}\}$. Os conjuntos $\{h_1, h_2, ..., h_n\}$ e $\{h_2, ..., h_n, h_{n+1}\}$ têm n elementos. Logo, pela hipótese de indução, $h_1 = h_2 = ... = h_n$ e $h_2 = ... = h_n = h_{n+1}$. Desse modo, todos os homens de A são iguais, ou seja, provamos o caso para $n+1$. Portanto, pelo PI, todos os homens são iguais.

■

Os princípios de indução são usados para a verificação de algumas fórmulas envolvendo números naturais. Como uma aplicação, verificaremos a validade da fórmula da soma dos n primeiros termos iniciais de uma progressão aritmética (PA).

Exemplo 3.3 *Se $(a_1, a_2, ..., a_n, ...)$ é uma progressão aritmética, com razão r, então: $a_n = a_1 + (n-1)r$.*

Dedução por indução sobre n.

Para $n = 1$, $a_1 = a_1 + (1-1)r$.

Na hipótese de indução, consideremos que a fórmula vale para n, isto é, $a_n = a_1 + (n-1)r$.

Daí, $a_{n+1} = a_n + r = a_1 + (n-1)r + r = a_1 + nr = a_1 + [(n+1) - 1]r$. Logo, a fórmula vale para $n+1$.

Assim, pelo PI, a fórmula vale para todo n inteiro tal que $n \geq 1$.

Exemplo 3.4 *Se $(a_1, a_2, ..., a_n, ...)$ é uma progressão aritmética,*

com razão r, então $S_n = \dfrac{(a_1 + a_n) \cdot n}{2}$ *é soma dos n primeiros termos da PA.*

A justificação é por indução sobre n.

Para $n = 1$, temos que $S_1 = (a_1 + a_1)\dfrac{1}{2} = a_1$.

Hipótese de indução: Seja $S_n = (a_1 + a_n)\dfrac{n}{2}$.

Daí: $S_{n+1} = S_n + a_{n+1} = (a_1 + a_n)\dfrac{n}{2} + a_{n+1} =$

$$\frac{na_1 + na_n + 2a_{n+1}}{2} = \frac{na_1 + n[a_1 + (n-1)r] + 2a_{n+1}}{2} =$$

$$\frac{na_1 + na_1 + n(n-1)r + 2a_{n+1}}{2} =$$

$$\frac{(n+1)a_1 + (n-1)a_1 + n(n-1)r + 2a_{n+1}}{2} =$$

$$\frac{(n+1)a_1 + (n-1)(a_1 + nr) + 2a_{n+1}}{2} =$$

$$\frac{(n+1)a_1 + (n-1)a_{n+1} + 2a_{n+1}}{2} = \frac{(n+1)a_1 + (n+1)a_{n+1}}{2} =$$

$$\frac{(n+1)(a_1 + a_{n+1})}{2} = (a_1 + a_{n+1})\frac{n+1}{2},$$ *ou seja,*

$S_{n+1} = (a_1 + a_{n+1})\dfrac{n+1}{2}$.

Assim, pelo PI, a fórmula vale para todo n inteiro, $n \geq 1$.

Exercício 3.4 *Mostrar que:*

(a) o termo geral de uma progressão geométrica de razão q é:

$a_n = a_1 q^{n-1}$, *para todo* $n \in \mathbb{N}$, *com* $n \geq 1$;

(b) o produto dos n termos iniciais de uma progressão geométrica de razão q é:

$P_n = (a_1 \cdot a_n)^{n/2}$, *para todo* $n \in \mathbb{N}$, *tal que* $n \geq 1$;

(c) a soma dos n termos iniciais de uma progressão geométrica de razão q é:

$$S_n = a_1(1 - q^n)/(1 - q).$$

Exercício 3.5 *Considerando a soma:* $S_n = 1/(1\cdot 2)+1/(2\cdot 3)+ 1/(3\cdot 4) + ... + 1/(n\cdot(n+1))$, *pede-se:*
(a) Calcular S_1, S_2, S_3, S_4*;*
(b) Observar os denominadores e respectivos numeradores e escrever uma fórmula para S_n*;*
(c) Verificar se a fórmula que você escreveu é válida para todo $n \geq 1$.

Exercício 3.6 *Fazer como no exercício acima para* $S_n = 1/3 + 1/15 + ... + 1/(4n^2 - 1)$.

Exercício 3.7 *Fazer como no exercício acima para* $S_n = 1 + 3 + 5 + ... + (2n - 1)$.

A indução para a justificação de desigualdades.

Exemplo 3.5 *Para todo* $n \in \mathbb{N}$*, valem: a)* $1 \leq 2^n$ *e b)* $n < 2^n$.

a) Fica como exercício.

b) Se $n = 0$*, então* $0 < 1 = 2^0$*. Assumamos, pela hipótese de indução, que* $n < 2^n$*, para* $n \in \mathbb{N}$*. Daí, devemos verificar que* $n + 1 < 2^{n+1}$:
$n + 1 < 2^n + 1 \leq 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$*. Logo,* $n < 2^n$ *para todo* $n \in \mathbb{N}$.

Exercício 3.8 *Encontrar o menor valor para* $\star$ *e Demonstrar as desigualdades:*
(a) $n! > 2^n$*, para todo* $n > \star$ *;*
(b) $2^n > 2n + 1$*, para todo* $n > \star$ *;*
(c) $2^n > n^2$*, para todo* $n > \star$ *;*
(d) $3n^2 - n > 20$*, para todo* $n > \star$.

Exercício 3.9 *Usar o princípio da boa ordem para mostrar que não existe inteiro m tal que $0 < m < 1$. Sugestão: Observar que $0 < n < 1 \Rightarrow 0 < n^2 < n$.*

A divisibilidade será detalhada no Capítulo 4, mas como exemplo de aplicação da indução matemática, façamos aqui uma breve introdução.

Dizemos que a *divide* b ou que b é *múltiplo* de a se existe $q \in \mathbb{Z}$ tal que $b = aq$.

Exemplo 3.6 *Para todo $n \in \mathbb{N}$, $2^{2n} - 1$ é múltiplo de 3.*

Se $n = 0$, então $2^{2.0} - 1 = 0$ e como $3 \cdot 0 = 0$, então $2^{2.0} - 1$ é múltiplo de 3.

Por hipótese de indução, assumamos que para $0 \leq k$, vale que $2^{2k} - 1$ é múltiplo de 3, isto é, $2^{2k} - 1 = 3q$. Daí, $2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 2^2 \cdot 2^{2k} - 1 = 4(3q + 1) - 1 = 12q + 3 = 3(4q + 1)$. Desde que $4q + 1 \in \mathbb{N}$, então $2^{2(k+1)} - 1$ é múltiplo de 3.

Exercício 3.10 *Demonstrar que para todo $n \in \mathbb{N}$, $n^3 + 2n$ é múltiplo de 3.*

A indução matemática pode ser usada para mostrar resultados da Geometria tais como os seguintes.

Exercício 3.11 *Mostrar que a soma, em graus, das medidas dos ângulos internos de um polígono convexo de n lados é $(n - 2) \cdot 180^o$, sabendo que a soma dos ângulos internos de um triângulo é 180^o.*

Exercício 3.12 *Mostrar que o número de diagonais de um polígono convexo de n lados é dado por $d_n = n(n - 3)/2$.*

Na Aritmética podemos, pela indução matemática, mostrar propriedades tais como a distributividade.

Exemplo 3.7 *Em* $(\mathbb{N}, +, \cdot, 0, 1)$ *vale a lei distributiva:* $m \cdot (n + p) = m \cdot n + m \cdot p$. *Lembrando que, por definição,* $m(q + 1) = mq + m$ *para quisquer naturais* m *e* q.

A justificação é por indução sobre p. *Consideremos o conjunto* $B = \{p \in \mathbb{N} : m \cdot (n + p) = (m \cdot n) + (m \cdot p)\}$. *Facilmente verificamos que* $0 \in B$, *pois* $m \cdot (n + 0) = m \cdot n = (m \cdot n) + 0 = (m \cdot n) + (m \cdot 0)$. *Agora, suponhamos que* $p \in B$. *Então:* $m \cdot (n + (p + 1)) = m \cdot ((n + p) + 1) = (m \cdot (n + p)) + m = (m \cdot n + m \cdot p) + m = m \cdot n + (m \cdot p + m) = m \cdot n + m \cdot (p + 1)$. *Logo* $p + 1 \in B$ *e, assim,* $B = \mathbb{N}$.

Resolver, por indução matemática, os dois exercícios seguintes da Lógica e da Teoria dos Conjuntos.

Exercício 3.13 *Na lógica proposicional clássica dizemos que uma fórmula tem* forma restrita *se ela envolve apenas os conectivos* $\neg, \wedge, \vee$. *Seja* A *uma fórmula proposicional restrita. Se* A' *é obtida a partir de* A *pela permutação de* $\wedge$ *por* $\vee$, *de* $\vee$ *por* $\wedge$ *e de cada proposição atômica por sua negação, então* A' *é logicamente equivalente a* $\neg A$.

Exercício 3.14 *Sejam* $A_1, A_2, ..., A_n$, n *conjuntos e* $2 \leq n$. *Mostrar que vale a lei de De Morgan:* $(A_1 \cap A_2 \cap ... \cap A_n)^C = {A_1}^C \cup {A_2}^C \cup ... \cup {A_n}^C$.

3.3 Fatorial, números binomiais e triângulo de Pascal

A indução permite a definição de alguns conceitos interessantes e usuais.

O *fatorial* de um número natural n é definido por recursão como:

(i) $0! = 1$

(ii) $(n+1)! = (n+1) \cdot n!$, para $n \geq 0$.

Assim, $n! = \begin{cases} 1 & se\ n = 0 \\ 1 \cdot 2 \cdot \ldots \cdot n & se\ n > 0 \end{cases}$

Exercício 3.15 *Demonstrar por indução que:*
$1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + ... + n \cdot n! = (n+1)! - 1$, *para todo* $n \in \mathbb{N}^*$.

Se $n, k \in \mathbb{N}$ e $n \geq k$, o *número binomial* de n e k é definido por: $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$.

O número binomial corresponde, na análise combinatória, ao número de combinações de n elementos tomados k a k.

Exercício 3.16 *Demonstrar que:*
(a) $\binom{n}{n} = \binom{n}{0} = 1$; *(b)* $\binom{n}{1} = \binom{n}{n-1} = n$;
(c) $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$; *(d)* $\binom{n}{k} = \binom{n}{n-k}$;

(e) Se A é um conjunto com n elementos, então $\binom{n}{k}$ *é a quantidade de subconjuntos de A que possuem k elementos;*
(f) $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ *para todo* $n \in \mathbb{N}$; *(observe que*

$\sum_{k=m}^{n} a(k) = \sum_{k=m+1}^{n+1} a(k-1)$ *e* $\sum_{k=m}^{n} a(k) = \sum_{k=m-1}^{n-1} a(k+1)$

(g) $\sum_{k=0}^{n} k\binom{n}{k} = n \cdot 2^{n-1}$ *para todo* $n \in \mathbb{N}^*$*;*

Se $x, y \in \mathbb{R}^*$ *e* $n \in \mathbb{N}^*$*, então*

(h) $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k$*; (Binômio de Newton)*

(i) Usar o item anterior para desenvolver $(x-y)^n$ *e* $(x+2)^4$*;*

(j) Para $x,\ y \in \mathbb{Z}^*$*, existem* $a, b \in \mathbb{Z}$ *tais que* $(x+y)^n = ax + y^n$ *e* $(x-y)^n = bx + (-1)^n.y^n$*;*

(k) Para $x,\ y \in \mathbb{Z}^*$*, existem* $a,\ b \in \mathbb{Z}$ *tais que* $(x+1)^n = ax + 1$ *e* $(x-1)^n = bx + (-1)^n$*;*

(l) $x^n - y^n = (x-y)\sum_{k=1}^{n} x^{n-k}y^{k-1}$,

$x^{2n} - y^{2n} = (x+y)\sum_{k=1}^{2n} x^{2n-k}y^{k-1}(-1)^{k-1}$ *e*

$x^{2n+1} + y^{2n+1} = (x+y)\sum_{k=0}^{2n} x^{2n-k}y^k(-1)^k$*;*

(m) $x^n - 1 = (x-1)\sum_{k=1}^{n} x^{n-k}$,

$x^{2n} - 1 = (x+1)\sum_{k=1}^{2n} x^{2n-k}(-1)^{k-1}$ *e*

$x^{2n+1} + 1 = (x+1)\sum_{k=0}^{2n} x^{2n-k}(-1)^k$*;*

(n) Encontrar $p(x,y)$ *e* $q(x,y)$ *tais que* $x^5 + y^5 = (x-y)\cdot p(x,y)$ *e* $x^6 - 1 = (x+1)\cdot q(x,y)$.

A figura seguinte apresenta os números binomiais numa ordem em forma de triângulo que é conhecida como *Triângulo de Pascal*.

$$\begin{array}{c} \binom{0}{0} \\ \binom{1}{0}\ \binom{1}{1} \\ \binom{2}{0}\ \binom{2}{1}\ \binom{2}{2} \\ \binom{3}{0}\ \binom{3}{1}\ \binom{3}{2}\ \binom{3}{3} \end{array}$$

$$\cdots$$

$$\begin{array}{c} \binom{n}{0}\ \binom{n}{1} \cdots \binom{n}{k-1}\ \binom{n}{k} \cdots \binom{n}{n-1}\ \binom{n}{n} \\ \binom{n+1}{0}\ \binom{n+1}{1} \cdots \binom{n+1}{k-1}\ \binom{n+1}{k} \cdots \binom{n+1}{n-1}\ \binom{n+1}{n}\ \binom{n+1}{n+1} \end{array}$$

No Triângulo de Pascal, a n-ésima linha fornece os coeficiente do termo $(x+y)^{(n-1)}$, para $n \in \{1,2,3,4,...\}$. Observe que a linha $n+1$ pode ser obtida da linha n, pois $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$ e também $\binom{n}{k-1}$ e $\binom{n}{k}$ estão acima de $\binom{n+1}{k}$ à esquerda e à direita. Por exemplo, a terceira linha fornece os coeficientes para $(x+y)^2 = x^2+2xy+y^2$, como podemos observar no Triângulo de Pascal dado abaixo:

$$\begin{array}{c} 1 \\ 1\ \ 1 \\ 1\ \ 2\ \ 1 \\ 1\ \ 3\ \ 3\ \ 1 \\ 1\ \ 4\ \ 6\ \ 4\ \ 1 \\ 1\ \ 5\ \ 10\ \ 10\ \ 5\ \ 1 \end{array}$$

$$\cdots$$

3.4 A indução matemática e a indução de Hume

A expressão indução é entendida no contexto científico como um tipo característico de procedimento inferencial.

Inferência deve ser entendido como o processo pelo qual se obtém uma conclusão a partir de uma coleção de dados. Esses dados recebem, em geral, o nome de *premissas*. Na Matemática é mais usual o nome *hipóteses*.

A inferência dedutiva, que é própria da Lógica e da Matemática, tem a característica de conduzir premissas verdadeiras para uma conclusão verdadeira. Se não for assim, a dedução está mal feita.

Nas ciências naturais, também precisamos dos procedimentos inferenciais, contudo as inferências dedutivas não dão conta de todas as possibilidades e necessidades. Surge dessa necessidade um outro tipo de inferência, chamada *inferência indutiva* ou *indução*.

A indução é também conhecida como indução de Hume, por ser este pensador britânico um dos primeiros homens a refletir e caracterizar a inferência indutiva.

Na indução, a veracidade das premissas não garante a conclusão, mas apenas apontam que ela provavelmente deva ser válida. Por exemplo, como todas as zebras que conhecemos são listradas, entendemos que as zebras são listradas. Mas isto não é uma verdade necessária, é apenas uma inferência indutiva, pois podemos eventualmente encontrarmos uma zebra não listrada. Também é uma conclusão indutiva a sentença 'o sol nascerá amanhã'.

A indução estabelece uma conexão entre afirmações que valem para um número finito de casos e o conjunto de todos os casos, que em algumas situações pode ser infinito.

Por exemplo, como em condições normais temos avaliado que toda porção de água ferve aos 100^o Célsius, então concluímos que a água ferve aos 100^o. Contudo, há sempre a possibilidade de alguma situação que venha contradizer essa conclusão. A avaliação de inúmeros casos, mesmo uma quantidade muito grande de casos, não é suficiente para a garantia da validade de todos os casos. Como na Estatística, o que pode-se afirmar é que provavelmente a conclusão seja verdadeira. Apenas isto.

Assim, temos uma distinção enorme entre a indução matemática que é um procedimento dedutivo, enquanto a indução de Hume, própria das ciências da natureza, a qual faz uma generalização da parte para o todo, não é dedutiva.

4 Divisibilidade e algoritmo da divisão

Nesse capítulo tratamos da divisibilidade entre números inteiros, suas características, particularidades e propriedades. Para tanto, iniciamos com a definição da relação de divisibilidade.

4.1 Divisibilidade

Se $a, b \in \mathbb{Z}$, com $a \neq 0$, então a *divide* b se existe $c \in \mathbb{Z}$ tal que $b = c.a$.

De acordo com a definição acima, dizemos também que a é um *divisor* de b ou que b é um *múltiplo* de a ou que b é *divisível* por a.

O inteiro c que ocorre na definição acima é único, pois se $b = c.a$ e $b = d.a$, então $c.a = d.a$ e, daí, como $a \neq 0$, então $d = c$.

Diante disso, dizemos que c é o *quociente* da divisão de b por a e denotamos isso por $c = \dfrac{b}{a}$.

Exemplo 4.1 *O inteiro* 7 *divide* 14*, pois* $14 = 2 \cdot 7$*;* -7 *divide* 14*, pois* $14 = (-2)\cdot(-7)$*. Nesse caso, temos que* $2 = \dfrac{14}{7}$*,* $7 = \dfrac{14}{2}$*,* $-2 = \dfrac{14}{-7}$ *e* $-7 = \dfrac{14}{-2}$*.*

Exemplo 4.2 *O inteiro* 5 *divide* 0*, pois* $0 = 0\cdot 5$*. De forma mais geral, para todo* $n \in \mathbb{Z}^*$*, temos que* n *divide* 0*, pois* $0 = 0 \cdot n$*.*

Exemplo 4.3 *O inteiro* 1 *divide* n*, para todo* $n \in \mathbb{Z}$*, pois* $n = 1 \cdot n$*.*

Exemplo 4.4 *Para qualquer* $n \in \mathbb{Z}^*$*,* n *divide* n*, pois* $n = 1 \cdot n$*.*

Exemplo 4.5 *Desde que* $12 = 2 \cdot 6 = 3 \cdot 4 = 1 \cdot 12 = (-1) \cdot (-12) = ...$, *então os números* $1, -1, 2, -2, 3, -3, 4, -4, 6, -6, 12$ *e* -12 *dividem* 12.

Denotamos a relação de divisibilidade por $a|b$ com o sentido de a divide b e quando a não divide b, denotamos por $a \nmid b$. Assim, $a|b \Leftrightarrow b = c.a$, para algum $c \in \mathbb{Z}$.

Exemplo 4.6 *Segue das considerações anteriores que* $4|20$, *pois* $20 = 4 \cdot 5$.

Se $a|b$, então $a|(-b)$, $(-a)|b$ e $(-a)|(-b)$, pois se $b = c.a$, então $b = (-c).(-a)$ e $-b = (-c).a = c.(-a)$.

Teorema 4.1 *Sejam* $a, b, c \in \mathbb{Z}$.

(i) Se $a|b$ *e* $a|c$, *então* $a|(b + c)$;

(ii) Se $a|b$, *então* $a|bc$;

(iii) Se $a|b$ *e* $a|c$, *então* $a|(rb + sc)$, *para todos* $r, s \in \mathbb{Z}$;

(iv) Se $a|b$ *e* $b > 0$, *então* $a \leq b$;

(v) Se $ab = 1$, *então* $a = 1$ *ou* $a = -1$;

(vi) Se $a|b$ *e* $b|a$, *então* $a = b$ *ou* $a = -b$;

(vii) Se $ab|ac$ *e* $a \neq 0$, *então* $b|c$;

(viii) Se $0 < a < b$ *então* $b \nmid a$.

Demonstração: *(i) Se* $a|b$ *e* $a|c$, *então existem* $d, e \in \mathbb{Z}$ *tais que* $b = da$ *e* $c = ea$. *Logo,* $b + c = da + ea = (d + e)a$ *e, portanto,* $a|(b + c)$;

(ii) Se $a|b$, *então existe* $d \in \mathbb{Z}$ *tal que* $b = ad$. *Logo,* $bc = adc$ *e, portanto,* $a|bc$;

(iii) Se $a|b$ *e* $a|c$, *então, por (ii),* $a|rb$ *e* $a|sc$, *para quaisquer* $r, s \in \mathbb{Z}$. *Logo, por (i),* $a|(rb + sc)$.

(iv) Como $a|b$, *então* $b = ac$, *para algum* $c \in \mathbb{Z}$. *Se* $a < 0$, *como* $0 < b$ *então* $a < b$. *Se* $a > 0$, *como* $b > 0$, *então* $c > 0$. *Logo*

$c \geq 1$ e, portanto, $b = ac \geq a1 = a$;
(v) Se $a > 0$, como $ab = 1$, então, por definição, $a|1$. Logo, por (iv), $a \leq 1$, isto é, $0 < a \leq 1$ e, portanto, $a = 1$. Se $a < 0$, então $-a > 0$. Como $(-a)(-b) = ab = 1$, do mesmo modo, temos $-a = 1$ e, portanto, $a = -1$. ∎

Observar que, pelo item (v) do teorema anterior, os únicos divisores de 1 são 1 e -1.

Exercício 4.1 *Fazer os ítens (vi), (vii) e (viii) do teorema acima.*

Teorema 4.2 *Sejam $a, b, c \in \mathbb{Z}$. Então:*
(i) se $a|b$ e $b|c$, então $a|c$;
(ii) $a|b$ se, e somente se, $a|(a + b)$;
(iii) se $a|b$ e $a|(b + c)$, então $a|c$;
(iv) se $a|b$ e $a \nmid c$, então $a \nmid (b + c)$.

Exercício 4.2 *Demonstrar o Teorema* 4.2.

4.2 O Algoritmo da divisão de Euclides

O algoritmo da divisão, como veremos, garante que se n e d são inteiros e $d \neq 0$, então podemos dividir n por d obtendo um único quociente q e um único resto r, em que $0 \leq r < d$. No teorema a seguir, temos o caso $d > 0$. O caso $d < 0$ é deixado como exercício.

Teorema 4.3 *(Algoritmo da Divisão de Euclides) Sejam $n, d \in \mathbb{Z}$, com $d > 0$. Então existem e são únicos $q, r \in \mathbb{Z}$ tais que $n = qd + r$ e $0 \leq r < d$.*
Demonstração: *(Existência)*

Consideremos inicialmente $n \geq 0$. Faremos a demonstração por indução e usaremos o PFI sobre n.
Para $n = 0$, temos que $n = 0 \cdot d + 0$ e, portanto $q = 0 = r$.
Pela hipótese de indução, consideremos que dado $n > 0$, o enunciado vale para todo natural m, com $m < n$.
Se $0 < n < d$, basta tomarmos $q = 0$ e $r = n$, isto é, $n = 0 \cdot d + n$.
Agora, se $n \geq d$. Como $n \geq d > 0$, então $n > n - d \geq 0$. Pela hipótese de indução, $n - d = qd + r$, com q, r inteiros positivos e $0 \leq r < d$. Assim, $n = n - d + d = qd + r + d = (q + 1)d + r$, ou seja, o algoritmo vale para n. Logo, pelo PFI, fica provada a existência de q e r, para $n \geq 0$.

Agora consideramos o caso $n < 0$. Desse modo $-n > 0$ e, portanto, $-n = qd + r$, com $0 \leq r < d$. Logo, $n = (-q)d - r$. Se $r = 0$, então $n = (-q)d + r$. Se $r > 0$, então $n = (-q)d - d + d - r = (-q - 1)d + (d - r)$ e $0 \leq d - r < d$.

Vamos demonstrar agora a unicidade de q e de r.

Sejam $n = qd + r$ e $n = q'd + r'$, com $q, q' \in \mathbb{Z}$ e r, r' inteiros positivos com $0 \leq r, r' < d$. Podemos supor, sem perda de generalidade, que $r' \leq r$. Nesse caso, $0 \leq r - r' = n - qd - (n - q'd) = (q' - q)d$, ou seja, $d|(r - r')$. Mas $0 \leq r - r' < d - r' \leq d$. Assim, $d|(r - r')$ e $0 \leq r - r' < d$. Logo, pelo Teorema 4.1 (iv), $r - r' = 0$, ou seja, $r = r'$. Temos então $0 = r - r' = (q' - q)d$. Como $d \neq 0$, então $q' - q = 0$ e, portanto, $q = q'$. ∎

Nas condições do teorema anterior, dizemos que q é o *quociente* e r é o *resto* da divisão de n por d.

Exemplo 4.7 *Temos que $20 = 3 \cdot 6 + 2$ e $-20 = (-4) \cdot 6 + 4$, ou seja, o resto da divisão de 20 por 6 é 2 e o resto da divisão de -20 por 6 é 4.*

Corolário 4.4 *Dados os números inteiros n e d, com $d > 0$.*

Então $d|n$ se, e somente se, o resto da divisão de n por d é zero.

Demonstração: ($\Rightarrow$) *Se $d|n$, então existe $q \in \mathbb{Z}$ tal que $n = qd = qd + 0$. Logo, o resto da divisão de n por d é zero.*
($\Leftarrow$) *Pelo algoritmo da divisão, existem e são únicos $q, r \in \mathbb{Z}$, com $0 \leq r < d$ tais que $n = qd + r$. Como, por hipótese, $r = 0$, então, $n = qd$, ou seja, $d|n$.* ∎

Exemplo 4.8 *O inteiro $4 \nmid 21$, pois $21 = 5 \cdot 4 + 1$, ou seja, o resto da divisão de 21 por 4 é 1.*

Exercício 4.3 *Mostrar que:*
(a) $2 \nmid 5$ *(b)* $3 \nmid 10$ *(c)* $4 \nmid 6$ *(d)* $2|6$ *(e)* $4|60$.

Exercício 4.4 *Verificar se cada afirmação abaixo é verdadeira ou falsa, e apresentar uma dedução ou um contra-exemplo.*
(a) Se $a|b$ e $c|d$, então $ac|bd$;
(b) Se $a|b$ e $c|d$, então $(a + c)|(b + d)$;
(c) Se $a|b$, então $b|a$;
(d) Se $a|bc$, então $a|b$ ou $a|c$;
(e) Se $a|(b + c)$, então $a|b$ ou $a|c$.

Dado um inteiro n, segundo o algoritmo da divisão, o resto r da divisão de n por 2 é 0 ou 1. Dizemos que n é *par* se $r = 0$ e n é *ímpar*, se $r = 1$.

Exercício 4.5 *Mostrar que:*
(a) a soma de dois pares é um par;
(b) a soma de dois ímpares é um par;
(c) a soma de um par com um ímpar é um ímpar;
(d) o produto de dois ímpares é um número ímpar;
(e) se m é par, então $m \cdot n$ é par;

(f) se dois números são consecutivos, então um é par e o outro é ímpar;
(g) se a é par e $n > 0$, então a^n é par;
(h) se a é ímpar e $n \geq 0$, então a^n é ímpar;
(i) quaisquer que sejam $a, m, n \in \mathbb{N}^*$, tem-se que $a^m + a^n$ é par;
(j) para qualquer inteiro a, $1 + 2a + a^2 - 5a^3$ é ímpar.

Exercício 4.6 *Sejam $m, n, r \in \mathbb{N}$ tais que $n > 1$, $0 \leq r < n$ e $n|m - r$. Mostrar que r é o resto da divisão de m por n.*

Exercício 4.7 *Se o resto da divisão de um inteiro n por 12 é 7, então:*
(a) qual o resto da divisão de $2n$ por 12?
(b) qual o resto da divisão de $-n$ por 12?
(c) qual o resto da divisão de n por 4?
(d) qual o resto da divisão de n^2 por 8?

Exercício 4.8 *Mostrar que se três números inteiros são consecutivos, então um deles é divisível por 3.*

Exercício 4.9 *Dado $a \in \mathbb{Z}$, mostrar que a ou $a + 2$ ou $a + 4$ é divisível por 3.*

Exercício 4.10 *Mostrar que se a é ímpar, então $8|(a^2 - 1)$.*

Exercício 4.11 *Mostrar que se a e b são ímpares, então $8|(a^2 - b^2)$.*

Exercício 4.12 *Mostrar que $(n - 1)^3 - n^3$ é ímpar, para qualquer inteiro n.*

Exercício 4.13 *Encontrar os possíveis inteiros n tais que o resto da divisão de n por 3 seja:*

(a) igual ao quociente;
(b) a metade do quociente;
(c) o dobro do quociente.

Exercício 4.14 *Se n é um inteiro que não é divisível por 3, mostrar que:*
(a) n^2 deixa resto 1 quando dividido por 3;
(b) $2n^2 + 1$ é divisível por 3;
(c) Se $m^2 + n^2$ é múltiplo de 3, então m e n são múltiplos de 3.

Exercício 4.15 *Mostrar que se a é um inteiro, então:*
(a) a^2 deixa resto 0 ou 1, quando dividido por 4;
(b) a^3 deixa resto 0, 1 ou 8, quando dividido por 9.

Exercício 4.16 *(Algoritmo da divisão para inteiros) "Sejam $n, d \in \mathbb{Z}$, com $d \neq 0$. Então existem e são únicos $q, r \in \mathbb{Z}$ tais que $n = qd + r$, com $0 \leq r < |d|$". Encontrar q e r para $n = -4$ e $d = -3$.*

5 Bases de numeração e representação

5.1 Introdução

Ao escrevermos um numeral, precisamos reconhecer em que base de numeração estamos trabalhando. Embora seja usual o tratamento com a base decimal, outras bases podem ser consideradas. Particularmente na computação, a base binária tem uma importância crucial.

Existem algumas maneiras diversas para representarmos um número inteiro. Por exemplo, o número 425, segundo a base decimal, significa 5 unidades, duas dezenas e quatro centenas, ou seja, 425 é a abreviação de $4 \cdot 10^2 + 2 \cdot 10 + 5$. De maneira semelhante, podemos representar 425 como $6 \cdot 8^2 + 5 \cdot 8 + 1$, isto é, usamos potências de 8 no lugar de potências de 10 e, considerando o número 8 como base para um sistema de numeração, temos que $(425)_{10} = (651)_8$, de modo que o sub-índice indica a base do sistema. Em ambos os casos, o que determina o valor do número é a posição dos algarismos. Por isso, sistemas desse tipo são chamados *sistemas posicionais*. Veremos que num sistema posicional com base a, em que a é inteiro maior que 1, todo número natural b pode ser escrito de modo único na forma $b = r_n.a^n + r_{n-1}.a^{n-1} + ... + r_1.a^1 + r_0.a^0$, com $0 \leq r_i < a$, para todo i. Esse número é representado por $(r_n r_{n-1} ... r_1 r_0)_a$. Assim, são necessários a algarismos $\{0, 1, ..., a-1\}$ para descrevermos os números na base a. Um dentre os mais antigos sistemas posicionais conhecidos é o sexagesimal (com 60 unidades), que surgiu na Babilônia por volta de 1800 a.C. Ainda reconhecemos alguns vestígios deste sistema de numeração na divisão da hora em 60 minutos, e na medida da circunferência em 360 graus, vinculados aos estudos astronômicos dos babilônios. Existem outros siste-

mas, como o vigesimal (com 20 unidades) usado pelos Maias da América Central. Também identificamos traços de um sistema vigesimal na língua francesa: 80 é designado por *quatre vingts*, literalmente, quatro vintes. Do sistema duodecimal (doze unidades) temos em uso a dúzia. No sistema de medidas inglês, 1 'pie' é igual a 12 polegadas, e no sistema monetário, 1 'chilin' equivale a 12 'pences'. O exemplo mais conhecido de sistema não posicional é o sistema romano. Este sistema tem uma coleção determinada de símbolos principais - unidade I, cinco V, dez X, cinquenta L, cem C, etc. ... - e todo número é representado como combinação destes símbolos. Por exemplo, o número 97 tem como numeral romano XCVII.

5.2 Representação de inteiros em uma base

Teorema 5.1 *(Representação na base a) Sejam* $a, b \in \mathbb{N}$ *e* $1 < a$. *Se* $b \neq 0$, *então existem* $r_0, r_1, ..., r_n \in \mathbb{N}$ *tais que* $b = r_n \cdot a^n + r_{n-1} \cdot a^{n-1} + ... + r_1 \cdot a + r_0$ *em que* $n \in \mathbb{N}$ *e, para todo* i, $0 \leq r_i < a$ *e* $r_n \neq 0$. *Esta representação de* b *é única.*

Demonstração: *(Existência)*

Se $b < a$, *basta tomarmos* $b = r_0$. *Agora, se* $b \geq a$, *faremos um processo indutivo para obter a representação.*

(1) *Seja* $q_0 = b$ *e* (2) *a partir de* q_i, *pelo algoritmo da divisão, obtemos* q_{i+1} *e* r_i, *tais que* $q_i = q_{i+1} \cdot a + r_i$, *com* $q_{i+1}, r_i \in \mathbb{N}$ *e* $0 \leq r_i < a$. *Observemos que* $q_{i+1} \cdot a = q_i - r_i \leq q_i$. *Logo, se* $q_i \neq 0$ *então* $q_{i+1} < q_i$, *pois* $q_{i+1} = 0$ *ou caso* $q_{i+1} > 0$, *sendo* $1 < a$, $q_{i+1} < q_{i+1} \cdot a = q_i - r_i \leq q_i$. (3) *Quando* $q_{i+1} \neq 0$, *repetimos o passo* (2). *Quando* $q_{i+1} = 0$, *o processo está terminado pois:*

$$b = q_0 = q_1 \cdot a + r_0$$
$$q_1 = q_2 \cdot a + r_1$$
$$q_2 = q_3 \cdot a + r_2$$

$$\vdots$$

$$q_{i-1} = q_i \cdot a + r_{i-1}$$

$$q_i = 0 \cdot a + r_i.$$

Assim, $b = q_1 \cdot a + r_0 = (q_2 \cdot a + r_1) \cdot a + r_0 = q_2 \cdot a^2 + r_1 \cdot a + r_0 = (q_3 \cdot a + r_2) \cdot a^2 + r_1 \cdot a + r_0 = q_3 \cdot a^3 + r_2 \cdot a^2 + r_1 \cdot a + r_0 = ... = q_i \cdot a^i + ... + r_1 \cdot a + r_0 = r_i \cdot a^i + ... + r_1 \cdot a + r_0$*, o que mostra a existência da representação.*

(Unicidade)

Demonstração por indução sobre b*.*

Se $b = 1$*, então* $n = 0$ *e* $r_0 = 1$*. Como hipótese de indução temos: a unicidade vale para todo* $c \in \mathbb{N}$*, com* $1 \leq c < b$*. Agora, se* $b = r_n \cdot a^n + ... + r_1 \cdot a + r_0$ *e* $b = s_m \cdot a^m + ... + s_1 \cdot a + s_0$ *são duas representações de* b*, com* $0 \leq r_i < a$ *e* $0 \leq s_j < a$*, para todos* i *e* j*, então* $(r_n \cdot a^{n-1} + ... + r_1) \cdot a + r_0 = (s_m \cdot a^{m-1} + ... + s_1) \cdot a + s_0$*. Desse modo,* r_0 *e* s_0 *são restos da divisão de* b *por* a *e* $r_n \cdot a^{n-1} + ... + r_1$ *e* $s_m \cdot a^{m-1} + ... + s_1$ *são quocientes da mesma divisão. Logo, pela unicidade do quociente e do resto, segundo o algoritmo da divisão,* $r_0 = s_0$ *e* $r_n \cdot a^{n-1} + ... + r_1 = s_m \cdot a^{m-1} + ... + s_1$*. Se* $s_m \cdot a^{m-1} + ... + s_1 = 0$ *então* $b = r_0 = s_0$*, portanto vale a unicidade. Se* $s_m \cdot a^{m-1} + ... + s_1 \neq 0$*, como* $1 < a$ *então* $s_m \cdot a^{m-1} + ... + s_1 < (s_m \cdot a^{m-1} + ... + s_1) \cdot a \leq (s_m \cdot a^{m-1} + ... + s_1) \cdot a + s_0 = b$*, então* $s_m \cdot a^{m-1} + ... + s_1 < b$*. Pela hipótese de indução,* $n = m$ *e* $r_i = s_i$*, para todo* $i \geq 1$ *e, portanto,* $r_i = s_i$ *para todo* i*. Assim, pelo PFI mostramos a unicidade da representação de cada* $b \in \mathbb{N}$*.* ∎

Na demonstração do teorema anterior, podemos observar que $b = (r_i \ r_{i-1} \ldots r_1 \ r_0)_a$ e a sequência $r_i, r_{i-1}, ..., r_1, r_0$ é a coluna dos restos tomada de baixo para cima.

Exemplo 5.1 *Escrever* 125 *na base* 2*.*

Para escrevermos números na base 2*, precisamos somente de dois algarismos:* 0 *e* 1*. Vejamos:*

$q_0 = 125 = 62 \cdot 2 + 1$

$q_1 = 62 = 31 \cdot 2 + 0$

$q_2 = 31 = 15 \cdot 2 + 1$

$q_3 = 15 = 7 \cdot 2 + 1$

$q_4 = 7 = 3 \cdot 2 + 1$

$q_5 = 3 = 1 \cdot 2 + 1$

$q_6 = 1 = 0 \cdot 2 + 1$ *(paramos ao chegar no quociente zero).*

Logo, $125 = 62 \cdot 2 + 1 = (31 \cdot 2 + 0)2 + 1 = 31 \cdot 2^2 + 1 = (15 \cdot 2 + 1)2^2 + 1 = 15 \cdot 2^3 + 1 \cdot 2^2 + 1 = (7 \cdot 2 + 1)2^3 + 1 \cdot 2^2 + 1 = ... = 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1$.

Assim, $125 = 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$ *e, portanto,* $(125)_{10} = (1111101)_2$*. Como já observamos,* 1111101 *é a coluna dos restos, segundo o algoritmo da divisão, tomada de baixo para cima.*

Exemplo 5.2 *Escrever* 743 *na base* 8*.*

Na base 8 *precisamos de* 8 *algarismos:* 0, 1, 2, 3, 4, 5, 6 *e* 7*.*

$743 = 92 \cdot 8 + 7$

$92 = 11 \cdot 8 + 4$

$11 = 1 \cdot 8 + 3$

$1 = 0 \cdot 8 + 1$.

Logo, $(743)_{10} = (1347)_8$*, ou seja,* $743 = 1 \cdot 8^3 + 3 \cdot 8^2 + 4 \cdot 8^1 + 7 \cdot 8^0$.

Exemplo 5.3 *Escrever* 743 *na base* 16*.*

Como na base 16 *precisamos de* 16 *algarismos, além dos símbolos* $0, 1, 2, 3, 4, 5, 6, 7, 8$ *e* 9*, tomamos também os símbolos* A, B, C, D, E *e* F*, os quais representam, respectivamente, os*

números $10, 11, 12, 13, 14$ *e* 15 *da base* 10.
$743 = 46 \cdot 16 + 7 = 46 \cdot 16 + 7$
$46 = 2 \cdot 16 + 14 = 2 \cdot 16 + E$
$2 = 0 \cdot 16 + 2 = 0 \cdot 16 + 2$.
Logo, $(743)_{10} = (2E7)_{16}$.

Exercício 5.1 *Fazer programa para computador que realize a operação de mudança de base. Por exemplo, transpor da base decimal para a base* 7.

5.3 Contagem e operações aritméticas

Os números foram inicialmente criados com o propósito de possibilitar a contagem. A contagem de objetos, de componentes de um rebanho, do número de membros de um clã. Apresentamos a seguir a seqüência numérica de contagem em várias bases de numeração, iniciando do zero e adicionando uma unidade em cada passo.
Base 10: 0 1 2 3 4 5 6 7 8 9 10 11 12 ... 19 20 21 22 ... 98 99 100 101 ... 109 110 111 112 ...
Base 2: 0 1 10 11 100 101 110 111 1000 ...
Base 3: 0 1 2 10 11 12 20 21 22 100 101 102 110 ...
Base 5: 0 1 2 3 4 10 11 12 13 14 20 21 ... 43 44 100 ...

A partir da contagem fica relativamente fácil realizarmos a adição de dois números.

$$\begin{array}{rcccccc} & (& 2 & 4 & 3 &)_5 \\ + & (& 2 & 2 & 3 &)_5 \\ \hline (& 1 & 0 & 2 & 1 &)_5 \end{array} \qquad \begin{array}{rcccccccc} & (& 1 & 0 & 1 & 1 & 0 & 1 &)_2 \\ + & (& & 1 & 0 & 1 & 1 & 0 &)_2 \\ \hline (& 1 & 0 & 0 & 0 & 0 & 1 & 1 &)_2 \end{array}$$

Exemplo 5.4 *Operações aritméticas na base* 6. *A partir da*

sequência dos números na base 6*:* 0, 1, 2, 3, 4, 5, 10, 11, 12, 13, 14, 15, 20, 21, ..., *construímos a tabela para a adição:*

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	10
2	2	3	4	5	10	11
3	3	4	5	10	11	12
4	4	5	10	11	12	13
5	5	10	11	12	13	14

A ***adição*** *de dois números: é feita do mesmo modo como na adição no sistema decimal:* $(4254)_6 + (5423)_6 = (14121)_6$.

Regra: Somamos primeiro as unidades e, depois, os algarismos da ordem seguinte, e assim por diante. No caso da base 6, $4 + 3 = 11$, *isto é, coloca-se* 1 *no resultado e acresce-se* 1 *na ordem seguinte.:*

$$\begin{array}{rr} & (4254)_6 \\ + & (5423)_6 \\ \hline & (14121)_6 \end{array}$$

Construímos também uma tabela para a multiplicação dos algarismos na base 6*:*

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	10	12	14
3	0	3	10	13	20	23
4	0	4	12	20	24	32
5	0	5	14	23	32	41

*A **multiplicação** de dois números: é feita pelo mesmo procedimento da multiplicação do sistema decimal:*

$$\begin{array}{r} (352)_6 \\ \times (5)_6 \\ \hline (3124)_6 \end{array}$$

*A **subtração** e a **divisão**: também seguem os algoritmos do sistema decimal:*

$$\begin{array}{rcccccc} & (3 & 0 & 1 & 5 & 2)_6 \\ - & (2 & 1 & 2 & 3 & 4)_6 \\ \hline & (0 & 4 & 5 & 1 & 4)_6 \end{array}$$

$$\begin{array}{rcccc} (1 & 4 & 0 & & 1)_6 \\ 1 & 2 & & & \\ & 2 & 0 & & \\ & 2 & 0 & & \\ & & 0 & & 1 \\ & & & & 0 \\ & & & & (1)_6 \end{array} \qquad \begin{array}{c|ccc} & (4)_6 & & \\ \hline (2 & 3 & & 0)_6 \end{array}$$

5.4 Breves comentários

O *sistema decimal* foi desenvolvido pelos astrônomos calculistas hindus dentre os quais destacam-se Bâhskara I e Yinabhadra Gani, por volta do ano 500 d.C. Foi adotado pelos islâmicos por volta de 825 d.C., particularmente, pelo matemático árabe Al Khawarismi. No início do Século XII, o monge inglês Adelard de Beth traduziu o livro de Al Khawarismi para o latim. O sistema numérico usado na Europa, até então, era o

romano e o conflito entre estes dois sistemas terminou no século XVI com a supremacia do modelo hindu-arábico.

O termo algarismo surgiu como homenagem ao matemático árabe Al Khawarismi e, naturalmente, o sistema Hindu-arábico é decimal pois sua base é constituída dos 10 algarismos $0, 1, 2, 3, 4, 5, 6, 7, 8$ e 9 e é apresentado na forma posicional. Considera-se, tradicionalmente, que a enorme evidência do sistema decimal esteja associada ao uso de partes do corpo humano como instrumentos de contagem, os 10 dedos das mãos (ou dos pés).

Para uma noção da utilidade do sistema binário, consideremos um medidor usual de luz. Ele é composto de vários relógios com 10 posições distintas e ponteiros que giram sobre estas dez posições. Se quiséssemos um contador numa base n, precisaríamos de n posições no relógio. Um medidor composto por relógios, ou outro processo mecânico qualquer, é relativamente lento para mudar de posição, e seria pouco prático usarmos tais medidores para a realização de milhares de operações aritméticas por segundo. Devido a isso, nos computadores convencionais são utilizados semi-condutores por onde uma corrente elétrica pode passar (quando o circuito está fechado) ou não (quando o circuito está aberto). Assim, associa-se o algarismo 0, quando não passa corrente, e 1 quando passa. Por ser um sistema eletrônico, e não mecânico, a mudança de estado aberto-fechado é operada em velocidade altíssima, permitindo a realização de operações aritméticas com velocidades muito grandes. Assim as máquina de Turing/von Neuman, que são os nossos computadores, operam com sistemas binários que traduzem na aritmética a passagem ou não de impulsos elétricos. É justamente a conversão de uma lin-

guagem em outra que possibilita a construção dos computadores.

Exercício 5.2 *Escrever o número* 128 *nas bases* $2, 4, 7, 8$ *e* 16.

Exercício 5.3 *Escrever os seguintes números na base decimal:* $(1234)_5$, $(1000)_3$, $(127)_{25}$ *e* $(1111111111)_2$.

Exercício 5.4 *Escrever* $(1234)_5$ *na base 6.*

Exercício 5.5 *Fazer uma tabela para a adição e uma para a multiplicação na base 8.*

Exercício 5.6 *Calcular, na base* 8, $(1246)_8 + (4375)_8$, $(1234)_8 \cdot (4321)_8$, $(17432)_8 - (5467)_8$ *e* $(17432)_8$ *dividido por* $(5)_8$.

Exercício 5.7 *Fazer a soma das horas:* $7 : 30 : 27 + 6 : 43 : 39$.

Exercício 5.8 *Determinar quantos múltiplos de* 5 *com* 3 *algarismos existem, se a soma dos algarismos de cada um desses números é igual a* 19.

Exercício 5.9 *Seja abc a representação de um número no sistema decimal, com* $a > c+1$. *Considerando xyz a representação decimal de* $abc - cba$, *mostrar que* $xyz + zyx = 1089$.

Exercício 5.10 *Ao permutarmos os dois algarismos da esquerda de um número com* 3 *algarismos, ele diminui de* 180 *unidades. Ao permutarmos os dois algarismos extremos ele diminui de* 297 *unidades. O que ocorre se permutarmos os dois algarismos da direita?*

6 Critérios de divisibilidade

Existem critérios simples que nos permitem determinar quando um número é divisível por 2, 3, 5, etc. Por exemplo, sem realizar a divisão, podemos concluir que 771 é divisível por 3, mas não é divisível por 2 e nem por 5. O teorema seguinte apresenta alguns desses critérios.

6.1 Alguns critérios

Teorema 6.1 *Se b é um número inteiro positivo cuja expansão decimal é $b = r_n 10^n + r_{n-1}10^{n-1} + ... + r_1 10 + r_0$, em que para todo i, $0 \leq r_i < 10$, isto é, $b = (r_n r_{n-1}...r_1 r_0)_{10}$, então:*

(i) $2|b \Leftrightarrow 2|r_0$;

(ii) $5|b \Leftrightarrow 5|r_0$;

(iii) $3|b \Leftrightarrow 3|(r_n + r_{n-1} + ... + r_0)$;

(iv) $9|b \Leftrightarrow 9|(r_n + r_{n-1} + ... + r_0)$;

(v) $11|b \Leftrightarrow 11|(r_0 - r_1 + r_2 - r_3 + ...)$;

(vi)Para $0 < m \leq n, 2^m|b \Leftrightarrow 2^m|(r_{m-1}10^{m-1} + ... + r_1 10 + r_0)$;

(vii)Para $0 < m \leq n, 5^m|b \Leftrightarrow 5^m|(r_{m-1}10^{m-1} + ... + r_1 10 + r_0)$.

Demonstração:

(i) $b = r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + ... + r_1 \cdot 10 + r_0 = (r_n \cdot 10^{n-1} + r_{n-1} \cdot 10^{n-2} + ... + r_1) \cdot 10 + r_0 = (r_n \cdot 10^{n-1} + r_{n-1} \cdot 10^{n-2} + ... + r_1) \cdot 5 \cdot 2 + r_0$. *Assim,* $b = 2c + r_0$, *com* $c = (r_n \cdot 10^{n-1} + r_{n-1} \cdot 10^{n-2} + ... + r_1) \cdot 5$. *Desse modo:*

($\Rightarrow$) *Se* $2|b$, *como* $2|2c$, *então* $2|(b - 2c) = r_0$.

($\Leftarrow$) *Se* $2|r_0$, *como* $2|2c$, *então* $2|(2c + r_0) = b$.

(ii) A demonstração de (ii) é análoga à prova de (i).

(iii) Observar que para todo $t \in \mathbb{N}$, *temos* $10^t = (9+1)^t = 9^t + \binom{t}{1} \cdot 9^{t-1} + ... + \binom{t}{t-1} \cdot 9 + 1 = [9^{t-1} + \binom{t}{1} \cdot 9^{t-2} + ... + \binom{t}{t-1}] \cdot 9 + 1$, *ou seja,* $10^t = s_t \cdot 9 + 1$ *e* $s_t = 9^{t-1}t + \binom{t}{1} \cdot 9^{t-2} + ... + \binom{t}{t-1}$ *é um número inteiro. Assim,* $b = r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + ... + r_1 \cdot 10 + r_0 = r_n \cdot (9 \cdot s_n + 1) + r_{n-1} \cdot (9 \cdot s_{n-1} + 1) + ... + r_1 \cdot (9 \cdot s_1 + 1) + r_0 = 9 \cdot (r_n \cdot s_n + r_{n-1} \cdot s_{n-1} + ... + r_1 \cdot s_1) + (r_n + r_{n-1} + ... + r_1 + r_0)$. *Portanto,* $b = 9c + (r_n + r_{n-1} + ... + r_1 + r_0)$, *em que* $c = (r_n \cdot s_n + r_{n-1} \cdot s_{n-1} + ... + r_1 \cdot s_1)$. *Assim:*
($\Rightarrow$) *Se* $3|b$, *como* $3|9c$, *então* $3|(b - 9c) = (r_n + r_{n-1} + ... + r_1 + r_0)$.
($\Leftarrow$) *Se* $3|(r_n + r_{n-1} + ... + r_1 + r_0)$, *desde que* $3|9c$, *então* $3|(9c + (r_n + r_{n-1} + ... + r_1 + r_0)) = b$.

(iv) A demonstração de (iv) é praticamente a mesma de (iii), com mudança no final:
($\Rightarrow$) *Se* $9|b$, *como* $9|9c$, *então* $9|(b - 9c) = (r_n + r_{n-1} + ... + r_1 + r_0)$.
($\Leftarrow$) *Se* $9|(r_n + r_{n-1} + ... + r_1 + r_0)$, *como* $9|9c$, *então* $9|(9c + (r_n + r_{n-1} + ... + r_1 + r_0)) = b$.

(v) A prova é análoga à de (iii), fazendo $10^t = (11 - 1)^t$.

(vi) $b = r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + ... + r_1 \cdot 10 + r_0 = (r_n \cdot 10^{n-m} + ... + r_m) \cdot 10^m + (r_{n-1} \cdot 10^{n-1} + ... + r_1 \cdot 10 + r_0) = (r_n \cdot 10^{n-m} + ... + r_m) \cdot 5^m \cdot 2^m + r_{m-1} \cdot 10^{m-1} + ... + r_1 \cdot 10 + r_0$. *Assim,* $b = 2^m \cdot c + r_{m-1} \cdot 10^{m-1} + ... + r_1 \cdot 10 + r_0$, *em que* $c = (r_n \cdot 10^{n-m} + ... + r_m) \cdot 5^m$ *é um inteiro. Desse modo:*
($\Rightarrow$) *Se* $2^m|b$, *como* $2^m|2^m \cdot c$, *então* $2|(b - 2^m \cdot c) = r_{m-1} \cdot 10^{m-1} + ... + r_1 \cdot 10 + r_0$.
($\Leftarrow$) *Se* $2^m|(r_{m-1} \cdot 10^{m-1} + ... + r_1 \cdot 10 + r_0)$, *como* $2|2^m c$, *então* $2|(2^m \cdot c + (r_{m-1} \cdot 10^{m-1} + ... + r_1 \cdot 10 + r_0)) = b$.

(vii) A demonstração de (vii) é análoga à de (vi). ∎

Observar que os itens (i) e (ii) da proposição acima são conseqüência de que 2 e 5 são divisores de 10. Observar que para $m > 1$ nos itens (vi) e (vii), temos critérios de divisibilidade para 4, 8, 16, ..., 25, 125, ...

Existem outros critérios de divisibilidade além dos apresentados no teorema anterior. Alguns deles, por exemplo, para o 7 e para o 13, podem ser encontrados na Revista do Professor de Matemática n. 58, publicada pela Sociedade Brasileira de Matemática.

Exemplo 6.1 $4|1928$*, pois* $4|28$*;*
$8|7808$*, pois* $8|808$*;*
$25|7675$*, pois* $25|75$*;*
$3|123456$*, pois* $3|21 = 1+2+3+4+5+6$*;*
$9 \nmid 123.456$*, pois* $9 \nmid 21 = 1+2+3+4+5+6$*;*
$11 \nmid 123.456$*, pois* $11 \nmid 3 = 6-5+4-3+2-1$;
$11|108.636$*, pois* $11|0 = 6-3+6-8+0-1$.

Exercício 6.1 *(Critérios de divisibilidade da base* 12*): Considerando que os divisores de* 12 *são* 1, 2, 3, 4, 6 *e* 12*, mostrar:*
(a) que um número na base 12 é divisível por 2 *se, e somente se, o algarismo das unidades deste número também é divisível por* 2*;*
(b) o mesmo para os números 3, 4 *e* 6.

Assim, se um número b está escrito na base 12, olhando seu algarismo de unidade, podemos concluir se este número é divisível por 2, 3, 4 ou 6.

Do ponto de vista da Matemática, o sistema numérico duodecimal, sobre a base 12, tem como vantagem sobre o sistema decimal, a maior quantidade de critérios de divisibilidade, dada pelo maior número de divisores da base. Nesse sentido, teria sido

melhor se o homem tivesse 6 dedos em cada mão, em lugar de 5, pois provavelmente estaríamos usando o sistema duodecimal.

O sistema sexagesimal, de base 60, seria mais rico em critérios de divisibilidade, pois os divisores de 60 são 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30 e 60, mas teria uma quantidade muito grande de símbolos para se representar os números nesse sistema. O artifício usado pelos babilônios, usuários de um sistema sexagesimal, era a combinação de alguns algarismos para a representação de outros. Por exemplo, o algarismo 59 era representado como na Figura 1, por 9 unidades e 5 dezenas.

Figura 1: O número 59

Exercício 6.2 *Se* $c = a_0 + a_1.12 + a_2.12^2 + ... + a_n.12^n$ *em que, para cada* i, $0 \leq a_i < 12$, *mostrar que:*
(a) $(a_n...a_1a_0)_{12}$ *é divisível por* $8 \Leftrightarrow (a_1a_0)_{12}$ *é divisível por 8;*
(b) $(a_n...a_1a_0)_{12}$ *é divisível por* $9 \Leftrightarrow (a_1a_0)_{12}$ *é divisível por 9;*
(c) $(a_n...a_1a_0)_{12}$ *é divisível por* $11 \Leftrightarrow (a_0 + a_1 + ... + a_n)_{12}$ *é divisível por* 11*;*
(d) $(a_n...a_1a_0)_{12}$ *é divisível por* $13 \Leftrightarrow (a_0 - a_1 + a_2 - a_3 + ...)_{12}$ *é divisível por* 13*.*

Exemplo 6.2 *Por exemplo, o número* $(233)_{12}$ *é divisível por* 3*, mas não é por* $2, 4$ *e* 6*;* $(40)_{12}$ *é divisível por* $2, 3, 4, 6$*;* $(47)_{12}$ *é divisível por* 11*;* $(827)_{12}$ *é divisível por* 13*.*

7 MDC e MMC

Como o próprio nome indica, o máximo divisor comum deve ser um número que divida alguns outros números e seja o maior entre os tais divisores. De modo semelhante, o mínimo múltiplo comum deve ser múltiplo de alguns números e ser o menor dentre eles.

7.1 Máximo divisor comum - MDC

O máximo divisor comum ou maior divisor comum de dois números receberá, a seguir, uma definição precisa. Como exemplo temos que: os divisores positivos de 36 são: 1, 2, 3, 4, 6, 9, 12, 18 e 36; os divisores positivos de 42 são 1, 2, 3, 6, 7, 14, 21 e 42. Assim, o máximo divisor comum de 36 e 42 é 6. A seguir, formalizamos o conceito.

Sejam $a, b \in \mathbb{Z}$, com pelo menos um deles diferente de zero. O *máximo divisor comum* de a e b é um inteiro positivo d tal que:

(i) $d|a$ e $d|b$;

(ii) se $c \in \mathbb{Z}$ é tal que $c|a$ e $c|b$, então $c|d$.

Denotamos o máximo divisor comum de a e b por $mdc(a, b)$. É claro que, existindo $mdc(a, b)$, então $mdc(a, b) = mdc(b, a)$.

A condição (i) diz que d é um divisor de a e b e a condição (ii) garante que d é o maior divisor comum para a e b. Garante também a unicidade do máximo divisor comum, pois se d e d' são máximos divisores comuns de a e b, então $d|d'$ e $d'|d$. Logo, pelo Teorema 4.1, $d = d'$.

A exigência para que $a \neq 0$ ou $b \neq 0$ é devido a que para todo $n \in \mathbb{Z}$, $n|0$ e, daí, não existe o máximo divisor de 0. Porém, se $n > 0$ então $mdc(n, 0) = n$ e $mdc(n, 1) = 1$.

O $mdc(a, b)$ sempre existe, pois se $a \neq 0$ e $b \neq 0$, então, pelo Teorema 4.1, $|a|$ é o maior divisor de a e $|b|$ é o maior divisor de b. Como 1 é um divisor comum de a e b, então $1 \leq mdc(a, b) \leq min\{|a|, |b|\}$. Também, $mdc(a, 0) = |a|$ e $mdc(0, b) = |b|$.

Assim, se $a \in \mathbb{Z}$, então a e $-a$ têm os mesmos divisores, logo, $mdc(a, b) = mdc(-a, b) = mdc(a, -b) = mdc(-a, -b)$, para quaisquer $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. Logo, $mdc(a, b) = mdc(|a|, |b|)$.

Exercício 7.1 *Mostre que*
(i) para qualquer $n \in \mathbb{N}^*$, $mdc(n, n) = n$
(ii) se para $a, b \in \mathbb{N}^*$, $a|b$ *então* $mdc(a, b) = a$

Exemplo 7.1 *Temos que* $mdc(3, 3) = mdc(3, -3) = 3$*;*
$mdc(-1, 5) = mdc(1, 5) = 1$.

Teorema 7.1 *Sejam* $a, b \in \mathbb{Z}$, $a \neq 0$ *ou* $b \neq 0$. *Então* $mdc(a, b)$ *é o menor inteiro positivo da forma* $ra + sb$ *para* $r, s \in \mathbb{Z}$.
Demonstração: *Seja* $M = \{ra + sb : r, s \in \mathbb{Z}\}$. *Claramente* $a, -a, b, -b \in M$ *(por exemplo,* $-a = -1 \cdot a + 0 \cdot b$*). Como* $a \neq 0$ *ou* $b \neq 0$, *então o conjunto* $M_+ = \{m \in M : m > 0\} \neq \emptyset$. *Logo, pelo princípio da boa ordem de* $\mathbb{N}$, M_+ *tem um menor elemento* d. *Desde que* $d \in M$, *então* $d = ra + sb$. *Mostraremos que* $d = mdc(a, b)$.

(i) $d|a$ *e* $d|b$*: Aplicando o algoritmo da divisão para* a *e* d, *segue que existem* $q, r' \in \mathbb{Z}$ *tais que* $a = qd + r'$ *e* $0 \leq r' < d$. *Logo,* $0 \leq r' = a - qd = a - q(ra + sb) = (1 - qr)a + (-qs)b \in M$.

Como d é o menor elemento de M_+ e $0 \leq r' < d$, então $r' = 0$ e, portanto, $a = qd$, ou seja, $d|a$. Analogamente, $d|b$.

(ii) Se $c \in \mathbb{Z}$ é tal que $c|a$ e $c|b$ então, pelo Teorema 4.1, $c|(ra + sb) = d$. Logo, $d = mdc(a, b)$. ∎

Dois números inteiros a e b são *primos entre si* (ou *relativamente primos*) se $mdc(a, b) = 1$.

Teorema 7.2 *Sejam $a, b \in \mathbb{Z}^*$. Se existem $r, s \in \mathbb{Z}$ tais que $ra + sb = 1$, então a e b são primos entre si.*
Demonstração: *Segundo o teorema anterior, $mdc(a, b)$ é o menor inteiro positivo da forma $ra+sb$. Mas, por hipótese, existem $r, s \in \mathbb{Z}$ tais que $ra + sb = 1$ e, assim, $mdc(a, b) = 1$.* ∎

Exemplo 7.2 *Se n é um inteiro positivo, então $mdc(n, n+1) = 1$, pois $(-1)n + 1(n + 1) = 1$.*

Exemplo 7.3 *Se $n \in \mathbb{Z}^*$, então $mdc(n, 1) = 1$, pois $1n + (1 - n)1 = 1$.*

Exercício 7.2 *Se para $n \in \mathbb{Z}$, $a = 4n + 3$ e $b = 5n + 4$, mostrar que $mdc(a, b) = 1$.*

Exercício 7.3 *Mostrar que se o resto da divisão de um inteiro n por 12 é 7, então $mdc(12, n^2) = 1$.*

Exercício 7.4 *Mostrar, através de um exemplo, que $ra+sb = 2$ não implica que $mdc(a, b) = 2$.*

Corolário 7.3 *Se $a, b \in \mathbb{Z}^*$ e $d = mdc(a, b)$, então $mdc(\frac{a}{d}, \frac{b}{d}) = 1$.*
Demonstração: *Pelo Teorema 7.1, existem $r, s \in \mathbb{Z}$ tais que*

$ra + sb = d$. Agora, se dividimos a igualdade por d, então obtemos $r\frac{a}{d} + s\frac{b}{d} = \frac{ra+sb}{d} = \frac{d}{d} = 1$. Logo, pelo Teorema 7.2, $mdc(\frac{a}{d}, \frac{b}{d}) = 1$. ∎

Exemplo 7.4 *Sabendo-se que $mdc(60, 112) = 4$, segue que $mdc(15, 28) = 1$.*

O conceito de máximo divisor comum já era conhecido na antiga Grécia e um algoritmo para sua determinação encontra-se no Livro VII dos Elementos de Euclides. Este algoritmo tem a seguinte estrutura.

Sejam a e b inteiros positivos. Toma-se $a_1 = a$ e $a_2 = b$ e aplica-se o algoritmo da divisão sucessivamente até obter-se o resto zero como no esquema abaixo:
(1) $a_1 = q_1a_2 + a_3$, com $q_1, a_3 \in \mathbb{Z}$ e $0 \leq a_3 < a_2$;
(2) $a_2 = q_2a_3 + a_4$, com $q_2, a_4 \in \mathbb{Z}$ e $0 \leq a_4 < a_3$;
(3) $a_3 = q_3a_4 + a_5$, com $q_3, a_5 \in \mathbb{Z}$ e $0 \leq a_5 < a_4$;
$\vdots$
(j-4) $a_{j-4} = q_{j-4}a_{j-3} + a_{j-2}$, com $q_{j-4}, a_{j-2} \in \mathbb{Z}$ e $0 \leq a_{j-2} < a_{j-1}$;
(j-3) $a_{j-3} = q_{j-3}a_{j-2} + a_{j-1}$, com $q_{j-3}, a_{j-1} \in \mathbb{Z}$ e $0 \leq a_{j-1} < a_{j-2}$.
(j-2) $a_{j-2} = q_{j-2}a_{j-1}$, com $q_{j-1} \in \mathbb{Z}$.

Na linha (j-2) temos que $a_{j-1}|a_{j-2}$, logo, na linha (j-3), $a_{j-1}|a_{j-3}$. Então, na linha (j-4), temos $a_{j-1}|a_{j-4}$ e, continuando o processo, chegamos em $a_{j-1}|a_2 = b$ e $a_{j-1}|a_1 = a$.

Se $c|a = a_1$ e $c|b = a_2$, então, na linha (1), vemos que $c|a_3$, pois $a_3 = a_1 - q_1a_2$. Do mesmo modo, na linha (2), $c|a_4$. Continuando este processo, chegamos a que $c|a_{j-4}$, $c|a_{j-3}$, $c|a_{j-2}$ e $c|a_{j-1}$. Assim $a_{j-1} = mdc(a, b)$, isto é, o último resto

diferente de zero é o máximo divisor comum de a e b.

Notar que $a_2 > a_3 > a_4 > ... \geq 0$, garantindo que em algum momento devemos chegar ao resto zero: $a_j = 0$. Nesse caso, sendo $a_{j-1} \neq 0$, então $a_{j-1} = mdc(a, b)$.

Exemplo 7.5 *Calcular* $mdc(36, 42)$*:*
$42 = 1 \cdot 36 + 6$
$36 = 6 \cdot 6 + 0.$
Logo $mdc(36, 42) = 6.$

Exemplo 7.6 *Calcular* $mdc(238, 630)$ *e encontrar* $r, s \in \mathbb{Z}$ *tais que* $mdc(238, 630) = r \cdot 238 + s \cdot 630.$

$$\begin{aligned} 630 &= 2 \cdot 238 + 154 \quad \Rightarrow \quad 154 = 630 - 2 \cdot 238 \\ 238 &= 1 \cdot 154 + 84 \quad \Rightarrow \quad 84 = 238 - 1 \cdot 154 \\ 154 &= 1 \cdot 84 + 70 \quad \Rightarrow \quad 70 = 154 - 1 \cdot 84 \\ 84 &= 1 \cdot 70 + 14 \quad \Rightarrow \quad 14 = 84 - 1 \cdot 70 \\ 70 &= 5 \cdot 14 + 0 \end{aligned}$$

Logo, $mdc(238, 630) = 14.$

Para encontrarmos r *e* s*, iniciamos o processo na penúltima linha e vamos subindo até chegarmos na primeira, do seguinte modo:* $14 = 84 - 70 = 84 - (154 - 1 \cdot 84) = 2 \cdot 84 - 154 = 2(238 - 1 \cdot 154) - 154 = 2 \cdot 238 - 3 \cdot 154 = 2 \cdot 238 - 3(630 - 2 \cdot 238) = 8 \cdot 238 - 3 \cdot 630$*, ou seja,* $mdc(238, 630) = 14 = 8 \cdot 238 - 3 \cdot 630.$

Exercício 7.5 *Calcular* $mdc(348, 152)$ *e encontrar* r *e* s *como no exemplo anterior.*

Exercício 7.6 *Idem para* $mdc(25, 100)$.

Exercício 7.7 *Para* a, b *e* c *inteiros, mostrar ou dar um contra-exemplo para cada enunciado abaixo:*
(a) $mdc(a, b + c) = mdc(a, b) + mdc(a, c)$*;*

(b) $mdc(a, bc) = mdc(a, b)mdc(a, c)$;
(c) $mdc(a, b)|mdc(a, bc)$;
(d) $mdc(a, b)mdc(c, d) = mdc(ac, bd)$;
(e) $mdc(a, a) = |a|$;
(f) $a|b \Rightarrow mdc(a, c)|mdc(b, c)$;
(g) $a|b$ *e* $b|c \Rightarrow mdc(a, b)|mdc(b, c)$;
(h) $mdc(a, b) = mdc(a^2, b)$;
(i) $mdc(a, b) = 2 \Rightarrow mdc(a, b + 2) = 2$;
(j) $mdc(a, b) = 2 \Rightarrow mdc(a, b + 1) = 1$.
(k) $mdc(a, b) = mdc(a, a + b)$

Exercício 7.8 *Fazer um programa para computador que determine o máximo divisor comum de dois números.*

Teorema 7.4 *Sejam* $a, b, c \in \mathbb{Z}$*:*

(i) Se $c|ab$ *e* $mdc(c, b) = 1$*, então* $c|a$*;*

(ii) Se $mdc(ab, c) = d$ *e* $mdc(a, c) = 1$*, então* $mdc(b, c) = d$*;*

(iii) Se $mdc(a, c) = 1$ *e* $mdc(b, c) = 1$*, então* $mdc(ab, c) = 1$*;*

(iv) Se $a|c$ *e* $b|c$*, então* $\dfrac{ab}{mdc(a, b)}|c$*;*

(v) Se $a|c$*,* $b|c$ *e* $mdc(a, b) = 1$*, então* $ab|c$.

Demonstração: *(i) Como* $mdc(c, b) = 1$*, existem* $r, s \in \mathbb{Z}$ *tais que* $r \cdot c + s \cdot b = 1$*. Multiplicando a igualdade por* a*, temos* $a \cdot r \cdot c + s \cdot a \cdot b = a$*. Como* $c|c$ *e* $c|a \cdot b$*, então* $c|(a \cdot r \cdot c + s \cdot a \cdot b) = a$ *(pelo Teorema* 4.1*).*

(ii) Por hipótese $d = mdc(a \cdot b, c)$*, logo,* $d|c$ *e* $d|a \cdot b$*. Também, por hipótese,* $mdc(a, c) = 1$*. Logo, existem* $r, s \in \mathbb{Z}$ *tais que* $r \cdot a + s \cdot c = 1$*. Multiplicando a igualdade por* b*, temos* $r \cdot a \cdot b + s \cdot b \cdot c = b$*. Como* $d|a \cdot b$ *e* $d|c$*, então* $d|b$*. Assim,* $d|c$ *e* $d|b$*. Seja* $e \in \mathbb{Z}$ *tal que* $e|b$ *e* $e|c$*. Então* $e|a \cdot b$ *e* $e|c$*. Logo,* $e|mdc(a \cdot b, c) = d$*. Assim, por definição,* $d = mdc(b, c)$.

(iii) Seja $mdc(a \cdot b, c) = d$*. Como* $mdc(a, c) = 1$*, por (ii),*

$mdc(b,c) = d$. Mas, por hipótese, $mdc(b,c) = 1$. Assim, $d = 1$, ou seja, $mdc(a \cdot b, c) = 1$.

(iv) Tomando $d = mdc(a,b)$, temos $d|a$ e $d|b$, portanto existem $a_1, b_1 \in \mathbb{Z}$ tais que $a = a_1 \cdot d$ e $b = b_1 \cdot d$. Logo, $mdc(a_1, b_1) = mdc(\frac{a}{d}, \frac{b}{d}) = 1$ (pelo Corolário 7.3) e $a\frac{b}{d} = a_1 \cdot b_1 \cdot d$. Como, por hipótese, $a|c$ e $b|c$, existem $c_1, c_2 \in \mathbb{Z}$ tais que $c = c_1 \cdot a = c_2 \cdot b$. Logo $c = c_1 \cdot a_1 \cdot d = c_2 \cdot b_1 \cdot d$ e, portanto, $\frac{c}{d} = c_1 \cdot a_1 = c_2 \cdot b_1$. Assim, $b_1|c_1 \cdot a_1$ e como $mdc(a_1, b_1) = 1$, por(i), temos que $b_1|c_1$, isto é, $c_1 = b_1 \cdot c_3$, para algum $c_3 \in \mathbb{Z}$. Temos então, $c = c_1 \cdot a_1 \cdot d = b_1 \cdot c_3 \cdot a_1 \cdot d = a_1 \cdot d \cdot b_1 \cdot c_3 = (a\frac{b}{d})c_3 = \frac{a \cdot b}{mdc(a,b)}c_3$. Logo, $\frac{a \cdot b}{mdc(a,b)}|c$.

(v) é conseqüência imediata de (iv). ∎

Exemplo 7.7 *Desde que $13|13.000 = 2 \cdot 6.500$ e $mdc(13, 2) = 1$, então $13|6500$.*

Exemplo 7.8 *Como $7|700$, $4|700$ e $mdc(4, 7) = 1$, então $28|700$.*

Exemplo 7.9 *Se $n \in \mathbb{Z}$ é tal que $2|n$ e $3|n$, então $6|n$, pois $mdc(2, 3) = 1$.*

Lema 7.5 *Sejam $a, b, c \in \mathbb{Z}$. Se $a \neq 0$, então $mdc(a, b) = mdc(a, b + ac)$.*

Demonstração: *Seja $d = mdc(a, b)$. Mostraremos que $d = mdc(a, b + ac)$. De $d = mdc(a, b)$, segue que $d|a$ e $d|b$ e, daí, $d|b + ac$. Se $e \in \mathbb{Z}$ é tal que $e|a$ e $e|b + ac$, então $e|ac$ e, portanto, $e|b + ac - ac = b$. Temos então que $e|a, e|b$ e $d = mdc(a, b)$. Assim, $e|d$ e, desse modo, $d = mdc(a, b + ac)$.* ∎

Exemplo 7.10 *Se $n \neq 0$, então $mdc(n, n+1) = mdc(n, n+1-n) = mdc(n, 1) = 1$.*

Exemplo 7.11 *Se $n \neq 0$, então $mdc(n,(n+1)^2) = mdc(n, n^2 + 2n + 1) = mdc(n, n^2 + 2n + 1 - n(n+2)) = mdc(n,1) = 1$.*

Corolário 7.6 *Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$. Se r é o resto da divisão de b por a, então $mdc(a,b) = mdc(a,r)$.*

Demonstração: *Sejam $q, r \in \mathbb{Z}$, respectivamente, o quociente e o resto da divisão de b por a, isto é, $b = qa + r$, com $0 \leq r < |a|$. Pelo lema anterior, $mdc(a,b) = mdc(a, b - qa) = mdc(a,r)$.* ∎

Exercício 7.9 *Dados $a, b \in \mathbb{Z}$, mostrar que:*
(a) se $mdc(a,b) = 1$, então $mdc(a,c) = mdc(a,bc)$;
(b) $mdc(a,b) = mdc(a,c) = 1$ se, e somente se, $mdc(a,bc) = 1$;
(c) $mdc(a,b) = 1$ se, e somente se, $mdc(a^n, b^m) = 1$, para quaisquer $m, n \in \mathbb{N}^*$;
(d) $mdc(a, a+b)|b$.

Exercício 7.10 *Mostrar que se $n \in \mathbb{N}^*$, então:*
(a) $mdc(n, 2n+1) = 1$;
(b) $mdc(n+1, 2n) = 1$ ou 2;
(c) $mdc(n, n^2 + n + 1) = 1$;
(d) $mdc(n+1, n^2 + n + 1) = 1$;
(e) $mdc(2n+2, 4n+3) = 1$;
(f) $mdc(2n+2, 4n+7) = 1$ ou 3;
(g) $mdc(2n+1, 5n+3) = 1$;
(h) $mdc(n^2 + 7n + 13, n+3) = 1$;
(i) $mdc(n+1, n^2+1) = 1$ ou 2.

Exercício 7.11 *Mostrar que $6|n(n+1)(2n+1)$.*

Exercício 7.12 *Mostrar que:*
(a) se n é par então $4|n$ ou $4|n+2$;

(b) se n é ímpar então $8|n^2-1$;
(c) $3|n(n^2-1)$;
(d) se n é ímpar então $24|n(n^2-1)$.

Exercício 7.13 *Sejam a, b e m inteiros, m positivo. Mostrar que $mdc(ma, mb) = m.mdc(a, b)$. Sugestão: Considerar $d = mdc(a, b)$ e mostrar que $md = mdc(ma, mb)$. Em algum momento será útil aplicar o Teorema* 7.1.

Exercício 7.14 *Sejam $a_1, a_2, ..., a_n$ inteiros de maneira que pelo menos um deles é diferente de zero. O máximo divisor comum entre $a_1, a_2, ..., a_n$ é um inteiro positivo d tal que:*
(i) $d|a_i$ para todo $i \in \{1, 2, ..., n\}$;
(ii) se $c \in \mathbb{Z}$ é tal que $c|a_i$ para todo $i \in \{1, 2, ..., n\}$, então $c|d$.
Mostrar que:
(a) $mdc(a_1, a_2, ..., a_n) = mdc(mdc(a_1, a_2, ..., a_{n-1}), a_n)$, com $n \in \mathbb{Z}$ e $n > 2$;
(b) se m é um inteiro positivo e $d = mdc(a_1, a_2, ..., a_n)$, então $mdc(m.a_1, m.a_2, ..., m.a_n) = m.d$;
(c) se $d = mdc(a_1, a_2, ..., a_n)$, então $mdc(\frac{a_1}{d}, \frac{a_2}{d}, ..., \frac{a_n}{d}) = 1$.

7.2 Mínimo múltiplo comum - MMC

O mínimo múltiplo comum de dois inteiros, como o próprio nome diz, é o menor múltiplo positivo de ambos. Abaixo, formalizamos a definição.

Sejam $a, b \in \mathbb{Z}^*$. O *mínimo múltiplo comum* de a e b é um inteiro positivo m tal que:

(i) $a|m$ e $b|m$;

(ii) Se $c \in \mathbb{Z}$ é tal que $a|c$ e $b|c$, então $m|c$.

Denotamos o mínimo múltiplo comum de a e b por $mmc(a, b)$.

A condição (i) nos diz que m é múltiplo de a e de b e a condição (ii) garante que m é o menor múltiplo positivo de a e de b. Garante também a unicidade de m.

Observar que se $n \in \mathbb{Z}^*$, então $mmc(n, 1) = |n|$, pois 1 e n dividem $|n|$ e se 1 e n dividem c então $|n|$ divide c.

Desde que $mmc(a, b) = mmc(-a, b) = mmc(a, -b) = mmc(-a, -b)$, podemos nos restringir aos casos em que $a > 0$ e $b > 0$.

Teorema 7.7 *Se a e b são números inteiros positivos, então $mmc(a, b) \cdot mdc(a, b) = a \cdot b$.*

Demonstração: *Temos que a divide $\dfrac{a \cdot b}{mdc(a, b)}$, pois $\dfrac{a \cdot b}{mdc(a, b)} = a \cdot \dfrac{b}{mdc(a, b)}$ e $\dfrac{b}{mdc(a, b)} \in \mathbb{Z}$. Do mesmo modo, b divide $\dfrac{a \cdot b}{mdc(a, b)}$. Se c é um inteiro tal que a divide c e b divide c, então, pelo Teorema 7.4, $\dfrac{a \cdot b}{mdc(a, b)}$ divide c. Assim, por definição, $mmc(a, b) = \dfrac{a \cdot b}{mdc(a, b)}$, ou seja, $mmc(a, b) \cdot mdc(a, b) = a \cdot b$.* ∎

Exemplo 7.12 *Como já vimos que $mdc(36, 42) = 6$, então $mmc(36, 42) \cdot 6 = 36 \cdot 42$. Portanto, $mmc(36, 42) = 252$.*

Exercício 7.15 *Sejam a e b inteiros positivos. Mostrar que se $mdc(a, b) = 1$, então $mmc(a, b) = ab$.*

Exercício 7.16 *Sejam a e b inteiros positivos. Se $mdc(a, b) = a$, então $mmc(a, b) = b$.*

Exercício 7.17 *Para os números* 1012 *e* 780 *calcular:*
(a) o máximo divisor comum;
(b) o mínimo múltiplo comum;
(c) encontrar inteiros r *e* s *tais que* $mdc(1012, 780) = r \cdot 1012 + s \cdot 780$.

Exercício 7.18 *Idem para os pares de números* 333 *e* 120*;* 1990 *e* 50*;* 12 *e* 18.

Exercício 7.19 *Mostrar que se* a *e* b *são inteiros positivos e se* $a|b$*, então* $mdc(a, b) = a$ *e* $mmc(a, b) = b$.

Exercício 7.20 *Sejam* a*,* b *e* m *inteiros positivos. Mostrar que* $mmc(m \cdot a, m \cdot b) = m \cdot mmc(a, b)$.

Exercício 7.21 *Para* $n \in \mathbb{N}^*$*, encontrar o mínimo múltiplo comum entre:*
(a) n *e* $2n + 1$*;*
(b) $n + 1$ *e* $2n$*;*
(c) n *e* $n^2 + n + 1$*;*
(d) $n + 1$ *e* $n^2 + n + 1$*;*
(e) $2n + 2$ *e* $4n + 3$*;*
(f) $2n + 2$ *e* $4n + 7$*;*
(g) $2n + 1$ *e* $5n + 3$*;*
(h) $n^2 + 7n + 13$ *e* $n + 3$*;*
(i) $n + 1$ *e* $n^2 + 1$.

Exercício 7.22 *Mostrar que se* $mdc(a, b) = mmc(a, b)$*, então* $a = \pm b$.

Exercício 7.23 *Sejam* $a_1, a_2, ..., a_n$ *inteiros de maneira que pelo menos um deles é diferente de zero. O mínimo múltiplo comum entre* $a_1, a_2, ..., a_n$ *é um inteiro positivo* m *tal que:*

(i) $a_i|m$ *para todo* $i \in \{1,\ 2, ..., n\}$*;*

(ii) se $c \in \mathbb{Z}$ *é tal que* $a_i|c$ *para todo* $i \in \{1, 2, ..., n\}$*, então* $c|m$*.*

Mostrar que $mmc(a_1, a_2, ..., a_n) = mmc(mmc(a_1,\ a_2,\ ...,\ a_{n-1}), a_n)$*, com* $n \in \mathbb{Z}$ *e* $n > 2$*.*

Exercício 7.24 *Seja* $f(x) = a_n.x^n + a_{n-1}.x^{n-1} + ... + a_1.x + a_0$ *um polinômio de grau* n*, com coeficientes inteiros, isto é, cada* a_i *é um inteiro e* $a_n \neq 0$*. Consideremos também* $a_0 \neq 0$*:*

(a) Mostrar que se o racional r/s *é uma raiz de* f*, onde* $r, s \in \mathbb{Z}$ *e* $mdc(r, s) = 1$*, então* $r|a_0$ *e* $s|a_n$*;*

(b) Mostrar que se $a_n = 1$ *e* q *é uma raiz racional de* f*, então* $q \in \mathbb{Z}$ *e* $q|a_0$*;*

(c) Encontrar as raízes de $f(x) = 6x^3 + 7x^2 - x - 2$*;*

(d) Idem para $f(x) = x^3 + 8x^2 + x - 42$*;*

(e) Idem para $f(x) = x^2 - 2$*.*

Exercício 7.25 *(Critério de divisibilidade por 7):*

(a) Seja n *um inteiro da forma* $n = 10 \cdot q + r$ *com* $0 \leq r < 10$*. Então* $7|n$ *se, e somente se,* $7|(q - 2r)$*;*

(b) Usar o critério acima para verificar se cada um dos números 103*,* 504*,* 5471 *é divisível por* 7*.*

8 Números primos

Os números primos desempenham um papel importante no estudo das propriedades multiplicativas de números inteiros, pois, como veremos, qualquer número inteiro pode ser escrito como um produto de números primos.

Problemas que envolvem os números primos têm uma tradição bastante antiga.

8.1 Sobre os números primos

Um inteiro p é um *número primo* se $p > 1$ e seus únicos divisores positivos são 1 e p. Se $p > 1$ não é primo, então p é *composto*.

Exercício 8.1 *Verificar que* 2, 3, 5 *e* 7 *são números primos. Lembre-se que se* $a|b$ *e* $b > 0$ *então* $a < b$.

Exercício 8.2 *Dar exemplos de números que não são primos.*

Teorema 8.1 *Seja* $p \in \mathbb{Z}$. *O número* p *é primo se, e somente se, satisfaz as seguintes condições:*

(i) $p > 1$;

(ii) dados $a, b \in \mathbb{N}$, *se* $p = a \cdot b$, *então* $a = 1$ *ou* $b = 1$.

Demonstração: *(⇒) Se* p *é um número primo, por definição,* $p > 1$. *Agora, se* $p = a \cdot b$, *com* $a, b \in \mathbb{N}$, *então* a *e* b *são divisores de* p. *Logo,* $a = 1$ *ou* $a = p$. *Se* $a = 1$, *nada temos a demonstrar. Se* $a = p$, *como* $p = a \cdot b = p \cdot b$, *então* $b = 1$.
(⇐) Por outro lado, se p *satisfaz as condições (i) e (ii). Seja* a *um divisor positivo de* p, *isto é, existe* $b \in \mathbb{N}$ *tal que* $p = a \cdot b$. *Pela condição (ii),* $a = 1$ *ou* $b = 1$. *Logo,* $a = 1$ *ou* $a = p$ *e, assim,* p *é um número primo.* ∎

Se n é um inteiro maior que 1 que não é um primo, então existem inteiros positivos a e b tais que $n = a \cdot b$, com $1 < a < n$ e $1 < b < n$, pois desde que n não é primo, então n possui um divisor positivo a, com $a \neq n$ e $a \neq 1$. Desse modo, $1 < a < n$, $n = a \cdot b$ e $1 < b < n$.

Lema 8.2 *Sejam p um número primo e a um inteiro.*

(i) Se $p \nmid a$, então $mdc(p, a) = 1$.

(ii) Se $0 < a < p$, então $mdc(p, a) = 1$.

Demonstração: *(i) Seja $d = mdc(p, a)$. Como $d|p$ e p é primo, então $d = 1$ ou $d = p$. Desde que $p \nmid a$, então $d \neq p$. Logo, $d = 1$. (ii) Se $p|a$, pelo Teorema 4.1 (ii), segue que $p \leq a$, o que contradiz a hipótese. Logo, $p \nmid a$ e, por(i), $mdc(p, a) = 1$* ∎

Teorema 8.3 *Se um número primo divide o produto de dois números inteiros, então ele divide pelo menos um deles.*

Demonstração: *Consideremos que $p|a \cdot b$, com $a, b \in \mathbb{Z}$. Se $p|a$, nada temos a demonstrar. Se $p \nmid a$, então $p \nmid |a|$ e pelo lema anterior, $mdc(p, a) = mdc(p, |a|) = 1$. Logo, pela Teorema 7.4 (i), $p|b$.* ∎

Exemplo 8.1 *Como $7|21.000 = 2 \cdot 10.500$ e $7 \nmid 2$, então $7|10.500$.*

Corolário 8.4 *Se um primo p divide um produto de inteiros, então p divide pelo menos um deles.*

Exercício 8.3 *Fazer a demonstração do corolário acima.*

Corolário 8.5 *Sejam $n \in \mathbb{Z}$ e p um número primo. Se $p|n^m$, para algum m inteiro positivo, então $p|n$.*

Exercício 8.4 *Fazer a demonstração do corolário acima.*

Exemplo 8.2 *Mostrar que $\sqrt{2}$ é um número irracional.*
Solução*: Suponhamos que $\sqrt{2}$ é um número racional, digamos, $\sqrt{2} = a/b$, em que a e b são inteiros positivos. Podemos considerar $mdc(a, b) = 1$ (ver o corolário do Teorema 7.2). Assim, $b \cdot \sqrt{2} = a$ e, elevando os dois termos ao quadrado, temos $b^2 \cdot 2 = a^2$, ou seja, $2|a^2$. Logo, pelo corolário anterior, $2|a$, isto é, $a = 2 \cdot c$. Ficamos então com $b^2 \cdot 2 = a^2 = 4 \cdot c^2 = 2 \cdot 2 \cdot c^2$. Cancelando 2 na igualdade, segue que $b^2 = 2 \cdot c^2$ e, daí, $2|b^2$. Portanto, $2|b$. Dessa maneira, $2|a$ e $2|b$ e, portanto, $2|mdc(a, b) = 1$ o que é uma contradição. A contradição surgiu de supor que $\sqrt{2}$ é um número racional. Logo, $\sqrt{2}$ é um número irracional.*

A solução acima permite-nos mostrar que para qualquer número primo p, tem-se que $\sqrt{p}$ é um número irracional (substituir 2 por p).

Exercício 8.5 *Verificar que $\sqrt{24}$ é um número irracional.*

Exercício 8.6 *Sejam p e q números primos. Mostrar a validade ou dar um contra-exemplo para:*
(a) $p \nmid a$ e $p \nmid b \Rightarrow p \nmid a + b$;
(b) $p \nmid a$ e $p \nmid b \Rightarrow p \nmid a \cdot b$;
(c) $p \nmid a$ e $q \nmid a \Rightarrow p + q \nmid a$;
(d) $p \nmid a$ e $q \nmid a \Rightarrow p \cdot q \nmid a$;
(e) $p|a \cdot b \Rightarrow p|a$ e $p|b$;
(f) $p \cdot q|a \cdot b \Rightarrow p|a$ e $q|b$ ou $q|a$ e $p|b$;
(g) $p \cdot q|a \cdot b$ e $p \nmid a \Rightarrow p|b$;
(h) $p \cdot q|a \cdot b$ e $p \nmid a \Rightarrow q \nmid b$.

8.2 O Teorema Fundamental da Aritmética

O Teorema Fundamental da Aritmética nos mostra que todo número inteiro maior que 1 se escreve de maneira única como um produto de números primos.

Teorema 8.6 *(Teorema Fundamental da Aritmética) Todo número inteiro $n > 1$ pode ser representado como um produto $n = p_1 \cdot p_2 \cdot ... \cdot p_r$ em que $p_1, p_2, ..., p_r$ são números primos. Além disso, se considerarmos $p_1 \leq p_2 \leq ... \leq p_r$, essa representação é única.*

Demonstração:

(Existência da representação)

Fazemos a demonstração por indução sobre n.

Se $n = 2$, então $n = p_1$ e $p_1 = 2$.

Hipótese de indução: consideramos se $m \in \mathbb{N}$ e é tal que $1 < m < n$, então m pode ser representado como um produto de primos.

Se n é primo, como no caso $n = 2$, temos $n = p_1$ e p_1 é primo. Agora, se n não é primo, já vimos que $n = a \cdot b$ com $a, b \in \mathbb{N}$ e $1 < a < n$ e $1 < b < n$. Então, pela hipótese de indução, a e b podem ser representados como produtos de primos e, portanto, $n = a \cdot b$ também tem uma representação como produto de primos.

Com isso, pelo PFI, mostramos a existência da representação. É claro que podemos sempre ordenar a representação $n = p_1 \cdot p_2 \cdot ... \cdot p_r$, de forma que $p_1 \leq p_2 \leq ... \leq p_r$.

(Unicidade da representação)

A demonstração também é por indução sobre n.

Se $n = 2 = p_1 \cdot p_2 \cdot ... \cdot p_r$. Como 2 é primo, então $p_1 = 2$ e $r = 1$. Portanto, a unicidade vale, pois se $r \geq 2$ então $1 = p_2 \cdot \cdots \cdot p_r$. Logo, $p_2 | 1$, portanto $p_2 \leq 1$, um absurdo.

Hipótese de indução: consideramos que a unicidade vale para todo $m \in \mathbb{N}$, tal que $1 < m < n$.

Se $n = p_1 \cdot p_2 \cdot ... \cdot p_r = q_1 \cdot q_2 \cdot ... \cdot q_s$, então $p_1 | q_1 \cdot q_2 \cdot ... \cdot q_s$. Logo, pelo Corolário 8.4, $p_1 | q_i$, para algum i, tal que $1 \leq i \leq s$ e como q_i é primo, então $p_1 = q_i$. Da mesma forma, $q_1 = p_j$ para

algum j tal que $1 \leq j \leq r$. Considerando $p_1 \leq p_2 \leq ... \leq p_r$ e $q_1 \leq q_2 \leq ... \leq q_r$, como $p_1 = q_i \geq q_1 = p_j \geq p_1$, então $p_1 = q_1$. Se n é primo, então como no caso $n = 2$, $n = p_1 = q_1$ e $r = s = 1$. Caso contrário, $r > 1$ e $s > 1$ e cancelando p_1 $(= q_1)$ na igualdade $p_1 \cdot p_2 \cdot ... \cdot p_r = q_1 \cdot q_2 \cdot ... \cdot q_s$, obtemos $p_2 \cdot ... \cdot p_r = q_2 \cdot ... \cdot q_s < q_1 \cdot q_2 \cdot ... \cdot q_s = n$. Assim, pela hipótese de indução, a representação $p_2 \cdot ... \cdot p_r = q_2 \cdot ... \cdot q_s$ é única, isto é, $r = s$ e $p_i = q_i$, para todo i tal que $2 \leq i \leq r$, o que verifica a unicidade. ∎

Uma fatoração em primos de um inteiro positivo n é uma representação de n como um produto de números primos ou como um produto de potências de números primos, ou seja $n = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_n^{r_n}$ em que $p_1 < p_2 < ... < p_n$ são números primos e cada r_i é um inteiro positivo. Se $n < -1$, podemos escrever $n = -(-n)$ e $-n$ tem uma fatoração como acima. Logo, podemos expressar $n = -p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_n^{r_n}$, em que cada p_i é um número primo.

Exemplo 8.3 *A fatoração de 72 é:* $72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^3 \cdot 3^2$.

Exemplo 8.4 *A fatoração de -20 é:* $-20 = -2 \cdot 2 \cdot 5 = -2^2 \cdot 5$.

Exercício 8.7 *Se $n > 0$ é um número composto, mostre que existe um primo $p < n$ tal que $p|n$.*

Exemplo 8.5 *O número 7 é primo, pois se fosse composto seria divisível por 2, 3 ou 5.*

Se p é um primo e $p|n$, então p aparece na fatoração de n pois, neste caso, $n = p \cdot m$, em que $m = \pm 1$ ou m é um produto de primos. Por exemplo, $2|28$, $28 = 2 \cdot 14 = 2 \cdot 2 \cdot 7$.

Lema 8.7 *Seja* $a = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_n^{r_n}$, *em que* $p_1 < p_2 < ... < p_n$ *são números primos e cada* r_i *é um número inteiro positivo. Se* d *é também um número inteiro positivo, então* $d|a$ *se, e somente se,* $d = p_1^{t_1} \cdot p_2^{t_2} \cdot ... \cdot p_n^{t_n}$ *em que, para cada* i, $0 \leq t_i \leq r_i$.

Demonstração: *Se* $d|a$, *então* $a = d.c$, *para algum inteiro* c. *Assim* $d|a$ *e* $c|a$. *Portanto, se* p *é um primo que divide* c *ou divide* d, *então* $p|a$. *Logo,* $p = p_i$ *para algum* i. *Desse modo, podemos tomar as fatorações de* c *e* d *nas formas* $c = p_1^{s_1} \cdot p_2^{s_2} \cdot ... \cdot p_n^{s_n}$ *e* $d = p_1^{t_1} \cdot p_2^{t_2} \cdot ... \cdot p_n^{t_n}$, *em que cada* r_i *e cada* t_i *é um número natural. De* $a = d.c$ *temos* $p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_n^{r_n} = (p_1^{t_1} \cdot p_2^{t_2} \cdot ... \cdot p_n^{t_n}) \cdot (p_1^{s_1} \cdot p_2^{s_2} \cdot ... \cdot p_n^{s_n}) = p_1^{t_1+s_1} \cdot p_2^{t_2+s_2} \cdot ... \cdot p_n^{t_n+s_n}$. *Logo, pelo Teorema* 8.6, $r_i = t_i + s_i \geq t_i \geq 0$.

Por outro lado, se $d = p_1^{t_1} \cdot p_2^{t_2} \cdot ... \cdot p_n^{t_n}$, *em que para cada* i, $0 \leq t_i \leq r_i$, *então existem números inteiros positivos* s_i *tais que* $r_i = t_i + s_i$. *Logo,* $a = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_n^{r_n} = p_1^{t_1+s_1} \cdot p_2^{t_2+s_2} \cdot ... \cdot p_n^{t_n+s_n} = (p_1^{t_1} \cdot p_2^{t_2} \cdot ... \cdot p_n^{t_n}) \cdot (p_1^{s_1} \cdot p_2^{s_2} \cdot ... \cdot p_n^{s_n}) = d \cdot (p_1^{s_1} \cdot p_2^{s_2} \cdot ... \cdot p_n^{s_n})$ *e, portanto,* $d|a$. ∎

Exemplo 8.6 $12|24$, $12 = 2^2 \cdot 3^1$ *e* $24 = 2^3 \cdot 3^1$.

Exemplo 8.7 $2|180$, $180 = 2^2 \cdot 3^2 \cdot 5^1$ *e* $2 = 2^1 \cdot 3^0 \cdot 5^0$.

8.2.1 Número de divisores de um inteiro

Seja a um inteiro maior que 1, por exemplo, $a = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_n^{r_n}$ com a sua decomposição em fatores primos e $p_1 < p_2 < ... < p_r$. Pelo lema anterior, cada divisor positivo d de a tem fatoração na forma $d = p_1^{t_1} \cdot p_2^{t_2} \cdot ... \cdot p_n^{t_n}$ em que, para cada i, $0 \leq t_i \leq r_i$. Assim, existem exatamente $(r_1 + 1) \cdot (r_2 + 1) \cdot \ ... \ \cdot (r_n + 1)$ possibilidades para d, ou seja, *o número de divisores* positivos de a é igual o número:

$$d(a) = (r_1 + 1) \cdot (r_2 + 1) \cdot \ ... \ \cdot (r_n + 1).$$

Exemplo 8.8 *Como* $20 = 2^2 \cdot 5$*, então* 20 *tem exatamente* $3 \cdot 2 = 6$ *divisores positivos. São eles:* $1, 2, 4, 5, 10,$ *e* 20*.*

Exemplo 8.9 *Se* $a = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_n^{r_n}$ *possui uma quantidade ímpar de divisores positivos, então* $d(a) = (r_1+1) \cdot (r_2+1) \cdot \ ... \ \cdot (r_n+1)$ *também é ímpar. Logo, cada* r_i *é par, digamos,* $r_i = 2t_i$*. Assim, para* $b = p_1^{t_1} \cdot p_2^{t_2} \cdot ... \cdot p_n^{t_n}$*, segue que* $b^2 = p_1^{2t_1} \cdot p_2^{2t_2} \cdot ... \cdot p_n^{2t_n} = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_n^{r_n} = a$*, ou seja,* a *é um quadrado perfeito.*

Exercício 8.8 *(a) Quantos divisores positivos tem o número 60?*
(b) Quantos divisores tem o número 60?

Exercício 8.9 *Encontrar todos os números* $a = 2^m \cdot 3^n$ *em cada caso:*
(a) a *tem um único divisor positivo;*
(b) a *tem exatamente dois divisores positivos;*
(c) a *tem exatamente três divisores positivos;*
(d) a *tem exatamente seis divisores positivos.*

Exercício 8.10 *Quais são os números que admitem:*
(a) apenas dois divisores positivos;
(b) apenas três divisores positivos;
(c) um número primo p *de divisores positivos.*

8.2.2 O cálculo do MDC e MMC a partir de fatoração

Teorema 8.8 *Sejam* a *e* b *inteiros positivos,* $a = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_n^{r_n}$ *e* $b = p_1^{s_1} \cdot p_2^{s_2} \cdot ... \cdot p_n^{s_n}$*, em que* $p_1 < p_2 < ... < p_n$ *são números primos e para todo* i*, tem-se* $r_i, s_i \in \mathbb{N}$*. Então* $mdc(a,b) = p_1^{u_1} \cdot p_2^{u_2} \cdot ... \cdot p_n^{u_n}$ *e* $mmc(a,b) = p_1^{t_1} \cdot p_2^{t_2} \cdot ... \cdot p_n^{t_n}$ *de modo que para cada* i*,* $u_i = min\{r_i, s_i\}$ *e* $t_i = max\{r_i, s_i\}$*.*

Demonstração: *Seja* $d = p_1^{u_1} \cdot p_2^{u_2} \cdot ... \cdot p_n^{u_n}$, *com* $u_i = min\{r_i, s_i\}$. *Pelo lema anterior,* $d|a$ *e* $d|b$. *Se* c *é um inteiro tal que* $c|a$ *e* $c|b$, *também pelo lema anterior, podemos tomar a fatoração de* c *na forma* $c = p_1^{v_1} \cdot p_2^{v_2} \cdot ... \cdot p_n^{v_n}$, *em que para cada* i, $v_i \leq r_i$, $v_i \leq s_i$ *e, portanto,* $v_i \leq min\{r_i, s_i\} = u_i$. *Logo, pelo Lema* 8.7, $c|d$ *e, então,* $d = mdc(a, b)$. *Para o caso* $mmc(a, b)$, *a demonstração segue ao observar-se que* $r_i + s_i = max\{r_i, s_i\} + min\{r_i, s_i\} = u_i + t_i$ *e aplicar-se o Teorema* 7.7*:* $mmc(a, b) \cdot mdc(a, b) = a \cdot b$.
■

Exemplo 8.10 *Como* $18 = 2 \cdot 3^2$ *e* $20 = 2^2 \cdot 5$, *podemos escrever* $18 = 2 \cdot 3^2 \cdot 5^0$ *e* $20 = 2^2 \cdot 3^0 \cdot 5$, *logo* $mdc(18, 20) = 2 \cdot 3^0 \cdot 5^0 = 2$ *e* $mmc(18, 20) = 2^2 \cdot 3^2 \cdot 5 = 180$.

Exemplo 8.11 *Calcular* $mdc(280, 300)$ *e* $mmc(280, 300)$.

Fazemos a fatoração dos números 280 e 300:

280	2	300	2
140	2	150	2
70	2	75	3
35	5	25	5
7	7	5	5
1		1	

Então, $280 = 2^3 \cdot 5 \cdot 7$ *e* $300 = 2^2 \cdot 3 \cdot 5^2$. *Logo,* $mdc(280, 300) = 2^2 \cdot 3^0 \cdot 5 \cdot 7^0 = 4 \cdot 5 = 20$ *e* $mmc(280, 300) = 2^3 \cdot 3 \cdot 5^2 \cdot 7 = 4.200$.

Exercício 8.11 *Encontrar números inteiros* a *e* b *tais que* $d(a) = 21$, $d(b) = 18$ *e* $mdc(a, b) = 20$.

Exercício 8.12 *Demonstrar ou dar um contra-exemplo:*
(a) Se $mdc(a, b) = 1$, *então* $d(a \cdot b) = d(a) \cdot d(b)$;

(b) Se $mdc(a, b) = 2$*, então* $d(a \cdot b) = d(a) \cdot d(b)$*.*

Teorema 8.9 *Se* n *é um número inteiro positivo composto, então* n *tem um divisor primo* p *tal que* $p \leq \sqrt{n}$*.*

Demonstração: *Desde que* n *é composto e positivo, podemos supor* $n = a \cdot b$*, com* $1 < a \leq b$*. De* $a \leq b$ *temos* $a^2 \leq a \cdot b = n$ *(1). De* $1 < a$*, pelo Teorema* 8.6*, temos que existe um primo* p *tal que* $p|a$*. Logo, pelo Teorema* 4.1*,* $p \leq a$ *e, portanto,* $p^2 \leq a^2$ *(2). De (1) e (2) segue que* $p^2 \leq n$ *e, portanto,* $p \leq \sqrt{n}$*.* ∎

Exemplo 8.12 *Verificar se* 127 *é um número primo.*

De acordo com a proposição acima, precisamos verificar se 127 *possui um divisor primo* $p \leq \sqrt{127} < 12$*. Como os primos menores que* 12 *são* $2, 3, 5, 7$ *e* 11 *e nenhum deles é divisor de* 127*, concluímos então que* 127 *é um número primo.*

8.3 O crivo de Eratóstenes

Eratóstenes (276 a.C. - 194 a.C.) foi matemático, bibliotecário e astrônomo. Nasceu em Cirene, na Grécia, e passou boa parte de sua vida em Alexandria.

Eratóstenes criou um algoritmo simples que permite determinar os números primos menores que um dado número inteiro positivo.

O *método de Eratóstenes* para listar os primos menores que um certo inteiro positivo $n > 1$, consiste do seguinte:

(i) Escrever uma lista com todos os inteiros entre 2 e $n-1$;

(ii) Para cada primo $p \leq \sqrt{n}$, elimina-se da lista todos os múltiplos $r \cdot p$ de p, para $r \geq 2$;

(iii) Os números que sobram são os primos menores que n.

Exemplo 8.13 *Para* $n = 40$*, consideremos a lista:* 2*,* 3*,* 4*,*

5, ..., 37, 38, 39. *Desde que* $\sqrt{40} < 7$, *eliminamos da lista os múltiplos de* $2, 3$ *e* 5, *com exceção deles próprios. Assim, ficamos com:* $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$ *e* 37 *que são todos os números primos menores que* 40.

Exercício 8.13 *Determinar os números primos menores que* 100.

Teorema 8.10 *Existe uma quantidade infinita de números primos.*

Demonstração: *Suponhamos que exista apenas uma quantidade finita de números primos:* $p_1, p_2, ..., p_n$. *Agora, tomemos* $a = 1 + p_1 \cdot p_2 \cdot \ ... \ \cdot p_n > p_i$, *para todo* $i \leq n$. *Assim,* a *é composto e, pelo Teorema* 8.9, a *possui um divisor primo, digamos,* p_i. *Como* $1 = a - p_1 \cdot p_2 \cdot \ ... \ \cdot p_n$, $p_i | a$ *e* $p_i | p_1 \cdot p_2 \cdot \ ... \ \cdot p_n$, *então* $p_i | 1$, *o que é uma contradição, pois os únicos divisores de* 1 *são* 1 *e* -1. *Assim, não pode existir somente uma quantidade finita de números primos.* ∎

Teorema 8.11 *Dado um inteiro positivo* m, *pode-se determinar* m *números compostos consecutivos.*

Demonstração: *Sejam* $m, a \in \mathbb{Z}$, *tais que* $2 \leq a \leq m + 1$. *Daí,* $a | (m+1)!$ *e, portanto,* $a | (m+1)! + a$. *Assim,* $(m+1)! + 2, (m+1)! + 3, ..., (m+1)! + (m+1)$ *são* m *inteiros compostos e consecutivos.* ∎

Exercício 8.14 *Encontrar o menor número composto da forma* $1 + p_1 \cdot p_2 \cdot \ ... \ \cdot p_n$, *em que* $p_1, p_2, ..., p_n$ *são os* n *primeiros números primos.*

Exercício 8.15 *Encontrar o menor* n *inteiro positivo, em cada caso:*

(a) $10 | n!$ *(b)* $100 | n!$ *(c)* $1000 | n!$

Exercício 8.16 *Encontrar a potência de* 2 *na decomposição em primos, em cada caso:*
(a) 10! *(b)* 20! *(c)* 1000!

Exercício 8.17 *Calcular o mínimo múltiplo comum e o máximo divisor comum dos seguintes pares de números:*
(a) 45 *e* 75 *(b)* 308 *e* 539 *(c)* 11 *e* 792 *(d)* 40 *e* 63
(e) 1 *e* 2001 *(f)* 2001 *e* 0

Exercício 8.18 *Mostrar que* $\sqrt[3]{4}$ *é um número irracional.*

Exercício 8.19 *Verificar se os números* 101, 173, 221, 961, 1969 *e* 2003 *são números primos.*

Exercício 8.20 *Dar um exemplo de dois inteiros* a *e* b *tais que* $a|b^2$, *mas* $a \nmid b$.

Exercício 8.21 *Mostrar que* $mdc(a^m, b^m) = mdc(a, b)^m$ *e* $mmc(a^m, b^m) = mmc(a, b)^m$ *para todo inteiro positivo* m.

Exercício 8.22 *Seja* p *um número primo maior que 3. Mostrar que:*
(a) 24 *divide* $p^2 - 1$ *(b)* p^2 *deixa resto* 1 *quando dividido por* 24.

Exercício 8.23 *Elaborar programas de computador para:*
(a) verificar se um número é primo;
(b) fazer a fatoração de um número positivo como produto de primos;
(c) fazer uma lista dos primos menores ou iguais a um inteiro positivo dado.

8.4 A Conjectura de Goldbach

O matemático prussiano Christian Goldbach (1690 - 1764) deve sua fama à elaboração de uma conjectura que, apesar de ter um enunciado muito simples, pode ser plenamente entendido e testado para uma quantidade muito grande de números naturais, e permanece como um problema não resolvido. Trata-se de um problema da Teoria dos Números e é um dos mais antigos que permanece em aberto.

O enunciado da conjectura de Goldbach é o seguinte: 'todo número par maior ou igual a 4 é a soma de dois primos'.

Como exemplo da validade para os primeiros números pares temos: $4 = 2 + 2$; $6 = 3 + 3$; $8 = 5 + 3$; $10 = 3 + 7 = 5 + 5$; $12 = 5 + 7$; $14 = 7 + 7$; $16 = 13 + 3$; $18 = 13 + 5$ e $20 = 13 + 7$.

Exercício 8.24 *Testar a validade da conjectura para números naturais até* 50.

A conjectura data de 1742, quando Christian Goldbach a apresentou, em uma carta, a Leonhard Euler. Algumas vezes ocorre também com pequenas variações do enunciado como: 'todo inteiro par maior que 5 pode ser escrito como a soma de dois primos ímpares'.

Naturalmente, verificações manuais exigem tempo e concentração. Mais recentemente, os computadores têm sido usados para verificações que confirmaram a conjectura para números da magnitude de pelo menos $3 \cdot 10^{17}$.

9 Congruências

O conceito de congruência na Teoria dos Números foi introduzido por Gauss em um trabalho publicado em 1801, tendo ele na época apenas 24 anos de idade. Veremos que uma das aplicações da congruência é encontrar o resto da divisão, devido ao fato de cada inteiro ser congruente ao resto de sua divisão pelo número que define a congruência.

9.1 A congruência e o resto da divisão

Sejam $a, b, n \in \mathbb{Z}$ e $n > 1$. A relação "*a é congruente a b módulo n*", denotada por $a \equiv b(mod\ n)$, é definida por:

$$a \equiv b(mod\ n) \Leftrightarrow n|a - b.$$

Exemplo 9.1 *Temos* $5 \equiv 2(mod\ 3)$, $7 \equiv -1(mod\ 4)$, $-1 \equiv 13(mod\ 7)$ *e* $31 \equiv 31(mod\ 77)$.

A congruência módulo n é uma relação de equivalência, pois:
- para todo $a \in \mathbb{Z}$, temos que $a - a = 0 = 0 \cdot n$, isto é, $a \equiv a(mod\ n)$ e, portanto, a relação é reflexiva;
- para todos $a, b \in \mathbb{Z}$, se $a \equiv b(mod\ n)$, então $a - b = c \cdot n$ e, portanto, $b - a = -(a - b) = -c \cdot n$. Logo, $b \equiv a(mod\ n)$ e, portanto, a relação é simétrica;
- para todos $a, b, c \in \mathbb{Z}$, se $a \equiv b(mod\ n)$ e $b \equiv c(mod\ n)$, então $a - b = d \cdot n$ e $b - c = e \cdot n$. Logo, $a - c = a - b + b - c = d \cdot n + e \cdot n = (d + e) \cdot n$. Portanto, $a \equiv c(mod\ n)$ e a relação é transitiva.

Teorema 9.1 *Sejam* $a, n, r \in \mathbb{Z}$, $n > 1$. *Se* r *é o resto da divisão de* a *por* n, *então* $a \equiv r(mod\ n)$.

Exercício 9.1 *Demonstrar o teorema anterior.*

Teorema 9.2 *Se $m \equiv r(mod\ n)$, com $1 < n$ e $0 \leq r < n$, então r é o resto da divisão de m por n.*

Exercício 9.2 *Demonstrar o teorema anterior.*

Corolário 9.3 *Sejam a e b inteiros. Então $a \equiv b(mod\ n)$ se, e somente se, a e b deixam o mesmo resto quando divididos por n.*

Exercício 9.3 *Demonstrar o corolário anterior.*

Teorema 9.4 *Sejam $a, b, c, d, n \in \mathbb{Z}$, com $n > 1$. Então:*

(i) Se $a \equiv b(mod\ n)$, então $a + c \equiv b + c(mod\ n)$;

(ii) Se $a \equiv b(mod\ n)$ e $c \equiv d(mod\ n)$, então $a + c \equiv b + d(mod\ n)$;

(iii) Se $a \equiv b(mod\ n)$, então $a \cdot c \equiv b \cdot c(mod\ n)$;

(iv) Se $a \equiv b(mod\ n)$ e $c \equiv d(mod\ n)$, então $a \cdot c \equiv b \cdot d(mod\ n)$;

(v) Se $a \equiv b(mod\ n)$ e $c > 0$, então $a^c \equiv b^c(mod\ n)$;

(vi) Se $a + c \equiv b + c(mod\ n)$, então $a \equiv b(mod\ n)$;

(vii) Se $c \neq 0$, $mdc(c, n) = 1$ e $a \cdot c \equiv b \cdot c(mod\ n)$, então $a \equiv b(mod\ n)$;

(viii) Se $c \neq 0$ e $a \cdot c \equiv b \cdot c(mod\ n)$, então $a \equiv b(mod\ \frac{n}{d})$, em que $d = mdc(c, n)$.

Demonstração: *(i) Se $a \equiv b(mod\ n)$, então $n|(a - b) = (a + c - c - b) = [(a + c) - (b + c)]$. Portanto, $a + c \equiv b + c(mod\ n)$;*

(ii) Se $a \equiv b(mod\ n)$ e $c \equiv d(mod\ n)$, por (i), temos que $a + c \equiv b + c(mod\ n)$ e $b + c \equiv b + d(mod\ n)$. Pela transitividade da relação $\equiv$, $a + c \equiv b + d(mod\ n)$. ∎

Exercício 9.4 *Completar a demonstração do Teorema 9.4.*

Exercício 9.5 *Mostrar a validade ou dar um contra-exemplo para:*
(a) $a \equiv b(mod\ n)$ *e* $c \equiv d(mod\ n) \Rightarrow a + b \equiv c + d(mod\ n)$;
(b) $a \equiv b(mod\ n)$ *e* $c \equiv d(mod\ n) \Rightarrow a + d \equiv b + c(mod\ n)$;
(c) $a \cdot c \equiv b \cdot c(mod\ n) \Rightarrow a \equiv b(mod\ n)$;
(d) $a \equiv b(mod\ n) \Rightarrow a + n \equiv b(mod\ n)$;
(e) $a \equiv b(mod\ n) \Rightarrow a \cdot n \equiv b(mod\ n)$;
(f) $a \equiv b(mod\ n) \Rightarrow c^a \equiv c^b(mod\ n)$;
(g) $a \equiv b(mod\ n)$ *e* $a \equiv b(mod\ m) \Rightarrow a \equiv b(mod\ n + m)$;
(h) $a \equiv b(mod\ n)$ *e* $a \equiv b(mod\ m) \Rightarrow a \equiv b(mod\ n \cdot m)$;
(i) $a \equiv b(mod\ n)$ *e* $a \equiv b(mod\ m) \Rightarrow a+m \equiv b+n(mod\ n+m)$;
(j) $n > m$, $a \equiv b(mod\ n)$ *e* $a \equiv b(mod\ m) \Rightarrow a + m \equiv b + n(mod\ n - m)$;
(k) $a^2 \equiv b^2(mod\ n) \Rightarrow a \equiv b(mod\ n)$;
(l) $a_i \equiv b_i(mod\ n)$ *para todo* $i = 1, \ldots, m \Rightarrow$
$a_1 + \cdots + a_m \equiv b_1 + \cdots + b_m(mod\ n)$ *e*
$a_1 \cdot \cdots \cdot a_m \equiv b_1 \cdot \cdots \cdot b_m(mod\ m)$.

Exemplo 9.2 *Encontrar o resto da divisão de* 5^{100} *e* 5^{101} *por* 24.

Temos que $5^2 - 1 = 25 - 1 = 24$, *ou seja,* $5^2 \equiv 1(mod\ 24)$.

Também, $5^{100} = (5^2)^{50}$. *Como* $5^2 \equiv 1(mod\ 24)$, *então* $(5^2)^{50} \equiv 1^{50}(mod\ 24)$, *ou seja,* $5^{100} \equiv 1(mod\ 24)$.

Desse modo, o resto da divisão de 5^{100} *por* 24 *é* 1.

Agora, como $5^{100} \equiv 1(mod\ 24)$ *e* $5 \equiv 5(mod\ 24)$, *então* $5 \cdot 5^{100} \equiv 5 \cdot 1(mod\ 24)$, *ou seja,* $5^{101} \equiv 5(mod\ 24)$. *Portanto, o resto da divisão de* 5^{101} *por* 24 *é* 5.

Exemplo 9.3 *Encontrar o resto da divisão de* 19^{138} *por* 17.

Temos $19 \equiv 2(mod\ 17)$,
$19^2 \equiv 2^2(mod\ 17) \equiv 4(mod\ 17)$,

$19^3 = 19^2 \cdot 19 \equiv 4 \cdot 2 (mod\ 17) \equiv 8 (mod\ 17)$,
$19^4 = 19^2 \cdot 19^2 \equiv 4 \cdot 4 (mod\ 17) \equiv 16 (mod\ 17) \equiv -1 (mod\ 17)$.

Como $138 = 4 \cdot 34 + 2$, *então* $19^{138} = 19^{4 \cdot 34 + 2} = (19^4)^{34} \cdot 19^2 \equiv (-1)^{34} \cdot 4 (mod\ 17) \equiv 4\ (mod\ \ 17)$.

Assim, o resto da divisão de 19^{138} *por* 17 *é* 4.

Exemplo 9.4 *Qual o resto da divisão e* 2^{125} *por 11?*

Podemos proceder como no exemplo anterior até chegarmos em $2^5 = 32 \equiv -1 (mod\ 11)$. *Como* $125 = 5 \cdot 25$, *então* $2^{125} = 2^{5 \cdot 25} = (2^5)^{25} \equiv (-1)^{25} (mod\ 11) \equiv -1 (mod\ 11) \equiv 10 (mod\ 11)$. *Assim, o resto da divisão de* 2^{125} *por* 11 *é* 10.

Exemplo 9.5 *Encontrar o algarismo das unidades de* 7^{100}.

Precisamos encontrar o resto da divisão de 7^{100} *por* 10. *Como* $7^2 = 49 \equiv -1 (mod\ 10)$, *então* $7^{100} = (7^2)^{50} \equiv (-1)^{50} (mod\ 10) \equiv 1 (mod\ 10)$. *Daí, o resto da divisão de* 7^{100} *por* 10 *é* 1. *Portanto, o algarismo das unidades de* 7^{100} *é* 1.

Exercício 9.6 *Qual o resto da divisão de:*

(a) 8^{765} *por* 7;
(b) 7^{5001} *por* 8;
(c) $33 \cdot 43 \cdot 60$ *por* 8;
(d) 94^{1000} *por* 13;
(e) 41^{41} *por* 7;
(f) $1^2 + 2^2 + \cdots + 100^2$ *por* 3;
(g) $1^2 + 2^2 + \cdots + 100^2$ *por* 4.

Exercício 9.7 *Encontrar o resto da divisão de* $(4^{103} + 2 \cdot 5^{104})^{122}$ *por* 13.

Exercício 9.8 *Se* $a \equiv b (mod\ n)$, *mostrar que* $mdc(n, a) = mdc(n, b)$. *Sugestão: aplicar o Lema* 7.5.

Exercício 9.9 *Verificar se* $a \equiv b (mod\ n)$ *implica* $mmc(n, a) = mmc(n, b)$.

9.2 O Pequeno Teorema de Fermat

Seja n um inteiro maior que 1. Um *sistema completo de resíduos módulo n* é um conjunto com n elementos tal que cada inteiro é congruente módulo n a um único elemento desse conjunto. Por exemplo, o Teorema 9.1 e o Exemplo 9.2 garantem que, dado um inteiro $n > 1$, o conjunto dos restos da divisão por n, $\{0, 1, ..., n-1\}$, é um sistema completo de resíduos.

Lema 9.5 *Um conjunto com n elementos tais que cada dois elementos não são congruentes módulo n, é um sistema completo de resíduos módulo n.*

Demonstração: *Seja $\{a_1, \ldots, a_n\}$ um conjunto de n inteiros tal que não ocorre $a_i \equiv a_j (mod\ n)$ se $i \neq j$. Então, pelo Corolário 9.3, se $i \neq j$, a_i e a_j são congruentes módulo n a elementos distintos de $\{0, 1, ..., n-1\}$, ou seja, cada a_i é congruente módulo n a um único elemento de $\{0, 1, ..., n-1\}$, pois este é um sistema completo de resíduos. Portanto, cada elemento de $\{0, 1, ..., n-1\}$ é congruente módulo n a um único elemento de $\{a_1, ..., a_n\}$. Assim, como cada inteiro m é congruente módulo n a um único elemento de $\{0, 1, ..., n-1\}$ então m é congruente módulo n a um único elemento de $\{a_1, ..., a_n\}$.* ∎

Lema 9.6 *Sejam $n > 1$ um inteiro e a um inteiro relativamente primo com n. Então:*

(i) $\{0, a, 2a, ..., (n-1)a\}$ é um sistema completo de resíduos;

(ii) cada elemento do conjunto $\{a, 2a, ..., (n-1)a\}$ é congruente a um único elemento de $\{1, ..., n-1\}$ módulo n.

Demonstração: *(i) Se $ra \equiv sa (mod\ n)$ com $r \neq s$, podemos considerar, sem perda de generalidade, que $0 \leq s < r < n$. Assim, $n | ra - sa = (r-s)a$ e como $mdc(n, a) = 1$ então $n | r - s$, ou seja, $n \leq r - s \leq r < n$, o que é um absurdo. Esse absurdo surgiu ao supormos $r \neq s$. Assim, os elementos de*

$\{0, a, 2a, ..., (n-1)a\}$ não são congruentes dois a dois módulo n. Logo, pelo lema anterior, este conjunto é um sistema completo de resíduos, pois contém exatamente n elementos. ∎

Exercício 9.10 *Demonstrar o item (ii) do lema anterior.*

Teorema 9.7 *(Pequeno Teorema de Fermat) Se p é primo e a é um inteiro qualquer, então:*

(i) $a^p \equiv a(mod\ p)$;

(ii) se a não é divisível por p, então $a^{p-1} \equiv 1(mod\ p)$.

Demonstração: *Mostraremos primeiro (ii) e depois que (ii) $\Rightarrow$ (i).*

(ii) Pelo lema anterior, cada elemento do conjunto $\{a, 2a, ..., (p-1)a\}$ é congruente a um único elemento de $\{1, ..., p-1\}$ módulo p. Segue daí que $a \cdot 2a \cdot 3a \cdot \ ... \ \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ ... \ \cdot (p-1)(mod\ p)$, ou seja, $(p-1)!a^{p-1} \equiv (p-1)!(mod\ p)$. Desse modo, $p|(p-1)!(a^{p-1}-1)$ e como $p \nmid (p-1)!$, então $p|(a^{p-1}-1)$, ou seja, $a^{p-1} \equiv 1(mod\ p)$.

(i) Se $p \nmid a$, por (ii), $a^{p-1} \equiv 1(mod\ p)$ e, então, $a^p \equiv a(mod\ p)$. Agora, se $p|a$, então $p|a^p$ e, daí, $p|(a^p - a)$. Portanto, $a^p \equiv a(mod\ p)$. ∎

Exemplo 9.6 *Pelo Pequeno Teorema de Fermat, temos $7|10^6 - 1$, $11|50^{10} - 1$ e $3|99^3 - 99$.*

Exemplo 9.7 *Verificar que se $3 \nmid a$, então $3|a^8 - 1$.*

Pelo Pequeno Teorema de Fermat, como $3 \nmid a$, então $3|a^2 - 1$. Como $a^8 - 1 = (a^4 - 1)(a^4 + 1) = (a^2 - 1)(a^2 + 1)(a^4 + 1)$ e $3|a^2 - 1$, então $3|(a^2 - 1)(a^2 + 1)(a^4 + 1) = a^8 - 1$.

Devemos observar que, se p é primo e $p|a$, então $p|a^{p-1}$. Portanto, $p \nmid a^{p-1} - 1$, pois em caso contrário $p|a^{p-1} - (a^{p-1} - 1) = 1$, o que é uma contradição.

Exemplo 9.8 *Temos* $3 \nmid 102^2 - 1$, $7 \nmid 77^6 - 1$.

Exemplo 9.9 *Pelo Pequeno Teorema de Fermat, temos que* $41|3^{40} - 1 = (3^{20} + 1)(3^{20} - 1)$.

Como 41 *é primo, então* $41|3^{20} + 1$ *ou* $41|3^{20} - 1$. *Mas* 41 *não pode dividir ambos, pois se* $41|3^{20} + 1$ *e* $41|3^{20} - 1$, *então* $41|(3^{20}+1)-(3^{20}-1) = 2$. *Daí,* $41 \leq 2$, *o que é uma contradição.*

Corolário 9.8 *Sejam* a *e* b *números inteiros e seja* p *um número primo. Então* $(a + b)^p \equiv a^p + b^p (mod\ p)$.

Demonstração: *Aplicando o Pequeno Teorema de Fermat, temos* $(a + b)^p \equiv a + b(mod\ p)$, $a^p \equiv a(mod\ p)$ *e* $b^p \equiv b(mod\ p)$. *Assim,* $a^p + b^p \equiv a + b(mod\ p)$ *e* $(a + b)^p \equiv a^p + b^p (mod\ p)$. ∎

Lema 9.9 *Se* $a \equiv b(mod\ m)$, $a \equiv b(mod\ n)$ *e* $mdc(m, n) = 1$, *então* $a \equiv b(mod\ m \cdot n)$.

Exercício 9.11 *Demonstrar o lema anterior. Sugestão: Teorema* $7.4 - (v)$.

Teorema 9.10 *Se* a *é um número inteiro, então* a *e* a^5 *possuem o mesmo algarismo das unidades.*

Demonstração: *Pelo Pequeno Teorema de Fermat,* $a^5 \equiv a(mod\ 5)$. *Sabemos também que* a *é par se, e somente se* a^n *é par, para todo* n *inteiro positivo. Assim,* $a^5 - a$ *é par, ou seja,* $2|a^5 - a$. *Portanto,* $a^5 \equiv a(mod\ 2)$. *Do lema anterior, concluímos que* $a^5 \equiv a(mod\ 10)$, *ou seja, que* a^5 *e* a *deixam o mesmo resto quando divididos por* 10, *pelo Corolário* 9.3. *Logo,* a^5 *e* a *possuem o mesmo algarismo das unidades.* ∎

Exercício 9.12 *Seja* a *um inteiro tal que* $5 \nmid a$.
(a) Mostrar que $5|a^{16} - 1$.

(b) Mostrar que a *e* a^{17} *possuem o mesmo algarismo das unidades.*
(c) Idem para a, a^9 *e* a^{33}.

Exercício 9.13 *Mostrar que se* $7 \nmid n$, *então:*
(a) $7|n^6 + 6$; *(b)* $7|n^8 - 8n^2$; *(c)* $7|n^8 + n^6 + 6n^2 - 8$;
(d) $14|n^8 + n^6 + 6n^2 - 8$.

Exercício 9.14 *Mostrar que* $22|a^{11} - a$, *para todo número inteiro* a.

Exercício 9.15 *Quais os possíveis restos da divisão de* n^6 *por* 7*?*

Exercício 9.16 *Seja* p *um número primo. Encontrar os possíveis restos da divisão de* 15^{p-1} *por* p.

Exercício 9.17 *Se* $a_i \equiv b_i (mod\ n)$, *para* $i = 1, 2, ..., m$, *então* $a_1 + a_1 + \cdots + a_m \equiv b_1 + b_2 + \cdots + b_m (mod\ n)$

Exercício 9.18 *Encontrar o resto da divisão de:*
(a) $1^{11} + 2^{11} + ... + 100^{11}$ *por* 11;
(b) $1^{10} + 2^{10} + ... + 100^{10}$ *por* 11.

Exercício 9.19 *Sejam* m *e* n *inteiros,* $n > 1$. *Mostre que* $\{m + 1, m + 2, ..., m + n\}$ *é um sistema de resíduos módulo* n.

9.3 O Teorema de Euler

O Pequeno Teorema de Fermat não pode ser generalizado para um inteiro qualquer. Por exemplo, como $4 \nmid 3^{4-1} - 1$, não ocorre $3^{4-1} \equiv 1 (mod\ 4)$. Mas esse teorema foi melhorado por Euler, no sentido que o Pequeno Teorema de Fermat poder ser

entendido um caso particular do Teorema de Euler.

A *função φ de Euler* é definida por $\varphi : \mathbb{N}^* \to \mathbb{N}^*$, em que $\varphi(n)$ é a quantidade de inteiros positivos menores ou iguais a n que são relativamente primos a n.

Por exemplo, $\varphi(1) = 1,\ \varphi(2) = 1,\ \varphi(6) = 4,\ \varphi(10) = 4$ e se p é primo, então $\varphi(p) = p - 1$.

Seja $n \in \mathbb{N},\ n > 1$ e seja a um inteiro relativamente primo com n. Seja $S = \{x_1, ..., x_{\varphi(n)}\}$ o conjunto dos inteiros positivos menores que n e relativamente primos com n tais que $x_i < x_j$ se $i < j$.

Exercício 9.20 *Verificar que no conjunto S valem:*
(a) $ax_i \equiv ax_j (mod\ n) \Rightarrow x_i = x_j$;
(b) Cada ax_i é congruente a exatamente um elemento x_j de S módulo n. (Sugestão: mostre que o resto da divisão de ax_i por n está em S).

Assim, $ax_1 \cdot ... \cdot ax_{\varphi(n)} \equiv x_1 \cdot ... \cdot x_{\varphi(n)} (mod\ n)$ e, portanto, $a^{\varphi(n)} \cdot x_1 \cdot ... \cdot x_{\varphi(n)} \equiv x_1 \cdot ... \cdot x_{\varphi(n)} (mod\ n)$, ou seja, $n | a^{\varphi(n)} \cdot x_1 \cdot ... \cdot x_{\varphi(n)} - x_1 \cdot ... \cdot x_{\varphi(n)} = (a^{\varphi(n)} - 1) \cdot (x_1 \cdot ... \cdot x_{\varphi(n)})$.

Como para cada i, $mdc(x_i, n) = 1$, então $mdc(x_1 \cdot\ ...\ \cdot x_{\varphi(n)}, n) = 1$ e, portanto, $n | a^{\varphi(n)} - 1$.

O que fizemos foi justamente demonstrar o teorema a seguir.

Teorema 9.11 *(Teorema de Euler) Se $n > 1$ é um inteiro e a é um inteiro relativamente primo com n, então $a^{\varphi(n)} \equiv 1 (mod\ n)$.*

Exemplo 9.10 *Pelo Teorema de Euler, temos que* $6|35^2 - 1$, $10|73^4 - 1$ *e* $15|77^8 - 1$.

9.4 A aritmética módulo n

Alguém que afirmasse que $10 + 10 = 5$ provavelmente seria considerado um maluco, pois as regras usuais de adição garantem que o resultado daquela operação deveria ser 20. Mas, quando trabalhamos com medida de ângulos em graus temos, por exemplo, que $230 + 170 = 40$. Logo, pode ser que em alguma situação a soma de 10 com 10 seja realmente 5. Veremos que isso é possível ao trabalharmos com congruências. A partir de relações de equivalência no conjunto dos números inteiros, definimos as operações de adição e multiplicação no conjunto quociente e obtemos regras de operações para um conjunto finito.

Dado n um inteiro positivo, para cada $a \in \mathbb{Z}$, denotamos a classe de equivalência de a módulo n por $\bar{a} = \{r \in \mathbb{Z} : r \equiv a(mod\ n)\}$.

Denotamos por $\mathbb{Z}_n$ o conjunto quociente de $\mathbb{Z}$ pela relação de congruência módulo n. Assim, $\mathbb{Z}_n = \{\bar{a} : a \in \mathbb{Z}\}$.

Exemplo 9.11 *Na congruência módulo 3 temos:*
$\bar{0} = \{a : a \equiv 0(mod\ 3)\} = \{a : 3|(a-0)\} = \{a : a = 3n,\ n \in \mathbb{Z}\}$
$= \{3n : n \in \mathbb{Z}\} = \{..., -9, -6, -3, 0, 3, 6, 9, ...\}$;
$\bar{1} = \{a : a \equiv 1(mod\ 3)\} = \{a : 3|(a-1)\} = \{a : a - 1 = 3n,\ n \in \mathbb{Z}\} = \{a : a = 3n + 1,\ n \in \mathbb{Z}\} = \{3n + 1 : n \in \mathbb{Z}\} = \{..., -8, -5, -2, 1, 4, 7, 10, ...\}$;
$\bar{2} = \{a : a \equiv 2(mod\ 3)\} = \{a : 3|(a-2)\} = \{a : a - 2 = 3n,\ n \in \mathbb{Z}\} = \{a : a = 3n + 2,\ n \in \mathbb{Z}\} = \{3n + 2 : n \in \mathbb{Z}\} = \{..., -7, -4, -1, 2, 5, 8, 11, ...\}$.

Na congruência módulo n, aplicando-se o algoritmo da divisão para a e n, temos que existem $q, r \in \mathbb{Z}$ tais que $a = q \cdot n + r$ e $0 \leq r < n$. Logo, $a - r = q \cdot n$, isto é, $a \equiv r(mod\ n)$ e, portanto, $\bar{a} = \bar{r}$, em que r é o resto da divisão de a por n. Temos então o conjunto quociente $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}\}$. Temos que $\mathbb{Z}_n$ tem exatamente n elementos, pois se $a, b \in \mathbb{Z}$ são tais que $0 \leq a < b < n$, então $a - a < b - a < n - a \leq n$. Logo, $0 < b - a < n$ e, portanto, $b - a$ não é múltiplo de n. Assim, b não é congruente a a módulo n e, desse modo, $\bar{b} \neq \bar{a}$. Logo, $Z_n = \{\bar{0}, \bar{1}, ..., \overline{n-1}\}$ é um conjunto com n elementos.

Vimos acima que se $a \in \mathbb{Z}$, então $\bar{a} = \bar{r}$, em que r é o resto da divisão de a por n. Assim, se $a, b \in \mathbb{Z}$ são tais que $a \equiv b(mod\ n)$, então $\bar{b} = \bar{a} = \bar{r}$ e, portanto, a e b fornecem o mesmo resto, quando divididos por n.

Exemplo 9.12 *Para $n = 5$, temos $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. Temos também $\overline{125} = \bar{0}$; $\overline{13} = \bar{3}$; $\overline{27} = \bar{2}$; $\overline{-4} = \bar{1}$; $\overline{1002} = \bar{2}$; $\overline{-1} = \bar{4}$. Assim, $\mathbb{Z}_5 = \{\overline{125}, \overline{-4}, \overline{1002}, \overline{13}, \overline{-1}\}$.*

Como vimos no exemplo acima, temos muitas formas para representar $\mathbb{Z}_n$, mas vamos assumir $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}\}$, para facilitar o tratamento algébrico.

9.4.1 Adição e multiplicação em $\mathbb{Z}_n$

Para $\bar{a}, \bar{b} \in \mathbb{Z}_n$ definimos:

(i) $\bar{a} + \bar{b} = \overline{a + b}$;

(ii) $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$.

Essas operações indicam que $\overline{a} + \overline{b} = \overline{r}$, em que r é o resto da divisão de $a + b$ por n e $\overline{a} \cdot \overline{b} = \overline{s}$, em que s é o resto da divisão

de $a \cdot b$ por n. Assim, $\overline{a} + \overline{b} \in \mathbb{Z}_n$ e $\overline{a} \cdot \overline{b} \in \mathbb{Z}_n$

Exemplo 9.13 *Em* $\mathbb{Z}_{15}$ *temos* $\overline{10}+\overline{10} = \overline{5}$*;* $\overline{3}+\overline{7} = \overline{10}$*;* $\overline{6}+\overline{12} = \overline{3}$*;* $\overline{5} \cdot \overline{5} = \overline{10}$*;* $\overline{10} \cdot \overline{6} = \overline{0}$.

Precisamos verificar que essas operações estão bem definidas, o que será feito a seguir.

Teorema 9.12 *Sejam* $a, b, c, d \in \mathbb{Z}$ *com* $\overline{a} = \overline{c}$ *e* $\overline{b} = \overline{d}$*. Então:*

(i) $\overline{a} + \overline{b} = \overline{c} + \overline{d}$*;*

(ii) $\overline{a} \cdot \overline{b} = \overline{c} \cdot \overline{d}$.

Demonstração: *Como* $\overline{a} = \overline{c}$ *e* $\overline{b} = \overline{d}$*, então* $a \equiv c (mod\ n)$ *e* $b \equiv d (mod\ n)$*. Pelo Teorema* 9.4*,* $a + b \equiv c + d (mod\ n)$ *e* $a \cdot b \equiv c \cdot d (mod\ n)$*. Assim,* $\overline{a+b} = \overline{c+d}$ *e* $\overline{a \cdot b} = \overline{c \cdot d}$*, pelo Corolário* 9.3*. Por definição,* $\overline{a} + \overline{b} = \overline{c} + \overline{d}$ *e* $\overline{a}.\overline{b} = \overline{c} \cdot \overline{d}$. ∎

Se $\bar{a} \in \mathbb{Z}_n$ e $\bar{a} \neq \bar{0}$, então o inverso aditivo de $\bar{a}$ é $-\overline{a} = \overline{n-a}$, pois $\bar{a} + \overline{(n-a)} = \overline{a+n-a} = \overline{a-a+n} = \overline{0+n} = \bar{n} = \bar{0}$, isto é, $\overline{a} + \overline{n-a} = \overline{0}$. É claro que o inverso aditivo de $\bar{0}$ é $\bar{0}$ mesmo. Assim, por exemplo, em $\mathbb{Z}_{15}$, $-\overline{7} = \overline{8}$ e $-\overline{1} = \overline{14}$.

9.4.2 Propriedades das operações em $\mathbb{Z}_n$ e o Teorema de Wilson

Seguem algumas propriedades da adição e da multiplicação de $\mathbb{Z}_n$.

Teorema 9.13 *Se* $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$*, então:*

(i) $\overline{a} + \overline{b} \in \mathbb{Z}_n$ *e* $\overline{a} \cdot \overline{b} \in \mathbb{Z}_n$ *(fechamento);*

(ii) $\overline{a} + \overline{b} = \overline{b} + \overline{a}$ *e* $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$ *(comutatividade);*

(iii) $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$ *e* $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$ *(associatividade);*

(iv) $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$ *(distributividade);*

(v) $\overline{a} + \overline{0} = \overline{a}$ *(elemento neutro da adição - zero);*

(vi) $\overline{1} \cdot \overline{a} = \overline{a}$ *(elemento neutro da multiplicação - unidade);*

(vii) $\overline{0} \cdot \overline{a} = \overline{0}$ *(elemento absorvente da multiplicação);*

(viii) $\overline{a} + (\overline{n-a}) = \overline{0}$ *(inverso aditivo).*

Demonstração: *(i) Já foi observado na definição das operações.*

(ii) Como $a + b = b + a$ *então* $\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}$. *De modo análogo, mostra-se,* $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$. ∎

Exercício 9.21 *Demonstrar as demais propriedades do teorema anterior.*

Dado $n \in \mathbb{Z},\ n > 1$, consideremos $\overline{a} \in \mathbb{Z}_n$. Dizemos que $\overline{a}$ é uma *unidade* em $\mathbb{Z}_n$ se existe $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$. Dizemos que $\overline{a}$ é um *divisor de zero* se $\overline{a} \neq \overline{0}$ e $\overline{a} \cdot \overline{b} = \overline{0}$, para algum $\overline{b} \in \mathbb{Z}_n$, com $\overline{b} \neq \overline{0}$.

Podemos fazer tabelas para a adição e a multiplicação em $\mathbb{Z}_n$. Por exemplo, para $\mathbb{Z}_4$ temos:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

A tabela da adição indica que os inversos aditivos de $\overline{1}$, $\overline{2}$ e $\overline{3}$ são, respectivamente, $\overline{3}$, $\overline{2}$ e $\overline{1}$. A tabela da multiplicação mostra $\overline{1}$ é o elemento neutro para a multiplicação; que $\overline{2}$ é um divisor de zero pois $\overline{2} \cdot \overline{2} = \overline{0}$ e que $\overline{3}$ é o seu próprio inverso multiplicativo, pois $\overline{3} \cdot \overline{3} = \overline{1}$.

Teorema 9.14 *Para* $a, n \in \mathbb{Z}$ *tais que* $1 < n$ *e* $0 < a < n$,

(i) se $mdc(n, a) = 1$, *então* $\overline{a}$ *é uma unidade em* $\mathbb{Z}_n$;

(ii) se $mdc(n, a) \neq 1$, *então* $\overline{a}$ *é um divisor de zero em* $\mathbb{Z}_n$.

Demonstração: *(i) Como* $mdc(n,a)=1$*, então existem* $r,s\in\mathbb{Z}$ *tais que* $r\cdot n+s\cdot a=1$*. Assim,* $s\cdot a=r\cdot n+1$*, isto é,* $\overline{s}\cdot\overline{a}=\overline{s\cdot a}=\overline{1}$ *e, portanto,* $\overline{a}$ *é uma unidade, pois* $\overline{s}=\overline{b}$*, sendo* b *o resto da divisão de* s *por* n*, e* $\overline{b}\cdot\overline{a}=\overline{s}\cdot\overline{a}=\overline{1}$*;*
(ii) Seja $d=mdc(n,a)>1$*. Então existem* $b,c\in\mathbb{Z}$ *tais que* $n=d\cdot b$ *e* $a=d\cdot c$*. Como* $0<n$ *e* $0<d$ *então* $0<b<b\cdot d=n$*, portanto* $\overline{b}\neq\overline{0}$*. Assim,* $\overline{a}\cdot\overline{b}=\overline{a\cdot b}=\overline{d\cdot c\cdot b}=\overline{d\cdot b\cdot c}=\overline{n\cdot c}=\overline{0}$*. Como* $0<a<n$ *então* $\overline{a}\neq 0$*. Logo,* $\overline{a}$ *é um divisor de zero.* ■

Exercício 9.22 *Encontrar as unidades e os divisores de zero de* $\mathbb{Z}_{15}$*.*

Corolário 9.15 *Se* p *é um número primo e* $\overline{a}\in\mathbb{Z}_p$*, com* $0<a<p$*, então existe um único* $\overline{b}\in\mathbb{Z}_p$ *tal que* $\overline{a}\cdot\overline{b}=1$ *(isto é,* $\overline{a}$ *é uma unidade).*
Demonstração: *(Existência)*

Seja $\overline{a}\in\mathbb{Z}_p$*, tal que* $\overline{a}\neq\overline{0}$*, isto é,* a *não é um múltiplo de* p*. Desde que* p *é um número primo, então* $mdc(a,p)=1$*. Assim, pelo teorema anterior,* $\overline{a}$ *é uma unidade.*

(Unicidade)

Se existem $\overline{b},\ \overline{c}\in\{\overline{1},...,\overline{p-1}\}$ *tais que* $\overline{a}\cdot\overline{b}=\overline{a}\cdot\overline{c}=1$*, então* $\overline{ab}=\overline{ac}$*. Podemos supor, sem perda de generalidade, que* $b\geq c$*. Logo,* $p|ab-ac=a(b-c)$*. Como* p *é primo e* $p\nmid a$*, então* $p|b-c$*. Mas como* $0\leq b-c<b<p$*, então* $b=c$*, o que mostra a unicidade.* ■

Teorema 9.16 *(Teorema de Wilson) O número natural* $p>1$ *é primo se, e somente se,* $(p-1)!\equiv -1(mod\ p)$*.*
Demonstração: $(\Rightarrow)$ *Se* p *é primo então, pelo corolário anterior, para cada* $i\in\{1,2,...,p-1\}$*, existe um único* $j\in\{1,2,..,p-1\}$ *tal que* $\overline{i}\cdot\overline{j}=\overline{1}$*, isto é,* $i\cdot j\equiv 1(mod\ p)$*. Pode*

ocorrer $i = j$ *somente nos casos em que* $i = 1$ *ou* $i = p - 1$, *pois* $i^2 \equiv 1(mod\ p) \Leftrightarrow p|i^2 - 1 = (i + 1)(i - 1) \Leftrightarrow p|i + 1$ *ou* $p|i - 1 \Leftrightarrow i = p - 1$ *ou* $i = 1$ *já que* $0 < i < p$ *e* p *é primo. Assim,* $2 \cdot 3 \cdot \ ... \ \cdot (p-2) \equiv 1(mod\ p)$, $1 \cdot 2 \cdot 3...(p-2) \cdot (p-1) \equiv 1 \cdot 1 \cdot (p-1)(mod\ p)$ *e, portanto,* $(p-1)! \equiv -1(mod\ p)$.
($\Leftarrow$) *Se* p *não é primo, então existe um inteiro* a *tal que* $1 < a < p$ *e* $a|p$. *Assim,* $a|(p-1)!$. *Como* $a \nmid 1$, *então* $a \nmid (p-1)! + 1$. *Como* $a|p$, *então* $p \nmid (p-1)! + 1$, *ou seja não ocorre* $(p-1)! \equiv -1(mod\ p)$. ∎

Exemplo 9.14 *Se* p *é um primo e* a *é um inteiro não divisível por* p, *então, pelo Pequeno Teorema de Fermat,* $p|a^{p-1} - 1$; *pelo Teorema de Wilson,* $(p-1)! \equiv -1(mod\ p)$, *isto é,* $p|(p-1)! + 1$. *Assim,* $p|a^{p-1} - 1 + (p-1)! + 1 = a^{p-1} + (p-1)!$. *Por exemplo,* $7|6^6 + 6!$.

Exemplo 9.15 *Alguns conjuntos do cotidiano podem ser identificados com algum* $\mathbb{Z}_n$. *Por exemplo, conjunto das horas pode ser identificado com* $\mathbb{Z}_{24}$ *e o conjunto das medidas inteiras dos ângulos (em graus) pode ser identificado com* $\mathbb{Z}_{360}$.

9.5 A Prova dos Noves Fora

A "prova dos noves fora", em tempos passados, era usada para verificar se o resultado de uma soma estava correta. Por exemplo, para verificar-se que $5782 + 4291 = 9973$, pelo método da "prova", deve-se ir somando os algarismos do primeiro membro da igualdade e subtraindo 9 sempre que a soma for maior ou igual a 9; faz-se o mesmo para os algarismos do segundo membro e, no final, comparar os resultados obtidos. Para os algarismos do primeiro membro, temos:
$5 + 7 + 8 + 2 + 4 + 2 + 9 + 1 = \mathbf{12} + 8 + 2 + 4 + 2 + 9 + 1 \rightarrow$

$\mathbf{3}+8+2+4+2+9+1 = \mathbf{11}+2+4+2+9+1 \rightarrow$
$\mathbf{2}+2+4+2+9+1 = \mathbf{4}+4+2+9+1 = \mathbf{8}+2+9+1 =$
$\mathbf{10}+9+1 \rightarrow \mathbf{1}+9+1 = \mathbf{10}+1 \rightarrow \mathbf{1}+1 = \mathbf{2}$
Para os algarismos do segundo membro, temos:
$9+9+7+3 \rightarrow 9+7+3 \rightarrow 7+3 = 10 \rightarrow 1$
Comparando os resultados encontrados, como $1 \neq 2$, então a conta está errada.

Utilizemos as congruências para avaliar a validade do método.

Se m é um inteiro positivo, então:

$$m = a_n 10^n + a_{n-1}10^{n-1} + ... + a_1 10 + a_0,$$

em que cada $a_i \in \mathbb{Z}$ e $0 \leq a_i < 10$. Assim,
$m = a_n(9+1)^n + a_{n-1}(9+1)^{n-1} + ... + a_1(9+1) + a_0 =$
$a_n(9c_n+1) + a_{n-1}(9c_{n-1}+1) + ... + a_1(9c_1+1) + a_0 =$
$9(a_n c_n + a_{n-1}c_{n-1} + \ldots + a_1 c_1) + (a_n + a_{n-1} + \ldots + a_1 + a_0)$.
Logo, $m \equiv (a_n + a_{n-1} + \ldots + a_1 + a_0)(mod\ 9)$, isto é, m e $a_n + a_{n-1} + \ldots + a_1 + a_0$ apresentam o mesmo resto na divisão por 9.

Assim, em $\mathbb{Z}_9$ temos $\overline{1599} = \overline{1+5+9+9} = \overline{24} = \overline{2+4} = \overline{6}$, isto é, o resto da divisão de 1599 por 9 é 6. Como $\overline{a}+\overline{b} = \overline{a+b}$ e $\overline{a}.\overline{b} = \overline{ab}$, então podemos aplicar a "prova dos noves fora" para saber se o resultado de operações contém algum erro.

Exemplo 9.16 *Verificar se* $453 + 751 = 1104$ *e* $453 \cdot 751 = 340.303$
$\overline{453+751} = \overline{4+5+3} + \overline{7+5+1} = \overline{3} + \overline{4} = \overline{7}$;
$\overline{453 \cdot 751} = \overline{4+5+3} \cdot \overline{7+5+1} = \overline{3} \cdot \overline{4} = \overline{12} = \overline{3}$.

Assim, o resto da divisão de $453 + 751$ *e* $453 \cdot 751$ *por* 9

são, respectivamente, 7 *e* 3*. Agora, como o resto das divisões de* 1104 *e* 340.303 *por* 9 *são, respectivamente,* 6 *e* 4*, então, ambas as operações estão incorretas.*

Esse processo é útil para se verificar se a conta está errada, porém ele não garante que a conta esteja correta. Por exemplo, a conta $1836 + 4527 = 6453$ está errada, mas passa pela "prova dos noves fora".

10 Equações diofantinas lineares

Equações da forma $ax+by=c$, em que a, b e c são números inteiros, com $a \neq 0$ ou $b \neq 0$, são conhecidas como equações diofantinas lineares, em virtude de Diofante de Alexandria ter sido o primeiro a se ocupar deste tipo de equação.

Estaremos interessados em soluções inteiras para essas equações, isto é, em pares de inteiros x e y que satisfaçam a equação $ax + by = c$.

Nem toda equação diofantina possui soluções inteiras. Por exemplo dada a equação $6x + 10y = 327$, para valores inteiros para x e y, obtemos, no primeiro membro, um número par, enquanto o segundo membro é um número ímpar.

10.1 Soluções de equações diofantinas lineares

O teorema seguinte apresenta condições para a existência de soluções.

Teorema 10.1 *Sejam $a, b, c \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$ e $d = mdc(a, b)$. A equação $ax + by = c$ tem solução se, e somente se, $d|c$.*

Demonstração: ($\Rightarrow$) *Sejam x e y soluções de inteiros para a equação $ax+by = c$. Como $d = mdc(a, b)$, então $d|a$ e $d|b$. Logo, pelo Teorema* 4.1*, $d|(ax + by) = c$.*

($\Leftarrow$) *Se $d|c$, então existe $e \in \mathbb{Z}$ tal que $c = ed$. Como $d = mdc(a, b)$, pelo Teorema* 7.1*, existem r e s inteiros tais que $ra + sb = d$. Assim, $era + esb = ed = c$. Logo, $x = er$ e $y = es$ é solução da equação $ax + by = c$.* ∎

Corolário 10.2 *Sejam $a, b, c \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. Se $mdc(a, b) = 1$, então a equação $ax + by = c$ sempre tem solução.*

Corolário 10.3 *Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. A equação $ax + by = 1$ tem solução se, e somente se, $mdc(a, b) = 1$.*

O resultado a seguir apresenta o formato de todas as soluções de uma equação diofantina, caso elas existam.

Teorema 10.4 *Seja $ax+by = c$ uma equação diofantina tal que $d = mdc(a, b)$ divida c. Se r e s são inteiros tais que $d = ra+sb$, então:*

(i) o par $x_0 = r\cdot\frac{c}{d}$, $y_0 = s\cdot\frac{c}{d}$ é uma solução para $ax+by = c$;

(ii) as soluções (x, y) são dadas por $x = x_0 + t \cdot \frac{b}{d}$ e $y = y_0 - t \cdot \frac{a}{d}$, $t \in \mathbb{Z}$.

Demonstração: *Vamos considerar $a \neq 0$ e $b \neq 0$, pois o caso em que um deles é zero é elementar.*

(i) Substituindo x por $x_0 = r \cdot \frac{c}{d}$ e y por $y_0 = s \cdot \frac{c}{d}$ em $ax + by$, obtemos $a \cdot r\frac{c}{d} + b \cdot s\frac{c}{d} = (ar + bs) \cdot \frac{c}{d} = d \cdot \frac{c}{d} = c$. Assim, o par (x_0, y_0) é uma solução para $ax + by = c$.

(ii) Sejam x, y inteiros tais que $ax + by = c$. Desde que $ax_0 + by_0 = c$, então $ax+by = a\cdot x_0+b\cdot y_0$. Logo, $a\cdot(x-x_0) = b\cdot(y_0-y)$ (1). Como $d = mdc(a, b)$, então $d|a$ e $d|b$, ou seja, existem os inteiros a_1 e b_1 de maneira $a = a_1 \cdot d$ e $b = b_1 \cdot d$ (2). Pelo Corolário 7.3, $mdc(a_1, b_1) = 1$ (3). De (1) e (2) temos que $a_1 \cdot (x - x_0) = b_1 \cdot (y_0 - y)$. Assim, $a_1|b_1 \cdot (y_0 - y)$ (4). Por (3) e (4) e pelo Teorema 7.4, $a_1|(y_0 - y)$, ou seja, existe $t \in \mathbb{Z}$ tal que $y_0 - y = t \cdot a_1$, isto é, $y = y_0 - t \cdot a_1 = y_0 - t \cdot \frac{a}{d}$. Substituindo y_0-y por $t\cdot a_1$ na igualdade $a_1\cdot(x-x_0) = b_1\cdot(y_0-y)$, obtemos $a_1 \cdot (x - x_0) = b_1 \cdot t \cdot a_1$. Como $a_1 \neq 0$ (pois estamos considerando a e b diferentes de 0), então $x-x_0 = b_1\cdot t$, ou seja, $x = x_0 + t \cdot b_1 = x_0 + t \cdot \frac{b}{d}$.

Por outro lado, para $x = x_0 + t \cdot \frac{b}{d}$, $y = y_0 - t \cdot \frac{a}{d}$ *e* $t \in \mathbb{Z}$ *temos* $ax + by = a(x_0 + t.\frac{b}{d}) + b(y_0 - t \cdot \frac{a}{d}) = ax_0 + by_0 = c$, *ou seja,* (x, y) *é uma solução da equação.* ∎

Exemplo 10.1 *Encontrar todas as soluções inteiras da equação* $15x - 51y = 42$.

Nota-se, neste caso, que $a = 15$, $b = -51$ *e* $d = mdc(a, b) = 3$.

Precisamos encontrar r *e* s *tais que* $15r + (-51)s = 3$*:*
$51 = 3 \cdot 15 + 6 \Rightarrow 6 = 51 - 3 \cdot 15$*;*
$15 = 2 \cdot 6 + 3 \Rightarrow 3 = 15 - 2 \cdot 6$*;*

Assim, $3 = 15 - 2 \cdot 6 = 15 - 2 \cdot (51 - 3 \cdot 15) = 7 \cdot 15 - 2 \cdot 51 = 15 \cdot 7 + (-51) \cdot 2$, *ou seja,* $r = 7$ *e* $s = 2$.

Então, $x_0 = r \cdot \frac{c}{d} = 7 \cdot \frac{42}{3} = 98$, *e* $y_0 = s \cdot \frac{c}{d} = 2 \cdot \frac{42}{3} = 28$. *Portanto,*

$$x = x_0 + t \cdot \frac{b}{d} = 98 + t \cdot \frac{-51}{3} = 98 - 17t \text{ e}$$
$$y = y_0 - t \cdot \frac{a}{d} = 28 - t \cdot \frac{15}{3} = 28 - 5t.$$

Assim, as soluções são dadas por $x = 98 - 17t$ *e* $y = 28 - 5t$.

Exemplo 10.2 *Um clube precisa comprar bolinhas de tênis para um torneio. As bolinhas são vendidas em embalagens com 8 e com 14 unidades. Qual a quantidade de cada tipo de embalagem deve ser comprada para se obter um total de 100 bolinhas?*
Solução*: Considerando* x *e* y *as quantidades de embalagens com* 8 *e* 14 *bolinhas, respectivamente, precisamos que* x *e* y *satisfaçam a equação* $8x + 14y = 100$.

Vamos nos utilizar do teorema anterior para encontrar soluções para o nosso problema. Na notação do teorema temos $a = 8$, $b = 14$, $c = 100$ *e* $d = mdc(a, b) = 2$. *Já aprendemos a encontrar* r *e* s*:* $r = 2$ *e* $s = -1$.

Assim, encontramos $x_0 = 2 \cdot \dfrac{100}{2} = 100$ *e* $y_0 = -1 \cdot \dfrac{100}{2} = -50$.

Como só interessam as soluções não negativas, precisamos encontrar t *para que:*

$$x = x_0 + t\frac{14}{2} = 100 + 7t \text{ e } y = y_0 - t\frac{8}{2} = -50 - 4t$$

não sejam negativos, ou seja, precisamos que $100 + 7t \geq 0$ *e* $-50 - 4t \geq 0$.

Resolvendo as duas desigualdades chegamos que $t > -14,3$ *e* $t < -12,5$*, ou seja,* t *é inteiro e* $-14,3 < t < -12,5$*. Temos então duas possibilidades:* $t = -13$ *e* $t = -14$.

Para $t = -13$*, temos* $x = 9$ *e* $y = 2$*. Para* $t = -14$*,* $x = 2$ *e* $y = 6$.

Assim, deve-se comprar nove embalagens com 8 unidades e duas embalagens com 14 unidades, ou ainda, duas embalagens com 8 unidades e seis embalagens com 14 unidades.

Exercício 10.1 *Encontrar as soluções inteiras para as equações diofantinas:*
(a) $36x + 10y = 96$*;*
(b) $2x + 3y = 9$*;*
(c) $9x + 15y = 141$*;*
(d) $18x + 7y = 302$*;*
(e) $21x + 42y = 127$.

Exercício 10.2 *Encontrar as soluções inteiras e positivas das equações diofantinas do exercício anterior.*

Exercício 10.3 *Um pote com capacidade para* 900 *balas não está totalmente cheio. Se forem retiradas* 13 *balas de cada vez, sobram* 5 *balas. Se forem retiradas* 31 *balas de cada vez, sobram* 19 *balas. Utilizar equações diofantinas para determinar todas as possibilidades para a quantidade de balas que está no pote.*

Exercício 10.4 *Expressar o número* 100 *como uma soma de dois inteiros positivos, de modo que um seja múltiplo de* 7 *e o outro seja múltiplo de* 13*.*

Exercício 10.5 *Mostrar que se* x *e* y *são inteiros tais que* $2x + 3y$ *é múltiplo de* 17*, então* $9x + 5y$ *também é.*

11 O Último Teorema de Fermat

Neste capítulo avaliamos ternas de números que satisfazem o Teorema de Pitágoras e fazemos algumas generalizações.

11.1 Ternas pitagóricas

Uma *terna pitagórica* de números inteiros positivos é uma tripla ordenada (a, b, c) tal que $a^2 + b^2 = c^2$.

A terna (a, b, c) é *primitiva* quando $mdc(a, b, c) = 1$.

Exemplo 11.1 $(3, 4, 5)$, $(6, 8, 10)$ *e* $(9, 12, 15)$ *são ternas pitagóricas e a primeira delas é uma terna primitiva.*

Exercício 11.1 *Dada uma terna pitagórica primitiva* (a, b, c)*, mostrar que para todo* $n \in N^*$ *tem-se que* (an, bn, cn) *é uma terna pitagórica.*

Lema 11.1 *Dada uma terna pitagórica* (a, b, c)*, seja* $mdc(a, b, c) = d$*. Se tomarmos* $a_1 = a/d$*,* $b_1 = b/d$ *e* $c_1 = c/d$*, então* (a_1, b_1, c_1) *é uma terna pitagórica primitiva.*
Demonstração: *Desde que* $d = mdc(a, b, c)$*, então* $mdc(a_1, b_1, c_1) = 1$*. Agora,* $a_1^2 + b_1^2 = (a/d)^2 + (b/d)^2 = (a^2 + b^2)/d^2 = c^2/d^2 = c_1^2$. ∎

A partir do último exercício acima e do lema anterior, segue que podemos investigar sobre ternas pitagóricas com enfoque especificamente sobre as ternas primitivas.

Lema 11.2 *Se* (a, b, c) *é uma terna pitagórica primitiva, então exatamente um dentre os dois primeiros termos* a *e* b *é par e os outros dois são ímpares.*

Demonstração: *Se a e b são pares, então c também é par, o que contradiz o fato de $mdc(a,b,c) = 1$. Logo, não podem ser ambos pares.*
Se a e b são ímpares, então a é do tipo $2m+1$ e b é do tipo $2n+1$. Daí, $a^2 + b^2 = (4m^2 + 4m + 1) + (4n^2 + 4n + 1) = 4(m^2+m+n^2+n)+2 = c^2$. Logo, $2|c^2$ e $2^2 \nmid c^2$. Mas $2|c$ e isso implica $2^2|c^2$. Portanto, temos uma contradição. Desse modo, não pode ocorrer que a e b sejam ambos números pares. ∎

Lema 11.3 *Se (a,b,c) é uma terna pitagórica primitiva, então os termos a, b e c são dois a dois primos entre si.*
Demonstração: *Se $d = mdc(a,b) > 1$, então existe um número primo p tal que $p|d$ e, daí, $p|a$ e $p|b$. Logo, $p|a^2 + b^2 = c^2$ e, portanto, $p|c$. Mas isto contradiz o fato de (a,b,c) ser primitiva. Os outros dois casos são verificados do mesmo modo.* ∎

Lema 11.4 *Sejam $m,n,c \in \mathbb{N}$. Se $m \cdot n = c^2$ e $mdc(m,n) = 1$, então m e n são quadrados.*
Demonstração: *Sejam $m = {p_1}^{r_1} \cdot \ ... \ \cdot {p_k}^{r_k}$ e $n = {q_1}^{s_1} \cdot \ ... \ \cdot {q_j}^{s_j}$ as fatorações em primos de m e n. Como $mdc(m,n) = 1$, então os termos p_k são distintos dos termos q_j. Assim, $m \cdot n = {p_1}^{r_1} \cdot \ ... \ \cdot {p_k}^{r_k} \cdot {q_1}^{s_1} \cdot \ ... \ \cdot {q_j}^{s_j}$ é a fatoração de $m \cdot n$. Como, por hipótese, $m \cdot n = c^2$, então todos os coeficientes r_k e s_j são pares e portanto $m = a^2$ e $n = b^2$, com $a = ({p_1}^{r_1/2} \cdot \ ... \ \cdot {p_k}^{r_k/2})^2$ e $b = ({q_1}^{s_1/2} \cdot \ ... \ \cdot {q_j}^{s_j/2})^2$.* ∎

Dois números inteiros a e b têm a *mesma paridade* quando ambos são pares ou ambos são ímpares. Isto é equivalente a dizer que $a+b$ (ou $a-b$) é par.

Teorema 11.5 *Sejam $m,n \in \mathbb{N}$, tais que $1 \leq m < n$, $mdc(m,n) = 1$ e m e n têm paridades distintas. Então $a = 2mn$,*

$b = n^2 - m^2$ e $c = m^2 + n^2$ determinam uma terna pitagórica primitiva. Toda terna pitagórica primitiva é deste tipo (a, b, c).
Demonstração: *Como $a^2 + b^2 = (2mn)^2 + (n^2 - m^2)^2 = 4m^2n^2 + n^4 - 2m^2n^2 + m^4 = m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2 = c^2$, então (a, b, c) é uma terna pitagórica.*

Agora, se $mdc(a, b, c) > 1$, existe um número primo p tal que $p|mdc(a, b, c)$. Assim, se p é ímpar, como $p|a = 2mn$, segue que $p|m$ ou $p|n$. Como $p|c$ e $c = m^2 + n^2$, então $p|m$ e $p|n$. Portanto, $1 < p \leq mdc(m, n) = 1$, o que é uma contradição. Se $p = 2$ então $2|n^2 - m^2$. Logo, n^2 e m^2 tem a mesma paridade, portanto n e m tem a mesma paridade, contradizendo a hipótese.

Dessa forma, (a, b, c) é uma terna primitiva.

Seja (a, b, c) uma terna pitagórica primitiva e consideremos que a é par e b é ímpar. O caso onde a é ímpar e b é par é análogo. Daí, $a^2 = c^2 - b^2 = (c - b) \cdot (c + b)$ e, portanto, $(c - b)/2 \cdot (c + b)/2 = a^2/4$. Neste caso, pelo Lema 11.2 temos que c é ímpar. Então $c - b$ e $c + b$ são pares e, daí, $a^2/4 \in \mathbb{N}$. Assim, $a^2/4 = r \cdot s$, em que $r = (c - b)/2$ e $s = (c + b)/2$.

Se $d = mdc(r, s)$, então, $d|r \pm s$. Agora, como $r + s = (c-b)/2+(c+b)/2 = c$ e $r-s = (c-b)/2-(c+b)/2 = b$, então $d|mdc(b, c)$. Pelo Lema 11.3, $mdc(b, c) = 1$ e, desse modo, $d = 1$, portanto $mdc(r, s) = 1$. Pelo lema anterior, r e s são quadrados, digamos $r = m^2$ e $s = n^2$. Segue daí que $mdc(m, n) = 1$. Como $b = r - s = m^2 - n^2 = (m - n)(m + n)$ e b é ímpar então $n - m$ é ímpar.

Além disso, $n^2 - m^2 = s - r = b$, $m^2 + n^2 = r + s = c$ e de $a^2/4 = r \cdot s = m^2 \cdot n^2$, segue que $a = 2mn$. ∎

Segue então que as ternas pitagóricas primitivas são do tipo $(2mn, n^2 - m^2, m^2 + n^2)$ e, de um modo geral, cada terna pitagórica tem a forma $(k \cdot 2mn, k \cdot (n^2 - m^2), k \cdot (m^2 + n^2))$, com

$m, n, k \in \mathbb{N}^*$, $1 \leq m < n$, $mdc(m, n) = 1$ e $n - m$ ímpar.

Vejamos alguns casos de ternas primitivas:

m	n	$a = 2mn$	$b = n^2 - m^2$	$c = n^2 + m^2$
1	2	4	3	5
2	3	12	5	13
1	4	8	15	17
3	4	24	7	25
2	5	20	21	29
4	5	40	9	41

Desde que em cada terna pitagórica primitiva ocorre um termo par e dois termos ímpares, para os próximos passos, faremos a convenção de que o primeiro termo a é par e, desse modo, b e c são ímpares.

Exercício 11.2 *Seja $b \in \mathbb{N}$, tal que $1 < b$ e b é ímpar. Mostrar que b ocorre em pelo menos uma terna pitagórica primitiva. Sugestão: todo ímpar é da forma $2t - 1 = t^2 - (t - 1)^2, t \in \mathbb{N}^*$. Observar o Teorema* 11.5.

Exercício 11.3 *Seja $a = 4t,\ t \in \mathbb{N}^*$. Mostrar que a ocorre em pelo menos uma terna pitagórica primitiva. Sugestão: Observar Teorema* 11.5.

Exercício 11.4 *Seja p um inteiro primo tal que $2 < p$. Mostrar que a terna $(\frac{p^2-1}{2}, p, \frac{p^2+1}{2})$ é pitagórica primitiva.*

Exercício 11.5 *Seja p um inteiro primo tal que $2 < p$. Mostrar que a terna $(\frac{p(p^2-1)}{2}, p^2, \frac{p(p^2+1)}{2})$ é pitagórica não primitiva.*

Exercício 11.6 *Seja p um inteiro primo tal que $2 < p$. Mostrar que a terna $(\frac{p^4-1}{2}, p^2, \frac{p^4+1}{2})$ é pitagórica primitiva.*

11.2 Sobre o Último Teorema de Fermat

Pierre de Fermat (1601 - 1665), embora não tenha sido um matemático profissional, foi considerado pelo filósofo, físico e matemático francês Blaise Pascal (1623 - 1662) um grande matemático.

Seu interesse na Matemática estava principalmente em questões vinculadas a desafios e problemas. Suas inquirições matemáticas atravessaram várias gerações. Ele fez contribuições importantes para o cálculo geométrico, infinitesimal e, principalmente, para a teoria dos números. O Último Teorema de Fermat, como passou a ser indicado, é o mais famoso dos trabalhos de Fermat. O seu enunciado simples diz que a equação: $x^n+y^n = z^n$ não tem solução de números inteiros e positivos para $n > 2$. Fermat escreveu nas margens do livro 'Aritmética', de Diofanto, com o qual estava trabalhando, que conseguira uma demonstração para o problema acima, mas que não havia espaço suficiente para ela na margem do livro. Hoje, não se acredita que ele tenha conseguido uma demonstração correta do problema, visto que este Teorema de Fermat, mesmo tendo atraído a atenção de muitos matemáticos, por mais de 300 anos ficou em aberto. O Último Teorema de Fermat desafiou matemáticos por 358 anos e apenas em 1993, o matemático britânico Andrew Wiles conseguiu uma demonstração que ainda precisou de reparos e só tornou-se definitiva em 1995. Para tanto Wiles utilizou recursos sofisticados dos quais Fermat não dispunha.

A seguir, daremos uma resposta parcial ao Último Teorema de Fermat, com uma contribuição dada pelo próprio Fermat.

Lema 11.6 *Sejam $n, r, s, t \in \mathbb{N}$ tais que $r|n$, $s|n$ e $t|n$. Se existe solução de inteiros positivos para a equação* [1] $x^n + y^n = z^n$, *então também há solução de inteiros positivos para* [2] $x^r + y^s = z^t$.

Demonstração: *De $r|n$, $s|n$ e $t|n$, segue que existem $a, b, c \in \mathbb{N}$ de modo que $n = ar = bs = ct$. Agora, seja (x_1, y_1, z_1) uma solução para a equação* [1] $x^n + y^n = z^n$, *isto é,* ${x_1}^n + {y_1}^n = {z_1}^n$. *Daí,* ${x_1}^{ar} + {y_1}^{bs} = {z_1}^{ct}$. *Tomando* $x_2 = {x_1}^a$, $y_2 = {y_1}^b$ *e* $z_2 = {z_1}^c$, *segue que* ${x_2}^r + {y_2}^s = {z_2}^t$ *e, portanto, (x_2, y_2, z_2) é uma solução para a equação* [2]. ∎

Exercício 11.7 *Seja $n \in \mathbb{N}$ tal que $4|n$. Mostrar que se $x^4 + y^4 = z^2$ não tem solução de inteiros positivos, então $x^n + y^n = z^n$ também não tem solução de inteiros positivos.*

Exercício 11.8 *Sejam $n, a, b, c \in \mathbb{N}^*$ e $d = mdc(a, b, c)$ tais que (a, b, c) é solução da equação $x^n + y^n = z^n$. Então $(\frac{a}{d}, \frac{b}{d}, \frac{c}{d})$ é uma terna primitiva que também é solução da equação $x^n + y^n = z^n$.*

Em vista do exercício anterior, vamos nos ater somente a soluções que são ternas primitivas e vamos denominar tais soluções de *soluções primitivas.*

Exercício 11.9 *Mostrar que se (a, b, c) é uma solução primitiva da equação $x^4 + y^4 = z^2$, então a e b são primos entre si.*

Teorema 11.7 ***(Fermat)*** *A equação $x^4 + y^4 = z^2$ não tem solução primitiva de inteiros positivos.*

Demonstração: *Suponhamos que a equação $x^4 + y^4 = z^2$ tenha solução de inteiros positivos. Seja $S = \{z \in \mathbb{N} : x^4 + y^4 = z^2,$ para $x, y \in \mathbb{N}$ e $mdc(x, y, z) = 1\}$. Assim, o conjunto $S \neq \emptyset$*

e $S \subseteq N$. *Logo, existe* z_0, *o menor elemento de* S. *Daí, existem* $x_0, y_0 \in \mathbb{N}$ *de maneira que* ${x_0}^4 + {y_0}^4 = {z_0}^2$ *e* x_0 *é o menor elemento de qualquer terna primitiva que seja solução dessa equação.*

Do exercício anterior, temos que $mdc(x_0, y_0) = 1$ *e daí* $mdc({x_0}^2, {y_0}^2) = 1$. *Como* $({x_0}^2)^2 + ({y_0}^2)^2 = {z_0}^2$, $mdc({x_0}^2, {y_0}^2) = 1$, *então* $({x_0}^2, {y_0}^2, z_0)$ *é uma terna pitagórica primitiva. De acordo com o Teorema* 11.5, *existem* $m, n \in \mathbb{N}$, *com* $n > m$, $mdc(m, n) = 1$ *e* $n-m$ *ímpar, tais que* ${x_0}^2 = 2mn, {y_0}^2 = n^2 - m^2$ *e* $z_0 = m^2 + n^2$.

Desde que m *e* n *têm paridades distintas, um tem que ser par e o outro ímpar. Nesse caso* n *é ímpar e* m *par, pois do contrário teríamos* $n = 2r$ *e* $m = 2s + 1$, *para* $r, s \in \mathbb{N}$ *e então* ${y_0}^2 = (2r)^2 - (2s+1)^2 = 4r^2 - 4s^2 - 4s - 1 = 4(r^2 - s^2 - s) - 1 = 4(r^2 - s^2 - s - 1) + 3$, *mas desde que* ${y_0}^2$ *é um quadrado perfeito ímpar, então deveria ter a forma* $4k + 1$.

Seja então $m = 2r$ *e* $n = 2s + 1$ *com* $r, s \in \mathbb{Z}$. *Daí* ${x_0}^2 = 2mn = 4nr$ *e* $(x_0/2)^2 = nr$. *Como* $mdc(m, n) = 1$, *então* $mdc(r, n) = 1$ *também e, desse modo,* r *e* n *são quadrados. Sejam* $r = w^2$ *e* $n = {z_1}^2$, *com* $w, z_1 \in \mathbb{N}$. *De* ${y_0}^2 = n^2 - m^2$, *segue que* $m^2 + {y_0}^2 = n^2$ *e como* $mdc(m, n) = 1$, *então* (m, y_0, n) *é uma terna pitagórica primitiva. Assim, existem* $u, v \in \mathbb{N}$ *tais que* $u > v$, $u-v$ *é ímpar,* $mdc(u, v) = 1$, *e* $m = 2uv$, $y_0 = u^2 - v^2$ *e* $n = u^2 + v^2$. *Daí,* $uv = m/2 = r = w^2$ *e, mais uma vez,* u *e* v *são quadrados. Consideremos* $u = {x_1}^2$ *e* $v = {y_1}^2$, *em que* $x_{1,1} \in \mathbb{N}$.

Assim, ${x_1}^4 + {y_1}^4 = u^2 + v^2 = n = z_1^2$. *Logo,* $z_1 \in S$, *pois* $n \in \mathbb{N}$ *e* $mdc(x_1, y_1, z_1) = 1$, *pois* $mdc({x_1}^2, {y_1}^2) = mdc(u, v) = 1$. *Contudo, como* $0 < z_1 \leq {z_1}^2 = n \leq n^2 < n^2 + m^2 = z_0$, *contradizendo o fato de* z_0 *ser o elemento mínimo de* S.

Portanto, o conjunto S é vazio e a equação $x^4 + y^4 = z^2$ não tem solução de inteiros positivos. ∎

Corolário 11.8 *A equação $x^n + y^n = z^n$ não tem solução de inteiros positivos, quando $4|n$.*
Demonstração: *A demonstração segue do teorema anterior e do exercício* 11.7. ∎

Corolário 11.9 *Se o Último Teorema de Fermat vale para todo número primo maior que* 2*, então o teorema é válido.*
Demonstração: *Suponhamos, por absurdo, que o teorema não vale. Assim, para algum $2 < n$ a equação* [1] $x^n + ^n = z^n$ *tem solução de inteiros positivos.*

Se n é um primo, isto contradiz a hipótese.

Se n é um composto, então $n = k \cdot p$ de maneira que p é primo. Se $p > 2$, então [1] $\Leftrightarrow x^{k \cdot p} + y^{k \cdot p} = z^{k \cdot p} \Leftrightarrow (x^k)^p + (^k)^p = (z^k)^p$ *e isto contradiz a hipótese. Agora, se n é apenas uma potência de* 2*, como $2 < n$, então $4|n$ e, pelo corolário anterior,* [1] *não tem solução.*

Portanto, se o Último Teorema de Fermat vale para todo número primo maior que 2*, o teorema vale para todo $n \in \mathbb{N}$ tal que $n > 2$.* ∎

Com o resultado desse corolário, a investigação sobre a validade do Último Teorema de Fermat pode se restringir aos números n primos. Mesmo assim a história nos mostrou o quão difícil foi a resolução deste problema de enunciado extremamente simples.

12 Números triangulares e quadrados perfeitos

Os números tratados neste capítulo têm um caráter lúdico e também geométrico, como veremos a seguir.

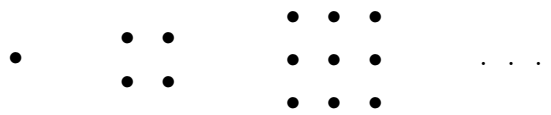
12.1 Quadrados

Um número $m \in \mathbb{N}^*$ é um *quadrado perfeito* se existe $y \in \mathbb{N}^*$ tal que $m = y^2$.

A seqüência dos quadrados é dada por:

$$(n^2)_{n\in\mathbb{N}^*} = (1, 4, 9, 16, 25, 36, ..., n^2, ...).$$

Podemos dar uma representação visual e geométrica para os quadrados:



12.2 Números triangulares

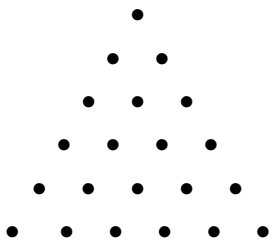
Dado $n \in \mathbb{N}^*$, o n-ésimo *número triangular* é definido por:

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

A seqüência dos números triangulares é dada por:

$$(t_n)_{n\in\mathbb{N}^*} = (1, 3, 6, 10, 15, 21, ...).$$

A disposição geométrica a seguir dá a motivação para o nome de número triangular:



Cada triângulo de lado n é determinado por $t_n = 1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$ pontos.

Teorema 12.1 *Seja $k \in \mathbb{N}^*$. O número k é triangular se, e somente se, $8k+1$ é um quadrado perfeito.*

Demonstração: *($\Rightarrow$) Seja k um número triangular, isto é, $k = t_n$, para algum $n \in \mathbb{N}^*$. Então: $8k+1 = 8 \cdot t_n + 1 = 8 \cdot \frac{n(n+1)}{2} + 1 = 4n^2 + 4n + 1 = (2n+1)^2$. Logo $8k+1$ é um quadrado perfeito. ($\Leftarrow$) Seja $8k+1$ um quadrado perfeito, isto é, $8k+1 = n^2$, para algum $n \in \mathbb{N}^*$. Daí, $k = \frac{n^2-1}{8}$. Desde que n^2 é ímpar, então n é ímpar também. Como $k \in \mathbb{N}^*$, então $n \geq 3$. Daí, $\frac{n-1}{2} \in \mathbb{N}^*$. Para $m = \frac{n-1}{2}$, segue que $t_m = t_{\frac{n-1}{2}} = \frac{\frac{n-1}{2} \cdot (\frac{n-1}{2}+1)}{2} = \frac{n^2-1}{8} = k$. Logo, k é um número triangular.* ∎

Exercício 12.1 *Mostrar que a soma de dois números triangulares consecutivos é um quadrado perfeito.*

Exercício 12.2 *Seja $n \in \mathbb{N}^*$ um quadrado perfeito. Mostrar que:*
(a) se n é par, então n é múltiplo de 4;
(b) se n é ímpar, então n é da forma $8k+1$, com $k \in \mathbb{N}^*$.

Exercício 12.3 *Dar exemplo de inteiro par múltiplo de 4 que não é quadrado perfeito.*

Exercício 12.4 *Dar exemplo de inteiro ímpar do tipo* $8k+1$ *que não é quadrado perfeito.*

Exemplo 12.1 *Na seqüência de números inteiros positivos* $(11, 111, 1111, ..., 111...111, ...)$ *não ocorre qualquer quadrado perfeito.*

O primeiro termo $11 = 8+3$ *não é quadrado perfeito.*

Se $n = 111...111 > 11$, *então* $n = 111...1000 + 111 = 111...1 \cdot 1000 + 8 \cdot 13 + 7 = 8 \cdot 111...1 \cdot 125 + 8 \cdot 13 + 7 = 8k+7$. *Assim, n não é um quadrado perfeito.*

Sejam $n, a, b \in \mathbb{N}$, com $1 \leq a$. A *diferença de dois quadrados* é qualquer número do tipo $n = a^2 - b^2$.

Desde que pode ocorrer $b = 0$, então cada quadrado perfeito é uma diferença de dois quadrados. Também, cada antecessor de um quadrado perfeito é do tipo $a^2 - 1^2$ e, assim, uma diferença de quadrados. Contudo, 2 e 6 não o são.

Lema 12.2 *Seja* $n \in \mathbb{N}$. *Se n é ímpar ou múltiplo de* 4, *então n é uma diferença de dois quadrados.*

Demonstração: *Se n é ímpar, como* $n \geq 1$, *então* $n-1$ *e* $n+1$ *são pares e, portanto,* $\frac{n-1}{2}$ *e* $\frac{n+1}{2}$ *não números naturais. Agora,* $(\frac{n+1}{2})^2 - (\frac{n-1}{2})^2 = \frac{n^2+2n+1-n^2+2n-1}{4} = \frac{4n}{4} = n$, *uma diferença de dois quadrados.*

Se n é do tipo $n = 4k$, *então* $n = (k+1)^2 - (k-1)^2$ *e, assim, n é uma diferença de dois quadrados.* ∎

Exercício 12.5 *Demonstrar a recíproca do lema anterior.*

Exercício 12.6 *Mostrar que a soma dos n primeiros números naturais ímpares é o n-ésimo quadrado perfeito, isto é,* $1 + 3 + 5 + 7 + ... + (2n-3) + (2n-1) = n^2$.

13 Números especiais e curiosidades

13.1 Números especiais

Alguns números naturais recebem uma denominação especial devido a satisfazerem determinadas propriedades. Como exemplo temos os números pares, ímpares, primos, quadrados, triangulares, dentre outros. Vamos apresentar mais alguns deles, sem nos preocuparmos em conhecer melhor suas propriedades.

Número de Mersenne: Um *número de Mersenne* é da forma $M_n = 2^n - 1$, em que n é um número natural.

Temos então que $M_0 = 0$, $M_1 = 1$, $M_2 = 3$, $M_3 = 7$, $M_4 = 15$, ... são números de Mersenne. Quando M_n é primo, dizemos que M_n é um primo de Mersenne.

Se n é composto, então M_n não é primo, pois $x^{ab} - 1 = (x^a - 1) \cdot (x^{a(b-1)} + x^{a(b-2)} + ... + x^{2a} + x^a + 1)$, para quaisquer a e b inteiros positivos. Assim, para que M_n seja primo é necessário que n seja primo. Mas, nem sempre n primo garante que M_n seja primo. Por exemplo, $2^{11}-1 = 2047 = 23 \cdot 89$.

Número de Fermat: Já vimos que um *número de Fermat* é da forma $M_n = 2^{2^n} + 1$, em que n é um número natural e que M_n é primo para $n = 0, 1, 2, 3, 4$, mas não é primo para $n = 5$.

Números perfeitos: Um número natural é *um número perfeito* se é igual à soma dos seus divisores positivos próprios.

Por exemplo, o número 6 é o menor número perfeito, pois os divisores positivos próprios de 6 são $1, 2$ e 3 e $6 = 1 + 2 + 3$. Os perfeitos seguintes são 28 e 496. Um número da forma $P = 2^{p-1} \cdot (2^p - 1)$, em que $2^p - 1$ é um primo de Mersenne, é sempre perfeito. A demonstração não é difícil e deixamos ao leitor como um bom exercício.

Exercício 13.1 *Fazer a demonstração indicada acima.*

Números amigos: Dois números naturais são *amigos* quando cada um deles é igual à soma dos divisores positivos próprios do outro.

Por exemplo, os divisores positivos próprios de $220 = 2^2 \cdot 5 \cdot 11$ são 1, 2, 4, 5, 10, 11, 20, 22, 44, 55 e 110; os divisores positivos próprios de $284 = 2^2 \cdot 71$ são 1, 2, 4, 71 e 142. Como $1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$ e $1 + 2 + 4 + 71 + 142 = 220$, então os números 220 e 284 são números amigos.

Estes são os menores números amigos. Os pares de números amigos seguintes são 1.184 e 1.210; 2.620 e 2.924; 5.020 e 5.564; 6.232 e 6.368; 10.774 e 10.856; 12.285 e 14.595; 17.296 e 18.416; 63.020 e 76.084; 66.928 e 66.992; 67.095 e 71.145; 69.615 e 87.633; 79.750 e 88.730.

Exercício 13.2 *Verificar que os três primeiros pares indicados acima são de números amigos.*

Primos gêmeos: *Primos gêmeos* são números primos p e q tais que $|p - q| = 2$.

Por exemplo, são pares de primos gêmeos: 3 e 5; 5 e 7; 11 e 13.

Exercício 13.3 *Encontrar mais dois pares de números gêmeos.*

Muitos outros tipos de números aparecem na literatura. Por exemplo, números levemente imperfeitos, sociáveis, capícuas, pentagonais, hexagonais, dentre outros.

Muitas questões sobre os números podem ser colocadas, especialmente a respeito dos primos, como por exemplo:

– Existem infinitos primos de Fermat?

– Existem infinitos primos de Mersenne?

– Existem infinitos pares de primos gêmeos?

– Existem infinitos números de Fermat que não são primos?

– Existe uma fórmula que gera os números primos?

– Cada número par maior que 5 é a soma de dois números primos ímpares? (Conjectura de Goldbach)

– Cada ímpar maior que 5 é soma de três primos ímpares? (Conjectura de Goldbach para ímpares)

– Existem números perfeitos ímpares?

Aos interessados sugerimos pesquisas para conhecer problemas em aberto na matemática, que podem ser encontrados na internet, nas bibliotecas ou com os próprios professores das diversas disciplinas.

13.2 Curiosidades

Muitas curiosidades podem ser encontradas a partir de operações com números. Colocamos, a seguir, alguns casos curiosos.

$153 = 1^3 + 5^3 + 3^3$;

$153 = 1 + 2 + 3 + \cdots + 17$;

$153 = 1! + 2! + 3! + 4! + 5!$;

$\sqrt{153 - (1 + 5 + 3)} = 15 - 3$;

$1634 = 1^4 + 6^4 + 3^4 + 4^4$;

$145 = 1! + 4! + 5!$

$111.111.111 \cdot 111.111.111 = 12.345.678.987.654.321.$

Multiplicação de 37 por múltiplos de 3 e de 3367 por múltiplos de 33:

$3 \cdot 37 = 111$	$33 \cdot 3367 = 11111$
$6 \cdot 37 = 222$	$66 \cdot 3367 = 22222$
$9 \cdot 37 = 333$	$99 \cdot 3367 = 33333$
$12 \cdot 37 = 444$	$132 \cdot 3367 = 44444$
$15 \cdot 37 = 555$	$165 \cdot 3367 = 55555$
$18 \cdot 37 = 666$	$198 \cdot 3367 = 66666$
$21 \cdot 37 = 777$	$231 \cdot 3367 = 77777$
$24 \cdot 37 = 888$	$264 \cdot 3367 = 88888$
$27 \cdot 37 = 999$	$297 \cdot 3367 = 99999$

Construindo pirâmides:

$$0 \cdot 9 + 1 = 1$$
$$1 \cdot 9 + 2 = 11$$
$$12 \cdot 9 + 3 = 111$$
$$123 \cdot 9 + 4 = 1111$$
$$1234 \cdot 9 + 5 = 11111$$
$$12345 \cdot 9 + 6 = 111111$$
$$123456 \cdot 9 + 7 = 1111111$$
$$1234567 \cdot 9 + 8 = 11111111$$
$$12345678 \cdot 9 + 9 = 111111111$$

$$1 \cdot 8 + 1 = 9$$
$$12 \cdot 8 + 2 = 98$$
$$123 \cdot 8 + 3 = 987$$
$$1234 \cdot 8 + 4 = 9876$$
$$12345 \cdot 8 + 5 = 98765$$
$$123456 \cdot 8 + 6 = 987654$$
$$1234567 \cdot 8 + 7 = 9876543$$
$$12345678 \cdot 8 + 8 = 98765432$$
$$123456789 \cdot 8 + 9 = 987654321$$

$$0 \cdot 9 + 8 = 8$$
$$9 \cdot 9 + 7 = 88$$
$$98 \cdot 9 + 6 = 888$$
$$987 \cdot 9 + 5 = 8888$$
$$9876 \cdot 9 + 4 = 88888$$
$$98765 \cdot 9 + 3 = 888888$$
$$987654 \cdot 9 + 2 = 8888888$$
$$9876543 \cdot 9 + 1 = 88888888$$
$$98765432 \cdot 9 + 0 = 888888888$$
$$987654321 \cdot 9 - 1 = 8888888888$$
$$9876543210 \cdot 9 - 2 = 88888888888$$

$$
\begin{aligned}
1 \times 1 &= 1 \\
11 \times 11 &= 121 \\
111 \times 111 &= 12321 \\
1111 \times 1111 &= 1234321 \\
11111 \times 11111 &= 123454321 \\
111111 \times 111111 &= 12345654321 \\
1111111 \times 1111111 &= 1234567654321 \\
11111111 \times 11111111 &= 123456787654321 \\
111111111 \times 111111111 &= 12345678987654321
\end{aligned}
$$

Uma boa recreação para leigos e alunos pré universitários é tentar entender porque ocorrem as igualdades.

Bibliografia

CHARTRAND, G.; POLIMENI, A.D.; ZHANG, P. **Mathematical proofs: a transition to advanced mathematics**. Boston: Addison Wesley, 2002.

FEITOSA, H.A.; NASCIMENTO, M.C.; ALFONSO, A.B. **Teoria dos conjuntos: sobre a fundamentação matemática e a construção dos conjuntos numéricos**. Rio de Janeiro: Editora Ciência Moderna, 2011.

FEITOSA, H.A.; PAULOVICH, L. **Um prelúdio à lógica**. São Paulo: Editora da UNESP, 2005.

HEFEZ, A. **Elementos de Aritmética**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2006.

MAIER, R.R. **Teoria dos números**. Brasília: Universidade de Brasília, 2005. (Notas de aula)

MILIES, C.P.; COELHO, S.P. **Números - Uma Introdução à Matemática**. São Paulo: EDUSP, 1998.

MONTEIRO, L.H.J. **Elementos de álgebra**. Rio de Janeiro: Livros Técnicos e Científicos, 1974. (IMPA: Coleção Elementos de Matemática).

ORE, O. **Invitation to number theory**. Washington: The Mathematical Association of America, 1967.

SANTOS, J.P.O. **Introdução à Teoria dos Números**. Rio de Janeiro: IMPA, 1998.

SIDKI, S. **Introdução à Teoria dos Números**. Rio de Janeiro: IMPA, 1975.

Sobre os autores

Mauri Cunha do Nascimento

Paulista de Catanduva, realizou a graduação, mestrado e doutorado em Matemática na UNICAMP, desenvolvendo trabalhos em Álgebra Comutativa. Iniciou sua carreira profissional na Universidade Estadual de Londrina, onde trabalhou entre os anos de 1979 e 1993. A partir de 1993, passou a ser professor efetivo do Departamento de Matemática da Faculdade de Ciências da UNESP, Câmpus de Bauru.

Hércules de Araujo Feitosa

O professor Hércules nasceu na cidade de São Paulo e cresceu em Gália, região de Bauru. Concluiu a Graduação em Matemática pela Fundação Educacional de Bauru em 1984. Defendeu Dissertação de Mestrado em Fundamentos da Matemática, na UNESP - IGCE, em 1992, com um trabalho sobre sistemas *fuzzy*. Concluiu o Doutorado em Lógica e Filosofia da Ciência, pela UNICAMP - IFCH, em 1998, com uma tese sobre traduções entre lógicas. É professor do Departamento de Matemática da UNESP - FC, Câmpus de Bauru, desde 1986. Atua no Programa de Pós-Graduação em Filosofia da UNESP - FFC, Câmpus de Marília, desde 2001.