UNIVERSIDADE FEDERAL DE ALAGOAS

Mestrado Profissional em Matemática em Rede Nacional

PROFMAT

DISSERTAÇÃO DE MESTRADO

Teoria dos Números: Uma Introdução Motivadora Direcionada aos Docentes do Ensino Básico

Alexandre Augusto Cavalcante de Faria

Instituto de Matemática

Maceió, Outubro de 2015

PROFMAT

UNIVERSIDADE FEDERAL DE ALAGOAS
INSTITUTO DE MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

ALEXANDRE AUGUSTO CAVALCANTE DE FARIA

TEORIA DOS NÚMEROS: UMA INTRODUÇÃO MOTIVADORA DIRECIONADA AOS DOCENTES DO ENSINO BÁSICO

MACEIÓ
2015

ALEXANDRE AUGUSTO CAVALCANTE DE FARIA

TEORIA DOS NÚMEROS: UMA INTRODUÇÃO MOTIVADORA DIRECIONADA AOS DOCENTES DO ENSINO BÁSICO

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) do Instituto de Matemática da Universidade Federal de Alagoas, como requisito parcial para obtenção do grau de Mestre em Matemática.

Orientador: Prof. Dr. José Carlos de Lima

MACEIÓ
2015

Catalogação na fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico
Bibliotecário Responsável: Valter dos Santos Andrade

F224t Faria, Alexandre Augusto Cavalcante de.
Teoria dos números: uma introdução motivadora direcionada aos docentes do Ensino básico / Alexandre Augusto Cavalcante de Faria. – 2015.
178 f. : il.

Orientador: José Carlos de Almeida Lima.
Dissertação (Mestrado Profissional em Matemática) – Universidade Federal de Alagoas. Instituto de Matemática. Programa de Pós Graduação de Mestrado Profissional em Matemática em Rede Nacional. Maceió, 2015.

Bibliografia: f. 177-178.

1. Matemática – Estudo ensino. 2. Professores – Formação. 3. Teorias dos números. 4. Divisão. 5. Congruência modular. I. Título.

CDU: 511.2

Folha de Aprovação

ALEXANDRE AUGUSTO CAVALCANTE DE FARIA

TEORIA DOS NÚMEROS: UMA INTRODUÇÃO MOTIVADORA DIRECIONADA AOS DOCENTES DO ENSINO BÁSICO

Dissertação submetida ao corpo docente do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) do Instituto de Matemática da Universidade Federal de Alagoas e aprovada em 16 de outubro de 2015.

Banca Examinadora:

Prof. Dr. José Carlos Almeida de Lima, UFAL (Orientador)

Prof. Dr. Fernando Pereira Micena, UFAL

Prof. Dr. Vicente Francisco de Sousa Neto

Ao meu pai,
Francisco Aníbal (*in memoriam*),
por me apresentar à Rainha das Ciências.

AGRADECIMENTOS

À DEUS, pois sem Ele, nada é possível.

À minha querida mãe, Rosa, pelo carinho salutar.

À minha esposa, Simone, companheira de todas as horas, por entender os tantos momentos de ausência.

À minha filha, Mariana, luz de minha vida.

À minha família. Em especial, ao meu tio Washington, pelo exemplo de força inabalável diante das situações adversas que a vida impõe.

À Sociedade Brasileira de Matemática, pela iniciativa do PROFMAT.

Ao Instituto de Matemática da Universidade Federal de Alagoas, por seus professores e técnicos, de modo especial, ao Prof. José Carlos pela valorosa orientação.

Aos colegas da turma PROFMAT/IM-UFAL 2013, pelo singular exemplo de dedicação e solidariedade acadêmica.

"A Teoria dos Números é uma pedra angular que sustenta uma apreciável porção do edifício matemático. E, claro, também é divertida."

TAO, Terence

RESUMO

Voltado ao professor de matemática do ensino básico, este trabalho apresenta extenso material motivador na área de Teoria dos Números, ramo da Matemática Pura que estuda os números inteiros, bem como uma larga classe de problemas que surge desse estudo. Os tópicos abordados são princípio da indução finita, divisibilidade, máximo divisor comum, números primos e congruência modular. A teoria é abordada de forma inteligível, equilibrada em seu formalismo, sempre precedida de exemplos motivadores e com uma quantidade razoável de exercícios resolvidos, dos clássicos até os de níveis olímpicos. Notas históricas também são inseridas como elemento motivacional. Também são apresentadas sugestões de atividades que podem ser aplicadas ao discente. O que se espera, com tudo, é ajudar o professor no seu desempenho em sala de aula, através da compreensão dos tópicos básicos de Teoria dos Números; instigando-o a formar doravante grupos olímpicos de treinamento intensivo, além de sensibilizá-lo acerca da importância de sua formação continuada, encorajando, assim, sua inscrição em algum programa de mestrado.

Palavras-chave: Teoria dos Números. Divisibilidade. Congruência Modular. Ensino de Matemática.

.

ABSTRACT

Facing the mathematics teacher of basic education, this paper presents extensive motivating material in Number Theory, area of Pure Mathematics branch that studies the integers as well as a wide class of problems arising from this study. Topics covered are finite principle of induction, divisibility, greatest common divisor, primes and modular congruence. The theory is discussed in an understandable, balanced in its formalism, always preceded by motivating examples and with a reasonable amount of exercise resolved, the classics to the Olympic level. Historical notes are also included as a motivational element. We also present suggestions for activities that can be applied to the student. What is expected, with everything, is to help the teacher in their performance in the classroom, by understanding the basic topics of number theory; urging him to now Olympic form groups of intensive training, and make them aware of the importance of their continuing education and thereby encourage, your enrollment in any master's program.

Key Word: Number Theory. Divisibility. Modular Congruence. Mathematics Teaching.

SUMÁRIO

INTRODUÇÃO

A cada dia que passa, constata-se que os profissionais do ensino são mais cobrados quanto à eficácia do seu trabalho, bem como quanto às exigências de uma formação mais sólida. Nesse contexto, o professor é convidado a ver sua profissão como algo a ser zelado e adubado com preparo teórico. Por isso, é necessário que ele tenha um bom domínio dos conteúdos de sua área, além de material de estudo o qual seja possível revisar conteúdos que não foram assimilados de forma eficiente durante sua graduação.

O professor de matemática não fica fora dessa realidade.

Nesse sentido, o objetivo deste trabalho é a elaboração de um extenso material na área de Teoria dos Números voltado ao professor de matemática do ensino básico. Visamos, então, aprimorar sua formação, subsidiando a sua prática pedagógica com atividades propostas, além de conscientizá-lo acerca da importância de sua formação continuada.

A Teoria dos Números é o ramo da Matemática que estuda os mistérios dos números inteiros. Sua utilidade à humanidade, no processo de criptografia usado nas transações bancárias pela internet, por exemplo; além dos desafiadores e belíssimos problemas, fazem dessa área, até hoje, uma das mais atrativas e inspiradoras dos amantes da Matemática.

São três os principais ramos da Teoria dos Números: Teoria Elementar, Teoria Analítica e Teoria Algébrica.

Este trabalho cobre os tópicos básicos da Teoria Elementar, algumas vezes, simplesmente chamada de *Aritmética*.

O trabalho foi estruturado em capítulos, divididos em seções, cada uma detalhando um tema central e trazendo alguns teoremas fundamentais. A teoria é abordada de forma inteligível, equilibrada em seu formalismo, muitas vezes precedida de contextualização histórica. Os conceitos são introduzidos através de exemplos e estes, por sua vez, organizados em uma linha crescente de dificuldade. Buscamos, desta forma, primeiro motivar e somente depois demonstrar formalmente algum resultado. Muitos desses exemplos são problemas resolvidos, que mostram que não é necessário um grande número de ferramentas sofisticadas para resolvê-los. Ao final de cada capítulo, segue uma lista de problemas, além de uma nota histórica, que foi inserida como elemento motivacional.

Fornecemos, a seguir, uma breve descrição do trabalho.

No capítulo 1, iniciamos com uma breve revisão sobre a caracterização dos números inteiros. Depois, introduzimos o poderoso *Princípio da Indução Finita*, que será utilizado nos

capítulos seguintes para demonstrar fatos importantes inerentes aos números inteiros. Esse capítulo pode ser estudado de forma independente, ou omitido, se o leitor já estiver familiarizado com a técnica de demonstração por indução.

No capítulo 2, definimos a importante noção de *divisibilidade* no conjunto dos números inteiros; enfatizamos a *Divisão Euclidiana*; provamos o *Teorema da Representação de um Número em uma Base qualquer* $b > 1$ e obtemos alguns critérios de divisibilidade.

No capítulo 3, dedicado à salutar noção de *máximo divisor comum (mdc)*, descrevemos o importante *Algoritmo de Euclides* para o cálculo do mdc de dois inteiros; explanamos sobre sua noção dual – o *mínimo múltiplo comum (mmc)* – e, ao final, discutimos a resolução de certas equações envolvendo inteiros.

No capítulo 4, nosso propósito é estudar as propriedades básicas dos números primos, um dos conceitos mais importantes de toda a matemática. Provamos o *Teorema Fundamental da Aritmética (TFA)*, e apresentamos suas principais consequências. Discutimos sobre distribuição dos números primos, apresentando o *Crivo de Eratóstenes*, que nos introduz à difícil tarefa de procurar e identificar números primos. Discorremos sobre expressões decimais finitas e infinitas e, ao final, apresentamos dois resultados interessantes.

No capítulo 5, definimos congruência módulo m e apresentamos suas propriedades fundamentais. Discorremos sobre teoremas importantes devidos a Wilson, Fermat e Euler, os quais somos capazes de obter resultados surpreendentes. Oferecemos também uma breve discussão acerca de sistemas de congruências lineares.

No capítulo 6, com intuito de mostra amplitude e eficiência dos resultados desenvolvidos nos capítulos anteriores, apresentamos uma miscelânea de 25 problemas olímpicos, juntamente com suas resoluções.

No capítulo 7, apresentamos algumas sugestões de atividades, que permitirão ao professor trabalhar em sala de aula alguns conteúdos apresentados neste trabalho.

No capítulo 8, expomos algumas sugestões para resolução dos problemas propostos. Aconselhamos só consultar esse capítulo depois de tentar exaustivamente resolver os problemas.

Com tudo, ressaltamos que esse trabalho é resultado de uma extensa pesquisa bibliográfica, e reflete nossa preocupação em contribuir de forma significativa à formação continuada do professor de matemática.

1 – PRINCÍPIO DA INDUÇÃO FINITA

Na matemática, muitas vezes resultados são enunciados a partir da consideração de casos particulares. Mas eles só são tidos como verdadeiros se puderem ser demonstrados, isto é, deduzidos de resultados já conhecidos. A aprendizagem da Matemática passa, necessariamente, pela construção dessas demonstrações.

Neste capítulo, iniciamos uma breve revisão sobre a caracterização dos números inteiros, enfatizando o *Princípio da Boa Ordenação*. Depois, introduzimos uma ferramenta básica de fundamental importância na obtenção de "provas" matemáticas, conhecido como *Princípio da Indução Finita.* Ele será utilizado nos capítulos seguintes para demonstrar fatos importantes inerentes aos números inteiros.

1.1 NÚMEROS INTEIROS

O ponto de partida deste trabalho é admitir a existência do *conjunto dos números inteiros*

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

juntamente com as operações de adição $(a, b) \to a + b$ e de multiplicação $(a, b) \to a \cdot b$ (denotaremos $a \cdot b$ também por ab), que gozam das seguintes propriedades:

1) **A adição e a multiplicação são bem definidas:**
   Para todos $a, b, a', b' \in \mathbb{Z}$, se $a = a'$ e $b = b'$, então $a + b = a' + b'$ e $ab = a'b'$.
2) **A adição e a multiplicação são comutativas:**
   Para todos $a, b \in \mathbb{Z}$, $a + b = b + a$ e $ab = ba$.
3) **A adição e a multiplicação são associativas:**
   Para todos $a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$ e $(ab)c = a(bc)$.
4) **A adição e a multiplicação possuem elementos neutros:**
   Para todo $a \in \mathbb{Z}$, $a + 0 = a$ e $a \cdot 1 = a$.
5) **A adição possui elementos simétricos:**
   Para todo $a \in \mathbb{Z}$, existe b (que denotaremos por $-a$) tal que $a + b = 0$.
6) **A multiplicação é distributiva em relação à adição:**
   Para todo $a, b, c \in \mathbb{Z}$, tem-se $a(b + c) = ab + ac$.

Uma vez que a adição e a multiplicação no conjunto dos números inteiros possuem as propriedades de 1 a 6, dizemos que os elementos de $\mathbb{Z}$, juntamente com suas operações, estão sujeitos às leis básicas da aritmética, ou na terminologia moderna dizemos que $\mathbb{Z}$ é um *anel*. Existem outros conjuntos que são anéis, por exemplo, o conjunto $\mathbb{Q}$ dos números racionais e o conjunto $\mathbb{R}$ dos números reais.

Em $\mathbb{Z}$ há um subconjunto que se destaca, qual seja, o conjunto dos *números naturais*:

$$\mathbb{N} = \{1,2,3, \dots\}.$$

A operação de adição permite-nos definir a operação de *subtração*: dados dois números inteiros a e b, define-se o número *b menos a*, denotado por $b - a$, como sendo

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

Admitimos também que no conjunto dos números inteiros valem as seguintes propriedades:

7) Fechamento de $\mathbb{N}$: O conjunto dos números naturais é fechado para adição e multiplicação, ou seja, para todo $a, b \in \mathbb{N}$, tem-se que $a + b \in \mathbb{N}$ e $ab \in \mathbb{N}$.

8) Tricotomia: Dados $a, b \in \mathbb{Z}$, uma e apenas uma, das seguintes possibilidades é verificada:

$$(i)\ a = b; \qquad (ii)\ b - a \in \mathbb{N}; \qquad (iii) - (b - a) \in \mathbb{N}.$$

Dados $a, b \in \mathbb{Z}$, dizemos que a é "$menor\ do\ que\ ou\ igual\ a$" b, denotado por $a \leq b$, toda vez que a Propriedade $8)(ii)$ é verificada, ou quando $a = b$. Note que

$$a \leq b \quad \Leftrightarrow \quad b - a \in \mathbb{N} \cup \{0\}.$$

A relação "*menor do que ou igual a"* possui as seguintes propriedades:

9) Reflexividade: Para todo $a \in \mathbb{Z}$, $a \leq a$.

10) Antissimetria: Se para todo $a, b \in \mathbb{Z}$, $a \leq b$ e $b \leq a$, então $a = b$.

11) Transitividade: Se para todo $a, b, c \in \mathbb{Z}$, $a \leq b$ e $b \leq c$, então $a \leq c$.

Com as propriedades acima, que goza a relação "menor do que ou igual a", $\mathbb{Z}$ é chamado de *conjunto ordenado***.** Note que $\mathbb{Q}$ e $\mathbb{R}$ também são conjuntos ordenados.

As propriedades dos números inteiros e de suas operações, que descrevemos até o momento, não bastam para caracterizá-los, destaca Hefez [1]. De fato, precisamos de uma propriedade adicional, o *Princípio da Boa Ordenação*, que passamos a descrever.

Dizemos que um subconjunto S de $\mathbb{Z}$ é *limitado inferiormente* quando existe pelo menos um número inteiro que é menor do que ou igual a todos os elementos do conjunto S. Perceba que o menor elemento de S, se existir, é único. O conjunto vazio é por definição

limitado inferiormente. Note, por exemplo, que $\mathbb{Z}$ não é limitado inferiormente, nem possui menor elemento.

12) Princípio da Boa Ordenação (PBO): *"Todo conjunto não vazio de números inteiros e limitado inferiormente possui um menor elemento"*.

Assumindo o PBO como verdade, dizemos que $\mathbb{Z}$ é um *conjunto bem ordenado***.** Em particular, como qualquer subconjunto de $\mathbb{N}$ é limitado inferiormente, temos que: *"todo subconjunto não vazio de números naturais possui um elemento mínimo".*

Assumiremos neste trabalho que o conjunto dos números inteiros gozará das propriedades acima mencionadas. Nesse caso, dizemos que $\mathbb{Z}$ é um *anel bem ordenado*.

Isso constitui a *base axiomática* necessária para o desenvolvimento da teoria, ou seja, todos os resultados (teoremas, proposições, corolários, lemas) são demonstrados assumindo que $\mathbb{Z}$ *é um anel bem ordenado*. Para um aprofundamento acerca da *base axiomática* aqui proposta, aconselhamos a leitura de [2].

1.2 DEDUÇÃO E INDUÇÃO

Para se compreender o *Princípio da Indução Finita (PIF)*, inicialmente é necessário saber distinguir entre dedução e indução, além de como esses métodos são utilizados na matemática.

A *dedução* é a passagem de uma afirmação geral para uma particular. Um exemplo simples:

(a) Todo brasileiro que mora em Alagoas gosta de Matemática.

(b) Geraldo é um brasileiro que mora em Alagoas.

(c) Geraldo gosta de matemática.

A afirmação (c) é obtida da afirmação geral (a) com o auxílio da afirmação (b).

A *indução* é a tentativa de generalização de uma afirmação particular. Ilustremos com um exemplo:

(1) 230 é divisível por 5.

Com base nessa afirmação, podemos fazer uma série de afirmações gerais. Por exemplo:

(2) Todo número com três dígitos é divisível por 5.

(3) Todo número terminado por zero é divisível por 5.

(4) Todo número terminado por 30 é divisível por 5.

(5) Todo número cuja soma de seus algarismos é 5 é divisível por 5.

As afirmações (2), (3), (4) e (5) são tentativas de generalização do caso particular (1). As afirmações (3) e (4) são verdadeiras, enquanto (2) e (5) são falsas.

Temos a seguinte questão: como usar indução em matemática de forma a obter somente conclusões verdadeiras? A próxima seção deste capítulo responderá essa pergunta, mas antes vamos a dois exemplos que figuram inadmissíveis generalizações em matemática.

Exemplo 1.1. Seja a soma dos n primeiros números ímpares, denotada por

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

Nosso propósito é conseguir uma fórmula que nos dê o valor desse somatório, para qualquer $n \in \mathbb{N}$, sem que para isso somemos todos os inteiros ímpares menores do que ou iguais a $2n - 1$.

É fácil ver que:

$$S_1 = 1 = 1^2$$
$$S_2 = 1 + 3 = 4 = 2^2$$
$$S_3 = 1 + 3 + 5 = 9 = 3^2$$
$$S_4 = 1 + 3 + 5 + 7 = 16 = 4^2$$

Como base nos resultados obtidos, poderíamos afirmar que, para todo número natural *n*,

$$S_n = n^2\ .$$

■

Exemplo 1.2. Considere o trinômio $P(n) = n^2 + n + 41$. Substituindo *n* por 1, 2, 3,…, 10, obtemos, respectivamente, os números primos 43, 47, 53, 61, 71, 83, 97, 113, 131, 151. Poderíamos afirmar, com base nesses resultados, que todos os valores que o trinômio $P(n)$ assume é um número primo, sempre que n for qualquer número natural.

■

Inferir conclusões gerais com respeito a um número natural somente com base no fato de essa afirmação ser verdadeira para certos valores de *n* é inadmissível na Matemática. Por um lado, a afirmação geral do exemplo 1.1 é verdadeira (provaremos formalmente na próxima seção, exemplo 1.4), mas o que garante isso? Por outro lado, a afirmação geral do exemplo 1.2 é falsa. De fato, se estudarmos cuidadosamente o trinômio $P(n) = n^2 + n + 41$, veremos que os valores de $P(n)$ são números primos quando substituímos *n* por 1, 2,…, 39. Todavia, para $n = 40$, temos:

$$P(40) = 40^2 + 40 + 41 = 40(40 + 1) + 41 = (41)(40 + 1) = 41^2$$

que é um número composto. Para sua informação, Hefez afirma em [3] que se pode provar que não existe nenhum polinômio em uma variável com coeficientes inteiros cujos valores nos naturais sejam sempre primos.

Matemáticos famosos verificaram que algumas proposições eram verdadeiras em certos casos especiais, chegando até a conjecturar sua validade, uma vez que seus esforços à procura de uma demonstração foram em vão. Todavia, muitas dessas proposições no caso geral eram falsas. O exemplo a seguir mostra uma dessas situações.

Exemplo 1.3. Pierre de Fermat (1601 – 1665), matemático francês, verificou que os números

$$2^{2^0}+1=3;\ 2^{2^1}+1=5;\ 2^{2^2}+1=17;\ 2^{2^3}+1=257;\ 2^{2^4}+1=65\,537$$

são todos números primos, e conjecturou que todos os números dessa forma ($2^{2^n}+1$, onde n é zero ou um inteiro positivo) – os quais são denominados *números de Fermat* – são primos também. Entretanto, o eminente matemático suíço, Leonard Euler (1707 – 1783), descobriu um século depois, que:

$$2^{2^5}+1=4\,294\,967\,297=(641)(6\,700\,417)$$

é um número composto. A propósito, segundo Ribenboim [4], o maior número primo de Fermat conhecido até o momento é justamente o 65 537 (o quarto primo). ■

1.3 PRINCÍPIO DA INDUÇÃO FINITA (PIF)

Os exemplos 1.2 e 1.3 denotam que uma afirmação pode ser válida em uma série de casos particulares e falsa em geral. Suponhamos agora que uma afirmação seja válida em muitos casos particulares e que seja impossível considerar todos os casos possíveis – por exemplo, uma afirmativa a respeito de todos os números naturais (como no exemplo 1.1). Como determinar se essa afirmativa é válida em geral? Algumas vezes, podemos resolver essa questão aplicando o *Princípio da indução finita (PIF)*. Ele é objeto central do teorema a seguir, cuja demonstração usa o fato de que *"todo subconjunto não vazio de números naturais possui um elemento mínimo"*.

Teorema 1.1.(Princípio da Indução Finita – PIF) *Seja A um subconjunto de números naturais. Se A possui as duas seguintes propriedades: (i) $1 \in A$; e (ii) $k+1 \in A$ sempre que $k \in A$. Então A contém todos os números naturais.*

Demonstração: Desejamos provar que se A é um subconjunto de números naturais, possuindo as propriedades (i) e (ii), então A, necessariamente, contém todos os números

naturais (A = $\mathbb{N}$). A prova que apresentamos é por contradição. Vamos supor que mesmo possuindo as propriedades (i) e (ii), A não contenha todos os números naturais. Seja B o conjunto de todos os números naturais que não pertencem ao conjunto A. Como B é um subconjunto não vazio de números naturais, então B possui um menor elemento e este é maior do que 1, pois $1 \in A$. Denote por a_0 o menor elemento de B. É claro que $a_0 - 1$ pertence a A e como A satisfaz a condição (ii), então o sucessor de $a_0 - 1$, que é a_0, também deve pertencer a A. Esta contradição nos leva a concluir que o conjunto B é vazio, o que conclui a demonstração.

■

No resto destas notas, $p(n)$ representa uma afirmação em relação ao natural n, podendo ser verdadeira ou falsa. O corolário a seguir é uma variante do PIF, apelidado às vezes de *Princípio "Fraco" de Indução Finita.*

Corolário 1.1 (PIF – forma "fraca"). *Considere n_0 um inteiro não negativo. Suponha que, para cada inteiro $n \geq n_0$, seja dada uma proposição $p(n)$. Suponha que se pode verificar as seguintes propriedades:*
(i) $p(n_0)$ é verdadeira;
(ii) se $p(k)$ é verdadeira então $p(k+1)$ também é verdadeira, para todo $k \geq n_0$.
Então, $p(n)$ é verdadeira para qualquer $n \geq n_0$.

Demonstração: Seja o conjunto

$$A = \{m \in \mathbb{N};\ p(n_0 + m - 1) \text{ é } verdadeira\ \}.$$

Claro que $1 \in A$, pois $p(n_0 + 1 - 1) = p(n_0)$ é verdadeira pela propriedade (i). Suponha que $k \in A$, logo $p(n_0 + k - 1)$ é verdadeira, o que implica por (ii) que

$$p((n_0 + k - 1) + 1) = p(n_0 + (k+1) - 1)$$

é verdadeira. Isso mostra que $k + 1 \in A$. Pelo teorema 1.1 temos que $A = \mathbb{N}$, ou seja, $p(n)$ é verdadeira para qualquer $n \geq n_0$. ■

O Princípio da Indução Finita pode ser entendido por meio do seguinte modelo. Suponha uma fila infinita de peças de dominó, um atrás do outro, distribuídos e espaçados. O que acontece se golpeamos o primeiro dominó? Todas as peças cairão? Teremos a certeza de que, golpeando a primeira peça de dominó, todas cairão se:

(a) a primeira peça cair ao ser golpeada; e
(b) as peças de dominó estiverem espaçadas de tal modo que, quando uma delas cai, atinge e faz cair a seguinte.

As afirmações (a) e (b), no parágrafo anterior, são os modelos para as condições (i) e (ii) do corolário 1.1, respectivamente. A afirmação (i) é chamada de *base da indução*, enquanto (ii) *de passo indutivo.* O fato de que $p(k)$ é verdadeira no item (ii) do corolário 1.1 é chamado de *hipótese de indução.*

Uma demonstração baseada no Princípio da Indução Finita é denominada *prova por indução*. Vejamos agora como se pode usar o Princípio da Indução para provar os mais variados resultados.

O exemplo 1.4 ilustra o primeiro registro histórico de utilização do PIF, feita por Francesco Maurolycus em 1575 [1].

Exemplo 1.4. *Demonstre que para qualquer $n \in \mathbb{N}$ é válida a igualdade:*

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

Solução: Aqui definimos a proposição:

$$p(n): 1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

e notamos que a mesma é válida se tomarmos, por exemplo, $n = 1(\ base\ da\ indução)$. De fato,

$$p(1): 1 = 1^2$$

Agora só resta provar o passo indutivo:

- Hipótese: suponhamos que $p(k)$ seja verdadeira para certo $k > 1, k \in \mathbb{N}$.
- Tese: devemos mostrar que $p(k + 1)$ também é verdadeira.

Com efeito, pela hipótese de indução, temos:

$$1 + 3 + 5 + \cdots + (2k - 1) = k^2,$$

Por outro lado, temos que

$$p(k + 1): 1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = k^2 + (2k + 1) = (k + 1)^2.$$

Portanto, assumindo que $p(k)$ é verdadeira, segue da igualdade acima que $p(k + 1)$ também é verdadeira. Portanto, o princípio da indução finita nos garante que $p(n)$ é verdadeira para qualquer $n \in \mathbb{N}$.

■

Exemplo 1.5. *Determine uma fórmula para a soma dos n primeiros números pares, isto é,*

$$S_n = 2 + 4 + 6 + \cdots + 2n.$$

Solução: Para induzir a fórmula, primeiro fazemos os cálculos para vários valores de n, para os quais apresentamos abaixo:

$$S_1 = 2 = 1 \cdot 2$$
$$S_2 = 2 + 4 = 6 = 2 \cdot 3$$
$$S_3 = 2 + 4 + 6 = 12 = 3 \cdot 4$$
$$S_4 = 2 + 4 + 6 + 8 = 20 = 4 \cdot 5$$
$$S_5 = 2 + 4 + 6 + 8 + 10 = 30 = 5 \cdot 6$$

No intuito de obter uma fórmula para respectiva soma, observemos se acontece algum padrão nestas somas. Para tanto, observe que: $S_n = n \cdot (n + 1)$. Entretanto, já sabemos que isso não constitui uma prova rigorosa desta fórmula. Provaremos agora que, de fato, ela é válida. Com efeito, definamos a proposição

$$p(n): 2 + 4 + 6 + \cdots + 2n = n(n + 1)$$

e observe que a mesma vale para $n = 1$ (base da indução); de fato

$$p(1): 2 = 1(1 + 1).$$

Agora partimos para a prova do passo indutivo:

- Hipótese: suponhamos que $p(k)$ seja verdadeira para certo $k > 1, k \in \mathbb{N}$.
- Tese: devemos mostrar que $p(k + 1)$ também é verdadeira.

Com efeito, pela hipótese de indução, temos:

$$2 + \cdots + 2k = k(k + 1),$$

Daí, temos que

$$p(k + 1): 2 + \cdots + 2k + 2(k + 1) = k(k + 1) + 2(k + 1) = (k + 1)(k + 2).$$

Está última igualdade afirma que $p(k + 1)$ também é verdadeira. Assim, pelo princípio da indução finita, $p(n)$ é verdadeira para qualquer $n \in \mathbb{N}$.

■

Os dois próximos exemplos são motivados pela seguinte história, citada por [6]: conta-se que Carl Friederich Gauss (1777 – 1855) ainda garoto, na escola, foi surpreendido por seu professor, que na tentativa de aquietar a turma de Gauss, mandou os alunos calcularem a soma de todos os números naturais de 1 até 100. Qual não foi a surpresa quando, pouco tempo depois, o "pequeno" Gauss deu a resposta: 5050. O que Gauss percebeu foi que a soma dos termos equidistantes é constante $(101 = 1 + 100 = 2 + 99 = \cdots = 49 + 52 = 50 + 51)$, logo somar todos os números de 1 até 100, equivale a soma de 50 parcelas de 101, ou seja, $50\ vezes\ 101$ que dá 5050.

Por suas contribuições à Matemática, Gauss é considerado um dos maiores matemático de todos os tempos, tendo dedicado boa parte de seu talento à aritmética, sua área de interesse preferida.

Exemplo 1.6 [6]**.** *Determinar uma fórmula para a soma dos n primeiros números naturais.*
Solução: Seja

$$S_n = 1 + 2 + 3 + \cdots + n$$

a soma dos n primeiros números naturais.
Somando a igualdade acima, membro a membro, com ela mesma, porém com as parcelas do segundo membro em ordem invertida, temos que

$$\begin{array}{rcccccccc} S_n & = & 1 & + & 2 & +\cdots+ & (n-1) & + & n \\ S_n & = & n & + & (n-1) & +\cdots+ & 2 & + & 1 \\ \hline 2S_n & = & (n+1) & + & (n+1) & +\cdots+ & 2 & + & 1 \end{array}$$

Daí segue-se que $2S_n = n(n+1)$, e, portanto,

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

■

Observação 1.1. Hefez em [3] chama a atenção de que para muitos, a solução do exemplo 1.6 está impecável, mas se alguém perguntasse o que está escondido atrás dos pontinhos (reticências), talvez nos sentíssemos atarracados. Como ter absoluta certeza de que nada acontece fora do nosso controle, exatamente na imensa região coberta pelos pontinhos? Dúvidas não podem pairar acerca de nosso resultado, logo vamos verificar a validade da fórmula acima utilizando o PIF.

◿

Exemplo 1.7. *Demonstre por indução que para qualquer $n \in \mathbb{N}$ é válida a igualdade:*

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

Demonstração: Definamos a proposição

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

e observe que a mesma trivialmente vale para $n = 1$ (base da indução).

Agora partimos para a prova do passo indutivo. Com efeito, suponhamos que $p(k)$ seja verdadeira para certo $k > 1, k \in \mathbb{N}$, logo

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

Verificaremos agora que $p(k+1)$ é verdadeira. Note que

$$p(k+1): 1 + 2 + 3 + \cdots + k + (k+1).$$

Dessa forma, usando a hipótese indutiva, temos que:

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

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

Donde concluímos que $p(k+1)$ também é verdadeira. Assim, o PIF nos garante que $p(n)$ é verdadeira para qualquer $n \in \mathbb{N}$. ■

Na observação 1.1 fizemos objeções acerca do uso dos pontinhos na solução empregada no exemplo 1.6; não que sejamos contra, enfatiza Hefez [3]: em geral eles nos ajudam muito a representar situações em que há um número grande (e finito) de objetos dos quais queremos visualizar suas propriedades.

Devemos lembrar que, o que estamos tentando estabelecer neste capítulo é um maior padrão de rigor no tratamento de certos problemas matemáticos (o uso do PIF proporciona isso). Mas, não esperamos que se tome esse rigor ao pé da letra. Certos argumentos informais, quando acompanhados de um raciocínio correto são corriqueiramente aceitos. Logo, a solução apresentada no exemplo 1.6 é perfeitamente aceitável. Portanto, não podemos, principalmente em sala de aula, deixar o formalismo se sobrepor à criatividade, pois em regra *primeiro vem a descoberta, e depois a formalização* [3].

Exemplo 1.8. *Demonstre que para qualquer $n \in \mathbb{N}$ é válida a igualdade:*

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Demonstração: Aqui definimos a proposição:

$$p(n): 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

e notamos que a mesma é válida para $n = 1$($base\ da\ indução$). Suponhamos que $p(k)$ seja verdadeira para certo $k > 1, k \in \mathbb{N}$, ou seja,

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

Somando $(k+1)^2$ a ambos os lados desta igualdade, temos que

$$p(k+1)\colon 1^2+2^2+3^2+\cdots+k^2+(k+1)^2=\frac{k(k+1)(2k+1)}{6}+(k+1)^2=$$

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

$$=\frac{(k+1)[(2k^2+k)+(6k+6)]}{6}=\frac{(k+1)(2k^2+7k+6)}{6}=\frac{(k+1)(k+2)(2k+3)}{6}.$$

Está última igualdade afirma que $p(k+1)$ também é verdadeira, pois

$$p(k+1)\colon\frac{(k+1)[(k+1)+1][2(k+1)+1]}{6}=\frac{(k+1)(k+2)(2k+3)}{6}.$$

Assim, o PIF nos garante que $p(n)$ é verdadeira para qualquer $n\in\mathbb{N}$.

■

O exemplo 1.8 mostra que o passo indutivo pode "algumas vezes" ser trabalhoso. Na verdade, na maioria das demonstrações por indução ele é. Por isso, um conselho: não devemos estudar matemática somente de forma contemplativa, passivamente no processo de ensino-aprendizagem. Contemplar as ideias, conceitos e uma quantidade razoável de exercícios resolvidos são importantes no primeiro momento da aprendizagem. Mas temos que "sujar as mãos" (e que seja pelo menos de grafite, tinta de caneta e pó de borracha) resolvendo o maior número de problemas possível, e também nos esforçando para escrever nossas próprias soluções. Essa é uma prática que devemos seguir, e que deve ser transmitida para nossos alunos.

Os dois próximos exemplos figuram o uso do PIF na demonstração de desigualdades.

Exemplo 1.9. *Mostre que para todo número* $n\in\mathbb{N}$, $n\geq 4$, *vale que* $2^n<n!$.

Solução: seja $p(n)\colon 2^n<n!$ com $n\in\mathbb{N}$ e $n\geq 4$. Note que a base indutiva é $n_0=4$. É claro que $p(4)$ é verdadeira, pois $2^4=16<4!=24$. Assumindo que $p(k)$ é válida para $k\geq 5$, mostraremos que $p(k+1)$ é verdadeira. Com efeito, por hipótese de indução:

$$p(k)\colon 2^k<k! \qquad (1.1)$$

para algum $k \geq 5$. Daí, $2 < k + 1$, e podemos multiplicar o lado esquerdo da desigualdade (1.1) por 2 e o lado direito por $k + 1$, sem alterar o sinal da desigualdade. Logo, temos que:

$$2^k . 2 < k!\,(k+1) = (k+1)!,$$

o que mostra que $p(k+1)$ é verdadeira. Assim, pelo PIF, temos que $p(n)$ é verdadeira para todo natural $n \geq 4$.

■

Observação 1.2. Chamamos a atenção de que não é essencialmente necessário começamos a indução em $n_0 = 1$, isso não é exigido no corolário 1.1. No entanto, no exemplo 1.9, n_0 é necessariamente diferente de 1, 2, 3; uma vez que a desigualdade $2^n < n!$ só faz sentido para todos os inteiros maiores do que ou iguais a 4. No modelo de peças de dominó, se tivéssemos escolhido qualquer peça acima da terceira para ser golpeada inicialmente, poderíamos afirmar que todas as peças seguintes cairiam.

◿

Exemplo 1.10 [7]**.** Prove que, para todo $n \in \mathbb{N}$,

$$\underbrace{\sqrt{2+\sqrt{2+\sqrt{2+\cdots\sqrt{2}}}}}_{n\,-\,radicais} < 2.$$

Solução: Note que a desigualdade é válida para $n = 1$ (base da indução), uma vez que $\sqrt{2} < 2$. Para o passo indutivo, suponha que para certo $k \in \mathbb{N}$ a desigualdade acontece, então

$$\underbrace{\sqrt{2+\sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}}}_{k\,-\,radicais} < 2.$$

Adicionando 2 em ambos os lados desta desigualdade tem-se

$$2 + \underbrace{\sqrt{2+\sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}}}_{k\,-\,radicais} < 2 + 2.$$

Tomando a raiz quadrada em ambos os lados desta última desigualdade obtemos

$$\underbrace{\sqrt{2+\sqrt{2+\sqrt{2+\sqrt{2+\cdots\sqrt{2}}}}}}_{k+1-radicais} < 2$$

como desejávamos.

■

O PIF possui outro variante conhecido na literatura como *Princípio "Forte" da Indução Finita*, ele é o objeto do corolário 1.2. Como veremos nos exemplos 1.11 e 1.12, esta nova formulação do PIF será útil nos casos em que a validade de $p(k+1)$ não puder ser obtida facilmente da validade de $p(k)$, mas sim da validade de algum $p(m)$, em que $1 \leq m \leq k$.

Corolário 1.2 (PIF – forma "forte"). *Considere n_0 um inteiro não negativo. Suponha que, para cada inteiro $n \geq n_0$, seja dada uma proposição $p(n)$ e que valem as propriedades:*
(i) *$p(n_0)$ é verdadeira;*
(ii) *Se para todo $k \in \mathbb{N} \cup \{0\}$, com $n_0 \leq k \leq n$, $p(k)$ é verdadeira, então $p(n+1)$ também é verdadeira.*
Então, a proposição $p(n)$ é verdadeira para qualquer $n \geq n_0$.

Demonstração: Seja o conjunto:

$$A = \{m \in \mathbb{N} \cup \{0\}\,;\; p(n_0), p(n_0+1), \ldots, p(m)\ são\ verdadeiras\}.$$

Pela condição (i) temos que $p(n_0)$ é verdadeira, ou seja, $n_0 \in A$. Tomemos um $n \geq n_0$ tal que $n \in A$. Ora, pela definição de A, $p(n_0), p(n_0+1), \ldots, p(n)$ são verdadeiras e pelo fato de $n_0 \leq n \leq n$, temos, pela propriedade (ii), que $p(n+1)$ também é verdadeira, logo $n+1$ é elemento do conjunto A. Assim, o PIF garante que o conjunto A contém todos os números inteiros não negativos $n \geq n_0$, ou seja, a proposição $p(n)$ é verdadeira para qualquer $n \geq n_0$.

■

Observação 1.3. O teorema 1.1 (PIF), o corolário 1.1 (PIF – forma "fraca") e o corolário 1.2 (PIF – forma "forte"), são todos equivalentes ao Princípio da Boa Ordenação, enunciado na seção 1.1. Este pode ser demonstrado assumindo o PIF (como qualquer um dos corolários mencionados) como um axioma, e reciprocamente. Para maiores detalhes aconselhamos a leitura do apêndice A em [5]. ◿

Definição 1.1. *Chamamos de Sequência de Fibonacci a sequência de números naturais*

$$1, 1, 2, 3, 5, 8, 13, 21, \ldots \qquad (1.2)$$

em que cada elemento, a partir do terceiro, é a soma dos dois anteriores.
Se F_n denota o n-ésimo termo dessa sequência, podemos defini-la por:

$$\begin{cases} F_1 = 1 \\ F_2 = 1 \\ F_n = F_{n-2} + F_{n-1}, \ \ se\ n \geq 3. \end{cases} \tag{1.3}$$

A sequência (1.2) tem o seu nome devido ao matemático italiano Leonardo de Pisa $(1170 - 1250)$, filho de Bonacci, e por isso apelidado de Fibonacci. Autor de *Liber abaci* (livro sobre o ábaco), escrito em 1202, Fibonacci conseguiu reunir em seu livro grande parte do conhecimento aritmético e algébrico dessa época, fundamental no desenvolvimento matemático na Europa Ocidental. Fibonacci é considerado um dos maiores matemáticos da Idade Média.

Exemplo 1.11. *Mostre que a sequência de Fibonacci satisfaz a desigualdade*

$$F_n < \left(\frac{7}{4}\right)^n \ para\ todo\ n \geq 1. \tag{1.4}$$

Demonstração: Definimos a proposição $p(n)$ a partir da afirmativa (1.4):

$$p(n)\text{: } F_n < \left(\frac{7}{4}\right)^n \ para\ todo\ n \geq 1.$$

Para $n = 1$ e $n = 2$ (base da indução), temos que $F_1 = 1 < \left(\frac{7}{4}\right)^1$ e $F_2 = 1 < \left(\frac{7}{4}\right)^2$, logo $p(1)$ e $p(2)$ são verdadeiras (duas bases para indução? Vide observação 1.4 acerca desse detalhe técnico).

Agora partimos para a prova do passo indutivo usando a condição (ii) do corolário 1.2:

- Hipótese: suponhamos que para todo k, $p(k)$ seja verdadeira, onde $1 \leq k \leq n$.
- Tese: devemos mostrar que $p(n+1)$ também é verdadeira.

Com efeito, pela definição 1.1

$$F_{n+1} = F_n + F_{n-1}, \ \ se\ n \geq 2. \tag{1.5}$$

Temos, por hipótese de indução, que:

$$F_n < \left(\frac{7}{4}\right)^n \qquad \text{e} \qquad F_{n-1} < \left(\frac{7}{4}\right)^{n-1} \tag{1.6}$$

Segue de (1.5) e (1.6) que:

$$F_{n+1} = F_n + F_{n-1} < \left(\frac{7}{4}\right)^n + \left(\frac{7}{4}\right)^{n-1} = \left(\frac{7}{4}\right)^n \left(1 + \frac{4}{7}\right) = \left(\frac{7}{4}\right)^n \left(\frac{11}{7}\right) < \left(\frac{7}{4}\right)^n \left(\frac{7}{4}\right) = \left(\frac{7}{4}\right)^{n+1}.$$

Daí, $F_{n+1} < \left(\frac{7}{4}\right)^{n+1}$, ou seja, $p(n+1)$ também é verdadeira. Assim, o corolário 1.2 nos garante que $p(n)$ é verdadeira para qualquer $n \in \mathbb{N}$, como queríamos demonstrar.

■

Observação 1.4. Quando o passo indutivo utiliza valores de dois termos anteriores, a base indutiva requer verificar a fórmula (desigualdade ou afirmativa) para os dois termos iniciais. Isso foi observado no exemplo 1.11 e será também no exemplo 1.12.

◿

Uma *recorrência* é uma fórmula que define um elemento de uma sequência a partir de termos anteriores. Na definição 1.1, (1.3) figura uma fórmula que define os termos da sequência de Fibonacci.

Quando é dada uma recorrência, um problema importante é determinar uma fórmula para o termo geral da sequência sem recorrer aos termos anteriores. No caso da sequência de Fibonacci, existe uma fórmula chamada *fórmula de Binet*, que é o objeto do nosso próximo exemplo.

Exemplo 1.12. *Prove que para todo* $n \in \mathbb{N}$, *tem-se que*

$$F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{\mathrm{n}} - \left(\frac{1-\sqrt{5}}{2}\right)^{\mathrm{n}}}{\sqrt{5}}\,. \tag{1.7}$$

Solução: Denotando por $\alpha = \frac{1+\sqrt{5}}{2}$ e por $\beta = \frac{1-\sqrt{5}}{2}$, temos que α e β são as raízes da equação $x^2 = x + 1$. Note que $\alpha - \beta = \sqrt{5}$. Com essas notações, definimos a proposição $p(n)$ a partir da afirmativa (1.7):

$$p(n)\colon F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} para\ todo\ n \geq 1\,.$$

Como $F_1 = \frac{\alpha^1 - \beta^1}{\alpha - \beta} = 1$ e $F_2 = \frac{\alpha^2 - \beta^2}{\alpha - \beta} = 1$ (base da indução), temos que $p(1)$ e $p(2)$ são verdadeiras (novamente a base indutiva requer duas verificações, observação 1.4). Agora suponhamos que para todo k, $p(k)$ seja verdadeira, onde $1 \leq k \leq n$, ou seja, $F_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}$ para todo k com $1 \leq k \leq n$ (hipótese de indução). Assim,

$$F_{n+1} = F_n + F_{n-1} = \frac{\alpha^n - \beta^n}{\alpha - \beta} + \frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} = \frac{(\alpha^n + \alpha^{n-1}) - (\beta^n + \beta^{n-1})}{\alpha - \beta} =$$

$$= \frac{\alpha^{n-1}(\alpha + 1) - \beta^{n-1}(\beta + 1)}{\alpha - \beta} = \frac{\alpha^{n-1}.\alpha^2 - \beta^{n-1}.\beta^2}{\alpha - \beta} = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta}$$

pois $\alpha^2 = \alpha + 1$ e $\beta^2 = \beta + 1$. Assim, $p(n+1)$ é verdadeira. Segue o resultado pelo PIF.

■

1.4 CUIDADOS AO USAR O PRINCÍPIO DA INDUÇÃO FINITA

Nas demonstrações usando o Princípio da Indução Finita pode parecer que estamos usando o fato de $p(n)$ ser verdadeira para deduzir que $p(n+1)$ é verdadeira, concluindo que $p(n)$ é verdadeira, ou seja, pode passa a impressão que estamos usando a tese como hipótese na demonstração. Mas não passa de uma impressão.

De fato, dado um número natural n, temos duas possibilidades:

(a) $p(n)$ é verdadeira ou (b) $p(n)$ é falsa.

No Teorema 1.1, corolário 1.1 e corolário 1.2, a hipótese indutiva não exige em absoluto que assumamos $p(n)$ verdadeira para todo $n \in \mathbb{N}$, podendo ser falsa para algum valor de n, ou mesmo para todos os valores de n. Ela exige que sempre que algum n pertença à categoria (a) acima, então $n+1$ também pertence a essa mesma categoria, não exigindo nada quando n pertença à categoria (b).

Assim, é nesse sentido que a aplicação do método de indução matemática requer certos cuidados. A seguir, o exemplo 1.13 mostra como o método pode ser aplicado de forma errada.

Exemplo 1.13 [7]**.** Seja a afirmação

"*Num conjunto qualquer com n bolas, todas têm a mesma cor".*

Solução: Para $n = 1$, nossa proposição é verdadeira, pois em qualquer conjunto com n bolas, todas as bolas têm a mesma cor, pois só existe uma bola. Assuma por hipótese de indução que a proposição é verdadeira para n e provemos que a proposição é verdadeira para $n+1$. Ora, seja $A = \{b_1, \ldots, b_n, b_{n+1}\}$ o conjunto com $n+1$ bolas referido. Considere os subconjuntos de B e C de A com n elementos, construídos como:

$$B = \{b_1, b_2, \ldots, b_n,\} \text{ e } C = \{b_2, \ldots, b_n, b_{n+1}\}.$$

Observe que ambos os conjuntos tem n elementos. Assim, as bolas do conjunto B têm a mesma cor. Do mesmo modo, as bolas do conjunto C têm a mesma cor. Em particular, a bola b_n tem a mesma cor que a bola b_{n+1}. Assim, todas as bolas tem a mesma cor.

É claro que essa proposição é falsa, e a demonstração empregada denota o uso incorreto do PIF. Com efeito, observe a validade do argumento quando o conjunto A tem dois elementos. Note que B e C não se intersectam. Em suma, o passo indutivo falha de $n = 1$ *para* $n = 2$.

■

PROBLEMAS PROPOSTOS

1.1. Mostre, usando o método da indução, a validade das seguintes fórmulas:

$(a)\ 1^3 + 2^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2.$

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

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

1.2. Use o princípio da indução finita para provar as seguintes desigualdades:

$(a)\ n! \geq 3^n, se\ n \geq 7.$

$(b)\ n^2 > 2n + 1, para\ todo\ n \geq 3.$

$(c)\ \frac{1}{n+1} + \frac{1}{n+2} + \frac{1}{n+3} + \cdots + \frac{1}{n+n} > \frac{13}{24}\ , para\ todo\ n \in \mathbb{N}\backslash\{1\}.$

1.3. Mostre as seguintes propriedades a respeito da sequência de Fibonacci F_n :

$(a)\ F_1 + F_2 + \cdots + F_n = F_{n+2} - 1.$

$(b)\ F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}.$

1.4. Dados $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$, mostre que

(a) Se $a \neq b$, então $(a^n - b^n) = (a - b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$.

(b) Se $a \neq -b\ e\ n$ for ímpar, então

$$(a^n + b^n) = (a + b)(a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1}).$$

1.5 (Pizza de Steiner). Calcule o número de regiões em que o plano é dividido por n retas distintas na posição geral, isto é, sem que haja duas retas paralelas ou três retas concorrentes em um mesmo ponto.

1.6. Mostre que o número de diagonais de um polígono convexo com $n\text{-}lados$ é igual a

$$\frac{n(n-3)}{2}.$$

1.7. Mostre que a soma dos ângulos internos de um polígono convexo com $n\text{-}lados$ é igual a $(n-2)\pi$ radianos.

EUCLIDES E OS ELEMENTOS

Neste tópico histórico, encontra-se a abordagem com base em [1], [9] e [10].

Quando Alexandre, o Grande, morreu, em 323 a.C., o mundo antigo já não era aquele que ele conquistará. Com suas conquistas, Alexandre levou a civilização grega a todos os recantos do mundo antigo. Ele havia fundado a cidade de Alexandria, no atual Egito, que estava destinada a substituir Atenas como centro comercial e cultural do mundo.

Após a morte de Alexandre, na divisão de seu império entre seus generais, coube a Ptolomeu I, o rei do Egito, fundar, aproximadamente a 300 a.C., o museu de Alexandria. O museu logo se tornou o centro dos maiores desenvolvimento acadêmicos da Grécia, seja nas ciências exatas, seja nas ciências humanas. As pessoas que trabalhavam no museu podiam morar em suas dependências e recebiam um salário para tal. Os sucessores de Ptolomeu I, trataram de organizar com muito zelo a biblioteca do museu , chegando a conter 500 000 volumes de todos os campos do conhecimento.

Foi aí que Euclides (325 – 265a.C.) viveu, trabalhou e construiu sua obra monumental: *Os Elementos* – um tratado que se tornaria um dos marcos mais importantes da Matemática. Para entender a importância de Euclides e de sua abra, precisamos entender um pouco do cenário matemático que o antecedeu.

Foi Tales de Mileto (640 – 546a.C.) que introduziu o estudo da Matemática na Grécia. Tales teria trazido para Grécia os rudimentos de geometria e da aritmética que aprendera com os sacerdotes egípcios, iniciando uma intensa atividade que ali se desenvolveu por mais de cinco séculos. Enquanto os egípcios encaravam a Matemática como uma arte que os auxiliavam em seus trabalhos de engenharia e de agrimensura, os gregos, a exemplo de Tales, assumiam um caráter científico, dada a atitude filosófica e especulativa que tinham em face da vida.

Em seguida, foram Pitágoras de Samos (580? – 500?a.C.) e sua escola (que durou vários séculos) que se cometeram no desenvolvimento e difusão da Matemática pela Grécia e sua colônias. A Escola pitagórica atribuía aos números um poder místico, adotando a aritmética como fundamento de seu sistema filosófico. Infelizmente, quase nada sobrou dessa fase da Matemática grega, apenas referências e comentários feitos por outros matemáticos posteriores.

A inclinação para filosofia e a lógica, que os gregos tinham, influenciou diretamente o modo de se fazer Matemática naquela época. Platão (429 – 348?a.C.), por exemplo, mesmo não sendo matemático, nela via um indispensável treinamento filosófico, ressaltando a metodologia axiomático-dedutiva a ser seguida em todos os campos do conhecimento. O domínio da geometria era uma condição necessária aos aspirantes para o ingresso de na sua academia. A preferência de Platão por parâmetros mais teóricos e conceituais fazia-o estabelecer uma clara diferença entre a ciência dos números, que chamava de aritmética, e a arte de calcular, que chamava de logística a qual desprezava por ser “infantil” e “vulgar”.

Euclides herdou toda essa herança cultural, e estava inserido dentro da efervescência intelectual grega. Pouco se sabe sobre os dados desse grande matemático, tendo chegado a nós, através das sucessivas edições de Os Elementos, tratado composto por 13 livros, onde se encontra sistematizada a maior parte do conhecimento matemático da época.

Em Os Elementos, aparentemente, não há criação de muitos resultados, o que evidencia o crédito de Euclides para com os matemáticos gregos que o antecederam. Todavia, Euclides teve mérito, pois estabeleceu em sua obra um padrão de apresentação e rigor jamais alcançados anteriormente em algum trabalho matemático, tido como exemplo a ser seguido nos milênios que se sucederam.

O plano geral de Os Elemento é o seguinte: os primeiros quatro livros versam sobre geometria plana, já então considerada elementar. É parte da obra que muito deve a Tales e a Pitágoras. Os dois seguintes tratam da teoria da proporção de Eudoxio (408? – 355a.C) e suas aplicações. O décimo trata da teoria dos incomensuráveis e os três últimos, da geometria espacial.

No livro VII, são definidos os conceitos de divisibilidade, número primo, máximo divisor comum, mínimo múltiplo comum, entre outros. No mesmo livro, além dessas definições, todas bem postas e até hoje utilizadas, encontra-se enunciada a chamada divisão euclidiana (nosso Teorema 2.1). Com o uso iterado dessas divisões, Euclides estabelece o

algoritmo mais eficiente, até hoje conhecido, para o cálculo do máximo divisor comum de dois inteiros, chamado de algoritmo de Euclides, que apresentamos no Capítulo 2.

No Livro VIII, são estudadas as propriedades de sequências de números em progressão geométrica. Já no Livro IX, Euclides mostra, de forma magistral, que a quantidade de números primos supera qualquer número dado; em outras palavras, existem infinitos números primos (nosso Teorema 4.2). Euclides também mostra que todo número natural pode ser escrito como o produto de números primos, o resultado hoje conhecido como Teorema Fundamental da Aritmética (nosso Teorema 4.1).

Com mais de mil edições, nenhum trabalho, exceto a Bíblia, foi tão largamente usado ou estudado e, provavelmente, nenhum exerceu influencia maior no pensamento científico. Isso, sem dúvida, faz de Os Elementos de Euclides uma herança ímpar para humanidade.

2 – DIVISIBILIDADE

Neste capítulo, apresentaremos definições e propriedades elementares acerca da *relação de divisibilidade* no conjunto dos números inteiros; enfatizando a *Divisão Euclidiana*; provaremos o *Teorema da Representação de um Número em uma Base qualquer* $b > 1$ e obteremos alguns critérios de divisibilidade. O caráter da exposição é elementar, todavia encontraremos resultados e exemplos bem interessantes.

2.1 DIVISIBILIDADE

Vamos definir a relação *divide* entre dois números inteiros, conhecida também como *relação de divisibilidade.*

Definição 2.1. *Dados dois números* $a, b \in \mathbb{Z}$*, dizemos que* b *"divide"* a*, e escrevemos* $b \mid a$*, se existir um* $c \in \mathbb{Z}$ *tal que* $a = bc$*. Caso* b *não divida* a*, escrevemos* $b \nmid a$*. Se* b *dividir* a*, dizemos que* b *é um divisor de* a*, que* a *é divisível por* b *ou ainda que* a *é um múltiplo de* b*.*

Observação 2.1. A notação $b \mid a$ não representa uma operação em $\mathbb{Z}$, nem tão pouco representa uma fração [1]. Trata-se apenas de uma sentença que diz ser verdade quando *existe um* $c \in \mathbb{Z}$ *tal que* $a = bc$. Por exemplo, $6 \mid 24$, pois existe o inteiro 4 tal que $24 = 6 \cdot 4$; enquanto $5 \nmid 13$, pois não existe nenhum inteiro c tal que $13 = 5 \cdot c$. É claro que todo inteiro não nulo é um divisor de si mesmo e de 0, ou seja, $n \mid n$ e $n \mid 0$ com $n \in \mathbb{Z}$. Também, o $1 \mid n$ para todo inteiro n. Assim, todo número inteiro n possui pelo menos dois divisores (1 e o próprio n).

◿

Exemplo 2.1. Dizemos que um número inteiro n é *par* se $2 \mid n$, ou seja, n for múltiplo de 2. Pela definição 1.1, dizer que um inteiro n é par é equivalente a escrevê-lo na forma $n = 2k$, onde $k \in \mathbb{Z}$. Denotando por $2\mathbb{Z}$ o conjunto dos números pares, temos que

$$2\mathbb{Z} = \{2k; \text{onde } k \in \mathbb{Z}\} = \{\dots, -6, -4, -2, 0, 2, 4, \dots\}.$$

Os números que não são pares são chamados de *ímpares*. Note que todo número ímpar é igual a um número par mais 1, de modo que todo ímpar pode ser escrito da forma $2k+1, k \in \mathbb{Z}$. Denotando por $2\mathbb{Z}+1$ o conjunto dos números ímpares, temos que

$$2\mathbb{Z}+1 = \{2k+1; \text{onde } k \in \mathbb{Z}\} = \{\dots, -5, -3, -1, 1, 3, 5, \dots\}.$$

■

Observação 2.2. Notemos que:

$$n, m \in 2\mathbb{Z} \implies n+m \in 2\mathbb{Z} \quad e \quad n \cdot m \in 2\mathbb{Z} \tag{2.1}$$

$$n, m \in 2\mathbb{Z}+1 \implies n+m \in 2\mathbb{Z} \quad e \quad n \cdot m \in 2\mathbb{Z}+1 \tag{2.2}$$

$$n \in 2\mathbb{Z} \ e \ m \in 2\mathbb{Z}+1 \implies n+m \in 2\mathbb{Z}+1 \quad e \quad n \cdot m \in 2\mathbb{Z} \tag{2.3}$$

A implicação (2.1) diz que a *adição e a multiplicação é fechada no conjunto* $2\mathbb{Z}$ *dos números pares* – somar ou multiplicar números pares resulta sempre em um número par. A implicação (2.2) diz que a *multiplicação é fechada no conjunto* $2\mathbb{Z}+1$ *dos números ímpares*, enquanto a adição não é – somar dois números ímpares resulta sempre em um número par. Já a (2.3) diz que a soma de um número par com um ímpar é ímpar, enquanto o produto é par.

◿

Alguns problemas podem ser resolvidos de forma eficiente usando a observação 2.2, ou seja, analisando se determinada soma ou produto de números inteiros é par ou ímpar – o que chamamos de *argumento de paridade.* Usamos isso no próximo exemplo.

Exemplo 2.2. *Prove que a equação* $x^3 + 7x + 17 = 0$ *não possui nenhuma solução inteira.*

Solução: Usaremos a demonstração por absurdo. Suponhamos que exista um $p \in \mathbb{Z}$ tal que $p^2 + 7p + 17 = 0$. Analisando a paridade de p, temos o seguinte:

$$p \in 2\mathbb{Z} \implies \underbrace{\underbrace{\underbrace{p^2}_{par} + \underbrace{7}_{ímpar} \cdot \underbrace{p}_{par}}_{par} + \underbrace{17}_{ímpar}}_{ímpar} = \underbrace{0}_{par} \tag{2.4}$$

$$p \in 2\mathbb{Z}+1 \implies \underbrace{\underbrace{\underbrace{p^2}_{ímpar} + \underbrace{7}_{ímpar} \cdot \underbrace{p}_{ímpar}}_{ímpar} + \underbrace{17}_{ímpar}}_{ímpar} = \underbrace{0}_{par} \tag{2.5}$$

As implicações (2.4) e (2.5) nos levam a um absurdo (zero ser ímpar). Logo não pode existir um $p \in \mathbb{Z}$ tal que $p^2 + 7p + 17 = 0$.

■

Exemplo 2.3. *Dados $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$, mostre que para todo $a \neq b$ temos que*

(i) *Se* $a \neq b$, *então* $(a-b) \mid (a^n - b^n)$.

(ii) *Se* $a \neq -b$ *e* n *for ímpar, então* $(a+b) \mid (a^n + b^n)$.

Demonstração: (i) Pelo problema 1.4 (a) do capítulo 1, temos que

$$(a^n - b^n) = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}).$$

Como $(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) \in \mathbb{Z}$, segue o resultado da definição 2.1.

(ii) Pelo problema 1.4 (b) do capítulo 1, temos que *se* $a \neq -b$ *e* n *for ímpar, então*

$$(a^n - b^n) = (a+b)(a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1}),$$

com $(a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1}) \in \mathbb{Z}$. Usamos novamente a definição 2.1 para chegar ao resultado.

■

Exemplo 2.4. *Mostre que* $7 \mid 43^n - 1$ *para todo* $n \in \mathbb{Z}$.

Solução: Note que $43^n - 1 = 43^n - 1^n$**.** Usando o item (i) do exemplo anterior, temos que $(43-1) \mid 43^n - 1$, ou seja, $42 \mid 43^n - 1$. Pela definição 2.1, $43^n - 1 = 42k = 7(6k)$ onde $k \in \mathbb{Z}$. Segue o resultado.

■

Proposição 2.1 (Transitividade). *Se* $a, b,$ *e* c *são inteiros,* $a \mid b$ *e* $b \mid c$, *então* $a \mid c$.

Demonstração: Como $a \mid b$ e $b \mid c$, existem inteiros k_1 e k_2 com $b = ak_1$ e $c = bk_2$. Logo,

$$c = bk_2 = (ak_1)k_2 = a(k_1k_2).$$

Essa última igualdade nos diz que $a \mid c$.

■

Proposição 2.2. *Se a, b, c, m, n são inteiros,* $c \mid a$ *e* $c \mid b$ *então* $c \mid (ma + nb)$.

Demonstração: Como $c \mid a$ e $c \mid b$, existem inteiros k_1 e k_2 com $a = ck_1$ e $b = ck_2$. Multiplicando estas equações por m e n, respectivamente, teremos que $ma = mck_1$ e n$b = nck_2$, donde obtemos $ma + \text{n}b = mck_1 + nck_2 = c(mk_1 + nk_2)$, o que nos diz que $c \mid (ma + nb)$.

■

Observação 2.3. Como caso particular da proposição anterior, temos que se $c \mid a \ e \ c \mid b$ *então* $c \mid (a \pm b)$. Podemos facilmente generalizar a proposição 2.2: se $c \mid a_1, \ c \mid a_2, \dots, c \mid a_n$, então $c \mid \ (x_1a_1 + \ x_2a_2 + \cdots + x_na_n)$, onde $x_1, x_2, \dots, x_n \in \mathbb{Z}$ (prove por indução!).

◿

Exemplo 2.5. Como $7 \mid 14$ e $14 \mid 42$, pela proposição 2.1, $7 \mid 42$. Como $3 \mid 15$ e $3 \mid 21$, pela proposição 2.2, $3 \mid (8 \cdot 15 + 11 \cdot 21)$.

■

Definição 2.2. *O valor absoluto de um número inteiro* a*, denotado por* $|a|$*, é definido por*

$$|a| = \begin{cases} a, se\ a \geq 0, \\ -a, se\ a < 0. \end{cases}$$

Para todo $a \in \mathbb{Z}$, $|a|$ é um número natural. Além disso, $|a| = |-a|$. Por exemplo, $|11| = |-11| = 11$. O valor absoluto de um número inteiro goza das seguintes propriedades: Para todo $a, b \in \mathbb{Z}$ e $r \in \mathbb{N}$

1) $|ab| = |a| \cdot |b|$;
2) $|a| \leq r \quad \Leftrightarrow \quad -r \leq a \leq r$;
3) $-|a| \leq a \leq |a|$;
4) *Desigualdade triangular:* $\big|\, |a| - |b| \,\big| \leq |a \pm b| \leq |a| + |b|$.

A proposição a seguir estabelece algumas propriedades básicas da relação de divisibilidade. Elas são um bom exercício para fixar a definição 2.1, por isso tente fazer sozinho para depois ver a demonstração.

Proposição 2.3. *A relação de divisibilidade goza das seguintes propriedades*

$(i) \ d \mid n \implies ad \mid an$,
$(ii) \ ad \mid an \ e \ a \neq 0 \implies d \mid a$,
$(iii) \ d \mid n \ e \ n \neq 0 \implies |d| \leq |n|$,
$(iv) \ d \mid n \ e \ n \mid d \implies |d| = |n|$,
$(v) \ d \mid n \ e \ d \neq 0 \implies (n/d) \mid n$,

Demonstração: (i) Como $d \mid n$ temos que $n = dk, k \in \mathbb{Z}$. Multiplicando esta equação por a, temos $an = adk$, ou seja, $ad \mid an$.
(ii) Assumindo que $ad \mid an$, temos que $an = adk$, para algum k inteiro. Uma vez que $a \neq 0$, podemos "cortar" nesta última equação a de ambos os membros. Segue o resultado.

(iii) Se $d \mid n$, então existe um $k \in \mathbb{Z}$ tal que $n = dk$. Isso implica que,

$$|n| = |dk| = |d| \cdot |k| \geq |d|, \text{ desde que seja } n \neq 0.$$

(v) Se $d \mid n \ e \ n \mid d$, então por (iii) $|n| \geq |d|$ e $|n| \leq |d|$; ou seja, $|n| = |d|$.

(v) Assumindo que $d \mid a$ e $d \neq 0$, basta notar que $n = d\left({}^{n}/_{d}\right)$, ou seja, $\left({}^{n}/_{d}\right) \mid n$.

■

Observação 2.4. Desde que $a \neq 0$ as propriedades (i) e (ii) são equivalentes; tal equivalência figura a chamada *lei do corte* para relação de divisibilidade. O item (iii) é conhecido como *propriedade de limitação* [8]. Ela diz que todo número inteiro não nulo tem somente um número finito de divisores. É claro que todo números inteiro não nulo possui pelo menos dois divisores (observação 2.1). Já a propriedade (iv) diz que se $d \mid n \ e \ n \mid d$ então $a = b$ ou $a = -b$.

◿

Os próximos dois exemplos denotam o uso do método de indução na demonstração de fatos envolvendo divisibilidade.

Exemplo 2.6. *Prove que* $9 \mid 10^n - 1$ *para qualquer número natural n.*

Demonstração: Vamos provar usando a forma "fraca" do PIF. Para isso, definimos a proposição

$$p(n)\colon 9 \mid 10^n - 1$$

e notemos que a mesma vale para $n = 1$; com efeito

$$p(1)\colon 9 \mid 10^1 - 1 = 9.$$

Para o passo indutivo, suponhamos que $p(k)$ seja verdadeira para certo $k > 1, k \in \mathbb{N}$. Devemos mostrar que $p(k+1)$ também é verdadeira. Com efeito, $9 \mid 10^k - 1$ (hipótese indutiva) e note que $9 \mid 9 \cdot 10^k$, donde pela a proposição 2.2:

$$9 \mid (10^k - 1) + 9 \cdot 10^k = 10^{k+1} - 1$$

Está última igualdade afirma que $p(k+1)$ também é verdadeira. Assim, $p(n)$ é verdadeira para qualquer $n \in \mathbb{N}$.

■

Usando o item (i) do exemplo 2.3 podemos facialmente verificar a validade de $p(n)$ do exemplo 2.6 ($10^k - 1 = 10^k - 1^k$ é divisível por $10 - 1 = 9$). Outra possibilidade é observa que

$$10^1 - 1 = 9 = 9 \cdot 1$$
$$10^2 - 1 = 99 = 9 \cdot 11$$
$$10^3 - 1 = 999 = 9 \cdot 111$$
$$\vdots \qquad \vdots \qquad \ddots$$
$$10^n - 1 = \underbrace{999 \ldots 99}_{n\ algarismos} = 9 \cdot \underbrace{111 \ldots 11}_{n\ algarismo}$$

Claramente um múltiplo de 9.

Exemplo 2.7. *Prove que* $8 \mid 3^{2n} + 7$ *para qualquer número natural n.*

Solução: Novamente, usamos a forma "fraca" do PIF. Seja a proposição

$$p(n): 8 \mid 3^{2n} + 7 \ .$$

Note que a mesma vale para $n = 1$, pois

$$p(1): 8 \mid 3^2 + 7 = 16.$$

Assuma que $p(k)$ verdadeira com $k > 1$, ou seja, $8 \mid 3^{2k} + 7$; e note que $8 \mid 8 \cdot 3^{2k}$ Logo, pela proposição 2.2, temos que:

$$8 \mid (3^{2k} + 7) + 8 \cdot 3^{2k} \ \Rightarrow \ 8 \mid 3^{2(k+1)} + 7$$

Assim, $p(k+1)$ também é verdadeira.

■

Exemplo 2.8. Prove que $8^n - 3^n - 6^n + 1^n$ é um múltiplo de 5, onde $n \in \mathbb{N}$.

Solução: Pelo exemplo 2.3 item (i), temos que

$$5 \mid 8^n - 3^n \quad \text{e} \quad 5 \mid 6^n - 1^n.$$

Logo, pela proposição 3.2, concluímos que

$$5 \mid 8^n - 3^n - (6^n - 1^n), \text{ ou seja, } 5 \mid 8^n - 3^n - 6^n + 1^n.$$

■

O próximo passo de nosso estudo é ver o que acontece quando um número inteiro não é divisível por outro.

2.2 DIVISÃO EUCLIDIANA

O que acontece quando um número inteiro não é divisível por outro?

No livro VII de *Os Elementos*, Euclides responde à pergunta acima com o resultado hoje conhecido como *Divisão Euclidiana*. Antes de introduzi-lo vamos analisar, por exemplo, se 71 é divisível por 17 e para isto listaremos a diferença entre 71 e os múltiplos positivos de 17, isto é:

$$r_1 = 71 - 17 \cdot 1 = 54,$$
$$r_2 = 71 - 17 \cdot 2 = 37,$$
$$r_3 = 71 - 17 \cdot 3 = 20,$$
$$\boxed{r_4 = 71 - 17 \cdot 4 = 3,}$$
$$r_5 = 71 - 17 \cdot 5 = -14,$$
$$r_6 = 71 - 17 \cdot 6 = -31, \ldots$$

É claro que 71 não é divisível por 7. Com efeito, se $7 \mid 71$ então alguma das diferenças acima seria igual a zero. Ora, isso é impossível, pois as diferenças $r_q = 71 - 17q$ com $1 \leq q \leq 4$ são todas positivas e com $q \geq 5$ são todas negativas. Todavia, entre todas as diferenças positivas a única que é menor do que 17 corresponde ao caso $q = 4$.

Note que apesar de 7 não poder dividir 71, de certa forma, 7 "*divide" 71 deixando um resto pequeno, ou seja ,um resto maior do que ou igual a* 0 *e menor do 7 (*$r_4 = 3$). De um modo geral, todo número inteiro pode ser "dividido" deixando um resto pequeno. Este resultado, a já comentada *Divisão Euclidiana*, não só é um importante instrumento na obra de Euclides, como também é um resultado central da Aritmética. Vamos usar a seguinte estratégia para demonstrá-lo: primeiro provaremos o lema 2.1 que é um caso particular, depois provaremos o caso geral (teorema 2.1).

Lema 2.1. *Sejam* $n, d \in \mathbb{N} \cup \{0\}$ *e* $d \geq 1$. *Então existem únicos* $q, r \in \mathbb{N} \cup \{0\}$, *tais que*

$$n = qd + r \quad e \quad 0 \leq r < d \qquad (r = 0 \iff d \mid n)$$

Demonstração: Como o resultado que queremos demonstrar envolve existência e unicidade, vamos dividir nossa demonstração em duas partes.

- 1ª parte **(existência)**: Fixemos um inteiro $d \geq 1$. Usaremos a forma "forte" do PIF, procedendo a indução sobre n. Seja a afirmação $p(n)$ onde $n \in \mathbb{N} \cup \{0\}$:

$$p(n): existem\ q, r \in \mathbb{N} \cup \{0\},\ tais\ que\ n = qd + r\ \ e\ \ 0 \leq r < d.$$

Se $0 \leq n < d$ então existem $q = 0$ e $r = n < d$, tal que $n = 0 \cdot d + n$. Isso mostra que $p(n)$ é verdadeira para $0 \leq n < d$. É claro que $p(d)$ é também verdadeira, pois $d = 1 \cdot d + 0$. Suponhamos que $p(k)$ é verdadeira para $d \leq k < n$. Então, como $0 < n - d < n$, temos que existem $q_1, r \in \mathbb{N} \cup \{0\}$ tais que $n - d = q_1 d + r \ \ e \ \ 0 \leq r < d$, ou seja, $n = (q_1 + 1)d + r$ onde $0 \leq r < d$. Isso mostra que $p(n)$ é verdadeira. Assim, pelo PIF, $p(n)$ é verdadeira para todo $n \in \mathbb{N} \cup \{0\}$.

2ª parte (**unicidade)**: Suponhamos que existam $q_1, r_1, q_2, r_2 \in \mathbb{N} \cup \{0\}$ tais que

$$n = q_1 d + r_1 \ , \ \ 0 \leq r_1 < d \quad \text{e} \quad n = q_2 d + r_2 \ \ e \ \ 0 \leq r_2 < d.$$

Daí segue que,

$$q_1 d + r_1 = q_2 d + r_2 \ \text{ onde} \ , \ \ 0 \leq r_1 < d \quad \text{e} \quad 0 \leq r_2 < d.$$

Suponhamos por absurdo que $r_1 \neq r_2$, para fixa ideias $r_1 > r_2$. Neste caso teríamos

$$0 < r_1 - r_2 = (q_1 - q_2)d.$$

Mas também $r_1 - r_2 < d$ pois $r_1 < d$ e $r_2 < d$, e daí segue que:

$$0 < r_1 - r_2 = (q_1 - q_2)d < d$$

o que é absurdo pois $(q_1 - q_2)d$ é um múltiplo positivo de d maior que ele. Isto termina a demonstração.

■

Teorema 2.1 (Divisão Euclidiana). *Sejam $n, d \in \mathbb{Z}$ e $d \neq 0$. Então existem únicos $q, r \in \mathbb{Z}$, tais que*

$$n = qd + r \ \ e \ \ 0 \leq r < |d|.$$

(q é chamado de quociente da divisão de n por d, enquanto r, resto da divisão de n por d).

Demonstração: Para existência, temos quatro caso a considerar

$$(1)\ n \geq 0 \ \ e \ d > 0;$$

$$(2)\ n \geq 0 \ \ e \ d < 0;$$

$$(3)\ n < 0 \ \ e \ d > 0;$$

$$(4)\ n < 0 \ \ e \ d < 0.$$

O caso (1) é o lema 2.1, ou seja, é a divisão euclidiana para os naturais juntamente com o zero. Os casos restantes tem uma demonstração similar. Mostraremos (4), deixando os outros casos como exercício. Como $n < 0 \ \ e \ d < 0$, temos que $-n > 0, \ -d > 0 \ e \ |d| = -d$. Pelo lema 3.1, temos que existem únicos

$$q_1, r_1 \in \mathbb{N} \cup \{0\} \text{ tais que } -n = q_1(-d) + r_1 \text{ com } 0 \leq r_1 < -d.$$

Se $r_1 = 0$, temos $n = q_1 d$, então, basta $q = q_1$ e $r = 0$.

Se $r_1 > 0$, temos $n = q_1 d + (-r_1)$ e, portanto,

$$n = q_1 d + d - d + (-r_1) = (q_1 + 1)d + (-d - r_1)$$

e então basta fazer $q = q_1 + 1$ e $r = -d - r_1$, pois como $0 \leq r_1 < -d$ temos

$$0 \leq -d - r_1 < -d = |d|.$$

Também deixamos como exercício a unicidade de q e r.

■

De um modo geral, fixando um número $d \geq 2$, pode-se sempre escrever qualquer número n, de modo único, na forma $n = dq + r$, onde $q, r \in \mathbb{Z}$ e $0 \leq r < d$. Por exemplo, todo número inteiro n pode se escrito em uma, e somente uma, das seguintes formas: $3q, 3q + 1 \; ou \; 3q + 2$. Ou ainda, todo número inteiro n pode se escrito em uma, e somente uma, das seguintes formas: $4q, 4q + 1, 4q + 2 \; ou \; 4q + 3$.

Os três corolários seguintes, além de importantes em si, ilustram utilizações típicas que fazemos com a divisão euclidiana.

Corolário 2.1 (Princípio de Eudoxius[1]) *Dados $a, b \in \mathbb{Z}$ com $b \neq 0$ então "a" é um múltiplo de "b" ou se encontra entre dois múltiplos consecutivos de "b", isto é, correspondendo a cada par de inteiros a e $b \neq 0$ existe um inteiro q tal que, para*

- $b > 0, temos \; qb < a < (q + 1)b$
- $b < 0, temos \; qb < a < (q - 1)b$

Demonstração: Dados $a, b \in \mathbb{Z}$ *com* $b \neq 0$, o teorema 2.1 garante que existem únicos $q, r \in \mathbb{Z}$ tais que

$$a = qb + r \;\; e \;\; 0 \leq r < |b| \;\; \Leftrightarrow \;\; 0 \leq a - qb < |b| \;\; \Leftrightarrow \;\; qb \leq a < |b| + qb.$$

Se $b > 0$, temos que $|b| = b$, então $qb < a < (q + 1)b$.

Se $b < 0$, temos que $|b| = -b, então \; qb < a < (q - 1)b$.

■

Para o enunciado do próximo corolário, lembre-se de que:

Definição 2.3. Um inteiro positivo n é dito um **quadrado** se $n = q^2$, para algum inteiro q. Um inteiro positivo n é dito um **cubo** se $n = q^3$, para algum inteiro q.

Corolário 2.2. *Todo quadrado deixa resto 0 ou 1 quando dividido por 3.*

Demonstração: Seja n um número natural. Pela divisão euclidiana, temos que

$$n = 3q, 3q + 1 \; ou \; 3q + 2, \text{ para algum inteiro } q.$$

[1]Este resultado costuma ser erroneamente atribuído a Arquimedes [5]

Agora:

- Se $n = 3q$, então $n^2 = 3 \cdot 3q^2 + 0$.
- Se $n = 3q + 1$, então $n^2 = 3(3q^2 + 2q) + 1$.
- Se $n = 3q + 2$, então $n^2 = 3(3q^2 + 4q + 1) + 1$.

No primeiro caso acima, n^2 deixa resto 0 quando dividido por 3; nos outros dois casos, n^2 deixa resto 1 quando dividido por 3.

■

Exemplo 2.9. *Se a é um número natural com* $a \geq 3$*, então* a^2 *deixa resto 1 na divisão por* $a - 1$.

Solução: Usando a identidade $a^2 - 1 = (a + 1)(a - 1)$ temos que $a^2 = (a + 1)(a - 1) + 1$ com $1 < a - 1$, de onde segue o resultado.

■

Proposição 2.3 [7]**.** *A soma e o produto de quaisquer dois números inteiros deixa o mesmo resto que a soma e o produto dos seus restos, na divisão por um inteiro.*

Demonstração: Sejam $n_1,\ n_2,\ a \in \mathbb{Z}$. Pela divisão euclidiana, temos que existem $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tais que

$$n_1 = aq_1 + r_1 \quad \text{e} \quad n_2 = aq_2 + r_2 \quad \text{com } 0 \leq r_1, r_2 < a.$$

Então:

$$\begin{aligned} n_1 n_2 &= (aq_1 + r_1)(aq_2 + r_2) \\ &= a^2 q_1 q_2 + aq_1 r_2 + aq_2 r_1 + r_1 r_2 \\ &= a(aq_1 q_2 + q_1 r_2 + q_2 r_1) + r_1 r_2 \\ &= aq + r_1 r_2 \end{aligned} \tag{2.6}$$

onde $q = aq_1 q_2 + q_1 r_2 + q_2 r_1$. Agora dividimos $r_1 r_2$ por a para obtermos

$$r_1 r_2 = ap + r, \ \ p \in \mathbb{Z}, \ \ 0 \leq r < a. \tag{2.7}$$

Das igualdades (2.6) e (2.7) segue que

$$n_1 n_2 = aq + ap + r = a(q + p) + r, \qquad 0 \leq r < a \tag{2.8}$$

Portanto, de (2.7) e (2.8) concluímos que os restos que $n_1 n_2$ e $r_1 r_2$ deixam na divisão por a são iguais, ficando provado o resultado para o produto. A prova para a soma é análoga.

■

O exemplo a seguir figura o uso da proposição 2.1. A vantagem desta proposição é que em certos problemas que envolvem números muito grandes podemos substituir estes por números muito menores e mais confortáveis para trabalhar [7]. Também, este resultado sugere que podemos buscar resultados de divisibilidade buscando uma *"aritmética de restos"*.

Exemplo 2.10. *Seja* $N = 4^1 + 4^2 + 4^3 + 4^4 + 4^5 + \cdots + 4^{1000}$. *Calcule o resto da divisão de N por 3.*

Solução: Um caminho para resolver o problema é fazer a trabalhosa conta para achar o valor de N e dividir este valor por 3 encontrando o resto (Não queremos fazer isso!). Vamos usar a proposição 2.1 na solução. De fato, como 4 deixa resto 1 quando divido por 3, temos que 4^n deixa o mesmo que resto $1^n = 1$ quando dividido por 3, para todo natural n. Logo, N quando dividido por 3 deixa resto

$$\underbrace{1 + 1 + 1 + \cdots + 1}_{1000\ parcelas} = 1000 = 10^3,$$

e uma vez que 10 deixa resto 1 quando dividido por 3, temos que 10^3 deixa resto $1^3 = 1$ quando dividido por 3. Assim, N deixa resto 1 quando dividido por 3.

■

Exemplo 2.11. *Mostre que todo inteiro que é, ao mesmo tempo, um cubo e um quadrado deixa resto 0, 1 ou 4 quando dividido por 5.*

Solução*:* Seja n um inteiro que é, ao mesmo tempo, um cubo e um quadrado, ou seja, existe um inteiro q tal que $n = q^6$, pois $n = (q^3)^2$ é um quadrado, e $n = (q^2)^3$ é um cubo. Pela divisão euclidiana, $q = 5k + r$, $k \in \mathbb{Z}$ e $r \in \{0, 1, 2, 3, 4\}$, logo, pela proposição 2.3, temos que os únicos restos possíveis da divisão de q^6 por 5 são os restos da divisão de $0^6, 1^6, 2^6, 3^6, 4^6$ por 5. Ora,

- $0^6 = 0$ deixa resto 0 quando dividido por 5;
- $1^6 = 1$ deixa resto 1 quando dividido por 5;
- $2^6 = 64$ deixa resto 4 quando dividido por 5;
- $3^6 = 729$ deixa resto 4 quando dividido por 5;
- $4^6 = 4096$ deixa resto 1 quando dividido por 5;

Assim, concluímos que os únicos restos possíveis da divisão de n por 5 são 0, 1 ou 4.

■

Exemplo 2.12 *Ache todos os múltiplos de* 5 *que se encontram entre* 1 *e* 253.

Solução: Entre 1 e 253 temos 253 números, inclusive. Logo para encontrar todos os múltiplos de 5 entre esses números, temos que encontrar todos os múltiplos de 5 que cabem em 253. Ora, pela divisão euclidiana

$$253 = 5 \cdot 50 + 3,$$

ou seja, o maior múltiplo de 5 que cabe em 253 é $5 \cdot 50$, onde 50 é o quociente da divisão de 253 por 5. Assim, temos 250 múltiplos.

■

Exemplo 2.13. *Quantos múltiplos de* 7 *existem entre* 123 *e* 2551.

Solução: Denotemos por:

x: o número de múltiplos de 7 entre 1 e 2551;

y: o número de múltiplos de 7 entre 1 e 123.

Uma vez que 123 não é múltiplo de 7, a diferença entre $x - y$ é exatamente a quantidade de múltiplos existentes entre 123 e 2551. Usando o raciocínio empregado no exemplo 2.12 (faça as contas), podemos concluir que $x = 364$ e $y = 17$. Assim, temos 367 múltiplos de 7 entre 123 e 2551.

■

Exemplo 2.14 [11]**.** *O cometa Halley visita a Terra a cada 76 anos. Sua última passagem por aqui foi em 1986. Em que ano foi sua primeira passagem na era Cristã? Quantas vezes ele visitou a Terra desde o nascimento de Cristo?*

Solução: Como 1986 dividido por 76 dá resto 10, todos os anos em que o cometa por aqui passou dão resto 10 quando divididos por 76. A primeira visita ocorreu entre os anos 1 e 76, inclusive. Entre esses anos, o único que dividido por 76 dá resto 10 é o ano 10. Para descobrir quantas vezes ele visitou a Terra, precisamos calcular a quantidade de múltiplos de 76 entre 10 e 1986, ou seja, entre 1 e 1986. A resposta é 27 vezes, pois esse é o quociente da divisão de 1986 por 76.

■

O exemplo a seguir mostra uma aplicação geométrica dos conceitos até aqui desenvolvidos.

Exemplo 2.15. *Prove que em qualquer triângulo retângulo com lados inteiros, pelo menos um deles é múltiplo de 3.*

Solução: Denotemos por a e b os catetos e por c a hipotenusa. Suponhamos que nenhum deles seja divisível por 3. Como todo quadrado deixa resto 0 ou 1 na divisão por 3 (corolário 2.2), a^2 e b^2 deixam resto 1 na divisão por 3. Logo, pela proposição 2.3, $a^2 + b^2$ deixa resto $1^2 + 1^2 = 2$ na divisão por 3. Uma vez que $a^2 + b^2 = c^2$ (Teorema de Pitágoras), temos que c^2 deixa resto 2 na divisão por 3, o que é absurdo.

■

2.3 REPRESENTAÇÃO DE UM NÚMERO INTEIRO EM UMA BASE

Sabemos que o sistema universalmente utilizado para representar os números inteiros é o *Sistema Decimal Posicional*. Todavia, existem outros sistemas de numeração em uso – o sistema binário usado na computação, por exemplo. Uma característica comum a esses sistemas de numeração é o fato de serem todos sistemas posicionais de base constante. Nesta seção, seguimos [1] restringindo nosso estudo à representação dos números naturais, uma vez que o 0 tem seu próprio símbolo e todo número inteiro negativo é representado por um número natural precedido pelo sinal $menos$.

Antes de demonstrar o próximo teorema, vamos exemplificar a ideia utilizada na demonstração. Nosso objetivo será representar o número $60\,451$ na base 7, mas antes vamos recordar como representá-lo na base 10. O número $60\,451$ representa 1 unidade, 5 dezenas, 4 centenas, 0 unidade de milhar e 6 dezenas de milhar. Isso costuma ser representado da seguinte forma:

$$60\,451 = 6 \cdot 10^4 + 0 \cdot 10^3 + 4 \cdot 10^2 + 5 \cdot 10^1 + 1.$$

A expressão acima é rica de informações sobre o número $60\,451$. Com efeito, ela diz que a maior potência de 10 menor do que ou igual a $60\,451$ é 10^4. Diz também que se dividimos $60\,451$ por 10^4 vamos encontrar um quociente igual a 6 e um resto inferior a 10^3, por causa do "$0 \cdot 10^3$". Que este resto é maior do que 10^2 e que, quando dividido por 10^2 dá quociente 4 e resto superior a 10. E, finalmente, que este último resto, quando dividido por 10 dá quociente 5 e resto 1.

Para expressamos $60\,451$ na base 7, vamos proceder de forma a obter informações semelhantes àquelas do parágrafo anterior, só que o 7 fará o papel do "10". Primeiro dividimos $60\,451$ por 7 obtendo quociente $8\,635$ e resto 6. Em seguida dividimos este quociente $8\,635$ por 7 obtendo um segundo quociente igual $1\,233$ e resto 4, em seguida repetimos este processo até chegarmos a um quociente nulo, obtende a seguinte sequência de igualdades:

$$60451 = 7 \cdot 8635 + 6$$
$$8635 = 7 \cdot 1233 + 4$$
$$1233 = 7 \cdot 176 + 1$$
$$176 = 7 \cdot 25 + 1$$
$$25 = 7 \cdot 3 + 4$$
$$3 = 7 \cdot 0 + 3$$

Note que a sequência de quocientes é decrescente e formada apenas por inteiros positivos, logo ela deve atingir o valor zero (isso é uma observação importante que será usada na demonstração do resultado geral). Na primeira destas equações substituímos o valor de 8635 dado na segunda equação. Na expressão resultante substituímos o valor de 1233 dado na terceira, nesta o valor 176 dado na quarta e assim sucessivamente obtendo a seguinte expressão:

$$\begin{aligned} 60451 &= 7(7 \cdot 1233 + 4) + 6 \\ &= 7^2 \cdot 1233 + 4 \cdot 7 + 6 \\ &= 7^2(7 \cdot 176 + 1) + 4 \cdot 7 + 6 \\ &= 7^3 \cdot 176 + 1 \cdot 7^2 + 4 \cdot 7 + 6 \\ &= 7^3(7 \cdot 25 + 1) + 1 \cdot 7^2 + 4 \cdot 7 + 6 \\ &= 7^4 \cdot 25 + 1 \cdot 7^3 + 1 \cdot 7^2 + 4 \cdot 7 + 6 \\ &= 7^4(7 \cdot 3 + 4) + 1 \cdot 7^3 + 1 \cdot 7^2 + 4 \cdot 7 + 6 \\ &= 3 \cdot 7^5 + 4 \cdot 7^4 + 1 \cdot 7^3 + 1 \cdot 7^2 + 4 \cdot 7 + 6 \end{aligned}$$

Esta última expressão representa o número 60451 na base 7 que denotaremos por $(341146)_7$.

O que acabamos de fazer para o número 60451 foi desenvolver explicitamente o algoritmo para encontrar sua representação na base 7. Essa é a ideia central usada em uma das demonstrações do teorema que se segue. Uma segunda demonstração é por indução.

Teorema 2.2 (Teorema da Representação de um Número numa Base) *Seja b um inteiro positivo maior do 1. Então todo natural n pode ser representado de maneira única da seguinte forma:*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b^1 + a_0$$

onde $k \geq 0$, $a_k \neq 0$ e $0 \leq a_i < b,\ i \in \{0,1,2,\ldots,k\}$.

Primeira demonstração [5]**:** Para mostrarmos a existência procederemos exatamente da forma que acabamos de fazer para o caso $b = 7$. Iniciamos pela divisão de n por b obtento quociente q_0 e resto a_0. Em seguida dividimos q_0 por b obtendo quociente q_1 e resto a_1, e, prosseguindo desta forma, obtemos a seguinte sequência de igualdades:

$$
\begin{aligned}
n &= bq_0 + a_0 \\
q_0 &= bq_1 + a_1 \\
q_1 &= bq_2 + a_2 \\
q_2 &= bq_3 + a_3 \\
&\vdots \\
q_{k-2} &= bq_{k-1} + a_{k-1} \\
q_{k-1} &= b \cdot 0 + a_k,
\end{aligned}
$$

onde $0 \leq a_j < b,\ j = 0, 1, 2, \ldots, k$.

Agora, na primeira destas equações, substituímos o valor de q_0 dado na segunda. Em seguida, nesta expressão, o valor de q_1 dado na terceira, e assim sucessivamente, obtendo:

$$
\begin{aligned}
n &= bq_0 + a_0 \\
&= b(bq_1 + a_1) + a_0 \\
&= b^2 q_1 + a_1 b + a_0 \\
&= b^2(bq_2 + a_2) + a_1 b + a_0 \\
&= b^3 q_2 + a_2 b^2 + a_1 b + a_0 \\
&= b^3(bq_3 + a_3) + a_2 b^2 + a_1 b + a_0 \\
&= b^4 q_3 + a_3 b^3 + a_2 b^2 + a_1 b + a_0 \\
&\ \ \vdots \qquad\qquad \vdots \qquad\qquad \ddots \\
&= b^k q_{k-1} + a_{k-1} b^{k-1} + \cdots + a_2 b^2 + a_1 b + a_0 \\
&= a_k b^k + a_{k-1} b^{k-1} + \cdots + a_2 b^2 + a_1 b + a_0.
\end{aligned}
$$

Agora, vamos mostrar a unicidade desta representação. Com efeito, considere $n > 1$ e vamos denotar por $d_b(n)$ o número de representações de n na base b. Queremos, portanto, mostrar que $d_b(n)$ é sempre igual a 1. Como alguns dos coeficientes a_j podem ser nulos podemos supor, excluindo tais termos, que n possa ser representado na forma

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_s b^s$$

onde a_k e a_s são não nulos. Logo

$$
\begin{aligned}
n - 1 &= a_k b^k + a_{k-1} b^{k-1} + \cdots + a_s b^s - 1 \\
&= a_k b^k + a_{k-1} b^{k-1} + \cdots + (a_s - 1) b^s + b^s - 1 \\
&= a_k b^k + a_{k-1} b^{k-1} + \cdots + (a_s - 1) b^s + (b - 1)(b^0 + b^1 + b^2 + \cdots + b^{s-1}).
\end{aligned}
$$

Isto diz que para cada representação de n na base b é possível encontrar uma representação, na base b, para $n - 1$.

Logo $d_b(n) \leq d_b(n-1)$. Esta desigualdade nos diz que para $m \geq n$, temos

$$d_b(m) \leq d_b(m-1) \leq d_b(m-2) \leq \cdots \leq d_b(n+1) \leq d_b(n)$$

Como $n > 1$ e $d_b(n) \geq 1$, obtemos $1 \leq d_b(n) \leq d_b(1) = 1$. Assim, $d_b(n) = 1$, o que conclui a demonstração.

■

Segunda demonstração do teorema 2.2. (Por Indução): usaremos a Indução forte sobre n. Se $0 < n < b$, basta tomar $k = 0$ e $a_0 = n$, ou seja, $n = nb^0$. A unicidade fica clara nesse caso. Suponhamos o resultado válido para todo número natural menor do n, onde $n \geq b$ (hipótese de indução). Vamos mostrar que o resultado também é válido para n (passo indutivo). Com efeito, pela divisão euclidiana, existem q e r, únicos tais que

$$n = bq + r, \text{ com } 0 \leq r < b. \tag{2.9}$$

Como $0 < q < n$, pela hipótese de indução, segue que q pode ser representado de maneira única da seguinte forma:

$$q = c_{p+1}b^p + c_p b^{p-1} + \cdots + c_2 b^1 + c_1 \tag{2.10}$$

onde $p \geq 0$, $a_i \neq 0$ e $0 \leq c_i < b$, $i = 1, 2, \ldots, p+1$.

Pelas desigualdades (2.9) e (2.10), temos que

$$\begin{aligned} n = bq + r &= b(c_{p+1}b^p + c_p b^{p-1} + \cdots + c_2 b^1 + c_1) + r \\ &= c_{p+1}b^{p+1} + c_p b^p + \cdots + c_2 b^2 + c_1 b + r. \end{aligned}$$

O resultado segue pondo $a_0 = r$ e $k = p + 1$.

■

A representação dada no teorema 2.2 é chamada de expansão relativa à base b. Quando $b = 10$ essa expansão é chamada *expansão decimal*, e quando $b = 2$, ela é chamada de *expansão binária.*

Os algoritmos empregados para efetuar a adição e subtração na base 10 são facilmente estendidos para qualquer outra base. Observe que

$$\begin{array}{rr} & (3\ \ 2\ \ 1)_6 \\ + & (2\ \ 3\ \ 5)_6 \\ \hline & (1\ \ 0\ \ 0\ \ 0)_6 \end{array} \qquad \text{e} \qquad \begin{array}{rr} & (3\ \ 2\ \ 1)_6 \\ - & (2\ \ 3\ \ 5)_6 \\ \hline & (4\ \ 2)_6 \end{array}$$

Exprimindo cada número na base 10, efetuando, então, as operações e escrevendo a resposta na base 6, podemos confirmar as operações apresentadas acima.

Para efetuar uma divisão em uma base qualquer, devemos ter em mente a tabela de multiplicação nesta base. Por exemplo, na base 6, temos:

$$\begin{array}{r|l} (321)_6 & (54)_6 \\ \cline{2-2} (250)_6 & (3)_6 \\ \cline{1-1} (31)_6 & \end{array}$$

$$(54)_6 \cdot (2)_6 = (152)_6$$
$$(54)_6 \cdot (3)_6 = (250)_6$$
$$(54)_6 \cdot (4)_6 = (344)_6$$

ou seja,

$$(321)_6 = (3)_6 \cdot (54)_6 + (31)_6.$$

Exemplo 2.16 [7]**.** *Se desejarmos pesar qualquer número inteiro de gramas de ouro, entre 1g e 100g, numa balança de dois pratos, onde os pesos só podem ser usados no prato esquerdo da balança. Mostre que a escolha adequada de 7 pesos diferentes é suficiente para realizar esta tarefa.*

Solução: Usando o sistema em base 2 temos que qualquer número n tal que $1 \leq n \leq 100$ pode ser expressado de forma única como

$$n = a_6 2^6 + a_5 2^5 + a_4 2^4 + a_3 2^3 + a_2 2^2 + a_1 2 + a_0,$$

com $a_i \in \{0,1\}$, $0 \leq i \leq 6$. Observe que $2^n \geq 128$, com $n \geq 7$, logo estas potências não são consideradas. Notemos também que o fato de cada a_i ser 0 ou 1 nos diz que não precisamos repetir nenhum dos pesos na realização de qualquer pesada, logo os pesos

$$1, 2, 2^2, 2^3, 2^4, 2^5, 2^6$$

são suficientes para realizar as pesadas de gramas de ouro entre $1g$ e $100g$. ■

2.4 ALGUNS CRITÉRIOS DE DIVISIBILIDADE

Um critério de divisibilidade é uma regra que permite verificar se um número é divisível por outro sem efetuar necessariamente a divisão euclidiana. Com isso, visualizando o número ou fazendo algumas operações aritméticas básicas com seus dígitos, somos capazes de identificar se ele é ou não divisível por outro. Infelizmente, muitos alunos e até docentes da área de matemática, usam as regras de divisibilidade sem justificar o porquê de sua funcionalidade, esquecendo que são verdades matemáticas e como tais, carecem de demonstração para assim serem qualificadas. O que faremos nesta seção é enunciar e

demonstrar alguns critérios de divisibilidade. É também uma boa oportunidade para colocar em prática os conceitos estudados nas seções anteriores.

Quando escrevemos um número natural $n = a_k a_{k-1} \ldots a_1 a_0$, estamos expressando que

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0, a_i \in \{0, 1, 2, \ldots, 9\}.$$

Para a demonstração dos critérios de divisibilidade, estaremos sempre considerando a representação de número n num sistema de numeração de base 10. A maioria das proposições abaixo são aplicações do teorema 2.2 e da proposição 2.2. Vamos começar pelo critério de divisibilidade por 2.

Proposição 2.4. (Divisibilidade por 2) *Um número natural é divisível por 2 se, e somente se, o algarismo da unidade é um número par.*

Demonstração: dado um número natural n, vamos considerar a sua representação na base 10, ou seja,

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0, a_i \in \{0, 1, 2, \ldots, 9\}.$$

Disto concluímos que se $2 \mid n$, então como $2 \mid a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$, pela proposição 2.2, 2 deve dividir a_0, ou seja, a_0 é par. Reciprocamente, se $2 \mid a_0$, então $2 \mid n$, uma vez que $2 \mid a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10$.

■

Observação 2.5. Para obtermos um critério de divisibilidade por 5 basta, no argumento acima, substituir 2 por 5, concluindo o seguinte: "*Um número natural é divisível por 5 se, e somente se, o algarismo da unidade é* 0 *ou* 5*".*

◿

Proposição 2.5 (Divisibilidade por 3) *Um número natural é divisível por 3 se, e somente se, a soma de seus algarismos for um número divisível por 3.*

Demonstração: Novamente, vamos considerar a representação:

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0, a_i \in \{0, 1, 2, \ldots, 9\}.$$

Fazemos a seguir as seguintes substituições:

$$10 = 9 + 1 = 9 \cdot 1 + 1$$
$$10^2 = 99 + 1 = 9 \cdot 11 + 1$$
$$10^3 = 999 + 1 = 9 \cdot 111 + 1$$
$$\vdots \qquad \vdots \qquad \ddots$$
$$10^{k-1} = \underbrace{999 \ldots 99}_{k-1\ algarismos} + 1 = 9 \cdot \underbrace{111 \ldots 11}_{k-1\ algarismo} + 1$$
$$10^k = \underbrace{999 \ldots 99}_{k\ algarismos} + 1 = 9 \cdot \underbrace{111 \ldots 11}_{k\ algarismo} + 1$$

obtendo:

$$n = a_k\left(9 \cdot \underbrace{111 \ldots 11}_{k\ algarismo} + 1\right) + a_{k-1}\left(9 \cdot \underbrace{111 \ldots 11}_{k-1\ algarismo} + 1\right) + \cdots + a_1(9 \cdot 1 + 1) + a_0$$

$$= 9\left(a_k \cdot \underbrace{111 \ldots 11}_{k\ algarismo} + a_{k-1} \cdot \underbrace{111 \ldots 11}_{k\ algarismo} + a_1\right) + (a_k + a_{k-1} + \cdots + a_1 + a_0).$$

Daí concluímos que se $3 \mid n$, então como

$$3 \mid 9\left(a_k \cdot \underbrace{111 \ldots 11}_{k\ algarismo} + a_{k-1} \cdot \underbrace{111 \ldots 11}_{k\ algarismo} + a_1\right),$$

pela proposição 2.2, 3 deve dividir $(a_k + a_{k-1} + \cdots + a_1 + a_0)$.

Reciprocamente, se $3 \mid (a_k + a_{k-1} + \cdots + a_1 + a_0)$, então $3 \mid n$, uma vez que

$$3 \mid 9\left(a_k \cdot \underbrace{111 \ldots 11}_{k\ algarismo} + a_{k-1} \cdot \underbrace{111 \ldots 11}_{k\ algarismo} + a_1\right).$$

■

Observação 2.6. Para obtermos um critério de divisibilidade por 9 basta, no argumento acima, substituir 3 por 9, concluindo o seguinte: "*Um número natural é divisível por 9 se, e somente se, a soma de seus algarismos é um número divisível por 9.*

◿

Exemplo 2.17. 4783 é divisível por 3 pois, $(4 + 7 + 8 + 3) = 21$ é divisível por 3. Todavia, não é divisível por 9, uma vez que $9 \nmid 21$.

■

Proposição 2.6 (Divisibilidade por 4) *Um número natural é divisível por 4 se, e somente se, seus dois últimos dígitos formarem um número for divisível por 4.*

Demonstração: Se a quantidade de dígitos do número for menor do que ou igual a 2, a divisibilidade por 4 é verificada trivialmente.

Considere a representação decimal de um natural n com pelo menos três algarismos:

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0, \;\; a_i \in \{0, 1, 2, \ldots, 9\}.$$

Colocando 100 em evidência, temos que:

$$n = 100(a_k 10^{k-2} + a_{k-1} 10^{k-3} + \cdots + a_2) + a_1 10 + a_0, \;\; a_i \in \{0, 1, 2, \ldots, 9\}.$$

Denotando por $q = a_k 10^{k-2} + a_{k-1} 10^{k-3} + \cdots + a_2$, podemos escrever esta última expressão da seguinte maneira

$$n = 100q + a_1 a_0$$

onde "$a_1 a_0$" representa um número formado pelos dois últimos dígitos de n, isto é, a dezena e a unidade. Disto concluímos que se $4 \mid n$, então como $4 \mid 100$, pela proposição 2.2, 4 deve dividir $a_1 a_0$. Reciprocamente, se $4 \mid a_1 a_0$, então $4 \mid n$, uma vez que $4 \mid 100$.

■

Exemplo 2.18. O número 7.457.032 é divisível por 4, pois $4 \mid 32$. Como 14 não é divisível por 4, então 86.714 não divisível por 4.

■

Proposição 2.7 (Divisibilidade por 7). *Seja* $n = 10k + i$, *onde* $k \in \mathbb{N}$ *e* $i \in \{0, 1, 2, 3, \ldots, 9\}$, *logo* $7 \mid n$ *se , e só se,* $7 \mid k - 2i$.

Demonstração: Se $7 \mid n = 10k + i$, então existe um inteiro m tal que $10k + i = 7m$ e, portanto, $k + 2i = k - 2(7m - 10k) = k - 14m + 20k = 21k - 14m = 7(3k - 2m)$ o que implica $7 \mid k - 2i$. Reciprocamente, se $7 \mid k - 2i$, então existe um inteiro n tal que $k - 2i = 7n$ e, portanto, $10k + i = 10(7n + 2i) + i = 70n + 21i = 7(10n + 3i)$ o que implica $7 \mid 10k + i$.

■

Poderíamos enunciar a proposição 2.7 da seguinte forma: *"Um número é divisível por 7 quando estabelecida a diferença entre o dobro do último e os demais algarismos, constituir um número divisível por 7".*

Exemplo 2.19. Para verificar se um dado número é divisível por 7, aplicamos sucessivas vezes a proposição 2.7, ou seja: separamos o dígito das unidades e, do restante, subtraímos o dobro deste dígito. Em seguida repetimos este procedimento até a obtenção de um número suficientemente pequeno que possamos reconhecer, facilmente, se é ou não divisível por 7. Vamos aplicar o que foi descrito para um $n = 74.256$:

$$74256 = 10(7425) + 6$$

Dessa forma, $7425 - 2.6 = 7413$. Repetindo o processo temos:

$$741 - 2.3 = 735.$$

Novamente, temos que

$$73 - 2.5 = 63.$$

Como 63 é divisível por 7, então 735 também é. Sendo 735 divisível por 7, então 7413 também deverá ser e, a divisibilidade deste por 7 implica que 74256 deverá ser divisível por 7.

■

Para provar um critério de divisibilidade por 11, vamos precisar dos seguintes lemas:

Lema 2.2. *Todo número da forma* $99\ldots9$*, onde o número de "9"s é par, é divisível por 11.*

Demonstração: Observe que:

$$99 = 9 \cdot 11$$

$$9999 = 99 \cdot 10^2 + 99 = 11 \cdot 9(10^2 + 1)$$

$$999999 = 99 \cdot 10^3 + 99 \cdot 10^2 + 99 = 11 \cdot 9(10^3 + 10^2 + 1)$$

$$\therdots \qquad \vdots \qquad \ddots$$

$$\underbrace{99\ldots99}_{2n\ \text{"9"}s} = 99 \cdot 10^n + 99 \cdot 10^{n-1} + \cdots + 99 \cdot 10^2 + 99 = 11 \cdot 9(10^n + 10^{n-1} + \cdots 10^2 + 1)$$

Fica claro com isso o resultado.

■

Lema 2.3. *Se um número da forma 100…01, onde o número de "*0*"s entre os dois "uns" é par; então este número é divisível por 11.*

Demonstração: Note que

$$1001 = 990 + 11 = 99 \cdot 10 + 11$$
$$100001 = 99990 + 11 = 9999 \cdot 10 + 11$$
$$10000001 = 9999990 + 11 = 999999 \cdot 10 + 11$$
$$\therdots \qquad \vdots \qquad \ddots$$
$$1\underbrace{00\ldots0}_{2n\ "0"s}1 = \underbrace{99\ldots99}_{2n\ "0"s}0 + 11 = \underbrace{99\ldots99}_{2n\ "0"s} \cdot 10 + 11$$

Aplicando o lema 2.2, segue o resultado.

■

Proposição 2.8 (Divisibilidade por 11). *Um número $n = a_k a_{k-1} \ldots a_1 a_0$ é divisível por 11, caso a diferença $(a_1 + a_3 + \cdots) - (a_0 + a_2 + \cdots)$ resultar em um número divisível por 11.*

Demonstração: Seja $n = a_k a_{k-1} \ldots a_1 a_0$ um número com k dígitos. Provaremos o resultado para k par, sendo análogo o raciocínio para k ímpar. Com efeito, podemos representar n da seguinte forma:

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_3 10^3 + a_2 10^2 + a_1 10 + a_0.$$

Fazendo as seguintes substituições

$$10 = 11 - 1$$
$$10^2 = 99 + 1$$
$$10^3 = 1001 - 1$$
$$10^4 = 999 + 1$$
$$\vdots$$
$$10^{k-1} = 1\underbrace{00\ldots0}_{k-2\ "0"s}1 - 1$$
$$10^k = \underbrace{999\ldots99}_{k-1\ "9"s} + 1$$

obtemos

$$n = a_k\left(\underbrace{99\ldots9}_{k-1\ "9"s} + 1\right) + a_{k-1}\left(1\underbrace{00\ldots0}_{k-2\ "0"s}1 - 1\right) + \cdots + a_3(1001 - 1) + a_2(99 + 1) +$$
$$+ a_1(11 - 1) + a_0 =$$

$$= \underbrace{99\ldots99}_{k-1\ "9"s}a_k + 1\underbrace{00\ldots0}_{k-2\ "0"s}1a_{k-1} + \cdots + 1001a_4 + 99a_3 + 11a_2 - [(a_{k-1} + a_{k-3} + \cdots +$$
$$a_3 + a_1) - (a_k + a_{k+2} + \cdots + a_2 + a_0)].$$

Como, pelos lemas 2.2 e 2.3,

$$11 \mid \left(\underbrace{99\ldots99}_{k-1\ "9"s}a_k + 1\underbrace{00\ldots0}_{k-2\ "0"s}1a_{k-1} + \cdots + 1001a_4 + 99a_3 + 11a_2\right)$$

então n será divisível por 11, se, e somente se,

$$11 \mid [(a_{k-1} + a_{k-3} + \cdots + a_3 + a_1) - (a_k + a_{k+2} + \cdots + a_2 + a_0)].$$

■

Exemplo 2.20. Seja $n = 503.217$. Como $(7 + 2 + 0) - (1 + 3 + 5) = 0$ é um número divisível por 11, então 503.217 também é.

■

PROBLEMAS PROPOSTOS

2.1. Demonstre, usando o método da indução, que:

(a) $6 \mid n^3 - 1$ para todo n natural.

(b) $24 \mid 5^n - 1$ para todo número natural n par.

(c) $2^n + 1$ é múltiplo de 3 para todo natural ímpar n

(d) $4^n + 15n - 1$ é um múltiplo de 9 para todo natural n.

2.2. Encontre o resto que deixa

(a) $2001 \cdot 2002 \cdot 2003 \cdot 2004 + 2005^2$ quando dividido por 7;

(b) 2^{100} quando dividido por 3;

(c) $13424136 + 1234567890$ quando dividido por 3.

2.3. Prove que 5 divide $1^{99} + 2^{99} + 3^{99} + 4^{99} + 5^{99}$.

2.4. Mostre que a equação $x^3 + px + q = 0$ não possui nenhuma solução racional, onde p *e* q são números ímpares.

2.5. Mostre que:

(a) N^2 nunca deixa resto 2 quando dividido por 6, onde N um número natural.

(b) $se\ n$ é ímpar, então a soma de n termos consecutivos de uma PA de números naturais é sempre divisível por n.

2.6.

(a) Encontre os possíveis restos da divisão de um cubo por 7.

(b) Se $x, y\, z$ são inteiros tais que $x^3 + y^3 - z^3$ é múltiplo de 7, prove que pelo menos um dentre os números x, y, z é múltiplo de 7.

2.7. Expresse o número 274 nas bases 2, 5, 7 e 9.

2.8. Transforme para base 10 os seguintes números:

(a) $(2351)_7$ (b) $(7706)_8$ (c) $(1001110)_2$ (d) $(11122)_4$

2.9.

(a) Mostre se um inteiro é um quadrado e um cubo, então ele é da forma $7k$ ou $7k + 1$.

(b) Mostre se um inteiro é um quadrado, então ele é da forma $5k$ ou $5k + 1$ ou $5k + 4$.

(c) Mostre se um inteiro é um quadrado, então ele é da forma $4k$ ou $4k + 1$.

(d) Mostre que nenhum quadrado pode ser da forma $3k + 2$.

2.10.

(a) Mostre que o algarismo das unidades de um quadrado só pode um dos seguintes: $0, 1, 4, 5, 6$ ou 9.

(b) Mostre que nenhum dos números 22, 222, 2222, … , ou 33, 333, 3333, … , ou 77, 777, 7777, … , ou ainda 88, 888, 8888, … , pode ser um quadrado.

2.11.

(a) Mostre que nenhum quadrado ou soma de dois quadrados é da forma $4k + 3$.

(b) Mostre que nenhum elemento da sequência 11, 111, 1111, … é um quadrado ou a soma de dois quadrados.

(c) Idem para nenhum elemento das seguintes sequências:

44, 444, 4444, … ; 55, 555, 5555, … ; 99, 999, 9999, … .

2.12. Mostre que, de n inteiros consecutivos, um, e somente um, deles é divisível por n.

2.13 Mostre que não existe dois cubos perfeitos cuja diferença seja 4.

DIOFANTO E FERMAT: RENASCE A TEORIA DOS NÚMEROS

Nesta nota histórica, encontra-se a abordagem com base em [1] e [10].

Após Euclides, a Teoria dos Números se estagnou por cerca de 500 anos, ressuscitando com os trabalhos de Diofanto de Alexandria, que viveu por volta de 250a.C. A obra que Diofanto nos legou chama-se *Aritmética*. Dos 13 volumes que constam em sua obra, apenas 7 deles chegaram até nós. Esta obra é primeiro tratado de álgebra até hoje conhecido. Diferente de seus precursores, Diofanto faz uma abordagem totalmente algébrica, não sendo revestida de qualquer interpretação ou linguagem geométrica. Muitas vezes ele se limita a encontrar soluções inteiras de determinadas equações algébricas com uma ou várias incógnitas, se abstendo dos aspectos conceituais e teóricos os quais Platão preconizava acerca da abordagem aritmética. Por exemplo, Diofanto chegou a descrever em números inteiros todas as soluções da equação $x^2 + y^2 = z^2$.

A obra de Diofanto, como veremos a seguir, foi fundamental para o renascimento da Teoria dos Números, 1300 anos depois.

A Renascença, movimento ocorrido entre os séculos XII e XV na Europa, cujas características principais foram a luta contra os preconceitos da época e a redescoberta da leitura dos clássicos gregos, teve por consequência uma revolução nas artes, nas ciências e nos costumes.

Este movimento atingiu a Matemática um pouco mais tardiamente. Em 1575, Regiomanto traduziu para o latim o *Aritmética,* de Diofanto. Em 1621, Bachet de Méziriac publicou uma edição francesa que se tornaria protagonista de uma das mais ricas das histórias de toda a Matemática.

Por essa época, que renasceu a Teoria dos Números, na acepção de Platão, essencialmente por obra do jurista francês Pierre de Fermat (1601 – 1665). Após Euclides e Eratóstenes, Fermat pode ser considerado o primeiro matemático a contribuir para o desenvolvimento da Teoria dos Números do ponto de vista teórico.

Algumas contribuições de Fermat ao assunto foram divulgadas por meio de correspondências, principalmente com o padre Marin Mersenne (1588-1648), que desempenhava o papel de divulgador das Ciências com uma extensa correspondência com os maiores cientistas da época. Em uma dessas cartas, por exemplo, que data 1640, Fermat enunciou o seu Pequeno Teorema (nosso Teorema 5.2), dizendo que não escreveria a demonstração por ser longa de mais.

Todavia, a maioria das contribuições de Fermat à Teoria dos Números se deu na forma de enunciados e notas escrita nas margens do exemplar que ele tinha do *Aritmética* de Diofanto, traduzido por Bachet. A sua contribuição mais marcante foi a anotação que deixou na margem do Problema 8, Livro 2, onde se encontravam descritas as infinitas soluções da equação $x^2 + y^2 = z^2$. Fermat escreveu: *"Por um lado, é impossível separar um cubo de dois cubos, ou uma biquadrada de duas biquadradas, ou, em geral, uma potência qualquer, exceto um quadrado em duas potências semelhantes. Eu descobri uma demonstração verdadeiramente maravilhosa disto, que, todavia esta margem não é suficiente para cabê-la."*. Essa afirmação, apesar de não demonstrada por ele, acabou sendo chamada de *Último Teorema de Fermat*.

Fermat chegou até a demonstrar que a equação $x^4 + y^4 = z^4$ não possui solução inteira , mas nenhum registro foi encontrado no tocante a demonstração do caso geral para a equação $x^n + y^n = z^n$. Passaram-se mais 350 anos para que isso fosse demonstrado.

Por suas contribuições à Matemática, Fermat é conhecido como "Príncipe dos Amadores".

3 - MÁXIMO DIVISOR COMUM

Uma noção cuja preponderância na aritmética é surpreendente, dada a sua simplicidade, é a noção de *máximo divisor comum (mdc),* que apresenta papel crucial em toda Teoria dos Números e suas extensões [12]. Ele é o objeto central deste capítulo onde definimos e provamos suas principais propriedades. Descrevemos o *Algoritmo de Euclides* para o cálculo do mdc de dois inteiros, explanamos acerca de sua noção "dual", o *mínimo múltiplo comum (mmc)* e, finalmente, mostramos como se resolvem certas equações envolvendo inteiros.

3.1 MÁXIMO DIVISOR COMUM

Dados dois números inteiros a e b (a ou b não nulos), a cada um deles pode-se associar seu conjunto de divisores, D_a e D_b respectivamente. A interseção $D_a \cap D_b$ é não vazia (já que 1 pertence à interseção). Por ser finito, $D_a \cap D_b$ possui elemento máximo. Exemplifiquemos.

Exemplo 3.1. Sejam

$D_{24} = \{\pm 24, \pm 12, \pm 8, \pm 6, \pm 4, \pm 3, \pm 2, \pm 1\}$ e $D_{-18} = \{\pm 18, \pm 9, \pm 6, \pm 3, \pm 2, \pm 1\}$,

respectivamente, os conjuntos dos divisores de 24 e -18, então o conjunto

$$D_{24} \cap D_{-18} = \{\pm 6, \pm 3, \pm 2, \pm 1\}$$

dos divisores comuns de tais números é finito e possui elemento máximo igual a 6.

■

Dessa forma, a definição abaixo é consistente.

Definição 3.1 (Máximo Divisor Comum – mdc). *Dizemos que $d \in \mathbb{N}$ é um máximo divisor comum de dois inteiros a e b ($a \neq 0$ ou $b \neq 0$), denotado por (a, b), se possuir as seguintes propriedades:* (i) $d \mid a$ e $d \mid b$, e (ii) $c \mid a$ e $c \mid b \Rightarrow c \mid d$.

Observação 3.1. Devemos observar que, na definição de máximo divisor comum, foi exigido que a e b fossem não simultaneamente nulos porque, caso contrário, qualquer inteiro c seria um divisor comum de a e b, o que tornaria impossível tomar o maior desses números. Quando $a = b = 0$ convencionamos o $(0, 0) = 0$.

◿

Note que na definição 3.1, o item (i) diz que d é um divisor comum de a e b; enquanto (ii) afirma que todo divisor comum de a e b tem que necessariamente dividir d, isso equivale a dizer que d é o maior inteiro com a propriedade (i). Além disso, a condição (ii) implica na unicidade do mdc. De fato, se $d\ e\ d'$ são dois mdc's de um mesmo par de números, então, $d \mid d'$ e $d' \mid d$, o que implica $|d| \leq |d'|$ e $|d'| \leq |d|$. Como $d, d' > 0$, segue que $d' = d$.

Mais ainda [1], para todo $b \in \mathbb{Z}$, temos que $a \mid b \Leftrightarrow (a, b) = |a|$. Com efeito, temos que $|a|$ é um divisor comum de a e b, e se c é um divisor comum de a e b, então c divide $|a|$, logo $|a| = (a, b)$. Reciprocamente, se $|a| = (a, b)$, segue-se que $|a|$ divide b, logo $a \mid b$.

Para efeitos de cálculo do mdc de dois números, podemos sempre supô-los não negativos. Com efeito [6], basta observar que dados dois inteiros a e b, temos sempre que $(a, b) = (-a, b) = (a, -b) = (-a, -b)$. Sendo assim, para efeitos de mdc, consideraremos daqui por diante os divisores positivos dos números.

O teorema a seguir é uma das ferramentas básicas na resolução de problemas que envolvem o mdc de dois números [7]. O resultado foi provado pela primeira vez por Claude-Gaspard Bachet de Méziriac (1581-1638) e mais tarde generalizado para polinômios por Étienne Bézout (1730-1783).

Teorema 4.1 (Teorema de Bachet- Bézout). *Seja $d = (a, b)$ com a ou b diferente de zero, então existem inteiros n_0 e m_0 tais que $d = n_0 a + m_0 b$.*

Demonstração: Seja o conjunto $B = \{na + mb; n, m \in \mathbb{Z}\}$. Como B possui algum valor natural (justifique), podemos escolher $n_0\ e\ m_0$ tais que $c = n_0 a + m_0 b$ seja o menor elemento de B. Afirmamos que $c \mid a$ e $c \mid b$. Mostraremos apenas que $c \mid a$, pois as demonstrações são similares. A prova é por contradição. Suponha que $c \nmid a$. Nesse caso, a divisão euclidiana garante que existem q e r tais que $a = qc + r$ com $0 < r < c$. Daí,

$$r = a - qc = a - q(n_0 a + m_0 b) = (1 - qn_0)a + (-qm_0)b$$

o que mostra que $r \in B$ uma vez que $(1 - qn_0)$ e $(-qm_0)$ são inteiros. Mas isso é uma contradição, pois $0 < r < c$ e c é o menor elemento de B.

Como d é um divisor comum de a e b, existem k_1 e k_2 tais que $a = k_1 d$ e $b = k_2 d$ e, portanto,

$$c = n_0 a + m_0 b = n_0 k_1 d + m_0 k_2 d = d(n_0 k_1 + m_0 k_2)$$

o que implica $d \mid c$. Ora, pela proposição 2.3(iii), temos que $0 < d \leq c$ e como $d < c$ não é possível, uma vez que d é o máximo divisor comum, concluímos que $d = c = n_0 a + m_0 b$.

■

Observação 3.2. O conjunto *B* usado na demonstração acima é chamado de *conjunto de todas as combinações lineares dos números a e b*. Mostramos não apenas que (a, b) pode ser expresso como uma combinação linear destes números, mas que (a, b) é o menor valor positivo dentre todas estas combinações, ou seja, $(a, b) = min\{na + mb > 0; n, m \in \mathbb{Z}\}$.

◿

Definição 3.2. *Dizemos que dois números inteiros a e b são primos entre si, ou coprimos quando o* $(a, b) = 1$.

Exemplo 3.2. Como $(4, 15) = 1$, temos que 4 e 15 são primos entre si.

■

Um resultado curioso relacionado a números coprimos, citado por Hefez em [2], é o teorema de Cesaro demonstrado em 1881. Este teorema diz que *a probabilidade de dois números inteiros positivos escolhidos ao acaso serem coprimos é* $6/\pi^2$ (aproximadamente 61%).

Corolário 3.1. *Dois inteiros a e b são primos entre si se, e somente se, existem números inteiros m e n tais que* $ma + nb = 1$.

Demonstração: Suponha que a e b são primos entre si, logo $(a, b) = 1$. O teorema de Bachet-Bézout garante que existem $m, n \in \mathbb{Z}$ tais que $ma + nb = 1$. Reciprocamente, assumindo que $ma + nb = 1$ temos que todo inteiro que divide a e b tem que dividir 1. Em particular $(a, b) \mid 1$ e, portanto, $(a, b) = 1$.

■

Algebricamente, esclarece Hefez em [1], o corolário 3.1 estabelece uma relação crucial entre a estrutura aditiva e multiplicativa dos números inteiros, o que permitirá provar, entre outros resultados, o importante teorema a seguir, conhecido como *Lema de Gauss*, em homenagem ao grande matemático alemão Johann Carl Friedrich Gauss (1777-1885).

Teorema 3.2. (Lema de Gauss) *Sejam a, b e c números inteiros. Se $c \mid ab$ e $(b,c) = 1$, então $c \mid a$.*

Demonstração: Das hipóteses temos que existem inteiros n_0 e m_0 tais que

$$bn_0 + cm_0 = 1.$$

Multiplicando a igualdade acima por a em ambos os lados, temos que

$$abn_0 + acm_0 = a.$$

Por outro lado, $ab = cq$ para algum inteiro q. Usando esta condição na última igualdade temos que

$$cqn_0 + acm_0 = c(qn_0 + am_0) = a,$$

logo $c \mid a$.

■

A seguir, outras consequências importantes do Teorema de Bachet- Bézout.

Proposição 3.1. Sejam $d, t \in \mathbb{N}$ *e* $a, b, c \in \mathbb{Z}$. *Então valem as seguintes afirmações:*

(i) $(ta, tb) = t(a, b)$.

(ii) *Se* $d \mid a$ *e* $d \mid b$, *então* $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b)$. *Consequentemente,* $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.

(iii) *Se* $(a, c) = (b, c) = 1$, *então* $(ab, c) = 1$.

Demonstração:

(i) Como t é positivo, usando a observação 3.2, temos

$$\begin{aligned}(ta, tb) &= min\{nta + mtb > 0; \quad n, m \in \mathbb{Z}\} \\ &= t \cdot min\{na + mb > 0; \quad n, m \in \mathbb{Z}\} \\ &= t(a, b).\end{aligned}$$

(ii) É uma consequência imediata da afirmação (i), observando que

$$(a, b) = \left(d\frac{a}{d}, d\frac{b}{d}\right) = d\left(\frac{a}{d}, \frac{b}{d}\right).$$

(iii) De $(a, c) = (b, c) = 1$, temos que existem inteiros n_1, n_2, m_1, m_2, tais que

$$an_1 + cm_1 = 1 \quad \text{e} \quad bn_2 + cm_2 = 1.$$

Multiplicando lado a lado as igualdades obtemos

$$(\underbrace{n_1 n_2}_{m})ab + \underbrace{(an_1 m_2 + m_1 bn_2 + cm_1 m_2)c}_{n} = 1.$$

Então a igualdade acima, juntamente com o teorema de Bachet- Bézout, resulta em $(ab, c) = 1$.

■

Exemplo 3.3. Como $(14,35) = 7$ temos que $(14/7\,, 35/7) = 1$. Como $4 \mid (27 \cdot 20)$, então $4 \mid 20$ uma vez que $(4, 27) = 1$.

■

Exemplo 3.4 [13]**.** Sejam a, b, c, d inteiros não nulos, tais que $c + d \neq 0$ e $ad - bc = 1$. Prove que a fração $\frac{a+b}{c+d}$ é irredutível (Uma fração é irredutível se seus constituintes, numerador e denominador, são números primos entre si).

Solução: Queremos provar que $(a + b, c + d) = 1$. Para isso, temos que encontrar inteiros m, n tais que

$$(a + b)n + (c + d)m = 1$$

Ora, desde que $ad - bc = 1$, basta tomar $n = d$ e $m = -b$.

■

3.2 ALGORITMO DE EUCLIDES

Observe que o processo que utilizamos no exemplo 3.1 para encontrar o mdc de 24 e -18 não é muito prático. Talvez pudéssemos pensar que, uma vez fixada a definição de mdc de dois inteiros a e b, pudéssemos sempre proceder como no exemplo 3.1, ou seja, calcular todos os divisores de a, todos os divisores de b e descobrir qual o maior elemento comum aos dois conjuntos. Mas se os números forem "grandes" como 123 400 e 567 800, por exemplo? Em [7], Oliveira esclarece que apesar de conhecermos propriedades teóricas do mdc entre dois inteiros, encontrá-lo de fato pode ser uma tarefa complicada, sem o auxílio de uma ferramenta correta.

Felizmente, Euclides, em *Os Elementos* (Livro VII, proposição 2), dá uma "receita" eficiente para o cálculo do mdc de dois inteiros. O método desenvolvido por ele, chamado de *Algoritmo de Euclides*, é um primor do ponto de vista computacional e pouco conseguiu-se aperfeiçoá-lo em mais de dois milênios [1].

A proposição a seguir é o ponto de partida para o desenvolvimento do Algoritmo de Euclides, não obstante um mecanismo eficiente para resolver alguns problemas (exemplos 3.5 e 3.6).

Proposição 3.2 (Lema de Euclides). *Para a, b e x inteiros temos que* $(a, b) = (a, b + ax)$.

Demonstração: Seja $d = (a, b + ax)$. Como $d \mid a$ e $d \mid b + ax$, segue da proposição 2.2 que $d \mid -ax + b + ax$, ou seja, $d \mid b$. Logo, d é um divisor comum de a e b. Suponha agora c seja um divisor comum de a e b. Logo, $c \mid a$ e $c \mid b + ax$ e, portanto, $c \mid d$. Daí, concluímos que $d = (a, b)$.

■

Exemplo 3.5. *Dados $a \in \mathbb{Z}$ com $a \neq 1$ e $m \in \mathbb{N}$, prove que*

$$\left(\frac{a^m - 1}{a - 1}, a - 1\right) = (a - 1, m).$$

Solução: Note que a igualdade é válida para $m = 1$. Supondo que $m \geq 2$, temos pelo problema 2.4.(a) que

$$\begin{aligned}\left(\frac{a^m - 1}{a - 1}, a - 1\right) &= (a^{m-1} + a^{m-2} + \cdots + a + 1, a - 1) \\ &= \left((a^{m-1} - 1) + (a^{m-2} - 1) + \cdots + (a - 1) + (m - 1) + 1, a - 1\right) \\ &= \left((a^{m-1} - 1) + (a^{m-2} - 1) + \cdots + (a - 1) + m, a - 1\right).\end{aligned}$$

Como, pelo exemplo 2.3 (i), temos que

$$a - 1 \mid (a^{m-1} - 1) + (a^{m-2} - 1) + \cdots + (a - 1),$$

segue que $(a^{m-1} - 1) + (a^{m-2} - 1) + \cdots + (a - 1) = n(a - 1)$ para algum $n \in \mathbb{Z}$. Assim, o lema de Euclides garante que

$$\left(\frac{a^m - 1}{a - 1}, a - 1\right) = (\, n(a - 1) + m, a - 1) = (a - 1, n(a - 1) + m) = (a - 1, m).$$

■

Exemplo 3.6. *Determine os valores de $a \in \mathbb{Z}$ e $n \in \mathbb{N}$ para os quais $a + 1$ divide $a^{2n} + 1$.*

Solução: Primeiro perceba que $a + 1 \mid a^{2n} + 1$ é equivalente a $(a + 1, a^{2n} + 1) = |a + 1|$. Como $a^{2n} + 1 = (a^{2n} - 1) + 2$ e $a + 1 \mid a^{2n} - 1$ (justifique), pelo lema de Euclides, temos que para todo n,

$$(a + 1, a^{2n} + 1) = (a + 1, (a^{2n} - 1) + 2) = (a + 1, 2).$$

Portanto, dizer que $a + 1 \mid a^{2n} + 1$, equivale a $(a + 1, 2) = |a + 1|$, o que ocorre se, e somente se, $a = 0, a = 1, a = -2$ ou $a = -3$ e n qualquer.

■

A proposição a seguir, que é consequência da proposição 2.2, nos apresenta um resultado bastante elementar, mas de grande importância na demonstração do algoritmo de Euclides.

Proposição 3.3. *Se a e b são naturais, então $(a,b) = (b,r)$, onde r é o resto da divisão de a por b.*

Demonstração: Pela divisão euclidiana, temos que existem q e r naturais tais que

$$a = bq + r \text{ com } 0 \leq r < b.$$

Disso, e pelo lema de Euclides, temos que

$$(b,r) = (b, a - bq) = (b,a) = (a,b).$$

■

O algoritmo de Euclides consiste na aplicação reiterada da proposição 3.3. Para fixa ideias acerca da demonstração do teorema 3.3, descrevê-la-emos através de um exemplo.

Exemplo 3.7. Vamos calcular o máximo divisor comum de 1001 e 109. Com efeito, utilizamos a divisão Euclidiana para dividir 1001 por 109. Em seguida, dividimos 109 pelo resto 20. Depois 20 pelo resto 9 e assim, sucessivamente, até obtermos resto zero – note que a sequências de restos formam uma sequência estritamente decrescente, logo temos que atingir eventualmente o zero.

$$\begin{aligned} 1001 &= 109 \cdot 9 + 20 \\ 109 &= 20 \cdot 5 + 9 \\ 20 &= 9 \cdot 2 + 2 \\ 9 &= 2 \cdot 4 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned} \qquad (3.1)$$

Da última equação temos que $(2,1) = 1$ e agora, pela proposição 3.3, podemos concluir da equação $9 = 2 \cdot 4 + 1$, que $(9,2) = (2,1)$, da equação $20 = 9 \cdot 2 + 2$ que $(20,9) = (9,2)$ e, por sucessivas aplicações da proposição 3.3, chegamos na sequências de igualdades

$$1 = (2,1) = (9,2) = (20,9) = (109,20) = (1001,109).$$

Dessa forma, $(1001,109) = 1$, ou seja, o máximo divisor comum de 1001 e 109 é o último resto não nulo da sequência de divisões descrita em (3.1).

Teorema 3.3 (Algoritmo de Euclides). *Sejam a e b inteiros não negativos com $b \neq 0$. Se a divisão euclidiana for aplicada sucessivamente para obter a seguinte sequência de igualdades*

$$\begin{cases} a = bq_1 + r_1, & 0 \leq r_1 < b \\ b = r_1q_2 + r_2, & 0 \leq r_2 < r_1 \\ r_1 = r_2q_3 + r_3, & 0 \leq r_3 < r_2 \\ \quad \ldots \quad \ldots \quad \ldots & \quad \ldots \quad \ldots \\ r_{n-2} = r_{n-1}q_n + r_n, & 0 \leq r_n < r_{n-1} \\ r_{n-1} = r_nq_{n+1}, & \end{cases} \tag{3.2}$$

até algum r_n dividir r_{n-1}. Assim, $(a, b) = r_n$, ou seja, o máximo divisor de a e b é o último resto não-nulo no processo de divisão anterior.

Demonstração: Tendo em mente o exemplo 3.7 fica fácil acompanhar a demonstração. Começamos observando que o processo de divisão (3.2) é finito. Com efeito, note que a cada passo o resto é sempre menor do que o anterior, e estamos lidando com números inteiros positivos, então após um número finito de aplicações da divisão euclidiana, teremos resto nulo. Examinando as igualdades em (3.2) de cima para baixo e usando a proposição 3.3 temos que

$$(a, b) = (a, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = r_n.$$

■

Observação 3.3. Veremos no próximo capítulo que podemos encontrar o mdc valendo-nos das fatorações dos números envolvidos, todavia quando estamos trabalhando com números grandes o algoritmo de Euclides, esclarece Oliveira em [7], em geral, é mais fácil que a fatoração, podendo ser esta última bem difícil.

◿

Exemplo 3.8. *Utilizando o algoritmo de Euclides, calcule o máximo divisor comum de 1126 e 522.*

Solução: Aplicando sucessivamente a divisão euclidiana, temos que

$$\begin{aligned} 1126 &= 522 \cdot 2 + 82 \\ 522 &= 82 \cdot 6 + 30 \\ 82 &= 30 \cdot 2 + 22 \\ 30 &= 22 \cdot 1 + 8 \\ 22 &= 8 \cdot 2 + 6 \\ 8 &= 6 \cdot 1 + 2 \\ 6 &= 2 \cdot 3 + 0. \end{aligned} \tag{3.3}$$

Pelo algoritmo de Euclides, temos que $(1126,522) = 2$, uma vez que 2 é o ultimo resto não-nulo no processo de divisão.

■

Podemos sintetizar o algoritmo de Euclides diagramando os números envolvidos no processo de divisão (3.2) como a seguir:

	q_1	q_2	q_3	...	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	...	r_{n-2}	r_{n-1}	$r_n = (a, b)$
r_1	r_2	r_3	r_4	...	r_n		

Por exemplo, diagramando os números do processo (3.3) do exemplo 3.8, temos que

	2	6	2	1	2	1	3
1126	522	82	30	22	8	6	$2 = (1126,522)$
82	30	22	8	6	2		

Observando a diagramação acima, o algoritmo de Euclides fornece-nos:

$$2 = 8 - 1 \cdot 6$$
$$6 = 22 - 2 \cdot 8$$
$$8 = 30 - 1 \cdot 22$$
$$22 = 82 - 2 \cdot 30$$
$$30 = 522 - 6 \cdot 82$$
$$82 = 1126 - 2 \cdot 522$$

Donde se segue que:

$$\begin{aligned} 2 &= 8 - 1 \cdot 6 = 8 - 1 \cdot (22 - 2 \cdot 8) \\ &= 3 \cdot 8 - 1 \cdot 22 = 3 \cdot (30 - 1 \cdot 22) - 1 \cdot 22 \\ &= 3 \cdot 30 - 4 \cdot 22 = 3 \cdot 30 - 4 \cdot (82 - 2 \cdot 30) \\ &= 11 \cdot 30 - 4 \cdot 82 = 11 \cdot (522 - 6 \cdot 82) - 4 \cdot 82 \\ &= 11 \cdot 522 - 70 \cdot 82 = 11 \cdot 522 - 70 \cdot (1126 - 2 \cdot 522) \\ &= 151 \cdot 522 + (-70) \cdot 1126 \end{aligned}$$

Temos, então, que

$$(522{,}1126) = 2 = 151 \cdot 522 + (-70) \cdot 1126.$$

Note que com algoritmo de Euclides de trás para frente, conseguimos escrever $(522{,}1126)$ como a combinação linear de 522 e 1126. De fato, encontramos os números 151 e -70 tais que $(522{,}1126) = 151 \cdot 522 + (-70) \cdot 1126$. Pela observação 3.2, este é o menor valor positivo dentre todas as combinações lineares dos números 522 e 1126.

Quando utilizarmos o algoritmo de Euclides para expressar (a, b) na forma $ma + nb$, com $m, n \in \mathbb{Z}$, chamá-lo-emos de *algoritmo de Euclides estendido.*

Notemos que o teorema de Bachet-Bézout pode ser obtido como consequência do algoritmo de Euclides estendido, uma vez que este exibe explicitamente a menor dentre todas as combinações lineares de dois números inteiros ambos não nulos.

Existe outra versão do algoritmo de Euclides que foi publicada em 1963. Para mais detalhes consulte a página 101 de [1].

3.3 MÍNIMO MÚLTIPLO COMUM

Com a teoria de mdc desenvolvida, podemos agora discorrer sobre sua noção dual, ou seja, a noção de *mínimo múltiplo Comum (mmc)*. Essa dualidade (maior *vesus* menor) se concentra exatamente no fato desses conceitos – mdc e mmc – se interligarem.

Se denotarmos por M_n o conjunto dos múltiplos não nulos de n, dados dois números inteiros a e b com $a \neq 0$ e $b \neq 0$, então a interseção de $M_a \cap M_b \cap \mathbb{N} \neq \emptyset$ é não vazia, já que

$|ab| \subset M_a \cap M_b$. Logo, pelo Princípio da Boa Ordenação, $M_a \cap M_b \cap \mathbb{N}$ possui um elemento mínimo.

Exemplo 3.9. Seja $a = -6$ e $b = 15$. O conjunto dos múltiplos não nulos de -6 é

$$M_{-6} = \{\pm 6, \pm 12, \pm 18, \pm 24, \pm 30, \dots\},$$

e o dos múltiplos não nulos de 15 é

$$M_{15} = \{\pm 15, \pm 30, \pm 45, \pm 24, \pm 60, \dots\}.$$

Portanto,

$$M_a \cap M_b \cap \mathbb{N} = \{30,60,90, \dots\},$$

donde o menor elemento desse conjunto é 30.

■

A existência do elemento mínimo no conjunto $M_a \cap M_b \cap \mathbb{N}$ é quem torna consistente a definição a seguir.

Definição 3.3 (Mínimo Múltiplo Comum – mmc) *Dizemos que um número inteiro* $m > 0$ *é um mínimo múltiplo comum de dois inteiros* a *e* b *não-nulos, denotado por* $[a, b]$, *se possuir as seguintes propriedades:*

$(i)\ a \mid m \ \ e \ \ b \mid m, e$

$(ii)\ a \mid c \ \ e \ \ b \mid \ c \ \ \Rightarrow \ \ m \mid c.$

Observação 3.4. Caso $a = 0$ ou $b = 0$, definimos o $[a, b] = 0$.

◿

Na definição 3.3, o item (i) diz que m é um múltiplo comum de a e b; enquanto (ii) afirma que todo múltiplo comum de a e b tem que necessariamente ser múltiplo de m, isso equivale a dizer que m é o menor inteiro positivo com a propriedade (i). Além disso, a condição (ii) implica na unicidade do mmc. De fato, se m e m' são dois mínimos múltiplos comuns de a e b, então, do item (ii) da definição 3.3, temos que $m \mid m'$ e $m' \mid m$, logo $m = m'$ uma vez que ambos são não negativos.

No cálculo do mmc de dois números, podemos supô-los não negativos. Basta observar que dados dois inteiros a e b, temos sempre que $[a, b] = [a, -b] = [a, -b] = [-a, -b]$. Sendo assim, para efeitos de mmc, consideraremos daqui por diante os múltiplos positivos dos números envolvidos.

O teorema a seguir estabelece uma relação entre o mdc e o mmc de dois números inteiros.

Teorema 3.4. *Dados dois inteiros a e b, temos que*

$$[a,b]\cdot(a,b)=|ab|.$$

Demonstração: Se $a=0$ ou $b=0$, pela observação 3.1 e 3.4, a igualdade acima é trivialmente satisfeita. Como já sabemos que $[a,b]=[a,-b]=[a,-b]=[-a,-b]$, sem perda de generalidade, podemos supor $a,b\in\mathbb{N}$. Ponhamos $m=\frac{ab}{(a,b)}$. Como

$$m=a\frac{b}{(a,b)}=b\frac{a}{(a,b)},$$

temos que $a\mid m$ e $b\mid m$. Portanto, m é um múltiplo comum de a e b. Seja c um múltiplo comum de a e b; logo $c=na$ e $c=n'b$. Segue daí que

$$n\frac{a}{(a,b)}=n'\frac{b}{(a,b)}.$$

Como, pela proposição 3.1 (ii), $\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1$, temos, pelo lema de Gauss, que $\frac{a}{(a,b)}$ divide n'. Portanto, $m=\frac{a}{(a,b)}b$ divide $n'b$ que é igual a c. Assim, $m=\frac{a}{(a,b)}b=[a,b]$, ou seja, $[a,b]\cdot(a,b)=ab$.

■

Em virtude do teorema acima, o mmc de dois inteiros ambos não nulos pode ser encontrado por meio do algoritmo de Euclides para o cálculo do mdc, pois basta dividir o módulo do produto dos dois números pelo seu mdc.

A situação-problema do exemplo a seguir figura o uso do teorema 3.4.

Exemplo 3.10. *Dois pilotos de kart disputam uma corrida em uma pista circular. Para dá uma volta completa um deles demora 18 minutos e o outro demora 15 minutos. Eles partem juntos e combinam interromper o passeio quando os dois se encontrarem pela primeira vez no ponto de partida. Quantas voltas deu cada um?*

Solução: Sejam n_1,n_2, respectivamente, o número de voltas que dá cada um dos pilotos. Notemos que o tempo total da corrida é o menor valor positivo que satisfaz as igualdades

$$T=18n_1=15n_2,$$

ou seja $T=[18{,}15]$. Daí, pelo teorema 3.4, temos que

$$T=[18{,}15]=\frac{18\cdot 15}{(18{,}15)}=\frac{270}{3}=90,$$

Logo $n_1 = \frac{90}{18} = 5$ e $n_2 = \frac{90}{15} = 6$.

■

Finalizamos está seção com uma bela interpretação geométrica do mínimo múltiplo comum.

Exemplo 3.11 [7]**.** *Um retângulo de lados inteiros $AB = m$ e $CD = n$, é dividido em quadrados de lado* 1*. Em cada um dos vértices ele possui um pequeno orifício. Uma raio de luz entra no retângulo por um dos vértices, na direção da bissetriz do ângulo reto, e é refletido sucessivamente nos lados do retãngulo. Quantos quadrados são atravessados pelo raio de luz?*

Solução: Se fizermos alguns testes preliminares dando valores a m e n, veremos que em cada caso a resposta coincidirá com $[m, n]$. Provemos que isto de fato vale para quaisquer m e n quaisquer. Para realizar a prova nos auxiliaremos da Figura 3.1.

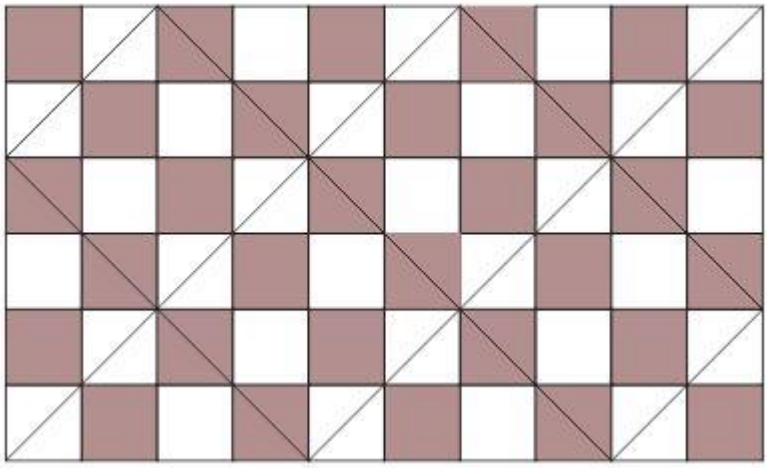

Figura 3.1

Primeiramente, notemos que cada vez que o raio de luz atravessa um quadrado ele avança uma unidade tanto na direção horizontal como na vertical. Usando este fato fazemos as observações a seguir.

- Se o raio entra pelo vértice A, terá que atravessar m quadrados até chegar ao lado BC, imediatamente mais m quadrados para chegar ao lado AD, depos mais m quadrados para chegar novamente ao lado BC, e assim sucessivamente. Além disso, depois do raio percorrer pm quadrados, com $p \in \mathbb{N}$, estará batendo no lado BC ou no lado AD.

- Analogamente o raio baterá no lado AB ou no lado DC se, e somente se, atravessar qn quadrados, com $q \in \mathbb{N}$.

- Somente nos vérticer B, C e D do retângulo pode acontecer que o raio incidente saia do retângulo, terminando assim o processo de reflexão.

Usando as observações acima é fácil ver que o raio chegará a um vértice quando chegar simultaneamente a dois lados perpendiculares do retângulo. Portanto, deve ter atravessado um número x de quadrados tal que $x = pm = qn$, ou seja, x deverá ser um múltiplo comum de m e n. É claro que a primeitra vez que o raio chega a um vértice o número x é o menor múltiplo comum de m e n, isto é, $x = [m, n]$. Note, por fim, que nenhum dos quadrados é atravessado duas vezes no percurso do raio de A até bater no primeiro vértice, pois como vemos na figura numa das direções os quadrados atravessados serão cinzas e na outra direção, serão todos brancos.

■

3.4 EQUAÇÕES DIOFANTINAS

No século III d.C., o matemática Diofanto, considerado um dos *pais* da álgebra e da teoria dos números, em seu livro *Aritmética*, procurou pela primeira vez estudar sistematicamente as soluções inteiras de certos tipos de equações polinomiais, as quais passaram merecidamente a ser conhecidas como *diofantinas.*

As *equa*ções *diofantinas* são equações em números inteiros com mais de uma variável. A análise dessas equações, de modo geral, é uma tarefa das mais difíceis, que exige argumentos bastante sofisticados [13]. Vejamos dois exemplo simples, todavia, não triviais.

Exemplo 3.12. *Prove que não existem* $x, y \in \mathbb{N}$ *tais que* $x^3 + 3 = 4y(y + 1)$.

Solução: Procedemos por contradição, isto é, suponhamos que existam $x, y \in \mathbb{N}$ tais que $x^3 + 3 = 4y(y + 1)$. Então

$$x^3 + 4 = 4y(y + 1) + 1 = (2y + 1)^2,$$

e, daí,

$$x^3 = (2y + 1)^2 - 2^2 = (2y - 1)(2y + 3).$$

Denote por $d = (2y - 1, 2y + 3)$. Observe que d é ímpar e $d \mid (2y + 3) - (2y - 1) = 4$, logo temos que $d = 1$. Portanto, o produto dos inteiros primos entre si $2y - 1$ e $2y + 3$ é um

cubo perfeito o que implica $2y-1$ e $2y+3$ serem ambos cubos perfeitos (justifique). Mas como não há dois cubos perfeitos cuja a diferença seja igual a 4 (problema 3.13). Chegamos a uma contradição.

■

Exemplo 3.13 [14]**.** *Dados três inteiros tais que $x^2+y^2=z^2$, mostre que x,y não são ambos ímpares e que xy é um múltiplo de 6.*

Solução: Suponha por absurdo que x,y são ambos ímpares, ou seja, da forma $2m+1$ e $2n+1$, respectivamente. Logo,

$$x^2+y^2=(2m+1)^2+(2n+1)^2=4\underbrace{(m^2+n^2+m+n)}_{k}+2=4k+2=z^2.$$

Mas, pelo problema 3.9 (c), o quadrado de um inteiro é da forma $4k$ *ou* $4k+1$ e nunca $4k+2$. Logo, $z^2=4k+2$ é impossível. Segue que um dos números x ou y é par. Daí xy é divisível por 2. Resta provar que que xy é divisível por 3. Novamente por redução ao absurdo, suponhamos que nem x nem y seja divisíveis por 3, ou seja, são da forma $x=3m\pm1$ e $y=3n\pm1$ (vide observação 3.5). Segue que:

$$x^2+y^2=(3m\pm1)^2+(3n\pm1)^2=3\underbrace{(3m^2+3n^2\pm2m\pm2n)}_{k}+2=3k+2.$$

Todavia, pelo problema 3.9 (d), o quadrado de um número inteiro nunca pode ser da forma $3k+2$, ou seja, $z^2=3k+2$ é impossível. Isso mostra que um dos números x ou y é divisível por 3. Consequentemente, pelo problema 3.5 (a) e (b), xy é divisível por $2\cdot3=6$.

■

Observação 3.5. Sabemos que a divisão euclidiana nos diz que todo inteiro n é da forma $3k+r$, onde $0\leq r<3$. No problema do exemplo 3.13 este fato foi usado com uma ligeira modificação. Observe que

$$3m+2=3m+3-3+2=3\underbrace{(m+1)}_{k}-1=3k-1,$$

logo afirmamos que todo número n é da forma $3k$, $3k+1$ ou $3k+2$, ou de forma simplificada, é da forma $3k$ ou $3k\pm1$.

◿

Obeservação 3.6. Três números inteiros x,y e z que satisfazem a equação diofantina $x^2+y^2=z^2$ constituem um *terno pitagórico*. Esta equação possui infinitas soluções e existem fórmulas que permitem gerar todas as soluções. Um tratamento sobre esse tipo de equação é feito em [1], página 109; ou com enfoque olímpico, em [13], página 59.

◿

Passamos agora a estudar as *equações diofantinas lineares de duas variáveis*, ou seja, equações do tipo $ax + by = c$, onde x, y são incógnitas inteiras e a, b e c são parâmetros inteiros dados. A teoria desenvolvida até agora para o estudo do mdc de dois inteiros permite resolver completamente este tipo de equação, conforme o seguinte

Teorema 3.5. *Sejam a, b e c inteiros não nulos dados. A equação $ax + by = c$ admite soluções $x, y \in \mathbb{Z}$ se, e somente se $(a, b) \mid c$. Nesse caso, se $d = (a, b)$ e $x = x_0$, $y = y_0$ for uma solução inteira qualquer, então as fórmulas*

$$x = x_0 + \frac{b}{d}t, \;\; y = y_0 - \frac{a}{d}t,$$

$t \in \mathbb{Z}$, dão todas as soluções inteiras possíveis.

Demonstração: Se $d \nmid c$, então a equação $ax + by = c$, não possui solução pois, como $d \mid a$ e $d \mid b$, d deveria dividir c, o qual é combinação linear de a e b. Suponhamos, pois, que $d \mid c$. Ora, pelo teorema de Bachet-Bézout, existem inteiros n_0 e m_0, tais que

$$an_0 + bm_0 = d \tag{3.4}$$

Como $d \mid c$, existe um inteiro t tal que $c = td$. Se multiplicarmos ambos os membros de (4.4) por t, teremos $a(n_0 t) + b(m_0 t) = td = c$. Denotando $x_0 = n_0 t$ e $y_0 = m_0 t$, temos que o par x_0, y_0 é uma solução da equação da equação $ax + by = c$.

Os pares da forma

$$x = x_0 + \frac{b}{d}t, \;\; y = y_0 - \frac{a}{d}t \tag{3.5}$$

são também soluções, uma vez que

$$\begin{aligned} ax + by &= a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) \\ &= ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t \\ &= ax_0 + by_0 \\ &= c. \end{aligned}$$

O acabamos de mostrar é que, conhecida uma solução particular (x_0, y_0) podemos, a partir dela, gerar infinitas soluções. Precisamos, agora, mostrar que todas as soluções da equação $ax + by = c$ é da forma (3.5). Com efeito, vamos supor que o par (x, y) seja uma solução, ou seja, $ax + by = c$. Mas $ax_0 + by_0 = c$, logo, obtemos,

$$ax + by - ax_0 - by_0 = a(x - x_0) + b(y - y_0) = 0,$$

o que implica $a(x - x_0) = b(y_0 - y)$. Portanto,

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y) \tag{3.6}$$

Uma vez que $d = (a, b)$ temos, pela proposição 2.1 (ii), que

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1,$$

logo, pelo lema de Gauss, $(b/d) \mid (x - x_0)$ e portanto existe um inteiro t tal que

$$x - x_0 = \frac{b}{d}t \quad \Leftrightarrow \quad x = x_0 + \frac{b}{d}t.$$

Substituindo este valor de x na equação (3.6), temos

$$\frac{a}{d}\left(x_0 + \frac{b}{d}t - x_0\right) = \frac{b}{d}(y_0 - y) \quad \Leftrightarrow \quad \frac{a}{d}t = y_0 - y \quad \Leftrightarrow \quad y = y_0 - \frac{a}{d}t,$$

o que conclui a demonstração. ■

Interpretando todos os pontos do plano como os pares ordenados (x, y), sabemos que a "curva" $C: ax + by = c$ representa geometricamente uma reta. Logo, as soluções de uma equação diofatina linear de duas variáveis são os pontos de coordenadas inteiras do plano cartesiano, que estão dispostos sobre a reta C. Por exemplo, os pontos $(-1, -2)$ e $(1,1)$ são soluções da equação diofantina $3x - 2y = 1$, veja a figura 3.2.

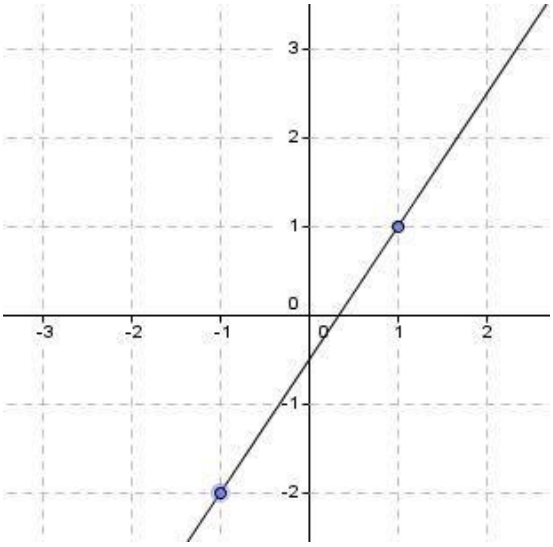

Figura 3.2

O exemplo a seguir mostra como devemos proceder para resolver equações diofantinas lineares de duas variáveis.

Exemplo 3.14. *Encontre todas as soluções inteiras da equação*

$$12x + 33y = 27.$$

Solução: Observemos que $(12,33) = 3$ e que $3 \mid 27$, logo a equação tem infinitas soluções. Como sabemos basta encontrar uma delas e teremos as restantes. Para achar esta solução temos duas maneiras, que descrevemos a seguir:

1) Reduzimos a equação à forma equivalente

$$4x + 11y = 9,$$

E por tentativa e erro vemos que $x_0 = 5$ e $y_0 = -1$ solucionam a mesma. Então pelo teorema 3.5 temos que

$$x = 5 + 11t \quad \text{e} \quad y = -1 - 4t, \quad t \in \mathbb{Z},$$

denotam todas as soluções que procuramos.

2) Aplicando o algoritmo estendido de Euclides para achar o $(12,33)$, obtemos o diagrama

	2	1	3
33	12	9	$3 = (12,33)$
9	3	0	

donde

$$3 = 12 - 1 \cdot 9$$
$$9 = 33 - 2 \cdot 12.$$

Usando estas duas igualdades, temos

$$3 = 12 - 1 \cdot 9 = 12 - 1 \cdot (33 - 2 \cdot 12) = 3 \cdot 12 + (-1) \cdot 33,$$

Multiplicando por 9 ambos os membros da igualdade $3 = 3 \cdot 12 + (-1) \cdot 33$, temos que

$$27 \cdot 12 + (-9) \cdot 33 = 27,$$

ou seja, achamos $x_0 = 27$ e $y_0 = -9$, garantidos pelo teorema de Bachet-Bézout, que validam $12x_0 + 33y_0 = 27$. Analogamente, como na alternativa anterior, podemos escrever a solução geral de forma $x = 27 + 11k \quad e \quad y = -9 - 4k, \quad s \in \mathbb{Z}$.

■

Um dos textos mais antigos, contendo problemas que envolvem equações diofantinas, foi encontrado na Europa e chegou até nossos dias: é um manuscrito provavelmente do século X. Acredita-se que ele seja uma cópia de uma coleção de quebra-cabeças preparada por Alcuin de York (735 – 804) para o rei Carlos Magno (742 – 814). O problema que nos interessa é o seguinte

Exemplo 3.15 [9]**.** *Quando 100 alqueires (medida antiga para cereais) de grãos são distribuidos entre 100 pessoas, de modo que cada homem receba 3 alqueires, cada mulher 2 alqueires e cada criança* $1/2$ *alqueire, qual é o número de homens, mulheres e crianças que participaram da distribuição?*

Solução: Para formular matematicamente esse problema, sejam x, y e z, respectivamente, o número de homens, mulheres e crianças participantes da distribuição. Então as condições dadas podem ser escritas através do sistema

$$\begin{cases} x + y + z = 100 \\ 3x + 2y + \frac{1}{2}z = 100 \end{cases}$$

onde $x, y, z \in \mathbb{N}$. Subtraindo a primeira equação de duas vezes a segunda, o sistema acima é equivalente ao sistema

$$\begin{cases} x + y + z = 100 \\ 5x + 3y = 100 \end{cases}$$

onde $x, y, z \in \mathbb{N}$. A equação $5x + 3y = 100$ possui solução particular $(-100,200)$, logo pelo teorema 3.5, sua solução geral é

$$x = -100 + 3t$$
$$y = 200 - 5t,$$

uma vez que o mdc de 5 e 3 é igual a 1. Logo, exigir que $x > 0$ e $y > 0$ é o mesmo que resolver o par de desigualdades

$$-100 + 3t > 0 \quad e \quad 200 - 5t > 0,$$

cuja solução é

$$t > 33 \quad e \quad t < 40.$$

Por outro lado,

$$z = 100 - (x + y) = 100 - (-100 + 3t + 200 - 5t) = 2t$$

e, então, temos as seguintes possibilidades:

$$t = 34 \quad \Rightarrow \quad x = 2, \quad y = 30 \quad e \quad z = 68$$
$$t = 35 \quad \Rightarrow \quad x = 5, \quad y = 25 \quad e \quad z = 70$$
$$t = 36 \quad \Rightarrow \quad x = 8, \quad y = 20 \quad e \quad z = 72$$
$$t = 37 \quad \Rightarrow \quad x = 11, \quad y = 15 \quad e \quad z = 74$$

$$t = 38 \quad \Rightarrow \quad x = 14, \;\; y = 10 \;\; e \;\; z = 76$$
$$t = 39 \quad \Rightarrow \quad x = 17, \;\; y = 5 \;\; e \quad z = 78$$ ■

Exemplo 3.16 [8]**.** *Sejam a,b inteiros positivos com* $(a, b) = 1$. *Mostre que para todo* $c \in \mathbb{Z}$ *com* $c > ab - a - b$, *a equação* $ax + by = c$ *admite soluções inteiras com* $x, y \geq 0$.

Solução: Seja x_0, y_0 uma solução inteira (que existe pelo torema de Bachet-Bézout). Devemos mostrar a existência de um inteiro k tal que

$$x = x_0 - bk > -1 \quad \text{e} \quad y = y_0 + ak > -1$$

ou seja,

$$-\frac{y_0 + 1}{a} < k < \frac{x_0 + 1}{b}.$$

Mas isso isto segue do fato de o intervalo aberto $\left(-\frac{y_0+1}{a}, \frac{x_0+1}{b}\right)$ ter o tamanho maior do que 1:

$$\frac{x_0 + 1}{b} - \left(-\frac{y_0 + 1}{a}\right) = \frac{ax_0 + by_0 + a + b}{ab} = \frac{c + a + b}{ab} > \frac{ab}{ab} = 1.$$

■

PROBLEMAS PROPOSTOS

3.1 Encontre o máximo divisor comum dos pares de números abaixo.

(a) 637 e 3887;

(b) 648 e 1218;

(c) 511 e 874;

(d) 7325 e 8485.

3.2. Para cada par de números, dados na questão anterior, determine os inteiros m e n tais que $(a, b) = ma + nb$.

3.3 Seja $n, m \in \mathbb{N}$ e $a \in \mathbb{Z} \setminus \{-1\}$. Mostre que

(a) $(n, 2n + 1) = 1$;

(b) $(2n + 9, 9n + 4) = 1$;

(c) $(n + 1, n^2 + n + 1) = 1$;

(c) $\left(\frac{a^{2n}-1}{a+1}, a + 1\right) = (a + 1, 2m)$.

3.4 Prove que a fração $\frac{2n+8}{4n+15}$ é irredutível para todo número natural.

3.5 Mostre que

(a) Se $ab \mid n$, então $a \mid n$ e $b \mid n$.

(b) Se a e b são primos entre si e $a \mid n$ e $b \mid n$, então $ab \mid n$.

3.6 Um prédio possui duas escadarias, uma delas com 780 degraus e a outra com 700 degraus. Sabendo que os degraus das duas escadas só estão no mesmo nível quando conduzem a um andar, descubra quantos andares tem o prédio.

3.7 Prove que:

(a) Se $(a, b) = 1$, então $(a^n, b^m) = 1$, para todo $n, m \in \mathbb{N} \cup \{0\}$.

(b) Para todo $a, b \in \mathbb{Z}$ e todo $n \in \mathbb{N}$, temos que $(a, b)^n = (a^n, b^n)$.

3.8. Ache o $(\underbrace{111 \ldots 111}_{100\ vezes}, \underbrace{111 \ldots 111}_{60\ vezes})$.

3.9 Encontre todas as soluções inteiras de:

(a) $15x + 16y = 17$;

(b) $15x - 51y = 41$.

3.10 Encontre todas as soluções positivas de:

$$\begin{cases} x + y + z = 31 \\ x + 2y + 3z = 41 \end{cases}$$

3.11 Divida 100 em duas parcelas inteiras e positivas, de modo que uma seja dividida por 7 e outra por 11.

3.12 Encontre todos os valores inteiros positivos de x e y que sejam soluções da equação indeterminada $7x + 19y = 1921$ de modo que a soma $x + y$ seja a menor possível.

3.13 De quantos maneiras pode-se comprar selos de R$3,00 e de R$5,00 de modo que se gaste R$100,00?

3.14 Determine o menor inteiro positivo que tem resto 11 e 35 quando dividido, respectivamente, 37 e 48.

O ÚLTIMO TEOREMA DE FERMAT

Nesta nota histórica, encontra-se a abordagem com base em [9].

A equação diofantina mais conhecida é a equação $x^n + y^n = z^n$ em que estamos procurando números inteiros que a satisfaçam. Por exemplo, se $n = 2$, os inteiros 3,4 e 5 representa um terno de soluções, bem como os inteiros 6,8 e 10. Na verdade, não é difícil ver que existe um número infinito de soluções para $n = 2$.

Sempre podemoes encontrar soluções triviais patra a equação anterior. Por exemplo, se n for par, $x = 0$ e $y = \pm z$. A pergunta se é possível encontrar soluções não triviais para a equação diofantina $x^n + y^n = z^n$, para $n \geq 3$, possui uma das histórias mais fascinantes da Matemática. Fermat deixou anotado, à margem de seu exemplar do *Aritmética*, de Diofanto, que a equação $x^n + y^n = z^n$ não possui soluções não triviais para $n \geq 3$. Tal afirmação ficou conhecida como o Último Teorema de Fermat.

Em vão, durante séculos, muito dos melhores matemáticos trabalharam, procurando, no início, a demonstração que Fermat afirmara haver descoberto e, posteriormente, desenvolvendo métodos novos para chegar ao resultado, já que as tentativas infrutíferas de encontrar uma solução elementar para o problema fazia crer que a desmonstração de Fermat estava incorreta.

No século XIII, ficou claro que o problema estava relacionado com a existência da fatoração única em vários domínios, de maneira semelhante ao Teorema Fundamental da Aritmética (nosso Teorema 4.1).

No final do século XX é que os avanços substanciais foram obtidos no problema, levando à solução no final dos anos 90, em circustâncias emocionantes. Em 1983, o matemático alemão G. Faltings (1954 –) provou que o número de soluções para $n = 3$ era finito. Restando provar que esse número finito era zero. Em 1986, no Congresso Internacional

de Matemática em Berkeley, Estados Unidos, Faltings recebeu a medalha Filds[2], a maior horaria existente em Matemática, por seu trabalho sobre o Último Teorema de Fermat.

Em junho de 1993, o Prof. Adrew Wiles (1953 –), da Universidade de Pricenton, ao final de uma série de 3 palestras na Universidade de Cambridge, anunciou que havia provado o Último Teorema de Fermat. Wiles havia trabalhado 10 anos em segredo no problema e nada fazia antever que ao final da série esse seria o resultado demonstrado.

Assim sendo, grande foi o furor provocado entre os presentes quando, à medida que a série de palestras ia chegando ao final, Wiles ia se aproximando da prova da chamada Conjectura de Tanayama-Weil, que todos ali presentes sabiam ser equivalente ao Último Teorema de Fermat. Chegado o grande dia, o auditório em Cambridge foi insuficiente para todos os matemáticos, de posse de suas máquinas fotográficas, interessados em testemunhar o grande dia.

A esse clímax seguiu-se o anticlímax. Quando Wiles submeteu à comunidade científica o correspondente trabalho escrito, para que fosse escrutinado pelos maiores especialistas da área e em seguida publicado, verificou-se que havia uma afirmativa no trabalho que não se sabia se era verdade. Todo o trabalho, portanto, dependia de se provar a veracidade daquela afirmação. Durantes meses, Wiles trabalhou de maneira incansável para conseguir uma demonstração do resultado, sem sucesso. Como muitas tentativas anteriores de se demonstrar o Último Teorema de Fermat haviam fracassado em circunstâncias semelhantes, muitos chegaram a pensar que esse seria o destino do trabalho de Wiles e que o Último Teorema permaneceria como uma fronteira intransponível da Matemática.

Wiles, então, propôs a Richard Taylor (1962 –), um jovem matemático inglês, que o ajudasse na demonstração do resultado. Trabalhando juntos, eles conseguiram, não a demonstração daquela afirmação duvidosa, mas sim evitá-la. Finalmente, em maio de 1995, a publicação especializada *Annals of mathematics* publica o artigo original de Wiles com a prova incompleta e a correção por Wiles e Taylor. Estava assim concluída a história do Último Teorema de Fermat.

[2] Até recentemente, a Medalha Fields era a maior distinção dada a um indivíduo por sua contribuição à Matemática. Entretanto, em 2003, foi outorgado, pela primeira vez, o Prêmio Abel para a Matemática, correspondente ao prémio Nobel para as outras áreas, e que foi conferido ao matemático francês Jean Pierre Serre, que também foi vencedor da Medalha Fields em 1954. Serre realizou importantes trabalhos em Teoria dos Números.

4 - NÚMEROS PRIMOS

Nosso propósito neste capítulo é o estudo das propriedades básicas dos números primos, um dos conceitos mais importantes de toda a Matemática. Entre essas propriedades, destaca-se o *Teorema Fundamental da Aritmética (TFA),* considerando a "pedra fundamental da Teoria Elementar dos Números". Entre suas consequências, expomos outra maneira de calcular o mmc e mdc de dois números inteiros. Discutimos sobre distribuição dos números primos, apresentando o *Crivo de Eratóstenes*, que nos introduz à difícil tarefa de procurar e identificar números primos. Discorremos sobre expressões decimais finitas e infinitas e, ao final, apresentamos mais duas aplicações interessantes da teoria.

4.1 TEOREMA FUNDAMENTAL DA ARITMÉTICA

Ao longo da história da Matemática, esclarece Oliveira em [7], os números primos foram os protagonistas de célebres problemas que motivaram o desenvolvimento de teorias e técnicas pelas mentes mais férteis, como Fermat e Gauss. Até hoje muitos problemas, simples de enunciar, que envolvem números primos são verdadeiros desafios intelectuais para toda a humanidade.

Logo, do ponto de vista matemático, os números primos são belos à medida que se tornam desafiadores. São também extremamente importantes para as atividades usuais de nosso dia a dia – nenhuma transação bancária pela internet estaria segura sem o uso de números primos muito grandes, exemplifica Oliveira [7].

Definição 4.1. *Um número natural* n $(n > 1)$ *possuindo somente dois divisores positivos,* n *e* 1*, é chamado primo. Se* $n > 1$ *não é primo dizemos que* n *é composto.*

Em outras palavras, a definição acima diz que um número natural n é primo se sempre que escrevemos $n = ab$, com $a, b \in \mathbb{N}$, temos necessariamente que **ou** $a = 1$ e $b = n$ **ou** $a = n$ e $b = 1$. Consequentemente, um número n é composto se existem $a, b \in \mathbb{N}$ com $1 < a < n$ e $1 < b < n$, tais $n = ab$. Observe que o número 1 não é primo nem composto.

Sejam p, q números primos, se $p \mid q$, então $p = q$. De fato, como $p \mid q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Sendo p primo, tem-se que $p > 1$, o que acarreta $p = q$. E ainda, se $p \nmid a$, para algum inteiro a, então $(p, a) = 1$. Com efeito, se $(p, a) = d$, temos que $d \mid p$ e $d \mid a$, portanto, $d = p$ ou $d = 1$. Mas $d \neq p$, pois $p \nmid a$ e, consequentemente, $d = 1$.

Exemplo 4.1. Os números $2, 3, 5, 7, 11$ e 13 são primos, enquanto $4, 6, 8, 10$ e 12 são compostos.

■

Exemplo 4.2. *O número* $n = 3^{20} - 25^6$ *é composto.*

Solução: escrevemos n de outra forma, com o objetivo de facilitar nosso trabalho. De fato, observemos que

$$n = (3^{10})^2 - (25^3)^2 = (3^{10} + 25^3)(3^{10} - 25^3),$$

portanto, n é composto.

■

Os números primos podem ser vistos como uma espécie de "atómos", multiplicativamente indivisíveis, a partir dos quais todos os números naturais são multiplicativamente construídos, ou seja, podemos decompô-lo até que os seus fatores sejam todos primos. Por exemplo,

$$180 = 2 \cdot 90 = 3 \cdot 30 \cdot 2 = 3 \cdot 3 \cdot 10 \cdot 2 = 3 \cdot 3 \cdot 5 \cdot 2 \cdot 2 = 2^2 \cdot 3^2 \cdot 5.$$

Observemos que, se um número foi expresso como um produto de primos, podemos dispor seus fatores primos em qualquer ordem. A experiência nos diz que, salvo pela arbitrariedade da ordenação, a decomposição de um número natural em fatores primos é única. Essa afirmação parece, à primeira vista, evidente. Todavia, ela não é uma trivialidade e sua demonstração, ainda que elementar, requer algumas sutilizas. A demonstração clássica desse resultado, conhecido como Teorema Fundamental da Aritmética, se baseia no algoritmo de Euclides. Ressaltamos que Euclides – em *Os Elementos*, Proposição 30, Livro VII – apenas demonstrou quanto à existência da fatoração de um número natural em primos. Acredita-se que Euclides conhecia a unicidade dessa fatoração e que, por dificuldade de notação, esclarece Fernandes [9], não conseguiu estabelecer a demonstração desse resultado (provaremos doravante no teorema 4.1.) Salientamos, entretanto, que a demonstração que apresentaremos no tocante à existência, será feita utilizando a forma "forte" do PIF. Vale

lembrar que Euclides não dispunha do PIF, ferramenta que passou a ser utilizada muito tempo depois.

Teorema 4.1 (Teorema Fundamental da Aritmética – TFA). Todo número inteiro maior do que 1 pode ser escrito de maneira única (a menos da ordem) como um produto de fatores primos.

Demonstração: Dividiremos a demonstração em duas partes. A primeira mostrará a existência dessa fatoração em números primos, a segunda mostrará a unicidade dessa fatoração, a menos da ordem.

(**existência)** Vamos usar a forma "forte" do PIF na demonstração. Definimos a proposição

$p(n)$: n é um número primo ou pode ser escrito como o produto de números primos.

Evidente que para $n = 2$ e $n = 3$ (base da indução), $p(n)$ é verdadeira (duas bases para indução, qualquer dúvida consulte a observação 1.4). Suponhamos agora que para todo k, $p(k)$ seja verdadeira, onde $1 < k \leq n$ (hipótese indutiva) e provaremos que $p(n+1)$ é verdadeira.

Por um lado, se $n+1$ é primo, então $p(n)$ é verdadeira. Por outro lado, se $n+1$ não for primo, ou seja, $n+1$ é composto; então $n+1 = ab$, em que $1 < a \leq n$ e $1 < b \leq n$. Portanto, a hipótese indutiva garante que: **ou** a e b podem ser escritos como produto de primos, **ou** são números primos. Logo, $p(n+1)$ é verdadeira, uma vez que $n+1 = ab$ é também um produto de primos, a saber, o produto dos números primos da fatoração de a, multiplicados pelos números primos da fatoração de b. Isso completa a demonstração da existência.

(unicidade) A demonstração é por absurdo. Considere o conjunto

$$S = \{n \in \mathbb{N}; n > 1 \; e \; n \; tem \; duas \; decomposições \; em \; fatores \; primos \; \}$$

e suponha, por absurdo, que $S \neq \emptyset$. Logo, pelo Princípio da Boa Ordem, S tem um menor elemento m. Assim,

$$m = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s \tag{4.1}$$

são duas fatorações distintas de m como o produto de números primos. Reordenando esses primos, se necessário, sem perda nenhuma de generalidade, podemos supor que

$$p_1 \leq p_2 \leq \cdots \leq p_r \quad \text{e} \quad q_1 \leq q_2 \leq \cdots \leq q_s.$$

Notemos que $p_1 \neq q_1$, pois, caso contrário, teríamos duas decomposições diferentes para um número natural menor do que m (a saber, m/p_1), contrariando assim o fato de m ser o elemento mínimo de S. Vamos supor que $p_1 < q_1$. Definimos então

$$m' = m - (p_1 q_2 \dots q_s).$$

Substituindo m pelas expressões dadas nas igualdades em (4.1), obtemos

$$m' = p_1 p_2 \dots p_r - p_1 q_2 \dots q_s = p_1(p_2 \dots p_r - q_2 \dots q_s) \quad (4.2)$$

$$m' = q_1 q_2 \dots q_s - p_1 q_2 \dots q_s = (q_1 - p_1)(q_2 q_3 \dots q_s) \quad (4.3)$$

Pela definição, $m' < m$. Em (4.2), se fosse $p_2 \dots p_r - q_2 \dots q_s = 0$, concluiríamos que $p_1 = q_1$. Caso contrário, $m' > 2$, pois $p_1 \mid m'$. Assim, $m' \notin S$, ou seja, m' tem decomposição única como produto de fatores primos. Agora, olhando para (4.3), como $p_1 < q_2 \leq \cdots \leq q_s$, necessariamente o fator primo p_1 tem que está presente na decomposição de $q_1 - p_1$, ou seja, $q_1 - p_1 = cp_1$. Ora, daí $q_1 = p_1(c + 1)$, mas isso é absurdo uma vez que q_1 é primo. Temos, assim, que $S = \emptyset$, o que completa a demonstração.

■

Observação 4.1. O TFA foi enunciado precisamente por Gauss. Seus antecessores, a exemplo de Fermat, utilizavam este teorema sem a preocupação de tê-lo enunciado ou demonstrado com precisão. ◿

Uma consequência imediata do TFA é que todo número inteiro não-nulo diferente de ± 1 pode ser escrito como ± 1 vezes o produto de números primos. Essa expressão é única, exceto pela ordem na qual os fatores primos aparecem. Um número negativo q cujo simétrico $-$q é um natural primo é chamado *número primo negativo*. Por exemplo, $2, 3$ e 5 são números primos, enquanto que $-2, -3$ e -5 são números primos negativos.

Motivamos o próximo exemplo, que figura outra consequência do TFA, com a seguinte história [15]: na Grécia Antiga, em Crotona, sul da Itália, havia uma seita filosófico-religiosa, liderada por Pitágoras. Um dos pontos fundamentais de sua doutrina era o lema "os números governam o mundo" (os números para eles eram os números naturais, admitindo-se tomar razões entre esses números, formando as frações, o que hoje chamamos de números racionais). Uma enorme crise, que abalou os alicerces do pitagorismo e, por algum tempo, toda a estrutura da Matemática grega, surgiu quando, entre os próprios discípulos de Pitágoras, alguém observou que o lado e a diagonal de um quadrado são segmentos incomensuráveis. Em outras palavras, a medida dessa diagonal representa sempre um número *irracional*.

Recordemos que um número *irracional* n é aquele que não pode ser escrito como um quociente p/q, onde $p, q \in \mathbb{Z}$, com $q \neq 0$. Pra fixar ideias, considere um quadrado de lado 1 e denote por d sua diagonal, logo pelo Teorema de Pitágoras temos que $d^2 = 2$. O exemplo a seguir prova justamente que $\sqrt{2}$ é um número irracional.

Exemplo 4.3. *Não existe nenhum número inteiro d tal que $d^2 = 2$.*

Solução: Por absurdo, sejam $p, q \in \mathbb{N}$ tal que $\left(\frac{p}{q}\right)^2 = 2$, ou seja, $p^2 = 2q^2$. O fator 2 aparece um número par de vezes na decomposição de p^2 e de q^2 em fatores primos. Daí, por um lado p^2 contém um número par de fatores iguais a 2 e, por outro, $2q^2$ contém um número ímpar desses fatores. Ora, isso viola a unicidade da decomposição em fatores primos. Assim sendo, não se pode ter $p^2 = 2q^2$. Segue o resultado.

■

Exemplo 4.4. *Determine todos os números primos p tais que $3p + 1$ seja um quadrado perfeito.*

Solução: Suponha $3p + 1$ um quadrado perfeito. Ora, existe um $n \in \mathbb{N}$ tal que $3p + 1 = n^2$. Logo,

$$3p = (n + 1)(n - 1) \tag{4.4}$$

Daí, note que não podemos ter $n + 1 = 1$, nem $n - 1 = 1$. Isso implica que devemos ter $n + 1 \geq 2$ e $n - 1 \geq 2$. Já que temos dois números primos do lado esquerdo da igualdade (4.4), o TFA garante que $n + 1$ e $n - 1$ são ambos primos. Só existem, então, duas possibilidades:

$$n + 1 = 3 \quad \text{e} \quad n - 1 = p, \quad \text{ou} \quad n + 1 = p \quad \text{e} \quad n - 1 = 3.$$

A única solução é, portanto, $p = 5$.

■

O corolário a seguir denota uma propriedade que caracteriza totalmente os números primos. Outra demonstração do TFA pode ser feita a partir dessa propriedade, no que diz respeito à unicidade da decomposição. A propósito, demonstrações que seguem essencialmente esse caminho podem ser encontradas em [5] e [6].

Corolário 4.1. *Sejam $a, b \in \mathbb{Z}$ e p um número primo. Se p for um fator de ab, então p é um fator de a ou p é um fator de b.*

Demonstração: Como $m \mid n$ se, e somente se, $m \mid (-n)$, é suficiente, então, mostrar esse resultado para a e b naturais. Por absurdo, se p não fosse um fator de a nem de b, então as

fatorações de a e b em produto de primos levaria a uma fatoração de ab não contendo p. Por outro lado como, por hipótese, p é um fator de ab, existiria um $q \in \mathbb{N}$ tal que $pq = ab$. Logo, o produto de p por uma fatoração de q daria uma fatoração de ab em primos contendo p, o que contraria a unicidade da decomposição de ab em primos.

■

Segue do corolário 4.1 que *se* $a_1, a_2, \dots, a_r$ *são números inteiros,* p *é primo e, se* $p \mid a_1 a_2 \dots a_r$*, então* $p \mid a_i$ *para algum* $i \in \{1, 2, \dots, r\}$. Para provar isso, use indução sobre r. Em particular, *se* $p, p_1, p_2, \dots, p_r$ *são números primos e, se* $p \mid p_1 p_2 \dots p_r$*, então* $p = p_i$ *para algum* $i \in \{1, 2, \dots, r\}$.

Observação 4.2. Considere os produtos:

(i) $1 \cdot 2 \cdot 3 \cdot \dots \cdot n$;

(ii) $x^1 \cdot x^2 \cdot x^3 \cdot \dots \cdot x^n$;

(iii) $1 \cdot 3 \cdot 5 \cdot \dots \cdot (2n-1)$.

Podemos simplificar estes produtos usando uma notação apropriada. Usaremos o símbolo Π, que é a letra maiúscula "Pi" do alfabeto grego. Esta letra corresponde ao nosso "P" e, naturalmente, nos faz lembrar a palavra produto. Logo os produtos anteriores são simplificados para:

(i) $\prod_{i=1}^{n} i$ (lê-se: produto de i, para i variando de 1 a n);

(ii) $\prod_{i=1}^{n} x^i$ (lê-se: produto da variável x elevada a i, para i variando de 1 a n);

(iii) $\prod_{i=1}^{n} (2i-1)$ (lê-se: produto de $(2i-1)$, para i variando de 1 a n);

De modo geral, dados os números naturais r e s, $r \leq s$, usamos $\prod_{i=r}^{s} a_i$ para representar o produto de $a_r \cdot a_{r+1} \cdot \dots \cdot a_s$, sendo i o índice do produtório e r e s os limites inferior e superior, respectivamente. Por exemplo, o produto dos cinco primeiros números naturais é $\prod_{i=1}^{5} i = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 5!$. Neste caso, diremos que este produto representa o *fatorial de 5*, simbolizado por 5!. De maneira geral, o produto dos n primeiros números naturais é dado por

$$\prod_{i=1}^{n} i = 1 \cdot 2 \cdot \dots \cdot n = n!.$$

Recordemos que dados os naturais n, k com $n \leq k$, temos que

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

onde tem-se $\binom{n}{k}$, lemos *binomial "$n-k$ a k"*. Não é difícil provar que o quociente acima é sempre um número natural, para mais detalhes consulte o capítulo 1 de [8].

◿

O exemplo a seguir é uma aplicação do corolário 4.1.

Exemplo 4.5. *Se p é um primo ímpar, então p divide cada um dos números*

$$\binom{p}{1}, \binom{p}{2}, \dots, \binom{p}{p-1}.$$

Solução: Seja $1 \leq k \leq p-1$. Como

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!} = \frac{(k+1)\cdot \dots \cdot (p-1)p}{(p-k)!}$$

é um número natural (observação 4.2), temos que $(p-k)!$ divide $(k+1)\cdot \dots \cdot (p-1)p$. Agora, como p é primo e $p \nmid 1, 2, \dots, p-k$, o corolário 4.1 garante que $p \nmid (p-k)!$, de sorte que $(p,(p-k)!) = 1$. Portanto, pelo lema de Gauss (teorema 3.2), concluímos que $(p-k)!$ divide $(k+1)\cdot \dots \cdot (p-1)$ e, daí

$$\binom{p}{k} = \underbrace{\frac{(k+1)\cdot \dots \cdot (p-1)}{(p-k)!}}_{\in \mathbb{N}} \cdot p,$$

um múltiplo de p. ■

Na fatoração de um inteiro $n \notin \{-1, 0, 1\}$, o mesmo primo p pode aparecer várias vezes. Agrupando esses primos, podemos escrever a decomposição de n como:

$$n = (\pm 1){p_1}^{a_1}{p_2}^{a_2} \cdot \dots \cdot {p_r}^{a_r} = (\pm 1)\prod_{i=1}^{r} {p_i}^{a_i} \qquad (4.5)$$

em que $0 < p_1 < p_2 < \dots < p_r$ e $a_i \in \mathbb{N}$ para $i \in \{1, 2, \dots, r\}$. Logo, ao nos referimos a uma decomposição (ou fatoração) de um número inteiro em números primos, estaremos nos referindo a essa decomposição em que os primos são todos positivos. Assim, por exemplo, aceitamos as decomposições

$$40 = 2^3 \cdot 5 \quad \text{e} \quad -12 = -(2^2 \cdot 3),$$

mas não aceitamos as decomposições

$$40 = (-2^3)\cdot(-5) \quad \text{e} \quad -12 = 2^2 \cdot (-3).$$

Hefez, em [1], afirma que quando estivermos lidando com a decomposição em fatores primos de dois, ou mais, números inteiros, é interessante utilizar o recurso de acrescentar

fatores da forma $p^0\ (=1)$, onde p é um número primo qualquer. Assim, empregando a notação (4.5), temos que dados $m, n \in \mathbb{N}\backslash\{1\}$ quaisquer, podemos escrever

$$m = (\pm 1) p_1{}^{a_1} p_2{}^{a_2} \dots p_r{}^{a_r} = (\pm 1) \prod_{i=1}^{r} p_i{}^{a_i}$$

$$\text{e} \quad n = (\pm 1)\, p_1{}^{b_1} p_2{}^{b_2} \dots p_r{}^{b_r} = (\pm 1) \prod_{i=1}^{r} p_i{}^{b_i}$$

usando o mesmo conjunto de primos $p_1, p_2, \dots, p_r$ desde que permitamos que os expoentes $a_1, a_2, \dots, a_r, b_1, b_2, \dots, b_r$ variem em $\mathbb{N} \cup \{0\}$ e não apenas em $\mathbb{N}$. Por exemplo, os números $2^3 \cdot 3^2 \cdot 7 \cdot 11$ e $2 \cdot 5^2 \cdot 13$ podem ser escritos, respectivamente, $2^3 \cdot 3^2 \cdot 5^0 \cdot 7 \cdot 11 \cdot 13^0$ e $2 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 11^0 \cdot 13$.

O resultado a seguir é colocado como corolário para dá destaque, embora elementar.

Corolário 4.2. *Seja $n = (\pm 1) \prod_{i=1}^{r} p_i{}^{a_i}$, onde $p_i's$ são os primos distintos, então o conjunto dos divisores positivos de n é o conjunto de todos os números da forma*

$$n = (\pm 1) \prod_{i=1}^{r} p_i{}^{c_i}, \quad 0 \le c_i \le a_i, \quad i \in \{1, 2, \dots, r\}.$$

Demonstração: Basta notar que se c_i não estiver no intervalo mencionado, o produto acima não será um divisor de n.

■

Observação 4.2. Santos, em [5], ressalta que se denotarmos a sequência de primos – que vamos considerar infinita (teorema 4.2) – em ordem crescente

$$p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \dots, p_n = \textit{enésimo primo},$$

então podemos representar, com um certo "abuso de notação", todo número inteiro da seguinte forma

$$n = (\pm 1) \prod_{i=1}^{\infty} p_i{}^{a_i}, \quad a_i \ge 0. \tag{4.6}$$

Por exemplo, o produto

$2^3 \cdot 3^2 \cdot 7^1 \cdot 11^1 = 2^3 \cdot 3^2 \cdot 5^0 \cdot 7^1 \cdot 11^1 \cdot 13^0 \cdot 17^0 \cdot 19^0 \cdot 23^0 \cdot 29^0 \cdot 31^0 \cdot \dots$.

Por outro lado, os divisores positivos de n são, agora, todos os números da forma

$$n = (\pm 1) \prod_{i=1}^{\infty} p_i{}^{c_i}, \quad 0 \le c_i \le 0. \tag{4.7}$$

Evidente que os produtos (4.6) e (4.7) são finitos, uma vez que o número de fatores primos de qualquer inteiro é sempre finito.

◿

Usando argumentos elementares de contagem, juntamente com o corolário 4.2, podemos calcular o *número de divisores positivos* $d(n)$ de um inteiro n. Esse é o conteúdo do próximo resultado. Para fixar ideias, vamos calcular, por exemplo, quantos são os divisores positivos do número $126\,000$. Com efeito, fatorando o número $n = 126\,000$, obtemos:

$$n = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7.$$

Considere alguns exemplos de divisores de n:

$$2^3 \cdot 5^3; \quad 2^2 \cdot 3 \cdot 7; \quad 2 \cdot 3^2 \cdot 5 \cdot 7; \quad 3; \quad 2^4 \; etc.$$

Podemos notar que nos divisores de n:

1. O expoente do fator 2 pode variar de 0 a 4: $(2^0; 2^1; 2^2; 2^3; 2^4)$.
2. O expoente do fator 3 pode variar de 0 a 2: $(3^0, 3^1, 3^2)$.
3. O expoente do fator 5 pode variar de 0 a 3: $(5^0, 5^1, 5^2, 5^3)$.
4. O expoente do fator 7 pode variar de 0 a 1: $(7^0, 7^1)$.

Logo, pelo corolário 4.2, podemos representar os divisores de n da forma

$$D = 2^x \cdot 3^y \cdot 5^z \cdot 7^w$$

de tal sorte que

1. x toma valores em $\{0, 1, 2, 3, 4\}$, resultando em 5 o número de possibilidades para o x.
2. y toma valores em $\{0, 1, 2\}$, resultando em 3 o número de possibilidades para o y.
3. z toma valores em $\{0, 1, 2, 3\}$, resultando em 3 o número de possibilidades para o z.
4. w toma valores em $\{0, 1\}$, resultando em 2 o número de possibilidades para o w.

Assim, pelo princípio fundamental da contagem, temos que

$$d(n) = 5 \cdot 3 \cdot 4 \cdot 2 = (4 + 1)(2 + 1)(3 + 1)(1 + 1) = 120$$

é o número de divisores de $126\,000$.

Corolário 4.3. *Dado* $n = (\pm 1) \prod_{i=1}^{r} {p_i}^{a_i}$, *onde os* ${p_i}'s$ *são primos distintos, o número de divisores positivos de n é*

$$d(n) = \prod_{i=1}^{r} (a_i + 1) = (a_1 + 1)(a_2 + 1) \dots (a_r + 1).$$

Demonstração: como $n = (\pm 1) \prod_{i=1}^{r} {p_i}^{a_i}$, temos

1. O expoente p_1 toma valores em $\{0, 1, 2, \dots, a_1\}$, resultando em $(a_1 + 1)$ o número de possibilidades de escolhas para ele.

2. O expoente p_2 toma valores em $\{0, 1, 2, \dots, a_2\}$, resultando em $(a_2 + 1)$ o número de possibilidades de escolhas para ele.

   ⋮

r. O expoente p_r toma valores em $\{0, 1, 2, \dots, a_r\}$, resultando em $(a_r + 1)$ o número de possibilidades de escolhas para ele.

Pelo princípio fundamental da contagem, segue o resultado.

■

Exemplo 4.6. *Mostre que um número natural n é um quadrado perfeito se e só se $d(n)$ for ímpar.*

Solução: Como $1 = 1^2$ e $d(1) = 1$ é ímpar, podemos supor que $n > 1$. Seja então $n > 1$ e $n = \prod_{i=1}^{r} {p_i}^{a_i}$ sua decomposição em fatores primos. Se n é um quadrado perfeito, então, para $1 \leq i \leq r$, existe $b_i \in \mathbb{N}$ tal que $a_i = 2b_i$. Daí, pelo corolário 4.3,

$$d(n) = \prod_{i=1}^{r}(a_i + 1) = \prod_{i=1}^{r}(2b_i + 1)$$

que é ímpar. A recíproca é análoga.

■

Apresentamos a seguir um problema recreativo que está relacionado com a propriedade provada no exemplo anterior. Acreditamos que o professor pode apresentá-lo em sala de aula transpondo didaticamente, através de uma atividade, as ideias nele inseridas.

Exemplo 4.7. *No vestuário de uma escola com* 100 *alunos, numerados de* 1 *a* 100*, há* 100 *armários enfileirados em um corredor, também numerados de* 1 *a* 100*. Um dia, os alunos resolveram fazer a seguinte brincadeira: o primeiro aluno abre todos os armários. Em seguida, o aluno de número 2 fecha todos os armários de número par. O aluno de número 3 inverte as posições das portas dos armários de número múltiplo de 3. O aluno de número 4 inverte a posição das portas dos armários de número múltiplo de 4, e assim sucessivamente. Ao final, quais armários ficaram abertos?*

Solução: Para responder à pergunta, note que um armário de número k é mexido pelos alunos cujos números são divisores de k. Ora, como $1 \leq k \leq 100$, temos que quando o *enésimo* aluno terminar sua tarefa, teremos passado por todos os divisores de k. Logo, uma porta ficará aberta ou fechada, a depender do número de divisores de k ser par ou ímpar. Daí, uma porta k ficará ao final aberta se, e somente se, k for um quadrado perfeito. Assim, ao final da brincadeira ficaram abertos os armários de números $4, 9, 16, 25, 36, 49, 64, 81$ e 100. ■

4.2 CÁLCULO DO MDC E MMC USANDO O TFA

Toda a estrutura multiplicativa de um número inteiro é revelada por sua fatoração em primos. Isso permite, entre outras coisas, determinar facilmente o mdc e o mmc de dois números inteiros, ambos não nulos.

No ensino básico, aprendemos que o mdc de dois inteiros positivos a e b é o número obtido ao se tomar o produto de todos os fatores primos comuns de a e b, com cada um desses fatores sendo escolhido com o menor dos expoentes que aparece nas fatorações de a e b. Vamos demonstrar esse fato (vamos utilizar no enunciado a seguir a notação apresentada na observação 4.2).

Proposição 4.1. *Se dois inteiros positivos a e b possuem as fatorações em primos*

$$a = \prod_{i=1}^{\infty} {p_i}^{a_i}, \quad b = \prod_{i=1}^{\infty} {p_i}^{b_i},$$

então o máximo divisor comum de a e b é igual a:

$$(a, b) = \prod_{i=1}^{\infty} {p_i}^{c_i}$$

onde $c_i = min\{a_i, b_i\}$.

Demonstração [5]**:** Para que um produto de fatores primos comum seja um divisor comum, nenhum expoente c_i de p_i poderá superar nem a_i e nem b_i. Como estamos interessados no maior divisor positivo, basta tomarmos, para c_i, o menor desses dois.

■

Exemplo 4.8. Se $a = 17\,640$ e $b = 47\,916$, então $(a, b) = 36$. Com efeito, fatorando a e b, temos que

$$a = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^2 \cdot 11^0 \cdot 13^1 \quad \text{e} \quad b = 2^2 \cdot 3^3 \cdot 5^0 \cdot 7^0 \cdot 11^3 \cdot 13^0.$$

Portanto, pela proposição 4.1,

$$(a, b) = 2^{min\{3,2\}} \cdot 3^{min\{2,3\}} \cdot 5^{min\{1,0\}} \cdot 7^{min\{2,0\}} \cdot 11^{min\{0,3\}} \cdot 13^{min\{1,0\}}$$

$$(a, b) = 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11^0 \cdot 13^0 = 4 \cdot 9 = 36.$$ ■

O algoritmo apresentado na proposição 4.1 para o cálculo do mdc é bem menos eficiente do que o de Euclides para inteiros muito grandes (que em geral não sabemos fatorar de forma eficiente computacionalmente), porém, esclarece Moreira em [16], é instrutivo saber que os dois algoritmos dão o mesmo resultado. Além disso, o algoritmo da proposição 4.1 tem

consequências teóricas importantes, como por exemplo: *Se* $(a,n)=1$ *e* $(b,n)=1$, *então* $(ab,n)=1$.

Aprendemos também no ensino básico, que o mmc de dois inteiros positivos a e b é o número obtido ao se tomar o produto de todos os fatores primos comuns de a e b, com cada um desses fatores sendo escolhido com o maior dos expoentes que aparece nas fatorações de a e b. Isto é demonstrado na proposição a seguir.

Proposição 4.2. *Se dois inteiros positivos a e b possuem as fatorações em primos*

$$a=\prod_{i=1}^{\infty} {p_i}^{a_i},\quad b=\prod_{i=1}^{\infty} {p_i}^{b_i},$$

então o mínimo múltiplo comum de a e b é igual a:

$$[a,b]=\prod_{i=1}^{\infty} {p_i}^{c_i}$$

onde $c_i=max\{a_i,b_i\}$.

Demonstração [5]**:** Da definição de mmc, nenhum fator p_i desse mínimo poderá ter expoente que seja inferior nem a_i e nem a b_i. Se tomarmos, pois, o maior destes dois para expoente de p_i teremos, não apenas um múltiplo comum, mas o menor possível dentre eles. O que conclui a demonstração.

■

Exemplo 4.9. *Seja* $a=17\,640$ *e* $b=47916$, *calcule* $[a,b]$.

Solução: Do exemplo 5.8, já sabemos que

$$a=2^3\cdot 3^2\cdot 5^1\cdot 7^2\cdot 11^0\cdot 13^1 \quad \text{e} \quad b=2^2\cdot 3^3\cdot 5^0\cdot 7^0\cdot 11^3\cdot 13^0.$$

Portanto, pela proposição 4.2, temos que

$$[a,b]=2^{max\{3,2\}}\cdot 3^{max\{2,3\}}\cdot 5^{max\{1,0\}}\cdot 7^{max\{2,0\}}\cdot 11^{max\{0,3\}}\cdot 13^{max\{1,0\}}$$

$$[a,b]=2^3\cdot 3^3\cdot 5^1\cdot 7^2\cdot 11^3\cdot 13^1=18\,687\,240.$$ ■

Observação 4.3. No ensino básico, vale ressaltar que geralmente usa-se para o cálculo do mmc o chamado *algoritmo da decomposição simultânea*, que é uma consequência imediata da proposição anterior. Por exemplo,

$$\begin{array}{r|l} 20\ ,\ 15 & 2 \\ 10\ ,\ 15 & 2 \\ 5\ ,\ 15 & 3 \\ 5\ ,\ 5 & 5\ \times \\ \hline 1\ ,\ 1 & 60 \end{array}$$

◿

Lema 4.1. *Se x e y são números inteiros, então*

$$max\{x, y\} + min\{x, y\} = x + y.$$

Demonstração: O resultado se verifica trivialmente quando $x = y$, uma vez que $max\{x, y\} = min\{x, y\} = x = y$. Sem perda de generalidade podemos supor que $x < y$, logo $max\{x, y\} = y$ e $min\{x, y\} = x$. Segue o resultado.

■

De posse das duas últimas proposições, juntamente com o lema 4.1, finalizamos está seção fornecendo outra demonstração para o teorema 3.4: *Dados dois inteiros a e b, temos que* $[a, b] \cdot (a, b) = |ab|$.

2ª Demonstração do Teorema 4.4. Sem perda de generalidade, podemos supor que $a, b \in \mathbb{N}$. Dadas, respectivamente, suas fatorações

$$a = \prod_{i=1}^{\infty} {p_i}^{a_i} \quad \text{e} \quad b = \prod_{i=1}^{\infty} {p_i}^{b_i},$$

temos, pelas proposições 4.1 e 4.2, que

$$(a, b) = \prod_{i=1}^{\infty} {p_i}^{min\{a_i, b_i\}} \quad \text{e} \quad [a, b] = \prod_{i=1}^{\infty} {p_i}^{max\{a_i, b_i\}},$$

donde, pelo lema 4.1, segue que

$$(a, b)[a, b] = \prod_{i=1}^{\infty} {p_i}^{min\{a_i, b_i\}} \cdot \prod_{i=1}^{\infty} {p_i}^{max\{a_i, b_i\}} = \prod_{i=1}^{\infty} {p_i}^{min\{a_i, b_i\} + max\{a_i, b_i\}}$$

$$= \prod_{i=1}^{\infty} {p_i}^{a_i + b_i} = \prod_{i=1}^{\infty} {p_i}^{a_i} \cdot \prod_{i=1}^{\infty} {p_i}^{b_i} = a \cdot b = |ab|.$$

■

4.3 DISTRIBUIÇÃO DOS NÚMEROS PRIMOS

Um considerável esforço tem sido despendido por diversos matemáticos desde tempos imemoriáveis no estudo dos números primos. Desse salutar esforço, Euclides em *Os*

elementos, proposição 20 do Livro IX, fincou um monumento ao engenho e à inteligência humana, onde demonstra astutamente que existe uma infinidade de números primos. Hefez em [6], destaca que essa demonstração é o primeiro registro matemático de uma demonstração por redução ao absurdo.

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

Demonstração: Dada qualquer conjunto finito $p_1, p_2, \dots, p_r$ de números primos, o número

$$n = p_1 \cdot p_2 \cdot \ \dots \cdot p_r + 1$$

não sendo divisível por nenhum dos primos desse conjunto, tem necessariamente, pelo TFA, um fator primo diferente de $p_1, p_2, \dots, p_r$. Assim, existe um primo que não pertence ao conjunto dado.

■

Esclarece Oliveira, em [7], que apesar de os números primos serem abundantes, em quantidade infinita, que não existe nenhum método razoável de produção de números primos, mesmo tendo em mãos a alta tecnologia de hoje em dia. Porém, ao longo do tempo algumas fórmulas e algoritmos se mostraram úteis para descoberta de números primos.

Nesse contexto, limitar-nos-emos a um dos mais antigos métodos para elaboração de tabelas de primos, devido ao matemático grego Eratóstenes, que viveu por volta de 230 a.C. O método, que é conhecido como *Crivo de Eratóstenes* (crivo significa peneira), se apoia no seguinte resultado:

Proposição 4.3. *Se n é um número composto, então n possui, necessariamente, um fator primo menor do que ou igual $\sqrt{n}$.*

Demonstração: Como n é composto, temos que $n = ab$, onde $1 < a < n$ e $1 < b < n$. Podemos supor, sem perda de generalidade, que $a \leq b$. Afirmamos que $a \leq \sqrt{n}$. Com efeito, se fosse $a > \sqrt{n}$, teríamos $n = ab > \sqrt{n} \cdot \sqrt{n} = n$, o que é absurdo. Como, pelo TFA, o número a possui algum fator primo p que deve ser menor do que ou igual a $\sqrt{n}$, e p sendo um fator de a, temos, então, que ele também será um fator primo de n, o que completa a demonstração. ■

Em outras palavras, a proposição 4.3 nos diz que para testarmos se um número é primo, é suficiente testarmos sua divisibilidade apenas pelos primos menores do que ou iguais a $\sqrt{n}$. Esse resultado, na verdade, fornece-nos também um *teste de primalidade*, ou seja, uma forma de verificar se um dado número n é primo.

A seguir, descrevemos o Crivo de Eratóstenes:

Escreve-se na ordem natural, todos os números naturais entre 2 e n, inclusive. Em seguida, eliminam-se todos os inteiros compostos que são múltiplos dos primos p tais que $p \leq \sqrt{n}$. Isto é: primeiro elimine todos os múltiplos de $2k$ de 2, com $k \geq 2$; a seguir, todos os múltiplos $3k$ de 3, com $k \geq 2$; depois os múltiplos de $5k$ de 5, com $k \geq 2$; e assim sucessivamente, para todo primo $p \leq \sqrt{n}$. Os números que sobrarem na lista são todos os primos entre 2 e n.

Vamos aplicar esse algoritmo no exemplo a seguir.

Exemplo 4.9. *Encontre todos os primos de entre 2 e 110, inclusive.*

Solução: Escrevendo na ordem natural, todos os números naturais entre 2 e 110, temos a seguinte tabela

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	77	76	77	78	79	80
81	88	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110

Tabela 4.1

Como $n = 110$, temos que $\sqrt{110} \cong 10{,}488088$, portanto se desejarmos obter todos os números primos entre 2 e 110, inclusive; devemos eliminar da tabela acima todos os números que são múltiplos de $2, 3, 5$ e 7 (estes são os primos menores do que ou iguais a $\sqrt{110}$), o que resulta na tabela abaixo

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	
		53			59
61				67	
71		73			79
		83			89
91				97	
101		103		107	109

Tabela 4.2

que figura todos os números primos menores do que 110.

■

No exemplo abaixo aplicamos a proposição 4.3 como critério de primalidade.

Exemplo 4.10. *Quais dos números é primo,* 239 *ou* 247*?*

Solução: Como $\sqrt{239} \cong 15{,}459624$, temos que verificar se 239 é divisível pelos primos menores do que 15, ou seja, $2, 3, 5, 7, 11$ e 13. De fato, nenhum desses números o divide (use uma calculadora ou os critérios de divisibilidade), logo, pela proposição 4.3, temos que 239 é primo. Já o número 247 é composto. De fato, $\sqrt{247} \cong 15{,}7162$, donde é suficiente verificar se 247 é múltiplo de algum primo menor do que 15. Ora, $247 = 13 \cdot 19$, portanto, um número composto.

■

Muitas questões interessantes sobre números primos não foram respondidas até hoje, principalmente aquelas que estão relacionadas à sua distribuição dentro dos números naturais. Em particular, qual a distância entre dois números primos consecutivos? Qual é a sua frequência?

No tocante à primeira pergunta, por um lado, observando a tabela 4.2, nota-se que há vários pares de números primos consecutivos. Em especial, há aqueles que diferem de duas unidades; quais sejam:

$$(3{,}5), (5{,}7), (11{,}13), (17{,}19), (41{,}43), (59{,}61),$$
$$(41{,}43), (59{,}61), (71{,}73), (101{,}103), (107{,}109).$$

A propósito, pares de números primos com essa propriedade são chamados de *primos gêmeos* (não se sabe até o presente momento se existe ou não uma infinidade desses primos). Por outro lado, contrasta com tais primos, o seguinte resultado:

Proposição 4.4. *Para qualquer natural n, existem n naturais consecutivos todos compostos.*

Demonstração: Seja n um número natural. Observe que, como $(n+1)!$ é divisível pelos naturais de 2 até $n+1$, temos que a sequência

$$(n+1)!+2,\ (n+1)!+3,\ (n+1)!+4,\ \dots,\ (n+1)!+n,\ (n+1)!+(n+1)$$

é, toda ela, composta por n números consecutivos compostos, concluindo a demonstração.

■

Ou seja, existem "saltos" arbitrariamente grandes na sequência de números primos. Portanto, a resposta à primeira pergunta é que não existe um padrão que descreva o quanto dois primos consecutivos estão longe um dos outros.

No tocante a segunda pergunta, queremos responder o quão frequentes são os números primos na sequência dos naturais. Para isso, seguimos Hefez [1], formalizando o conceito de frequência de primos, que é a mesma coisa que probabilidade. Dado $x \in \mathbb{N}$, denotamos, por $\pi(x)$, a quantidade de números primos menores do que ou iguais a x. Logo, a probabilidade de que um elemento do conjunto $\{1, \dots, x\}$ seja primo é dada por

$$\frac{\pi(x)}{x}. \tag{4.8}$$

Uma vez que esse quociente é uma função bastante complexa, esclarece Hefez [1], o que se espera é achar uma função de comportamento bem conhecido que se aproxime do quociente acima. A respeito disso, Fernandes, em [9], esclarece-nos que Gauss em seus estudos sobre números primos conjecturou que, para valores grandes de x, $\pi(x)$ era aproximadamente igual a $x/(ln\, x)$. Grandes matemáticos, como Legendre (1752 – 1833), Riemann (1826 – 1866) e Chebychev (1821 – 1894) tentaram achar aproximações para o quociente (4.8). Em 1896, esse problema foi resolvido de forma independente por C. J. de la Vallée-Poussin (1866 – 1962) e Hadamard (1865 – 1963). Esse importante e profundo resultado ficou conhecido como *Teorema dos Números Primos.*

Enunciamos a seguir esse importante resultado, cuja demonstração pode ser vista em cursos avançados de Teoria dos Números. Ressaltamos que existe uma demonstração completa no apêndice A de [8].

Teorema 4.2(dos Números Primos). *Sejam $x \in \mathbb{R}$,com $x > 0$, e $\pi(x)$ o número de primos p tais que $p \leq x$. Defina*

$$f(x) = \frac{x}{\ln x} \quad e \quad g(x) = \int_2^x \frac{dt}{\ln t}.$$

Então vale:

$$\lim_{x\to\infty} \frac{\pi(x)}{f(x)} = \lim_{x\to\infty} \frac{\pi(x)}{g(x)} = 1.$$

Exemplo 4.11. Pode-se afirmar que entre $a = 2\,600\,000$ e $b = 2\,700\,000$ existem exatamente 6762 primos. A estimativa feita por meio da integral é

$$\int_a^b \frac{dt}{\ln t} \cong 6761{,}332.$$

■

O exemplo a seguir é um caso especial de um importante resultado, conhecido, segundo Santos [5], como *Teorema dos Primos em Progressão Aritmética*, devido ao matemático alemão Dirichlet (1805 – 1859). Esse teorema diz que: *Se a e b são naturais coprimos, então a progressão aritmética $an + b$ (n é natural) contém um número infinito de primos.*

Exemplo 4.12. *Prove que existem infinitos primos da forma $4k + 3$, com $n \in \mathbb{N}$.*

Solução: Primeiro note que todo primo ímpar é da forma $4k + 1$ ou $4k + 3$. Depois observe que o conjunto

$$A = \{4x + 1\,; x \in \mathbb{N}\}$$

é fechado multiplicativamente, ou seja,

$$a \in A \quad \text{e} \quad \text{b} \in \text{A} \quad \Rightarrow \quad ab \in A.$$

Com efeito, sejam $a = 4x + 1$ e $b = 4x' + 1$, logo

$$ab = (4x + 1)(4x' + 1) = 4(4xx' + x + x') + 1 \quad \Longrightarrow \quad ab \in A$$

Prosseguindo, vamos supor por absurdo que exista um número finito de números primos $3 < p_1 < p_2 < \cdots p_n$ da forma $3k + 3$. Portanto, o número $y = 4(p_1.p_2 \ldots p_n) + 3$ não é divisível por nenhum dos primos $3, p_1, p_2, \ldots, p_n$ e , consequentemente, sua decomposição em fatores primos só pode conter primos da forma $4k + 1$. Assim, y é da forma $4k + 1$, o que é uma contradição, uma vez que y é da forma $4k + 3$. Segue o resultado.

■

Diante do que discorremos até agora nesta seção, ainda cabe a seguinte pergunta: existem fórmulas que geram números primos? Nesta pergunta figura um dos problemas mais antigos de que se tem notícia, qual seja: *será que existe algum polinômio que gera todos os números primos ou cujos valores fossem somente primos.* Alguns matemáticos da Idade Média acreditavam, por exemplo, que o polinômio $P(n) = n^2 + n + 41$ assumisse valores iguais a números primos para qualquer número natural n. Isso não é verdade, como já vimos no exemplo 1.2, pois $P(40)$ é um número composto. De forma geral, Legendre mostrou que não existe uma função algébrica (isto é, o quociente de dois polinômios) que forneça somente números primos. Todavia, segundo Fernandes [9], não é fácil exibi-las.

A história da Matemática nos revela que buscar números primos não é uma tarefa fácil. Muitos matemáticos tentaram obter fórmulas que gerassem números primos, mas as tentativas feitas nesse sentido revelaram-se erradas. Contudo, essa procura contribuiu de maneira significativa para o desenvolvimento da Teoria dos Números. A seguir, discorrendo acerca de duas dessas buscas:

1. **(Números de Fermat)**

Já vimos no capítulo 1 que Fermat observou que, para $n = 0, 1, 2, 3$ e 4, os números da forma

$$F_n = 2^{2^n} + 1$$

eram primos; em 1640 ele conjecturou que, para qualquer $n \in \mathbb{N}$, F_n era um número primo. Mas, Euler mostrou que F_5 é múltiplo de 641. Desde então, tentou-se descobrir outros números primos de Fermat, além dos cinco primeiros. Hoje, se sabe que F_n não é primo para $5 \leq n \leq 16$, mas ainda não foi provado se o número de primos de Fermat é finito ou infinito.

Um fato interessante a respeito dos números de Fermat é que eles são dois a dois coprimos. Esse é o conteúdo da próxima proposição, que, como consequência, nos fornece uma segunda demonstração de infinitude dos números primos.

Proposição 4.5. *Quaisquer dois números de Fermat distintos F_n e F_m são relativamente primos.*

Demonstração: Vamos mostrar, primeiramente, que a seguinte relação se verifica

$$F_0 F_1 \cdot \ldots \cdot F_{n-1} = F_n - 2. \tag{4.9}$$

A prova é por indução. Como o caso $n = 1$ se verifica, isto é, $F_0 = F_1 - 2$, vamos supor a validade para n (hipótese indutiva) e mostrar que a mesma relação também vale para $n + 1$.

De fato,

$$\begin{aligned} F_0F_1 \cdot \ldots \cdot F_n &= (F_0F_1 \cdot \ldots \cdot F_{n-1}) \cdot F_n \\ &= (F_n - 2)\, F_n \\ &= (2^{2^n} + 1 - 2)\,(2^{2^n} + 1) \\ &= (2^{2^n} - 1)\,(2^{2^n} + 1) = 2^{2^{n+1}} - 1 \\ &= 2^{2^{n+1}} + 1 - 2 = F_{n+1} - 2 \end{aligned}$$

Portanto, pelo PIF, segue que a igualdade (4.8) é verdadeira para todo $n \in \mathbb{N} \cup \{0\}$. Suponhamos agora $n < m$, logo, pela relação (4.8), temos que

$$F_0F_1 \cdot \ldots \cdot F_n \cdot \ldots \cdot F_{m-1} = F_m - 2,$$

ou seja,

$$F_m = F_0F_1 \cdot \ldots \cdot F_n \cdot \ldots \cdot F_{m-1} + 2.$$

Daí, pelo lema de Euclides (proposição 3.2), temos que

$$(F_n\,,\ F_m) = (F_n\,,\ F_0F_1 \cdot \ldots \cdot F_n \cdot \ldots \cdot F_{m-1} + 2) = (F_n\,, 2) = 1,$$

uma vez que F_n é ímpar.

■

Podemos concluir da proposição anterior que o *conjunto dos números primos é infinito*. Com efeito, sendo infinita a sequência de números de Fermat e não possuindo fatores primos comuns, isto não poderia acontecer se o conjunto dos números primos fosse finito.

2. (Números de Mersenne)

Todo números natural da forma

$$M_k = 2^k - 1, \qquad (4.10)$$

é chamado *número de Mersenne*. Marin Mesenne (1588 – 1648) foi um monge francês que nasceu na cidade de Maine e foi um dos grandes influenciadores de Matemática francesa nos séculos XVI e XVII. Um processo para determinar números primos grandes utiliza os números da forma (4.10). Tais números primos nesta forma são chamados devidamente de *primos de Mersenne.* Um resultado elementar acerca deles, segue na proposição seguinte.

Proposição 4.6. *Se* $M_k = 2^k - 1$ *é primo, então k é primo.*

Demonstração: Assuma que $M_k = 2^k - 1$ é primo e suponha por absurdo que k é composto. Digamos, sem perda de generalidade, que $k = ab$ e $a \geq b > 1$. Então M_k é composto (absurdo). De fato, basta notar que

$$M_k = M_{a.b} = 2^{ab} - 1 = (2^b)^a - 1^a = (2^b - 1)\left(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1\right),$$

■

Em 1644, Mersenne afirmou: *Se* $p \in \{2, 3, 5, 7, 13, 17, 31, 67, 127, 257\}$, *então todo número* M_p *é primo.* M_p*é composto para os outros primos* p *tais que* $2 < p < 257$.

Observe que

$$M_2 = 3,\ \ M_3 = 7,\ \ M_5 = 31,\ \ M_7 = 127,\ \ M_{13} = 8191$$
$$M_{17} = 131\,071,\ \ M_{19} = 524\,287 \ \text{ e } \ M_{31} = 2\,147\,483\,647.$$

Naquela época, esclarece Fernandes em [9], a afirmação de Mersenne era motivo de muitas controvérsias, uma vez que não existiam processos práticos para se verificar, por exemplo, se M_{31} era primo ou não. Com efeito, a maior tábua de números primos conhecida então só continha primos menores do que 750. Para verificar a afirmação de Mersenne, completa Fernandes [9], era necessária uma tábua com todos os números primos até $46\,340$.

A conjectura de Mersenne não era correta: ele errou ao incluir os números 67 e 257, e ao excluir os primos $19{,}61{,}89$ e 107. À propósito, no exemplo 5.11 mostramos efetivamente que a recíproca da proposição 4.2 é falsa (M_{83} é composto, apesar de 83 ser primo). Por curiosidade, um supercomputador calculou, no final de 2003, o maior primo de Mersenne, qual seja, o $M_{20\,996\,011}$, o qual possui $6\,320\,430$ algarismos.

Por fim, seguindo recomendação de Hefez em [1], não podemos deixar de mencionar o problema mais importante em aberto em Teoria dos Números: *a Hipótese de Riemann*. Trata-se de uma conjectura formulada pelo matemático alemão Bernhard Riemann (1826 – 1866) e está muito além do material aqui exposto. Se provada, muito dos mistérios dos números primos serão revelados, o que deixará o seu realizador, completa Hefez [1], num destacado lugar entre os imortais da Matemática.

4.4 EXPRESSÕES DECIMAIS FINITAS E INFINITAS

Nesta seção, encontra-se a abordagem com base em [10].

Um número racional é um número que pode ser escrito na forma a/b, em que a e b são números inteiros, com b diferente de zero. Por exemplo,

$$-\frac{3}{2}, \qquad \frac{1}{7}, \qquad \frac{25}{12} \quad \text{e} \quad \frac{3}{1}$$

são números racionais. Como qualquer número inteiro a pode ser escrito da forma $a/1$, temos que todo inteiro é racional.

Existe outra maneira de representar um número racional, chamada *representação decimal:*

$$-\frac{3}{2} = -1{,}5 \quad \frac{1}{7} = 0{,}14285714257\ldots \quad \frac{25}{12} = 2{,}08333\ldots \quad 3 = 3{,}0.$$

Essas expressões decimais são obtidas dividindo-se o numerador pelo denominador, segundo a divisão euclidiana (teorema 2.1), e multiplicando-se o resto por 10 e em seguida dividindo-se o último número obtido pelo denominador e assim sucessivamente:

```
1    | 7
10   0,1428571…
 30
  20
   60
    40
     50
      10
       ⋮
```

```
1    | 8
20   2,25
 40
  0
```

Se no decorrer desse processo, obtivermos um resto nulo, como no caso $1/8$, então a *expressão decimal é finita*. No entanto, podemos nunca obter um resto nulo, como no caso $1/7$, quando obtivemos os restos $1, 3, 2, 6, 4, 5$ e então novamente 1. Nesse ponto, reaparece a divisão de 10 por 7 e uma parte dos algarismos da expressão decimal de $1/7$, denominada *período*, começa a se repetir. Em ambos os casos, dizemos que a *expressão decimal é periódica* (daí o nome *dízima periódica*), já que o caso em que existe um resto nulo pode ser englobado por esse: $2{,}25 = 2{,}25000\ldots$

No caso geral a/b, sabemos que, ao efetuarmos a divisão de a por b, os únicos restos possíveis são $0, 1, \ldots, b-1$. Portanto, se não obtivermos o resto zero, podemos ter certeza de que, após um número finito de operações, haverá a repetição de algum resto, dando origem a um período não nulo. Vamos demonstrar esse resultado a seguir:

Proposição 4.7. *Todo número racional tem uma expressão decimal que se repete a partir de um determinado ponto.*

Demonstração: É suficiente provar o resultado para números racionais positivos. Suponhamos, então, que $r = a/b$. Sem perda de generalidade, podemos supor que essa fração é irredutível, ou seja, $(a, b) = 1$. Então,

$$\begin{aligned} a &= bq_0 + r_0, \quad com \quad 0 \leq r_0 < b \\ 10r_0 &= bq_1 + r_1, \quad com \quad 0 \leq r_1 < b \\ 10r_1 &= bq_2 + r_2, \quad com \quad 0 \leq r_2 < b \\ \vdots & \qquad \vdots \end{aligned}$$

De modo que

$$\frac{a}{b} = q_0 + \frac{q_1}{10} + \frac{q_2}{10} + \cdots.$$

Considere a sequência numérica

$$r_0, r_1, r_2, \ldots, r_{n-1}, r_n, \ldots$$

Se, nessa sequência, temos resto r_s nulo para algum s natural, a expressão decimal é finita. Caso contrário, como todos os números são positivos e menores do que b, ao menos dois desses números são iguais. Certamente deverá ocorrer repetição do resto antes de realizarmos b divisões. Dividir $10r_{s+d}$ por b resulta o mesmo quociente e resto da divisão de $10r_s$ por b. Isso significa que

$$q_{s+1} = q_{s+d+1} \text{ e } r_{s+1} = r_{s+d+1}.$$

O mesmo argumento mostra que

$$q_{s+2} = q_{s+d+2} \text{ e } r_{s+2} = q_{s+d+2},$$

e assim sucessivamente. Isso completa a demonstração.

■

Como todo número racional possui uma expressão decimal periódica, dizemos que esta expressão decimal é *finita*, se a partir de um determinado ponto os algarismos são todos nulos. Caso contrário, a expressão decimal é *infinita*. Por exemplo, os números racionais

$$\frac{3}{2} = 1{,}5 \quad \text{e} \quad \frac{3}{1} = 3{,}0$$

possuem representação decimal finita. Porém,

$$\frac{1}{7} = 0{,}1425714257 \ldots \quad \text{e} \quad \frac{25}{12} = 2{,}08333 \ldots$$

não possuem expressões decimais finitas.

Se a expressão decimal de um número r é finita, então é possível representá-lo como um quociente cujo denominador é uma potência de 10. Por exemplo:

$$2{,}2375 = \frac{22375}{10^4}$$

E que podemos simplificar essa fração até torna-la *irredutível*, isto é, até que o numerador e o denominador não possuam fatores primos em comum:

$$\frac{22375}{10^4} = \frac{7 \cdot 5^5}{2^4 \cdot 5^4} = \frac{7 \cdot 5}{2^4} = \frac{35}{16}.$$

Observe que, como o denominador é sempre uma potência de 10, os únicos números primos que podem aparecer na fatoração do denominador da fração na forma irredutível são 2 e 5, ou mesmo nenhum deles

$$1{,}5 = \frac{3}{2}, \quad 0{,}04 = \frac{1}{5^2}, \quad 3{,}0 = \frac{3}{1}, \quad 0{,}1 = \frac{1}{10}.$$

Por outro lado, se considerarmos uma fração irredutível a/b, tal que b possua, no máximo, os primos 2 e 5 em sua fatoração, podemos garantir que a expressão decimal de a/b é finita. Por exemplo, seja

$$\frac{a}{b} = \frac{3087}{200} = \frac{3^2 \cdot 7^3}{2^3 \cdot 5^2}.$$

Para obtermos a expressão decimal de a/b, devemos transformar a fração a/b numa outra, cujo denominador seja uma potência de 10. Para isso, nesse caso, basta multiplicarmos o numerador e o denominador por 5:

$$\frac{3087}{200} = \frac{3087}{2^3 \cdot 5^2} = \frac{3087 \cdot 5}{2^3 \cdot 5^2 \cdot 5} = \frac{15435}{(2 \cdot 5)^3} = \frac{15435}{10^3} = 15{,}435$$

Vamos demonstrar o resultado geral:

Proposição 4.8. *Um número racional a/b, na forma irredutível, possui uma expressão decimal finita se, e somente se, o denominador b não tiver fatores primos além de* 2 *e* 5.

Demonstração: Se r for um número racional que possui uma expressão decimal finita, então

$$r = a_1 a_2 \ldots a_n \, , b_1 b_2 \ldots b_s = \frac{a_1 a_2 \ldots a_n b_1 b_2 \ldots b_s}{10^s}$$

Em que $n \geq 1$ e $s \geq 0$. Logo, simplificando a fração, obteremos uma fração irredutível $r = a/b$, em que b não possui nenhum fator primo além de 2 e 5, pois b é um divisor de 10^s. Reciprocamente, seja a/b uma fração irredutível cujo denominador b possua, no máximo, os fatores primos 2 e 5. Logo,

$$b = 2^m \cdot 5^n, \text{ em que } \; m \geq 0 \;\; \text{e} \;\; n \geq 0.$$

Temos apenas duas possibilidades: $n \leq m$ ou $n > m$.

Por um lado, se $n \leq m$, então $m - n \geq 0$ e $5^{m-n} \in \mathbb{N}$. Portanto, multiplicando o numerador e o denominador por 5^{m-n}, obtemos a fração equivalente:

$$\frac{a}{b} = \frac{a}{2^m \cdot 5^n} = \frac{a \cdot 5^{m-n}}{2^m \cdot 5^n \cdot 5^{m-n}} = \frac{a \cdot 5^{m-n}}{2^m \cdot 5^m} = \frac{c}{10^m},$$

em que $c = a \cdot 5^{m-n} \in \mathbb{N}$. Como a divisão de c por 10^m requer apenas que coloquemos a vírgula no lugar correto, obtemos a expressão decimal finita de a/b.

Por outro lado, se $n > m$, então $n - m > 0$ e $5^{n-m} \in \mathbb{N}$. Multiplicando o numerador e o denominador por 5^{n-m}, obtemos:

$$\frac{a}{b} = \frac{a}{2^m \cdot 5^n} = \frac{a \cdot 5^{n-m}}{2^m \cdot 5^n \cdot 5^{n-m}} = \frac{a \cdot 5^{n-m}}{2^n \cdot 5^n} = \frac{d}{10^n},$$

em que $d = a \cdot 5^{n-m} \in \mathbb{N}$. Obtivemos, assim, uma expressão decimal para a/b.

■

4.5 DUAS PERGUNTAS INTERESSANTES

Nesta seção, nosso objetivo é responder as seguintes perguntas:

1) Dado um número natural n, existe uma fórmula para determinar a soma dos divisores positivos de n?

2) Como achar a fatoração em números primos de $n!$, onde n á um número natural arbitrário?

No tocante a primeira pergunta, a resposta é positiva. Denotemos por $\sigma(n)$ a soma de todos os divisores naturais do natural n. Note que $\sigma(n) = n + 1$ se, e só se, n é primo. A próxima proposição nos fornece uma fórmula geral para $\sigma(n)$.

Antes, motivamos a ideia da demonstração calculando, por exemplo, a soma de todos os divisores positivos de 90. De forma prática, no ensino básico, geralmente fazemos esse cálculo decompondo 90 em fatores primos; depois combinamos todos os produtos possíveis de seus fatores primos, obtendo todos os divisores de 90 (tal algoritmo é uma consequência do corolário 4.2). Assim, fica fácil calcular $\sigma(90)$, como segue:

		1
90	2	2
45	3	3,6
15	3	9,18
5	5	5,10,15,30,45,90
1		(Divisores de 90)

Logo,

$$\sigma(90) = 1 + 2 + 3 + 5 + 6 + 9 + 10 + 15 + 18 + 30 + 45 + 90 = 234.$$

Por outro lado,

$$\sigma(90) = \sigma(2^1 \cdot 3^2 \cdot 5^1) = 234 = 3 \cdot 13 \cdot 8 = \underbrace{(1 + 2^1)}_{fator1}\underbrace{(1 + 3^1 + 3^2)}_{fator2}\underbrace{(1 + 5^1)}_{fator3},$$

portanto, como o *fator 1*, o *fator 2* e o *fator 3* denotam, cada um, a soma de uma progressão geométrica de razão 2,3 e 5, respectivamente, temos que

$$\sigma(90) = \sigma(2^1 \cdot 3^2 \cdot 5^1) = \left(\frac{2^2-1}{2-1}\right)\left(\frac{3^3-1}{3-1}\right)\left(\frac{5^2-1}{5-1}\right).$$

Estamos em condições de demonstrar a seguinte proposição:

Proposição 4.9. Seja $n = \prod_{i=1}^{r} {p_i}^{a_i}$ a decomposição de n em fatores primos p_i distintos. Então:

$$\sigma(n) = \prod_{i=1}^{r} \frac{{p_i}^{a_i+1}-1}{p_i-1}. \qquad (4.11)$$

Demonstração: Fixada a ideia descrita anteriormente, considere a igualdade

$$(1 + p_1 + \cdots + {p_1}^{a_1}) \times \ldots \times (1 + p_r + \cdots + {p_r}^{a_r}) = \sum \left({p_1}^{b_1} \ldots {p_r}^{b_r}\right), \qquad (4.12)$$

onde o somatório do lado direito da igualdade é tomado sobre todas as *r*-uplas $(b_1, \ldots, b_r)$ ao variar cada b_i no intervalo $0 \leq b_i \leq a_i$, para $i \in \{1,2,\ldots,r\}$. Como tal somatório representa $\sigma(n)$, a fórmula (4.11) resulta da soma de uma progressão geométrica de cada soma do lado esquerdo da igualdade (4.12).

■

Observação 4.4. A validade da igualdade (4.12) pode ser vista do seguinte modo: seu primeiro membro, quando expandido, dá origem a uma soma cujas parcelas correspondem exatamente a todas as maneiras possíveis de multiplicar uma das parcelas do 1º fator, por uma das parcelas do 2º fator, …, etc.

◿

Exemplo 4.13.

$$\sigma(28) = \sigma(2^2 \cdot 7) = \left(\frac{2^3-1}{2-1}\right)\left(\frac{7^2-1}{7-1}\right) = 56.$$

$$\sigma(18) = \sigma(2 \cdot 3^2) = \left(\frac{2^2-1}{2-1}\right)\left(\frac{3^2-1}{3-1}\right) = 39.$$

■

Vamos agora responder a segunda pergunta. Queremos encontra uma forma de fatorar $n!$, onde n é um natural qualquer. Para isso, vamos antes introduzir algumas notações.

Definição 4.2. *Dado $x \in \mathbb{R}$, sua parte inteira, denotada por $\lfloor x \rfloor$ é o maior inteiro menor do que ou igual a x, ou seja, $\lfloor x \rfloor = max\{n \in \mathbb{Z}; n \leq x\}$. Ou de outro modo, para $n \in \mathbb{Z}$, temos*

$$\lfloor x \rfloor = n \quad \Leftrightarrow \quad n \leq x < n + 1.$$

Exemplo 4.14. Como $1 < \sqrt{2} < 2$, temos que $\lfloor \sqrt{2} \rfloor = 1$; Como $-3 < -2{,}3 < -2$, temos que $\lfloor -2{,}3 \rfloor = -3$.

■

Note que com a definição 4.2, a partir do teorema 2.1 (divisão euclidiana), temos que dados $n, d \in \mathbb{Z}$ e $d > 0$, podemos denotar o quociente e o resto da divisão de n por d por $q = \left\lfloor \frac{a}{d} \right\rfloor$ e $r = n - \left\lfloor \frac{a}{d} \right\rfloor d$.

Outra notação importante, que está relacionada com o TFA, é a seguinte:

Definição 4.3. *Se $n \in \mathbb{Z}\backslash\{0\}$ e p é um número primo, denotaremos por $E_p(n)$ o expoente da maior potência de p que divide n.*

Exemplo 4.15. Como $360 = 2^3 \cdot 3^2 \cdot 5^1$, temos $E_2(360) = 3$, $E_3(360) = 2$ e $E_5(360) = 1$.

■

Usando a definição 4.3 e o TFA, podemos caracterizar a igualdade de dois números naturais m e n: $m = n \Leftrightarrow E_p(m) = E_p(n)$.

A proposição a seguir, devido ao matemático francês Adriene-Marie Legendre (1752 – 1833), ensina como calcular o expoente do primo p da decomposição de $n!$ em fatores primos, mesmo que não conheçamos tal decomposição explicitamente, que seria bastante trabalhosa. A fórmula (4.13) é conhecida como **fórmula de Legendre**.

Proposição 4.10. *Sejam $n > 1$ natural e p primo. Então:*

$$E_p(n) = \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \qquad (4.13)$$

Demonstração: Note inicialmente que a soma acima é sempre finita, uma vez que, para $p^k > n$, temos que $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$. Seja agora $k \in \mathbb{N}$ qualquer e $p^k, 2p^k, \ldots, mp^k$ os múltiplos de p^k menores do que ou iguais a n. Então

$$mp^k \leq n < (m+1)p^k,$$

ou de forma equivalente,

$$m \leq \frac{n}{p^k} < m + 1.$$

Portanto, m é o maior inteiro menor do que ou igual a $^{n}/_{p^k}$, ou seja, $m = \left\lfloor {}^{n}/_{p^k} \right\rfloor$. Assim, para cada $k \geq 1$ há exatamente

$$\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor$$

naturais menores do que ou iguais a n e que são múltiplos de p^k mas não de p^{k+1}. Como cada um de tais números contribui exatamente com k fatores para $E_p(n)$, segue que

$$\begin{aligned} E_p(n) &= 1 \cdot \left(\left\lfloor \frac{n}{p^1} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor \right) + 2 \cdot \left(\left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor \right) + 3 \cdot \left(\left\lfloor \frac{n}{p^3} \right\rfloor - \left\lfloor \frac{n}{p^4} \right\rfloor \right) + \cdots \\ &= \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \end{aligned}$$ ■

Com a fórmula de Legendre, fica fácil calcular a fatoração 10!, por exemplo. Com efeito, devemos achar $E_p(10!)$ Para todo primo $p \leq 10$. Sendo

$$E_2(10!) = 5 + 2 + 1 = 8$$
$$E_3(10!) = 3 + 1 = 4$$
$$E_5(10!) = 2$$
$$E_7(10!) = 1$$

segue que

$$10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7.$$

O exemplo a seguir traz uma aplicação interessante da fórmula de Legendre.

Exemplo 4.16. Encontre o número de zeros consecutivos no final de 1000!.

Solução: Podemos escrever

$$1000! = 2^{E_2(1000!)} 5^{E_5(1000!)} m,$$

onde $m \in \mathbb{N}$. Logo, a fim de calcular a maior potência de 10 que divide 1000!, basta calcular o menor dos números $E_2(1000!)$ e $E_5(1000!)$. O menor de tais números claramente é $E_5(1000!)$, o qual pode ser calculado por intermédio da fórmula de Legendre:

$$E_5(1000!) = \left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{5^2} \right\rfloor + \left\lfloor \frac{1000}{5^3} \right\rfloor + \left\lfloor \frac{1000}{5^4} \right\rfloor = 200 + 40 + 8 + 1 = 249.$$

■

PROBLEMAS PROPOSTOS

4.1. Encontre todos os pares de primos p e q tais que $p - q = 3$.

4.2. Calcule o menor número natural n tal que n, $n+1$, $n+2$, $n+3$, $n+4$ e $n+5$ são todos compostos.

4.3. Mostre que 7 é o único número primo da forma $n^3 - 1$.

4.4. Mostre que três números naturais ímpares consecutivos não podem ser todos primos, com exceção de 3, 5 e 7.

4.5. Mostre que o número $7^{27} - 41^{81}$ é composto.

4.6. Mostre que todo número da forma $n^4 + 4^n$, com $n \in \mathbb{N}$, é composto.

4.7. Mostre que

(a) $\sqrt{5}$ é uma número irracional;

(b) se p é primo, então $\sqrt{p}$ é um número irracional.

4.8. Usando o TFA, mostre que

(a) $\sqrt{1000}$ é irracional;

(b) se n não é um quadrado perfeito, então $\sqrt{n}$ é irracional.

4.9. Mostre que existem infinitos primos da forma $6n + 5$.

EULER: O LEGADO DE UM GIGANTE

Nesta nota histórica, encontra-se a abordagem com base em [6].

Leonard Euler (1707 – 1783) foi, sem dúvida, um dos maiores e mais férteis matemáticos de todos os tempos.

Euler possuia uma grande facilidade para o aprendizado de línguas e uma prodigiosa memória, aliada a uma extraordinária habilidade para efetuar cálculos complexos mentalmente, habilidade essa que lhe seria útil no final de sua vida. Aos 14 anos, ingressou na universidade da Basiléia, onde foi aluno de Johann Bernoulli, com quem teve a sua verdadeira iniciação científica à Matemática. Aos 20 anos de idade, Euler recebeu a menção horosa da Academia de Ciências de Paris por um trabalho sobre a tragetória do mastro de um barco em movimento, ganhando reconhecimento internacional.

Em 1727, começou sua carreira profissional, assumindo uma posição como físico na nova Academia de São Petersburgo, na Rússia. Foi nessa época que conheceu Cristian Goldbach, que chamou sua atenção para os problemas tratados por Fermat, fato esse responsável pela grande obra de Euler em Teoria dos Números.

Euler provou todos os resultados de Fermat, com exceção do Último Teorema, do qual mostrou sua validade para as equações $x^3 + y^3 = z^3$ e $x^4 + y^4 = z^4$.

Euler produziu freneticamente resultados matemáticos ao longo de sua longa vida científica, que só cessou com sua morte. Em 1738, Euler perde a visão de seu olho direito, ficando totalmente cego em 1771, não diminuindo por isto a sua produtividade científica. Durante muito tempo, cerca de metade de cada volume dos anais da Academia São Petersburgon era dedicada a seus trabalhos e , durante 48 anos após a sua morte, ainda neles eram publicados artigos seus.

Euler escreveu sobre os mais variados assuntos, tais como teoria das funções, teoria das partições e mecânica, cálculo diferencial e integral, números complexos, acústica, música, teoria dos números, entre muitos outros, ocupando, indiscutivelmente, um lugar entre os maiores matemáticos de todos os tempos.

5 - CONGRUÊNCIA MODULAR

Para avançar no estudo dos números inteiro é necessário introduzir a teoria de congruência modular. Essa teoria está intimamente relacionada ao nome de Carl F. Gauss (1777 – 1855), que contribuiu à Teoria dos Números de forma essencial em seu trabalho publicado em 1801 (*Disquisitiones Arithmeticae)*, quando tinha apenas 24 anos.

Neste capítulo, definimos congruência módulo m e apresentamos suas propriedades fundamentais. Discorremos sobre teoremas importantes devidos a Wilson, Fermat e Euler, os quais somos capazes de obter resultados surpreendentes. Por fim, oferecemos uma breve discussão acerca de sistemas de congruências lineares.

5.1 DEFINIÇÃO E PROPRIEDADES

Os exemplos a seguir apresentam uma característica comum que passaremos a explorar mais profundamente ao longo do texto e será o alicerce da definição de congruência modular entre dois números inteiros.

Exemplo 5.1. Determine o horário de chegada a certo destino de um transeunte, sabendo que sua viagem dura, com paradas e pernoites, 73 horas, e que o horário de partida é às 17 horas.

Solução: Para isso, basta obter o resto da divisão $73 + 17 = 90$ por 24, uma vez que o dia tem 24 horas:

$$90 = 24 \cdot 3 + 18.$$

Assim, o horário de chegada é 18 horas.

■

Exemplo 5.2. Comprei uma lancha e vou pagá-la em 107 prestações mensais. Se estamos em março, em qual mês terminarei de pagá-la?

Solução: Considerando a numeração usual dos meses, temos que março corresponde ao mês 3. Logo, para encontrar o mês o qual termina as prestações, basta obter o resto da divisão de $3 + 107 = 110$ por 12 (o ano tem 12 meses):

$$110 = 9 \cdot 12 + 2.$$

Assim, o mês será o 2, que corresponde ao de fevereiro.

■

Os dois últimos exemplos apresentados figuram situações de fenômenos periódicos. Note que no exemplo 5.1 a repetição considerada foi diária (24horas), enquanto no exemplo 5.1 foi anual (12 meses).

No exemplo 5.1, gostaríamos de identificar os inteiros que deixam o mesmo resto quando divididos por 24. Se agora são 5 horas, daqui a 24 horas serão novamente 5 horas. Gostaríamos, então, de identificar 5 com $5 + 24 = 27$ (números que deixam o mesmo resto quando divididos por 24). Teríamos, nesse caso, 24 tipos de inteiros, quais sejam, os que deixam resto 0, 1, 2, …, 22 e 23 quando divididos por 24.

No exemplo 5.2, gostaríamos de identificar dois inteiros que deixam o mesmo resto quando divididos por 12. Com efeito, se estamos no mês 3 (março), daqui a 12 meses estaremos novamente em março. Logo, gostaríamos de identificar 3 com $3 + 12 = 15$. Note que esse número deixa resto 3 quando dividido por 12. Nesse exemplo, temos 12 tipos de inteiros, quais sejam, os que deixam resto 0, 1, 2, …, 10 e 11 quando divididos por 12.

Em várias situações, como nos dois últimos exemplos, os números inteiros nos interessam somente em relação ao resto que eles deixam ao serem divididos por determinado inteiro m.

Definição 5.1. *Se a e b são inteiros dizemos que $\boldsymbol{a}$ é congruente a $\boldsymbol{b}$ módulo m $(m > 0)$ se $m \mid (a - b)$. Denotamos isto por $a \equiv b\ (mod\ m)$. Se $b \nmid (a - b)$ dizemos que $\boldsymbol{a}$ é incongruente a $\boldsymbol{b}$ módulo m e denotamos $a \not\equiv b\ (mod\ m)$.*

Exemplo 5.3. Note que $21 \equiv 1\ (mod\ 4)$ pois $4 \mid (21 - 1)$. Como $4 \nmid 13$ e $13 = 19 - 6$ temos que $19 \not\equiv 6\ (mod\ 4)$. De modo geral, observemos o que ocorre com os inteiros positivos módulo 4:

$$4k \equiv 0\ (mod\ 4),\quad 4k + 1 \equiv 1\ (mod\ 4),$$
$$4k + 2 \equiv 2\ (mod\ 4) \text{ e } 4k + 3 \equiv 3\ (mod\ 4).$$

Então, a sequência $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, \ldots$ dos inteiros positivos é igual, módulo 4, à sequência

$$1, 2, 3, 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2\ \ldots$$

Logo, todo número natural é congruente, módulo 4, ao resto de sua divisão por 4.

◿

A proposição a seguir figura uma maneira equivalente de enxergar a definição 5.1.

Proposição 5.1. $a \equiv b\ (mod\ m)$ *se ,e somente se,* a *e* b *deixam o mesmo resto quando divididos por* m.

Demonstração: Se $a \equiv b\ (mod\ m)$, então $m \mid (a-b)$, logo existe $k \in \mathbb{Z}$ tal que

$$a = b + km.$$

Por outro lado, a divisão euclidiana garante que existem únicos inteiros q e r tais que

$$a = qm + r, \quad \text{como} \quad 0 \leq r < |m|.$$

Logo,

$$b + km = qm + r$$

e, portanto,

$$b = (q-k)m + r, \quad \text{como} \quad 0 \leq r < |m|.$$

Reciprocamente, se a e b deixam o mesmo resto quando divididos por m, então

$$a = qm + r \quad \text{e} \quad b = tm + r, \quad \text{em que} \ \ 0 \leq r < |m|$$

para certos inteiros q e t. Logo,

$$a - b = (q-t)m,$$

ou seja,

$$m \mid (a-b) \implies a \equiv b\ (mod\ m).$$

■

Observação 5.1. Para provar que $a \equiv b\ (mod\ m)$ temos, pela proposição 5.1, duas alternativas: mostrar diretamente que $m \mid (a-b)$, ou mostrar que a e b deixam o mesmo resto quando divididos por m. A segunda alternativa é mais didática para uma apresentação aos discentes do ensino básico, uma vez que usamos diretamente a divisão euclidiana, resultado já familiar entre os alunos daquele nível de ensino.

◿

Exemplo 5.4. Observe que $3\,111 \equiv 3813\ (mod\ 9)$, pois $3\,111$ e $3\,813$ deixam resto 6 quando divididos por 9.

■

A notação $a \equiv b\ (mod\ m)$, introduzida por Gauss em sua obra *Disquisitiones Arithmeticae,* é convenientemente semelhante à igualdade.

A seguir, apresentamos as propriedades básicas da relação de congruência módulo m.

Proposição 5.2. *Seja* $m \in \mathbb{N}\backslash\{1\}$. *Para quaisquer inteiros* a, b, c, d *temos:*

1. *(Reflexividade)* $a \equiv a \ (mod\ m)$;
2. *(Simetria) se* $a \equiv b \ (mod\ m)$, *então* $b \equiv a \ (mod\ m)$;
3. *(Transitividade) se* $a \equiv b \ (mod\ m)$ *e* $b \equiv c \ (mod\ m)$, *então* $a \equiv c \ (mod\ m)$;
4. *(Compatibilidade com a adição e subtração) Podemos adicionar e subtrair "membro a membro":*

$$\begin{cases} a \equiv b \left(mod\ m\right) \\ c \equiv d \left(mod\ m\right) \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d \left(mod\ m\right) \\ a - c \equiv b - d \left(mod\ m\right) \end{cases}.$$

Em particular, se $a \equiv b \ (mod\ m)$, *então* $ka \equiv kb \ (mod\ m)$ *para todo* $k \in \mathbb{N}$.

5. *(Compatibilidade com o produto) podemos multiplicar "membro a membro":*

$$\begin{cases} a \equiv b \left(mod\ m\right) \\ c \equiv d \left(mod\ m\right) \end{cases} \Rightarrow \quad ac \equiv bd \ (mod\ m).$$

Em particular, se $a \equiv b \ (mod\ m)$, *então* $a^k \equiv b^k \ (mod\ m)$ *para todo* $k \in \mathbb{N}$.

6. *(Cancelamento) Se* $(c, m) = 1$, *então*

$$ac \equiv bc \ (mod\ m) \quad \Leftrightarrow \quad a \equiv b \ (mod\ m).$$

Demonstração: As três primeiras propriedades são imediatas, basta notar que:

(1) $m \mid a - a = 0$.

(2) Se $m \mid (a - b)$, então $m \mid -(a - b) = (b - a)$.

(3) Se $n \mid (a - b)$ e $n \mid (b - c)$, então $n \mid (a - b) + (b - c) = (a - c)$.

Quanto às outras propriedades:

(4) De $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, temos que $m \mid (a - b)$ e $m \mid (c - d)$, então $m \mid (a - b) + (c - d) = (a + c) - (b + d)$. Logo, $a + c \equiv b + d \ (mod\ m)$. Também, se $m \mid (a - b)$ e $m \mid (c - d)$, temos $m \mid (a - b) - (c - d) = (a - c) - (b - d)$, ou seja, $a - c \equiv b - d \ (mod\ m)$. Com tais resultados, por indução, prova-se facialmente que $ka \equiv kb \ (mod\ m)$, onde k é um número natural.

(5) De $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, temos que $m \mid (a - b)$ e $m \mid (c - d)$, então $m \mid (a - b)c + (c - d)b = ac - bd$. Logo, $ac \equiv bc \ (mod\ m)$. De posse desse resultado, por indução, prova-se facialmente que $a^k \equiv b^k \ (mod\ m)$, onde k é um número natural.

(6) Finalmente, como $ac \equiv bc \ (mod\ m)$, temos $m \mid (ac - bc) = c(a - b)$. Uma vez que $(c, m) = 1$, pelo lema de Gauss, temos que $m \mid (a - b)$, ou seja, $a \equiv b \ (mod\ m)$.

■

Observação 5.2. Uma relação entre pares de elementos de um determinado conjunto (a igualdade de números racionais ou a congruência módulo m) é chamada de **relação de equivalência** se ela satisfaz as propriedades reflexiva, simétrica e transitiva. Assim, a proposição anterior, itens 1), 2) e 3), mostra que a congruência módulo m é uma relação de equivalência. Por isso, tal relação tem um comportamento similar à relação de igualdade.

◿

Chamamos a atenção para item 6) da proposição 5.2. Ele é um caso particular da proposição abaixo:

Proposição 5.3. Sejam $a, b, c, m \in \mathbb{Z}$ como $m > 1$. Temos que

$$ac \equiv bc\ (mod\ m) \quad \Leftrightarrow \quad a \equiv b\ \left(mod\ \frac{m}{(c,m)}\right).$$

Demonstração: Uma vez que $\left(\frac{c}{(c,m)}, \frac{m}{(c,m)}\right) = 1$, segue-se que

$$ac \equiv bc\ (mod\ m) \ \Leftrightarrow\ m \mid (a-b)c \ \Leftrightarrow\ \frac{m}{(c,m)} \mid (a-b)\frac{c}{(c,m)} \ \Leftrightarrow\ \frac{m}{(c,m)} \mid (a-b).$$

Assim, $a \equiv b\ \left(mod\ \frac{m}{(c,m)}\right)$, como queríamos demonstrar.

■

Vamos agora a alguns exemplos que nos revelarão a riqueza do campo de aplicação da relação de congruência módulo m. Nesse sentido, ao leitor interessado, aconselhamos a leitura de [1], página 216, que nos fornece uma exímia aplicação (no calendário) desta salutar relação.

Neto [13] esclarece que uma das vantagens do uso de congruências é o ganho computacional, que nos permite mecânica e rapidamente calcular restos da divisão como o exemplo a seguir.

Exemplo 5.5. *Mostre que* $20^{15} - 1$ *é múltiplo de 31.*

Solução: Notemos que, calcular $20^{15} - 1$, para depois dividir por 13, não é o melhor caminho. Vamos ser econômicos. Queremos mostrar que $31 \mid 20^{15} - 1$, ou seja, que $20^{15} \equiv 1\ (mod\ 31)$. Para isso, vamos localizar uma congruência módulo 31 que nos ajude a buscar congruências módulo 31 com as potências de base 20. Observando que

$$20 \equiv -11\ (mod\ 31), \tag{5.1}$$

temos que, pela proposição 5.2 (5) que

$$20^2 \equiv (-11)^2 (mod\ 31) \quad \Leftrightarrow \quad 20^2 \equiv 121\ (mod\ 31).$$

Como $121 \equiv -3\ (mod\ 31)$, temos, pela transitividade, que

$$20^2 \equiv -3(mod\ 31). \qquad (5.2)$$

Pela compatibilidade da multiplicação, multiplicando (5.1) e (5.2) membro a membro, obtemos $20^3 \equiv 33(mod\ 31)$ e, uma vez que $33 \equiv 2(mod\ 31)$, temos que

$$20^3 \equiv 2(mod\ 31).$$

Elevando a 5 ambos os membros desta última congruência, temos que $20^{15} \equiv 32(mod\ 31)$. Como $32 \equiv 1(mod\ 31)$, obtemos

$$20^{15} \equiv 1\ (mod\ 31),$$

que é o resultado almejado.

■

Exemplo 5.6. *Mostre que para todo natural ímpar n, temos que $13^{3n} + 17^{3n}$ é sempre divisível por 45.*

Solução: Como $13^2 = 169 \equiv 34\ (mod\ 45)$, temos, multiplicando por 13 membro a membro, que $13^3 \equiv 442\ (mod\ 45)$. Daí, $442 \equiv -8\ (mod\ 45)$, então $13^3 \equiv -8\ (mod\ 45)$. Uma vez que n é ímpar, a proposição 5.2(5) nos garante que:

$$13^{3n} \equiv -8^{3n}\ (mod\ 45) \qquad (5.3)$$

Por outro lado, como $17^2 = 19 \equiv 34\ (mod\ 45)$, temos, multiplicando por 17 membro a membro, que $17^3 \equiv 323\ (mod\ 45)$. Como $323 \equiv 8\ (mod\ 45)$, então $17^3 \equiv 8\ (mod\ 45)$, donde, novamente pela proposição 5.2(5), infere-se que

$$17^{3n} \equiv 8^n\ (mod\ 45) \qquad (5.4)$$

Somando membro a membro (5.3) e (5.4), temos que

$$13^{3n} + 17^{3n} \equiv 0\ (mod\ 45) \quad \Leftrightarrow \quad 45 \mid 13^{3n} + 17^{3n}.$$

■

É possível utilizar a notação e as propriedades de congruência módulo m para demonstrar várias afirmações já provadas ao longo do texto. A seguir daremos vários exemplos onde a utilização deste conceito torna as demonstração dessas afirmações mais diretas como mostram os exemplos a seguir.

Exemplo 5.7. Sob a ótica da teoria de congruência módulo m, vamos demonstrar novamente o critério de divisibilidade por 3 e 9. Seja $n = a_r 10^r + a_{r-1}10^{r-1} + \cdots + a_1 10 + a_0$ a representação do natural n na base 10. Como $10 \equiv 1\ (mod\ 3)$ e $10 \equiv 1\ (mod\ 9)$, então, pela proposição 5.2(5), temos que $10^k \equiv 1\ (mod\ 3)$ e $10^k \equiv 1\ (mod\ 9)$ para todo natural $k \geq 0$. Logo, temos que

$$n = a_r 10^r + a_{r-1}10^{r-1} + \cdots + a_1 10 + a_0 \equiv a_r + a_{r-1} + \cdots + a_1 + a_0\ (mod\ 9)$$

e

$$n = a_r 10^r + a_{r-1}10^{r-1} + \cdots + a_1 10 + a_0 \equiv a_r + a_{r-1} + \cdots + a_1 + a_0 \ (mod\ 3),$$

ou seja, n é congruente módulo 3 (e 9) à soma de seus dígitos. Logo, 3 ou 9 divide n se, e só se, 3 ou 9 divide $a_r + a_{r-1} + \cdots + a_1 + a_0$.

■

Observação 5.3. Hefez, em [1], esclarece que: *para verificar se um dado número é divisível por 3 ou por 9, somam-se os seus algarismos, desprezando-se, ao efetuar a soma, cada parcela igual a nove. Se o resultado final for zero, então o número é divisível por 9. Se o resultado final for um dos algarismos 0, 3 ou 6, então o número é divisível por 3.* Essa regra é conhecida como *Regra dos nove fora.*

◿

Exemplo 5.8. Fornecemos agora uma nova demonstração do critério de divisibilidade por 11 apresentado no Capítulo 2. Seja $n = a_r 10^r + a_{r-1}10^{r-1} + \cdots + a_2 10^2 + a_1 10 + a_0$ a representação do natural n na base 10. Como $10 \equiv -1\ (mod\ 11)$, logo, pela proposição 5.2(5), temos que

$$10^i = \begin{cases} 1\ (mod\ 11), & se\ i\ é\ par \\ -1\ (mod\ 11), & se\ i\ é\ ímpar. \end{cases}$$

Logo,

$$n = a_r 10^r + a_{r-1}10^{r-1} + \cdots + a_2 10^2 + a_1 10 + a_0 \ (mod\ 11)$$

e, portanto,

$$n \equiv (a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots)\ (mod\ 11).$$

Assim, um número natural é divisível por 11 se, e somente se, a diferença entre a soma dos algarismos de ordem par e a soma dos algarismos de ordem ímpar na sua representação decimal for divisível por 11.

■

O próximo exemplo estabelece uma regra muito popular nas primeiras séries do ensino básico, a *prova dos noves*.

Exemplo 5.9 [1]**.** A *prova dos noves* é um teste que se realiza nas quatro operações para detectar erros de contas. Suponhamos que efetuamos a multiplicação $a \cdot b$, obtendo um resultado c, e que na base 10, tenhamos

$$a = a_n a_{n-1} \ldots a_1 a_0, \quad b = b_m b_{m-1} \ldots b_1 b_0, \quad c = c_r c_{r-1} \ldots c_1 c_0.$$

Após ter posto os noves fora (observação 5.3) em $a_n + a_{n-1} + \cdots + a_1 + a_0$, obtém-se o algarismo a'. Fazendo o mesmo para b e c, obtemos os algarismos b' e c'. Efetua-se a multiplicação de $a' \cdot b'$ e põem-se os nove fora, obtendo c''. Se $c' \neq c''$, então, certamente, foi cometido um erro de operação. A justificativa é a seguinte:

$$c' \equiv c \equiv a \cdot b \equiv a' \cdot b' \equiv c''(mod\ 9)$$

com $0 \leq c' < 9$ e $0 \leq c'' < 9$.

Caso $c' = c''$, nado podemos afirmar quanto a exatidão da operação efetuada, mas podemos garantir que nossa conta tornou-se mais confiável por ter passado por um teste.

■

Exemplo 5.10. Já sabemos – exemplo 1.3 – que Leonard Euler descobriu que o quinto número de Fermat, $F_5 = 2^{2^5} + 1$, não é primo. Usando o conceito de congruência módulo m, vamos provar esse resultado. Com efeito, note que da igualdade $641 = 5 \cdot 2^7 + 1$, temos que $5 \cdot 2^7 \equiv -1\ (mod\ 641)$. Portanto, pela proposição 5.2(5), segue-se que

$$5^4 \cdot 2^{28} = (5 \cdot 2^7)^4 \equiv (-1)^4 = 1\ (mod\ 641).$$

Disso, e da igualdade $641 = 5^4 + 2^4$, temos que

$$2^{28} \cdot (5^4 + 2^4) \equiv 0\ (mod\ 641)$$

$$\underbrace{5^4 \cdot 2^{28}}_{\equiv 1 (mod\ 641)} + 2^{32} \equiv 0\ (mod\ 641)$$

$$1 + 2^{32} \equiv 0\ (mod\ 641)$$

$$2^{2^5} + 1 \equiv 0\ (mod\ 641),$$

o que mostra que $641 \mid F_5$.

■

Exemplo 5.11. Vamos mostrar que a recíproca da proposição 4.6 não é válida. Afirmamos que o número de Mersenne $M_{83} = 2^{83} - 1$ não é primo, apesar de 83 ser primo. De fato, temos que

$$2^8 = 256 \equiv 89\ (mod\ 167)$$

$$2^{16} \equiv 89^2 = 7921 \equiv 72\ (mod\ 167)$$

$$2^{32} \equiv 72^2 = 5184 \equiv 7\ (mod\ 167)$$

$$2^{64} \equiv 7^2 = 49\ (mod\ 167),$$

portanto, segue-se que

$$2^{83} = 2^{64}2^{16}2^3 \equiv 49 \cdot 72 \cdot 8 \equiv 1\ (mod\ 167).$$

Assim, $167 \mid M_{83}$.

■

Retomando o exemplo 5.3, notemos que de forma geral, pela divisão euclidiana, todo número inteiro n é congruente módulo m ao resto da divisão de n por m, ou seja, congruente módulo m a um dos números 0, 1, 2, …, $m-1$. É claro que dois desses números distintos são incongruentes módulo m, portanto para achar o resto da divisão de um número n por m, devemos encontrar o número natural $r \in \{0, 1, 2, \dots, m-1\}$ tal que $n \equiv r \ (mod\ m)$.

Quando $h, k \in \mathbb{Z}$ são tais que $h \equiv k \ (mod\ m)$, dizemos que k é um *resíduo* de h módulo m.

Definição 5.2. *Chamaremos de "sistema completo de resíduos módulo m" a todo conjunto de números inteiros cujos restos pela divisão por m são os números 0, 1, 2, ..., $m-1$, sem repetição e numa ordem qualquer.*

Por essa definição, todo sistema completo de resíduos modulo m possui exatamente m elementos. Também, fica claro que se $a_1, \dots, a_m$ são m números inteiros, dois a dois incongruentes módulo m, então eles formam um sistema completo de resíduos módulo m. De fato, os restos da divisão dos a_i por m são dois a dois distintos, o que implica que são os números 0, 1, 2, …, $m-1$ em alguma ordem. Em suma, para mostrar que um conjunto $R = \{r_1, \dots, r_s\}$ é um sistema completo de resíduos módulo m, basta verificar se as duas condições abaixo são verdadeiras:

(1) $r_i \not\equiv r_j \ (mod\ m)$ para $i \neq j$;

(2) para todo inteiro n existe um r_i tal que $n \equiv r_i \ (mod\ m)$, ou seja, algum r_i é um resíduo de n módulo m.

Exemplo 5.12. *Mostre que se $R = \{r_1, \dots, r_m\}$ é um sistema completo de resíduos módulo m e $\boldsymbol{a}$ e $\boldsymbol{b}$ são inteiros tais que $(a, m) = 1$, então o conjunto*

$$R' = \{ar_1 + b, ar_2 + b, \dots, ar_m + b\}$$

também é um sistema completo de resíduos módulo m.

Demonstração: Vamos verificar que dois elementos distintos de R' são incongruentes módulo m. A prova é por contradição, suponhamos que

$$ar_i + b \equiv ar_j + b \ (mod\ m), \text{ para algum } i \neq j.$$

Pela proposição 6.2(4), temos que $ar_i \equiv ar_j \ (mod\ m)$, mas como por hipótese $(a, m) = 1$, a proposição 6.2(6) garante que $r_i \equiv r_j \ (mod\ m)$. Isso implica, uma vez que R é um sistema

completo de resíduos módulo m, que $i = j$; o que é absurdo. Logo, $ar_i + b \not\equiv ar_j + b\ (mod\ m)$, para todo $i \neq j$.

Ainda devemos mostrar que todo inteiro n é resíduo módulo m de algum elemento de R'. Com efeito, do fato de R ser um conjunto completo de resíduos módulo m, temos que $n \equiv r_i\ (mod\ m)$, e uma vez que r_i é congruente módulo m a exatamente um elemento de R', então $n \equiv ar_j + b\ (mod\ m)$, o que conclui a demonstração.

■

Com a notação de congruência, suas propriedades básicas e o conceito de sistema completo de resíduos módulo m, insere-se dentro do conjunto dos números inteiros uma salutar aritmética, conhecida na literatura como *Aritmética de Restos Módulo m*. É nisso que reside a riqueza da notação, e a eficiência da teoria que Gauss propôs: buscar resultados acerca dos números inteiros a partir do estudo de seus resíduos módulo m.

Como exemplo adicional, fornecemos um problema que nos fornece uma salutar simplificação computacional que a notação de congruência nos oferece.

Exemplo 5.13. *Mostre que nenhum número da forma* $8k + 7$, $k \in \mathbb{Z}$, *pode ser escrito como a soma dos quadrados de três inteiros.*

Solução: Seja $n = 8k + 7$, $k \in \mathbb{Z}$. Queremos mostrar que não existe inteiros a, b e c tais que $n = a^2 + b^2 + c^2$. Usando a notação de congruência, temos que $n \equiv 7\ (mod\ 8)$. Se fosse $n = a^2 + b^2 + c^2$, então teríamos $a^2 + b^2 + c^2 \equiv 7\ (mod\ 8)$.

Vamos agora analisar que valores o quadrado de um número inteiro pode assumir módulo 8. Se u for um inteiro, então u é congruente a um único elemento r do conjunto $R = \{0, 1, 2, 4, 5, 6, 7\}$, que é um sistema completo de resíduos módulo 8. Então,

$$u^2 \equiv r^2\ (mod\ 8).$$

Verificamos imediatamente:

$$\begin{aligned}
r = 0 &\quad \Rightarrow \quad u^2 \equiv 0\ (mod\ 8)\\
r = 1 &\quad \Rightarrow \quad u^2 \equiv 1\ (mod\ 8)\\
r = 2 &\quad \Rightarrow \quad u^2 \equiv 4\ (mod\ 8)\\
r = 3 &\quad \Rightarrow \quad u^2 \equiv 1\ (mod\ 8)\\
r = 4 &\quad \Rightarrow \quad u^2 \equiv 0\ (mod\ 8)\\
r = 5 &\quad \Rightarrow \quad u^2 \equiv 1\ (mod\ 8)\\
r = 6 &\quad \Rightarrow \quad u^2 \equiv 4\ (mod\ 8)\\
r = 7 &\quad \Rightarrow \quad u^2 \equiv 1\ (mod\ 8)
\end{aligned}$$

Portanto, não há maneira de combinar os quadrados de a^2, b^2 e c^2 de modo a produzir um número congruente a 7 módulo 8. De fato, pelo menos um desses números deve ser congruente a 4 módulo 8: se todos eles fossem congruentes a 0 ou 1, a soma seria congruente a, no máximo, 3 módulo 8. Se $a^2 \equiv 4\ (mod\ 8)$, então, claramente não podemos tomar b^2 e c^2 congruentes a 0 ou 1, pois a soma seria congruente a, no máximo, 6 módulo 8. Finalmente, se tomarmos também $b^2 \equiv 4\ (mod\ 8)$, então a soma $a^2 + b^2 \equiv 0\ (mod\ 8)$. Como não há número cujo quadrado seja congruente a 7 módulo 8, temos que $a^2 + b^2 + c^2 \not\equiv 7\ (mod\ 8)$.

■

A proposição a seguir nos fornece algumas propriedades adicionais das congruências.

Proposição 5.4. *Sejam* $a, b \in \mathbb{Z}$ *e* $m, n, m_1, \dots, m_r$ *inteiros maiores do que* 1. *Temos que*

(a) *se* $a \equiv b\ (mod\ m)$ *e* $n \mid m$, *então* $a \equiv b\ (mod\ n)$;

(b) $a \equiv b\ (mod\ m_i)$, *para todo* $i = 1, 2, \dots, r \iff a \equiv b\ (mod\ [m_1, \dots, m_r])$;

(c) *se* $a \equiv b\ (mod\ m)$, *então* $(a, m) = (b, m)$.

Demonstração:

$(\boldsymbol{a})$ Se $a \equiv b\ (mod\ m)$, então $m \mid (a - b)$. Como $n \mid m$, por transitividade da divisibilidade, temos $n \mid (a - b)$, ou seja, $a \equiv b\ (mod\ n)$.

$(\boldsymbol{b})$ Se $a \equiv b\ (mod\ m_i)$, para todo $i = 1, 2, \dots, r$, então $m_i \mid (a - b)$, para todo i. Uma vez que $a - b$ é múltiplo de m_i, tem-se que $[m_1, \dots, m_r]$ divide $(a - b)$. Portanto,

$$a \equiv b\ (mod\ [m_1, \dots, m_r]).$$

A recíproca é imediata, e decorre da definição de mmc.

$(\boldsymbol{c})$ Se $a \equiv b\ (mod\ m)$, então $m \mid (a - b)$ e, portanto, $b = a + qm$ com $q \in \mathbb{Z}$. Logo, pelo lema de Euclides (proposição 3.2), temos que

$$(a, m) = (a + qm, m) = (b, m).$$

■

O exemplo a 5eguir é uma aplicação direta da proposição anterior.

Exemplo 5.14. *Encontre o menor múltiplo positivo de* 7 *que deixa resto* 1 *quando dividido por* $2, 3, 4, 5$ e 6.

Solução: queremos encontrar o menor inteiro positivo x, tal que

$$7x \equiv 1\ (mod\ 2)$$

$$7x \equiv 1\ (mod\ 3)$$

$$7x \equiv 1\ (mod\ 4)$$

$$7x \equiv 1\ (mod\ 5)$$
$$7x \equiv 1\ (mod\ 6).$$

Pela proposição 5.4(b), uma vez que $[2,3,4,5,6,] = 60$, x deve satisfazer a congruência $7x \equiv 1\ (\ mod\ [2,3,4,5,6,])$ e reciprocamente. Logo, o problema se resume a calcularmos o menor inteiro positivo x tal que $7x \equiv 1\ (mod\ 60)$. Ora, resolver tal congruência é equivalente a resolver a equação diofantina $7x - 60y = 1$. O par $(x_0, y_0) = (-17, -2)$ é uma solução particular dessa equação. Portanto, a solução geral é dada por $x = -17 + 60t$ e $y = -2 - 7t$, com $t \in \mathbb{Z}$. Finalmente, o menor valor positivo de x de modo que exista solução para equação diofantina $7x - 60y = 1$, é quando tomamos $t = 1$, isto é, $x = -17 + 60 \cdot 1 = 43$. Então, o número procurado é $7x = 7 \cdot 43 = 301$.

■

5.2 TRÊS TEOREMAS FUNDAMENTAIS

O objetivo desta seção é discorrer acerca de três relevantes resultados, quais sejam, o Teorema de Wilson, o Pequeno Teorema de Fermat e o Teorema de Euler. Mas antes precisamos de uma abordagem preliminar acerca de alguns apontamentos que nos auxiliarão nos resultados doravante demonstrados.

Sejam a, b e m inteiros tais que $m \geq 1$ e $(a, m) = d$. Pelo exemplo 5.14, já sabemos que encontrar os valores inteiros x que satisfazem a congruência $ax \equiv b\ (mod\ m)$, equivale a resolver a equação diofantina $ax - my = b$. Pelo teorema 3.5, temos que se $d \nmid b$, então essa equação não possui nenhuma solução, isto implica que não existe solução para congruência $ax \equiv b\ (mod\ m)$. Do contrário, se $d \mid b$, então a congruência $ax \equiv b\ (mod\ m)$ possui exatamente d soluções incongruentes módulo m. Com efeito, sejam os pares (x_0, y_0), (x_1, y_1), (x_2, y_2) soluções da equação diofantina $ax - my = b$. Usando novamente o Teorema 3.5, vamos tentar descobrir sob que condições

$$x_1 = x_0 - (m/d)t_1 \quad \text{e} \quad x_2 = x_0 - (m/d)t_2$$

são congruentes módulo m.

Para isso, note que se $x_1 \equiv x_2\ (mod\ m)$, então $x_0 - (m/d)t_1 \equiv x_0 - (m/d)t_2\ (mod\ m)$. O que implica $(m/d)t_1 \equiv (m/d)t_2\ (mod\ m)$. Como $(m/d) \mid m$, temos que

$$(m/d\ , m) = m/d;$$

usando o resultado da proposição 5.3, temos que

$$\frac{(m/d)}{(m/d)} t_1 \equiv \frac{(m/d)}{(m/d)} t_2\ \left(mod\ \frac{m}{(m/d)}\right) \Longrightarrow t_1 \equiv t_2\ (mod\ d).$$

Isso nos mostrar que soluções incongruentes serão obtidas ao tomarmos $x_1 = x_0 - (m/d)t_1$, onde t_1 percorre um sistema completo de resíduos módulo d. Assim, $ax \equiv b\ (mod\ m)$ possui exatamente d soluções incongruentes módulo m, toda vez que $(a, m) \mid b$.

Uma solução x_0 da congruência $ax \equiv b\ (mod\ m)$ é chamada de *solução única módulo m* quando qualquer outra solução x_1 for congruente a x_0 módulo m.

Definição 5.3. *Uma solução* $\overline{\boldsymbol{a}}$ *da congruência* $ax \equiv 1\ (mod\ m)$ *é chamada de um inverso de* $\boldsymbol{a}$ *módulo* m.

Se $(a, m) = 1$, então a congruência $ax \equiv 1\ (mod\ m)$ possui uma única solução módulo m, ou seja, $\boldsymbol{a}$ possui um único inverso módulo m. O resultado a seguir nos informa sob que condições um inteiro $\boldsymbol{a}$ é inverso de ele mesmo módulo p, onde p é um número primo.

Proposição 5.5. *Se* p *é um número primo. O inteiro positivo* $\boldsymbol{a}$ *é o seu próprio inverso módulo* p *se, e só se* $a \equiv 1\ (mod\ p)$ *ou* $a \equiv -1\ (mod\ p)$.

Demonstração: Se a é o seu próprio inverso módulo p, temos que $a^2 \equiv 1\ (mod\ p)$. Daí, $p \mid (a^2 - 1)$, ou seja, $p \mid (a + 1)(a - 1)$. Como p é primo, temos que $p \mid (a - 1)$ ou $p \mid (a + 1)$, o que implica $a \equiv 1\ (mod\ p)$ ou $a \equiv -1\ (mod\ p)$. A recíproca é imediata.

■

5.2.1 TEOREMA DE WILSON

O resultado que demonstraremos a seguir é atribuído a Wilson (1741 – 1793), mas na realidade Hefez [6] esclarece que este resultado foi demonstrado a primeira vez por J. L. Lagrange (1736 – 1813).

Para fixa a ideia empregada na demonstração do Teorema de Wilson, exemplifiquemos o resultado para o primo $p = 17$.

Dentre os números $1, 2, \dots, 16$, a proposição 5.5 garante que 1 e 16 são os únicos números que são seus próprios inversos módulo 17. A proposição 5.5 garante também que nenhum dos números $2, 3, \dots, 15$ é congruente a 1 ou a -1 módulo 17. Ora, como todos os números $2, 3, \dots, 15$ são coprimos, temos que cada um deles possui um único inverso módulo 17. Portanto, podemos agrupá-lo em 7 pares $(7 = (17 - 3)/2)$, da seguinte forma:

$$2 \cdot 9 \equiv 1\ (mod\ 17)$$

$$3 \cdot 6 \equiv 1 \ (mod\ 17)$$
$$4 \cdot 13 \equiv 1 \ (mod\ 17)$$
$$5 \cdot 7 \equiv 1 \ (mod\ 17)$$
$$8 \cdot 15 \equiv 1 \ (mod\ 17)$$
$$10 \cdot 12 \equiv 1 \ (mod\ 17)$$
$$11 \cdot 14 \equiv 1 \ (mod\ 17).$$

Multiplicando membro a membro todas estas congruências, obtemos

$$2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 15 \equiv 1 \ (mod\ 17).$$

Multiplicando ambos os membros desta congruência por 16, temos que

$$2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 15 \cdot 16 \equiv 16 \equiv -1 \ (mod\ 17).$$

Portanto, $(17-1)! \equiv -1 \ (mod\ 17)$.

Já estamos em condições de demonstrar o seguinte resultado:

Teorema 5.1 (de Wilson). *Um número p é primo se, e somente se,* $(p-1)! \equiv -1 \ (mod\ p)$.

Demonstração: Trivialmente, o resultado é válido para $p = 2$. Como $ax \equiv 1 \ (mod\ p)$ tem uma única solução no conjunto $\{1, 2,\ 3, \ldots, p-1\}$ e como, destes elementos, somente 1 e $p-1$ são seus próprios inversos módulo p podemos agrupar $2,\ 3, \ldots, p-2$ em $(p-3)/2$ pares cujo o produto seja congruente a 1 módulo p. Se multiplicarmos estas congruências, membro a membro, teremos que $2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1 \ (mod\ p)$. Multiplicando-se ambos os lados desta congruência por $p-1$, teremos

$$2 \cdot 3 \cdot \ldots \cdot (p-2)(p-1) \equiv p-1 \equiv -1 \ (mod\ p),$$

ou seja,

$$(p-1)! \equiv -1 \ (mod\ p).$$

Reciprocamente, suponhamos $(p-1)! \equiv -1 \ (mod\ p)$, isto é, $p \mid (p-1)! + 1$, e que p não seja primo. Ou seja $p = r \cdot s$, $1 < r < p$ e $1 < s < p$. Nessas condições, $r \mid (p-1)!$ e sendo r um divisor de p, temos que $r \mid (p-1)! + 1$, o que implica $r \mid 1$, o que é absurdo, uma vez que $r > 1$. Assim, se p satisfaz a congruência $(p-1)! \equiv -1 \ (mod\ p)$, p é necessariamente um número primo.

■

O Teorema de Wilson é de certa forma extraordinário, enfatiza Fernandes [9]. Ele nos fornece uma condição necessária e suficiente para que um inteiro positivo seja primo. Todavia, a caracterização de primos por meio deste teorema não é prática, esclarece

Ribemboim [4]. E ainda completa, não se conhece um algoritmo, a não ser o da definição, para calcular rapidamente $n!$.

A seguir, vamos a duas aplicações do Teorema de Wilson:

Exemplo 5.15 *Encontre o menor resíduo positivo de* $8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13$ *módulo* 7.

Solução: Para achar o menor resíduo positivo de $8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13$, primeiramente notemos que

$$8 \equiv 1 \ (mod\ 7)$$
$$9 \equiv 2 \ (mod\ 7)$$
$$10 \equiv 3 \ (mod\ 7)$$
$$11 \equiv 4 \ (mod\ 7)$$
$$12 \equiv 5 \ (mod\ 7)$$
$$13 \equiv 6 \ (mod\ 7),$$

logo, multiplicando membro a membro todas estas congruências, temos que

$$8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \ (mod\ 7).$$

Pelo Teorema de Wilson, $6! \equiv -1 \equiv 6 \ (mod\ 7)$, então

$$8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \equiv 6 (mod\ 7).$$

Assim, o resultado é 6.

■

Exemplo 5.16. *Sejam* p *um número primo e* $m, n \in \mathbb{N} \cup \{0\}$ *tais que* $m + n = p - 1$. *Então* $m!\, n! \equiv (-1)^{n+1} \ (mod\ \ p)$.

Solução [1]**:** Seja $0 \leq n \leq p - 1$. Temos que

$$(p - n) \cdots (p - 2)(p - 1) \equiv (-1)^n n! \ (mod\ \ p).$$

Pondo $m = p - 1 - n$, temos que

$$(p - 1)! \equiv 1 \cdot 2 \cdots (p - 1 - n)(p - n) \cdots (p - 1) = m!\, (-1)^n n! \ \ (mod\ p).$$

Pela congruência acima e pelo Teorema de Wilson, temos que

$$m!\, n! \equiv (p - 1)!\, (-1)^n \equiv (-1)^{n+1} \ (mod\ \ p).$$

■

5.2.2 PEQUENO TEOREMA DE FERMAT

Numa carta dirigida ao matemático amador Frénicle de Bessey, datada de 18 de outubro de 1640, Fermat escreveu o seguinte:

> Parece-me que depois disto lhe devo dizer qual a fundação na qual assento todas as demonstrações que dizem respeito a progressões geométricas, nomeadamente:
>
> Todo o número primo mede infalivelmente uma das potências menos a unidade em qualquer progressão, e o expoente dessa potência é um divisor do dado número primo menos um; e depois de encontrada a primeira potência que satisfaz essa condição, todas aqueles que o expoente são múltiplos do primeiro satisfazem essa mesma condição (FERMAT,1640).

Em outras palavras:

Teorema 5.2 (Pequeno Teorema de Fermat). *Se p é um número primo e $\boldsymbol{a}$ é um inteiro não divisível por p, então $a^{p-1} \equiv 1\ (mod\ p)$.*

Vale a pena esclarecer [12]: o adjetivo pequeno não deve aqui ser tomado como algo de importância irrelevante. Ao contrário, esse é um dos resultados mais fecundos de Fermat. O termo "pequeno teorema" é usado na literatura apenas para distinguir tal teorema do Último Teorema de Fermat , que muitas vezes é qualificado como "Grande".

Daremos aqui duas demonstrações do Pequeno Teorema de Fermat. Nosso intuito é ilustrar que mesmo em caminhos distintos podemos chegar ao mesmo resultado; e que tais caminhos podem oferecer diferentes perspectivas. Isto é um pensamento que deve perdurar na cabeça de quem estuda matemática e devemos, como professores, difundi-lo entre os nossos educandos.

Com o intuito de ilustrar a ideia usada na primeira demonstração, vamos provar o resultado para um caso particular. Digamos, $p = 11$ e $a = 5$. Logo temos:

$$
\begin{array}{ll}
1 \cdot 5 \equiv\ \ 5\ (mod\ 11) & \quad 6 \cdot 5 \equiv 8\ (mod\ 11) \\
2 \cdot 5 \equiv 10\ (mod\ 11) & \quad 7 \cdot 5 \equiv 2\ (mod\ 11) \\
3 \cdot 5 \equiv\ \ 4\ (mod\ 11) & \quad 8 \cdot 5 \equiv 7\ (mod\ 11) \\
4 \cdot 5 \equiv\ \ 9\ (mod\ 11) & \quad 9 \cdot 5 \equiv 1\ (mod\ 11) \\
5 \cdot 5 \equiv\ \ 3\ (mod\ 11) & \quad 10 \cdot 5 \equiv 6\ (mod\ 11)
\end{array}
$$

Note que 11 não divide nenhum produto do primeiro membro das congruências acima. Observe que todos eles são incongruentes módulo 11. Logo, como nenhum é congruente a zero módulo 11 e todos são incongruentes módulo 11, eles devem ser congruentes a diferentes números dentre $1, 2, 3, \dots, 10$. Veja que todos estes números aparecem, sem repetição, no membro das congruências acima. Multiplicando, membro a membro, estas congruências, obtemos

$$(1 \cdot 5)(2 \cdot 5) \cdots (10 \cdot 5) \equiv 5 \cdot 10 \cdot 4 \cdot 9 \cdot 3 \cdot 8 \cdot 2 \cdot 7 \cdot 1 \cdot 6 \ (mod\ 11)$$

e, portanto,

$$5^{10} \cdot 10! \equiv 10! \ (mod\ 11).$$

Como $(10!, 11) = 1$, pela proposição 5.2(6), temos que

$$5^{10} \equiv 1 (mod\ 11)$$

o que mostra a validade do teorema para $p = 11$ e $a = 5$.

Com essa ideia em mente, vamos à primeira demonstração:

Demonstração 1 [5]**:** sabemos que o conjunto formado pelos p números $0, 1, \dots, p-1$ constitui um sistema completo de resíduos módulo p. Isto significa que qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado em correspondência biunívoca com um subconjunto de $\{0, 1, \dots, p-1\}$. Vamos, agora, considerar os números $a, 2a, 3a, \dots, (p-1)a$. Como $(a, p) = 1$, nenhum desses ia, $1 \leq i \leq p-1$ é divisível por p, ou seja, nenhum é congruente a zero módulo p. Quaisquer dois deles são incongruentes módulo p, pois $aj \equiv ak \ (mod\ p)$ implica $j \equiv k \ (mod\ p)$ e isso só é possível se $j = k$, uma vez que ambos são positivos e menores do que p. Temos, portanto, um conjunto $p-1$ elementos incongruentes módulo p e não-divisíveis por p. Logo, cada um deles é congruente a exatamente um dentre os elementos $0, 1, \dots, p-1$. Se multiplicarmos estas congruências, membro a membro, teremos:

$$a(2a)(3a) \cdots (p-1)a \equiv 1.2.3. \cdots (p-1) (mod\ p),$$

ou seja

$$a^{p-1}(p-1)! \equiv (p-1)! \ (mod\ p).$$

Mas como $(p-1)!$ e p são coprimos, podemos cancelar o fator $(p-1)!$ Em ambos os lados desta última congruência, obtendo

$$a^{p-1} \equiv 1 (mod\ p),$$

como queríamos demonstrar.

■

Na segunda demonstração, procederemos por indução:

Demonstração 2: Vamos demonstrar que dado um p primo, tem-se que p divide o número $a^p - a$, para todo $a \in \mathbb{Z}$, ou seja, $a^p \equiv a\ (mod\ p)$. Note que o resultado é obvio para $p = 2$. Suponhamos que p seja um primo ímpar. Nesse caso, claramente basta mostrar o resultado para $a \geq 0$. Para isso vamos provar o resultado por indução sobre a. O resultado vale claramente para $a = 0$, pois $p \mid 0$. Supondo o resultado válido para a, iremos prová-lo para $a + 1$. Pela fórmula do binômio de Newton, temos que

$$(a+1)^p - (a+1) = a^p - a + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a.$$

Pela hipótese de indução e do fato que $\binom{p}{i} \equiv 0\ (mod\ p)$ para todo $i = 1, \ldots, p-1$ (exemplo 4.5), tem-se que o segundo membro da igualdade anterior é congruente a 0 módulo p. Donde concluímos que $a^p \equiv a\ (mod\ p)$. Finalmente, por hipótese, $(a, p) = 1$, então

$$a^{p-1} \equiv 1\ (mod\ p)$$

que é o resultado que queríamos demonstrar.

■

O uso de congruências para calcular restos é consideravelmente simplificado se encontrarmos expoentes que tornem certa potência congruente a 1. É isso que torna o resultado de Fermat um dos mais importantes da teoria elementar dos números. Vamos a algumas aplicações do Pequeno Teorema de Fermat.

Exemplo 5.17. *Encontre o resto da divisão de* $2^{100\,000}$ *por 17.*

Solução: Como 17 é primo e $(17,2) = 1$, temos, pelo pequeno teorema de Fermat, que $2^{16} \equiv 1\ (mod\ 17)$. Mas $100\,000 = 6250 \cdot 16$ e, portanto,

$$2^{100\,000} = (2^{16})^{6250} \equiv 1^{6250} \equiv 1\ (mod\ 17).$$

Assim, o resto da divisão de $2^{100\,000}$ por 17 é 1.

■

Exemplo 5.18. *Se p e q são primos distintos, prove que pq divide $p^{q-1} + q^{p-1} - 1$.*

Solução: Note que $(p, q) = 1$, pois p e q são primos distintos. Então, pelo pequeno teorema de Fermat

$$p^{q-1} - 1 \equiv 0\ (mod\ q) \text{ e } q^{p-1} - 1 \equiv 0\ (mod\ p).$$

Mas, como $q \mid q^{p-1}$ e $p \mid p^{q-1}$, temos que

$$p^{q-1} + q^{p-1} - 1 \equiv 0\ (mod\ q) \text{ e } p^{q-1} + q^{p-1} - 1 \equiv 0\ (mod\ p).$$

Assim, pela proposição 6.4(b), tem-se

$$p^{q-1} + q^{p-1} - 1 \equiv 0 \ (mod\ [p,q]) \Longrightarrow p^{q-1} + q^{p-1} - 1 \equiv 0 \ (mod\ pq).$$

E, portanto,

$$pq \mid p^{q-1} + q^{p-1} - 1 \ .$$

■

Exemplo 5.19. *Mostre que* $13 \mid 2^{70} + 3^{70}$.

Solução: Por Fermat, $2^{12} \equiv 1 \ (mod\ 13)$, logo $2^{60} \equiv 1 \ (mod\ 13)$. Mas $2^5 \equiv 6 \ (mod\ 13)$, e portanto, $2^{10} \equiv 36 \equiv -3 \ (mod\ 13)$. Logo, $2^{60}2^{10} \equiv -3(mod\ 13)$, isto é,

$$2^{70} \equiv -3(mod\ 13). \qquad (5.1)$$

Sabendo-se que $3^3 \equiv 1(mod\ 13)$, donde $3^{69} \equiv 1(mod\ 13)$. Como $3 \equiv 3(mod\ 13)$, temos que

$$3^{70} \equiv 3(mod\ 13). \qquad (5.2)$$

Assim, somando-se, membro a membro, as congruências (5.1) e (5.2), obtemos

$$2^{70} + 3^{70} \equiv 0(mod\ 13) \Leftrightarrow 13 \mid 2^{70} + 3^{70}. \qquad ■$$

5.2.3 TEOREMA DE EULER

Estudaremos agora um importante resultado, devido a Euler, que na verdade é uma generalização do pequeno teorema de Fermat. O teorema de Euler e suas consequências são fundamentais na teoria elementar dos números. Entre suas aplicações, destaca-se seu uso no estudo de sistemas criptográficos, entre eles o sistema RSA, de vital importância na segurança das transações bancárias pela internet. Para mais detalhes, consulte o Capítulo 13, de [1].

Antes de enunciar e demonstrar o teorema de Euler é necessário introduzir alguns conceitos e resultados preliminares.

Se n é um inteiro positivo, a *função ϕ de Euler*, denotada por $\phi(n)$, é definida como sendo o número de inteiros positivos menores do que ou iguais n que são relativamente primos com n.

Definição 5.4. *Um "sistema reduzido de resíduos módulo m" é um conjunto de $\phi(m)$ inteiros $r_1, r_2, \dots, r_{\phi(m)}$, tais que cada elemento do conjunto é relativamente primo com m, e se $i \neq j$, então $r_i \not\equiv r_j \ (mod\ m)$.*

Sabemos que o conjunto $R_{10} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ é um sistema completo de resíduos módulo 10, portanto $R'_{10} = \{1, 3, 7, 9\}$ é um sistema reduzido de resíduos módulo 10. Note que para formar o conjunto R'_{10}, retiramos do conjunto R_{10} os elementos que não são relativamente primos com 10. Em geral, a fim de se obter um sistema reduzido de resíduos módulo m, basta retirar os elementos do sistema completo que não são coprimos com m.

Proposição 5.5. *Seja* $\boldsymbol{a}$ *um inteiro positivo tal que* $(a, m) = 1$. *Se* $r_1, r_2, \dots, r_{\phi(m)}$ *é um sistema reduzidos módulo* m, *então* $ar_1, ar_2, \dots, ar_{\phi(m)}$ *é, também, um sistema reduzido de resíduos módulo* m.

Demonstração [5]**:** Como na sequência $ar_1, ar_2, \dots, ar_{\phi(m)}$ temos $\phi(m)$, devemos mostrar que todos eles são relativamente primos com m e, dois a dois, incongruentes módulo m. Como $(a, m) = 1$ e $(r_i, m) = 1$, temos que $(ar_1, m) = 1$. Logo, nos resta mostrar que se $ar_i \not\equiv ar_j \ (mod\ m)$ se $i \neq j$. Mas, como $(a, m) = 1$, de $ar_i \equiv ar_j \ (mod\ m)$ temos que $r_i \equiv r_j \ (mod\ m)$ se $i = j$, uma vez que $r_1, r_2, \dots, r_{\phi(m)}$ é um sistema reduzido de resíduo módulo m, o que conclui a demonstração.

■

Vamos agora ilustrar a ideia empregada na demonstração do teorema de Euler, constatando sua validade para um caso particular. Sejam $m = 10$ e $a = 3$. Sabemos que o conjunto $\{1, 3, 7, 9\}$ é um sistema reduzido de resíduos módulo 10. Considere o conjunto $\{3 \cdot 1, 3 \cdot 3, 3 \cdot 7, 3 \cdot 9\}$. Pela proposição 5.5, este conjunto também consiste em um sistema reduzido de resíduos módulo 10. Isto significa que cada um dos elementos de $\{3 \cdot 1, 3 \cdot 3, 3 \cdot 7, 3 \cdot 9\}$ é congruente módulo 10 a exatamente um dos elementos de $\{1, 3, 7, 9\}$. Temos, então, que

$$3 \cdot 1 \equiv 3 \ (mod\ 10)$$
$$3 \cdot 3 \equiv 9 \ (mod\ 10)$$
$$3 \cdot 7 \equiv 1 \ (mod\ 10)$$
$$3 \cdot 9 \equiv 7 (mod\ 10).$$

Multiplicando-se, membro a membro, obtemos:

$$3^4(1 \cdot 3 \cdot 7 \cdot 9) \equiv (1 \cdot 3 \cdot 7 \cdot 9)(mod\ 10).$$

Segue que

$$3^4 \equiv 1 \ (mod\ 10),$$

pois $(1 \cdot 3 \cdot 7 \cdot 9, 10) = 1$. Provamos que $3^{\phi(10)} \equiv 1\ (mod\ 10)$, uma vez que $\phi(10) = 4$. Vamos demonstrar o teorema de Euler:

Teorema 5.3 (de Euler). *Se m é um inteiro positivo e* $\boldsymbol{a}$ um inteiro com $(a, m) = 1$, então

$$a^{\phi(m)} \equiv 1\ (mod\ m).$$

Demonstração: se $(a, m) = 1$ e $\{r_1, r_2, \dots, r_{\phi(m)}\}$ é um sistema reduzido de resíduo módulo m, então, pela proposição 5.5, o conjunto $\{ar_1, ar_2, \dots, ar_{\phi(m)}\}$ constitui um sistema reduzido de resíduos módulo m. Isto nos diz que, cada ar_i é congruente a exatamente um dos r_j, $1 \leq j \leq \phi(m)$, e portanto

$$ar_1.ar_2 \cdots ar_{\phi(m)} \equiv r_1.r_2 \cdots r_{\phi(m)}\ (mod\ m),$$

ou seja

$$a^{\phi(m)}(r_1.r_2 \cdots r_{\phi(m)}) \equiv (r_1.r_2 \cdots r_{\phi(m)})\ (mod\ m),$$

o que implica que

$$a^{\phi(m)} \equiv 1\ (mod\ m)$$

uma vez que $\left(\prod_{i=1}^{\phi(m)} r_i\ , m\right) = 1$.

■

Note que quando p é primo, $\phi(p) = p - 1$. Então para $m = p$ o teorema acima é uma generalização o pequeno teorema de Fermat.

Para aplicar de forma eficiente o teorema de Euler é necessário saber calcular $\phi(m)$, vamos discorrer acerca disso a seguir.

Proposição 5.6. *Sejam* $m', m \in \mathbb{N}$ *tais que* $(m', m) = 1$, *então* $\phi(m \cdot m') = \phi(m)\phi(m')$.

Demonstração [6]**:** O resultado é trivial para $m = 1$ ou $m' = 1$. Portanto, vamos supor que $m > 1$ e $m' > 1$. Considere a seguinte tabela formada pelos números naturais de 1 até $m \cdot m'$:

$$\begin{array}{ccccccc} 1 & 2 & \cdots & k & \cdots & m' \\ m'+1 & m'+2 & \cdots & m'+k & \cdots & 2m' \\ \vdots & \vdots & & \vdots & & \vdots \\ (m-1)m'+1 & (m-1)m'+2 & \cdots & (m-1)m'+k & \cdots & m \cdot m' \end{array}$$

Como se tem que

$$(t, m \cdot m') = 1 \Leftrightarrow (t, m') = (t, m) = 1,$$

para calcular $\phi(m \cdot m')$, devemos determinar os inteiros na tabela acima que são simultaneamente primos com m e m'. Com efeito, note que se o primeiro elemento de uma coluna não for primo com m', então todos os elementos da coluna não o são também. Portanto, os elementos primos com m' estão necessariamente nas colunas restantes que são em número $\phi(m')$, cujos elementos são primos com m', como é fácil verificar. Vejamos agora quais são os elementos primos com m em cada uma dessas colunas. O conjunto $\{k, m' + k, \dots, (m-1)m' + k\}$ forma um sistema completo de resíduos módulo m, pois $(m, m') = 1$; e, portanto, $\phi(m)$ desses elementos são primos com m. Assim, o número de elementos simultaneamente primos com m' e m é $\phi(m)\phi(m')$.

■

Esta última proposição afirma que a função ϕ de Euler é multiplicativa.

Seja p um número primo e r um número natural. Queremos calcular $\phi(p^r)$. Como de 1 até p^r, temos p^r números naturais, então excluindo entre esses números os que não são primos com p^r, ou seja, todos os múltiplos de p (que são precisamente $p, 2p, \dots, p^{r-1}p$, cujo o número é p^{r-1}), concluímos que

$$\phi(p^r) = p^r - p^{r-1} = p^r\left(1 - \frac{1}{p}\right). \tag{5.3}$$

Com esse resultado, fica fácil determinar uma expressão para $\phi(m)$. Com efeito, seja

$$m = \prod_{i=1}^{r} {p_i}^{a_i}$$

a decomposição de m em fatores primos, com $a_i \in \mathbb{N}$ Logo, usando a expressão (5.3), juntamente com a proposição 5.6, temos finalmente que:

$$\phi(m) = \phi\left(\prod_{i=1}^{r} {p_i}^{a_i}\right) = \prod_{i=1}^{r} \phi({p_i}^{a_i}) = \prod_{i=1}^{r}\left[{p_i}^{a_i}\left(1 - \frac{1}{p_i}\right)\right],$$

isto é,

$$\phi(m) = \left(\prod_{i=1}^{r} {p_i}^{a_i}\right)\left(\prod_{i=1}^{r}\left[\left(1 - \frac{1}{p_i}\right)\right]\right). \tag{5.4}$$

A expressão (5.4) pode ser reescrita como se segue:

$$\phi\left(\prod_{i=1}^{r} {p_i}^{a_i}\right) = \left(\prod_{i=1}^{r} {p_i}^{a_i - 1}\right)\left(\prod_{i=1}^{r}(p_i - 1)\right). \tag{5.5}$$

Apresentamos a seguir, duas aplicações do teorema de Euler:

Exemplo 5.20. *Encontre o resto da divisão de* 3^{100} *por 34.*

Solução: Como $(3,34) = 1$, pelo teorema de Euler, temos que $3^{\phi(34)} \equiv 1\ (mod\ 34)$. Pela expressão (5.5), $\phi(34) = \phi(2 \cdot 17) = 2^0 \cdot 17^0(2-1)(17-1) = 16$. Logo,

$$3^{16} \equiv 1\ (mod\ 34).$$

Assim, $3^{100} = 3^{16\times 6+4} \equiv 3^4(3^{16})^6 \equiv 3^4.1^6 \equiv 13\ (mod\ 34)$, donde 13 é o resto da divisão *de* 3^{100} por 34.

■

Exemplo 5.21. *Mostre que existem infinitos números da forma* $200\ldots01$*(com mais de dois zeros) que é múltiplo de 2001.*

Solução [17]**:** Note que $2\underbrace{00\ldots0}_{n\ zeros}1 = 2 \cdot 10^{n+1} + 1$. Logo, para resolver o problema basta encontrarmos infinitos valores $n > 2$ para os quais

$$2 \cdot 10^{n+1} + 1 \equiv 0\ (mod\ 2001).$$

Mas

$$2 \cdot 10^{n+1} + 1 \equiv 0\ (mod\ 2001) \Leftrightarrow 2 \cdot 10^{n+1} + 1 \equiv 2001\ (mod\ 2001)$$

$$\Leftrightarrow 2 \cdot 10^{n+1} \equiv 2000\ (mod\ 2001) \Leftrightarrow 2 \cdot 10^{n+1} \equiv 2000\ (mod\ 2001)$$

$$\Leftrightarrow\ 10^{n+1} \equiv 10^3\ (mod\ 2001).$$

Como $n + 1 > 3$, temos então que encontrar infinitos $n's$ tais que

$$10^{n-2} \equiv 1\ (mod\ 2001). \qquad (5.6)$$

Observe que a expressão acima é parecida com a que aparece no teorema de Euler. De fato, como $(10,2001) = 1$, temos que existe um expoente $\phi(2001)$ tal que

$$10^{\phi(2001)} \equiv 1\ (mod\ 2001).$$

Elevando a um número k de cada lado da última congruência, temos que

$$10^{k\phi(2001)} \equiv 1\ (mod\ 2001). \qquad (5.7)$$

Assim, tomando $n - 2 = k\phi(2001) \Leftrightarrow n = k\phi(2001) + 2$, temos a partir de (5.7), o que queremos em (5.6). Então, existem infinitos números da formar $200\ldots01$ (aqueles com $n = k\phi(2001) + 2$) que são múltiplos de 2001. ■

5.3 SISTEMAS DE CONGRUÊNCIA LINEAR

Um sistema de congruências lineares é um sistema do tipo

$$\begin{cases} a_1 x \equiv b_1 \ (mod\ m_1) \\ a_2 x \equiv b_2 \ (mod\ m_2) \\ \quad\quad \cdots \\ a_r x \equiv b_r \ (mod\ m_r) \end{cases} \tag{5.8}$$

Nesta seção, nosso objetivo é responder duas perguntas, quais sejam:

(1) Qual a condição necessária e suficiente para que o sistema (5.8) tenha solução?

(2) Uma vez que exista solução de (5.8), como calcular de forma sistemática todas as suas soluções?

Discutir a resolubilidade ou não de congruências do tipo $ax \equiv b\ (mod\ m)$ é a "chave" para encontrar a resposta de (1). Sabemos que tal congruência é equivalente à equação diofantina linear $ax - my = b$. Pelo teorema 3.5, essa equação só possui soluções inteiras se, e somente se, $(a, m) | b$. Logo,

$$ax \equiv b\ (mod\ m)\ \textit{tem solução inteira} \iff (a, m)\ \textit{é divisor de}\ b.$$

Ora, temos então que o sistema (5.8) só possui solução se, somente se, $(a_i, m_i) \mid b_i$ para todo $i = 1, \dots, r$. Isso responde a pergunta (1).

Note: se x_0 é solução da congruência $ax \equiv b\ (mod\ m)$, então todo $x \equiv x_0\ (mod\ m)$ também é solução da congruência, pois $ax \equiv ax_0 \equiv b\ (mod\ m)$. Ora, temos então que toda solução particular determina uma infinidade de soluções da congruência. Essas soluções serão identificadas (módulo m).

Discutimos no início da seção anterior que a equação diofantina $ax - my = b$ (ou $ax \equiv b\ (mod\ m)$), uma vez que $(a, m) | b$, possui exatamente (a, m) soluções incongruentes módulo m. Um conjunto de soluções da congruência $ax \equiv b\ (mod\ m)$, dois a dois incongruentes, é chamado de *sistema completo de soluções incongruentes da congruência.* A proposição a seguir exibe um desses conjuntos.

Proposição 5.7. *Sejam $a, b, m \in \mathbb{N}$, com $m > 1$ e $(a, m) | b$. Se x_0 é a menor solução da congruência $ax \equiv b\ (mod\ m)$, então*

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \dots, x_0 + (d-1)\frac{m}{d},$$

onde $d = (a, m)$ formam um sistema completo de soluções incongruentes da congruência.

Demonstração: Como $d = (a, m) \mid b$, sabemos que a congruência tem solução. É claro que para todo $i \in \{1,\ 2, \dots, d-1\}$, $x_0 + i\frac{m}{d}$ é solução da congruência, pois

$$a\left(x_0 + i\frac{m}{d}\right) \equiv ax_0 + i\frac{a}{d}m \equiv ax_0 \equiv b\ (mod\ m).$$

Esses números são dois a dois incongruentes. De fato, para todo $i < j < d$, tem-se

$$x_0 + i\frac{m}{d} \equiv x_0 + j\frac{m}{d}\ (mod\ m) \Longrightarrow i \equiv j\ (mod\ d) \Longrightarrow i = j,$$

isto é, para todo natural $i < j < d$

$$i \neq j \ \Longrightarrow\ x_0 + i\frac{m}{d} \not\equiv x_0 + j\frac{m}{d}\ (mod\ m).$$

Por fim, devemos mostrar que toda solução da congruência $ax \equiv b\ (mod\ m)$ é congruente, módulo m, a um dos $x_0 + i\left({}^{m}/_{d}\right)$, com $i < d$. Com efeito, seja $x \neq x_0$ uma solução qualquer da congruência, então

$$ax \equiv ax_0\ mod\ (mod\ m) \Longrightarrow x \equiv x_0\ mod\ \left(mod\ \frac{m}{d}\right) \Longrightarrow \exists\ k \in \mathbb{N}\ tal\ que\ x - x_0 = k\frac{m}{d}.$$

Pela divisão euclidiana, existe $i < d$ tal que $k = qd + i$, portanto

$$x = x_0 + k\frac{m}{d} = x_0 + (qd + i)\frac{m}{d} = x_0 + qm + i\frac{m}{d} \equiv x_0 + i\frac{m}{d}\ (mod\ m)$$

■

Exemplo 5.22. *Resolva a congruência* $8x \equiv 4\ (mod\ 12)$.

Solução: Como $d = (8,12) = 4$ divide 4, temos, pela proposição anterior, quatro soluções incongruentes módulo 12. Por tentativa e erro, temos a solução mínimal $x_0 = 2$. Assim, o conjunto solução módulo 12 da congruência é

$$\left\{2, 2 + 1 \cdot \frac{12}{4}, 2 + 2 \cdot \frac{12}{4}, 2 + 3 \cdot \frac{12}{4}\right\} = \{2, 2 + 3, 2 + 6, 2 + 9\}.$$ ■

Observação 5.4: Da proposição 5.7, temos uma consequência teórica importante. Se $(a, m) = 1$, então a congruência $ax \equiv b\ (mod\ m)$ possui uma única solução módulo m. Logo, se R' é um sistema reduzido de resíduos módulo m, então, para todo $r \in R'$, a congruência $rx \equiv a\ (mod\ m)$ possui uma única solução em R'.

◿

Observação 5.5. Note que se a congruência $a_i \equiv b_i\ (mod\ m_i)$, $1 \leq i \leq r$, do sistema (5.8), possui solução, então, $d_i = (a_i, m_i) \mid b_i$. Colocando,

$$a'_i = \frac{a_i}{d_i}, \qquad b'_i = \frac{b_i}{d_i}, \qquad n_i = \frac{m_i}{d_i},$$

temos as equivalências

$$a_i \equiv b_i\ (mod\ m_i) \Leftrightarrow a'_i \equiv b'_i\ (mod\ n_i) \underbrace{\Leftrightarrow}_{(*)} x \equiv c_i\ (mod\ n_i),$$

onde $c_i = b'_i a''_i$, sendo a''_i o inverso multiplicativo de $c_i = b'_i a''_i$, sendo a''_i o inverso de a'_i módulo n_i (a equivalência $(*)$ se justifica pela observação 5.4).

◿

Pelas observações 5.4 e 5.5, o sistema (5.8) é equivalente a um da forma

$$\begin{cases} x \equiv c_1 \ (mod\ n_1) \\ x \equiv c_2 \ (mod\ n_2) \\ \quad \cdots \\ x \equiv c_r \ (mod\ n_r) \end{cases} \tag{5.9}$$

Finalmente, a resposta à pergunta (2) é fornecida pelo teorema abaixo, conhecido como Teorema do Resto Chinês, uma vez que já era conhecido, na antiguidade, pelos matemáticos chineses.

Teorema 5.3 (do Resto Chinês). *Se no sistema* (5.9)*, temos que* $(n_i, n_j) = 1$*, para todo* $i \neq j$*, então o sistema* (5.9) *possui uma única solução módulo* $N = n_1 n_2 \cdots n_r$*. Tal solução pode ser obtida como se segue:*

$$x = N_1 y_1 c_1 + N_2 y_2 c_2 \ldots + N_r y_r c_r,$$

onde $N_i = N/n_i$ *e* y_i *é solução da congruência* $N_i y \equiv 1 \ (mod\ n_i), i = 1, \ldots, r$

Demonstração: Vamos, inicialmente, provar que x é uma solução simultânea do sistema (5.9). De fato, como $n_i \mid N_j$, se $i \neq j$, e $N_i y_i \equiv 1 \ (mod\ n_i)$, segue-se que

$$x = N_1 y_1 c_1 + N_2 y_2 c_2 \ldots + N_r y_r c_r \equiv c_i \ (mod\ n_i).$$

Por outro lado, se x' é outra solução do sistema (5.9), então $x \equiv x' \ (mod\ n_i)$ para todo $i = 1, \ldots, r$. Daí, $x \equiv x' \ (mod\ [n_1, n_2, \ldots, n_r])$. Como $[n_1, n_2, \ldots, n_r] = n_1, n_2 \cdots n_r = N$, pois $(n_i, n_j) = 1$ se $i \neq j$, temos que

$$x \equiv x' \ (mod\ [n_1, n_2, \ldots, n_r]) \Leftrightarrow x \equiv x' \ (mod\ \ N).$$

Isso mostra que o sistema (5.9) possui uma única solução módulo $N = n_1 n_2 \cdots n_r$, o que conclui a demonstração.

■

Vamos finalizar apresentando duas aplicações acerca do Teorema do resto Chinês.

Exemplo 5.23. O matemático chinês Sun-Tsu**,** que viveu no século I, propôs o seguinte problema: *qual é o número que deixa resto* $2, 3$ *e* 2 *quando divididos, respectivamente, por* $3,5$ *e* 7*?* A resposta de Sun-Tsu foi 23, mas com o Teorema do resto Chinês, já somos capazes

de fornecer todas as soluções deste problema. Primeiro vamos traduzir para linguagem de congruência o problema. De fato, ele é equivalente a resolver o sistema:

$$\begin{cases} x \equiv 2\ (mod\ 3) \\ x \equiv 3\ (mod\ 5) \\ x \equiv 2\ (mod\ 7) \end{cases} \tag{5.10}$$

É claro que cada congruência do sistema (5.10) tem solução, logo o sistema (5.10) tem solução. Como $(3,5) = (3,7) = (5,7) = 1$, esse sistema admite, pelo teorema do resto Chinês, uma única solução módulo $N = 3 \cdot 5 \cdot 7 = 105$. Nesse caso, $N_1 = 35$, $N_2 = 21$ e $N_3 = 15$. Por outro lado, $y_1 = 2$, $y_2 = 21$ e $y_3 = 1$ são soluções, respectivamente, das congruências $35y_1 \equiv 1\ (mod\ 3)$, $21y_2 \equiv 1\ (mod\ 5)$ e $15y_3 \equiv 1\ (mod\ 7)$. Portanto, uma solução módulo $N = 105$ é dado por

$$x = N_1 y_1 c_1 + N_2 y_2 c_2 + N_3 y_3 c_3 = 233.$$

Como $233 \equiv 23\ (mod\ 105)$, segue que 23 é a solução mínima do sistema (5.10). Na verdade a resposta para o problema de Sun-Tsu é qualquer número da forma $23 + 105k$, com $k \in \mathbb{N}$.

■

Exemplo 5.24. *Um professor pede a um aluno que escolha um número natural menor do que 1001 e que diga o resto r_7, r_{11}, r_{13} desse número quando dividido por 7, 11 e 13, respectivamente. Sem nenhuma outra informação, mostre que o professor é capaz de adivinhar o número escolhido pelo aluno?*

Solução: Seja $x_0 < 1001$ o número escolhido pelo aluno e, uma vez fornecidos r_7, r_{11}, r_{13} podemos construir o seguinte sistema de congruências

$$\begin{cases} x \equiv r_7\ (mod\ 7) \\ x \equiv r_{11}\ (mod\ 11) \\ x \equiv r_{13}\ (mod\ 13) \end{cases} \tag{5.11}$$

Claro que x_0 é a solução mínima do sistema acima. Para calculá-lo podemos aplicar o teorema do resto chinês. De fato, $N = 7 \cdot 11 \cdot 13 = 1001$, $N_1 = 143$, $N_2 = 91$ e $N_3 = 77$. Por outro lado, $y_1 = 5$, $y_2 = 4$ e $y_3 = 12$ são soluções, respectivamente, das congruências $143y \equiv 1\ (mod\ 7)$, $91y \equiv 1\ (mod\ 11)$ e $77y \equiv 1\ (mod\ 13)$. Portanto, o sistema (5.11) tem solução

$$x = N_1 y_1 r_7 + N_2 y_2 r_{11} + N_3 y_3 r_{13} = 715r_7 + 369r_{11} + 924r_{13} \text{ módulo } 1001$$

Assim, para o professor descobrir o número que o aluno escolheu, basta calcular o resto da divisão por 1001 de $715r_7 + 369r_{11} + 924r_{13}$.

■

PROBLEMAS PROPOSTOS

5.1. Encontre o resto da divisão

(a) de 7^{10} por 51

(b) de 14^{256} por 17

(c) de 12^{12} por 5

5.2. Prove que para todo $n \in \mathbb{N}$, tem-se que

(a) $70 \mid 101^{6n} - 1$

(b) $17 \mid 19^{8n} - 1$

5.3. Determine resto da divisão:

(a) de $10^{10} + 10^{10^2} + \cdots + 10^{10^{100}}$ por 7

(b) de $1^7 + 7^7 + \cdots + 100^7$ por 7

(c) de $1 + 2 + 2^2 + \cdots + 2^{19}$ por 4

(d) de $1 + 2^5 + \cdots + 100^5$ por 4

5.4. Determine:

(a) o algarismo das unidades do número 9^{9^9}.

(b) os algarismo das unidades e das centenas do número 7^{999999}.

5.5. Mostre que a soma dos quadrados de quatro números naturais consecutivos nunca podem ser um quadrado.

5.6. Suponha que $(a, m) = (a - 1) = 1$, mostre que

$$1 + a + a^2 + \cdots + a^{\phi(m)-1} \equiv 0 \ (mod\ m).$$

5.7. Mostre que , se $p > 2$ é um número primo, então

(a) $p \mid (p-2)! - 1$

$(b) p \mid (p-3)! - (p-1)/2$

5.8. Um grupo de 17 macacos guarda suas bananas em 11 cestas de igual conteúdoe em uma 12ª cesta contendo 6 bananas. Eles podem dividir o total de suas bananas em 17 grupos. Qual é o menor número de bananas que eles podem possuir?

5.9. Dispomos de uma quantia de x reais menor do que 3 000. Se distribuirmos essa quantia entre 11 pessoas, sobre R$ 1,00; se a distribuirmos entre 12 pessoas, sobram R$ 2,00 e se distribuirmos entre 13 pessoas, sobram R$ 3,00. De quantos reais dispomos?

5.10. Resolva o sistema $\begin{cases} x \equiv 7\ (mod\ 11) \\ 3x \equiv 5\ (mod\ 13) \\ 7x \equiv 4 (mod\ 5) \end{cases}$.

GAUSS: O PRÍNCIPE UNIVERSAL

Nesta nota histórica, encontra-se a abordagem com base em [1] e [18].

Novos eventos começaram a soprar na virada do século XVIII para o XIX sobre a pesquisa matemática. De um lado verificou-se um abandono progressivo da ideia de que essa pesquisa devesse vincular-se necessariamente a problemas práticos. Do outro, com o crescimento enorme e a diversificação do campo de matemática, começa assurgir a figura do especialista. Todavia, o espaço para o universalismo em matemática ainda não estava esgotado, como mostra a brilhante obra de Carl F. Gauss (1777 – 1855).

Gauss nasceu em Brunswick, Alemanha, sendo seus pais bastante simples e pobres. Porém, desde muito cedo ele se revelou uma notável criança prodígio, especialmente quanto à Matemática (quando adulto, costumava dizer que aprendera a calcular sozinho, antes de saber falar). Sua brilhante inteligência chamou a atenção do duque Ferdinand de Brunswick que se propôs a custear seus estudos, primeiro numa escola preparatória local e depois na Universidade de Göttingen (1795 a 1798). Durante sua passagem pela escola preparatória Gauss formulou, independentemente, o método dos mínimos quadrados para estimar o valor mais provável de uma variável a partir de um conjunto de observações aleatórias (ele divide a primazia da descoberta com Legendre, primeiro a publicar em 1806).

Aos 17 anos, Gauss decide incursionar na Teoria dos Números, com o projeto de esclarecer, completar e desenvolver o que os seus predecessores haviam realizado. Em 1798, aos 21 anos, ele produziu uma das obras-primas da Matemática, o livro *Disquisitiones Arithmeticae* (pesquisas aritméticas), que seria publicado somente em 1801. No livro, Gauss introduz a noção de congruência, estabelecendo resultados fundamentais, além de demonstrar

resultados profundos da Teoria dos Números. Por exemplo, demonstrou, dentro de uma quadro mais geral, o Teorema de Fermat, que assegura que todo número primo da forma $4n + 1$ escreve-se como a soma de dois números naturais. Na última seção, Gauss deduz o belo e famoso teorema que diz que um polígono regular com um número primo n de lados, inscrito num círculo, é construtível com régua e compasso se, e somente se, n é um número primo de Fermat.

Em 1799, em sua tese de doutorado na Universidade de Helmstedt, Gauss demonstra, pela primeira vez, o Teorema Fundamental da Álgebra, que havia sido enunciado por vários antecessores, mas jamais provado corretamente. Foi também um dos primeiros a tratar os números complexo como entidade matemática, dando-lhes representação geométrica como pontos do plano cartesiano.

A partir de 1807, Gauss fez contribuições à Astronomia, calculando com precisão a órbita de alguns planetas. Na Física, foi um dos criadores do Eletromagnetismo (inventou o telégrafo elétrico); contribuiu para o estudo da capilaridade e para óptica. Na Matemática pura, sua maior paixão, deu contribuições à teoria das probabilidades, foi um dos criadores das geometrias não euclidianas, da geometria diferencial, das funções de variável complexa e inaugurou um novo ramo da Teoria dos Números: a Teoria Algébrica.

Com sua universalidade e seus trabalhos revolucionários dotados de extremo rigor, concisão e elegância (superando Euler nesse sentido), Gauss teve o poder de mudar os rumos da Matemática. Por isso, foi considerado, por seus contemporâneos e pelas gerações que se sucederam, o príncipe da rainha das ciências.

6 - MISCELÂNEA OLÍMPICA

Segundo Moreira [16], as Olimpíadas de Matemática nos moldes atuais são disputadas desde 1894, quando foram organizadas competições na Hungria. Com o passar dos anos, competições similares foram se espalhando pelo leste europeu, culminando em 1959, com a organização da I Olimpíada Internacional de Matemática, na Romênia, com a participação de países daquela região. No Brasil, a Sociedade Brasileira de Matemática (SBM) organizou em 1979 a I Olímpiada Brasileira de Matemática (OBM). Hoje, além dela, existem várias competições locais, além de muitas regionais, destacando-se a nível nacional as Olimpíadas Brasileiras de Matemática das Escolas Públicas (OBMEP).

Nosso intuito neste capítulo é apresentar 25 problemas de nível olímpico, juntamente com suas resoluções. Mostraremos, com isso, a amplitude e eficiência dos resultados até aqui apresentados na solução de problemas, muitas vezes não triviais, que exigem certo engenho e esforços considerados para vencê-los. Assim, convidamos o professor a fazer uma imersão olímpica na Teoria Elementar dos Números, desenvolvendo e aperfeiçoando a sua capacitação, reacendendo seu interesse pela descoberta, afinal, é uma experiência extremamente gratificante resolver um problema que, no começo, parecia muito difícil. Então, inicialmente, procure não olhar a solução sem tentar resolver seriamente cada um. Leia atentamente, e escolha o que lhe agrada.

6.1 PROBLEMAS

1. Quantos quadrados perfeitos existem entre $40\,000$ e $640\,000$ que são múltiplos simultaneamente de 3, 4 e 5.

2. Seja n um inteiro maior que 1. Mostre que $4^n + n^4$ não é primo.

3. Se $n > 4$ é um número composto, prove que $(n-1)!$ É um múltiplo de n.

4. Mostre que o número de soluções de $\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=\frac{1}{1\,983}$, com x, y e z inteiros, é finito.

5. Mostre que, para todo natural $n \geq 2$, o número $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$ não é inteiro.

6. Seja p um número natural primo e k um número natural. Se p é um divisor de $\binom{k}{i}$ para todo $1 \leq i \leq k-1$, então existe um natural m tal que $k = p^m$.

7. Determine todos os primos que são a soma e a diferença de dois primos.

8. Seja k um inteiro positivo tal que $k(k+1)/3$ é um quadrado perfeito. Prove que $k/3$ e $(k+1)$ são quadrados perfeitos.

9. Mostre que a equação $x^3 + 1990y^3 = z^4$ tem infinitas soluções inteiras para $x > 0$, $y > 0$ e $z > 0$.

10. Mostre que existe um número da forma

$$1\underbrace{99\ldots9}_{n\ noves}1$$

com mais de dois noves que é múltiplo de 1991.

11. Prove que existe um natural n tal que a expansão decimal de n^{1992} comece com 1992 algarismos iguais a 1.

12. Encontre todos os números que são formados por 4 algarismos da forma $aabb$ e que sejam quadrados perfeitos.

13. Determine todos os inteiros n para os quais a equação $1/a + 1/b = n/(a+b)$ tenha alguma solução inteira a e b, com a, b e $a+b$ não-nulos.

14. Mostre que, para qualquer inteiro não negativo n, o número $1^n + 2^n + 3^n + 4^n$ é divisível por 5 se, e somente se, for divisível por 4.

15. Determine todos os inteiros $n \geq 1$ tais que $(2^n + 1)/n^2$ seja inteiro.

16. Encontre todos os números naturais x e y tais que $2^x = 3^y - 1$.

17. Mostre que existem infinitos números da forma $20000 \ldots 009$ que são múltiplos de 2009.

18. Encontre um número $n \in \mathbb{N}$ tal que $2^n > 10^{2000}$ e 2^n tenha entre suas 2000 últimas casas decimais pelo menos 1000 zeros consecutivos.

19. Mostre que a equação $x^3 - 117y^3 = 5$ não possui soluções inteiras.

20. Dado um natural n, mostre que existem n naturais consecutivos, nenhum dos quais é *livre de quadrados*[3].

21. Prove que existe uma potência de 2 com 1000 zeros consecutivos em sua representação decimal.

22. Seja $p = 2q + 1$ um número primo, onde q é ímpar. Mostre que $q! \equiv 1\ (mod\ p)$ ou $q! + 1 \equiv 0\ (mod\ p)$.

23. Encontre os dois últimos dois dígitos na representação decimal de 3^{200}.

24. Sejam $m, n, p \in \mathbb{N}$, com p sendo um primo ímpar. Se $\frac{7^m + p \cdot 2^n}{7^m - p \cdot 2^n} \in \mathbb{N}$, prove que tal número é primo.

25. Mostre que não existe inteiro x tal que $103 \mid x^3 - 2$.

6.2 SOLUÇÕES

1. Quantos quadrados perfeitos existem entre $40\,000$ e $640\,000$ que são múltiplos simultaneamente de 3, 4 e 5.

Solução: Lembre que se p é primo e $p \mid ab$, então $p \mid a$ ou $p \mid b$. Em particular, se $p \mid n^2$, então $p \mid n$. Para resolver, devemos procurar números n^2 satisfazendo $40\,000 \leq n^2 \leq 64\,000$

[3] Um número inteiro é livre de quadrados se ele não é divisível pelo quadrado de nenhum número inteiro maior do que 1.

e tais que $3 \mid n^2$, $4 \mid n^2$ e $5 \mid n^2$. Mas isso equivale a procurar inteiros n com $200 \leq n \leq 800$ e tais que $3 \mid n$, $2 \mid n$ e $5 \mid n$ (note que $4 \mid n^2 \Longrightarrow 2 \mid n^2 \Longrightarrow 2 \mid n$), ou seja, devemos procurar os múltiplos de 30 entre 200 e 800. Vinte ao todo, pois

$$\left\lfloor \frac{800}{30} \right\rfloor - \left\lfloor \frac{200}{30} \right\rfloor = 26 - 6 = 20.$$

■

2. Seja n um inteiro maior que 1. Mostre que $4^n + n^4$ não é primo.

Solução: Se n for par, $4^n + n^4$ será par e maior do que 2, portanto não é primo. Se n for ímpar, vamos tentar escrever $4^n + n^4$ como o produto de dois fatores. Com efeito, uma possibilidade, dependendo da existência do inteiro a, é que:

$$4^n + n^4 = (2^n + n^2 + a)(2^n + n^2 - a). \qquad (5.1)$$

Desenvolvendo o produto do segundo membro desta última expressão, temos:

$$4^n + n^4 = (2^n + n^2)^2 - a^2 = 4^n + 2^{n+1}n^2 + n^4 - a^2,$$

Logo vemos que a igualdade (5.1) se verifica se $a^2 = 2^{n+1}n^2$. Sendo n ímpar, $n = 2k + 1$, o que nos dá $a^2 = [2^{k+1}(2k + 10)]^2 \Longrightarrow a = 2^{k+1}(2k + 1) = 2^{k+1} \cdot n$. Portanto,

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

Para terminar a demonstração, devemo-nos certificar de que o menor dos fatores nesta última expressão não é igual a 1. De fato,

$$\begin{aligned} 2^n + n^2 - 2^{k+1} \cdot n &= 2^{2k+1} + (2k + 1)^2 - 2^{k+1} \cdot (2k + 1) \\ &= 2 \cdot 2^{2k} - 2 \cdot 2^k \cdot (2k + 1) + (2k + 1)^2 \\ &= (2^k - (2k + 1))^2 + 2^k \geq 5, \end{aligned}$$

pois, por hipótese, $k \geq 1$ (lembre que n é um número maior do que 1).

■

3. Se $n > 4$ é um número composto, prove que $(n - 1)!$ É um múltiplo de n.

Solução: Sendo n composto, $n = ab$ com $1 < a, b < n$. Se $a \neq b$, temos que

$$(n - 1)! = 1 \cdot 2 \cdot \ldots \cdot a \cdot \ldots \cdot b \cdot \ldots \cdot (n - 1)$$

e, portanto, $ab \mid (n - 1)!$. Se $n = a^2$, então $a < n$ e $2a < n$, pois, caso contrário,

$$2a \geq n \Longrightarrow 4a^2 \geq n^2 \Longrightarrow 4n \geq n^2 \Longrightarrow n \leq 4,$$

o que contraria a hipótese de $n > 4$. Portanto,

$$(n - 1)! = 1 \cdot 2 \cdot \ldots \cdot a \cdot \ldots \cdot 2a \cdot \ldots \cdot (n - 1),$$

isto é, $a^2 \mid (n - 1)!$.

■

4. Mostre que o número de soluções de $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{1}{1\,983}$, com x, y e z inteiros, é finito.

Solução: Podemos supor que $x \leq y \leq z$. Logo, devemos ter $x \leq 3 \cdot 1983$, pois, do contrário, $x > 3 \cdot 1983$, $y > 3 \cdot 1983$ e $z > 3 \cdot 1983$ e, daí,

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} < \frac{1}{1983}$$

Portanto, x só pode assumir um número finito de valores. Seja t um desses valores de x. Teremos:

$$\frac{1}{y} + \frac{1}{z} = \frac{1}{1983} - \frac{1}{t} = m.$$

Devemos ter $y \leq 2/m$, pois do contrário, $y > 2/m$ e $z > 2/m$ e daí

$$\frac{1}{y} + \frac{1}{z} < \frac{2}{m} + \frac{2}{m} = m.$$

Assim, para cada um dos finitos valores de x, existem apenas finitos valores que y pode assumir e, fixados x e y, z estará determinado. Logo, o número de soluções inteiras da equação dada é finito.

■

5. Mostre que, para todo natural $n \geq 2$, o número $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ não é inteiro.

Solução: Antes de resolver o problema, vamos listar 3 fatos que ajudam na resolução:

- Todo número natural n pode ser escrito na forma $n = 2^a b$, onde $a \geq 0$ e b é um natural ímpar (Justifique com o TFA).
- Todo natural n está entre duas potências consecutivas de 2, isto é, dado n, exite um k natural tal que $2^k \leq n \leq 2^{k+1}$ (Justifique pela representação de n na base 2).
- Se $2^k \leq n \leq 2^{k+1}$, nenhum número inteiro menor do que ou igual a n, salvo 2^k, será divisível por 2^k. (Também, justifica-se pela representação de n na base 2).

Inicialmente, através de um exemplo, vamos ver como os três fatos acima resolvem o problema.

Seja $n = 12$, $12 = 2^2 \cdot 3$ e $2^3 \leq 12 \leq 2^4$.

$$x = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{8} + \cdots + \frac{1}{12}$$

$$= \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{2^2} + \frac{1}{5} + \frac{1}{2 \cdot 3} + \frac{1}{7} + \frac{1}{2^3} + \frac{1}{3 \cdot 3} + \frac{1}{2 \cdot 5} + \frac{1}{11} + \frac{1}{2^2 \cdot 3}$$

Seja I o produto de todos os números ímpares menores do que ou igual a 12, isto é,

$$I = 3 \cdot 5 \cdot 7 \cdot 9 \cdot 11.$$

Multipliquemos a igualdade acima por $2^2 \cdot I$. Obtemos:

$$x \cdot 2^2 \cdot I = m + \frac{2^2 \cdot I}{2^3}$$

onde m é um número inteiro. O segundo membro desta igualdade, $m + \frac{I}{2}$, não é inteiro, logo, o primeiro membro também não é inteiro. Daí se conclui que x não é inteiro.

Em geral: $2^k \leq n \leq 2^{k+1}$ e seja

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

Seja I o produto de todos os números ímpares menores do que ou iguais a n. Multiplicando a igualdade acima por $I \cdot 2^{k-1}$, todas as parcelas do segundo membro serão números inteiros, salvo

$$\frac{I \cdot 2^{k-1}}{2^k} = \frac{I}{2}.$$

Temos, então, que

$$x \cdot 2^{k-1} \cdot I = m + \frac{I}{2},$$

com m inteiro. O segundo membro desta igualdade não é um número inteiro, logo o primeiro membro também não é e, portanto, x não é um número inteiro.

■

6. Seja p um número natural primo e k um número natural. Se p é um divisor de $\binom{k}{i}$ para todo $1 \leq i \leq k-1$, então existe um natural m tal que $k = p^m$.

Solução: Antes de resolver o problema, vamos listar 2 fatos que ajudam na resolução:

- Se p é um primo e k é um natural maior do que 1, existirá um $n \in \mathbb{N} \cup \{0\}$ tal que $p^n < k \leq p^{n+1}$ (represente k na base p).
- Se $x \in \mathbb{R}$ e $m \in \mathbb{Z}$, então $\lfloor x + m \rfloor = \lfloor x \rfloor + m$ (isso é uma consequência imediata da definição de $\lfloor x \rfloor$, adaptada para x real).

O número k está entre duas potências consecutivas de p, ou seja, $p^n < k \leq p^{n+1}$ e, portanto, um dos valores que i pode assumir é p^n. Como p é um divisor de $\binom{k}{p^n} = \frac{k!}{(p^n)!(k-p^n)!} \in \mathbb{N}$. Vamos contar quantas vezes o fator p aparece em $k!$, em $(p^n)!$ e em $(k-p^n)!$ usando a fórmula de Legendre (proposição 4.10):

$$E_p(k!) = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{k}{p^n} \right\rfloor + \left\lfloor \frac{k}{p^{n+1}} \right\rfloor \tag{6.2}$$

$$E_p\big((p^n)!\big) = \left\lfloor \frac{p^n}{p} \right\rfloor + \left\lfloor \frac{p^n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{p^n}{p^n} \right\rfloor = p^{n-1} + \cdots + p^2 + p + 1 \tag{6.3}$$

$$E_p\big((k-p^n)!\big) = \left\lfloor \frac{k-p^n}{p} \right\rfloor + \left\lfloor \frac{k-p^n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{k-p^n}{p^n} \right\rfloor =$$

$$= \left\lfloor \frac{k}{p} - p^{n-1} \right\rfloor + \left\lfloor \frac{k}{p^2} - p^{n-2} \right\rfloor + \cdots + \left\lfloor \frac{k}{p^n} - 1 \right\rfloor$$

$$= \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{k}{p^n} \right\rfloor - (p^{n-1} + \cdots + p^2 + p + 1) \qquad (6.4)$$

Portanto, de (6.2), (6.3) e (6.4), temos que

$$E_p\left[\binom{k}{p^n}\right] = E_p(k!) - E_p\big((p^n)!\big) - E_p\big((k-p^n)!\big) = \left\lfloor \frac{k}{p^{n+1}} \right\rfloor.$$

Logo, como $k \leq p^{n+1}$, este expoente será não nulo somente se $k = p^{n+1}$ e , somente neste caso, p divide $\binom{k}{p^n}$.

■

7. Determine todos os primos que são a soma e a diferença de dois primos.

Solução: Seja p um primo tal que $p = p_1 + p_2$ e $p = p_4 - p_3$, onde p_1, p_2, p_3, p_4 são primos com $p_2 \geq p_1$ e $p_4 \geq p_3$. Obviamente $p > 2$, o que implica $p_1 = p_3 = 2$. Logo, $p_1 = p - 2$, p e $p_4 = p + 2$ são três ímpares consecutivos e, portanto, um deles é múltiplo de 3. Como esses três números são primos, segue-se que $p_1 = 3 \Longrightarrow p = 5$. Assim, o único primo que é soma e diferença de dois primos é o 5.

■

8. Seja k um inteiro positivo tal que $k(k+1)/3$ é um quadrado perfeito. Prove que $k/3$ e $(k+1)$ são quadrados perfeitos.

Solução: Lembre que todo n^2 deixa resto 0 ou 1 quando dividido por 3. Seja

$$k(k+1)/3 = n^2,$$

temos os seguintes casos a considerar:

- $k \equiv 1\ (mod\ 3) \Longrightarrow k+1 \equiv 2\ (mod\ 3) \Longrightarrow k(k+1) \equiv 2\ (mod\ 3)$ (absurdo!).
- $k \equiv 2\ (mod\ 3) \Longrightarrow k+1 \equiv 0\ (mod\ 3) \Longrightarrow 3\ |(k+1)$. Note que k e $(k+1)/3$ são primos entre si e, uma vez que $k(k+1)/3$ é um quadrado perfeito, temos que k e $(k+1)/3$ são também quadrados perfeitos. Ora, isso é absurdo (k não pode ser um quadrado perfeito, pois $k \equiv 2\ (mod\ 3)$).
- $k \equiv 0\ (mod\ 3) \Longrightarrow 3 \mid k$. Do fato de $k/3$ e $(k+1)$ serem primos entre si e, uma vez que $k(k+1)/3$ é um quadrado perfeito, temos que $k/3$ e $(k+1)$ são também quadrados perfeitos.

Assim, este último caso é o único possível, do que concluímos que $k/3$ e $(k+1)$ são também quadrados perfeitos.

■

9. Mostre que a equação $x^3 + 1990y^3 = z^4$ tem infinitas soluções inteiras para $x > 0$, $y > 0$ e $z > 0$.

Solução: Considerando $x = y$,

$$x^3 + 1990y^3 = z^4 \Leftrightarrow 1991x^3 = z^4.$$

O fato 1991que aparece nos sugere que tomar $x = 1991^t$ e, portanto,

$$1991^{3t+1} = z^4.$$

Como existem infinitos valores positivos para os quais $3t + 1$ é múltiplo de 4, isso completa a demonstração.

■

10. Mostre que existe um número da forma

$$1\underbrace{99\ldots9}_{n\ noves}1$$

com mais de dois noves que é múltiplo de 1991.

Solução: Observe que

$$1\underbrace{99\ldots9}_{n}1 = 2\underbrace{000\ldots0}_{n+1} - 9 = 2 \cdot 10^{n+1} - 9,$$

e que

$$2000 \equiv 9\ (mod\ 1991) \Longrightarrow 1\underbrace{99\ldots9}_{n}1 \equiv 9(10^{n-2} - 1)\ (mod\ 1991).$$

Como queremos que $1\underbrace{99\ldots9}_{n}1$ seja múltiplo de 1991, devemos ter:

$$9(10^{n-2} - 1) \equiv 0\ (mod\ 1991) \Longrightarrow (10^{n-2} - 1) \equiv 0\ (mod\ 1991),$$

pois 9 e 191 são primos entre si.

Note que: $1991 = 11 \cdot 181$. Pelo pequeno teorema de Fermat temos:

$$\left.\begin{matrix} 10^{180} \equiv 1\ (mod\ 181) \\ 10^{10} \equiv 1\ (mod\ 11) \end{matrix}\right\} \Longrightarrow 10^{180} \equiv 1\ (mod\ 11) \Longrightarrow 10^{180} \equiv 1\ (mod\ [11{,}181]) \Longrightarrow$$

$$\Longrightarrow 10^{180} \equiv 1\ (mod\ 1991) \Longrightarrow 10^{180} - 1 \equiv 0\ (mod\ 1991).$$

Assim, para $n = 182$, tem-se

$$1\underbrace{99\ldots9}_{182}1 \equiv 9(10^{180} - 1) \equiv 0\ (mod\ 1991).$$

■

11. Prove que existe um natural n tal que a expansão decimal de n^{1992} comece com 1992 algarismos iguais a 1.

Solução: Basta mostrarmos que existe $n \in \mathbb{N}$ tal que

$$\underbrace{11\ldots1}_{1992\ uns} \cdot 10^k \leq n^{1992} < \underbrace{11\ldots12}_{1992\ uns} \cdot 10^k. \qquad (*)$$

para um certo $k \in \mathbb{N}$. Temos que

$$(*) \Leftrightarrow \sqrt[1992]{11\ldots1 \cdot 10^k} \leq n < \sqrt[1992]{11\ldots12 \cdot 10^k}$$
$$\Leftrightarrow \sqrt[1992]{11\ldots1} \cdot 10^t \leq n < \sqrt[1992]{11\ldots12} \cdot 10^t,$$

Sendo $k = 1992t$, com t natural.

Os números $\sqrt[1992]{11\ldots1}$ e $\sqrt[1992]{11\ldots12}$ possuem a mesma parte inteira. Seja, então, t tal que a primeira casa depois da vígula na qual esses números diferenciam a $t-ésima$. Como $\sqrt[1992]{11\ldots12}$ é irracional, podemos tomar

$$n = \left\lfloor \underbrace{\sqrt[1992]{11\ldots1}}_{1992\ uns} \cdot 10^t \right\rfloor + 1.$$

■

12. Encontre todos os números que são formados por 4 algarismos da forma $aabb$ e que sejam quadrados perfeitos.

Solução: Como o número $aabb$ é um quadrado perfeito, significa que

$$n^2 = aabb$$
$$n^2 = a10^3 + a10^2 + b10 + b$$
$$n^2 = (10^3 + 10^2)a + (10 + 1)b$$
$$n^2 = (1100)a + (11)b$$
$$n^2 = 11(100a + b) = 11(99a + a + b).$$

Como 11 é primo, temos que $11^2 \mid n^2$, o que nos leva a $11 \mid (a + b)$. Como $aabb$ tem 4 algarismos, $a \neq 0$; portanto

$$a \in \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$
$$b \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

Donde, $a + b \leq 18$, mas $a + b$ é múltiplo de 11, logo $a + b = 11$. Podemos observar que $a \neq 1$, pois do contrário $b = 10$. Analogamente, $b \neq 0$ e $b \neq 1$. Portanto,

$$a \in \{2, 3, 4, 5, 6, 7, 8, 9\} \quad \text{e} \quad b \in \{2, 3, 4, 5, 6, 7, 8, 9\}.$$

Como em todo quadrado perfeito o algarismo da unidade somente pode acabar em $0, 1, 4, 5, 6$ e 9. Segue-se que $b \in \{4, 5, 6, 9\}$. Certamente $b \neq 5$, pois todo número que acaba em 5 quando elevado ao quadrado sempre acaba em 25. Assim, $b \in \{4, 6, 9\}$.

- Se $b = 4$, então $a = 7$. Nesse caso o número seria 7744 que é um quadrado perfeito;

- Se $b = 6$, então $a = 5$. Nesse caso o número seria 5566 que não é um quadrado perfeito;
- Se $b = 9$, então $a = 2$. Nesse caso o número seria 2299 que não é um quadrado perfeito.

Assim, a única solução possível é $aabb = 7766 = 88^2$.

■

13. Determine todos os inteiros n para os quais a equação $1/a + 1/b = n/(a + b)$ tenha alguma solução inteira a e b, com a, b e $a + b$ não-nulos.

Solução: Note que

$$\frac{1}{a} + \frac{1}{b} = \frac{n}{(a+b)} \Leftrightarrow (a+b)^2 = nab \Leftrightarrow a^2 + (2-n)ab + b^2 = 0.$$

Calculando o valor de a, temos

$$a = \frac{b}{2}\left[(n-2) \pm \sqrt{(n-2)^2 - 4}\right].$$

Como a é inteiro, certamente $(n-2)^2 - 4$ é um quadrado perfeito. Como os intervalos entre quadrados sucessivos ficam maiores do que 4, logo após os primeiros quadrados, precisamos apenas testar os valores pequenos de n. Portanto, $(n-2)^2 = 4$, ou seja, n é 0 ou 4. Podemos agora tratar separadamente cada caso, encontrando, para cada um deles, ou uma solução ou uma prova de que ela não exista.

Caso $n = 0$, $(a+b)^2 = 0$ e, portanto, $a + b = 0$ o que não é permitido.

Caso $n = 2$, $(a+b)^2 = 4ab \Longrightarrow a^2 - 2ab + b^2 = 0 \Longrightarrow (a-b)^2 = 0$. Logo, $a = b$. Isto não é uma contradição, mas uma solução. A resposta, portanto, é $n = 4$.

■

14. Mostre que $n \nmid 2^n - 1$ para todo inteiro $n \geq 2$.

Solução: A demonstração é por absurdo. Suponhamos que exista um valor n tal que divida $2^n - 1$. Seja p o menor inteiro que divide n. Logo, temos que $p \mid 2^n - 1$, ou seja,

$2^n \equiv 1\ (mod\ p)$. Seja d o menor expoente tal que $2^d \equiv 1\ (mod\ p)$. Como $\phi(p) = p - 1$, temos que

$$\left.\begin{aligned} 2^d &\equiv 1\ (mod\ p) \\ 2^{p-1} &\equiv 1\ (mod\ p) \\ 2^n &\equiv 1\ (mod\ p) \end{aligned}\right\} \Rightarrow \begin{cases} (p-1) \equiv 0\ (mod\ d) \\ n \equiv 0\ (mod\ d) \end{cases}$$

Logo, d é divisor comum de $p - 1$ e n e, portanto, d divide o máximo divisor comum de $p - 1$ e n. Todavia, todos os divisores primos de $p - 1$ são menores do que p, logo não

aparecem na fatoração de n. Assim, $(p-1, n) = 1$ e o único valor possível para d é 1, o que implica $2^1 \equiv 1\ (mod\ p) \Leftrightarrow p = 1$, absurdo. Segue o resultado.

■

15. Mostre que, para qualquer inteiro não negativo n, o número $1^n + 2^n + 3^n + 4^n$ é divisível por 5 se, e somente se, n não for divisível por 4.

Solução: Vamos estudar separadamente os termos $1^n\ (mod\ 5)$, $2^n\ (mod\ 5)$, $3^n\ (mod\ 5)$ e $4^n\ (mod\ 5)$ antes de somarmos.

					$(mod\ 5)$
n	1^n	2^n	3^n	4^n	$1^n+2^n+3^n+4^n$
0	1	1	1	1	4
1	1	2	3	4	0
2	1	4	4	1	0
3	1	3	2	4	0
4	1	1	1	1	4
5	1	2	3	4	0
6	1	4	4	1	0
7	1	3	2	4	0
8	1	1	1	1	4

Note que a periodicidade da tabela é evidente: cada um dos termos 1^n, 2^n, 3^n e 4^n é periódico com período 4. De fato,

$$1^{n+4} \equiv 1^n\ (mod\ 5)$$

$$2^{n+4} \equiv 2^n \cdot 16 \equiv 2^n\ (mod\ 5)$$

$$3^{n+4} \equiv 3^n \cdot 81 \equiv 3^n\ \ (mod\ 5)$$

$$4^{n+4} \equiv 4^n \cdot (16)^2 \equiv 4^n\ \ (mod\ 5)$$

Resulta, então, que $1^n+2^n + 3^n + 4^n$ é periódico com período 4, e isto implica que só precisamos verificar nosso problema para $n \in \{0, 1, 2, 3\}$. Verificando a tabela, vemos que

$$1^n+2^n + 3^n + 4^n \equiv 0\ (mod\ 5) \Leftrightarrow 1^n+2^n + 3^n + 4^n \not\equiv 0\ (mod\ 4).$$

■

16. Encontre todos os números naturais x e y tais que $2^x = 3^y - 1$.

Solução: Observe inicialmente que

$$2^x = 3^y - 1 \Longrightarrow 2^x \equiv 3^y - 1\ (mod\ 4) \Leftrightarrow 2^x \equiv (-1)^y - 1\ (mod\ 4).$$

Se $x = 0$, temos que $2^0 = 3^y - 1 \Leftrightarrow 3^y = 2$, o que não é possível. Se $x = 1$, temos que $2^1 = 3^y - 1 \Leftrightarrow 3^y = 3 \Leftrightarrow y = 1$, logo $x = 1$ e $y = 1$ é uma solução. Se $x \geq 2$, temos que

$2^x \equiv 0\ (mod\ 4)$, logo $(-1)^y - 1 \equiv 0\ (mod\ 4)$, o que ocorre se, e somente se, y é par. Daí, $y = 2a$, onde a é natural e, temos que

$$2^x = 3^{2a} - 1 = (3^a - 1)(3^a + 1).$$

Como $(3^a - 1)$ e $(3^a + 1)$ são divisores de uma potência de 2, então $(3^a - 1)$ e $(3^a + 1)$ são ambas potências de 2. Todavia, $(3^a + 1) - (3^a - 1) = 2$, e as únicas potências de 2 tão "próximas" são 2 e 4. Consequentemente, $3^a - 1 = 2 \Leftrightarrow a = 1$ e logo $y = 2$ e $x = 3$. Enfim, as únicas soluções são $x = 3$ e $y = 2$ e $x = y = 1$.

■

17. Mostre que existem infinitos números da forma $20000 \ldots 009$ que são múltiplos de 2009.

Solução: O problema é equivalente a encontrar infinitos naturais tais que

$$2 \cdot 10^k + 9 \equiv 0\ (mod\ 2009) \Leftrightarrow 2 \cdot 10^k + 9 \equiv 2009\ (mod\ 2009)$$

$$2 \cdot 10^k \equiv 2 \cdot 10^3\ (mod\ 2009) \Leftrightarrow 10^{k-3} \equiv 1\ (mod\ 2009).$$

pois $(2000, 2009) = 1$. Pelo teorema de Euler,

$$10^{\phi(2009)} \equiv 1\ (mod\ 2009) \Longrightarrow 10^{\phi(2009)t} \equiv 1\ (mod\ 2009), t \in \mathbb{N}.$$

Assim, basta tomar $k = \phi(2009)t + 3$.

■

18. Encontre um número $n \in \mathbb{N}$ tal que $2^n > 10^{2000}$ e 2^n tenha entre suas 2000 últimas casas decimais pelo menos 1000 zeros consecutivos.

Solução: Pelo teorema de Euler, temos que

$$2^{\phi(5^{2000})} \equiv 1\ (mod\ 5^{2000}),$$

logo existe b natural com

$$2^{\phi(5^{2000})} = 5^{2000}b + 1,$$

o que implica

$$2^{2000} \cdot 2^{\phi(5^{2000})} = 2^{2000} \cdot 5^{2000}b + 2^{2000}\ ,$$

logo

$$2^{2000+\phi(5^{2000})} = 10^{2000}b + 2^{2000}.$$

Portanto, os 2000 últimos dígitos de $2^{2000+\phi(5^{2000})}$ coincidem com a representação decimal 2^{2000}, que tem no máximo 667 dígitos, pois

$$2^{2000} < (2^3)^{667} < 10^{667}.$$

Desta forma, há pelo menos $2000 - 667 = 1333$ zeros consecutivos dentre as 2000 últimas casas decimais de $2^{2000+\phi(5^{2000})}$ e assim

$n = \phi(5^{2000}) + 2000 = 4 \cdot 5^{1999} + 2000$ satisfaz as condições do enunciado.

■

19. Mostre que a equação $x^3 - 117y^3 = 5$ não possui soluções inteiras.

Solução: Observe que 117 é múltiplo de 9, logo qualquer solução inteira deve satisfazer

$$x^3 - 117y^3 \equiv 5\ (mod\ 9) \Leftrightarrow x^3 \equiv 5\ (mod\ 9).$$

Ora, x só pode deixar resto $0, 1, \ldots, 8$ na divisão por 9. Analisando estes casos, temos

$x\ (mod\ 9)$	0	1	2	3	4	5	6	7	8
$x^3\ (mod\ 9)$	0	1	8	0	1	8	0	1	8

Ou seja, x^3 só pode deixar resto 0, 1 ou 8 na divisão por 9. Assim, $x^3 \equiv 5\ (mod\ 9)$ é impossível e equação $x^3 - 117y^3 = 5$ não possui solução.

■

20. Dado um natural n, mostre que existem n naturais consecutivos, nenhum dos quais é *livre de quadrados*.

Solução: Seja n um natural qualquer**.** Sejam $p_1, p_2, \ldots, p_n$ primos distintos. O teorema do resto chinês nos garante que o sistema

$$x \equiv -1\ (mod\ {p_1}^2)$$
$$x \equiv -2\ (mod\ {p_2}^2)$$
$$\vdots$$
$$x \equiv -n\ (mod\ {p_2}^2)$$

tem solução. Se x_0 é uma solução positiva do sistema, então cada um dos números

$$x_0, x_0 + 1, x_0 + 2, \ldots, x_0 + n$$

é divisível pelo quadrado de um inteiro maior do que 1, logo nenhum deles é livre de quadrados.

■

21. Prove que existe uma potência de 2 com 1000 zeros consecutivos em sua representação decimal.

Solução: Usamos a mesma ideia usada na resolução do problema 18, todavia vamos incrementar algumas novas ideias neste problema. Temos que $2^{\phi(5^k)} \equiv 1\ (mod\ 5^k)$. Mas como $\phi(5^k) = 4 \cdot 5^{k-1}$, deve existir um inteiro positivo q para o qual $2^{4 \cdot 5^{k-1}} = 5^k q + 1$. Multiplicando ambos os membros dessa igualdade por 2^k, obtemos então que

$$2^{k + 4 \cdot 5^{k-1}} = 10^k q + 2^k.$$

Denote m o número de algarismos de 2^k. Então $10^{m-1} \leq 2^k \leq 10^m$. Daí,

$$m-1 \leq \log_{10} 2^k \leq m \Longrightarrow m-1 = \lfloor log_{10}\, 2^k \rfloor = \lfloor k\, log_{10}\, 2 \rfloor,$$

ou seja, 2^k possui $m = \lfloor k\, log_{10}\, 2 \rfloor + 1$ algarismos. Por outro lado, $10^k q$ tem exatamente k zeros, portanto $2^{k+4\cdot 5^{k-1}} = 10^k q + 2^k$ possui ao menos $k - (\lfloor k\, log_{10}\, 2 \rfloor + 1)$ zeros consecutivos em sua representação decimal. Todavia, como

$$\begin{aligned} k - (\lfloor k\, log_{10}\, 2 \rfloor + 1) \geq k - k\, log_{10}\, 2 - 1 &= k(1 - log_{10}\, 2) - 1 \\ &= k(log_{10}\, 10 - log_{10}\, 2) - 1 \\ &= klog_{10}(10/2) - 1 \\ &= klog_{10}\, 5 - 1. \end{aligned}$$

basta tomar um natural k tal que $klog_{10}\, 5 - 1 > 1000$ para garantir que a representação decimal de $2^{k+4\cdot 5^{k-1}}$ tem mais de 1000 zeros consecutivos.

■

22. Seja $p = 2q + 1$ um número primo, onde q é ímpar. Mostre que $q! \equiv 1\ (mod\ p)$ ou $q! + 1 \equiv 0\ (mod\ p)$.

Solução: Considere as congruências

$$\begin{array}{rcrcl} q & + & (q+1) & \equiv & 0\ (mod\ p) \\ (q-1) & + & (q+2) & \equiv & 0\ (mod\ p) \\ \vdots & & & & \\ 1 & + & 2q & \equiv & 0\ (mod\ p). \end{array}$$

Ou seja,

$$\left.\begin{array}{rcrl} q & \equiv & -(q+1) & 0\ (mod\ p) \\ (q-1) & \equiv & -(q+2) & 0\ (mod\ p) \\ \vdots & & & \\ 1 & \equiv & -2q & 0\ (mod\ p). \end{array}\right\} q \text{ congruências}$$

Multiplicando membro a membro todas as congruências, temos que

$$q(q-1)\cdots 1 \equiv (-1)^q (q+1)(q+2)\cdots 2q(mod\ p),$$

e do fato de q ser ímpar, segue-se que

$$q! \equiv -2(q+1)(q+2)\cdots 2q(mod\ p) \Leftrightarrow (q!)^2 \equiv -q!\,(q+1)(q+2)\cdots(q+q)(mod\ p),$$

e, como $2q = p - 1$, pelo teorema de Wilson, segue que

$$(q!)^2 \equiv -(2q)!\,(mod\ p) \Leftrightarrow (q!)^2 \equiv -(p-1)!\,(mod\ p) \Leftrightarrow (q!)^2 \equiv 1(mod\ p).$$

Assim, $(q!)^2 - 1 \equiv 0(mod\ p)$, ou seja, $q! \equiv 1\ (mod\ p)$ ou $q! + 1 \equiv 0(mod\ p)$.

■

23. Encontre os dois últimos dois dígitos na representação decimal de 3^{200}.

Solução: O problema se resume a calcular a seguinte congruência:

$$3^{200} \equiv x \ (mod\ 100).$$

Utilizando o binômio de Newton, podemos simplificar as contas:

$$3^{200} = 9^{100} = (10-1)^{100} = \sum_{k=0}^{100} \binom{100}{k} 10^{100-k}(-1)^k,$$

logo

$$3^{200} \equiv -\binom{100}{99} 10 + \binom{100}{100} \ (mod\ 100) \Leftrightarrow 3^{200} \equiv 1 \ (mod\ 100)$$

e assim os dois últimos dígitos de 3^{200} são 01.

■

24. Sejam $m, n, p \in \mathbb{N}$, com p sendo um primo ímpar. Se $\frac{7^m + p \cdot 2^n}{7^m - p \cdot 2^n} \in \mathbb{N}$, prove que tal número é primo.

Solução: Seja $a = \frac{7^m + p \cdot 2^n}{7^m - p \cdot 2^n}$. Como

$$a = 1 + \frac{p \cdot 2^{n+1}}{7^m - p \cdot 2^n} = -1 + \frac{p \cdot 7^m}{7^m - p \cdot 2^n},$$

segue que $(7^m - p \cdot 2^n)$ divide $(7 \cdot 2^{n+1}, 2 \cdot 7^m)$. Há, agora, duas possibilidades:

$(\boldsymbol{i})$ $p = 7$: neste caso,

$$(7^m - 7 \cdot 2^n) \text{ divide } (7 \cdot 2^{n+1}, 2 \cdot 7^m) = 14$$

e, daí, $(7^{m-1} - 2^n) \mid 2$. Isso implica que $7^{m-1} - 2^n = 1$; porém, analisando essa equação módulo 3, obtemos $1^{m-1} - (-1)^n \equiv 1 \ (mod\ 3)$, o que é um absurdo.

$(\boldsymbol{ii})$ $p \neq 7$: neste caso, temos que $(p \cdot 2^{n+1}, 2 \cdot 7^m) = 2$ e, daí, $(7^m - p \cdot 2^n) \mid 2$. Novamente, isso implica que $7^m - p \cdot 2^n = 1$ e, analisando tal equação também módulo 3, obtemos $1^m - p \cdot 2^n \equiv 1 \ (mod\ 3)$, donde $p = 3$. Segue então que $7^m - 3 \cdot 2^n = 1$ e $a = 7^m - 3 \cdot 2^n$.

Se $m = 1$, então $n = 1$ e, daí, $a = 13$, um número primo. Se $m > 1$, temos $n > 1$ e

$$2^{n-1} = \frac{7^m - 1}{6} = 7^{m-1} + \cdots + 7 + 1.$$

Como a soma dos m números ímpares de segundo membro da igualdade acima deve ser par, segue que m é par, digamos $m = 2k$. Daí, obtemos $49^k - 1 = 3 \cdot 2^n$, a parti de onde consideramos dois subcasos:

- Se $k = 1$, então $m = 2$ e $n = 4$, donde $a = 97$, novamente um primo.
- Se $k > 1$, então

$$(49-1)(49^{k-1}+\cdots+49+1)=49^k-1=3\cdot 2^n,$$

ou ainda $49^{k-1}+\cdots+49+1=2^{n-3}$. Essa igualdade nos dá, como acima, k par. Por fim, sendo $k=2l$, segue que

$$3\cdot 2^n=49^{2l}-1\equiv(-1)^{2l}-1\equiv 0\ (mod\ 5),$$

um absurdo.

■

25. Mostre que não existe inteiro x tal que $103 \mid x^3-2$.

Solução: Note primeiramente que 103 é primo. Agora suponha que $x^3\equiv 2\ (mod\ 103)$, de modo que $103 \mid x$. Elevando ambos os lados desta congruência a $(103-1)/3=34$, obtemos $x^{102}\equiv 2^{34}\ (mod\ 103)$ e sabemos pelo teorema de Euler que

$$x^{102}\equiv 46\ (mod\ 103),$$

que é uma contradição. Logo não há inteiro x tal que $103 \mid x^3-2$.

■

7 - ATIVIDADES PROPOSTAS

Neste capítulo, apresentamos algumas sugestões de atividades, que permitirão ao professor trabalhar em sala de aula alguns conteúdos apresentados neste trabalho. As atividades apresentadas podem ser usadas no ensino básico a partir do sétimo ano, e devem ser selecionadas de acordo com a maturidade matemática de cada turma. Objetivamos, assim, auxiliar o trabalho do professor, que pode, dentro de suas necessidades pedagógicas, adaptar as atividades aqui apresentadas, complementando-as inclusive.

7.1 ATIVIDADES

Proposta de Atividade 7.1.1. Divisão Euclidiana

Objetivo:

- Apresentar o enunciado da divisão euclidiana;
- Conhecer os diversos significados que o quociente e o resto da divisão euclidiana podem ter na resolução de problemas.

Descrição Geral:

- Expor o enunciado da divisão euclidiana com diversos exemplos, apresentando exercícios para encontrar o resto e o quociente.
- Apresentar problemas que vise buscar os significados do quociente da divisão euclidiana;
- Apresentar problemas que apresentem situações cíclicas (periódicas) com o intuito de buscar significados do resto da divisão euclidiana.

Problemas Propostos para Atividade 7.1.1.

1. Encontre o quociente e o resto na divisão de:

(a) 30 por 40

(b) -58 por 7

(c) 60 por 12

(d) -81 por 15

2. Quantos múltiplos 7 existe de 1 até 234?

3. Quantos múltiplos 5 existe de 113 até 800?

4. Deseja-se repartir 30 bolinhas de gude em 6 sacos. Quantas bolinhas ficaram em cada saco?

5. Uma padaria recebeu uma encomenda para fazer 1000 salgados, essa padaria tem a capacidade de fazer 200 salgados por dia, em quantos dias serão feitos todos os salgados?

6. Dona Fabrícia distribuiu igualmente 38 brigadeiros entre 12 alunos. Quantos brigadeiros cada um recebeu? Sobraram brigadeiros?

7. Em 11720 dias há quantos meses?

8. Contando a partir de um domingo, em que dia da semana cai o milésimo dia?

Proposta de Atividade 7.1.2. Divisor, Divisor Comum e Máximo Divisor Comum

Objetivo:

- Revisar conteúdo relacionado a divisor, divisor comum e máximo divisor comum de dois ou mais números usando a decomposição por primos;
- Aprofundar algumas propriedades do mdc.

Descrição Geral:

- Fazer uma revisão de máximo divisor comum, propondo atividades que usem a sua definição e seu cálculo, usando a decomposição com primos.

Problemas Propostos para Atividade 7.1.2.

Observação 7.1. As questões a seguir ajudam a relembrar o conceito de mdc.

1. Considere o número 72.

(a) Cite um divisor de 72

(b) Cite todos os divisores de 36

2. Como definir divisor de um número inteiro?

3. Considere os números 32 e 40.

(a) Cite todos os divisores de 32

(b) Cite todos os divisores de 40

(c)Quais os divisores comuns de 32 e 40

(d) Qual o maior dos divisores comuns de 32 e 40?

(e) Como se chama o maior dos divisores comuns de 32 e 40?

4. Responda:

(a) Quais os divisores de 36?

(b) Os números 24 e 36 possuem quantos divisores comuns?

(c) Qual o maior dos divisores comuns?

Observação 7.2. As questões a seguir são usadas para trabalhar algumas das propriedades do mdc.

5. Calcule o *mdc* sem fazer nenhum cálculo:

(a) $mdc(0, 31)$

(b) $mdc(1, 234)$

(c) $mdc(657, 657)$

(d) $mdc(1, 3547)$

(e) $mdc(43,43)$

6. Observando a propriedade: se $a \mid b$, então $mdc(a, b) = a$. Complete.

(a) Como $5 \mid 35$, pois $35 = 5 \cdot 7$, então $mdc(5, 35) =$_____.

(b) Como $20 \mid 100$, pois _____, então $mdc(20,100) =$_____.

(c) Como $25 \mid 125$, pois _____, então $mdc(25, 125) =$_____.

(d) Como $12 \mid 36$, pois _____, então $mdc(16, 36) =$_____.

7. Em cada item, encontre o mdc usando a decomposição em primos.

$(a)\ mdc(14, 28)$ $(d)\ mdc(450{,}125\ )$

$(b)\ mdc(128, 40)$ $(e)\ mdc(280{,}335)$

$(c)\ mdc(30, 75)$

Proposta de Atividade 7.1.3. Algoritmo de Euclides e Aplicações do Máximo Divisor Comum

Objetivo:

- Conhecer o algoritmo de Euclides e sua praticidade para o cálculo do mdc.

Descrição Geral:

- Apresentar o algoritmo de Euclides usando exemplos que mostram a prática desse método na obtenção do mdc de dois números naturais.
- Apresentar uma lista de exercícios para os alunos resolverem.
- Propor um comparativo entre o método visto na atividade 7.1.1 (da decomposição por primos) e o algoritmo de Euclides.
- Intervencionar acerca das limitações do método. Mostrar, por fim, alguns problemas que envolvam mdc.

Problemas Propostos para Atividade 7.1.3.

1. Em cada um dos itens abaixo, encontre o mdc usando o algoritmo de Euclides, também use a decomposição por primos.

$(a)\ mdc(14, 12)$ $(d)\ mdc(1234{,}896)$

$(b)\ mdc(120, 100)$ $(e)\ mdc(65214{,}5434)$

$(c)\ mdc(1502, 672)$

Pergunta: Qual dos métodos é mais rápido para a obtenção do mdc: da decomposição por primos, ou o algoritmo de Euclides?

2. Uma empresa de logística é composta por três áreas: administrativa, operacional e vendedores. A área administrativa é composta por 30 funcionários, a operacional por 48 e a de vendedores com 36. Ao final do ano, a empresa realiza uma integração entre as três áreas, de modo que todos os funcionários participem ativamente. As equipes devem conter o mesmo número de funcionários com o maior número possível. Determine quantos funcionários devem participar de cada equipe e o número possível de equipes.

3. Tenho 84 balas de coco, 144 balar de chocolate e 60 balas de leite. Quero formar pacotes de balas, sem misturar sabores. Todos os pacotes de balas devem ter a mesma quantidade de balas e essa quantidade deve ser a maior possível. Quantas balas eu devo colocar em cada pacote? Quantos pacotes eu devo formar?

4. A livraria de seu Edvan Horácio precisa atender dois pedidos: um de 126 livros e outro de 270 livros. Os livros de esses dois pedidos serão empacotados. Todos os pacotes devem ter o mesmo número de livros e o número de pacotes deve ser o menor possível. Determinar quantos livros seu Edvan Horácio deve colocar em cada pacote e quantos pacotes ele deve fazer?

5. Um marceneiro recebeu 40 toras de madeira, com 8 metros de comprimento cada uma, e 60 toras, com 6 metros cada uma. Ele deve cortar todas as toras em pedaços de mesmo tamanho, sendo esse tamanho o maior possível. Qual o tamanho de cada pedaço? Quantos pedaços serão obtidos?

Proposta de Atividade 7.1.4. Teorema de Bachet-Bêzout e Equações Diofantinas Lineares

Objetivo:

- Desenvolver a capacidade de utilizar o algoritmo estendido de Euclides para obter a combinação linear que nos forneça o mdc de dois números naturais.
- Apresentar um método de resolução para uma equação diofantina linear.

Descrição Geral:

- Enunciar o Teorema de Bachet-Bêzout, sem demonstração, através de exemplos numéricos;

- Usar o algoritmo de Euclides, fazendo substituição de restos deixados pelas divisões sucessivas, encontrando, a combinação linear que gere o *mdc;*
- Expor o método de resolução de uma equação diofantina linear;
- Fazer uma lista de exercícios que corroborem com as atividades propostas.

Problemas Propostos para Atividade 7.1.4.

1. Usando o processo de divisões sucessivas encontre dois números, x_0 e y_0 para que o $mdc(a,b) = a \cdot x_0 + b \cdot y_0$ em cada item abaixo:

$(a)\ mdc(12, 45)$

$(b)\ mdc(25, 80)$

$(c)\ mdc(124, 64)$

$(d)\ mdc(36{,}120)$

2. Verificar se cada equação diofantina linear abaixo existe solução:

$(a)\ 4x + 5y = 17$

$(b)\ 6x + 3y = 20$

$(c)\ -42 + 24y = 19$

$(d)\ 44 - 32 = 64$

3. Resolva as seguintes equações diofantinas, se tiver solução:

$(a)\ 4x + 5y = 17$

$(b)\ 6x + 3y = 20$

$(c)\ -42 + 24y = 19$

$(d)\ 44 - 32 = 64$

4. Uma camisa custa R$ 21,00, mas o comprador só tem notas de R$ 2,00, e o caixa, só de R$ 5,00. Nessas condições, será possível pagar a importância da compra, e de que modo?

5. Decomponha o número 100 em duas parcelas positivas tais que uma é múltiplo de 7 e outra é de 11.

7. O valor da entrada de um cinema é R$ 8,00 e da meia entrada R$ 5,00. Qual é o menor número de pessoas que pode assistir a uma sessão de maneira que a bilheteria seja de R$ 500,00.

Proposta de Atividade 7.1.5. Procurando Números Primos

Objetivo:

- Desenvolver o Crivo de Eratóstenes na procura de números primos;

Descrição Geral:

- Enunciar o *Crivo de Eratóstenes*;
- Executar uma sequência de atividades em torno da procura de números primos.

Sequência para Atividade 7.1.5.

1. Construa uma tabela com os números naturais de 2 até 300. Utilizando o *Crivo de Eratóstenes*, encontre todos os números primos entre 2 e 300.

2. Você percebeu que a partir de certo momento não foi mais preciso riscar nenhum número pois todos números a serem riscados já haviam sido riscados anteriormente? Qual foi o último número primo que teve algum múltiplo riscado? Porquê?

3. Para saber de um determinado número é primo, é necessário e suficiente verificar que n não divisível por todos os números primos p tais que $p \leq \sqrt{n}$. Discuta com seus colegas essa conclusão.

4. Utilizando a tabela construída no exercício 1, encontre todos os pares de *primos gêmeos* (primos separados por um único número natural) menores do que 300.

5. Escreva todos os números primos pares entre 4 e 50 como soma de dois primos.

7. Construa uma sequência de 7 números consecutivos, todos compostos. Existe alguma outra sequência como esta formada por números menores?

Proposta de Atividade 7.1.6. Congruência Modular

Objetivo:

- Conhecer a definição de congruência módulo m e usar corretamente a notação;
- Conhecer e aplicar adequadamente algumas propriedades de congruência.
- Operar sobre congruências;

Descrição Geral:

- Apresentar a relação de congruência módulo m como: $a \equiv b \ (mod\ m)$ se, e somente se, a e b deixam o mesmo resto quando divididos por m.
- Expor com exemplos as propriedades básicas que fazem da relação de congruência, uma relação de equivalência;
- Apresentar as propriedades operacionais com grande quantidade de exemplos;
- Resolver exercícios com os discentes.

Problemas Propostos para Atividade 7.1.6.

1. Determine se cada item abaixo é verdadeiro ou falso. Em caso negativo, corrija a congruência usando o símbolo de não-congruente $\not\equiv$.

$(a)\ 20 \equiv 5\ (mod\ 3)$

$(b)\ 14 \equiv 6\ (mod\ 8)$

$(c)\ 19 \equiv 13\ (mod\ 5)$

$(d)\ 49 \equiv 19\ (mod\ 10)$

$(e)\ 76 \equiv 7\ (mod\ 10)$

2. Verifique se as congruências são verdadeiras usando o fato que $a \equiv b \ (mod\ m)$ se, e só se, $m \mid (a - b)$.

$(a)\ 20 \equiv 5\ (mod\ 3)$

$(b)\ 14 \equiv 6\ (mod\ 8)$

$(c)\ 19 \equiv 13\ (mod\ 5)$

$(d)\ 49 \equiv 19\ (mod\ 10)$

$(e)\ 76 \equiv 7\ (mod\ 10)$

3. Complete as frases abaixo conforme o exemplo:

Exemplo: 73 e 52 na divisão por 3, temos:$73 = 3 \cdot 24 + 1$ e também $52 = 3 \cdot 17 + 1$, então $73 - 52 = (3 \cdot 24 + 1) - (3 \cdot 17 + 1) = 21$, como 21 é múltiplo de 3, ou seja, $3 \mid 21$, logo vale a congruência $73 \equiv 52\ (mod\ 3)$.

(a) 65 e 33 na divisão por 4, temos:_____ e também_____, então_____, como _____ é múltiplo de 3, ou seja, _____, logo vale a congruência_____.

(b) 30 e 16 na divisão por 14, temos:_____ e também_____, então_____, como _____ é múltiplo de 3, ou seja, _____, logo vale a congruência_____.

(c) 46 e 21 na divisão por 5, temos:_____ e também_____, então_____, como _____ é múltiplo de 3, ou seja, _____, logo vale a congruência_____.

(d) 123 e 13 na divisão por 10, temos:_____ e também_____, então_____, como _____ é múltiplo de 3, ou seja, _____, logo vale a congruência_____.

3. Complete as frases abaixo conforme o exemplo e tente compreender o que se procede:

Exemplo: tomando a congruência $46 \equiv 24\ (mod\ 11)$, como sabemos ser verdade, pois $11 \mid 46 - 24$, por que $46 - 24 = 22 = 11 \cdot 2$. Desta mesma forma $24 - 46 = -22$ que também é múltiplo de 11, logo $24 \equiv 46\ (mod\ 11)$.

(a) Tomando a congruência $12 \equiv 21\ (mod\ 9)$, como sabemos ser verdade, pois_____, por que_____. Desta mesma forma _____ que também é múltiplo de 9, logo_____.

(b) Tomando a congruência $-4 \equiv 16\ (mod\ 10)$, como sabemos ser verdade, pois_____, por que_____. Desta mesma forma _____ que também é múltiplo de 10, logo_____.

(c) Tomando a congruência $-9 \equiv -27\ (mod\ 6)$, como sabemos ser verdade, pois_____, por que_____. Desta mesma forma _____ que também é múltiplo de 6, logo_____.

(d) Tomando a congruência $41 \equiv -8\ (mod\ 7)$, como sabemos ser verdade, pois_____, por que_____. Desta mesma forma _____ que também é múltiplo de 7, logo_____.

4. Em cada uma das congruências abaixo, some e multiplique cada um dos membros por um número de sua escolha., Verifique que a congruência permanece válida.

Exemplo: $15 \equiv 3\ (mod\ 4)$

Resposta: Tomando o número 8, temos que

$$15 \equiv 3\ (mod\ 4) \Longrightarrow 15 + 8 \equiv 3 + 8\ (mod\ 4) \Longrightarrow 23 \equiv 11 (mod\ 4)$$ é válida.

Por outro lado,

$$15 \equiv 3\ (mod\ 4) \Longrightarrow 15 \cdot 8 \equiv 3 \cdot 8\ (mod\ 4) \Longrightarrow 120 \equiv 24\ (mod\ 4)$$ é tmbém válida.

$(a)\ 29 \equiv 35\ (mod\ 2)$

$(b)\ 17 \equiv 3\ (mod\ 8)$

$(c)\ 10 \equiv 19\ (mod\ 5)$

$(d)\ 49 \equiv 19\ (mod\ 10)$

$(e)\ 50 \equiv 65\ (mod\ 15)$

5. Mostre que

$(a)\ 10^{20} \equiv 1\ (mod\ 11)$

$(b)\ 9^{100} \equiv 1\ (mod\ 10)$

$(c)\ 21^{1000} \equiv 1\ (mod\ 20)$

$(d)\ 2^{20} \equiv 1\ (mod\ 41)$

6. Ache o resto da divisão:

$(a)\ 7^{20}\ por\ 51$

$(b)\ 5^{21}\ por\ 127$

$(c)\ 2^{100}\ por\ 17$

$(d)\ 12^{480} por\ 15$

8 - SUGESTÕES DOS PROBLEMAS

Neste capítulo apresentamos algumas sugestões dos problemas propostos. Esperamos que o leitor só consulte estas sugestões depois de tentar resolver de forma efetiva os problemas.

8.1 SUGESTÕES PARA O CAPÍTULO 1

1.1 Inspire-se no exemplo 1.7. No passo indutivo é só desenvolver cálculo algébrico elementar.

1.2 (a) No passo indutivo use o fato de $n+1 \geq 8 > 3$ e $(n+1)! = (n+1)n!$.

(b) Note que $2n \geq 6 > 1$ e desenvolva $(n+1)^2$. Isso suficiente para desenvolver o passo indutivo.

(c)Note que:

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

Adicionar $\frac{1}{n+1}$ a ambos os membros dessa última igualdade e utilizar a hipótese indutiva.

1.3 Use a definição de F_n e a hipótese indutiva.

1.4 (a) Para o passo indutivo perceba que

$$a^{n+1} - b^{n+1} = aa^n - bb^n = aa^n - ba^n + ba^n - bb^n = a^n(a-b) + b(a^n - b^n).$$

Daí é só aplica o passo indutivo que sai o resultado.

(b) Note $n = 2k+1$, $k \in \mathbb{N}$, pois n é ímpar. Logo,

$$a^n + b^n = a^{2k+1} + b^{2k+1} = a^{2k+1} - (-b)^{2k+1}.$$

Segue o resultado aplicando o item (a).

1.5 Seja x_n o número de regiões para n retas. Quando se acrescenta mais uma reta, ela começa criando uma região a mais e o mesmo acontece após cada interseção dela com cada uma das n retas já existentes, ou seja, se há n retas, a colocação de mais uma reta acrescenta

$n+1$ regiões já existentes. Em suma, $x_{n+1} = x_n + (n+1)$ para todo $n \geq 1$. Faça a experimentação dos valores que x_n assume e conjectura a fórmula $x_n = 1 + \frac{n(n+1)}{2}$. Prove a sua validade por indução.

1.6 Seja d_n o número de diagonais de um polígono convexo com n lados. Quando se acrescenta mais um lado a esse polígono de forma que continue convexo acrescentamos $n-1$ diagonais. Logo, $d_{n+1} = d_n + (n-1)$. Use esse fato no passo indutivo.

1.7 Todo polígono convexo pode ser decomposto em $n-2$ triângulos.

8.2 SUGESTÕES PARA O CAPÍTULO 2

2.1. Inspire-se nos exemplos 2.6 e 2.7. Manipulações algébricas simples resolvem o passo indutivo.

2.2. (a) Os números 2001, 2002, 2003, 2004 e 2005, quando divididos por 7, deixam resto 6, 0, 1, 2 e 3, respectivamente. Aplique a proposição 2.3.

(b) Aplique a proposição 2.3, notando que $2^{100} = 32^2$ e que 32 deixa resto 2 quando dividido por 3.

(c) Use o critério de divisibilidade por 3, juntamente com a proposição 2.3.

2.3. Mais uma aplicação da proposição 2.3.

2.4. Use o critério de paridade. Inspire-se no exemplo 2.2.

2.5. (a) Todo número natural pode ser escrito da forma $6k, 6k+1, 6k+2, 6k+3, 6k+4$ ou $6k+5$.

(b) Seja $a_n = a_1 + n \cdot r$ o termo geral de uma PA de razão r inteira, onde $r, a_1, n \in \mathbb{N}$ e $n = 2k+1$. Note que $\sum_{i=1}^{2k+1} a_i = (2k+1)a_1 + \left(\sum_{i=1}^{2k+1} i\right)r$. Daí, podemos concluir o resultado. Generalize para uma sequência arbitrária de n termos da PA.

2.6. Faça o estudo dos restos possíveis de um cubo quando dividido por 7. Aplique a proposição 2.3 para encontrar as soluções.

2.7. Aplicação do Teorema 2.2.

2.8. Aplicação do teorema 2.2. Use uma calculadora caso seja necessário.

2.9. Faça o estudo dos restos possíveis de um cubo e de um quadrado, quando divididos por 3, 4, 5 e 7. Execute algumas provas por contradição.

2.10. Faça o estudo dos possíveis resto de um quadrado perfeito quando dividido 10, uma vez que queremos saber o algarismo das unidades. Conclua a partir disso o resultado da letra (b).

2.11. Faça o estudo dos restos possíveis de um quadrado e da soma de dois quadrados, quando divididos por 4. Use redução ao absurdo. Conclua as letras (a) e (b).

2.12. Inspire-se na sugestão da questão **3.5** (b).

2.13. Se $a^3 - b^3 = 4$, então $(a-b)(a^2+ab+b^2) = 4$. Como $4 = 4\cdot 1 = 1\cdot 4 = 2\cdot 2$, podemos formar três sistemas que serão incompatíveis.

8.3 SUGESTÕES PARA O CAPÍTULO 3

3.1. Use o algoritmo de Euclides.

3.2. Use o algoritmo estendido de Euclides.

3.3. Use o lema de Euclides**.** O Exemplo 3.5 norteia a técnica empregada na resolução.

3.4. Temos que provar que $(2n+8, 4n+15) = 1$. Use o lema de Euclides.

3.5. (a) Consequência imediata da definição de divisibilidade.

(b) Suponha por absurdo que $ab \nmid n$, isso implica pela divisão euclidiana que $n = (ab)q + r$, onde $0 < r < |ab|$. Daí sai as seguintes implicações:

$$\left.\begin{array}{lll} a \mid n = (ab)q + r & \Rightarrow & a \mid r \\ b \mid n = (ab)q + r & \Rightarrow & b \mid r \end{array}\right\} \quad \Rightarrow \quad (a,b) \neq 1 \text{ (absurdo!)}$$

3.6. Fixe m e proceda a indução sobre n.

3.8. Use $\underbrace{11\ldots111}_{n\ vezes} = 10^n + 10^{n-1} + \cdots + 10 + 1 = \frac{10^{n+1}-1}{10-1}$ e o lema de Euclides.

3.9. Use o teorema 4.5**,** além do algoritmo estendido de Euclides para encontrar uma solução particular.

3.10. Guia-se pelo Exemplo 4.15.

3.11. Resolver a equação diofantina linear $7x + 11y = 100$.

3.12. Resolver a equação diofantina linear $7x + 19y = 1921$ com a condição $x + y$ se o menor valor possível.

3.13. Resolver a equação diofantina linear $3x + 5y = 100$.

3.14. Seja z o número procurado, logo $z = 37x + 11$ e $z = 48y + 35$. Isso implica que $37x - 48y = 24$. Resolva essa equação encontrando sua solução minimal.

8.4 SUGESTÕES PARA O CAPÍTULO 4

4.1. Como $p - q$ é ímpar, p e q devem ter paridades diferentes. Isto é: um dos dois é par e o outro é ímpar. Como o único primo par é 2, a solução única é 5 – 2 = 3 ($p = 5$ e $q = 2$).

4.2. Verifique os 40 primeiros números compostos para encontrar tal sequência.

4.3. Use $n^3 - 1 = (n-1)(n^2 + n + 1)$ e definição de número primo.

4.4. Use o fato de que todo número primo maior do que é da forma $4k + 1$ ou $4k + 3$, onde com $k \geq 1$.

4.5. Use a fatoração $a^3 - b^3 = (a-b)(a^2 + ab + b^2)$.

4.6. Use a seguinte identidade $a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$.

4.7 Use a ideia contida no exemplo 4.3.

4.8 Aplicação do TFA, juntamente com a ideia do problema anterior.

4.9. Use a ideia contida no exemplo 4.12.

8.5 SUGESTÕES PARA O CAPÍTULO 5

5.1. Aplique o Pequeno Teorema de Fermat.

5.2. Use o teorema de Euler.

5.3. Estude em cada item como se comportam as potências utilizando congruência. Visualize o período para aplicar na soma.

5.4. Utilize congruência módulo 10 e o Teorema de Euler.

5.5. Use o teorema de Euler adequadamente.

5.6. Use o teorema de Euler adequadamente.

5.7. Estude os quadrados perfeito módulo 10 e depois a soma de quatro quadrados consecutivos.

$\left.\begin{matrix}\mathbf{5.8}\\ \mathbf{5.9}\\ \mathbf{5.10}\end{matrix}\right\}$ são aplicações diretas do Teorema do resto Chinês.

CONSIDERAÇÕES FINAIS

Foi abordado neste trabalho tópicos básicos da Teoria Elementar dos Números.

Como ponto de partida, foi revisado importantes propriedades acercar da caracterização dos números inteiro, enfatizando sua boa ordenação.

Para tornar efetivo o entendimento de muitos resultados, foi necessário discorrer acerca do método de demonstração por indução. Nesse sentido, foi esclarecida a diferença entre dedução e indução, além de provado o Princípio da Indução Finita (PIF) – suas versões "forte" e "fraca". Várias aplicações foram feitas, mostrando poder do PIF nas demonstrações matemáticas. Ao final, chamou-se a atenção para alguns cuidados que devemos ter ao usar o método.

Prosseguiu-se apresentando a relação de divisibilidade. Demonstramos suas propriedades básicas; e resolvemos alguns problemas usando argumentos bem simples. O teorema da divisão euclidiana foi demonstrado com riqueza de detalhes, alguns resultados imediatos – como o princípio de Eudoxius – também foram demonstrados. Foi discorrido acerca da representação de um número inteiro em uma base, e também expusemos as provas de critérios clássicos de divisibilidade, que muitas vezes são usados no ensino básico sem o devido esclarecimento.

A teoria do máximo divisor comum também foi apresentada. Vimos que o teorema de Bachet-Bézout assume papel fundamental no desenvolvimento da teoria, pois permite demonstrar, entre outros resultados, o importante Lema de Gauss. Provou-se o algoritmo de Euclides para o cálculo do mdc de dois inteiros, como também, foi enfatizada sua importância computacional. A noção dual do mdc, o mínimo múltiplo comum, foi também exibida, onde proporcionamos o seu entendimento através de uma interpretação geométrica bem interessante. Ao final, aplicou-se a teoria ali discorrida na resolução de equações diofantinas lineares.

O estudo dos números primos foi também objeto de estudo. O importante Teorema Fundamental da Aritmética, que foi demonstrado com total rigor, desvenda de uma vez por todas a estrutura multiplicativa dos números inteiros. Entre tantas consequências, vimos que ele implica na existência de números irracionais, além de nos proporcionar uma nova forma de encarar problemas em teoria dos Números. Foi provado também os clássicos algoritmos para o mmc e mdc de dois números inteiros, via fatoração por primos, de grande valor teórico, todavia, ineficiente computacionalmente. A distribuição e procura de primo também foi um

tema importante. Nesse sentido, apresentou-se o crivo de Eratóstenes e foi enunciado o profundo Teorema dos Números Primos. Aplicou-se a teoria desenvolvida nas expressões decimais finitas e infinitas. Foi apresentado, ao final, a interessante Fórmula de Legendre, que permitiu fatoramos em primos o $n!$.

A profícua noção de congruência modular foi apresentada no último bloco teórico deste trabalho. Provamos suas propriedades fundamentais. Expusemos vários problemas resolvidos, que mostraram a eficiência dessa noção, uma vem que se assemelha à relação de igualdade. Os teoremas de Euler, Wilson e Fermat foram exibidos de forma concisa e inteligível, sempre precedidos da ideia empregada na demonstração. Isso proporcionou um efetivo entendimento das demonstrações ali empregadas. No final, foi provado o Teorema do resto Chinês, que permitiu dentro de suas hipóteses, resolver alguns sistemas de congruências lineares.

Por sua vez, com os 25 problemas olímpicos apresentados, espera-se que o professor note a amplitude que os resultados apresentados podem proporcionar na resolução de problemas muitas vezes não triviais.

No tocante às sugestões das atividades apresentadas, esperamos que sirvam de base para o desenvolvimento de outras, não obstante sejam aplicadas na íntegra. O que queremos é ajudar o professor a trabalhar alguns conteúdos aqui apresentados.

Com tudo, o que se espera ao final é ajudar o professor do ensino básico no seu desempenho em sala de aula, através da compreensão de tópicos básicos da Teoria Elementar dos números; instigando-o a formar doravante grupos olímpicos de treinamento intensivo, além de sensibilizá-lo acerca da importância de sua formação continuada, encorajando, assim, sua inscrição em algum programa de mestrado.

Bibliografia

1. HEFEZ, A. **Aritmética**. 2ª Ed. Rio de Janeiro: SBM, 2013. (Coleção PROFMAT).
2. HEFEZ, A. **Curso de Álgebra volume 1**. 5ª Ed. Rio de Janeiro: SBM, 2013. (Coleção Matemática Universitária).
3. HEFEZ, A. Indução Matemática. **Olimpíadas Brasileiras das Escolas Públicas (OBMEP)**. Disponivel em: <http://www.obmep.org.br/docs/Apostila4-Inducao.pdf>.
4. RIBENBOIM, P. **Números Primos:** mistérios e recordes. 1ª Ed. Rio de Janeiro: IMPA, 2001 (Coleção Matemática Universitária).
5. SANTOS, J. P. O. **Introdução à Teoria dos Números**. 2ª Ed. Rio de Janeiro: IMPA, 2000. (Coleção Matemática universitária).
6. HEFEZ, A. **Elementos de Aritmética**. 2ª Ed. Rio de janeiro: SBM, 2011. (Coleção Textos Universitários).
7. OLIVEIRA, K. I. M.; FERNÁNDEZ, A. J. C. **Iniciação à Matemática:** um curso com problemas e soluções. 2ª Ed. Rio de Janeiro: SBM, 2010. (Coleção Olimpíadas de Matemática).
8. MOREIRA, C. G. et al. **Teoria dos Números:** um passei com primos e outros números familiares pelo mundo. 3ª Ed. Rio de Janeiro: IMPA, 2013 (Projeto Euclides).
9. FERNANDES, A. M. V. et al. **Fundamentos de Álgebra**. 1ª Ed. atualizada. Minas Gerais: Editora UFMG, 2009. (Coleção Didática).
10. EVES, H. **Introdução à história da matemática**. Campinas,SP: UNICAMP, 2008.
11. LIMA, E. L. et al. **A Matemática do Ensino Médio - Volume 2**. 5ª Ed. Rio de Janeiro: SBM, 2004. (Coleção do Professor de Matemática).
12. SÁ, C. C. D.; ROCHA, J. **Trezes Viagens pelo Mundo da Matemática**. 2ª Ed. Rio de Janeiro: SBM, 2012 (Coleção do Professor de Matemática).
13. NETO, A. C. M. **Tópicos de Matemática Elementar:** Teoria dos Números. 1ª Ed. Rio de Janeiro : SBM, v. 5, 2012 (Coleção do Professor de Matemática; 28).
14. ÉLIO MEGA, R. W. **Olímpiadas Brasileiras de Matemática 1ª a 8ª:** problemas e resoluções. 1ª Ed. Rio de Janeiro: SBM, 2010. (Coleção Olímpiadas de Matemática).
15. LIMA, E. L. et al. **A Matemática do Ensino Médio - Volume 1**. 4ª Ed. Rio de Janeiro:

SBM, 1999. (Coleção do Professor de Matemática).

16. MOREIRA, C. G. et al. **Olimpíadas Brasileiras de Matemática 9ª a 16ª:** problemas e resoluções. 1ª Ed. Rio de Janeiro: SBM, 2009. (Coleção Olimpíadas de Matemática).
17. SHINE, C. Y. **21 Aulas de Matemática Olímpica**. 1ª Ed. Rio de Janeiro: SBM, 2009. (Coleção Matemática Olímpica).
18. IEZZI, G.; DOLCE, O.; MURAKAMI, C. **Fundamentos de Matemática Elementar**. 8ª Ed. São Paulo: Atual Editora, v. 2, 1996.
19. HEFEZ, A.; FERNANDES, C. S. **Introdução à Algebra Linear**. 1ª Ed. Rio de Janeiro: SBM, 2012. (Coleção PROFMAT).
20. SANTOS, J. P. O.; MELLO, M. P.; MURADI, I. T. C. **Introdução à Análise Combinatória**. 3ª Ed. Campinas: Editora da Unicamp, 2002.
21. GONÇALVES, A. **Introdução à Álgebra**. 3ª Ed. Rio de Janeiro: IMPA, 1979. (Projeto Euclides).