UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

Paulo Vitor Serpa Gonçalves

Divisibilidade e suas Aplicações nas Olimpíadas Científicas de Matemática

BELÉM
2021

UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

PAULO VITOR SERPA GONÇALVES

DIVISIBILIDADE E SUAS APLICAÇÕES NAS OLIMPÍADAS CIENTÍFICAS DE MATEMÁTICA

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional da Universidade Federal do Pará como requisito parcial para obtenção do título de mestre em Matemática em Rede Nacional

BELÉM
2021

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD
Sistema de Bibliotecas da Universidade Federal do Pará
Gerada automaticamente pelo módulo Ficat, mediante os dados fornecidos pelo(a) autor(a)

S481d Serpa Gonçalves, Paulo Vitor.
Divisibilidade e Suas Aplicações nas Olimpíadas Científicas de Matemática / Paulo Vitor Serpa Gonçalves. — 2021.
46 f. : il.

Orientador(a): Prof. Dr. Rogelio Daniel Benavides Guzmán
Dissertação (Mestrado) - Universidade Federal do Pará, Instituto de Ciências Exatas e Naturais, Programa de Pós-Graduação em Matemática em Rede Nacional, Belém, 2021.

1. Divisibilidade. 2. Teoria dos Números. 3. Olimpíadas. 4. Matemática. 5. Resolução de Problemas. I. Título.

CDD 512.7

CERTIFICADO DE AVALIAÇÃO

PAULO VITOR SERPA GONÇALVES

DIVISIBILIDADE E SUAS APLICAÇÕES NAS OLIMPÍADAS CIENTÍFICAS DE MATEMÁTICA

Esta Dissertação, apresentada ao Curso Profissional de Matemática, da Universidade Federal do Pará, como requisito parcial para obtenção do Título de Mestre em Matemática, foi julgada e aprovada pela seguinte banca examinadora:

Rogelio B. Guzmán

Prof. Dr. ROGÉLIO DANIEL BENAVIDES GUZMÁN (Orientador) - UFPA

Amanda Suellen Sena Corrêa Leão.

Prof. Dr. AMANDA SUELLEN SENA CORRÊA LEÃO - UFPA

Francisco Paulo Marques Lopes

Prof. Dr. FRANCISCO PAULO MARQUES LOPES - UFPA

Tania Begazo

Prof. Dr. TANIA MADELEINE BEGAZO VALDIVIA - UFPA

APROVADO EM: 30 de Abril de 2021.

CONCEITO: EXC

Resumo

A carência de materiais sobre teoria dos números para o ensino básico que quando encontrado é de alto custo, inspirou o desenvolvimento deste trabalho, apresentando uma linguagem simples sobre divisibilidade e quais situações poderemos aplica-la, reunindo informações variadas de livros, artigos e problemas olímpicos, visando um embasamento para o aluno que pretende prestar esses exames e professores que visam enriquecer seus conhecimentos, apresentando primeiramente a teoria e posteriormente os seus exercícios e soluções.

Palavra chave: Teoria dos números, divisibilidade, Olimpíadas de Matemática, Resolução de Problemas.

Abstract

The lack of high-priced number theory materials for basic education has inspired the development of this work, presenting a simple language about divisibility and what situations we can apply it, gathering varied information from books, articles and Olympic problems, aiming at a foundation for the student that intends to take these exams and teachers that aim to enrich their knowledge, presenting first the theory and later its exercises and solutions.

Keyword: Number theory, divisibility, Math Olympics, Problem Solving.

Sumário

1 Introdução

A teoria dos números é baseada no estudo dos números inteiros e suas generalizações, que veio sendo estudada por Euclides de Alexandria (300 a.c), Diofanto de Alexandria, Pierre de Fermat, Euler, Legendre, Gauss, entre outros estudiosos e que veio sendo desenvolvida na primeira metade do século XX.

Sendo uma disciplina com uma variedade de aplicações e tendo como um dos seus campos de estudo a divisibilidade, que se faz muito presente no ensino básico, de acordo o PCN e a BNCC de Matemática do Ensino Fundamental, que se encontra na página 300 a 301, do sexto ano:

- Unidade Temática: Números

  Objetivo: Operações (adição, subtração, multiplicação, divisão e potenciação) com números naturais e Divisão euclidiana.

  Habilidades: **(EF06MA04)** Construir algoritmo em linguagem natural e representá-lo por fluxograma que indique a resolução de um problema simples (por exemplo, se um número natural qualquer é par).

  (EF06MA05) Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos ?é múltiplo de?, ?é divisor de?, ?é fator de?, e estabelecer, por meio de investigações, critérios de divisibilidade por 2, 3, 4, 5, 6, 8, 9, 10, 100 e 1000.

  (EF06MA06) Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor.

Por ser um assunto que por muitas vezes é deixada de lado pelo professor, além de ser pouco abordado nos livros didáticos é de extrema importância em concursos militares e vestibulares concorridos como USP, UNICAMP e UNB, também muito presente em problemas olímpicos de matemática.

resolvi fazer um material que aborde esses assuntos e suas variantes, assim como suas aplicações, sendo detalhado em cada capítulo suas propriedades e demonstrações, para posteriormente apresentar uma série de exercícios de concursos e exames variados, para que possa fixar o assunto abordado.

O trabalho abordará temas relevantes que envolvem a divisibilidade, primeiramente explicando o que é e suas propriedades no campo dos $\mathbb{Z}$, posteriormente, o conjunto dos divisores de um inteiro, a divisão Euclidiana e problemas que envolvem resto, alguns critérios de divisibilidade, paridade de um inteiro e ao final será abordado o tema de sistemas de numeração, todos esses tópicos constam exercícios resolvidos de problemas olímpicos nacionais e internacionais, para que sirva de base não só para os alunos da educação básica, mas para os professores em geral que buscam sempre aprimorar-se, assim como estudantes de licenciatura ou bacharelado na disciplina de Teoria dos Números ou Aritmética para o curso do mestrado PROFMAT.

2 Divisibilidade em $\mathbb{Z}$

Definicão 1. *Sejam a e b dois inteiros. Diz-se que a divide b se e somente se existe um inteiro $q \in \mathbb{Z}$, tal que*

$$b = aq.$$

Outras formas equivalentes de afirmar que a divide b, são, b é múltiplo de a, a é fator de b ou b é divisível por a. Quando a dividir b utilizaremos a seguinte notação $a \mid b$ indicando que $a \neq 0$ divide b e $a \nmid b$ para $a \neq 0$ não dividir b. Essa relação denomina-se divisibilidade em $\mathbb{Z}$.

Observação 1. *se a é divisor de b, então $-a$ também é um divisor de b, pelo fato de $b = aq = (-a)(-q)$.*

Observação 2. *Caso* $0 \mid 0$.

Existe uma indeterminação, pois $0 = 0 \cdot q$, sendo $q \in \mathbb{Z}$, como todo produto por zero resulta em zero, sendo assim podemos concluir que existem infinitos valores para q.

Deste modo concluímos que os divisores de um inteiro qualquer são dois a dois iguais em um valor absoluto e de sinais opostos.

Partindo do que foi exposto acima, podemos enunciar o seguinte teorema.

Teorema 2.1. *Se um número b dividir outro a, então b dividirá todos os múltiplos de a.*

Demonstração. Como b divide a, então podemos concluir que $a = bq$, sendo $q \in \mathbb{Z}$.

Tomando $c = ka$, sendo $k \in \mathbb{Z}$, um múltiplo qualquer de a, podemos escrevê-lo da seguinte forma, $c = kbq$, logo b divide um múltiplo qualquer de a. □

Exemplo:

Podemos afirmar que $3 \mid 6$, pois $6 = 3 \times 2$, como também dividirá seus múltiplos, isto é, $3 \mid 6k$, sendo $k \in \mathbb{Z}$.

Como já temos a ideia inicial sobre a divisibilidade, daremos continuidade apresentando as propriedades básicas e algumas consequências.

2.1 Propriedades da divisibilidade

propriedade 2.1.1. *$a \mid 0$, $1 \mid a$ e $a \mid a$, $\forall\ a \in \mathbb{Z}$.*

Demonstração. Com efeito temos que $0 = a.0$, $a = 1.a$ e $a = a.1$, $\forall\ a \in \mathbb{Z}$. □

propriedade 2.1.2. *Se $a \mid 1$, então $a = \pm 1$, $\forall\ a \in \mathbb{Z} - \{0\}$.*

Demonstração. Se $a \mid 1$, então $1 = aq$, sendo $q \in \mathbb{Z}$, o que implica $a = 1$ e $q = 1$ ou $a = -1$ e $q = -1$, isto é $a = \pm 1$. □

propriedade 2.1.3. *Se $a \mid b$ e se $c \mid d$, então $ac \mid bd$, $\forall\ a, b, c, d \in \mathbb{Z}$.*

Demonstração. Temos $a \mid b$, então $b = aq$ e $c \mid d$, então $d = cq_1$, onde $q, q_1 \in \mathbb{Z}$. Multiplicando as equações teremos:

Utilizando a associatividade e comutatividade em $\mathbb{Z}$,

$$bd = acqq_1 = ac(qq_1)$$

Fazendo $qq_1 = q' \in \mathbb{Z}$. teremos $bd = acq'$, concluindo que $ac \mid bd$. □

Observação 3. *A recíproca dessa propriedade é falsa, pois:*

$$2 \times 3 \mid 9 \times 4, \textit{ mas } 2 \nmid 9 \textit{ e } 3 \nmid 4$$

propriedade 2.1.4. *Se $a \mid b$ e se $b \mid a$, então $a = \pm b$, $\forall\ a, b \in \mathbb{Z}$.*

Demonstração. Como $a \mid b$ e $b \mid a$, teremos $b = aq$ e $a = bq_1$, onde $q, q_1 \in \mathbb{Z}$, multiplicando as equações encontraremos $ba = abqq_1$, simplificando os lados da igualdade teremos $qq_1 = 1$, concluímos assim que $q_1 \mid 1$, logo $q_1 = \pm 1$, substituindo na equação $a = bq_1$ encontraremos $a = b(\pm 1)$, concluindo assim que $a = \pm b$. □

propriedade 2.1.5. *Se $a \mid b$, com $b \neq 0$, então $|a| \leq |b|$, $\forall\ a, b \in \mathbb{Z}$.*

Demonstração. Se $a \mid b$, com $b \neq 0$, então $b = aq$, sendo $q \neq 0$ e $q \in \mathbb{Z}$,assim $|b| = |a| \,.\, |q|$. Como $q \neq 0$, segue-se que $|q| \geq 1$, concluímos que $|b| = |a| \,.\, |q| \geq |a|$, ou seja $|b| \geq |a|$. □

propriedade 2.1.6. *Se $a \mid (b \pm c)$, então $a \mid b \Leftrightarrow a \mid c$.*

Demonstração. ($\Longrightarrow$) Sendo, $a \mid (b + c)$, então $b + c = aq$ com $q \in \mathbb{Z}$.

Se $a \mid b$, então $b = aq_1$, com $q_1 \in \mathbb{Z}$ e substituindo na equação $b + c = aq$, teremos $aq_1 + c = aq$, onde $c = aq - aq_1 = a(q - q_1)$. Fazendo $q - q_1 = q' \in \mathbb{Z}$, concluímos que $c = aq'$, logo $a \mid c$.

($\Longleftarrow$) Se $a \mid c$, então $c = aq_2$, com $q_2 \in \mathbb{Z}$ e substituindo na equação $b+c = aq$, teremos $b + aq_2 = aq$, donde $b = aq - aq_2 = a(q - q_2)$. Fazendo $q - q_2 = q'' \in \mathbb{Z}$, logo concluímos que $b = aq''$, então $a \mid b$.

Sendo, $a \mid (b - c)$, então $b - c = aq$ com $q \in \mathbb{Z}$.

($\Longrightarrow$) Se $a \mid b$, então $b = aq_1$, com $q_1 \in \mathbb{Z}$ e substituindo na equação $b - c = aq$, teremos $aq_1 - c = aq$, onde $c = aq_1 - aq = a(q_1 - q)$. Fazendo $q_1 - q = q' \in \mathbb{Z}$, concluímos que $c = aq'$, logo $a \mid c$.

($\Longleftarrow$) Se $a \mid c$, então $c = aq_2$, com $q_2 \in \mathbb{Z}$ e substituindo na equação $b - c = aq$, teremos $b - aq_2 = aq$, donde $b = aq + aq_2 = a(q + q_2)$. Fazendo $q + q_2 = q'' \in \mathbb{Z}$, logo concluímos que $b = aq''$, então $a \mid b$.

□

propriedade 2.1.7. *Se $a \mid b$ e $a \mid c$, sendo $a, b \in \mathbb{Z} - \{0\}$, então $a \mid (bx + cy)$, $\forall x, y \in \mathbb{Z}$.*

Demonstração. Sendo, $a \mid b$ e $a \mid c$, existem $q, q_1 \in \mathbb{Z}$, tais que $b = aq$ e $c = aq_1$.

Portanto, quaisquer que sejam $x, y \in \mathbb{Z}$, teremos:

$$\begin{aligned} bx + cy &= aqx + aq_1y \\ &= a(qx + q_1y) \end{aligned}$$

Como $qx + q_1y \in \mathbb{Z}$, conclui-se que $a \mid bx + cy$. □

Outro fator muito importante para a resolução de problemas em divisibilidade são as operações com polinômios, onde serão apresentadas a seguir.

2.2 Divisibilidades polinomiais

Listaremos a seguir algumas consequências da definição de divisibilidade.

Consequência 2.2.1. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N} \cup \{0\}$. Temos que $a - b$ divide $a^n - b^n$.*

Demonstração. Provaremos essa propriedade por indução sobre n.

Se $n = 0$, teremos $a^0 - b^0 = 1 - 1 = 0$, concluindo que $a - b \mid 0$.

Tomando $n = 1$, teremos $a^1 - b^1 = a - b$, assim é perceptível que $a - b \mid a - b$.

Supondo que a sentença $a - b \mid a^n - b^n$ seja válida para n, devemos garantir que $a - b \mid a^{n+1} - b^{n+1}$.

Como $a^{n+1} - b^{n+1} = aa^n - bb^n$, somando e diminuindo ba^n na equação, teremos,

$$a^{n+1} - b^{n+1} = a^n - ba^n + ba^n - bb^n = a^n(a - b) + (a^n - b^n)b.$$

Como $a - b \mid (a - b)$ e por hipótese $a - b \mid (a^n - b^n)$, mostramos assim que a propriedade é válida para todo $n \in \mathbb{N} \cup \{0\}$. □

Consequência 2.2.2. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N} \cup \{0\}$. Temos que $a+b$ divide $a^{2n+1}+b^{2n+1}$.*

Demonstração. Demonstraremos essa propriedade também por indução sobre n. Tomando $n = 0$, teremos $a^{2(0)+1} + b^{2(0)+1} = a^1 + b^1 = a + b$, assim é perceptível que $a + b \mid a^1 + b^1$.

Supondo que a sentença $a+b \mid a^{2n+1}+b^{2n+1}$ seja válida para n, agora nos resta garantir que $a + b \mid a^{2n+3} + b^{2n+3}$:

$$\begin{aligned} a^{2(n+1)+1} + b^{2(n+1)+1} &= a^{2n+1+2} + b^{2n+1+2} \\ &= a^2a^{2n+1} + b^2b^{2n+1} \end{aligned}$$

somando e subtraindo b^2a^{2n+1} na equação, teremos:

$$a^{2n+3} + b^{2n+3} = a^2a^{2n+1} - b^2a^{2n+1} + b^2a^{2n+1} + b^2b^{2n+1} = (a^2 - b^2)a^{2n+1} + (a^{2n+1} + b^{2n+1})b^2.$$

Como $a+b$ divide $a^2-b^2=(a-b)(a+b)$ e por hipótese $a+b \mid (a^{2n+1}+b^{2n+1})$, mostramos assim que a propriedade é válida para todo $n \in \mathbb{N} \cup \{0\}$. $\square$

Consequência 2.2.3. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{Z}$. Temos que $a+b$ divide $a^{2n}-b^{2n}$.*

Demonstração. Novamente usaremos indução sobre n.

Tomando $n=0$, teremos $a^{2(0)}-b^{2(0)}=a^0-b^0=1-1=0$, assim $a+b \mid 0$.

Tomando $n=1$, teremos $a^{2(1)}-b^{2(1)}=a^2-b^2=(a+b)(a-b)$, logo $a+b \mid a^2-b^2$.

Supondo a sentença $a+b \mid a^{2n}-b^{2n}$, seja válida para n, resta-nos mostrar que $a+b \mid a^{2n+2}-b^{2n+2}$. Tem-se que:

$$\begin{aligned} a^{2(n+1)}-b^{2(n+1)} &= a^{2n+2}-b^{2n+2} \\ &= a^2a^{2n}-b^2b^{2n} \end{aligned}$$

somando e subtraindo b^2a^{2n} na equação, teremos:

$$a^{2n+2}-b^{2n+2}=a^2a^{2n}-b^2a^{2n}+b^2a^{2n}-b^2b^{2n}=(a^2-b^2)a^{2n}+(a^{2n}-b^{2n})b^2$$

Como $a+b \mid a^2-b^2$ e por hipótese $a+b \mid a^{2n}-b^{2n}$, mostramos assim que a propriedade é valida para todo $n \in \mathbb{N}$. $\square$

2.3 Algumas Fatorações importantes

Por não ser o foco do nosso estudo, enunciaremos sem demonstração algumas identidades que servirão de base para a resolução de alguns problemas aqui abordados.

1. $a^2-b^2=(a-b)(a+b)$
2. $a^3+b^3=(a+b)(a^2-ab+b^2)$
3. $a^3-b^3=(a-b)(a^2+ab+b^2)$
4. $a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+...+ab^{n-2}+b^{n-1})$, sendo $n \in \mathbb{N}$.
5. $a^n+b^n=(a+b)(a^{n-1}-a^{n-2}b+...-ab^{n-2}+b^{n-1})$, sendo $n \in \mathbb{N}$.

2.4 Exercícios Resolvidos

Exercício 2.1. *A soma de todos os múltiplos positivos de 6 que se escrevem (no sistema decimal) com dois algarismos é:*

(A) 612 *(B) 684* *(C) 756* *(D) 810* *(E) 864*

Solução. : Para resolvermos esse problema devemos ter o primeiro e o último múltiplo de 6 que possuem dois algarismos, o primeiro será 12, pois $6 \times 2 = 12$ e o último será 96, pois $6 \times 16 = 96$. Podemos considerar uma PA de razão 6, sendo $a_1 = 12$ o primeiro termo e $a_n = 96$ seu último termo. Encontrando n teremos a quantidade de termos desta PA. Resolvemos:

$$\begin{gathered}12 + (n-1)\,6 = 96\\ 12 + 6n - 6 = 96\\ 6n = 90\\ n = 15\end{gathered}$$

Agora nos resta calcular a soma S_n dos termos, onde:

$$S_n = \frac{(a_1 + a_n) \cdot n}{2}$$

Tem-se que.

$$S_{15} = \frac{(12 + 96) \cdot 15}{2} = 810$$

Assim a soma dos múltiplos de 6 de dois algarismos será 810. □

Exercício 2.2. *Com quantos zeros termina o número* 100!.

Solução. : Sabemos que no desenvolvimento de 100! existem um número muito grande de múltiplos de 2, assim, nos resta saber a quantidade de múltiplos de 5 e 25, pois cada par formado por 2 e 5, produz um zero no final de 100!. Tomando como base o exercício anterior:

Para os múltiplos de 5: $a_1 = 5$, $a_n = 100$ e $r = 5$.

$$\begin{gathered}5 + (n-1)\,5 = 100\\ 5n = 100\\ n = 20.\end{gathered}$$

Para os múltiplos de 25: $a_1 = 25$, $a_n = 100$ e $r = 25$.

$$\begin{gathered}25 + (n-1)\,25 = 100\\ 25n = 100\\ n = 4.\end{gathered}$$

Somando as quantidades de múltiplos teremos $20 + 4 = 24$, logo 100! terá 24 zeros. □

Exercício 2.3. *Mostre que* $7 \mid 3a + 2b$ *se, e somente se* $7 \mid 4a - 2b$, *sendo* $a, b \in \mathbb{Z}$.

Solução 1. : Sendo $7 \mid 7a$ e $7 \mid 3a + 2b$, teremos $7a = 7q$ e $3a + 2b = 7k$, sendo $q, k \in \mathbb{Z}$. Subtraindo as equações respectivamente, teremos $4a - 2b = 7\,(q - k)$, logo $7 \mid 4a - 2b$.

Sendo $7 \mid 7a$ e $7 \mid 4a - 2b$, teremos $7a = 7q$ e $4a - 2b = 7k$, sendo $q, k \in \mathbb{Z}$. Subtraindo as equações respectivamente, teremos $3a + 2b = 7\,(q - k)$, logo $7 \mid 3a + 2b$. □

Solução 2. : Sendo $7 \mid 7a$, $7 \mid 3a+2b$ e como $4a-2b = 7a-3a-2b = \underbrace{7a}_{7|} - \underbrace{(3a+2b)}_{7|}$, concluímos assim que $7 \mid 4a-2b$.

Sendo $7 \mid 7a$, $7 \mid 4a-2b$ e como $3a+2b = 7a-4a+2b = \underbrace{7a}_{7|} - \underbrace{(4a-2b)}_{7|}$, concluímos assim que $7 \mid 3a+2b$. □

Exercício 2.4. *Sendo n um inteiro positivo, mostrar que $665 \mid (9^{3n} - 8^{2n})$.*

Solução. : Sendo $9^{3n} - 8^{2n}$, temos que:

$$\begin{aligned} 9^{3n} - 8^{2n} &= \left(9^3\right)^n - \left(8^2\right)^n \\ &= 729^n - 64^n \end{aligned}$$

Como $665 = 729 - 64$, então, pela fatoração 4 da página 12:

$$729^n - 64^n = (729-64)\left(729^{n-1} + 729^{n-2}64 - ... - 729.64^{n-2} + 64^{n-1}\right)$$

Logo $665 \mid (9^{3n} - 8^{2n})$. □

Exercício 2.5. *Para quais valores de $a \in \mathbb{N}$ temos $a-2 \mid a^3+4$.*

Solução. : Como $a^3-b^3 = (a-b)\left(a^2+ab+b^2\right)$, resulta $a-b \mid a^3-b^3$. Assim $a-2 \mid a^3-8$.

Sendo

$$\begin{aligned} a^3+4 &= a^3-8+8+4 \\ &= \left(a^3-2^3\right)+12 \end{aligned}$$

Devemos ter que $a-2 \mid 12$. Assim os únicos valores para a serão 3, 4, 5, 6, 8 e 14. □

Exercício 2.6. *Mostrar que o inteiro $N = 2^{48}-1$ é divisível por dois inteiros compreendidos entre 60 e 70.*

Solução. : Para a resolução do problema, faremos a fatoração de $2^{48}-1$, Assim:

$$\begin{aligned} 2^{48}-1 &= \left(2^{24}+1\right)\left(2^{24}-1\right) \\ &= \left(2^{24}+1\right)\left(2^{12}+1\right)\left(2^{12}-1\right) \\ &= \left(2^{24}+1\right)\left(2^{12}+1\right)\left(2^{6}-1\right)\left(2^{6}+1\right) \\ &= \left(2^{24}+1\right)\left(2^{12}+1\right)(65)(63) \end{aligned}$$

Assim os valores procurados são 63 e 65. □

Exercício 2.7. *Sendo $a, n \in \mathbb{N}$, mostre que se n divide a, então, 2^n-1 divide 2^a-1.*

Solução. : Como $n \mid a$, então, $a = nq$, sendo $q \in \mathbb{N}$. Então de acordo a fatoração 4 da página 12.

$$\begin{aligned} 2^a - 1 &= 2^{nq} - 1 \\ &= (2^n)^q - 1 \\ &= (2^n - 1) \cdot \left[(2^n)^{q-1} + (2^n)^{q-2} + ... + (2^n) + 1\right] \end{aligned}$$

Assim concluímos que $2^n - 1 \mid 2^a - 1$, quando $n \mid a$. □

Exercício 2.8. *Qual é o maior inteiro n para o qual $n^3 + 100$ é divisível por $n + 10$?*

Solução. : Para iniciarmos a resolução do problema, usaremos a identidade 3 da página 12 para encontrarmos o quociente e o resto da divisão de $n^3 + 100$ por $n + 10$. Sendo $n^3 + 10^3$, teremos:

$$n^3 + 10^3 = (n + 10)\left(n^2 - 10n + 100\right)$$

Então, a partir da fatoração acima podemos encontrar o quociente e o resto de $n^3 + 100$ por $n + 10$ da seguinte maneira.

$$\begin{gathered} n^3 + 1000 = (n + 10)\left(n^2 - 10n + 100\right) \\ n^3 + 100 + 900 = (n + 10)\left(n^2 - 10n + 100\right) \\ n^3 + 100 = (n + 10)\left(n^2 - 10n + 100\right) - 900 \end{gathered}$$

Dessa forma, para que $n + 10 \mid n^3 + 100$, devemos ter $n + 10 \mid 900$, logo, o maior inteiro n somado a 10 que divide 900 será $n = 890$. □

Exercício 2.9. *Encontre todos os naturais a e b tais que $a \mid b + 1$ e $b \mid a + 1$.*

Solução. : Pela **propriedade 2.1.5**, devemos ter que $a \leq b + 1$ e $b \leq a + 1$. Então $a - 1 \leq b \leq a + 1$. Vamos analisar os seguintes casos:

- Caso $a = b$.

  Como $a \mid b+1$ e $a \mid b$, temos que $a \mid [(b + 1) - b] = 1$. Assim, $a = 1$, logo, só teremos uma única solução $(a, b) = (1, 1)$

- Caso $a = b + 1$.

  Como $b \mid a + 1$ e $b \mid a - 1$, temos que $b \mid [(a + 1) - (a - 1)] = 2$. Assim, $b = 1$ ou $b = 2$ e nesse caso, teremos duas soluções para (a, b), $(3, 2)$ e $(2, 1)$.

- Caso $a = b - 1$.

  Como $a \mid b + 1$ e $a \mid b - 1$, temos que $a \mid (b + 1) - (b - 1) = 2$, assim teremos $a = 1$ ou $a = 2$ e nesse caso teremos duas soluções para (a, b); $(1, 2)$ e $(2, 3)$.

□

3 Divisão Euclidiana

Divisão euclidiana, divisão inteira ou divisão com resto é o processo de dividir um número inteiro por outro, de maneira que produza um quociente e um restante menor que o divisor. Sua principal característica é que o quociente e o restante existam e sejam únicos, assim como mostra o teorema abaixo.

Teorema 3.1. *Se a e b são dois inteiros, com $b > 0$, então existem e são únicos os inteiros q e r que satisfazem as condições:*

$$a = bq + r,\ 0 \leq r < b.$$

Demonstração. Seja S o conjunto de todos os inteiros não negativos que são da forma $a - bx$, com $x \in \mathbb{Z}$, isto é:

$$S = \{a - bx : x \in \mathbb{Z}, a - bx \geq 0\}$$

Este conjunto S não é vazio, porque, sendo $b > 0$, temos $b \geq 1$ e, portanto, para $x = -|a|$, resulta:

$$a - bx = a + b|a| \geq a + |a| \geq 0$$

Assim sendo, pelo *"Principio da boa ordem"*, existe o elemento mínimo r do conjunto S tal que $r \geq 0$ e $r = a - b$ ou $a = bq + r$, com $q \in \mathbb{Z}$. Além disso, temos $r < b$, pois, se fosse $r \geq b$, teríamos:

$$0 \leq r - b = a - bq - b = a - b(q + 1) \leq r_0 < r$$

Isto é, r não seria o elemento mínimo de S, já que existe $r_0 \in S$ com $r_0 < r$.

Para mostrar a unicidade de q e r, suponhamos que existem dois outros inteiros q_1 e r_1 tais que:

$$a = bq_1 + r_1, \text{ com } 0 \leq r_1 < b$$

Então, temos:

$$bq_1 + r_1 = bq + r \Rightarrow r_1 - r = (q - q_1)b$$

Assim concluímos que $b \mid (r_1 - r)$.

Por outro lado, teremos:

$$-b < -r \leq 0 \text{ e } 0 \leq r_1 < b$$

Somando as duas equações, implica:

$$-b < r_1 - r < b, \text{ isto é, } |r_1 - r| < b$$

Assim, $b \mid r_1 - r$ e $|r_1 - r| < b$, portanto, $r_1 - r = 0$ e como $b \neq 0$, também temos $q - q_1 = 0$. Logo, $r_1 = r$ e $q = q_1$. □

Corolário 3.1. *Se a e b são dois inteiros, com $b \neq 0$, existem e são únicos os inteiros q e r que satisfazem as condições:*

$$a = bq + r \text{ e } 0 \leq r < |b|$$

Demonstração. : Com efeito, se $b > 0$, nada há que demonstrar, e se $b < 0$, então $|b| > 0$, e, por conseguinte existem e são únicos os inteiros q_1 e r tais que:

$$a = |b|\, q_1 \text{ e } 0 \leq r < |b|$$

Ou seja, por ser $|b| = -b$:

$$a = b(-q_1) + r \text{ e } 0 \leq r < |b|$$

Portanto, existem e são únicos os inteiros $q = -q_1$ e r tais que:

$$a = bq + r \text{ e } 0 \leq r < |b|$$

□

Os inteiros q e r chamam-se respectivamente quociente e resto na divisão de a por b.

Observe que b é divisor de a se e somente se o resto $r = 0$. Neste caso, temos $a = bq$ e o quociente q na divisão exata de a por b indica-se também por $\frac{a}{b}$ ou a/b, onde $q = \frac{a}{b} = a/b$, que se lê "a sobre b".

3.1 Propriedades dos restos

propriedade 3.1.1. *O resto da divisão de uma soma por um número $a \in \mathbb{Z}^*$ é o mesmo que o da divisão da soma dos restos das parcelas por esse mesmo número.*

Demonstração. Sejam N e P, dois inteiros, tais que $N = aq_1 + r_1$ e $P = aq_2 + r_2$, sendo $q_1, q_2 \in \mathbb{Z}$ e $r_1, r_2 \in \mathbb{Z}$ seus respectivos quocientes e restos na divisão por $a \in \mathbb{Z}^*$, somando teremos:

$$\begin{aligned} N + P &= aq_1 + r_1 + aq_2 + r_2 \\ &= a(q_1 + q_2) + (r_1 + r_2) \\ &= aq' + r' \end{aligned}$$

Como $a \mid a(q_1+q_2)$, então a soma r_1+r_2 dividida por a vai resultar o valor do resto. □

propriedade 3.1.2. *O resto da divisão de um produto por um número $a \in \mathbb{Z}$ é o mesmo que o da divisão do produto dos restos dos fatores por esse número.*

Demonstração. Sejam N e P, dois inteiros, tais que $N = aq_1 + r_1$ e $P = aq_2 + r_2$, sendo $q_1, q_2 \in \mathbb{Z}$ e $r_1, r_2 \in \mathbb{Z}$ seus respectivos quocientes e restos na divisão por $a \in \mathbb{Z}^*$, fazendo a multiplicação teremos:

$$\begin{aligned} N \times P &= (aq_1 + r_1)(aq_2 + r_2) \\ &= a^2 q_1 q_2 + aq_1 r_2 + aq_2 r_1 + r_1 r_2 \\ &= a(aq_1 q_2 + q_1 r_2 + q_2 r_1) + (r_1 r_2) \\ &= aq' + r' \end{aligned}$$

Como $a \mid a(aq_1q_2 + q_1r_2 + q_2r_1)$, então o produto r_1r_2 dividido por a vai resultar o valor do resto. $\square$

3.2 Exercícios Resolvidos

Exercício 3.1. *Efetue a divisão euclidiana nos seguintes casos:*

(A) 38 por 5 *(B) 38 por -5* *(C) -27 por -6* *(D) -25 por 4*

Solução. : (A) Primeiro passo é encontrar um valor que multiplicado por 5, esteja mais próximo de 38, procedendo da seguinte forma:

$$
\begin{aligned}
38 - 5 &= 33\\
38 - (2)\cdot 5 &= 28\\
38 - (3)\cdot 5 &= 23\\
38 - (4)\cdot 5 &= 18\\
38 - (5)\cdot 5 &= 13\\
38 - (6)\cdot 5 &= 8\\
38 - (7)\cdot 5 &= 3
\end{aligned}
$$

Como $0 < 3 < |5|$, assim teremos que $q = 7$ e $r = 3$, pois $38 = 5 \cdot (7) + 3$.

(B) Seguiremos a mesma ideia do problema anterior:

$$38 - (-5) = 33$$

Para que possamos preservar a subtração, devemos multiplicar -5 por valores negativos.

$$
\begin{aligned}
38 - (-2)\cdot(-5) &= 28\\
38 - (-3)\cdot(-5) &= 23\\
38 - (-4)\cdot(-5) &= 18\\
38 - (-5)\cdot(-5) &= 13\\
38 - (-6)\cdot(-5) &= 8\\
38 - (-7)\cdot(-5) &= 3
\end{aligned}
$$

Como $0 < 3 < |-5|$, assim teremos $q = -7$ e $r = 2$, pois $38 = (-5)\cdot(-7) + 3$.

(C) Aplicando o método dos problemas anteriores:

$$-27 - (-6) = -21$$

Queremos encontrar um resultado inteiro positivo, multiplicaremos -6 por valores inteiros positivos.

$$
\begin{aligned}
-27 - (2)\cdot(-6) &= -15\\
-27 - (3)\cdot(-6) &= -9\\
-27 - (4)\cdot(-6) &= -3\\
-27 - (5)\cdot(-6) &= 3
\end{aligned}
$$

Como $0 < 3 < |-6|$, assim teremos $q = 5$ e $r = 3$, pois $-27 = (-6) \cdot (5) + 3$.

(D) Aplicando o método dos problemas anteriores:

$$-25 - 4 = -29$$

Queremos encontrar um resultado inteiro positivo, multiplicaremos 4 por valores inteiros negativos.

$$-25 - (-2) \cdot 4 = -17$$
$$-25 - (-3) \cdot 4 = -13$$
$$-25 - (-4) \cdot 4 = -9$$
$$-25 - (-5) \cdot 4 = -5$$
$$-25 - (-6) \cdot 4 = -1$$
$$-25 - (-7) \cdot 4 = 3$$

Como $0 < 3 < |4|$, assim teremos $q = -7$ e $r = 3$, pois $-25 = 4 \cdot (-7) + 3$. □

Exercício 3.2. *Uma fábrica produz chicletes que são embalados em pacotes de cinco unidades cada. Quantos pacotes serão produzidos com 3257 unidades?*

Solução. : Como cada pacote contém cinco unidades, devemos dividir 3257 por 5, afim de saber a quantidade de pacotes. Feita a divisão, ficará da seguinte forma:

$$3257 = 5 \cdot (651) + 2$$

Assim teremos 611 pacotes e mais duas unidades fora. □

Exercício 3.3. *A divisão de um certo número positivo N por 1994 deixa resto 148. Calcule o resto da divisão de* $N + 2000$ *pelo mesmo número 1994.*

Solução. : De acordo o enunciado do problema, pelo algoritmo da divisão:

$$N = 1994q + 148$$

onde $q \in \mathbb{Z}$ é o quociente da divisão.

Somando 2000 aos dois lados da igualdade.

$$N + 2000 = 1994q + 148 + 2000$$

Como $2000 = 1994 + 6$, teremos $N + 2000 = 1994q + 148 + 1994 + 6$, deixando 1994 em evidência ficará.

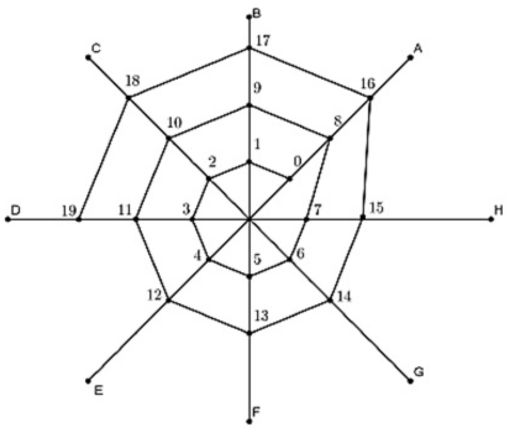
$$N + 2000 = 1994\,(q + 1) + 154$$

Como $q + 1 \in \mathbb{Z}$ e $154 < 1994$, o resto da divisão de $N + 200$ por 1994 será 154. □

Exercício 3.4. *A, B, C, D, E, F, G e H são fios de apoio que uma aranha usa para construir sua teia, conforme mostra a figura. A aranha continua seu trabalho. Sobre qual fio de apoio estará o número 118?*

Solução. : Colocaremos a problemática em uma tabela, até a segunda linha:

A	B	C	D	E	F	G	H
0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15



Como são 8 o número de colunas, os seus elementos quando divididos por 8 deixarão restos de acordo a última linha:

A	B	C	D	E	F	G	H
0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
$r = 0$	$r = 1$	$r = 2$	$r = 3$	$r = 4$	$r = 5$	$r = 6$	$r = 7$

Então, dividindo 118 por 8 teremos:

$$118 = 8 \cdot (14) + 6$$

Como o resto da divisão de 118 por 8 deixa resto 6, pela tabela acima concluímos que a aranha estará sobre o fio G. □

Exercício 3.5. *Qual o algarismo das unidades de* 3^{1998}.

Solução. : Para encontrarmos o algarismo das unidades, devemos conhecer os dígitos das unidades das potências consecutivas de 3:

3^0	1	3^4	1
3^1	3	3^5	3
3^2	9	3^6	9
3^3	7	3^7	7

Assim concluímos que o dígito das unidades das potências de 3 segue um padrão 4 a 4 nos valores dos dígitos, conhecendo esses valores, devemos descobrir o resto da divisão de cada expoente por quatro, gerando assim a seguinte tabela:

3^0	1	3^4	81	resto $= 0$
3^1	3	3^5	243	resto $= 1$
3^2	9	3^6	729	resto $= 2$
3^3	27	3^7	2187	resto $= 3$

- Se o resto da divisão do expoente por 4 é 0 o digito das unidades é 1.

- Se o resto da divisão do expoente por 4 é 1 o digito das unidades é 3.
- Se o resto da divisão do expoente por 4 é 2 o digito das unidades é 9.
- Se o resto da divisão do expoente por 4 é 3 o digito das unidades é 7.

Agora dividindo 1998 por 4:

$$1998 = 4 \cdot (499) + 2$$

Pela análise acima o algarismo das unidades de 3^{1998} é 9.

Exercício 3.6. *Achar o resto da divisão de 6^{2012} por 10.*

Como a divisão é por 10, precisamos saber apenas o algarismo das unidades de 6^{2012} para concluirmos a resolução do problema.

Para isso, iremos fazer uma tabela que nos mostre as potências de 6:

6^0	1
6^1	6
6^2	36
6^3	216
6^4	1296

Se $n > 1$, 6^n terá a seguinte representação $6^n = 10 \cdot q + 6$, sendo $q \in \mathbb{Z}$ onde terá 6 como último algarismo, assim 6^{2012}, o resto da divisão procurado é 6. $\square$

Exercício 3.7. *Considere a e b dois números inteiros, tais que $a - b = 23$, sendo $b > 0$. Sabendo-se que, na divisão de a por b, o quociente é 8 e o resto é o maior valor possível nessa divisão, então $a + b$ é igual a.*

(A) 29 *(B) 26* *(C) 32* *(D) 36*

Solução. : Como na divisão de a por b o quociente é 8 e o resto é maior possível, temos que $r = b - 1$. Assim resulta o seguinte sistema:

$$\begin{cases} a - b = 23 \\ a = 8b + b - 1 \end{cases} \quad \text{ou seja,} \quad \begin{cases} a - b = 23 \\ a - 9b = -1 \end{cases}$$

A partir da equação $a - b = 23$ temos $a = 23 + b$, substituindo na equação $a - 9b = -1$.

$$\begin{aligned} (23 + b) - 9b &= -1 \\ 23 - 8b &= -1 \\ -8b &= -24 \\ b &= 3 \end{aligned}$$

Substituindo b na equação $a = 23 + b$, encontraremos $a = 26$.

Concluímos assim que $a + b = 29$. Alternativa (A). $\square$

Exercício 3.8. *Determinar o resto r da divisão por 3 da soma* $34+2487+36427+6123134$, *sem efetuá-la.*

Solução. : Para resolvermos esse problema usaremos a **propriedade 4.1.1**

Vamos dividir cada parcela por 3.

$$34 = 3 \cdot (11) + 1$$
$$2487 = 3 \cdot (829) + 0$$
$$36427 = 3 \cdot (12142) + 1$$
$$6123134 = 3 \cdot (2041044) + 2$$

Somando os restos teremos $1 + 0 + 1 + 2 = 4$, como 4 dividido por 3 deixa resto 1, encontramos assim nossa solução, $r = 1$. □

Exercício 3.9. *Qual é o resto da divisão de* $2010 \times 2011 \times 2012$ *por 12:*

(A) 0 *(B) 2* *(C) 4* *(D) 6* *(E) 10*

Solução. : Segundo a **propriedade 4.1.2**, devemos fazer as seguintes divisões, 2010 por 12, 2011 por 12 e 2012 por 12:

$$2010 = 12 \cdot (167) + 6$$
$$2011 = 12 \cdot (167) + 7$$
$$2012 = 12 \cdot (167) + 8$$

Multiplicando os restos teremos $6 \times 7 \times 8 = 336$. Dividindo 336 por 12, teremos:

$$336 = 12 \cdot (28) + 0$$

Assim a resposta do problema será resto zero, alternativa (A). □

Exercício 3.10. *Dois colecionadores de selos têm, juntos, 500 selos. Cada colecionador comprou um álbum para colocar seus selos. Os dois álbuns eram idênticos, tendo o mesmo número de páginas. Se o primeiro colecionador colocar exatamente 21 selos em cada página, ele vai conseguir colocar todos os seus selos e usar todas as páginas do álbum. Se o segundo colecionador colocar 20 de seus selos em cada página do álbum, sobrarão alguns selos. Caso ele coloque 23 selos em cada página, sobra pelo menos uma, totalmente vazia, podendo haver ainda uma outra página com menos de 23 selos. Quantas páginas há no álbum?*

Solução. : Sejam n o número de páginas do álbum, x o número de selos do segundo colecionador e $500 - x$ o número de selos do primeiro colecionador, então teremos:

- Com 21 selos por página o primeiro colecionador completa o álbum sem sobra de selos e de páginas, então $21n = 500 - x$, então $x = 500 - 21n$.

- Com 20 selos por página o álbum do segundo colecionador fica completo e sobram selos, então $x > 20n$, logo $500 - 21n > 20n$, ou seja $n < 13$.

- Com com 23 selos por página o álbum do segundo colecionador fica com pelo menos uma página totalmente vazia, então $x < 23 \cdot (n - 1)$, então $500 - 21n < 23n - 23$, ou seja, $n > 11$.

Portanto podemos concluir que o álbum possui 12 páginas. □

Exercício 3.11. *Mostre que de três inteiros consecutivos um e apenas um deles é múltiplo de 3.*

Solução. : Suponha que os três inteiros consecutivos sejam a, $a + 1$ e $a + 2$. Pelo algorítimo da divisão temos as seguintes possibilidades: a deixa resto 0, 1 ou 2 quando dividido por 3.

- Suponha que a deixe resto 0 quando dividido por 3, ou seja, $a = 3q$. Logo, $a + 1 = 3q + 1$ e $a + 2 = 3q + 2$. Assim, um e apenas um dos três números é múltiplo de 3, a saber, a.

- Suponha que a deixe resto 1 quando dividido por 3, ou seja, $a = 3q + 1$. Logo, $a+1 = 3q+2$ e $a+2 = 3q+3 = 3\,(q + 1)$. Assim, um e apenas um dos três números é múltiplo de 3, a saber, $a + 2$.

- Suponha que a deixe resto 2 quando dividido por 3, ou seja, $a = 3q + 2$. Logo, $a + 1 = 3q + 3 = 3\,(q + 1)$ e $a + 2 = 3q + 4 = 3\,(q + 1) + 1$. Assim, um e apenas um dos três números é múltiplo de 3, a saber, $a + 1$.

□

Definicão 2. *Três primos consecutivos são chamados primos trigêmeos se o módulo da diferença entre dois primos consecutivos da terna é 2.*

Exercício 3.12. *a) Mostre que dados três números a, $a + 2$ e $a + 4$, um e apenas um deles é múltiplo de 3. b) Usando este fato, mostre que a única terna de primos trigêmeos é (3, 5, 7).*

Solução. : a) Se $a \in \mathbb{N}$, podemos escrever $a = 3k + r$, com $r = 0$, 1 ou 2.

- Se $r = 0$, temos $a = 3k$, $a + 2 = 3k + 2$ e $a + 4 = 3k + 4 = 3\,(k + 1) + 1$. Logo apenas a é múltiplo de 3.

- Se $r = 1$, temos $a = 3k+1$, $a+2 = 3k+3 = 3\,(k + 1)$ e $a+4 = 3k+5 = 3\,(k + 1)+2$. Logo apenas $a + 2$ é múltiplo de 3.

- Se $r = 2$, temos $a = 3k+2$, $a+2 = 3k+4 = 3(k+1)+1$ e $a+4 = 3k+6 = 3(k+2)$. Logo apenas $a+4$ é múltiplo de 3.

b) Dados três primos a, $a+2$ e $a+4$, pelo item (a), apenas um deles é múltiplo de 3. Sendo este número primo, ele deve ser 3. Portanto, a única possibilidade é $a = 3$, $a+2 = 5$ e $a+4 = 7$. □

4 Paridade de um Inteiro

Na divisão de um inteiro qualquer a por $b = 2$ os possíveis restos serão $r = 0$ ou $r = 1$. Se $r = 0$, então o inteiro $a = 2q$ é denominado par, por outro lado, se $r = 1$, então o inteiro $a = 2q+1$ é denominado ímpar.

Observação: Elevando ao quadrado um número par e um impar:

$a^2 = (2q)^2 = 4q^2$

$a^2 = (2q+1)^2 = 4q^2 + 4q + 1 = 4(q^2+q) + 1$, onde $(q^2+q) \in \mathbb{Z}$

Assim na divisão do quadrado de um inteiro qualquer por 4 o resto é 0 ou 1. 0 se a for par e 1 se a for ímpar.

4.1 Algumas operações

Dados dois números inteiros N e P, iremos determinar suas paridades.

4.1.1 Soma

- Caso 1: N e P pares.

  Sendo $N = 2k$ e $P = 2q$, onde $k, q \in \mathbb{Z}$.

  Somando ambos teremos $N + P = 2k + 2q = 2(k+q)$, onde $k + q \in \mathbb{Z}$.

- Caso 2: N e P ímpares.

  Sendo $N = 2k+1$ e $P = 2q+1$, onde $k, q \in \mathbb{Z}$.

  Somando ambos teremos $N + P = 2k + 1 + 2q + 1 = 2k + 2q + 2 = 2(k+q+1)$, onde $(k+q+1) \in \mathbb{Z}$.

- Caso 3: N ímpar e P par.

  Sendo $N = 2k+1$ e $P = 2q$, onde $k, q \in \mathbb{Z}$.

  Somando ambos teremos $N + P = 2k + 1 + 2q = 2(k+q) + 1$, onde $(k+q) \in \mathbb{Z}$.

Concluímos assim que em uma soma de dois pares, seu resultado será par, na soma de dois ímpares sua soma será par e na soma de um par e um ímpar, resultará ímpar.

4.1.2 Multiplicação

- Caso 1: N e P pares.

  Se $N = 2k$ e $P = 2q$, onde $k, q \in \mathbb{Z}$.

  Multiplicando ambos teremos $N \times P = 2q \times 2k = 4kq = 2(2kq)$, onde $kq \in \mathbb{Z}$.

- Caso 2: N e P ímpares.

  Se $N = 2k + 1$ e $P = 2q + 1$, onde $k, q \in \mathbb{Z}$.

  Multiplicando ambos $N \times P = (2k+1)(2q+1) = 4kq+2k+2q+1 = 2(2kq+k+q)+1$, onde $(2kq + k + q) \in \mathbb{Z}$.

- Caso 3: N ímpar e P par.

  Se $N = 2k + 1$ e $P = 2q$, onde $k, q \in \mathbb{Z}$.

  Multiplicando ambos $N \times P = (2k+1)(2q) = 4kq+2q = 2(2kq+q)$, onde $(2kq+q) \in \mathbb{Z}$.

Concluímos assim que um uma multiplicação de dois pares, seu resultado será par, na multiplicação de dois ímpares, resultará ímpar e na multiplicação entre um par e um ímpar, resultará par.

4.2 Exercícios Resolvidos

Exercício 4.1. *Qual das expressões abaixo tem como resultado um número ímpar?*

(A) $7 \times 5 \times 11 \times 10 \times 2$

(B) $(2005 - 2003) \times (2004 + 2003)$

(C) $7 + 9 + 11 + 13 + 15 + 17$

(D) $5^2 + 3^2$

(E) $3 \times 5 + 7 \times 9 + 11 \times 13$

Solução. : Para não termos o trabalho de multiplicarmos tudo ou somarmos de maneira bem direta, que seria perda de tempo, faremos a seguinte análise:

(A) Produto de três ímpares, resultará ímpar, multiplicado por um par, resultará par.

(B) Subtração de dois ímpares resulta em par multiplicado por um resultado ímpar, resultará par.

(C) Soma de seis ímpares será par.

(D) Potência de ímpar resulta em ímpar, soma de ímpares será par.

(E) Produto entre ímpares gera ímpar, soma de três ímpares, resultado ímpar.

Solução do nosso problema será alternativa (E). □

Exercício 4.2. *Existem números inteiros a e b que satisfazem a igualdade $a \cdot b \cdot (a - b) = 8507$?*

Solução. : Para que haja solução o produto entre a, b e $(a-b)$ deverá ser ímpar.

Caso a seja par ou b par, o produto obviamente será par.

Caso a seja ímpar e b seja par, o produto $a \cdot b$ será par, logo o produto $ab(a-b)$ será par.

Caso a seja ímpar e b ímpar também o produto $a \cdot b$ será ímpar, porém $(a-b)$ será par, resultando em um produto par.

Assim concluímos que a igualdade não poderá ser satisfeita, pois o número $a \cdot b \cdot (a-b)$ sempre é par. $\square$

Exercício 4.3. *Determine a paridade do seguinte número:*

$$(123275 + 346231)^{234} + (3451 + 4532)^{542}$$

Solução. : Primeiramente efetuaremos as somas:

$$(123275 + 346231)^{234} + (3451 + 4532)^{542} = (469506)^{234} + (7983)^{542}$$

Para $(469506)^{234}$, teremos um resultado par, pois o produto de números pares, sempre será par.

Para $(7983)^{542}$, teremos resultado ímpar, pois o produto de números ímpares, sempre resultará em ímpar.

Somando as parcelas teremos como resultado um número ímpar, pois par somado a ímpar resulta em ímpar. $\square$

Exercício 4.4. *Os números de 1 a 10 estão escritos em uma linha. É possível colocar os sinais de "$+$" e de "$-$" entre eles de modo que o valor da expressão resultante seja igual a zero?*

Solução. : Para que isso seja possível, deve-se dividir o conjunto dos números de 1 a 10 em dois grupos de somas iguais para colocar um conjunto de "$+$" em um deles e no outro grupo, colocar outro conjunto de "$-$" e entre os grupos um sinal de "$+$". Ou seja, a soma de todos os números de 1 a 10 deve ser par para haver tal possibilidade. Porém, a soma é 55. Logo, não é possível. $\square$

Exercício 4.5. *Em um quartel existem 100 soldados e, todas as noites, três desses soldados são escolhidos para trabalhar de sentinela. É possível que, após certo tempo, um dos soldados tenha trabalhado com cada um dos outros exatamente uma vez?*

Solução. : Fixando um soldado qualquer, para cada noite em que trabalhe, o soldado deverá ter a companhia de dois soldados diferentes. Assim, será necessário agruparmos os demais soldados de 2 em 2 para definirmos as escalas do soldado fixado, ou seja, necessitaremos de um número par de soldados. Mas, além do soldado fixado, há um número ímpar de soldados que sobrou no quartel. Portanto, não podemos formar pares de soldados diferentes para trabalhar com o soldado fixo, consequentemente deve ter trabalhado com pelo menos um mais de uma vez. $\square$

Exercício 4.6. *Cada um de nós, ao longo da vida, teremos saudado com um aperto de mão muitas pessoas. Mostrar que em qualquer grupo é par o número de pessoas que já apertaram um número ímpar de mãos no grupo.*

Solução. : Indiquemos por N o número de pessoas do grupo, por n_k o número de apertos de mão dados pela pessoa k, e seja m o número total de apertos de mão trocados. Temos:

$$n_1 + n_2 + n_3 + ... + n_k = 2m$$

Ora, como o resultado dessa soma é par, ela tem de ter um número par de parcelas ímpares. □

Exercício 4.7. *Sejam a e b números naturais relacionados da forma $a = 1 + b^2$. Se b é ímpar, prove que a é par.*

Solução 1. : Sendo $a = 1 + b^2$, como $b = 2k + 1$, sendo $k \in \mathbb{Z}$, então:

$$\begin{aligned} a &= 1 + (2k+1)^2 \\ &= 1 + 4k^2 + 4k + 1 \\ &= 4k^2 + 4k + 2 \\ &= 2\left(2k^2 + 2k + 1\right) \end{aligned}$$

Como $(2k^2 + 2k + 1) \in \mathbb{Z}$, então provamos que a é par. □

Solução 2. : Como $b^2 = a - 1$ é um número ímpar, então claramente a deverá ser par. □

Exercício 4.8. *Mostre que o dobro de um número ímpar é par mas nunca múltiplo de 4.*

Solução. : Para um número N ser ímpar basta considerar $N = 2q + 1$. Na divisão por 4 temos somente as possibilidades $N = 4q + 1$ e $N = 4q + 3$, sendo $q \in \mathbb{Z}$

Tomando o dobro de cada valor, teremos:

- $N = 2q + 1$:

  $2N = 2(2q + 1)$, como $2q + 1 \in \mathbb{Z}$, obviamente $2N$ será par, porém $N = 4q + 2$, deixa resto dois na divisão por 4.

- $N = 4q + 1$:

  $2N = 2(4q + 1)$, como $4q + 1 \in \mathbb{Z}$, então $2N$ será par, porém $N = 8q + 2$, deixando resto dois na divisão por 4.

- $N = 4q + 3$:

  $2N = 2(4q + 3)$, como $4q + 3 \in \mathbb{Z}$, então $2N$ será par, porém $N = 8q + 6 = 8q + 4 + 2 = 4(2q + 1) + 2$, deixando resto dois na divisão por 4.

$\square$

Exercício 4.9. *Se k é um número ímpar, prove que $k^2 - 1$ é divisível por 8.*

Solução 1. : Qualquer ímpar é da forma $k = 4q + 1$ ou $k = 4q + 3$, sendo $q \in \mathbb{Z}$, assim:

- Se $k = 4q + 1$

$$\begin{aligned} k^2 - 1 &= (4q+1)^2 - 1 \\ &= 16q^2 + 8q + 1 - 1 \\ &= 16q^2 + 8q = 8\left(2q^2 + q\right) \end{aligned}$$

  Como $(2q^2 + q) \in \mathbb{Z}$, então $k^2 - 1$ será divisível por 8.

- Se $k = 4q + 3$

$$\begin{aligned} k^2 - 1 &= (4q+3)^2 - 1 \\ &= 16q^2 + 24q + 9 - 1 \\ &= 16q^2 + 24q + 8 = 8\left(2q^2 + 3q + 1\right) \end{aligned}$$

  Como $(2q^2 + 3q + 1) \in \mathbb{Z}$, então $k^2 - 1$ será divisível por 8.

$\square$

Solução 2. :
Sendo $k = 4q + 1$, $q \in \mathbb{Z}$, então.

$$\begin{aligned} k^2 &= (4q+1)^2 \\ &= 16q^2 + 8q + 1 \\ &= 8\left(2q^2 + q\right) + 1 \end{aligned}$$

Como $k^2 = 8(2q^2 + q) + 1$, então $k^2 - 1 = 8(2q^2 + q)$.

$\square$

Exercício 4.10. *Sendo a e b dois inteiros quaisquer, mostrar que os inteiros a e $a + 2b$ tem sempre a mesma paridade.*

Solução. : Sejam $k, q \in \mathbb{Z}$, vamos analisar os seguintes casos.

- Sejam a e b pares, isto é, $a = 2q$ e $b = 2k$:

  Como $a = 2q$, então $a + 2b = 2q + 4k = 2(q + 2k)$, segue que a e $a + 2b$ tem a mesma paridade.

- Sejam a e b ímpares, isto é, $a = 2q + 1$ e $b = 2k + 1$:

  Como $a = 2q + 1$, então $a + 2b = 2q + 1 + 4k + 2 = 2(q + 2k + 1) + 1$, eles tem a mesma paridade.

- Seja a ímpar e b par, isto é, $a = 2q + 1$ e $b = 2k$:

  Como $a = 2q + 1$, então $a + 2b = 2q + 1 + 4k = 2(q + 2k) + 1$, segue que a e $a + 2b$ tem a mesma paridade.

- Seja a par e b ímpar, isto é, $a = 2q$ e $b = 2k + 1$:

  Como $a = 2q$, então $a + 2b = 2q + 4k + 2 = 2(q + 2k + 1)$, segue que a e $a + 2b$ tem a mesma paridade.

□

Exercício 4.11. *Mostre que dentre dois inteiros consecutivos um deles é par e o outro ímpar.*

Solução. : Supondo um inteiro qualquer n, seu sucessor será $n + 1$, vamos analisar os dois casos possíveis:

- Seja $n = 2q$ (Par), sendo $q \in \mathbb{Z}$. Então $n + 1 = 2q + 1$, ímpar.

  Então para n par, teremos $2q$ e $2q + 1$ dois números consecutivos.

- Seja $n = 2q + 1$ (Ímpar), sendo $q \in \mathbb{Z}$. Então $n + 1 = 2q + 2 = 2(q + 1)$, par.

  Então para n ímpar, teremos $2q + 1$ e $2q + 2$ dois consecutivos.

□

5 Sistemas de Numeração

Sistema de Numeração é a representação consistente de um conjunto de números e suas várias utilidades, dando ao mesmo uma única representação, refletindo suas estruturas algébricas e aritméticas.

Nosso sistema convencional é o decimal, porém não é a única forma de representar um número, exemplo disso é a base 60 usada para contar tempo em minutos e segundos, a base 12, muito utilizada no comércio, a base 2 na linguagem computacional, entre outra bases, assim como essas veremos adiante outras formas de representação de um número.

Como já mencionado anteriormente, no sistema decimal todo e qualquer inteiro sendo ele 2, 4, 35, 100..., pode ser escrito na forma:

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

onde $0 \leq a_n \leq 9$, sendo $n \in \mathbb{N}$.

Exemplo 3: O número 1998, na base 10, tem a seguinte representação

$$N = 1.10^3 + 9.10^2 + 9.10 + 8$$

Os sistemas de numeração baseiam-se nos seguintes teoremas.

Teorema 5.1. *Dado um inteiro qualquer $b \geq 2$, todo inteiro positivo n admite uma única representação da forma:*

$$n = a_m b^m + a_{m-1} b^{m-1} + ... + a_2 b^2 + a_1 b + a_0$$

onde os coeficientes a_i são tais que $0 \leq a_i < b$, sendo $i = 0, 1, 2, ..., m$.

Demonstração. Pelo algoritmo da divisão aplicado nos inteiros n e b, temos que:

$$n = bq_1 + a_0, \text{ onde } 0 \leq a_0 < b$$

Aplicando, agora, o algoritmo da divisão ao quociente q_1 e ao inteiro b, temos:

$$q_1 = bq_2 + a_1, \text{ onde } 0 \leq a_1 < b$$

Continuando a aplicar o algoritmo da divisão aos quocientes obtidos q_i e ao inteiro b, temos:

$$q_2 = bq_3 + a_2, \text{ onde } 0 \leq a_2 < b$$
$$q_3 = bq_4 + a_3, \text{ onde } 0 \leq a_3 < b$$

e assim por diante.

Como $n > q_1 > q_2 > q_3 > ...$ e cada $q_i \geq 0$, esta sequência decrescente dos quocientes q_i é finita, isto é, existe um índice m tal que:

$$q_{m-1} = bq_m + a_{m-1}, \text{ onde } 0 \leq a_{m-1} < b$$
$$q_m = b \cdot 0 + a_m = a_m, \text{ onde } 0 \leq a_m < b$$

Multiplicando por b ambos os membros de $q_1 = bq_2 + a_1$, por b^2 ambos os membros de $q_2 = bq_3 + a_2$, por b^3 ambos os membros de $q_3 = bq_4 + a_3$, ..., por b^{m-1} ambos os membros de $q_{m-1} = bq_m + a_{m-1}$, obtemos o conjunto de igualdades:

$$n = bq_1 + a_0, \text{ onde } 0 \leq a_0 < b$$
$$bq_1 = b^2 q_2 + a_1 b, \text{ onde } 0 \leq a_1 < b$$
$$b^2 q_2 = b^3 q_3 + a_2 b^2, \text{ onde } 0 \leq a_2 < b$$
$$b^3 q_3 = b^4 q_4 + a_3 b^3, \text{ onde } 0 \leq a_3 < b$$
$$................................$$
$$b^{m-1} q_{m-1} = b^m q_m + a_{m-1} b^{m-1}, \text{ onde } 0 \leq a_{m-1} < b$$

Somando ordenadamente todas essas igualdades, teremos:

$$n + (bq_1 + b^2q_2 + ... + b^{m-1}q_{m-1})$$
$$(bq_1 + b^2q_2 + ... + b^{m-1}q_{m-1}) + a_0 + a_1b + a_2b^2 + ... + a_{m-1}b^{m-1} + a_mb_m$$
$$n = a_mb^m + a_{m-1}b^{m-1} + ... + a_2b^2 + a_1b + a_0$$

□

Teorema 5.2. *Um número possui apenas uma única representação em determinada base.*

Demonstração. Suponhamos. por absurdo, que um determinado número n possua duas diferentes representações em uma determinada base b, $n = a_nb^n + a_{n-1}b^{n-1} + ... + a_2b^2 + a_1b + a_0$ e $n = c_mb^m + c_{m-1}b^{m-1} + ... + c_2b^2 + c_1b + c_0$.

Igualando os números, teremos:

$$a_nb^n + a_{n-1}b^{n-1} + ... + a_2b^2 + a_1b + a_0 = c_mb^m + c_{m-1}b^{m-1} + ... + c_2b^2 + c_1b + c_0.$$
$$c_0 - a_0 = a_nb^n + a_{n-1}b^{n-1} + ... + a_2b^2 + a_1b - c_mb^m - c_{m-1}b^{m-1} - ... - c_2b^2 - c_1b$$
$$c_0 - a_0 = b(a_nb^{n-1} + a_{n-1}b^{n-2} + ... + a_2b + a_1 - c_mb^{m-1} - c_{m-1}b^{m-2} - ... - c_2b - c_1)$$

Assim comprovamos que $b \mid c_0 - a_0$.

Entretanto, como a_0 e c_0 são dígitos em base b tem-se que $0 \leq a_0, c_0 \leq b - 1$, fazendo com que o intervalo de variação de $c_0 - a_0$ obedeça o intervalo $-(b-1) \leq c_0 - a_0 \leq b - 1$. Neste intervalo o único número inteiro divisível por b é zero, ou seja, obrigatoriamente temos $a_0 = c_0$.

Assim $a_nb^n + a_{n-1}b^{n-1} + ... + a_2b^2 + a_1 - c_mb^m - c_{m-1}b^{m-1} - ... - c_2b^2 - c_1 = 0$.

refazendo o procedimento anterior.

$$c_1 - a_1 = a_nb^{n-1} + a_{n-1}b^{n-2} + ... + a_2b - c_mb^{m-1} - c_{m-1}b^{m-2} - ... - c_2b$$
$$c_1 - a_1 = b(a_nb^{n-2} + a_{n-q}b^{n-3} + ... + a_2 - c_mb^{m-2} - c_{m-1}b^{m-3} - ... - c_2)$$

Comprovando novamente que $b \mid c_1 - a_1$. Pelo mesmo critério anterior, concluímos que $a_1 = c_1$.

Prosseguindo pelo mesmo processo conclui-se que $a_3 = c_3$, $a_4 = c_4$, ..., $a_n = c_m$.

Assim as duas representações são idênticas, implicando que existe uma, e somente uma maneira de representar um número em uma determinada base. □

Com base nos teoremas, queremos abordar como comparar dois números escritos em suas expansões na base b, onde segue a proposição abaixo.

Proposição 5.1. *Sejam dados os números inteiros $b > 1$, $n,n' \geq 0$, $0 \leq r_0, ..., r_n < b$ e $0 \leq r'_0, ..., r'_{n'} < b$, tem-se que:*

1. $r_0 + r_1b + ... + r_nb^n < b^{n+1}$;

2. $n > n'$ *e* $r_n \neq 0 \Longrightarrow r_0 + r_1b + ... + r_nb^n > r'_0 + r'_1b + ... + r'_{n'}b^{n'}$.

3. $n = n'$ *e* $r_n > r'_n \Longrightarrow r_0 + r_1b + ... + r_nb^n > r'_0 + r'_1b + ... + r'_{n'}b^{n'}$

Demonstração. 1. Temos, para todo $i = 0, 1, ..., n$, que $r_i \leq b - 1$ e $r_i b^i \leq (b-1)\, b^i = b^{i+1} - b^i$.

Tomando o somatório de ambos os lados do exposto acima, ao variar de i no intervalo $0 \leq i \leq n$, obtemos

$$r_0 + r_1 b + ... + r_n b^n \leq b^{n+1} - 1 < b^{n+1}.$$

2. Pelo item anterior, temos que se $n > n'$ e $r_n \neq 0$, então

$$r_0' + r_1' b + ... + r_{n'}' b^{n'} < b^{n'+1} \leq b^n \leq r_0 + r_1 b + ... + r_n b^n.$$

3. Nessa situação, temos por (2) que

$$r_0 + r_1 b + ... + (r_n - r_n')\, b^n > r_0' + r_1' b + ... + r_{n-1}' b^{n-1}.$$

o que prova o resultado, já que $(r_n - r_n') > 0$.

□

A partir do exposto acima, mostraremos de forma prática como funciona a mudança de base através de exercícios.

5.1 Exercícios Resolvidos

Exercício 5.1. *Represente o número 723 na base 5.*

Solução. : Pra representarmos o número em outra base, faremos divisões euclidianas sucessivas.

$$\begin{aligned} 723 &= 5 \cdot (144) + 3 \\ 144 &= 5 \cdot (28) + 4 \\ 28 &= 5 \cdot (5) + 3 \\ 5 &= 5 \cdot (1) + 0 \\ 1 &= 5 \cdot (0) + 1 \end{aligned}$$

Portanto,

$$723 = 1 \cdot 5^4 + 0 \cdot 5^3 + 3 \cdot 5^2 + 4 \cdot 5 + 3$$

e, consequentemente, $723 = [10343]_5$.

A expressão $N = a_n b^n + a_{n-1} b^{n-1} + ... + a_1 b + a_0$ será denotado por $N = [a_0 a_1 ... a_n]_b$, para representar um número $N = a_0 a_1 ... a_n$, na base b. □

Observação 4. *Se $b \geq 11$ na representação de $N = [a_n a_{n-1} ... a_1 a_0]_b$ utiliza-se os símbolos gregos α, β,..., para representar os "dígitos" acima de 10.*

Exercício 5.2. *Representar o número 4967 na base 12.*

Solução. : Como a base b é maior do que 10, devemos acrescentar novos símbolos para representar os números 10, 11 e outros valores acima de 10, que se tornam algarismos de um $N \in \mathbb{Z}_+$. Para isso denotaremos por α, β, e outras letras gregas que a substituem.

Assim,

$$\begin{aligned} 4967 &= 12 \cdot (413) + 11 \\ 413 &= 12 \cdot (34) + 5 \\ 34 &= 12 \cdot (2) + 10 \\ 2 &= 12 \cdot (0) + 2, \end{aligned}$$

Portanto,

$$4967 = 11 + 5 \cdot 12 + 10 \cdot 12^2 + 2 \cdot 12^3$$

Os números 10 e 11 serão substituídos por α e β respectivamente.

Logo, $4967 = [2\alpha 5\beta]_{12}$. □

Exercício 5.3. *Escreva o número* $[1001]_2$ *na forma decimal.*

Solução. :

Basta fazer a representação na base 2 e efetuar.

$$1001 = 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 8 + 1 = 9$$

Ou seja $[1001]_2 = [9]_{10}$.

□

O sistema de numeração em base dois é chamado de binário e os algarismos binários são conhecidos como bits, podendo assumi unicamente 0 ou 1 em sua composição.

Exercício 5.4. *No sistema de numeração de base 3 um número é escrito como 2101. Determine o sistema no qual esse número se escreve 224.*

Solução. : Das hipóteses dada, resulta na base 10:

$$\begin{gathered} [2101]_3 = [224]_b \\ 2 \cdot 3^3 + 1 \cdot 3^2 + 0 \cdot 3 + 1 = 2 \cdot b^2 + 2 \cdot b + 4 \\ 2 \cdot b^2 + 2 \cdot b + 4 = 64 \\ 2 \cdot b^2 + 2 \cdot b - 60 = 0 \\ b^2 + b - 30 = 0 \\ (b+6)(b-5) = 0 \end{gathered}$$

Assim o único valor possível para b será 5. □

Exercício 5.5. *Os números naturais* $a = 2121$ *e* $b = 136$ *estão escritos nos sistemas de numeração de bases 3 e 7, respectivamente.*

(a) Como se procede para descobrir qual deles é o maior?

(b) Determine, então, o maior deles.

Solução. : (a) Primeiro deve colocá-los na base decimal e fazer a comparação.

(b) Convertendo $[2121]_3$ e $[136]_7$ para base decimal, teremos.

$$[2121]_3 = 2 \cdot 3^3 + 1 \cdot 3^2 + 2 \cdot 3 + 1 = 70$$
$$[136]_7 = 1 \cdot 7^2 + 3 \cdot 7 + 6 = 76$$

Com isso concluímos que $b > a$. □

Exercício 5.6. *Admita a possibilidade de contar objetos de duas maneiras, uma na base* x *e outra na base* $(x+3)$*. Ao empregar essas duas maneiras para contar um determinado grupo de objetos, obtemos* $[2343]_x = [534]_{x+3}$*. Determine o valor da base* x*.*

Solução. : Na base 10:

$$\begin{aligned}
[2343]_x &= [534]_{x+3} \\
2 \cdot x^3 + 3 \cdot x^2 + 4 \cdot x + 3 &= 5\,(x+3)^2 + 3\,(x+3) + 4 \\
2x^3 + 3x^2 + 4x + 3 &= 5x^2 + 30x + 45 + 3x + 13 \\
2x^3 - 2x^2 - 29x - 55 &= 0 \\
x^3 - x^2 - \frac{29}{2}x - \frac{55}{2} &= 0 \\
(x-5)\left(x^2 + 4x + \frac{11}{2}\right) &= 0
\end{aligned}$$

Como x é base de um sistema de numeração em que os valores devem ser inteiros positivos, então $x = 5$, pois as outras raízes serão da forma $-2 + 3i$ e $-2 - 3i$. □

Exercício 5.7. *Calcule quantos números de três algarismos distintos existem no sistema de base 7.*

Solução. : Como é um sistema de base 7, logo só teremos 0, 1, 2, 3, 4, 5 e 6 como dígitos.

Como o primeiro dígito só poderá ser 1, 2, 3, 4, 5 ou 6, então teremos 6 possibilidades para o primeiro algarismo.

Já no segundo teremos a presença do zero menos o número que foi colocado como primeiro algarismo, assim teremos também 6 possibilidades.

Já no terceiro teremos todas as possibilidades menos os dois números colocados nos dois primeiros algarismos, assim teremos 5 possibilidades.

Assim no sistema de base 7 existem $6 \times 6 \times 5 = 180$ números de 3 algarismos. □

Exercício 5.8. *Escreva o número* $2^n - 1$ *na base 2, sendo* $n \in \mathbb{N}$ *e* $n \geq 2$*.*

Solução. : Para resolvermos esse problema, temos que ter em mente a seguinte fatoração:

$$a^n - b^n = (a-b)\left(a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1}\right), \text{ sendo } n \in \mathbb{N} \text{ e } n \geq 2.$$

Tomando como base a fatoração acima, teremos:

$$\begin{aligned} 2^n - 1 &= (2-1)\left(2^{n-1} + 2^{n-2} + 2^{n-3} + ... + 2^2 + 2 + 1\right) \\ &= \left(2^{n-1} + 2^{n-2} + 2^{n-3} + ... + 2^2 + 2 + 1\right) \end{aligned}$$

Assim concluímos que $[2^n - 1]_2 = \left[\underbrace{1111...11}_{n}\right]_2$. □

6 Critérios de divisibilidade

Os critérios têm por finalidade verificar se um dado número inteiro qualquer é divisível por um número natural, sem se efetuar a divisão.

Para darmos início a este tópico e possamos ter um bom entendimento, devemos formalizar o seguinte teorema.

Teorema 6.1. *Todo número inteiro positivo N admite uma única representação da forma:*

$$N = a_n a_{n-1} ... a_2 a_1 a_0 = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10 + a_0$$

onde $0 < a_n \leq 9$, $0 \leq a_{n-1}, ..., a_1, a_0 \leq 9$ *e* $N = 0, 1, 2, ..., n$.

Daremos continuidade ao nosso estudo a partir da representação dada no teorema acima, para todo número inteiro, focando os critérios de divisibilidade por 2 a 11, que são os mais comuns e mais cobrados nos testes e exames.

6.1 Alguns critérios de divisibilidade

1. **Divisibilidade por 2**: Um número inteiro é divisível por 2 se e somente, se seu último algarismo for divisível por 2.

   Demonstração. Seja,

   $$\begin{aligned} N &= a_n a_{n-1} ... a_2 a_1 a_0 \\ &= a_n a_{n-1} ... a_2 a_1 0 + a_0 \\ &= 10(a_n a_{n-1} ... a_2 a_1) + a_0 \end{aligned}$$

   Sendo $10(a_n a_{n-1} ... a_2 a_1)$ um número divisível por 2, temos que, $2 \mid N$ se, e somente se $2 \mid a_0$. □

2. **Divisibilidade por 3**: Um número inteiro é divisível por 3 se a soma dos seus algarismos for divisível por 3.

Demonstração. Seja,

$$\begin{aligned}
N &= a_n a_{n-1} ... a_2 a_1 a_0 \\
&= 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10 a_1 + a_0 \\
&= (\underbrace{99...9}_{n} + 1) a_n + (\underbrace{99...9}_{n-1} + 1) a_{n-1} + ... + (99+1) a_2 + (9+1) a_1 + a_0 \\
&= \underbrace{99...9}_{n} a_n + \underbrace{99...9}_{n-1} a_{n-1} + ... + 99 a_2 + 9 a_1 + a_n + a_{n-1} + ... + a_1 + a_0 \\
&= (\underbrace{99...9}_{n} a_n + \underbrace{99...9}_{n-1} a_{n-1} + ... + 99 a_2 + 9 a_1) + a_n + a_{n-1} + ... + a_1 + a_0 \\
&= 3(\underbrace{33...3}_{n} a_n + \underbrace{33...3}_{n-1} a_{n-1} + ... + 33 a_2 + 3 a_1) + a_n + a_{n-1} + ... + a_1 + a_0
\end{aligned}$$

Sendo $3(\underbrace{33...3}_{n} a_n + \underbrace{33...3}_{n-1} a_{n-1} + ... + 33 a_2 + 3 a_1)$ divisível por 3, temos que, $3 \mid N$ se, e somente se $3 \mid a_n + a_{n-1} + ... + a_1 + a_0$. □

3. **Divisibilidade por 4**: Um número inteiro é divisível por 4 se e somente, se o número formado por seus dois últimos algarismos for divisível por 4.

   Demonstração. Seja,

$$\begin{aligned}
N &= a_n a_{n-1} ... a_2 a_1 a_0 \\
&= a_n a_{n-1} ... a_2 00 + a_1 a_0 \\
&= 100(a_n a_{n-1} ... a_2) + a_1 a_0
\end{aligned}$$

   Sendo $100(a_n a_{n-1} ... a_2)$ divisível por 4, temos que, $4 \mid N$ se, e somente se $4 \mid a_1 a_0$. □

4. **Divisibilidade por 5**: Um número inteiro é divisível por 5 se e somente, se o seu último algarismo for igual a 0 ou 5.

   Demonstração. Sendo,

$$\begin{aligned}
N &= a_n a_{n-1} ... a_1 a_0 \\
&= (a_n a_{n-1} ... a_1 0) + a_0 \\
&= 10(a_n a_{n-1} ... a_1) + a_0
\end{aligned}$$

   Como $10(a_n a_{n-1} ... a_1) + a_0$ é divisível por 5, temos que, $5 \mid N$ se, e somente se $a_0 = 0$ ou $a_0 = 5$. □

5. **Divisibilidade por 6**: Um número inteiro é divisível por 6, se a soma de seu algarismos é divisível por 3 e o algarismo das unidades for par.

Demonstração. Para que um número seja divisível por 6, deverá ser:

- Divisível por 3:

  $N = a_n + a_{n-1} + ... + a_2 + a_1 + a_0$ deverá ser um múltiplo de 3, em outras palavras, da forma $3k$, sendo $k \in \mathbb{N}$.

- Divisível por 2:

  O algarismo a_0 na soma $N = a_n + a_{n-1} + ... + a_2 + a_1 + a_0 = 3k$, deverá ser um número par.

  Concluímos assim que para um número ser divisível por 6, deverá ser par e múltiplo de 3.

□

6. **Divisibilidade por 7**: Um número inteiro $N = a_n a_{n-1} ... a_1 a_0$ é divisível por 7 se, e somente se o inteiro $a_0 + 3a_1 + 2a_2 + 6a_3 + 4a_4 + 5a_5 + a_6 + 3a_7 + 2a_8 + 6a_9 + ...$ for divisível por 7.

Demonstração. Tomando $N = a_n a_{n-1} ... a_1 a_0$, teremos:

$$\begin{aligned} N &= a_n a_{n-1} ... a_1 a_0 = a_0 + 10a_1 + 10^2 a_2 + 10^3 a_3 + 10^4 a_4 + 10^5 a_5 + ... \\ &= a_0 + (7+3)a_1 + (98+2)a_2 + (994+6)a_3 + (9996+4)a_4 + (99995+5)a_5 + ... \\ &= a_0 + (7a_1 + 3a_1) + (98a_2 + 2a_2) + (994a_3 + 6a_3) + (9996a_4 + 4a_4) + (99995a_5 + 5a_5) + \\ &= 7a_1 + 98a_2 + 994a_3 + 9996a_4 + 99995a_5 + ... + a_0 + 3a_1 + 2a_2 + 6a_3 + 4a_4 + 5a_5 + ... \\ &= 7(a_1 + 14a_2 + 142a_3 + 1428a_4 + 14285a_5 + ...) + a_0 + 3a_1 + 2a_2 + 6a_3 + 4a_4 + 5a_5 + ... \end{aligned}$$

Sendo $7(a_1 + 14a_2 + 142a_3 + 1428a_4 + 14285a_5 + ...)$ divisível por 7, temos que, $7 \mid N$ se, e somente se $7 \mid a_0 + 3a_1 + 2a_2 + 6a_3 + 4a_4 + 5a_5 + ...$

□

Uma outra forma de saber que um número é divisível por sete, dá-se da seguinte maneira.

7. **Divisibilidade por 7**: Um número inteiro $N = a_n a_{n-1} ... a_1 a_0$ é divisível por 7 se, e só se, o número inteiro $a_n a_{n-1} ... a_1 - 2a_0$ é divisível por 7.

Demonstração. (a) Sendo $a_n a_{n-1} a_{n-2} ... a_1 - 2a_0$ divisível por 7, temos:

$$a_n a_{n-1} a_{n-2} ... a_1 - 2a_0 = 7q$$

onde $q \in \mathbb{Z}$.

Multiplicando por 10 os lados da igualdade teremos.

$$a_n a_{n-1} a_{n-2} ... a_1 0 - 20a_0 = 70q$$

Somando as igualdades $21a_0$, teremos

$$a_n a_{n-1} a_{n-2} ... a_1 0 - 20a_0 + 21a_0 = 70q + 21a_0$$

Realizando as operações

$$a_n a_{n-1} a_{n-2} ... a_1 0 + a_0 = 7(10q + 3a_0)$$

Concluímos assim que $a_n a_{n-1} a_{n-2} ... a_1 a_0$ é divisível por 7.

(b) Existe $k \in \mathbb{Z}$, tal que:

$$a_n a_{n-1} a_{n-2} ... a_1 a_0 = a_n a_{n-1} a_{n-2} ... a_1 0 + a_0 = 7k$$

Escrevendo $a_0 = 21a_0 - 20a_0$, teremos.

$$\begin{aligned} a_n a_{n-1} a_{n-2} ... a_1 0 + 21a_0 - 20a_0 &= 7k \\ a_n a_{n-1} a_{n-2} ... a_1 0 - 20a_0 &= 7k - 21a_0 \\ 10(a_n a_{n-1} a_{n-2} ... a_1 - 2a_0) &= 7(k - 3a_0) \end{aligned}$$

Daí como $10(a_n a_{n-1} a_{n-2} ... a_1 - 2a_0)$ é divisível por 7 e como $7 \nmid 10$, então $7 \mid a_n a_{n-1} a_{n-2} ... a_1 - 2a_0$.

□

8. **Divisibilidade por 8**: Um número inteiro é divisível por 8 se e somente, se o número formado por seus três últimos algarismos for divisível por 8.

Demonstração. Seja,

$$\begin{aligned} N &= a_n a_{n-1} ... a_2 a_1 a_0 \\ &= a_n a_{n-1} ... a_3 000 + a_2 a_1 a_0 \\ &= 1000(a_n a_{n-1} ... a_3) + a_2 a_1 a_0 \end{aligned}$$

Sendo $1000(a_n a_{n-1} ... a_3)$ divisível por 8, temos que, $8 \mid N$ se, e somente se $8 \mid a_2 a_1 a_0$. □

9. **Divisibilidade por 9**: Um número inteiro é divisível por 9 se a soma dos seus algarismos for divisível por 9.

Demonstração. Sendo,

$$\begin{aligned}
N &= a_n a_{n-1}...a_2 a_1 a_0 \\
&= 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10 a_1 + a_0 \\
&= (\underbrace{99...9}_{n} + 1) a_n + (\underbrace{99...9}_{n-1} + 1) a_{n-1} + ... + (99+1) a_2 + (9+1) a_1 + a_0 \\
&= \underbrace{99...9}_{n} a_n + \underbrace{99...9}_{n-1} a_{n-1} + ... + 99 a_2 + 9 a_1 + a_n + a_{n-1} + ... + a_1 + a_0 \\
&= (\underbrace{99...9}_{n} a_n + \underbrace{99...9}_{n-1} a_{n-1} + ... + 99 a_2 + 9 a_1) + a_n + a_{n-1} + ... + a_1 + a_0 \\
&= 9(\underbrace{11...1}_{n} a_n + \underbrace{11...1}_{n-1} a_{n-1} + ... + 11 a_2 + a_1) + a_n + a_{n-1} + ... + a_1 + a_0
\end{aligned}$$

Como $9(\underbrace{11...1}_{n} a_n + \underbrace{11...1}_{n-1} a_{n-1} + ... + 11 a_2 + a_1)$ é divisível por 9, então, $9 \mid N$ se, e somente se $9 \mid a_n + a_{n-1} + ... + a_1 + a_0$ □

10. **Divisibilidade por 10**: Um número inteiro é divisível por 10 se e somente, se o seu último algarismo for igual a 0.

Demonstração. Sendo,

$$\begin{aligned}
N &= a_n a_{n-1}...a_1 a_0 \\
&= (a_n a_{n-1}...a_1 0) + a_0 \\
&= 10(a_n a_{n-1}...a_1) + a_0
\end{aligned}$$

Como $10(a_n a_{n-1}...a_1)$ é divisível por 10, então, $10 \mid N$ se, e somente se $a_0 = 0$. □

11. **Divisibilidade por 11**: Um número inteiro $N = a_n a_{n-1}...a_1 a_0$ é divisível por 11 se, e somente se o inteiro $a_0 - a_1 + a_2 - a_3 + a_4 - a_5 + ... + (-1)^n a_n$ for divisível por 11.

Demonstração. Seja,

$$\begin{aligned}
N &= a_n a_{n-1}...a_1 a_0 \\
&= a_0 + 10 a_1 + 10^2 a_2 + ... + 10^{n-1} a_{n-1} + 10^n a_n \\
&= a_0 + (11-1) a_1 + (99+1) a_2 + ... + (1\underbrace{0...0}_{n} + (-1)^{n+1} + (-1)^n) a_n \\
&= a_0 + (11 a_1 - a_1) + (99 a_2 + a_2) + ... + (1\underbrace{0...0}_{n} + (-1)^{n+1} + (-1)^n) a_n \\
&= a_0 - a_1 + a_2 - a_3 + ... + (-1)^n a_n + 11(a_1 + 9 a_2 + 91 a_3 + ...)
\end{aligned}$$

Como 11 divide $11(a_1 + 9a_2 + 91a_3 + ...)$, então $11 \mid N$ se, e somente se $11 \mid a_0 - a_1 + a_2 - a_3 + ... + (-1)^n a_n$. □

6.2 Exercícios Resolvidos

Exercício 6.1. *Dado o número $57a3b$, substituir a e b por algarismos que tornem esse número divisível por 5 e 9.*

Solução. : Para que $57a3b$ seja divisível por 5, b deverá ser 5 ou 0.

Para que seja divisível por 9, a soma de seus alarismos deverá ser um número múltiplo de nove.

$$5 + 7 + a + 3 + b = 9k, \text{ sendo } k \in \mathbb{N}$$

Assim:

$$15 + a + b = 9k$$

Faremos a análise nas duas situações, $b = 0$ e $b = 5$.

Para $b = 0$:

$$15 + a = 9k$$
$$a = 9k - 15$$

substituindo $k = 2$, teremos $a = 9 \cdot (2) - 15 = 3$.

Para $b = 5$:

$$20 + a = 9k$$
$$a = 9k - 20$$

Substituindo $k = 3$, teremos $a = 9 \cdot (3) - 20 = 7$.

Portanto concluímos que, para $b = 0$, tem-se $a = 3$ e para $b = 5$, tem-se $a = 7$. Os números que satisfazem o problema serão 57330 ou 57735. □

Exercício 6.2. *O número $1234a6$ é divisível por 7. O algarismo a vale:*

Solução. : Pelo critério de divisibilidade por 7, devemos:

$$6 + 3a + 2 \cdot 4 + 6 \cdot 3 + 4 \cdot 2 + 5 = 7q, \text{ com } q \in \mathbb{Z}$$
$$45 + 3a = 7q$$
$$3a = 7q - 45$$

Atribuindo apropriados valores naturais para q, chegaremos em $q = 9$, resultando $45 + 3a = 63$, assim $a = 6$. O número resultante é 123466. □

Exercício 6.3. *O número $583ab$ é divisível por 9, o valor máximo da soma dos algarismos a e b, será.*

(A) ∞ *(B) 20* *(C) 18* *(D) 11* *(E) 2*

Solução. : Para que $583ab$, seja divisível por 9, devemos ter $5+8+3+a+b=9k$, sendo $k \in \mathbb{N}$.

$$5+8+3+a+b=9k$$
$$a+b=9k-16$$

Como a e b, são algarismos, sua soma não poderá exceder 18. Atribuindo valores para k, teremos:

Para $k=2$, teremos $a+b=2$.

Para $k=3$, teremos $a+b=11$.

Para $k=4$, teremos $a+b=20$, que não satisfaz, pois excede 18.

Logo o valor máximo para a soma será 11. Alternativa (D). □

Exercício 6.4. *Determinar os dígitos a e b tais que o número de 7 cifras* $6a74b14$ *seja múltiplo de 9 e de 11. Dar todas as possibilidades.*

Solução. : Pelo critério de divisibilidade por 11:

$$4-1+b-4+7-a+6=11q, \text{ com } q \in \mathbb{Z}$$
$$12+b-a=11q$$
$$b-a=11q-12$$

Se $q=2$, teremos $b-a=10$, então seria impossível termos algum valor para b e a, pois a subtração de dois algarismos nunca poderá exceder 9, a igualdade só será valida para $q=1$. Neste caso $b-a=-1$.

Analisando o caso de ser divisível por 9:

$$4+1+b+4+7+a+6=9k, \text{ com } k \in \mathbb{Z}$$
$$22+b+a=9k$$
$$b+a=9k-22$$

Como estamos trabalhando com uma soma, seu resultado não poder ser negativo $(9k-22>0)$ e muito menos ultrapassar 18, que é o valor máximo para uma soma de dois algarismos.

Assim o único valor que satisfaz o problema será $k=3$, logo $b+a=5$. Resultando o sistema.

$$\begin{cases} b-a=-1 \\ b+a=5 \end{cases}$$

Efetuando a soma das equações encontraremos $2b=4$, logo $b=2$, substituindo em qualquer uma das equações do sistema encontraremos $a=3$. Concluindo então que a única possibilidade será 6374214. □

Exercício 6.5. *Qual o menor número natural que se deve somar a 4312 para que resulte em um número divisível por 3.*

Solução. : Para que seja divisível por 3, a soma de seus algarismos deve ser um número múltiplo de 3, como $4+3+1+2=10$ é a soma dos algarismos de 4312, o menor número natural múltiplo de 3 acima de 10 é 12, então faremos a subtração $12-10=2$, logo devemos somar 2 ao número 4312, para que seja divisível por 3. □

Exercício 6.6. *O Aluno Gui não prestou atenção na aula e não aprendeu como verificar, sem realizar a divisão, se um número é múltiplo de 7 ou não. Por isso, Gui decidiu usar a regra do 3, ou seja, ele vai somar os dígitos e verificar se o resultado é um múltiplo de 7. Para quantos números inteiros positivos menores que 100 esse método incorreto indicará que um número é múltiplo de 7, sendo o número realmente múltiplo de 7?*

(A) 0 *(B) 1* *(C) 2* *(D) 3* *(E) 4*

Solução. : Como são todos inteiros positivos menores que 100, os números procurados só podem ter um ou dois dígitos. Como a soma máxima para dois algarismos é $9+9=18$ e erroneamente o aluno utilizou a regra da divisibilidade por 3, assim as possíveis somas dos algarismos múltiplos de 7 só podem ser, 7 ou 14, resultando nos números 07, 70 e 77. Alternativa (D). □

Exercício 6.7. *Seja* $N = 12345678a$, *onde* a *é o algarismo das unidades. Se* N *deixa resto 3 quando dividido por 4, a soma dos possíveis valores de* a *é igual a:*

(A) 4 *(B) 8* *(C) 9* *(D) 10*

Solução. : Como N dividido por 4 deixa resto 3, como diz o enunciado do problema, então

$$1+2+3+4+5+6+7+8+a = 4k+3, \text{ sendo } k \in \mathbb{N}.$$
$$1+2+3+4+5+6+7+8+a = 4k+3$$
$$36+a = 4k+3$$
$$a = 4k-33$$

Para $k=9$, teremos $a=3$.

Para $k=10$, teremos $a=7$.

Para $k=11$, teremos $a=11$, que não satisfaz o problema, logo a soma dos possíveis valores será $3+7=10$. □

Exercício 6.8. *Seja* N *o menor número inteiro positivo que multiplicado por 33 resulta em um número cujos algarismos são todos iguais a 7. Determine a soma dos algarismos de* N.

Solução. : O critério de divisibilidade por 11 nos diz que se o número $33N$ possui todos os seus algarismos iguais e é divisível por 11, de acordo o enunciado do exercício, então ele deve possuir um número par de algarismos. O critério de divisibilidade por 3 também nos diz que a soma dos algarismos deve ser múltiplo de 3 e isso obriga a quantidade de algarismos 7 seja divisível por 3. O menor número que cumpre essas condições é 777777, ou seja, $N = \dfrac{777777}{33} = 23569$. Assim, a soma dos algarismos de N é $2+3+5+6+9 = 25$ $\square$

Exercício 6.9. *Quantos múltiplos de 6 menores que 1000 tem a propriedade de que a soma de suas cifras é 21?*

Solução. : Para resolvermos esse problema, temos que ter em mente a seguinte informação, nenhum número de dois algarismos múltiplo de 6 terá como soma 21. Como queremos encontrar os múltiplos de 6 cuja soma dos seus algarismos é 21, então conclui que os números que satisfazem as condições requeridas serão divisíveis por 3 e 2, possuindo assim três algarismos.

Como já sabemos que o número só poderá ter 3 algarismos e é divisível por 3, nos resta analisar o caso em que N é divisível por 2.

Supondo $N = a_2a_1a_0$, para que seja divisível por 2, c deverá ser igual a 0, 2, 4, 6 ou 8.

- Caso $c = 0$:

  teremos $a + b = 21$, que não pode, pois a somá máxima só poderá ser 18.

- caso $c = 2$:

  teremos $a + b = 19$, que também não satisfaz o problema.

- Caso $c = 4$:

  teremos $a + b = 17$, assim as possíveis somas serão $(9 + 8)$ e $(8 + 9)$, logo teremos dois resultados 984 e 894.

- Caso $c = 6$:

  Teremos $a+b = 15$, assim as possíveis somas serão $(9 + 6)$, $(6 + 9)$, $(8 + 7)$ e $(7 + 8)$, logo teremos como resultado 966, 696, 876 e 786.

- Caso $c = 8$:

  Teremos $a+b = 13$, assim as possíveis somas serão $(9 + 4)$, $(4 + 9)$, $(8 + 5)$, $(5 + 8)$, $(7 + 6)$ e $(6 + 7)$ logo teremos teremos como resultado 948, 498, 858, 588, 768 e 678.

Concluímos assim que teremos 12 múltiplos de 6 cuja soma dos seus algarismos é 21. $\square$

Exercício 6.10. *Um inteiro positivo N é composto somente dos dígitos 0 e 1, e é divisível por 2475. Determine o menor número possível de dígitos de N.*

Solução. : Primeiramente vamos fatorar o número 2475, resultando $2475 = 9 \cdot 25 \cdot 11$. Vamos analisar em partes o problema.

- divisibilidade por 25:

  Como o Número é formado apenas por dígitos 1 ou 0, para $25 \mid N$, os dois últimos algarismos devem ser divisíveis por 25, assim a única forma de 25 dividir N, os dois últimos dígitos devem ser 0.

- divisibilidade por 11:

  A soma dos seus algarismos de ordem par, subtraído da soma dos algarismos de ordem ímpar resulta em um número múltiplo de 11, assim os algarismos 1 devem ser em quantidade par.

- divisibilidade por 9:

  A soma dos seus algarismos deve ser múltiplo de 9, como 9 é ímpar. O próximo número múltiplo de 9 é 18 que é par.

Como o problema quer o menor valor, então o número de algarismos será 20. $\square$

7 Divisores de um inteiro

Dizer que um número inteiro é divisor de outro inteiro significa afirmar que se pode dividir esse número de forma exata.

O conjunto de todos os divisores de um inteiro qualquer a, de maneira formal indica-se por $D(a)$, isto é:

$$D(a) = \{x \in \mathbb{Z}^* : x \mid a\}$$

Tem-se que:
$D(0) = \{x \in \mathbb{Z}^* : x \mid 0\} = \mathbb{Z}^*$
$D(1) = \{x \in \mathbb{Z}^* : x \mid 1\} = \{\pm 1\}$
$D(2) = \{x \in \mathbb{Z}^* : x \mid 2\} = \{\pm 1, \pm 2\}$
$D(8) = \{x \in \mathbb{Z}^* : x \mid 8\} = \{\pm 1, \pm 2, \pm 4, \pm 8\}$

Temos nestes exemplos que os inteiros a e $-a$ possuem o mesmo conjunto de divisores, isto é:

$$D(a) = D(-a)$$

Como $a = a \times 1 = (-a)(-1)$, podemos concluir que 1, -1, a e $-a$ são sempre divisores de a, denominados divisores triviais de a. Em particular, os inteiros 1 ou -1, só admitem divisores triviais.

Qualquer que seja o inteiro $a \neq 0$, se $x \mid a$, então:

$$-a \leq x \leq a \Rightarrow D(a) \subset [-a; a]$$

o que comprova que qualquer inteiro $a \neq 0$ tem um número finito de divisores.

Para darmos continuidade em nossos estudos, será enunciado o *Teorema Fundamental da Aritmética*, que nos servirá de base para o tópico seguinte.

Inicialmente devemos ter em mente que um **número primo** é aquele que é dividido apenas por um e por ele mesmo.

Teorema 7.1. *Teorema Fundamental da Aritmética. Todo número natural maior do que 1 ou é primo ou pode ser escrito de forma única, a menos da ordem dos fatores, como produto de números primos.*

Este Teorema também pode ser enunciado da maneira seguinte.

Teorema 7.2. *Seja $n > 1$ um número natural. Existem números primos $p_1 < p_2 < p_3 < ... < p_r$ e, também, números naturais não nulos $n_1, n_2, n_3, ..., n_r$, sendo $r \geq 1$, tais que*

$$n = p_1^{n_1} p_2^{n_2} p_3^{n_3} ... p_r^{n_r}$$

Demonstração. Se n é primo, nada há para demonstrar.

Se n é composto, então possui um divisor primo p_1, e temos:

$$n = p_1 n_1,\ 1 < n_1 < n$$

Se n_1 é primo, então esta igualdade representa n como produto de fatores primos, e se, n_1 é composto, então, possui um divisor primo p_2, isto é, $n_1 = p_2 n_2$, e temos:

$$n = p_1 p_2 n_2,\ 1 < n_2 < n_1$$

Se n_2 é primo, então esta igualdade representa n como produto de fatores primos, e se, n_2 é composto, então, possui um divisor primo p_3, isto é, $n_2 = p_3 n_3$, e temos:

$$n = p_1 p_2 p_3 n_3,\ 1 < n_3 < n_2$$

Assim por diante.

Assim sendo, temos a sequência decrescente:

$$n > n_1 > n_2 > n_3 > ... > 1$$

Como só existe um número finito de inteiros positivos menores que n e maiores que 1, existe necessariamente n_r que é primo, $n_r = p_r$, e por conseguinte teremos:

$$n = p_1 p_2 p_3 ... p_r$$

Essa igualdade que representa o inteiro positivo $n > 1$ como produto de fatores primos. □

Corolário 7.1. *A decomposição de um inteiro positivo $n > 1$ como produto de fatores primos é única, a menos da ordem dos fatores.*

Demonstração. Suponha que n admita duas decomposições como produto de fatores primos, isto é:

$$n = p_1 p_2 p_3 ... p_r = q_1 q_2 q_3 ... q_s,\ r \leq s$$

onde os p_i e os q_j são todos inteiros primos e tais que.

$$p_1 \leq p_2 \leq p_3 \leq ... \leq p_r,\ q_1 \leq q_2 \leq q_3 \leq ... \leq q_s$$

Como $p_1 \mid q_1 q_2 q_3 ... q_s$, existe um índice k, com $1 \leq k \leq s$, tal que $p_1 = q_k$, de modo que $p_1 \geq q_1$. Analogamente $q_1 = p_h$, com $1 \leq h \leq r$, de modo que $q_1 \geq p_1$. Portanto, temos $p_1 = q_1$, o que implica:

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

Com o mesmo raciocínio conclui-se que $p_2 = q_2$, o que implica:

$$p_3 p_4 ... p_r = q_3 q_4 ... q_s$$

E assim por diante.

Assim sendo, se subsiste a desigualdade $r < s$, então se chega necessariamente a igualdade:

$$1 = q_{r+1} q_{r+2} ... q_s$$

O que é absurdo, porque cada $q_j > 1$. Logo, $r = s$ e temos:

$$p_1 = q_1,\ p_2 = q_2, ..., p_r = q_r$$

Isto é, as duas decomposições do inteiro positivo $n > 1$ como produto de fatores primos são idênticas, ou seja, n admite uma única decomposição como produto de fatores primos. □

7.1 Quantidades de divisores de um número natural

Seja n um inteiro positivo. O seu número de divisores positivos é denotado por $d(n)$.

Exemplo: Os divisores positivos de 14 são 1, 2, 7 e 14, de modo que $d(14) = 4$

Observação 5. *Se p é primo, então $d(p) = 2$, pois seus únicos divisores são ele mesmo e a unidade. Caso seja p^2, seus divisores serão, 1, p e p^2, sendo assim $d(p^2) = 3$. De um modo geral teremos $d(p^n) = n + 1$, pois seus divisores são 1, p, p^2, ..., p^n.*

Teorema 7.3. *Se $N = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} ... p_r^{\beta_r}$ é a decomposição canônica do inteiro positivo $N > 1$, então:*

$$d(n) = (\beta_1 + 1)(\beta_2 + 1) ... (\beta_r + 1)$$

Demonstração. Os divisores positivos de n são precisamente inteiros d na forma:

$$d = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} ... p_r^{\alpha_r}$$

onde, $0 \leq \alpha_1 \leq \beta_1$, $0 \leq \alpha_2 \leq \beta_2$, ..., $0 \leq \alpha_r \leq \beta_r$.

Temos β_1+1 maneiras de escolher o expoente α_1, β_2+1 maneiras de escolher o expoente α_2. Seguindo o mesmo raciocínio para todos os expoentes, teremos por fim $\beta_r + 1$ formas de escolher α_r, portanto, o número total de formas de escolher os expoentes α_1, α_2, ..., α_r é dado pelo produto:

$$(\beta_1 + 1)(\beta_2 + 1)...(\beta_r + 1)$$

Sendo assim, a quantidade de divisores naturais do inteiro $N = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} ... p_r^{\beta_r}$ é dado por:

$$d(n) = (\beta_1 + 1)(\beta_2 + 1)...(\beta_r + 1)$$

□

7.1.1 Soma dos divisores positivos de um inteiro

Teorema 7.4. *Seja N um inteiro positivo, cuja decomposição canônica é $N = p_1^{n_1} p_2^{n_2} p_3^{n_3} ... p_r^{n_r}$, onde $p_1, p_2, p_3, ..., p_r$, são números primos distintos e $n_1, n_2, n_3, ..., n_r$ números naturais. A soma dos divisores positivos de N é dada por:*

$$s\,(n) = \frac{p_1^{n_1+1} - 1}{p_1 - 1} \times \frac{p_2^{n_2+1} - 1}{p_2 - 1} \times ... \times \frac{p_r^{n_r+1} - 1}{p_r - 1}$$

Demonstração. A soma dos divisores será o produto de todas as combinações possíveis dos fatores primos do numero natural $N = p_1^{n_1} p_2^{n_2} p_3^{n_3} ... p_r^{n_r}$:

$$s(n) = (p_1^0 + p_1^1 + ... + p_1^{n_1}) \cdot (p_2^0 + p_2^1 + ... + p_2^{n_2}) \cdot ... \cdot (p_r^0 + p_r^1 + ... + p_r^{n_r})$$

Como as parcelas dos fatores estão em PG de razão $p_1, p_2, p_3, ..., p_r$ respectivamente, iremos calcular a soma de cada uma e multiplica-las, para isso devemos saber a quantidade de termos que cada fator possui, o que for feito para uma será válido para todos, pois começam de zero e terminam nos valores máximos dos seus expoentes ($a_1 = p_1^0$ e $a_n = p_1^{n_1}$), vemos que o número de termos no primeiro fator será n_1+1, o segundo n_2+1 e seu último será $n_r + 1$, pois:

$$\begin{gathered} a_n = a_1 q^{n-1} \\ p_1^{n_1} = p_1^0 p_1^{n-1} \\ p_1^{n_1} = p_1^{n-1} \Longrightarrow n = n_1 + 1 \end{gathered}$$

Concluímos assim que a soma dos divisores do número N será,

$$\begin{aligned} s\,(n) &= \left(\frac{p_1^{n_1+1} - 1}{p_1 - 1}\right) \times \left(\frac{p_2^{n_2+1} - 1}{p_2 - 1}\right) \times ... \times \left(\frac{p_r^{n_r+1} - 1}{p_r - 1}\right) \\ &= \left(\frac{p_1^{n_1+1} - 1}{p_1 - 1}\right) \times \left(\frac{p_2^{n_2+1} - 1}{p_2 - 1}\right) \times ... \times \left(\frac{p_r^{n_r+1} - 1}{p_r - 1}\right) \end{aligned}$$

$\square$

7.2 Exercícios Resolvidos

Exercício 7.1. *Determine quantos divisores positivos possui o número 200.*

Solução. : Decompondo 200 em fatores primos, teremos:

$$200 = 2^3 5^2$$

Assim sua quantidade de divisores positivos será:

$$d\,(200) = (3+1) \times (2+1) = 4 \times 3 = 12$$

Logo 200 terá 12 divisores positivos. $\square$

Exercício 7.2. *Determine a quantidade de divisores de* $12^5 45^7$.

Solução. : Temos que:

$$\begin{aligned} 12^5 45^7 &= \left(2^2 3\right)^5 \cdot \left(3^2 5\right)^7 \\ &= \left(2^2\right)^5 (3)^5 \left(3^2\right)^7 (5)^7 \\ &= 2^{10} 3^5 3^{14} 5^7 \\ &= 2^{10} 3^{19} 5^7 \end{aligned}$$

Agora vamos calcular a quantidade de divisores positivos:

$$d\,(12^5 45^7) = (10+1)\,(19+1)\,(7+1) = 11 \times 20 \times 8 = 1760$$

Porém o resultado encontrado serve apenas para os inteiros positivos, nosso resultado será $2 \cdot 1760 = 3520$. $\square$

Exercício 7.3. *Se* $n = 2^3 3^x 7^2$*, determine o valor de* x*, sabendo que* N *possui 48 divisores naturais.*

(A) 1. *(B) 2.* *(C) 3.* *(D) 4.* *(E) 5.*

Solução. : Faremos o calculo de forma direta:

$$d\,(n) = (3+1)\,(x+1)\,(2+1)$$

Como $d\,(n)$ é igual a 48, como dito no problema, teremos:

$$\begin{gathered} 4 \times (x+1) \times 3 = 48 \\ 12 \times (x+1) = 48 \\ x+1 = \frac{48}{12} \\ x+1 = 4 \\ x = 3 \end{gathered}$$

Assim teremos como resposta a (alternativa C). $\square$

Exercício 7.4. *Qual o menor número inteiro positivo que tem 15 divisores positivos?*

Solução. : Sendo $d(n) = 15$ e $15 = 3 \times 5$, então $15 = (2+1)(4+1)$, como temos dois fatores e o problema nos pede o menor número inteiro positivo, usaremos os dois menores números primos, que são 2 e 3. Então podemos escrever $n = 2^4 3^2 = 144$. $\square$

Para a resolução do exercício seguinte, utilizaremos o teorema abaixo.

Teorema 7.5. *n é quadrado perfeito se, e somente se, a sua quantidade de divisores for ímpar.*

Demonstração. Sejam, $\alpha_1, \alpha_2, ..., \alpha_n$ os expoentes dos fatores primos da decomposição de n. Assim, teremos que o número de divisores positivos de n é:

$$d(n) = (\alpha_1 + 1) \times (\alpha_2 + 1) \times ... \times (\alpha_n + 1)$$

Para que o produto resulte em ímpar todos os seus fatores deverão ser ímpar e seus expoentes $\alpha_1, \alpha_2, ..., \alpha_n$ deverão ser par. Então n é um quadrado perfeito.

Reciprocamente, se a quantidade de divisores for ímpar, os fatores de $(\alpha_n + 1)$ serão todos ser ímpar, assim os valores de α deverão ser todos par. $\square$

Exercício 7.5. *O número $N = 14a$, sendo a um algarismo, possui exatamente 15 divisores. Determine o valor de a.*

Solução. : Como $14a \in \{140, ..., 149\}$ e sendo a quantidade de divisores $d(n)$ ímpar, então este número N deve ser um quadrado perfeito. Como entre 140 e 149 existe apenas 144 que é quadrado perfeito, temos $a = 4$. Claramente $d(n) = 144 = 2^4 3^2$ e $(4+1)(2+1) = 5 \times 3 = 15$. $\square$

Exercício 7.6. *Um concurso oferece um prêmio para cada pergunta respondida corretamente. São 10 perguntas, sendo que, dos 10 prêmios, são 3 bombons iguais, 4 chocolates iguais e 3 pirulitos iguais. De quantas maneiras diferentes um candidato deste concurso poderá ser premiado?*

(A) 50. *(B) 80.* *(C) 120.* *(D) 132.* *(E) 180.*

Solução. : Calcular a quantidade de maneiras diferentes é o mesmo que calcular a quantidade de divisores do número $a^3 b^4 c^3$, onde $a =$ bombons, $b =$ chocolates e $c =$ pirulito, são números primos, assim teremos:

$$d(a^3 b^4 c^3) = (3+1)(4+1)(3+1) = 4 \times 5 \times 4 = 80$$

Assim teremos 80 maneiras diferentes de ser premiado. (alternativa B). $\square$

Exercício 7.7. *Sobre uma mesa existem 3 pilhas de moedas: a primeira pilha possui 5 moedas amarelas com o número 2 em suas faces; a segunda possui 3 moedas verdes com o numero 3; e a última pilha possui 2 moedas azuis com o número 7. Uma pessoa deve escolher qualquer quantidade de moedas da mesa e multiplicar os números de suas faces. Quantos números diferentes podem ser formados?*

(A) 71. *(B) 70.* *(C) 10.* *(D) 120.* *(E) 30.*

Solução. : Temos 5 moedas amarelas com o número 2, 3 moedas verdes com o número 3 e 2 moedas azuis com o número 7, fazendo o produto de suas faces $2 \times 2 \times 2 \times 2 \times 2 \times 3 \times 3 \times 3 \times 7 \times 7 = 2^5 3^3 7^2$. Calculando a quantidade de divisores e excluindo 1 como divisor, teremos:

$$d(n) - 1 = (5 + 1)(3 + 1)(2 + 1) = 72 - 1 = 71.$$

Logo teremos 71 possibilidades, (alternativa A). □

Exercício 7.8. *Encontre a soma dos divisores positivos do número 100?*

Solução. : Primeiramente, fatorando 100, teremos $100 = 2^2 5^2$. Então a soma dos divisores será:

$$s(100) = \left(\frac{2^{2+1} - 1}{2 - 1}\right) \cdot \left(\frac{5^{2+1} - 1}{5 - 1}\right) = \left(\frac{2^3 - 1}{2 - 1}\right) \cdot \left(\frac{5^3 - 1}{5 - 1}\right) = 7 \cdot \left(\frac{124}{4}\right) = 217.$$

□

Exercício 7.9. *Quantos números entre 100 e 110 tem exatamente 4 divisores naturais?*

Solução. : Para que um número tenha exatamente 4 divisores, ele deve ser resultado do produto de dois números primos, pois de acordo a fórmula da quantidade de divisores de um inteiro, encontraremos $4 = (1 + 1) \cdot (1 + 1)$, comprovando assim o produto de dois fatores primos. Já que 1 e o próprio número já são divisores, devemos ter um produto de primos com expoentes 1 que resulta em um valor entre 100 e 110, tem que $2 \times 53 = 106$ será o único número entre 100 e 110 com exatamente 4 divisores. □

Exercício 7.10. *Determine a quantidade de divisores do número* $2^{16} - 1$.

Solução. : Vamos decompor $2^{16} - 1$ para facilitar as contas. Tem-se que:

$$\begin{aligned} N = 2^{16} - 1 &= \left(2^8 + 1\right)\left(2^8 - 1\right) \\ &= \left(2^8 + 1\right)\left(2^4 + 1\right)\left(2^4 - 1\right) \\ &= \left(2^8 + 1\right)\left(2^4 + 1\right)\left(2^2 + 1\right)\left(2^2 - 1\right) \\ &= \left(2^8 + 1\right)\left(2^4 + 1\right)\left(2^2 + 1\right)(2 + 1)(2 - 1) \end{aligned}$$

No produto $(256 + 1)(16 + 1)(4 + 1)(2 + 1) = 257 \times 17 \times 5 \times 3$, os quatro fatores são todos números primos, então:

$$D(N) = (1 + 1)(1 + 1)(1 + 1)(1 + 1) = 2 \times 2 \times 2 \times 2 = 16$$

Assim $2^{16} - 1$ terá 16 divisores. □

Exercício 7.11. *Determine a soma de todos os números inteiros n para os quais* $\dfrac{n^2 + 1}{n - 1}$ *é um número inteiro.*

Solução. : Sendo $a^2 - b^2 = (a+b)(a-b)$, então $a - b \mid a^2 - b^2$, daí $n - 1 \mid n^2 - 1$.

De outro lado:

$$\begin{aligned} n^2 + 1 &= n^2 - 1 + 1 + 1 \\ &= \left(n^2 - 1\right) + 2 \end{aligned}$$

Segue-se que $n - 1$ deverá dividir 2, então os possíveis valores para n serão 2, 3, 0 e -1. Então a soma será $2 + 3 + 0 - 1 = 4$. $\square$

8 Referências Bibliográficas

1. BRASIL. Ministério da Educação. **Base Nacional Comum Curricular**. Brasília, 2018.

2. FILHO, Edgard de Alencar. **Teoria Elementar dos Números**. 2.ed. São Paulo: Nobel, 1988.

3. HEFEZ, Abramo. **Aritmética**. 2.ed. Rio de Janeiro, 2016.

4. HEFEZ, Abramo. **Iniciação à Aritmética**. 1.ed. Rio de Janeiro: IMPA, 2015.

5. LACERDA, José Carlos Admo. **Praticando a Aritmética**. 6.ed. Rio de Janeiro: XYZ, 2007.

6. MACHADO, Antônio dos Santos. **Matemática Temas e Metas: Trigonometria e Progressões**. 22.ed. São Paulo, 2008.

7. NÚMEROS especiais – pares e ímpares: Problemas envolvendo paridade. **Clubes de Matemática da OBMEP**. Disponível em <http://clubes.obmep.org.br/blog/numeros-especiais-pares-e-impares/numeros-especiais-pares-e-impares-problemas-envolvendo-paridade/>. Acesso em: 19, janeiro de 2020.

8. OLIVEIRA, Marcelo Rufino de. **Elementos de Matemática 0**. 2.ed. Belém: GTR, 2009.

9. OLIVEIRA, Marcelo Rufino de. **Elementos de Matemática 1: Conjuntos, Funções e Aritmética**. 2.ed. Belém: GTR, 2009.

10. ORM Grande PoA, **PARIDADE DE NÚMEROS INTEIROS**. UFRGS: 2013.

11. SOUZA, Renato Carneiro de. **Teoria dos Números - Um Curso Intermediário**. 1.ed. Fortaleza: Vestseller, 2013.