**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**

**Centro de Ciências Exatas**

**Programa de Pós-Graduação em Matemática em Rede Nacional - PROFMAT**

EUFÉLIX MONTEIRO MAURÍCIO

# UMA PROPOSTA DE SEQUÊNCIA DIDÁTICA PARA O ENSINO DE MDC E MMC NA EDUCAÇÃO BÁSICA

VITÓRIA

FEVEREIRO DE 2014

**EUFÉLIX MONTEIRO MAURÍCIO**

# UMA PROPOSTA DE SEQUÊNCIA DIDÁTICA PARA O ENSINO DE MDC E MMC NA EDUCAÇÃO BÁSICA

Dissertação de Mestrado Profissional submetido ao Programa de Pós-Graduação em Matemática em Rede Nacional da Universidade Federal do Espírito Santo, como requisito parcial para obtenção do título de Mestre em Matemática.

**Orientador:** Moacir Rosado Filho

VITÓRIA

FEVEREIRO DE 2014

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

Centro de Ciências Exatas

Programa de Pós-Graduação em Matemática em Rede Nacional - PROFMAT

# "Uma Proposta de Sequência Didática para o Ensino de MDC e MMC na Educação Básica"

## Eufélix Monteiro Maurício

Defesa de Dissertação de Mestrado Profissional submetida ao Programa de Pós-Graduação em Matemática em Rede Nacional da Universidade Federal do Espírito Santo como requisito parcial para a obtenção do título de Mestre em Matemática.

Aprovada em 27/03/2014 por:

Moacir Rosado Filho - UFES

Florêncio Ferreira Guimarães Filho - UFES

Ana Lucia da Silva – UEL

Dados Internacionais de Catalogação-na-publicação (CIP)
(Biblioteca Central da Universidade Federal do Espírito Santo, ES, Brasil)

---

Mauricio, Eufélix Monteiro, 1978 -
M455p

**Uma proposta de sequência**
**didática para o ensino de MDC e MMC na educação básica**
Eufélix Monteiro Mauricio. - 2014
45 f.

Orientador: Moacir Rosado Filho
Dissertação (Mestrado Profissional em Matemática) –
Universidade Federal do Espírito Santo, Centro de Ciências Exatas.

1. Números primos. 2. Fatoração (Matemática). 3. Mínimo múltiplo comum. 4. Máximo divisor comum. I. Rosado Filho, Moacir, 1963-.
II. Universidade Federal do Espírito Santo. Centro de Ciências Exatas.
III. Título CDU:51

---

*Dedico este trabalho a toda a minha família,*
*em especial à minha mãe.*

# Agradecimentos

A Deus, por me conceder a incumbência de ser um educador.

À minha mãe, Eunice, pelo amor incomensurável despendido a mim.

A todos os meus irmãos, em especial Vania, Estélia e Hortência, pelo estímulo dado em todos os momentos da minha vida.

Ao meu professor de Matemática do Ensino Médio, Nilton Lapa, por suas aulas excepcionais.

Ao professor Moacir Rosado Filho, pelas suas sábias orientações no que tange à realização desse trabalho.

Aos professores do Departamento de Matemática da UFES atuantes no PROFMAT.

À Secretaria Estadual de Educação, pela licença concedida, por tempo suficiente à conclusão desse mestrado.

À Capes, pelo apoio financeiro.

Por fim, à Sociedade Brasileira de Matemática pela realização desse programa.

# Resumo

Este trabalho consiste em uma sequência didática voltada aos professores da educação básica, principalmente, da rede pública estadual. Essa sequência trata em especial do cálculo do *mdc* por meio da divisão euclidiana. Aproveitamos o ensejo para discorrer um pouco sobre divisibilidade, *mmc* e primos. A proposta em questão é formada por 4 capítulos. Em cada um deles há uma lista de exercícios. Ao final do capítulo 4, acrescentamos uma sequência de exercícios complementares.

# Abstract

This work consists in a didactic sequel reported to the basic education teachers, mostly from public schools of the State. This sequence is particularly about the calculation of the gcd (greatest common divisor) by the Euclidean division. We take this opportunity to discuss a little about divisibility, lcm (least common multiple) and primes. The proposal in query is formed in chapters. In each one of them there is a list of exercises. At the end of chapter 4, we added a series of additional exercises.

# Sumário

# Introdução

Ministrando aulas para turmas de ensino médio desde 1996, pude observar que ao longo dos anos, os principais e melhores livros didáticos do mercado, nessas modalidades de ensino, têm explorado menos o conceito de mmc e mdc, bem como os processos práticos para o cálculo dos mesmos. E isso é preocupante, uma vez que tais conteúdos possuem muitas aplicações práticas, inclusive no cotidiano dos alunos que fazem parte desse nível de ensino. Não obstante disso, os conceitos elementares relacionados com esses tópicos são fáceis de serem compreendidos e aplicados na resolução de problemas.

É válido ressaltar que as poucas bibliografias que tratam desse assunto negligenciam a abordagem do cálculo do mdc pela divisão euclidiana. E esse processo é muito mais rápido, quando envolve números muito grandes. Isso será exemplificado no capítulo 4 dessa dissertação.

Além disso, não há, nesses materiais, a relação existente entre o mmc e o mdc de dois ou mais números, usada também na solução de problemas.

A partir dessas reflexões, sugere-se que os professores preparem um material à parte que possa suprir essa deficiência. No entanto, alguns pormenores são constantemente questionados pelos profissionais em curso de aperfeiçoamento de professores, como por exemplo: esse tópico não faz parte do CBC (Currículo Básico Comum); a maioria dos alunos não tem interesse; não temos tempo disponível para preparar um material desse tipo; o cumprimento do programa será comprometido, se dedicarmos parte do tempo para lecionar detalhadamente tais conteúdos.

Em suma, surge a necessidade de preparar um material que pudesse servir de subsídio para os professores que tiverem o interesse de realizar uma proposta pedagógica voltada ao ensino desses conceitos.

Esse projeto deve ser desenvolvido, em horários alternados, no sábado ou mesmo nas aulas regulares, com aqueles alunos que gostam e têm interesse de aprender e se preparar para concursos que envolvem matemática. Tais alunos muitas vezes são ignorados em sala de aula, pelo fato de os professores não terem tempo de elaborar uma aula direcionada a eles, pois são, na grande maioria das vezes, pressionados a contemplar, em seus planejamentos, os alunos que apresentam mais dificuldades ou desinteresse.

Para finalizar reafirmo que os conteúdos citados acima não constam no Currículo Básico Comum às escolas da rede estadual de ensino do Espírito Santo.

# Capítulo 1

# Divisibilidade em $\mathbb{Z}$

**Definição 1.1.** *Seja $a$ um número inteiro. O valor absoluto (ou módulo) de $a$, representado por $|a|$ , é definido assim:*

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

**Exemplo 1.2.**

- $|3| = 3$ ;
- $|-7| = -(-7) = 7$.

**Proposição 1.3.**

*i.* $|a| = |-a|$ ;
*ii.* $|ab| = |a| \cdot |b|$ ;
*iii.* $|a| = |b| \iff a = b \quad ou \quad a = -b$ .

***Prova:***

i. Se $a \geq 0$, então $-a \leq 0$. Segue daí que $|-a| = -(-a) = a = |a|$. Por outro lado, sendo $a \leq 0$, tem-se $-a \geq 0$. Logo, $|-a| = -a = |a|$.
ii. Se $a, b \geq 0$, então $ab \geq 0$. Então, vê-se que $|a \cdot b| = a \cdot b = |a| \cdot |b|$. Caso $a \geq 0$ e $b \leq 0$, tem-se $ab \leq 0$. Logo, $|ab| = -(ab) = a(-b) = |a| \cdot |b|$. Para os outros casos, procedemos de maneira análoga.

iii. Se $a = b$ ou $a = -b$, então $|a| = |b|$ ou $|a| = |-b| = |b|$. Logo, $|a| = |b|$. Reciprocamente, se $|a| = |b|$, então $|b| = -a$, se $a \leq 0$ e $|b| = a$, se $a \geq 0$. Caso $b \leq 0$, tem-se $-a = -b$ ou $a = -b$. Portanto, $a = b$ ou $a = -b$. O caso $b \geq 0$ é feito de forma análoga.

□

**Definição 1.4.** *Sejam $a$ e $b$ inteiros. Dizemos que $a$ divide $b$, representando por $a|b$, se existir um inteiro $c$ tal que $b = a \cdot c$. Também usaremos as frases: $a$ é divisor de $b$, $a$ é fator de $b$, $b$ é múltiplo de $a$ ou ainda, $b$ é divisível por $a$ para nos referirmos ao fato mencionado acima. Quando $a$ não divide $b$ , representamos esse fato por $a \nmid b$ .*

**Exemplo 1.5.** *$3|12$, pois $12 = 3 \cdot 4$, mas $3 \nmid 8$, já que não existe um número $c$ inteiro tal que $8 = 3 \cdot c$.*

**Proposição 1.6.** *Sejam $a$,$b$ e $c$ números inteiros. Então,*

*i. $1|a$, $a|a$ e $a|0$ ;*

*ii. Se $a|b$ e $b|c$, então $a|c$ ;*

*iii. Se $a|b$ e $a|c$, então $a|b + c$ e $a|b - c$ ;*

*iv. Se $a$ e $b$ são positivos e $a|b$, então $a \leq b$ ;*

*v. Se $a|b$ e $b|a$, então $a = b$ ou $a = -b$ ;*

*vi. Se $a|b$, então $a|b \cdot d$ para qualquer inteiro $d$ ;*

*vii. Se $a|b$, então $a \cdot d|b \cdot d$ para qualquer inteiro $d$ .*

***Prova:***

i. Basta notar que $a = 1 \cdot a$ , $a = a \cdot 1$ e $0 = a \cdot 0$.

ii. Se $a|b$ e $b|c$, então existem $q_1$ e $q_2$ inteiros, tais que $b = a \cdot q_1$ e $c = b \cdot q_2$. Segue daí que $c = (a \cdot q_1) \cdot q_2 = a \cdot (q_1 \cdot q_2)$, com $q_1 \cdot q_2$ inteiro. Logo, $a|c$.

iii. Já que $a|b$ e $a|c$, então existem $r_1$ e $r_2$ inteiros, de modo que $b = a \cdot r_1$ e $c = a \cdot r_2$. Isso acarreta $b + c = ar_1 + ar_2 = a(r_1 + r_2)$ com $r_1 + r_2$ inteiro.
Portanto, $a|b + c$. De maneira análoga provamos que $a|b - c$.

iv. Se $a, b > 0$ e $a|b$, então existe $q$ inteiro, tal que $b = a \cdot q$, com $q \geq 1$. Multiplicando essa última desigualdade por $a > 0$, tem-se $b = a \cdot q \geq a > 0$.

v. Uma vez que $a|b$ e $b|a$, tem-se $|a|\Big||b|$ e $|b|\Big||a|$.
De acordo com o item anterior, $|a| \leq |b|$ e $|b| \leq |a|$. Isso implica em $|a| = |b|$. Logo, pelo item (iii) da proposição 1.3, $a = b$ ou $a = -b$.

vi. Como $a|b$, deve existir $q_3$ inteiro, tal que $b = a \cdot q_3$ . Isso implica em $b \cdot d = (a \cdot q_3)d = a(q_3 \cdot d)$. Logo, $a|b \cdot d$.

vii. Se $a|b$, então existe $q$ inteiro, de modo que $b = a \cdot q$ . Isso acarreta $b \cdot d = (a \cdot q)d = (a \cdot d)q$ , para $q$ inteiro. Portanto, $a \cdot d|b \cdot d$ .

□

**Exemplo 1.7.**

- $1|-50$ , $727|727$ , $6143|0$;
- *Como* $4|12$ *e* $12|36$, *temos* $4|36$;
- *Já que* $3|15$ *e* $3|27$, *tem-se* $3|(15+27)$ *e* $3|(15-27)$;
- *Uma vez que* $-5|30$ , *temos* $-5 \cdot 7|30 \cdot 7$ , *isto é,* $-35|210$ .

## 1.1 Algoritmo da Divisão (Divisão Euclidiana)

Sejam $a$ e $b$ inteiros, com $b \neq 0$. Existem únicos $q$ e $r$, também inteiros, tais que $a = bq + r$, com $0 \leq r < |b|$. Tais inteiros $q$ e $r$ são, respectivamente, o quociente e o resto da divisão de $a$ por $b$.

***Prova:*** Vamos supor, inicialmente, $b > 0$. Seja $q$ o maior inteiro, de modo que $b \cdot q \leq a$. Sendo assim, temos $bq \leq a < b(q+1)$. Segue daí que $0 \leq a - bq < b = |b|$ e basta definir $r = a - bq$. Se $b < 0$, então $-b > 0$, portanto, existem inteiros $q$ e $r$ tais que $a = (-b)q + r$, com $0 \leq r < -b = |b|$. Isso acarreta $a = b(-q) + r$, o que conclui a primeira parte.
A fim de provarmos a unicidade, admitamos que existam inteiros $q_1$ e $r_1$, de tal maneira que $a = bq_1 + r_1$, com $0 \leq r_1 < |b|$. Dessa forma, tem-se $(bq+r)-(bq_1+r_1) =$

0, o que implica em $b(q-q_1) = r_1 - r$ donde $|b| \Big| |r_1 - r|$. Mas, uma vez que $0 \leq r_1 < |b|$ e $0 \leq r < |b|$, então $|r_1 - r| < |b|$, portanto, como $|b| \Big| |r_1 - r|$, temos $r_1 - r = 0$ , o que acarreta $r = r_1$. Logo, $bq_1 = bq \Rightarrow q_1 = q$, já que $b \neq 0$. □

**Exemplo 1.8.** *Em cada um dos itens abaixo, determine o quociente $q$ e o resto $r$ na divisão euclidiana de $a$ por $b$:*

*i.* $a = -65$ , $b = 3$;

*ii.* $a = -65$ , $b = -3$.

Solução:

i) Note que $3 \cdot (-22) = -66$ , $3 \cdot (-21) = -63$ e $-66 \leq -65 < -63$. Pelo algoritmo da divisão euclidiana, $q = -22$ e $r = a - bq = -65 - 3 \cdot (-22) = -65 + 66 = 1$.

ii)Já que $-3 \cdot 22 = -66$ , $-3 \cdot 21 = -63$ e $-66 \leq -65 < -63$ , vê-se que $q = 22$ e $r = -65 - (-3) \cdot 22 = -65 + 66 = 1$ .

**Exemplo 1.9.** *Considere $x$, $y$ e $z$ números naturais. Na divisão euclidiana de $x$ por $y$, obtém-se quociente $z$ e resto 8. Sabe-se que a representação decimal de $\frac{x}{y}$ , é a dízima periódica $7,363636...$ Determine quanto vale $x + y + z$.*

*Solução:*

*Pela divisão euclidiana, temos $x = y \cdot z + 8$ , com $y \geq 8$, o que implica em $\frac{x}{y} = z + \frac{8}{y}$. Além disso, $\frac{x}{y} = 7,3636\ldots = 7 + \frac{36}{99} = 7 + \frac{4}{11} = 7 + \frac{8}{22}$. Da unicidade da divisão euclidiana , vê-se que $z = 7$ e $\frac{8}{y} = \frac{8}{22}$, donde, $z = 7$, $y = 22$ e $x = 22 \cdot 7 + 8 = 162$ .*

*Portanto, $x + y + z = 162 + 22 + 7 = 191$.*

# Exercícios

1. Encontre o quociente $q$ e o resto $r$ na divisão euclidiana de $a$ por $b$ nos seguintes casos:

   (a) $a = 390$ , $b = 74$

   (b) $a = -124$ , $b = 18$

   (c) $a = -420$ , $b = 58$

   (d) $a = 227$ , $b = -13$

   (e) $a = -562$ , $b = -21$

2. Na divisão euclidiana de $a$ por $b$ o quociente é 6 e o resto, o menor possível. Ache $a$ e $b$ nos seguintes casos:

   (a) $a - b = 525$

   (b) $a + b = 234$

3. Seja $m$ um inteiro cujo resto da divisão por 6 é 5. Qual o resto da divisão de $m$ por 3?

4. (UFMG) Na divisão de dois números inteiros, o quociente é 16 e o resto é o maior possível. Sabendo que a soma do dividendo e do divisor é 125, descubra qual é o resto dessa divisão.

5. Qual é o resto da divisão de $1 \times 2 \times 3 \times 4 \times \cdots \times 2011 + 21$ por 8?

6. Mostre que nenhum número pode deixar resto 5 quando dividido por 12 e resto 4 quando dividido por 15.

# Capítulo 2

# Máximo Divisor Comum (MDC)

**Definição 2.1** (Máximo Divisor Comum)**.** *Sejam $a$ e $b$ inteiros, onde um deles é não nulo. O máximo divisor comum de $a$ e $b$ , representado por $mdc(a, b)$, é o maior dentre os divisores positivos comuns de $a$ e $b$.*

**Exemplo 2.2.** *Sejam $a = 6$ e $b = 8$. Indicando por $D_6$ e $D_8$ o conjunto dos divisores positivos de 6 e 8, respectivamente, temos: $D_6 = \{1, 2, 3, 6\}$ e $D_8 = \{1, 2, 4, 8\}$ do que segue $D_6 \cap D_8 = \{1, 2\}$. Logo, 2 é o maior divisor comum de 6 e 8, isto é, $mdc(6, 8) = 2$.*

**Proposição 2.3.** *Sejam $a$ e $b$ inteiros positivos. Assim,*

*i. Se $b$ é divisor de $a$, então $mdc(a, b) = b$ ;*

*ii. Se $a = bq + c$, com $c \neq 0$, então o conjunto dos divisores comuns dos números $b$ e $c$ é igual ao conjunto dos divisores comuns de $a$ e $b$ . Em particular, $mdc(a, b) = mdc(b, c)$ .*

***Prova:***

i. Todo divisor comum de $a$ e $b$ é um divisor de $b$. Como $b$ é divisor de $a$, tem-se todo divisor de $b$ é também divisor de $a$, ou seja, um divisor comum de $a$ e $b$. Portanto, o conjunto dos divisores comuns dos números $a$ e $b$ é igual ao conjunto dos divisores de $b$. Como o maior divisor de $b$ é ele mesmo, tem-se $mdc(a, b) = b$ .

ii. Usando os itens iii e vi da proposição 1.6, tem-se que todo divisor comum de $a$ e $b$ também divide $c$, consequentemente, é um divisor comum de $b$ e $c$ . Pelo mesmo motivo todo divisor comum de $b$ e $c$ também divide $a$, consequentemente, é um divisor comum de $a$ e $b$. Logo, os divisores comuns de $a$ e $b$ são os mesmos que os divisores comuns de $b$ e $c$ . Em particular, também coincidem os maiores divisores comuns, ou seja, $mdc(a,b) = mdc(b,c)$ .

□

**Teorema 2.4** (Algoritmo de Euclides)**.** *Sejam $a$ e $b$ números inteiros positivos. Aplica-se sucessivamente a divisão euclidiana para obter a seguinte sequência de igualdades:*

$$
\begin{aligned}
a &= b \cdot q_1 + r_1 \ , \ 0 \leq r_1 < b \qquad (2.1)\\
b &= r_1 \cdot q_2 + r_2 \ , \ 0 \leq r_2 < r_1,\\
r_1 &= r_2 \cdot q_3 + r_3 \ , \ 0 \leq r_3 < r_2,\\
&\vdots \qquad\qquad \vdots \qquad\qquad \vdots\\
r_{n-3} &= r_{n-2} \cdot q_{n-1} + r_{n-1} \ , \ 0 \leq r_{n-1} < r_{n-2}\\
r_{n-2} &= r_{n-1} \cdot q_n + r_n \ , \ 0 \leq r_n < r_{n-1}\\
r_{n-1} &= r_n \cdot q_{n+1} + 0 \ ,
\end{aligned}
$$

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

**Observação 2.5.** *Escrevendo as desigualdades dos restos, uma seguida da outra, temos $b > r_1 > r_2 > r_3 \cdots \geq 0$ . Como entre $b$ e 0 há apenas uma quantidade finita de inteiros, essa sequência não pode continuar indefinidamente. Mas ela só chega ao final se um dos restos for zero. Isso garante que o algoritmo sempre para.*

***Prova:*** Da última divisão de 2.4, decorre que $r_n$ divide $r_{n-1}$ . Logo, pela proposição 2.3 (item i), $mdc(r_{n-1}, r_n) = r_n$ . Aplicando o item ii da proposição

2.3 na penúltima divisão, conclui-se que $mdc(r_{n-2}, r_{n-1}) = mdc(r_{n-1}, r_n) = r_n$ . Usando novamente esse mesmo item, na antepenúltima divisão, tem-se $mdc(r_{n-3}, r_{n-2}) = mdc(r_{n-2}, r_{n-1}) = r_n$ . Continuando com esse raciocínio , até a primeira divisão, chega-se a $mdc(a, b) = r_n$ e isso é exatamente o que se desejava verificar. □

**Exemplo 2.6.** *Usando o processo, mostrado no teorema 2.4, encontre o* $mdc(140, 648)$ .

Solução:

$$\begin{aligned} 648 &= 140 \cdot 4 + 88 \\ 140 &= 88 \cdot 1 + 52 \\ 88 &= 52 \cdot 1 + 36 \\ 52 &= 36 \cdot 1 + 16 \\ 36 &= 16 \cdot 2 + 4 \\ 16 &= 4 \cdot 4 + 0 \end{aligned} \tag{2.2}$$

Logo, $mdc(140, 648) = 4$ . Em geral, usa-se o seguinte dispositivo prático:

| Quociente | | 4 | 1 | 1 | 1 | 2 | 4 |
|---|---|---|---|---|---|---|---|
| | 648 | 140 | 88 | 52 | 36 | 16 | 4 |
| Resto | 88 | 52 | 36 | 16 | **4** | 0 | |

Recomendamos que esse quadro seja comparado com a sucessão anterior de igualdades.

O Algoritmo de Euclides usado de trás para frente nos dá uma informação adicional muito importante:

Das igualdades acima podemos escrever:

$$\begin{aligned} 4 &= 36 - 16 \cdot 2 \\ 16 &= 52 - 36 \cdot 1 \\ 36 &= 88 - 52 \cdot 1 \\ 52 &= 140 - 88 \cdot 1 \\ 88 &= 648 - 140 \cdot 4 \end{aligned} \tag{2.3}$$

Logo,

$$\begin{aligned}
4 &= 36 - (52 - 36 \cdot 1) \cdot 2 \\
&= 36 - 52 \cdot 2 + 36 \cdot 2 \\
&= 36 \cdot 3 - 52 \cdot 2 \\
&= (88 - 52 \cdot 1) \cdot 3 - 52 \cdot 2 \\
&= 88 \cdot 3 - 52 \cdot 3 - 52 \cdot 2 \\
&= 88 \cdot 3 - 52 \cdot 5 \\
&= 88 \cdot 3 - (140 - 88 \cdot 1) \cdot 5 \\
&= 88 \cdot 3 - 140 \cdot 5 + 88 \cdot 5 \\
&= 88 \cdot 8 - 140 \cdot 5 \\
&= (648 - 140 \cdot 4) \cdot 8 - 140 \cdot 5 \\
&= 648 \cdot 8 - 140 \cdot 32 - 140 \cdot 5 \\
&= 648 \cdot 8 - 140 \cdot 37.
\end{aligned}$$

Sendo assim, podemos escrever

$$4 = mdc(648, 140) = 648 \cdot 8 - 140 \cdot 37 = 648 \cdot 8 + 140 \cdot (-37). \tag{2.4}$$

Esse processo sempre funciona nos conduzindo ao seguinte resultado, muito importante na matemática:

**Teorema 2.7** (Relação de Bézout)**.** . *Considere $a$ e $b$ inteiros, com um deles diferente de zero. Existem dois números inteiros $n$ e $m$ , de modo que*

$$mdc(a, b) = a \cdot n + b \cdot m \qquad . \tag{2.5}$$

**Proposição 2.8.** *Sejam $a$ e $b$ inteiros não ambos nulos e $d = mdc(a, b)$. Se $d_1$ é um divisor comum de $a$ e $b$ , então $d_1|d$.*

***Prova:*** Uma vez que $d = mdc(a, b)$ , pela relação de Bézout, existem inteiros $x$ e $y$ , tais que $ax + by = d$. Como $d_1|a$ e $d_1|b$ , pelos itens iii e vi da proposição 1.6, temos $d_1|ax + by$ . Por conseguinte, $d_1|d$. □

**Proposição 2.9.** *Sejam $a$ e $b$ inteiros, onde um deles é não nulo. Então,*

$$mdc(a, b) = mdc(|a|, |b|)$$

.

***Prova:*** Para cada $c$ e $d$ inteiros, tem-se $d|c$ se, e somente se, $d\Big||c|$. Dessa forma, os divisores comuns de $a$ e $b$ são exatamente os divisores comuns de $|a|$ e $|b|$. Em particular, também coincidem os maiores divisores comuns, ou seja, $mdc(a,b) = mdc(|a|,|b|)$. □

**Exemplo 2.10.**

- $mdc(-4,6) = mdc(|4|,|6|) = mdc(4,6) = 2$ ;
- $mdc(-7,-21) = mdc(|-7|,|-21|) = mdc(7,21) = 7$ .

**Exemplo 2.11.** *(U.E. Londrina - PR) Para levar os alunos de certa escola a um museu, pretende-se formar grupos que tenha iguais quantidades de alunos e de modo que em cada grupo todos sejam do mesmo sexo. Se nessa escola estudam 1350 rapazes e 1224 garotas e cada grupo deverá ser acompanhado de um único professor, qual o número mínimo de professores necessários para acompanhar todos os grupos nessa visita?*

Solução:

Sejam $x$ e $y$ a quantidade de grupos formados por garotas e rapazes, respectivamente. Considere agora $z$ como o número de estudantes de cada equipe. Sendo assim, temos: $x \cdot z = 1224$ e $y \cdot z = 1350$ . Para que o número de professores que irão acompanhar os alunos seja mínimo, a quantidade $z$ de discentes, por grupo, deve ser máxima. Em virtude de $z$ ser divisor de 1224 e 1350 e ser o maior possível, temos $z = mdc(1224, 1350)$ .

Usando o dispositivo, prático temos:

| | 1 | 9 | 1 | 2 | 2 |
|---|---|---|---|---|---|
| 1350 | 1224 | 126 | 90 | 36 | 18 |
| 126 | 90 | 36 | 18 | 0 | |

Logo, $z = 18$. Isso acarreta $x = \frac{1224}{18} = 68$ e $y = \frac{1350}{18} = 75$. Portanto, o número mínimo de professores necessários para acompanhar esses alunos é 68+75=143.

Define-se o máximo divisor comum $mdc(a_1, a_2, \ldots, a_n)$ de vários inteiros $a_1, a_2, \ldots, a_n$, não todos nulos, de maneira análoga ao caso de dois inteiros, como sendo o maior divisor positivo comum de $a_1, a_2, \ldots, a_n$. Vale a seguinte proposição:

**Proposição 2.12.** *Sejam $a_1, a_2, a_3, \cdots, a_{n-1}, a_n$ números inteiros, onde um deles é não nulo. Então,*

$$mdc(a_1, a_2, a_3, \cdots, a_{n-1}, a_n) = mdc(mdc(a_1, \cdots, a_{n-1}), a_n). \tag{2.6}$$

**Exemplo 2.13.** *Determine $mdc(6, 27, 42)$ .*

Solução:
Como $mdc(6, 27) = 3$ e $mdc(3, 42) = 3$ , pela proposição 2.12, temos $mdc(6, 27, 42) = mdc(mdc(6, 27), 42) = mdc(3, 42) = 3$ .

# Exercícios

1. Determine:

   (a) $mdc(60, 8)$

   (b) $mdc(41, 12)$

   (c) $mdc(132, -64)$

   (d) $mdc(-384, -144)$

2. (UE Londrina - PR) Existem, para doação a escolas, 200 ingressos de um espetáculo e 1575 de outro. Cada escola deve receber ingressos para somente um dos espetáculos e todas as escolas devem receber a mesma quantidade de ingressos. Se todos os ingressos forem distribuídos, qual o número mínimo de escolas que poderão ser contempladas nessa doação?

3. Uma concessionária vendeu no mês de outubro $n$ carros do tipo $A$ e $m$ carros do tipo $B$, totalizando 216 carros. Sabendo-se que o número de carros vendidos de cada tipo foi maior do que 20, que foram vendidos menos carros do tipo $A$ do que do tipo $B$, isto é, $n < m$, e que $mdc(n, m) = 18$, determine os valores de $n$ e $m$ .

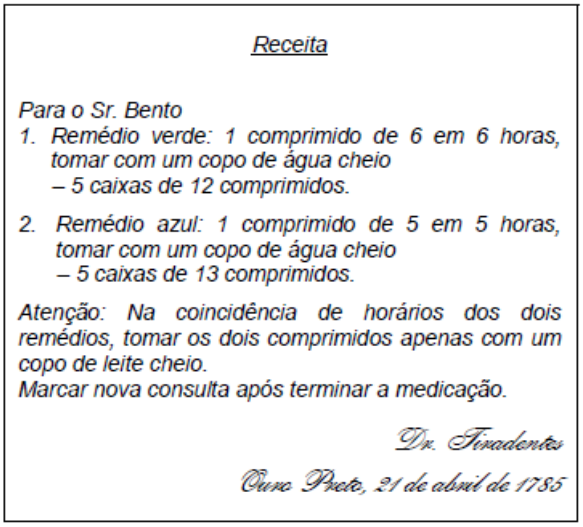
4. Entre algumas famílias de um bairro, foi distribuído um total de 144 cadernos, 192 lápis e 216 borrachas. Essa distribuição foi feita de modo que o maior número possível de famílias fosse contemplado e todos recebessem o mesmo

número de cadernos, o mesmo número de lápis e o mesmo número de borrachas, sem haver sobra de qualquer material.

Determine o número de cadernos que cada família ganhou.

5. O máximo divisor comum de dois números é 20. Para se chegar a esse resultado pelo processo das divisões sucessivas, os quocientes encontrados foram, pela ordem, 2,1,3 e 2 . Ache os números.

6. (OBMEP) Para curar uma infecção dentária de Bento, o Dr. Tiradentes prescreveu o tratamento descrito na receita abaixo.



*Receita*

*Para o Sr. Bento*

1. *Remédio verde: 1 comprimido de 6 em 6 horas, tomar com um copo de água cheio – 5 caixas de 12 comprimidos.*
2. *Remédio azul: 1 comprimido de 5 em 5 horas, tomar com um copo de água cheio – 5 caixas de 13 comprimidos.*

*Atenção: Na coincidência de horários dos dois remédios, tomar os dois comprimidos apenas com um copo de leite cheio.*
*Marcar nova consulta após terminar a medicação.*

*Dr. Tiradentes*

*Ouro Preto, 21 de abril de 1785*

Bento iniciou o tratamento às 6 horas da manhã do dia 22 de abril de 1785, tomando um comprimido verde e um azul. Quantos copos de água e quantos de leite Bento tomou por causa do tratamento?

# Capítulo 3

# Mínimo Múltiplo Comum (MMC)

**Definição 3.1.** *Considere $a$ e $b$ inteiros não nulos. O mínimo múltiplo comum de $a$ e $b$, indicado por mmc(a,b), é o menor dentre os múltiplos positivos comuns de $a$ e $b$.*

**Proposição 3.2.** *Sejam $a$ e $b$ inteiros positivos. Se $a$ é múltiplo de $b$, então $mmc(a, b) = a$.*

***Prova:*** Todo múltiplo comum de $a$ e $b$ é múltiplo de $a$. Todo múltiplo de $a$ é múltiplo de $b$, ou seja, um múltiplo comum de $a$ e $b$. Portanto, o conjunto dos múltiplos comuns de $a$ e $b$ é igual ao conjunto dos múltiplos de $b$. Como o menor múltiplo positivo de $a$ é ele mesmo, tem-se que $mmc(a, b) = a$. □

**Teorema 3.3.** *Se $a$ e $b$ são inteiros positivos, então*

$$mmc(a, b) = \frac{a \cdot b}{mdc(a, b)}. \tag{3.1}$$

***Prova:*** Considere $m = \frac{ab}{mdc(a,b)}$ e $d = mdc(a, b)$ . Uma vez que $d = mdc(a, b)$ , devem existir inteiros $a'$ e $b'$ , de forma que $a = a'd$ e $b = b'd$ . Como $m = \frac{ab}{mdc(a,b)} = \frac{a}{d} \cdot b = a \cdot \frac{b}{d} = a'b = ab'$ , tem-se $m$ é um múltiplo comum de $a$ e $b$. Seja $M$ um múltiplo comum de $a$ e $b$. Dessa forma, há inteiros $p$ e $q$ , de modo que $ap = bq = M$. Cancelando o fator $d$ em todos os membros, obtemos $a'p = b'q = \frac{M}{d}$ . O fato de $d = mdc(a, b)$, pela relação de Bézout, acarreta na existência de números inteiros $x$ e $y$ , tais que $ax + by = d$ . E isso implica em $a'x + b'y = 1$ . Multiplicando todos os membros dessa última igualdade por $p$, obtém-se $a'px + b'py = p$ . Substituindo $a'p$

por $b'q$, temos $b'qx + b'py = p$ . Logo, $b'|p$ . Mas isso garante que $a'b|ap$ . Portanto, $m|M$ . Consequentemente, $m \leq M$ . Segue daí que $m = mmc(a, b)$ . □

**Proposição 3.4.** *Sejam $a$ e $b$ inteiros não nulos e $m = mmc(a, b)$. Se $m_1$ é um múltiplo comum de $a$ e $b$, então $m|m_1$ .*

***Prova:*** Pela divisão euclidiana, devem existir inteiros $q$ e $r$ , tais que $m_1 = mq + r$, com $0 \leq r < m$ . Como $a|m$ e $a|m_1$ , segue da proposição 1.6, que $a|m_1 - mq$ , isto é, $a|r$ . Analogamente $b|r$. Logo, $r$, com $0 \leq r < m$, é um múltiplo comum de $a$ e $b$ . Desde que $m$ é o menor múltiplo comum positivo de $a$ e $b$, então a única possibilidade é termos $r = 0$, o que acarreta $m|m_1$ . □

A prova da proposição seguinte, por ser análoga à demonstração da proposição 2.9 , fica a cargo do leitor.

**Proposição 3.5.** *Considere $a$ e $b$ inteiros, com um deles não nulo. Assim,*

$$mmc(a, b) = mmc(|a|, |b|).$$

**Exemplo 3.6.** $mmc(-12, -15) = mmc(|-12|, |-15|) = mmc(12, 15) = \frac{12 \cdot 15}{mdc(12,15)} = \frac{12 \cdot 15}{3} = 12 \cdot 5 = 60.$

Define-se o mínimo múltiplo comum $mmc(a_1, a_2, \ldots, a_n)$ de vários inteiros $a_1, a_2, \ldots, a_n$, não nulos, de maneira análoga ao caso de dois inteiros, como sendo o menor múltiplo positivo comum de $a_1, a_2, \ldots, a_n$. Vale a seguinte proposição:

**Proposição 3.7.** *Sejam $a_1, a_2, a_3, \cdots, a_{n-1}, a_n$ números inteiros positivos. Então, tem-se que:*

$$mmc(a_1, a_2, a_3, \cdots, a_{n-1}, a_n) = mmc((a_1, a_2, a_3, \cdots, a_{n-1}), a_n). \tag{3.2}$$

**Exemplo 3.8.** *(VEST UFES-2011) Um feirante levava sempre a mesma quantidade $N$ de laranjas para serem vendidas na feira. Quando ele dividia as $N$ laranjas em sacolas contendo 4 laranjas cada uma, não sobrava nenhuma laranja. Quando dividia as $N$ laranjas em sacolas de 5 laranjas cada uma e quando as dividia em sacolas de 6 laranjas, cada uma, também não sobrava nenhuma laranja. Destaque-se que esse feirante nunca levava mais de 400 laranjas para a feira. Determine:*

***a)*** *Os possíveis valores de $N$ com base apenas nos dados acima.*

***b)****O valor de $N$, sabendo ainda que, no dia em que o feirante dividiu as $N$ laranjas em sacolas de 7 laranjas, cada uma, sobraram 3 laranjas.*

Solução:

**a)** Já que o resto da divisão de $N$ por 4, 5 e 6 é zero, $N$ deve ser múltiplo comum desses números. A fim de encontrarmos os possíveis valores de $N$, determinemos primeiro o $mmc(4, 5, 6)$. Esse número é 60. Sendo assim, os candidatos a valor de $N$ são os múltiplos de 60. Sabe-se também que o feirante nunca levava mais de 400 laranjas. Portanto, 60,120,180,240,300 e 360 são os possíveis valores de $N$.

**b)** O resto da divisão de $N$ por 7 é 3. Desse modo, para responder essa pergunta basta dividir cada um dos números obtidos no item anterior, por 7. Feito isso, observa-se que o único número que cumpre tais condições é 360. Portanto, $N = 360$.

# Exercícios:

1. Calcule:

   (a) $mmc(60, 8)$

   (b) $mmc(41, 12)$

   (c) $mmc(-132, 64)$

   (d) $mmc(-384, -144)$

   (e) $mmc(60, 132, -64)$

2. Se $x$ e $y$ são números naturais em que $mmc(y, x) = 115$ e $mdc(y, x) = 214$ , qual o resto da divisão $xy$ por 23?

3. Três navios fazem viagens entre dois pontos. O primeiro a cada 4 dias, o segundo a cada 6 dias e o terceiro a cada 9 dias. Se esses navios partirem juntos, depois de quantos dias voltarão a sair juntos, novamente?

4. (UE-RJ) O número de fitas de vídeo que Marcela possui está compreendido entre 100 e 150. Agrupando-as de 12 em 12, de 15 em 15 ou de 20 em 20, sempre resta uma fita.
   Qual é a soma dos três algarismos do número total de fitas que ela posui?

   (a) Os possíveis valores de $N$ com base apenas nos dados acima.

(b) O valor de $N$, sabendo ainda que, no dia em que o feirante dividiu as $N$ laranjas em sacolas de 7 laranjas, cada uma, sobraram 3 laranjas.

5. Numa pista de videogame, um carrinho dá uma volta completa em 30 segundos, outro em 45 segundos e um terceiro carrinho em 1 minuto. Se os três partem do mesmo ponto, no mesmo instante, determine o número de voltas que o mais rápido terá dado quando os três se encontrarem novamente.

6. (VUNESP) Em uma floricultura, há menos de 65 botões de rosas e um funcionário está encarregado de fazer ramalhetes, todos com a mesma quantidade de botões. Ao iniciar o trabalho, esse funcionário percebeu que se colocasse em cada ramalhete 3, 5 ou 12 botões de rosas, sempre sobrariam 2. Determine o número de botões de rosa.

# Capítulo 4

# Números Primos

**Definição 4.1.** *Um número inteiro $p > 1$ é dito primo se seus únicos divisores positivos forem 1 e $p$ (ele mesmo). Um número inteiro $a > 1$ que não é primo é chamado composto. Listamos abaixo os números primos menores que 50:*

$$2,3,5,7,11,13,17,19,23,29,31,37,41,43,47\ .$$

**Exemplo 4.2.** *O número $n = 2^{20} - 25^4$ é composto.*

Solução:

$n = 2^{20} - 25^4 = (2^{10})^2 - (25^2)^2 = 1024^2 - 625^2 = (1024 + 625) \cdot (1024 - 625)$

$n = 1649 \cdot 399.$

Como $399|2^{20} - 25^4$ , temos que $n$ é composto.

**Proposição 4.3.** *Se $p|a \cdot b$ , $p$ primo, então $p|a$ ou $p|b$.*

***Prova:*** Se $p|a$, então nada a fazer. Por outro lado, caso $p \dagger a$ , tem-se $mdc(p, a) = 1$, já que $p$ é primo. Sendo assim, pela relação de Bézout, devem existir $x$ e $y$ inteiros, de modo que $px + ay = 1$ . Multiplicando a igualdade por $b$ , obtemos $pbx + aby = b$. Como $p|pbx$ e $p|aby$ , tem-se $p|pbx + aby = b$ . Isso conclui a prova. □

**Exemplo 4.4.** *De que maneiras podemos comprar selos de cinco e sete reais, de modo a gastar cem reais?*

Solução:

Sejam $x$ e $y$ a quantidade de selos de cinco e sete reais, respectivamente.

Dessa forma,$5x + 7y = 100$. Segue daí que $7y = 100 - 5x$ é divisível por 5. Uma vez que 5 é primo e $5 \nmid 7$, tem-se que $y$ é múltiplo de 5. Por outro lado, $x \geq 0$ , pois representa uma quantidade. Logo, $5x = 100 - 7y \geq 0$. Isso acarreta $y \leq \frac{100}{7} \Rightarrow y < 15$. Portanto, os possíveis valores para $y$ são 0, 5 e 10.

A tabela abaixo ilustra as possíveis maneiras de comprar tais selos.

| Selos de 7 reais | 0 | 5 | 10 |
|---|---|---|---|
| Selos de 5 reais | 20 | 13 | 6 |
| Total de selos | 20 | 18 | 16 |
| Total a pagar (em reais) | $0 \cdot 7 + 20 \cdot 5 = 100$ | $5 \cdot 7 + 13 \cdot 5 = 100$ | $10 \cdot 7 + 6 \cdot 5 = 100$ |

## 4.1 O Teorema Fundamental da Aritmética

Os números primos são as células dos números naturais, no sentido de que qualquer número natural é produto de números primos. Por exemplo, $360 = 36 \cdot 10 = 4 \cdot 9 \cdot 2 \cdot 5 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 2 \cdot 5$ onde cada um dos fatores que aparecem no produto é primo. E se começássemos com outra fatoração inicial de 360, por exemplo, $360 = 9 \cdot 40$? Vejamos:

$$360 = 9 \cdot 40 = 3 \cdot 3 \cdot 5 \cdot 8 = 3 \cdot 3 \cdot 3 \cdot 5 \cdot 2 \cdot 2 \cdot 2.$$

Surpreendentemente chegamos à mesma representação anterior, com exceção da ordem dos fatores.

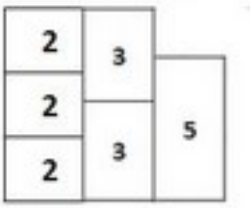



Figura 4.1:

Na figura acima, vemos que o número 360 é composto de 3 células do tipo 2, 2 células do tipo 3 e uma célula do tipo 5.

O fato observado acima vale para qualquer número natural maior que 1. Especificamente, temos o seguinte resultado como teorema fundamental da aritmética.

**Teorema 4.5** (Teorema Fundamental da Aritmética)**.** *Todo número inteiro n maior do que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

**Prova da existência.** Se $n$ for primo, então a prova está feita. Senão, seja $p_1 (p_1 > 1)$ o menor dos divisores de $n$. $p_1$ é primo. Isso é verdade, pois, caso não fosse, existiria $p$ , $1 < p < p_1$ com $p|p_1$ . Logo, $p|n$. Isso é um absurdo, pois $p_1$ é o menor inteiro positivo com tal propriedade.
Portanto, $n = p_1 \cdot n_1$ . Se $n_1$ for primo, então a prova está encerrada. Caso contrário, seja $p_2$ o menor fator positivo de $n_1$. Usando o mesmo argumento anterior, $p_2$ é primo e temos que $n = p_1 \cdot p_2 \cdot n_2$ . Repetindo esse processo, obtemos uma sequência decrescente de inteiros positivos $n_1, n_2, \cdots, n_r$ . Como todos eles são inteiros maiores do que 1, este processo finaliza. Já que os primos na sequência $p_1, p_2, \cdots, p_k$ não são necessariamente distintos, $n$ terá, em geral, a forma

$$n = p_1^{c_1} \cdot_2^{c_2} \cdots p_k^{c_k}. \tag{4.1}$$

***Prova da Unicidade.*** Sejam $p_1, p_2, \ldots, p_n, q_1, q_2, \ldots, q_m$ primos tais que $p_1 \cdot p_2 \cdots p_n = q_1 \cdot q_2 \cdots q_m$. Deve-se ter $m = n$, pois de outro modo, por exemplo, se $n < m$, ter-se-ia $p_1 \cdot p_2 \cdots p_n = q_1 \cdot q_2 \cdots q_n \cdots q_m$. Desde que $p_1$ é primo e divide $q_1 \cdot q_2 \cdots q_n \cdots q_m$, aplicando a proposição 4.3 várias vezes e reordenando os fatores no produto $q_1 \cdot q_2 \cdots q_n \cdots q_m$, se necessário, pode-se supor que $p_1$ divide $q_1$. Uma vez que $p_1$ divide $q_1$ e ambos $p_1$ e $q_1$ são primos, tem-se $p_1 = q_1$. Como $p_1 = q_1$ e $p_1 \cdot p_2 \cdots p_n = q_1 \cdot q_2 \cdots q_n \cdots q_m$ , então $p_2 \cdot p_3 \cdots p_n = q_2 \cdot q_3 \cdots q_n \cdots q_m$. Repetindo o mesmo argumento com $p_2$, conclui-se que $p_2 = q_2$ e $p_3 \cdot p_4 \cdots p_n = q_3 \cdot q_4 \cdots q_n \cdots q_m$.
Executando várias vezes o mesmo processo, conclui-se que $p_3 = q_3, \ldots, p_n = q_n$ e $1 = q_{n+1} \cdots q_m$ , o que não é verdade, pois $q_m$, sendo primo, não pode ser divisor de 1. Assim, de fato, $n = m$ e, após uma possível reordenação dos fatores em $q_1 \cdot q_2 \cdots q_n$ , tem-se $p_1 = q_1, p_2 = q_2, \ldots, p_n = q_n$. □

**Exemplo 4.6.** *Escreva 1080 como produto de primos.*

Solução:

$1080 = 2 \cdot 540 = 2 \cdot 2 \cdot 270 = 2 \cdot 2 \cdot 27 \cdot 10 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 2 \cdot 5 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5$

$1080 = 2^3 \cdot 3^3 \cdot 5.$

Usando um dispositivo prático, temos:

| | |
|---|---|
| 1080 | 2 |
| 540 | 2 |
| 270 | 2 |
| 135 | 3 |
| 45 | 3 |
| 15 | 3 |
| 5 | 5 |
| 1 | |

$$1080 = 2^3 \cdot 3^3 \cdot 5$$

Como consequência do teorema acima, temos o seguinte teste de primalidade de um número inteiro $n > 1$ . Este resultado se deve ao matemático grego Erastóstenes de Cirene.

**Proposição 4.7.** *Se um inteiro $n > 1$ não é divisível por nenhum primo tal que $p \leq \sqrt{n}$ , então $n$ é primo.*

***Prova:*** Suponha que $n$ não seja primo. Seja $q$ o menor número primo que divide $n$. Sendo assim, $n = qn_1$ , com $q \leq n_1$ , o que acarreta $q^2 \leq qn_1 = n$, portanto, $q \leq \sqrt{n}$. Logo, $n$ é divisível por um número primo $q$ tal que $q \leq \sqrt{n}$ , que é um absurdo. □

**Exemplo 4.8.** *Use a proposição 4.7 para provar que 311 é primo.*

***Prova:*** Note que $17 < \sqrt{311} < 18$ . Já que 311 não é divisível por nenhum primo $p \leq 17$ , pela proposição 4.7, temos 311 é primo. □

Para o lema seguinte, é útil estendermos a decomposição em fatores primos de um número inteiro maior que 1, permitindo expoentes iguais a 0. Por exemplo,

podemos escrever $48 = 2^4 \cdot 3$ e $270 = 2 \cdot 3^3 \cdot 5$ utilizando os primos 2,3 e 5 em ambos os casos, isto é, escrevendo $48 = 2^4 \cdot 3 \cdot 5^0$ e $270 = 2 \cdot 3^3 \cdot 5$.

**Lema 4.9.** *Sejam* $a = p_1^{n_1} \cdot p_2^{n_2} \cdots p_t^{n_t}$ *e* $d = p_1^{m_1} \cdot p_2^{m_2} \cdots p_t^{m_t}$ *inteiros positivos, onde* $p_1, \cdots, p_t$ *são primos e* $n_i, m_i \geq 0$ , $1 \leq i \leq t$ . *Então,* $d|a$ *se, e somente se,* $m_i \leq n_i$, $1 \leq i \leq t$ .

***Prova:*** Primeiro, deve-se provar que, se $d|a$, então $m_i \leq n_i$ , $1 \leq i \leq t$ . Se $d|a$, então existe um número $c$ tal que $a = dc$.
Escrevendo $c = p_1^{r_1} \cdot p_2^{r_2} \cdots p_t^{r_t}$, tem-se:

$$p_1^{n_1} \cdots p_t^{n_t} = p_t^{m_1} \cdot p_t^{m_t} \cdot p_1^{r_1} \cdots p_t^{r_t} = p_1^{m_1+r_1} \cdots p_t^{m_t+r_t}.$$

Pela unicidade do teorema fundamental da aritmética, vê-se que $n_i = m_1 + r_i$ . Segue daí que $n_1 \geq m_i, 1 \leq i \leq t$ . Assim a primeira parte está feita.
Agora deve-se provar que, caso $m_i \leq n_i, 1 \leq i \leq t$ , então $d|a$ .
Seja $m_i \leq n_i$ , $1 \leq i \leq t$ . Chamando $r_i = n_i - m_i$, obtém-se

$a = p_1^{m_1+r_1} \cdots p_t^{m_t+r_t} = p_1^{m_1} \cdots p_t^{m_t} \cdot p_1^{r_1} \cdots p_t^{r_t} = d \cdot p_1^{r_1} \cdots p_t^{r_t} = d$. Logo, $d|a$. $\square$

A partir do próximo teorema, usaremos a notação $\min\{a, b\}$ , para representar o elemento $x \in \{a, b\}$ tal que $x \leq a$ e $x \leq b$ . O $\max\{a, b\}$ é o elemento $y \in \{a, b\}$ , de modo que $y \geq a$ e $y \geq b$ .

**Exemplo 4.10.**

- $\min\{2, 4\} = 2$ ;
- $\max\{5, 11\} = 11$ ;
- $\min\{17, 17\} = \max\{17, 17\} = 17$ .

**Teorema 4.11.** *Se* $a = p_1^{n_1} \cdots p_t^{n_t}$ *e* $b = p_1^{m_1} \cdots p_t^{m_t}$ *são inteiros, nas condições do lema anterior, então valem as sentenças*

*(a)* $d = p_1^{\alpha_1} \cdots p_t^{\alpha_t} = mdc(a, b)$ , *em que* $\alpha_i = \min\{n_i, m_i\}$, *com* $1 \leq i \leq t$. ;

*(b)* $m = p_1^{\beta_1} \cdots p_t^{\beta_t} = mmc(a, b)$ , *em que* $\beta_i = \max\{n_i, m_i\}$ , *com* $1 \leq i \leq t$ .

***Prova:***

(a) Como $\alpha_i = \min\{n_i, m_i\}$ com $1 \leq i \leq t$ , pelo lema anterior, tem-se $d|a$ e $d|b$ . Seja $c$ um divisor comum de $a$ e $b$. Então tem-se $c = p_1^{c_1} \cdots p_t^{c_t}$ , com $c_i \leq n_i$ e $c_i \leq m_i$ , $1 \leq i \leq t$ , o que acarreta $c_i \leq \min\{n_i, m_i\}$ . Logo, $c|d$ , o que implica em $c \leq d$ . Portanto, $d = mdc(a, b)$ .

(b) Já que $\beta_i = \max\{n_i, m_i\}$ , com $1 \leq i \leq t$ , ainda pelo lema 4.9 , $a|m$ e $b|m$ . Seja $M$ um múltiplo comum de $a$ e $b$ , tem-se então que $M = p_1^{k_1} \cdots p_t^{k_t}$ , com $k_i \geq n_i$ e $k_i \geq m_i$ com $1 \leq i \leq t$ , o que implica em $k_i \geq \max\{n_i, m_i\}$ . Logo , $m|M$ , o que acarreta $m \leq M$ . Conclui-se então, que $m = mmc(a, b)$.

□

**Exemplo 4.12.** *Calcule o mmc e mdc de 36 e 90, usando a decomposição desses números em fatores primos.*

Solução:

Usando o dispositivo pratico, tem-se:

| | |
|---|---|
| 36 | 2 |
| 18 | 2 |
| 9 | 3 |
| 3 | 3 |
| 1 | |

$$\begin{aligned} & 2^2 \cdot 3^2 \\ 36 \;\; = \;\; & 2^2 \cdot 3^2 \cdot 5^0 \end{aligned} \tag{4.2}$$

| | |
|---|---|
| 90 | 2 |
| 45 | 3 |
| 15 | 3 |
| 5 | 5 |
| 1 | |

$$\begin{aligned} & 2 \cdot 3^2 \cdot 5 \\ 90 = \; & 2 \cdot 3^2 \cdot 5 \end{aligned}$$

$$\begin{aligned} mmc(36, 90) &= 2^2 \cdot 3^2 \cdot 5 = 4 \cdot 9 \cdot 5 = 180 \\ mdc(36, 90) &= 2 \cdot 3^2 \cdot 5 = 2 \cdot 9 = 18. \end{aligned}$$

Embora pareça ser mais simples, esse método deixa de ser útil quando os números envolvidos são grandes. Nesse caso, descobrir quais são os fatores primos

dos mesmos é trabalhoso e leva muito tempo. O exemplo seguinte ilustra bem isso.

**Exemplo 4.13.** *Sejam $p_1, p_2, ..., p_n$ primos distintos. Então, $mdc(q \cdot p_1 \cdot p_2 \cdots p_n + 1, p_1 \cdot p_2 \cdots p_n) = 1$, para todo inteiro $q$. Chega-se à essa conclusão em uma única etapa do algoritmo de Euclides, já que o resto da divisão de $q \cdot p_1 \cdot p_2 \cdots p_n + 1$ por $p_1 \cdot p_2 \cdots p_n$ é igual a 1 ( e o quociente é $q$). Por outro lado, para achar que $mdc(q \cdot p_1 \cdot p_2 \cdots p_n + 1, p_1 \cdot p_2 \cdots p_n) = 1$ pela fatoração em primos dá muito mais trabalho porque, nesse caso, teríamos que fatorar $q \cdot p_1 \cdot p_2 \cdots p_n + 1$ e $p_1 \cdot p_2 \cdots p_n$. Por exemplo, tomando $b = 270764039 = 7 \cdot 13 \cdot 29 \cdot 37 \cdot 47 \cdot 59$ e $a = 77 \cdot b + 1 = 20848831004$, tem-se que $mdc(a, b) = 1$, o que é verificado em um único passo no algoritmo de Euclides. Porém, será muito trabalhoso fatorar em primos $a = 20848831004$ e $b = 270764039$.*

**Lema 4.14.** *Considere $x$ e $y$ inteiros. Então,*

$$\max\{x, y\} + \min\{x, y\} = x + y.$$

***Prova:*** Se $x = y$, então $\max\{x, y\} = \max\{x, x\} = x = \min\{x, x\} = \min\{x, y\}$ . Logo, $\max\{x, y\} + \min\{x, y\} = x + x = x + y$. Se $x < y$, então $\max\{x, y\} = y$ e $\min\{x, y\} = x$, portanto, $\max\{x, y\} + \min\{x, y\} = x + y$.
Para o caso de $x > y$, procedemos de maneira análoga. □

O teorema 3.3 pode ser provado usando o teorema fundamental da aritmética, como segue:

**Teorema 4.15.** *Se $a$ e $b$ são inteiros positivos, então $mmc(a, b) \cdot mdc(a, b) = a \cdot b$ .*

***Prova:*** Se $a = 1$ ou $b = 1$, o resultado segue imediatamente. Se $a > 1$ e $b > 1$, pelo teorema 4.4 , então existem primos $p_1, \ldots, p_t$ , tais que $a = p_1^{n_1} \ldots p_t^{n_t}$ e $b = p_1^{m_1} \cdots p_t^{m_t}$ , com $m_i, n_i \geq 0$ , $0 \leq i \leq t$. Usando o lema 4.9, temos:
$mmc(a, b) = p_1^{\alpha_1} \ldots p_t^{\alpha_t}$ e $mdc(a, b) = p_1^{\beta_1} \cdots p_t^{\beta_t}$ em que
$\alpha_i = \max\{n_i, m_i\}$ e $\beta_i = \min\{n_i, m_i\}$ com $1 \leq i \leq t$ . Sabemos que, pelo lema 4.14, $\min\{n_t, m_t\} + \max\{n_t, m_t\} = n_t + m_t$. Logo,
$mmc(a, b) \cdot mdc(a, b) = p_1^{\alpha_1} \cdots p_t^{\alpha_t} \cdot p_1^{\beta_1} \cdots p_t^{\beta_t} = p_1^{\alpha_1 + \beta_1} \cdots p_t^{\alpha_t + \beta_t} = p_1^{\max\{n_1, m_1\} + \min\{n_1, m_1\}} \ldots p_t^{\max\{n_t, m_t\} + \min\{n_t, m_t\}} = p_1^{n_1 + m_1} \cdots p_t^{n_t + m_t} = p_1^{n_1} \cdots p_t^{n_t} \cdot p_1^{m_1} \cdots p_t^{m_t} = ab$ . □

**Exemplo 4.16.** *Qual o valor de n dos números:* $n_1 = 45 \cdot 60^n$ *e* $n_2 = 45^n \cdot 60$ *, se apenas sabe-se que o mmc desses números é 12 vezes o mdc deles.*

Solução:

Note que $45 = 3^2 \cdot 5$ e $60 = 2^2 \cdot 3 \cdot 5$. Sendo assim, podemos reescrever $n_1$ e $n_2$ da seguinte maneira: $n_1 = (3^2 \cdot 5) \cdot (2^2 \cdot 3 \cdot 5)^n = 2^{2n} \cdot 3^{n+2} \cdot 5^{n+1}$ e $n_2 = (3^2 \cdot 5)^n \cdot 2^2 \cdot 3 \cdot 5 = 2^2 \cdot 3^3 \cdot 5^{n+1}$. Sabe-se, também, que $mmc(n_1, n_2) = 12 \cdot mdc(n_1, n_2)$ . Segue daí, pelo teorema (4.10), que $12 \cdot mdc(n_1, n_2) \cdot mdc(n_1, n_2) = n_1 \cdot n_2$. Mas, $mdc(n_1, n_2) = 3 \cdot 2^2 \cdot 3^3 \cdot 5^{n+1}$. Logo, $12 \cdot (2^2 \cdot 3^3 \cdot 5^{n+1}) \cdot (2^2 \cdot 3^3 \cdot 5^{n+1}) = (2^{2n} \cdot 3^{n+2} \cdot 5^{n+1}) \cdot 2^2 \cdot 3^3 \cdot 5^{n+1}$. Após algumas manipulações algébricas, obtemos $n = 2$ .

# Exercícios

1. Determine o mmc e o mdc, dos pares de números abaixo, usando a decomposição desses números em fatores primos.

   (a) 25 e 80

   (b) 127 e 43

   (c) 2140 e 120

   (d) 414 e 68

2. Dois números naturais, de dois algarismos cada, tem produto igual a 972. Se o mdc deles é 9, quais são esses números?

3. (U.F. Lavras - MG) Sejam os números $m = 2^5 \cdot 3^3 \cdot 6^2$ , $n = 2 \cdot 3 \cdot 4^2 \cdot 5^2$. Assinale a alternativa INCORRETA.

   a) Se um número inteiro $c$ divide 96, então $c$ divide $m$ e $n$.
   b) O máximo divisor comum de $m$ e $n$ é 96.
   c) O mínimo múltiplo comum de $m$ e $n$ é $2^7 \cdot 3^5 \cdot 5^2$. d) $m$ é maior que $n$.
   e) O resto da divisão de $m$ por $n$ é zero.

4. Calcular o valor mínimo da soma $m+n+p$ tal que o mdc entre $A = 2^m \cdot 3^3 \cdot 5^p$ e $B = 2^2 \cdot 3^n \cdot 5^3$ seja igual a $60 \cdot 75$ .

5. Se $x$ é um número natural em que $mmc(14, x) = 154$ e $mdc(14, x) = 2$ , é correto dizer que $x$:

   (a) é um número primo.

   (b) é um número ímpar.

   (c) é maior que 50.

   (d) é divisível por 11.

   (e) é múltiplo de 14.

6. Numa criação de coelhos e galinhas, contavam-se 400 pés. Quantas são as galinhas e quantos são os coelhos, sabendo que a diferença entre esses dois números é a menor possível?

# Exercícios Complementares

1. (OBMEP) Valdemar vai construir um muro de 2m de altura por 7m de comprimento. Ele vai usar tijolos de 5cm de altura por 20cm de comprimento unidos por uma fina camada de cimento. Sabendo que os tijolos são vendidos em milheiros, quantos milheiros Valdemar vai ter que comprar para construir o muro?

2. (OBMEP) Catarina tem 210 cartões numerados de 1 a 210.

   (a) Quantos desses cartões têm um número que é múltiplo de 3?

   (b) Quantos desses cartões têm um número par que não é múltiplo de 3?

   (c) Qual é o menor número de cartões que Catarina deve pegar, ao acaso, para ter certeza de que 2 ou 3 seja divisor comum dos números escritos em pelo menos dois dos cartões selecionados?

3. (OBMEP) Quantos sinais de adição foram utilizados na expressão $2+0+1+3+2+0+1+3+2+0+1+3+\ldots+2+0+1=2013$?

4. Um terreno plano, de forma retangular, medindo 720m de comprimento por 540m de largura, foi dividido em lotes quadrados, com dimensões iguais. Considerando que esses lotes tenham lados com maior comprimento possível, determine em quantos lotes o terreno foi dividido.

5. (OBMEP) Lucas pensou em um número, dividiu-o por 285 e obteve o resto 77. Se ele dividir o número em que pensou por 57, qual é o resto que ele vai encontrar?

6. Um prédio possui duas escadarias, uma delas com 1000 degraus e a outra com 800 degraus. Sabendo que os degraus das duas escadas só estão no mesmo nível quando conduzem a um andar, descubra quantos andares tem o prédio.

7. (OBMEP) Em certo ano bissexto (isto é, o ano que tem 366 dias) o número de sábados foi maior que o número de domingos. Em que dia da semana caiu dia 20 de janeiro desse ano?

8. (OBMEP) A professora de Emília comprou 96 balas para repartir igualmente entre seus alunos, sem que sobrassem balas. No dia da distribuição todos os alunos foram à escola, exceto Emília. A professora distribuiu igualmente as balas entre os alunos presentes, mas sobraram 5 balas. Quantos alunos tem a turma de Emília?

9. (PROFMAT) O máximo divisor comum entre dois números naturais é 16 e o mínimo múltiplo comum desses números é 576. É correto afirmar que:

   (a) Os dois números são maiores que 50.

   (b) O produto dos dois números é maior que 8000.

   (c) Os dois números são múltiplos de 32.

   (d) Os dois números são divisores de 96.

   (e) Um dos números é múltiplo do outro.

10. (OBMEP) Uma piscina com fundo e paredes retangulares está totalmente revestida com azulejos quadrados iguais, todos inteiros. O fundo da piscina tem 231 azulejos e as quatro paredes têm um total de 1024 azulejos. Qual é em número de azulejos, a profundidade da piscina?

11. (CESGRANRIO) Seja $N$ um inteiro tal que $200 < N < 300$. Seja igual a 2 o resto da divisão de $N$ por 3, por 5 e por 8. Então a soma dos algarismos de $N$ é:

    (a) 5

    (b) 7

    (c) 8

    (d) 10

    (e) 12

12. (OBMEP) Rosa e Maria começam a subir uma escada de 100 degraus no mesmo instante. Rosa sobe 10 degraus a cada 15 segundos e Maria sobe 10

degraus a cada 20 segundos. Quando uma delas chegar ao último degrau, quanto tempo faltará para a outra completar a subida?

13. Ache dois números cujo produto é 4800 e seu *mdc* é 20.

14. Subindo uma escada de dois em dois degraus, sobra um degrau. Subindo a mesma escada de três em três degraus, sobram dois degraus. Determine quantos degraus possui a escada, sabendo que o número é múltiplo de 7 e está compreendido entre 40 e 100.

15. (PROFMAT) Um grupo de crianças brinca em torno de várias cadeiras. Se duas crianças sentam em cada cadeira, uma criança fica de pé. Se três sentam em cada cadeira, uma cadeira fica vazia. Qual o número de crianças?

16. (PROFMAT) Sejam $x$ e $y$ números inteiros tais que $10x + y$ seja um múltiplo de 7. Assinale a alternativa correta.

    (a) $x - 2y$ será certamente um múltiplo de 7.

    (b) $2x + y$ será certamente um múltiplo de 7.

    (c) $x - y$ será certamente um múltiplo de 7.

    (d) $2x - y$ será certamente um múltiplo de 7.

17. Em certo país, as cédulas são de \$4 e \$7 . Com elas é possível pagar, sem troco, qualquer quantia inteiro:

    (a) a partir de \$11, inclusive

    (b) a partir de \$18, inclusive

    (c) ímpar, a partir de \$7, inclusive

    (d) que seja \$1 mais do que um múltiplo de \$3

    (e) que seja \$1 menos do que um múltiplo de \$5

18. (OBMEP) Os 535 alunos e os professores de uma escola fizeram um passeio de ônibus. Os ônibus, com capacidade para 46 passageiros cada, ficaram lotados. Em cada ônibus havia um ou dois professores. Em quantos ônibus havia 2 professores?

19. (OBMEP) Uma professora distribuiu 286 bombons igualmente entre seus alunos da $6^a$ série. No dia seguinte, ela distribuiu, também igualmente 286 bombons, entre seus alunos da $7^a$ série. Os alunos da $7^a$ série reclamaram que cada um deles recebeu 2 bombons a menos que os alunos da $6^a$ série. Quantos alunos tem na $7^a$ série?

20. (OBMEP) Quantos números inteiros, múltiplos de 3, existem entre 1 e 2005?

21. (OBMEP) Uma turma tem 36 alunos e cada um deles tem um número de 1 a 36 na lista de chamada. Ontem, a professora chamou Lia ao quadro negro e mais os outros seis alunos cujos números eram múltiplos do número de Lia. Qual foi o maior número chamado?

22. (ENC-2012) O resto da divisão do inteiro $N$ por 20 é 8. Qual é o resto da divisão de $N$ por 5?

23. (OBMEP) O múltiplo irado de um número natural é o menor múltiplo do número formado apenas pelos algarismos 0 e 1. Por exemplo, o múltiplo irado de 2, bem como de 5, é 10; já o múltiplo irado de 3 é 111 e o de 110 é ele mesmo.

    "Um número inteiro é divisível por 3 e por 9 se, e somente se, a soma dos algarismos for divisível por 3 e por 9."

    (a) Qual é o múltiplo irado de 20?

    (b) Qual é o múltiplo irado de 9?

    (c) Qual é o múltiplo irado de 45?

    (d) Qual é o menor número natural cujo múltiplo irado é 1110?

24. (PROFMAT) Seja $N = 12^{2012} + 2012^{12}$. Qual é o maior valor de $n$ tal que $2^n$ é divisor de $N$.

25. (OBMEP) Cirilo associa a cada palavra um número, da seguinte maneira: ele troca cada letra por um número usando a tabela a seguir e, em seguida, multiplica esses números.

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 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 |

Por exemplo, o número associado à palavra MAR é 13x1x18=234.

(a) Qual é o número associado à palavra CABIDE?

(b) Escreva uma palavra com 4 letras cujo número associado seja 455.

(c) Explique por que não existe palavra cujo número associado seja 2013.

# Respostas dos exercícios

## Capitulo 1

1. **a)** $q = 5$ **e** $r = 20$. **b)**$q = -7$ **e** $r = 2$. **c)**$q = -8$ **e** $r = 44$. **d)**$q = -17$ **e** $r = 6$. **e)**$q = 27$ **e** $r = 16$.

**2. a)** $a = 630$ **e** $b = 105$. **b)** $a = 201$ **e** $b = 33$.

**3. 2.**

**4.6.**

**5. 5.**

## Capitulo 2

1. **a)4. b)1. c)4. d)18. e)4.**

**2. 143.**

**3.** $n = 36$ **e** $m = 180$.

**4.** 6.

**5. 500 e 180.**

**6. 103 e 11.**

# Capitulo 3

1.**a)**120. **b)**492. **c)**2012. **d)**3092. **e)**31680.

**2. 0.**

**3. 36.**

**4. 121. 5. 3.**

**6. 62.**

# Capitulo 4

1. **a)**400 **e** 5. **b)**5969 **e** 1. **c)**12840 **e** 20. **d)**14076 **e** 2.

**2. 108 e 9 ou 36 e 27.**

**3. c).**

**4. 7.**

**5. d.**

**6. 67 e 66.**

# Exercícios complementares

**1. 2.**

**2. a)**70. **b)**70. **c)**73.

**3. 1006.**

**4. 12.**

**5. 20.**

**6. 200.**

**7. quarta-feira.**

**8. 8.**

**9. b.**

**10. 16 azulejos.**

**11. c.**

**12. 50.**

**13. 240 e 20 ou 80 e 60.**

**14. 77.**

**15. 9 crianças.**

**16. a.**

**17. b.**

**18. 5.**

**19. 26.**

**20. 668.**

**21. 35.**

**22. 3.**

**23. a)**100. **b)**111111111. **c)**1111111110. **d)**6.

**24. 24**

**25. a)**1080. **b)Palavras formadas pelas letras A,E,G e M.**

# Referências Bibliográficas


Fabio Brochero Martinez, Carlos Gustavo Moreira, Nicola Saldanha e Eduardo Tengan. *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro.* Projeto Euclides, 2010.

Hygino H. Domingues. *Fundamentos de aritmética.* Atual Editora, 1991.

Krerley Irraciel Martins Oliveira e Adán José Corcho Fernándes. *Iniciação à Matemática: um curso com problemas e soluções.* SBM, 2012.

Abramo Hefez. *Elementos de Aritmética.* SBM, 2004.

Gelson Iezzi and Carlos Murakami. *Fundamentos de Matemática Elementar.* Atual Editora, 2004.

Antonio Caminha Muniz Neto. *Tópicos de Matemática Elementar: teoria dos números/Caminha Muniz.* SBM, coleção do professor de Matemática, 2013.

José Plínio de Oliveira Santos. *Introdução à Teoria dos Números.* impa (instituto nacional de matemática aplicada), 2007.

S. C. Coutinho. *Números inteiros e criptografia RSA.* instituto de matemática pura e aplicada - IMPA, sociedade brasileira de matemática - SBM , Série de computação e matemática, 1997.