Nazaré Bezerra

TEORIA DOS NÚMEROS

Um Curso Introdutório

editAedi
Assessoria de Educação a Distância • UFPA

Nazaré Bezerra

TEORIA DOS NÚMEROS

Um Curso Introdutório

1ª Edição

Belém

editAedi
Assessoria de Educação a Distância • UFPA

2018

AUTORA
Maria de Nazaré Carvalho Bezerra

CAPA
Giordanna De Gregoriis

IMAGEM
Wikimedia Commons

EDITORA
EditAedi

Dados Internacionais de Catalogação-na-Publicação (CIP)

Bezerra, Maria de Nazaré Carvalho
Teoria dos Números: um curso introdutório / Maria de Nazaré
Carvalho Bezerra. Belém: AEDI/UFPA, 2018

ISBN: 978-85-65054-57-7

1. Matemática
2. Teoria dos números

Conteúdo

1 O Anel dos Inteiros **7**

Axiomas da Adição: 7

Axiomas da Multiplicação: 8

Ordem em $\mathbb{Z}$ 9

2 Indução Matemática **12**

1 Introdução 12

2 Demonstração por Indução Matemática 14

3 Princípio da Indução Finita 17

3 Divisibilidade em $\mathbb{Z}$ **23**

1 Divisor de um Inteiro 23

2 Propriedades da Divisibilidade 24

3 Divisão Euclidiana 25

Algoritmo da Divisão 27

4 Paridade de um Inteiro 31

4 Sistema de Numeração **37**

1 Introdução 37

2 Representação de um inteiro em bases arbitrárias 39

5 Máximo Divisor Comum **46**

1 Introdução 46

2 MDC 47

3 Cálculo do MDC 48

Algoritmo para o Cálculo do MDC 50

4 Existência e Unicidade do MDC 51

5 Inteiros Relativamente Primos 55

6 Mínimo Múltiplo Comum **60**

1 Introdução 60

2 Múltiplos de um Inteiro 60

3 Mínimo Múltiplo Comum 62

4 Relação entre MDC e MMC 63

7 Números Primos **67**

1 Definição 67

2 Propriedades dos Números Primos 68

3 A Infinitude do Conjunto dos Primos 68

4 Decomposição em Fatores Primos 71

8 Aplicações da Decomposição em Fatores Primos **75**

1 Cálculo dos Divisores 75

2 Números de Divisores 77

3 Soma dos Divisores 78

4 Algoritmo II para o cálculo do MDC e MMC 80

9 Congruência em $\mathbb{Z}$ **84**

1 Introdução 84

2 Inteiros Congruentes 85

Propriedades Elementares da Congruência 86

3 Congruência no Conjunto dos Restos 88

4 Propriedades da Congruência 89

5 Aplicação da Congruência no Cálculo do Resto 91

10 Aplicações da Congruência em $\mathbb{Z}$ **98**

1 Introdução 98

2 Teorema de Euler 104

3 Teorema de Wilson 107

11 O Anel $\mathbb{Z}_m$ **112**

1 Inteiros Módulo m 112

2 Classes de Congruência 112

3 Propriedades das Classes de Equivalência 113

4 Conjunto das Classes Residuais 114

5 Operações em $\mathbb{Z}_m$ 116

6 Propriedades das Operações em $\mathbb{Z}_m$ . . . 118
Propriedades da Adição . . . 118
Propriedades da Multiplicação: . . . 119
7 Elementos Inversíveis em $\mathbb{Z}_m$ . . . 121
8 Divisores de Zero em $\mathbb{Z}_m$ . . . 122

12 Equações Diofantinas Lineares **128**
1 Introdução . . . 128
2 Definição . . . 128
3 Solução da Equação Diofantina . . . 129
4 Condição de Existência da Solução . . . 130
5 Conjunto Solução da Equação Diofantina . . . 132

13 Congruência Linear **137**
1 Introdução . . . 137
2 Condição de Existência da Solução . . . 138
3 Solução da Congruência Linear . . . 139
4 Conjunto Solução da Congruência Linear . . . 141
5 Congruência Lineares Equivalentes . . . 142

14 Sistema de Congruências Lineares **148**
1 Introdução . . . 148
2 Definição . . . 149
3 Solução do Sistema . . . 149
Algoritmo da Aplicação do Teorema Chinês do Resto . . . 150

15 Os Números Naturais **159**
1 Os Axiomas de Peano . . . 159
2 Operações em $\mathbb{N}$ . . . 160
Adição em $\mathbb{N}$ . . . 161
Multiplicação em $\mathbb{N}$ . . . 164
3 Ordem em $\mathbb{N}$ . . . 167
Propriedades da Relação de Ordem em $\mathbb{N}$ . . . 168
4 Princípio da Boa Ordem em $\mathbb{N}$ . . . 170

16 A Construção de $\mathbb{Z}$ **174**
1 Introdução . . . 174

2 A Relação de Equivalencia em $\mathbb{N} \times \mathbb{N}$ 175
3 Classes de Equivalência 176
4 O Conjunto dos Números Inteiros 177
5 Operações em $\mathbb{Z}$ 178
Adição em $\mathbb{Z}$ 178
Multiplicação em $\mathbb{Z}$ 181
6 Relação de Ordem em $\mathbb{Z}$ 185
Propriedades da Relação de Ordem em $\mathbb{Z}$ 186
7 Inteiros Positivos e Negativos 188
8 Princípio da Boa Ordem em $\mathbb{Z}$ 190

Bibliografia **192**

Prefácio

Este livro foi escrito para servir como material de apoio na disciplina Teoria dos Números, do Curso de Licenciatura em Matemática da UFPA, que atende ao alunos do PARFOR - Plano Nacional de Formação de Professores da Educação Básica, projeto que visa consolidar a formação acadêmica dos professores que ainda não tem graduação universitária, ou são graduados, mas atuam em áreas distintas de sua formação acadêmica.

O objetivo do livro é fornecer ao estudante as primeiras noções de Teoria dos Números, área da Matemática que estuda as propriedades dos números inteiros. São apresentadas no texto as propriedades que decorrem da estrutura de anel que $\mathbb{Z}$ possui, quando munido das operações de adição e multiplicação. Os conceitos e propriedades apresentados são, em sua grande maioria, os mesmos que o aluno-professor ministra no ensino fundamental e médio. O diferencial está no nível de abordagem e no rigor matemático, com as devidas justificativas e demonstrações de todas as afirmações feitas.

Na medida do possível, procuramos usar uma linguagem menos formal. Muitos teoremas são enunciados e demonstrados, dialogando-se com o leitor, de modo a conduzi-lo aos resultados desejados, sem menção das palavras *Teorema - Demonstração*, por vezes tão temíveis. No final de cada capítulo, apresentamos uma lista de exercícios. Optamos por exercícios com um baixo grau de dificuldade, os quais tem como objetivo principal o entendimento dos conceitos e resultados apresentados e, em algumas situações, conduzir o estudante a antecipar resultados em vêm à frente.

A experiência tem mostrado, que a pouca habilidade que tem o estudante, no início da graduação, para entender e construir demonstrações matemáticas, acaba por tornar extremamente confuso e improdutivo, o curso de Teoria dos Números, quando este começa demonstrando as propriedades elementares de $\mathbb{Z}$, as quais são o alicerce de toda a teoria que segue. Assim, assumimos no Capítulo 1, um conjunto de propriedades como verdadeiras (onze axiomas) e, nos treze capítulos subsequentes, seguimos demonstrando as demais propriedades dos inteiros. Levando dessa forma, o aluno a familiarizar-se gradativamente com as demonstrações matemáticas. Nos dois capítulos finais, 15 e 16, retornamos para demonstrar as afirmações feitas inicialmente. No Capítulo 15, estudamos os Números Naturais, a partir da axiomatização de Peano. Por fim, no Capítulo 16, fazemos a construção de $\mathbb{Z}$ a partir de $\mathbb{N}$, e demonstramos todas as propriedades apresentadas como axiomas no Capítulo 1.

Capítulo 1

O Anel dos Inteiros

Ao longo de todo este texto denotaremos por $\mathbb{Z}$ o conjunto

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

cujos elementos são chamados **números inteiros**. Nesta disciplina estudaremos eminentemente propriedades dos números inteiros.

Usaremos o símbolo $:=$ para indicar que a identidade define o objeto. Por exemplo, $a := b$, indica que a é igual a b, por definição.

Em $\mathbb{Z}$ estão definidas duas operações:
(i) **adição:** que associa a todo par (a, b) de números inteiros, a soma $a+b \in \mathbb{Z}$;
(ii) **multiplicação:** que associa a todo par (a, b) de números inteiros, o produto $a.b \in \mathbb{Z}$.

Em geral, representaremos o produto $a.b$ apenas por ab.

O conjunto $\mathbb{Z}$, juntamente com essas duas operações, tem algumas propriedades, apresentadas aqui como axiomas, isto é, assumiremos tais propriedades como verdadeiras, não sendo necessário demonstrá-las.

Axiomas da Adição:

(A1) A adiçao é **comutativa**, isto é, para quaisquer $a, b \in \mathbb{Z}$, tem-se:

$$a + b = b + a.$$

(A2) A adiçao é **associativa**, isto é, para quaisquer $a, b, c \in \mathbb{Z}$, tem-se:

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

(A3) **Existência** e unicidade do **elemento neutro** da adição:
Para qualquer $a \in \mathbb{Z}$, tem-se:

$$a + 0 = a.$$

Em função dessa propriedade, 0 (zero) é chamado o **elemento neutro da adição** e o único elemento em $\mathbb{Z}$ que tem essa propriedade.

(A4) Existência e Unicidade do **Oposto**:
Para cada inteiro a, existe um único inteiro, denotado por $-a$, chamado o **oposto ou inverso aditivo** de a, de modo que:

$$a + (-a) = 0.$$

Axiomas da Multiplicação:

(M1) A multiplicação é **comutativa**, isto é, para quaisquer $a, b \in \mathbb{Z}$:

$$ab = ba.$$

(M2) A multiplicação é **associativa**, isto é, para quaisquer $a, b, c \in \mathbb{Z}$:

$$(ab)c = a(bc).$$

(M3) Existência e unicidade do **elemento unidade**:
Para qualquer $a \in \mathbb{Z}$, tem-se que:

$$a.1 = a.$$

1 (um) é chamado o elemento neutro da multiplicação ou **elemento unidade**, sendo o único elemento em $\mathbb{Z}$ com essa característica.

Dado $a \in \mathbb{Z}$, definimos

$$\begin{cases} a^0 = 1 \\ a^n = \underbrace{a.a. \dots .a}_{n \text{ fatores}}, \quad \text{para} \quad n = 1, 2, 3, \dots \end{cases}$$

O axioma (D1) abaixo, relaciona as duas operações.

(D1) Distributividade da multiplicação com relação à adição:
Para quaisquer $a, b, c \in \mathbb{Z}$, tem-se:

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

Por possuir as oito propriedades acima, dizemos que o conjunto $\mathbb{Z}$, juntamente com as operações de adição e multiplicação, isto é, o terno $(\mathbb{Z}, +, .)$ é um anel comutativo e com elemento unidade - chamado **Anel dos Inteiros**.

O produto de dois inteiros somente é nulo quando pelo menos um dos fatores é zero, conforme o axioma abaixo. Por esta razão, dizemos que o anel dos inteiros é sem divisores de zero.

Ou equivalentemente, se $a \neq 0$ e $b \neq 0$, então $ab \neq 0$.

(D2) O conjunto $\mathbb{Z}$ é **sem divisores de zero**, isto é, para quaisquer $a, b \in \mathbb{Z}$, se $ab = 0$, então $a = 0$ ou $b = 0$.

Ordem em $\mathbb{Z}$

Usaremos as seguintes notações para os subconjuntos de $\mathbb{Z}$:

$$\begin{array}{ll} \mathbb{Z}^* = \mathbb{Z} - \{0\} & \text{(conjuntos dos inteiros não nulos);} \\ \mathbb{Z}_+ = \{0, 1, 2, 3, ...\} & \text{(conjuntos os inteiros não negativos)} \\ \mathbb{Z}_+^* = \{1, 2, 3, ...\} & \text{(conjuntos os inteiros positivos).} \end{array}$$

Dados inteiros a e b, dizemos que a **é menor do que** b (ou que b é maior do que a) e escrevemos $a < b$ (resp. $b > a$) se existe um **inteiro positivo** c, isto é, $c \in \mathbb{Z}_+^*$, tal que:

$$b = a + c.$$

Escrevemos $a \leq b$ (a é menor do que ou igual a b) se $a < b$ ou $a = b$.

$a \leq b$, se existe $c \in \mathbb{Z}_+$, tal que $b = a + c$.

Assumiremos, ainda, que soma e produto de inteiros positivos são sempre inteiros positivos, isto é, $\mathbb{Z}_+^*$ é fechado sob as operações de adição e multiplicação, conforme axioma abaixo.

(F1) Para quaisquer $a, b \in \mathbb{Z}_+^*$, tem-se:
(i) $a + b \in \mathbb{Z}_+^*$;
(ii) $a.b \in \mathbb{Z}_+^*$.

Dizemos que $n \in \mathbb{Z}$ é uma **cota inferior** de um subconjunto A de $\mathbb{Z}$, se $n \leq a$, para todo $a \in A$. E dizemos que A é limitado inferiormente, se A possui cota inferior.

Um número inteiro a_0 diz-se um **elemento mínimo** de um subconjunto A de $\mathbb{Z}$ ($a_0 = minA$), se $a_0 \leq a$, para todo $a \in A$ (isto é, a_0 é cota inferior de A) e $a_0 \in A$.

Em $\mathbb{Z}$, temos ainda o Princípio da Boa Ordem, também dado aqui como axioma.

(BPO) Princípio da Boa Ordem em $\mathbb{Z}$:

Todo subconjunto não vazio de $\mathbb{Z}$, limitado inferiormente, tem elemento mínimo.

$$\emptyset \neq A \subset \mathbb{Z}_+, \quad \Downarrow \quad \exists\, a_0 = minA.$$

Lista de Exercícios 1.

(01) Compare os axiomas da adição e os da multiplicação. Quais as semelhanças e quais as diferenças entre eles?

(02) Usando o axioma (A3):
(a) Determine o oposto ou os opostos dos seguintes inteiros: 3, -7 e 0. Em cada caso quantos opostos foram encontrados?
(b) Seja $a \in \mathbb{Z}$, mostre que o oposto de a é único.

(03) Sejam b e c dois inteiros.
(a) Sabendo-se que $5 + b = 5 + c$, o que se pode concluir sobre b e c? Por quê?
(b) Sabendo-se que $b + (-3) = c + (-3)$, o que se pode concluir sobre b e c? Prove sua afirmação.
(c) Mostre que para quaisquer $a, b, c \in \mathbb{Z}$, $a + b = a + c \Rightarrow b = c$. (Essa propriedade é chamada cancelamento da adição).

(04) Calcule 3.0, $(-30).0$, 27.0. Qual a conclusão tirada?

(05) Mostre $a.0 = 0.a = 0$, para todo $a \in \mathbb{Z}$.

(06) Usando apenas os axiomas dados no texto e resultados mostrados nas questões anteriores, mostre que para quaisquer $a, b, c \in \mathbb{Z}$, tem-se:
(a) $-(-a) = a$;
(b) $(-a)b = a(-b) = -(ab)$;
(c) $(-a)(-b) = ab$.

(07) Responda e justifique: $2 < 5$? $-2 \leq 2$? $7 \leq 7$? $-7 \leq -10$?

(08) Sejam $a, b \in \mathbb{Z}_+ = \{0, 1, 2, 3, ...\}$. Mostre que se $a+b = 0$, então $a = b = 0$.

(09) Mostre que para quaisquer $a, b, c \in \mathbb{Z}$ são válidas as propriedades:
(a) **reflexiva**: $a \leq a$;
(b) **antissimétrica**: se $a \leq b$ e $b \leq a$, então $a = b$;
(c) **transitiva**: Se $a \leq b$ e $b \leq c$, então $a \leq c$.

(10) Sejam $a, b, c \in \mathbb{Z}$. Mostre que:
(a) $a \leq b \Rightarrow a + c \leq b + c$;
(b) $a \leq b$ e $c \geq 0 \Rightarrow ac \leq bc$;
(c) $a \leq 0 \Rightarrow -a \geq 0$;
(d) $a \leq b$ e $c \leq 0 \Rightarrow bc \leq ac$.

(11) Dê exemplo de um número inteiro, cujo quadrado seja um número negativo. Prove sua afirmação.

(12) Pela tricotomia em $\mathbb{Z}$, uma e somente uma das condições a seguir se verifica: $0 < 1$ ou $0 = 1$ ou $1 < 0$. Qual é a verdadeira? Prove sua afirmação.

(13) Mostre que se $A \subset \mathbb{Z}$ tem elemento mínimo, então ele é único.

(14) Usando o axioma (PBO), mostre que todo subconjunto não vazio de $\mathbb{Z}_+$ tem elemento mínimo.

(15) Considere o conjunto $A = \{n \in \mathbb{Z} \mid 0 < n < 1\}$. Quantos elementos tem A? Prove sua afirmação.

Capítulo 2

Indução Matemática

1 Introdução

Usaremos a notação $P(n)$ para indicar uma propriedade associada a um inteiro n. Vejamos alguns exemplos:

Exemplo 1: Seja $P(n)$ a propriedade válida para todo inteiro positivo n, dada por:

$$P(n): \quad (3^n - 1) \text{ é um número par.} \tag{2.1}$$

A propriedade em questão diz que, se n é um inteiro positivo, então o número $(3^n - 1)$ é par. Nessa notação, a variável em questão é n, a qual deve sempre ser substituída por um número inteiro positivo.

Um inteiro é dito par, se é divisível por 2.

A pergunta que você deve estar fazendo é: - Isso é verdade, $(3^n - 1)$ é sempre um número par, qualquer que seja o inteiro positivo n?

• Como verificar se esta propriedade é verdadeira para $n = 4$, por exemplo?

- Basta substituir n por 4 na expressão (2.1) e conferir se a afirmação resultante é verdadeiro.

$$P(4): \quad (3^4 - 1) \quad \text{é um número par.}$$

Como $3^4 - 1 = 80$, que é um número par, a afirmação é verdadeira para $n = 4$.

• A propriedade $P(n)$ é verdadeira para $n = 7$?

Fazendo $n = 7$ em (2.1) e conferindo o resultado:

$$P(7): \quad (3^7 - 1) \quad \text{é um número par.}$$

Sendo $3^7 - 1 = 2186$, que é um número par, a afirmação é verdadeira para $n = 7$.

Você entendeu a notação? Para melhor fixar, verifique se são verdadeiras $P(2), P(9)$ e $P(16)$.

Exemplo 2: Considere $P(n)$ a propriedade associada ao inteiro positivo n, dada abaixo:

$$P(n): \quad 1^3 + 2^3 + ... + n^3 = (1 + 2 + ... + n)^2. \tag{2.2}$$

Inicialmente, vamos entender o que diz a propriedade. No lado esquerdo de (2.2) temos a soma dos cubos dos n primeiros inteiros positivos e no lado direito, o quadrado da soma destes n inteiros. A propriedade diz que esses dois valores são iguais, qualquer que seja o inteiro positivo atribuído à variável n.

Antes de questionarmos a validade da mesma, vamos treinar um pouco mais o uso dessa notação. Usando (2.2) escreva $P(5)$, $P(7)$, $P(k)$, $P(n+1)$ e $P(n+2)$. Depois confira suas respostas com as dadas abaixo.

Respostas:
$P(5): \quad 1^3 + 2^3 + 3^3 + 4^3 + 5^3 = (1 + 2 + 3 + 4 + 5)^2$
$P(7): \quad 1^3 + 2^3 + 3^3 + 4^3 + 5^3 + 6^3 + 7^3 = (1 + 2 + 3 + 4 + 5 + 6 + 7)^2$
$P(k): \quad 1^3 + 2^3 + ... + k^3 = (1 + 2 + ... + k)^2$
$P(n+1): \quad 1^3 + 2^3 + ... + n^3 + (n+1)^3 = (1 + 2 + ... + n + (n+1))^2$
$P(n+2): \quad 1^3 + 2^3 + ... + (n+1)^3 + (n+2)^3 = (1 + 2 + ... + (n+1) + (n+2))^2.$

• Como verificar se essa propriedade é verdadeira para $n = 3$?

Inicialmente, reescrevemos a propriedade substituindo n por 3. Nesse caso, nos dois lados teremos somas com 3 parcelas.

$$P(3): \quad 1^3 + 2^3 + 3^3 = (1 + 2 + 3)^2.$$

Como os dois valores são iguais a 36, temos uma identidade. Logo, a afirmação é verdadeira para $n = 3$.

• Como verificar se a propriedade é verdadeira para $n = 5$?

Fazendo $n = 5$ em (2.2) temos:

$$P(5): \; 1^3 + 2^3 + 3^3 + 4^3 + 5^3 = (1 + 2 + 3 + 4 + 5)^2.$$

Como ambas os valores são iguais a 225, a afirmação é verdadeira.

• Expresse a propriedade para $n = 4$ e $n = 7$ e verifique se são verdadeiras.

Exemplo 3: Considere a propriedade válida para todo inteiro positivo ímpar n, dada por:

$$P(n): \; (3n + 2) \text{ é um número primo.} \tag{2.3}$$

Um inteiro é primo se possui exatamente dois divisores positivos distintos.

• Você acha que esta afirmação é verdadeira?

Vejamos como fica a propriedade para os primeiros cinco inteiros positivos ímpares: 1, 3, 5, 7, 9:

- $P(1)$: $(3.1 + 2)$ é um número primo;
- $P(3)$: $(3.3 + 2)$ é um número primo;
- $P(5)$: $(3.5 + 2)$ é um número primo;
- $P(7)$: $(3.7 + 2)$ é um número primo;
- $P(9)$: $(3.9 + 2)$ é um número primo.

Como 5, 11, 17, 23 e 29 são todos números primos, $P(n)$ vale para todos esses inteiros. Isso já é suficiente para garantir que a propriedade vale para todo inteiro ímpar? Verifiquemos para $n = 11$:

$$P(11) \ : (3.11 + 2) \text{ é um número primo.}$$

Como $(3.11 + 2) = 35$, que não é um número primo, a afirmação feita não vale para $n = 11$ e consequemente não é verdadeira para todo inteiro positivo ímpar, sendo portanto, uma afirmação falsa.

2 Demonstração por Indução Matemática

No geral, se $P(n)$ é uma propriedade em n e afirma-se que a mesma é válida para todo inteiro positivo n, como verificar ou mostrar que tal afirmação é de fato verdadeira?

Como existem infinitos números inteiros positivos, a rigor deveríamos verificar se são verdadeiras as afirmações:

$$P(1), P(2), P(3), P(4), P(5), P(6), P(7), ...$$

ou seja, temos que verificar a validade de infinitas afirmações, sendo impossível tal fato. Nesta aula você vai aprender um método para mostrar que uma propriedade $P(n)$ é verdadeira para todo inteiro $n \geq n_0$, para algum inteiro n_0 fixado. O método usado para fazer essa prova é chamado **Demonstração por Indução Matemática**, o qual consiste em dois passos:

Passo 1 : Base da Indução:

Mostra-se que $P(n_0)$ é verdadeira, isto é, que a propriedade é válida para o primeiro inteiro n_0;

Passo 2: Passo Indutivo:

Assume-se que $P(n)$ é verdadeira para um inteiro arbitrário $n \geq n_0$ - chamada a *hipótese de indução* - e mostra-se que $P(n + 1)$ é verdadeira.

Daí, conclui-se que $P(n)$ é verdadeira para todo inteiro $n \geq n_0$.

Vejamos alguns exemplos de demonstrações por indução.

✓ **Exercícios 1.**

(01) Mostre que para todo inteiro $n \geq 1$, temos a identidade:

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

Solução:
Queremos mostrar que a propriedade:

$$P(n): \quad 1+2+3+....+n=\frac{n(n+1)}{2} \tag{2.4}$$

é verdadeira para todo inteiro $n \geq 1$. Como temos que provar a validade de uma afirmação para todo inteiro positivo, então faremos a demonstração por indução em n. Executaremos os dois passos da demonstração:

(i) **Base de Indução:** Mostrar que vale para o primeiro inteiro mencionado na propriedade.

Como queremos mostrar que a propriedade é válidade para todo inteiro $n \geq 1$, o primeiro inteiro para o qual se deve verificar a validade é $n = 1$. Assim, na base de indução devemos mostrar que $P(1)$ é verdadeira.

$$P(1): \quad 1=\frac{1(1+1)}{2}.$$

Ficamos com a identidade $1 = 1$. Logo, a afirmação é verdadeira para $n = 1$. No geral, a base de indução é apenas uma verificação da validade da propriedade.

(ii) **Passo Indutivo:** Assumir que $P(n)$ é verdadeira e mostrar que $P(n+1)$ é também verdadeira.

Seja $n \geq 1$ um inteiro arbitrário e suponha que $P(n)$ é verdadeira, isto é,

$$P(n): \quad 1+2+3+...+n=\frac{n(n+1)}{2} \quad \text{(hipótese de indução)} \tag{2.5}$$

Agora, devemos mostrar que $P(n+1)$ é verdadeira. Para melhor visualizarmos o que precisamos mostrar, vamos escrever $P(n+1)$. Como você já aprendeu, isto é feito substituindo n por $n+1$ em (2.4):

$$P(n+1): \quad 1+2+3+...+(n+1)=\frac{(n+1)((n+1)+1)}{2} \tag{2.6}$$

Essa é portanto a identidade que precisa ser mostrada. E o que temos a nossa disposição para mostrar tal igualdade? Temos a hipótese de indução dada em (2.5). Pense um pouco, que manipulações algébricas podemos fazer em (2.5) para obtermos (2.6)?

Somando $(n+1)$ em ambos os lados de (2.5):

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

No lado esquerdo, temos a mesma soma dada em (2.6), pois trata-se da soma dos $n+1$ primeiros inteitos positivos. No lado direito, somando as duas parcelas obtemos:

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

que é a identidade dada em (2.6), a qual queríamos mostrar. Provamos assim, que se a propriedade vale para n, então também vale para $n + 1$. Com esses dois passos podemos concluir que a propriedade é verdadeira para todo inteiro $n \geq 1$. $\square$

(02) Mostre que para todo inteiro positivo $\mathbf{n}, (\mathbf{3^n - 1})$ é um número par.

Solução:

Queremos mostrar que a propriedade:

$$P(n): \quad (3^n - 1) \text{ é um número par}$$

é verdadeira para todo inteiro $n \geq 1$. Faremos a demonstração por indução em n.

Base de Indução: Mostrar que $P(1)$ é verdadeira:

$$P(1): \quad (3^1 - 1) \quad \text{é um número par.}$$

Como $(3^1 - 1) = 2$ é um número par, $P(1)$ é verdadeira.

Passo Indutivo: Vamos assumir que $P(n)$ é verdadeira e mostrar que $P(n+1)$ é também verdadeira.

Seja $n \geq 1$ um inteiro arbitrário e suponha que $P(n)$ é verdadeira, isto é,

$$P(n): \quad (3^n - 1) \text{ é um número par} \qquad \text{(hipótese de indução)}$$

Agora devemos mostrar que $P(n + 1)$ é verdadeiro, isto é,

$$P(n + 1): \quad (3^{n+1} - 1) \text{ é um número par.}$$

O que precisamos fazer para provar que $(3^{n+1} - 1)$ é um número par? Lembremos que um inteiro é dito par se é divisível por 2, o que implica ser da forma $2k$, para algum inteiro k. Da hipótese de indução, temos que $(3^n - 1)$ é um número par, então podemos escrever $3^n - 1 = 2k$, com $k \in \mathbb{Z}$. E portanto, $3^n = 2k + 1$. Assim,

$$(3^{n+1} - 1) = 3.3^n - 1 = 3(2k + 1) - 1 = 2(3k + 1),$$

o qual é um número par. Logo, $P(n + 1)$ é verdadeira.

Com esses dois passos, podemos concluir que a propriedade é verdadeira para todo inteiro $n \geq 1$. $\square$

(03) Mostre que $\mathbf{n}! > \mathbf{n^2}$, para todo inteiro $\mathbf{n} \geq \mathbf{4}$.

Lembrando:
$$\begin{cases} 0! = 1, \\ n! = n.(n-1)!, \end{cases}$$

Solução:
Considere a propriedade:
$$P(n): \quad n! > n^2.$$

Usando demonstração por indução, mostraremos que $P(n)$ é verdadeira para todo inteiro $n \geq 4$.
(i) **Base de Indução:**
- Qual o inteiro que devemos usar para a base de indução? Observe que o enunciado diz que a propriedade é válida para todo $n \geq 4$, então devemos tomar $n_0 = 4$:
$$P(4): \quad 4! > 4^2.$$

Como $4! = 24 > 16 = 4^2$, $P(4)$ é verdadeira.

(ii) **Passo Indutivo:** Assumir que $P(n)$ é verdadeira e como consequência, provar que $P(n+1)$ é também verdadeira.

Seja $n \geq 4$ um inteiro e suponha que
$$P(n): \quad n! > n^2 \quad \text{(hipótese de indução)}$$

- O que devemos mostrar? Que $P(n+1)$ é verdadeira, ou seja,
$$P(n+1): \quad (n+1)! > (n+1)^2$$

Usando a definição de fatorial e a hipótese de indução temos:
$(n+1)! = (n+1).n!$ - definição de fatorial
$> (n+1)n^2$ - pela hipótese de indução $n! > n^2$
$> (n+1)(n+1)$ - pois $n^2 > (n+1)$ para todo inteiro $n \geq 2$.
$= (n+1)^2$. Assim, $(n+1)! > (n+1)^2$. De (i) e (ii), conclui-se que a propriedade é válida para todo inteiro $n \geq 4$. □

3 Princípio da Indução Finita

Vimos que a Demonstração por Indução, constituída de dois passos, é a técnica usada para mostrar que certa propriedade $P(n)$ é válida para todo número inteiro n maior ou igual a um valor inicial n_0. Você deve estar se perguntando:
- Por que os dois passos da demonstraçao garantem que as infinitas afirmações
$$P(n_0), P(n_0+1), P(n_0+2), P(n_0+3), \ldots.$$

são todas válidas? A resposta é dada no corolário a seguir, conhecido como *Princípio da Indução Finita.*

Teorema 1. *Sejam n_0 um inteiro e*

$$S \subset \{n_0, n_0+1, n_0+2, n_0+3, ...\},$$

o qual tem as seguintes propriedades:
(i) $n_0 \in S$;
(ii) Para todo inteiro $n \geq n_0$, se $n \in S$, então $n+1$ também pertence a S.

Nestas condições,

$$S = \{n_0, n_0+1, n_0+2, n_0+3, ...\}.$$

Com isso podemos enunciar o seguinte corolário, o qual justifica a demonstração por indução.

Corolário 1. *(Princípio da Indução Finita - 1^a Forma)*
Sejam n_0 um inteiro e $P(n)$ uma propriedade associada ao inteiro n. Se
(i) $P(n_0)$ é verdadeira e
(ii) Para todo inteiro $n \geq n_0$, temos a implicação:

$$P(n) \text{ verdadeira} \Rightarrow P(n+1) \text{ verdadeira.}$$

Nestas condições, $P(n)$ é verdadeira para todo inteiro $n \geq n_0$.

Para um melhor entendimento do Colorário 10, retornemos a questão 01 dos exercícios resolvidos anteriormente. Usando a demonstração por indução mostramos que:

$$P(n): \quad 1+2+3+...+n = \frac{n(n+1)}{2}$$

é validada para todo inteiro $n \geq 1$.

No passo 1, mostramos que essa propriedade vale para $n = 1$. Mas, se vale para $n = 1$, pelo passo 2, podemos concluir que a propriedade é também válida para $n = 2$. E novamente pelo passo 2, se vale para 2, então vale para 3. Aplicando repetidamente o passo de indução, segue que se vale para 3, vale para 4, se vale para 4, vale para 5 e assim sucessivamente. Sendo portanto válida para todos os inteiros maiores do que ou iguais a 1. É isso que afirma o Corolário 10.

Existe um variante do Princípio da Indução Finita, conhecido como Princípio da Indução Finita - 2^a Forma ou Princípio da Indução Completa.

Corolário 2. *(Princípio da Indução Finita - 2^a Forma)*
Sejam n_0 um inteiro e $P(n)$ uma propriedade associada ao inteiro n. Se
(i) $P(n_0)$ é verdadeira e;
(ii) Para todo inteiro $n \geq n_0$, temos a implicação:

$$P(n_0), P(n_0+1), P(n_0+2), ..., P(n) \text{ são verdadeiras} \Rightarrow P(n+1) \text{ é verdadeira.}$$

Nestas condições, $P(n)$ é verdadeira para todo inteiro $n \geq n_0$.

• Explique a diferença básica entre a 1^a e a 2^a Forma do Princípio de Indução Finita.

Lista de Exercícios 2.

(01) Dado um inteiro $n \geq 1$, seja $P(n)$ a propriedade dada por:

$$P(n): \quad 4 + 10 + 16 + ... + (6n - 2) = n(3n + 1)$$

(a) Expresse $P(5)$ e verifique se a mesma é verdadeira;
(b) Expresse $P(7)$ e verifique se a mesma é verdadeira;
(c) Expresse $P(k)$, $P(k + 1)$, $P(k + 3)$, considerando k um inteiro.

(02) Dado um inteiro $n \geq 1$, seja $P(n)$ a propriedade dada por:

$$P(n): \quad n! > n^3$$

(a) Expresse $P(4)$ e verifique se a mesma é verdadeira;
(b) Expresse $P(6)$ e verifique se a mesma é verdadeira;
(c) Expresse $P(k)$, $P(k + 1)$ e $P(k + 2)$, considerando k um inteiro.

Nas questões de (03) a (12), use Demonstração por Indução para provar que são válidas as afirmações feitas, onde n é um número inteiro.

(03) $1 + 3 + 5 + 7 + ... + (2n - 1) = n^2$, $\forall n \geq 1$.

(04) $4 + 10 + 16 + ... + (6n - 2) = n(3n + 1)$, $\forall n \geq 1$.

(05) $(-\frac{5}{2}) + (-2) + (-\frac{3}{2}) + (-1)... + \frac{n-6}{2} = \frac{n(n-11)}{4}$, $\forall n \geq 1$.

(06) $1^2 + 2^2 + 3^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}$, $\forall n \geq 1$.

(07) $1^3 + 2^3 + ... + n^3 = \left[\frac{n(n+1)}{2}\right]^2$, $\forall n \geq 1$.

(08) $1^2 + 3^2 + 5^2 + ... + (2n - 1)^2 = \frac{n}{3}(4n^2 - 1)$, $\forall n \geq 1$.

(09) $\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + ... + \frac{1}{2^n} = 1 - \frac{1}{2^n}$, $\forall n \geq 1$.

(10) $1.2 + 2.3 + 3.4 + 4.5 + ... + n(n + 1) = \frac{n(n+1)(n+2)}{3}$, $\forall n \geq 1$.

(11) $\frac{1}{1.2} + \frac{1}{2.3} + ... + \frac{1}{n(n+1)} = \frac{n}{n+1}$, $\forall n \geq 1$.

(12) $(1 + \frac{1}{1})(1 + \frac{1}{2})(1 + \frac{1}{3})...(1 + \frac{1}{n}) = n + 1$, $\forall n \geq 1$.

(13) Mostre que $n^2 > (n + 1)$ para todo inteiro $n \geq 2$.

(14) Mostre que $3n^2 > 3n + 5$, para todo inteiro $n \geq 2$.

(15) Mostre que $n^3 > 3n(n + 1) + 1$, para todo inteiro $n \geq 4$.

(16) Mostre que $2^n > n^3$, para todo inteiro $n \geq 10$.

(17) Mostre que $n! > 3^n$, para todo inteiro $n \geq 7$.

(18) Mostre que $n! > n^3$, para todo inteiro $n \geq 6$.

(19) Mostre que para todo inteiro $n \geq 1$, o número $(5^n - 5)$ é um múltiplo de 4.

(20) (**Somatório**) Seja $n \geq 1$ um natural e $a_1, a_2, ...a_n$ números reais. Escrevemos de modo abreviado a soma $a_1 + a_2 + ... + a_n$ como $\sum_{i=1}^{n} a_i$ (lê-se: somatório de a_i para i variando de 1 a n). Expresse cada uma das parcelas $a_1, a_2, ..., a_n$ dos somatórios abaixo e calcule o valor da soma:
(a) $\sum_{i=1}^{5}(2i+3)$;
(b) $\sum_{i=1}^{4}(i+1)(i+2)$;
(c) $\sum_{j=1}^{2}\sum_{i=1}^{3} 2^i.3^j$.

(21) (**Propriedades do Somátorio**) Dadas as sequências de números reais $a_1, a_2, ...a_n$ e $b_1, b_2, ..., b_n$ e c um número real, mostre que para todo inteiro $n \geq 1$,tem-se:
(a) $\sum_{i=1}^{n}(a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i$;
(b) $\sum_{i=1}^{n} ca_i = c\sum_{i=1}^{n} a_i$.

(22) (**Questão Desafio**) As **Torres de Hanói** é um jogo que consiste de uma base de madeira onde estão firmadas três hastes verticais (as torres) e um certo número de disco de madeira, de diâmetros diferentes, furados no centro. No começo do jogo os discos estão todos enfiados em uma das hastes, em ordem decrescente de tamanho, com o menor disco acima de todos. O objetivo do jogo é mover todos os discos para uma outra haste, obedecendo as seguintes regras:
(I) Somente um disco pode ser movido de cada vez;
(II) Um disco maior nunca pode ser posto sobre um disco menor.

(a) Determine o número mínimo de movimentos para se transferir 1 disco de uma torre a outra;
(b) Determine o número mínimo de movimentos para se transferir 2 discos de uma torre a outra;
(c) Determine o número mínimo de movimentos para se transferir 3 discos de uma torre a outra;
(d) Mostre que o número mínimo de movimentos para se transferir n discos de uma torre a outra é $2^n - 1$, para todo inteiro $n \geq 1$.

(23) (ENADE-2008) Considere a sequência numérica definida por

$$\begin{cases} a_1 = \sqrt{a} \\ a_{n+1} = \sqrt{a + \sqrt{a_n}}, \quad \text{para } n = 1, 2, 3, ... \end{cases}$$

Usando o princípio da indução finita, mostre que $a_n < a$ para todo $n \geq 1$ e $a \geq 2$. Para isso, resolva o que se pede nos itens a seguir:
(a) Escreva a hipótese e a tese da propriedade a ser demonstrada;
(b) Prove que $a(a-1) > 0$ para $a \geq 2$;

(c) Mostre que $\sqrt{a} < a$, para todo $a \geq 2$;
(d) Supondo que $a_n < a$, prove que $a_{n+1} < \sqrt{2a}$;
(e) Mostre que $a_{n+1} < a$;
(f) A partir dos passos anteriores, conclua a prova por indução.

(24) (ENADE-2011) Considere a sequência númerica definida por:

$$\begin{cases} a_1 = a \\ a_{n+1} = \frac{4a_n}{2+a_n^2}, \quad \text{para } n \geq 1 \end{cases}$$

Use o princípio de indução finita e mostre que $a_n < \sqrt{2}$ para todo número natural $n \geq 1$ e para $0 < a < \sqrt{2}$, seguindo os passos indicados nos itens a seguir:
(a) Escreva a hipótese e a tese da propriedade a ser demonstrada;
(b) Mostre que $s = \frac{4a}{2+a^2} > 0$ para $a > 0$;
(c) prove que $s^2 < 2$, para todo $0 < a < \sqrt{2}$;
(d) Mostre que $0 < s < \sqrt{2}$
(e) Suponha que $a_n < \sqrt{2}$ e prove que $a_{n+1} < \sqrt{2}$.
(f) Conclua a prova por indução.

Respostas da Lista de Exercícios 2

(01.a) Fazendo $n = 5$ na sentença dada, temos:
$P(5): \quad 4 + 10 + 16 + ... + (6.5 - 2) = 5.(3.5 + 1)$. Isso indica que o somatório no lado esquerdo tem o número 4 na primeira parcela e 28, na última parcela. Ficando então:
$P(5): \quad 4 + 10 + 16 + 22 + 28 = 5.16$. Como os valores resultantes em ambos os lados são iguais a 80, verifica-se a identidade, logo $P(5)$ é verdadeira;
(01.b) $P(7): \quad 4 + 10 + 16 + 22 + 28 + 34 + 40 = 7.22$. Ambos os resultante são iguais a 154, logo $P(7)$ é verdadeira;
(01.c) $P(k): \quad 4 + 10 + 16 + ... + (6k - 2) = k(3k + 1)$;
$P(k + 1): \quad 4 + 10 + 16 + ... + (6k - 2) + (6(k + 1) - 2) = (k + 1)(3k + 4)$;
$P(k + 2): \quad 4 + 10 + 16 + ... + (6(k + 1) - 2) + (6(k + 2) - 2) = (k + 2)(3k + 7)$.
(02.a) $P(4): \quad 4! > 4^3$, a qual é falsa, pois $4! = 24 < 4^3 = 64$;
(02.b) $P(6): \quad 6! > 6^3$, a qual é verdadeira, pois $6! = 720 > 6^3 = 216$;
(02.c) $P(k): \quad k! > k^3$; $P(k + 1): \quad (k + 1)! > (k + 1)^3$; $P(k + 2): \quad (k + 2)! > (k + 2)^3$.
(06) Fazendo a demonstração por indução em n:
(i) Base de Indução:
Para $n = 1$, temos a igualdade: $1^2 = \frac{1.(1+1)(2.1+1)}{6}$. Logo $P(1)$ é verdadeira;
(ii) Passo Indutivo: $P(n) \Rightarrow P(n + 1)$:
ou seja,

$$\underbrace{1^2 + 2^2 + ... + n^2 = \frac{n(n + 1)(2n + 1)}{6}}_{P(n)-\text{Hipótese de Indução}} \Rightarrow \underbrace{1^2 + ... + n^2 + (n + 1)^2 = \frac{(n + 1)((n + 1) + 1)(2(n + 1) + 1)}{6}}_{P(n+1)}$$

Suponha $P(n)$ verdadeira. Somando $(n + 1)^2$ em ambos os lados em $P(n)$ obtemos:
$1^2 + 2^2 + ... + n^2 + (n + 1)^2 = \frac{n(n+1)(2n+1)}{6} + (n + 1)^2$.
Somando agora as parcelas no lado direito:
$1^2 + 2^2 + ... + n^2 + (n + 1)^2 = \frac{(n+1)}{6}(n(2n + 1) + 6(n + 1)) = \frac{(n+1)(n+2)(2n+3)}{6}$, a qual é a identidade dada em $P(n + 1)$. Com isto mostramos a implicação $P(n) \Rightarrow P(n + 1)$.
De (i) e (ii), segue que $P(n)$ é verdadeira para todo $n \geq 1$.
(16) Fazendo a demonstração por indução em n:
(i) Base de Indução:
Para $n = 10$, verifica-se a desigualdade, pois $2^{10} = 1024 > 10^3 = 1000$.
(ii) Passo Indutivo: $P(n) \Rightarrow P(n + 1)$:
ou seja,

$$\underbrace{2^n > n^3}_{P(n)-\text{Hipótese de Indução}} \Rightarrow \underbrace{2^{n+1} > (n + 1)^3}_{P(n+1)}$$

Suponha $P(n)$ verdadeira. Então

$$\begin{aligned} 2^{n+1} = 2.2^n &> 2.n^3 \text{ - pela hipótese de indução} \\ &= n^3 + n^3 > n^3 + 3n(n + 1) + 1 \text{ - pela questão (15)} \\ &= n^3 + 3n^2 + 3n + 1 = (n + 1)^3. \end{aligned}$$

Portanto $2^{n+1} > (n + 1)^3$. Com isto mostramos a implicação $P(n) \Rightarrow P(n + 1)$.
De (i) e (ii) segue que $P(n)$ é verdadeira para todo inteiro $n \geq 10$.
(20.a) $\sum_{i=1}^{5}(2i + 3) = (5 + 7 + 9 + 11 + 13) = 45$;
(20.b) $\sum_{i=1}^{4}(i + 1)(i + 2) = (2.3 + 3.4 + 4.5 + 5.6) = 68$;
(20. c) $\sum_{j=1}^{2}\sum_{i=1}^{3} 2^i.3^j = \sum_{i=1}^{3} 2^i.3 + \sum_{i=1}^{3} 2^i.3^2 = (2 + 4 + 8).3 + (2 + 4 + 8).9 = 168$.

Capítulo 3

Divisibilidade em $\mathbb{Z}$

1 Divisor de um Inteiro

Definição 1. *Dizemos que um inteiro* **b** ***divide*** *outro inteiro* **a**, *se existe* $c \in \mathbb{Z}$, *tal que*

$$a = bc.$$

Escreve-se $b|a$ para simbolizar que b divide a e $b \nmid a$, para indicar que b não divide a.

Se b divide a, dizemos também que b é um *divisor* de a ou que b é um *fator* de a, ou ainda que a é um *múltiplo* de b.

Exemplos:
(01) $3|21$, pois $21 = 3.7$ e $7 \in \mathbb{Z}$;
(02) $-4|-24$, pois $-24 = (-4).6$ e $6 \in \mathbb{Z}$;
(03) $-9|36$, pois $36 = (-9).(-4)$ e $-4 \in \mathbb{Z}$;
(04) $0|0$, pois $0 = 0.2$ e $2 \in \mathbb{Z}$ (mais geralmente, $0 = 0.k$, $\forall k \in \mathbb{Z}$);
(05) $5 \nmid 16$, pois não existe $c \in \mathbb{Z}$, tal que $16 = 5.c$;
(06) $0 \nmid 2$, pois não existe $c \in \mathbb{Z}$, tal que $2 = 0.c$.

Não confundir as notações $2|6$ e $\frac{6}{2}$. O primeiro caso é uma afirmação, ela diz que 2 é um divisor de 6. No segundo caso, temos uma fração. Podemos escrever $\frac{6}{2} = 3$.
.

✓ Exercícios 2.
(01) Responda e justifique:
(a) $2|18$?
(b) $-3|18$?
(c) $-15|-120$?
(d) $3|25$?
(e) $0|3$?
(f) $3|0$?

(02) Mostre que se a é um inteiro e $0|a$, então $a = 0$ (ou seja, o único inteiro divisível por zero é o próprio zero).

(03) Mostre que para qualquer $a \in \mathbb{Z}$, os inteiros 1 e a são divisores de a.

2 Propriedades da Divisibilidade

A proposição a seguir dá uma importante propriedade da divisibilidade.

Proposição 1. *Sejam a, b e c inteiros. Se $a|b$ e $a|c$, então*

$$a|(bm + cn)$$

quaisquer que sejam $m, n \in \mathbb{Z}$. Em particular, se $a|b$, então $a|bm$, para qualquer inteiro m.

Demonstração:
Como $a|b$ e $a|c$, pela Definição 1, isso implica que existem inteiros c_1 e c_2, tais que

$$b = ac_1$$

e

$$c = ac_2.$$

Então, dados inteiros quaisquer m e n, multiplicando a primeira identidade por m e a segunda por n obtemos:

$$bm = a(c_1m)$$

$$cn = a(c_2n).$$

Somando essas duas identidades:

$$bm + cn = a(c_1m + c_2n) \Rightarrow a|(bm + cn),$$

pois $c_1m + c_2n \in \mathbb{Z}$. Em particular, para $c = b$ e $n = 0$, temos que $a|bm$. □

Exemplos:
(01) Como $4|20$ e $4|8$, segue que $4|(20m+8n)$, quaisquer que sejam os inteiros m e n. Assim, podemos afirmar que $4|(20.(-3) + 8.5)$ e também $4|(20.144 + 8.(-19))$, por exemplo. □

A próxima proposição fornece o intervalo no qual estão os possíveis divisores positivos de um inteiro.

Lembrando:

$|a| = a$, **se** $a \geq 0$

$|a| = -a$, **se** $a < 0$

Proposição 2. *Sejam a e b inteiros, com $a \neq 0$. Se $b|a$, então $|b| \leq |a|$.*

Demonstração:
Suponha que $b|a$ e $a \neq 0$, então existe $0 \neq c \in \mathbb{Z}$, tal que: $a = b.c$. Usando a propriedade de módulo temos:

$$a = b.c \Rightarrow |a| = |b.c| = |b|.|c| \geq |b|.1 = |b|,$$

pois $|c| \geq 1$, qualquer que seja o inteiro $c \neq 0$. Assim, temos que $|b| \leq |a|$. □

Se b é um divisor positivo de um inteiro não nulo a, pela proposição anterior, $1 \leq b \leq |a|$. Se $b \mid a$ e $1 < b < |a|$, diz-se que b é um **divisor próprio** de a.

3 Divisão Euclidiana

Considere que você tem 20 moedas de $R\$1,00$ e quer dividir esse valor por 5 pessoas, de modo que todas elas recebam o mesmo número de moedas, sendo esse número o maior possível. Como

$$20 = 5.4$$

então você deverá dar 4 moedas a cada pessoa, ficando com zero moedas.

E se você tiver que dividir as mesmas 20 moedas por 6 pessoas? Como 6 não é um divisor de 20, a pergunta neste caso é: - qual a quantidade máxima de moeda que pode ser dada a cada uma delas? Se você for distribuindo uma a uma, descobrirá que pode dar 3 moedas a cada uma delas e restarão 2 moedas. Expressamos isso escrevendo:

$$20 = 6.3 + 2.$$

Dizemos que 3, a quantidade de moedas recebida por cada uma das 6 pessoas, é o quociente dessa divisão e 2 é o resto. Este resultado, enunciado no próximo teorema, conhecido como Algoritmo da Divisão ou Algoritmo de Euclides, é de suma importância na teoria dos números inteiros.

Em preparação ao teorema, façamos os exercícios a seguir.

✓ **Exercícios 3.**

(01) Dados inteiros $b > 0$ e a qualquer, definamos o conjunto:

$$S := \{a - bx \mid x \in \mathbb{Z} \;\text{ e }\; a - bx \geq 0\}.$$

Usando essa definição, construa S para a e b abaixo e determine, caso exista, o elemento mínimo de S e o valor correspondente de $x \in \mathbb{Z}$, para o qual se obtém esse elemento mínimo:

(a) $a = 13$, $b = 4$;

Solução:

Usando a definição, temos:

$$S := \{13 - 4x \mid x \in \mathbb{Z} \text{ e } \; 13 - 4x \geq 0\}.$$

$13 - 4x \geq 0 \Rightarrow x \leq \frac{13}{4} \Rightarrow S = \{13 - 4x \mid x \in \mathbb{Z} \;\text{ e }\; x \leq 3\} = \{1, 5, 9, 13, 17, ...\}$.
Logo, $minS = 1 = 13 - 4.3 \Rightarrow$ o minimo de S é obtido para $x = 3$. □

(b) $a = -13$, $b = 4$;

Solução:

Pela definição:

$$S := \{-13-4x \mid x \in \mathbb{Z} \text{ e } -13-4x \geq 0\} = \{13-4x \mid x \in \mathbb{Z} \text{ e } x \leq -4\} = \{3, 7, 11, 15, ...\}.$$

Assim, $minS = 3 = -13 - 4.(-4)$, obtido para $x = -4$. □

(c) $a = 12$, $b = 20$;
Solução:
Usando a definição:

$$S := \{12 - 20x \geq 0 \mid x \in \mathbb{Z}\}.$$

$12 - 20x \geq 0 \Rightarrow x \leq \frac{12}{20} \Rightarrow S = \{12 - 20x \mid x \in \mathbb{Z} \text{ e } x \leq 0\} = \{12, 32, 52, 72, ...\}$.
Logo, $minS = 12 = 12 - 20.0$, obtido quando $x = 0$. $\square$

(d) $a = -12$, $b = 20$;
Solução:
$-12 - 20x \geq 0 \Rightarrow x \leq -\frac{12}{20} \Rightarrow S = \{-12 - 20x \mid x \in \mathbb{Z} \text{ e } x \leq -1\} = \{8, 28, 48, 68, ..\}$. Assim, $minS = 8 = -12 - 20.(-1)$, obtido para $x = -1$. $\square$

(e) $a = 92$, $b = 5$;

(f) $a = -92$, $b = 5$.

(02) Dados inteiros $b > 0$ e a qualquer, considerando S o conjunto definido na questão 01, mostre que:
(a) $S \neq \emptyset$;
Solução:
Para garantir que $S \neq \emptyset$, precisamos mostrar que quaisquer que sejam a e $b > 0$, sempre existe $x \in \mathbb{Z}$, tal que $a - bx \geq 0$. Como $b \geq 1$, tomando $x = -|a|$, segue que $a - bx = a + b|a| \geq a + |a| \geq 0$. Assim, $a + b|a| \in S$, quaisquer que sejam a e b, logo $S \neq \emptyset$. $\square$

(b) Se $r = minS$, então $0 \leq r < b$.
Solução:
Como $r = minS \Rightarrow r \in S \Rightarrow r \geq 0$, pela definição de S. Resta mostrar que $r < b$. Suponhamos, que isso seja falso, isto é, $r \geq b \Rightarrow r - b \geq 0$. Como $r \in S$, $r = a - bx$, para algum $x \in \mathbb{Z}$. Assim,

$$0 \leq r - b = (a - bx) - b = a - b(x + 1) \Rightarrow r - b \in S.$$

Um absurdo, pois $r - b < r = minS$. Portanto, $0 \leq r < b$. $\square$

Teorema 2. ***(Algoritmo da Divisão)*** *Dados inteiros a e b, com $b \neq 0$,* ***existem únicos*** *inteiros q e r, tais que*

$$a = bq + r,$$

com $0 \leq r < |b|$.

Demonstração:
(I) Existência de q e r:
Inicialmente, mostraremos a existência de q e r. Como $b \neq 0$, temos dois casos possíveis:

Caso 1: $b > 0$:
Considere o conjunto $S = \{a - bx \mid x \in \mathbb{Z} \text{ e } \ ax - bx \geq 0\}$, como definido no exercício anterior. Conforme mostrado na questão 02, $\emptyset \neq S \subset \mathbb{Z}_+$, logo pelo Princípio da Boa Ordem (Axioma (PBO)), existe $r = minS \Rightarrow r \in S$
$\Rightarrow r = a - bq$, para algum $q \in \mathbb{Z} \Rightarrow a = bq + r$, com $q, r \in \mathbb{Z}$ e como mostrado na letra (b) da questão 02, $0 \leq r < b$.

Caso 2: $b < 0$
Nesse caso, $|b| = -b > 0$ e pelo Caso 1, existem q' e r' tais que:

$$a = |b|q' + r' = b(-q') + r', \text{ com } 0 \leq r' < |b|.$$

Assim, basta tomar $q = -q'$ e $r = r'$. □

(II) Unicidade de q e r:
Suponha que existam $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, tais que:

$$a = bq_1 + r_1 \quad \text{ e } \quad a = bq_2 + r_2$$

com $0 \leq r_1, r_2 < |b|$.

Se $r_1 \neq r_2$, suponhamos $r_1 < r_2$, então

$$0 < r_2 - r_1 = b(q_1 - q_2) \Rightarrow b|(r_2 - r_1) \Rightarrow |b| \leq |r_2 - r_1| = (r_2 - r_1).$$

Um absurdo, pois $r_2 - r_1 \leq r_2 < |b|$. Assim, $r_1 = r_2 \Rightarrow b(q_1 - q_2) = 0$ e como $b \neq 0$, $q_1 = q_2$. □

Os números q e r do teorema anterior, chamam-se respectivamente, o **quociente** e o **resto** da divisão de a por b. Costuma-se chamar **divisão euclidiana** a divisão entre inteiros satisfazendo as condições dadas no Teorema 2.

Dizemos também que a é o dividendo e b, o divisor.

Algoritmo da Divisão

Dados inteiros a e $b \neq 0$, para garantir a existência do quociente q e do resto r citados no Teorema 2, construímos o conjunto $S = \{a - bx \geq 0 \mid x \in \mathbb{Z}\}$ e tomamos $r = minS$ e q o inteiro para o qual temos $r = a - bq$ (para $b > 0$) ou $r = a + bq$ (para $b < 0$). Na prática, veremos como encontar q e r. Vamos considerar dois casos, conforme o sinal do divisor b:

- **Caso 1:** $b > 0$
  Dependo do valor de a, temos os seguintes subcasos:
  - **Caso 1.1 -** $a \geq 0$
    Tomamos q como a parte inteira da divisão de a por b e $r = a - bq$. Vejamos os exemplos a seguir:

Exemplos:
(01) Encontre o quociente e o resto da divisão de:
(a) 83 por 8
Tomando q como a parte inteira da divisão de 83 por 8 e $r = 83 - 8q$, temos: $q = 10$ e $r = 3$. Assim, $83 = 8.10 + 3$. □

Observe que também temos as identidades:

$$
\begin{aligned}
83 &= 8.9 + 11 \\
83 &= 8.8 + 19 \\
83 &= 8.7 + 27 \\
83 &= 8.11 + (-5) \\
&....
\end{aligned}
$$

que correspondem aos demais elementos do conjunto S. Porém, em todos esses casos, o resto r não está de acordo com a condição $0 \leq r < 8$, conforme enunciado no Teorema 2, portanto em nenhum deles temos a divisão euclidiana. □

(b) 36 por 9
Como $36 = 9.4$, então $q = 4$ e $r = 36 - 9.4 = 0$. □

(c) 9 por 36
Tomando q como a parte inteira da divisão de 9 por 36 e $r = 9 - 36q$, temos $9 = 36.0 + 9$, ou seja, $q = 0$ e $r = 9$. □

– **Caso 1.2:** $a < 0$
Nesse caso, efetuamos a divisão de $|a|$ por b, conforme descrito no Caso 1.1. Encontramos q' e r', com $0 \leq r' < b$, tais que:

$$|a| = b.q' + r'$$

Como $a < 0$, então $|a| = -a$ e essa identidade fica:

$$-a = b.q' + r'$$

Multiplicando a identidade por -1:

$$a = b.(-q') + (-r')$$

Se $r' = 0$, então $q = -q'$ e $r = r' = 0$. Porém se $r' \neq 0$, então $-r' < 0$, logo não pode ser o resto da divisão euclidiana. Para encontrarmos o resto, adicionamos $(b - b)$ no lado direito da identidade e rearrumamos:

$$a = b.(-q') + (-r') + (b - b)$$

$$\Downarrow$$

$$a = b.(-q' - 1) + (b - r').$$

Assim, $q = -q' - 1$ e $r = b - r'$. Como, $0 < r' < b \Rightarrow 0 < b - r' < b$. Logo, $r = b - r'$ é de fato o resto da divisão euclidiana.

Exemplos:
(01) Encontre o quociente e o resto da divisão de :
(a) -36 por 9
Solução:
Fazemos a divisão de $|-36|$ por 9.
Como $36 = 9.4 + 0 \Rightarrow -36 = 9.(-4) + 0$, então $q = -4$ e $r = 0$. $\square$

(b) -83 por 8
Fazemos a divisão de $|-83|$ por 8. Já vimos que:

$$83 = 8.10 + 3$$

Assim, $q' = 10$ e $r' = 3$. Usando o que já foi deduzido acima, temos que $q = -q' - 1 = -11$ e $r = b - r' = 8 - 3 = 5$. Daí,

$$-83 = 8.(-11) + 5.$$

Lembramos que podemos deduzir os valores de q e r, repetindo o procedimento feito no Caso 1.2, não sendo necessário memorizar tais valores. $\square$

(c) -112 por 42
Fazemos a divisão de $|-112|$ por 42:

$$112 = 42.2 + 28$$

Para um melhor entendimento do que foi feito no Caso 1.2, vamos repetir novamente todo o procedimento, em vez de tomarmos diretamente os valores de q e r como feito no letra (b).
Multiplicando a identidade acima por por -1:

$$-112 = 42.(-2) + (-28)$$

Como $-28 < 0$, não trata-se do resto da divisão euclidiana. Adicionando $(42 - 42)$ no lado direito e reescrevendo a expressão:

$$-112 = 42.(-2) + (-28) + (42 - 42)$$

$$-112 = 42.(-2 - 1) + (42 - 28) \Rightarrow -112 = 42.(-3) + 14$$

Assim, $q = -3$ e $r = 14$. $\square$

- **Caso 2:** $b < 0$**:**
Como $|b| > 0$, pelo Caso 1, existem q' e r', tais que

$$a = |b|.q' + r',$$

com $0 \leq r' < |b|$. Como $|b| = -b$, a identidade acima fica:

$$a = (-b).q' + r' \Rightarrow a = b.(-q') + r'.$$

Assim, $q = -q'$ e $r =$ r'.

Exemplos:
(01) Encontre o quociente e o resto da divisão:
(a) 36 por -9
Solução:
Dividimos 36 por $|-9|$:
$36 = 9.4 + 0 \Rightarrow 36 = (-9).(-4) + 0$. Assim, $q = -4$ e $r = 0$. $\square$

(b) 83 por -8
Solução:
Dividimos 83 por $|-8|$:
$83 = 8.10 + 3 \Rightarrow 83 = (-8).(-10) + 3$. Assim, $q = -10$ e $r = 3$. $\square$

(c) -83 por -8
Solução:
Dividimos $|-83|$ por $|-8|$:

$$83 = 8.10 + 3$$

Usando o Caso 1.2, multiplicamos a identidade por -1:

$$-83 = 8.(-10) + (-3)$$

Somamos $(8 - 8)$ no lado direito a fim de obtermos um resto positivo:

$$-83 = 8.(-10) + (-3) + (8 - 8) \Rightarrow -83 = 8.(-10 - 1) + (8 - 3)$$

Assim,

$$-83 = 8.(-11) + 5$$

Resta agora fazermos uma inversão de sinais entre divisor e quociente:

$$-83 = (-8).11 + 5$$

Portanto, $q = 11$ e $r = 5$. $\square$

(d) -112 por -42
Solução:
Dividindo $|-112|$ por $|-42|$, obtemos:

$$112 = 42.2 + 28$$

Multiplicando por -1:

$$-112 = 42.(-2) + (-28)$$

Somando $(42 - 42)$ no lado direito:

$-112 = 42.(-2) + (-28) + (42 - 42) \Rightarrow -112 = 42.(-2 - 1) + (42 - 28)$

Assim,

$$-112 = 42.(-3) + 14 \Rightarrow -112 = (-42).3 + 14$$

Assim, $q = 3$ e $r = 14$. $\square$

4 Paridade de um Inteiro

Segue do algoritmo da divisão que todo inteiro n pode ser escrito na forma $n = 2q + r$, com $0 \leq r < 2$. Se $r = 0$, isto é, $n = 2q$, então diz-se que n é um inteiro **par**, e se $r = 1$, $n = 2q + 1$ é dito um inteiro **ímpar**. Chama-se **paridade** de um inteiro a sua propriedade de ser par ou ímpar.

Exemplos:
(01) 26 é um número par, pois deixa resto 0 na divisão por 2, isto é, $26 = 2.13 + 0$. Já -15 é um inteiro ímpar, pois deixa resto 1 na divisão por 2, uma vez que
$-15 = 2.(-8) + 1$. $\square$

(02) Qualquer que seja o inteiro n, segue que n e $n+6$ têm a mesma paridade.

De fato, sejam q e r, respectivamente o quociente e o resto da divisão de n por 2. Então

$$n = 2q + r,$$

com $0 \leq r < 2$. Somando 6 a esta identidade obtemos:

$$n + 6 = 2q + r + 6 = 2(q + 3) + r.$$

Assim, ambos deixam o mesmo resto na divisão por 2, tendo portanto, a mesma paridade.

(03) Para todo $n \in \mathbb{Z}$, os inteiros n e $n + 5$ têm paridades distintas. $\square$

Considere q e r, respectivamente o quociente e o resto da divisão de n por 2. Então

$$n = 2q + r,$$

com $0 \leq r < 2$. Somando 5 a essa identidade obtemos:

$$n + 5 = 2q + r + 5 = \begin{cases} 2(q + 2) + 1, & \text{se} \quad r = 0 \\ 2(q + 3) + 0, & \text{se} \quad r = 1 \end{cases}$$

Portanto, n e $n + 5$ têm restos diferentes na divisão por 2, logo suas paridades são distintas. $\square$

Lista de Exercícios 3.

(01) Responda e justifique:
(a) $14|168$?
(b) $-12|60$?
(c) $-9|28$?
(d) $7|-35$?
(e) $-11|-143$?

(02) Sejam a e b inteiros não nulos. Mostre que se $a|b$, então
(a) $-a|b$;
(b) $-a|-b$.

(03) Sejam a, b inteiros. Mostre que:
(a) Se $a|3$ e $3|b$, então $a|b$;
(b) Se $a|-15$ e $-15|b$, então $a|b$;
(c) Para qualquer inteiro c, se $a|c$ e $c|b$, então $a|b$ (dizemos que a divisibilidade é transitiva).

(04) Seja a um inteiro. Mostre que:
(a) Se $a|2$ e $a|3$, então $a|6$;
(b) Se $a|-7$ e $a|9$, então $a|-63$;
(c) Para quaisquer inteiros b e c, se $a|b$ e $a|c$, então $a|bc$.

(05) Sejam a e b inteiros. Mostre que:
(a) Se $a|5$ e $b|13$, então $ab|65$;
(b) Se $a|-11$ e $b|4$, então $ab|-44$;
(c) Se m e n são inteiros quaisquer e $a|m$ e $b|n$, então $ab|mn$.

(06) Sejam a e b inteiros. Mostre que:
(a) Se $a|b$, então $a^2|b^2$;
(b) Se $a|b$, então $a^3|b^3$;
(c) Se $a|b$, então $a^n|b^n$, para todo inteiro $n \geq 2$.(*Sugestão*: use indução em n).

(07) Faça o que se pede:
(a) Dê exemplo de dois inteiros distintos a e b, tais que $a|b$ e $b|a$;
(b) Mostre que se a e b são inteiros não nulos e $a|b$ e $b|a$, então $a = b$ ou $a = -b$;

(08) Sejam a e b inteiros quaisquer. Mostre que:
(a) Se $a|5$ e $a|7$, então $a|2$;
(b) Se $a|5$ e $a|7$, então $a|6$;
(c) Se $a|5$ e $a|7$, então $a|(5m + 7n)$, para quaisquer $m, n \in \mathbb{Z}$.

(09) Considere a, b e c inteiros. Verifique se as afirmações abaixo são verdadeiras ou falsas. Sendo verdadeira, demonstre-a. Se for falsa, dê um contraexemplo.
(a) $a|(b + c)$, então $a|b$ ou $a|c$;
(b) Se $a|bc$, então $a|b$ ou $a|c$.

(10) Determine o quociente **q** e o resto **r** da divisão euclidiana de **a** por **b**, onde
(a) $a = 144$ e $b = 7$;
(b) $a = -144$ e $b = 7$;
(c) $a = 144$ e $b = -7$;
(d) $a = -144$ e $b = -7$;
(e) $a = 139$ e $b = 14$;
(f) $a = -139$ e $b = 14$;
(g) $a = 139$ e $b = -14$;
(h) $a = -139$ e $b = -14$.

(11) Na divisão de 477 por um inteiro positivo b o resto é 12. Determine os possíveis valores para o divisor b e o quociente q.

(12) Na divisão de 632 por um inteiro positivo b, o quociente é 15. Determine os possíveis valores do divisor b e do resto r correspondente.

(13) Na divisão de a por b o quociente é 7 e o resto, o maior possível. Sabendo que a e b são inteiros positivos cuja soma é 116, determine o valor de a e b.

(14) Na divisão de a por b, o resto é o maior possível. Sabendo que a e b são inteiros positivos cuja soma é 181, determine os possíveis valores para a e b.

(15) Sabendo que na divisão do inteiro a por 12 o resto é 7, calcule o resto da divisão de cada um dos inteiros abaixo por 12:
(a) $3a$;
(b) $5a + 7$;
(c) $4a - 4$

(16) Mostre que o produto de dois inteiros consecutivos é sempre um número par.

(17) Mostre que para quaisquer inteiros a e b, $(a^2 - b^2) + (a - b)$ é sempre um número par. (*Sugestão: Use a questão anterior.*)

(18) Mostre que se a e b são dois inteiros ímpares, então $a^2 - b^2$ é divisível por 8. (*Sugestão: Use a questão anterior.*)

(19) Mostre que o quadrado de um inteiro qualquer é da forma $3k$ ou $3k + 1$, para algum inteiro k. (*Sugestão: Divida o inteiro por 3.*)

(20) De exemplo, caso exista, de um inteiro a, tal que a^2;
(a) termina em 5;
(b) termina em 9;
(c) termina em 2;

(d) termina em 7.

(21) Mostre que se a é um inteiro, então a^2 termina em um dos algarismos 0, 1, 4, 5, 6 ou 9.

(22) Mostre que dado três inteiros consecutivos, um deles é divsível por 3.

(23) Mostre que o produto de 3 inteiros consecutivos é sempre divisível por 6.

(24) Seja a um inteiro qualquer. Mostre que exatamente um dos inteiros a, $a + 2$ ou $a + 4$ é divisível por 3.

(25) Mostre que todo número ímpar é da forma $4k + 1$ ou $4k + 3$, para algum inteiro k.

(26) Mostre que para qualquer inteiro não nulo n, $6|n(n + 1)(2n + 1)$.

(27) Mostre que se a é um número ímpar, então $a(a^2 - 1)$ é divisivel por 24.
(*Sugestão: Use a questão anterior.*)

(28) Sejam a e b inteiros quaisquer. Mostre que $a + b$ e $a - b$ tem a mesma paridade.

(29) Sendo a e b inteiros quaisquer, mostre que os inteiros a e $5a + 6b$ tem sempre a mesma paridade.

(30) Mostre que para qualquer inteiro a, os números a e $(5a+1)$ tem paridades distintas.

Respostas da Lista de Exercícios 3

(01.b) Sim, pois $60 = (-12)(-5)$ (01.c) Não, pois não existe $c \in \mathbb{Z}$, tal que $28 = (-9).c$
(02) $a|b \Rightarrow \exists c \in \mathbb{Z}$, tal que $b = ac \Rightarrow b = (-a)(-c) \Rightarrow -a|b$ e também $-b = (-a)c \Rightarrow -a|-b$.
(03.c) $a|c$ e $c|b \Rightarrow \exists x, y \in \mathbb{Z}$, $c = ax$ e $b = cy \Rightarrow b = (ax)y = a(xy) \Rightarrow a|b$, pois $xy \in \mathbb{Z}$.
(04.c) $a|b$ e $a|c \Rightarrow \exists x, y \in \mathbb{Z}$, $b = ax$ e $c = ay \Rightarrow bc = (ax)(ay) = a(axy) \Rightarrow a|bc$, pois $axy \in \mathbb{Z}$.
(07.c) $a|b$ e $b|a \Rightarrow \exists x, y \in \mathbb{Z}$, $b = ax$ e $a = by \Rightarrow ab = (ab)(xy) \Rightarrow ab(1 - xy) = 0$, como a e b são não nulos e $\mathbb{Z}$ é sem divisores de zero, segue que $1 - xy = 0 \Rightarrow xy = 1 \Rightarrow x = y = 1 \Rightarrow a = b$ ou $x = y = -1 \Rightarrow a = -b$.
(10.a) $144 = 7.20 + 4 \Rightarrow q = 20$ e $r = 4$ (10.b) $-144 = 7.(-21) + 3 \Rightarrow q = -21$ e $r = 3$
(10.c) $144 = (-7).(-20) + 4 \Rightarrow q = -20$ e $r = 4$ (10.d) $-144 = (-7).21 + 3 \Rightarrow q = 21$ e $r = 3$;
(10.e) $139 = 14.9 + 13 \Rightarrow q = 9$ e $r = 13$ (10.f) $-139 = 14.(-10) + 1 \Rightarrow q = -10$ e $r = 1$
(10.g) $139 = (-14).(-9) + 13 \Rightarrow q = -9$ e $r = 13$ (10.h) $-139 = (-14).10 + 1 \Rightarrow q = 10, r = 1$.
(11) Procuramos inteiros b e q, tais que $477 = b.q + 12$, com $12 < b$. Então $b.q = 465 \Rightarrow b|465 \Rightarrow b \in \{15, 31, 93, 155, 465\}$. Logo os possíveis valores para o par (b, q) são:
$(15, 31), (31, 15), (93, 5), (155, 3), (465, 1)$.
(12) Procuramos inteiros b e r tais que $632 = b.15 + r$, com $0 \leq r < b$. Dividindo 632 por 15 encontramos: $632 = 42.15 + 2$. Atribuindo a b os valores inteiros mais próximos a 42, isto é, $b \in \{..., 39, 40, 41, 42, 43, 44, ..\}$ verifica-se que:
$632 = 39.15 + 47 \Rightarrow r = 47 > b = 39$ (não é a divisão euclidiana)
$632 = 40.15 + 32 \Rightarrow r = 32 < b = 40$ (divisão euclidiana)
$632 = 41.15 + 17 \Rightarrow r = 17 < b = 41$ (divisão euclidiana)
$632 = 42.15 + 2 \Rightarrow r = 2 < b = 42$ (divisão euclidiana)
$632 = 43.15 + (-13) \Rightarrow r = -17 < 0$ (não é divisão euclidiana)
Assim, os únicos valores para o par (b, q) são $(40, 32), (41, 17), (42, 2)$.
(13) O maior resto que se obtém na divisão por b é $(b-1)$, então $a = 7b+(b-1)$ e $a+b = 116$. Dessas duas equações obtemos $a = 103$ e $b = 13$.
(14) $a = bq + (b - 1)$ e $a + b = 181 \Rightarrow b(q + 1) = 182 \Rightarrow b|182 \Rightarrow b \in \{1, 2, 7, 14, 26, 91, 182\}$. Como a e b são positivos e $a + b = 181$ os possíveis valores para o par (a, b) são:
$(180, 1), (179, 2), (174, 7), (167, 14), (155, 26), (90, 91)$.
(15) Como $a = 12q + 7$, então
(a) $3a = 12(3q) + 21 = 12(3q + 1) + 9 \Rightarrow r = 9$;
(b) $5a + 7 = 12(5q) + 35 + 7 = 12(5q + 3) + 6 \Rightarrow r = 6$;
(c) $4a - 4 = 12(4q) + 28 - 4 = 12(4q - 2) + 0 \Rightarrow r = 0$.
(17) Pela questão (16), para qualquer inteiro a, $a(a+1)$ é um número par. Então $(a^2 - b^2) + (a - b) = (a^2 + a) - (b^2 + b) = a(a + 1) - b(b + 1) = 2n_1 - 2n_2 = 2(n_1 - n_2)$, com $n_1, n_2 \in \mathbb{Z}$.
(21) O último algarismo de qualquer inteiro a é exatamente o resto da divisão de a por 10. Sejam q e r, respectivamente, o quociente e resto da divisão de a por 10, então $a = 10q + r$, com $0 \leq r < 10$. Portanto,

$$a^2 = 100q^2 + 20qr + r^2 = 10(10q^2 + 2qr) + \begin{cases} 0 & \text{se} \quad r = 0 \\ 1 & \text{se} \quad r = 1 \,\text{ou}\, 9 \\ 4 & \text{se} \quad r = 2 \,\text{ou}\, 8 \\ 5 & \text{se} \quad r = 5 \\ 6 & \text{se} \quad r = 4 \,\text{ou}\, 6 \\ 9 & \text{se} \quad r = 3 \,\text{ou}\, 7 \end{cases}$$

(23) Mostraremos que $6|a(a+1)(a+2)$, qualquer que seja o inteiro a. Pelo algoritmo da divisão temos que $a = 3q + r$, com $r = 0, 1$ ou 2. Se $a = 3q$, então $a(a+1)(a+2) = 3q(3q+1)(3q+2) = 3q.2m = 6(qm)$, pois $(3q+1)(3q+2) = 2m$, $m \in \mathbb{Z}$, conforme questão (16). Se $a = 3q+1$, então $a(a+1)(a+2) = (3q+1)(3q+2)(3q+3) = 2m.3(q+1) = 6(m(q+1))$. Se $a = 3q+2$, neste caso, sendo a par, então $a = 3q+2 = 2m$, $m \in \mathbb{Z}$, daí, $a(a+1)(a+2) = 2m(3q+3)(3q+4) = 6(m(q+1)(3q+4)$, que é um múltiplo de 6. Se a é impar, então necessariamente q é também ìmpar, isto é, $q = 2k+1$ (verifique). Assim, $a+1 = (3q+2)+1 = 3(q+1) = 3(2k+2) = 6(k+1)$, assim, $a(a+1)(a+2)$ é um múltiplo de 6, pois $(a+1)$ o é.

(29) Sejam $a = 2q_1 + r_1$ e $b = 2q_2 + r_2$ dois inteiros quaisquer, com $0 \leq r_1, r_2 < 2$. Então $5a + 6b = 5(2q_1 + r_1) + 6(2q_2 + r_2) = 2(5q_1 + 2r_1 + 6q_2 + 3r_2) + r_1$. Portanto a e $5a + 6b$ tem o mesmo resto na divisão por 2, logo a mesma paridade.

Capítulo 4

Sistema de Numeração

1 Introdução

Tomemos dois inteiros positivos, $a = 1924$ e $b = 10$. Pelo algoritmo da divisão, podemos dividir a por b, encontrando um quociente q e um resto r, com $0 \leq r < b$. Nesse caso,

$$1924 = 192.10 + \underbrace{4}_{resto}.$$

Aplicando agora o algoritmo da divisão aos inteiros 192 e 10, obtemos:

$$192 = 19.10 + \underbrace{2}_{resto}.$$

Substituindo essa identidade na primeira:

$$1924 = 192.10 + 4 = (19.10 + 2).10 + 4 = 19.10^2 + 2.10 + 4.$$

Repetindo o processo, dessa vez para o quociente 19:

$$19 = 1.10 + \underbrace{9}_{resto}.$$

Daí,

$$1924 = (1.10 + 9).10^2 + 2.10 + 4 = 1.10^3 + 9.10^2 + 2.10 + 4.$$

Por fim, divindo 1 por 10, teremos o quociente nulo:

$$1 = 0.10 + \underbrace{1}_{resto}.$$

$$1924 = (0.10 + 1).10^3 + 9.10^2 + 2.10 + 4 = 1.10^3 + 9.10^2 + 2.10 + 4.$$

Obtemos assim a identidade:

$$1924 = \mathbf{1}.10^3 + \mathbf{9}.10^2 + \mathbf{2}.10 + \mathbf{4}.10^0.$$

Ou seja, expressamos 1924 como uma soma de múltiplos de potências de 10, sendo os coeficientes das potências exatamente os restos obtidos nas divisões acima, os quais, nesse caso, coincidem com os dígitos que aparecem na representação do número.

Nesse exemplo, como dividimos por 10, qualquer que fosse o valor atribuído a a, em sua representação só poderiam constar os 10 restos possíveis: $0, 1, 2, ..., 8, 9$.

Vamos repetir o mesmo processo, tomando $b = 7$, em vez de 10.

$$1924 = 274.7 + \underbrace{6}_{resto}.$$

Dividindo agora o quociente 274 por 7:

$$274 = 39.7 + \underbrace{1}_{resto}.$$

Substituindo esse valor na primeira identidade:

$$1924 = (39.7 + 1).7 + 6 = 39.7^2 + 1.7 + 6.$$

Repetimos o processo, até que o quociente seja nulo:

$$39 = 5.7 + \underbrace{4}_{resto}.$$

Daí,

$$1924 = (5.7 + 4).7^2 + 1.7 + 6 = 5.7^3 + 4.7^2 + 1.7 + 6.$$

Por fim, dividindo 5 por 7:

$$5 = 0.7 + \underbrace{5}_{resto}.$$

$$\Downarrow$$

$$1924 = (0.7 + 5).7^3 + 4.7^2 + 1.7 + 6 = 5.7^3 + 4.7^2 + 1.7 + 6.$$

Portanto,

$$1924 = \mathbf{5}.7^3 + \mathbf{4}.7^2 + \mathbf{1}.7 + \mathbf{6}.7^0.$$

Dessa forma, também expressamos 1924 como uma soma de múltiplos de potências de 7. E com antes, os coeficientes das potências são exatamente os restos obtidos nas sucessivas divisões.

Tal como fizemos para $b = 10$, podemos representar esse número, usando somente os restos obtidos nas divisões, desde que fique indicado o inteiro b usado como divisor. Nesse caso, escreve-se:

$$(5416)_7,$$

e dizemos que essa é a expansão de 1924 na base 7.

No segundo exemplo, como tomamos para o divisor $b = 7$, os restos possíveis são: 0, 1, 2, 3, 4, 5, 6. Assim, somente esses sete dígitos aparecerão na representação do inteiro a, qualquer que seja o valor atribuído a ele.

Podemos repetir esse processo, quaisquer que sejam os inteiros positivos a e b. Isso é o que afirma o próximo teorema, o qual é uma aplicação da divisão euclidiana e a base para os sistemas de numeração posicional.

2 Representação de um inteiro em bases arbitrárias

Teorema 3. *Seja $b \geq 2$ um inteiro. Para todo inteiro $a \geq 1$, existem únicos inteiros $r_0, r_1, ..., r_n$, $n \geq 0$, tais que:*

$$a = r_n b^n + r_{n-1} b^{n-1} + ... + a_1 b + r_0.$$

com $0 \leq r_i < b$, para todo i e $r_n \neq 0$.

Demonstração:
Faremos a demonstração por indução em a.
(i) Base de Indução: $a = 1$:
Como $b \geq 2 > a$, dividindo a por b, obtemos:

$$a = 0.b + a.$$

Assim, tomando $n = 0$ e $r_0 = a < b$, segue a existência dos r_i. Para a unicidade, suponhamos que também existam inteiros $0 \leq s_0, s_1, ..., s_{m-1}, s_m < b$, para algum $m \geq 0$, com $s_m \neq 0$, tais que:

$$a = s_m b^m + s_{m-1} b^{m-1} + ... + s_1 b + s_0.$$

Se $m \geq 1$, então

$$(s_m b^{m-1} + s_{m-1} b^{m-2} + ... + s_1) b + s_0 = 0.b + a.$$

Da unicidade do quociente e resto na divisão euclidiana, segue que $s_0 = a$ e $s_m b^{m-1} + s_{m-1} b^{m-2} + ... + s_1 = 0 \Rightarrow s_m = s_{m-1} = ... = s_1 = 0$, um absurdo, pois $s_m \neq 0$. Assim, $m = 0$ e $s_0 = a$, provando a unicidade.

(ii) Passo Indutivo:
Usaremos a 2^a Forma do Princípio da Indução Finita (Corolário 2). Para isso, suponhamos o resultado válido para todo inteiro q, com $1 \leq q < a$. Pelo algoritmo da divisão, existem únicos inteiros q_0 e r_0, com $0 \leq r_0 < b$, tais que:

$$a = b q_0 + r_0. \tag{4.1}$$

Se $q_0 = 0$, então $r_0 = a \neq 0$. Se $q_0 \geq 1$, como $b \geq 2$, então $1 \leq q_0 < a$. Logo, pela hipótese de indução, existem únicos inteiros $r'_0, r'_1, ..., r'_m$, tais que:

$$q_0 = r'_m b^m + r'_{m-1} b^{m-1} + ... + r'_1 b + r'_0$$

com $0 \leq r'_0, r'_1, ..., r'_m < b$ e $r'_m \neq 0$. Substituindo o valor de q_0 em (4.1) obtemos:

$$a = b(r'_m b^m + r'_{m-1} b^{m-1} + ... + r'_1 b + r'_0) + r_0 = r'_m b^{m+1} + r'_{m-1} b^m + ... + r'_1 b^2 + r'_0 b + r_0.$$

Fazendo $n = m + 1$, $r_j = r'_{j-1}$, para $j = 1, 2, ..., m$, obtemos o resultado desejado. A unicidade dos r_i, segue da unicidade de r_0 e dos r'_j. $\square$

A representação do inteiro a como no teorema, isto é,

$$a = r_n b^n + r_{n-1} b^{n-1} + ... + r_1 b + r_0, \tag{4.2}$$

é chamada a **expansão de a na base b**, e utiliza-se a notação

$$(r_n r_{n-1} ... r_1 r_0)_b \tag{4.3}$$

Se $b = 10$ a expressão (4.2) é é chamada expansão decimal, e se $b = 2$, é dita expansão binária.

para representar esta expansão. Assim, temos:

$$\boxed{a = (r_n r_{n-1} ... r_1 r_0)_b \Leftrightarrow a = r_n b^n + r_{n-1} b^{n-1} + ... + r_1 b + r_0}$$

No caso da base 10, que é a usual, omitem-se os parênteses e a indicação da base em (4.3).

Exemplos:
(01) Como

$$3427 = 2.6^4 + 3.6^3 + 5.6^2 + 1.6^1 + 1.6^0,$$

escrevemos

$$(23511)_6$$

para representar a expansão do número 3427 na base 6.

(02) Como

$$3427 = 6.8^3 + 5.8^2 + 4.8 + 3.8^0,$$

então,

$$(6543)_8$$

representa a expansão de 3427 na base 8.

(03) Sendo

$$3427 = 1.5^5 + 0.5^4 + 2.5^3 + 0.5 + 2.5^0,$$

então,

$$(102202)_5$$

representa a expansão, em base 5, de 3427.

(04) Como
$$3427 = 3.10^3 + 4.10^2 + 2.10 + 7,$$
a notação
$$(3427)_{10}$$
é a representação da expansão de 3427 na base 10. Nesse caso, escrevemos apenas 3427, como é usual, omitindo-se os parênteses e a base.

(05) A notação
$$(11000110)_2$$
indica a expansão em base 2 (ou expansão binária) de um certo inteiro N. Para determinar N, basta lembrar o significado desta notação. Assim,
$$N = 1.2^7 + 1.2^6 + 0.2^5 + 0.2^4 + 0.2^3 + 1.2^2 + 1.2 + 0.2^0 = 198.$$
Portanto, essa expressão representa a expansão binária do número 198.

(06) A notação $(324)_5$ indica a expansão de um certo inteiro N em base 5. Como
$$N = (324)_5 \Rightarrow N = 3.5^2 + 2.5 + 4.5^0 = 89.$$
$(324)_5$ representa a expansão em base 5 de 89.

(07) $(1a7b6)_{12}$ é a representação de um certo inteiro N em base 12, onde estamos usando os símbolos a e b para representar, respectivamente, os números 10 e 11. Então,
$$N = (1a7b6)_{12} \Rightarrow N = 1.12^4 + \underbrace{a}_{=10}.12^3 + 7.12^2 + \underbrace{b}_{=11}.12^1 + 6.12^0 = 39162.$$
Portanto, $N = 39162$.

✓ **Exercícios 4.**

(01) Determine o número N (em base 10) que na base dada, tem a expansão abaixo:
(a) $(2345)_7$
Solução:
$(2345)_7 = 2.7^3 + 3.7^2 + 4.7 + 5.7^0 = 686 + 147 + 28 + 5 = 866.$ □
(b) $(2012001)_3$
Solução:
$(2012001)_3 = 2.3^6 + 0.3^5 + 1.3^4 + 2.3^3 + 0.3^2 + 0.3^1 + 1.3^0 = 1594.$ □
(c) $(100001)_2$
Solução:
$(100000)_2 = 1.2^5 + 0.2^4 + 0.2^3 + 0.2^2 + 0.2^1 + 1.2^0 = 32.$ □

(02) Escreva a expansão do inteiro a na base b, sendo:

(a) $a = 2945$ e $b = 6$;
Solução:
Inicialmente, dividimos a pela base b:

$$2945 = 490.6 + 5.$$

A seguir, dividimos o quociente obtido nesssa divisão, novamente pela base b e substituímos o resultado no valor do quociente acima (como no teorema):
Como

$$490 = 81.6 + 4,$$

então

$$2945 = 490.6 + 5 = (81.6 + 4).6 + 5 = 81.6^2 + 4.6 + 5.6^0.$$

Repetimos esse processo, sempre dividindo o quociente pela base, até obter um quociente $q_n = 0$:

$$\begin{aligned} 2945 &= 81.6^2 + 4.6 + 5.6^0 = (13.6 + 3).6^2 + 4.6 + 4.6^0 = 13.6^3 + 3.6^2 + 4.6 + 5.6^0 \\ &= (2.6 + 1).6^3 + 3.6^2 + 4.6 + 5.6^0 = 2.6^4 + 1.6^3 + 3.6^2 + 4.6 + 4.6^0 \\ &= (0.6 + 2).6^4 + 1.6^3 + 3.6^2 + 4.6 + 5.6^0 = 2.6^4 + 1.6^3 + 3.6^2 + 4.6 + 4.6^0 \end{aligned}$$

Assim, $(21345)_6$ é a expansão de 2945 em base 6. $\square$

(b) $a = 2945$ e $b = 5$;
Solução:
Vamos efetuar as sucessivas divisões, até obter um quociente nulo, e depois tomar os restos $r_0, r_1, ..., r_n$ obtidos, conforme feito na introdução:

$$2945 = 589.5 + \underbrace{0}_{r_0}.$$

$$589 = 117.5 + \underbrace{4}_{r_1}.$$

$$117 = 23.5 + \underbrace{2}_{r_2}.$$

$$23 = 4.5 + \underbrace{3}_{r_3}.$$

$$4 = 0.5 + \underbrace{4}_{r_4}.$$

Assim, $2945 = (r_4r_3r_2r_1r_0)_5 = (43240)_5$.

(c) $a = 2945$ e $b = 2$;

Solução:
Efetuando as sucessivas divisões:

$$2945 = 1472.2 + \underbrace{1}_{r_0}.$$

$$1472 = 736.2 + \underbrace{0}_{r_1}.$$

$$736 = 368.2 + \underbrace{0}_{r_2}.$$

$$368 = 184.2 + \underbrace{0}_{r_3}.$$

$$184 = 92.2 + \underbrace{0}_{r_4}.$$

$$92 = 46.2 + \underbrace{0}_{r_5}.$$

$$46 = 23.2 + \underbrace{0}_{r_6}.$$

$$23 = 11.2 + \underbrace{1}_{r_7}.$$

$$11 = 5.2 + \underbrace{1}_{r_8}.$$

$$5 = 2.2 + \underbrace{1}_{r_9}.$$

$$2 = 1.2 + \underbrace{0}_{r_{10}}.$$

$$1 = 0.2 + \underbrace{1}_{r_{11}}.$$

e tomando os restos, temos $2945 = (101110000001)_2$. □

(d) $a = 563$ e $b = 12$, convencionando $10 = a$ e $b = 11$.
Solução:
$563 = 46.12 + 11 = (3.12 + 10).12 + 11.12^0 = 3.12^2 + 10.12 + 11.12^0 = (3ab)_{12}$
□

(03) Escreva $(7645)_8$ no sistema de base 12.
Solução:
Inicialmente vamos converter para a base 10 e posteriormente para a base 12.
$(7645)_8 = 7.8^3 + 6.8^2 + 4.8^1 + 5.8^0 = 4005$
Agora,

$$\begin{aligned}4005 &= 333.12 + 9 = (27.12 + 9).12 + 9.12^0 = 27.12^2 + 9.12 + 9.12^0\\ &= (2.12 + 3).12^2 + 9.12 + 9.12^0\\ &= 2.12^3 + 3.12^2 + 9.12 + 9.12^0\end{aligned}$$

Portanto $(7645)_8 = (2399)_{12}$. □

(04) Determine a base b de um sistema na qual $(2006)_8$ se escreve como $(613)_b$.
Solução:

$$(613)_b = (2006)_8.$$
$$\Downarrow$$
$$6.b^2 + 1.b + 3.b^0 = 2.8^3 + 0.8^2 + 0.8 + 6.8^0$$
$$\Downarrow$$
$$6b^2 + b - 1027 = 0 \Rightarrow b = 13.$$

$\square$

(05) Efetue as somas:
(a) $(1012)_3 + (212)_3$.
Solução 1:
Podemos determinar a expansão dos inteiros em base 10, efetuar a soma nessa base e posteriormente converter o resultado para a base 3:
$(1012)_3 = 1.3^3 + 0.3^2 + 1.3^1 + 2.3^0 = 32$ e $(212)_3 = 2.3^2 + 1.3 + 2 = 23$.
Assim, $(1012)_3 + (212)_3 = 32 + 23 = 55 = 2.3^3 + 0.3^2 + 0.3 + 1 = (2001)_3$.

Solução 2:
Podemos efetuar a soma diretamente em base 3. Neste caso, lembrar que o resultado da soma dos elementos de cada coluna deve ser convertida para base 3 e, como feito na base 10, coloca-se no resultado apenas o coeficiente r_0, sendo os demais coeficientes adicionados às colunas seguinte.

$$\begin{array}{c} 1012 \\ \underline{0212} \\ 2001 \end{array}$$

(b) $(2134)_5 + (1143)_5$
Solução:
Somando diretamente em base 5 temos:

$$\begin{array}{c} 2134 \\ \underline{1143} \\ 3332 \end{array}$$

Assim, $(2134)_5 + (1143)_5 = (3332)_5$. $\square$

Lista de Exercícios 4.
(01) Determine o número N (em base 10) que na base dada, tem a expansão abaixo:
(a) $(110011)_2$;
(b) $(2013)_5$;
(c) $(20163)_8$;
(d) $(264102)_7$;
(e) $(22010011)_3$.

(02) Escreva a expansão de 34561 em base:
(a) 12;
(b) 8;
(c) 5;
(d) 2.

(03) Escreva a expansão em base 8 de $(110111)_2$.

(04) Escreva a expansão em base 5 de $(231330)_4$.

(05) Escreva a expansão em base 3 de $(237014)_8$.

(06) Determine a base b de um sistema na qual $(234)_6$ se escreve como $(28)_b$.

(07) Sabendo que $(10001101)_2 = (215)_b$, determine b.

(08) Efetue as somas, apresentando o resultado na base dada:
(a) $(110101)_2 + (11111)_2$
(b) $(220121)_3 + (2201)_3$
(c) $(64587)_9 + (22453)_9 + (460113)_9$
(d) $(a987a)_{12} + (56a3b)_{12}$, sendo $a = 10$ e $b = 11$.

(09) Seja $N = r_n 10^n + r_{n-1} 10^{n-1} + \dots r_1 10 + r_0$, com $0 \leq r_i \leq 9$, para $i = 1, 2, ..n$. Mostre que:
(a) $2|N \Leftrightarrow 2|r_0$;
(b) $3|N \Leftrightarrow 3|(r_0 + r_1 + ... + r_n)$;
(c) $5|N \Leftrightarrow 5|r_0$;
(d) $11|N \Leftrightarrow 11|(r_0 - r_1 + r_2 - ... + (-1)^n r_n)$;

Respostas da Lista de Exercícios 4
(01.a) $N = 51$ (01.b) $N = 258$ (01.c) $N = 8307$ (01.d) $N = 49443$ (01.e) $N = 5917$
(02.a) $(18001)_{12}$ (02.b) $(103401)_8$ (02.c) $(2101221)_5$ (02.d) $(1000011100000001)_2$
(03) $(67)_8$
(04) $(43230)_5$
(05) $(11010200120)_3$
(06) $b = 43$
(07) $b = 8$
(08.a) $(1010100)_2$ (08.b) $(1000022)_3$ (08.c) $(557264)_9$ (08.d) $(1446b9)_{12}$.
(09.b) Sugestão: Mostre e use que $\forall n \geq 1$, $10^n = 9k + 1$, $k \in \mathbb{Z}$;
(09.c) Sugestão: Mostre e use que $\forall n \geq 1$, $10^n = 11k + (-1)^n$, $k \in \mathbb{Z}$.

Capítulo 5

Máximo Divisor Comum

1 Introdução

As duas oitavas séries de uma escola vão participar de uma gincana. Para realizar as tarefas, a comissão organizadora decidiu dividir as duas turmas em equipes, de modo que todas as equipes tenham o mesmo número de alunos e em cada uma delas, os alunos sejam todos da mesma turma. Sabendo que a $8^a A$ tem 40 alunos e a $8^a B$ 50, determine o número de alunos que deverá ficar em cada equipe, de modo que este número seja o maior possível.

Solução:
Vamos denotar por d o número de alunos em cada equipe. Pela natureza do problema, obviamente d é um inteiro positivo. Os 40 alunos da $8^a A$ serão divididos em n_1 equipes com d alunos cada uma, ou seja,

$$40 = dn_1.$$

Portanto, d é um divisor positivo de 40, logo $d \in \{1, 2, 4, 5, 8, 10, 20, 40\}$. Analogamente, os 50 alunos da $8^a B$ serão divididos em n_2 equipes com d alunos cada uma, ou seja,

$$50 = dn_2.$$

Como d é também um divisor positivo de 50, então $d \in \{1, 2, 5, 10, 25, 50\}$.

Portanto, d é simultaneamente divisor de 40 e 50. Assim,

$$d \in \{1, 2, 4, 5, 8, 10, 20, 40\} \cap \{1, 2, 5, 10, 25, 50\} = \{1, 2, 5, 10\}.$$

Como queremos que o número d seja o maior possível, dentre os **divisores comuns**, devemos tomar o **maior** deles, no caso 10.

Conlcuímos assim que a comissão deverá dividir a $8^a A$ em 4 equipes e a $8^a B$ em 5 equipes, cada uma delas com 10 alunos. $\square$

2 MDC

O número $d = 10$, solução do problema anterior, é o maior dentre os divisores comuns dos inteiros 40 e 50, é o que chamados de máximo divisor comum, conforme definido abaixo.

Definição 2. *Sejam a e b dois inteiros não conjuntamente nulos ($a \neq 0$ e/ou $b \neq 0$). Diz-se que um inteiro positivo d é o **máximo divisor comum** de a e b, se d verifica as seguintes condições:*
(i) $d|a$ e $d|b$;
(ii) para todo $d' \in \mathbb{Z}$, se $d' \mid a$ e $d' \mid b$, então $d' \mid d$.

Usaremos a notação $mdc(a, b)$ para indicar o máximo divisor comum de a e b.

A condição (i) da Definição 2 diz que o $mdc(a, b)$ é um divisor comum de a e b e a condição (ii), que ele é o maior dos divisores comuns, pois se d' é qualquer outro divisor comum de a e b, então $d'|mdc(a, b)$ e portanto, $d' \leq |d'| \leq mdc(a, b)$.

Exemplos:
(01) $mdc(4, 6) = 2$.
De fato, 2 satisfaz as condições (i) e (ii) da definição acima, isto é,
(i) 2 é um divisor comum de 4 e 6, pois $2|4$ e $2|6$;
(ii) 2 é o maior dos divisores comuns de 4 e 6, pois se $d' \in \mathbb{Z}$ é tal que $d'|4$ e $d'|6$, então pela Proposição 1, $d'|(6 - 4)$, ou seja, $d'|2$. $\square$

(02) $mdc(3, -5) = 1$.
De fato, 1 é um divisor comum de 3 e -5 e se $d' \in \mathbb{Z}$ é tal que $d'|3$ e $d'|-5$, então pela Proposição 1, $d'|(3.2 + (-5))$. Portanto, 1 satisfaz as condições (i) e (ii) da Definição 2. $\square$

(03) $mdc(0, 3) = 3$.
Observe que $3|0$ e $3|3$ e se $d' \in \mathbb{Z}$ é um divisor comum de 0 e 3, então $d'|3$. $\square$

(04) $mdc(8, 20) = 4$.
4 é um divisor comum de 8 e 20, e se d' é também um dividor comum de 8 e 20, então $d'|(8m + 20n)$, quaisquer que sejam $m, n \in \mathbb{Z}$. Em particular, $d'|(8.(-2) + 20.1)$. Assim, 4 é um inteiro que está de acordo com o exigido na Definição 2. $\square$

✓ Exercícios 5.

(01) Use a Definição 2 para justificar as afirmações abaixo:
(a) $mdc(6, 9) = 3$;
(b) $mdc(42, 7) = 7$;
(c) $mdc(-8, 28) = 4$;
(d) $mdc(-11, -35) = 1$.

(02) Determine o mdc abaixo e mostre que o valor encontrado satisfaz as condições (i) e (ii) da Definição 2:
(a) $mdc(32, 18)$;
(b) $mdc(-12, 38)$;
(c) $mdc(0, 31)$;
(d) $mdc(1, 129)$;
(e) $mdc(14, 84)$.
(03) Dê exemplo de dois inteiros não nulos a e b, para os quais não existe $mdc(a, b)$.
(04) Encontre, caso exista, um inteiro positivo $d \neq 3$, tal que $d = mdc(6, 9)$.
(05) Encontre, caso exista, um inteiro positivo $d \neq 4$, tal que $d = mdc(-8, 28)$.

Segue claramente da Definição 2, que para qualquer par de inteiros $(a, b) \neq (0, 0)$, temos:

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

3 Cálculo do MDC

Que conclusões podemos tirar das questões 03, 04 e 05 do exercício anterior? O que você deve estar conjecturando é afirmado no Teorema 5, dado na próxima seção, o qual garante a existência e unicidade do máximo divisor comum de dois inteiros quaisquer a e b, não simultaneamente nulos. Antes porém, daremos um algoritmo, que usa a divisão euclidiana, para o cálcular o máximo divisor comum de dois inteiros. Vejamos primeiramente o caso em que um dos inteiros é nulo, cujo cálculo é imediato.

✓ **Exercícios 6.**
(01) Usando a Definição 2, determine:
(a) $mdc(0, 2)$
(b) $mdc(0, 5)$
(c) $mdc(0, -3)$
(d) $mdc(3927, 0)$

Proposição 3. *Para todo inteiro não nulo a, tem-se:*

$$mdc(a, 0) = |a|.$$

Demonstração:
Como, $0 = 0.|a|$ e $a = \pm 1.|a|$, segue que $|a|$ é um divisor comum de a e 0. Se $d' \in \mathbb{Z}$ é um divisor comum de a e 0, então $d'|a \Rightarrow d'||a|$. Portanto, $|a|$ está de acordo com a Definição 2. $\square$

Teorema 4. *Sejam a e b inteiros com $b \neq 0$, q e r respectivamente o quociente e o resto da divisão de a por b, isto é ,*

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

Então

$$mdc(a, b) = mdc(b, r).$$

Demonstração:
Suponha $d = mdc(a, b)$. Vamos mostrar que $d = mdc(b, r)$. De fato,
(i) Como $d = mdc(a, b) \Rightarrow d|a$ e $d|b$, então pela Proposição 1, $d|\underbrace{(a - bq)}_{=r} \Rightarrow d|r$.
Assim d é um divisor comum de b e r;
(ii) Seja d' um inteiro, tal que $d'|b$ e $d'|r \Rightarrow d'|\underbrace{(bq + r)}_{=a} \Rightarrow d'|a$. Como $d = mdc(a, b)$ e d' é divisor comum de a e b, segue da Definição 2, que $d'|d$. $\square$

Recapitulando, o Teorema 4 afirma que se

$$\underbrace{a}_{dividendo} = \underbrace{b}_{divisor} \cdot \underbrace{q}_{quociente} + \underbrace{r}_{resto}$$

então

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

ou seja, na divisão euclidiana

$$\boxed{\mathbf{mdc(dividendo, divisor) = mdc(divisor, resto)}}$$

Exemplos:
(01) Usando o Teorema 4 e a Proposição 3, vamos calcular:
(a) $mdc(398, 12)$:
Solução:
Dividindo 398 por 12 obtemos:

$$398 = 12.33 + 2.$$

Segue do teorema anterior que $mdc(398, 12) = mdc(12, 2)$. Dividindo 12 por 2:

$$12 = 2.6 + 0.$$

Então, novamente pelo Teorema 4, temos que $mdc(12, 2) = mdc(2, 0)$. Assim,

$$mdc(398, 12) = mdc(12, 2) = mdc(2, 0) = 2.$$

Na última identidade usamos a Proposição 3, pois um dos inteiros é nulo. $\square$

(b) $mdc(138, 24)$:
Solução:
Dividindo o número maior pelo menor obtemos:

$$138 = 24.5 + 18.$$

Então

$$mdc(138, 24) = mdc(24, 18).$$

Por sua vez,

$$24 = 18.1 + 6 \Rightarrow mdc(24, 18) = mdc(18, 6).$$

E como $18 = 6.3 + 0$, então

$$mdc(138, 24) = mdc(24, 18) = mdc(18, 6) = mdc(6, 0) = 6.$$

□

Algoritmo para o Cálculo do MDC

Formalizaremos agora um algoritmo para cálcular o máximo divisor comum de dois inteiros a e b não conjuntamente nulos. Como $mdc(a, b) = mdc(b, a) = mdc(|a|, |b|)$, assumiremos a e b positivos, com $a \geq b$. Temos dois casos:

Caso 1: $b = 0$
Como os inteiros não são simultaneamente nulos, necessariamente $a \neq 0$. Assim,

$$mdc(a, b) = mdc(a, 0) = |a|,$$

conforme Proposição 3.

Caso 2: $b \neq 0$
Neste caso, efetuando as sucessivas divisões:

$$\begin{array}{ll}
a = bq_0 + r_1, & 0 \leq r_1 < b; \\
b = r_1q_1 + r_2, & 0 \leq r_2 < r_1; \\
r_1 = r_2q_2 + r_3, & 0 \leq r_3 < r_2; \\
r_2 = r_3q_3 + r_4, & 0 \leq r_4 < r_3 \\
\vdots & \\
r_k = r_{k+1}q_{k+1} + r_{k+2}, & 0 \leq r_{k+2} < r_{k+1}; \\
\vdots &
\end{array}$$

obtemos a sequência decrescente de inteiros não negativos

$$b > r_1 > r_2 > r_3 > ... > r_k > ... \geq 0.$$

Como existe um número finito de inteiros no intervalo $[0, b)$, necessariamente vai existir um índice s, tal que o resto $r_{s+1} = 0$. Neste caso, as duas últimas divisões da sequência acima serão:

$$r_{s-2} = r_{s-1}q_{s-1} + r_s, \quad 0 \leq r_s < r_{s-1};$$
$$r_{s-1} = r_s q_s + 0$$

Pelo Teorema 3, temos que:

$$mdc(a, b) = mdc(b, r_1) = mdc(r_1, r_2) = ... = mdc(r_{s-1}, r_s) = mdc(r_s, 0) = r_s.$$

Resumindo:

ALGORITMO PARA O CÁLCULO DO MDC
SE $\mathbf{a}$ E $\mathbf{b}$ SÃO INTEIROS NÃO NULOS, PARA CALCULAR $\mathbf{mdc}(\mathbf{a}, \mathbf{b})$, COMEÇAMOS DIVIDINDO O MAIOR PELO MENOR DENTRE OS INTEIROS $\|\mathbf{a}\|$ E $\|\mathbf{b}\|$ E, SEGUE-SE EFETUANDO DIVISÕES SUCESSIVAS ATÉ OBTER UM RESTO NULO, ONDE A DIVISÃO SEGUINTE É SEMPRE FEITA DIVIDINDO O DIVISOR PELO RESTO DA DIVISÃO ANTERIOR. DAÍ, $\mathbf{mdc}(\mathbf{a}, \mathbf{b}) =$ AO ÚLTIMO RESTO NÃO NULO OBTIDO NAS SUCESSIVAS DIVISÕES.

✓ **Exercícios 7.**

(01) Use o algoritmo acima para calcular:
(a) $mdc(8, 76)$;
(b) $mdc(312, 42)$;
(c) $mdc(-23, 14)$;
(d) $mdc(-18, -52)$;
(e) $mdc(234, -415)$.

4 Existência e Unicidade do MDC

Teorema 5. *Para quaisquer inteiros a e b não conjuntamente nulos, sempre* ***existe*** *um* ***único*** *inteiro positivo d, tal que*

$$d = mdc(a, b).$$

Demonstração:
Pelo Teorema 4 e algoritmo acima, fica garantido que o resto $r_s = mdc(a, b)$, logo sempre existe. Resta mostrar a unicidade. Suponha que d_1 e d_2 sejam ambos $mdc(a, b)$. Pela condição (i) da Definição 2, ambos são divisores comuns de a e b. Mas pela condição (ii), isto implica que $d_1|d_2$, pois $d_2 = mdc(a, b)$ e d_1 é um divisor comum. Analogamente, $d_2|d_1$, pois $d_1 = mdc(a, b)$ e d_2 é um divisor comum. Como ambos são positivos, pela Proposição 2, segue que $d_1 \leq d_2$ e $d_2 \leq d_1$. Logo, $d_1 = d_2$. Assim, o máximo divisor de dois inteiros a e b, existe e é único. $\square$

✓ **Exercícios 8.**

(01) Use divisões sucessivas para calcular $mdc(a,b)$ e determine inteiros r e s, tais que:

$$mdc(a,b) = ra + sb.$$

(a) $a = 24$ e $b = 14$.
Solução:
Começamos dividindo o número maior pelo menor:

(1) $$\underbrace{24}_{dividento} = \underbrace{14}_{divisor} \cdot \underbrace{1}_{quociente} + \underbrace{10}_{resto}$$

Agora efetuamos divisões sucessivas até obter um resto nulo, onde a divisão seguinte é sempre feita dividindo o divisor da divisão anterior pelo resto.

(2) $14 = 10.1 + 4$
(3) $10 = 4.2 + 2$ $\leftarrow$ último resto não nulo.
(4) $4 = 2.2 + 0$ $\leftarrow$ resto nulo.

Pela Teorema 4,

$$mdc(24,14) = mdc(14,10) = mdc(10,4) = mdc(4,2) = mdc(2,0) = 2.$$

ou seja, $mdc(24,14)$ é o último resto não nulo obtido nas sucessivas divisões.

Para encontrar r e s, isolaremos todos os restos não nulos em cada uma das divisões obtidas acima, sem efetuar as multiplicações e as somas. Apenas deixaremos indicadas as operações:

(1) $10 = 24 + (-1).14$
(2) $4 = 14 + (-1).10$
(3) $2 = 10 + (-2).4.$

Tomamos agora a última dessas equações e vamos substituindo os valores dos restos encontrados nas anteriores, até que a identidade fique só em função dos inteiros 24 e 14:

$$\begin{aligned}
2 &= 10 + (-2).4 && \text{- Tomando a equação (3), onde o resto} = mdc(24,14)\\
&= 10 + (-2).(14 + (-1).10) && \text{- substituindo o valor do resto 4 dado na equação (2)}\\
&= (-2).14 + 3.10 && \text{- organizando a soma}\\
&= (-2).14 + 3.(24 + (-1).14) && \text{- substituindo o valor do resto 10 dado na equação (1)}\\
&= 3.24 + (-5).14 && \text{- organizando a soma.}
\end{aligned}$$

Portanto:

$$2 = 3.24 + (-5).14$$

□

assim $r = 3$ e $s = -5$.

(b) -124 e 52.
Solução:
Como $mdc(-124,52) = mdc(|-124|,|52|)$, calcularemos $mdc(124,52)$.

Dividindo o maior valor pelo menor:

(1) $124 = 52.2 + 20$

Agora efetuamos divisões sucessivas até obter um resto nulo:

(2) $52 = 20.2 + 12$

(3) $20 = 12.1 + 8$

(4) $12 = 8.1 + 4 \leftarrow$ último resto não nulo.

(5) $8 = 4.2 + 0 \leftarrow$ resto nulo.

Portanto,

$$mdc(124, 52) = mdc(52, 20) = mdc(20, 12) = mdc(12, 8) = mdc(8, 4) = mdc(4, 0) = 4.$$

Para encontrar r e s, isolaremos todos os restos não nulos em cada uma das divisões obtidas:

(1) $20 = 124 + (-2).52$

(2) $12 = 52 + (-2).20$

(3) $8 = 20 + (-1).12.$

(4) $4 = 12 + (-1).8.$

Tomandos agora a última destas equações e substituindo os valores dos restos encontrados nas anteriores:

$$\begin{aligned}
4 &= 12 + (-1).8 && \\
&= 12 + (-1).(20 + (-1).12) && \text{- substituindo valor do resto 8 dado na equação (3)}\\
&= (-1).20 + 2.12 && \text{- organizando a soma}\\
&= (-1).20 + 2.(52 + (-2).20) && \text{- substituindo o valor do resto 12 dado na equação (2)}\\
&= 2.52 + (-5).20 && \text{- organizando a soma}\\
&= 2.52 + (-5).(124 + (-2).52) && \text{- substituindo o valor do resto 20 dado na equação (1)}\\
&= (-5).124 + 12.52 && \text{- organizando a soma.}
\end{aligned}$$

Portanto:

$$4 = (-5).124 + 12.52.$$

Mas, como queremos de fato calcular $mdc(-124, 52)$, basta alternamos o sinal dos fatores na primeira parcela:

$$4 = 5.(-124) + 12.52.$$

Assim $r = 5$ e $s = 12$. □

Note que uma vez calculado o $mdc(a, b)$ usando o Algoritmo de Euclides, é sempre possível encontrar inteiros r e s, tais que $mdc(a, b) = ra + sb$. Esse resultado, conhecido como Teorema de Bézout, é enunciado abaixo:

Teorema 6. *(Teorema de Bézout) Sejam a e b inteiros não conjuntamente nulos, então existem inteiros r e s, tais que:*

$$mdc(a, b) = ra + sb.$$

No letra (a) do exercício anterior encontramos

$$2 = 3.24 + (-5).14$$

Mas, observe que também podemos escrever:

$$2 = 10.24 + (-17).14$$

ou

$$2 = (-4).24 + 7.14$$

$\square$

dentre outras soluções. Portanto, r e s mencionados no Teorema 6, não são únicos. O algoritmo dado acima é apenas um método de encontrar inteiros r e s, tais que $mdc(a, b) = ar + sb$.

O Teorema 6 afirma que se $d = mdc(a, b)$, então então existem $r, s \in \mathbb{Z}$, tais que

$$d = ra + sb. \tag{5.1}$$

Uma pergunta natural é: - Vale a recíproca desse teorema, isto é, se $d = ra + sb$, com r, $s \in \mathbb{Z}$, isso implica que $d = mdc(a, b)$?

Esse fato nem sempre é verdadeiro, por exemplo,

$$8 = (-7).\mathbf{6} + 5.\mathbf{10}$$

porém $mdc(6, 10) \neq 8$. No caso particular, em que a soma dada em (5.1) é igual a 1, fica garantida a recíproca do Teorema 6, conforme proposição abaixo.

Proposição 4. *Sejam a e b inteiros. Se existem inteiros r e s, tais que*

$$ra + sb = 1$$

então

$$mdc(a, b) = 1.$$

Demonstração:
Considere que existam inteiros r e s, tais que $ra + sb = 1$ e suponha $d = mdc(a, b)$. Vamos mostrar que $d = 1$. Como $d = mdc(a, b)$, então $d|a$ e $d|b$, logo $d|(ra + sb) \Rightarrow d|1 \Rightarrow d = \pm 1$. Mas, como $d > 0$, então $d = 1$. $\square$

Exemplos:
(01) Como $1 = 3.5 + (-2).7$, segue da Proposição 4 que $mdc(3, 7) = 1$;
(02) Da igualdade $1 = (-23).63 + 29.50$, pode concluir que $mdc(63, 50) = 1$;
(03) Da identidade $1 = (-1).n + 1.(n + 1)$, segue que $mdc(n, n + 1) = 1$, qualquer que seja $n \in \mathbb{Z}$.

5 Inteiros Relativamente Primos

Inteiros para os quais o máximo divisor comum é a unidade recebem denominação especial, conforme definição abaixo.

Definição 3. *Dois inteiros a e b dizem-se **relativamente primos** ou **primos entre si**, se $mdc(a, b) = 1$.*

Exemplos:
(01) 2 e 3 são relativamente primos, pois $mdc(2, 3) = 1$;
(02) 4 e 15 são primos entre si, pois $mdc(4, 15) = 1$;
(03) 4 e 10 não são relativamente primos, pois $mdc(4, 10) = 2$.

Proposição 5. *Se*
$$mdc(a, b) = d,$$
então
$$mdc(\frac{a}{d}, \frac{b}{d}) = 1.$$

Demonstração:
$d = mdc(a, b) \Rightarrow$ existem inteiros r e s, tais que:
$$d = ra + sb$$
$$\Downarrow$$
$$1 = r.\tfrac{a}{d} + s.\tfrac{b}{d}, \quad \text{com } \tfrac{a}{d}, \tfrac{b}{d} \in \mathbb{Z}$$
$$\Downarrow$$
$$mdc(\tfrac{a}{d}, \tfrac{b}{d}) = 1,$$
conforme Proposição 4. □

✓ Exercícios 9.

(01) Determine todos os inteiros positivos a e b, para os quais $2a + b = 160$ e $mdc(a, b) = 8$.
Solução:
Como $mdc(a, b) = 8 \Rightarrow a = 8k_1$ e $b = 8k_2$, com $k_1, k_2 \in \mathbb{Z}_+^*$. Então

$$2a + b = 160 \Rightarrow 2(8k_1) + 8k_2 = 160 \Rightarrow k_2 = 20 - 2k_1$$
$$\Downarrow$$
$$(k_1, k_2) \in \{(1, 18), (2, 16), (3, 14), (4, 12), (5, 10), (6, 8), (7, 6), (8, 4), (9, 2)\}.$$

Agora, como $8 = mdc(a, b) = mdc(8k1, 8k2) \Rightarrow mdc(k_1, k_2) = 1$, conforme Proposicão 5. Assim, as únicas soluções possíveis são:
$k_1 = 1, k_2 = 18 \Rightarrow a = 8$ e $b = 144$;
$k_1 = 3, k_2 = 14 \Rightarrow a = 24$ e $b = 112$;
$k_1 = 7, k_2 = 6 \Rightarrow a = 56$ e $b = 48$;
$k_1 = 9, k_2 = 2 \Rightarrow a = 72$ e $b = 16$. □

Na questão 09 da Lista de Exercício 3, você encontrou inteiros a, b e c, com $a|bc$, porém $a \nmid b$ e $a \nmid c$. Por exemplo, $4|(2.6)$, porém $4 \nmid 2$ e $4 \nmid 6$. Também temos, que $9|(3.15)$, porém $9 \nmid 3$ e $9 \nmid 15$. O teorema a seguir, atribuído a Euclides, dá a condição para que isso não ocorra.

Teorema 7. *(De Euclides) Sejam a, b e c inteiros, tais que $a|bc$. Se a e b são relativamente primos, então $a|c$.*

Demonstração:
Como, $mdc(a, b) = 1$, existem inteiros r e s, tais que $1 = ra + sb$. Por outro lado, como $a|bc$, existe $k \in \mathbb{Z}$, tal que $bc = ak$. Multiplicando a equação

$$1 = ra + sb$$

por c e usando o valor de bc acima:
$1 = ra + sb \Rightarrow c = a(rc) + (bc)s \Rightarrow c = a(rs) + a(ks) = a(rs + ks) \Rightarrow a|c.$ □

Exemplos:
(01) Se $3|(7.a)$, com $a \in \mathbb{Z}$, necessariamente $3|a$, pois $mdc(3, 7) = 1$;
(02) Para quaisquer inteiros $n \neq 0$ e a, se $n|(an + a)$, então $n|a$. (Justifique).

Lista de Exercícios 5.

(01) Usando a Definição 2, mostre que:
(a) $mdc(80, 30) = 10$;
(b) $mdc(0, -12) = 12$;
(c) $mdc(8, 32) = 8$;
(d) $mdc(-24, -148) = 4$.

(02) Para cada par de inteiros a e b, determine $mdc(a, b)$ e encontre inteiros r e s, tais que $mdc(a, b) = ra + sb$:
(a) $a = 8$, $b = 76$;
(b) $a = 312$, $b = 42$;
(c) $a = -23$, $b = 14$;
(d) $a = -18$, $b = -52$;
(e) $a = 234$, $b = -415$;
(f) $a = 392$ e $b = 490$.

(03) Para cada uma das equações abaixo, determine um par de inteiros (x, y) que seja solução da mesma:
(a) $11x + 9y = 1$;
(b) $11x + 9y = 60$;
(c) $54x + 21y = 3$;
(d) $54x + 21y = 15$;
(e) $56x + 72y = 8$;
(f) $56x + 72y = -40$.

(04) Determine todos os inteiros a, para os quais $mdc(a, 0) = 13$.

(05) Determine todos os inteiros positivos a e b, com $a \leq b$, para os quais $a + b = 96$ e $mdc(a, b) = 12$.

(06) Determine todos os inteiros positivos a e b, com $a \leq b$, para os quais $a.b = 294$ e $mdc(a, b) = 7$.

(07) Calcule:
(a) $mdc(mdc(6, 16), 12))$;
(b) $mdc(6, mdc(16, 12))$;
(c) $mdc(mdc(5, 12), 16)$;
(d) $mdc(5, mdc(12, 16))$.

(08) Sejam a, b e c inteiros não nulos. Mostre que $mdc(mdc(a, b), c) = mdc(a, mdc(b, c))$.

(09) A Definição 2 pode ser estendida para um quantidade finita $n \geq 2$ qualquer de inteiros, isto é, dados inteiros $a_1, a_2, ..., a_n$, não simultamente nulos, dizemos que o inteiro positivo d é o máximo divisor comum de $a_1, a_2, ..., a_n$ e escrevemos $d = mdc(a_1, a_2, .., a_n)$, se
(i) $d|a_1, d|a_2, ..., d|a_n$;
(ii) para todo $d' \in \mathbb{Z}$, se $d'|a_i$, para todo $i = 1, 2, .., n$, então $d'|d$.

Usando esta definição e a questão (08), calcule:
(a) $mdc(22, 16, 38)$
(b) $mdc(8, 15, 4, 23)$
(c) $mdc(180, -90, 84, -294, 60)$.

(10) Sejam a e b inteiros não nulos. Mostre que se $b|a$, então $mdc(a, b) = |b|$.

(11) Sejam a, b e c inteiros não nulos. Mostre que:
(a) Se $mdc(a, c) = mdc(b, c) = 1$, então $mdc(ab, c) = 1$;
(b) Se $mdc(a, b) = 1$, então $mdc(a + b, b) = 1$;
(c) Se $mdc(a, b) = 1$, então $mdc(a + b, ab) = 1$.

(12) Sejam a e b inteiros não nulos e $d = mdc(a, b)$. Mostre que para cada par de inteiros (r, s), tais que $d = ra + sb$, tem-se que $mdc(r, s) = 1$.

(13) Sejam a e b inteiros. Mostre que se $mdc(a, b) = 1$, então $mdc(a^n, b) = 1$, para todo inteiro $n \geq 1$. (*Sugestão: use indução em* n).

(14) Sejam $x_1, x_2, ..., x_k, n$ inteiros positivos. Mostre que se $mdc(x_i, n) = 1$, para todo $i = 1, 2, .., k$, então $mdc(x_1x_2...x_k, n) = 1$.

(15) Mostre que quaisquer dois inteiros consecutivos são relativamente primos.

(16) Mostre que para todo $n \in \mathbb{Z}$, os inteiros $2n + 1$ e $2n - 1$ são relativamente primos.

(17) Sejam a, b e c inteiros. Mostre que se $mdc(a, b) = 1$ e $c|(a + b)$, então $mdc(a, c) = mdc(b, c) = 1$. (*Sugestão: use a hipótese para encontrar inteiros* x, y, z, w, *tais que* $ax + cy = 1$ *e* $bz + cw = 1$).

(18) Sejam a, b e c inteiros. Mostre que se $100a|bc$ e a e b são relativamente primos, então $a|c$.

(19) Sejam a, b e c inteiros. Mostre que:
(a) se a é divisível simultaneamente por 3 e 5, então a é divisível por 15;
(b) se a é divisível simultameamente por 8 e 9, então a é divisível por 72;
(c) se a é divisível simultaneamente por b e c e $mdc(b, c) = 1$, então $bc|a$.

(20) João tem 864 bolinhas de gude, sendo 480 vermelhas e o restante, pretas. Ele resolveu guardá-las em saquinhos, de modo que todos os saquinhos tenham a mesma quantidade de bolinhas e que em cada um deles todas as bolinhas sejam da mesma cor. Desejando colocar a maior quantidade possível de bolinhas em cada saquinho, quantos saquinhos de cada cor serão formados e qual a quantidade de bolinhas em cada um deles?

Respostas da Lista de Exercícios 5

(01.a) $80 = 8.10$ e $30 = 3.10 \Rightarrow 10|80$ e $10|30 \Rightarrow 10$ é um divisor comum de 80 e 10. Se $d' \in \mathbb{Z}$ é tal que $d'|80$ e $d'|30$, então $d'|(80.(-1) + 30.3) \Rightarrow d'|10$. Portanto $mdc(80, 30) = 10$.

(02.a) $mdc(8, 76) = 4 = (-9).8 + 1.76$ (02.b) $mdc(312, 42) = 6 = (-2).312 + 15.42$

(02.c) $mdc(-23, 14) = 1 = 3.(-23) + 5.14$ (02.d) $mdc(-18, -52) = 2 = (-3).(-18) + 1.(-52)$

(02.e) $mdc(234, -415) = 1 = 94.234 + 53.(-415)$ (02.f) $mdc(392, 490) = 98 = (-1).392 + 1.490$

(03.a) $(4, 5)$ (03.b) $(-240, 300)$ (03.c) $(2, -5)$ (03.d) $(10, -25)$ (03.e) $(4, -3)$ (03.f) $(-20, 15)$

(04) $a = -13$ ou $a = 13$.

(05) Os possíveis valores para o par (a, b) são $(12, 84)$ ou $(36, 60)$.

(06) Os possíveis valores para o par (a, b) são $(7, 42)$ ou $(14, 21)$.

(09.a) $mdc(22, 16, 38) = 2$ (09.b) $mdc(8, 15, 4, 23) = 1$ (09.c) $mdc(180, -90, 84, -294, 60) = 6$.

(11.a) $mdc(a, c) = mdc(b, c) = 1 \Rightarrow \exists\, x, y, z, w \in \mathbb{Z}$, tais que $ax + cy = 1$ e $bz + cw = 1 \Rightarrow (ax + cy)(bz + cw) = 1 \Rightarrow ab(xz) + c(axw + bzy + cyw) = 1 \Rightarrow mdc(ab, c) = 1$, conforme Proposição 4, pois xz e $(axw + bzy + cyw) \in \mathbb{Z}$.

(11.b) $mdc(a, c) = 1 \Rightarrow \exists\, x, y \in \mathbb{Z}$, tais que $ax + by = 1 \Rightarrow ax + bx + by - bx = 1 \Rightarrow (a + b)x + b(y - x) = 1 \Rightarrow mdc(a + b, b) = 1$, pois x e $(x - y) \in \mathbb{Z}$.

(19.c) $mdc(b, c) = 1 \Rightarrow \exists\, x, y \in \mathbb{Z}$, tais que $bx + cy = 1 \Rightarrow abx + acy = a$. Como $b|a$ e $c|a \Rightarrow \exists\, k_1, k_2 \in \mathbb{Z}$, tais que $a = bk_1 = ck_2$. Substituindo esses valores no lado esquerdo da equação anterior: $(bc)(xk_2) + (bc)(yk_1) = a \Rightarrow bc(xk_2 + yk_1) = a \Rightarrow bc|a$.

(20) 5 saquinhos com bolinhas vermelhas e 4 com bolinhas pretas, todos com 96 unidades.

Capítulo 6

Mínimo Múltiplo Comum

1 Introdução

Na gincana escolar, citada no capítulo anterior, a turma que obtiver o maior número de pontos na realização das tarefas será a vencedora e levará o prêmio, o qual consiste de N livros. A quantidade N de livros foi estabelecida de modo que possa ser igualmente dividida entre todos os alunos da turma vencedora, qualquer que seja ela. Determine o valor de N, sabendo que ele é o menor inteiro possível com essa propriedade.
Solução:
Como N pode ser dividido de forma exata entre os alunos de quaisquer das turmas, então

$$40|N \quad \text{e} \quad 50|N$$

isto é, N é um **múltiplo positivo comum** de ambos os inteiros. Assim,

$$N \in \{40, 80, 120, 160, 200, ...\} \cap \{50, 100, 150, 200, 250, ...\} = \{200, 400, 600, ...\}.$$

Sendo N o **menor** possível, então $N = 200$. $\square$

O inteiro $N = 200$, por ser o menor dentre os múltiplos positivos comuns dos inteiros 40 e 50, é chamado o mínimo múltiplo comum desses inteiros, conforme definido a seguir.

2 Múltiplos de um Inteiro

Dado um inteiro n, usaremos a notação $n\mathbb{Z}$ para representar o conjunto de todos os inteiros que são múltiplos de n, isto é,

$$n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\} = \{..., -3n, -2n, -n, 0, n, 2n, 3n, ...\}$$

Exemplos:
(01) $5\mathbb{Z} = \{5k \mid k \in \mathbb{Z}\} = \{..., -15, -10, -5, 0, 5, 10, 15, ...\}$;

(02) $-4\mathbb{Z} = \{-4k \mid k \in \mathbb{Z}\} = \{..., -12, -8, -4, 0, 4, 8, 12, ...\} = 4\mathbb{Z}$;
(03) $10\mathbb{Z} = \{10k \mid k \in \mathbb{Z}\} = \{..., -40, -30, -20, -10, 0, 10, 20, 30, ...\}$;
(04) $-15\mathbb{Z} = \{-15k \mid k \in \mathbb{Z}\} = \{..., -45, -30, -15, 0, 15, 30, 45, ...\} = 15\mathbb{Z}$.

Definição 4. *Sejam a e b inteiros não nulos ($a \neq 0$ e $b \neq 0$). Um inteiro c diz-se um* ***múltiplo comum*** *de a e b se ambos são divisores de c, isto é, $a|c$ e $b|c$.*

Observe que se c é um múltiplo comum de a e b, então $c \in a\mathbb{Z} \cap b\mathbb{Z}$.

Exemplos:
(a) 15 é um múltiplo comum de 3 e 5, pois $3|15$ e $5|15$;
(b) -30 é um múltiplo comum de 10 e -15, pois $10|-30$ e $-15|-30$;
(c) 40 é um múltiplo comum de 8 e 20, pois $40 \in 8\mathbb{Z} \cap 20\mathbb{Z} = \{..., -40, 0, 40, 80, ...\}$.

✓ **Exercícios 10.**

(01) Determine:
(a) $2\mathbb{Z} \cap 4\mathbb{Z}$;
Solução:
Observe que se $c \in 4\mathbb{Z}$, então existe $k \in \mathbb{Z}$, tal que $c = 4k = 2(2k) \in 2\mathbb{Z} \Rightarrow 4\mathbb{Z} \subset 2\mathbb{Z} \Rightarrow 2\mathbb{Z} \cap 4\mathbb{Z} = 4\mathbb{Z}$. □

(b) $2\mathbb{Z} \cap 3\mathbb{Z}$;
Solução:
$c \in 2\mathbb{Z} \cap 3\mathbb{Z} \Rightarrow c \in 2\mathbb{Z} \Rightarrow c = 2k_1$, com $k_1 \in \mathbb{Z}$ e $c \in 3\mathbb{Z} \Rightarrow c = 3k_2$, com $k_2 \in \mathbb{Z}$. Assim, temos:
$c = 2k_1 = 3k_2 \Rightarrow 2|3k_2 \Rightarrow 2|k_2$, conforme Teorema 7, pois $mdc(2, 3) = 1$. Portanto, $k_2 = 2k$, $k \in \mathbb{Z}$. Daí,

$$c = 3k_2 = 3(2k) = 6k \in 6\mathbb{Z} \Rightarrow 2\mathbb{Z} \cap 3\mathbb{Z} \subset 6\mathbb{Z}.$$

Por outro lado, para todo $6k \in 6\mathbb{Z}$, temos $6k = 2(3k) = 3(2k) \in 2\mathbb{Z} \cap 3\mathbb{Z}$. Portanto, também temos a inclusão no outro sentido. Logo, $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$. □

(c) $4\mathbb{Z} \cap 10\mathbb{Z}$;
Solução:
$c \in 4\mathbb{Z} \cap 10\mathbb{Z} \Rightarrow c = 4k_1 = 10k_2$, $k_1, k_2 \in \mathbb{Z} \Rightarrow 2k_1 = 5k_2 \Rightarrow 2|5k_2 \Rightarrow 2|k_2$, pois $mdc(2, 5) = 1$. Assim, $k_2 = 2k \Rightarrow c = 10k_2 = 20k \in 20\mathbb{Z} \Rightarrow 4\mathbb{Z} \cap 10\mathbb{Z} \subset 20\mathbb{Z}$ e obviamente, que $20\mathbb{Z} \subset 4\mathbb{Z} \cap 10\mathbb{Z}$. Assim, $4\mathbb{Z} \cap 10\mathbb{Z} = 20\mathbb{Z}$. □

(02) Mostre que para quaisquer inteiros não nulos a e b, $a\mathbb{Z} \cap b\mathbb{Z} \neq \{0\}$.
Solução:
Como a e b são não nulos, então $0 \neq ab \in a\mathbb{Z} \cap b\mathbb{Z}$, pois é um múltiplo comum de a e b. □

3 Mínimo Múltiplo Comum

Definição 5. *Sejam a e b inteiros não nulos. Diz-se que um inteiro positivo m é o* ***mínimo múltiplo comum de*** a **e** b*, se m verifica as seguintes condições:*
(i) $a|m$ e $b|m$;
(ii) Se m' é um inteiro tal que $a|m'$ e $b|m'$, então $m|m'$.

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

A condição (i) da definição acima, diz que o $mmc(a, b)$ é um múltiplo comum de a e b e a condição (ii), que ele é o menor dos múltiplos positivos comuns de a e b, pois se $m' > 0$ é qualquer outro múltiplo comum de a e b, então $mmc(a, b)|m'$ e portanto, $mmc(a, b) \leq m'$.

Para o mmc, temos observações análogas às feitas para o mdc, isto é,

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

✓ **Exercícios 11.**
(01) Use a Definição 5 para justificar as afirmações abaixo:
(a) $mmc(2, 5) = 10$;
Solução:
Temos que mostrar que 10 satistaz as condições (i) e (ii) da Definição 5. De fato,
(i) $2|10$ e $5|10$, logo, 10 é um múltiplo positivo comum de 2 e 5;
(ii) Se $m' \in \mathbb{Z}$ é tal que $2|m'$ e $5|m'$, então $m' = 2k_1 = 5k_2$, com $k_1, k_2 \in \mathbb{Z}$. Mas, como $2k_1 = 5k_2 \Rightarrow 2|5k_2 \Rightarrow 2|k_2$, pois $mdc(2, 5) = 1$. Assim, $k_2 = 2k$, $k \in \mathbb{Z}$. Logo $m' = 5k_2 = 5(2k) = 10k \Rightarrow 10|m'$, sendo 10, portanto, o menor dos múltiplos positivos comuns de 2 e 5. □

(b) $mmc(-5, 25) = 25$;
Solução:
De fato, $-5|25$ e $25|25$, logo 25 é um múltiplo comum de -5 e 25. E se $m' \in \mathbb{Z}$ é tal que $-5|m'$ e $25|m' \Rightarrow m' = -5k_1 = 25k_2 \Rightarrow -k_1 = 5k_2 \Rightarrow m' = -5k_1 = 5(-k_1) = 5(5k_2) = 25k_2 \Rightarrow 25|m'$. Portanto, $25 = mdc(-5, 25)$. □

(c) $mmc(6, 14) = 42$.
Solução:
Como $6|42$ e $14|42$, 42 é um múltiplo comum dos dois inteiros. E se $m' \in \mathbb{Z}$ é tal que $6|m'$ e $14|m' \Rightarrow m' = 6k_1 = 14k_2 \Rightarrow 3k_1 = 7k_2 \Rightarrow 3|7k_2 \Rightarrow 3|k_2$, pois $mdc(3, 7) = 1$. Assim, $k_2 = 3k$, $k \in \mathbb{Z}$. Portanto, $m' = 14k_2 = 14(3k) = 42k \Rightarrow 42|m'$. Assim, $42 = mmc(6, 14)$. □

(d) $mmc(6, 9) = 18$;
(e) $mmc(42, 7) = 42$;
(f) $mmc(-8, 28) = 56$;
(g) $mmc(-11, -35) = 385$.

4 Relação entre MDC e MMC

Nos exercícios resolvidos anteriormente, foi informado o valor do *mmc* de dois inteiros e tivemos apenas que mostrar que aquele valor estava de acordo com a definição dada. Porém, ainda não sabemos como encontrar tal inteiro. A próxima proposição estabelece uma relação entre o *mdc* e *mmc* de dois inteiros não nulos, fornecendo assim, um algoritmo para o cálculo do *mmc*.

Proposição 6. *Sejam a e b inteiros não nulos, então*

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

Demonstração:
Seja $d = mdc(a,b)$. Vamos mostrar que o inteiro $m := \frac{|ab|}{d}$ é o mínimo múltiplo comum de a e b, isto é, $m = mmc(a,b)$. De fato, temos que:
(i) $a|m$ e $b|m$.
Observe que sendo $d = mdc(a,b)$, então $\frac{a}{d}$ e $\frac{b}{d}$ são números inteiros e como

$$m = |a|\frac{|b|}{d} = |b|\frac{|a|}{d} \Rightarrow a|m \quad \text{e} \quad b|m.$$

(ii) m é menor dos múltiplos positivos comuns de a e b:
Seja $m' \in \mathbb{Z}$ tal que $a|m'$ e $b \mid m'$. Então existem inteiros k_1, k_2, tais que:

$$m' = ak_1 = bk_1 \Rightarrow \frac{a}{d}k_1 = \frac{b}{d}k_2 \Rightarrow \frac{b}{d}|(\frac{a}{d}.k_1).$$

Como $mdc(\frac{a}{d}, \frac{b}{d}) = 1$, segue do Teorema 7, que $\frac{b}{d} \mid k_1 \Rightarrow k_1 = \frac{b}{d}.k$, com $k \in \mathbb{Z}$. Assim,

$$m' = ak_1 = \frac{ab}{d}k = \pm\frac{|ab|}{d}k = \pm mk \Rightarrow m \mid m'.$$

De (i) e (ii) segue que:

$$mmc(a,b) = \frac{|ab|}{d} \Rightarrow |ab| = mmc(a,b).d = mmc(a,b).mdc(a,b).$$

□

✓ **Exercícios 12.**
(01) Usando a Proposição 6, calcule:
(a) $mmc(24, 14)$;
Solução:
Já vimos que $mdc(24, 14) = 2$, então pela Proposição 6:
$mmc(24, 14) = \frac{24.14}{mdc(24,14)} = \frac{336}{2} = 168.$ □

(b) $mmc(-124, 52)$;
Solução:
Pela Proposição 6, $mmc(-124, 52) = \frac{|-124.52|}{mdc(-124,52)} = \frac{6448}{4} = 1612.$ □

(c) $mmc(13,8)$;
Solução:
Pela Proposição 6:
$mmc(13,8) = \frac{|13.8|}{mdc(13,8)} = \frac{104}{1} = 104.$ $\square$

(02) Determine todos os valores possíveis para o par de inteiros positivos (a,b), com $a \leq b$, sabendo que $ab = 6720$ e $mmc(a,b) = 1680$.
Solução 1:
Como $mdc(a,b).mmc(a,b) = |ab| \Rightarrow mdc(a,b) = \frac{ab}{mmc(a,b)} = \frac{6720}{1680} = 4.$ Portanto $4|a$ e $4|b \Rightarrow a = 4k_1$ e $b = 4k_2$, com $k_1, k_2 \in \mathbb{Z}$. Então,

$$6720 = ab = (4k_1)(4k_2) \Rightarrow 6720 = 16k_1k_2 \Rightarrow k_1k_2 = 420.$$

Para determinarmos os possíveis valores para k_1 e k_2, vejamos todas as decomposição de 420 como o produto de dois inteiros positivos:

$$\begin{aligned} k_1k_2 = 420 &= 1.420 = 2.210 = 3.140 = 4.105 = 5.84 = 6.70 \\ &= 7.60 = 10.42 = 12.35 = 14.30 = 15.28 = 20.21. \end{aligned}$$

Agora, como $4 = mdc(a,b) = mdc(4k_1, 4k_2) \Rightarrow mdc(k_1,k_2) = 1$. Assim, para a solução do problema só servem os produtos em que os fatores são relativamente primos. Tomando k_1 e k_2 com essa condição e lembrando que $a = 4k_1$ e $b = 4k_2$, os pares (a,b) de inteiros positivos satisfazendo a condição dada são: $(4,1680), (12,560), (16,420), (20,336), (28,240), (48,140), (60,112)$ e $(80,84)$. $\square$

Solução 2:
Podemos também tomar todas as decomposições de 6720 como produto de dois inteiros positivos, nesse caso, teremos 56 formas de fazer essa decomposição:

$$ab = 6720 = 1.6720 = 2.3360 = 3.2240 = 4.1680 = ... = 80.84$$

e então verificar em quais dessas decomposições temos $mmc(a,b) = 1680$. $\square$

Lista de Exercícios 6.

(01) Use a Definição 5 para justificar as afirmações abaixo:
(a) $mmc(8, 40) = 40$;
(b) $mmc(21, 30) = 210$;
(c) $mmc(14, -33) = 462$;
(d) $mmc(-8, -9) = 72$.

(02) Usando a Proposição 6, calcule:

(a) $mmc(1, 12)$	(b) $mmc(-1, 129)$;	(c) $mmc(3, 6)$;
(d) $mmc(-5, 30)$;	(e) $mmc(31, 31)$;	(f) $mmc(3, 5)$;
(g) $mmc(7, 8)$;	(h) $mmc(36, -27)$;	(i) $mmc(-6, -28)$;
(j) $mmc(11, 24)$;	(k) $mmc(32, 18)$;	(l) $mmc(-12, 38)$.

(03) Mostre que:
(a) $8\mathbb{Z} \cap 24\mathbb{Z} = 24\mathbb{Z}$;
(b) $6\mathbb{Z} \cap 7\mathbb{Z} = 42\mathbb{Z}$;
(c) $12\mathbb{Z} \cap 14\mathbb{Z} = 84\mathbb{Z}$.

(04) Determine:
(a) $7\mathbb{Z} \cap 35\mathbb{Z}$;
(b) $12\mathbb{Z} \cap 13\mathbb{Z}$;
(c) $8\mathbb{Z} \cap 12\mathbb{Z}$.

(05) Determine o valor do inteiro positivo b, para o qual tem-se $mdc(48, b) = 6$ e $mmc(48, b) = 432$.

(06) Mostre que para todo inteiro não nulo a, $mmc(a, 1) = |a|$.

(07) Sejam a e b inteiros não nulos. Mostre que se $a|b$, então $mmc(a, b) = |b|$.

(08) Mostre que se a e b são inteiros primos entre si, então $mmc(a, b) = |ab|$.

(09) Sejam a e b inteiros não nulos. Mostre que $mdc(a, b)$ divide $mmc(a, b)$.

(10) Sejam a e b inteiros positivos. Mostre que se $mdc(a, b) = mmc(a, b)$, então $a = b$.

(11) Determine todos os possíveis valores para o par de inteiros positivos (a, b), com $a \leq b$, sabendo que:
(a) $mmc(a, b) = 35$ e a e b são relativamente primos;
(b) $mdc(a, b) = 2$ e $mmc(a, b) = 104$;
(c) $ab = 408$ e $mmc(a, b) = 204$;
(d) $mmc(a, b) = mdc(a, b) = 35$;
(e) $mdc(a, b) + mmc(a, b) = 266$ e $mdc(a, b).mmc(a, b) = 528$.

(12) Seja $n \in \mathbb{Z} - \{-1, 0\}$. Calcule $mmc(n, n + 1)$.

(13) Seja $n \in \mathbb{Z} - \{-1, 0\}$. Mostre que $mmc(2n-1, 2n+1) = (2n-1)(2n+1)$.

(14) Um país tem eleições para presidente de 5 em 5 anos e para governador, de 4 em 4 anos. Em 2000, essas duas eleições coindidiram. Quando serão as três próximas vezes que elas voltarão a coincidir? Justifique sua resposta.

(15) Em uma estação rodoviária os ônibus com destino às cidades A, B e C, partem em intervalos de 6, 8 e 5 horas, respectivamente. Em certo momento a partida dos ônibus para essas três cidades ocorreu exatamente no mesmo instante. Quando tempo depois, isto ocorrerá novamente? Justifique sua resposta.

Respostas da Lista de Exercícios 6

(01.c) Vamos mostrar que 210 satisfaz as condições (i) e (ii) da Definição 5. Como $21|210$ e $30|210$, 210 é um múltiplo comum dos dois inteiros. E se $m' \in \mathbb{Z}$ é tal que $21|m'$ e $30|m' \Rightarrow m' = 21k_1 = 30k_2 \Rightarrow 7k_1 = 10k_2 \Rightarrow 7|10k_2 \Rightarrow 7|k_2$, pois $mdc(7, 10) = 1$. Assim, $k_2 = 7k$. Portanto, $m' = 30k_2 = 30(7k) = 210k \Rightarrow 210|m'$.

(02.a) $mmc(1, 12) = 12$ (02.b) $mmc(-1, 129) = 129$ (02.c) $mmc(3, 6) = 6$

(02.d) $mmc(-5, 30) = 30$ (02.e) $mmc(31, 31) = 31$ (02.f) $mmc(3, 5) = 15$

(02.g) $mmc(7, 8) = 56$ (02.h) $mmc(36, -27) = 108$ (02.i) $mmc(-6, -28) = 84$

(02.j) $mmc(11, 24) = 264$ (02.k) $mmc(32, 18) = 288$ (02.l) $mmc(-12, 38) = 228$.

(04.a) $35\mathbb{Z}$ (04.b) $156\mathbb{Z}$ (04.c) $24\mathbb{Z}$.

(05) $b = 54$

(11.a) (1, 35) ou (5, 7) (11.b) (2, 104) ou (8, 26)

(11.c) (2, 204), (4, 102), (6, 68) ou (12, 34)

(11.d) $a = b = 35$ (11.e) (2, 264), (6, 68), (8, 66) ou (24, 22)

(12) $mmc(n, n+1) = n(n+1)$

(14) 2020, 2040 e 2060

(15) 120 horas depois

(14) 2.678

(15) 120 minutos.

Capítulo 7

Números Primos

1 Definição

Definição 6. *Um número inteiro p diz-se **primo** se ele tem exatamente dois divisores positivos distintos, 1 e $|p|$.*

Denotando por $D_+(a)$ o conjunto dos divisores positivos de um inteiro a, então $p \in \mathbb{Z}$ é primo se $D_+(p) = \{1, |p|\}$ é um conjunto com exatamente dois elementos distintos.

Um número $a \in \mathbb{Z} - \{-1, 0, 1\}$ que não é primo, diz-se ***composto***.

Exemplos:
(a) 5 é um número primo, pois $D_+(5) = \{1, 5\}$;
(b) -7 é um número primo, pois $D_+(-7) = \{1, 7\}$;
(c) 1 não é um número primo, pois $D_+ = \{1\}$.
(d) 4 é um número composto, pois $D_+(4) = \{1, 2, 4\}$.

Observe que se $a \in \mathbb{Z} - \{-1, 0, 1\}$ é um inteiro composto, então existe $b \in \mathbb{Z}$, tal que $b|a$ e $1 < b < |a|$. Como visto no Capítulo 3 , todo inteiro com essa propriedade é chamado *divisor próprio* de a. Assim, todo inteiro composto tem pelo menos um divisor próprio.

✓ **Exercícios 13.**

(01) Determine $D_+(a)$ para cada inteiro a abaixo e classifique-o em primo ou composto:
(a) $a = 23$;
(b) $a = 26$;
(c) $a = -11$;
(d) $a = -97$.

2 Propriedades dos Números Primos

Vejamos a seguir algumas propriedades dos números primos.

Proposição 7. *Sejam a e p números inteiros. Se p é primo e* $p \nmid a$*, então* $mdc(p, a) = 1$.

Demonstração:
Suponha $d = mdc(p, a) \Rightarrow d|p$. Como $d > 0$ e p é primo, então ou $d = 1$ ou $d = |p|$. Porém, como $p \nmid a$, então $d \neq |p|$, pois $d|a$. Logo, $d = 1$. □

Já vimos que se a, b e c são inteiros e $a|bc$, não necessariamente a divide algum dos fatores. Por exemplo, $6|(8.9)$, mas $6 \nmid 8$ e também $6 \nmid 9$. Porém, se a é relativamente primo com um dos fatores, que não é o caso desse exemplo, aí a necessariamente deverá dividir o outro fator, conforme Teorema 7. E o que dizer se a for um número primo? Usando o Teorema 7 e a proposição acima, a resposta, que você já deve ter inferido, é dada na proposição a seguir.

Proposição 8. *Sejam p, b e c números inteiros. Se p é primo e* $p|bc$*, então* $p|b$ *ou* $p|c$.

Demonstração:
Suponha que $p|bc$. Se $p|b$, a demonstração está encerrada. Se $p \nmid b$, pela Proposição 7, $mdc(p, b) = 1$ e pelo Teorema 7, $p|c$. □

Exemplos:
(01) $5|60$ e como 5 é primo, qualquer que seja a decomposição de 60 como produto de dois inteiros, 5 necessariamente dividirá pelo menos um dos fatores. Veja:

$$5|(1.60) \qquad 5|(2.30) \qquad 5|(3.10) \qquad 5|(4.15) \qquad 5|(5.12) \qquad 5|(6.10)$$

(02) Como 7 é primo e $7|84$, então qualquer que seja a decomposição de 84 como o produdo de dois inteiros, necessariamente 7 dividirá pelo menos um dos fatores. Verifique.

A proposição acima pode se estendida para um número $n \geq 2$ qualquer de fatores. Para a demonstração, usa-se indução no número n de fatores.

Corolário 3. *Sejam* $a_1, a_2, ..., a_n$ *e p números inteiros, com* $n \geq 2$*. Se p é um número primo e* $p|(a_1 a_2 ....a_n)$*, então* $p|a_k$*, para algum* $1 \leq k \leq n$.

3 A Infinitude do Conjunto dos Primos

Repetindo, um número inteiro $p > 1$ é dito primo, se ele não possui divisor próprio, isto é, entre os inteiros dos conjunto $A = \{2, 3, 4, 5, ..., p-1\}$ nenhum deles o divide. Ora, quando maior o inteiro p, mais elementos tem o conjunto

A e a intuição nos leva a acreditar que a probabilidade de não haver em A nenhum divisor de p, torna-se muito baixa. Então, os números inteiros "muito grandes" são todos números compostos? Esses eram questionamentos dos matemáticos da antiguidade: - Existe um número primo maior que todos os outros? - Quantos números primos existem? A Resposta é dada no próximo teorema, cuja demonstração foi feito por Euclides. Em preparação ao teorema, veremos antes um lema. E em preparação ao lema, façamos o exercício a seguir.

✓ **Exercícios 14.**

(01) Dê exemplo de um divisor primo p, para cada um dos inteiros abaixo:
(a) 10 (b) 2 (c) 1349 (d) 2847 (e) 13 (f) 317 (g) 913
(02) Dê exemplo de um interio $a > 1$, que não possui nenhum divisor primo.

O lema a seguir mostra porque você não obteve sucesso na questão 02 do exercício acima.

Lema 1. *Todo inteiro $a > 1$ tem um divisor primo.*

Demonstração:
Faremos a demonstração por indução em a. Usaremos a 2^a Forma do Princípio da Indução Finita (Corolário 2).
(i) Base de Indução: $a = 2$:

Nesse caso, o resultado é verdadeiro, pois 2 é primo e $2|2$.

(ii) Passo Indutivo: Seja $a \geq 2$ um inteiro e considere o resultado válido para todo inteiro k, com $1 < k < a$.

Se a é primo o resultado é imediato. Se a é composto, então existem inteiros d, q, com $1 < d, q < a$, tais que $a = dq$. Como $1 < d < a$, segue da hipótese de indução que d tem um divisor primo p. E como $p|d$ e $d|a$, segue que $p|a$. □

Suponha que você seleciona 5 números primos $p_1, p_2, ..., p_5$ e efetua o produto deles obtendo $N = p_1p_2p_3p_4p_5$. O inteiro N tem divisor primo? Por quê? E $N + 1$ tem divisor primo? Por quê?

Por fim, vamos ao teorema.

Teorema 8. *O conjunto dos números primos é infinito.*

Demonstração:
Considere P_+ o conjunto de todos os números primos positivos. Suponhamos, por absurdo, que este conjunto seja finito, digamos

$$P_+ = \{p_1, p_2, ..., p_n\}.$$

Usando os elementos de P_+ podemos construir o inteiro

$$N = p_1p_2...p_n + 1.$$

Como $N > 1$, pelo Lema 1, ele tem um divisor primo positivo, isto é, existe $p_i \in P_+$, tal que $p_i|N$, então existe $k \in \mathbb{Z}$, tal que $N = p_i k$. Assim,

$$p_1 p_2 ... p_{i-1} p_i p_{i+1} ... p_n + 1 = p_i k \Rightarrow p_i(k - p_1 p_2 ... p_{i-1} p_{i+1} ... p_n) = 1 \Rightarrow p_i|1,$$

um absurdo, pois p_i é primo. Logo, o conjunto P_+ não pode ser finito e obviamente o conjunto de todos os primos é também infinito. □

Por maior que seja um número inteiro n, já vimos que este pode ser primo ou composto, já que o conjunto dos números primos é infinito. Mas como verificar se n é primo ou composto? A rigor, para afirmar que n é primo, devemos garantir que ele não tem nenhum divisor no conjunto:

$$A = \{2, 3, ..., n - 1\}.$$

Se n é um inteiro muito grande, esta verificação torna-se trabalhosa. Com auxílio do Lema 1, podemos diminuir consideravelmente esse trabalho. É o que veremos na próxima proposição.

Proposição 9. *Se $n > 2$ é um número composto, então n tem um divisor primo p, com $1 < p \leq \sqrt{n}$.*

Demonstração:
Como n é composto, ele tem divisor próprio, isto é, existem inteiros d_1, d_2, tais que $n = d_1 d_2$, com $1 < d_1, d_2 < n$. Suponhamos $d_1 \leq d_2$. Então,

$$d_1 \leq d_2 \Rightarrow d_1^2 \leq d_1 d_2 = n \Rightarrow d_1 \leq \sqrt{n}.$$

Agora, como $d_1 > 1$, pela Lema 1, existe p primo, tal que $p|d_1 \Rightarrow p \leq d_1 \leq \sqrt{n}$. E como $p|d_1$ e $d_1|n$, segue que $p|n$. □

✓ Exercícios 15.

(01) Use a Proposição 9 para verificar se os números abaixo são primos ou compostos:
(a) 233;
Solução:
Pela Proposição 9, se 233 é um número composto, ele terá um divisor primo $p \leq \sqrt{233} \approx 15,26$, ou seja, existe $p \in \{2, 3, 5, 7, 11, 13\}$, tal que $p|233$. Porém, como nenhum desses inteiros divide 233, podemos garantir que 233 é um número primo. □
(b) 319;
(c) 1043;
(d) 5047;
(e) 33817.

4 Decomposição em Fatores Primos

Lema 2. *Todo inteiro $a > 1$ pode ser escrito como um produto de números primos.*

Demonstração:
Faremos a demonstraçao por indução em a. Assumiremos também que o "produto" possa ter um único fator.
(i) Base de Indução: $a = 2$:
Isto é verdadeiro, pois a já é primo.

(ii) Passo Indutivo: Suponha por hipótese de indução que a afirmaçao é válida para todo inteiro b, com $2 \leq b < a$.
Se a é primo, a demonstraçao está encerrada. Se a não é primo, existem inteiros b, c, tais que $a = bc$, com $1 < b, c < a$. Segue da hipótese de induçao que existem primos $p_1, p_2, ..., p_r$, $p'_1, p'_2, ...p'_s$, tais que $b = p_1p_2....p_r$ e $c = p'_1p'_2...p'_s$. Assim,

$$a = bc = p_1p_2...p_r.p'_1p'_2...p'_s,$$

que é um produto de números primos. □

Teorema 9. *(* ***Teorema Fundamental da Aritmética****) Para todo inteiro $a > 1$, existem primos positivos $p_1 \leq p_2 \leq p_3 \leq ... \leq p_t$, tais que*

$$a = p_1p_2p_3...p_t$$

e essa decomposição é única.

Este teorema foi demonstrado por Carl Friedrich Gauss em 1796.

Demonstração:
Seja $a > 1$ um inteiro. A existência da decomposição de a em fatores primos já foi provada no Lema 2. Mostraremos agora a unicidade. Suponha que:

$$a = p_1p_2...p_n = q_1q_2...q_s,$$

com $p_1 \leq p_2 \leq ... \leq p_n$ e $q_1 \leq q_2 \leq .... \leq q_s$ primos positivos. Faremos a demonstração por indução no número n de fatores primos na decomposição.
(i) Se $n = 1$

$$a = p_1 = q_1q_2...q_s \Rightarrow q_1|p_1.$$

Como p_1 e q_1 são primos positivos, então $p_1 = q_1$. Fazendo $p_1 = q_1$ na identidade acima e efetuando o cancelamento, obtemos:

$$1 = q_2(q_3...q_s).$$

Se $s > 1$, então $q_2|1$, um absurdo, pois q_2 é primo. Logo $s = 1 = n$ e $a = p_1 = q_1$. Portanto, para $n = 1$ a decomposição é única.

(ii) Suponha que o resultado é válido para todo inteiro que se decompõe em

$k \geq 1$ fatores primos. E considere

$$a = p_1p_2...p_kp_{k+1} = q_1q_2...q_s.$$

duas decomposiçoes de a em fatores primos positivos. Segue daí que

$$q_1|p_1p_2...p_kp_{k+1} \Rightarrow q_1|p_i, \text{ para algum } 1 \leq i \leq k+1.$$

Como p_i é primo, então $q_1 = p_i \geq p_1$. De modo análogo, obtem-se $p_1 = q_j \geq q_1$, para algum j. Logo $p_1 = q_1$. Substituindo esses valores na identidade acima e usando a lei do cancelamento obtemos:

$$p_2p_3...p_kp_{k+1} = q_2q_3...q_s.$$

Como à direita temos uma decomposição em k fatores primos, segue da hipótese de induçao, segue que $k = s - 1 \Rightarrow k + 1 = s$, $p_i = q_i$, para $i = 2, 3, ..., k + 1$. □

Nessa decomposição, podemos agrupar os primos eventualmente repetidos e enunciar o resultado acima, dizendo que todo inteiro $a \geq 2$ se escreve na forma:

$$a = p_1^{n_1}p_2^{n_2}...p_t^{n_t},$$

com $1 < p_1 < p_2 < ... < p_t$ primos e $n_i \geq 1$, para $i = 1, 2, ..., t$ - conhecida como a **Decomposição de a em Fatores Primos**.

✓ **Exercícios 16.**

(01) Escreva a decomposição de a em fatores primos, onde:
(a) $a = 7$
Solução:
Como 7 já é um número primo, então a decompoisção fica:

$$7 = 7.$$

□

(b) $a = 105$
Solução:
Inicialmente identificamos o menor primo que divide 105 e repetimos o processo para os fatores que vão sendo encontrados, até obtermos somente fatores primos:
$105 = 3 \times 35 = 3 \times 5 \times 7.$ □

(c) $a = 352$
Solução:
$352 = 2 \times 176 = 2 \times (2 \times 88) = 2^2 \times (2 \times 44) = 2^3 \times (2 \times 22) = 2^4 \times (2 \times 11)$
$= 2^5 \times 11.$ □

Lista de Exercícios 7.

(01) Verifique se os inteiros abaixo são primos ou compostos:
(a) 607 (b) 943 (c) 2411 (d) 19769 (e) 50653

(02) Faça a decomposição em fatores primos, de cada um dos inteiros abaixo:
(a) 13 (b) 286 (c) 3685 (d) 13800 (e) 50653

(03) Encontre todos os primos positivos p e q, tais que $p - q = 3$.

(04) Determine todos os primos positivos que dividem 50!.

Um inteiro N é dito um quadrado perfeito, se existe $a \in \mathbb{Z}$, tal que $N = a^2$.

(05) Seja $a = p_1^{n_1} p_2^{n_2} .... p_t^{n_t}$ a decomposição de um inteiro $a > 1$ em fatores primos. Mostre que a é um quadrado perfeito se, e somente se, n_i é par para todo $i = 1, 2, .., t$.

(06) Encontre todos os números primos positivos que são iguais a um quadrado perfeito menos 1.

(07) Encontre todos os primos positivos que são iguais a um cubo perfeito menos 1.

(08) Mostre que três ímpares positivos consecutivos não podem ser todos primos, à exceção de 3, 5 e 7.

(09) Mostre que todo primo positivo, à exceção de 2 e 3, é da forma $6k + 1$ ou $6k - 1$, para algum inteiro k.

(10) Seja $n \geq 2$ um inteiro. Mostre que se $n^2 + 2$ é um número primo, então $3|n$. (*sugestão: use redução ao absurdo*).

(11) Dê exemplos, caso existam, de dois números primos da forma $2^n - 1$, com $n \geq 2$ sendo:
(a) n primo; (b) n composto.

(12) Seja $n \geq 2$ um inteiro. Mostre que se $(2^n - 1)$ é primo, então n é primo.

(13) Seja $a = p_1^{n_1} p_2^{n_2} ... p_t^{n_t}$ a decomposição de um inteiro positivo a em fatores primos. Mostre que se $d = p_1^{m_1} p_2^{m_2} ... p_t^{m_t}$, com $0 \leq m_i \leq n_i$, para $i = 1, 2, .., t$, então $d|a$.

(14) Use o Teorema 9 para mostrar que:
(a) $\sqrt{2}$ não é um número racional.
(b) Se p e q são primos, então $\sqrt{pq}$ não é um número racional.

(15) Mostre que se $p > 0$ é primo, então $mdc(p, (p-1)!) = 1$.

(16) Usando indução em n, prove o Corolário 3.

Respostas da Lista de Exercícios 7

(01.a) 607 é primo (01.b) 943 é composto (01.c) 2411 é primo

(01.d) 19769 é composto (01.e) 50653 é composto

(02.a) 13=13 (02.b) 286=2.11.13 (02.c) 3685=5.11.67

(02.d) $13800 = 2^3.3.5^2.23$ (02.e) $50653 = 37^3$

(03) $p = 5$ e $q = 2$

(04) Os primos positivos $p < 50$, ou seja, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

(06) 3

(07) 7

(08) Sejam $N_1 = 2n + 1, N_2 = 2n + 3$ e $N_3 = 2n + 5$ três ímpares consecutivos. Se $n = 1$, temos os primos 3, 5 e 7. Suponhamos N_1, N_2 e N_3 todos primos, com $n \geq 2$. Dentre os 3 inteiros consecutivos $2n + 1, 2n + 2$ e $2n + 3$, um deles é divisível por 3 (questão 22 da Lista de Exercícios 3). Como $N_1, N_2 > 3$ e ambos são primos, segue que o divisível por 3 é $2n+2 \Rightarrow 2n+2 = 3k, k \in \mathbb{Z} \Rightarrow N_3 = 2n+5 = 3k+3 = 3(k+1) \Rightarrow 3|N_3$, um absurdo, pois $N_3 > 3$ e é primo.

(09) Seja $p \geq 5$ um primo. Pelo algoritimo da divisão existem inteiros k e r, tais que $p = 6k + r$, com $0 \leq r \leq 5$. Porém, como p é primo, $r \notin \{0, 2, 3, 4\}$, pois nesses casos, $2|p$ ou $3|p$, contrariando o fato de p ser um primo ≥ 5. Assim, $p = 6k + 1$ ou $p = 6k + 5 = 6k + (6 - 1) = 6(k + 1) - 1 = 6k' - 1$, com $k' \in \mathbb{Z}$.

(11.a) $7 = 2^3 - 1$; $127 = 2^7 - 1$ são primos; (11.b) Não existe, conforme questão (12)

(12) Suponhamos, por absurdo que $2^n - 1$ é primo, com n composto. Como n é composto, então $n = n_1 n_2$, com $1 < n_1, n_2 < n$. Daí,
$2^n - 1 = 2^{n_1 n_2} - 1 = (2^{n_1})^{n_2} - 1 = (2^{n_1} - 1)((2^{n_1})^{n_2 - 1} + (2^{n_1})^{n_2 - 2} + ... + 1) \Rightarrow (2^{n_1} - 1)|(2^n - 1)$
e como $1 < n_1 < n \Rightarrow 1 < 2^{n_1} - 1 < 2^n - 1 \Rightarrow 2^{n_1} - 1$ é um divisor próprio de $2^n - 1$. Um absurdo.

(15) Seja $d = mdc(p, (p-1)!) \Rightarrow d|p$ e $d|(p-1)!$. Como p é primo, $d = 1$ ou $d = p$. Se $d = p$, temos $p|(p - 1)! \Rightarrow p|((p - 1)(p - 2)(p - 3)...2.1) \Rightarrow p|(p - k) \Rightarrow p \leq (p - k)$, para algum inteiro k, com $1 \leq k \leq p - 1$, um absurdo. Assim, $d = 1$.

Capítulo 8

Aplicações da Decomposição em Fatores Primos

1 Cálculo dos Divisores

Nesta seção veremos como determinar os divisores positivos de um número inteiro, a partir de sua decomposição em fatores primos.

Proposição 10. *Seja*

$$a = p_1^{n_1} p_2^{n_2} p_3^{n_3} ... p_t^{n_t}$$

a decomposiçao de um inteiro $a > 1$ *em fatores primos positivos e distintos. Um inteiro* d *é um divisor positivo de* a *se, e somente se,*

$$d = p_1^{m_1} p_2^{m_2} p_3^{m_3} ... p_t^{m_t},$$

com $0 \leq m_i \leq n_i$*, para* $i = 1, 2, ..., t$.

Demonstração:
$(\Rightarrow)$ $\;d = p_1^{m_1} p_2^{m_2} ... p_t^{m_t}$, com $0 \leq m_i \leq n_i \quad \Rightarrow \quad d|a$.

Suponha $d = p_1^{m_1} p_2^{m_2} ... p_t^{m_t}$, com $0 \leq m_i \leq n_i$, para todo i. Como $m_i \leq n_i$, então $n_i - m_i \geq 0$. Assim, podemos escrever:

$$a = p_1^{n_1} p_2^{n_2} ... p_t^{n_t} = p_1^{m_1 + (n_1 - m_1)} . p_2^{m_2 + (n_2 - m_2)} ... p_t^{m_t + (n_t - m_t)}$$

$$= (p_1^{m_1} p_2^{m_2} ... p_t^{m_t})(p_1^{n_1 - m_1} . p_2^{n_2 - m_2} ... p_t^{n_t - m_t}) = dc,$$

onde $c = p_1^{n_1 - m_1} . p_2^{n_2 - m_2} ... p_t^{n_t - m_t} \in \mathbb{Z}$. Logo, $d|a$.

$(\Leftarrow)$ $d|a \quad \Rightarrow \quad d = p_1^{m_1} p_2^{m_2} ... p_t^{m_t}$, com $0 \leq m_i \leq n_i$, para $i = 1, 2, .., t$.

Suponha que $d|a \Rightarrow$ existe um inteiro c, tal que

$$a = dc$$

Como d e c são inteiros, esses também se decompõem em fatores primos. Porém, $a = dc$, segue da unicidade da decomposição em fatores primos que na decomposição de d e c só estarão presentes os primos que aparecem na decomposição de a. Assim,

$$d = p_1^{m_1} p_2^{m_2} p_3^{m_3} ... p_t^{m_t} \qquad \text{e} \qquad c = p_1^{r_1} p_2^{r_2} p_3^{r_3} ... p_t^{r_t}$$

com $m_i, r_i \geq 0$. Então

$$a = dc$$
$$\Downarrow$$
$$p_1^{n_1} p_2^{n_2} p_3^{n_3} ... p_t^{n_t} = p_1^{m_1+r_1} p_2^{m_2+r_2} p_3^{m_3+r_3} ... p_t^{r_t+m_t}$$
$$\Downarrow$$
$$n_i = m_i + r_i \Rightarrow 0 \leq m_i \leq n_i, \forall i.$$

□

✓ **Exercícios 17.**

(01) Usando a Proposição 10, determine todos os divisores positivos de cada um dos inteiros abaixo:
(a) 38
Solução:
$38 = 2.19$ é a decomposição de 38 em fatores primos. Pela Proposição 10, $d|38$ se, e só se, $d = 2^{m_1}.19^{m_2}$, com $m_1, m_2 \in \{0, 1\}$. Fazendo m_1, m_2 assumirem todos os valores possíveis, temos os seguintes divisores:
$d_1 = 2^0.19^0 = 1$, $d_2 = 2^0.19^1 = 19$, $d_3 = 2^1.19^0 = 2$ e $d_4 = 2^1.19^1 = 38$. □

(b) 360
Solução:
A decomposição de 360 em fatores primos é $360 = 2^3.3^2.5$. Então os divisores positivos de 360 são os inteiros da forma

$$d = 2^{m_1}.3^{m_2}.5^{m_3}, \text{ com } m_1 \in \{0, 1, 2, 3\},\ m_2 \in \{0, 1, 2\} \text{ e } m_3 \in \{0, 1\}.$$

Atribuindo a m_1, m_2 e m_3 os valores possíveis, encontramos os seguintes divisores:

$2^0.3^0.5^0 = 1,$	$2^0.3^0.5^1 = 5,$	$2^0.3^1.5^0 = 3,$	$2^0.3^1.5^1 = 15,$	$2^0.3^2.5^0 = 9,$	$2^0.3^2.5^1 = 45,$
$2^1.3^0.5^0 = 2,$	$2^1.3^0.5^1 = 10,$	$2^1.3^1.5^0 = 6,$	$2^1.3^1.5^1 = 30,$	$2^1.3^2.5^0 = 18,$	$2^1.3^2.5^1 = 90,$
$2^2.3^0.5^0 = 4,$	$2^2.3^0.5^1 = 20,$	$2^2.3^1.5^0 = 12,$	$2^2.3^1.5^1 = 60,$	$2^2.3^2.5^0 = 38,$	$2^2.3^2.5^1 = 180,$
$2^3.3^0.5^0 = 8,$	$2^3.3^0.5^1 = 40,$	$2^3.3^1.5^0 = 24,$	$2^3.3^1.5^1 = 120,$	$2^3.3^2.5^0 = 72,$	$2^3.3^2.5^1 = 360,$

Logo, o conjunto dos divisores positivos de 360 é

$$\{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 18, 20, 24, 30, 38, 40, 45, 60, 72, 90, 120, 180, 360\},$$

contendo um total de

$$\underbrace{4}_{\text{opções de } m_1} \times \underbrace{3}_{\text{opções de } m_2} \times \underbrace{2}_{\text{opções de } m_3} = 24 \quad \text{elementos.}$$

□

(c) 547;
Solução:
Como $547 = 547$ é a decomposição de 547 em fatores primos, então $d|547 \Leftrightarrow d = 547^m$, com $0 \leq m \leq 1 \Rightarrow 547^0 = 1$ e $547^1 = 547$ são os únicos divisores positivos de 547. □
(d) 105;
(e) 352
(f) p, com p primo.
(g) p^n, com $n \geq 1$ e p primo.

2 Números de Divisores

Em muitos casos, não estamos interessados em encontrar os divisores de um inteiro, mas apenas saber quantos são eles. Essa quantidade é facilmente obtida a partir da proposição anterior.

Corolário 4. *Seja*

$$a = p_1^{n_1} p_2^{n_2} p_3^{n_3} ... p_t^{n_t}$$

a decomposiçao do inteiro $a > 1$ em fatores primos positivos. Então, o número de divisores positivos de a é dada pelo produto:

$$(n_1 + 1)(n_2 + 1)(n_3 + 1)....(n_t + 1).$$

Demonstração:
Pela Proposição 10, existem tantos divisores positivos de a quantos são os inteiros da forma

$$d = p_1^{m_1} p_2^{m_2} p_3^{m_3} ... p_t^{m_t}, \text{ com } 0 \leq m_i \leq n_i, \text{ para todo } i = 1, 2, ..., t.$$

Para construir um inteiro desta forma efetuamos as seguintes passos:
(1) - Escolhemos um valor para m_1 - temos n_1+1 opções, pois $m_1 \in \{0, 1, 2, ..., n_1\}$;
(2) - Escolhemos um valor para m_2 - temos n_2+1 opções, pois $m_2 \in \{0, 1, 2, ..., n_2\}$;
...
(t) - Escolhemos um valor para m_t - temos n_t+1 opções, pois $m_t \in \{0, 1, 2, ..., n_t\}$.

Pelo Princípio Multiplicativo, o total de modos de construir d é dado pelo produto: $(n_1 + 1)(n_2 + 1)(n_3 + 1)....(n_t + t)$. □

✓ **Exercícios 18.**

(01) Usando o Corolário 4, determine o número de divisores positivos de cada um dos inteiros:
(a) 3920
Solução:
$3920 = 2^4.5.7^2$, então o número de divisores de 3920 é dado por:

$$\underbrace{(4+1)}_{\text{opções de } m_1} \times \underbrace{(1+1)}_{\text{opções de } m_2} \times \underbrace{(2+1)}_{\text{opçoes de } m_3} = 30.$$

□

(b) 23
Solução:
Como $23 = 23$ é a decomposição de 23 em fatores primos, então o número de seus divisores positivos é dado por $(1+1) = 2$. □
(c) 72;
(d) 416;
(e) 815;
(f) p, com p primo;
(g) p^n, com $n \geq 1$ e p primo.

3 Soma dos Divisores

Vejamos agora, como obter a soma dos divisores positivos de um inteiro, sem a necessidade de relacionar esses divisores. Para um melhor entendimento, vejamos antes alguns exercícios resolvidos.

✓ **Exercícios 19.**

(01) Determine a soma S dos divisores positivos de cada um dos inteiros abaixo:
(a) 7.
Solução:
Como 7 é primo, seus divisore são: 7^0 e 7^1. Portanto, $S = (7^0 + 7^1) = 8$. □

(b) p, com p primo.
Solução:
Já vimos que os divisores de p são p^0 e p^1, logo $S = (p^0 + p^1) = (p+1)$. □

(c) 128
Solução:
$128 = 2^7$ é a decomposição de 128 em fatores primos, logo seus divisores são 2^k, com $0 \leq k \leq 7$. Assim,

$$S = (2^0 + 2^1 + ... + 2^7)$$

S é portanto, a soma dos 8 primeiros termos da progressão geométrica (P.G.) $2^0, 2^1, 2^2, 2^3, ...$. Como a soma dos n primeiros termos da P.G. $a, aq, aq^2, aq^3, ...$

é dada por:

$$a + aq + aq^2 + ... + aq^{n-1} = \frac{a(q^n - 1)}{q - 1}.$$

Então,

$$S = (2^0 + 2^1 + ... + 2^7) = \frac{1.(2^8 - 1)}{2 - 1} = 255.$$

(d) p^n, com $n \geq 1$ e p primo.
Solução:
Trata-se de uma generalização do caso anterior. Como $p^0, p^1, ..., p^n$ são os divisores positivos de a, então

$$S = (p^0 + p^1 + p^2 + ... + p^n) = \frac{p^0.(p^{n+1} - 1)}{p - 1} = \frac{p^{n+1} - 1}{p - 1}.$$

□

(e) 36
Solução:
Como $36 = 2^2.3^2$, os divisores positivos de 36 são:

$$d = 2^m.3^n, \qquad \text{com} \quad 0 \leq m, n \leq 2.$$

Assim,
$S = \sum_{m=0}^{2} \sum_{n=0}^{2} (2^m.3^n) = 2^0 \sum_{n=0}^{2} 3^n + 2^1 \sum_{n=0}^{2} 3^n + 2^2 \sum_{n=0}^{2} 3^n$
$= (2^0 + 2^1 + 2^2) \sum_{n=0}^{2} 3^n$
$= (2^0 + 2^1 + 2^2)(3^0 + 3^1 + 3^2) = (\frac{2^3-1}{2-1}).(\frac{3^3-1}{3-1}) = 7.13 = 91.$ □

(f) $p^m.q^n$, com p, q primos.
Solução:
Trata-se de uma generalização do caso anterior. Pela Proposição 10, os divisores positivos de $p^m.q^n$ são

$$d = p^\alpha q^\beta, \quad \text{com} \quad 0 \leq \alpha \leq m \quad \text{e} \quad 0 \leq \beta \leq n.$$

Assim,
$S = \sum_{\alpha=0}^{m} \sum_{\beta=0}^{n} (p^\alpha.q^\beta) = p^0 \sum_{\beta=0}^{n} q^\beta + p^1 \sum_{\beta=0}^{n} q^\beta + ... + p^m \sum_{\beta=0}^{n} q^\beta$
$= (p^0 + p^1 + p^2 + ... + p^m) \sum_{\beta=0}^{n} q^\beta$
$= (p^0 + p^1 + ... + p^m)(q^0 + q^1 + ... + q^n)$
$= (\frac{p^{m+1}-1}{p-1}).(\frac{q^{n+1}-1}{q-1}).$
Em cada um dos parênteses acima, temos a soma dos termos de uma P.G. □

Corolário 5. *Seja*

$$a = p_1^{n_1} p_2^{n_2} ... p_t^{n_t}$$

a decomposiçao do inteiro $a > 1$ em fatores primos. Então a soma S dos divisores positivos de a é dada pelo produto:

$$S = (\frac{p_1^{n_1+1} - 1}{p_1 - 1})(\frac{p_2^{n_2+1} - 1}{p_2 - 1})...(\frac{p_t^{n_t+1} - 1}{p_t - 1}).$$

Demonstração:
Como $a = p_1^{n_1} p_2^{n_2} ... p_t^{n_t}$, pela Proposição 10, os divisores se a são:

$$d = p_1^{\alpha_1}.p_2^{\alpha_2}...p_t^{\alpha_t} \qquad \text{com cada} \quad 0 \leq \alpha_i \leq n_i$$

Assim,
$S = \sum_{\alpha_1=0}^{n_1} \sum_{\alpha_2=0}^{n_2} ... \sum_{\alpha_t=0}^{n_t} (p_1^{\alpha_1}.p_2^{\alpha_2}...p_t^{\alpha_t})$
$= p_1^0.(\sum_{\alpha_2=0}^{n_2} ... \sum_{\alpha_t=0}^{n_t} p_2^{\alpha_2}...p_t^{\alpha_t}) + p_1^1.(\sum_{\alpha_2=0}^{n_2} ... \sum_{\alpha_t=0}^{n_t} p_2^{\alpha_2}...p_t^{\alpha_t}) + ...+$
$p_1^{n_1}.(\sum_{\alpha_2=0}^{n_2} ...p_1^{n_t} \sum_{\alpha_t=0}^{n_t} p_2^{\alpha_2}...p_t^{\alpha_t})$
$= (p_1^0 + p_1^1 + ... + p_1^{n_1})(\sum_{\alpha_2=0}^{n_2} ... \sum_{\alpha_t=0}^{n_t} p_2^{\alpha_2}...p_t^{\alpha_t})$
...
$= (p_1^0 + p_1^1 + p_1^2 + ...p_1^{n_1}).(p_2^0 + p_2^1 + p_2^2 + ...p_2^{n_1})...(p_t^0 + p_t^1 + p_t^2 + ...p_t^{n_t}).$

Como cada um desses fatores é a soma dos termos de uma P.G., então aplicando a fórmula citada acima obtemos:

$$S = (\frac{p_1^{n_1+1} - 1}{p_1 - 1})(\frac{p_2^{n_2+1} - 1}{p_2 - 1})...(\frac{p_t^{n_t+1} - 1}{p_t - 1}).$$

□

4 Algoritmo II para o cálculo do MDC e MMC

O próximo teorema diz como calcular o *mdc* e *mmc* de dois inteiros a partir de suas decomposições em fatores primos.

Teorema 10. *Sejam*

$$a = p_1^{n_1} p_2^{n_2} ... p_t^{n_t} \qquad e \qquad b = p_1^{m_1} p_2^{m_2} ... p_t^{m_t}$$

inteiros positivos, com $1 < p_1 < p_2 < ... < p_n$ *primos e* $0 \leq n_i, m_i$*, para todo* $i = 1, 2, ..., t$*. Então*
(I) $mdc(a, b) = p_1^{\alpha_1} p_2^{\alpha_2} ... p_t^{\alpha_t}$*, onde* $\alpha_i = min\{n_i, m_i\}$*, para todo* $i = 1, 2, ..., t$*.*

(II) $mmc(a, b) = p_1^{\beta_1} p_2^{\beta_2} ... p_t^{\beta_t}$*, onde* $\beta_i = max\{n_i, m_i\}$*, para todo* $i = 1, 2, ..., t$*.*

Demonstração:
(I) $mdc(a, b) = p_1^{\alpha_1} p_2^{\alpha_2} ... p_t^{\alpha_t}$, onde $\alpha_i = min\{n_i, m_i\}$

Vamos mostrar que $d = p_1^{\alpha_1} p_2^{\alpha_2} ... p_t^{\alpha_t}$, com $\alpha_i = min\{n_i, m_i\}$, satisfaz as condições (i) e (ii) da Definição 2. De fato,
(i) Como $\alpha_i = min\{n_i, m_i\}$, então $\alpha_i \leq n_i$ e $\alpha_i \leq m_i$, para todo i. Logo, pelo Proposição 10, $d|a$ e $d|b$.
(ii) Seja d' um inteiro tal que $d'|a$ e $d'|b$. Então, pela Proposição 10,
$d' = p_1^{r_1} p_2^{r_2} ... p_t^{r_t}$, onde $r_i \leq n_i$ e $r_i \leq m_i$, para todo i. Logo
$r_i \leq min\{n_i, m_i\} = \alpha_i$, e novamente pelo Proposição 10, segue que $d'|d$.

De (i) e (ii) segue que $d = mdc(a, b)$.

(II) $mmc(a, b) = p_1^{\beta_1} p_2^{\beta_2} ... p_t^{\beta_t}$, com $\beta_i = max\{n_i, m_i\}$.

Mostraremos que $m = p_1^{\beta_1} p_2^{\beta_2} ... p_t^{\beta_t}$, onde $\beta_i = max\{n_i, m_i\}$, satisfaz as condições (i) e (ii) da Definição 5. De fato,

(i) Como $n_i \leq \beta_i$ e $m_i \leq \beta_i$, para todo $i = 1, 2, .., t$, segue da Proposição 10 que, $a|m$ e $b|m$.

(ii) Seja $m' = p_1^{r_1} p_2^{r_2} ... p_t^{r_t}$ um inteiro tal que $a|m'$ e $b|m'$. Da Proposição 10, segue que $n_i \leq r_i$ e $m_i \leq r_i$, para todo i. Assim, $r_i \geq max\{n_i, m_i\} = \beta_i \Rightarrow m'|m$. Portanto, $m = mmc(a, b)$ □

✓ **Exercícios 20.**

(01) Usando a decomposição em fatores primos, calcule $mdc(a, b)$ e $mmc(a, b)$, onde:

(a) $a = 360, b = 6804$

Solução:

Inicialmente, faremos a decomposição de cada um dos inteiros em fatores primos:

$$360 = 2^3.3^2.5 \quad \text{e} \quad 6804 = 2^2.3^5.7$$

Agora, reescrevemos essa decomposição de modos que ambas tenha os mesmos números primos em suas decomposições. Para isso, consideramos decomposições da forma $a = p_1^{n_1}.p^{n_2}...p_t^{n_t}$, com $\mathbf{n_i \geq 0}$, ou seja, estamos admitindo a possibilidade de **expoentes nulos**. Fazendo isso para as decomposições acima obtemos:

$$360 = 2^3.3^2.5.7^0 \quad \text{e} \quad 6804 = 2^2.3^5.5^0.7$$

Comparamos agora os expoentes de cada número primo presente nas decomposições. Para o mdc tomamos o menor deles e para o mmc, o maior:

$$mdc(360, 6804) = 2^2.3^2.5^0.7^0 = 36$$
$$mmc(360, 6804) = 2^3.3^5.5.7 = 68040.$$ □

(b) $a = 1352$ e $b = 4004$

Solução:

Como

$$1352 = 2^3.13^2 \quad \text{e} \quad 4004 = 2^2.7.11.13,$$

escrevemos:

$$1352 = 2^3.7^0.11^0.13^2 \quad \text{e} \quad 4004 = 2^2.7.11.13,$$

portanto:

$$mdc(1352, 4004) = 2^2.7^0.11^0.13 = 52$$
$$mmc(1352, 4004) = 2^3.7.11.13^2 = 104104.$$ □

Lista de Exercícios 8.

(01) Usando a decomposição em fatores primos, determine todos os divisores positivos de cada um dos inteiros abaixo:
(a) 316
(b) 921
(c) 4012
(d) 22315
(e) $p^m.q^n$, com p, q primos.

(02) Determine o número de divisores positivos de cada um dos inteiros abaixo:
(a) 256
(b) 918
(c) 7704
(d) 25075
(e) $p^m.q^n$, com p, q primos.

(03) Determine o número de divisores próprios de cada um dos inteiros:
(a) 535
(b) 724
(c) 4848
(d) 1111
(e) $p^m.q^n$, com p, q primos.

(04) Determine a soma dos divisores positivos de cada um dos inteiros abaixo:
(a) 5 (b) 91 (c) 280 (d) 792

(05) Usando a decomposição em fatores primos, determine $mdc(a, b)$ e $mmc(a, b)$:
(a) $a = 28$, $b = 58$;
(b) $a = 108$, $b = 96$;
(c) $a = 33$, $b = 24$;
(d) $a = 139$, $b = 148$;
(e) $a = 286$, $b = 1058$;
(f) $a = 4612$, $b = 248$;
(g) $a = 3612$, $b = 108$.

(06) (ENADE-2014) Os números perfeitos foram introduzidos na Grécia, antes de Cristo. Um número n é dito perfeito se ele for igual à soma de seus divisores positivos e próprios, ou seja, dos divisores positivos menores que n.
(a) Verifique se 28 é um número perfeito;
(b) Dado $n = 2^2 \times 4^2 \times 127$, determine o número de divisores próprios de n (menores que n) e verifique se n é um número perfeito;
(c) Mostre que se $2^k - 1$ é primo, $k > 1$, então o inteiro positivo, $n = 2^{k-1}(2^k - 1)$ é um número perfeito;
(d) Seja n o número obtido adicionando-se as potências $2^0, 2^1, 2^2, 2^3$, ...até que a soma seja igual ao décimo primeiro número primo, e, em seguida, multiplicando a soma obtida pela última potência. Mostre que n é um número perfeito.

Respostas da Lista de Exercícios 8

(01.a) 1, 2, 4, 79, 158, 316 (01.b) 1, 3, 307, 921
(01.c) 1, 2, 4, 17, 34, 59, 68, 118, 236, 1003, 2006, 4012 (01.d) 1, 5, 4463, 22315
(01.e) $1, q, q^2, ..., q^n$, $p, pq, pq^2, ..., pq^n$, $p^2, p^2q, p^2q^2, ..., p^2q^n$,... $p^m, p^mq, p^mq^2, ..., p^mq^n$
(02.a) 9 (02.b) 16 (02.c) 24 (02.d) 12 (02.e) $(m+1)(n+1)$
(03.a) 2 (03.b) 4 (03.c) 18 (03.d) 2 (03.e) $(m+1)(n+1)-2$
(04.a) 6 (04.b) 112 (04.c) 720 (04.d) 2340
(05.a) $mdc(28, 58) = 2$ e $mmc(28, 58) = 812$
(05.b) $mdc(108, 96) = 12$ e $mmc(108, 96) = 864$
(05.c) $mdc(33, 24) = 3$ e $mmc(33, 24) = 264$
(05.d) $mdc(139, 148) = 1$ e $mmc(139, 148) = 20572$
(05.e) $mdc(286, 1058) = 2$ e $mmc(286, 1058) = 151294$
(05.f) $mdc(4612, 248) = 2$ e $mmc(4612, 248) = 285944$
(05.g) $mdc(3612, 108) = 12$ e $mmc(3612, 108) = 32508$.
(06.a) Pela definição, n é perfeito se $S = 2n$. Como $28 = 2^2.7$, a soma dos divisores de 28 é dada por $S = (\frac{2^3-1}{2-1})(\frac{7^2-1}{7-1}) = 7.8 = 56 = 2.28 \Rightarrow 28$ é um número perfeito;
(06.b) $n = 2^2 \times 4^2 \times 127 = 8128$ tem $(2+1).(2+1).(1+1) = 18$ divisores, entre eles o próprio n. Logo, n tem 17 divisores próprios, conforme definido na questão e a soma de seus divisores é dada por $S(\frac{2^3-1}{2-1})(\frac{4^3-1}{4-1})(\frac{127^2-1}{127-1}) = 7.21.128 = 18816 = 2 \times 9408 \neq 2.n$, logo n não é um número perfeito.
(06.c) Considere $n = 2^{k-1}.p$, onde $p = (2^k - 1)$ é primo. Como 2 e p são primos, a soma dos divisores positivos de n é dada por $S = (\frac{2^k-1}{2-1})(\frac{p^2-1}{p-1}) = \frac{(2^k-1).(p-1)(p+1)}{(p-1)} = (2^k-1)(2^k-1+1) = 2^k(2^k-1) = 2.2^{k-1}.p = 2n \Rightarrow n$ é um número perfeito.
(06.d) Seja $p = 2^0 + 2^1 + ... + 2^k = (2^{k+1} - 1)$ o 11^0 número primo obtido somando-se as parcelas como no comando da questão, com k o expoente para o qual isto acontece e $n = 2^k.p$. Como os dois fatores são números primos, segue que $S = \frac{(2^{k+1}-1)(p^2-1)}{p-1} = (2^{k+1}-1)(p+1) = (2^{k+1}-1)(2^{k+1}-1+1) = 2(2^k.(2^{k+1}-1) = 2(2^kp) = 2n \Rightarrow n$ é um número perfeito.

Capítulo 9

Congruência em $\mathbb{Z}$

1 Introdução

• Em uma festa infantil, um grupo de 7 crianças - Ana, Beatriz, Carlos, Davi, Eduardo, Fernanda e Gabriela - reuniu-se próximo a uma mesa para brincar de 'esconde-esconde', um jogo no qual uma criança é separada dos demais, que procuram locais para se esconder, sem que a escolhida as veja, pois esta tentará encontrá-las após um tempo estabelecido previamente. Assim, era necessário escolher qual delas seria aquela que iria procurar todas as outras.

Para efetuar essa escolha, as crianças se dispuseram em um círculo, na mesma ordem descrita anteriormente e, simultaneamente, mostraram um número de dedos das mãos. Os números de dedos mostrados foram somados, resultando em um quantidade que vamos chamar de TOTAL. Ana começou contar de 1 até TOTAL, e, a cada número dito, apontava para uma criança da seguinte forma: 1 - Ana, 2 - Beatriz, 3 - Carlos, 4 - Davi, e assim por diante. Quanto chegasse ao número TOTAL, a criança correspondente a esse número seria aquela que iria procurar as demais. Se o número TOTAL é igual a 64, qual a criança designada para procurar as demais?

Solução:
Pensemos em uma solução para o problema acima, o qual trata-se de uma questão do ENADE-2014. Observe que temos um grupo de 7 crianças, dispostas em um círculo e Ana atribui a cada uma delas um número de 1 a TOTAL, da seguinte forma:

Ana	Beatriz	Carlos	Davi	Eduardo	Fernanda	Gabriela
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
...	...	...	...	...	...	...

Como temos um círculo com 7 pessoas, a cada 7 unidades, retorna-se à mesma criança.

À Beatriz ficam atribuidos os números:

$$2 = 7.0 + 2$$

$$9 = 7.1 + 2$$

$$16 = 7.2 + 2$$

$$...$$

ou seja, todos os números da forma:

$$n = 7.k + 2.$$

À Fernanda, por sua vez, recebe os números:

$$6 = 7.0 + 6$$

$$13 = 7.1 + 6$$

$$20 = 7.2 + 6.$$

$$...$$

ou seja, todos os números da forma:

$$n = 7.k + 6.$$

Portanto, o que identifica a criança a qual será atribuído um número n qualquer, é exatamente o **resto** da divisão de n por 7, segundo tabela abaixo:

	Ana	Beatriz	Carlos	Davi	Eduardo	Fernanda	Gabriela
Resto:	1	2	3	4	5	6	0

Como

$$\text{TOTAL} = 64 = 7.9 + 1 \Rightarrow r = 1 \Rightarrow \quad \text{a criança é a Ana.}$$

Em linguagem matemática, dizemos que estamos operando em *módulo* 7 e que os números atribuídos a uma mesma criança são todos *congruentes módulo* 7, conforme definiremos a seguir. Nesta unidade estudaremos a aritmética dos restos obtidos na divisão euclidiana.

2 Inteiros Congruentes

Definição 7. *Dado um inteiro não nulo m, dizemos que os inteiros a e b são **congruentes módulo** m, se eles deixam o mesmo resto na divisão euclidiana por m.*

Exemplos:
(a) 7 e 4 são congruentes módulo 3, pois ambos deixam resto 1 na divisão por 3;
(b) 8 e -10 são congruentes módulo -6, já que deixam resto 2 na divisão por -6;
(c) 25 e 9 são congruentes módulo 4, pois ambos deixam resto 1 na divisão por 4;
(d) 25 e 9 não são congruentes módulo 5, pois deixam restos distintos na divisão por 5.

Para indicar que a e b são congruentes módulo m, escreve-se:

$$a \equiv b(mod m).$$

Quando a afirmação $a \equiv b(mod m)$ for falsa, diremos que a e b não são congruentes (ou são incongruentes) módulo m e escreveremos $a \not\equiv b(mod m)$.

Exemplos:
Com a notação acima, os exemplos anteriores ficam:
(a) $7 \equiv 4(mod 3)$;
(b) $8 \equiv -10(mod(-6))$;
(c) $25 \equiv 9(mod 4)$;
(d) $25 \not\equiv 9(mod 5)$.

✓ **Exercícios 21.**

(01) Responda e justifique:
(a) $30 \equiv 10(mod 4)$?
(b) $23 \equiv 17(mod 4)$?
(c) $-30 \equiv -14(mod 8)$?
(d) $12 \equiv 37(mod(-5))$?
(e) $6 \equiv 6(mod 7)$?
(f) $1907 \equiv 3917(mod 1)$?

Propriedades Elementares da Congruência

Da Definição 7, segue de forma imediata, que a congruência módulo m tem as seguintes propriedades para quaisquer inteiros a, b e c:
(C1) **Reflexiva**: $a \equiv a(mod m)$;
(C2) **Simétrica**: Se $a \equiv b(mod m)$, então $b \equiv a(mod m)$;
(C3) **Transitiva**: Se $a \equiv b(mod m)$ e $b \equiv c(mod m)$, então $a \equiv c(mod m)$.

Observe que:
(1) Como o resto da divisão de qualquer inteiro por 1 é sempre zero, então para quaisquer inteiros a e b, tem-se

$$a \equiv b(mod 1).$$

(02) Se $a \equiv b(mod m)$, ambos deixam o mesmo resto na divisão por m, isto é, existem inteiros q_1, q_2 e r, com $0 \leq r < |m|$, tais que:

$$a = mq_1 + r \text{ e } b = mq_2 + r.$$

Segue daí, que:

$$a = (-m)(-q_1) + r \text{ e } b = (-m)(-q_2) + r$$

ou seja, a e b também deixam o mesmo resto na divisão por $-m$, portanto também temos $a \equiv b(mod(-m))$.
Resumindo:

$$a \equiv b(mod m) \Leftrightarrow a \equiv b(mod(-m)).$$

Em vista das observações (1) e (2) vamos nos restringir ao caso em que o inteiro $m > 1$.

A próxima proposição dá uma forma equivalente de definir a congruência módulo m.

Proposição 11. *Seja $m > 1$ um inteiro. Para quaisquer inteiros a, b tem-se que*

$$a \equiv b(mod m) \textit{ se, e somente se, } m|(a-b).$$

Demonstração:
$(\Rightarrow)$ $a \equiv b(mod m) \Rightarrow m|(a-b)$:

$a \equiv b(mod m) \Rightarrow$ existem inteiros q_1, q_2 e r, com $0 \leq r < m$, tais que:

$$a = mq_1 + r \quad \text{e} \quad b = mq_2 + r \Rightarrow a - b = m(q_1 - q_2) \Rightarrow m \mid (a-b).$$

$(\Leftarrow)$ $m|(a-b) \Rightarrow a \equiv b(mod m)$:

$m|(a-b) \Rightarrow \exists\, k \in \mathbb{Z}$, tal que $a - b = mk \Rightarrow a = b + mk$. Seja r o resto da divisão de a por m, então $a = mq + r$, com $q \in \mathbb{Z}$. Assim,

$$a = b + mk = mq + r \Rightarrow b = m(q-k) + r$$

Como $0 \leq r < m$, da unicidade do resto, segue que r é também o resto da divisão de b por m, logo $a \equiv b(mod m)$. □

Resumindo, temos:

$$\boxed{a \equiv b(mod m) \Leftrightarrow m|(a-b).}$$

Exemplos:
(a) $47 \equiv 11(mod 9)$, pois $9|(47 - 11)$;
(b) $24 \equiv 314(mod 29)$, pois $29|(24 - 314)$;
(c) $8 \equiv 8(mod 7)$, pois $7|(8 - 8)$;
(d) $16 \not\equiv 5(mod 4)$, pois $4 \nmid (16 - 5)$.

✓ **Exercícios 22.**

(01) Usando agora a Proposição 11, responda e justifique:
(a) $30 \equiv 10(mod 4)$?
(b) $23 \equiv 17(mod 4)$?
(c) $-30 \equiv -14(mod 8)$?
(d) $12 \equiv 37(mod 5)$?
(e) $6 \equiv 6(mod 7)$?
(f) $1907 \equiv 3917(mod 33)$?

3 Congruência no Conjunto dos Restos

Já vimos que na divisão euclidiana por um inteiro $m > 1$, os possíveis restos pertencem ao conjunto:

$$R := \{0, 1, 2, ..., m - 1\}$$

Vejamos algumas conclusões relevantes, referentes à congruência, que podemos tirar sobre o conjunto R.

• Sabemos que para qualquer inteiro a, existem únicos inteiros q e r, com $r \in R$, tais que $a = mq + r$. Então,

$$a = mq + r \Rightarrow a - r = mq \Rightarrow m|(a - r) \Rightarrow a \equiv r(mod m).$$

Com isto podemos afirmar:

> **Todo** inteiro **é congruente módulo** m ao seu resto r na divisão por m, e como esse resto é único, ele é congruente a um **único** elemento do conjunto $R = \{0, 1, 2, ..., m - 1\}$.

Exemplos:
(01) 23 é congruente ao seu resto na divisão por 5. De fato,

$$23 = 5.4 + 3 \Rightarrow 5|(23 - 3) \Rightarrow 23 \equiv 3(mod 5).$$

E esse é o único inteiro no conjunto $\{0, 1, 2, 3, 4\}$ ao qual 23 é congruente módulo 5;

(02) 249 é congruente módulo 12 a um único elemento do conjunto $\{0, 1, 2, ..., 11\}$, sendo esse elemento o resto da divisão de 249 por 12, a saber $249 \equiv 9(mod 12)$;

(03) Quantos e quais elementos em $\{0, 1, 2, ..., 16\}$ são congruentes módulo 17 ao inteiro 52626? Justifique.

(04) Quantos e quais elementos em $\{0, 1, 2, ..., 49\}$ são congruentes módulo 50 ao inteiro 52626? Justifique.

• Existem elementos **distintos** $b, c \in R = \{0, 1, 2, ..., m-1\}$, tais que $b \equiv c(mod m)$?

Para responder a essa pergunta, suponhamos que existam $b, c \in R$, distintos, tais que $b \equiv c(mod m)$. Sendo distintos, então $b < c$ ou $c < b$. Vamos considerar $b < c$. Como

$$0 \leq b < c \leq m-1 \Rightarrow 0 < c-b \leq m-1.$$

Porém, se

$$b \equiv c(mod m) \Rightarrow m|(c-b) \Rightarrow m \leq (c-b) \leq m-1 \Rightarrow m \leq m-1,$$

um absurdo. Portanto, podemos afirma:

> Quaisquer dois elementos distintos em $R = \{0, 1, 2, ..., m-1\}$ são incongruentes módulo m. Portanto, se $r_i, r_j \in R$, são tais que:
>
> $$r_i \equiv r_j(mod m) \;\Rightarrow\; r_i = r_j.$$

4 Propriedades da Congruência

Já vimos que a reflexividade, a simetria e a transitividade são propriedades elementares da congruência. Como a congruência está estritamente relacionada com a divisibilidade, podemos deduzir mais algumas propriedades que seguem diretamente das propriedades de divisibilidade vistas no Capítulo 3.

Dado um inteiro $m > 1$, a relação de congruência módulo m, definida em $\mathbb{Z}$, tem as seguintes propriedades, para quaisquer inteiros a, b, c e d:

(C4) Se $a \equiv b(mod m)$, então $\begin{cases} a + c \equiv b + c(mod m) \\ ac \equiv bc(mod m) \end{cases}$.

Demonstração:
$a \equiv b(mod m) \Rightarrow m \mid (a-b)$. Das propriedades de divisibilidade, segue que:
(i) $m \mid [(a-b)+(c-c)] \Rightarrow m \mid [(a+c)-(b+c)] \Rightarrow a+c \equiv b+c(mod m)$.
(ii) $m \mid (a-b)c \Rightarrow m \mid (ac-bc) \Rightarrow ac \equiv bc(mod m)$. □

(C5) **Cancelamento da adição na congruência**:

Se
$$a + c \equiv b + c(mod.m),$$
então,
$$a \equiv b(modm).$$

Demonstração:
$a+c \equiv b+c(modm) \Rightarrow m \mid [(a+c)-(b+c)] \Rightarrow m \mid a-b \Rightarrow a \equiv b(modm)$. □

(C6) **Cancelamento da multiplicação na congruência**:

Se
$$ac \equiv bc(modm) \text{ e } \mathbf{mdc(c, m) = 1},$$
então,
$$a \equiv b(modm).$$

Demonstração:
$ac \equiv bc(modm) \Rightarrow m \mid (ac - bc) \Rightarrow m \mid (a-b)c$. Como $mdc(m, c) = 1$, pelo Teorema 7, $m \mid (a-b) \Rightarrow a \equiv b(modm)$. □

(C7) Se $\begin{cases} a \equiv b(modm) \\ \text{e} \\ c \equiv d(modm) \end{cases}$, então $\begin{cases} a + c \equiv b + d(modm) \\ ac \equiv bd(modm) \end{cases}$.

Demonstração:
$a \equiv b(modm)$ e $c \equiv d(modm) \Rightarrow m \mid (a-b)$ e $m \mid (c-d)$.
Segue das propriedades de divisibilidade que:
(i) $m \mid [(a-b)+(c-d)] \Rightarrow m \mid [(a+c)-(b+d)] \Rightarrow a+c \equiv b+d(modm)$;
(ii) $m \mid (a-b)c$ e $m \mid (c-d)b \Rightarrow m \mid [(ac-bc)+(bc-bd)]$
$\Rightarrow m \mid (ac-bd) \Rightarrow ac \equiv bd(modm)$. □

(C8) Se
$$a \equiv b(modm),$$
então, para todo inteiro $n \geq 0$, tem-se também:
$$a^n \equiv b^n(modm).$$

Demonstração:
Faremos a demonstração por indução em n.

(i) $n = 0$:
$a^0 - b^0 = 1 - 1 = 0 = 0.m \Rightarrow m|(a^0 - b^0) \Rightarrow a^0 \equiv b^0(mod m)$.
(ii) Seja $n \geq 0$ e suponha $a^n \equiv b^n(mod m)$:
Como $a \equiv b(mod m)$ (hipótese) e $a^n \equiv b^n(mod m)$ (hipótese de indução), segue da propriedade (C7), segue que $a^n.a \equiv b^n.b(mod m) \Rightarrow a^{n+1} \equiv b^{n+1}(mod m)$. $\square$

5 Aplicação da Congruência no Cálculo do Resto

Vejamos agora como usar a congruência para resolver o problema proposto no início da aula, cujo objetivo é calcular o resto da divisão de 3^{212} por 40.
Solução:
Já sabemos que para todo inteiro $n \geq 1$, $3^n \equiv r(mod 40)$, onde r é o resto da divisão de 3^n por 40. Comecemos por calcular os restos da divisão das primeiras potências positivas de 3 por 40:

$3^1 \equiv 3(mod 40)$
$3^2 \equiv 9(mod 40)$
$3^3 \equiv 27(mod 40)$
$3^4 \equiv 1(mod 40)$
$3^5 \equiv 3(mod 40)$
...

Para facilitar os cálculos, escolhamos a congruência $3^4 \equiv 1(mod 40)$, por deixar o menor resto. Dividindo o expoente 212 por 4, encontramos $212 = 53.4$. Então, aplicando a propriedade (C8) à congruência escolhida:

$$3^4 \equiv 1(mod 4) \Rightarrow (3^4)^{53} \equiv 1^{53}(mod 40) \Rightarrow 3^{212} \equiv 1(mod 40).$$

Como $1 \in \{0, 1, 2, ..., 39\}$, ele é o resto da divisão de 3^{212} por 40. $\square$

✓ **Exercícios 23.**
(01) Que número entre 0 e 6 é congruente módulo 7 ao produto
$11 \times 22 \times 2322 \times 13 \times 9$?
Solução:
Seja $P = 11 \times 22 \times 2322 \times 13 \times 9$. Obviamente, que está sendo pedido o resto da divisão de P por 7. Como trata-se de um número não muito grande, podemos calcular diretamente P e efetuar a divisão. Porém, como processo de aprendizagem, vamos determinar o resto usando as propriedades da congruência. Inicialmente, calcularemos o resto na divisão por 7, de cada um dos fatores de P:

$11 \equiv 4(mod 7)$
$22 \equiv 1(mod 7)$
$2322 \equiv 5(mod 7)$
$13 \equiv 6(mod 7)$
$9 \equiv 2(mod 7)$.

Aplicando repetidamente a propriedade (C7), temos:

$$11 \times 22 \times 2322 \times 13 \times 9 \equiv 4 \times 1 \times 5 \times 6 \times 2(mod 7) \Rightarrow P \equiv 240 \equiv 2(mod 7).$$

Portanto, o número procurado é 2. □

(02) Calcule o resto da divisão de 19^n por 14, para $n = 1, 2, 3, ..., 20$.
Solução:
Como $19 = 14.1 + 5$, então
$$19 \equiv 5(mod 14).$$
Multiplicando ambos os lados desta congruência por 19 (propriedade (C4)) e usando a transitividade (propriedade (C3)) temos:
$$19^2 \equiv 5.19(mod14) \text{ e como } 5.19 \equiv 11(mod9) \Rightarrow 19^2 \equiv 11(mod14)$$
Repetindo o processo:
$$19^3 \equiv 11.19(mod14) \Rightarrow 19^3 \equiv 13(mod14)$$
$$19^4 \equiv 13.19(mod14) \Rightarrow 19^4 \equiv 9(mod14)$$
$$19^5 \equiv 9.19(mod14) \Rightarrow 19^5 \equiv 3(mod14)$$
$$19^6 \equiv 3.19(mod14) \Rightarrow 19^6 \equiv 1(mod14)$$
Para o o expoente 6, obtivemos resto igual a 1, então pela propriedades (C8), para qualquer inteiro $k \geq 0$, temos:
$$(19^6)^k \equiv 1^k(mod19)$$
e pela propriedade C4, para todo inteiro $r = 0, 1, 2, ..., 6$:
$$19^{6k}.19^r \equiv 1.19^r(mod9) \Rightarrow 19^{6k+r} \equiv 19^r(mod14).$$
Assim,
$$19^8 = 19^{6.1+2} \equiv 19^2 \equiv 11(mod14);$$
$$19^9 = 19^{6.1+3} \equiv 19^3 \equiv 13(mod14).$$
$$....$$
$$19^{20} = 19^{6.3+2} \equiv 19^2 \equiv 11(mod14).$$
Logo, as potências $19, 19^2, 19^3, 19^4, ..., 19^{20}$ deixam respectivamente os restos 5, 11, 13, 9, 3, 1, 5, 11, 13, 9, 3, 1, 5, 11, 13, 9, 3, 1, 5 e 11 na divisão por 14.□

(03) Calcule o resto da divisão de 18^n por 7, para um inteiro $n \geq 1$, arbitrário.
Solução:
$$18 \equiv 4(mod7)$$
$$18^2 \equiv 4.18 \equiv 2(mod7)$$
$$18^3 \equiv 2.18 \equiv 1(mod7)$$
Para o expoente 3, obtivemos resto igual a 1. Logo, usando as propriedades (C8) e (C4), dado um inteiro $n \geq 1$, se k e r são, respectivamente, o quociente e resto da divisão de n por 3, então
$$18^n = 18^{3k+r} = (18^3)^k.18^r \equiv 1^k.18^r \equiv 18^r(mod7).$$
Portanto, o resto da divisão de 18^n por 7 é igual ao resto da divisão de 18^r por 7, sendo r é o resto da divisão de n por 3. Por exemplo,
. Como $20 = 3.6 + 2$, então $18^{20} \equiv 18^2 \equiv 2(mod7)$;
. Como $3202 = 3.1067 + 1$, então $18^{3202} \equiv 18 \equiv 4(mod7)$. □

(04) Determinar o resto da divisão de 7^{46} por 15.
Solução:
Inicialmente vamos calcular os restos distintos que obtemos na divisão das primeiras potências positivas de 7 por 15:

$$\begin{aligned}7 &\equiv 7(mod 15)\\ 7^2 &\equiv 4(mod 15)\\ 7^3 &\equiv 13(mod 15)\\ 7^4 &\equiv 1(mod 15)\end{aligned}$$

Dessa última congruência, usando a propriedade (C8) e (C4), para quaisquer inteiros não negativos k e r, temos:

$$7^{4k+r} = (7^4)^k.7^r \equiv 1^k.7^r \equiv 7^r(mod 15).$$

Assim,
$7^{46} = 7^{4.11+2} \equiv 7^2 \equiv 4(mod 15)$ e como $4 < 15$, 4 é o resto procurado. □

(05) Determine o algarismo das unidades de 8^{80}.
Solução:
Observe que o algarismo das unidades de qualquer inteiro é exatemento seu o resto na divisão por 10. Portanto, o problema consiste em encontrar o resto da divisão de 8^{80} por 10. Vejamos quais os restos deixados pelas primeiras potências positivas de 8 na divisão por 10:

$$\begin{aligned}8 &\equiv 8(mod 10)\\ 8^2 &\equiv 4(mod 10)\\ 8^3 &\equiv 2(mod 10)\\ 8^4 &\equiv 6(mod 10)\\ 8^5 &\equiv 8(mod 10).\end{aligned}$$

A partir desse expoente, os restos começam a repetir, logo, qualquer que seja a potência positiva de 8, só temos os restos 2, 4, 6 e 8. Aqui, ao contrário dos exemplos anteriores, nenhuma potência de 8 deixa resto 1 na divisão por 10. Porém, como

$$8^5 \equiv 8(mod 10),$$

para quaisquer inteiros $k \geq 0$ e $r \in \{0, 1, 2, 3, 4\}$:

$$8^{5k+r} = (8^5)^k.8^r \equiv 8^k.8^r = 8^{k+r}(mod 10).$$

Portanto,

$$8^{5k+r} \equiv 8^{k+r}(mod 10).$$

Assim,

$$8^{80} = 8^{5.16+0} \equiv 8^{16+0}(mod 10) \Rightarrow 8^{5.3+1} \equiv 8^{3+1} \equiv 6(mod 10).$$

Outra solução, é tomar a potência que deixa o menor resto, no caso 8^3, e como $80 = 3.26 + 2$, então

$$8^{80} = 8^{3.26+2} \equiv (8^3)^{26}.8^2 \equiv 2^{26}.4 = 2^{28} = (8^3)^3.2 \equiv 2^3.2 \equiv 6(mod 10).$$

Portanto, o algarismo das unidades de 8^{80} é 6. □

(06) Determinar o resto da divisão de 27^{303} por 15.
Calculando os resto das primeiras potências positivas de 27 na divisão por 15:

$$\begin{aligned}
&27 \equiv 12(mod 15)\\
&27^2 \equiv 27.12 \equiv 9(mod 15)\\
&27^3 \equiv 27.9 \equiv 3(mod 15)\\
&27^4 \equiv 27.3 \equiv 6(mod 15)\\
&27^5 \equiv 27.6 \equiv 12(mod 15).
\end{aligned}$$

Obtivemos aqui o mesmo resto da primeira potência. Segue então, que para qualquer inteiro $n \geq 1$, na divisão de 27^n por 15 os únicos restos possíveis são 3, 6, 9, 12. Portanto, nenhuma potência deixa resto 1. Como $27^5 \equiv 27(mod 15)$, para quaisquer inteiros $k \geq 0$ e $r \in \{0, 1, 3, 4\}$, temos:

$$27^{5k+r} = (27^5)^k.27^r \equiv 27^{k+r}(mod 15).$$

Assim,

$$27^{302} = 27^{5.60+2} \equiv 27^{62} = 27^{5.12+2} \equiv 27^{14} = 27^{5.2+4} \equiv 27^6 = 27^{5.1+1} \equiv 27^2 \equiv 9(mod 15).$$

Portanto, o resto é 9.

Outra solução é trabalhar com a potência que deixa o menor resto, no caso, 27^3. Assim,
$27^{302} = (27^3)^{100}.27^2 \equiv 3^{100}.9 \equiv 3^{102} = (3^3)^{34} = 27^{34} \equiv (27^3)^{10}.27^4$
$\equiv 3^{10}.6 = (27^3).3.6 \equiv 3.18 \equiv 9(mod 15).$ □

(07) Determine o resto da divisão de 5^{21} por 127.
Solução:
Na divisão de um inteiro qualquer por 127, podemos ter 127 restos distintos. Então, a tarefa de encontrar todos os restos distintos deixados pelas potências de 5, como feito nas questões anteriores, pode ser muito fatigante. Por outro lado, observa-se facilmente, que:
$127 = 125 + 2 = 5^3 - (-2) \Rightarrow 127|(5^3 - (-2)) \Rightarrow 5^3 \equiv -2(mod 127)$
$\Rightarrow (5^3)^7 \equiv (-2)^7 \equiv 126(mod 127).$
Portanto, o resto é 126. □

Lista de Exercícios 9.

(01) Responda e justifique:

(a) $23 \equiv 47(mod3)$?	(b) $-145 \equiv -12(mod7)$?
(c) $34508 \equiv 111(mod10)$	(d) $212 \equiv (-1)^9(mod3)$?
(e) $32768 \equiv 1906(mod13)$?	(f) $1234549 \equiv 3333333(mod1)$?
(g) $423 \equiv 326(mod(-6))$?	(h) $2^2+3^2+4^2+5^2 \equiv 16(mod4)$?

(02) Usando agora a Proposição 11, mostre que para quaisquer inteiros a, b e c são verdadeiras as propriedades:
(a) (C1): $a \equiv a(modm)$ (reflexiva);
(b) (C2): Se $a \equiv b(modm)$, então $b \equiv a(modm)$ (simétrica);
(c) (C3): Se $a \equiv b(modm)$ e $b \equiv c(modm)$, então $a \equiv c(modm)$ (transitiva).

(03) Quantos e quais elementos em $\{0, 1, 2, ..., 11\}$ são congruentes módulo 12 ao inteiro 8008? Justifique.

(04) Determine os elementos em $\{0, 1, 2, ..., 6\}$ que são congruentes módulo 7 ao inteiro 12^5? Justifique.

(05) Determine todos os possíveis valores para $x \in \mathbb{Z}$, que tornam verdadeira a congruência:
(a) $x \equiv 8(mod12)$;
(b) $x \equiv 25(mod7)$;
(c) $5 \equiv x(mod8)$;
(d) $2x \equiv 8(mod12)$;
(e) $5x \equiv 3x - 4(mod8)$;
(f) $7x + 2 \equiv 4x - 10(mod9)$;

(06) Determine todos os inteiros $m > 1$ para os quais temos:
(a) $186 \equiv 165(modm)$;
(b) $8012 \equiv 8056(modm)$;
(c) $3456 \equiv 2169(modm)$.

(07) Explique, usando linguagem natural, o que diz a propriedade (C4).

(08) Sejam m e k inteiros, com $m > 1$. Mostre, indicando as propriedades usadas, que se $3k + 5 \equiv 7k + 20(modm)$, então:
(a) $3k + 25 \equiv 7k + 40(modm)$;
(b) $4k \equiv -15(modm)$;
(c) $16k + 60 \equiv 0(modm)$.

(09) Sejam m e k inteiros, com $m > 1$. Mostre que se $9k + 6 \equiv k - 1(modm)$, então $3(3k^2 - k - 2) \equiv (k - 1)^2(modm)$.

(10) Mostre que se $40x \equiv 50y(mod8)$, então $120x \equiv 150y(mod8)$.

(11) Explique, em lingaguem natural, o que diz a propriedade (C5).

(12) Mostre que se $5k + 8 \equiv 6k + 18(mod 5)$, então $5k \equiv 6k + 10(mod 5)$.

(13) Mostre que $40x \equiv 50y(mod 8)$ se, e só se, $80x + 50y \equiv 40x + 100y(mod 8)$.

(14) Encontre 4 inteiros a, b, c e $m > 1$, para o quais temos $ac \equiv bc(mod m)$, porém $a \not\equiv b(mod m)$, mostrando assim que $ac \equiv bc(mod m) \nRightarrow a \equiv b(mod m)$.

(15) Encontre 4 inteiros a, b, c e $m > 1$, para o quais temos $ac \equiv bc(mod m)$ e cancelando c nessa congruência, vale $a \equiv b(mod m)$. Compare esse exemplo com o dado na questão anterior e diga que propriedade adicional ele tem, que torna, nesse caso, a implicação válida.

(16) Mostre que se $6x \equiv 10y(mod 7)$, então $3x \equiv 5y(mod 7)$.

(17) Mostre que se $-3x \equiv 6y(mod 8)$, então $x + 2y \equiv 0(mod 8)$.

(18) Sejam a e p inteiros para os quais temos $a + 4 \equiv (a - 2)^2(mod p)$. Mostre que se p é primo e $p \nmid a$, então $a \equiv 5(mod p)$.

(19) Usando propriedades de congruência, mostre que se $m|(a - b)$, então $m|(a^n - b^n)$, qualquer que seja o inteiro $n \geq 1$.

(20) Mostre que para qualquer inteiro $n \geq 1$, na divisão de 15^n por 8, os únicos restos são 1 e 7.

(21) Mostre que $21^n \equiv 6(mod 15)$ para todo inteiro $n \geq 1$.

(22) Determine o resto da divisão:
(a) 2^{1000} por 11;
(b) 7^{10} por 51;
(c) 4^{31} por 257;
(d) $(4^{18} + 5^{19} + 6^{20})$ por 7;
(e) $1 + 5 + 5^2 + 5^3 + 5^4 + ... + 5^{20}$ por 25;
(f) 23^{333333} por 26.

(23) Determine o algarismo das unidades do número 13^{211}.

(24) Mostre que para todo inteiro $n \geq 1$, $13^n \equiv (3r + 1)(mod 9)$, onde r é o resto da divisão de n por 3.

(25) Sejam a, b, m e n inteiros, com $m, n > 1$, sendo $a \equiv b(mod m)$ e $a \equiv b(mod n)$. Mostre que m e n são relativamente primos, então $a \equiv b(mod mn)$.

(26) (ENADE-2005) O mandato do reitor de uma universidade começa no dia 15 de novembro de 2005, uma segunda-feira, e terá a duração de exatamente quatro anos, sendo um deles bissexto. Determine o dia da semana que ocorrerá o último dia do mandato desse reitor.

Respostas da Lista de Exercícios 9

(03) Como $8008 = 12.667 + 4$, então $8008 \equiv 4(mod 12)$. Suponha agora que exista $s \in \{0, 1, 2, ...11\}$, tal que $8008 \equiv s(mod 12)$. Pela propriedades (C2) e (C3), temos $s \equiv 4(mod 12)$, como $s, 4 \in \{0, 1, ..., 11\}$, segue que $s = 4$. Portanto, 8008 é congruente módulo 12 a um único elemento desse conjunto, no caso, 4

(04) $12^5 \equiv 3(mod 7)$, pois 3 é o resto da divisão de 12^5 por 7.

(05.a) $x = 12k + 8$, $k \in \mathbb{Z}$; (05.b) $x = 7k + 4$, $k \in \mathbb{Z}$; (05.c) $x = 8k + 5$, $k \in \mathbb{Z}$;
(05.d) $x = 6k + 4$, $k \in \mathbb{Z}$; (05.e) $x = 4k + 2$, $k \in \mathbb{Z}$; (05.f) $x = 3k + 2$, $k \in \mathbb{Z}$.

(06.a) 3, 7 ou 21 (06.b) 2, 4, 11, 22 ou 44 (06.c) 3, 9, 11, 13, 33, 39, 99, 117, 143, 429, 1287

(16) $6x \equiv 10y(mod 7) \Rightarrow 2.3x \equiv 2.5y(mod 7)$, como $mdc(2, 7) = 1$, pela propriedade C6, podemos cancelar 2 nos dois lados da congruência, obtendo $3x \equiv 5y(mod 7)$.

(17) $-3x \equiv 6y(mod 8) \Rightarrow 3.(-x) \equiv 3.2y(mod 8)$
$\Rightarrow -x \equiv 2y(mod 8)$ - propriedade (C6), uma vez que $mdc(3, 8) = 1$
$\Rightarrow 0 \equiv x + 2y(mod 8)$ - propriedade (C4)
$\Rightarrow x + 2y \equiv 0(mod 8)$ - propriedade (C2).

(18) $a + 4 \equiv (a - 2)^2(mod p) \Rightarrow p|[(a + 4) - (a - 2)^2] \Rightarrow p|a.(-a + 5) \Rightarrow p|(-a + 5)$, já que $mdc(p, a) = 1$. Então $a \equiv 5(mod p)$.

(20) Temos que, $15 \equiv 7(mod 8)$ e $15^0 \equiv 15^2 \equiv 1(mod 8)$. Dado $n \geq 1$, sejam k e r, respectivamente, quociente e resto da divisão de n por 2, ou seja, $n = 2k + r$, com $r = 0$ ou $r = 1$. Então,

$$15^n = (15^2)^k.15^r \equiv 1^k.15^r \equiv 15^r \equiv \begin{cases} 1(mod 8), & \text{se} \quad r = 0 \\ 7(mod 8), & \text{se} \quad r = 1 \end{cases}$$

(21) Mostraremos por indução em n. Se $n = 1$, isso é verdadeiro, pois $15|(21 - 6)$. Suponha o resultado verdadeiro para $n \geq 1$. Então, temos $21 \equiv 6(mod 15)$ (caso $n = 1$) e $21^n \equiv 6(mod 15)$ (hipótese de indução). Aplicando a propriedade (C4) a essas duas congruências e posteriormente a transitividade obtemos: $21^n.21 \equiv 6^2 \equiv 6(mod 15) \Rightarrow 21^{n+1} \equiv 6(mod 15)$.

(22.a) 1 (22.b) 19 (*sugestão:* $51 : 7^2 + 2$) (22.c) 193 (*sugestão:* $257 : 4^4 + 1$)) (22.d) 0 (22.e) 6

(22.f) 25. Veja uma solução: $23 \equiv (-3)(mod 26) \Rightarrow 23^3 \equiv (-3)^3 \equiv -1(mod 26)$
$\Rightarrow (23^3)^{111111} \equiv (-1)^{111111}(mod 26) \Rightarrow 23^{333333} \equiv -1 \equiv 25(mod 26) \Rightarrow$ resto é 25.

(23) 7

(24) Para as primeiras 3 potências não negativas de 13, temos as congruências, em módulo 9:

$$13^r \equiv \begin{cases} 1 = 3.r + 1, & \text{se} \quad r = 0 \\ 4 = 3.r + 1, & \text{se} \quad r = 1 \\ 7 = 3.r + 1, & \text{se} \quad r = 2 \end{cases}$$

Dado um inteiro $n \geq 1$, sejam q e r, respectivmente o quociente e resto da divisão de n por 3. Então $n = 3q + r$, com com $r = 0, 1$ ou 2. Daí, $13^n = (13^3)^q.13^r \equiv 1^q.13^r(mod 9)$. Usando o resultado acima, temos $13^n \equiv (3r + 1)(mod 9)$.

(25) $a \equiv b(mod m)$ e $a \equiv b(mod n) \Rightarrow m|(a - b)$ e $n|(a - b) \Rightarrow \exists k_1, k_2 \in \mathbb{Z}$, tais que
$a - b = mk_1 = nk_2 \Rightarrow m|nk_2 \Rightarrow m|k_2$, pois $mdc(m, n) = 1$. Assim, $k_2 = mk$, $k \in \mathbb{Z}$
$\Rightarrow a - b = nk_2 = nm.k \Rightarrow nm|(a - b) \Rightarrow a \equiv b(mod mn)$.

(26) sábado.

Capítulo 10

Aplicações da Congruência em $\mathbb{Z}$

1 Introdução

Na resolução de alguns exercícios no capítulo anterior, vimos que dados inteiros a e $m > 1$, se existe um inteiro positivo k, tal que $a^k \equiv 1(modm)$, então para todo inteiro $n \geq 1$, se $n = kq + r$, com $0 \leq r < k$, segue das propriedades C8 e C4, que:

$$a^n = a^{kq+r} = (a^k)^q.a^r \equiv 1^q.a^r \equiv a^r(modm).$$

Resumindo,

$$\boxed{\begin{array}{l} \text{Se existe um inteiro } k \geq 1, \text{ tal} \\ \qquad\qquad a^k \equiv 1(modm), \\ \text{então para todo inteiro } n \geq 1, \text{ tem-se:} \\ \qquad\qquad a^n \equiv a^r(modm), \\ \text{onde } r \text{ é o resto da divisão de } n \text{ por } k. \end{array}} \tag{10.1}$$

Esse resultado, simplifica grandemente o cálculo do resto na divisão de potências. Uma vez, que conhecendo o resto da divisão de a^r por m, para $r = 0, 1, 2, ..(k-1)$, podemos determinar o resto da divisão de a^n por m, qualquer que seja o inteiro $n \geq 1$.

A questão é saber, se para quaisquer a e $m > 1$, sempre existe alguma potência positiva de a que deixa resto 1 na divisão por m? Caso afirmativo, como encontrar o expoente k? Neste capítulo, veremos alguns resultados nesse sentido, o Pequeno Teorema de Fermat e uma generalização desse, que é o Teorema de Euler. Veremos também o Teorema de Wilson, o qual nos fornece o resto para um tipo particular de divisão.

Para inteiros a e $m > 1$ arbitrários, comecemos supondo que exista um inteiro $k \geq 1$, tal que

$$a^k \equiv 1(mod m).$$

Isso implica que $m|(a^k - 1) \Rightarrow \exists s \in \mathbb{Z};\ \ a^k - 1 = ms$ e como $k \geq 1$, então

$$a^k - 1 = ms \Rightarrow a.a^{k-1} + m(-s) = 1 \Rightarrow mdc(a, m) = 1.$$

Portanto, $mdc(a, m) = 1$ é um condição necessária para a existência do expoente k. Temos assim, o seguinte resultado:

Proposição 12. *Dados inteiros $m > 1$ e a. Se existe um inteiro $k \geq 1$, tal que*

$$a^k \equiv 1(mod m),$$

então $mdc(a, m) = 1$.

Exemplos:
(01) Como $mdc(8, 10) \neq 1$, então $8^k \not\equiv 1(mod 10)$, qualquer que seja o inteiro $k \geq 1$, conforme já tínhamos deduzido no capítulo anterior;
(02) Como $mdc(27, 15) \neq 1$, não existe $k \geq 1$, tal que $27^k \equiv 1(mod 15)$.

O próximo passo é investigar se $mdc(a, m) = 1$ é também uma condição suficente para a existência do expoente k. Sabe-se que se p é um número primo e $p \nmid a$, então $mdc(p, a) = 1$. Iniciaremos nossa análise para inteiros relativamente primos, com essa particularidade.

Dados um inteiro a qualquer e um primo positivo p, denotaremos por $M(a, p)$ o conjunto dos primeiros $(p - 1)$ múltiplos positivos de a, isto é,

$$M(a, p) := \{na \mid n \in \mathbb{Z},\ 1 \leq n \leq p - 1\} = \{a, 2a, 3a, ..., (p - 1)a\}.$$

Exemplos:
(01) $M(2, 11) = \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20\}$;
(02) $M(25, 7) = \{25, 50, 75, 100, 125, 150\}$.

Façamos agora, algumas análises no conjunto $M(a, p)$, para esses dois exemplos particulares.

(01) $M(2, 11) = \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20\}$;
Dividindo cada elemento desse conjunto por $p = 11$, encontramos as seguintes congruências:

$$\begin{cases} 2 \equiv 2(mod11) \\ 4 \equiv 4(mod11) \\ 6 \equiv 6(mod11) \\ 8 \equiv 8(mod11) \\ 10 \equiv 10(mod11) \\ 12 \equiv 1(mod11) \\ 14 \equiv 3(mod11) \\ 16 \equiv 5(mod11) \\ 18 \equiv 7(mod11) \\ 20 \equiv 9(mod11) \end{cases}$$

Portanto, o conjunto dos restos das divisões dos elementos de $M(2,11)$ por 11 é $\{1,2,3,4,5,6,7,8,9,10\}$. Observe que, como os restos são todos distintos, segue da Definição 7, que quaisquer dois elementos distintos de $M(2,11)$ são incongruentes módulo 11. E observa-se também, que nenhum deles deixa resto 0 na divisão por 11. Aplicando agora repetidamente a propriedade C7 às congruências acima obtemos:

$$(2.4.6.8.10.12.14.16.18.20) \equiv (2.4.6.8.10.1.3.5.7.9)(mod11)$$

ou ainda,

$$(2.1).(2.2).(2.3).(2.4).(2.5).(2.6).(2.7).(2.8).(2.9).(2.10) \equiv (1.2.3.4.5.6.7.8.9.10)(mod11)$$

$$\Downarrow$$

$$(1.2.3.4.5.6.7.8.9.10).2^{10} \equiv (1.2.3.4.5.6.7.8.9.10)(mod11)$$

$$\Downarrow$$

$$10!.2^{10} \equiv 10!(mod11)$$

Como $mdc(10!,11) = 1$, pelo cancelamento da multiplicação na congruência (propriedade C6), obtemos a congruência:

$$2^{10} \equiv 1(mod11).$$

□

(02) $M(25,7) = \{25,50,75,100,125,150\}$:
Dividindo os elemento desse conjunto por $p = 7$, encontramos as seguintes congruências:

$$\begin{cases} 25 \equiv 4(mod7) \\ 50 \equiv 1(mod7) \\ 75 \equiv 5(mod7) \\ 100 \equiv 2(mod7) \\ 125 \equiv 6(mod7) \\ 150 \equiv 3(mod7) \end{cases}$$

Novamente, observa-se que os restos são todos distintos e nenhum deles é nulo, implicando que quaisquer dois elementos distintos de $M(25,7)$ são incongruentes módulo 7 e nenhum deles é divisível por 7. Como no exemplo anterior, multiplicando membro a membro todas as congruências acima (propriedade C7) obtemos:

$$25.50.75.100.125.150 \equiv 4.1.5.2.6.3(mod5)$$
$$\Downarrow$$
$$(1.2.3.4.5.6).25^6 \equiv 1.2.3.4.5.6.(mod7)$$
$$\Downarrow$$
$$6!.25^6 \equiv 6!(mod7)$$

Como $mdc(6!, 7) = 1$, pela propriedade C6, segue que:

$$25^6 \equiv 1(mod7).$$

□

Nos dois exemplos, obtivemos como resultado a mesma congruência:

$$a^{p-1} \equiv 1(modp).$$

A questão é: - Esse é um resultado geral? Ele vale sempre?

Vamos tentar generalizar o que foi feito nos exemplos acima, para inteiros arbitrários a e p, com $p > 1$ primo e $p \nmid a$, garantindo assim que $mdc(p, a) = 1$, conforme Proposição 7.

Tomando o conjunto dos primeiros $(p-1)$ múltiplos positivos de a:

$$M(a, p) = \{a, 2a, 3a, ..., (p-1)a\}$$

e dividindo cada um de seus elementos por p, obtemos as $(p-1)$ congruências:

$$\begin{cases} a \equiv r_1(modp) \\ 2a \equiv r_2(modp) \\ 3a \equiv r_3(modp) \\ ... \\ (p-1)a \equiv r_{p-1}(modp) \end{cases}$$

onde $r_1, r_2, ...r_{p-1}$ são os restos obtidos nas divisões. Aplicando agora repetidamente a propriedade C7 às congruências acima, segue que:

$$a.2a.3a...(p-1)a \equiv r_1.r_2.r_3....r_{p-1}(modp).$$
$$\Downarrow$$
$$(p-1)!.a^{p-1} \equiv r_1.r_2.r_3....r_{p-1}(modp). \tag{10.2}$$

No caso geral, não podemos precisar exatamente o valor de cada resto r_i. Sabemos apenas que $r_1, r_2, ...r_{p-1} \in R = \{0, 1, 2, ...p-1\}$. Como nos exemplos, são todos eles distintos?

Suponhamos que existam $n_i, n_j \in \{1, 2, ...p-1\}$, tais que $r_i = r_j$, então $n_i a \equiv n_j a(modp)$. Como $mdc(a, p) = 1$, pela propriedade C6,

$n_i \equiv n_j(modp) \Rightarrow n_i = n_j$. Logo, $r_1, r_2, ..., r_{p-1}$ são $(p-1)$ elementos distintos de R. Como R tem p elementos, a pergunta é: - que elemento de R não aparece entre os $(p-1)$ restos encontrados? Nos exemplos acima, vimos que nenhuma das potências deixou resto zero. No geral, suponhamos que exista $1 \leq n_j \leq (p-1)$, tal que:

$$n_j a \equiv 0(modp) \Rightarrow p|n_j a$$

Com $mdc(p, a) = 1 \Rightarrow p|n_j \Rightarrow p \leq n_j$, um absurdo. Então, $r_i \neq 0$, para todo i e assim, $r_1, r_2, ..., r_{p-1} \in \{1, 2, 3, ..., p-1\}$, sendo todos distintos. Portanto, $r_1 r_2 r_3 ... r_{p-1} = 1.2.3....(p-1) = (p-1)!$ e a identidade (10.2) fica:

$$(p-1)!.a^{p-1} \equiv (p-1)!(modp).$$

Como p é primo, $mdc((p-1)!, p) = 1$ (questão 15 do Capítulo 6). Logo, pela propriedade C6:

$$a^{p-1} \equiv 1(modp).$$

□

Com isso demonstramos o seguinte teorema:

Teorema 11. *(Pequeno Teorema de Fermat) Sejam a e p inteiros, com $p > 1$ primo. Se $p \nmid a$, então*

$$a^{p-1} \equiv 1(modp).$$

Exemplos:
(01) Como 13 é primo e $13 \nmid 8$, pelo Teorema de Fermat:

$$8^{12} \equiv 1(mod13).$$

Pela propriedade C8, para todo inteiro $q \geq 0$:

$$(8^{12})^q \equiv 1^q \Rightarrow 8^{12q} \equiv 1(mod13).$$

Assim, 8^{840}, 8^{636}, 8^{6000}, todos deixam resto 1 na divisão por 13.

(02) Como 23 é primo e $23 \nmid 2$, $2^{22} \equiv 1(mod23) \Rightarrow 2^{22q} \equiv 1(mod23)$, para todo inteiro $q \geq 0$.

Tomando a congruência do Teorema de Fermat e multiplicando ambos os lados por a (propriedade C4), obtemos:

$$a^p \equiv a(modp).$$

Essa congruência é também válida, mesmo que não tenhamos a condição $p \nmid a$, exigida no teorema, pois, se $p|a$, como $p > 1$, segue que $(a^{p-1} - 1) \in \mathbb{Z}$, assim $p|a(a^{p-1} - 1)$, e portanto,

$$a^p \equiv a(modp).$$

Asim, se $p|a$ ou se $p \nmid a$, sempre teremos a congruencia $a^p \equiv a(modp)$, desde que p seja primo. Enunciamos esse fato no corolário a seguir.

Corolário 6. *Sejam a e p inteiros, com $p > 1$ primo. Então*

$$a^p \equiv a(mod p).$$

Exemplos:
(01) Como 7 é primo, pelo corolário acima, $7|(23^7 - 23)$;
(02) Pelo Corolário 6, podemos afirmar que 43^{11} deixa resto 10 na divisão por 11. De fato, como 11 é primo, então $11|(43^{11} - 43) \Rightarrow \exists q \in \mathbb{Z}; 43^{11} - 43 = 11q$ $\Rightarrow 43^{11} = 11q + 43 = 11(q + 3) + 10$. Logo, 10 é o resto da divisão de 43^{11} por 11;
(03) 34^{17} deixa resto 0 na divisão por 17, pois $17|(34^{17} - 34) \Rightarrow \exists q \in \mathbb{Z};$ $34^{17} = 17q + 34 = 17(q + 2) + 0$.

✓ **Exercícios 24.**
(01) Determinar o resto da divisão de 2^{50} por 7.
Solução:
Como 7 é primo e $7 \nmid 2$, segue do teorema de Fermat, que $2^6 \equiv 1(mod 7)$
$\Rightarrow (2^6)^8 \equiv 1^8(mod 7) \Rightarrow 2^{48} \equiv 1(mod 7) \Rightarrow 2^{50} \equiv 2^2(mod 7) \Rightarrow 2^{50} \equiv 4(mod 7)$.
E como $4 \in \{0, 1, 2, ..., 6\}$, ele é o resto procurado. □

(02) Calcular o resto da divisão de 8^{92} por 19.
Solução:
Como 19 é primo e $19 \nmid 8$, pelo teorema de Fermat:

$$8^{18} \equiv 1(mod 19) \Rightarrow (8^{18})^5 \equiv 1^5(mod 7) \Rightarrow 8^{90}.8^2 \equiv 8^2 \equiv 7(mod 19).$$

Logo, 7 é o resto procurado. □

(03) Calcular o resto da divisão de 3^{1034^2} por 1033.
Solução:
Como 1033 é primo (verifique) e não divide 3, pelo teorema de Fermat:

$$3^{1032} \equiv 1(mod 1033) \Rightarrow 3^{1032q} \equiv 1(mod 1033), \forall q \in \mathbb{Z}_+.$$

Vejamos agora como relacionar o expoente 1034^2 dado na questão, com o expoente 1032 da congruência acima:

$$1034 \equiv 2(mod 1032) \Rightarrow 1034^2 \equiv 2^2(mod 1032) \Rightarrow 1034^2 = 1032q + 4, \quad \text{com} \quad q \in \mathbb{Z}.$$

Usando propriedades de potências, temos a igualdade:

$$3^{1034^2} = 3^{1032q+4} = 3^{1032q}.3^4$$

Como

$$3^4 \equiv 81(mod 1033)$$

Então,

$$3^{1034^2} = 3^{1032q}.3^4 \equiv 1.81 \equiv 81(mod 1033)$$

Portanto, o resto é 81. □

(04) Calcular o resto da divisão de 4^{61^5} por 59.
Solução:
59 é primo e não divide 4, logo, pelo teorema de Fermat:

$$4^{58} \equiv 1(mod 59) \Rightarrow 4^{58q} \equiv 1(mod 59), \forall q \in \mathbb{Z}_+.$$

Dividindo a base do expoente dado na questão pelo expoente acima temos:

$$61 \equiv 3(mod 58) \Rightarrow 61^5 \equiv 3^5 \equiv 11(mod 58) \Rightarrow 61^5 = 58q + 11,\ q \in \mathbb{Z}.$$

Usando as propriedades de potências e a congruência $4^{11} \equiv 53(mod 59)$, temos:

$$4^{61^5} = 4^{58q}.4^{11} \equiv 1.53 \equiv 53(mod 159).$$

Portanto, o resto é 53. □

2 Teorema de Euler

Na demonstração do Teorema de Fermat, mostramos essencialmente, que se $m > 1$ e a são inteiros **relativamente primos**, então temos a congruência:

$$(m-1)!.a^{m-1} \equiv (m-1)!.(mod m).$$

Se m é primo, segue que $mdc((m-1)!, m) = 1$, o que nos permite cancelar o fator comum e obter a congruência $a^{m-1} \equiv 1(mod m)$. Porém, se m é composto, então $mdc((m-1)!, m) \neq 1$. Nesse caso, para a aplicação da propriedade C6, precisamos eliminar do conjunto $M(a, m)$ os múltiplos na para os quais $mdc(n, m) \neq 1$. Assim, dado um inteiro $m > 1$, vamos considerar o conjunto:

$$A_m = \{n \in \mathbb{Z} \mid 1 \leq n \leq m \ \text{ e } \ mdc\{n, m\} = 1\}.$$

Suponhamos A_m com t elementos, digamos $A_m = \{n_1, n_2, ..., n_t\}$. No lugar de $M(a, m)$, consideraremos agora o conjunto:

$$\{na \mid n \in A_m\} = \{n_1a, n_2a, ..., n_ta\}.$$

Denotando por r_i o resto da divisão de n_ia por m, temos as t congruências:

$$\begin{cases} n_1a \equiv r_1(mod m) \\ n_2a \equiv r_2(mod m) \\ n_3a \equiv r_3(mod m) \\ ... \\ n_ta \equiv r_t(mod m) \end{cases}$$

E pela propriedade C7:

$$n_1n_2...n_t.a^t \equiv r_1r_2...r_t(mod m). \tag{10.3}$$

Como já mostrado anteriormente, se $mdc(a,m) = 1$, então os restos r_i são todos distintos e nenhum deles é nulo. Assim, para todo i,

$$r_i \in \{1, 2, ..., m-1\} \supset \{n_1, n_2, ..., n_t\}.$$

Para cada $i = 1, 2, ..., t$, seja $d_i = mdc(r_i, m)$. Então $d_i|r_i$ e $d_i|m \Rightarrow d_i|(mk + r_i)$, qualquer que seja $k \in \mathbb{Z}$. Em particular, se $n_i a = mq_i + r_i$, então $d_i|n_i a$. Assim, d_i é também um divisor comum de m e $n_i a$, consequentemente, $d_i|mdc(n_i a, m)$. Agora, pela definição de A_m e a hipótese, temos que:

$$mdc(n_i, m) = 1 = mdc(a, m) \Rightarrow mdc(n_i a, m) = 1.$$

Assim, $d_i|1 \Rightarrow d_i = 1 \Rightarrow r_i \in A_m$, para todo i. Portanto, $r_1 r_2 ... r_t = n_1 n_2 ... n_t$ e assim, (12.2) fica:

$$n_1 n_2 ... n_t . a^t \equiv n_1 n_2 ... n_t (mod n)$$

Como $mdc(n_i, m) = 1$, para todo $i = 1, 2, ..., t$, segue que $mdc(n_1 n_2 ... n_t, m) = 1$ e pela propriedade C6, obtemos a congruência:

$$a^t \equiv 1 (mod m),$$

onde t é número de elementos do conjunto A_m.

A função ϕ dada por:

$$\begin{aligned} \phi :\ & \mathbb{Z}_+^* \to \mathbb{Z}_+^* \\ & m \to \phi(m) := \# A_m. \end{aligned}$$

onde $\# A_m$ indica o número de elementos do conjunto A_m, é chamada *Função ϕ de Euler.*

Exemplos:

(01) Como $A_6 = \{n \in \mathbb{Z} \mid 1 \leq n \leq 6 \ \text{ e } mdc\{n, 6\} = 1\} = \{1, 5\}$, então $\phi(6) = \# A_6 = 2$;

(02) $\phi(9) = 6$, neste caso, $A_9 = \{1, 2, 4, 5, 7, 8\}$ e $\# A_9 = 6$;

(03) Se p é primo, então todo inteiro positivo menor que p é relativo com p, logo
$A_p = \{1, 2, 3, ...p - 1\}$ e portanto $\phi(p) = p - 1$.

Usando a função ϕ de Euler, vamos enunciar o que foi mostrado acima:

Teorema 12. *(Teorema de Euler) Sejam $m > 1$ e a inteiros. Se $mdc(a, m) = 1$, então*

$$a^{\phi(m)} \equiv 1 (mod m).$$

Exemplos:

(01) Como $mdc(25, 6) = 1$, então $25^{\phi(6)} \equiv 1 (mod 6)$, ou seja, $25^2 \equiv 1 (mod 6)$;

(02) Sendo $mdc(13, 9) = 1$, segue que, $13^{\phi(9)} \equiv 1 (mod 9) \Rightarrow 13^6 \equiv 1 (mod 9)$.

Se $m = p$ é primo e $p \nmid a$, então $mdc(a,p) = 1$, e pelo teorema de Euler,

$$a^{\phi(p)} \equiv 1(mod p) \Rightarrow a^{p-1} \equiv 1(mod p).$$

Assim, o teorema de Fermat é um caso particular do teorema de Euler. □

✓ **Exercícios 25.**

(01) Determine o resto da divisão de 4^{50} por 9.
Solução:
Aqui não podemos aplicar o Teorema de Fermat, pois 9 não é primo. Porém, como $mdc(4,9) = 1$, pelo Teorema de Euler,

$$4^{\phi(9)} \equiv 1(mod 9)$$

$$\Downarrow$$

$$4^6 \equiv 1(mod 9) \Rightarrow 4^{48} \equiv 1^8(mod 9) \Rightarrow 4^{50} \equiv 16 \equiv 7(mod 9).$$

Portanto, o resto é 7. □

(02) Determine o resto da divisão de 5^{3015^3} por 9.
Solução:
Como $mdc(5,9) = 1$, pelo Teorema de Euler:

$$5^{\phi(9)} \equiv 1(mod 9) \Rightarrow 5^6 \equiv 1(mod 9).$$

Relacionando 6 com o expoente 3015^3, temos:

$$3015 \equiv 3(mod 6) \Rightarrow 3015^3 \equiv 3^3 \equiv 3(mod 6) \Rightarrow 3015^3 = 6q + 3, q \in \mathbb{Z}$$

Então,

$$5^{3015^3} = 5^{6q+3} = 5^{6q}.5^3$$

Como $5^6 \equiv 1(mod 9) \Rightarrow 5^{6q} \equiv 1(mod 9)$ e $5^3 \equiv 8(mod 9)$, segue que:

$$5^{3015^3} = 5^{5q}.5^3 \equiv 1.8 \equiv 8(mod 9).$$

Portanto, o resto é 8. □

O Teorema de Euler mostra que vale a recíproca da Proposição 12. Juntando esses dois resultados temos:

Sejam $m > 1$ e a são inteiros arbitrários. Existe um inteiro $k \geq 1$, tal que: $$a^k \equiv 1(mod m) \quad \Leftrightarrow \quad mdc(a,m) = 1.$$

Com o Teorema de Fermat, podemos melhorar o resultado dado em (10.1):

Se
$$mdc(a, m) = 1$$
então para todo inteiro $n \geq 1$, tem-se:
$$a^n \equiv a^r (modm),$$
onde r é o resto da divisão de n por $\phi(m)$.

Exemplos:
(01) Como $mdc(9, 8) = 1$, então
$$8^{465} \equiv 8^3 \equiv 8(mod9),$$
já que $465 = \phi(9).77 + 3$.

(02) 14^{1045} deixa resto 4 na divisão por 5, uma vez que $mdc(14, 5) = 1$ e $1045 = \phi(5).261 + 1$, segue que $14^{1045} \equiv 14^1 \equiv 4(mod5)$.

3 Teorema de Wilson

Já vimos que se $p > 1$ é um número primo, então $p \nmid (p-1)!$. Logo, existem únicos inteiros q e r, tais que:
$$(p-1)! = pq + r$$
com $1 \leq r \leq p-1$. Vamos mostrar que nesse caso, qualquer que seja o primo p, o resto r é sempre o maior possível, isto é $r = (p-1)$.

Lema 3. *Seja $p > 1$ um número primo. Para todo $a \in A = \{1, 2, 3, ..., p-1\}$, existe $r \in A$, tal que:*
$$ar \equiv 1(modp).$$

Demonstração:
Como p é primo e $p \nmid a$, pois $a < p$, segue que $mdc(a, p) = 1 \Rightarrow \exists\, x, y \in \mathbb{Z}$, tais que
$$ax + py = 1.$$
Sejam q e r, respectivamente, o quociente e o resto da divisão de x por p. Então,
$$x = pq + r, \quad \text{com } 0 \leq r \leq p-1.$$
Portanto,
$$ar-1 = a(x-pq)-1 = (ax-1)-paq = p(-y-aq) \Rightarrow p|(ar-1) \Rightarrow ar \equiv 1(modp).$$
Resta mostrar que $r \in A$. Como $ax + py = 1 \Rightarrow mdc(p, x) = 1 \Rightarrow p \nmid x$, logo $1 \leq r \leq p-1 \Rightarrow r \in A$. $\square$

Exemplos:
(01) Pelo lema acima, para todo $a \in A = \{1, 2, 3, 4, 5, 6\}$ existe $r \in A$, tal que $ar \equiv 1(mod7)$. De fato, temos as 4 congruências:

$$1.1 \equiv 1(mod7), \quad 2.4 \equiv 1(mod7), \quad 3.5 \equiv 1(mod7) \text{ e } 6.6 \equiv 1(mod7);$$

(02) Para todo $a \in A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ existe $r \in A$, tal que $ar \equiv 1(mod11)$. Para encontrar $r \in A$, tal que $ar \equiv 1(mod11)$, podemos proceder como na demonstração do lema. Vejamos como exemplo, tomando $a = 7$.

Como $mdc(7, 11) = 1$, usando o algoritmo de Euclides, encontramos inteiros x e y, tais que $7x + 11y = 1$. Posteriormente divimos x por 11, sendo r o resto dessa divisão. Nesses caso, $7.(-3) + 11.2 = 1$ e como $-3 = 11.(-1) + 8$, segue que $r = 8$. Portanto, $7.8 \equiv 1(mod11)$. Procedendo dessa forma, encontramos as 6 congruências:

$$1.1 \equiv 1(mod11)$$
$$2.6 \equiv 1(mod11)$$
$$3.4 \equiv 1(mod11)$$
$$5.9 \equiv 1(mod11)$$
$$7.8 \equiv 1(mod11)$$
$$10.10 \equiv 1(mod11).$$

Nos dois exemplos acima, para $p = 7$ e $p = 11$, encontramos $r = a$, ou seja, ocorre a congruência $a^2 \equiv 1(modp)$, somente para $a = 1$ ou $a = p - 1$. O próximo lema afirma que esse é o caso geral.

Lema 4. *Sejam $p > 1$ um número primo. Se $a \in A = \{1, 2, 3, ..., p - 1\}$ é tal que:*

$$a^2 \equiv 1(modm),$$

então $a = 1$ ou $a = p - 1$.

Demonstração:
Suponha $1 \leq a \leq p - 1$, tal que $a^2 \equiv 1(modp) \Rightarrow p|(a^2 - 1)$ e como p é primo, segue que $p|(a-1)$ ou $p|(a+1)$. Agora, se $p|(a-1)$ e $a \neq 1$, então $p \leq a - 1 \leq p - 2$, um absurdo. Assim, nesse caso, $a = 1$. E se, $p|(a + 1)$, então $p \leq a + 1$. Por outro lado, como $1 \leq a \leq p - 1 \Rightarrow a + 1 \leq p \Rightarrow p = a + 1 \Rightarrow a = p - 1$. □

No geral, para um primo $p > 2$, temos as $\frac{1}{2}(p - 3)$ congruências

$$ar \equiv 1(modp)$$

com $a, r \in A' = \{2, 3, ..., p - 2\}$ e $a \neq r$.

Teorema 13. ***(Teorema de Wilson)*** *Se $p > 1$ é um número primo, então p divide $(p-1)! + 1$.*

Demonstração:
O resultado é obviamente verdadeiro para $p = 2$. Supondo $p \geq 3$, então pelos Lemas 3 e 4, para cada $a_i \in A' = \{2, 3, ..., p-2\}$, existe $r_i \in A'$, com $r_i \neq a_i$, tal $a_i r_i \equiv 1(modp)$. Assim, temos as $\frac{1}{2}(p-3)$ congruências:

$$a_1 r_1 \equiv 1(mop)$$

$$a_2 r_2 \equiv 1(mop)$$

$$...$$

$$a_{\frac{1}{2}(p-3)} r_{\frac{1}{2}(p-3)} \equiv 1(mop).$$

Multiplicando essas congruências obtemos:

$$2.3.4...(p-2) \equiv 1(modp).$$

Por outro lado, também temos a congruência elementar:

$$(p-1) \equiv (-1)(modp).$$

Multiplicando essas duas últimas congruencia, obtem-se:

$$2.3.4...(p-2)(p-1) \equiv (-1)(modp) \Rightarrow (p-1)! \equiv -1(modp) \Rightarrow p|\left((p-1)! + 1\right).$$

□

Corolário 7. *Se $p > 1$ é um número primo, então $(p-1)!$ deixa resto $(p-1)$ na divisão por p.*

Demonstração:
Pelo Teorema de Wilson, $p|((p-1)! + 1) \Rightarrow \exists q \in \mathbb{Z}$, tal que:

$$(p-1)! + 1 = pk \Rightarrow (p-1)! = pk - 1 + (p-p) = p(k-1) + (p-1).$$

Assim,

$$(p-1)! = pq + r,$$

onde $q = k - 1 \in \mathbb{Z}$ e $r = p - 1 \in \{0, 1, 2, ..., p-1\}$. Da unicidade do quociente e resto, segue que $r = (p-1)$ é o resto da divisão de $(p-1)!$ por p. □

Exemplo:
(01) Como 7 é primo, pelo Teorema de Wilson, sabemos que $7|(6! + 1)$;
(02) Como $(11! + 1) = 39916801 = 3326400 \times 12 + 1 \Rightarrow 12 \nmid (11! + 1)$, logo podemos usar o teorema anterior, para afirmar que 12 não é um número primo;
(03) Pelo Corolário 7, podemos afirmar que 12! deixa resto 12 na divisão por 13;
(04) Como 29 é primo, então 28! deixa resto 28 na divisão por 29.

Lista de Exercícios 10.

(01) Aplique o Teorema de Fermat para os pares de inteiros a e p abaixo:
(a) $a = 20$, $p = 7$;
(b) $a = 8$, $p = 11$;
(c) $a = 16$, $p = 47$.

(02) Calcule a imagem de cada inteiro abaixo pela função ϕ de Euler:
(a) $\phi(12)$;
(b) $\phi(15)$;
(c) $\phi(p^n)$, com p primo e $n \geq 1$ inteiro.

(03) Determine o resto da divisão de 5^{30} por 11.

(04) Determine o resto da divisão de 13^{111} por 11.

(05) (ENADE-2008) Determine o resto da divisão de 2^{333} por 23.

(06) Determine o resto da divisão de 8^{300} por 9.

(07) Determine o resto da divisão de 7^{105} por 12.

(08) Determine o resto da divisão de 14^{30} por 15.

(09) Determine o resto da divisão de 5^{303^5} por 7.

(10) Determine o resto da divisão de 8^{405^3} por 9.

(11) Determine o resto da divisão de 8^{20^6} por 15.

(12) Determine o resto da divisão de $9^{42^{42}}$ por 25.

(13) Determine o resto da divisão de $(1^7 + 2^7 + 3^7 + ... + 30^7)$ por 7.

(14) Determine o resto da divisão de $(1^6 + 2^6 + 3^6 + ... + 30^6)$ por 7.

(15) Determine o resto da divisão de $(1^{11} + 2^{11} + 3^{11} + ... + 50^{11})$ por 11.

(16) Determine o resto da divisão de $(1^{10} + 2^{10} + 3^{10} + ... + 50^{10})$ por 11.

(17) Determine o resto da divisão de $(2222^{5555} + 5555^{2222})$ por 7.

(18) Determine o algarismo das unidades do número $9^{55^{77}}$.

(19) Mostre que se $p > 1$ é primo, então $(p-1)! \equiv (p-1)(mod p)$.

(20) Mostre que se $p \geq 3$ é um número primo, então $p|((p-2)! - 1)$.

Respostas da Lista de Exercícios 10
(01.a) $20^6 \equiv 1(mod 7)$ (01.b) $8^{10} \equiv 1(mod 11)$ (01.c) $16^{46} \equiv 1(mod 47)$.
(02.a) $\phi(12) = 4$ (02.b) $\phi(15) = 8$ (02.c) $\phi(p^n) = p^{n-1}(p-1)$.
(03) 1
(04) 2
(05) 16
(06) 1
(07) 7
(08) 1
(09) 6
(10) 8
(11) 1
(12) 11
(13) 3
(14) 5
(15) 10
(16) 4
(17) 0
(18) 9

Capítulo 11

O Anel $\mathbb{Z}_m$

1 Inteiros Módulo m

Lembremos que dado um inteiro $m > 1$, definimos em $\mathbb{Z}$ a seguinte relação:

$$a \equiv b(modm) \Leftrightarrow m \mid (a - b),$$

a qual é chamada **Relação de Congruência Módulo** m. Essa relação, conforme visto, tem as seguinte propriedades , para quaisquer $a, b, c \in \mathbb{Z}$:
(i) Reflexiva:

$$a \equiv a(modm);$$

(ii) Simétrica:

$$\text{Se } a \equiv b(modm), \text{ então } b \equiv a(modm);$$

(iii) Transitiva:

$$\text{Se } a \equiv b(modm) \text{ e } b \equiv c(modm), \text{ então } a \equiv c(modm).$$

Por possuir essas três propriedades, diz-se que a relação de congruência módulo m é uma **relação de equivalência** no conjunto $\mathbb{Z}$.

2 Classes de Congruência

Para cada $a \in \mathbb{Z}$, o conjuntos dos inteiros congruentes a a módulo m, é chamado a **classe de equivalência de** a **pela relação de congruência módulo** m e denotado por $\overline{a}$. Assim, por definição,

$$\overline{a} := \{b \in \mathbb{Z} \mid b \equiv a(modm)\}.$$

Observe que:

$$b \in \overline{a} \Rightarrow b \equiv a(modm) \Rightarrow m \mid (b-a) \Rightarrow b-a = mk, \Rightarrow b = mk+a, \text{ com } k \in \mathbb{Z}.$$

Reciprocamente, se existe $k \in \mathbb{Z}$, tal que:

$$b = mk + a \Rightarrow m \mid (b - a) \Rightarrow b \equiv a(modm) \Rightarrow b \in \overline{a}.$$

Desta forma, podemos descrever precisamente os elementos da classe $\overline{a}$:

$$\boxed{\overline{a} = \{mk + a \mid k \in \mathbb{Z}\}}$$

Cada elemento do conjunto $\overline{a}$ é dito um *representante da classe* $\overline{a}$.

Exemplos:
(01) Na relação de congruência módulo 3, as classes $\overline{0}$, $\overline{1}$ e $\overline{-5}$ são:
$\overline{0} = \{3k + 0 \mid k \in \mathbb{Z}\} = \{..., -6, -3, 0, 3, 6, ...\}$, que é o conjunto dos inteiros que deixam resto 0 na divisião por 3. Os números -6, 0, 21 são alguns representantes da classe $\overline{0}$;
$\overline{1} = \{3k + 1 \mid k \in \mathbb{Z}\} = \{..., -5, -2, 1, 4, 7, ...\}$, que é o conjunto dos inteiros que deixam resto 1 na divisão por 3. Os inteiros -11, 1, 22, 253, elementos desse conjunto, são alguns representantes dessa classe;
$\overline{-5} = \{3k + (-5) \mid k \in \mathbb{Z}\} = \{3(k - 2) + 1 \mid k \in \mathbb{Z}\} = \{3k_1 + 1 \mid k_1 \in \mathbb{Z}\}$, que também é o conjunto dos inteiros que deixam resto 1 na divisão por 3, logo $\overline{-5} = \overline{1}$, em módulo 3.

(02) Na relação $\equiv (mod5)$, as classes $\overline{0}$, $\overline{1}$ e $\overline{-5}$ são:
$\overline{0} = \{5k + 0 \mid k \in \mathbb{Z}\} = \{..., -10, -5, 0, 5, 10, ...\}$, o qual é o conjunto dos inteiros que deixam resto 0 na divisião por 5;
$\overline{1} = \{5k + 1 \mid k \in \mathbb{Z}\} = \{..., -9, -4, 1, 6, 11, ...\}$ é o conjunto inteiros que deixam resto 1 na divisão por 5;
$\overline{-5} = \{5k + (-5) \mid k \in \mathbb{Z}\} = \{5(k - 1) \mid k \in \mathbb{Z}\} = \{5k_1 + 0 \mid k_1 \in \mathbb{Z}\} = \overline{0}$. Portanto, $\overline{-5} = \overline{0}$, em módulo 5.

3 Propriedades das Classes de Equivalência

Os exemplos acima, mostram que inteiros distintos podem produzir a mesma classe de equivalência. A próxima proposição dá a condição para que ocorra a igualdade das classes.

Proposição 13. *Seja $m > 1$ um inteiro. Para quaisquer inteiros a e b tem-se:*

$$\overline{a} = \overline{b} \Leftrightarrow a \equiv b(modm).$$

Demonstração:
$(\Rightarrow)$ $\overline{a} = \overline{b} \Rightarrow a \equiv b(modm)$:
Da reflexividade da relação de congruência e da hipótese, segue que:
$a \equiv a(modm) \Rightarrow a \in \overline{a} = \overline{b}$. Da definição de $\overline{b}$, segue que $a \equiv b(modm)$.

($\Leftarrow$) $a \equiv b(mod m) \Rightarrow \overline{a} = \overline{b}$.
Seja $x \in \overline{a} \Rightarrow x \equiv a(mod m)$. Como por hipótese $a \equiv b(mod m)$, usando a transitividade da relação, segue que $x \equiv b(mod m) \Rightarrow x \in \overline{b} \Rightarrow \overline{a} \subset \overline{b}$.
De modo, análogo, mostra-se que $\overline{b} \subset \overline{a}$. Portanto, temos a igualdade $\overline{a} = \overline{b}$. $\square$

Exemplos:
(01) Como $843 \equiv 10(mod 7)$, segue que $\overline{843} = \overline{10}$, em módulo 7;
(02) Como $912 \equiv 282 \equiv 147 \equiv 3 \equiv (-6)(mod 9)$, temos, em módulo 9, a igualdade das classes $\overline{912} = \overline{282} = \overline{147} = \overline{3} = \overline{-6}$. Observe que os representantes de todas essas classses deixam o mesmo resto na divisão por 9, uma vez que estão relacionados pela relação de congruência módulo 9;
(03) Na divisão por 2, só temos dois restos possíveis, então para todo $a \in \mathbb{Z}$, temos que $a \equiv 0(mod 2) \Rightarrow \overline{a} = \overline{0}$ ou $a \equiv 1(mod 2) \Rightarrow \overline{a} = \overline{1}$. Assim, em módulo 2, só temos duas classes distintas, $\overline{0}$ e $\overline{1}$.

Para as classes dadas no exemplos acima, não encontramos nenhum inteiro que pertença simultaneamente a mais de uma classe. Vejamos se esse é o caso geral.

Dadas $\overline{a}$ e $\overline{b}$, classes **distintas** em módulo m, suponha existir $x \in \mathbb{Z}$ que pertença simultaneamente a $\overline{a}$ e $\overline{b}$. Se $x \in \overline{a} \cap \overline{b}$, então $x \in \overline{a} \Rightarrow x \equiv a(mod m)$ e pela Proposição 13, $\overline{x} = \overline{a}$. Analogamente, se $x \in \overline{b} \Rightarrow \overline{x} = \overline{b}$ e portanto, $\overline{a} = \overline{b}$, contrariando a suposição das classes serem distintas. Assim, uma consequência da proposição anterior é que classes distintas, não tem elementos comuns. Temos assim, o seguinte corolário:

Corolário 8. *Sejam $m > 1$ um inteiro. Em módulo m, para quaisquer $a, b \in \mathbb{Z}$ tem-se que:*

$$\overline{a} \neq \overline{b} \Rightarrow \overline{a} \cap \overline{b} = \emptyset.$$

Exemplos:
(01) Como $14 \not\equiv 3(mod 7)$, segue que, em módulo 7, $\overline{14} \neq \overline{3}$. Então, pelo corolário acima, essas duas classes são disjuntas, isto é, $\overline{14} \cap \overline{3} = \emptyset$;
(02) Em módulo 5, $\overline{22}$ e $\overline{16}$ são classes distintas, uma vez que $22 \not\equiv 16(mod 5)$. Assim, pelo Corolário 8, $\overline{22} \cap \overline{16} = \emptyset$. De fato, se $x \in \overline{22}$, então x deixa resto 2 na divisão por 5; se $x \in \overline{16}$, x deixa resto 1 na divisão por 5. Da unidade do resto, segue que não existe $x \in \overline{22} \cap \overline{16}$.

4 Conjunto das Classes Residuais

Dado um inteiro $m > 1$, denota-se por $\mathbb{Z}_m$ o conjunto das classes de equivalência módulo m, isto é,

$$\mathbb{Z}_m := \{\overline{a} \mid a \in \mathbb{Z}\}.$$

O conjunto $\mathbb{Z}_m$ é chamado conjunto das **Classes Residuais Módulo** m.

Por definição,

$$\mathbb{Z}_m = \{..., \overline{-3}, \overline{-2}, \overline{-1}, \overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}, \overline{m}, \overline{m+1}, ...\}$$

Mas, já vimos que inteiros distintos podem produzir a mesma classe, desde que estejam relacionados. Portanto, nem todos os elementos do conjunto acima são distintos. A questão é: - Quantas são as classes de equivalências distintas em $\mathbb{Z}_m$?

A resposta segue dos resultados abaixo, vistos Capítulo 9, sobre o conjunto $R = \{0, 1, ..., m-1\}$:

(i) Todo inteiro é congruente a único elemento de R, no caso, o seu resto na divisão m, Assim, para todo $a \in \mathbb{Z}$, existe $r \in R$, tal que $a \equiv r(modm)$ $\Rightarrow \overline{a} = \overline{r} \Rightarrow \mathbb{Z}_m \subset \{\overline{0}, \overline{1}, ..., \overline{m-1}\}$;

(ii) Quaisquer dois elementos distintos de R são incongruentes módulo m. Então, pela Proposição 13, as classes do conjunto $\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$ são todas distintas, ou seja, esse conjunto tem exatamente m elementos distintos.

Com esses dois resultados podemos descrever exatamente o conjunto $\mathbb{Z}_m$, conforme proposição abaixo.

Proposição 14. *Para cada inteiro $m > 1$,*

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, ...\overline{m-1}\},$$

o qual tem exatamente m elementos distintos.

Demonstração:
Por definição,

$$\mathbb{Z}_m = \{\overline{a} \mid a \in \mathbb{Z}\} = \{..., \overline{-3}, \overline{-2}, \overline{-1}, \overline{0}, \overline{1}, ..., \overline{m-1}, \overline{m}, \overline{m+1}, ...\}.$$

Já mostramos que $\mathbb{Z}_m \subset \{\overline{0}, \overline{1}, ..., \overline{m-1}\}$. A outra inclusao é imediata. Assim, temos a igualdade:

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, ...\overline{m-1}\},$$

e conforme item (ii) acima, $\mathbb{Z}_m$ tem exatamente m elementos distintos. □

Exemplos:
(01) $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$;
(02) $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$;
(03) $\mathbb{Z}_{12} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{10}, \overline{11}\}$.

Resumindo, dado $m > 1$, toda classe residual módulo m é um subconjunto não vazio de $\mathbb{Z}$ e para cada $a \in \mathbb{Z}$, existe um único inteiro r, com $0 \leq r \leq m-1$, tal que $a \in \overline{r}$. Dizemos assim, que $\mathbb{Z}_m$ é uma partição de $\mathbb{Z}$, ou seja,

$$\boxed{\mathbb{Z} = \overline{0} \cup \overline{1} \cup ... \cup \overline{(m-1)}}$$

sendo essa união disjunta, isto é, para quaisquer $0 < r_i \neq r_j < m$, $\overline{r_i} \cap \overline{r_j} = \emptyset$.

✓ **Exercícios 26.**

(01) Determine $\mathbb{Z}_6$ e descreva a classe $\overline{3}$.
Solução:
Pela Proposição 14,

$$\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\},$$

sendo $\overline{3} = \{6k + 3 \mid k \in \mathbb{Z}\} = \{..., -15, -9, -3, 3, 9, 15, ...\}$. □

(02) Determine $\mathbb{Z}_{11}$ e descreva as classes $\overline{3}$ e $\overline{7}$.

(03) Encontre o único representante r da classe $\overline{36} \in \mathbb{Z}_9$, com $0 \leq r \leq 8$.
Solução:
Dividindo 36 por 9 obtemos $36 = 4.9 + 0 \Rightarrow 4|(36 - 0) \Rightarrow 36 \equiv 0(mod 9) \Rightarrow \overline{36} = \overline{0}$. Assim, $r = 0$ é o representante da classe $\overline{36}$ no intervalo pedido. □

(04) Encontre o único representante r da classe $\overline{-316} \in \mathbb{Z}_{13}$, com $0 \leq r \leq 12$.
Solução:
Dividindo -316 por 13 obtemos $-316 = -25.13 + 9 \Rightarrow 13|(-316 - 9)$
$\Rightarrow -316 \equiv 9(mod 13) \Rightarrow \overline{-316} = \overline{9}$. Assim, $r = 9$ é o representante da classe $\overline{-316}$ no intervalo pedido. □

(05) Encontre o representante r da classe $\overline{29} \in \mathbb{Z}_{10}$, com $0 \leq r \leq 9$.
(06) Encontre o representante r da classe $\overline{-414} \in \mathbb{Z}_{16}$, com $0 \leq r \leq 15$.
(07) Generalizando, dado $a \in \mathbb{Z}$ arbitrário, descreva um procedimento para encontrar o único representante r de $\overline{a} \in \mathbb{Z}_m$, com $0 \leq r \leq m - 1$.
Solução:
Dividindo a por m, encontramos q e r, tais que $a = mq + r$, com $0 \leq r \leq m - 1$. Daí, $m|(a - r) \Rightarrow a \equiv r(modm) \Rightarrow \overline{a} = \overline{r}$. Portanto, o representante no intervalo pedido, é exatamente o resto da divisão euclidiana de a por m. □

5 Operações em $\mathbb{Z}_m$

Definiremos agora uma adição e uma multiplicação em $\mathbb{Z}_m$, dando assim, ao conjunto das classes residuais uma estrutura de anel, com propriedades análogas as do anel $\mathbb{Z}$

.

Dadas $\overline{a}, \overline{b} \in \mathbb{Z}_m$ definimos:

(I) **Adição:**

$$\overline{a} + \overline{b} := \overline{a + b}$$

(II) **Multiplicação:**

$$\overline{a}.\overline{b} := \overline{a.b}$$

✓ **Exercícios 27.**
(01) Usando as definições acima, efetue as operações no conjunto indicado:
Em $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, ..., \overline{6}\}$:
(a) $\overline{2} + \overline{3}$;
Solução:
Pela definição, $\overline{2} + \overline{3} = \overline{2+3} = \overline{5}$. $\square$
(b) $\overline{2}.\overline{3}$;
Solução:
$\overline{2}.\overline{3} = \overline{2.3} = \overline{6}$;
(c) $\overline{3} + \overline{5}$
Solução:
$\overline{3} + \overline{5} = \overline{3+5} = \overline{8} = \overline{1}$; $\square$
(d) $\overline{3}.\overline{5}$;
Solução:
$\overline{3}.\overline{5} = \overline{3.5} = \overline{15} = \overline{1}$. $\square$
(e) $\overline{4} + \overline{5}$;
(f) $\overline{4}.\overline{5}$;

(02) Em $\mathbb{Z}_{12} = \{\overline{0}, \overline{1}, ..., \overline{11}\}$:
(a) $\overline{2} + \overline{3}$;
Solução:
$\overline{2} + \overline{3} = \overline{2+3} = \overline{5}$. $\square$
(b) $\overline{2}.\overline{3}$;
Solução:
$\overline{2}.\overline{3} = \overline{2.3} = \overline{6}$. $\square$
(c) $\overline{3} + \overline{5}$;
Solução:
$\overline{3} + \overline{5} = \overline{3+5} = \overline{8}$;
(d) $\overline{3}.\overline{5}$;
Solução:
$\overline{3}.\overline{5} = \overline{3.5} = \overline{15} = \overline{3}$. $\square$
(e) $\overline{17} + \overline{18}$;
(f) $\overline{17}.\overline{18}$.

(03) Descreva o procedimento usado para efetuarmos a soma $\overline{a} + \overline{b}$ e o produto $\overline{a}.\overline{b}$ em $\mathbb{Z}_m$.

Para efetuarmos a soma de duas classes residuais, tomamos um representante de cada uma das parcelas (que são números inteiros), somamos em $\mathbb{Z}$ esses representantes e então determinamos a classe residual do inteiro resultante. Procedimento analógo ocorre com a multiplicação. Cabe aqui uma pergunta: - Como essas operações são feitas usando representantes das classes, o resultado será o mesmo quaisquer que sejam os representantes escolhidos para as classes? Por exemplo, em $\mathbb{Z}_{12}$, $\overline{5} = \overline{17}$ e $\overline{6} = \overline{18}$. Daí, $\overline{5} + \overline{6} = \overline{17} + \overline{18}$?

A próxima proposição mostra que as operações acima estão bem definidas, isto é, independem do representante escolhido para a classe.

Proposição 15. *Sejam* $\overline{a_1}, \overline{b_1}, \overline{a_2}, \overline{b_2} \in \mathbb{Z}_m$. *Se*

$$\overline{a_1} = \overline{a_2} \quad e \quad \overline{b_1} = \overline{b_2},$$

então
(i) $\overline{a_1} + \overline{b_1} = \overline{a_2} + \overline{b_2}$;
(ii) $\overline{a_1}.\overline{b_1} = \overline{a_2}.\overline{b_2}$.

Demonstração:
Como $\overline{a_1} = \overline{a_2}$ e $\overline{b_1} = \overline{b_2}$, pela Proposição 13,

$$a_1 \equiv a_2 (mod m) \quad \text{e} \quad b_1 \equiv b_2 (mod m).$$

Usando a propriedade C7 de congruências e a Proposição 13, temos:
(i) $a_1 + b_1 \equiv a_2 + b_2 (mod m) \Rightarrow \overline{a_1 + b_1} = \overline{a_2 + b_2} \Rightarrow \overline{a_1} + \overline{b_1} = \overline{a_2} + \overline{b_2}$ e
(ii) $a_1.b_1 \equiv a_2.b_2 (mod m) \Rightarrow \overline{a_1.b_1} = \overline{a_2.b_2} \Rightarrow \overline{a_1}.\overline{b_1} = \overline{a_2}.\overline{b_2}$. $\square$

Exemplos: Abaixo, as tábuas da adição e multiplicação de $\mathbb{Z}_6$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$.$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

6 Propriedades das Operações em $\mathbb{Z}_m$

A adição e a multiplicação definidas em $\mathbb{Z}_m$ tem as seguintes propriedades (compare com as propriedades das operações em $\mathbb{Z}$, vistas no Capítulo 1):

Propriedades da Adição

(A1) **Associatividade:**
para quaisquer $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$, tem-se:

$$(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c}).$$

Demonstração:
Sejam $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$. Então

$$\begin{aligned}
(\overline{a}+\overline{b})+\overline{c} &= \overline{a+b}+\overline{c} && \text{- definição da soma em } \mathbb{Z}_m\\
&= \overline{(a+b)+c} && \text{- definição da soma em } \mathbb{Z}_m;\\
&= \overline{a+(b+c)} && \text{- pela associatividade da soma em } \mathbb{Z};\\
&= \overline{a}+\overline{b+c} && \text{- definição da soma em } \mathbb{Z}_m;\\
&= \overline{a}+(\overline{b}+\overline{c}) && \text{- definição da soma em } \mathbb{Z}_m.
\end{aligned}$$

Portanto, $(\overline{a}+\overline{b})+\overline{c}=\overline{a}+(\overline{b}+\overline{c})$. □

(A2) **Comutatividade**

$$\overline{a}+\overline{b}=\overline{b}+\overline{a},$$

para quaisquer $\overline{a},\overline{b}\in\mathbb{Z}_m$.

(A3) **Existência do elemento neutro**:
A classe $\overline{0}$ é o elemento neutro da adição, isto é, para todo $\overline{a}\in\mathbb{Z}_m$, tem-se:

$$\overline{a}+\overline{0}=\overline{a}.$$

(A4) **Existência do oposto**:
Para todo $\overline{a}\in\mathbb{Z}_m$ existe $\overline{b}\in\mathbb{Z}_m$, tal que:

$$\overline{a}+\overline{b}=\overline{0}.$$

O elemento $\overline{b}$ é chamado o oposto (ou inverso aditivo) de $\overline{a}$ e será denotado por $-\overline{a}$.

Propriedades da Multiplicação:

(M1) **Associatividade**:

$$(\overline{a}.\overline{b}).\overline{c}=\overline{a}.(\overline{b}.\overline{c}),$$

para quaisquer $\overline{a},\overline{b},\overline{c}\in\mathbb{Z}_m$;

(M2) **Comutatividade**:
A multiplicação é comutativa, isto é, para quaisquer $\overline{a},\overline{b}\in\mathbb{Z}_m$ tem-se:

$$\overline{a}.\overline{b}=\overline{b}.\overline{a}.$$

(M2) **Existência do elemento unidade:**
A classe $\overline{1}$ é o elemento neutro da multiplicação, - chamado elemento unidade - isto é, para todo $\overline{a}\in\mathbb{Z}_m$:

$$\overline{a}.\overline{1}=\overline{a}.$$

Além disso, vale a propriedade distributiva que relaciona as duas operações.

(D1) **Distributividade da multiplicação em relação à adição:**

$$\overline{a}.(\overline{b}+\overline{c}) = \overline{a}.\overline{b}+\overline{a}.\overline{c},$$

para quaisquer $\overline{a}, \overline{b}$ e $\overline{c} \in \mathbb{Z}_m$.

Por possuir essas oito propriedades dizemos que $(\mathbb{Z}_m, +, .)$ é um **anel comutativo com elemento unidade**.

✓ **Exercícios 28.**

(01) Faça a demonstração de todas as propriedades acima.

(02) Determine o oposto de $\overline{3}$ em $\mathbb{Z}_5$;

Solução:

Como $\overline{3}+\overline{2}=\overline{5}=\overline{0}$, então $-\overline{3}=\overline{2}$. □

(03) Determine o oposto de $\overline{3}$ em $\mathbb{Z}_8$.

Solução:

Como $\overline{3}+\overline{5}=\overline{8}=\overline{0} \Rightarrow -\overline{3}=\overline{5}$. □

(04) Determine um representate r do oposto de $\overline{16} \in \mathbb{Z}_{10}$, com $0 \leq r \leq 9$.

Solução:

Como $\overline{16}+\overline{-16} = \overline{0} \Rightarrow -(\overline{16}) = \overline{(-16)}$, ou seja, -16 é um representante da classe oposta. Para encontrar um representante desta classe no intervalo pedido, basta dividir -16 por 10 e tomar o resto como representante: $-16 = 10.(-2)+4 \Rightarrow -(\overline{16}) = \overline{(-16)} = \overline{4}$. □

(05) Dado $\overline{a} \in \mathbb{Z}_m$, descreva um procedimento para encontrar o representante r classe oposta $-\overline{a}$, com $0 \leq r \leq m-1$.

Solução:

Como $\overline{a}+(\overline{-a}) = \overline{a-a} = \overline{0}$, então dada $\overline{a} \in \mathbb{Z}_m$, $-a$ é sempre um representante da classe oposta $-\overline{a}$. Para encontrar um representante r desta classe, com $0 \leq r \leq m-1$, procedemos como descrito no exercício anterior, dividindo $-a$ por m e tomando a classe determinadada pelo resto. Por exemplo, claramente temos que -20 é um representante da classe $-\overline{20} \in \mathbb{Z}_8$. Para encontrar um respresentante desta classe no intervalo pedido, dividindos -20 por 8 e tomamos o resto: $-20 = -3.8+4 \Rightarrow -\overline{20} = \overline{-20} = \overline{4}$ e de fato, $\overline{20}+\overline{4} = \overline{24} = \overline{0}$, em $\mathbb{Z}_8$.□

(06) Resolva em $\mathbb{Z}_5$ as equações:

(a) $\overline{2}+x = \overline{3}.\overline{4}$;

Solução:

$\overline{2}+x = \overline{3}.\overline{4} \Rightarrow \overline{2}+x = \overline{12} = \overline{2} \Rightarrow \overline{3}+(\overline{2}+x) = \overline{3}+\overline{2} \Rightarrow x = \overline{0}$. □

(b) $\overline{2}.x = \overline{3}+\overline{4}$.

Solução:

$\overline{2}.x = \overline{3}+\overline{4} \Rightarrow \overline{2}.x = \overline{2} \Rightarrow \overline{3}.\overline{2}.x = \overline{3}.\overline{2} \Rightarrow \overline{6}.x = \overline{6} = \overline{1} \Rightarrow x = \overline{1}$. □

(07) Resolva em $\mathbb{Z}_7$ as equações:

(a) $\overline{2}+x = \overline{3}.\overline{4}$;

(b) $\overline{2}.x = \overline{3}+\overline{4}$.

7 Elementos Inversíveis em $\mathbb{Z}_m$

Definição 8. *Um elemento* $\overline{a} \in \mathbb{Z}_m$ *diz-se inversível (para a multiplicação) se existe* $\overline{b} \in \mathbb{Z}_m$*, tal que* $\overline{a}.\overline{b} = \overline{1}$*.*

O elemento $\overline{b}$, citado na definição acima, é chamado o inverso (multiplicativo) de $\overline{a}$ e denotado por $(\overline{a})^{-1}$.

Exemplos:
(01) $\overline{3}$ é inversível em $\mathbb{Z}_5$ tendo como inverso $\overline{2}$, pois $\overline{3}.\overline{2} = \overline{1}$;
(02) $\overline{3}$ é inversível em $\mathbb{Z}_8$, pois $\overline{3}.\overline{3} = \overline{1}$;
(03) $\overline{4}$ não é inversível em $\mathbb{Z}_6$, pois $\overline{4}.\overline{b} \neq \overline{1}$, qualquer que seja $\overline{b} \in \mathbb{Z}_6$.

A próxima proposição identifica os elementos não nulos que são inversíveis em $\mathbb{Z}_m$.

Proposição 16. *Um elemento* $\overline{0} \neq \overline{a} \in \mathbb{Z}_m$ *é inversível se, e somente se,* $mdc(a, m) = 1$*.*

Demonstração:
$(\Rightarrow)$ $mdc(a, m) = 1 \Rightarrow \overline{a}$ é inversível:
$mdc(a, m) = 1 \Rightarrow$ existem inteiros r e s, tais que:
$ar + ms = 1 \Rightarrow \overline{ar + ms} = \overline{1} \Rightarrow \overline{a}.\overline{r} + \overline{m}.\overline{s} = \overline{1} \Rightarrow \overline{a}.\overline{r} + \overline{0}.\overline{s} = \overline{1} \Rightarrow \overline{a}.\overline{r} = \overline{1}$
$\Rightarrow \overline{r}$ é o inverso de $\overline{a}$, o qual é portanto inversível.

$(\Leftarrow)$ $\overline{a}$ é inversível $\Rightarrow mdc(a, m) = 1$:
$\overline{a}$ é inversível $\Rightarrow$ existe $\overline{b} \in \mathbb{Z}_m$ tal que:
$\overline{a}.\overline{b} = \overline{1} \Rightarrow \overline{ab} = \overline{1} \Rightarrow ab \equiv 1(mod m) \Rightarrow m \mid (ab - 1) \Rightarrow$ existe $k \in \mathbb{Z}$, tal que $ab - 1 = mk \Rightarrow ab + m(-k) = 1 \Rightarrow mdc(a, m) = 1$. □

Se p é um primo positivo, para todo $0 < a < p$, tem-se que $mdc(a, p)$, então temos o corolário abaixo.

Corolário 9. *Seja* p *um número primo positivo. Então todos os elementos não nulos de* $\mathbb{Z}_p$ *são inversíveis.*

Exemplos:
(01) Em $\mathbb{Z}_8 = \{\overline{0}, \overline{1}, ..., \overline{7}\}$, a classe $\overline{5}$ é inversível, pois $mdc(5, 8) = 1$. Para encontrar o inverso de $\overline{5}$, determinamos inteiros r e s, tais que $5r + 8s = 1$, sendo então $(\overline{5})^{-1} = \overline{r}$. Como

$$5.(-3) + 8.2 = 1 \Rightarrow \overline{5}.\overline{(-3)} + \overline{8}.\overline{2} = \overline{1} \Rightarrow \overline{5}.\overline{(-3)} = \overline{1} \quad \text{e como } \overline{(-3)} = \overline{5},$$

segue $(\overline{5})^{-1} = \overline{5}$.

(02) Como $mdc(4, 8) = 2$, em $\mathbb{Z}_8$ o elemento $\overline{4}$ não é inversível, ou seja, não existe $\overline{b} \in \mathbb{Z}_8$, tal que $\overline{4}.\overline{b} = \overline{1}$, como você pode verificar.

✓ **Exercícios 29.**

(01) Determine o inverso de cada uma das classses abaixo, caso exista. Não existindo, justifique:
(a) $\overline{5} \in \mathbb{Z}_{14}$;
Solução:
Como $mdc(5,14) = 1$, $\overline{5}$ é inversível. Da identidade, $5.3 + 14.(-1) = 1$
$\Rightarrow \overline{5.3} = \overline{14.(-1)} = \overline{1} \Rightarrow \overline{5}.\overline{3} = \overline{1}$. Assim, $(\overline{5})^{-1} = \overline{3}$. □
(b) $\overline{6} \in \mathbb{Z}_{14}$;
Solução:
Como $mdc(6,14) = 2$, $\overline{6}$ não é inversível. □
(c) $\overline{8} \in \mathbb{Z}_{12}$;
(d) $\overline{8} \in \mathbb{Z}_{9}$;
(e) $\overline{8} \in \mathbb{Z}_{17}$.

8 Divisores de Zero em $\mathbb{Z}_m$

Definição 9. *Um elemento não nulo $\overline{a} \in \mathbb{Z}_m$ diz-se um divisor não nulo de zero em $\mathbb{Z}_m$, se existe um $\overline{b} \in \mathbb{Z}_m$, também não nulo, tal que*

$$\overline{a}.\overline{b} = \overline{0}.$$

Exemplos:
(01) $\overline{2}$ e $\overline{3}$ são divisores não nulos de zero em $\mathbb{Z}_6$, pois ambos são não nulos e $\overline{2}.\overline{3} = \overline{6} = \overline{0}$;
(02) $\overline{6}$ e $\overline{8}$ são divisores não nulos de zero em $\mathbb{Z}_{12}$, pois $\overline{6}.\overline{8} = \overline{48} = \overline{0}$.
(03) $\overline{3}$ não é um divisor de zero em $\mathbb{Z}_5$, pois $\overline{3}.\overline{b} \neq \overline{0}$, para qualquer $\overline{0} \neq \overline{b} \in \mathbb{Z}_m$. (Verifique)

Vejamos como identificar se $\overline{0} \neq \overline{a} \in \mathbb{Z}_m$ é um divisor de zero.

Pela proposição 16, se $\overline{0} \neq \overline{a} \in \mathbb{Z}_m$ não é inversível, $mdc(a,m) = d > 1$. Como $d|m$ e $d|a$, $\frac{m}{d}$ e $\frac{a}{d}$ são números inteiro e $1 < \frac{m}{d} < m$. Portanto, a classe $\overline{(\frac{m}{d})} \in \mathbb{Z}_m$ é não nula e

$$\overline{a}.\overline{(\frac{m}{d})} = \overline{m}.\overline{(\frac{a}{d})} = \overline{0}.$$

Logo, $\overline{a}$ é um divisor de zero.

Exemplos:
(01) Como $mdc(6,14) \neq 2$, segue que $\overline{6} \in \mathbb{Z}_{14}$ não é inversível, logo será um divisor de zero, ou seja, existe $\overline{0} \neq \overline{b} \in \mathbb{Z}_{14}$, tal que $\overline{6}.\overline{b} = \overline{0}$. Para encontrar um respresentante para $\overline{b}$, tomamos $b = \frac{14}{mdc(6,14)} = 7$. Assim, $\overline{6}.\overline{7} = \overline{42} = \overline{0}$.

(02) Como $mdc(12,18) = 6$, então $\overline{12} \in \mathbb{Z}_{18}$ não é inversível, sendo portanto um divisor de zero. De fato, tomando $b = \frac{18}{mdc(12,18)} = 3$, temos que $\overline{12}.\overline{3} = \overline{36} = \overline{0}$.

Por outro lado, suponha $\overline{a}$ inversível, então existe $(\overline{a})^{-1} \in \mathbb{Z}_m$, tal que $\overline{a}.(\overline{a})^{-1} = \overline{1}$. Assim, se $\overline{b} \in \mathbb{Z}_m$ é tal que:

$$\overline{a}.\overline{b} = \overline{0} \Rightarrow (\overline{a})^{-1}.(\overline{a}\overline{b}) = (\overline{a})^{-1}.\overline{0} \Rightarrow ((\overline{a})^{-1}.\overline{a}).\overline{b} = \overline{0} \Rightarrow \overline{1}.\overline{b} = \overline{0} \Rightarrow \overline{b} = \overline{0}.$$

Portanto, a não inversibilidade de $\overline{a}$ é uma condição necessária e suficiente para que este seja um divisor de zero. Enunciamos esse resultado na proposição a seguir.

Proposição 17. *Seja $\overline{0} \neq \overline{a} \in \mathbb{Z}_m$. Então*

$$\overline{a} \text{ é um divisor de zero} \Leftrightarrow \overline{a} \text{ não é inversível.}$$

Corolário 10. *$\mathbb{Z}_m$ é sem divisores não nulos de zero se, e somente se, m é um número primo.*

Demonstração:
Se m é primo, pelo Corolário 9, todo $\overline{0} \neq \overline{a} \in \mathbb{Z}_m$ é inversível e portanto não é divisor de zero. Se m é composto, então existem inteiros $1 < r, s < m$, tais que $r.s = m$. Assim, $\overline{r}$ e $\overline{s}$ são não nulos e $\overline{r}.\overline{s} = \overline{m} = \overline{0}$. Logo $\overline{r}$ (e também $\overline{s}$) é um divisor não nulo de zero. □

✓ **Exercícios 30.**
(01) Determine todos os elementos inversíveis e todos os divisores não nulos de zero dos seguintes anéis:
(a) $\mathbb{Z}_6$;
Solução:
$\overline{a} \in \mathbb{Z}_6$ é inversível se, e só se, $mdc(a, 6) = 1$. Assim são inversíveis $\overline{1}$ e $\overline{5}$ e são divisores não nulos de zeros todas as demais classes não nulas: $\overline{2}, \overline{3}$ e $\overline{4}$. □
(b) $\mathbb{Z}_9$;
Solução:
Inversíveis: $\{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$ e os divisores não nulos de zero são $\{\overline{3}, \overline{6}\}$. □
(c) $\mathbb{Z}_{12}$;
(d) $\mathbb{Z}_{15}$;
(02) Dê exemplos, caso existam, de elementos não nulos $\overline{a}$, $\overline{b}$ e $\overline{c} \in \mathbb{Z}_{20}$, para os quais temos $\overline{a}.\overline{c} = \overline{b}.\overline{c}$, porém $\overline{a} \neq \overline{b}$.
Solução:
Tomando $\overline{a} = \overline{7}$, $\overline{b} = \overline{17}$ e $\overline{c} = \overline{6}$, temos que $\overline{a}.\overline{c} = \overline{b}.\overline{c} = \overline{2}$, embora $\overline{7} \neq \overline{17}$, em $\mathbb{Z}_{20}$. □
(03) Dê exemplos, caso existam, de elementos não nulos $\overline{a}$, $\overline{b}$ e $\overline{c} \in \mathbb{Z}_{19}$, para os quais temos $\overline{a}.\overline{c} = \overline{b}.\overline{c}$, porém $\overline{a} \neq \overline{b}$.
Solução:
Suponha $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_{19}$, para os quais temos $\overline{a}.\overline{c} = \overline{b}.\overline{c} \Rightarrow (\overline{a} - \overline{b}).\overline{c} = \overline{0}$. Como todo elemento de $\mathbb{Z}_{19}$ é inversível (Corolário 9), então $\overline{c}$ é inversível, logo existe $(\overline{c})^{-1} \in \mathbb{Z}_{19}$, tal que $\overline{c}.(\overline{c})^{-1} = 1$. Assim, $(\overline{a} - \overline{b}).\overline{c}(\overline{c})^{-1} = \overline{0}.(\overline{c})^{-1} \Rightarrow \overline{a} = \overline{b}$. Portanto, em $\mathbb{Z}_{19}$, tais elementos não existem. □

Lista de Exercícios 11.

(01) Determine as classes $\overline{0}, \overline{1}$ e $\overline{-5}$, em módulo m, para:
(a) $m = 4$;
(b) $m = 6$;
(c) $m = 10$.

(02) Responda e justifique:
(a) $\overline{23} = \overline{77}$, em módulo 8?
(b) $\overline{23} = \overline{77}$, em módulo 9?
(c) Para que valores de $m > 1$, temos $\overline{-14} = \overline{-6}$, em módulo m?
(c) Para que valores de $m > 1$, temos $\overline{83} = \overline{68}$, em módulo m?

(03) Determine $\mathbb{Z}_m$ e descreva as classes $\overline{0}$, $\overline{4}$ e $\overline{20} \in \mathbb{Z}_m$, para:
(a) $m = 8$;
(b) $m = 10$;
(c) $m = 13$.

(04) Determine o representante r da classe $\overline{a} \in \mathbb{Z}_m$, dada abaixo, com $0 \leq r < m$, sendo:
(a) $\overline{a} = \overline{33}$ e $m = 12$;
(b) $\overline{a} = \overline{33}$ e $m = 23$;
(c) $\overline{a} = \overline{-22}$ e $m = 7$;
(d) $\overline{a} = \overline{-22}$ e $m = 15$;
(e) $\overline{a} = \overline{41}$ e $m = 19$.

(05) Efetue as operações abaixo:
(a) Em $\mathbb{Z}_7$, $\overline{4} + \overline{4}$ e $\overline{4}.\overline{4}$;
(c) Em $\mathbb{Z}_9$, $\overline{5} + \overline{8}$ e $\overline{5}.\overline{8}$;
(e) Em $\mathbb{Z}_{13}$, $\overline{7} + \overline{9}$ e $\overline{7}.\overline{9}$.

(06) Construa as tábuas da adição e multiplicação para $\mathbb{Z}_7$ e $\mathbb{Z}_8$.

(07) Determine um representate r do oposto de $\overline{a} \in \mathbb{Z}_m$, com $0 \leq r < m$, para a e m abaixo:
(a) $a = 5$, $m = 13$;
(b) $a = 12$, $m = 33$;
(c) $a = -8$, $m = 4$;
(d) $a = 58$, $m = 7$.

(08) Resolva em $\mathbb{Z}_8$ as equações:
(a) $\overline{2} + x = \overline{4}.\overline{5}$;
(b) $\overline{3}.x = \overline{4} + \overline{-13}$.

(09) Resolva em $\mathbb{Z}_{13}$ as equações:
(a) $\overline{-5} + \overline{2}.x = \overline{7}.\overline{-3}$;
(b) $\overline{-6} + \overline{4}.x = \overline{-10} + \overline{6}$.

(10) Determine o inverso multiplicativo de cada uma das classes abaixo, caso exista. Não existindo, justifique:
(a) $\overline{7} \in \mathbb{Z}_{13}$;
(b) $\overline{7} \in \mathbb{Z}_{20}$;
(c) $\overline{12} \in \mathbb{Z}_{13}$;
(d) $\overline{12} \in \mathbb{Z}_{26}$.

(11) Em $\mathbb{Z}_{20}$, determine:
(a) o menor representante positivo das classes $\overline{34}$ e $\overline{-51}$
(b) Todos os divisores não nulos de zero.

(12) Mostre que se $\overline{a} \in \mathbb{Z}_m$ é inversível, então seu inverso é único.

(13) Em $\mathbb{Z}_{18}$ determine:
(a) o oposto de $\overline{4}$;
(b) o oposto de $\overline{-13}$;
(c) o inverso multiplicativo de $\overline{13}$, caso exista;
(d) o inverso multiplicativo de $\overline{8}$, caso exista;
(e) um elemento não nulo $\overline{b}$, tal que $\overline{14}.\overline{b} = \overline{0}$.

(14) (ENADE-2008) Em $\mathbb{Z}_{12}$, determine:
(a) todos divisores não nulos de zero;
(b) todos os elementos inversíveis.

(15) Verifique se $\overline{3640}$ é inversível em $\mathbb{Z}_{7297}$. Caso afirmativo, calcule seu inverso.

(16) Determinar todos os divisores não nulos de zero e os elementos inversíveis de $\mathbb{Z}_{26}$.

(17) Sejam $\overline{a}$, $\overline{b}$ e $\overline{c}$ elementos de $\mathbb{Z}_m$, tais que $\overline{a}.\overline{c} = \overline{b}.\overline{c}$. Mostre que se $mdc(c, m) = 1$, então $\overline{a} = \overline{b}$.

(18) Sejam p um primo positivo e $\overline{a}$ um elemento de $\mathbb{Z}_p$. Mostre que $\overline{a}^p = \overline{a}$.

(19) Seja p um número primo positivo. Determine em $\mathbb{Z}_p$ as soluções da equação $x^2 = \overline{1}$.

(20) Seja $p \geq 5$ um número primo. Resolver em $\mathbb{Z}_p$ a equação $x^p = \overline{4}$.

Respostas da Lista de Exercícios 11

(01.a) $\overline{0} = \{4k + 0 \mid k \in \mathbb{Z}\} = \{..., -12, -8, -4, 0, 4, 8, 12, ...\}$;
$\overline{1} = \{4k + 1 \mid k \in \mathbb{Z}\} = \{..., -11, -7, -3, 1, 5, 9, 13, ...\}$;
$\overline{-5} = \{4k + (-5) \mid k \in \mathbb{Z}\} = \{4k' + 3 \mid k' \in \mathbb{Z}\} = \{..., -9, -5, -1, 3, 7, 11, ...\}$;
(01.b) $\overline{0} = \{6k + 0 \mid k \in \mathbb{Z}\} = \{..., -18, -12, -6, 0, 6, 12, 18, ...\}$;
$\overline{1} = \{6k + 1 \mid k \in \mathbb{Z}\} = \{..., -17, -11, -5, 1, 7, 13, ...\}$;
$\overline{-5} = \{6k + (-5) \mid k \in \mathbb{Z}\} = \{6k' + 1 \mid k' \in \mathbb{Z}\} = \overline{1}$;
(01.c) $\overline{0} = \{10k + 0 \mid k \in \mathbb{Z}\} = \{-30, -20, -10, 0, 10, 20, 30, ...\}$;
$\overline{1} = \{10k + 1 \mid k \in \mathbb{Z}\} = \{-29, -19, -9, 1, 11, 21, 31, ...\}$;
$\overline{-5} = \{10k + (-5) \mid k \in \mathbb{Z}\} = \{10k' + 5 \mid k' \in \mathbb{Z}\} = \{-25, -15, -5, 5, 15, 25, ...\}$;
(02.a) $8 \nmid (23 - 77) \Rightarrow 23 \not\equiv 77(mod 8) \Rightarrow \overline{23} \neq \overline{77}$ em módulo 8.
(02.a) $9 \mid (23 - 77) \Rightarrow 23 \equiv 77(mod 9) \Rightarrow \overline{23} = \overline{77}$ em módulo 9.
(02.c) $\overline{-14} = \overline{-6}$, em módulo $m \Leftrightarrow -14 \equiv (-6)(mod m) \Leftrightarrow m|(-14 + 6) \Leftrightarrow m = 2$, 4 ou 8.
(02.d) $\overline{83} = \overline{68}$, em módulo $m \Leftrightarrow 83 \equiv 68(mod m) \Leftrightarrow m|(83 - 68) \Leftrightarrow m = 3$, 5 ou 15.
(03.a) $\mathbb{Z}_8 = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{7}\}$, sendo
$\overline{0} = \{8k+0 \mid k \in \mathbb{Z}\} = \{..., -16, -8, 0, 8, 16, ...\}$; $\overline{4} = \{8k+4 \mid k \in \mathbb{Z}\} = \{..., -12, -4, 4, 12, 20, ...\}$;
Como $20 \equiv 4(mod 8) \Rightarrow \overline{20} = \overline{4}$;
(03.b) $\mathbb{Z}_{10} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{9}\}$, sendo
$\overline{0} = \{10k+0 \mid k \in \mathbb{Z}\} = \{..., -20, -10, 0, 10, 20, ...\}$; $\overline{4} = \{10k+4 \mid k \in \mathbb{Z}\} = \{..., -16, -6, 4, 14, 24, ...\}$;
Como $20 \equiv 0(mod 10) \Rightarrow \overline{20} = \overline{0}$;
(03.c) $\mathbb{Z}_{13} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{12}\}$, sendo
$\overline{0} = \{13k+0 \mid k \in \mathbb{Z}\} = \{..., -26, -13, 0, 13, 26, ...\}$; $\overline{4} = \{13k+4 \mid k \in \mathbb{Z}\} = \{..., -22, -9, 4, 17, 30, ...\}$;
Como $20 \equiv 7(mod 13) \Rightarrow \overline{20} = \overline{7} = \{13k + 7 \mid k \in \mathbb{Z}\} = \{..., -19, -6, 7, 20, 33, ...\}$.
(04.a) Como $33 = 12.2 + 9 \Rightarrow r = 9$;
(04.b) $33 = 23.1 + 10 \Rightarrow r = 10$;
(04.c) $-22 = 7.(-4) + 6 \Rightarrow r = 6$;
(04.d) $-22 = 15.(-2) + 8 \Rightarrow r = 8$;
(04.d) $41 = 19.2 + 3 \Rightarrow r = 3$.
(05.a) $\overline{4} + \overline{4} = \overline{4 + 4} = \overline{8} = \overline{1}$; $\overline{4}.\overline{4} = \overline{4.4} = \overline{16} = \overline{2}$;
(05.b) $\overline{5} + \overline{8} = \overline{4}$; $\overline{5}.\overline{8} = \overline{4}$;
(05.c) $\overline{7} + \overline{9} = \overline{3}$; $\overline{7}.\overline{9} = \overline{11}$.
(06) Tábuas de $\mathbb{Z}_7$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$

$.$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{4}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{3}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{2}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

(07.a) $-(\overline{5}) = \overline{8}$;
(07.b) $-(\overline{12}) = \overline{21}$;
(07.c) $-(\overline{-8}) = \overline{8}$;
(07.d) $-(\overline{58}) = -(\overline{2}) = \overline{5}$;
(08.a) $x = \overline{2}$; (8.b) $x = \overline{3}$
(09.a) $x = \overline{5}$; (09.b) $x = \overline{7}$
(10.a) $(\overline{7})^{-1} = \overline{2}$;
(10.b) $(\overline{7})^{-1} = \overline{3}$;
(10.c) $(\overline{12})^{-1} = \overline{12}$;
(10.d) como $mdc(12, 26) = 2$, $\overline{12}$ não é inversível em módulo 26;
(11.a) $\overline{34} = \overline{14}$ e $\overline{-51} = \overline{9}$
(11.b) divisores não nulos de zero: $\{\overline{2}, \overline{4}, \overline{5}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{15}, \overline{16}, \overline{18}\}$.

(12) Suponha $\overline{a}$ inversível com inversos $\overline{b}, \overline{c}$. Então, $\overline{a}.\overline{b} = \overline{b}.\overline{a} = \overline{1}$ e $\overline{a}.\overline{c} = \overline{c}.\overline{a} = \overline{1}$. Daí, $\overline{b} = \overline{b}.\overline{1} = \overline{b}.(\overline{a}.\overline{c}) = (\overline{b}.\overline{a}).\overline{c} = \overline{1}.\overline{c} = \overline{c}$.
(13.a) $-(\overline{4}) = \overline{14}$;
(13.b) $\overline{-13} = \overline{5}$;
(13.c) $(\overline{13})^{-1} = \overline{7}$;
(13.d) como $mdc(8, 18) = 2$, $\overline{8}$ não é inversível em módulo 18;
(13.e) $\overline{14}.\overline{9} = \overline{0}$.
(14.a) Os divisores não nulos de zero são: $\overline{2}, \overline{3}, \overline{4}, \overline{6}, \overline{8}, \overline{9}$ e $\overline{10}$;
(14.b) os elementos inversíveis são $\overline{1}$, $\overline{5}$, $\overline{7}$ e $\overline{11}$.
(15) $(\overline{3640})^{-1} = \overline{3863}$;
(16) Elementos inversíveis: $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{11}, \overline{15}, \overline{17}, \overline{19}, \overline{21}, \overline{23}, \overline{25}\}$, divisores não nulos de zero: $\{\overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{13}, \overline{14}, \overline{16}, \overline{18}, \overline{20}, \overline{22}, \overline{24}\}$ (17) $\overline{a}.\overline{c} = \overline{b}.\overline{c} \Rightarrow \overline{ac} = \overline{bc} \Rightarrow ac \equiv bc(modm)$. Como $mdc(c, m) = 1$, pela lei do cancelamento na congruência, $a \equiv b(modm) \Rightarrow \overline{a} = \overline{b}$.
(18) Como p é primo, pelo Corolário 6, para todo inteiro a, tem-se $a^p \equiv a(modp) \Rightarrow \overline{a}^p \equiv \overline{a}$.
(19) Seja $\overline{a} \in \mathbb{Z}_p$ solução desta equação, então $\overline{a}^2 \equiv \overline{1} \Rightarrow a^2 \equiv 1(modp) \Rightarrow p|(a^2 - 1) \Rightarrow a = 1$ ou $a = p - 1 \Rightarrow x = \overline{1}$ ou $x = \overline{p-1}$.
(20) Seja $\overline{a} \in \mathbb{Z}_p$ uma solução da equação, então $\overline{a}^p = \overline{4} \Rightarrow a^p \equiv 4(modm)$. Por outro lado, como p é primo, pelo Corolario 6, $a^p \equiv a(modp)$, para todo $a \in \mathbb{Z}$. Pela simetria e transsitividade, temos $a \equiv 4(modp) \Rightarrow \overline{a} = \overline{4}$.

Capítulo 12

Equações Diofantinas Lineares

1 Introdução

Um jogo eletrônico tem o seguinte funcionamento: A máquina exibe um número inteiro positivo, que corresponde a pontuação exata que o jogador deverá marcar para vencer a partida. Os pontos são marcados cada vez que o jogador abate um invasor, que o fica desafiando na tela. Existem dois tipos de invasores: os marcianos (na cor vermelha), valendo cada um 22 pontos e os jupiterianos (na cor verde), com o valor individual de 18 pontos. Suponha que você vai participar deste jogo e a máquina lhe exibe o número 540. De quantas maneiras você pode vencer o jogo? Quantos invasores de cada cor você deverá abater?

Em busca da resposta, vamos formalizar o problema. O que queremos saber?
- O número de marcianos e o número de jupiterianos que devem ser abatidos. Denotaremos, respectivamente por x e y essas quantidades. Relacionando as variáveis temos a equação abaixo:

$$22x + 18y = 540.$$

A questão agora é saber se essa equação tem solução inteira, e se sim, como encontrá-la?

A técnica para encontrar o conjunto solução de tais equações - chamadas Equações Diofantinas Lineares - é o que estudaremos nesta aula.

2 Definição

Tais equações recebem este nome em homenagem a Diophanto de Alexandria ($\approx$ 250 d.c.).

Definição 10. *Chama-se* ***Equação Diofantina Linear*** *nas incognitas x e y, a toda equação da forma*

$$ax + by = c \tag{12.1}$$

onde a, b e c são inteiros fixos, com $ab \neq 0$.

✓ **Exercícios 31.**
(01) Das equações abaixo, quais estão de acordo com a Definição 10, ou seja, são equações diofantinas lineares com duas incognitas? Justifique.
(a) $6x + 8y = 76$;
(b) $4x + 10y = 16$;
(c) $2x + 4y = 7$;
(d) $3x^2 + 5y = 10$;
(e) $5x + \frac{1}{2}y = 14$;
(f) $3x + 0y = 12$;
(g) $4x + 8y = \frac{3}{5}$;
(h) $2x + 5y = -47$.

(02) Dê exemplo de duas equações diofantinas lineares com duas incognitas.

3 Solução da Equação Diofantina

Todo par de inteiros (x_0, y_0) para o qual

$$ax_0 + by_0 = c,$$

diz-se uma solução da equação (12.1).

Exemplos:
(a) O par $(-38, 38)$ é uma solução da equação diofantina linear

$$6x + 8y = 76,$$

pois

$$6.(-38) + 8.38 = 76.$$

(b) O par $(9, -2)$ é um solução da equação

$$4x + 10y = 16,$$

pois

$$4.9 + 10.(-2) = 16.$$

(c) A equação diofantina linear

$$2x + 4y = 7$$

não apresenta solução inteira, pois para qualquer par de inteiros (x_0, y_0),

$$2x_0 + 4y_0 \neq 7$$

uma vez que à esquerda da equação teremos um número par e à direita, um número ímpar.

Obs: Doravante, sempre que falarmos de solução de uma equação diofantina, fica subentendido que estamos falando de soluções inteiras.

✓ **Exercícios 32.**
(01) Dê uma solução, caso exista, para cada uma das equações abaixo:
(a) $2x + 3y = 7$;
(b) $8x + 6y = 61$;
(c) $5x + 7y = 33$;
(d) $12x + 16x = 30$.

(02) Dê uma solução para cada um dos exemplos dados por você na questão 02, do exercício anterior.

4 Condição de Existência da Solução

As perguntas que queremos responder são:
- Como saber se a equação $22x + 18y = 540$ tem solução?
- Se sim, como encontrá-las?

Relembrando, uma solução da equação diofantia

$$ax + by = c \tag{12.2}$$

é qualquer par de inteiros (x_0, y_0), tal que

$$ax_0 + by_0 = c.$$

No caso particular, em que o termo independente $c = d$, onde $d = mdc(a, b)$, a equação vai ter solução, pois, como já vimos, existem inteiros r e s, tais que

$$ar + bs = d. \tag{12.3}$$

- É possível a partir da solução dada em (12.3) obter uma solução da equação (12.2)?

Vejamos. Se $d|c$, então existe $k \in \mathbb{Z}$, tal que $c = dk$. Neste caso, multiplicando a equação (12.3) por k obtemos:

$$a(rk) + b(sk) = c.$$

Logo, o par de inteiros (rk, sk) é uma solução da equação original (12.2). Portanto, o $mdc(a, b)$ ser um divisor do termo constante c garante a existência de pelo menos uma solução para a equação. Dizemos que essa é uma condição suficiente para a existência de solução. Será ela também necessária, isto é, se $mdc(a, b) \nmid c$, a equação não terá solução?

Vamos supor que $d \nmid c$, porém a equação (12.2) tem solução. Então existem inteiros x_0, y_0, tais que

$$ax_0 + by_0 = c$$

Colocando d em evidência nesta equação:

$$d(\frac{a}{d}x_0 + \frac{b}{d}y_0) = c$$

Como d é um divisor comum de a e b, $\frac{a}{d}$ e $\frac{b}{d}$ são números inteiros. Assim, $(\frac{a}{d}x_0 + \frac{b}{d}y_0) \in \mathbb{Z}$, e portanto, $d|c$, contrariando nossa suposição inicial.

Podemos então enunciar o seguinte resultado:

> A equação diofantina linear
>
> $$ax + by = c$$
>
> tem solução se, e somente se, $mdc(a, b)$ divide c.

✓ **Exercícios 33.**

(01) Verifique se as equações diofantinas abaixo tem solução. Caso afirmativo, encontre uma solução particular da equação.
(a) $22x + 18y = 540$;
Solução:
Como $mdc(22, 18) = 2$ e $2|540$, esta equação tem solução. Para encontrar uma solução particular, incialmente procuramos inteiros r e s, tais que $22r+18s = 2$. Usando o algoritmo dado no Capítulo 5, obtemos:

$$22(-4) + 18.5 = 2.$$

Agora multiplicamos esta equação por $\frac{540}{2} = 270$ (isto é, por $\frac{c}{mdc(a,b)}$):

$$22.(-1080) + 18.(1350) = 540$$

Portanto, o par $(-1080, 1350)$ é uma solução da equação dada. □

(02) $24x + 14y = 36$;
Solução:
Como $mdc(24, 14) = 2$ e $2|36$ a equação tem solução. No Capítulo 5, vimos que

$$24.3 + 14.(-5) = 2.$$

Multiplicando esta equação por $\frac{36}{2} = 18$ obtemos:

$$24.54 + 14.(-90) = 36.$$

Portanto, $(54, -90)$ é uma solução particular da equação. □

(03) $-124x + 52y = -20$
Solução:
Como $mdc(-124, 52) = 4$ e $4| - 20$ a equação tem solução. Como já calculado anteriormente:

$$(-124).5 + 52.12 = 4.$$

Multiplicando esta equação por -5:

$$(-124).(-25) + 52.(-60) = -20.$$

Portanto, $(-25, -60)$ é uma solução particular dessa equaçao. $\square$

(04) $40x + 56y = 34$.
Solução:
Como $mdc(40, 56) = 8$ e $8 \nmid 34$, essa equação não tem solução inteira. $\square$

5 Conjunto Solução da Equação Diofantina

Na seção anterior, aprendemos a identificar quando uma equação diofantina linear tem solução, e no caso da existência, como encontrar uma solução particular. Veremos agora como encontrar o conjunto de todas as soluções possíveis, ou seja, o conjunto solução da equação.

Proposição 18. *Sejam*

$$ax + by = c$$

$\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$.

uma equação diofantina linear e $d = mdc(a, b)$, *com* $d \mid c$. *Se* $(x_0, y_0) \in \mathbb{Z}^2$ *é uma solução particular, então o conjunto de todas as soluções dessa equação é dado por:*

$$S = \{(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t) \mid t \in \mathbb{Z}\}.$$

Demonstração:
Por definição, o conjunto solução da equação diofantina $ax + by = c$ é dado por:

$$S = \{(u, v) \in \mathbb{Z}^2 \mid au + bv = c\}.$$

Considere o conjunto $X := \{(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t) \mid t \in \mathbb{Z}\}$. Vamos mostrar que $X = S$. De fato,

(i) $X \subset S$.
Seja $(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t) \in X$, então

$$a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = (ax_0 + by_0) + (\frac{ab}{d} - \frac{ab}{d})t = c + 0 = c.$$

Logo, $(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}r) \in S \Rightarrow X \subset S$.

(ii) $S \subset X$.
Seja $(u, v) \in S$. Como (x_0, y_0) é uma solução particular, então

$$au + bv = c = ax_0 + by_0 \Rightarrow a(u - x_0) = b(y_0 - v) \Rightarrow \frac{a}{d}(u - x_0) = \frac{b}{d}(y_0 - v).$$

Como $\frac{a}{d}$ é um inteiro, isto implica que $\frac{a}{d} \mid \frac{b}{d}(y_0 - v)$. Porém, $mdc(\frac{a}{d}, \frac{b}{d}) = 1$, logo, segue do Teorema 7, que $\frac{a}{d} \mid (y_0 - v)$, então existe $t \in \mathbb{Z}$, tal que:

$$y_0 - v = \frac{a}{d}t \Rightarrow v = y_0 - \frac{a}{d}t.$$

Substituindo este valor na identidade $a(u - x_0) = b(y_0 - v)$ obtemos $u = x_0 + \frac{b}{d}t$. Assim $(u, v) \in X \Rightarrow S \subset X$.

De (i) e (ii) segue que $S = \{(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t) \mid t \in \mathbb{Z}\}$. $\square$

✓ **Exercícios 34.**

(01) Encontre o conjunto solução de cada uma das equações diofantinas abaixo:
(a) $22x + 18y = 540$;
Solução:
Já vimos $mdc(22, 18) = 2$ e que $x_0 = -1080$ e $y_0 = 1350$ é uma solução particular da equação. Portanto, o conjunto solução é dado por:

$$S = \{(-1080 + \frac{18}{2}t, 1350 - \frac{22}{2}t) \mid t \in \mathbb{Z}\} = \{(-1080 + 9t, 1350 - 11t) \mid t \in \mathbb{Z}\}.$$

$\square$

(02) $24x + 14y = 36$;
Solução:
$mdc(24, 14) = 2$ e $x_0 = 54$ e $y_0 = -90$ é uma solução particular da equação. Logo, o conjunto solução é dado por:

$$S = \{(54 + 7t, -90 - 12t) \mid t \in \mathbb{Z}\}.$$

$\square$

(03) $-124x + 52y = -20$
Solução:
Como $mdc(-124, 52) = 4$, o par $(-25, -60)$ é uma solução particular da equaçao, então

$$S = \{(-25 + 13t, -60 - 31t) \mid t \in \mathbb{Z}\}.$$

$\square$

(04) $40x + 56y = 34$.
Solução:
Como $mdc(40, 56) = 8 \nmid 34$ esta equação não tem solução alguma, logo seu conjunto solução é o conjunto vazio, isto é, $S = \emptyset$. $\square$

(05) Encontre todas as soluções para o problema proposto no início da aula.
Solução:
O conjunto solução da equação $22x + 18y = 540$ é dado por:

$$S = \{(-1080 + 9t, 1350 - 11t) \mid t \in \mathbb{Z}\}.$$

Para o nosso problema particular, nem todas as soluções são válidas, pois como x e y representam as quantidades de invasores, servem somente soluções inteiras não negativas. Assim, devemos impor a condição:

$$-1080 + 9t \geq 0 \quad \text{e} \quad 1350 - 11t \geq 0$$

Resolvendo essas inequações encontramos:

$$t \geq 120 \quad \text{e} \quad t \leq 122,72$$

Como $t \in \mathbb{Z}$, podemos ter $t = 120, 121$ ou 122. Substituindo esses valores em $(-1080+9t, 1350-11t)$ obtemos as seguintes soluções: $(0,30), (9,19)$ e $(18,8)$. Assim, para ganhar o jogo deve-se abater 30 jupiterianos e nenhum marciano; ou 9 marcianos e 19 jupterianos ou ainda 18 marcianos e 8 jupterianos. $\square$

Lista de Exercícios 12.

(01) Verifique se as equações diofantinas abaixo tem solução. Caso afirmativo, use o algoritmo dado no Capítulo 5, para encontrar uma solução particular da equação.
(a) $2x + 3y = 9$;
(b) $3x + 5y = 47$;
(c) $12x + 45y = 18$;
(d) $24x + 14y = 8$;
(e) $56x + 72y = 40$;
(f) $60x + 72y = 16$;
(g) $47x - 29y = 15$.

(02) Determine o conjunto solução de cada uma das equações diofantinas dadas na questão anterior.

(03) Determine todas as soluções inteiras positivas das equações abaixo:
(a) $54x + 21y = 906$;
(b) $182x - 86y = 166$.

(04) Um caixa eletrônico tem apenas notas de $R\$10,00$ e $R\$\ 50,00$.
(a) De quantas maneiras este caixa pode liberar um saque de $R\$\ 530,00$?
(b) Que valores podem ser sacados neste caixa?

(05) De quantos modos podemos decompor o número primo 751 como uma soma de dois inteiros positivos, sendo um deles múltiplo de 5 e o outro múltiplo de 7?

(06) Determine todos os múltiplos negativos de 8 e 17, cuja soma é igual a -300.

(07) Expresse o número 277 como soma de dois inteiros positivos, de modo que o primeiro deixa resto 2 na divisão por 12 e o segundo, deixa resto 5 na divisão por 18.

(08) Determinado produto é vendido em recipientes de 7 e 9 litros. De quantas e quais maneiras se pode comprar 120 litros deste produto?

(09) Quanto um professor dividiu os n alunos de sua turma em grupos de 7, sobraram 3 alunos e quando os dividiu em grupos de 6, sobraram 5. Quantos são os alunos dessa turma, sabendo que $50 \leq n \leq 80$?

(10) Isabel deverá tomar duas medicações A e B, no total de 60 comprimidos. Na primeira dose, A e B foram tomados simultaneamnte. A partir daí, a medição A deverá ser tomada de 6 em 6 horas e B, a cada intervalo de 9 horas. Quantos comprimidos de cada medicamento ela deverá tomar, de modo que o intervalo de tempo entre as doses finais dos dois remédios seja a menor possível?

Respostas da Lista de Exercícios 12

(01.a) $x_0 = -36$ e $y_0 = 27$

(01.b) $x_0 = 94$ e $y_0 = -47$

(01.c) $x_0 = 24$ e $y_0 = -6$

(01.d) $x_0 = 12$ e $y_0 = -20$

(01.e) $x_0 = 20$ e $y_0 = -15$

(01.f) A equação não tem solução

(01.g) $x_0 = -120$ e $y_0 = -195$

(02.a) $S = \{(-36 + 3t, 27 - 2t) \mid t \in \mathbb{Z}\}$

(02.b) $S = \{(94 + 5t, -47 - 3t) \mid t \in \mathbb{Z}\}$

(02.c) $S = \{(24 + 15t, -6 - 4t) \mid t \in \mathbb{Z}\}$

(02.d) $S = \{(12 + 7t, -20 - 12t) \mid t \in \mathbb{Z}\}$

(02.e) $S = \{(20 + 9t, -15 - 7t) \mid t \in \mathbb{Z}\}$

(02.f) $S = \emptyset$

(02.g) $S = \{(-120 - 29t, -195 - 47t) \mid t \in \mathbb{Z}\}$

(03.a) $\{(2, 38), (9, 20), (16, 2)\}$

(03.b) $\{(8, 15), (51, 106), (94, 197)\}$

(04.a) Representando por x o número de notas de 10 reais e por y o número de notas de 50 reais, os valores possíveis para o par (x, y) são: $(3, 10)$, $(8, 9)$, $(13, 8)$, $(18, 7)$, $(23, 6)$, $(3, 10)$, $(28, 5)$, $(33, 4)$, $(38, 3)$, $(43, 2)$, $(48, 1)$.

(04.b) Apenas valores que são múltiplos de 10.

(05) Podemos decompor como $751 = (11265 + 35t) + (-10.514 - 35t), -321 \leq t \leq -301$. Portanto, existem 21 formas de escrever a soma pedida.

(06) $(-232, -68)$ e $(-96, -204)$.

(07) $277 = (-538 + 36t) + (815 - 36t)$, com $15 \leq t \leq 22$.

(08) De duas maneiras: 12 recipientes de 7 litros e 4 de 9 livros ou 3 recipientes de 7 litros e 11 de 9.

(09) $n = 59$

(10) 42 de A e 18 de B.

Capítulo 13

Congruência Linear

1 Introdução

- Certo dia um professor dividiu os n alunos da sua turma em grupos, ficando exatamente 6 alunos em cada grupo. Na aula seguinte usou a mesma estratégia, só que desta vez colocou 8 pessoas em cada grupo e sobraram 4. Sabendo que o número n de alunos dessa turma está no intervalo, $50 \leq n \leq 100$, quais os valores possíveis para n?

Pensemos juntos na solução desse problema. Seja n o número de alunos da turma. Se ao dividir a turma em grupos de 6, a divisão foi exata, n é um múltiplo de 6, isto é,

$$n = 6x, \quad x \in \mathbb{Z}.$$

Por outro lado, ao dividir n por 8 restaram 4, então

$$n \equiv 4(mod8).$$

Substituindo n por $6x$ na congruência acima obtemos $6x \equiv 4(mod8)$. Portanto, para encontrar os possíveis valores de n, devemos resolver em $\mathbb{Z}$ a equação:

$$6x \equiv 4(mod8).$$

Definição 11. *Seja $m > 1$ um inteiro. Chamamos **congruência linear** a todo equação da forma:*

$$ax \equiv b(modm) \tag{13.1}$$

onde a e b são inteiros fixos.

Exemplos:
(01) $6x \equiv 4(mod8)$;
(02) $3x \equiv 5(mod8)$;
(03) $2x \equiv 3(mod4)$;
(04) $18x \equiv 30(mod42)$;
(05) $x \equiv -5(mod7)$.

2 Condição de Existência da Solução

Todo inteiro x_0, tal que

$$ax_0 \equiv b(modm)$$

é chamado uma **solução da congruência linear** $ax \equiv b(modm)$.

A questão imediata é saber se toda congruência linear tem solução.

Se a congruência linear $ax \equiv b(modm)$ tem solução, então existe $x_0 \in \mathbb{Z}$, tal que

$$ax_0 \equiv b(modm)$$
$$\Downarrow$$
$$m|(ax_0 - b)$$

Consequentemente, existe $y_0 \in \mathbb{Z}$, tal que:

$$ax_0 - b = my_0 \Rightarrow ax_0 + (-m)y_0 = b.$$

Logo, (x_0, y_0) é uma solução da equação diofantina linear $ax + (-m)y = b$. Concluímos assim, que se a congruência linear $ax \equiv b(modm)$ tem solução, então a equação diofantina $ax + (-m)y = b$ também o tem.

Reciprocamente, se a equação diofantina $ax + (-m)y = b$ tem solução, então existe um par de inteiros (x_0, y_0), tal que:

$$ax_0 + (-m)y_0 = b \Rightarrow ax_0 - b = my_0 \Rightarrow m|(ax_0 - b) \Rightarrow ax_0 \equiv b(modm)$$
$$\Downarrow$$
$$x_0 \text{ é solução da congruência linear } ax \equiv b(modm).$$

Portanto temos que:

$ax \equiv b(modm)$ tem solução se, e somente se, $ax + (-m)y = b$ tem solução.

Por sua vez,

$ax + (-m)y = b$ tem solução se, e somente se, $mdc(a, -m)$ divide b.

Juntando estes dois resultado e o fato de $mdc(a, -m) = mdc(a, m)$, podemos afirmar:

A congruência linear

$$ax \equiv b(modm)$$

tem solução se, e somente se, $mdc(a, m)$ divide b.

Dizemos que $ax + (-m)y = b$ é a **equação diofantina associada** a congruência linear $ax \equiv b(modm)$.

✓ **Exercícios 35.**

(01) Verifique quais das congruências abaixo tem solução:
(a) $6x \equiv 4(mod 8)$;
Solução:
Neste caso, $a = 6$, $b = 4$ e $m = 8$. Como $mdc(a, m) = mdc(6, 8) = 2$ e $2|4$, a congruência tem solução. □

(b) $8x \equiv 24(mod 12)$;
Solução:
Aqui, $a = 8$, $b = 24$ e $m = 12$. Como $mdc(8, 12) = 4$ e $4|24$, a congruência tem solução. □

(c) $4x \equiv 13(mod 20)$.
Solução:
Como $mdc(4, 20) = 4$ e $4 \nmid 13$, a congruência não tem solução. □

3 Solução da Congruência Linear

Já vimos que a congruência linear

$$ax \equiv b(mod m)$$

tem solução se, e só se, a equação diofantina

$$ax + (-m)y = b$$

o tiver. Para encontrar uma solução particular x_0 da primeira, devemos então encontrar uma solução da segunda. Relembremos como encontrar tal solução.

Inicialmente escrevemos $d = mdc(a, m)$ como soma de múltiplos inteiros de a e m, isto é, encontramos inteiros r e s, tais que:

$$ar + ms = d.$$

Em seguida multiplicamos esta equação pelo inteiro $\frac{b}{d}$:

$$a(r\frac{b}{d}) + m(s\frac{b}{d}) = d\frac{b}{d}$$

ou ainda,

$$a(r\frac{b}{d}) + (-m)(-s\frac{b}{d}) = b.$$

Logo, $(r\frac{b}{d}, -s\frac{b}{d})$ é uma solução da equação diofantina linear $ax + (-m)y = b$ e consequentemente $x_0 = r\frac{b}{d}$ é uma solução da congruência $ax \equiv b(mod m)$.

✓ **Exercícios 36.**
(01) Encontre uma solução particular para cada uma das congruências lineares:
(a) $6x \equiv 4(mod 8)$.
Solução:
Para encontrar uma solução da congruência linear $6x \equiv 4(mod 8)$, devemos determinar uma solução da equação diofantina associada $6x + (-8)y = 4$. Inicialmente, escrevemos $d = mdc(6, 8) = 2$ como soma de múltiplos de 6 e 8, o que pode ser feito usando o algoritmo de Euclides. Nesse caso temos que:

$$6.(-1) + 8.1 = 2.$$

Pelo que vimos acima, uma equação particular é dada por
$x_0 = r\frac{b}{d} = -1.\frac{4}{2} = -2$. Porém, para uma melhor aprendizagem, vamos encontrar tal valor repetindo todo o procedimento feito anteriormente.

Multiplicamos a equação acima por $\frac{b}{d} = \frac{4}{2} = 2$:

$$6.(-2) + 8.2 = 4.$$

Como os coeficientes da equação diofantina são 6 e -8, rearrumamos a equação escrevendo:

$$6.(-2) + (-8).(-2) = 4.$$

Assim, $(-2, -2)$ é uma solução da equação $6x+(-8)y = 4$ e consequentemente $x_0 = -2$ é uma solução particular da congruência $6x \equiv 4(mod 8)$.
(b) $8x \equiv 24(mod 12)$;
Solução:
Inicialmente vamos procurar uma solução da equação diofantina associada: $8x + (-12)y = 24$. Como $mdc(8, 12) = 4$ usando o algoritmo de Euclides encontramos:

$$8.(-1) + 12.1 = 4.$$

Multiplicamos essa equação por $\frac{24}{4} = 6$:

$$8.(-6) + 12.6 = 24.$$

ou ainda,

$$8.(-6) + (-12).(-6) = 24.$$

Assim, $(-6, -6)$ é uma solução da equação $8x + (-12)y = 24$ e consequentemente $x_0 = -6$ é uma solução particular da congruência $8x \equiv 24(mod 12)$. □

(c) $18x \equiv 30(mod 42)$.
Solução:
A equação diofantina associada a essa congruência é $18x+(-42)y = 30$ e como $mdc(18, 42) = 6$ e $6|30$, a equação tem solução. Para uma solução particular, usamos a identidade:

$$18.(-2) + 42.1 = 6.$$

e multiplicamos essa equação por $\frac{b}{d} = \frac{30}{6} = 5$:

$$18.(-10) + 42.5 = 30 \Rightarrow 18.(-10) + (-42).(-5) = 30.$$

Assim, $(-10, -5)$ é uma solução da equação $18x+(-42)y = 30$ e consequentemente $x_0 = -10$ é uma solução particular da congruência $18x \equiv 30(mod 42)$.

4 Conjunto Solução da Congruência Linear

Já sabemos calcular uma solução particular da congruência linear $ax \equiv b(modm)$, quando essa tem solução. Vejamos agora como, a partir de uma solução particular, encontrar o conjunto de todas as soluções.

Como já visto na Proprosição 18, se (x_0, y_0) é uma solução da equação diofantina $ax + (-m)y = b$ e $d = mdc(a, m)$, então o conjunto solução da equação é dado por:

$$S = \{(x_0 - \frac{m}{d}t, y_0 - \frac{a}{d}t) \mid t \in \mathbb{Z}\}.$$

Portanto, se α é uma solução da congruência linear $ax \equiv b(modm)$, então $a\alpha \equiv b(modm) \Rightarrow m|(a\alpha - b) \Rightarrow a\alpha - b = mk,\ k \in \mathbb{Z} \Rightarrow a\alpha + (-m)k = b \Rightarrow (\alpha, k) \in S \Rightarrow \alpha = x_0 - \frac{m}{d}t$, para algum inteiro t.

Reciprocamente, se $\alpha = x_0 - \frac{m}{d}t$, para algum $t \in \mathbb{Z}$, então o par $(x_0 - \frac{m}{d}t, y_0 - \frac{a}{d}t) \in S$, logo é solução da equação diofantina $ax + (-m)y = b$ e portanto,

$$a(x_0 - \frac{m}{d}t) + (-m)(y_0 - \frac{a}{d}t) = b$$

$$\Downarrow$$

$$a(x_0 - \frac{m}{d}t) - b = m(y_0 - \frac{a}{d}t) \Rightarrow m| \left(a(x_0 - \frac{m}{d})t - b\right)$$

$$\Downarrow$$

$$a(x_0 - \frac{m}{d}t) \equiv b(modm)$$

$$\Downarrow$$

$\alpha = x_0 - \frac{m}{d}t$ é solução da congruencia linear $ax \equiv b(modm)$.

Com isso, identificamos o conjunto solução da congruência $ax \equiv b(modm)$, quando essa tem solução, dado a seguir:

> O conjunto solução da congruência linear $ax \equiv b(mod)$, quando $d = mdc(a, m)$ divide b é dado por:
>
> $$S' = \{x_0 + \frac{m}{d}t \mid t \in \mathbb{Z}\}.$$

Obs: $S' = \{x_0 - \frac{m}{d}t \mid t \in \mathbb{Z}\} = \{x_0 + \frac{m}{d}t \mid t \in \mathbb{Z}\}$.

✓ **Exercícios 37.**

(01) Encontre o conjunto solução das congruências abaixo:
(a) $6x \equiv 4(mod 8)$.
Solução:
Como $x_0 = -2$ é uma solução particular da congruência, então seu conjunto solução é dado por:

$$S = \{-2 + 4t \mid t \in \mathbb{Z}\}.$$

Assim, os inteiros -6, -2, 2, 6, 10, 18 são algumas dessas soluções. De posse do conjunto solução, podemos agora responder a questão proposta no início da aula. Lembremos que o número n de alunos da turma é dado por $n = 6x$, onde $x \in S$. Assim, $n = -12 + 24t$, com $t \in \mathbb{Z}$. Além disso , temos a informação adicional de que $50 < n \leq 100$. Assim, $50 \leq -12 + 24t \leq 100 \Rightarrow \frac{31}{12} \leq t \leq \frac{14}{3} \Rightarrow t \in \{3, 4\}$. Logo, os possíveis valores para o número de alunos é 60 ou 84. □

(b) $8x \equiv 24(mod 12)$;
Solução:
Tomando a solução particular $x_0 = -6$ já encontrada anteriormente, segue que

$$S = \{-6 + 3t \mid t \in \mathbb{Z}\}.$$

□

(c) $18x \equiv 30(mod 42)$.
Solução:
Usando a solução particular $x_0 = -10$ já encontrada, segue que

$$S = \{-10 + 7t \mid t \in \mathbb{Z}\}.$$

□

(d) $4x \equiv 13(mod 20)$;
Solução:
Como a equação não tem solução, então seu conjunto solução é $S = \emptyset$. □

5 Congruência Lineares Equivalentes

Definição 12. *Dizemos que as congruências lineares*

$$a_1x \equiv b_1(mod m_1) \quad e \quad a_2x \equiv b_2(mod m_2)$$

são equivalentes se elas têm o mesmo conjunto solução.

Exemplos:
(01) As congruências $3x \equiv 9(mod6)$ e $x \equiv 9(mod2)$ são equivalentes, pois ambas tem
$$S = \{1 + 2t \mid t \in \mathbb{Z}\}.$$
como conjunto solução. □

(02) As congruências $8x \equiv 20(mod12)$ e $4x \equiv 100(mod3)$ são equivalentes, tendo
$$S = \{1 + 3t \mid t \in \mathbb{Z}\}.$$
como conjunto solução. □

Considere a congruência linear
$$ax \equiv b(modm) \tag{13.2}$$
com b sendo um múltiplo de $mdc(a, m)$. Vejamos como obter uma congruência linear equivalente a ela e em geral de mais fácil resolução.

Sejam $d = mdc(a, m)$ e r e s inteiros, tais que:
$$d = ar + ms. \tag{13.3}$$

Se x_0 é uma solução qualquer de (13.2), então
$$ax_0 \equiv b(modm) \Rightarrow m|(ax_0 - b) \Rightarrow ax_0 - b = mk, \quad k \in \mathbb{Z}.$$
Multiplicando a última identidade por r, obtemos:
$$(ar)x_0 - br = m(rk).$$
Substituindo nessa identidade o valor de ar dado em (13.3):
$$(d - ms)x_0 - br = m(rk)$$
$$\Downarrow$$
$$dx_0 - br = m(rk + sx_0) \Rightarrow x_0 - \frac{b}{d}r = \frac{m}{d}(rk + sx_0)$$
$$\Downarrow$$
$$x_0 \equiv \frac{b}{d}r(mod\frac{m}{d})$$
Portanto, x_0 é também solução da congruência linear $x \equiv \frac{b}{d}r(mod\frac{m}{d})$.

Reciprocamente, se x_0 é solução da congruência linear $x \equiv \frac{b}{d}r(mod\frac{m}{d})$, então
$$x_0 \equiv \frac{b}{d}r(mod\frac{m}{d}).$$
De (13.3) obtemos a congruencia linear:
$$\frac{a}{d}r \equiv 1(mod\frac{m}{d})$$

Multiplicando membro a membro essas congruencias (propriedade C7):

$$\frac{a}{d}rx_0 \equiv \frac{b}{d}r(mod\frac{m}{d}) \tag{13.4}$$

Como $d = ar + ms \Rightarrow 1 = \frac{a}{d}r + \frac{m}{d}s \Rightarrow mdc(r, \frac{m}{d}) = 1$. Assim, podemos usar a lei do cancelamento em (13.4), obtendo:

$$\frac{a}{d}x_0 \equiv \frac{b}{d}(mod\frac{m}{d})$$

$$\Downarrow$$

$$\frac{a}{d}x_0 - \frac{b}{d} = \frac{m}{d}k,\ k \in \mathbb{Z} \Rightarrow ax_0 - b = mk \Rightarrow ax_0 \equiv b(modm).$$

$$\Downarrow$$

$$x_0 \quad \text{é solução da congruencia linear } \ ax \equiv b(modm).$$

Desta forma, provamos o que é enunciado na proposição abaixo.

Proposição 19. *Sejam a e $m > 1$ inteiros, com $d = mdc(a, m)$. Para quaisquer inteiros r e s, tais que*

$$d = ar + ms,$$

e qualquer $b \in d\mathbb{Z}$, as congruências lineares:

$$ax \equiv b(modm) \qquad e \qquad x \equiv \tfrac{b}{d}r(mod\tfrac{m}{d})$$

são equivalentes.

✓ **Exercícios 38.**

(01) Encontre uma congruência linear equivalente a equação dada e seu conjunto solução:
(a) $18x \equiv 30(mod42)$.
Solução:
Como $mdc(18, 42) = 6$ e 30 é um múltiplo de 6, então pela Proposição 19, essa congruência é equivalente a congruência linear

$$x \equiv 5r(mod7)$$

qualquer que seja o inteiro r, para o qual existe $s \in \mathbb{Z}$, tal que $18r + 42s = 6$. Em particular, como $18.(-2) + 42.1 = 6$, segue que

$$x \equiv -10(mod7)$$

é equivalente a equação dada. Facilmente, vemos que $x_0 = -3$ é uma solução particular dessa última, portanto seu conjunto solução (o qual é também congruência original) é dado por:

$$S = \{-3 + 7t \mid t \in \mathbb{Z}\}.$$

(b) $15x \equiv 20(mod 10)$;
Solução:
Como $mdc(15, 10) = 5|20$, essa congruencia é equivalente a congruência linear:

$$x \equiv 4r(mod 2)$$

qualquer que seja o inteiro $r \in \mathbb{Z}$, para o qual existe $s \in \mathbb{Z}$, tal que $15r+10s = 5$. Como $15.1 + 10.(-1) = 5$, então

$$x \equiv 4(mod 2)$$

é equivalente a equação dada. Claramente, $x_0 = -2$ é uma solução particular dessa última, portanto o conjunto solução de ambas as congruências é dado por:

$$S = \{-2 + 2t \mid t \in \mathbb{Z}\}.$$

Como também temos as identidades

$$15.3 + 10.(-4) = 5$$

e

$$15.(-7) + 10.10 = 5$$

obtemos também as congruências equivalentes

$$x \equiv 12(mod 2) \quad \text{e} \quad x \equiv -28(mod 2)$$

dentre outras.

Lista de Exercícios 13.

(01) Verifique quais das congruências abaixo tem solução:
(a) $3x \equiv 5(mod 8)$;
(b) $3x \equiv 6(mod 18)$;
(c) $-6x \equiv 5(mod 4)$;
(d) $34x \equiv 60(mod 98)$;
(e) $4x \equiv 13(mod 20)$;
(f) $27x \equiv 45(mod 18)$.

(02) Encontre o conjunto de cada uma das congruências lineares da questão (01).

(03) Encontre uma congruencia linear que seja equivalente a congruência abaixo:
(a) $3x \equiv 5(mod 8)$.
(b) $18x \equiv 30(mod 42)$.
(c) $5x \equiv 20(mod 7)$.
(d) $25x \equiv 15(mod 29)$
(e) $5x \equiv 2(mod 26)$

(04) Determine todos os múltiplos de 5 que deixa resto 7 na divisão por 9.

(05) Determine todos os múltiplos positivos de 11, que deixam resto 2 na divisão por 5.

(06) Encontre todos os anos bissextos até 2016, que deixam resto 5 na divisão por 9.

Respostas da Lista de Exercícios 13
(01.a) $mdc(3,8) = 1|5 \Rightarrow$ a congruência tem solução.
(01.b) $mdc(3,18) = 3|6 \Rightarrow$ a congruência tem solução.
(01.c) $mdc(-6,4) = 2 \nmid |5 \Rightarrow$ a congruência não tem solução.
(01.d) $mdc(34,98) = 2|60 \Rightarrow$ a congruência tem solução.
(01.e) $mdc(4,20) = 4 \nmid 13 \Rightarrow$ a congruência não tem solução.
(01.f) $mdc(27,18) = 9|45 \Rightarrow$ a congruência tem solução.
(02.a) $S = \{15 + 8t \mid t \in \mathbb{Z}\}$.
(02.b) $S = \{2 + 6t \mid t \in \mathbb{Z}\}$.
(02.c) $S = \emptyset$.
(02.d) $S = \{-690 + 49t \mid t \in \mathbb{Z}\}$.
(02.e) $S = \emptyset$.
(02.f) $S = \{5 + 2t \mid t \in \mathbb{Z}\}$.
(03.a) $x \equiv 15(mod 8)$.
(03.b) $x \equiv -60(mod 7)$.
(03.c) $x \equiv 60(mod 7)$.
(03.d) $x \equiv 105(mod 29)$
(03.e) $x \equiv -10(mod 26)$
(04) $45t + 25$, $t \in \mathbb{Z}$
(05) $22 + 55t$, $t \geq 0$.
(06) $-40 + 36t$, $2 \leq t \leq 57$.

Capítulo 14

Sistema de Congruências Lineares

1 Introdução

- Quanto um professor dividiu os alunos de sua turma em equipes com sete pessoas cada uma, sobrou um aluno. E quando dividiu em equipes com cinco ou com oito pessoas, aí sobraram três alunos. Qual o menor número possível de alunos nessa turma?

Solução:
Vamos representar por x o número de alunos na turma, o qual queremos determinar. Do enunciando acima, conclui-se que x deixa resto 1 na divisão por 7 e resto igual 3 na divisão por 5 e também por 8. Usando linguagem de congruência, isso equivale a dizer que x deve verifica simultaneamente as seguintes congruências lineares:

$$\begin{cases} x \equiv 3(mod5) \\ x \equiv 1(mod7) \\ x \equiv 3(mod8) \end{cases}$$

Temos assim um sistema de congruências lineares. Vejamos, uma maneira de determinar o valor de x, usando propriedades da congruência já estudadas.

(i) Resolvemos a primeira equação $x \equiv 3(mod5)$:

$$x \equiv 3(mod5) \Rightarrow 5|(x-3) \Rightarrow x = 3 + 5y, \quad \text{com} \quad y \in \mathbb{Z};$$

(ii) Substituindo o valor encontrado para x na segunda equação:
$x \equiv 1(mod7) \Rightarrow (3+5y) \equiv 1(mod7) \Rightarrow 5y \equiv -2(mod7) \Leftrightarrow y \equiv -6(mod7)$
$\Rightarrow y = -6 + 7z$;
(iii) Substituindo o valor encontrado para y na equação $x = 3 + 5y$:

$$x = 3 + 5y = 3 + 5(-6 + 7z) \Rightarrow x = -27 + 35z$$

(iv) Substuindo o último valor encontrado para x na terceira equação: $x \equiv 3(mod8) \Rightarrow (-27 + 35z) \equiv 3(mod8) \Rightarrow 35z \equiv 30(mod8) \Leftrightarrow z \equiv 90(mod8)$

$\Rightarrow z = 90 + 8t.$

Assim,

$$x = -27 + 35z = -27 + 35(90 + 8t) = 3123 + 280t.$$

Como x representa a quantidade de alunos na turma, então $x \geq 0$. Assim,

$$x = 280t + 3123 \geq 0 \Rightarrow t \geq -11.$$

Por fim, sendo x uma função crescente de t, então o menor valor de x é assumido quando t é mínimo, ou seja, quando $t = -11$. Portanto, o menor número de alunos na turma é igual a 43. $\square$

2 Definição

O que fizemos no exemplo acima foi encontrar um valor para uma variável x que satisfaz simultaneamente a mais de uma congruência linear, ou seja, a um Sistema de Congruências Lineares, conforme definido a seguir.

Definição 13. *Chamamos de* ***Sistema de Congruências Lineares*** *a todo sistema da forma:*

$$\begin{cases} a_1x & \equiv b_1 \quad (mod m_1) \\ a_2x & \equiv b_2 \quad (mod m_2) \\ ... & ... \quad ... \\ a_kx & \equiv b_k \quad (mod m_k) \end{cases}$$

onde $a_1, a_2, ..., a_k, b_1, b_2, ..., b_k, m_1, m_2, ..., m_k$ *são inteiros fixados, com* $m_i > 1$, *para todo* $i = 1, 2, .., k$.

Exemplos:

$$(01) \begin{cases} x & \equiv 2 \quad (mod 3) \\ x & \equiv 3 \quad (mod 5) \\ x & \equiv 2 \quad (mod 7) \end{cases}$$

$$(02) \begin{cases} 6x & \equiv 2 \quad (mod 4) \\ 2x & \equiv 1 \quad (mod 3) \\ 4x & \equiv 2 \quad (mod 7) \end{cases}$$

$$(03) \begin{cases} x & \equiv -1 \quad (mod 4) \\ x & \equiv 2 \quad (mod 6) \end{cases}.$$

3 Solução do Sistema

Vejamos agora um resultado - conhecido como Teorema Chinês do Resto - o qual dá uma condição a para a existência de solução de um sistema de congruências lineares e fornece um algoritmo para calcular uma solução particular do mesmo.

Teorema 14. *(**Teorema Chinês do Resto**) Se os inteiros $m_1, m_2, ..., m_k$ são dois a dois relativamente primos, então o sistema de congruências lineares:*

Dizer que a solução é única módulo m, implica dizer que se x_1, x_2 são duas soluções do sistema, então $x_1 \equiv x_2 (mod m)$.

$$\begin{cases} x \equiv b_1 (mod m_1) \\ x \equiv b_2 (mod m_2) \\ \quad ... \\ x \equiv b_k (mod m_k) \end{cases}$$

admite uma solução, que é única módulo $m = m_1 m_2 ... m_k$.

Algoritmo da Aplicação do Teorema Chinês do Resto

Daremos a seguir os passos para encontrar uma solução particular x_0 de um sistema de congruência lineares, quando este verifica as hipóteses do Teorema acima. De posse de x_0, determinamos o conjunto solução.

Passo 1: Construir inteiros m, $M_1, M_2, ..., M_k$, onde

$$m = m_1 m_2 ... m_k$$

e

$$M_1 = \frac{m}{m_1}, \quad M_2 = \frac{m}{m_2}, \quad ... \quad M_i = \frac{m}{m_i}, \quad ... \quad M_k = \frac{m}{m_k}.$$

Passo 2: Encontrar inteiros r_i e s_i:
Para cada $i = 1, 2, ..., k$, $mdc(M_i, m_i) = 1$, logo existe inteiros r_i e s_i, tais que:

$$M_1.r_1 + m_1.s_1 = 1$$

$$M_2.r_2 + m_2.s_2 = 1$$

$$....$$

$$M_k.r_k + m_k.s_k = 1$$

Determina-se inteiros r_i e s_i que verifiquem essas condições;

Passo 3: Determinar a solução particular:
A solução particular x_0 é dada por:

$$x_0 = b_1 M_1 r_1 + b_2 M_2 r_2 + ... + b_k M_k r_k.$$

Passo 4: Determinar o conjunto solução:
Todas as demais soluções do sistema são congruentes a x_0 módulo m, logo o conjunto solução é dado por:

$$S = \{x_0 + mt \mid t \in \mathbb{Z}\}.$$

Exemplos:
(01) Usaremos o algoritmo acima para resolver novamente o sistema proposto no início do capítulo:

$$\begin{cases} x \equiv 3(mod5) \\ x \equiv 1(mod7) \\ x \equiv 3(mod8). \end{cases}$$

Solução:
Como

$$mdc(5,7) = mdc(5,8) = mdc(7,8) = 1,$$

os inteiros $m_1 = 5$, $m_2 = 7$ e $m_3 = 8$ são dois a dois relativamente primos, logo o sistema tem uma única solução x_0 módulo $m_1m_2m_3 = 280$. Para determinar x_0 seguiremos os passos dados no algoritmo acima:
Passo 1: Determinar m e M_1, M_2, M_3:

$$m = m_1m_2m_3 = 280$$

e

$$M_1 = \frac{m}{m_1} = \frac{280}{5} = 56, \quad M_2 = \frac{m}{m_2} = \frac{280}{7} = 40 \quad \text{e} \quad M_3 = \frac{m}{m_3} = \frac{280}{8} = 35.$$

Passo 2: Encontrar inteiros r_i e s_i:
Escrevendo $1 = mdc(56,5) = mdc(40,7) = mdc(35,8)$ como soma de múltiplos desses inteiros temos:

$$1 = 56.1 + 5.(-11)$$
$$1 = 40.3 + 7.(-17)$$
$$1 = 35.3 + 8.(-13)$$

Passo 3: Determinar uma solução particular:
Então

$$x_0 = b_1M_1r_1 + b_2M_2r_2 + b_3M_3r_3 = 3.56.1 + 1.40.3 + 3.35.3 = 603.$$

Passo 4: Determinar o conjunto solução:
Como $x_0 = 603$ é uma solução, então

$$S = \{603 + 280t \mid t \in \mathbb{Z}\}.$$

(02) Usando o algoritmo do Teorema Chinês do Resto, resolveremos o sistema:

$$\begin{cases} x \equiv 2(mod3) \\ x \equiv 3(mod5) \\ x \equiv 2(mod7). \end{cases}$$

Solução:
Como

$$mdc(3,5) = mdc(3,7) = mdc(5,7) = 1,$$

os inteiros $m_1 = 3$, $m_2 = 5$ e $m_3 = 7$ são dois a dois relativamente primos, logo o sistema tem uma única solução x_0 módulo $m_1m_2m_3 = 105$. Para determinar x_0 seguiremos os passos dados acima:
Passo 1: Determinar m e M_1, M_2, M_3:

$$m = m_1m_2m_3 = 105$$

e

$$M_1 = \tfrac{m}{m_1} = \tfrac{105}{3} = 35, \quad M_2 = \tfrac{m}{m_2} = \tfrac{105}{5} = 21 \quad \text{e} \quad M_3 = \tfrac{m}{m_3} = \tfrac{105}{7} = 15.$$

Passo 2: Determinar os inteiros r_i e s_i:
Escrevendo $1 = mdc(35,3) = mdc(21,5) = mdc(15,7)$ como soma de múltiplos destes inteiros temos:

$$1 = 35.(-1) + 3.12$$
$$1 = 21.1 + 5.(-4)$$
$$1 = 15.1 + 7.(-2)$$

Passo 3: Determinar uma solução particular:
Então

$$x_0 = b_1M_1r_1 + b_2M_2r_2 + b_3M_3r_3 = 2.35.(-1) + 3.21.1 + 2.15.1 = 23.$$

Passo 4: Determinar o conjunto solução:
Como $x_0 = 23$ é uma solução, então

$$S = \{23 + 105t \mid t \in \mathbb{Z}\}.$$

□

Agora que você já entendeu e se familiarizou com o enunciado do Teorema 14, vamos demonstrá-lo. Para tal, precisaremos de alguns resultados, dados no Lema a seguir.

Lema 5. *Dados inteiros m_1, m_2, ...,m_k, para cada $i = 1, 2, ..., k$, definamos*

$$M_i = \frac{m_1m_2...m_{i-1}m_im_{i+1}...m_k}{m_i} = m_1m_2....m_{i-1}m_{i+1}...m_k.$$

Se os inteiros $m_1, m_2, ..., m_k$ são dois a dois relativamente primos, então
(i) M_i e m_i são também relativamente primos, para todo $i = 1, 2, .., n$;
(ii) Se a é um inteiro tal que, $m_i|a$, para todo $i = 1, 2, ..., k$, então $m_1m_2...m_k|a$.

Demonstração:
(i) Como $m_1, m_2, ..., m_k$ são dois a dois relativamente primos, então para cada

$i \in \{1, 2, ..., k\}$ arbitrário, temos:

$$mdc(m_1, m_i) = ... = mdc(m_{i-1}, m_i) = mdc(m_{i+1}, m_i) = ...mdc(m_k, m_i) = 1,$$

logo,

$$mdc(m_1 m_2 ... m_{i-1} m_{i+1} ... m_k, m_i) = 1 \Rightarrow mdc(M_i, m_i) = 1.$$

□

(ii) Faremos a demonstração por indução em k:
Base de Indução: $k = 2$
$m_1|a$ e $m_2|a \Rightarrow a = m_1k_1 = m_2k_2$, com $k_1, k_2 \in \mathbb{Z}$.
Como $mdc(m_1, m_2) = 1 \Rightarrow \exists x, y \in \mathbb{Z}$, tais que:

$$m_1x + m_2y = 1$$

$$\Downarrow (\times a)$$

$$a(m_1x) + a(m_2y) = a \Rightarrow (m_2k_2)(m_1x) + (m_1k_2)(m_2y) = a \Rightarrow m_1m_2(k_2x + k_1y) = a$$

$$\Downarrow$$

$$m_1m_2|a.$$

Passo Indutivo: Vamos assumir, como hipótese de indução, a implicação:

$$m_1|a, m_2|a, ..., m_k|a \Rightarrow m_1m_2...m_k|a.$$

E suponha que, $m_1|a$, $m_2|a$, ..., $m_k|a$, $m_{k+1}|a$. Então,

$$\underbrace{m_1m_2...m_k|a}_{\text{hipótese de indução}} \qquad \text{e } m_{k+1}|a,$$

Pelo item (i), segue que $(m_1m_2...m_k)m_{k+1}|a$. □

Agora vamos à demonstração do teorema.

Demonstração do Teorema 14:

Seja $m = m_1m_2...m_k$ e considere os inteiros:

$$M_1 = \frac{m}{m_1}, \qquad M_2 = \frac{m}{m_2}, ... \qquad M_i = \frac{m}{m_i}, ..., \qquad M_k = \frac{m}{m_k}.$$

Pelo Lema 5,

$$mdc(M_i, m_i) = 1, \forall i = 1, 2, ..., k$$

já que $mdc(m_i, m_j) = 1$, para todo $i \neq j$. Então, existem inteiros r_i, s_i, tais que:

$$M_1.r_1 + m_1.s_1 = 1$$

$$M_2.r_2 + m_2.s_2 = 1$$

$$....$$

$$M_k.r_k + m_k.s_k = 1$$

Mostraremos que

$$x_0 := c_1M_1r_1 + c_2M_2r_2 + ... + c_kM_kr_k.$$

é uma solução particular do sistema.

Observe inicialmente que para todo $i \neq j$, tem-se

$$M_j = m_1...m_i...m_{j-1}m_{j+1}...m_k \Rightarrow m_i|M_j \Rightarrow M_j \equiv 0(modm_i) \Rightarrow c_jr_jM_j \equiv 0(modm_i),$$

Assim, temos as congruências:

$$c_1M_1r_1 \equiv 0(modm_i)$$
$$c_2M_2r_2 \equiv 0(modm_i)$$
$$...$$
$$c_{i-1}M_{i-1}r_{i-1} \equiv 0(modm_i)$$
$$c_{i+1}M_{i+1}r_{i+1} \equiv 0(modn_i)$$
$$...$$
$$c_kM_kr_k \equiv 0(modm_i)$$

De onde obtemos:

$$c_1M_1r_1 + c_2M_2r_2 + c_{i-1}M_{i-1}r_{i-1} + c_{i+1}M_{i+1}r_{i+1} + ... + c_kM_kr_k \equiv 0(modm_i)$$

Somando $c_iM_ir_i$ em ambos os lados da congruência:

$$c_1M_1r_1 + ... + c_{i-1}M_{i-1}r_{i-1} + c_iM_ir_i + c_{i+1}M_{i+1}r_{i+1} + ... + c_kM_kr_k \equiv c_iM_ir_i(modm_i)$$

$$\Downarrow$$

$$x_0 \equiv c_iM_ir_i(mdom_i), \quad \forall i = 1, 2, ..., k$$

Por outro lado, multiplicando por c_i a identidade $M_ir_i + m_is_i = 1$, temos:

$$c_iM_ir_i + c_im_is_i = c_i \Rightarrow c_iM_ir_i - c_i = m_i(c_is_i) \Rightarrow c_iM_ir_i \equiv c_i(modm_i)$$

Por transitividade, tem-se:

$$x_0 \equiv c_i(modm_i), \quad \forall i = 1, 2, ..., k$$

Sendo portanto x_0 solução de todas as congruências do sistema.

Resta mostrar a unicidade desta solução módulo m. Seja w outra solução do sistema. Então para todo $i = 1, 2, ..., k$, temos

$$w \equiv c_i(modm_i) \text{ e } x_0 \equiv c_i(modm_i) \Rightarrow m_i \mid (w - x_0)$$

para todo $i = 1, 2, ..., k$. Comos os m_i são dois a dois relativamente primos, segue do item (ii) do Lema 5 que:

$$m_1m_2...m_k|(w - x_0) \Rightarrow m|(w - x_0)$$

e portanto $w \equiv x_0(modm)$. $\square$

✓ **Exercícios 39.**

Resolva os sistemas lineares abaixo. Use o Teorema Chinês do Resto, quando possível.

(01) $\begin{cases} x \equiv 5(mod6) \\ x \equiv 4(mod11) \\ x \equiv 3(mod7) \end{cases}$

Solução:

Como

$$mdc(6, 11) = mdc(6, 7) = mdc(11, 7) = 1,$$

os inteiros $m_1 = 6$, $m_2 = 11$ e $m_3 = 7$ são dois a dois relativamente primos, portanto o Teorema 14 garante a existência de uma única solução x_0 módulo $m_1m_2m_3$. Vamos determinar x_0.

Passo 1: Determinar m e M_1, M_2, M_3:

$$m = m_1m_2m_3 = 6.11.7 = 462$$

e

$$M_1 = \tfrac{m}{m_1} = \tfrac{462}{6} = 77, \quad M_2 = \tfrac{m}{m_2} = \tfrac{462}{11} = 42 \quad \text{e} \quad M_3 = \tfrac{m}{m_3} = \tfrac{462}{7} = 66.$$

Passo 2: Determine os inteiros r_i e s_i:

Temos:

$$1 = 77.(-1) + 6.13$$

$$1 = 42.5 + 11.(-19)$$

$$1 = 66.(-2) + 7.(19)$$

Passo 3: Determinar uma solução particular:

Então

$$x_0 = b_1M_1r_1 + b_2M_2r_2 + b_3M_3r_3 = 5.77.(-1) + 4.42.5 + 3.66.(-2) = 59.$$

Passo 4: Determinar o conjunto solução:

Como $x_0 = 59$ é uma solução e $m = 462$, então

$$S = \{59 + 462t \mid t \in \mathbb{Z}\}.$$

$\square$

(02) $\begin{cases} 9x \equiv 4(mod 8) \\ 3x \equiv 6(mod 21) \end{cases}$

Solução:

Observe que o sistema dado não está como apresentado no enunciado do Teorema 14, pois $a_1 = 9$ e $a_2 = 3$, ao passo que no teorema os coeficientes das variáveis são todos iguais a 1. Logo, não podemos aplicar o algoritmo diretamente nesse sistema. Para encontrar o conjunto solução, procuremos um sistema equivalente que esteja naquela forma.

Como
$mdc(9,8) = 1 = 9.1+8.(-1)$, então $9x \equiv 4(mod 8)$ é equivalente a $x \equiv 4(mod 8)$;
$mdc(3,21) = 3 = 3.1 + 21.0$, $3x \equiv 6(mod 21)$ é equivalente a $x \equiv 2(mod 7)$.
Assim, o sistema a ser resolvido tem o mesmo conjunto solução do sistema:

$$\begin{cases} x \equiv 4(mod 8) \\ x \equiv 2(mod 7) \end{cases}$$

o qual podemos aplicar o Teorema 14.

Passo 1: Determinar m, M_1 e M_2:
$m_1 = 8$, $m_2 = 7 \Rightarrow m = m_1 m_2 = 56$ e

$$M_1 = \frac{m}{m_1} = 7, \quad M_2 = \frac{m}{m_2} = 8.$$

Passo 2: Determinar os inteiros r_i e s_i:

$$1 = 7.(-1) + 8.1$$

$$1 = 8.1 + 7.(-1)$$

Passo 3: Determinar uma solução particular:

$$x_0 = b_1 M_1 r_1 + b_2 M_2 r_2 = 4.7.(-1) + 2.8.1 = -12.$$

Passo 4: Determinar o conjunto solução:
Como $x_0 = -12$, então

$$S = \{-12 + 56t \mid t \in \mathbb{Z}\}.$$

□

(03) $\begin{cases} x \equiv 4(mod 6) \\ x \equiv 13(mod 15) \end{cases}$

Solução:

Como $mdc(6,15) \neq 1$, não estamos nas condições da hipótese do Teorema 14. Vamos tentar resolvê-lo diretamente.

(i) Resolvendo a primeira equação encontramos:

$$x \equiv 4(mod 6) \Rightarrow x = 4 + 6y,\ y \in \mathbb{Z};$$

(ii) Substituindo este valor na 2a. equação:

$$x \equiv 13(mod 15) \Rightarrow (4 + 6y) \equiv 13(mod 15) \Rightarrow 6y \equiv 9(mod 15)$$

$$\Updownarrow$$

$$y \equiv -6(mod 5) \Rightarrow y = -6 + 5t, t \in \mathbb{Z};$$

Então $x = 4 + 6y = 4 + 6(-6 + 5t) = -32 + 30t, t \in \mathbb{Z}$. Logo,

$$S = \{-32 + 30t \mid t \in \mathbb{Z}\}.$$

□

(04) $\begin{cases} x \equiv 8(mod 14) \\ x \equiv 5(mod 7) \end{cases}$

Solução:

Como $mdc(7, 14) = 7$, o sistema não está de acordo com as hipóteses do Teorema 14. Vamos resolvê-lo diretamente.

(i) Resolvendo a 1^a equação encontramos:

$$x \equiv 8(mod 14) \Rightarrow x = 8 + 14y, y \in \mathbb{Z};$$

(ii) Substituindo este valor na 2^a equação:

$$x \equiv 5(mod 7) \Rightarrow (8 + 14y) \equiv 5(mod 7) \Rightarrow 14y \equiv -3(mod 7);$$

Como $mdc(14, 7) = 7 \nmid -3$, essa equação não tem solução, logo o sistema em questão não tem solução. Assim, seu conjunto solução é

$$S = \emptyset.$$

□

Lista de Exercícios 14.

(01) Encontre o conjunto solução de cada um dos sistemas abaixo:

(a) $\begin{cases} x \equiv 1(mod3) \\ x \equiv 2(mod5) \end{cases}$

(b) $\begin{cases} x \equiv 8(mod6) \\ x \equiv -4(mod7) \end{cases}$

(c) $\begin{cases} x \equiv 3(mod9) \\ 6x \equiv 4(mod8) \end{cases}$

(d) $\begin{cases} x \equiv 1(mod3) \\ x \equiv 2(mod5) \\ x \equiv 3(mod7) \end{cases}$

(e) $\begin{cases} x \equiv 5(mod6) \\ x \equiv 4(mod11) \\ x \equiv 3(mod7) \end{cases}$

(f) $\begin{cases} x \equiv 4(mod6) \\ x \equiv 13(mod15) \\ x \equiv 8(mod14) \\ x \equiv 1(mod7) \end{cases}$

(02) Determine o inteiro positivo, menor que 1000, que na divisão por 13, 36 e 41, deixa como restos 8, 5 e 3, respectivamente.

(03) Determine o menor inteiro positivo, que tem como restos 6 e 5, na divisão por respectivamente 7 e 9.

(04) Determine o menor inteiro positivo, sabendo que seu quádruplo deixa resto 1 na divisão por 13, seu quíntuplo deixa resto 3 na divisão por 7 e seu óctuplo, deixa resto 4 na divisão por 5.

(05) Determinar o menor inteiro $a > 10$ tal que $3|(a+1)$, $4|(a+2)$ e $5|(a+3)$.

Respostas da Lista de Exercícios 14

(01.a) $S = \{7 + 15t \mid t \in \mathbb{Z}\}$.
(01.b) $S = \{80 + 42t \mid t \in \mathbb{Z}\}$.
(01.c) $S = \{66 + 36t \mid t \in \mathbb{Z}\}$.
(01.d) $S = \{52 + 105t \mid t \in \mathbb{Z}\}$.
(01.e) $S = \{59 + 462t \mid t \in \mathbb{Z}\}$.
(01.f) $S = \{-3002 + 210t \mid t \in \mathbb{Z}\}$.
(02) 905
(03) 41
(04) 23
(05) 62.

Capítulo 15

Os Números Naturais

Ao longo de todo este texto, apresentamos diversas propriedades e aplicações dos números inteiros. Tudo o que foi provado teve como alicerce as propriedades apresentadas no Capítulo 1. Dessa forma, a validade de tudo que você aprendeu até então, dependende grandemente da veracidade daquelas afirmações, que foram apresentadas como axiomas, mas não o são. Todas são passíveis de demonstrações. Visando eliminar desestímulos, que surgem em geral, decorrentes da pouca habilidade que tem o aluno, no inicio do curso, para trabalhar com desmonstrações matemática, optamos por assumir as propriedades como verdadeiras (axiomas) e seguir demonstrando as demais propriedades em $\mathbb{Z}$ à partir daqueles axiomas. Estamos agora preparados para retornar àquela propriedades e provar as afirmações feitas no Capítulo 1.

Como em qualquer teoria axiomatica, precisamos de um ponto de partida. O alicerce são os axiomas de Peano, formulados pelo matemático italiano Guiseppe Peano, em 1879. Peano assume a existência de um conjunto satisfazendo certos axiomas, os quais caracterizam de forma rigoroza e precisa, a idéia intuitiva que temos do conjunto dos números naturais. Todas as demais propriedades seguem desses axiomas. A partir da existência do conjunto dos Naturais faremos então a construção do conjunto dos números inteiros para enfim, mostrar todas as propriedades. Neste capítulo, estudaremoss as Propriedades do conjunto $\mathbb{N}$ dos números naturais e no próximo, faremos a construção do conjunto $\mathbb{Z}$ dos números inteiros.

1 Os Axiomas de Peano

Na axiomatização de Peano são dados como objetos não definidos:

- um **conjunto** $\mathbb{N}$, cujos elementos são chamados **números naturais**;
- uma **função** $s : \mathbb{N} \to \mathbb{N}$.

A imagem $s(n)$, de cada $n \in \mathbb{N}$, pela função s é chamada o **sucessor** de n e $s(\mathbb{N}) = \{s(n) \mid n \in \mathbb{N}\}$ é o conjunto imagem dessa função. Com essas notações, apresentamos abaixo os três axiomas de Peano:

(Axioma 1): A função s é injetora, isto é, para quaisquer $m, n \in \mathbb{N}$:

$$m \neq n \Rightarrow s(n) \neq s(m).$$

(Axioma 2): Existe $0 \in \mathbb{N} - s(\mathbb{N})$.

(Axioma 3): **Princípio da Indução**: Se $X \subset \mathbb{N}$ verifica simultaneamente as duas condições:

(i) $0 \in X$;

(ii) Para todo $n \in \mathbb{N}$, temos a implicação: $n \in X \Rightarrow s(n) \in X$;

então,

$$X = \mathbb{N}.$$

O Axioma 1, diz que números naturais distintos tem sucessores distintos. Já o Axioma 2, afirma que existe um número natural que não é sucessor de nenhum outro. Esse número é reprentado pelo símbolo 0 e chamado **zero**. Assim, $0 \neq s(n)$, para todo $n \in \mathbb{N}$. Por sua vez, o Axioma 3, diz que o único subconjunto de $\mathbb{N}$ que contém 0 (zero) e o sucessor de todos os seus elementos, é o próprio $\mathbb{N}$.

À primeira vista, parece ter-se afirmado a existência de um único elemento em $\mathbb{N}$ (Axioma 2). Porém, como $s(\mathbb{N}) \subset \mathbb{N}$, então:

$$X = \{0, s(0), s(s(0)), s(s(s(0))), s(s(s(s(0)))), ...\},$$

é um subconjunto de $\mathbb{N}$, o qual contém 0 e o sucessor de todos os seus elementos, logo pelo Axioma 3, $X = \mathbb{N}$. Assim,

$$\mathbb{N} = \{0, s(0), s(s(0)), s(s(s(0))), s(s(s(s(0)))), ...\}.$$

Dos Axiomas 1 e 2, segue que esses elementos são todos distintos.(Veja questão 01)

Denotaremos por $\mathbb{N}^*$ o conjunto dos números naturais sem 0, isto é,

$$\mathbb{N}^* = \mathbb{N} - \{0\}.$$

Claramente, temos que $\mathbb{N} = s(\mathbb{N}) \cup \{0\}$ e como $0 \notin s(\mathbb{N})$, então,

$$s(\mathbb{N}) = \mathbb{N}^*.$$

Assim, para todo $n \in \mathbb{N}^*$, existe $n' \in \mathbb{N}$, tal que $n = s(n')$.

2 Operações em $\mathbb{N}$

Usando a função s, definem-se duas operações em $\mathbb{N}$, chamadas de adição (+) e multiplicação (.).

Adição em $\mathbb{N}$

Definição 14. *A adição de $m, n \in \mathbb{N}$, denotada por $m+n$, é definida como segue:*

$$\begin{cases} m+0 & = & m; \\ m+s(n) & = & s(m+n). \end{cases}$$

Como $\mathbb{N}^* = s(\mathbb{N})$, dado $m \in \mathbb{N}$, a soma $m+n$, está perfeitamente definida, qualquer que seja $n \in \mathbb{N}$.

Antes de vermos alguns exemplos de uso da definida acima, definiremos o sucessor de 0.

Definição 15. *O sucessor de 0 é chamado de **um** e denotado por **1**, isto é, $s(0) := 1$.*

Definem-se também:

$$\begin{array}{ll} s(1) := 2 & \text{(dois);} \\ s(2) := 3 & \text{(três);} \\ s(3) := 4 & \text{(quatro);} \\ s(4) := 5 & \text{(cinco);} \end{array}$$

e assim, sucessivamente. Dessa forma, temos agora,

$$\mathbb{N} = \{0, s(0), s(s(0), s(s(s(0))), s(s(s(s(0)))), ...\} = \{0, 1, 2, 3, 4, ...\}.$$

Exemplos:
Usando a Definição 14, temos:
(01) $1 + 0 = 1$;

(02) $1 + 1 = 1 + s(0)$ - pela Definição 15
$= s(1 + 0)$ - pela Definição 14
$= s(1) := 2$ - pela Definição 14.

(03) $2 + 1 = 2 + s(0) = s(2 + 0) = s(2) := 3$.

(04) $3 + 4 = 3 + s(3) = s(3 + 3) = s(3 + s(2)) = s(s(3 + 2)) = s(s(3 + s(1)))$
$= s(s(s(3 + 1))) = s(s(s(3 + s(0))) = s(s(s(s(3 + 0))))$
$= s(s(s(s(3)))) = s(s(s(4))) = s(s(5)) = s(6) = 7$.

Definindo $\begin{cases} s^0 = I_{\mathbb{N}} \text{ (função indentidade de } \mathbb{N}) \\ s^n = \underbrace{s \circ s \circ ... \circ s}_{n\times}, \text{ para } n = 1, 2, 3, .. \end{cases}$,
então para quaisquer $m, n \in \mathbb{N}$, tem-se:

$$m + n = s^n(m).$$

Observe, que para todo $m \in \mathbb{N}$, tem-se:

$$m + 1 = m + s(0) = s(m + 0) = s(m).$$

Assim,

$$s(m) = m + 1.$$

Propriedades da Adição

A adição definida em $\mathbb{N}$ tem as seguintes propriedades:

(A'_1) **Associativa**:

$$(m + n) + p = m + (n + p), \quad \forall\, m, n, p \in \mathbb{N}.$$

Demonstração:
Sejam $m, n \in \mathbb{N}$ fixados. Vamos mostrar a propriedade usando indução em p. Considere o conjunto:

$$X = \{p \in \mathbb{N} \mid (m + n) + p = m + (n + p)\}.$$

Para mostrar que $X = \mathbb{N}$, portanto que a propriedade vale para quaisquer $m, n, p \in \mathbb{N}$, é necessário mostrar que $0 \in X$ e que temos a implicação $p \in X \Rightarrow s(p) \in X$.

Pela Definição 14, segue que:

$$(m + n) + 0 = m + n = m + (n + 0) \Rightarrow 0 \in X.$$

Suponha agora $p \in X$. Então

$$\begin{aligned} m + (n + s(p)) &= m + s(n + p) && \text{- pela Definição 14} \\ &= s(m + (n + p)) && \text{- pela Definição 14} \\ &= s((m + n) + p) && \text{- pela hipótese de indução} \\ &= (m + n) + s(p) && \text{- pela Definição 14.} \end{aligned}$$

Assim,

$$m + (n + s(p)) = (m + n) + s(p) \Rightarrow s(p) \in X.$$

Pelo Axioma 3, temos que $X = \mathbb{N}$, conforme queríamos demonstrar. □

(A'_2) **Existência de Elemento Neutro para Adição:**
Zero é o **elemento neutro** da adição, isto é, para todo natural m, tem-se:

$$m + 0 = m = 0 + m.$$

Demonstração:

A primeira identidade já foi dada na Definição 14. Resta mostrar que $0 + m = m, \forall m \in \mathbb{N}$. Para tanto, considere o conjunto:

$$X = \{m \in \mathbb{N} \mid 0 + m = m\}.$$

Como $0 + 0 = 0 \Rightarrow 0 \in X$. Por outro lado, se $m \in X$, isto é, $0 + m = m$, então

$$0 + s(m) = s(0 + m) = s(m) \Rightarrow s(m) \in X \Rightarrow X = \mathbb{N}.$$

$\square$

Obviamente, que 0 é o único elemento em $\mathbb{N}$ com essa própriedade, pois se $u \in \mathbb{N}$, é tal que

$$u + m = m = m + u, \quad \forall m \in \mathbb{N},$$

então teremos:

$$0 = u + 0 = u.$$

Mostrando assim, que o elemento neutro da adição é único.

na identidade $u + 0 = u$, usamos que $u \in \mathbb{N}$ e 0 é o elemento neutro e $u + 0 = 0$, segue de $0 \in \mathbb{N}$ e u ser o elemento neutro.

(A_3') Para qualquer $m \in \mathbb{N}$, tem-se:

$$m + 1 = 1 + m.$$

Demonstração:
Considere o conjunto:

$$X = \{m \in \mathbb{N} \mid m + 1 = 1 + m\}.$$

Pela propriedade (A_2'), $0 + 1 = 1 = 1 + 0 \Rightarrow 0 \in X$. Se $m \in X$, então $m + 1 = 1 + m$. Logo,

$$1+s(m) = s(1+m) = s(m+1) = s(m+s(0)) = s(s(m+0)) = s(s(m)) = s(m)+1$$

$\Rightarrow s(m) \in X$. Pelo Axioma 3, $X = \mathbb{N}$, ou seja, $m + 1 = 1 + m, \forall m \in \mathbb{N}$. $\square$

Assim, para qualquer $m \in \mathbb{N}$, tem-se:

$$\boxed{s(m) = m + 1 = 1 + m.}$$

Na verdade, podemos estender a comutatividade dada em (A_3'), para quaisquer $m, n \in \mathbb{N}$.

(A_4'): **Comutatividade**:

$$m + n = n + m, \quad \forall m, n \in \mathbb{N}.$$

Demonstração:

Sejam $m \in \mathbb{N}$ fixado e $X = \{n \in \mathbb{N} \mid m + n = n + m\}$.
Suponha $n \in \mathbb{N}$, tal que $m + n = n + m$. Então,
$m + s(n) = m + (1 + n)$ - pois, $s(n) = n + 1 = 1 + n$
$= (m + 1) + n$ - por (A'_1)
$= (1 + m) + n$ - por (A'_3)
$= 1 + (m + n)$ - por (A'_1)
$= 1 + (n + m)$ - pela hipótese de indução
$= (1 + n) + m$ - pela propriedade (A'_1)
$= s(n) + m$. - pois $1 + n = s(n)$
Assim, $n \in X \Rightarrow s(n) \in X$ e pela Propriedade (A'_2), $0 \in X$. Consequentemente, $X = \mathbb{N}$. □

(A'_5) **Cancelamento da Adição:**
Dados $m, n, p \in \mathbb{N}$, temos a implicação:

$$m + p = n + p \Rightarrow m = n.$$

Demonstração:
Dados $m, n \in \mathbb{N}$, considere:

$$X = \{p \in \mathbb{N} \mid m + p = n + p \Rightarrow m = n\}.$$

Obviamente, $0 \in X$. E se $p \in X$, então,
$m + s(p) = n + s(p) \Rightarrow m + (p + 1) = n + (p + 1)$ - pois $s(p) = p + 1$
$\Rightarrow (m + p) + 1 = (n + p) + 1$ - por (A'_1)
$\Rightarrow s(m + p) = s(n + p)$ - por (A'_3)
$\Rightarrow m + p = n + p$ - pois s é injetiva
$\Rightarrow m = n$ - pela hipótese de indução.
Logo, $s(p) \in X$. Portanto, $X = \mathbb{N}$. □

✓ **Exercícios 40.**
(01) Sejam $m, n \in \mathbb{N}$. Mostre que se $m + n = 0$, então $m = n = 0$.
Solução:
Suponha, por absurdo, que $m + n = 0$, porém $n \neq 0$, isto é, $n \in \mathbb{N}^* = s(\mathbb{N}) \Rightarrow \exists n' \in \mathbb{N}$, tal que $n = s(n') \Rightarrow 0 = m + n = m + s(n') = s(m + n')$, contrariando o Axioma 2. Assim, $n = 0$ e pela hipótese e Definição 14, temos $0 = m + n = m + 0 = m$. Portanto, $m = n = 0$. □

Multiplicação em $\mathbb{N}$

Definição 16. *A multiplicação de $m, n \in \mathbb{N}$, denotada por $m.n$, é definida como segue:*

$$\begin{cases} m.0 & = & 0; \\ m.s(n) & = & m.n + m. \end{cases}$$

Quando necessário, usaremos apenas mn para o produto $m.n$.

Como $\mathbb{N}^* = s(\mathbb{N})$, segue que está operação está definida para quaisquer $m, n \in \mathbb{N}$.

Exemplos:
Usando as Definições 16 e 14, temos:
(01) $2.0 = 0$;

(02) $2.1 = 2.s(0) = 2.0 + 2 = 0 + 2 = 2$;

(03) $3.2 = 3.s(1) = 3.1+3 = 3.s(0)+3 = (3.0+3)+3 = (0+3)+3 = 3+3 = 6$.

(04) $2.3 = 2.s(2) = 2.2 + 2 = 2.s(1) + 2 = (2.1 + 2) + 2 = (2.s(0) + 2) + 2$
$= ((2.0 + 2) + 2) + 2 = ((0 + 2) + 2) + 2) = (2 + 2) + 2 = 4 + 2 = 6$.

Propriedades da Multiplicação

A Multiplicação definida em $\mathbb{N}$ tem as seguintes propriedades:

(M'_1) Para $m \in \mathbb{N}$:
$$m.0 = 0.m = 0.$$

Demonstração:
Considere $X = \{m \in \mathbb{N} \mid m.0 = 0.m = 0\}$. Pela Definição 16, já temos que $m.0 = 0$. Resta mostrar que $0.m = 0$. Como, $0.0 = 0 \Rightarrow 0 \in X$. E se $m \in X$, pela Definição 16 e a hipótese de indução, temos:
$0.s(m) = 0.m + 0 = 0 + 0 = 0 \Rightarrow s(m) \in X \Rightarrow X = \mathbb{N}$. □

(M'_2) **Distributividade (à direita)**:

$$(m + n)p = mp + np, \quad \forall\, m, n, p \in \mathbb{N}.$$

Demonstração:
Sejam $m, n \in \mathbb{N}$ fixados e considere $X = \{p \in \mathbb{N} \mid (m + n)p = mp + np\}$.
Como $(m + n).0 = 0 = m.0 + n.0$, segue que $0 \in X$. Por outro lado, se $p \in \mathbb{N}$ é tal que $(m + n)p = mp + np$, então
$(m + n)s(p) = (m + n)p + (m + n)$ - Definição 16
$= (mp + np) + (m + n)$ - hipótese de indução
$= (mp + m) + (np + n)$ - propriedades (A'_4) e (A'_1)
$= m.s(p) + n.s(p)$ - Definição 16.
Portanto, $p \in X \Rightarrow s(p) \in X$. Assim, $X = \mathbb{N}$. □

(M'_3) **Existência e Unicidade do Elemento Unidade**:

$$m.1 = 1.m = m, \quad \forall\, m \in \mathbb{N}.$$

Sendo 1 o único elemento em $\mathbb{N}$ com esta propriedade.

Demonstração:
Por (M'_1), essa propriedade é válida para $m = 0$. Além disso, pela Definição 16 e (M'_1), para todo $m \in \mathbb{N}$, tem-se:

$$m.1 = m.s(0) = m.0 + m = 0 + m = m.$$

Em particular, para $m = 1$, temos $1.1 = 1$. Agora, se $m \in \mathbb{N}$ é tal que

$$m.1 = 1.m = m$$

então,

$$1.s(m) = 1.m + 1 = m.1 + 1.1 = (m+1).1 = s(m).1.$$

Portanto, essa propriedade vale para todo natural m.

Resta mostrar a unicidade. Se existe $1' \in \mathbb{N}$, tal que $1'.m = m.1' = m$, para todo $m \in \mathbb{N}$. Como $1, 1' \in \mathbb{N}$, segue que $1 = 1.1' = 1'$. $\square$

(M'_4) **Comutatividade:**

$$m.n = n.m, \quad \forall, m, n \in \mathbb{N}.$$

Demonstração:
Fixado $m \in \mathbb{N}$, seja $n \in \mathbb{N}$, tal que $m.n = n.m$. Usando (M'_3) e (M'_2) e a hipótese de indução:

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

Assim, temos a implicação $m.n = n.m \Rightarrow m.s(n) = s(n).m$ e como $m.0 = 0.m$, segue a validade da propriedade para quaisquer $m, n \in \mathbb{N}$. $\square$

Usando a comutivativa, podemos estender a distributividade para também à esquerda, isto é, para todo $m, n, p \in \mathbb{N}$:

$$p(m+n) = pm + pn.$$

(M'_4) **Associatividade**:

$$(mn)p = m(np), \quad \forall\, m, n, p \in \mathbb{N}.$$

Demonstração:
Sejam $m, n \in \mathbb{N}$ fixados e considere o conjunto:

$$X = \{p \in \mathbb{N} \mid (mn)p = m(np)\}.$$

Pela Definição 16, temos:

$$(mn).0 = 0 = m.(n.0) \Rightarrow 0 \in X.$$

Além disso, por (M_3'), temos que $(mn).1 = mn = m(n.1) \Rightarrow 1 \in X$.
Assim, se $p \in X$, então $(mn)p = m(np)$. Daí,
$(mn).s(p) = (mn)p + mn$ - Definição 16
$= (mn)p + (mn).1$ - por (M_3')
$= m(np) + (mn).1$ - hipótese de indução
$= m(np) + m(n.1)$ - $1 \in X$
$= m(np + n.1)$ - pela distributividade
$= m(n(p + 1))$ -pela distributividade
$= m(n.s(p))$.
Assim,

$$(mn).s(p) = m(n.s(p)) \Rightarrow s(p) \in X \Rightarrow X = \mathbb{N}.$$

□

3 Ordem em $\mathbb{N}$

Definiremos agora uma relação em $\mathbb{N}$, que nos permite colocar os números naturais em uma sequência, formalizando assim a idéia intuitiva que temos de ordem nesse conjunto.

Se $m \leq n$, diz-se também que n é maior do que ou igual a m.

Definição 17. *Dados $m, n \in \mathbb{N}$, dizemos que m é menor do que ou igual a n, simbolicamente escrevemos $m \leq n$, se existe $p \in \mathbb{N}$, tal que*

$$n = m + p.$$

Dizemos que m é (estritamente) menor do que n, e escrevemos $m < n$, se $m \leq n$, porém $m \neq n$, isto é, existe $p \in \mathbb{N}^*$, tal que $n = m + p$.

Exemplos:
(01) $4 \leq 6$, pois $6 = 4 + 2$;
(02) $4 \leq 4$, pois $4 = 4 + 0$;
(03) $4 < 6$, pois $4 = 6 + 2$ e $2 \neq 0$.

✓ Exercícios 41.

(01) Sejam $m, n \in \mathbb{N}$. Mostre que se $m < n$, então $m + 1 \leq n$.
Solução:
$m < n \Rightarrow n = m + p$, com $p \in \mathbb{N}^* \Rightarrow p = s(p') = p' + 1$. Assim,

$$n = m + (p' + 1) = (m + 1) + p' \Rightarrow m + 1 \leq n.$$

□

Propriedades da Relação de Ordem em $\mathbb{N}$

Vejamos algumas propridades que tem a relaçao de ordem, definida acima.

A relação $\leq$, definida em $\mathbb{N}$, tem as seguintes propriedades:

(R'_1) **Reflexiva:**
Para qualquer $m \in \mathbb{N}$, tem-se
$$m \leq m.$$

Demonstração:
Como $m = m + 0 \Rightarrow m \leq m$. □

(R'_2) **Antissimétrica:**
Para quaisquer $m, n \in \mathbb{N}$ tem-se:
$$m \leq n \quad \text{e} \quad n \leq m \Rightarrow m = n.$$

Demonstração:
Se $m \leq n \Rightarrow n = m + p_1$, $p_1 \in \mathbb{N}$;
e
$n \leq m \Rightarrow m = n + p_2$, $p_2 \in \mathbb{N}$.
Usando a propriedade (A'_5) e Exercício 40, segue que: $m = m + (p_1 + p_2) \Rightarrow p_1 + p_2 = 0 \Rightarrow p_1 = p_2 \Rightarrow m = n$. □

(R'_3) **Transistiva:**
Para quaisquer m, n, $p \in \mathbb{N}$, tem-se:
$$m \leq n \quad \text{e} \ n \leq p \Rightarrow m \leq p.$$

Demonstração:
$m \leq n \Rightarrow n = m + q_1$, $q_1 \in \mathbb{N}$
e
$n \leq p \Rightarrow p = n + q_2$, $q_2 \in \mathbb{N}$.
Daí,
$p = n + q_2 = (m + q_1) + q_2 = m + (q_1 + q_2)p \leq m$. □

Por possuir as propriedades (R'_1), (R'_2) e (R'_3), dizemos que $\leq$ é uma relação de ordem em $\mathbb{N}$ e que $\mathbb{N}$ é um conjunto ordenado. Veremos que esta ordem compatível com as operações definidas em $\mathbb{N}$, conforme propriedade (R'_4) abaixo.

(R'_4) **Monotonicidade:**
Sejam $m, n \in \mathbb{N}$. Se
$$m \leq n,$$
então, para qualquer número natural p, também temos:
(i) $m + p \leq n + p$;

(ii) $mp \leq np$.

Demonstração:
Suponha $m \leq n$, então existe $h \in \mathbb{N}$, tal que $n = m + h$. Segue daí que:
(i) $(n + p) = (m + p) + h \Rightarrow m + p \leq m + p$
e
(ii) $np = (m + h)p = mp + hp \Rightarrow mp \leq np$.

$\square$

(R_5') **Tricotomia em** $\mathbb{N}$:
Para quaisquer m e $n \in \mathbb{N}$, verifica-se uma, e somente uma, das condições:
(i) $m < n$;
(ii) $m = n$;
(iii) $n < m$.

Demonstração:
Inicialmente, vamos mostrar que quaisquer duas delas não podem ocorrer simultaneamente. Por definição, (ii) é incompatível com (i) e com (ii). Suponhamos que tenhamos as condições (i) e (iii) simultaneamente, isto é, $m < n$ e $n < m$. Então, existem $p, p' \in \mathbb{N}^*$ tais que:

$$n = m + p \text{ e } m = n + p' \Rightarrow m + 0 = m + (p + p') \Rightarrow 0 = p + p'$$

Pelo Exercício 40 acima, segue que $p = p' = 0$, uma contradição. Assim, quaisquer duas delas não podem ocorrer simultaneamente. Resta mostrar que uma delas sempre ocorre.

Considere $m \in \mathbb{N}$ fixado e n arbitrário. Mostraremos, usando indução em n. Seja
$$X = \{n \in \mathbb{N} \mid m < n \text{ ou } m = n \text{ ou } n < n\}.$$
Como $m \in \mathbb{N}$ é arbitrário, então

$$m = 0 \quad \text{ou} \quad m \neq 0 \Rightarrow m = s(m') > 0.$$

Logo, $0 \in X$.
Suponha agora, $n \in X \Rightarrow m < n$ ou $m = n$ ou $n < m$. Vejamos o que pode-se deduzir sobre $s(n)$ em cada uma dessas situações:
(i) $m < n$:
$\Rightarrow \exists\, p \in \mathbb{N}^*$, tal que $n = m + p \Rightarrow s(n) = n + 1 = m + (p + 1) \Rightarrow s(n) > m$;
(ii) $m = n$:
$\Rightarrow s(n) = s(m) = m + 1 \Rightarrow s(n) > m$;
(iii) $n < m$:
$\Rightarrow \exists\, p \in \mathbb{N}^*$, tal que $m = n + p$. Como $p \neq 0 \Rightarrow p = p' + 1$
$\Rightarrow m = (n + 1) + p' \Rightarrow m = s(n) + p' \Rightarrow s(n) = m$, se $p' = 0$ ou $s(n) < m$, se $p' \neq 0$.
Assim, $n \in X \Rightarrow s(n) \in X$. Portanto, $X = \mathbb{N}$. $\square$

Com uso da tricotomia, podemos também enunciar a propriedade do cancelamento para a multiplicação em $\mathbb{N}$.

(R_6') **Cancelamento na Multiplicação**:
Sejam $m, n, p \in \mathbb{N}$. Se

$$mp = np, \quad \text{com} \quad p \neq 0, \quad \text{então } m = n.$$

Demonstração:
Suponhamos que temos a identidade $mp = np$, porém $m \neq n$. Pela Tricotomia, segue que $m < n$ ou $n < m$. Como $p \neq 0$, segue que $mp < np$ ou $np < mp$ (veja questão 16), contrariando a hipótese. Assim, necessariamente, $m = n$.$\square$

4 Princípio da Boa Ordem em $\mathbb{N}$

Lembremos que s_0 é o elemento mínimo de um subconjunto $S \subset \mathbb{N}$, isto é, $s_0 = minS$, se $s_0 \in S$ e $s_0 \leq x$, para todo $x \in S$.

Exemplos:
(01) Considere $S = \{7, 14, 23, 28, 29, 30, 31...\} \subset \mathbb{N}$.
Tomemos agora o conjunto:

$$X = \{n \in \mathbb{N} \mid n \leq x, \, \forall x \in S\} = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

X é um subconjunto próprio de $\mathbb{N}$ (isto é, $X \subset \mathbb{N}$, porém $X \neq \mathbb{N}$) que contém 0. Pelo Axioma 3, isso implica existir $x \in X$, tal que $s(x) \notin X$. No caso, esse elemento é 7 e observe que $7 = minS$.

(02) Seja $S = \{23, 45, 60, 80, 203\} \subset \mathbb{N}$.
Tomemos agora o conjunto

$$X = \{n \in \mathbb{N} \mid n \leq x, \, \forall x \in S\} = \{0, 1, 2, 3, 4, ..., 23\}$$

Como $0 \in X$ e $X \subsetneqq \mathbb{N}$, então existe $x \in X$, tal que $s(x) \notin X$. No caso, $x = 23 = minS$.

Vamos generalizar o que foi feito acima, para mostrar o Princípio da Boa Ordem em $\mathbb{N}$.

Teorema 15. ***(Princípio da Boa Ordem em*** $\mathbb{N}$*)*
Todo subconjunto não vazio de $\mathbb{N}$ *tem elemento mínimo.*

Demonstração:
Seja S um subconjnto não vazio de $\mathbb{N}$. Vamos mostrar que existe $s_0 = minS$. Como nos exemplos acima, vamos considerar o conjunto:

$$X = \{n \in \mathbb{N} \mid n \leq x, \, \forall x \in S\}.$$

$S \neq \emptyset$, logo existe $s \in S$ e como $s < s + 1 \Rightarrow s + 1 \notin X$. Por outro lado, $0 \leq x, \forall x \in \mathbb{N}$, logo $0 \in X$. Assim, X é um subconjunto próprio de $\mathbb{N}$ que contém 0. Pelo Axioma 3, deve necessariamente exitir $s_0 \in X$, porém $s(s_0) = s_0 + 1 \notin X$. Vamos mostrar que $s_0 = minS$. De fato, com $s_0 \in X$, então $s_0 \leq x, \forall x \in S$. Resta mostrar que $s_0 \in S$. Suponha, por absurdo, que isso não ocorra, isto é, $s_0 \notin S$. Neste caso, temos a desigualdade estrita $s_0 < x, \forall\, x \in S$. Pelo Exercício 41, temos $s_0 + 1 \leq x, \forall x \in S \Rightarrow s(s_0) \in X$, uma contradição. Assim, $s_0 \in S$, sendo portanto $s_0 = minS$. $\square$

Lista de Exercícios 15.

(01) Moste que se os elementos do conjunto $\{0, s(0), s(s(0)), s(s(s(0))), ...\}$ são todos distintos.

(02) Mostre que $s(\mathbb{N}) = \mathbb{N}^*$.

(03) Mostre que para quaisquer $m, n \in \mathbb{N}$, a soma $m + n$ está perfeitamente definida.

(04) Usando a Definição 14, calcule:
(a) $2 + 5$;
(b) $4 + 9$;

(05) Mostre que para quaisquer $m, n \in \mathbb{N}$, tem-se, $m + n = s^n(m)$, onde s^0 é a função identidade em $\mathbb{N}$ e para $n = 1, 2, 3, ...$, $s^n = \underbrace{s \circ s \circ ... \circ s}_{n\times}$.

(06) Usando a questão (05), calcule:
(a) $7 + 8$
(b) $8 + 7$
(c) $8 + 0$
(d) $0 + 8$

(07) Mostre que a multiplicação em $\mathbb{N}$ está definida, quaisquer que sejam $m, n \in \mathbb{N}$.

(08) Usando a Definição 16, calcule:
(a) 3.5
(b) 0.5
(c) 5.5
(d) 8.10

(09) Mostre que para quaisquer números naturais m e $n \geq 1$, tem-se $m.n = \underbrace{m + m + ... + m}_{n\times}$.

(10) Responda e justifique:
(a) $8 \leq 8$?
(b) $8 < 8$?
(c) $8 \leq 9$?
(d) $8 < 9$?
(e) $9 < 8$?

(11) Mostre que para todo $n \in \mathbb{N}$, $s(n) > 0$.

(12) Sejam $m, n \in \mathbb{N}$. Mostre que $m.n = 0 \Rightarrow m = 0$ ou $n = 0$.

(13) Mostre que para todo $n \in \mathbb{N}$, $n > 0$. Em particular, $1 > 0$.

(14) Mostre que $s(n) > n$, para todo $n \in \mathbb{N}$.

(15) Sejam $m, n, p \in \mathbb{N}$. Mostre que $m < n$, então $m + p < n + p$.

(16) Sejam $m, n, p \in \mathbb{N}$. Mostre que $m < n$ e $p \neq 0$, então $mp < np$.

(17) Sejam $m, n, p \in \mathbb{N}$. Mostre que $m + p \leq n + p$, então $m \leq n$.

(18) Sejam $m, n, p \in \mathbb{N}$. Mostre que $mp \leq np$ e $p \neq 0$, então $m \leq n$.

(19) Sejam m, n naturais. Mostre que $m + n = 1 \Rightarrow m = 1$ ou $n = 1$.

(20) Sejam $a \in \mathbb{N}$ e $X \subset \mathbb{N}$. Mostre que se X satisfaz simultaneamente as condições:
$a \in X$ e $x \in X \Rightarrow s(x) \in X$, então $X = \{a, s(a), s(s(a)), ...\}$.

Capítulo 16

A Construção de $\mathbb{Z}$

1 Introdução

Neste Capítulo faremos a construção teórica do conjunto $\mathbb{Z}$ dos números inteiros e então provaremos as propriedades apresentadas, como axiomas, no Capítulo 1.

A equação

$$x + 2 = 7$$

tem uma única solução no conjunto dos números naturais. Embora, a "subtração" não esteja definida em $\mathbb{N}$, sabemos que a solução é obtida, efetuando a diferença $7 - 2$.

Por outro, a equação

$$x + 7 = 2$$

não tem solução em $\mathbb{N}$. Nesse caso, a solução $(2 - 7)$ não pertence ao conjunto dos naturais. Nosso objetivo, é então "ampliar"o conjunto dos naturais, usando tão somente o recurso teórico desenvolvido no capítulo anterior, para um conjunto que contenha também as soluções de equações desse tipo.

Generealizando, para cada par de números naturais (a, b), sabemos que a solução da equação

$$x + b = a$$

é dada pelo "número"$a - b$. Assim, para cada par de números naturais (a, b), podemos definir o número inteiro $z(a, b) := a - b$ e o conjunto $\mathbb{Z}$, dos números inteiros, por:

$$\mathbb{Z} = \{z(a, b) \mid a, b \in \mathbb{N}\}$$

Essa estratégia apresenta dois inconvenientes a serem contornados:
(i) Existem infinitos pares de naturais $(a_1, b_1), (a_2, b_2), (a_3, b_2), ...$, cuja diferença geram o mesmo inteiro z. Por exemplo, $(7, 2)$, $(22, 17)$, $(5, 0)$ representam o mesmo inteiro. Logo, os elementos em $\mathbb{Z}$ não são todos distintos;
(ii) A diferença $a - b$ não foi definida em $\mathbb{N}$;

Para contornar o primeiro problema, podemos definir uma relação de equivalência, de modo que todos os pares de números naturais que gerem o mesmo inteiro, pertençam à mesma classe de equivalência. E definimos o inteiro, não como a diferença, e sim como a classe de equivalência, a qual conterá todos os pares relacionados entre si. Desses modo, pares que geram o mesmo inteiro serão visto como um único objeto. Assim, se $a - b = c - d$, então diremos que (a, b) e (c, d) estão relacionados pela relação em questão. Representando a relaçao por $\sim$, podemos definir:

$$(a, b) \sim (c, d) \Leftrightarrow a - b = c - d.$$

Por fim, precisamos eliminar dessa definição a "diferença", por não ser uma operação definida em $\mathbb{N}$. Como $a - b = c - d \Leftrightarrow a + d = b + c$. Então, diremos que $(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$. Formalizaremos tudo a seguir.

2 A Relação de Equivalencia em $\mathbb{N} \times \mathbb{N}$

Definamos no conjunto $\mathbb{N} \times \mathbb{N} = \{(a, b) \mid a, b \in \mathbb{N}\}$ a seguinte relação:

$$\boxed{(a, b) \sim (c, d) \Leftrightarrow a + d = b + c.}$$

Exemplos:
(01) $(11, 6) \sim (8, 3)$, pois $11 + 3 = 6 + 8$;
(02) $(0, 7) \sim (2, 9)$, pois $0 + 9 = 7 + 2$;
(03) $(1, 4) \not\sim (4, 1)$, pois $1 + 1 \neq 4 + 4$.

A relação definida acima tem as seguintes propriedades para quaisquer $(a, b), (c, d), (e, f) \in \mathbb{N} \times \mathbb{N}$:

(1) Reflexiva: $(a, b) \sim (a, b)$.
Demonstração:
Pela comutativade da adição em $\mathbb{N}$, temos $a + b = b + a \Rightarrow (a, b) \sim (a, b)$. $\square$

(2) Simétrica: Se $(a, b) \sim (c, d) \Rightarrow (c, d) \sim (a, b)$.
Demonstração:
Se $(a, b) \sim (c, d) \Rightarrow a + d = b + c \Rightarrow c + b = d + a \Rightarrow (c, d) \sim (a, b)$. $\square$

(3) Transitiva: Se $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$, então $(a, b) \sim (e, f)$.
Demonstração:
$(a, b) \sim (c, d) \Rightarrow a + d = b + c$
e
$(c, d) \sim (e, f) \Rightarrow c + f = d + e$.
Pela comutatividade e associativade em $\mathbb{N}$, segue então que

$$(a + d) + (c + f) = (b + c) + (d + e) \Rightarrow (a + f) + (d + c) = (b + e) + (d + c).$$

Pelo cancelamento da adição em $\mathbb{N}$, obtemos:

$$a + f = b + e \Rightarrow (a, b) \sim (e, f).$$

$\square$

Fica dessa forma provada que $\sim$ é uma relação de quivalência em $\mathbb{N} \times \mathbb{N}$.

3 Classes de Equivalência

Para cada $(a, b) \in \mathbb{N} \times \mathbb{N}$, denotaremos por $\overline{(a, b)}$, o conjunto de todos os elementos de $\mathbb{N} \times \mathbb{N}$, que estão relacionados com (a, b) pela relação $\sim$:

$$\overline{(a, b)} := \{(c, d) \in \mathbb{N} \times \mathbb{N} \mid (a, b) \sim (c, d)\}.$$

$\overline{(a, b)}$ é chamado a classe de equivalência de (a, b) pela relação de equivalência $\sim$. Cada elemento desse conjunto é chamado um **representante** da classe.

Exemplos:

$$\begin{aligned}(01)\ \overline{(3,1)} &= \{(x, y) \in \mathbb{N}^2 \mid (3, 1) \sim (x, y)\} = \{(x, y) \in \mathbb{N}^2 \mid 3 + y = x + 1\}\\ &= \{(y + 2, y) \mid y \in \mathbb{N}\} = \{(2, 0), (3, 1), (4, 2), (5, 3), ...\};\end{aligned}$$

$$\begin{aligned}(02)\ \overline{(2,7)} &= \{(x, y) \in \mathbb{N}^2 \mid (2, 7) \sim (x, y)\} = \{(x, y) \in \mathbb{N}^2 \mid 2 + y = 7 + x\}\\ &= \{(x, 5 + x) \mid x \in \mathbb{N}\} = \{(0, 5), (1, 6), (2, 7), (3, 8), ...\}.\end{aligned}$$

$$\begin{aligned}(03)\ \overline{(4,4)} &= \{(x, y) \in \mathbb{N}^2 \mid (4, 4) \sim (x, y)\} = \{(x, y) \in \mathbb{N}^2 \mid 4 + y = 4 + x\}\\ &= \{(x, x) \mid x \in \mathbb{N}\} = \{(0, 0), (1, 1), (2, 2), (3, 3), ...\}.\end{aligned}$$

Como $\sim$ é uma relação reflexiva, então para todo par $(a, b) \in \mathbb{N} \times \mathbb{N}$, tem-se que $(a, b) \in \overline{(a, b)}$. Assim, se $\overline{(a, b)} = \overline{(c, d)}$, então $(a, b) \sim (c, d)$. Reciprocamente, se $(a, b) \sim (c, d)$, então dado $(x, y) \in \overline{(a, b)} \Rightarrow (x, y) \sim (a, b)$ e como temos $(a, b) \sim (c, d)$, por transitividade, tem-se que $(x, y) \sim (c, d) \Rightarrow (x, y) \in \overline{(c, d)} \Rightarrow \overline{(a, b)} \subset \overline{(c, d)}$. De modo análogo, obtemos a inclusão no outro sentido. Portanto, temos um resultado análogo ao que foi obtido para a relação de congruência definida em $\mathbb{Z}$, estuda no Capítulo 9:

$$\overline{(a, b)} = \overline{(c, d)} \Leftrightarrow (a, b) \sim (c, d).$$

Na verdade, esse é um resulto válida em qualquer relação de equivalencia:

$$\boxed{\text{Classes de equivalência iguais} \Leftrightarrow \text{seus representantes estão relacionados.}}$$

Exemplos: Usando os exemplos anteriores, da observação acima, temos que:
(01) $\overline{(2, 0)} = \overline{(3, 1)} = \overline{(4, 2)} = \overline{(200, 198)}$;

(02) $\overline{(0,5)} = \overline{(2,7)} = \overline{(1,6)} = ... = \overline{(314,319)}$;

(03) $\overline{(0,0)} = \overline{(1,1)} = \overline{(4,4)} = ... = \overline{(415,415)}$.

4 O Conjunto dos Números Inteiros

O Conjunto de todas as classes de equivalência, pela relação $\sim$, é denotado por $\mathbb{Z}$ e chamado o conjunto dos números inteiros. Então, por definição,

o Símbolo $\mathbb{Z}$ vem da palavra alemã *Zahl*, que significa número.

$$\mathbb{Z} := \{\overline{(a,b)} \mid a, b \in \mathbb{N}\}.$$

Dessa forma, cada número inteiro $\alpha \in \mathbb{Z}$ é na verdade uma classe de equivalência, isto é,

$$\alpha := \overline{(a,b)} = \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid a + x = b + y\}$$

sendo portando, um conjuto de pares ordenados de números naturais.

A construção de $\mathbb{Z}$ foi pensado como uma extensão de $\mathbb{N}$. Porém, esses conjuntos tem objetos de naturezas distintas. A próxima proposição mostra como podemos associar a cada número natural m uma única classe de equivalência em $\mathbb{Z}$, e assim "enxergar" $\mathbb{N}$ como subconjunto de $\mathbb{Z}$.

Proposição 20. *A função $f : \mathbb{N} \to \mathbb{Z}$, definida por:*

$$f(m) = \overline{(m,0)}$$

é injetora.

Demonstração:
Sejam $m_1, m_2 \in \mathbb{N}$, tais que:

$$f(m_1) = f(m_2) \Rightarrow \overline{(m_1,0)} = \overline{(m_2,0)} \Rightarrow (m_1,0) \sim (m_2,0) \Rightarrow m_1+0 = 0+m_2 \Rightarrow m_1 = m_2.$$

Logo, f é injetora. $\square$

A imagem de f é o conjunto:

$$f(\mathbb{N}) = \{\overline{(m,0)} \mid m \in \mathbb{N}\} \subset \mathbb{Z}.$$

E como f é injetora, então a restrição $f : \mathbb{N} \to f(\mathbb{N})$ é uma bijeção, logo temos que $\mathbb{N} \simeq f(\mathbb{N}) \subset \mathbb{Z}$. Assim, por meio da identifição

$$m \leftrightarrow \overline{(m,0)}$$

podemos pensar $\mathbb{N}$ como um subconjunto de $\mathbb{Z}$. A função f, definida na proposição acima, é chamada *imersão* de $\mathbb{N}$ em $\mathbb{Z}$.

Exemplos:
Com a identicação acima tem-se que:
. 0 corresponde ao inteiro $\overline{(0,0)} = \{(m,m) \mid m \in \mathbb{N}\}$;
. 1 corresponde ao inteiro $\overline{(1,0)} = \{(m+1,m) \mid m \in \mathbb{N}\}$;
...
. 7 corresponde ao inteiro $\overline{(7,0)} = \{(m+7,m) \mid m \in \mathbb{N}\}$.
...
No geral, para $a \in \mathbb{N}$, usaremos
a para representar o inteiro $\overline{(a,0)} = \{(m+a,m) \mid m \in \mathbb{N}\}$.

5 Operações em $\mathbb{Z}$

Definiremos agora duas operações $\mathbb{Z}$, uma adição (+) e uma multiplicação (.).

Adição em $\mathbb{Z}$

Definição 18. *Dados $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Z}$, definimos a soma $\overline{(a,b)} + \overline{(b,c)}$ como abaixo:*
$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)}.$$

Exemplos:
(01) $\overline{(3,4)} + \overline{(9,2)} = \overline{(12,6)}$;
(02) $\overline{(10,11)} + \overline{(15,8)} = \overline{(25,19)}$;
(03) $\overline{(3,3)} + \overline{(14,3)} = \overline{(17,6)}$;
(04) $\overline{(5,2)} + \overline{(2,5)} = \overline{(7,7)}$.

Uma vez que a classe representante da soma é obtida operando-se com os representes tomados para as classes, precisamos garantir que essa operação está bem definido, isto é, independe do representante escolhido para a classe.

Proposição 21. *Sejam $a, a', b, b', c, c', d, d' \in \mathbb{N}$. Se*
$$\overline{(a,b)} = \overline{(a',b')} \quad e \quad \overline{(c,d)} = \overline{(c',d')},$$
então
$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a',b')} + \overline{(c',d')}.$$

Demonstração:
$\overline{(a,b)} = \overline{(a',b')} \Rightarrow (a,b) \sim (a',b') \Rightarrow a + b' = b + a'$
e
$\overline{(c,d)} = \overline{(c',d')} \Rightarrow (c,d) \sim (c',d') \Rightarrow c + d' = d + c'$.
Segue daí, que:
$$(a+b') + (c+d') = (b+a') + (d+c').$$
Pela comutatividade e associatividade da adição em $\mathbb{N}$, tem-se:
$$(a+c) + (b'+d') = (b+d) + (a'+c')$$

$$\Downarrow \quad \text{(pela definição de } \sim\text{)}$$

$$(a+c, b+d) \sim (a'+c', b'+d')$$

$$\Downarrow \quad \text{(elementos relacionados, classes iguais)}$$

$$\overline{(a+c, b+d)} = \overline{(a'+c', b'+d')}$$

$$\Downarrow \quad \text{(Definição 18)}$$

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a',b')} + \overline{(c',d')}.$$

□

Veremos que a função imersão definida na Proprosição 20 preserva a soma, conforme dado na proposição a seguir.

Proposição 22. *Considerando a função imersão* $f : \mathbb{N} \to \mathbb{Z}$, *definida na Proposição 20, para quaisquer* $m_1, m_2 \in \mathbb{N}$, *tem-se:*

$$f(m_1 + m_2) = f(m_1) + f(m_2)$$

Demonstração:
De fato, dados $m_1, m_2 \in \mathbb{N}$, então

$$f(m_1 + m_2) = \overline{(m_1 + m_2, 0)} = \overline{(m_1, 0)} + \overline{(m_2, 0)} = f(m_1) + f(m_2).$$

□

Propriedades da Adição em $\mathbb{Z}$

A adição definida em $\mathbb{Z}$ tem as seguintes propriedades:

(A1) **Comutativa:**
Para quaisquer α e $\beta \in \mathbb{Z}$, tem-se:

$$\alpha + \beta = \beta + \alpha.$$

Demonstração:
Sejam $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)} \in \mathbb{Z}$. Usando a a comutatividade da adição em $\mathbb{N}$, temos:

$$\begin{aligned}\alpha + \beta &= \overline{(a,b)} + \overline{(c,d)} \\ &= \overline{(a+c, b+d)} \\ &= \overline{(c+a, d+b)} \\ &= \overline{(c,d)} + \overline{(a,b)} \\ &= \beta + \alpha.\end{aligned}$$

□

(A2) **Associativa:**
Para quaisquer α, β e $\gamma \in \mathbb{Z}$, tem-se:

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma).$$

Demonstração:
Sejam $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)} \in \mathbb{Z}$. Usando a associativada e a comutatividade da adição em $\mathbb{N}$, temos:

$$\begin{aligned}
(\alpha + \beta) + \gamma &= (\overline{(a,b)} + \overline{(c,d)}) + \overline{(e,f)} \\
&= \overline{(a+c, b+d)} + \overline{(e,f)} \\
&= \overline{((a+c)+e, (b+d)+f)} \\
&= \overline{(a+(c+e), b+(d+f))} \\
&= \overline{(a,b)} + \overline{((c+e),(d+f))} \\
&= \overline{(a,b)} + (\overline{(c,d)} + \overline{(e,f)}) \\
&= \alpha + (\beta + \gamma).
\end{aligned}$$

□

(A3) **Existencia e Unicidade do Elemento Neutro da Adição:**
A classe $0 = \overline{(0,0)} \in \mathbb{Z}$ é elemento neutro da adição, isto é, para qualquer $\alpha \in \mathbb{Z}$, tem-se:

$$\alpha + 0 = \alpha.$$

Demonstração:
De fato, como 0 é o elemento neutro da adição em $\mathbb{N}$, então dado $\alpha = \overline{(a,b)} \in \mathbb{Z}$:

$$\alpha + 0 = \overline{(a,b)} + \overline{(0,0)} = \overline{(a+0, b+0)} = \overline{(a,b)} = \alpha.$$

□

A demonstração da unicidade é análoga àquela feita para a adição em $\mathbb{N}$. □

(A4) **Existência e unicidade do oposto:**
Para todo $\alpha \in \mathbb{Z}$, existe um único $\beta \in \mathbb{Z}$, tal que

$$\alpha + \beta = 0.$$

Demonstração:
Dado $\alpha = \overline{(a,b)} \in \mathbb{Z}$, tomando $\beta = \overline{(b,a)} \in \mathbb{Z}$, temos:

$$\alpha + \beta = \overline{(a,b)} + \overline{(b,a)} = \overline{(a+b, b+a)} = \overline{(0,0)} = 0.$$

Se β e $\beta' \in \mathbb{Z}$ são tais que $\alpha + \beta = \alpha + \beta' = 0$, segue das propriedades (A1), (A2) e (A3) acima que:

$$\beta = \beta + 0 = \beta + (\alpha + \beta') = (\beta + \alpha) + \beta' = 0 + \beta' = \beta'.$$

□

Assim, dado $\alpha \in \mathbb{Z}$, existe um único $\beta \in \mathbb{Z}$, tal que $\alpha + \beta = 0$. O inteiro β é chamado o **oposto**, (simétrico ou inverso aditivo) de α e denotado por $-\alpha$. Assim, para qualquer $\alpha \in \mathbb{Z}$, tem-se:

$$\alpha + (-\alpha) = 0.$$

(A5) **Cancelamento da adição em $\mathbb{Z}$**:
Para quaisquer $\alpha, \beta, \gamma \in \mathbb{Z}$, temos a implicação:

$$\alpha + \gamma = \beta + \gamma \Rightarrow \alpha = \beta.$$

Demonstração:
Sejam $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)} \in \mathbb{Z}$. Então:
$\alpha + \gamma = \beta + \gamma \Rightarrow \overline{(a,b)} + \overline{(e,f)} = \overline{(c,d)} + \overline{(e,f)}$
$\Rightarrow \overline{(a+e, b+f)} = \overline{(c+e, d+f)}$ - Definição 18
$\Rightarrow (a+e, b+f) \sim (c+e, d+f)$ - classes iguais, representantes relacionados
$\Rightarrow (a+e)+(d+f) = (b+f)+(c+e)$ - definição da relação $\sim$
$= (a+d)+(e+f) = (b+c)+(e+f)$ - por (M'1) e (M'5) em $\mathbb{N}$
$\Rightarrow a+d = b+c$ - cancelamento da adição em $\mathbb{N}$
$\Rightarrow \underline{(a,b)} \sim \underline{(c,d)}$ - definição de $\sim$
$\Rightarrow \overline{(a,b)} = \overline{(c,d)}$ - elementos relacionaos, classes iguais
$\Rightarrow \alpha = \beta$. $\square$

Multiplicação em $\mathbb{Z}$

Definição 19. *Dados $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Z}$ definimos o produto $\overline{(a,b)}.\overline{(b,c)}$ como abaixo:*

$$\overline{(a,b)}.\overline{(c,d)} = \overline{(ac+bd, ad+bc)}.$$

Exemplos:
(01) $\overline{(3,4)}.\overline{(9,2)} = \overline{(3.9+4.2, 3.2+4.9)} = \overline{(35,42)}$;
(02) $\overline{(10,11)}.\overline{(15,8)} = \overline{(10.15+11.8, 10.8+11.15)} = \overline{(238,245)}$;
(03) $\overline{(3,3)}.\overline{(14,3)} = \overline{(3.14+3.3, 3.3+3.14)} = \overline{(51,51)}$;
(04) $\overline{(5,2)}.\overline{(4,3)} = \overline{(5.4+2.3, 5.3+2.4)} = \overline{(26,23)}$.

Mostraremos agora que a multiplicação definida acima, independe do representante escolhido para a classe.

Proposição 23. *Sejam $a, a', b, b', c, c', d, d' \in \mathbb{N}$. Se*

$$\overline{(a,b)} = \overline{(a',b')} \quad e \quad \overline{(c,d)} = \overline{(c',d')},$$

então

$$\overline{(a,b)}.\overline{(c,d)} = \overline{(a',b')}.\overline{(c',d')}.$$

Demonstração:
Da hipótese $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')}$, obtemos as identidades

$$a + b' = b + a' \tag{16.1}$$

e

$$c + d' = d + c' \tag{16.2}$$

Multiplicando (16.1) por c e por d obtemos as equações:

$$ac + b'c = bc + a'c \quad \text{e} \quad ad + b'd = bd + a'd$$

De onde segue, que:

$$(ac + b'c) + (bd + a'd) = (bc + a'c) + (ad + b'd)$$

ou ainda,

$$(ac + bd) + (b'c + a'd) = (ad + bc) + (a'c + b'd) \tag{16.3}$$

Multiplicando agora (16.2) por b' e depois por a', obtemos as equações:

$$b'c + b'd' = b'd + b'c' \quad \text{e} \quad a'c + a'd' = a'd + a'c'$$

E daí, segue:

$$(b'c + b'd') + (a'd + a'c') = (b'd + b'c') + (a'c + a'd')$$

ou ainda,

$$(b'c + a'd) + (a'c' + b'd') = (a'c + b'd) + (b'c' + a'd') \tag{16.4}$$

Somando as equações (16.3) e (16.4) obtemos:

$$[(ac+bd)+(b'c+a'd)]+[(a'c+b'd)+(b'c'+a'd')] = [(ad+bc)+(a'c+b'd)]+[(b'c+a'd)+(a'c'+b'd')]$$

usando a comutatividade e associatividade em $\mathbb{N}$:

$$(ac+bc)+(a'd'+b'c')+[(a'c+b'd)+(b'c+a'd)] = (ad+bc)+(a'c'+b'd')+[(a'c+b'd)+(b'c+a'd)]$$

Pelo cancelamento da adição em $\mathbb{N}$, obtem-se:

$$(ac + bc) + (a'd' + b'c') = (ad + bc) + (a'c' + b'd')$$

$$\Downarrow$$

$$(ac + bc, ad + bc) \sim (a'c' + b'd', a'd' + b'c')$$

$$\Downarrow$$

$$\overline{(ac + bd, ad + bc)} = \overline{(a'c' + b'd', a'd' + b'c')}$$

$$\Downarrow$$

$$\overline{(a,b)}.\overline{(c,d)} = \overline{(a',b')}.\overline{(c',d')}.$$

$\square$

A próxima proposiçao mostra que a função imersão $f : \mathbb{N} \to \mathbb{Z}$ também preserva o produto.

Proposição 24. *Considerando a função imersão $f : \mathbb{N} \to \mathbb{Z}$, definida na Proposição 20, para quaisquer $m_1, m_2 \in \mathbb{N}$ tem-se:*

$$f(m_1.m_2) = f(m_1).f(m_2)$$

Demonstração:
Se $m_1, m_2 \in \mathbb{N}$, então
$f(m_1.m_2) = \overline{(m_1m_2, 0)} = \overline{(m_1m_2 + 0, 0 + 0)}$
$= \overline{(m_1m_2 + 0.0,\ m_1.0 + 0.m_2)} = \overline{(m_1, 0)}.\overline{(m_2, 0)} = f(m_1).f(m_2).$ □

Propriedades da Multiplicação em $\mathbb{Z}$

A Multiplicação, definida em $\mathbb{Z}$, tem as seguintes propriedades:

(M1) **Associativa:**
Para quaisquer α, β e $\gamma \in \mathbb{Z}$, tem-se:

$$(\alpha\beta)\gamma = \alpha(\beta\gamma).$$

Demonstração:
Sejam $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)} \in \mathbb{Z}$. Usando a associativada e a comutatividade da adição em $\mathbb{N}$, temos:

$$\begin{aligned}
(\alpha\beta)\gamma &= (\overline{(a,b)}.\overline{(c,d)}).\overline{(e,f)}\\
&= \overline{(ac+bd, ad+bc)}.\overline{(e,f)}\\
&= \overline{((ac+bd)e+(ad+bc)f, (ac+bd)f+(ad+bc)e)}\\
&= \overline{((ac)e+(bd)e+(ad)f+(bc)f, (ac)f+(bd)f+(ad)e+(bc)e)}\\
&= \overline{((a(ce)+a(df))+(b(de+b(cf)), (a(cf)+a(de))+(b(df)+b(ce))}\\
&= \overline{(a(ce+df)+b(cf+de), a(cf+de)+b(ce+df))}\\
&= \overline{(a,b)}.\overline{(ce+df), (cf+de)}\\
&= \overline{(a,b)}.(\overline{(c,d)}.\overline{(e,f)})\\
&= \alpha(\beta\gamma).
\end{aligned}$$
□

(M2) **Comutativa:**
Para quaisquer $\alpha, \beta \in \mathbb{Z}$ tem-se:

$$\alpha\beta = \beta\alpha.$$

Demonstração:
Sejam $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)} \in \mathbb{Z}$. Então
$\alpha\beta = (\overline{(a,b)}.\overline{(c,d)}) = \overline{(ac+bd, ad+bc)} = \overline{(ca+db, cb+da)} = \overline{(c,d)}.\overline{(a,b)} = \beta\alpha.$ □

(M3) **Existência e Unicidade do Elemento Unidade:**
A classe $1 = \overline{(1,0)}$ é o elemento neutro da multiplicação, isto é, para todo $\alpha \in \mathbb{Z}$, tem-se:

$$\alpha.1 = \alpha.$$

Demonstração:
Para $\alpha = \overline{(a,b)} \in \mathbb{Z}$, temos:

$$\alpha.1 = \overline{(a,b)}.\overline{(1,0)} = \overline{(a.1+b.0, a.0+b.1)} = \overline{(a,b)} = \alpha.$$

Mostra-se também que $1 = \overline{(1,0)}$ é o único elemento em $\mathbb{Z}$ com esta propriedade, sendo chamado o **elemento unidade** de $\mathbb{Z}$. $\square$

(M4) **Cancelamento da Multiplicação em** $\mathbb{Z}$:
Sejam $\alpha, \beta, \gamma \in \mathbb{Z}$.

$$\text{Se} \quad \alpha\gamma = \beta\gamma \textbf{ e } \gamma \neq \mathbf{0}, \text{ então} \quad \alpha = \beta.$$

Demonstração:

Sejam $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)} \in \mathbb{Z}$, com$\gamma \neq 0$. Se
$\alpha\gamma = \beta\gamma \Rightarrow \overline{(ae+bf, af+be)} = \overline{(ce+df, cf+de)}$
$\Rightarrow (ae+bf, af+be) \sim (ce+df, cf+de)$
$\Rightarrow (ae+bf)+(cf+de) = (af+be)+(ce+df)$
$\Rightarrow (a+d)e+(b+c)f = (b+c)e+(a+d)f.$

Como $\gamma = \overline{(e,f)} \neq \overline{(0,0)} \Rightarrow e \neq f$. Logo, pela Tricotomia em $\mathbb{N}$, $e < f$ ou $f < e$. Suponhamos $e < f \Rightarrow f = e+h$, para algum $h \in \mathbb{N}^*$. Daí, temos:
$\alpha\beta = \alpha\gamma \Rightarrow (a+d)e+(b+c)(e+h) = (b+c)e+(a+d)(e+h)$
$\Rightarrow (a+d)e+(b+c)e+(b+c)h = (b+c)e+(a+d)e+(a+d)h$
$\Rightarrow (b+c)h = (a+d)h$
$\Rightarrow (b+c) = (a+d) \Rightarrow (a,b) \sim (c,d) \Rightarrow \overline{(a,b)} = \overline{(c,d)} \Rightarrow \alpha = \beta.$ $\square$

(M5) **Distributividade:**
Para quaisquer $\alpha, \beta, \gamma \in \mathbb{Z}$, tem-se:

$$\alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma.$$

Demonstração:
Sejam $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)} \in \mathbb{Z}$. Então
$\alpha(\beta+\gamma) = \overline{(a,b)}.(\overline{(c,d)} + \overline{(e,f)})$
$= \overline{(a,b)}.\overline{(c+e, d+f)}$ - Definição 19
$= \overline{(a(c+e)+b(d+f), a(d+f)+b(c+e))}$ - Definção 19
$= \overline{(ac+bd)+(ae+bf), (ad+bc)+(af+be))}$ - Por (M1),(M2) e (M3) em $\mathbb{N}$
$= \overline{(ac+bd, ad+bc)} + \overline{(ae+bf, af+be)}$ - Definição 18
$= \overline{(a,b)}.\overline{(c,d)} + \overline{(a,b)}.\overline{(e,f)}$ - Definição 19
$= \alpha\beta + \alpha\gamma.$ $\square$

6 Relação de Ordem em $\mathbb{Z}$

Análogo ao que fizemos no conjunto dos naturais, definiremos uma relação em $\mathbb{Z}$, a qual permite comparar dois inteiros α e β quaisquer.

Definição 20. *Dados inteiros $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$, dizemos que α é menor do que β, indicado por $\alpha \leq \beta$, se $a+d \leq b+c$, isto é,*

$$\boxed{\overline{(a,b)} \leq \overline{(c,d)} \Leftrightarrow a+d \leq b+c.}$$

E dizemos que α é (estritramente) menor do que β, indicado por $\alpha < \beta$, se $\alpha \leq \beta$, porém $\alpha \neq \beta$, isto é,

$$\boxed{\overline{(a,b)} < \overline{(c,d)} \Leftrightarrow a+d < b+c.}$$

Exemplos:
(01) $\overline{(5,2)} \leq \overline{(10,3)}$, pois $5+3 < 2+10$;
(02) $\overline{(18,10)} \leq \overline{(9,1)}$, pois $18+1 = 10+9$;
(03) $\overline{(5,10)} < \overline{(3,3)}$, pois $5+3 < 10+3$.

A próxima proposição mostra que a relação $\leq$, definida acima, independe do representante escolhido para a classe, portanto, está bem definida.

Proposição 25. *Sejam $a, a', b, b', c, c', d, d' \in \mathbb{N}$. Se*

$$\overline{(a,b)} = \overline{(a',b')} \quad e \quad \overline{(c,d)} = \overline{(c',d')},$$

então

$$\overline{(a,b)} \leq \overline{(c,d)} \Rightarrow \overline{(a',b')} \leq \overline{(c',d')}.$$

Demonstração:
$\overline{(a,b)} = \overline{(a',b')} \Rightarrow (a,b) \sim (a',b') \Rightarrow a+b' = b+a'$
e
$\overline{(c,d)} = \overline{(c',d')} \Rightarrow (c,d) \sim (c',d') \Rightarrow c+d' = d+c'$.
E daí, obtemos $(a+d)+(b'+c') = (b+c)+(a'+d')$.
Então se, $\overline{(a,b)} \leq \overline{(c,d)} \Rightarrow a+d \leq b+c \Rightarrow (b+c) = (a+d)+h$, para algum $h \in \mathbb{N}$. Daí,
$(a+d)+(b'+c') = (b+c)+(a'+d') \Rightarrow (a+d)+(b'+c') = (a+d)+(a'+d')+h$
e pelo cancelamento em $\mathbb{N}$, obtemos:
$(b'+c') = (a'+d')+h \Rightarrow a'+d' \leq b'+c' \Rightarrow \overline{(a',b')} \leq \overline{(c',d')}$. $\square$

Propriedades da Relação de Ordem em $\mathbb{Z}$

A relação $\leq$, definida em $\mathbb{Z}$, tem as seguintes propriedades:

(R1) **Reflexiva:**
Para qualquer $\alpha \in \mathbb{Z}$, tem-se
$$\alpha \leq \alpha.$$

Demonstração:
Seja $\alpha = \overline{(a,b)} \in \mathbb{Z}$. Como $a+b = b+a \Rightarrow \alpha \leq \alpha$. □

(R2) **Antissimétrica:**
Para quaisquer $\alpha, \beta \in \mathbb{Z}$ tem-se:
$$\alpha \leq \beta \quad \text{e} \quad \beta \leq \alpha \Rightarrow \alpha = \beta.$$

Demonstração:
Sejam $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)} \in \mathbb{Z}$. Se,
$\alpha \leq \beta \Rightarrow a+d \leq b+c \Rightarrow (b+c) = (a+d) + h_1,\ h_1 \in \mathbb{N}$;
e
$\beta \leq \alpha \Rightarrow b+c \leq a+d \Rightarrow (a+d) = (b+c) + h_2,\ h_2 \in \mathbb{N}$.
Segue daí, que
$(b+c) = (b+c) + (h_1+h_2) \Rightarrow h_1+h_2 = 0 \Rightarrow h_1 = h_2 = 0 \Rightarrow a+d = b+c \Rightarrow$
$(a,b) \sim (c,d) \Rightarrow \overline{(a,b)} = \overline{(c,d)} \Rightarrow \alpha = \beta$. □

(R3) **Transistiva:**
Para quaisquer α, β, $\gamma \in \mathbb{Z}$, tem-se:
$$\alpha \leq \beta \quad \text{e} \ \beta \leq \gamma \Rightarrow \alpha \leq \gamma.$$

Demonstração:
$\alpha \leq \beta \Rightarrow (b+c) = (a+d) + h_1,\ h_1 \in \mathbb{N}$
e
$\beta \leq \gamma \Rightarrow (d+e) = (c+f) + h_2,\ h_1 \in \mathbb{N}$.
Daí,
$(b+c) + (d+e) = (a+d) + (c+f) + (h_1+h_2)$
$\Rightarrow (b+e) + (c+d) = (a+f) + (c+d) + (h_1+h_2)$
$\Rightarrow (b+e) = (a+f) + (h_1+h_2)$
$\Rightarrow a+f \leq b+e \Rightarrow \alpha \leq \gamma$. □

De (R1), (R2) e (R3), segue que $\leq$ é uma relação de ordem em $\mathbb{Z}$, logo $\mathbb{Z}$ é um conjunto ordenado. Esta ordem é compatível com as operações definidas em $\mathbb{Z}$, conforme propriedade (R4) e (R5) abaixo.

(R4) **Monotonicidade da Adição:**

Sejam $\alpha, \beta \in \mathbb{Z}$. Se

$$\alpha \leq \beta,$$

para qualquer $\gamma \in \mathbb{Z}$, temos

$$\alpha + \gamma \leq \beta + \gamma.$$

Demonstração:

Sejam $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)} \in \mathbb{Z}$, com $\alpha \leq \beta$. Então
$\overline{(a,b)} \leq \overline{(c,d)} \Rightarrow a + d \leq b + c \Rightarrow (a+d) + (e+f) \leq (b+c) + (e+f)$
$\Rightarrow (a+e) + (d+f) \leq (b+f) + (c+e)$
$\Rightarrow \overline{(a+e, b+f)} \leq \overline{(c+e, d+f)}$
$\Rightarrow \overline{(a,b)} + \overline{(e,f)} \leq \overline{(c,d)} + \overline{(e,f)} \Rightarrow \alpha + \gamma \leq \beta + \gamma.$ □

(R4) **Monotonicidade Multiplicação:**
Sejam $\alpha, \beta, \gamma \in \mathbb{Z}$. Se

$$\alpha \leq \beta,$$

para qualquer $\gamma \geq \overline{(0,0)}$ em $\mathbb{Z}$, tem-se:

$$\alpha\gamma \leq \beta\gamma.$$

Demonstração:
Sejam $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)} \in \mathbb{Z}$, com $\alpha \leq \beta$ e $\gamma \geq \overline{(0,0)}$. Então
$\overline{(a,b)} \leq \overline{(c,d)} \Rightarrow a + d \leq b + c \Rightarrow \exists\, p \in \mathbb{N}$, tal que:

$$(b+c) = (a+d) + p. \tag{16.5}$$

Multiplicando (16.5) por e, e posteriormente por f, obtemos as equações:

$$(a+d)e + pe = (b+c)e \qquad \text{e} \qquad (b+c)f = (a+d)f + pf.$$

Somando essas duas equações obtem-se:

$$(a+d)e + (b+c)f + pe = (a+d)f + (b+c)e + pf \tag{16.6}$$

Agora, como $\overline{(0,0)} \leq \overline{(e,f)} \Rightarrow f \leq e \Rightarrow e = f + q$, $q \in \mathbb{N}$. Multiplicando essa equação por p, tem-se:

$$pe = pf + pq$$

Substituindo esse valor em(16.6):

$$(a+d)e + (b+c)f + (pf + pq) = (a+d)f + (b+c)e + pf$$

Pelo cancelamento da adição em $\mathbb{N}$, ficamos com:

$$(a+d)f + (b+c)e = (a+d)e + (b+c)f + pq$$

$$\Downarrow$$

$$(a+d)e+(b+c)f \leq (a+d)f+(b+c)e$$

$$\Downarrow$$

$$(ae+bf)+(cf+de) \leq (af+be)+(ce+df) \Rightarrow \overline{(ae+bf,af+be)} \leq \overline{(ce+df,cf+de)}$$

$$\Downarrow$$

$$\overline{(a,b)}.\overline{(e,f)} \leq \overline{(c,d)}.\overline{(e,f)} \Rightarrow \alpha\gamma \leq \beta\gamma.$$

□

Por fim, veremos que a função imersão $f : \mathbb{N} \to \mathbb{Z}$ também preserva a ordem definida em $\mathbb{Z}$.

Proposição 26. *Considerando a função imersão definida na Proposição 20, para quaisquer $m_1, m_2 \in \mathbb{N}$ tem-se a implicação:*

$$m_1 \leq m_2 \Rightarrow f(m_1) \leq f(m_2).$$

Demonstração:
Se $m_1 < m_2 \Rightarrow m_1 + 0 < 0 + m_2 \Rightarrow \overline{(m_1, 0)} < \overline{(m_2, 0)} \Rightarrow f(m_1) < f(m_2)$. □

7 Inteiros Positivos e Negativos

Proposição 27. *Para todo $\alpha \in \mathbb{Z}$, temos uma, e somente uma, das afirmações:*
(i) $\alpha < 0$;
(ii) $\alpha = 0$;
(iii) $\alpha > 0$.

Demonstração:
Segue diretamente da Tricotomia em $\mathbb{N}$, pois, se $\alpha = \overline{(a,b)} \in \mathbb{Z}$, pela tricotomia em $\mathbb{N}$, ocorre uma e somente uma, das condições:
(i) $a < b \Rightarrow a + 0 < b + 0 \Rightarrow \overline{(a,b)} < \overline{(0,0)} \Rightarrow \alpha < 0$;
(ii) $a = b \Rightarrow a + 0 = b + 0 \Rightarrow \overline{(a,b)} = \overline{(0,0)} \Rightarrow \alpha = 0$;
(iii) $b < a \Rightarrow b + 0 < a + 0 \Rightarrow \overline{(0,0)} < \overline{(a,b)} \Rightarrow \alpha > 0$. □

Como consequência da proposião acima e da Tricotomia em $\mathbb{N}$, segue a tricotomia em $\mathbb{Z}$.

Corolário 11. ***(Tricotomia em $\mathbb{Z}$)***
Dados $\alpha, \beta \in \mathbb{Z}$ ocorre uma, e somente uma, das afirmações:
(i) $\alpha < \beta$;
(ii) $\alpha = \beta$;
(iii) $\alpha > \beta$.

Demonstração:
Considere $\gamma = \alpha + (-\beta) \in \mathbb{Z}$. Com o uso das propriedades (R3) e (R4), segue que ocorre uma e somente uma das condições:
(i) $\gamma < 0 \Rightarrow \alpha + (-\beta) < 0 \Rightarrow \alpha < \beta$;
(ii) $\gamma = 0 \Rightarrow \alpha - \beta = 0 \Rightarrow \alpha = \beta$;
(iii) $\gamma < 0 \Rightarrow \alpha - \beta > 0 \Rightarrow \beta < \alpha$. □

Definição 21. *Diz-se que um inteiro $\alpha \in \mathbb{Z}$ é:*
(i) *positivo, se $\alpha > 0$;*
(ii) *não negativo, se $\alpha \geq 0$;*
(iii) *negativo, se $\alpha < 0$;*
(iv) *não positivo, se $\alpha \leq 0$.*

Denotaremos por:
$\mathbb{Z}_+$ - o conjunto dos inteiros não negativos;
$\mathbb{Z}_-$ - o conjuntos dos inteiros não positivos;
$\mathbb{Z}_+^*$ - o conjunto dos inteiros positivos;
$\mathbb{Z}_-^*$ - o conjunto dos inteiros negativos;

Vamos agora caracterizar os inteiros positivos, isto é, descrever o conjunto $\mathbb{Z}_+^*$. Se $\alpha = \overline{(a,b)} \in \mathbb{Z}_+^*$, então $\alpha > 0$. Assim, temos:
$\overline{(0,0)} < \overline{(a,b)} \Rightarrow 0 + b < 0 + a \Rightarrow a = b + m,\ m \in \mathbb{N}^*$
$\Rightarrow a + 0 = b + m \Rightarrow (a,b) \sim (m,0) \Rightarrow \overline{(a,b)} = \overline{(m,0)}$, com $m \in \mathbb{N}^*$.

Reciprocamente, para cada $m \in \mathbb{N}^*$, temos:
$0 + 0 < m + 0 \Rightarrow \overline{(0,0)} < \overline{(m,0)} \Rightarrow \overline{(m,0)} \in \mathbb{Z}_+^*$.
Assim,

$$\mathbb{Z}_+^* = \{\overline{(m,0)} \mid m \in \mathbb{N}^*\}.$$

Analogamente, se $\alpha = \overline{(a,b)} \in \mathbb{Z}_-^*$, então $\alpha < 0$. Daí,
$\overline{(a,b)} < \overline{(0,0)} \Rightarrow a < b \Rightarrow b = a + m,\ m \in \mathbb{N}^*$
$\Rightarrow a + m = b + 0 \Rightarrow (a,b) \sim (0,m) \Rightarrow \overline{(a,b)} = \overline{(0,m)}$, com $m \in \mathbb{N}^*$.

De modo recíproco, para cada $m \in \mathbb{N}^*$, tem-se,
$0 + 0 < m + 0 \Rightarrow \overline{(0,m)} < \overline{(0,0)} \Rightarrow \overline{(0,m)} \in \mathbb{Z}_-^*$.
Portanto, o conjunto dos inteiros negativos é dado por:

$$\mathbb{Z}_-^* = \{\overline{(0,m)} \mid m \in \mathbb{N}^*\}.$$

Da Proposição 27, segue que:

$$\mathbb{Z} = \mathbb{Z}_-^* \cup \{0\} \cup \mathbb{Z}_+^*$$

ou seja,

$$\mathbb{Z} = \{\overline{(0,m)} \mid m \in \mathbb{N}^*\} \cup \{\overline{(0,0)}\} \cup \{\overline{(m,0)} \mid m \in \mathbb{N}\}, \tag{16.7}$$

sendo essa união disjunta.

Podemos agora demonstrar que o conjunto $\mathbb{Z}_+$ é fechado com relação as operações definidas em $\mathbb{Z}$.

Proposição 28. *Para quaisquer* $\alpha, \beta \in \mathbb{Z}_+^*$, *temos:*
(*i*) $\alpha + \beta \in \mathbb{Z}_+^*$;
(*ii*) $\alpha.\beta \in \mathbb{Z}_+^*$;

Demonstração:
Pelo exposto acima, se $\alpha, \beta \in \mathbb{Z}_+^*$, então existem $m_1, m_2 \in \mathbb{N}^*$, tais que $\alpha = \overline{(m_1, 0)}$ e $\beta = \overline{(m_2, 0)}$. Daí,
(*i*) $\alpha + \beta = \overline{(m_1 + m_2, 0)} \in \mathbb{Z}_+^*$ e
(*ii*) $\alpha.\beta = \overline{(m_1.m_2, 0)} \in \mathbb{Z}_+^*$. □

Proposição 29. $\mathbb{Z}$ *é sem divisores de zero, isto é, para quaisquer* $\alpha, \beta \in \mathbb{Z}$, *se* $\alpha.\beta = 0$,*e ntão* $\alpha = 0$ *ou* $\beta = 0$.

Demonstração:
Sejam α, $\beta = (a, b) \in \mathbb{Z}$, para os quais temos $\alpha.\beta = 0$. Se $\alpha = 0$, nada há a demonstrar. Suponha $\alpha \neq 0$. Pela Proposição 27, temos dois casos possíveis:
(*i*) $\alpha < 0 \Rightarrow \alpha = \overline{(0, m)}$, para algum $m \in \mathbb{N}^*$. Assim,
$\alpha.\beta = 0 \Rightarrow \overline{(0, m)}.\overline{(a, b)} = \overline{(mb, ma)} = \overline{(0, 0)} \Rightarrow ma = mb \Rightarrow a = b$, pois $m \neq 0$. Assim, $\beta = \overline{(a, a)} = 0$;
(*ii*) $\alpha > 0 \Rightarrow \alpha = \overline{(m, 0)}$, para algum $m \in \mathbb{N}^*$. Assim,
$\alpha.\beta = 0 \Rightarrow \overline{(m, 0)}.\overline{(a, b)} = \overline{(ma, mb)} = \overline{(0, 0)} \Rightarrow ma = mb \Rightarrow a = b$, pois $m \neq 0$. Assim, $\beta = \overline{(a, a)} = 0$. □

Dado $m \in \mathbb{N}$, já vimos que o oposto do inteiro $\alpha = \overline{(m, 0)} \in \mathbb{Z}$ é a classe $-\alpha = \overline{(0, m)}$. Usando a identificação dada pela função de imersão:

$$m \leftrightarrow \overline{(m, 0)}$$

obtemos:

$$-m = -\overline{(m, 0)} = \overline{(0, m)}$$

Com esta identificação, (16.7) fica:

$$\mathbb{Z} = \{-m \mid m \in \mathbb{N}^*\} \cup \{0\} \cup \{m \mid m \in \mathbb{N}^*\} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$$

coincidindo com a notação usual. Além disso, dados $a, b \in \mathbb{N}$, temos:

$$a - b = a + (-b) = \overline{(a, 0)} + -\overline{(b, 0)} = \overline{(a, 0)} + \overline{(0, b)} = \overline{(a, b)}.$$

Dessa forma, identitificamos a classe $\overline{(a, b)}$ com o inteiro obtido pela diferença $a - b$, conforme usado para na definição da equivalência $\sim$.

8 Princípio da Boa Ordem em $\mathbb{Z}$

Dizemos que $X \subset \mathbb{Z}$ é limitado inferiormente, se existe $n \in \mathbb{Z}$, tal que

$$n \leq x, \quad \text{para todo} \quad x \in X.$$

Todo $n \in \mathbb{Z}$ que satisfaz a condição acima é dito uma cota inferior de X.

Exemplos:
(01) $X = \{4, 8, 12, 16, 20, ...\}$ é um subconjunto não vazio de $\mathbb{Z}$, limitando inferiormente. Claramamente vemos que $4 = minX$. Vejamos, um algorítmo que nos permite determinar esse elemento mínimo, usando o Princípio da Boa Ordem em $\mathbb{N}$.

Comecemos tomando uma cota inferior qualquer de X. Observe que tal cota existe, pois X é limitado inferiormente. Por exemplo, $n = 1$ é um cota inferior de X, pois $1 \leq x$, para todo $x \in X$. Agora, consideremos o conjunto X', abaixo definido:

$$X' = \{x - n \mid x \in X\} = \{x - 1 \mid x \in X\} = \{3, 7, 11, 15, 19, ...\}$$

Como $X \neq \emptyset$ e $1 \leq x$ para todo $x \in X$, X' é um subconjunto não vazio de $\mathbb{N}$, logo, pelo Princípio da Boa Ordem, X' tem elemento mínimo, isto é, existe $m' = minX$. Neste caso, $m' = 3$. E observe que, $4 = minX = m' + n$.

(02) $X = \{-7, -1, 0, 1, 21, 22, 23, ...\}$ é um subconjunto não vazio de $\mathbb{Z}$, limitando inferiormente. Claramamente, vemos que $-7 = minX$. Vamos usar o mesmo processo acima, para chegar a esse elemento mínimo.

Tomemos uma cota inferior qualquer de X, por $n = -10$ e construamos o conjunto:

$$X' = \{x - n \mid x \in X\} = \{x + 10 \mid x \in X\} = \{3, 9, 10, 11, 31, 32, 33, ...\}$$

X' é um subconjunto não vazio de $\mathbb{N}$, logo, existe $m' = minX = 3$. E também temos que, $-7 = minX = m' + n$

Vejamos a generalização desse processo na demonstração do próximo teorema.

Teorema 16. ***(Princípio da Boa Ordem em*** $\mathbb{Z}$***)***
Todo subconjunto não vazio de $\mathbb{Z}$*, limitado inferiomente, tem elemento mínimo.*

Demonstração:
Seja $\emptyset \neq X \subset \mathbb{Z}$, limitado inferiormente. Então, existe $n \in X$, tal que $n \leq x$, para todo $x \in X$. Consideremos o conjunto:

$$X' = \{x - n \mid x \in X\}.$$

Claramente, $\emptyset \neq X' \subset \mathbb{N}$ e pelo Princípio da Boa Ordem em $\mathbb{N}$, existe
$m' = minX' \Rightarrow m' \in X'$ e $m' \leq x', \forall x' \in X'$. Como $m' \in X' \Rightarrow m' = x - n$, para algum $x \in X$. Vamos mostrar que $m := m' + n$ é o elemento mínimo de X. De fato,
. $m = m' + n$ e $m' = x - n \Rightarrow m = (x - n) + n = x \in X$;
. $m' \leq x'$, para todo $x' \in X \Rightarrow m' \leq x - n, \forall x \in X \Rightarrow m' + n \leq x$,

$\forall x \in X \Rightarrow m \leq x, \forall x \in X$;
Portanto, $m = minX$. $\square$

Corolário 12. *Não existe $x \in \mathbb{Z}$, tal que $0 < x < 1$.*

Demonstração:
Seja $X = \{x \in \mathbb{Z} \mid 0 < x < 1\}$. Claramente, X é um subconjunto de $\mathbb{Z}$, limitado inferior. Se $X \neq \emptyset$, então pelo princípio da Boa Ordem em $\mathbb{Z}$, existe $x_0 = \min X$. Então,

$$x_0 \in X \Rightarrow 0 < x_0 < 1 \underbrace{\Rightarrow}_{\times x_0} 0.x_0 < x_0.x_0 < x_0.1 \Rightarrow 0 < x_0^2 < x_0 < 1 \Rightarrow x_0^2 \in X.$$

Uma contradição, pois $x_0^2 < x_0 = \min X$. Logo $X = \emptyset$.

Bibliografia

[1] FERREIRA, Jamil. *A Construção dos Números*. Textos Universitários, SBM, Rio de Janeiro, 2011.

[2] FILHO, Edgar de Alencar. *Teoria Elementar dos Números*. Ed. Nobel, 1985.

[3] HEFEZ, Abramo. *Elementos de Aritmética*.SBM, Rio de Janeiro, 2006.

[4] MARTINEZ, Fábio Brochero, MOREIRA, Carlos Gustavo, SALDANA, Nicolau e TENGAN, Eduado. *Teoria dos Números: Um passeio com primos e outros números familiares pelo mundo inteiro*, IMPA, Rio de Janeiro: , 2011.

[5] MILES, Francisco César Polcino e COELHO, Sônia Pitta. *Números - Uma Introdução à Matemática*. Edusp, São Paulo, 2003.

[6] MOREIRA, Carlos Gustavo, MARTINEZ, Fábio Brochero, SALDANA, Nicolau. *Tópicos de Teoria dos Números - Coleção PROFMAT*, Fábio Brochero SBM, Rio de Janeiro, 2012.

[7] SANTOS, José Plínio de Oliveira. *Introdução à Teoria dos Números*. IMPA, Rio de Janeiro, 1998.

[8] SHOKRANIAN, Salahoddin, SOARES, Marcos e GODINHO, Hemar. *Teoria dos Números*. Editora UnB, Brasília, 1994.