UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONALIZANTE EM MATEMÁTICA

TEOREMA CHINÊS DOS RESTOS E APLICAÇÕES

Audemir dos Santos

MANAUS
2017

UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
PROGRAMA DE MESTRADO PROFISSIONALIZANTE EM MATEMÁTICA

Audemir dos Santos

TEOREMA CHINÊS DOS RESTOS E APLICAÇÕES

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática da Universidade Federal do Amazonas, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Nilomar Vieira de Oliveira

MANAUS
2017

Ficha Catalográfica

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Santos, Audemir dos
S237t Teorema Chinês dos Restos e Aplicações / Audemir dos Santos. 2017
79 f.: 31 cm.

Orientador: Nilomar Vieira de Oliveira
Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Federal do Amazonas.

1. Teorema Chinês dos Restos. 2. Indução. 3. Congruências. 4. Equações Diofantinas Lineares. I. Oliveira, Nilomar Vieira de II. Universidade Federal do Amazonas III. Título

AUDEMIR DOS SANTOS

TEOREMA CHINÊS DOS RESTOS E APLICAÇÕES

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática da Universidade Federal do Amazonas, como requisito parcial para obtenção do título de Mestre em Matemática.

Aprovado em maio de 2017.

BANCA EXAMINADORA

Prof. Dr. Nilomar Vieira de Oliveira
Presidente

Prof. Dr. Valtemir Martins Cabral
Membro

Prof. Dr. Alcides de Castro Amorim Neto
Membro

AGRADECIMENTOS

A Deus, pelo dom da vida e bênçãos a mim concedidas, por ter mudado minha vida para melhor e por sempre guiar meus passos para realizar com sucesso os meus objetivos.

A minha família, em especial à minha esposa Erycka Alves de Mesquita pelo companheirismo, amor, incentivo, respeito, e principalmente pela paciência nessa minha caminhada demonstrado e pelo grande presente que me deu em 2015 minha filha e amada Lúcia Ayla Mesquita dos Santos , que veio para me encorajar cada vez mais e dar sentido a tudo que estou fazendo.

Aos meus colegas do Profmat-Am 2014, em especial a André Lopes, Clicio, Celiomar, Felipe, Genilce e Mauricio pela motivação, carinho e caminhada em nosso grupo de estudos nos dias normais como nos feriados e finais de semanas incansáveis tanto na Ufam como em minha residência, no qual fez nos unir mais ainda como amigos que somos e pela guarra e admiração a todos.

E não menos importantes a todo corpo docente do PROFMAT pólo UFAM, em especial ao meu orientador Prof. Dr. Nilomar Vieira de Oliveira, pelo incentivo, profissionalismo e contribuição no desenvolvimento da dissertação, assim como na confiança e exemplo de dedicação a área de educação.

RESUMO

O foco deste trabalho é o problema Chinês dos Restos e algumas de suas aplicações elementares. Para este fim, dos capítulos 2 ao 5, abordamos alguns assuntos na revisão bibliográfica, dentre os quais podemos destacar: Conjunto dos Números Inteiros e suas Propriedades Básicas, a Divisão nos Inteiros, Máximo Divisor Comum, Mínimo Múltiplo Comum, Equações Diofantinas Lineares e Congruências. Além disso, alguns conteúdos foram tratados de uma maneira mais profunda do que usualmente é feita no ensino básico, pois embora tenham um papel importante na resolução de muitos problemas envolvendo os números inteiros, estão de certa forma subutilizados no ensino básico, em especial, quando se trata de fundamentações para olimpíadas e graduações de Matemática. No capítulo 6 apresentamos a demonstração do Teorema Chinês dos Restos e nove exemplos de suas aplicações. Acreditamos que tais assuntos da forma em que foram tratados neste trabalho de conclusão de curso possam servir de apoio para professores e alunos que buscam material suplementares para resolução de problemas.

Palavras-chave: Teorema Chinês dos Restos, Indução, Congruências, Equações Diofantinas Lineares

ABSTRACT

The focus of this research is the Chinese Remains problem and some of its elementary applications. To achieve this goal, from Chapters 2 to 5, we appoach some content in the bibliographic review, among which we can highlight: Set of Integer Numbers and their Basic Properties, Integer Division, Greatest Common Divisor, Common Multiple Minimum, Linear Diophantine Equations and Congruences. In addition, some content has been dealt with in a deeper way than is usually done in basic education, because although it plays an important role in solving many problems involving whole numbers, they are somewhat underutilized in basic education, especially when these are fundamentals for Olympics and Mathematics graduations. In Chapter 6 we present the proof of the Chinese Remainder Theorem and nine examples of its applications. We believe that such issues, in the way they were handled in this monograph can be supportive for teachers and students seeking supplementary problem solving materials.

Keywords: Chinese Remainder Theorem, Induction, Congruences, Linear Diofantine Equations.

LISTA DE SÍMBOLOS

$\mathbb{N}$	Conjunto dos números naturais.
$\mathbb{Q}$	Conjunto dos números racionais.
$\mathbb{Z}$	Conjunto dos números inteiros.
$\mathbb{R}$	Conjunto dos números reais.
$\Longrightarrow$	Implica em.
$=$	Igual.
$\neq$	Diferente.
$>$	Maior.
$<$	Menor.
$\geq$	Maior ou igual.
$\leq$	Menor ou igual.
$\equiv$	Congruente.
$\not\equiv$	Incongruente.
$\mid$	Divide.
$\nmid$	Não divide.
$\blacksquare$	Indica o fim de uma demonstração.

Sumário

Capítulo 1

Introdução

1.1 Abordagem Histórica

O teorema chinês dos restos, como um problema com números específicos, aparece no livro Sunzi's Mathematical Classic (século III), pelo matemático chinês Sun Tzu. Sun Tzu não mostra nenhuma prova ou algoritmos completo para seu problema proposto. Um algoritmo para resolver esse problema foi descrito por Arybhata (século VI). Casos especiais de teorema chinês dos restos também eram conhecido por Brahmagupta (século VII), e também apareceram em Fibbonacci Liber Abaci (1202). O resultado mais tarde generalizado com uma solução completa chamada Dayanshu em Qin Jiushao 1247 Mathematical Treatise em nove seções (Shushu Jiuzhang). [6]

A noção de congruência foi primeiramente introduzida por Gauss em suas Disquisitiones Arithmeticae de 1801. Gauss ilustrou o teorema chinês dos restos sobre um problema envolvendo calendários, a saber, "To find the years that have a certain period number with respect to the solar and lunar cycle and the Roman indiction.". Gauss introduziu um procedimento para resolver o problema. Mas esse procedimento ja havia sido usado por Euler e na verdade era um método antigo que já havia aparecido várias vezes.

1.2 Motivação e Métodos do Trabalho

O principal motivo de escolha desse tema é devido ao nosso gosto pessoal, em primeiro lugar, mas também por vermos a dificuldade dos colegas quando tinham que resolver problemas envolvendo o Teorema Chinês dos Restos e suas aplicações. Além disso, constatamos uma carência muito grande de bibliografia referente ao conteúdo abordado e, consequentemente, os professores e alunos do Ensino Básico que precisam lidar com este tema e têm bastante dificuldade em encontrar material de apoio. Nesse sentido, esse trabalho poderá agregar-se à bibliografia existente em Língua Portuguesa como também ser uma outra alternativa de abordagem, como poderá ser verificada no penúltimo Capítulo desse trabalho, onde podem ser observadas várias aplicações que surgem de uma metodologia, que embora não seja novidade, não encontramos facilmente.

A metodologia para a realização deste trabalho foi a pesquisa bibliográfica. Estudamos o conteúdo através de vários autores [[1] [2] [3] [4] [5]] e algumas referências por eles citadas, organizamos os prerrequisitos necessários para a demonstração do Teorema Chinês dos Restos destes e, finalmente, aplicamos esse arcabouço teórico para a razão principal do estudo de matemática, a saber, a resolução de problemas.

1.3 Estrutura do Trabalho

A seguir, no Capítulo 2, apresentamos as noções fundamentais sobre o conjuntos dos números inteiros e suas propriedades básicas. Tais propriedades, incluindo a indução finita, foram amplamente utilizadas no decorrer e, apesar de relativamente simples, são essenciais para a compreensão de alguns teoremas que surgirão no decorrer do texto.

No Capítulo 3, o foco é a divisão de números inteiros. São apresentadas neste capítulo os elementos básicos da divisão, por exemplo, definições de divisibilidade, conjunto de divisores, etc., culminando no algoritmo da divisão euclidiana e sua aplicação para classificação da paridade de números inteiros, entre outras.

No Capítulo 4, fazemos o estudo de diversos termos relacionados aos números inteiros que culminarão no estudo do MMC e MDC de pares destes, ou número de inteiros maiores que 2. Para chegar a este objetivo, percorremos um primeiro estudo sobre os números primos. Finalmente, neste capítulo ainda, estabelecemos uma relação entre o MDC e o MMC.

O Capítulo 5 apresenta um pequeno esboço do estudo de equações diofantinas lineares conteúdo importante para verificar se uma determinada equação possui solução inteira. Esse fato será essencial quando formos fazer o estudo de um sistema de equações lineares inteiras que podemos dizer, antecipadamente, terá solução somente quando *qualquer* uma das equações tiver solução inteira.

Nos Capítulos 6, procedemos ao estudo das congruências lineares. Neste capítulos são espe-

cificadas as principais propriedades dos restos de divisão inteira, além de sistema de congruências lineares temos a demonstração do Teorema Principal: (Chinês) dos Restos, além de algumas de suas aplicações. Abordamos praticamente todos os prerrequisitos necessários para chegar nesse resultado, onde pudemos fazer a demonstração formal de uma maneira mais acessível possível aos leitores interessados, professores e alunos do Ensino Básico.

Finalmente, apresentamos as considerações finais no Capítulo 7. Nele, fazemos um breve resumo do caminho percorrido no trabalho para atingir o Teorema Chinês dos Restos e suas Aplicações, a contribuição que acreditamos estar dando à comunidade acadêmica que, como já mencionado anteriormente, é servir de suporte para alunos e professores que necessitam de bibliografia acessível e diferenciada da existente atualmente no mercado.

Capítulo 2

Números Inteiros: Noções Fundamentais

2.1 Números Inteiros

Os números inteiros ou apenas os inteiros são:

$$..., -4, -3, -2, -1, 0, 1, 2, 3, 4, ...$$

onde o conjunto é representado pela letra $\mathbb{Z}$, ou seja,

$$\mathbb{Z} = \{..., -4, -3, -2, -1, 0, 1, 2, 3, 4, ...\}$$

Podemos destacar os seguintes subconjuntos de $\mathbb{Z}$.

(1) Conjunto dos números inteiros não nulos ($\neq 0$) representado por $\mathbb{Z}^*$

$$\mathbb{Z}^* = \{x \in \mathbb{Z}; x \neq 0\} = \{\pm 1, \pm 2, \pm 3, \pm 4, ...\}$$

(2) Conjunto dos números inteiros não negativos (≥ 0) , representado por $\mathbb{Z}_+$

$$\mathbb{Z}_+ = \{x \in \mathbb{Z}; x \geq 0\} = \{0, 1, 2, 3, 4, ...\}$$

(3) Conjunto dos números inteiros não positivos (≤ 0), representado por $\mathbb{Z}_-$

$$\mathbb{Z}_- = \{x \in \mathbb{Z}; x \leq 0\} = \{0, -1, -2, -3, -4, ...\}$$

(4) Conjunto dos números inteiros positivos (> 0), representado por $\mathbb{Z}_+^*$

$$\mathbb{Z}_+^* = \{x \in \mathbb{Z}; x > 0\} = \{1, 2, 3, 4, ...\}$$

(5) Conjunto dos números inteiros negativos (< 0), representado por $\mathbb{Z}_-^*$

$$\mathbb{Z}_-^* = \{x \in \mathbb{Z}; x < 0\} = \{-1, -2, -3, -4, ...\}$$

Os números *inteiros positivos* são também conhecidos por números *naturais* e representados pela letra $\mathbb{N}$ ($\mathbb{N} = \mathbb{Z}_+^*$).

2.2 Propriedades Básicas

O conjunto $\mathbb{Z}$ dos números inteiros (positivos, negativos e zero), cujos elementos são números inteiros, tendo $\mathbb{Z}$ dois elementos destacados, 0 (zero) e 1 (um), e também duas operações, a adição (+) e a multiplicação ($\cdot$).

Sejam m e n dois inteiros quaisquer, denotamos por $m + n$ a soma de m e n, e por $m \cdot n$ (ou por mn, quando isto não nos causar confusão), o produto de m por n.

Os inteiros satisfazem aos seguintes axiomas.

(i) *Fechamento*: $m + n$ e $m \cdot n$ são inteiros sempre que m e n forem inteiros.

(ii) *Leis comutativas*: $m + n = n + m$ e $m \cdot n = n \cdot m, \forall\, m, n \in \mathbb{Z}$

(iii) *Leis associativas*: $(m + n) + p = m + (n + p)$ e $(m \cdot n) \cdot p = m \cdot (n \cdot p), \forall\, m, n, p \in \mathbb{Z}$

(iv) *Leis dos elementos neutros*: $m + 0 = m$ e $m \cdot 1 = m, \forall\, m \in \mathbb{Z}$

(v) *Lei distributiva*: $(m + n) \cdot p = m \cdot p + n \cdot p,\ \forall\, m, n, p \in \mathbb{Z}$

(vi) *Lei da existência de inversos aditivos*: Para cada inteiro m, existe um inteiro a tal que $m + a = 0$. Este inteiro a é chamado inverso aditivo ou oposto de m e é denotado por $-m$. Sendo m e n dois inteiros, define-se $m - n = m + (-n)$

(vii) *Lei do cancelamento da multiplicação*: Se m, n e p são inteiros, com $p \neq 0$, e $m \cdot p = n \cdot p$ então $m = n$.

A partir das propriedades (i) a (vii), tomadas aqui como axiomas (ou postulados, e das propriedades habituais da igualdade, podemos deduzir outras propriedades dos números inteiros, na qual chamaremos de teoremas).

Teorema 2.1. Se m é um inteiro qualquer $m \cdot 0 = 0$.

Demonstração: Se $m \cdot 0 = a$, então

$$\begin{aligned} a = m \cdot 0 &= m \cdot (0 + 0), \quad \text{pois 0 é o elemento neutro da adição} \\ &= m \cdot 0 + m \cdot 0 \quad \text{(lei distributiva)} \\ &= a + a. \end{aligned}$$

Desse modo,

$$a + a = a.$$

Somando o oposto de a em ambos os lados da igualdade, temos

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

Aplicando a lei associativa da adição, temos

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

ou seja, a + 0 = 0 e como 0 é o elemento neutro da adição, teremos $a = 0$. Portanto, $m.0 = 0$. ■

Também existe uma "relação de ordem" entre os inteiros, que é representado pelo sinal $<$ (menor que), no qual possui as seguintes propriedades:

(*viii*) Se $m \neq 0$, então $m < 0$ ou $0 < m$.

(*ix*) Se $m < n$ e $n < p$, então $m < p$

(*x*) Se $m < n$, então $m + p < n + p$

(*xi*) Se $m < n$ e $0 < p$, então $m \cdot p < n \cdot p$

(*xii*) Se $m < n$ e $p < 0$, então $n \cdot p < m \cdot p$

Muitas outras propriedades dos inteiros podem ser deduzidas a partir das propriedades citadas acima.

2.3 Indução Matemática

Indução finita matemática é uma técnica muito comum para provar que determinadas proposições são válidas para todo número natural a partir de um certo $n_0 \in \mathbb{N}$. O processo consiste inicialmente em provar que a referida proposição é verdadeira para n_0. Em seguida, assume-se a veracidade para um valor qualquer a partir de n_0 afim de mostrar que também vale para o seu sucessor. Intuitivamente, a propriedade requerida estará de fato provada pelo seguinte motivo: é válido para n_0 e para seu sucessor n_0+1, e também para seu sucessor n_0+2, e assim sucessivamente para qualquer natural maior ou igual a n_0.

Imagine o processo de indução finita como a construção de uma fileira de dominós. A indução é usada geralmente quando se deseja provar que algo é verdade para qualquer número inteiro positivo sem precisar provar para os infinitos casos particulares. Ela tem duas partes: enfileirar os dominós e, em seguida, derrubar o primeiro. Enfileirar os dominós deixando um espaço apropriado entre eles significa provar que se um qualquer cair, o próximo cairá. Derrubar o primeiro é provar que ele cai. Matemáticos chamam esses dois passos de "passo indutivo"e "passo inicial", respectivamente.

Antes de anunciarmos nosso principal resultado dessa seção necessitamos conhecer o seguinte axioma.

Axioma 1. Todo subconjunto $\mathcal{S} \subset \mathbb{N}$; $\mathcal{S} \neq \emptyset$, possui um elemento mínimo, isto é,

$$\text{existe } s_0 \in \mathcal{S} \text{ tal que } s_0 \leq s, \text{ para todo } s \in \mathcal{S}.$$

Formalmente, o Principio da Indução Finita é descrito abaixo:

Teorema 2.2. Seja $P(n)$ uma sentença que é verdadeira para cada $n \in \mathbb{N}$. Se

1. $P(1)$ é verdadeira, e

2. para cada $k \in \mathbb{N}$, se $P(k)$ é verdadeira, então $P(k+1)$ é verdadeira.

Então $P(n)$ é verdadeira para cada $n \in \mathbb{N}$.

Demonstração: Consideremos o conjunto $\mathcal{S} = \{n \in \mathbb{N}; P(n) \text{ é falso}\}$. Vamos mostrar que $\mathcal{S} = \emptyset$, resultando que $P(n)$ é verdadeiro para todo $n \in \mathbb{N}$.

Suponhamos que $\mathcal{S} \neq \emptyset$. Como $\mathcal{S}$ é um subconjunto não-vazio dos números naturais, existe $n_0 = \min \mathcal{S}$, pelo Princípio da Boa Ordenação dos números naturais. Devido $P(1)$ ser verdadeiro, temos $1 \notin \mathcal{S}$, isto é, $n_0 > 1$.

Como n_0 é o menor elemento de $\mathcal{S}$, o número $n_0 - 1 \notin \mathcal{S}$. Assim, $P(n_0 - 1)$ é verdadeiro, e pela hipótese indutiva, $P[(n_0 - 1) + 1] = P(n_0)$ é verdadeiro. Mas, $n_0 \in \mathcal{S}$, pois é o menor elemento de $\mathcal{S}$. Temos uma contradição: $n_0 \in \mathcal{S}$ e $n_0 \notin \mathcal{S}$.

Portanto, $\mathcal{S} = \emptyset$, e com as hipóteses do problema, temos que $P(n)$ é verdadeiro para todo $n \in \mathbb{N}$ ■

Temos uma outra forma de enunciarmos o teorema 2.2.

Teorema 2.3. Dado um subconjunto $\mathcal{S}$ do conjunto $\mathbb{N}$ dos inteiros positivos; tal que:
1) $1 \in \mathcal{S}$
2) Para todo inteiro positivo k, se $k+1 \in \mathcal{S}$ sempre que $1, 2, 3, \ldots, k \in \mathcal{S}$, então $\mathcal{S}$ contém todos os inteiros positivos.

Para mais detalhes sobre o capitulo, o leitor pode recorrer a [1].

Agora, veremos algumas aplicações do Princípio da Indução Finita, que deixam mais claro como essa ferramenta é utilizada.

Exemplo 2.1. Para todo inteiro $n \geq 1$, tem-se

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

Demonstração : Para $n = 1$, a afirmação é verdadeira, visto que

$$1 = \frac{1 \cdot (1+1)}{2}$$

Suponhamos que a proposição seja verdadeira para $n = k$, isto é:

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

E mostraremos que vale para $n = k + 1$, ou seja,

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

De fato, da hipótese de indução temos:

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

Somando em ambos os lados $(k+1)$, obtemos:

$$\begin{aligned} 1 + 2 + \cdots + k + (k+1) &= \frac{k \cdot (k+1)}{2} + (k+1) \\ &= \frac{(k+1) \cdot (k+2)}{2} \end{aligned}$$

Portanto, $1 + 2 + \cdots + n = \dfrac{n \cdot (n+1)}{2}$, para todo $n \in \mathbb{N}$ ■

Exemplo 2.2. Se $x \geq 0$, então

$$(1+x)^n \geq 1 + nx + \frac{n \cdot (n-1)}{2} x^2$$

para todo $n \in \mathbb{N}$.

Demonstração : Para $n = 1$, a afirmação é verdadeira, visto que

$$(1+x)^1 = 1 + 1 \cdot x.$$

Suponhamos que a proposição seja verdadeira para $n = k$, isto é

$$(1+x)^k \geq 1 + kx + \frac{k \cdot (k-1)}{2} x^2 \; ; \quad x \geq 0$$

E mostraremos que vale para $n = k + 1$, ou seja,

$$(1+x)^{k+1} \geq 1 + (k+1)x + \frac{(k+1) \cdot [(k+1)-1)]}{2} x^2 \; ; \quad x \geq 0.$$

De fato, da hipótese de indução temos:

$$(1+x)^k \geq 1 + kx + \frac{k(k-1)}{2} x^2.$$

Multiplicando ambos os lados por $(1+x) > 0$,

$$\begin{aligned} (1+x)^k(1+x) = (1+x)^{k+1} &\geq \left[1 + kx + \frac{k(k-1)}{2}\, x^2\right](1+x) \\ &= 1 + (k+1)x + \frac{(k+1)k}{2}\, x^2 + \frac{k(k-1)}{2}\, x^3 \\ &\geq 1 + (k+1)x + \frac{(k+1)k}{2}\, x^2, \end{aligned}$$

pois $\dfrac{k(k-1)}{2}\, x^3 \geq 0$.

Assim,

$$(1+x)^k \geq 1+kx+\frac{k(k-1)}{2}x^2 \Longrightarrow (1+x)^{k+1} \geq 1+(k+1)x+\frac{(k+1)k}{2}\ x^2.$$

Portanto, $(1+x)^n \geq 1+nx+\frac{n(n-1)}{2}x^2$, para todo $n \in \mathbb{N}$ se $x \geq 0$ ■

Exemplo 2.3. Para todo $x \in \mathbb{R}$, $x \geq -1$ e $n \in \mathbb{N}$ tem-se

$$(1+x)^n \geq 1+nx.$$

Demonstração : Para $n = 1$, a afirmação é verdadeira, visto que

$$(1+x)^1 = 1+1\cdot x.$$

Suponhamos que a proposição seja verdadeira para $n = k$, isto é

$$(1+x)^k \geq 1+kx.$$

E mostraremos que vale para $n = k+1$, ou seja,

$$(1+x)^{k+1} \geq 1+(k+1)x.$$

De fato, da hipótese de indução temos:

$$(1+x)^k \geq 1+kx.$$

Multiplicando ambos os lados por $[x \geq -1 \Longrightarrow (x+1) \geq 0]$, temos,

$$\begin{aligned}(1+x)^k(1+x) = (1+x)^{k+1} &\geq (1+kx)(1+x)\\ &= 1+(k+1)x+kx^2\\ &\geq 1+(k+1)x,\end{aligned}$$

pois $kx^2 \geq 0$.

Assim,

$$(1+x)^k \geq 1+kx \Longrightarrow (1+x)^{k+1} \geq 1+(k+1)x.$$

Portanto, $(1+x)^n \geq 1+nx$, para todo $n \in \mathbb{N}$ ■

Exemplo 2.4. Sejam quais forem a, $n \in \mathbb{N}$ e $a \neq 1$, teremos

$$1+a+\cdots+a^n = \frac{a^{n+1}-1}{a-1}.$$

Demonstração : Para $n = 1$, a afirmação é verdadeira, visto que

$$1 + a = \frac{a^2 - 1}{a - 1} = \frac{(a + 1)(a - 1)}{a - 1} = a + 1.$$

Suponhamos que a proposição seja verdadeira para $n = k$, isto é

$$1 + a + \cdots + a^k = \frac{a^{k+1} - 1}{a - 1}.$$

E mostraremos que vale para $n = k + 1$, ou seja,

$$1 + a + \cdots + a^k + a^{k+1} = \frac{a^{(k+1)+1} - 1}{a - 1}.$$

De fato, da hipótese de indução temos:

$$1 + a + \cdots + a^k = \frac{a^{k+1} - 1}{a - 1}.$$

Somando ambos os lados por a^{k+1}, temos

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

Portanto, $1 + a + \cdots + a^n = \frac{a^{n+1} - 1}{a - 1}$, sejam quais forem a, $n \in \mathbb{N}$, $a \neq 1$. ■

Exemplo 2.5. Para qualquer $n \in \mathbb{N}$, é assegurado que

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

Demonstração : Para $n = 1$, a afirmação é verdadeira, visto que

$$\frac{1}{1 \cdot 2} = \frac{1}{1 + 1}.$$

Suponhamos que a proposição seja verdadeira para $n = k$, isto é

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

E mostraremos que vale para $n = k + 1$, ou seja,

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

De fato, da hipótese de indução temos:

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

Somando ambos os lados por $\frac{1}{(k+1)(k+2)}$, obtemos

$$\begin{aligned}\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{k(k+1)}+\frac{1}{(k+1)(k+2)} &= \frac{k}{k+1}+\frac{1}{(k+1)(k+2)}\\ &= \frac{(k+1)^2}{(k+1)(k+2)}\\ &= \frac{k+1}{k+2}\end{aligned}$$

Portanto, $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{n(n+1)}=\frac{n}{n+1}$, para todo $n\in\mathbb{N}$. ■

Exemplo 2.6. Para todo $n\in\mathbb{N}$,

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

Demonstração: Para $n=1$, a afirmação é verdadeira, visto que

$$1=1^2.$$

Suponhamos que a proposição seja verdadeira para $n=k$, isto é

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

E mostraremos que vale para $n=k+1$, ou seja,

$$1+3+5+\cdots+[2(k+1)-1]=(k+1)^2.$$

De fato da hipótese de indução temos:

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

Somando $2k+1$, em ambos os lados, temos

$$\begin{aligned}1+3+5+\cdots+(2k-1)+(2k+1) &= k^2+(2k+1)\\ 1+3+5+\cdots+(2k-1)+[2(k+1)-1] &= (k+1)^2\end{aligned}$$

Portanto, $1+3+5+\cdots+(2n-1)=n^2$, para todo $n\in\mathbb{N}$. ■

Capítulo 3

Divisão nos Inteiros

3.1 Divisibilidade

Definição: Sejam m e n dois inteiros, com $m \neq 0$. Dizemos que m divide n, se e somente se, existe um inteiro q tal que $n = mq$.

Se m divide n também diremos que m é um divisor de n, e mais ainda que n é um múltiplo de m, que n é divisível por m, ou simplesmente que m é um fator de n.

Denotamos por $m \mid n$ no qual se tem o seguinte significado que m divide n; $m \neq 0$, e caso m não divide n; $m \neq 0$, representamos por $m \nmid n$.

Notação m divide n ($m \mid n$) chama-se *relação de divisibilidade em* $\mathbb{Z}$.

Se m é um divisor de n, então $-m$ também é um divisor de n, pois a igualdade $n = mq$ implica $n = (-m)(-q)$, de tal modo que os divisores de um inteiro qualquer são dois a dois iguais em valor absoluto e de sinais opostos (simétricos).

Exemplo 3.1.

$$\begin{aligned} 3 \mid 12, &\quad \text{pois } 12 = 3 \cdot 4 \\ -7 \mid 35, &\quad \text{pois } 35 = (-7) \cdot (-5) \\ 5 \mid -30, &\quad \text{pois } -30 = 5 \cdot (-6) \\ 11 \nmid 20, &\quad \text{pois não existe } q \in \mathbb{Z};\ 20 = 11 \cdot q \end{aligned}$$

Teorema 3.1. Sejam m, n, q, r inteiros quaisquer, tem -se que:

(i) $1 \mid m, m \mid m$, e $m \mid 0$

(ii) Se $m \mid 1$, então $m = \pm 1$

(iii) Se $m \mid n$ e $q \mid r$, então $m \cdot q \mid n \cdot r$

(iv) Se $m \mid n$ e $n \mid q$, então $m \mid q$

(v) Se $m \mid n$ e $n \mid m$, então $m = \pm n$

(vi) Se $m \mid n$, com $n \neq 0$, então $\mid m \mid \leq \mid n \mid$

(*vii*) Se $m \mid n$ e $m \mid q$, então $m \mid (na + qb), \forall\, a, b \in \mathbb{Z}$

(*viii*) $0 \mid m \Leftrightarrow m = 0$

Demonstração:

(*i*) Temos que:
$m = 1 \cdot m, m = m \cdot 1$ e $0 = m \cdot 0$ ■

(*ii*) Como $m \mid 1$, então $1 = m \cdot q;\ q \in \mathbb{Z}$.
O que implica $m = 1$ e $q = 1$ ou $m = -1$ e $q = -1$, isto é $m = \pm 1$ ■

(*iii*) Temos que:
$m \mid n \Longrightarrow n = m \cdot a$, com $a \in \mathbb{Z}$
$q \mid r \Longrightarrow r = q \cdot b$, com $b \in \mathbb{Z}$
Desse modo $n \cdot r = (m \cdot q) \cdot ab \Longrightarrow m \cdot q \mid n \cdot r$ ■

(*iv*) Temos que:
$m \mid n \Longrightarrow n = m \cdot a;$ com $a \in \mathbb{Z}$
$n \mid q \Longrightarrow q = n \cdot b;$ com $b \in \mathbb{Z}$.
Substituindo $n = ma$ em $q = nb$; temos: $q = m(ab) \Longrightarrow m \mid q$ ■

(*v*) De $m \mid n \Longrightarrow n = m \cdot a$; $a \in \mathbb{Z}$ e de $n \mid m \Longrightarrow m = nb$; $b \in \mathbb{Z}$.
Portanto $m = n(ab) \Longrightarrow ab = 1 \Longrightarrow a = b = \pm 1 \Longrightarrow m = \pm n$ ■

(*vi*) Com efeito $m \mid n$, com $n \neq 0$ implica que $n = ma$.
Tomando módulos, temos que $|n| = |m| \cdot |a|$.
Como $n \neq 0$, temos que $|a| \neq 0$, portanto $1 \leq |a|$.
E consequentemente, $|m| \leq |a| \cdot |m| \Longrightarrow |m| \leq |m| \cdot |a| = |n| \Longrightarrow |m| \leq |n|$ ■

(*vii*) Com efeito $m \mid n \Longrightarrow n = mr$; $r \in \mathbb{Z}$ e de $m \mid q \Longrightarrow q = m \cdot s, s \in \mathbb{Z}$.
Portanto, quaisquer que sejam $a, b \in \mathbb{Z}$
$an + bq = a(mr) + b(ms) = m(ar) + m(bs) = m(ar + bs) \Longrightarrow m \mid (na + qb)$ ■

(*viii*) Suponhamos que $0 \mid m$, logo existe $a \in \mathbb{Z}$ tal que $m = a \mid 0$ ■

Proposição 3.1. *Se $a, b, c \in \mathbb{Z}$, tais que $a \mid (b \pm c)$. Então $a \mid b \Longleftrightarrow a \mid c$*

Demonstração: Será demonstrado apenas a seguinte implicação:
Se $a \mid (b + c)$, então $a \mid b \Longleftrightarrow a \mid c$
($\Longrightarrow$) Como $a \mid (b + c)$, existe $d \in \mathbb{Z}$, tal que

$$b + c = ad \tag{3.1}$$

Agora se $a \mid b$, logo existe $e \in \mathbb{Z}$, tal que

$$b = ae \tag{3.2}$$

Substituindo (3.2) em (3.1), temos:

$$ae + c = ad \Longrightarrow c = ad - ae \Longrightarrow c = a(d - e).$$

Portanto, $a \mid c$

($\Longleftarrow$) Suponhamos que $a \mid (b + c)$, existe $d \in \mathbb{Z}$, tal que

$$b + c = ad \tag{3.3}$$

E se $a \mid c$, logo existe $f \in \mathbb{Z}$, tal que

$$c = af \tag{3.4}$$

Substituindo a equação (3.4) em (3.3), temos:

$$b + af = ad \Longrightarrow b = ad - af \Longrightarrow b = a(d - f).$$

Portanto, $a \mid b$ ■

Proposição 3.2. Se $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$, então $(a - b) \mid (a^n - b^n)$

Demonstração: Para $n = 1$, a afirmação é verdadeira, visto que

$$a - b \mid a^1 - b^1.$$

Suponhamos verdadeira para $n = k$, isto é,

$$a - b \mid a^k - b^k.$$

E mostraremos que vale para $n = k + 1$, ou seja,

$$a - b \mid a^{k+1} - b^{k+1}.$$

Temos que

$$a^{k+1} - b^{k+1} = a \cdot a^k - b \cdot b^k, \tag{3.5}$$

e

$$b \cdot a^k - b \cdot a^k = 0. \tag{3.6}$$

Somando (3.6) na equação (3.5), teremos:

$$a \cdot a^k - b \cdot b^k + b \cdot a^k - b \cdot a^k = a^k \cdot (a - b) + b \cdot (a^k - b^k).$$

Como $(a - b) \mid a^k \cdot (a - b)$ e, por hipótese de indução, $(a - b) \mid (a^k - b^k)$.
Decorre da propriedade (*vii*) do **Teorema** 3.1 que $(a - b) \mid (a^{k+1} - b^{k+1})$.
Portanto o resultado é verdadeiro para todo $n \in \mathbb{N}$. ■

Proposição 3.3. Se $a, b \in \mathbb{Z}$ e $n \in \mathbb{N} \cup \{0\}$. Então $(a+b) \mid (a^{2n+1} + b^{2n+1})$.

Demonstração: Para $n = 0$, a afirmação é verdadeira, visto que

$$(a+b) \mid (a^{2\cdot 0+1} + b^{2\cdot 0+1})$$

Suponhamos verdadeiro para $n = k$, isto é,

$$(a+b) \mid (a^{2k+1} + b^{2k+1}).$$

E mostraremos que vale para $n = k+1$, ou seja,

$$(a+b) \mid (a^{2(k+1)+1} + b^{2(k+1)+1}).$$

Temos que

$$a^{2(k+1)+1} + b^{2(k+1)+1} = a^{2k+1}a^2 + b^{2k+1}b^2, \tag{3.7}$$

e

$$b^2a^{2k+1} - b^2a^{2k+1} = 0. \tag{3.8}$$

Somando (3.8) na equação (3.7), teremos:

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

Como, $(a+b) \mid (a^2 - b^2)a^{2k+1}$ e por hipótese de indução $(a+b) \mid (a^{2k+1} + b^{2k+1})$.
Decorre da propriedade (vii) do **Teorema** 3.1 que $(a+b) \mid (a^{2(k+1)+1} + b^{2(k+1)+1})$.
Portanto vale para todo $n \in \mathbb{N}$. ■

Proposição 3.4. Se $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Então $(a+b) \mid (a^{2n} - b^{2n})$.

Demonstração: Para $n = 1$, a afirmação é verdadeira, visto que

$$(a+b) \mid (a^{2.1} - b^{2.1}) \Longrightarrow (a+b) \mid (a^2 - b^2).$$

Suponhamos verdadeiro para $n = k$, isto é,

$$(a+b) \mid (a^{2k} - b^{2k}).$$

E mostraremos que vale para $n = k+1$, ou seja,

$$(a+b) \mid (a^{2(k+1)} - b^{2(k+1)})$$

Temos que

$$a^{2(k+1)} - b^{2(k+1)} = a^{2k}a^2 - b^{2k}b^2 \tag{3.9}$$

e

$$a^{2k}b^2 - a^{2k}b^2 = 0. \tag{3.10}$$

Somando (3.10) na equação (3.9), teremos:

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

Como, $(a + b) \mid a^{2k}(a^2 - b^2)$ e por hipótese de indução $(a + b) \mid (a^{2k} - b^{2k})$.
Decorre da propriedade (vii) do **Teorema** 3.1 que $(a + b) \mid (a^{2(k+1)} - b^{2(k+1)})$.
Portanto vale para todo $n \in \mathbb{N}$. ■
Para mais detalhes sobre os teoremas e proposições acima, o leitor pode recorrer a [3]

Exemplo 3.2. Sejam $a, b \in \mathbb{Z}$.
a) Se $a \neq b$, mostre que, para todo $n \in \mathbb{N}, n \geq 2$, temos

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

Solução: Para $n = 2$, a proposição é verdadeira visto que

$$\frac{a^2 - b^2}{a - b} = a^{2-1} + a^{2-2} \cdot b.$$

Suponhamos verdadeiro para $n = k$, ou seja,

$$\frac{a^k - b^k}{a - b} = a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}. \tag{3.11}$$

E mostraremos que vale para $n = k + 1$, isto é,

$$\frac{a^{k+1} - b^{k+1}}{a - b} = a^k + a^{k-1}b + \cdots + ab^{k-1} + b^k.$$

Temos que

$$\frac{a^{k+1} - b^{k+1}}{a - b} = \frac{a^k a - b^k b}{a - b}. \tag{3.12}$$

E

$$\frac{a^k b - a^k b}{a - b} = 0. \tag{3.13}$$

Somando (3.13) na equação (3.12) teremos:

$$\frac{a^k a - b^k b + a^k b - a^k b}{a - b} = \frac{a^k(a - b)}{a - b} + \frac{b(a^k - b^k)}{a - b} = a^k + \frac{b(a^k - b^k)}{a - b}. \tag{3.14}$$

Substituindo a hipótese de indução (3.11) na equação (3.14), teremos

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

Portanto é verdadeira para todo $n \geq 2$; $n \in \mathbb{N}$ ■

b) Se $a + b \neq 0$, mostre que, para todo $n \in \mathbb{N}$,

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

Solução: Para n = 0, a afirmação é verdadeira, visto que:

$$\frac{a^{2.0+1} + b^{2.0+1}}{a+b} = a^{2.0}.$$

Suponhamos verdadeiro para $n = k$, ou seja,

$$\frac{a^{2k+1} + b^{2k+1}}{a+b} = a^{2k} - a^{2k-1}b + \cdots - ab^{2k-1} + b^{2k}. \tag{3.15}$$

E mostraremos que vale para $n = k + 1$, isto é,

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

Temos que

$$\frac{a^{2(k+1)+1} + b^{2(k+1)+1}}{a+b} = \frac{a^2a^{2k+1} + b^2b^{2k+1}}{a+b} \tag{3.16}$$

e

$$\frac{b^2a^{2k+1} - b^2a^{2k+1}}{a+b} = 0. \tag{3.17}$$

Somando (3.17) na equação (3.16) teremos:

$$\begin{aligned} \frac{a^2a^{2k+1} + b^2b^{2k+1} + b^2a^{2k+1} - b^2a^{2k+1}}{a+b} &= \frac{a^{2k+1}(a^2 - b^2)}{a+b} + \frac{b^2(a^{2k+1} + b^{2k+1})}{a+b} \\ &= a^{2k+1}(a-b) + \frac{b^2(a^{2k+1} + b^{2k+1})}{a+b} \end{aligned} \tag{3.18}$$

Substituindo a hipótese de indução (3.15) na equação (3.18), teremos

$$\begin{aligned} a^{2k+1}(a-b) + b^2(a^{2k} - a^{2k-1}b + \cdots - ab^{2k-1} + b^{2k}) &= \\ = a^{2k+2} - a^{2k+1}b + a^{2k}b^2 - \cdots - ab^{2k+1} + b^{2k+2}) &= \\ = a^{2(k+1)} - a^{2(k+1)-1}b + \cdots - ab^{2(k+1)-1} + b^{2(k+1)}. \end{aligned}$$

Assim temos que

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

Portanto é verdadeiro para todo $n \in \mathbb{N}$. ■

c) Se $a + b \neq 0$, mostre que, para todo $n \in \mathbb{N}$,

$$\frac{a^{2n} - b^{2n}}{a+b} = a^{2n-1} - a^{2n-2}b + \cdots + ab^{2n-2} - b^{2n-1}$$

Solução: Para n = 1, a afirmação é verdadeira, visto que

$$\frac{a^{2.1} - b^{2.1}}{a+b} = a^{2.1-1} - a^{2.1-2}b.$$

Suponhamos verdadeiro para $n = k$, ou seja,

$$\frac{a^{2k} - b^{2k}}{a+b} = a^{2k-1} - a^{2k-2}b + \cdots + ab^{2k-2} - b^{2k-1}. \tag{3.19}$$

E mostraremos que vale para $n = k + 1$, isto é,

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

Temos que

$$\frac{a^{2(k+1)} - b^{2(k+1)}}{a+b} = \frac{a^{2k}a^2 - b^{2k}b^2}{a+b}, \tag{3.20}$$

e

$$\frac{a^{2k}b^2 - a^{2k}b^2}{a+b} = 0. \tag{3.21}$$

Somando (3.21) na equação (3.20) teremos:

$$\begin{aligned} \frac{a^{2k}a^2 - b^{2k}b^2 + a^{2k}b^2 - a^{2k}b^2}{a+b} &= \frac{a^{2k}(a^2 - b^2)}{a+b} + \frac{b^2(a^{2k} - b^{2k})}{a+b} \\ &= a^{2k}(a-b) + \frac{b^2(a^{2k} - b^{2k})}{a+b} \end{aligned} \tag{3.22}$$

Substituindo a hipótese de indução (3.19) na equação (3.22), teremos

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

$$= a^{2k+1} - a^{2k}b + a^{2k-1}b^2 - a^{2k-2}b^2 + \cdots + ab^{2k} - b^{2k+1}.$$

Assim teremos que

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

Portanto é verdadeiro para todo $n \in \mathbb{N}$. ■

3.2 Conjunto dos divisores de um inteiro

Dado um inteiro qualquer a, o conjunto de todos os divisores de a é indicado por $D(a)$, ou seja:

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

Assim, por exemplo:

$$\begin{aligned} D(0) &= \{x \in \mathbb{Z}^*;\ x \mid 0\} = \mathbb{Z}^* \\ D(1) &= \{x \in \mathbb{Z}^*;\ x \mid 1\} = \{\pm 1\} \\ D(3) &= \{x \in \mathbb{Z}^*;\ x \mid 3\} = \{\pm 1,\ \pm 3\} \\ D(10) &= \{x \in \mathbb{Z}^*;\ x \mid 10\} = \{\pm 1,\ \pm 2,\ \pm 5,\ \pm 10\} \end{aligned}$$

E temos ainda que para todo inteiro a, $D(a) = D(-a)$, e também

$$a = a \cdot 1 = (-a) \cdot (-1).$$

Logo 1, -1, a e $-a$ são divisores de a, na qual denominamos *divisores triviais* de a. E mais ainda, o inteiro 1 (ou -1) só admite *divisores triviais*.

Para todo inteiro $a \neq 0$, se $x \mid a$, então

$$-a \leq x \leq a \Longrightarrow D(a) \subset [-a, a],$$

ou seja, para todo inteiro $a \neq 0$ temos um número finito de divisores.

3.3 Divisores comuns de dois inteiros

Definição: Sejam a e b dois inteiros quaisquer, chama - se *divisor comum* de a e b todo inteiro $d \neq 0$, tal que $d \mid a$ e $d \mid b$.

Dados os inteiros a e b, denominamos $D(a, b)$ o conjunto de todos os divisores comuns de a e b. Simbolicamente, temos:

$$D(a, b) = \{x \in \mathbb{Z}^*;\ x \mid a \text{ e } x \mid b\},$$

ou seja:

$$D(a, b) = \{x \in \mathbb{Z}^*;\ x \in D(a) \text{ e } x \in D(b)\},$$

logo:

$$D(a, b) = D(a) \cap D(b).$$

Temos que a intersecção é uma operação comutativa, ou seja, $D(a, b) = D(b, a)$.

Notamos que -1 e 1 são divisores comuns de dois inteiros quaisquer a e b, logo $D(a, b) \neq \varnothing$.

E se $a = b = 0$, então todo inteiro não nulo é um divisor comum de a e b, assim $D(a, b) = \mathbb{Z}^*$.

Sobre a seção 3.2 e 3.3 o leitor poderá recorrer a referência [1].

Exemplo 3.3. Sejam os inteiros $a = 24$ e $b = -16$, quais os divisores comuns de a e b?

Solução:

$$\begin{aligned} D(24) &= \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24\} \\ D(-16) &= \{\pm 1, \pm 2, \pm 4, \pm 8, \pm 16\}. \end{aligned}$$

Portanto:

$$D(24, -16) = D(24) \cap D(-16) = \{\pm 1, \ \pm 2, \pm 4, \pm 8\}.$$

Exemplo 3.4. Sejam os inteiros $a = 2$ e $b = 13$, quais os divisores comuns de a e b?

Solução:

$$\begin{aligned} D(2) &= \{\pm 1, \pm 2\} \\ D(13) &= \{\pm 1, \pm 13\}. \end{aligned}$$

Portanto:

$$D(2, 13) = D(2) \cap D(13) = \{\pm 1\}.$$

3.4 Divisão Euclidiana

Teorema 3.2 (Divisão Euclidiana)**.** Sejam $a, b \in \mathbb{Z}$; $0 < a < b$. Existem dois únicos números inteiros q e r, tais que

$$b = aq + r, \text{ com } 0 \leq r < |a|$$

Demonstração: (Existência) Suponhamos que $0 < a$ e $q \in \mathbb{Z}$, tal que q é o maior inteiro e $aq \leq b$. Assim, temos

$$\begin{aligned} aq \leq b < a \cdot (q+1) &\implies aq \leq b < aq + a \\ &\implies 0 \leq b - aq < a, \text{ definimos } r = b - aq, \text{ou seja, } 0 \leq r < a. \end{aligned}$$

(Unicidade) Sejam q, q_1, r, r_1 inteiros tais que $b = aq + r$, $b = aq_1 + r_1$ e $0 \leq r, r_1 < |a|$. Logo, teremos que $|r - r_1| < a$ e de $b = aq + r$ (I) e $b = aq_1 + r_1$ (II), e fazendo (I) - (II), temos

$$0 = aq + r - aq_1 - r_1$$

$$r_1 - r = aq - aq_1$$

$$r_1 - r = a(q - q_1).$$

Suponhamos que $q \neq q_1$. Assim teremos que $1 \leq |q - q_1|$. Multiplicando a desigualdade por $|a|$, teremos

$|a| \leq |a| \cdot |q - q_1| = |r_1 - r| < |a|$, ou seja, $|a| < |a|$, absurdo, desse modo $q = q_1$ e $r = r_1$ ■

Sobre o teorema 3.2 o leitor pode consultar [3]

3.5 Paridade de um inteiro

Dado um inteiro qualquer a, ao dividirmos a por $b = 2$ os possíveis valores para os restos são $r = 0$ ou $r = 1$. Se $r = 0$, então o inteiro a é da forma $a = 2q$ e denominamos par, para algum $q \in \mathbb{Z}$. Caso $r = 1$, então o inteiro $a = 2q + 1$ e é denominado ímpar, para algum $q \in \mathbb{Z}$.

Proposição 3.5. Se a é um inteiro qualquer, então a^2 dividido por 4 deixa resto 0 ou 1.

Demonstração: Seja $q \in \mathbb{Z}$, temos que:

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

ou

$$a^2 = (2q+1)^2 \implies a^2 = 4q^2 + 4q + 1 \implies a^2 = 4(q^2 + q) + 1$$

Portanto os possíveis restos é 0 ou 1. ■

Exemplo 3.5. Se a é um inteiro qualquer, então um dos inteiros a, $a+2$, $a+4$ é divisível por 3.

Solução: Ao dividirmos um inteiro qualquer a por 3, os possíveis restos são $0, 1$, ou 2. Desse modo temos $a = 3y$ ou $a = 3y+1$ ou $a = 3y+2$, para algum $y \in \mathbb{Z}$.

Caso $a = 3y \Longrightarrow 3 \mid a$

Caso $a = 3y+1$, adicionamos 2 unidades em ambos os lados da igualdade teremos
$a+2 = 3y+1+2$
$a+2 = 3y+3$
$a+2 = 3(y+1) \Longrightarrow 3 \mid (a+2)$

Caso $a = 3y+2$ adicionamos 4 unidades em ambos os lados da igualdade teremos
$a+4 = 3y+2+4$
$a+4 = 3y+6$
$a+4 = 3(y+2) \Longrightarrow 3 \mid (a+4)$

Exemplo 3.6. Para todo $a \in \mathbb{Z}$, temos que:
a) $2 \mid (a^2 - a)$
b) $3 \mid (a^3 - a)$

Solução: a) Temos que $a^2 - a = a(a-1)$, então $2 \mid a(a-1)$, logo existe $c \in \mathbb{Z};\ a(a-1) = 2c$, porém a pode ser par ou ímpar, assim analisaremos.

Se $a = 2k; k \in \mathbb{Z} \Longrightarrow 2 \mid 2k(2k-1) \Longrightarrow 2 \mid 2(2k^2 - k) \Longrightarrow 2 \mid 2d; \quad d = 2k^2 - k.$

Se $a = 2k+1; k \in \mathbb{Z} \Longrightarrow 2 \mid (2k+1)(2k+1-1) \Longrightarrow 2 \mid (2k+1)(2k) \Longrightarrow 2 \mid 2(2k^2+k) \Longrightarrow 2 \mid 2e$; $e = 2k^2 + k$.

Portanto $2 \mid (a^2 - a)$
b) Temos que $a^3 - a = a(a^2-1) = a(a+1)(a-1) = (a-1)a(a+1)$.

Se $3 \mid a^3 - a \Longrightarrow 3 \mid (a-1)a(a+1)$.

Se $a = 3k;\ k \in \mathbb{Z} \Longrightarrow 3 \mid (3k-1)3k(3k+1) \Longrightarrow 3 \mid 3[k(3k-1)(3k+1)] \Longrightarrow 3 \mid 3b; b = k(3k-1)(3k+1)$.

Se $a = 3k+1;\ k \in \mathbb{Z} \Longrightarrow 3 \mid (3k+1-1)(3k+1)(3k+1+1) \Longrightarrow 3 \mid 3k(3k+1)(3k+2) \Longrightarrow 3 \mid 3[k(3k+1)(3k+2)] \Longrightarrow 3 \mid 3c;\ c = k(3k+1)(3k+1)$.

Se $a = 3k+2;\ k \in \mathbb{Z} \Longrightarrow 3 \mid (3k+2-1)(3k+2)(3k+2+1) \Longrightarrow 3 \mid (3k+1)(3k+2)(3k+3) \Longrightarrow 3 \mid (3k+1)(3k+2)3(k+1) \Longrightarrow 3 \mid 3(k+1)(3k+1)(3k+2) \Longrightarrow 3 \mid 3d;\ d = (k+1)(3k+1)(3k+2)$.

Portanto $3 \mid a^3 - a$. ■

Capítulo 4

Máximo Divisor Comum

Definição: Sejam a e b dois inteiros não simultaneamente nulos ($a \neq 0$ ou $b \neq 0$). Diremos que um inteiro positivo $d\,(d > 0)$ é o máximo divisor comum (mdc) de a e b se satisfaz às seguintes condições.

(i) $d \mid a$ e $d \mid b$

(ii) se $c \mid a$ e $c \mid b$, então $c \leq d$.

Notemos que pela condição (i), d é um divisor comum de a e b, e pela condição (ii), d é o maior dentre todos os divisores comuns de a e b.

Indicaremos $\text{mdc}(a, b)$ como máximo divisor comum de a e b.

Temos que o mdc de a e b não depende da ordem em que são tomados a e b, desse modo diremos que $\text{mdc}(a, b) = \text{mdc}(b, a)$.

Se a e b são dois inteiros, se existir o mdc de a e b, então:

$$\text{mdc}(a, b) = \text{mdc}(-a, b) = \text{mdc}(a, -b) = \text{mdc}(-a, -b).$$

Assim sendo, temos que para o cálculo do mdc de dois números inteiros, podemos sempre tomar os números inteiros positivos. Além disso, valem as seguintes propriedades:

(1) $\text{mdc}(0, 0)$ não existe

(2) $\text{mdc}(a, 1) = 1$, para qualquer $a \in \mathbb{Z}$

(3) se $a \neq 0$, então $\text{mdc}(a, 0) = |a|$

(4) se $a \mid b$, então $\text{mdc}(a, b) = |a|$

Assim, por exemplo:

$$\begin{aligned} \text{mdc}(6, 1) &= 1 \\ \text{mdc}(-7, 0) &= |-7| = 7 \\ \text{mdc}(-4, 16) &= |-4| = 4 \end{aligned}$$

4.1 Existência e Unicidade do MDC

O máximo divisor comum entre dois inteiros sempre existe. Isso é mostrado através de um método conhecido como Algoritmo de Euclides, que permite calcular o mdc de dois números naturais quaisquer. Para a prova desse método, é usado, essencialmente, a proposição abaixo.

Proposição 4.1. Dados os inteiros a, b, n. Se existe $\text{mdc}(a, b - na)$, então, $\text{mdc}(a, b)$ existe e

$$\text{mdc}(a, b) = \text{mdc}(a, b - na).$$

Demonstração: Seja $d = \text{mdc}(a, b - na)$. Desse modo $d \mid a$ e $d \mid (b - na)$, e mais ainda d divide $b = b - na + na$. Portanto, d é um divisor comum de a e b.

Suponhamos agora que m seja um divisor comum de a e b. Assim, m é um divisor comum de a e $b - na$ e, portanto, $m \mid d$. O que demonstra que $d = \text{mdc}(a, b)$.

A proposição 4.1 é utilizada para o cálculo do mdc de dois números inteiros positivos, na qual será essencial estabelecer o Algoritmo de Euclides, assim veremos nos exemplos a seguir.

O resultado abaixo é bem conhecido e pode ser encontrado, por exemplo, em [5].

Proposição 4.2. Sejam a e b dois inteiros não simultaneamente nulos ($a \neq 0$ ou $b \neq 0$). Existem $x, y \in \mathbb{Z}$ tais que

$$\text{mdc}(a, b) = ax + by,$$

ou seja, o $\text{mdc}(a, b)$ é uma combinação linear de a e b.

Exemplo 4.1. Seja $a \in \mathbb{Z}$ com $a \neq 1$ e $m \in \mathbb{N}$, temos que

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

Solução: Verifiquemos o resultado acima.

Para $m = 1$, a proposição é verdadeira, visto que

$$\text{mdc}\left(\frac{a^1 - 1}{a - 1}, a - 1\right) = \text{mdc}(a - 1, 1)$$

Suponhamos que $m \geq 2$ e $m \in \mathbb{N}$. E chamando de d o primeiro membro da igualdade, e pelo exemplo 8a, temos que

$$d = \text{mdc}(a^{m-1} + a^{m-2} + \cdots + a + 1, a - 1) = (\text{mdc}(a^{m-1} - 1) + \text{mdc}(a^{m-2} - 1) + \cdots + \text{mdc}(a - 1) + m \cdot 1, a - 1).$$

E como, pela proposição 3.2, temos que

$$a - 1 | \text{mdc}(a^{m-1} - 1) + \text{mdc}(a^{m-2} - 1) + \cdots + \text{mdc}(a - 1),$$

logo

$$\text{mdc}(a^{m-1} - 1) + \text{mdc}(a^{m-2} - 1) + \cdots + \text{mdc}(a - 1) = n \cdot \text{mdc}(a - 1),$$

para algum $n \in \mathbb{N}$, e portanto pela proposição 4.1 , temos que

$$d = \text{mdc}(n \cdot (a-1) + m, a-1) = \text{mdc}(a-1, n(a-1)+m) = \text{mdc}(a-1, m).$$

Exemplo 4.2. Qual o valor do

$$\text{mdc}\left(\frac{3^{40}-1}{3^5-1}, 3^5-1\right).$$

Solução:
Pelo exemplo 4.1 , teremos:

$$\text{mdc}\left(\frac{3^{40}-1}{3^5-1}, 3^5-1\right) = \text{mdc}\left(\frac{(3^5)^8-1}{3^5-1}, 3^5-1\right) = \text{mdc}(3^5-1, 8) = \text{mdc}(8, 242) = 2.$$

Teorema 4.1. Se a e b são inteiros e $b = aq + r$, onde q e r são inteiros, então $\text{mdc}(a, b) = \text{mdc}(a, r)$.

Demonstração: Da relação $b = aq + r$, pelo **Teorema** 3.1 (*vii*), observamos que todo divisor de a e r é um divisor de b. E desta mesma relação segue que $r = b - aq$, de onde obtemos que todo divisor de a e b é um divisor de r. Portanto, o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de a e r, de onde concluímos que $\text{mdc}(a, b) = \text{mdc}(a, r)$. ■

Temos que o máximo divisor comum entre dois ou mais números é o algarismo de maior valor no qual divide todos os números ao mesmo tempo. E esse algoritmo pode ser calculado através da regra prática ou pela divisão sucessiva. Sendo assim iremos abordar o cálculo do máximo divisor comum através da divisão sucessivas de Euclides no qual enunciaremos a seguir.

Teorema 4.2 (Método das Divisões Sucessivas de Euclides)**.** Sejam $r_0 = b$ e $r_1 = a$ inteiros não-negativos com $a \neq 0$. Se o algoritmo da divisão for aplicado sucessivamente para se obter

$$r_j = q_{j+1} r_{j+1} + r_{j+2}, \quad 0 \leq r_{j+2} < r_{j+1}$$

para $j = 0, 1, 2, \ldots, n-1$ e $r_{n+1} = 0$, então $\text{mdc}(a, b) = r_n$, o último resto não-nulo.

Demonstração: Inicialmente aplicaremos o Teorema do Algoritmo da Divisão para dividir $r_0 = b$ por $r_1 = a$, obtendo $r_0 = q_1 r_1 + r_2$, em seguida dividimos r_1 por r_2 obtendo $r_1 = q_2 r_2 + r_3$ e assim sucessivamente até que obtivermos o resto $r_{n+1} = 0$. Note que, em cada passo, o resto é sempre menor que o anterior, e como os números em questão são positivos, após um número finito de aplicações do Teorema do Algoritmo da Divisão, vamos obter um resto nulo.

Nesse caso, teremos a seguinte sequência de equações:

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2 \qquad 0 < r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3 \qquad 0 < r_3 < r_2 \\
r_2 &= q_3 r_3 + r_4 \qquad 0 < r_4 < r_3 \\
&\vdots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n \qquad 0 < r_n < r_{n-1} \\
r_{n-1} &= q_n r_n + 0.
\end{aligned}$$

Resulta da última equação que, pelo Teorema 4.1, o máximo divisor comum de r_n e r_{n-1} é r_n. A penúltima, que este número é igual a $\text{mdc}(r_{n-1}, r_{n-2})$ e, prosseguindo assim teremos, através da aplicação sucessiva do Teorema 4.1, a seguinte sequência de igualdades:

$$r_n = \text{mdc}(r_{n-1}, r_n) = \text{mdc}(r_{n-2}, r_{n-1}) = \ldots = \text{mdc}(r_1, r_2) = \text{mdc}(r_0, r_1) = \text{mdc}(a, b).$$

Portanto, o máximo divisor comum de a e b é o último resto não-negativo das sequência de divisões acima descrita. ■

O método das divisões sucessivas de Euclides, pode ser reescrito de uma maneira apropriada para os alunos do ensino fundamental, onde aqui mostraremos a configuração do método.
Para um caso mais geral efetuamos a divisão $b = aq_1 + r_1$

	q_1	
b	a	
r_1		

Em seguida, prosseguindo a divisão $a = r_1q_2 + r_2$ e colocamos os números envolvidos no diagrama temos

	q_1	q_2	
b	a	r_1	
r_1	r_2		

Continuando, enquanto for possível, obteremos:

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

Agora faremos alguns exemplos utilizando o método de divisão sucessivas de Euclides.

Exemplo 4.3. Vamos calcular o $\text{mdc}(637, 3887)$.

Solução: Aplicando o Algoritmo de Euclides ao $\text{mdc}(637, 3887)$, teremos:

$$\begin{aligned} 3887 &= 6 \cdot 637 + 65 \\ 637 &= 9 \cdot 65 + 52 \\ 65 &= 1 \cdot 52 + 13 \\ 52 &= 4 \cdot 13 \end{aligned}$$

Utilizando a o diagrama em formato de tabela teremos a seguinte configuração:

	6	9	1	4
3887	637	65	52	13
65	52	13		

Assim sendo dizemos que um número d é combinação linear nos inteiros dos números a e b, se existirem $x, y \in \mathbb{Z}$, tais que $d = ax + by$. E notamos que o mdc de 3887 e 637 é uma combinação linear desses número, no qual observamos no exemplo acima, o Algoritmo de Euclides fornece-nos:

$$\begin{aligned} 13 &= 65 - 1 \cdot 52 \\ 52 &= 637 - 9 \cdot 65 \\ 65 &= 3887 - 6 \cdot 637 \end{aligned}$$

No qual segue que

$$\begin{aligned} 13 &= 65 - 1 \cdot 52 = 65 - 1 \cdot (637 - 9 \cdot 65) = \\ &= 10 \cdot 65 - 637 = 10 \cdot (3887 - 6 \cdot 637) - 637 = \\ &= 3887 \cdot 10 - 66 \cdot 637 \end{aligned}$$

Assim, podemos escrever:

$$13 = 3887 \cdot 10 + 637 \cdot (-61)$$

Exemplo 4.4. Calcularemos o inteiro positivo k tal que os restos das divisões de 4933 e 4435 por k são respectivamente 37 e 19.

Solução: Notemos que 37 é o resto da divisão de 4933 por k, assim sendo o resto da divisão de $4933 - 37 = 4896$ por k é igual a zero, e mais ainda o número 4896 é um múltiplo de k. De modo análogo temos que o número $4435 - 19 = 4416$ também é um múltiplo de k. Assim k é um divisor comum dos números 4896 e 4416, portanto, k é um máximo divisor comum desses dois números.

Desse modo aplicaremos o Algoritmo de Euclides para calcular este mdc

	1	9	5
4896	4416	480	96
480	96		

Portanto, o $\text{mdc}(4896, 4416) = 96$, além disso temos como divisores de 96.

$$D(96) = \{1, 2, 3, 4, 6, 8, 12, 16, 24, 32, 48, 96\}.$$

Observamos que o resto da divisão de 4933 por k é igual a 37, assim podemos concluir que o número k é um valor maior que 37, pois caso contrário deixaria um resto menor que 37, portanto $37 < k$. Logo, como k também é um divisor de 96, vemos que as únicas possibilidades são $k = 48$ e $k = 96$.

Exemplo 4.5. Utilizando o Algoritmo de Euclides vamos calcular $d = \text{mdc}(-39, 17)$, em seguida escrever $d = a \cdot x + b \cdot y$.

Solução: Como o mdc$(-39, 17)$ = mdc$(39, 17)$, aplicaremos o algoritmo de Euclides ao mdc$(39, 17)$ desse modo:

$$\begin{aligned} 39 &= 2 \cdot 17 + 5 \\ 17 &= 3 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

Utilizando a o diagrama em formato de tabela teremos a seguinte configuração:

	2	3	2	2
39	17	5	2	1
5	2	1		

Portanto, o mdc(-39,17) = 1.

Assim sendo dizemos que um número d é combinação linear nos inteiros dos números a e b, se existirem $x, y \in \mathbb{Z}$, tais que $d = ax+by$. E notamos que o mdc de -39 e 17 é uma combinação linear desses número, no qual observamos no exemplo acima, o Algoritmo de Euclides fornece-nos:

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ 2 &= 17 - 3 \cdot 5 \\ 5 &= 39 - 2 \cdot 17 \end{aligned}$$

No qual segue que

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 = 5 - 2 \cdot (17 - 3 \cdot 5) = \\ &= 7 \cdot 5 - 2 \cdot 17 = 7 \cdot (39 - 2 \cdot 17) - 2 \cdot 17 = \\ &= (-39) \cdot (-7) + 17 \cdot (-16) \end{aligned}$$

Assim, podemos escrever:

$$1 = (-39) \cdot (-7) + 17 \cdot (-16)$$

4.2 Inteiros primos entre si

Definição: Sejam $a, b \in \mathbb{Z}$ não simultaneamente nulos ($a \neq 0$ e $b \neq 0$). Diremos que a e b são primos entre si, ou coprimos se e somente se o mdc$(a, b) = 1$.

Assim, por exemplo:

São primos entre si os inteiros: 3 e 7, -11 e 20, -30 e -41, visto que

$$\text{mdc}(3, 7) = \text{mdc}(-11, 20) = \text{mdc}(-30, -41) = 1$$

Teorema 4.3. Sejam a e b dois inteiros não simultaneamente nulos ($a \neq 0$ ou $b \neq 0$), diremos que a e b são primos entre si, se e somente se, existem $x, y \in \mathbb{Z}$ tais que

$$ax + by = 1.$$

Demonstração: ($\Longrightarrow$) Como a e b são primos entre si, então $\text{mdc}(a, b) = 1$, logo pelo Proposição 4.2 existem, $x, y \in \mathbb{Z}$, tais que

$$ax + by = 1.$$

($\Longleftarrow$) Reciprocamente, se existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$ e se o $\text{mdc}(a, b) = d$, logo $d \mid a$ e $d \mid b$. Portanto, $d \mid (ax + by)$ e $d \mid 1$, o que implica $d = \pm 1$ ou $\text{mdc}(a, b) = 1$, ou seja, a e b são primos entre si. ■

Proposição 4.3. Dados $a, b, c \in \mathbb{Z}^*$, então vale as seguintes propriedades:

(i) Sejam $a, b \in \mathbb{Z}$, não simultaneamente nulos, então $\text{mdc}\left(\frac{a}{\text{mdc}(a,b)}, \frac{b}{\text{mdc}(a,b)}\right) = 1$.

(ii) Se $a \mid b$ e $\text{mdc}(b, c) = 1$, então $\text{mdc}(a, c) = 1$.

(iii) Se $a \mid c$, e $b \mid c$ e se $\text{mdc}(a, b) = 1$, então $ab \mid c$.

(iv) Se $\text{mdc}(a, b) = 1 = \text{mdc}(a, c)$, então o $\text{mdc}(a, bc) = 1$.

(v) Se o $\text{mdc}(a, bc) = 1$, então $\text{mdc}(a, b) = 1 = \text{mdc}(a, c)$.

(vi) Se $a \mid bc$ e se $\text{mdc}(a, b) = 1$, então $a \mid c$.

(vii) Se $b \mid a$ e $c \mid a$, se e somente se, $\frac{bc}{\text{mdc}(b,c)} \mid a$.

Demonstração:
(i) Seja $d = \text{mdc}(a, b)$, temos que $d \mid a$ e $d \mid b$, assim existem $m, n \in \mathbb{Z}$, tal que

$$a = dm \qquad \text{e} \qquad b = dn$$

E também existem $x, y \in \mathbb{Z}$, tal que

$$ax + by = d$$

Logo,

$$dmx + dny = d \tag{4.1}$$

Dividindo a equação 4.1 por d, teremos

$$mx + ny = 1,$$

ou seja,

$$\frac{a}{d}x + \frac{b}{d}y = 1$$

Portanto pelo **Teorema** 4.3 , temos que $\text{mdc}\left(\frac{a}{\text{mdc}(a,b)}, \frac{b}{\text{mdc}(a,b)}\right) = 1$. ■

(*ii*) Se $a \mid b$, então, existe $m \in \mathbb{Z}; b = am$
Se $\text{mdc}(b, c) = 1$, então pelo **Teorema** 4.3 , existem $x, y \in \mathbb{Z}$, tal que

$$bx + cy = 1$$

Assim,

$$\begin{aligned} 1 &= (am)x + cy \\ &= a(mx) + cy \\ &= an + cy\,; \ \ (n = mx). \end{aligned}$$

Portanto $\text{mdc}(a, c) = 1$. ■

(*iii*) Se $a|c$ e $b|c$, então, existem $m, n \in \mathbb{Z}$; $c = am$ e $c = bn$.
Se $\text{mdc}(a, b) = 1$, então, pelo **Teorema** 4.3, existem $x, y \in \mathbb{Z}$, tal que

$$\begin{aligned} ax + by = 1 \implies & \frac{c}{m}x + \frac{c}{n}y = 1 \\ \implies & c(nx + my) = mn \\ \implies & abc(nx + my) = abmn \\ \implies & abc(nx + my) = c^2 \\ \implies & ab(nx + my) = c. \end{aligned}$$

Portanto, $ab|c$. ■

(*iv*) Se $\text{mdc}(a, b) = 1$, então, pelo **Teorema** 4.3 , existem $x, y \in \mathbb{Z}$;

$$ax + by = 1 \tag{4.2}$$

E se $\text{mdc}(a, c) = 1$, então, pelo **Teorema** 4.3 , existem $p, q \in \mathbb{Z}$;

$$ap + cq = 1 \tag{4.3}$$

Multiplicando a equação 4.2 pela 4.3 teremos:

$$\begin{aligned} 1 &= (ax + by)(ap + cq) \\ &= a(axp + xcq + byp) + bc(yq) \\ &= az + bcw; (z = axp + xcq + byp \text{ e } w = yq). \end{aligned}$$

Portanto, $\text{mdc}(a, bc) = 1$ ■

(v) Se $\text{mdc}(a, bc) = 1$, então, pelo **Teorema** 4.3, existem $x, y \in \mathbb{Z}$;

$$\begin{aligned} 1 &= ax + bcy \\ &= ax + b(cy) = ax + c(by). \end{aligned}$$

Portanto, $\text{mdc}(a, b) = 1 = \text{mdc}(a, c)$. ■

(vi) Se $a \mid bc$, então existe $m \in \mathbb{Z}$; $bc = am$.
Se $\text{mdc}(a, b) = 1$, então, pelo **Teorema** 4.3 existem $x, y \in \mathbb{Z}$;

$$\begin{aligned} ax + by = 1 &\implies acx + bcy = c \\ &\implies acx + amy = c \\ &\implies a(cx + my) = c \\ &\implies an = c\,;\ (n = cx + my). \end{aligned}$$

Portanto, $a \mid c$. ■

(vii) $\implies$ Se $b \mid a$ e $c \mid a$, temos que existem $m, n \in \mathbb{Z}$, tal que $a = mb = nc$. Logo

$$m\frac{b}{\text{mdc}(b, c)} = n\frac{c}{\text{mdc}(b, c)}.$$

■

Poderemos também estender a definição de máximo divisor comum de dois inteiros para o caso de vários números inteiros como mostraremos a seguir.

Definição: Sejam $a_1, \cdots a_n \in \mathbb{Z}$ não todos nulos. Dizemos que $d \in \mathbb{Z}$ é um *máximo divisor comum de* $a_1, \cdots, a_n$, se satisfaz às seguintes condições.

(i) $d > 0$;

(ii) $d \mid a_i$, para todo $i = 1, \cdots, n$;

(iii) se $c \mid \mathbb{Z}$ for tal que $c \mid a_i\,(i = 1, \cdots, n)$, então $c \mid d$.

O máximo divisor comum, quando existe, é decerto único e denotaremos por:

$$\text{mdc}(a_1, \cdots, a_n).$$

A propriedade a seguir nada mais é do que um processo indutivo para o cálculo do mdc de n números inteiros, no qual se reduz à aplicação do Algoritmo de Euclides a $n - 1$ pares de inteiros.

Proposição 4.4. Sejam $a_1, \cdots, a_n$ inteiros não todos nulos, existe o mdc e

$$\text{mdc}(a_1, \cdots, a_n) = \text{mdc}(a_1, \cdots, \text{mdc}(a_{n-1}, a_n)).$$

Diremos que os inteiros $a_1, \cdots, a_n$ são primos entre si, ou coprimos, se $\text{mdc}(a_1, \cdots, a_n) = 1$

Exemplo 4.6. Suponha que $\text{mdc}(a, 4) = 2 = \text{mdc}(b, 4)$. Então temos que $\text{mdc}(a + b, 4) = 4$.

Solução: Como $\text{mdc}(a, 4) = 2$ e $\text{mdc}(b, 4) = 2$ temos que a e b são pares e mais ainda não são múltiplos de 4, pois caso contrário, 2 não seria o mdc entre eles.

Assim sendo o resto da divisão de a e b por 4 é 2.

Desse modo existem $n_1, n_2 \in \mathbb{Z}$ tais que

$$a = 4n_1 + 2 \tag{4.4}$$

e

$$b = 4n_2 + 2. \tag{4.5}$$

Somando membro a membro as equações 4.4 e 4.5, teremos:

$$\begin{aligned} a + b &= 4(n_1 + n_2 + 1) \\ &= 4m;\ (m = n_1 + n_2 + 1). \end{aligned}$$

Portanto, $4|a + b$, logo $\text{mdc}(a + b, 4) = 4$, o que prova nossa afirmação

Exemplo 4.7. Vamos encontrar os inteiros positivos a e b de modo que:

$$a + b = 63 \qquad \text{e} \qquad \text{mdc}(a, b) = 9$$

Solução: Como $\text{mdc}(a, b) = 9$, temos que $9|a$ e $9|b$. Assim existem inteiros n_1 e n_2, tal que:

$$a = 9n_1 \qquad \text{e} \qquad b = 9n_2.$$

De modo que n_1 e n_2 são primos entre si.

$$\begin{aligned} 9n_1 + 9n_2 &= 63 \\ n_1 + n_2 &= 7 \end{aligned}$$

Logo os possíveis valores para n_1 e n_2 são os seguintes:

$$\begin{aligned} n_1 = 1 \quad &\text{e} \quad n_2 = 6, \\ n_1 = 2 \quad &\text{e} \quad n_2 = 5, \\ n_1 = 3 \quad &\text{e} \quad n_2 = 4. \end{aligned}$$

Portanto, obtemos os seguintes valores para os inteiros a e b, que satisfazem o enunciado:

$$a = 9, \qquad b = 54, \qquad a = 18, \qquad b = 45, \qquad a = 27 \qquad \text{e} \qquad b = 36$$

Exemplo 4.8. Vamos encontrar os inteiros positivos a e b de modo que:

$$ab = 756 \qquad \text{e} \qquad \text{mdc}(a, b) = 6.$$

Solução: Como $\text{mdc}(a, b) = 6$, temos que $6 \mid a$ e $6 \mid b$; assim existem inteiros n_1 e n_2, tal que:

$$a = 6n_1 \qquad \text{e} \qquad b = 6n_2.$$

De modo que n_1 e n_2 são primos entre si.

$$\begin{aligned} 6n_1 6n_2 &= 756 \\ n_1 n_2 &= 21 \end{aligned}$$

Logo os possíveis valores para n_1 e n_2 são os seguintes:

$$\begin{aligned} n_1 = 1 \quad \text{e} \quad n_2 = 21, \\ n_1 = 3 \quad \text{e} \quad n_2 = 7. \end{aligned}$$

Portanto, obtemos os seguintes valores para os inteiros a e b, que satisfazem o enunciado:

$$a = 6, \qquad b = 126, \qquad a = 18 \qquad \text{e} \qquad b = 42.$$

4.3 Números Primos

Definição: Um número inteiro positivo $p > 1$ que possui apenas dois divisores positivos p e 1 é dito um *número primo* ou apenas primo. Caso contrário, dizemos que p é *composto.*

Assim, por exemplo os inteiros positivos 2, 3, 5, 7 e 11 são todos primos, enquanto os inteiros positivos 4,6,8,10 e 12 são todos compostos.

Já o inteiro positivo 1 não é primo e nem composto, assim sendo, se a é um inteiro positivo qualquer, então a é primo, ou a é composto ou $a = 1$.

Notamos que o número 2 é o único inteiro positivo par que é *primo*.

Teorema 4.4. Seja $a \in \mathbb{Z}$ e p primo, se $p \nmid a$, então a e p são primos entre si.

Demonstração: Seja $d = \text{mdc}(a, p)$. Então $d \mid a$ e $d \mid p$. De $d \mid p$ temos que $d = 1$ ou $d = p$, como p é primo, desse modo a segunda igualdade é impossível, visto que $p \nmid a$, segue que $d = 1$, ou seja, $\text{mdc}(a, p) = 1$.

Portanto, a e p são primos entre si. ■

Corolário 1. Se p é primo tal que $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Demonstração: Suponha que

$$\begin{aligned} p \nmid a \quad &\Longrightarrow \quad \text{mdc}(a,p) = 1 \\ &\overset{\exists\, m,n \in \mathbb{Z}}{\Longrightarrow} \quad am + np = 1 \\ &\overset{x\, b}{\Longrightarrow} \quad abm + nbp = b \end{aligned}$$

Por hipótese $p \mid ab$, então existe $k \in \mathbb{Z}; ab = kp$, logo

$$\begin{aligned} &\Longrightarrow \quad kpm + nbp = 1 \\ &\Longrightarrow \quad p(km + nb) = b \\ &\Longrightarrow \quad pt = b;\ t \in \mathbb{Z};\ t = km + nb \\ &\Longrightarrow \quad p \mid b. \end{aligned}$$

Portanto, $p \mid b$ ■

Corolário 2. Se p é primo tal que $p \mid a_1 a_2 \cdots an$, então existe um índice s, com $1 \leq s \leq n$, tal que $p \mid a_s$.

Demonstração: Utilizando a indução matemática sobre n, teremos que a proposição é verdadeira para $n = 1$, e para $n = 2$ pelo corolário 1 . Suponhamos por hipótese que $n > 2$ e que, se p divide um produto com menos de n fatores, então p divide pelo menos um dos fatores.

Pelo corolário 1 , se $p \mid a_1 a_2 \cdots an$, então

$$p \mid a_n \qquad \text{ou} \qquad p \mid a_1 a_2 \cdots a_{n-1}$$

Se $p \mid a_n$, a proposição estará demonstrada, porém se $p \mid a_1 a_2 \cdots a_{n-1}$, teremos pela hipótese de indução que $p \mid a_s$, com $1 \leq s \leq n-1$. assim em qualquer dos dois casos, p divide um dos inteiros $a_1 a_2 \cdots a_n$. ■

Corolário 3. Se os inteiros $p, a_1, a_2, \cdots, a_n$ são todos primos e se $p \mid a_1 a_2 \cdots a_n$, então existe um índice s, com $1 \leq s \leq n$, tal que $p = a_s$.

Demonstração: Pelo corolário 2 existe um índice s, com $1 \leq s \leq n$, tal que $p \mid a_s$, e como os únicos divisores positivos de a_s são 1 e a_s, visto que a_s é primo, logo $p = 1$ ou $p = a_s$. No entanto, $p > 1$, já que p é primo. Portanto, $p = a_s$. ■

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

Demonstração: Se n é um número primo não há nada a ser demonstrado. Suponhamos então que n seja composto. Consideremos p_1 ($p_1 > 1$), o menor dos divisores positivos de n. O número p_1 deve ser primo, pois caso contrário, existiria p, $1 < p < p_1$ com $p \mid n$, o que é uma contradição à escolha de p_1. Logo, $n = p_1 n_1$.

Se n_1 for primo, então a demonstração está completa. Caso contrário, podemos tomar p_2 como o menor fator de n_1. Analogamente, ao argumento anterior, p_2 deve ser primo e podemos escrever $n = p_1 p_2 n_2$.

Repetindo este procedimento, obtemos uma sequência decrescente de inteiros positivos $n_1, n_2, \ldots, n_r$. Como todos eles são maiores do que 1, este processo deve terminar. Como os primos na sequência $p_1, p_2, \ldots, p_k$ não são necessariamente distintos, n terá, em geral, a seguinte forma:

$$n = p^{m_1} p^{m_2} \ldots p_k^{m_k}.$$

Para prova a unicidade, usaremos indução sobre n. Para $n = 2$, a afirmação é verdadeira. Suponhamos então, que a afirmação se verifica para todos os inteiros maiores do que 1 e menores do que n. Vamos provar que ela é verdadeira para n.

De fato, se n é primo, não há nada para demonstrar. Suponhamos, portanto, que n seja composto e que tenha duas formas distintas de fatoração, isto é,

$$n = p_1 p_2 \ldots p_s = q_1 q_2 \ldots q_r.$$

Vamos provar que $s = r$ e que cada p_i é igual a algum q_j. Como p_1 divide o produto $q_1 q_2 \ldots q_r$, ele divide pelo menos um dos fatores q_j. Sem perda de generalidade podemos supor que $p_1 \mid q_1$. Logo,

$$n/p_1 = p_2 p_3 \ldots p_s = q_2 q_3 \ldots q_r.$$

Como $1 < n/p_1 < n$, a hipótese de indução nos diz que as duas fatorações são idênticas, isto é, $s = r$ e, a menos da ordem, as fatorações $p_1 p_2 \ldots p_s$ e $q_1 q_2 \ldots q_r$ são iguais. ■

Corolário 4. Seja n um inteiro positivo, tal que $n > 1$ sua decomposição como produto de fatores primos é única, a menos da ordem de fatores.

Corolário 5. Todo inteiro positivo n admite uma única decomposição da seguinte forma:

$$n = {p_1}^{s_1} {p_2}^{s_2} \cdots {p_q}^{s_q}$$

onde, para $i = 1, 2, \cdots, q$, cada q_i é um inteiro positivo e cada p_i é um primo, com $p_1 < p_2 < \cdots < p_q$, denominada decomposição canônica do inteiro positivo $n > 1$

Exemplo 4.9. Vamos encontrar a decomposição canônica do inteiro positivo $n = 5040$.

Solução: Temos que $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$

O teorema a seguir tem uma aplicação prática de muita importância, pois nos diz que para sabermos se um determinado número a é primo, basta testarmos a divisibilidade apenas pelos primos $\leq \sqrt{a}$.

Teorema 4.6. Se a não é primo, então a possui, necessariamente, um fator primo menor do que ou igual a $\sqrt{a}$.

Demonstração: Sendo a composto então $a = a_1 \cdot a_2$ onde $1 < a_1 < a$, e $1 < a_2 < a$. Sem perda de generalidade vamos supor que $a_1 \leq a_2$. Assim a_1 tem que ser $\leq \sqrt{a}$, pois caso contrário, teríamos $a = a_1 \cdot a_2 > \sqrt{a} \cdot \sqrt{a} = a$ no qual teríamos um contradição. Assim, pelo Teorema 4.5 a_1 possui algum fator primo p, no qual deve ser $\leq \sqrt{a}$. Como p é um fator primo de a_1 é também um fator de n, assim a demonstração está completa. ■

4.4 Conjunto dos múltiplos de um inteiro

Dado um inteiro qualquer $a \neq 0$, o conjunto de todos os múltiplos de a é indicado por $M(a)$, ou seja:

$$M(a) = \{x \in \mathbb{Z}\,;\, a \mid x\} = \{a \cdot m\,;\, m \in \mathbb{Z}\}.$$

Assim, por exemplo:

$$\begin{aligned} M(-1) &= M(1) = \mathbb{Z} \\ M(2) &= \{2m\,;\, m \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \pm 6, \cdots\}. \end{aligned}$$

E temos ainda que para todo inteiro $a \neq 0$, $M(a) = M(-a)$.

4.5 Múltiplo comum de dois inteiros

Definição: Sejam a e b dois inteiros diferentes de zero, chama - se *múltiplo comum* de a e b todo inteiro x tal que $a \mid x$ e $b \mid x$.

Dados os inteiros a e b, denominamos $M(a, b)$ o conjunto de todos os múltiplos comuns de a e b. Simbolicamente, temos:

$$M(a, b) = \{x \in \mathbb{Z};\ a \mid x \text{ e } b \mid x\},$$

ou seja:

$$M(a, b) = \{x \in \mathbb{Z};\ x \in M(a) \text{ e } x \in M(b)\},$$

logo:

$$M(a, b) = M(a) \cap M(b).$$

Temos que a intersecção é uma operação comutativa, ou seja, $M(a, b) = M(b, a)$.

Notamos que 0 é um múltiplo comum de a e b, no qual temos que $0 \in M(a, b)$.

E os produtos ab e $-(ab)$ também são múltiplos de a e b.

Exemplo 4.10. Sejam os inteiros $a = 6$ e $b = -8$, quais os múltiplos comuns de a e b?

Solução:

$$\begin{aligned} M(6) &= \{6n; n \in \mathbb{Z}\} = \{0, \pm 6, \pm 12, \pm 18, \pm 24, \pm 30, \pm 36, \pm 42, \pm 48, \cdots\} \\ M(-8) &= \{-8n; n \in \mathbb{Z}\} = \{0, \pm 8, \pm 16, \pm 24, \pm 32, \pm 40, \pm 48, \pm 56, \cdots\}. \end{aligned}$$

Portanto:

$$M(6,-8) = M(6) \cap M(-8) = \{0, \pm 24, \pm 48, \cdots\}.$$

4.6 Mínimo Múltiplo Comum

Definição: Sejam a e b inteiros não - nulos. Diremos que um inteiro positivo $m\,(m > 0)$ é o *mínimo múltiplo comum (mmc)* de a e b se satisfaz às seguintes condições

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

(ii) se $a \mid c$ e $b \mid c$, com $c > 0$, então $m \leq c$.

Notemos que pela condição (i), m é um múltiplo comum de a e b, e pela condição (ii), m é o menor dentre todos os múltiplos comuns positivos de a e b.

Indicaremos mmc(a, b) como mínimo múltiplo comum de a e b.

As proposições 4.5 , 4.6 e 4.7 abaixo pode ser encontrado, por exemplo, em [5].

Proposição 4.5. Sejam a e b inteiros não nulos. Então

(i) mmc$(a, b) \geq max\{|a|, |b|\}$;

(ii) mmc(a, b) é único,

(iii) mmc$(a, b) =$ mmc(b, a),

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

Temos uma outra caracterização do mínimo múltiplo comum, no qual é utilizado em outros textos como definição, como enunciaremos abaixo.

Proposição 4.6. Sejam a e b inteiros não nulos. O inteiro m é o mínimo múltiplo comum de a e b se, e somente se, satisfaz:

(i) $m > 0$;

(ii) $a \mid m$ e $b \mid m$;

(iii) se $c \in \mathbb{Z}$ for tal que $a \mid c$ e $b \mid c$, então $m \mid c$.

Aprendemos no ensino básico que o mínimo múltiplo comum de dois números inteiros positivos a e b é o número que obtemos ao se tomar o produto de todos os fatores primos comuns de a e b, onde cada um desses fatores sendo tomado com o maior dos expoentes que aparece nas decomposições de a e b. Sendo assim faremos a demonstração desse resultado, para isso simplificaremos a notação utilizada, no qual escreveremos as decomposições de a e b com exatamente os mesmos fatores primos, admitindo assim a existência de expoentes nulos.

Assim por exemplo,

$$\begin{aligned} 14 &= 2 \cdot 3^0 \cdot 5^0 \cdot 7 \\ 21 &= 2^0 \cdot 3 \cdot 5^0 \cdot 7 \end{aligned}$$

Proposição 4.7. Sejam a e b inteiros positivos, com decomposições em fatores primos, ou seja,

$$\begin{aligned} a &= p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} \\ b &= p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}, \end{aligned}$$

em que cada fator p_i é um número primo distinto, $r_i \geq 0$ e $s_i \geq 0$ (para $i = 1, 2, \cdots, k$). Então

$$mmc(a, b) = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k},$$

em que $t_i = max\{r_i, s_i\}$.

4.7 Relação entre MDC e MMC

Teorema 4.7. Sejam a e b dois inteiros não-nulos, então $\text{mdc}(a, b) \cdot \text{mmc}(a, b) = ab$.

Demonstração: Seja $d = \text{mdc}(a, b)$ e $m = \text{mmc}(a, b)$. Como $a \mid a(b/d)$ e $b \mid b(a/d)$, assim ab/d é um *múltiplo comum de a e b.* Logo, existe um inteiro positivo k tal que

$$ab/d = m; k \in \mathbb{N}$$

o que implica

$$a/d = (m/b)k \qquad \text{e} \qquad b/d = (m/a)k$$

isto é, k é um divisor comum dos inteiros a/d e b/d. Porém, a/d e b/d são primos entre si, de modo que $k = 1$. Assim sendo, temos

$$ab/d = m \qquad \text{ou} \qquad ab = dm$$

ou seja

$$ab = \text{mdc}(a, b) \cdot \text{mmc}(a, b)$$ ■

Notamos que a notação acima é importante devido permitir determinar o mmc de dois inteiros quando se conhece o seu mdc, e vice-versa.

Exemplo 4.11. Sejam a e b dois inteiros positivos, tais que $\text{mdc}(a, b) = 5$ e $\text{mmc}(a, b) = 105$. Qual é o valor de b se $a = 35$?

Solução: Como $ab = \text{mdc}(a, b) \cdot \text{mmc}(a, b)$, então

$$\begin{aligned} 35 \cdot b &= 5 \cdot 105 \\ b &= 15 \end{aligned}$$

Portanto, temos que $b = 15$.

Exemplo 4.12. Sejam a e b dois inteiros positivos, tais que $\text{mmc}(a, b) + \text{mdc}(a, b) = a + b$ então prove que um dos números a e b é múltiplo do outro.

Solução: Seja $d = \text{mdc}(a, b)$, isto é,

$$a = dk_1 \qquad \text{e} \qquad b = dk_2; \quad k_1 \text{ e } k_2 \text{ inteiros primos entre si.}$$

Porém, temos que:

$$\begin{aligned} \text{mmc}(a, b) \cdot \text{mdc}(a, b) &= ab \\ \text{mmc}(a, b) \cdot d &= d^2 k_1 k_2 \\ \text{mmc}(a, b) &= dk_1 k_2. \end{aligned}$$

Assim,

$$\begin{aligned} \text{mmc}(a, b) + \text{mdc}(a, b) &= a + b \\ dk_1 k_2 + d &= dk_1 + dk_2 \\ k_1 k_2 + 1 &= k_1 + k_2 \\ k_1 k_2 - k_1 - k_2 + 1 &= 0 \\ (k_1 - 1)(k_2 - 1) &= 0 \end{aligned}$$

Desse modo, temos duas opções:

(i) $k_1 = 1 \Longrightarrow a = d \Longrightarrow b = ak_2 \Longrightarrow a \mid b$;

(ii) $k_2 = 1 \Longrightarrow b = d \Longrightarrow a = bk_1 \Longrightarrow b \mid a$

Corolário 6. Para todo par de inteiros positivos a e b, o mmc(a,b) =ab se e somente se o mdc(a,b)=1.

Demonstração: ($\Longrightarrow$) Se o $\text{mmc}(a, b) = ab$, então:

$$\begin{aligned} \text{mdc}(a, b) \cdot \text{mmc}(a, b) &= ab \\ \text{mdc}(a, b) \cdot (ab) &= ab \\ \text{mdc}(a, b) &= 1. \end{aligned}$$

($\Longleftarrow$) Reciprocamente, se o $\text{mdc}(a, b) = 1$, então:

$$\begin{aligned} \text{mdc}(a, b) \cdot \text{mmc}(a, b) &= ab \\ 1 \cdot \text{mmc}(a, b) &= ab \\ \text{mmc}(a, b) &= ab. \end{aligned}$$

■

Capítulo 5

Equações Diofantinas Lineares e Congruências

5.1 Equações Diofantinas Lineares

Uma equação com mais de uma váriavel para a qual deseja se soluções inteiras são chamadas de equações diofantinas, isso em homenagem ao famoso matemático grego Diofantos de Alexandria, que investigou tais equações.

Definição: Uma equação da forma $ax + by = c$, onde a, b e c são inteiros é chamada **equação diofantina linear**.

Todo par de inteiros x_0, y_0 em que $ax_0 + by_0 = c$, chama - se uma *solução inteira ou apenas solução da equação* $ax + by = c$.

Teorema 5.1. A equação diofantina linear $ax + by = c$ tem solução se, e somente se, $d = \text{mdc}(a, b)$ é um divisor de c.

Demonstração: ($\Longrightarrow$) Se (x_0, y_0) é uma solução, então vale a igualdade

$$ax_0 + by_0 = c.$$

Como $d \mid a$ e $d \mid b$, então $d \mid c$, existem inteiros m e n tais que $a = dm$ e $b = dn$, desse modo:

$$c = ax_0 + by_0 = dmx_0 + dny_0 = d(mx_0 + ny_0)$$

E como $mx_0 + ny_0$ é um inteiro, temos que d divide c.

($\Longleftarrow$) Como $d = \text{mdc}(a, b)$, então devido ao Teorema 4.2, podemos determinar m_0, $n_0 \in \mathbb{Z}$ tais que $an_0 + bm_0 = d$. Mas, por hipótese, $d \mid c$ e, portanto, $c = dq$ para algum $q \in \mathbb{Z}$. Consequentemente,

$$c = dq = (an_0 + bm_0)q = a(n_0q) + b(m_0q),$$

o que implica que o par (n_0q, m_0q) é solução da equação considerada. ■

Exemplo 5.1. A equação diofantina $2x + 3y = 10$ tem solução, pois $\text{mdc}(2, 3) = 1$ divide 10. Já a equação diofantina $4x + 8y = 14$ não possui solução, pois o $\text{mdc}(4, 8) = 4$ não divide 14.

Teorema 5.2. Se a equação diofantina $ax + by = c$ tem uma solução (x_0, y_0), então tem infinitas soluções e o conjuntos destas é

$$S = \left\{ \left(x_0 + \frac{b}{d}\, t,\ y_0 - \frac{a}{d}\, t \right); \quad t \in \mathbb{Z} \right\},$$

onde $d = \text{mdc}(a, b)$.

Demonstração: Mostraremos inicialmente que todo par $(x_0 + (b/d)t,\ y_0 - (a/d)t)$ é solução da equação considerada. De fato,

$$a\left(x_0 + \frac{b}{d}\ t \right) + b\left(y_0 - \frac{a}{d}\ t \right) = ax_0 + by_0 + \left(\frac{ab - ba}{d} \right) t = ax_0 + by_0 = c,$$

pois, por hipótese, (x_0, y_0) é solução da equação diofantina.

De outra parte, seja (x', y') uma solução genérica da equação diofantina dada. Então:

$$ax' + by' = c = ax_0 + by_0 \qquad \Longrightarrow \qquad a(x' - x_0) = b(y_0 - y').$$

Mas, como d é divisor de a e b, então existem $r, s \in \mathbb{Z}$, com $\text{mdc}(r, s) = 1$, tais que $a = dr$ e $b = ds$. Assim,

$$dr(x' - x_0) = ds(y_0 - y') \qquad \Longrightarrow \qquad r(x' - x_0) = s(y_0 - y').$$

Da última igualdade, segue que r divide $s(y_0 - y')$. E, como r e s são primos entre si, então r divide $y_0 - y'$, pela Proposição 4.3 (vi). Logo,

$$y_0 - y' = rt,$$

para algum $t \in \mathbb{Z}$. Como $r = a/d$, então

$$y' = y_0 - \frac{a}{d}\, t.$$

Observando-se agora que, em consequência,

$$r(x' - x_0) = s(y_0 - y') = srt,$$

segue que

$$x' = x_0 + \frac{b}{d}\, t.$$

■

Corolário 7. Se a equação diofantina $ax + by = c$ tem uma solução (x_0, y_0), onde $\text{mdc}(a, b) = 1$, então tem infinitas soluções e o conjuntos destas é

$$S = \{(x_0 + bt,\ y_0 - at)\,;\quad t \in \mathbb{Z}\}\,.$$

Exemplo 5.2. Determinar todas as soluções da equação diofantina linear

$$90x + 28y = 22.$$

Solução: Determinaremos, inicialmente, o $\text{mdc}(45, 14)$ pelo algoritmo de Euclides.

$$\begin{aligned} 90 &= 28 \cdot 3 + 6 \\ 28 &= 6 \cdot 4 + 4 \\ 6 &= 4 \cdot 1 + 2 \\ 4 &= 2 \cdot 2 \end{aligned}$$

Portanto, o $\text{mdc}(90, 28) = 2$ e como $2 \mid 22$, a equação dada tem solução.

$$\begin{aligned} 2 &= 6 - 4 \cdot 1 \\ 4 &= 28 - 6 \cdot 4 \\ 6 &= 90 - 28 \cdot 3 \end{aligned}$$

No qual segue:

$$\begin{aligned} 2 &= 6 - 4 \cdot 1 = 6 - 1 \cdot (28 - 4 \cdot 6) = 6 - 28 + 4 \cdot 6 = \\ &= -28 + 5 \cdot 6 = -28 + 5 \cdot (90 - 28 \cdot 3) = -28 + 5 \cdot 90 - 15 \cdot 28 = \\ &= 90 \cdot 5 + 28 \cdot (-16). \end{aligned}$$

isto é:

$$2 = 90 \cdot 5 + 28 \cdot (-16)$$

Multiplicando ambos os membros desta igualdade por $22/2 = 11$, obtemos:

$$22 = 90 \cdot 55 + 28 \cdot (-176)$$

Logo o par de inteiros $x_0 = 55$ e $y_0 = -176$ é uma solução particular da equação proposta, assim todas as outras soluções são dadas pelas fórmulas :

$$\begin{aligned} x &= 55 + (28/2)t = 55 + 14t \\ y &= -176 - (90/2)t = -176 - 45t; \quad t \in \mathbb{Z}. \end{aligned}$$

5.2 Congruências

Definição: Sejam a e b dois inteiros, dizemos que a é **congruente** a b módulo m ($m > 0$) se $m \mid (a - b)$. Simbolicamente temos que

$$a \equiv b \mod m \iff m \mid (a - b),$$

ou seja,

$$a \equiv b \mod m \iff \exists k \in \mathbb{Z};\ a - b = km.$$

Porém, se $m \nmid (a - b)$ dizemos que a é **incongruente** a b módulo m e escreveremos, nesse caso, $a \not\equiv b \mod m$.

Exemplo 5.3.

$$\begin{aligned} 25 &\equiv 17 \mod 8, \text{ pois } 8 \mid (25 - 17) \\ -21 &\equiv 12 \mod 3, \text{ pois } 3 \mid (-21 - 12) \\ 28 &\not\equiv 15 \mod 5, \text{ pois } 5 \nmid (28 - 15). \end{aligned}$$

Percebe-se que dois inteiros quaisquer são congruentes módulo 1, enquanto que dois inteiros ambos pares ou ambos ímpares são congruentes módulo 2.

Em particular, $a \equiv 0 \mod m$ se e somente se o *módulo m divide a* ($m \mid a$).

Teorema 5.3. Se a, b, c e m são inteiros, $m > 0$, valem as seguintes propriedades:

1. $a \equiv a \mod m$
2. Se $a \equiv b \mod m$, então $b \equiv a \mod m$
3. Se $a \equiv b \mod m$ e $b \equiv c \mod m$, então $a \equiv c \mod m$.

Demonstração: (1) Como $m \mid 0$, então $m \mid (a - a)$, o que implica que $a \equiv a \mod m$.

(2) Se $a \equiv b \mod m$, então $m \mid (a - b)$, logo existe $k \in \mathbb{Z}$ tal que $(a - b) = km$, e daí, segue que $(b - a) = -km$. Portanto, $m \mid (b - a)$ e, consequentemente, $b \equiv a \mod m$.

(3) Como $a \equiv b \mod m$, então existe $k_1 \in \mathbb{Z}$ tal que

$$(a - b) = k_1 m, \tag{5.1}$$

e como $b \equiv c \mod m$, então existe $k_2 \in \mathbb{Z}$ tal que

$$(b - c) = k_2 m \tag{5.2}$$

Somando-se membro a membro as equações 5.1 e 5.2 , obtemos $a - c = (k_1 + k_2)m$, o que acarreta $a \equiv c \mod m$. ■

Teorema 5.4. Se a, b, c e m são inteiros tais que $a \equiv b \mod m$, então

1. $a + c \equiv b + c \mod m$
2. $a - c \equiv b - c \mod m$
3. $ac \equiv bc \mod m$

Demonstração: (1) Como $a \equiv b \mod m$, temos que $a - b = km$ e, portanto, como $a - b = (a + c) - (b + c)$ temos $a + c \equiv b + c \mod m$.

(2) Como $(a - c) - (b - c) = a - b$ e, por hipótese, $a - b = km$ temos que $a - c \equiv b - c \mod m$.

(3) Como $a - b = km$, então $ac - bc = ckm$, de onde obtemos que $m \mid (ac - bc)$ e, portanto, $ac \equiv bc \mod m$. ■

Teorema 5.5. Se a, b, c, d e m são inteiros tais que $a \equiv b \mod m$ e $c \equiv d \mod m$, então

1. $a + c \equiv b + d \mod m$
2. $a - c \equiv b - d \mod m$
3. $ac \equiv bd \mod m$

Demonstração: (1) Como $a \equiv b \mod m$, então existe $r \in \mathbb{Z}$ tal que

$$a - b = rm. \tag{5.3}$$

E como $c \equiv d \mod m$, então existe $s \in \mathbb{Z}$ tal que

$$c - d = sm. \tag{5.4}$$

Somando-se membro a membro as equações (5.3) e (5.4) obtemos

$$(a + c) - (b + d) = (r + s)m,$$

e isto acarreta que

$$a + c \equiv b + d \mod m.$$

(2) De modo análogo, utilizando a hipótese do teorema, e subtraindo-se as equações (5.3) e (5.4) obtemos

$$(a - b) - (c - d) = (a - c) - (b - d) = (r - s)m,$$

o que implica que $a - c \equiv b - d \mod m$.

(3) Multiplicando ambos os membros de $a-b = rm$ por c e ambos os membros de $c-d = sm$ por b, obtemos $ac - bc = crm$ e $bc - bd = bsm$. Somando membro a membro estas últimas igualdades obtemos

$$ac - bc + bc - bd = ac - bd = (cr + bs)m$$

o que implica que $ac \equiv bd \mod m$. ■

Corolário 8. Se a, b, n e m são inteiros com $n > 0$ e $a \equiv b \mod m$, então $a^n \equiv b^n \mod m$.

Demonstração: Para $n = 1$ a proposição é verdadeira, visto que,

$$a^1 \equiv b^1 \mod m.$$

Suponhamos verdadeiro para $n = k$, isto é,

$$a^k = b^k \mod m \tag{5.5}$$

e mostraremos que vale para $n = k + 1$, ou seja,

$$a^{k+1} = b^{k+1} \mod m. \tag{5.6}$$

Temos pelo **Teorema** 5.5 (3) que

$$ac \equiv bd \mod m,$$

assim multiplicando na equação 5.5 pela hipótese

$$a \equiv b \mod m,$$

teremos:

$$\begin{aligned} a^k \cdot a &\equiv b^k \cdot b \mod m \\ a^{k+1} &\equiv b^{k+1} \mod m \end{aligned}$$

isto é, a proposição é verdadeira para inteiro positivo $k + 1$. Logo, a proposição é verdadeira para todo inteiro positivo n. ■

Exemplo 5.4. Qual o resto da divisão de $5^{131} + 7^{131} + 9^{131} + 15^{131}$ por 12?

Solução: Temos que:

$$\begin{aligned} 7 &\equiv -5 \mod 12 \\ 7^{131} &\equiv (-5)^{131} \mod 12 \qquad (5.7) \\ 5^{131} &\equiv 5^{131} \mod 12. \qquad (5.8) \end{aligned}$$

De 5.7 e 5.8 e da Proposição 5.4 1 segue que

$$5^{131} + 7^{131} \equiv 0 \mod 12. \tag{5.9}$$

De modo análogo temos

$$\begin{aligned} 15 &\equiv -9 \mod 12 \\ 15^{131} &\equiv (-9)^{131} \mod 12 \qquad (5.10) \\ 9^{131} &\equiv 9^{131} \mod 12. \qquad (5.11) \end{aligned}$$

De 5.10 e 5.11 e da Proposição 5.4 1 segue que

$$15^{131} + 9^{131} \equiv 0 \mod 12. \tag{5.12}$$

Somando as congruências 5.9 e 5.12, obtemos: $5^{131} + 7^{131} + 9^{131} + 15^{131} \equiv 0 \mod 12$, desse modo temos que o resto da divisão de $5^{131} + 7^{131} + 9^{131} + 15^{131}$ por 12 é igual a zero. ■

Teorema 5.6. Se $ac \equiv bc \mod m$ e se o mdc$(c, m) = d$, então $a \equiv b \mod m/d$.

Demonstração: Se $ac \equiv bc \mod m$, então $ac - bc = (a-b)c = km;\ k \in \mathbb{Z}$.

E se mdc$(c, m) = d$, existem inteiros q e r tais que $c = dq$ e $m = rd$, onde q e r são primos entre si. Logo:

$$(a-b)dq = krd \quad \text{ou} \quad (a-b)q = kr$$

o que implica $r \mid (a-b)q$, como mdc$(q, r) = 1$, teremos pela proposição 4.3 (vi) que $r \mid (a-b)$ e $a \equiv b \mod r$, porém $r = m/d$, logo $a \equiv b \mod m/d$. ■

Corolário 9. Se $ac \equiv bc \mod m$ e se o mdc$(c, m) = 1$, então $a \equiv b \mod m$.

Demonstração: Se $ac \equiv bc \mod m$, então $m \mid (a-b)c$. Como mdc$(m, c) = 1$. temos que $m \mid (a-b)$, isto é, $a \equiv b \mod m$ ■

Corolário 10. Se $ac \equiv bc \mod p$, com p primo, e se $p \nmid c$, então $a \equiv b \mod p$.

Demonstração: Das hipóteses $p \nmid c$ e p é primo, implicam que o mdc$(c, p) = 1$, portanto $a \equiv b \mod p$ ■

Exemplo 5.5. Resolva a congruência $4x \equiv 12 \mod 14$, isto é, encontre todos os inteiros x tais que $4x \equiv 12 \mod 14$.

Demonstração: Observe que

$$\begin{aligned} 4x \equiv 12 \mod 14 &\Leftrightarrow 2x \equiv 6 \mod 7 \quad (\text{pelo Teorema 5.6}) \\ &\Leftrightarrow x \equiv 3 \mod 7 \quad (\text{pelo corolário 9}). \end{aligned}$$

Assim, $4x \equiv 12 \mod 14 \Leftrightarrow x \equiv 3 \mod 7$. ■

Exemplo 5.6. Resolva a congruência $6x \equiv 15 \mod 21$.

Demonstração: Desta vez temos

$$\begin{aligned} 6x \equiv 15 \mod 21 &\Leftrightarrow 2x \equiv 5 \mod 7 \quad (\text{pelo Teorema 5.6}) \\ &\Leftrightarrow 2x \equiv 12 \mod 7 \\ &\quad (\text{usando } 5 \equiv 12 \mod 7 \text{ para obter um número par}) \\ &\Leftrightarrow x \equiv 6 \mod 7 \quad (\text{pelo corolário 9}). \end{aligned}$$

Assim, $6x \equiv 15 \mod 21 \Leftrightarrow x \equiv 6 \mod 7$. ■

Teorema 5.7. Sejam a e b inteiros quaisquer, e sejam m, n, d e k inteiros positivos.

(i) Se $a \equiv b \mod m$ e $d \mid m$, então $a \equiv b \mod d$;

(ii) se $a \equiv b \mod n$ e $a \equiv b \mod k$, então $a \equiv b \mod \text{mmc}(n,k)$;

(iii) se $na \equiv nb \mod m$, então $a \equiv b \mod \frac{m}{\text{mdc}(n,m)}$;

(iv) se $na \equiv nb \mod nm$, então $a \equiv b \mod m$.

Capítulo 6

Congruências Lineares e Sistemas de Congruências Lineares

6.1 Congruências Lineares

Definição: Chamamos de **congruência linear** em uma variável a uma congruência da forma $ax \equiv b \mod m$, onde x é uma incógnita.

Em uma congruência linear verificaremos que a mesma poderá ter uma solução, várias soluções ou até mesmo não ter solução. Para isso analisaremos os casos a seguir, e mais ainda a condição para existência de solução, como segue abaixo:

Teorema 6.1. A congruência linear $ax \equiv b \mod m$ tem solução se, e somente se, d divide b, onde $d = \text{mdc}(a, m)$.

Demonstração: ($\Longrightarrow$) Suponhamos que a congruência linear $ax \equiv b \mod m$ tem como solução o inteiro x_0, ou seja, que $ax_0 \equiv b \mod m$. Então, existe um inteiro y_0, de modo que

$$ax_0 - b = my_0 \quad \text{ou} \quad ax_0 - my_0 = b$$

e como $d = \text{mdc}(a, m)$, logo $d \mid a$ e $d \mid m$, desse modo $d \mid (ax_0 - my_0)$ e, portanto, $d \mid b$.

($\Longleftarrow$) Reciprocamente, suponhamos que $d \mid b$, ou seja, existe $k \in \mathbb{Z}$, tal que $b = dk$.

E como $d = \text{mdc}(a, m)$, existem inteiros x_0, y_0, tais que

$$ax_0 + my_0 = d, \tag{6.1}$$

multiplicando ambos os membros da equação 6.1 por k, teremos:

$$\begin{aligned} a(kx_0) &+ m(ky_0) = dk = b \\ a(kx_0) &- b = m(-ky_0) \end{aligned}$$

o que acarreta

$$a(kx_0) \equiv b \mod m.$$

Portanto, o inteiro kx_0 é uma solução da congruência linear

$$ax \equiv b \mod m.$$ ■

Teorema 6.2. Seja $d = \text{mdc}(a, m)$ e suponha que $d \mid b$. Então a congruência linear

$$ax \equiv b \mod m$$

tem precisamente d soluções mutuamente incongruentes módulo m.

Demonstração: Temos que a congruência linear $ax \equiv b \mod m$ é equivalente a equação diofantina $ax - my = b$, onde a mesma tem solução se e somente se $d \mid b$, onde $d = \text{mdc}(a, m)$. E como ja foi visto no Teorema 5.2 se $d \mid b$ e se o par de inteiros (x_0, y_0) é uma solução particular da equação $ax - my = b$, então todas as outras soluções desta equação são dadas pelo conjunto solução:

$$S = \left\{\left(x_0 + \frac{m}{d}\,t,\ y_0 + \frac{a}{d}\,t\right);\quad t \in \mathbb{Z}\right\},$$

Dentre o número infinito de inteiros dados pela primeira dessas fórmulas consideremos apenas aquelas que resultam de atribuir a t os valores $0, 1, 2, 3, \cdots, d-1$, ou seja, os d inteiros:

$$x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\left(\frac{m}{d}\right),\ \cdots,\ x_0 + (d-1)\left(\frac{m}{d}\right).$$

Desse modo mostraremos que estes d inteiros são *mutuamente incongruentes módulo m* e que todos os demais inteiros dados pela fórmula $x_0 + \left(\frac{m}{d}\right)t$ são *congruentes módulo m* a algum desses d inteiros. Com efeito, se fosse

$$x_0 + \left(\frac{m}{d}\right)t_1 \equiv x_0 + \left(\frac{m}{d}\right)t_2 \mod m$$

onde $0 \leq t_1 < t_2 \leq d-1$, assim, teríamos :

$$\left(\frac{m}{d}\right)t_1 \equiv \left(\frac{m}{d}\right)t_2 \mod m.$$

Como o $\text{mdc}\left(\frac{m}{d}, m\right) = \frac{m}{d}$, podemos cancelar o fator comum $\frac{m}{d}$, o que dá a congruência:

$$t_1 \equiv t_2 \mod m$$

o que significa $d \mid (t_2 - t_1)$, o que é um absurdo, já que $0 < t_2 - t_1 < d$.

E mais ainda, qualquer outro inteiro $x_0 + \left(\frac{m}{d}\right)t$ é *congruente módulo m* a algum dos d inteiros enumerados anteriormente. Com efeito, pelo algoritmo da divisão, temos:

$$t = dq + r, \quad \text{onde} \quad 0 \leq r \leq d-1$$

e, portanto:

$$x_0 + \left(\frac{m}{d}\right)t = x_0 + \left(\frac{m}{d}\right)(dq + r) = x_0 + mq + \left(\frac{m}{d}\right)r$$

ou seja;

$$x_0 + \left(\frac{m}{d}\right)t \equiv x_0 + \left(\frac{m}{d}\right)r \mod m$$

onde $x_0 + \left(\frac{m}{d}\right)r$ é um dos d inteiros que foram selecionados. ■

Corolário 11. Seja o mdc$(a, m) = 1$. Então a congruência linear $ax \equiv b \mod m$ tem uma única solução módulo m.

Definição: Dizemos que uma solução x_0 de $ax \equiv b \mod m$ é única módulo m quando qualquer outra solução x_1 for congruente a x_0 módulo m.

Exemplo 6.1. Resolva a congruência linear $3x \equiv 6 \mod 18$.

Solução: Temos que o mdc$(3, 18) = 3$, e como $3 \mid 6$, logo pelo teorema 6.2 a congruência dada tem exatamente 3 soluções mutuamente incongruentes modulo 18.

Como $3 \cdot x \equiv 3 \cdot 2 \mod 3 \cdot 6 \Longrightarrow x \equiv 2 \mod 6$, assim a solução da congruência dada

$$x = 2 + 6t; \quad t = 0, 1, 2.$$

Portanto, x = 2, 8, 14.

Exemplo 6.2. Vamos resolver a seguinte congruência linear $2x \equiv 1 \mod 17$.

Solução: Temos que o mdc$(2, 17) = 1$, assim pelo corolário 11 , a congruência linear tem uma única solução módulo 17.

Como $2 \cdot 9 \equiv 1 \mod 17$, logo $x_0 = 9$, e por conseguinte a solução é dada por

$$x = 9 + \left(\frac{17}{1}\right)t = 9 + 17t,$$

ou seja,

$$x \equiv 9 \mod 17.$$

Exemplo 6.3. Resolva a congruência linear $36x \equiv 8 \mod 102$.

Solução: O mdc$(36, 102) = 6$, e como $6 \nmid 8$, logo pelo teorema 6.1 a congruência linear não tem solução.

Definição: Seja a um inteiro. Chama - se *inverso de a módulo m* um inteiro $\overline{a}$ tal que

$$a\overline{a} \equiv 1 \mod m.$$

Teorema 6.3. Seja o mdc$(a, m) = 1$. Então a tem um único inverso módulo m.

Demonstração: Se o mdc$(a, m) = 1$, então a congruência linear

$$ax \equiv 1 \mod m$$

tem uma única solução $x_0 \mod m$, ou seja,

$$ax_0 \equiv 1 \mod m$$

de modo que o inteiro a tem um *único inverso módulo m*:

$$\overline{a} = x_0.$$ ■

Proposição 6.1. Se p é primo, então o inteiro positivo a é o seu próprio inverso módulo p se, e somente se, $a \equiv 1 \mod p$ ou $a \equiv -1 \mod p$.

Demonstração: ($\Longrightarrow$) Se a é seu próprio inverso, então

$$\begin{aligned} a \cdot a &\equiv 1 \mod p \\ a^2 &\equiv 1 \mod p, \end{aligned}$$

logo $p \mid (a^2 - 1)$, ou seja, $p \mid (a-1) \cdot (a+1)$, como p é primo, $p \mid (a-1)$ ou $p \mid (a+1)$, desse modo, $a \equiv 1 \mod p$ ou $a \equiv -1 \mod p$.

($\Longleftarrow$) Reciprocamente, se $a \equiv 1 \mod p$ ou $a \equiv -1 \mod p$, então $p \mid (a-1)$ ou $p \mid (a+1)$. Portanto, $p \mid (a-1)(a+1)$ o que acarreta $a^2 \equiv 1 \mod p$. ■

6.1.1 Resolução de Equação Diofantina por Congruência

Foi visto anteriormente no Teorema 5.1, que a equação diofantina linear

$$ax + by = c \tag{6.2}$$

tem solução se, e somente se, $d \mid c$, onde $d = \text{mdc}(a, b)$. Desse modo, se o par de inteiros x_0, y_0 é uma solução particular qualquer desta equação, então:

$$ax_0 + by_0 = c \qquad \text{e} \qquad ax_0 - c = -by_0,$$

o que implica

$$ax_0 \equiv c \mod b. \tag{6.3}$$

Portanto, para obter uma solução particular da equação diofantina linear 6.2 , basta determinar uma solução qualquer $x = x_0$ da congruência linear

$$ax \equiv c \mod b. \tag{6.4}$$

e substituir o valor x_0 de x na equação 6.2 para que possamos encontrar o valor correspondente y_0 de y, ou seja,

$$ax_0 + by_0 = c.$$

Porém, também podemos obter uma solução particular da equação diofantina linear 6.2 determinando uma solução qualquer $y = y_0$ da congruência linear:

$$by = c \mod a.$$

Exemplo 6.4. Vamos resolver por congruência a equação diofantina linear:

$$4x + 51y = 9$$

Solução: Como o mdc$(4, 51) = 1$, a equação dada tem solução e , portanto, para obter uma *solução particular* desta equação cumpre determinar uma *solução* qualquer da congruência linear.

$$\begin{aligned} 4x &\equiv 9 \mod 51, \quad \text{que por tentativa teremos como resultado} \\ 4 \cdot 15 &\equiv 9 \mod 51. \end{aligned}$$

Portanto, $x_0 = 15$ e substituindo na equação diofantina teremos $y_0 = -1$. Desse modo, o par de inteiros $(15, -1)$ é uma solução particular da equação diofantina linear $4x + 51y = 9$ são dadas pelas fórmulas:

$$x = 15 + 51t \qquad \text{e} \qquad y = -1 - 4t.$$

Exemplo 6.5. Resolva por congruência a equação diofantina linear:

$$7x + 6y = 9$$

Solução: Como o mdc$(7, 6) = 1$, a equação dada tem solução e , portanto, para obter uma *solução particular* desta equação cumpre determinar uma *solução* qualquer da congruência linear.

$$\begin{aligned} 6y &\equiv 9 \mod 7, \quad \text{como} \quad \text{mdc}(6, 7) = 1, \quad \text{logo} \\ 2y &\equiv 3 \mod 7. \end{aligned}$$

E desse modo uma solução particular da congruência linear é $y_0 = -2$, e substituindo na equação diofantina teremos $x_0 = 3$. Desse modo, o par de inteiros $(3, -2)$ é uma solução particular da equação diofantina linear $7x + 6y = 9$, e todas as outras soluções são dadas pelas fórmulas:

$$x = 3 + 6t \qquad \text{e} \qquad y = -2 - 7t.$$

Definição: Se t e k são dois inteiros com $t \equiv k \mod m$, dizemos que k é um *resíduo* de t módulo m.

Definição: O conjunto dos inteiros $\{r_1, r_2, r_3, \cdots, r_s\}$ é um *sistema completo de resíduos* módulo m se

(i) $r_i \not\equiv r_j \mod m$ para $i \neq j$,

(ii) para todo inteiro n existe um r_i tal que $n = r_i \mod m$.

Exemplo 6.6. O conjunto $\{0, 1, 2, 3, \cdots, m-1\}$ é um sistema completo de resíduos módulo m.

Teorema 6.4 (**Pequeno Teorema de Fermat**). Se p é um primo e se p não divide o inteiro a ($p \nmid a$), então:

$$a^{p-1} \equiv 1 \mod p.$$

Demonstração: Temos que o conjunto $\{0, 1, 2, 3, \cdots, p-1\}$ é um sistema completo de resíduos módulo p. Ou seja, qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado em correspondência biunívoca com um subconjunto de $\{0, 1, 2, 3, \cdots, p-1\}$. Consideraremos os números $a, 2a, 3a, \cdots, (p-1)a$, tal que $\text{mdc}(a, p) = 1$, nenhum destes números ia, $\quad 1 \leq i \leq p-1$ é divisível por p, ou seja, nenhum é congruente a $0 \mod p$.

Quaisquer dois são incongruentes módulo p, visto que $at \equiv ak \mod p$ implica $t \equiv k \mod p$, pois $\text{mdc}(a, p) = 1$, e isto só é possível se $t = k$, uma vez que ambos t e k são positivos e menores que p. Temos, portanto, um conjunto de $(p-1)$ elementos incongruentes módulo p e não divisíveis por p. Portanto, cada um deles é congruente a exatamente um dentre os elementos $1, 2, 3, \cdots p-1$. Assim se multiplicarmos estas congruências, membro a membro, teremos:

$$a \cdot (2a) \cdot (3a) \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \mod p,$$

ou seja,

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \mod p$$

e como p é primo e p não divide $(p-1)!$, podemos cancelar o fator comum $(p-1)!$, o que nos dá a congruência:

$$a^{p-1} \equiv 1 \mod p,$$

o que conclui a demonstração. ■

Corolário 12. Se p é um primo, então $a^p \equiv a \mod p$, qualquer que seja o inteiro a.

Demonstração: Temos dois casos a analisar, são eles:

(i) Se $p \mid a$, então:

$$a \equiv 0 \mod p \quad \text{e} \quad a^p \equiv 0 \mod p,$$

o que implica:

$$a^p \equiv a \mod p.$$

(ii) Se $p \nmid a$, então pelo teorema 6.4

$$\begin{aligned} a^{p-1} &\equiv 1 \mod p, \quad \text{e portanto:} \\ a \cdot a^{p-1} &\equiv a \cdot 1 \mod p \\ a^p &\equiv a \mod p. \end{aligned}$$

Assim, em ambos os casos, $a^p \equiv a \mod p$. ■

Exemplo 6.7 (**PROFMAT-MA14-2011).** Ache o resto da divisão por 17 do número

$$S = 1^{16} + 2^{16} + 3^{16} + \cdots + 85^{16}.$$

Solução: Como 17 é primo, assim pelo Pequeno Teorema de Fermat, teremos:

$$\begin{aligned} a^{16} &\equiv 1, \quad \text{se 17 não divide } a, \\ a^{16} &\equiv 0, \quad \text{se 17 divide } a. \end{aligned}$$

E como $85 = 17 \cdot 5$, temos que de 1 a 85 existem 5 múltiplos de 17, desse modo retirando esses múltiplos, obteremos 85-5 = 80 que não são múltiplos de 17 (ou seja, primos com 17), logo:

$$S = 80 \cdot 1 \mod 17 \equiv 12 \mod 17.$$

Portanto, o resto da divisão de S por 17 é 12.

Exemplo 6.8 (**PROFMAT-MA14-2012).** Ache o resto da divisão de $1^5 + 2^5 + \cdots + 183^5$ por 5.

Solução: Seja $S = 1^5 + 2^5 + \cdots + 183^5$, assim pelo Pequeno Teorema de Fermat, temos que

$$\begin{gathered} a^5 \equiv a \mod p; \quad \text{p = 5 é primo, logo} \\ 1^5 + 2^5 + \cdots + 183^5 \equiv (1 + 2 + \cdots + 183) \mod 5. \end{gathered}$$

Porém, $1+2+3+\cdots+183$ é uma soma dos 183 primeiros termos de uma progressão aritmética, onde o primeiro é igual a 1 e o último termo 183, desse modo

$$1 + 2 + 3 + \cdots + 183 = \frac{184 \cdot 183}{2} = 92 \cdot 183$$

e

$$\begin{aligned} 92 &\equiv 2 \mod 5 \\ 183 &\equiv 3 \mod 5, \end{aligned}$$

logo

$$\begin{aligned} 1^5 + 2^5 + \cdots + 183^5 &\equiv 92 \cdot 183 \mod 5 \\ &\equiv 2 \cdot 3 \mod 5 \\ &\equiv 6 \mod 5 \\ &\equiv 1 \mod 5. \end{aligned}$$

Portanto, o resto da divisão de S por 5 é 1.

Exemplo 6.9. Encontre o resto da divisão de 8^{900} por 29.

Solução: Como 29 é primo, utilizando o Pequeno Teorema de Fermat, temos:

$$\begin{aligned} 8^{28} &\equiv 1 \mod 29 \\ (8^{28})^{32} &\equiv 1^{32} \mod 29 \\ 8^{896} &\equiv 1 \mod 29. \end{aligned} \tag{6.5}$$

E temos que:

$$\begin{aligned} 8^2 &\equiv 6 \mod 29 \\ (8^2)^2 &\equiv (6)^2 \mod 29 \\ 8^4 &\equiv 36 \mod 29 \\ 8^4 &\equiv 7 \mod 29. \end{aligned} \tag{6.6}$$

Da congruência 6.5 e 6.6 e utilizando o **Teorema** 5.5 (3) temos que

$$\begin{aligned} 8^{896} \cdot 8^4 &\equiv 1 \cdot 7 \mod 29 \\ 8^{900} &\equiv 7 \mod 29. \end{aligned}$$

Portanto, o resto da divisão de 8^{900} por 29 é 7.

6.2 Sistemas de Congruências Lineares

Na solução de sistemas de congruências lineares surgem algumas dificuldades. Uma delas é que um sistema de duas ou mais congruências lineares pode não ter solução, embora cada uma das congruências do sistema isoladamente tenha solução. Assim, por exemplo, não existe nenhum inteiro x que verifique simultaneamente as congruências lineares:

$$x \equiv 2 \mod 3 \qquad \text{e} \qquad x \equiv 0 \mod 6,$$

mesmo que cada uma delas, isoladamente, tenha solução.

Outro caso que pode surgir é aquele em que uma das congruências não tenha solução e, quando isso acontecer, o sistema de congruências também não terá solução.

6.3 Teorema Chinês dos Restos

Na antiguidade, os generais chineses costumavam contar suas tropas perdidas após a guerra da seguinte forma: ordenavam que as tropas formassem várias colunas com um determinado tamanho e depois contavam quantas sobravam, e faziam isto para vários tamanhos diferentes.

Por exemplo, um general chinês possuía 2000 soldados para uma batalha. Após o confronto ele precisou verificar suas baixas. Assim alinhou os soldados de 7 em 7 e sobraram 5. Quando alinhou de 9 em 9 sobraram 4. E quando alinhou de 10 em 10 sobrou apenas 1. Quantos soldados haviam na formatura, sabendo que há mais de 1500 indivíduos na formatura?

Para resolver este problema, é necessário saber lidar com congruências. Além disso, vamos utilizar uma poderosa arma em Teoria dos Números, chamada de Teorema Chinês dos Restos. De fato, o problema apresentado acima é uma aplicação direta deste teorema.

Para isso, temos que saber interpretar o problema, pois quando o general alinha seus soldados, formando colunas de tamanho n, ele está realizando uma divisão do número de soldados por n, e depois verificando seu resto.

Observe que, na prática, contar o resto é muito mais fácil que contar o número total, ou o quociente. Aliás, quem conhece um pouco de Teoria dos Números, sabe que raramente estamos interessados no quociente, o resto é o que importa.

Teorema 6.5 (**Teorema Chinês dos Restos).** Sejam $m_1, m_2, m_3, \cdots, m_r$ inteiros positivos primos entre si dois a dois (i.e. tais que $\text{mdc}(m_i,\ m_j) = 1 \quad \forall \quad i \neq j$). Então o sistema de congruência lineares

$$\begin{cases} x \equiv A_1 \mod m_1 \\ x \equiv A_2 \mod m_2 \\ x \equiv A_3 \mod m_3 \\ \vdots \\ x \equiv A_r \mod m_r \end{cases}$$

tem solução única, $\mod (m_1 m_2 m_3 \cdots m_r)$, onde $A_1,\ A_2,\ A_3,\ \cdots,\ A_r$ são inteiros dados.

A seguir apresentaremos um algoritmo e sua generalização que será utilizada na demonstração do Teorema 6.5 acima.

Iremos montar uma tabela e, para isso, consideraremos o preenchimento da seguinte maneira:

(i) Na 1^a coluna, escreveremos as equações dada no problema;

(ii) Na 2^a coluna, na qual identificaremos por **A** colocaremos os valores dos restos de cada equação, ou seja, número que vem logo após o sinal de congruência;

(iii) Na 3^a coluna, identificaremos por **M**, o produto de todos os m_i com exceção do módulo no qual a linha esta associada. Assim, para cada linha, teremos $\mathbf{M_i} = \frac{\mathbf{M}}{\mathbf{m_i}}$;

(iv) Na 4^a coluna, identificamos por $\overline{\mathbf{M}}$ e escreveremos a classe de equivalência que o $\mathbf{M_i}$ está associado com $\mathbf{m_i}$;

(*v*) Na 5^a coluna, identificaremos por $(\overline{\mathbf{M}})^{-\mathbf{1}}$ a classe inversa de cada elemento da coluna $\overline{\mathbf{M}}$, sempre respeitando o módulo referente a cada linha, ou seja, é o elemento que multiplicado com $\overline{\mathbf{M}}_\mathbf{i}$ deixa resto $\mathbf{1} \mod \mathbf{m_i}$;

(*vi*) Na 6^a coluna, identificamos por $\mathbf{A} \cdot \mathbf{M} \cdot (\overline{\mathbf{M}})^{-\mathbf{1}}$ colocamos o produto dos elementos de cada linha, com exceção do $\overline{\mathbf{M}}$ que o mesmo esta na tabela para poder facilitar encontrar o valor do $(\overline{\mathbf{M}})^{-\mathbf{1}}$.

Assim teremos a tabela como segue:

	A	M	$\overline{M}$	$(\overline{M})^{-1}$	A · M ·$(\overline{M})^{-1}$
$x \equiv A_1 \mod m_1$	A_1	M_1	$\overline{M_1}$	$(\overline{M_1})^{-1}$	$A_1 \cdot M_1 \cdot (\overline{M_1})^{-1}$
$x \equiv A_2 \mod m_2$	A_2	M_2	$\overline{M_2}$	$(\overline{M_2})^{-1}$	$A_2 \cdot M_2 \cdot (\overline{M_2})^{-1}$
$x \equiv A_3 \mod m_3$	A_3	M_3	$\overline{M_3}$	$(\overline{M_3})^{-1}$	$A_3 \cdot M_3 \cdot (\overline{M_3})^{-1}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$x \equiv A_r \mod m_r$	A_r	M_r	$\overline{M_r}$	$(\overline{M_r})^{-1}$	$A_r \cdot M_r \cdot (\overline{M_r})^{-1}$

Desse modo, temos que uma solução do sistema de congruência é dado pelo algoritmo da seguinte maneira:

$$x = A_1 \cdot M_1 \cdot (\overline{M_1})^{-1} + A_2 \cdot M_2 \cdot (\overline{M_2})^{-1} + A_3 \cdot M_3 \cdot (\overline{M_3})^{-1} + \cdots + A_r \cdot M_r \cdot (\overline{M_r})^{-1}.$$

Onde:

$$\begin{aligned} M_1 &= m_2 m_3 \cdots m_r \\ M_2 &= m_1 m_3 \cdots m_r \\ M_3 &= m_1 m_2 \cdots m_r \\ &\vdots \\ M_r &= m_1 m_2 \cdots m_{r-1}. \end{aligned}$$

Demonstração: Primeiramente vamos mostrar que existe solução e que a mesma é da forma:

$$x = A_1 \cdot M_1 \cdot (\overline{M_1})^{-1} + A_2 \cdot M_2 \cdot (\overline{M_2})^{-1} + A_3 \cdot M_3 \cdot (\overline{M_3})^{-1} + \cdots + A_r \cdot M_r \cdot (\overline{M_r})^{-1}.$$

Agora reescreveremos a suposta solução em módulo m_1, ou seja:

$$x \equiv (A_1 \cdot M_1 \cdot (\overline{M_1})^{-1} + A_2 \cdot M_2 \cdot (\overline{M_2})^{-1} + A_3 \cdot M_3 \cdot (\overline{M_3})^{-1} + \cdots + A_r \cdot M_r \cdot (\overline{M_r})^{-1}) \mod m_1.$$

Porém, temos que $M_2 = m_1 \cdot m_3 \cdots m_r$, ou seja, $m_1 \mid (A_2 \cdot M_2 \cdot (\overline{M_2})^{-1})$, com isso concluímos que:

$$A_2 \cdot M_2 \cdot (\overline{M_2})^{-1} \equiv 0 \mod m_1.$$

De maneira análoga:

$$\begin{aligned} m_1 &\mid (A_3 \cdot M_3 \cdot (\overline{M_3})^{-1}) \Longrightarrow A_3 \cdot M_3 \cdot (\overline{M_3})^{-1} \equiv 0 \mod m_1 \\ &\vdots \\ m_1 &\mid (A_r \cdot M_r \cdot (\overline{M_r})^{-1}) \Longrightarrow A_r \cdot M_r \cdot (\overline{M_r})^{-1} \equiv 0 \mod m_1. \end{aligned}$$

Portanto, temos que:

$$x \equiv A_1 \cdot M_1 \cdot (\overline{M_1})^{-1} \mod m_1$$

E como estamos trabalhando com congruências, vamos tomar a liberdade em trocar M_1 pela sua classe de equivalência $\mod m_1$, assim:

$$x \equiv A_1 \cdot M_1 \cdot (\overline{M_1})^{-1} \mod m_1 \equiv A_1 \cdot \overline{M_1} \cdot (\overline{M_1})^{-1} \mod m_1 \equiv A_1 \mod m_1.$$

Mostramos que o modelo dado resolve a primeira equação do sistema de congruências.
De forma análoga, utilizando a ideia anterior teremos:

$$\begin{aligned} x &\equiv A_2 \cdot M_2 \cdot (\overline{M_2})^{-1} \mod m_2 \equiv A_2 \cdot \overline{M_2} \cdot (\overline{M_2})^{-1} \mod m_2 \equiv A_2 \mod m_2 \\ x &\equiv A_3 \cdot M_3 \cdot (\overline{M_3})^{-1} \mod m_3 \equiv A_3 \cdot \overline{M_3} \cdot (\overline{M_3})^{-1} \mod m_3 \equiv A_3 \mod m_3 \\ &\vdots \\ x &\equiv A_r \cdot M_r \cdot (\overline{M_r})^{-1} \mod m_r \equiv A_r \cdot \overline{M_r} \cdot (\overline{M_r})^{-1} \mod m_r \equiv A_r \mod m_r. \end{aligned}$$

Como vimos o sistema de congruência tem solução da forma:

$$x = A_1 \cdot M_1 \cdot (\overline{M_1})^{-1} + A_2 \cdot M_2 \cdot (\overline{M_2})^{-1} + A_3 \cdot M_3 \cdot (\overline{M_3})^{-1} + \cdots + A_r \cdot M_r \cdot (\overline{M_r})^{-1}.$$

Agora mostraremos que a solução é única $\mod (m_1 m_2 m_3 \cdots m_r)$.
Suponhamos que exista uma outra solução $\widetilde{x}$ tal que $\widetilde{x} \not\equiv x$. Pelo fato de $\widetilde{x}$ ser solução do sistema, em particular é solução da primeira equação, desse modo:

$$\widetilde{x} \equiv A_1 \mod m_1 \tag{6.7}$$

$$x \equiv A_1 \mod m_1 \tag{6.8}$$

Subtraindo 6.7 de 6.8 teremos:

$$\widetilde{x} - x \equiv 0 \mod m_1 \quad \Longrightarrow \quad m_1 \mid (\widetilde{x} - x).$$

Analogamente;

$$\begin{aligned} m_2 &\mid (\widetilde{x} - x) \\ m_3 &\mid (\widetilde{x} - x) \\ &\vdots \\ m_r &\mid (\widetilde{x} - x). \end{aligned}$$

Como por hipótese $m_1, m_2, m_3, \cdots, m_r$ são primos entre si dois a dois, pode - se afirmar que:

$$\begin{aligned} (m_1 \cdot m_2 \cdot m_3 \cdots m_r) \mid \widetilde{x} - x \quad &\Longrightarrow \quad \widetilde{x} - x \equiv 0 \mod (m_1 m_2 m_3 \cdots m_r) \\ &\Longrightarrow \quad \widetilde{x} \equiv x \mod (m_1 m_2 m_3 \cdots m_r). \end{aligned}$$ ■

6.3.1 Aplicação do Teorema Chinês dos Restos

Agora estamos aptos a resolver o problema proposto no inicio deste capitulo, pois o mesmo satisfaz a hipótese do Teorema Chinês dos Restos.

Exemplo 6.10. Um general chinês possuía 2000 soldados para uma batalha. Após o confronto ele precisou verificar suas baixas. Assim alinhou os soldados de 7 em 7 e sobraram 5. Quando alinhou de 9 em 9 sobraram 4. E quando alinhou de 10 em 10 sobrou apenas 1. Quantos soldados haviam na formatura, sabendo que há mais de 1500 indivíduos na formatura?

Solução: Seja x a quantidade de soldados que haviam na formatura, tal que $1500 < x < 2000$, e montando o sistema temos:

$$\begin{cases} x \equiv 5 \mod 7 \\ x \equiv 4 \mod 9 \\ x \equiv 1 \mod 10. \end{cases}$$

Como $\text{mdc}(7,9) = \text{mdc}(7,10) = \text{mdc}(9,10) = 1$, usaremos o Teorema Chinês dos Restos para resolvê -lo:

	A	M	$\overline{M}$	$(\overline{M})^{-1}$	$\text{A} \cdot \text{M} \cdot (\overline{M})^{-1}$
$x \equiv 5 \mod 7$	5	90	6	6	2700
$x \equiv 4 \mod 9$	4	70	7	4	1120
$x \equiv 1 \mod 10$	1	63	3	7	441

$$\begin{aligned} x &\equiv (2700 + 1120 + 441) \mod (7 \cdot 9 \cdot 10) \\ x &\equiv 4261 \mod 630. \end{aligned}$$

Porém,

$$4261 \equiv 481 \mod 630.$$

Logo:

$$x \equiv 481 \mod 630 \quad \Longrightarrow \quad x = 630t + 481; \quad t \in \mathbb{Z}.$$

Como $1500 < x < 2000$, teremos somente a solução inteira quando $t = 2$, resultando

$$\begin{aligned} x &= 630 \cdot 2 + 481 \\ x &= 1741. \end{aligned}$$

Portanto, haviam na formatura 1741 soldados.

Exemplo 6.11. Em um cesto, há uma quantidade N de ovos. Se os ovos forem agrupados de 3 em 3, sobram 2. Se os ovos forem agrupados de 4 em 4, sobra 1. Quantos ovos no minimo pode haver no cesto?

Solução: Seja N a quantidade de ovos que há na cesta, assim

$$\begin{cases} N \equiv 2 \mod 3 \\ N \equiv 1 \mod 4 \end{cases}$$

Como $\text{mdc}(3,4) = 1$, usaremos o Teorema Chinês dos Restos para resolvê -lo:

	A	M	$\overline{M}$	$(\overline{M})^{-1}$	A · M ·$(\overline{M})^{-1}$
$N \equiv 2 \mod 3$	2	4	1	4	32
$N \equiv 1 \mod 4$	1	3	3	3	9

$$\begin{aligned} N &\equiv (32 + 9) \mod (3 \cdot 4) \\ N &\equiv 41 \mod 12. \end{aligned}$$

Porém,

$$41 \equiv 5 \mod 12.$$

Logo:

$$N \equiv 5 \mod 12 \implies N = 5t + 12; \quad t \in \mathbb{Z}.$$

Como queremos o menor valor para N, teremos a solução do problema quando $t = 0$, resultando

$$\begin{aligned} N &= 12 \cdot 0 + 5 \\ N &= 5 \end{aligned}$$

Portanto, existem na cesta 5 ovos.

Exemplo 6.12 (**PROFMAT-MA14-2011).** Dispomos de uma quantidade de x reais menor do que 3000. Se distribuirmos essa quantidade entre 11 pessoas, sobra um real, se distribuirmos entre 12 pessoas, sobram dois reais, e se distribuirmos entre 13 pessoas, sobram três reais. De quantos reais dispomos?

Solução: Seja x a quantidade em dinheiro que dispomos, tal que $x < 3000$, logo:

$$\begin{cases} x \equiv 1 \mod 11 \\ x \equiv 2 \mod 12 \\ x \equiv 3 \mod 13. \end{cases}$$

Como $\text{mdc}(11,12) = \text{mdc}(11,13) = \text{mdc}(12,13) = 1$, usaremos o Teorema Chinês dos Restos para resolvê -lo:

	A	M	$\overline{M}$	$(\overline{M})^{-1}$	$\text{A} \cdot \text{M} \cdot (\overline{M})^{-1}$
$x \equiv 1 \mod 11$	1	156	2	6	936
$x \equiv 2 \mod 12$	2	143	11	11	3146
$x \equiv 3 \mod 13$	3	132	2	7	2772

$$\begin{aligned} x &\equiv (936 + 3146 + 2772) \mod (11 \cdot 12 \cdot 13) \\ x &\equiv 6854 \mod 1716. \end{aligned}$$

Porém,

$$6854 \equiv 1706 \mod 1716$$

Logo:

$$x \equiv 1706 \mod 1716 \implies x = 1716t + 1706; \quad t \in \mathbb{Z}.$$

Como $x < 3000$, teremos somente a solução inteira quando $t = 0$, resultando

$$\begin{aligned} x &= 1716 \cdot 0 + 1706 \\ x &= 1706 \end{aligned}$$

Portanto, a quantia que dispomos é 1706 reais.

Exemplo 6.13 (**PROFMAT-MA14-2011).** Quando um macaco sobe uma escada de dois em dois degraus, sobra um degrau, quando sobe de três em três degraus, sobram dois degraus e quando sobe de cinco em cinco degraus, sobram três degraus. Quantos degraus possui a escada, sabendo que o número de degraus está entre 150 e 200?

Solução: Seja x a quantidade de degraus, tal que $150 < \text{x} < 200$, assim

$$\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5. \end{cases}$$

Como $\text{mdc}(2,3) = \text{mdc}(2,5) = \text{mdc}(3,5) = 1$, usaremos o Teorema Chinês dos Restos para resolvê -lo:

	A	M	$\overline{M}$	$(\overline{M})^{-1}$	A · M $\cdot(\overline{M})^{-1}$
$x \equiv 1 \mod 2$	1	15	1	3	45
$x \equiv 2 \mod 3$	2	10	1	4	80
$x \equiv 3 \mod 5$	3	6	1	6	108

$$\begin{aligned} x &\equiv (45 + 80 + 108) \mod (2 \cdot 3 \cdot 5) \\ x &\equiv 233 \mod 30. \end{aligned}$$

Porém,

$$233 \equiv 23 \mod 30$$

Logo:

$$x \equiv 23 \mod 30 \implies x = 30t + 23; \quad t \in \mathbb{Z}.$$

Como $150 < x < 200$, teremos somente a solução inteira quando $t = 5$, resultando

$$\begin{aligned} x &= 30 \cdot 5 + 23 \\ x &= 173 \end{aligned}$$

Portanto, a quantidade de degraus é 173.

Exemplo 6.14 (**PROFMAT-MA14-2014).** Ao formar grupos de trabalho numa turma o professor verificou que, tomando grupos com 3 componentes sobrariam 2 alunos, com 4 componentes sobraria 1 aluno e que conseguia formar grupos com 5 componentes, sem sobras, desde que ele próprio participasse de um dos grupos. Sabendo que a turma tem menos de 50 alunos, quais são as possíveis quantidades de alunos nessa turma?

Solução: Seja x a quantidade de alunos da turma em questão, tal que $x < 50$. E como o professor conseguia formar grupos com 5 alunos sem sobra de componentes, desde que o mesmo estivesse no grupo, desse modo, retiraremos o professor da última equação de congruência, sendo assim montaremos o sistema como segue.

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 1 \mod 4 \\ x \equiv 4 \mod 5. \end{cases}$$

Como $\text{mdc}(3,4) = \text{mdc}(3,5) = \text{mdc}(4,5) = 1$, usaremos o Teorema Chinês dos Restos para resolvê -lo:

	A	M	$\overline{M}$	$(\overline{M})^{-1}$	A · M $\cdot(\overline{M})^{-1}$
$x \equiv 2 \mod 3$	2	20	2	2	80
$x \equiv 1 \mod 4$	1	15	3	3	45
$x \equiv 4 \mod 5$	4	12	2	3	144

$$\begin{aligned} x &\equiv (80+45+144) \mod (3\cdot 4\cdot 5) \\ x &\equiv 269 \mod 60. \end{aligned}$$

Porém,

$$269 \equiv 29 \mod 60$$

Logo:

$$x \equiv 29 \mod 60 \implies x = 60t + 29; \quad t \in \mathbb{Z}.$$

Como $x < 50$, teremos somente a solução inteira quando $t = 0$, resultando

$$\begin{aligned} x &= 60\cdot 0 + 29 \\ x &= 29 \end{aligned}$$

Portanto, a quantidade de alunos na turma é 29.

Exemplo 6.15 (**PROFMAT-MA14-2014).** Dispomos de uma quantia em reais maior que 1000 e menor que 2000. Se distribuirmos essa quantia entre 11 pessoas, sobra 1 real; se distribuirmos entre 10 pessoas, sobram 2 reais e se distribuirmos entre 9 pessoas sobram 4 reais. De quantos reais dispomos?

Solução: Seja x a quantia de dinheiro que dispomos, tal que $1000 < x < 2000$. Assim

$$\begin{cases} x \equiv 1 \mod 11 \\ x \equiv 2 \mod 10 \\ x \equiv 4 \mod 9. \end{cases}$$

Como $\text{mdc}(11,10) = \text{mdc}(11,9) = \text{mdc}(10,11) = 1$, usaremos o Teorema Chinês dos Restos para resolvê -lo:

	A	M	$\overline{M}$	$(\overline{M})^{-1}$	$\text{A}\cdot\text{M}\cdot(\overline{M})^{-1}$
$x \equiv 1 \mod 11$	1	90	2	6	540
$x \equiv 2 \mod 10$	2	99	9	9	1782
$x \equiv 4 \mod 9$	4	110	2	5	2200

$$\begin{aligned} x &\equiv (540+1782+2200) \mod (11\cdot 10\cdot 9) \\ x &\equiv 4522 \mod 990. \end{aligned}$$

Porém,

$$4522 \equiv 562 \mod 990$$

Logo:

$$x \equiv 562 \mod 990 \implies x = 990t + 562; \quad t \in \mathbb{Z}.$$

Como $1000 < x < 2000$, teremos somente a solução inteira quando $t = 1$, resultando

$$\begin{aligned} x &= 990 \cdot 1 + 562 \\ x &= 1552 \end{aligned}$$

Portanto, a quantia que dispomos é de 1552 reais.

Exemplo 6.16 (**ENQ-2014.2).** Em uma cesta contendo ovos, na contagem de dois em dois, de três em três, de quatro em quatro e de cinco em cinco, sobram 1,2,3 e 4 ovos, respectivamente. Qual é a menor quantidade de ovos que a cesta pode ter?

Solução: Seja x a quantidade de ovos existente na cesta, logo:

$$\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 2 \mod 3 \\ x \equiv 3 \mod 4 \\ x \equiv 4 \mod 5. \end{cases}$$

Como $\text{mdc}(2,4) = 2$, assim não teremos como usar o Teorema Chinês dos Restos envolvendo as quatro congruências, porém o $\text{mdc}(3,4) = \text{mdc}(3,5) = \text{mdc}(4,5) = 1$. Assim,

$$x \equiv 1 \mod 2 \implies x = 2a + 1; \quad a \in \mathbb{Z}$$

E substituindo o valor de x na congruência

$$\begin{aligned} x &\equiv 3 \mod 4 \\ 2a + 1 &\equiv 3 \mod 4 \\ 2a &\equiv 2 \mod 4 \\ a &\equiv 1 \mod 2 \\ a &= 2b + 1; \quad b \in \mathbb{Z} \end{aligned}$$

Substituindo o valor de a em

$$\begin{aligned} x &= 2a + 1, \quad \text{obteremos} \\ x &= 2(2b + 1) + 1 \\ x &= 4b + 3 \\ x &\equiv 3 \mod 4 \end{aligned}$$

Portanto todas as soluções de

$$\begin{aligned} x &\equiv 3 \mod 4, \quad \text{também é solução da congruência} \\ x &\equiv 1 \mod 2 \end{aligned}$$

Logo, resolveremos o seguinte sistema de congruência pelo Teorema Chinês dos Restos

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 4 \\ x \equiv 4 \mod 5. \end{cases}$$

	A	M	$\overline{M}$	$(\overline{M})^{-1}$	A · M ·$(\overline{M})^{-1}$
$x \equiv 2 \mod 3$	2	20	2	2	80
$x \equiv 3 \mod 4$	3	15	3	3	135
$x \equiv 4 \mod 5$	4	12	2	3	144

$$\begin{aligned} x &\equiv (80 + 135 + 144) \mod (3 \cdot 4 \cdot 5) \\ x &\equiv 359 \mod 60. \end{aligned}$$

Porém,

$$359 \equiv 59 \mod 60$$

Logo:

$$x \equiv 59 \mod 60 \implies x = 60t + 59; \quad t \in \mathbb{Z}.$$

Como estamos interessado no menor valor de x, assim teremos somente a solução inteira quando $t = 0$, resultando

$$\begin{aligned} x &= 60 \cdot 0 + 59 \\ x &= 59 \end{aligned}$$

Portanto, a menor quantidade de ovos que a cesta pode ter é 59.

Exemplo 6.17. Ache todos os números inteiros que deixam restos 2, 3 e 4 quando divididos por 3, 4 e 5, respectivamente.

Solução: Seja x o número que satisfaz a hipótese do problema, desse modo,

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 4 \\ x \equiv 4 \mod 5. \end{cases}$$

Como $\text{mdc}(3,4) = \text{mdc}(3,5) = \text{mdc}(4,5) = 1$, usaremos o Teorema Chinês dos Restos para resolvê -lo:

	A	M	$\overline{M}$	$(\overline{M})^{-1}$	A · M ·$(\overline{M})^{-1}$
$x \equiv 2 \mod 3$	2	20	2	2	80
$x \equiv 3 \mod 4$	3	15	3	3	135
$x \equiv 4 \mod 5$	4	12	2	3	144

$$\begin{aligned} x &\equiv (80 + 135 + 144) \mod (3 \cdot 4 \cdot 5) \\ x &\equiv 359 \mod 60. \end{aligned}$$

Porém,

$$359 \equiv 59 \mod 60$$

Logo:

$$x \equiv 59 \mod 60 \implies x = 60t + 59; \quad t \in \mathbb{Z}.$$

Portanto, temos que $x = 60t + 59 \quad \forall \quad t \in \mathbb{Z}$.

Exemplo 6.18. Ache o menor número natural que deixa restos 1, 3 e 5 quando divididos por 5, 7 e 9, respectivamente.

Solução: Seja x o menor número natural que satisfaça o enunciado da questão, assim:

$$\begin{cases} x \equiv 1 \mod 5 \\ x \equiv 3 \mod 7 \\ x \equiv 5 \mod 9. \end{cases}$$

Como $\text{mdc}(5,7) = \text{mdc}(5,9) = \text{mdc}(7,9) = 1$, usaremos o Teorema Chinês dos Restos para resolvê -lo:

	A	M	$\overline{M}$	$(\overline{M})^{-1}$	A · M $\cdot(\overline{M})^{-1}$
$x \equiv 1 \mod 5$	1	63	3	2	126
$x \equiv 3 \mod 7$	3	45	3	5	675
$x \equiv 5 \mod 9$	5	35	8	8	1400

$$\begin{aligned} x &\equiv (126 + 675 + 1400) \mod (5 \cdot 7 \cdot 9) \\ x &\equiv 2201 \mod 315. \end{aligned}$$

Porém,

$$2201 \equiv 311 \mod 315$$

Logo:

$$x \equiv 311 \mod 315 \implies x = 315t + 311; \quad t \in \mathbb{Z}.$$

Como queremos o menor número natural, logo para t = 0, teremos

$$\begin{aligned} x &= 315 \cdot 0 + 311 \\ x &= 311 \end{aligned}$$

Portanto, o menor número natural que satisfaz o problema é 311.

Observação: Para os interessados verificarem o seu grau de entendimento do assunto, podem consultar o seguinte site:

`http://matematica.obmep.org.br/index.php/modulo/ver?modulo=72&tipo=5`

Nele poderão ser encontrados exemplos de diferentes instâncias do problema chinês dos restos.

Capítulo 7

Considerações Finais

Ao longo desse Trabalho de Conclusão de Curso foi feito um estudo do Problema Chinês dos Restos. Para este fim, foi feita uma pesquisa bibliográfica dos assuntos que são necessários para a demonstração do Teorema relativo ao tema em questão. Além disso, após a demonstração formal desse resultado, apresentamos uma série de exemplos que servem de ilustração de sua aplicação.

A prova do Teorema Chinês dos Restos e suas aplicações foram apresentadas no capítulo 6, sendo ideais para alunos que estão no Ensino Básico e professores que têm interesse no aprofundamento do estudo de problemas que envolvam esse tipo de situação. Para atingir tal objetivo houve necessidade de ressaltar certos conteúdos da Teoria Elementar dos Números, tais como Números Inteiros, Divisão nos Inteiros, MDC, MMC, Números Primos, Equações Diofantinas, Congruências e Sistemas de Congruências Lineares, os quais foram essenciais para o entendimento e compreensão do resultado principal desse trabalho.

Referências Bibliográficas

[1] ALENCAR FILHO, E. A., **Teoria Elementar dos Números.** São Paulo: Livraria Nobel S.A., 1981.

[2] FOMIM, D., GENKIN, S., ITENBERG, I., **Círculos Matemáticos : A Experiência Russa** Tradução: IÓRIO, V. M. Rio de Janeiro: IMPA, 2010.

[3] HEFEZ, A., **Aritmética.** Rio de Janeiro: IMPA, 2013.

[4] SANTOS, J. P. O., **Introdução à Teoria dos Números.** 3 ed. Rio de Janeiro: IMPA, 2006.

[5] VIDIGAL, A., AVRITZER, D., SOARES, E. F., BUENO, H. P., FERREIRA, M. C. C., FARIA, M. C. **Fundamentos de Álgebra.** Belo Horizonte: Editora UFMG, 2005.

[6] <https://en.wikipedia.org/wiki/Chinese_remainder_theorem>

[7] <http://legauss.blogspot.com.br/2009/06/o-general-e-o-teorema-chines-dos-restos.html>. Acesso em: 24 de junho 2016.