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

TEOREMA CHINÊS DOS RESTOS: ENSINO E APLICAÇÕES

Walace da Silva Glória

MANAUS
2019

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

Walace da Silva Glória

TEOREMA CHINÊS DOS RESTOS: ENSINO 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
2019

Ficha Catalográfica

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

Glória, Walace da Silva
G568t Teorema Chinês dos Restos: Ensino e Aplicações / Walace da Silva Glória. 2019
72 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. Números Primos. 3. Congruências. 4. Equações Diofantinas Lineares. I. Oliveira, Nilomar Vieira de II. Universidade Federal do Amazonas III. Título

WALACE DA SILVA GLÓRIA

TEOREMA CHINÊS DOS RESTOS: ENSINO 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 29 de agosto de 2019.

WALACE DA SILVA GLÓRIA

TEOREMA CHINÊS DOS RESTOS: ENSINO 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 29 de agosto de 2019.

BANCA EXAMINADORA

Prof. Dr. Nilomar Vieira de Oliveira
Presidente

Prof. Dr. Valtemir Martins Cabral
Membro Interno

Profa. Dra. Jeanne Moreira de Sousa
Membro Externo

AGRADECIMENTOS

A Deus que sempre está comigo, me dando saúde, força, coragem e determinação.

A minha família, a minha esposa Francisca Félix Pereira pelo apoio, companheirismo, amor, incentivo, respeito, e principalmente me ajudando em tudo.

Aos meus queridos colegas do Profmat-Am 2017,que caminharam juntos: Alex, Anselmo, Átila, Bruno, Eloy, Everton, Fábio, Franckson, João, Lucas, Marcelo, Manoel, Osmar, Pedro, Thiago, Robervani e Wilson pela motivação, carinho e caminhada em nosso grupo de estudos nos dias normais como nos feriados e finais de semanas incansáveis na Ufam.

A todo corpo docente do PROFMAT pólo UFAM, em especial ao meu orientador Prof. Dr. Nilomar Vieira de Oliveira, pelo apoio, incentivo, profissionalismo e colaboração no desenvolvimento da dissertação.

RESUMO

O foco deste trabalho é o Teorema Chinês dos Restos, seu ensino e algumas aplicações elementares. Nesse sentido, o uso deste teorema e sua aplicação prática no ensino fundamental e médio na educação básica, pode servir de base teórica para futuros alunos e professores que buscam exercícios ou atividades relacionadas ao Teorema Chinês dos Restos. Para conseguir esses objetivos, dos capítulos 2 ao 4 foram abordados assuntos numa revisão bibliográfica com os seguintes tópicos: Os Números Inteiros e suas Propriedades Básicas, Divisibilidade, Máximo Divisor Comum, Mínimo Múltiplo Comum, Números Primos, Equações Diofantinas Lineares e Congruências. No capítulo 5 apresentamos a demonstração do Teorema Chinês dos Restos e vinte e dois exemplos de suas aplicações com a finalidade de melhor aprendizado baseado nas resoluções. Este trabalho busca dar suporte para os professores e alunos que visam aprimorar seus estudos e pesquisas posteriores nesse conteúdo.

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

ABSTRACT

The focus of this work is the Chinese Remains Theorem, its teaching and some elementary applications. In this sense, the use of this theorem and its practical application in elementary and high school in basic education can serve as a theoretical basis for future students and teachers seeking exercises or activities related to the Chinese Theorem of Rest. To achieve these goals, chapters 2 through 4 addressed topics in a literature review with the following topics: Integer Numbers and their Basic Properties, Divisibility, Maximum Common Divisor, Common Minimum, Prime Numbers, Linear Diophantine Equations, and Congruences. In Chapter 5 we present the demonstration of the Chinese Theorem of Remnants and twenty-two examples of its applications for the purpose of better resolution-based learning. This paper seeks to support teachers and students aiming to improve their studies and further research on this content. Enviar feedback Histórico Salvas Comunidade

Keywords: Chinese Remainder Theorem, Primal Numbers, 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.
$\mid$	Divide.
$\nmid$	Não divide.
$\blacksquare$	Indica o fim de uma demonstração.

Sumário

Capítulo 1

Introdução

1.1 Histórico

O surgimento do Teorema Chinês dos Restos ocorreu no livro do matemático chinês Sun Zi Suanjing chamado "Manual de aritmética do Sol"durante os primeiros séculos entre 280 d.C a 483 d.C. O livro se divide em três capítulos, em que o primeiro capítulo contém apenas dois problemas que tratam de métodos para fazer multiplicações e divisões, utilizando palitinhos chineses, já o capítulo dois trata de vinte e oito problemas envolvendo frações, extrações de raiz quadrada, calculo de áreas e volumes, proporções e regra de três simples, e finalmente o capítulo três que contém 36 problemas aritméticos e no problema vigésimo sexto conhecido como problema do mestre Sun, utiliza-se pela primeira vez o Teorema Chinês dos Restos. O chinês Sun-tsu no princípio do século a.C., escreveu num livro intitulado Suan-Ching (Aritmética), abordava num verso chamado tai-yen (grande generalização), o seguinte problema: Achar um número que dividido por 3, 5 e 7 de restos 2,3 e 2, respectivamente. Seu método de resolução tinha como base em determinar números auxiliares 70, 21 e 15 e observar que 233 = $2 \cdot 70$ + $3 \cdot 21$ + $2 \cdot 15$ é solução. Dividindo esse resultado por $3 \cdot 5 \cdot 7$, resultava em 23 como resto, que é a menor solução positiva do problema. Em 1852 esses resultados tornaram-se conhecidos na Europa, após algumas divergências sobre a validade do método de trabalho, mas em 1874 essa técnica era essencialmente a mesma contida na *Disquisitiones Arithmeticae*, de K. F. Gauss. [1],[2], [3], [7]

O pitagórico Nichomanus por volta do ano 100 a.C., tendo o mesmo problema que Sun-Tsu e encontrou a mesma solução 23.

Na linguagem de congruências, o problema de Sun-Tsu consiste em encontrar um inteiro que seja solução das seguintes equações:

$$\begin{aligned} X &\equiv 2 \mod 3 \\ X &\equiv 3 \mod 5 \\ X &\equiv 2 \mod 7 \end{aligned} \tag{1.1}$$

1.2 Motivação e Métodos do Trabalho

A escolha desse tema é apreciação ao trabalho desenvolvido pelos matemáticos chineses, foram as primeiras civilizações a trabalharem com números, o Teorema Chinês dos Restos ensino e suas aplicações, foi o tema escolhido com a finalidade de colaborar com futuros alunos na graduação e mestrado acadêmico, mas o foco principal é antecipar no ensino fundamental e médio, para os egressos na graduação e mestrado não tenha dificuldades em resolver tais problemas. A maior dificuldade é em encontrar bibliografia, mas o trabalho foi bem elaborado para conhecimentos aos professores e alunos do Ensino Básico como material de apoio. Portanto, esse trabalho poderá agregar-se à bibliografia da olimpíada de matemática, pois trabalhamos com 45 alunos da obmep na rede pública municipal, como futuro desafios em questões bem elaboradas e resolvidas pelos mesmos.

A metodologia utilizada na realização deste trabalho foi a pesquisa bibliográfica. Pesquisamos o conteúdo através de vários autores [[1], [2] ,[3] ,[4] ,[5] , [7] e [8]], organizamos os pre requisitos necessários para a demonstração do Teorema Chinês dos Restos destes e, finalmente, aplicamos vários exemplos de exercícios.

1.3 Estrutura do Trabalho

A seguir, no Capítulo 2, apresentamos os números inteiros e suas propriedades básicas. Assim como alguns assuntos: Divisibilidade, Máximo Divisor Comum, Mínimo Múltiplo Comum e Números Primos.

No Capítulo 3, apresentamos as Equações Diofantinas Lineares para verificação de solução inteira em algumas equações.

No Capítulo 4, apresentamos as congruências lineares. Neste capítulos são especificadas as principais propriedades dos restos de divisão inteira.

No Capítulo 5, apresentamos o Teorema Chinês dos Restos. Abordamos uma variedades de exercícios, buscando o melhor entendimento aos professores e alunos do Ensino Básico.

E finalmente, apresentamos as Considerações finais. Relatando todo percurso percorrido durante o trabalho para chegar ao Teorema Chinês dos Restos Ensino e suas Aplicações, a colaboração e contribuição é dar material de apoio à comunidade acadêmica e para alunos e professores que necessitam de bibliografia acessível para solucionarem futuros problemas

envolvendo o Teorema Chinês dos Restos.

Capítulo 2

Os Números Inteiros

Iniciaremos nossa abordagem com o conjunto dos números inteiros representado pelo simbolo $\mathbb{Z}$.

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

Tendo como finalidade obter o conjunto solução de problemas posteriores, as propriedades básicas de adição e multiplicação serão abordadas de forma axiomática nas quais não haverá necessidades de demonstrá-las.

2.1 Propriedades básicas dos números inteiros

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 $m = n$.

2.2 Indução Matemática

O Princípio de Indução finita matemática é aplicada para provarmos propriedades para todo número natural n, a partir de um $n_0 \in \mathbb{N}$. Inicialmente verificamos que a referida propriedade é válida para n_0. Posteriormente verifica-se um valor qualquer a partir de n_0 de modo a demonstrar que também é válido para o seu consecutivo. Desta maneira a propriedade referida estará provada pelo seguinte motivo: é válido para n_0 e para seu consecutivo $n_0 + 1$, e também para seu consecutivo $n_0 + 2$, e assim consecutivamente para qualquer natural maior ou igual a n_0.[4],[5],[7],[8]

Axioma 2.1. Todo subconjunto $\mathcal{W} \subset \mathbb{N}$; $\mathcal{W} \neq \varnothing$, tem um elemento mínimo, isto é,

$$\text{existe } w_0 \in \mathcal{W} \text{ tal que } w_0 \leq w, \text{ para todo } w \in \mathcal{W}.$$

O Principio da Indução Finita é descrito logo abaixo:

Teorema 2.1. Seja $Q(x)$ uma sentença verdadeira para cada $x \in \mathbb{N}$. Se

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

Então $Q(x)$ é verdadeira para cada $x \in \mathbb{N}$.

Demonstração: Consideremos o conjunto $\mathcal{W} = \{x \in \mathbb{N}; Q(x) \text{ é falso}\}$. Vamos mostrar que $\mathcal{W} = \varnothing$, resultando que $Q(x)$ é verdadeiro para todo $x \in \mathbb{N}$.

Suponhamos que $\mathcal{W} \neq \varnothing$. Como $\mathcal{W}$ é um subconjunto não-vazio dos números naturais, existe $x_0 = \min \mathcal{W}$, pelo Princípio da Boa Ordenação dos números naturais. Devido $Q(1)$ ser verdadeiro, temos $1 \notin \mathcal{W}$, isto é, $x_0 > 1$.

Como x_0 é o menor elemento de $\mathcal{W}$, o número $x_0 - 1 \notin \mathcal{W}$. Assim, $Q(x_0 - 1)$ é verdadeiro, e pela hipótese indutiva, $Q[(x_0 - 1) + 1] = Q(x_0)$ é verdadeiro. Mas, $x_0 \in \mathcal{W}$, pois é o menor elemento de $\mathcal{W}$. Temos uma contradição: $x_0 \in \mathcal{W}$ e $x_0 \notin \mathcal{W}$.

Portanto, $\mathcal{W} = \varnothing$, e com as hipóteses do problema, temos que $Q(x)$ é verdadeiro para todo $x \in \mathbb{N}$ ■

Teorema 2.2. Dado um subconjunto $\mathcal{W}$ do conjunto $\mathbb{N}$ dos inteiros positivos; tal que:
1) $1 \in \mathcal{W}$
2) Para todo inteiro positivo y, se $y + 1 \in \mathcal{W}$ sempre que $1, 2, 3, \ldots, y \in \mathcal{W}$, então $\mathcal{W}$ contém todos os inteiros positivos.

Temos algumas aplicações do Princípio da Indução Finita.

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

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

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

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

Suponhamos que a proposição seja verdadeira para $x = y$, isto é:

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

E mostraremos que vale para $x = y + 1$, ou seja,

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

De fato, da hipótese de indução temos:

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

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

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

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

Exemplo 2.2. Se $a \geq 0$, então

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

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

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

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

Suponhamos que a proposição seja verdadeira para $x = y$, isto é

$$(1+a)^y \geq 1 + ya + \frac{y \cdot (y-1)}{2} a^2 \; ; \quad a \geq 0$$

E mostraremos que vale para $x = y + 1$, ou seja,

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

De fato, da hipótese de indução temos:

$$(1+a)^y \geq 1 + ya + \frac{y(y-1)}{2} a^2.$$

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

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

pois $\dfrac{y(y-1)}{2}\ a^3 \geq 0$.

Assim,

$$(1+a)^y \geq 1 + ya + \frac{y(y-1)}{2} a^2 \Longrightarrow (1+a)^{y+1} \geq 1 + (y+1)a + \frac{(y+1)y}{2}\ a^2.$$

Portanto, $(1+a)^x \geq 1 + xa + \dfrac{x(x-1)}{2} a^2$, para todo $x \in \mathbb{N}$ se $a \geq 0$ ■

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

$$(1+a)^x \geq 1 + xa.$$

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

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

Suponhamos que a proposição seja verdadeira para $x = y$, isto é

$$(1+a)^y \geq 1 + ya.$$

E mostraremos que vale para $x = y + 1$, ou seja,

$$(1 + a)^{y+1} \geq 1 + (y + 1)a.$$

De fato, da hipótese de indução temos:

$$(1 + a)^y \geq 1 + ya.$$

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

$$\begin{aligned}(1 + a)^y(1 + a) = (1 + a)^{y+1} &\geq (1 + ya)(1 + a)\\ &= 1 + (y + 1)a + ya^2\\ &\geq 1 + (y + 1)a,\end{aligned}$$

pois $ya^2 \geq 0$.

Assim,

$$(1 + a)^y \geq 1 + ya \Longrightarrow (1 + a)^{y+1} \geq 1 + (y + 1)a.$$

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

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

$$1 + r + \cdots + r^x = \frac{r^{x+1} - 1}{r - 1}.$$

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

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

Suponhamos que a proposição seja verdadeira para $x = y$, isto é

$$1 + r + \cdots + r^y = \frac{r^{y+1} - 1}{r - 1}.$$

E mostraremos que vale para $x = y + 1$, ou seja,

$$1 + r + \cdots + r^y + r^{y+1} = \frac{r^{(y+1)+1} - 1}{r - 1}.$$

De fato, da hipótese de indução temos:

$$1 + r + \cdots + r^y = \frac{r^{y+1} - 1}{r - 1}.$$

Somando ambos os lados por r^{y+1}, temos

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

Portanto, $1 + r + \cdots + r^x = \dfrac{r^{x+1} - 1}{r - 1}$, sejam quais forem r, $x \in \mathbb{N}$, $r \neq 1$. ■

Exemplo 2.5. Para qualquer $x \in \mathbb{N}$, é afirmado que

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

Demonstração : Para $x = 1$, a afirmação é verdadeira, pois

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

Suponhamos que a proposição seja verdadeira para $x = y$, isto é

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

E mostraremos que vale para $x = y + 1$, ou seja,

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

De fato, da hipótese de indução temos:

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

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

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

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

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

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

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

$$1=1^2.$$

Suponhamos que a proposição seja verdadeira para $x=y$, isto é

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

E mostraremos que vale para $x=y+1$, ou seja,

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

De fato da hipótese de indução temos:

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

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

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

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

2.3 Divisibilidade

Definição: Dados dois números inteiros w e a dizemos que w divide a, escrevendo $w\mid a$, onde w é um divisor de a e que a é um múltiplo de w, se existir $l\in\mathbb{Z}$ com $a=lw$. Cuja negação escreveremos $w\nmid a$. [7][8]

Vejamos alguns exemplos:

Exemplo 2.7.

$$-6 \mid 12, \quad \text{mas} \quad 12 \nmid -6$$

.

Estabelecemos a seguir algumas propriedades da divisibilidade.

Proposição 2.1. *Sejam $w, a, b, c \in \mathbb{Z}$. Temos*

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

(ii) Se $w \mid 1$, então $w = \pm 1$

(iii) Se $w \mid b$ e $a \mid c$, então $w \cdot a \mid b \cdot c$

(iv) Se $w \mid a$ e $a \mid b$, então $w \mid b$

(v) Se $w \mid a$ e $a \mid w$, então $w = \pm a$

(vi) Se $w \mid a$, com $a \neq 0$, então $\mid w \mid \leq \mid a \mid$

(vii) Se $w \mid a$ e $w \mid b$, então $w \mid (an + bq), \forall\, n, q \in \mathbb{Z}$

$(viii)$ $0 \mid w \leftrightarrow w = 0$

Demonstração:

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

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

(iii) Temos que:
$w \mid a \Longrightarrow a = w \cdot q$, com $q \in \mathbb{Z}$
$b \mid c \Longrightarrow c = b \cdot r$, com $r \in \mathbb{Z}$
Desse modo $a \cdot c = (w \cdot b) \cdot qr \Longrightarrow w \cdot b \mid a \cdot c$ ■

(iv) Temos que:

$w \mid a \Longrightarrow a = w \cdot q$; com $q \in \mathbb{Z}$

$a \mid b \Longrightarrow b = a \cdot r$; com $r \in \mathbb{Z}$.

Substituindo $a = wq$ em $b = ar$; temos: $b = w(qr) \Longrightarrow w \mid b$ ■

(v) De $w \mid a \Longrightarrow a = w \cdot q$; $q \in \mathbb{Z}$ e de $a \mid w \Longrightarrow w = ar$; $r \in \mathbb{Z}$.

Portanto $w = a(qr) \Longrightarrow qr = 1 \Longrightarrow q = r = \pm 1 \Longrightarrow w = \pm a$ ■

(vi) Com efeito $w \mid a$, com $a \neq 0$ implica que $a = wq$.

Tomando módulos, temos que $|a| = |w| \cdot |q|$.

Como $a \neq 0$, temos que $|q| \neq 0$, portanto $1 \leq |q|$.

E consequentemente, $|w| \leq |q| \cdot |w| \Longrightarrow |w| \leq |w| \cdot |q| = |a| \Longrightarrow |w| \leq |a|$ ■

(vii) Com efeito $w \mid a \Longrightarrow a = wc$; $c \in \mathbb{Z}$ e de $w \mid b \Longrightarrow b = w \cdot d, d \in \mathbb{Z}$.

Portanto, quaisquer que sejam $n, q \in \mathbb{Z}$

$an + bq = n(wc) + q(wd) = w(cn) + w(dq) = w(cn + dq) \Longrightarrow w \mid (cn + dq)$ ■

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

Proposição 2.2. *Se $r, s, t \in \mathbb{Z}$, tais que $r \mid (s \pm t)$. Então $r \mid s \Longleftrightarrow t \mid t$*

Demonstração: Será demonstrado apenas a seguinte implicação:

Se $r \mid (s + t)$, então $r \mid s \Longleftrightarrow r \mid t$

$(\Longrightarrow)$ Como $r \mid (s + t)$, existe $u \in \mathbb{Z}$, tal que

$$s + t = ru \tag{2.1}$$

Agora se $r \mid s$, logo existe $v \in \mathbb{Z}$, tal que

$$s = rv \tag{2.2}$$

Substituindo (2.2) em (2.1), temos:

$$rv + t = ru \Longrightarrow t = ru - rv \Longrightarrow t = r(u - v).$$

Portanto, $r \mid t$

($\Longleftarrow$) Suponhamos que $r \mid (s+t)$, existe $u \in \mathbb{Z}$, tal que

$$s + t = ru \tag{2.3}$$

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

$$t = rw \tag{2.4}$$

Substituindo a equação (2.4) em (2.3), temos:

$$s + rw = ru \Longrightarrow s = ru - rw \Longrightarrow s = r(u - w).$$

Portanto, $r \mid s$ ■

Proposição 2.3. Se $r, s \in \mathbb{Z}$ e $x \in \mathbb{N}$, então $(r - s) \mid (r^x - s^x)$

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

$$r - s \mid r^1 - s^1.$$

Suponhamos verdadeira para $x = y$, isto é,

$$r - s \mid r^y - s^y.$$

E mostraremos que vale para $x = y + 1$, ou seja,

$$r - s \mid r^{y+1} - s^{y+1}.$$

Temos que

$$r^{y+1} - s^{y+1} = r \cdot r^y - s \cdot s^y, \tag{2.5}$$

e

$$s \cdot r^y - s \cdot r^y = 0. \tag{2.6}$$

Somando (2.6) na equação (2.5), teremos:

$$r \cdot r^y - s \cdot s^y + s \cdot r^y - s \cdot r^y = r^y \cdot (r - s) + s \cdot (r^y - s^y).$$

Como $(r - s) \mid r^y \cdot (r - s)$ e, por hipótese de indução, $(r - s) \mid (r^y - s^y)$.
Decorre da propriedade (vii) , que $(r - s) \mid (r^{y+1} - s^{y+1})$.
Portanto o resultado é verdadeiro para todo $x \in \mathbb{N}$. ■

Proposição 2.4. Se $r, s \in \mathbb{Z}$ e $x \in \mathbb{N} \cup \{0\}$. Então $(r+s) \mid (r^{2x+1} + s^{2x+1})$.

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

$$(r+s) \mid (r^{2\cdot 0+1} + s^{2\cdot 0+1})$$

Suponhamos verdadeiro para $x = y$, isto é,

$$(r+s) \mid (r^{2y+1} + s^{2y+1}).$$

E mostraremos que vale para $x = y+1$, ou seja,

$$(r+s) \mid (r^{2(y+1)+1} + s^{2(y+1)+1}).$$

Temos que

$$r^{2(y+1)+1} + s^{2(y+1)+1} = r^{2y+1}r^2 + s^{2y+1}s^2, \tag{2.7}$$

e

$$s^2 r^{2y+1} - s^2 r^{2y+1} = 0. \tag{2.8}$$

Somando (2.8) na equação (2.7), teremos:

$$r^{2y+1}r^2 + s^{2y+1}s^2 + s^2 r^{2y+1} - s^2 r^{2y+1} = r^{2y+1}(r^2 - s^2) + s^2(r^{2y+1} + s^{2y+1}).$$

Como, $(r+s) \mid (r^2 - s^2)r^{2y+1}$ e por hipótese de indução $(r+s) \mid (r^{2y+1} + s^{2y+1})$.
Decorre da propriedade que $(r+s) \mid (r^{2(y+1)+1} + s^{2(y+1)+1})$.
Portanto vale para todo $x \in \mathbb{N}$. ■

Proposição 2.5. Se $r, s \in \mathbb{Z}$ e $x \in \mathbb{N}$. Então $(r+s) \mid (r^{2x} - s^{2x})$.

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

$$(r+s) \mid (r^{2.1} - s^{2.1}) \Longrightarrow (r+s) \mid (r^2 - s^2).$$

Suponhamos verdadeiro para $x = y$, isto é,

$$(r+s) \mid (r^{2y} - s^{2y}).$$

E mostraremos que vale para $x = y+1$, ou seja,

$$(r+s) \mid (r^{2(y+1)} - s^{2(y+1)})$$

Temos que

$$r^{2(y+1)} - s^{2(y+1)} = r^{2y}r^2 - s^{2y}s^2 \tag{2.9}$$

e

$$r^{2y}s^2 - r^{2y}s^2 = 0. \tag{2.10}$$

Somando (2.10) na equação (2.9), teremos:

$$r^{2y}r^2 - s^{2y}s^2 + r^{2y}s^2 - r^{2y}s^2 = r^{2y}(r^2 - s^2) + s^2(r^{2y} - s^{2y}).$$

Como, $(r+s) \mid r^{2y}(r^2 - s^2)$ e por hipótese de indução $(r+s) \mid (r^{2y} - s^{2y})$.
Decorre da propriedade que $(r+s) \mid (r^{2(y+1)} - s^{2(y+1)})$.
Portanto vale para todo $x \in \mathbb{N}$. ■

Exemplo 2.8. Sejam $r, s \in \mathbb{Z}$.
a) Se $r \neq s$, mostre que, para todo $x \in \mathbb{N}, x \geq 2$, temos

$$\frac{r^x - s^x}{r - s} = r^{x-1} + r^{x-2}s + \cdots + rs^{x-2} + s^{x-1}.$$

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

$$\frac{r^2 - s^2}{r - s} = r^{2-1} + r^{2-2} \cdot s.$$

Suponhamos verdadeiro para $x = y$, ou seja,

$$\frac{r^y - s^y}{r - s} = r^{y-1} + r^{y-2}s + \cdots + rs^{y-2} + s^{y-1}. \tag{2.11}$$

E mostraremos que vale para $x = y + 1$, isto é,

$$\frac{r^{y+1} - s^{y+1}}{r - s} = r^y + r^{y-1}s + \cdots + rs^{y-1} + s^y.$$

Temos que

$$\frac{r^{y+1} - s^{y+1}}{r - s} = \frac{r^y r - s^y s}{r - s}. \tag{2.12}$$

E

$$\frac{r^y s - r^y s}{r - s} = 0. \tag{2.13}$$

Somando (2.13) na equação (2.12) teremos:

$$\frac{r^y r - s^y s + r^y s - r^y s}{r - s} = \frac{r^y(r - s)}{r - s} + \frac{s(r^y - s^y)}{r - s} = r^y + \frac{s(r^y - s^y)}{r - s}. \tag{2.14}$$

Substituindo a hipótese de indução (2.11) na equação (2.14), teremos

$$r^y + \frac{s(r^y - s^y)}{r-s} = r^y + s(r^{y-1} + r^{y-2}s + \cdots + rs^{y-2} + s^{y-1}) = r^y + r^{y-1}s + r^{y-2}s^2 + \cdots + rs^{y-1} + s^y.$$

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

b) Se $r + s \neq 0$, mostre que, para todo $x \in \mathbb{N}$,

$$\frac{r^{2x+1} + s^{2x+1}}{r+s} = r^{2x} - r^{2x-1}s + \cdots - rs^{2x-1} + s^{2x}.$$

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

$$\frac{r^{2.0+1} + s^{2.0+1}}{r+s} = r^{2.0}.$$

Suponhamos verdadeiro para $x = y$, ou seja,

$$\frac{r^{2y+1} + s^{2y+1}}{r+s} = r^{2y} - r^{2y-1}s + \cdots - rs^{2y-1} + s^{2y}. \tag{2.15}$$

E mostraremos que vale para $x = y + 1$, isto é,

$$\frac{r^{2(y+1)+1} + s^{2(y+1)+1}}{r+s} = r^{2(y+1)} - r^{2(y+1)-1}s + \cdots - rs^{2(y+1)-1} + s^{2(y+1)}.$$

Temos que

$$\frac{r^{2(y+1)+1} + s^{2(y+1)+1}}{r+s} = \frac{r^2 r^{2y+1} + s^2 s^{2y+1}}{r+s} \tag{2.16}$$

e

$$\frac{s^2 r^{2y+1} - s^2 r^{2y+1}}{r+s} = 0. \tag{2.17}$$

Somando (2.17) na equação (2.16) teremos:

$$\begin{aligned} \frac{r^2 r^{2y+1} + s^2 s^{2y+1} + s^2 r^{2y+1} - s^2 r^{2y+1}}{r+s} &= \frac{r^{2y+1}(r^2 - s^2)}{r+s} + \frac{s^2(r^{2y+1} + s^{2y+1})}{r+s} \\ &= r^{2y+1}(r-s) + \frac{s^2(r^{2y+1} + s^{2y+1})}{r+s} \end{aligned} \tag{2.18}$$

Substituindo a hipótese de indução (2.15) na equação (2.18), teremos

$$\begin{aligned} r^{2y+1}(r-s) + s^2(r^{2y} - r^{2y-1}s + \cdots - rs^{2y-1} + s^{2y}) &= \\ = r^{2y+2} - r^{2y+1}s + r^{2y}s^2 - \cdots - rs^{2y+1} + s^{2y+2}) &= \\ = r^{2(y+1)} - r^{2(y+1)-1}s + \cdots - rs^{2(y+1)-1} + s^{2(y+1)}. \end{aligned}$$

Assim temos que

$$\frac{r^{2(y+1)+1}+s^{2(y+1)+1}}{r+s} = r^{2(y+1)} - r^{2(y+1)-1}s + \cdots - rs^{2(y+1)-1} + s^{2(y+1)}.$$

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

c) Se $r+s \neq 0$, mostre que, para todo $x \in \mathbb{N}$,

$$\frac{r^{2x}-s^{2x}}{r+s} = r^{2x-1} - r^{2x-2}s + \cdots + rs^{2x-2} - s^{2x-1}$$

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

$$\frac{r^{2.1}-s^{2.1}}{r+s} = r^{2.1-1} - r^{2.1-2}s.$$

Suponhamos verdadeiro para $x = y$, ou seja,

$$\frac{r^{2y}-s^{2y}}{r+s} = r^{2y-1} - r^{2y-2}s + \cdots + rs^{2y-2} - s^{2y-1}. \tag{2.19}$$

E mostraremos que vale para $x = y+1$, isto é,

$$\frac{r^{2(y+1)}-s^{2(y+1)}}{r+s} = r^{2y+1} - r^{2y}s + \cdots + rs^{2y} - s^{2y+1}.$$

Temos que

$$\frac{r^{2(y+1)}-s^{2(y+1)}}{r+s} = \frac{r^{2y}r^2 - s^{2y}s^2}{r+s}, \tag{2.20}$$

e

$$\frac{r^{2y}s^2 - r^{2y}s^2}{r+s} = 0. \tag{2.21}$$

Somando (2.21) na equação (2.20) teremos:

$$\begin{aligned} \frac{r^{2y}r^2 - s^{2y}s^2 + r^{2y}s^2 - r^{2y}s^2}{r+s} &= \frac{r^{2y}(r^2-s^2)}{r+s} + \frac{s^2(r^{2y}-s^{2y})}{r+s} \\ &= r^{2y}(r-s) + \frac{s^2(r^{2y}-s^{2y})}{r+s} \end{aligned} \tag{2.22}$$

Substituindo a hipótese de indução (2.19) na equação (2.22), teremos

$$r^{2y}(r-s) + s^2(r^{2y-1} - r^{2y-2}s + \cdots + rs^{2y-2} - s^{2y-1}) =$$

$$= r^{2y+1} - r^{2y}s + r^{2y-1}s^2 - r^{2y-2}s^2 + \cdots + rs^{2y} - s^{2y+1}.$$

Assim teremos que

$$\frac{r^{2(y+1)} - s^{2(y+1)}}{r+s} = r^{2y+1} - r^{2y}s + \cdots + rs^{2y} - s^{2y+1}.$$

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

2.4 Máximo Divisor Comum

Definição: Dados dois inteiros w e a não nulos ($w \neq 0$ ou $a \neq 0$). Diremos que um inteiro positivo $d\,(d > 0)$ é o máximo divisor comum (mdc) de w e a se satisfaz às seguintes condições.[7] [8]

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

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

Observemos que pelo item (i), d é um divisor comum de w e a, e pelo item (ii), d é o maior dentre todos os divisores comuns de w e a.

Diremos que mdc(w, a) como máximo divisor comum de w e a.

Assim o mdc de w e a não depende da ordem de w e a, e dessa maneira diremos que mdc$(w, a) =$ mdc(w, a).

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

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

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) mdc$(0, 0)$ não existe

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

(3) se $w \neq 0$, então mdc$(w, 0) = |w|$

(4) se $w \mid a$, então mdc$(w, a) = |w|$

Assim, por exemplo:

$$\begin{aligned} \text{mdc}(7, 1) &= 1 \\ \text{mdc}(-8, 0) &= |-8| = 8 \\ \text{mdc}(-5, 25) &= |-5| = 5 \end{aligned}$$

2.5 Divisão Euclidiana

Teorema 2.3 (Divisão Euclidiana)**.** Sejam $x, y \in \mathbb{Z}$; $0 < x < y$. Existem dois únicos números inteiros s e t, tais que

$$y = xs + t, \text{ com } 0 \leq t < |x|$$

Demonstração: (Existência) Suponhamos que $0 < x$ e $s \in \mathbb{Z}$, tal que s é o maior inteiro e $xs \leq y$. Assim, temos

$$\begin{aligned} xs \leq y < x \cdot (s+1) &\implies xs \leq y < xs + x \\ &\implies 0 \leq y - xs < x, \text{ definimos } t = y - xs, \text{ ou seja, } 0 \leq t < x. \end{aligned}$$

(Unicidade) Sejam s, s_1, t, t_1 inteiros tais que $y = xs + t$, $y = xs_1 + t_1$ e $0 \leq t, t_1 < |x|$. Logo, teremos que $|t - t_1| < x$ e de $y = xs + t\,(I)$ e $y = xs_1 + t_1\,(II)$, e fazendo (I) - (II), temos

$$0 = xs + t - xs_1 - t_1$$

$$t_1 - t = xs - xs_1$$

$$t_1 - t = x(s - s_1).$$

Suponhamos que $s \neq s_1$. Assim teremos que $1 \leq |s - s_1|$. Multiplicando a desigualdade por $|x|$, teremos

$|x| \leq |x| \cdot |s - s_1| = |t_1 - t| < |x|$, ou seja, $|x| < |x|$, absurdo, desse modo $s = s_1$ e $t = t_1$ ■

Sobre o teorema 2.3 o leitor pode consultar [7]

2.6 Mínimo Multiplo Comum

Definição: Um número inteiro será um mínimo múltiplo comum quando é simultaneamente múltiplo desses números.[7] [8]

Todo caso, os números w e a e 0 serão múltiplos comuns de w e a.

Um número $m \geq 0$ é denominado *mínimo múltiplo comum (mmc)* de w e a se satisfaz às seguintes condições

(i) m é um múltiplo comum de w e a, e

(ii) se b é um múltiplo comum de w e a, então $m \mid b$

Por exemplo, 30 é múltiplo de 3 e 5, mas não é considerado *mmc* desses números. O número 15 é o *mmc* de 3 e 5.

Tomamos m e m' como dois mínimos múltiplos comuns de w e a, então, do item (ii) definido acima, temos $m \mid m'$ e $m' \mid m$. E m e m' são números inteiros não negativos, obtemos $m = m'$, demonstrando que o mínimo múltiplo comum é único.

Mas se m é o *mmc* de w e a e b é múltiplo comum de w e a, então $m \mid b$. Logo se b é positivo, temos $m \leq b$, demonstrando que m é o menor múltiplo comum de w e a.

O *mínimo múltiplo comum* de w e a, se existe, é denotado por $[w, a]$. Se existir $[w, a]$ temos:

$$[-w, a] = [w, -a] = [-w, -a] = [w, a]$$

Logo, o cálculo do *mmc* de dois números, sempre supomos não negativos. Observa-se que $[w, a] = 0$ se, e somente, se, $w = 0$ ou $a = 0$. Então $[w, a] = 0$, onde 0 divide $w\ a$, que é múltiplo de w e de a, logo $wa = 0$ e, portanto, $w = 0$ ou $a = 0$. E se $w = 0$ ou $a = 0$, então 0 é o único múltiplo comum de w e a, portanto $[w, a] = 0$.

Proposição 2.6. Sejam w e a dois números inteiros, temos que $[w, a]$ existe e

$$[w, a](w, a) = |wa|$$

Demonstração: Se $w = 0$ ou $a = 0$, a proposição citada acima é satisfatória. E a igualdade é aceita para w e a se, e somente, se, ela é aceita para $\pm w$ e $\pm a$. Logo, supormos $w, a \in \mathbb{N}$. Colocamos $m = \dfrac{w \cdot a}{(w, a)}$. Como

$$m = w \cdot \frac{a}{(w, a)} = a \cdot \frac{w}{(a, w)}$$

obtemos $w \mid m$ e $a \mid m$. Portanto, m é um múltiplo comum de w e a; logo, $b = n \cdot w = n' \cdot a$. Segue daí que

$$n \cdot \frac{w}{(w, a)} = n' \cdot \frac{a}{(w, a)}$$

Como $\dfrac{w}{(w, a)}$ e $\dfrac{a}{(w, a)}$ são primos entre si, temos $\dfrac{w}{(w, a)}$ divide n', e, portanto $m = \dfrac{w}{(w, a)}\ a$ divide $n' \cdot a$ que é igual a b.[7]

2.7 Números Primos

Definição: Dado um número inteiro positivo $q > 1$ que tenha dois divisores positivos q e 1 é denominado um *número primo* ou somente primo. Do contrário, q é *composto.*

Logo, como exemplo teremos os inteiros positivos 2, 3, 5, 7, 11, 13, 17, 19, 23 primos, enquanto os inteiros positivos 4,6,8,9,10,12,14,15,16,18,20,21 e 22 compostos.

Temos o número inteiro positivo 1 não sendo número primo e nem composto, portanto, se w é um número inteiro positivo qualquer, logo w é primo, ou w é composto ou $w = 1$.

O número inteiro positivo 2 é o único número inteiro positivo par que é $primo$.[7] [8]

Teorema 2.4. Seja $w \in \mathbb{Z}$ e q primo, se $q \nmid w$, então w e q são primos entre si.

Demonstração: Seja $s = \text{mdc}(w, q)$. Logo $s \mid w$ e $s \mid q$. De $s \mid q$ temos então $s = 1$ ou $s = q$, como q é primo, dessa maneira a segunda igualdade será impossível, devido $q \nmid w$, por conseguinte $s = 1$, ou seja, $\text{mdc}(w, q) = 1$.

Portanto, w e q são primos entre si. ■

Corolário 1. Se q é primo tal que $q \mid wr$, então $q \mid w$ ou $q \mid r$.

Demonstração: Suponha que

$$\begin{aligned} q \nmid w &\implies \text{mdc}(w, q) = 1 \\ &\implies wx + qy = 1 \\ &\implies wsx + xsq = s \end{aligned}$$

Por hipótese $q \mid ws$, então existe $z \in \mathbb{Z}; ws = yq$, logo

$$\begin{aligned} &\implies zqx + ysq = 1 \\ &\implies q(zx + ys) = s \\ &\implies qz = s;\ z \in \mathbb{Z};\ z = zx + ys \\ &\implies q \mid s. \end{aligned}$$

Portanto, $q \mid s$ ■

Corolário 2. Se q é primo tal que $q \mid r_1 r_2 \cdots rx$, então existe um índice w, com $1 \leq w \leq x$, tal que $q \mid r_w$.

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

Pelo corolário 1 , se $q \mid r_1 r_2 \cdots rx$, então

$$q \mid r_x \qquad \text{ou} \qquad q \mid r_1 r_2 \cdots r_{x-1}$$

Se $q \mid r_x$, a proposição estará demonstrada, porém se $q \mid r_1 r_2 \cdots r_{x-1}$, teremos pela hipótese de indução que $q \mid r_w$, com $1 \leq w \leq r - 1$. assim em qualquer dos dois casos, q divide um dos inteiros $r_1 r_2 \cdots r_x$. ■

Corolário 3. Se os inteiros $q, r_1, r_2, \cdots, r_x$ são todos primos e se $q \mid r_1 r_2 \cdots r_x$, então existe um índice w, com $1 \leq w \leq x$, tal que $q = r_w$.

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

Teorema 2.5 (Teorema Fundamental da Aritmética)**.** Qualquer número inteiro maior que 1 deve ser representado de maneira única (a menos de ordem) como um produto de fatores primos.

Demonstração: Se x é um número primo, então não tem nada a ser demonstrado. Suponhamos então que x seja composto. Consideremos q_1 $(q_1 > 1)$, o menor dos divisores positivos de x. O número q_1 deve ser primo, pois caso contrário, existiria q, $1 < q < q_1$ com $q \,|\, x$, o que é uma contradição à escolha de q_1. Logo, $x = q_1 x_1$.

Se x_1 for primo, então a demonstração estará completa. Caso contrário, podemos ter q_2 como o menor fator de x_1. Consequentemente q_2 deve ser primo e podemos escrever $x = q_1 q_2 x_2$.

Repetindo este procedimento, obtemos uma sequência decrescente de inteiros positivos $x_1, x_2, \ldots, x_t$. Temos todos eles maiores do que 1, este processo terminará. Como os primos na sequência $q_1, q_2, \ldots, q_y$ não são necessariamente distintos, x terá, em geral, a seguinte forma:

$$x = q^{u_1} q^{u_2} \ldots q_y^{u_y}.$$

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

De fato, se x é primo, então não tem nada a ser demonstrado. Suponhamos, portanto, que x seja composto e que tenha duas formas distintas de fatoração, isto é,

$$x = q_1 q_2 \ldots q_w = r_1 r_2 \ldots r_s.$$

Vamos provar que $w = s$ e que cada q_i é igual a algum r_j. Como q_1 divide o produto $r_1 r_2 \ldots r_s$, ele divide pelo menos um dos fatores r_j. Sem perda de generalidade podemos supor que $q_1 \,|\, r_1$. Logo,

$$x/r_1 = r_2 r_3 \ldots q_w = r_2 r_3 \ldots r_s.$$

Como $1 < x/q_1 < x$, a hipótese de indução nos diz que as duas fatorações são idênticas, isto é, $w = s$ e, a menos da ordem, as fatorações $q_1 q_2 \ldots q_w$ e $r_1 r_2 \ldots r_s$ são iguais. ■

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

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

$$x = {q_1}^{w_1} {q_2}^{w_2} \cdots {q_r}^{w_r}$$

onde, para $i = 1, 2, \cdots, r$, cada r_i é um inteiro positivo e cada q_i é um primo, com $q_1 < q_2 < \cdots < q_r$, denominada decomposição canônica do inteiro positivo $x > 1$

Exemplo 2.9. Vamos encontrar a decomposição canônica do inteiro positivo $n = 2520$.

Solução: Temos que $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$

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

Teorema 2.6. Se r não é primo, então r possui, necessariamente, um fator primo menor do que ou igual a $\sqrt{r}$.

Demonstração: Sendo r composto então $r = r_1 \cdot r_2$ onde $1 < r_1 < r$, e $1 < r_2 < r$. Sem perda de generalidade vamos supor que $r_1 \leq r_2$. Assim r_1 tem que ser $\leq \sqrt{r}$, pois caso contrário, teríamos $r = r_1 \cdot r_2 > \sqrt{r} \cdot \sqrt{r} = r$ no qual teríamos um contradição. Assim, pelo Teorema 2.5 r_1 possui algum fator primo q, no qual deve ser $\leq \sqrt{r}$. Como q é um fator primo de r_1 é também um fator de x, assim a demonstração está completa. ■

Capítulo 3

Equações Diofantinas Lineares

Para uma equação com mais de uma váriavel em que se deseja obter soluções inteiras, são conhecidas como equações diofantinas, homenageando o matemático grego Diofantos de Alexandria, que trabalhou na pesquisa de tais equações. [7] [8]

Definição: Uma equação da forma $kr + ls = m$, onde k, l e m são inteiros é chamada **equação diofantina linear**.

Todo par de inteiros r_0, s_0 em que $kr_0 + ls_0 = m$, chama - se uma *solução inteira ou apenas solução da equação kr + ls = m.*

Teorema 3.1. A equação diofantina linear $kr + ls = m$ tem solução se, e somente se, $n =$ mdc(k, l) é um divisor de m.

Demonstração: $(\Longrightarrow)$ Se (r_0, s_0) é uma solução, então vale a igualdade

$$kr_0 + ls_0 = m.$$

Como $n \mid k$ e $n \mid l$, então $n \mid m$, existem inteiros x e y tais que $k = nx$ e $l = ny$, desse modo:

$$m = kr_0 + ls_0 = nxr_0 + nys_0 = n(xr_0 + ys_0)$$

E como $xr_0 + ys_0$ é um inteiro, temos que n divide m.

$(\Longleftarrow)$ Como $n =$ mdc(k, l), então podemos determinar x_0, $y_0 \in \mathbb{Z}$ tais que $ky_0 + lx_0 = n$. Mas, por hipótese, $n \mid m$ e, portanto, $m = np$ para algum $p \in \mathbb{Z}$. Consequentemente,

$$m = np = (ky_0 + lx_0)p = k(y_0p) + l(x_0p),$$

o que implica que o par (y_0p, x_0p) é solução da equação considerada. ■

Exemplo 3.1. A equação diofantina $3r + 5s = 8$ tem solução, pois $\text{mdc}(3, 5) = 1$ divide 8. Já a equação diofantina $8r + 12s = 18$ não possui solução, pois o $\text{mdc}(8, 12) = 4$ não divide 18.

Teorema 3.2. Se a equação diofantina $kr+ls = m$ tem uma solução (r_0, s_0), então tem infinitas soluções e o conjuntos destas é

$$S = \left\{ \left(r_0 + \frac{l}{n}\, u,\ s_0 - \frac{k}{n}\, u \right) ; \quad u \in \mathbb{Z} \right\},$$

onde $n = \text{mdc}(k, l)$.

Demonstração: Mostraremos inicialmente que todo par $(k_0 + (l/n)u,\ s_0 - (k/n)u)$ é solução da equação considerada. De fato,

$$k\left(r_0 + \frac{l}{n}\ u \right) + l\left(s_0 - \frac{k}{n}\ u \right) = kr_0 + ls_0 + \left(\frac{kl - lk}{n} \right) u = kr_0 + ls_0 = m,$$

pois, por hipótese, (r_0, s_0) é solução da equação diofantina.

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

$$kr' + ls' = m = kr_0 + ls_0 \qquad \Longrightarrow \qquad k(r' - r_0) = l(s_0 - s').$$

Mas, como n é divisor de k e l, então existem $a,\ b \in \mathbb{Z}$, com $\text{mdc}(a, b) = 1$, tais que $k = na$ e $l = nb$. Assim,

$$na(r' - r_0) = nb(s_0 - s') \qquad \Longrightarrow \qquad a(r' - r_0) = b(s_0 - s').$$

Da última igualdade, segue que a divide $b(s_0 - s')$. E, como a e b são primos entre si, então a divide $s_0 - s'$, pela Proposição (vi). Logo,

$$s_0 - s' = au,$$

para algum $u \in \mathbb{Z}$. Como $a = k/n$, então

$$s' = s_0 - \frac{k}{n}\, u.$$

Observando-se agora que, em consequência,

$$a(r' - r_0) = b(s_0 - s') = srt,$$

segue que

$$r' = r_0 + \frac{l}{n}\, u.$$

■

Corolário 6. Se a equação diofantina $kr+ls = m$ tem uma solução (r_0, s_0), onde mdc$(k, l) = 1$, então tem infinitas soluções e o conjuntos destas é

$$S = \{(r_0 + lu,\ s_0 - ku)\,;\quad u \in \mathbb{Z}\}\,.$$

Exemplo 3.2. Determinar todas as soluções da equação diofantina linear

$$45r + 14s = 11.$$

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

$$\begin{aligned} 45 &= 14 \cdot 3 + 3 \\ 14 &= 3 \cdot 4 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 1 + 1 \\ 1 &= 1 \cdot 1 \end{aligned}$$

Portanto, o mdc$(45, 14) = 1$ e como $1 \mid 11$, a equação dada tem solução.

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ 2 &= 14 - 3 \cdot 4 \\ 3 &= 45 - 14 \cdot 3 \end{aligned}$$

No qual segue:

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 = 3 - 1 \cdot (14 - 3 \cdot 4) = 3 - 14 + 3 \cdot 4 = \\ &= -14 + 5 \cdot 3 = -14 + 5 \cdot (45 - 14 \cdot 3) = -14 + 5 \cdot 45 - 15 \cdot 14 = \\ &= 45 \cdot 5 + 14 \cdot (-16). \end{aligned}$$

isto é:

$$1 = 45 \cdot 5 + 14 \cdot (-16)$$

Multiplicando ambos os membros desta igualdade por 11, obtemos:

$$11 = 45 \cdot 55 + 14 \cdot (-176)$$

Logo o par de inteiros $r_0 = 55$ e $s_0 = -176$ é uma solução particular da equação proposta, assim todas as outras soluções são dadas pelas fórmulas :

$$\begin{aligned} r &= 55 + 14u \\ y &= -176 - 45u; \quad u \in \mathbb{Z}. \end{aligned}$$

Capítulo 4

Congruências

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

$$a \equiv f \mod n \iff n \mid (a - f),$$

ou seja,

$$a \equiv f \mod n \iff \exists\, l \in \mathbb{Z};\ a - f = ln.$$

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

Em particular, $a \equiv 0 \mod n$ se e somente se o *módulo n divide a ($n \mid a$). [7] [8]*

Teorema 4.1. Se a, f, g e n são inteiros, $n > 0$, valem as seguintes propriedades:

1. $a \equiv a \mod n$
2. Se $a \equiv f \mod n$, então $f \equiv a \mod n$
3. Se $a \equiv f \mod n$ e $f \equiv g \mod n$, então $a \equiv g \mod n$.

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

(2) Se $a \equiv f \mod n$, então $n \mid (a - f)$, logo existe $l \in \mathbb{Z}$ tal que $(a - f) = ln$, e daí, segue que $(f - a) = -ln$. Portanto, $n \mid (f - a)$ e, consequentemente, $f \equiv a \mod n$.

(3) Como $a \equiv f \mod n$, então existe $l_1 \in \mathbb{Z}$ tal que

$$(a - f) = l_1 m, \tag{4.1}$$

e como $f \equiv g \mod n$, então existe $l_2 \in \mathbb{Z}$ tal que

$$(f - g) = l_2 m \tag{4.2}$$

Somando-se membro a membro as equações 4.1 e 4.2 , obtemos $a - g = (l_1 + l_2)n$, o que acarreta $a \equiv g \mod n$. ■

Teorema 4.2. Se a, f, g e n são inteiros tais que $a \equiv f \mod n$, então

1. $a + f \equiv f + g \mod n$
2. $a - g \equiv f - g \mod n$
3. $ag \equiv fg \mod n$

Demonstração: (1) Como $a \equiv f \mod n$, temos que $a - f = lm$ e, portanto, como $a - f = (a + g) - (f + g)$ temos $a + g \equiv f + g \mod n$.

(2) Como $(a - g) - (f - g) = a - f$ e, por hipótese, $a - f = ln$ temos que $a - g \equiv f - g \mod n$.

(3) Como $a - f = ln$, então $ag - fg = gln$, de onde obtemos que $n \mid (ag - fg)$ e, portanto, $ag \equiv fg \mod n$. ■

Teorema 4.3. Se a, f, g, h e n são inteiros tais que $a \equiv f \mod n$ e $g \equiv h \mod n$, então

1. $a + g \equiv f + h \mod n$
2. $a - g \equiv f - h \mod n$
3. $ag \equiv fh \mod n$

Demonstração: (1) Como $a \equiv f \mod n$, então existe $t \in \mathbb{Z}$ tal que

$$a - f = tn. \tag{4.3}$$

E como $g \equiv h \mod n$, então existe $v \in \mathbb{Z}$ tal que

$$g - h = vn. \tag{4.4}$$

Somando-se membro a membro as equações (4.3) e (4.4) obtemos

$$(a + g) - (f + h) = (t + v)n,$$

e isto acarreta que

$$a + g \equiv f + h \mod n.$$

(2) De modo análogo, utilizando a hipótese do teorema, e subtraindo-se as equações (4.3) e (4.4) obtemos

$$(a-f)-(g-h)=(a-g)-(f-h)=(t-v)n,$$

o que implica que $a-g \equiv f-h \mod n$.

(3) Multiplicando ambos os membros de $a-f=tn$ por g e ambos os membros de $g-h=vn$ por f, obtemos $ag-fg=gtn$ e $fg-fh=fvn$. Somando membro a membro estas últimas igualdades obtemos

$$ag-fg+fg-fh=ag-fh=(gv+fv)n$$

o que implica que $ag \equiv fh \mod n$. ■

Corolário 7. Se a, f, q e n são inteiros com $q>0$ e $a \equiv f \mod n$, então $a^q \equiv f^q \mod n$.

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

$$a^1 \equiv f^1 \mod n.$$

Suponhamos verdadeiro para $q=l$, isto é,

$$a^l = f^l \mod n \tag{4.5}$$

e mostraremos que vale para $q=l+1$, ou seja,

$$a^{l+1} = f^{l+1} \mod n. \tag{4.6}$$

Temos pelo **Teorema** 4.3 (3) que

$$ag \equiv fh \mod n,$$

assim multiplicando na equação 4.5 pela hipótese

$$a \equiv f \mod n,$$

teremos:

$$\begin{aligned} a^l \cdot a &\equiv f^l \cdot f \mod n \\ a^{l+1} &\equiv f^{l+1} \mod n \end{aligned}$$

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

Exemplo 4.1. Qual o resto da divisão de $5^{61}+7^{61}+9^{61}+15^{61}$ por 12?

Solução: Temos que:

$$\begin{aligned} 7 &\equiv -5 \mod 12 \\ 7^{61} &\equiv (-5)^{61} \mod 12 \quad (4.7) \\ 5^{61} &\equiv 5^{61} \mod 12. \quad (4.8) \end{aligned}$$

De 4.7 e 4.8 e da Proposição 4.2 1 segue que

$$5^{61}+7^{61} \equiv 0 \mod 12. \quad (4.9)$$

De modo análogo temos

$$\begin{aligned} 15 &\equiv -9 \mod 12 \\ 15^{61} &\equiv (-9)^{61} \mod 12 \quad (4.10) \\ 9^{61} &\equiv 9^{61} \mod 12. \quad (4.11) \end{aligned}$$

De 4.10 e 4.11 e da Proposição 4.2 1 segue que

$$15^{61}+9^{61} \equiv 0 \mod 12. \quad (4.12)$$

Somando as congruências 4.9 e 4.12, obtemos: $5^{61}+7^{61}+9^{61}+15^{61} \equiv 0 \mod 12$, desse modo temos que o resto da divisão de $5^{61}+7^{61}+9^{61}+15^{61}$ por 12 é igual a zero. ■

Teorema 4.4. Se $ag \equiv fg \mod n$ e se o mdc$(g,n)=h$, então $a \equiv f \mod n/h$.

Demonstração: Se $ag \equiv fg \mod n$, então $ag-fg=(a-f)g=ln;\ l \in \mathbb{Z}$.

E se mdc$(g,n)=h$, existem inteiros p e t tais que $g=hp$ e $n=th$, onde p e t são primos entre si. Logo:

$$(a-f)hp=lth \quad \text{ou} \quad (a-f)p=lt$$

o que implica $t \mid (a-f)p$, como mdc$(p,t)=1$, teremos pela proposição (vi) que $t \mid (a-f)$ e $a \equiv f \mod t$, porém $t=n/h$, logo $a \equiv f \mod n/h$. ■

Corolário 8. Se $ag \equiv fg \mod n$ e se o mdc$(g, n) = 1$, então $a \equiv f \mod n$.

Demonstração: Se $ag \equiv fg \mod n$, então $n \mid (a - f)g$. Como mdc$(n, g) = 1$. temos que $n \mid (a - f)$, isto é, $a \equiv f \mod n$ ■

Corolário 9. Se $ag \equiv fg \mod j$, com j primo, e se $j \nmid g$, então $a \equiv f \mod j$.

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

Exemplo 4.2. Resolva a congruência $4y \equiv 12 \mod 14$, isto é, encontre todos os inteiros y tais que $4y \equiv 12 \mod 14$.

Demonstração: Observe que

$$\begin{aligned} 4y \equiv 12 \mod 14 &\Leftrightarrow 2y \equiv 6 \mod 7 \quad (\text{pelo Teorema } 4.4) \\ &\Leftrightarrow y \equiv 3 \mod 7 \quad (\text{pelo corolário } 8). \end{aligned}$$

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

Exemplo 4.3. Resolva a congruência $6y \equiv 15 \mod 21$.

Demonstração: Desta vez temos

$$\begin{aligned} 6y \equiv 15 \mod 21 &\Leftrightarrow 2y \equiv 5 \mod 7 \quad (\text{pelo Teorema } 4.4) \\ &\Leftrightarrow 2y \equiv 12 \mod 7 \\ &\quad (\text{usando } 5 \equiv 12 \mod 7 \text{ para obter um número par}) \\ &\Leftrightarrow y \equiv 6 \mod 7 \quad (\text{pelo corolário } 8). \end{aligned}$$

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

Teorema 4.5. Sejam a e f inteiros quaisquer, e sejam n, q, h e l inteiros positivos.

(i) Se $a \equiv f \mod n$ e $h \mid n$, então $a \equiv f \mod h$;

(ii) se $a \equiv f \mod q$ e $a \equiv f \mod l$, então $a \equiv f \mod \text{mmc}(q, l)$;

(iii) se $qa \equiv qf \mod n$, então $a \equiv f \mod \dfrac{n}{\text{mdc}(q, n)}$;

(iv) se $qa \equiv qf \mod qn$, então $a \equiv f \mod n$.

4.1 Congruências Lineares

Definição: Denominamos de **congruência linear** em uma variável a uma congruência da forma $ay \equiv f \mod n$, onde y é uma incógnita. [7] [8]

Numa congruência linear terá uma solução, várias soluções ou até mesmo não ter nenhuma solução. Então analisaremos as situações a seguir, e a condição para existência de solução, como segue:

Teorema 4.6. A congruência linear $ay \equiv f \mod n$ tem solução se, e somente se, h divide f, onde $h = \text{mdc}(a, n)$.

Demonstração: $(\Longrightarrow)$ Suponhamos que a congruência linear $ay \equiv f \mod n$ tem como solução o inteiro y_0, ou seja, que $ay_0 \equiv f \mod n$. Então, existe um inteiro x_0, de modo que

$$ay_0 - f = nx_0 \quad \text{ou} \quad ay_0 - nx_0 = f$$

e como $h = \text{mdc}(a, n)$, logo $h \mid a$ e $h \mid n$, desse modo $h \mid (ay_0 - nx_0)$ e, portanto, $h \mid f$.

$(\Longleftarrow)$ Reciprocamente, suponhamos que $h \mid f$, ou seja, existe $l \in \mathbb{Z}$, tal que $f = hl$.

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

$$ay_0 + nx_0 = h, \tag{4.13}$$

multiplicando ambos os membros da equação 4.13 por l, teremos:

$$\begin{aligned} a(ly_0) &+ n(lx_0) = hl = f \\ a(ly_0) &- f = n(-lx_0) \end{aligned}$$

o que acarreta

$$a(ly_0) \equiv f \mod n.$$

Portanto, o inteiro ly_0 é uma solução da congruência linear. ■

$$ay \equiv f \mod n.$$ ■

Teorema 4.7. Seja $d = \text{mdc}(a, n)$ e suponha que $h \mid f$. Então a congruência linear

$$ay \equiv f \mod n$$

tem precisamente h soluções mutuamente incongruentes módulo n.

Demonstração: Temos que a congruência linear $ay \equiv f \mod n$ é equivalente a equação diofantina $ay - nx = f$, onde a mesma tem solução se e somente se $h \mid f$, onde $h = \text{mdc}(a, n)$. E como ja foi visto no Teorema 3.2 se $h \mid f$ e se o par de inteiros (y_0, x_0) é uma solução particular da equação $ay - nx = f$, então todas as outras soluções desta equação são dadas pelo conjunto solução:

$$S = \left\{ \left(y_0 + \frac{n}{h}\, r,\ x_0 + \frac{a}{h}\, r \right);\ \ r \in \mathbb{Z} \right\},$$

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

$$y_0,\ y_0 + \frac{n}{h},\ y_0 + 2\left(\frac{n}{h}\right),\ \cdots,\ y_0 + (h-1)\left(\frac{n}{h}\right).$$

Desse modo mostraremos que estes h inteiros são *mutuamente incongruentes módulo n* e que todos os demais inteiros dados pela fórmula $y_0 + \left(\frac{n}{h}\right) r$ são *congruentes módulo n* a algum desses h inteiros. Com efeito, se fosse

$$y_0 + \left(\frac{n}{h}\right) r_1 \equiv y_0 + \left(\frac{n}{h}\right) r_2 \mod n$$

onde $0 \leq r_1 < r_2 \leq h - 1$, assim, teríamos :

$$\left(\frac{n}{h}\right) r_1 \equiv \left(\frac{n}{h}\right) r_2 \mod n.$$

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

$$r_1 \equiv r_2 \mod n$$

o que significa $h \mid (r_2 - r_1)$, o que é um absurdo, já que $0 < r_2 - r_1 < h$.

E mais ainda, qualquer outro inteiro $y_0 + \left(\frac{n}{h}\right) r$ é *congruente módulo n* a algum dos h inteiros enumerados anteriormente. Com efeito, pelo algoritmo da divisão, temos:

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

e, portanto:

$$y_0 + \left(\frac{n}{h}\right) r = y_0 + \left(\frac{n}{h}\right)(hp + t) = y_0 + np + \left(\frac{n}{h}\right) t$$

ou seja;

$$y_0 + \left(\frac{n}{h}\right) r \equiv y_0 + \left(\frac{n}{h}\right) t \mod n$$

onde $y_0 + \left(\frac{n}{h}\right) t$ é um dos h inteiros que foram selecionados. ■

Corolário 10. Seja o mdc$(a, n) = 1$. Então a congruência linear $ay \equiv f \mod n$ tem uma única solução módulo n.

Definição: Dizemos que uma solução y_0 de $ay \equiv f \mod n$ é única módulo n quando qualquer outra solução y_1 for congruente a y_0 módulo n.

Exemplo 4.4. Resolva a congruência linear $3y \equiv 6 \mod 18$.

Solução: Temos que o mdc$(3, 18) = 3$, e como $3 \mid 6$, logo pelo teorema 4.7 a congruência dada tem exatamente 3 soluções mutuamente incongruentes modulo 18.

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

$$y = 2 + 6r; \quad r = 0, 1, 2.$$

Portanto, y = 2, 8, 14.

Teorema 4.8. Seja o mdc$(a, n) = 1$. Então a tem um único inverso módulo n.

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

$$ay \equiv 1 \mod n$$

tem uma única solução $y_0 \mod n$, ou seja,

$$ay_0 \equiv 1 \mod n$$

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

$$\overline{a} = y_0.$$

■

Proposição 4.1. Se q é primo, então o inteiro positivo a é o seu próprio inverso módulo q se, e somente se, $a \equiv 1 \mod q$ ou $a \equiv -1 \mod q$.

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

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

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

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

4.1.1 Resolução de Equação Diofantina por Congruência

Foi visto anteriormente no Teorema 3.1, que a equação diofantina linear

$$ax + fy = g \tag{4.14}$$

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

$$ax_0 + fy_0 = g \qquad \text{a} \qquad ax_0 - g = -fy_0,$$

o que implica

$$ax_0 \equiv g \mod f. \tag{4.15}$$

Portanto, para obter uma solução particular da equação diofantina linear 4.14 , basta determinar uma solução qualquer $x = x_0$ da congruência linear

$$ax \equiv g \mod f. \tag{4.16}$$

e substituir o valor x_0 de x na equação 4.14 para que possamos encontrar o valor correspondente y_0 de y, ou seja,

$$ax_0 + fy_0 = g.$$

Porém, também podemos obter uma solução particular da equação diofantina linear 4.14 determinando uma solução qualquer $y = y_0$ da congruência linear:

$$fy = g \mod a.$$

Exemplo 4.5. Vamos resolver por congruência a equação diofantina linear:

$$4x + 51y = 9$$

Solução: Como o $\text{mdc}(4, 51) = 1$, 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:

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

Exemplo 4.6. 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:

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

Definição: Se r e l são dois inteiros com $r \equiv l \mod n$, dizemos que l é um *resíduo* de r módulo n.

Definição: O conjunto dos inteiros $\{t_1, t_2, t_3, \cdots, t_v\}$ é um *sistema completo de resíduos* módulo n se

Exemplo 4.7. O conjunto $\{0, 1, 2, 3, \cdots, n-1\}$ é um sistema completo de resíduos módulo n.

Teorema 4.9 (**Pequeno Teorema de Fermat).** Se q é um primo e se q não divide o inteiro a $(q \nmid a)$, então:

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

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

Quaisquer dois são incongruentes módulo q, visto que $ar \equiv al \mod q$ implica $r \equiv l \mod q$, pois mdc$(a, q) = 1$, e isto só é possível se $r = l$, uma vez que ambos r e l são positivos e menores que q. Temos, portanto, um conjunto de $(q-1)$ elementos incongruentes módulo q e não divisíveis por q. Portanto, cada um deles é congruente a exatamente um dentre os elementos $1, 2, 3, \cdots q-1$. Assim se multiplicarmos estas congruências, membro a membro,

teremos:

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

ou seja,

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

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

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

o que conclui a demonstração. ■

Corolário 11. Se q é um primo, então $a^q \equiv a \mod q$, qualquer que seja o inteiro a.

Demonstração: Temos dois casos a analisar, são eles:

(i) Se $q \mid a$, então:

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

o que implica:

$$a^q \equiv a \mod q.$$

(ii) Se $q \nmid a$, então pelo teorema 4.9

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

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

Exemplo 4.8 (PROFMAT-MA14-2011). Ache o resto da divisão por 17 do número

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

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:

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

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

Exemplo 4.9 (PROFMAT-MA14-2012). Ache o resto da divisão de $1^5 + 2^5 + \cdots + 183^5$ por 5.

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

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

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 W por 5 é 1.

Exemplo 4.10. Encontre o resto da divisão de 8^{900} por 29.

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

$$\begin{aligned} 8^{28} &\equiv 1 \mod 29 \\ (8^{28})^{32} &\equiv 1^{32} \mod 29 \\ 8^{896} &\equiv 1 \mod 29. \end{aligned} \tag{4.17}$$

E temos que:

$$\begin{aligned} 8^2 &\equiv 6 \mod 29 \\ (8^2)^2 &\equiv (6)^2 \mod 29 \\ 8^4 &\equiv 36 \mod 29 \\ 8^4 &\equiv 7 \mod 29. \end{aligned} \tag{4.18}$$

Da congruência 4.17 e 4.18 e utilizando o **Teorema** 4.3 (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.

4.2 Sistemas de Congruências Lineares

Na resolução de sistemas de congruências lineares as dificuldades aparecem. E uma delas é que um sistema de duas ou mais congruências lineares não tem solução, mesmo que cada uma das congruências do sistema separadamente tenha solução. Então, por exemplo, não existe nenhum inteiro y que verifique simultaneamente as congruências lineares:

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

mesmo que cada uma delas, separadamente, tenha solução.

Pode surgir outro caso em que uma das congruências não tenha solução e, quando isso ocorrer, o sistema de congruências não haverá solução. [7]

Capítulo 5

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. [4] [7] [8] [11]

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 5.1 (Teorema Chinês dos Restos). Sejam $n_1, n_2, n_3, \cdots, n_t$ inteiros positivos primos entre si dois a dois (i.e. tais que mdc$(n_i,\ n_j) = 1 \quad \forall \quad i \neq j$). Então o sistema de congruência lineares

$$\begin{cases} y \equiv \ E_1 \mod n_1 \\ y \equiv \ E_2 \mod n_2 \\ y \equiv \ E_3 \mod n_3 \\ \ \ \vdots \\ y \equiv \ \ E_t \mod n_t \end{cases}$$

tem solução única, $\mod (n_1 n_2 n_3 \cdots n_t)$, onde $E_1,\ E_2,\ E_3,\ \cdots,\ E_t$ são inteiros dados.

A seguir apresentaremos um algoritmo e sua generalização que será utilizada na demonstração do Teorema 5.1 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, usaremos $\mathbf{E}$ para os valores dos restos de cada equação.

(iii) Na 3^a coluna, usaremos $\mathbf{N}$, o produto de todos os n_i com exceção do módulo no qual a linha esta presente. Assim, para cada linha, teremos $\mathbf{N_i} = \frac{\mathbf{N}}{\mathbf{n_i}}$;

(iv) Na 4^a coluna, usaremos $\overline{\mathbf{N}}$ e escreveremos a classe de equivalência que o $\mathbf{N_i}$ está associado com $\mathbf{n_i}$;

(v) Na 5^a coluna, usaremos $(\overline{\mathbf{N}})^{-\mathbf{1}}$ a classe inversa de cada elemento da coluna $\overline{\mathbf{N}}$, sempre respeitando o módulo referente a cada linha, ou seja, é o elemento que multiplicado com $\overline{\mathbf{N}}_\mathbf{i}$ deixa resto $\mathbf{1} \mod \mathbf{n_i}$;

(vi) Na 6^a coluna, usaremos $\mathbf{E} \cdot \mathbf{N} \cdot (\overline{\mathbf{N}})^{-\mathbf{1}}$ colocamos o produto dos elementos de cada linha, com exceção do $\overline{\mathbf{N}}$ que o mesmo esta na tabela para poder facilitar encontrar o valor do $(\overline{\mathbf{N}})^{-\mathbf{1}}$.

Assim teremos a tabela como segue:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	E · N ·$(\overline{N})^{-1}$
$y \equiv E_1 \mod n_1$	E_1	N_1	$\overline{N_1}$	$(\overline{N_1})^{-1}$	$E_1 \cdot N_1 \cdot (\overline{N_1})^{-1}$
$y \equiv E_2 \mod n_2$	E_2	N_2	$\overline{N_2}$	$(\overline{N_2})^{-1}$	$E_2 \cdot N_2 \cdot (\overline{N_2})^{-1}$
$y \equiv E_3 \mod n_3$	E_3	N_3	$\overline{N_3}$	$(\overline{N_3})^{-1}$	$E_3 \cdot N_3 \cdot (\overline{N_3})^{-1}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$y \equiv E_t \mod n_t$	E_t	N_t	$\overline{N_t}$	$(\overline{N_t})^{-1}$	$E_t \cdot N_t \cdot (\overline{N_t})^{-1}$

Desse modo, temos que uma solução do sistema de congruência é dado pelo algoritmo da seguinte maneira:

$$y = E_1 \cdot N_1 \cdot (\overline{N_1})^{-1} + E_2 \cdot N_2 \cdot (\overline{N_2})^{-1} + E_3 \cdot N_3 \cdot (\overline{N_3})^{-1} + \cdots + E_t \cdot N_t \cdot (\overline{N_t})^{-1}.$$

Onde:

$$\begin{aligned} N_1 &= n_2 n_3 \cdots n_t \\ N_2 &= n_1 n_3 \cdots n_t \\ N_3 &= n_1 n_2 \cdots n_t \\ &\vdots \\ N_t &= n_1 n_2 \cdots n_{t-1}. \end{aligned}$$

Demonstração: Primeiramente vamos mostrar que existe solução e que a mesma é da forma:

$$y = E_1 \cdot N_1 \cdot (\overline{N_1})^{-1} + E_2 \cdot N_2 \cdot (\overline{N_2})^{-1} + E_3 \cdot N_3 \cdot (\overline{N_3})^{-1} + \cdots + E_t \cdot N_t \cdot (\overline{N_t})^{-1}.$$

Agora reescreveremos a suposta solução em módulo n_1, ou seja:

$$y \equiv (E_1 \cdot N_1 \cdot (\overline{N_1})^{-1} + E_2 \cdot N_2 \cdot (\overline{N_2})^{-1} + E_3 \cdot N_3 \cdot (\overline{N_3})^{-1} + \cdots + E_t \cdot N_t \cdot (\overline{N_t})^{-1}) \mod n_1.$$

Porém, temos que $N_2 = n_1 \cdot n_3 \cdots n_t$, ou seja, $n_1 \mid (E_2 \cdot N_2 \cdot \overline{(N_2)}^{-1})$, com isso concluímos que:

$$E_2 \cdot N_2 \cdot \overline{(N_2)}^{-1} \equiv 0 \mod n_1.$$

De maneira análoga:

$$\begin{aligned} n_1 &\mid (E_3 \cdot N_3 \cdot \overline{(N_3)}^{-1}) \Longrightarrow E_3 \cdot N_3 \cdot \overline{(N_3)}^{-1} \equiv 0 \mod n_1 \\ &\vdots \\ n_1 &\mid (E_t \cdot N_t \cdot \overline{(N_t)}^{-1}) \Longrightarrow E_t \cdot N_t \cdot \overline{(N_t)}^{-1} \equiv 0 \mod n_1. \end{aligned}$$

Portanto, temos que:

$$y \equiv E_1 \cdot N_1 \cdot (\overline{N_1})^{-1} \mod n_1$$

E como estamos trabalhando com congruências, vamos tomar a liberdade em trocar N_1 pela sua classe de equivalência $\mod n_1$, assim:

$$y \equiv E_1 \cdot N_1 \cdot (\overline{N_1})^{-1} \mod n_1 \equiv E_1 \cdot \overline{N_1} \cdot (\overline{N_1})^{-1} \mod n_1 \equiv E_1 \mod n_1.$$

Mostramos que o modelo dado resolve a primeira equação do sistema de congruências.
De forma análoga, utilizando a ideia anterior teremos:

$$\begin{aligned} y &\equiv E_2 \cdot N_2 \cdot (\overline{N_2})^{-1} \mod n_2 \equiv E_2 \cdot \overline{N_2} \cdot (\overline{N_2})^{-1} \mod n_2 \equiv E_2 \mod n_2 \\ y &\equiv E_3 \cdot N_3 \cdot (\overline{N_3})^{-1} \mod n_3 \equiv E_3 \cdot \overline{N_3} \cdot (\overline{N_3})^{-1} \mod n_3 \equiv E_3 \mod n_3 \\ &\vdots \\ y &\equiv E_t \cdot N_t \cdot (\overline{N_t})^{-1} \mod n_t \equiv E_t \cdot \overline{N_t} \cdot (\overline{N_t})^{-1} \mod n_t \equiv E_t \mod n_{t.} \end{aligned}$$

Como vimos o sistema de congruência tem solução da forma:

$$y = E_1 \cdot N_1 \cdot (\overline{N_1})^{-1} + E_2 \cdot N_2 \cdot (\overline{N_2})^{-1} + E_3 \cdot N_3 \cdot (\overline{N_3})^{-1} + \cdots + E_t \cdot N_t \cdot (\overline{N_t})^{-1}.$$

Agora mostraremos que a solução é única $\mod (n_1 n_2 n_3 \cdots n_t)$.
Suponhamos que exista uma outra solução $\widetilde{y}$ tal que . Pelo fato de $\widetilde{y}$ ser solução do sistema,

em particular é solução da primeira equação, desse modo:

$$\widetilde{y} \equiv E_1 \mod n_1 \tag{5.1}$$
$$y \equiv E_1 \mod n_1 \tag{5.2}$$

Subtraindo 5.1 de 5.2 teremos:

$$\widetilde{y} - y \equiv 0 \mod n_1 \implies n_1 \mid (\widetilde{y} - y).$$

Analogamente;

$$\begin{aligned} n_2 &\mid (\widetilde{y} - y) \\ n_3 &\mid (\widetilde{y} - y) \\ &\vdots \\ y_t &\mid (\widetilde{y} - y). \end{aligned}$$

Como por hipótese $n_1, n_2, n_3, \cdots, n_t$ são primos entre si dois a dois, pode - se afirmar que:

$$\begin{aligned} (n_1 \cdot n_2 \cdot n_3 \cdots n_t) \mid \widetilde{y} - y \quad &\implies \quad \widetilde{y} - y \equiv 0 \mod (n_1 n_2 n_3 \cdots n_t) \\ &\implies \quad \widetilde{y} \equiv y \mod (n_1 n_2 n_3 \cdots n_t). \end{aligned}$$

■

5.1 Aplicação do Teorema Chinês dos Restos

Com a aplicação do Teorema Chinês dos Restos estamos habilitados a solucionar o problema proposto no inicio deste capitulo.

Observação: Toda vez que o sistema de congruências tiver solução e se uma congruência tiver zero como resto, então a solução será um múltiplo dessa congruência.Temos os exemplos 5.10 e 5.22 como referência.

Exemplo 5.1. 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 y a quantidade de soldados que haviam na formatura, tal que $1500 < y < 2000$, e montando o sistema temos:

$$\begin{cases} y \equiv 5 \mod 7 \\ y \equiv 4 \mod 9 \\ y \equiv 1 \mod 10. \end{cases}$$

Como mdc$(7, 9) =$ mdc$(7, 10) =$ mdc$(9, 10) = 1$, usaremos o Teorema Chinês dos Restos para resolvê -lo:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	E $\cdot$ N $\cdot(\overline{N})^{-1}$
$y \equiv 5 \mod 7$	5	90	6	6	2700
$y \equiv 4 \mod 9$	4	70	7	4	1120
$y \equiv 1 \mod 10$	1	63	3	7	441

$$\begin{aligned} y &\equiv (2700 + 1120 + 441) \mod (7 \cdot 9 \cdot 10) \\ y &\equiv 4261 \mod 630. \end{aligned}$$

Porém,

$$4261 \equiv 481 \mod 630.$$

Logo:

$$y \equiv 481 \mod 630 \implies y = 630w + 481; \quad w \in \mathbb{Z}.$$

Como $1500 < y < 2000$, teremos somente a solução inteira quando $w = 2$, resultando

$$\begin{aligned} y &= 630 \cdot 2 + 481 \\ y &= 1741. \end{aligned}$$

Portanto, haviam na formatura 1741 soldados.

Exemplo 5.2. Vamos resolver o sistema de congruências

$$\begin{cases} y \equiv 1 \mod 2 \\ y \equiv 2 \mod 3 \\ y \equiv 3 \mod 5. \end{cases}$$

Como mdc$(2, 3) =$ mdc$(2, 5) =$ mdc$(3, 5) = 1$, utilizaremos o Teorema Chinês dos Restos para solucionar o sistema de congruências:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	E $\cdot$ N $\cdot(\overline{N})^{-1}$
$y \equiv 1 \mod 2$	1	15	1	1	15
$y \equiv 2 \mod 3$	2	10	1	1	20
$y \equiv 3 \mod 5$	3	6	1	1	18

$$\begin{aligned} y &\equiv (15 + 20 + 18) \mod (2 \cdot 3 \cdot 5) \\ y &\equiv 53 \mod 30. \end{aligned}$$

Porém,

$$53 \equiv 23 \mod 30.$$

Logo:

$$y \equiv 23 \mod 30 \implies y = 30w + 23; \quad w \in \mathbb{Z}.$$

Exemplo 5.3. Resolva o seguinte sistema de congruências

$$\begin{cases} y \equiv 1 \mod 3 \\ y \equiv 2 \mod 5 \\ y \equiv 3 \mod 7. \end{cases}$$

Como $\text{mdc}(3,5) = \text{mdc}(3,7) = \text{mdc}(5,7) = 1$, utilizaremos o Teorema Chinês dos Restos para solucionar o sistema de congruências:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	$\text{E} \cdot \text{N} \cdot (\overline{N})^{-1}$
$y \equiv 1 \mod 3$	1	35	2	2	70
$y \equiv 2 \mod 5$	2	21	1	1	42
$y \equiv 3 \mod 7$	3	15	1	1	45

$$\begin{aligned} y &\equiv (70 + 42 + 45) \mod (3 \cdot 5 \cdot 7) \\ y &\equiv 157 \mod 105. \end{aligned}$$

Porém,

$$157 \equiv 52 \mod 105.$$

Logo:

$$y \equiv 52 \mod 105 \implies y = 105w + 52; \quad w \in \mathbb{Z}.$$

Exemplo 5.4. Vamos resolver o sistema de congruências

$$\begin{cases} y \equiv 1 \mod 9 \\ y \equiv 5 \mod 7 \\ y \equiv 3 \mod 5. \end{cases}$$

Como $\text{mdc}(9,7) = \text{mdc}(9,5) = \text{mdc}(7,5) = 1$, utilizaremos o Teorema Chinês dos Restos para solucionar o sistema de congruências:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	$\text{E} \cdot \text{N} \cdot (\overline{N})^{-1}$
$y \equiv 1 \mod 9$	1	35	8	8	280
$y \equiv 5 \mod 7$	5	45	3	5	1125
$y \equiv 3 \mod 5$	3	63	3	2	378

$$\begin{aligned} y &\equiv (280 + 1125 + 378) \mod (9 \cdot 7 \cdot 5) \\ y &\equiv 1783 \mod 315. \end{aligned}$$

Como,

$$1783 \equiv 208 \mod 315.$$

Logo:

$$y \equiv 208 \mod 315 \implies y = 315w + 208; \quad w \in \mathbb{Z}.$$

Exemplo 5.5. Em um cesto, há uma quantidade M 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 M a quantidade de ovos que há na cesta, assim

$$\begin{cases} M \equiv 2 \mod 3 \\ M \equiv 1 \mod 4 \end{cases}$$

Como mdc$(3, 4) = 1$, usaremos o Teorema Chinês dos Restos para resolvê -lo:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	E · N $\cdot(\overline{N})^{-1}$
$M \equiv 2 \mod 3$	2	4	1	4	32
$M \equiv 1 \mod 4$	1	3	3	3	9

$$\begin{aligned} M &\equiv (32 + 9) \mod (3 \cdot 4) \\ M &\equiv 41 \mod 12. \end{aligned}$$

Como,

$$41 \equiv 5 \mod 12.$$

Logo:

$$M \equiv 5 \mod 12 \implies M = 5w + 12; \quad w \in \mathbb{Z}.$$

Para o menor valor de M, a solução do problema é quando $w = 0$, resultando

$$\begin{aligned} M &= 12 \cdot 0 + 5 \\ M &= 5 \end{aligned}$$

Portanto, existem na cesta 5 ovos.

Exemplo 5.6. Ache um inteiro y tal que $y \equiv 3 \mod 11$, $y \equiv 5 \mod 19$, $y \equiv 10 \mod 29$. (Euler).

$$\begin{cases} y \equiv 3 \mod 11 \\ y \equiv 5 \mod 19 \\ y \equiv 10 \mod 29. \end{cases}$$

Como mdc$(11, 19)$ = mdc$(11, 29)$ = mdc$(19, 29)$ = 1, utilizaremos o Teorema Chinês dos Restos para solucionar o sistema de congruências:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	E · N $\cdot(\overline{N})^{-1}$
$y \equiv 3 \mod 11$	3	551	1	1	1653
$y \equiv 5 \mod 19$	5	319	15	14	22330
$y \equiv 10 \mod 29$	10	209	6	5	10450

$$\begin{aligned} y &\equiv (1653 + 22330 + 10450) \mod (11 \cdot 19 \cdot 29) \\ y &\equiv 34433 \mod 6061. \end{aligned}$$

Porém,

$$34433 \equiv 4128 \mod 6061.$$

Logo:

$$y \equiv 4128 \mod 6061 \implies y = 6061w + 4128; \quad w \in \mathbb{Z}.$$

Para o valor de y, a solução do problema é qualquer valor inteiro de w, então $w = 0$, resulta 4128.

Exemplo 5.7 (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 mdc$(11, 12)$ = mdc$(11, 13)$ = mdc$(12, 13)$ = 1, usaremos o Teorema Chinês dos Restos para resolvê -lo:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	E · N $\cdot(\overline{N})^{-1}$
$x \equiv 1 \mod 11$	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:

$$x \equiv 1706 \mod 1716 \implies x = 1716w + 1706; \quad w \in \mathbb{Z}.$$

Como $x < 3000$, teremos somente a solução inteira quando $w = 0$, resultando

$$\begin{aligned} x &= 1716 \cdot 0 + 1706 \\ x &= 1706 \end{aligned}$$

Portanto, a quantia que dispomos é 1706 reais.

Exemplo 5.8. Ache um inteiro x tal que $x \equiv 3 \mod 11$, $x \equiv 5 \mod 19$, $x \equiv 15 \mod 17$. (Regiomontanus - séc.XV).

$$\begin{cases} x \equiv 3 \mod 11 \\ x \equiv 5 \mod 19 \\ x \equiv 15 \mod 17. \end{cases}$$

Como $\text{mdc}(11, 19) = \text{mdc}(11, 17) = \text{mdc}(19, 17) = 1$, utilizaremos o Teorema Chinês dos Restos para solucionar o sistema de congruências:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	$\text{E} \cdot \text{N} \cdot (\overline{N})^{-1}$
$x \equiv 3 \mod 11$	3	323	4	3	2907
$x \equiv 5 \mod 19$	5	187	16	6	5610
$x \equiv 15 \mod 17$	15	209	5	7	21945

$$\begin{aligned} x &\equiv (2907 + 5610 + 21945) \mod (11 \cdot 19 \cdot 17) \\ x &\equiv 30462 \mod 3553. \end{aligned}$$

Porém,

$$30462 \equiv 2038 \mod 3553.$$

Logo:

$$x \equiv 2038 \mod 3553 \implies x = 3553w + 2038; \quad w \in \mathbb{Z}.$$

Para o valor de x, a solução do problema é qualquer valor inteiro de w, então $w = 0$, resulta 2038.

Exemplo 5.9 (**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 < x < 200, assim

$$\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5. \end{cases}$$

Como mdc$(2,3) =$ mdc$(2,5) =$ mdc$(3,5) = 1$, usaremos o Teorema Chinês dos Restos para resolvê -lo:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	E · N $\cdot(\overline{N})^{-1}$
$x \equiv 1 \mod 2$	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 5.10 (**Antigo problema chinês).** Um bando de 17 piratas, ao tentar dividir entre si, igualmente, as moedas de ouro de uma arca, verifica que 3 moedas sobrariam. Na discussão que se seguiu um dos piratas foi morto; na nova tentativa de divisão, já com um pirata a menos, desta feita 10 moedas sobrariam. Novo qüiproquo e mais um pirata é morto. Mas agora, por fim, é possível dividir igualmente a fortuna entre eles. Qual o menor número de moedas que a arca poderia conter?

Solução: Seja x a quantidade de moedas, assim

$$\begin{cases} x \equiv \quad 3 \mod 17 \\ x \equiv 10 \mod 16 \\ x \equiv \quad 0 \mod 15. \end{cases}$$

Como mdc$(17, 16) =$ mdc$(17, 15) =$ mdc$(16, 15) = 1$, usaremos o Teorema Chinês dos Restos para resolvê -lo:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	E $\cdot$ N $\cdot(\overline{N})^{-1}$
$x \equiv 3 \mod 17$	3	240	2	2	6480
$x \equiv 10 \mod 16$	10	255	15	15	38250
$x \equiv 0 \mod 15$	0	272	2	8	0

$$\begin{aligned} x &\equiv (6480 + 38250 + 0) \mod (17 \cdot 16 \cdot 15) \\ x &\equiv 44730 \mod 4080. \end{aligned}$$

Porém,

$$44730 \equiv 3930 \mod 4080$$

Logo:

$$x \equiv 3930 \mod 4080 \implies x = 4080w + 3930; \quad w \in \mathbb{Z}.$$

Para o menor valor inteiro de x, teremos somente a solução inteira quando $w = 0$, resultando

$$\begin{aligned} x &= 4080 \cdot 0 + 3930 \\ x &= 3930 \end{aligned}$$

Portanto, a quantidade de moedas é 3930.

Exemplo 5.11 (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 mdc$(3,4) =$ mdc$(3,5) =$ mdc$(4,5) = 1$, usaremos o Teorema Chinês dos Restos para resolvê -lo:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	E $\cdot$ N $\cdot(\overline{N})^{-1}$
$x \equiv 2 \mod 3$	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

$$\begin{aligned} x &\equiv (80 + 45 + 144) \mod (3 \cdot 4 \cdot 5) \\ x &\equiv 269 \mod 60. \end{aligned}$$

Como,

$$269 \equiv 29 \mod 60$$

Logo:

$$x \equiv 29 \mod 60 \implies x = 60w + 29; \quad w \in \mathbb{Z}.$$

Como $x < 50$, teremos somente a solução inteira quando $w = 0$, resultando

$$\begin{aligned} x &= 60 \cdot 0 + 29 \\ x &= 29 \end{aligned}$$

Portanto, a quantidade de alunos na turma é 29.

Exemplo 5.12. Resolva o seguinte sistema de congruências

$$\begin{cases} x \equiv 1 \mod 10 \\ x \equiv 4 \mod 11 \\ x \equiv 6 \mod 13. \end{cases}$$

Como mdc$(10,11) =$ mdc$(10,13) =$ mdc$(11,13) = 1$, utilizaremos o Teorema Chinês dos Restos para solucionar o sistema de congruências:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	E · N $\cdot(\overline{N})^{-1}$
$x \equiv 1 \mod 10$	1	143	3	7	1001
$x \equiv 4 \mod 11$	4	130	9	5	2600
$x \equiv 6 \mod 13$	6	110	6	11	7260

$$\begin{aligned} x &\equiv (1001 + 2600 + 7260) \mod (10 \cdot 11 \cdot 13) \\ x &\equiv 10861 \mod 1430. \end{aligned}$$

Como,

$$10861 \equiv 851 \mod 1430.$$

Logo:

$$x \equiv 851 \mod 1430 \implies x = 1430w + 851; \quad w \in \mathbb{Z}.$$

Exemplo 5.13 (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:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	E · N $\cdot(\overline{N})^{-1}$
$x \equiv 1 \mod 11$	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

$$\begin{aligned} x &\equiv (540 + 1782 + 2200) \mod (11 \cdot 10 \cdot 9) \\ x &\equiv 4522 \mod 990. \end{aligned}$$

Como,

$$4522 \equiv 562 \mod 990$$

Logo:

$$x \equiv 562 \mod 990 \implies x = 990w + 562; \quad w \in \mathbb{Z}.$$

Como $1000 < x < 2000$, teremos somente a solução inteira quando $w = 1$, resultando

$$\begin{aligned} x &= 990 \cdot 1 + 562 \\ x &= 1552 \end{aligned}$$

Portanto, a quantia que dispomos é de 1552 reais.

Exemplo 5.14. Resolva o seguinte sistema de congruências

$$\begin{cases} x \equiv 5 \mod 7 \\ x \equiv 8 \mod 9 \\ x \equiv 6 \mod 10. \end{cases}$$

Como mdc$(7, 9) =$ mdc$(7, 10) =$ mdc$(9, 10) = 1$, utilizaremos o Teorema Chinês dos Restos para solucionar o sistema de congruências:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	E $\cdot$ N $\cdot(\overline{N})^{-1}$
$x \equiv 5 \mod 7$	5	90	6	6	2700
$x \equiv 8 \mod 9$	8	70	7	4	2240
$x \equiv 6 \mod 10$	6	63	3	7	2646

$$\begin{aligned} x &\equiv (2700 + 2240 + 2646) \mod (7 \cdot 9 \cdot 10) \\ x &\equiv 7586 \mod 630. \end{aligned}$$

Como,

$$7586 \equiv 26 \mod 630.$$

Logo:

$$x \equiv 26 \mod 630 \implies x = 630w + 26; \quad w \in \mathbb{Z}.$$

Exemplo 5.15 (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 mdc$(2,4) = 2$, assim não teremos como usar o Teorema Chinês dos Restos envolvendo as quatro congruências, porém o mdc$(3,4) =$ mdc$(3,5) =$ mdc$(4,5) = 1$. Assim,

$$x \equiv 1 \mod 2 \quad \Longrightarrow \quad x = 2a + 1; \quad a \in \mathbb{Z}$$

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

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 4 \\ x \equiv 4 \mod 5. \end{cases}$$

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	E · N $\cdot(\overline{N})^{-1}$
$x \equiv 2 \mod 3$	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

$$\begin{aligned} x &\equiv (80 + 135 + 144) \mod (3 \cdot 4 \cdot 5) \\ x &\equiv 359 \mod 60. \end{aligned}$$

Como,

$$359 \equiv 59 \mod 60$$

Logo:

$$x \equiv 59 \mod 60 \implies x = 60w + 59; \quad w \in \mathbb{Z}.$$

Como estamos interessado no menor valor de x, assim teremos somente a solução inteira quando $w = 0$, 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 5.16. 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:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	$\text{E} \cdot \text{N} \cdot (\overline{N})^{-1}$
$x \equiv 2 \mod 3$	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

$$\begin{aligned} x &\equiv (80 + 135 + 144) \mod (3 \cdot 4 \cdot 5) \\ x &\equiv 359 \mod 60. \end{aligned}$$

Como,

$$359 \equiv 59 \mod 60$$

Logo:

$$x \equiv 59 \mod 60 \implies x = 60w + 59; \quad w \in \mathbb{Z}.$$

Portanto, temos que $x = 60w + 59 \quad \forall \quad w \in \mathbb{Z}$.

Exemplo 5.17. 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 mdc$(5,7) =$ mdc$(5,9) =$ mdc$(7,9) = 1$, usaremos o Teorema Chinês dos Restos para resolvê -lo:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	E · N $\cdot(\overline{N})^{-1}$
$x \equiv 1 \mod 5$	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.

Exemplo 5.18. Dispomos de uma quantia de reais menor do que 3000. Se distribuirmos essa quantia entre 11 pessoas, sobra 1 real, se a distribuirmos entre 12 pessoas, sobram 2 reais e se distribuirmos entre 13 pessoas, sobram 3 reais. De quantos reais dispomos?

Solução: Seja x o número natural que satisfaça o enunciado da questão, assim:

$$\begin{cases} x \equiv 1 \mod 11 \\ x \equiv 2 \mod 12 \\ x \equiv 3 \mod 13. \end{cases}$$

Como mdc$(11,12) =$ mdc$(11,13) =$ mdc$(12,13) = 1$, usaremos o Teorema Chinês dos Restos para resolvê -lo:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	E · N $\cdot(\overline{N})^{-1}$
$x \equiv 1 \mod 11$	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:

$$x \equiv 1706 \mod 1716 \implies x = 1716w + 1706; \quad w \in \mathbb{Z}.$$

Como x < 3000, teremos somente a solução inteira quando $w = 0$, resultando

$$\begin{aligned} x &= 1716 \cdot 0 + 1706 \\ x &= 1706 \end{aligned}$$

Portanto, o número natural que satisfaz o problema é 1706.

Exemplo 5.19. Um macaco, ao subir uma escada de dois em dois degraus, deixa de sobra um degrau; ao subir de três em três degraus, sobram dois degraus; e ao subir 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 o número natural que satisfaça o enunciado da questão, assim:

$$\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5. \end{cases}$$

Como mdc$(2, 3)$ = mdc$(2, 5)$ = mdc$(3, 5)$ = 1, usaremos o Teorema Chinês dos Restos para resolvê -lo:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	E · N $\cdot(\overline{N})^{-1}$
$x \equiv 1 \mod 2$	1	15	1	1	15
$x \equiv 2 \mod 3$	2	10	1	1	20
$x \equiv 3 \mod 5$	3	6	1	1	18

$$\begin{aligned} x &\equiv (15+20+18) \mod (2\cdot 3\cdot 5) \\ x &\equiv 53 \mod 30. \end{aligned}$$

Como,

$$53 \equiv 23 \mod 30$$

Logo:

$$x \equiv 23 \mod 30 \implies x = 30w + 23; \quad w \in \mathbb{Z}.$$

Como 150 < x < 200, teremos somente a solução inteira quando $w = 5$, resultando

$$\begin{aligned} x &= 30\cdot 5 + 23 \\ x &= 173 \end{aligned}$$

Portanto, o número de degraus é 173.

Exemplo 5.20. **[ENQ-2015.1]**Considere o seguinte sistema de congruências

$$\begin{cases} x \equiv 1 \mod 9 \\ x \equiv 5 \mod 7 \\ x \equiv 3 \mod 5. \end{cases}$$

(a)Encontre o menor número natural que satisfaz o sistema.

(b)Alguma solução do sistema é solução da congruência$x \equiv 926 \mod 3$?

Solução: (a) Como mdc$(9,7) =$ mdc$(9,5) =$ mdc$(7,5) = 1$, usaremos o Teorema Chinês dos Restos para resolvê -lo:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	E · N $\cdot(\overline{N})^{-1}$
$x \equiv 1 \mod 9$	1	35	8	8	280
$x \equiv 5 \mod 7$	5	45	3	5	1125
$x \equiv 3 \mod 5$	3	63	3	2	378

$$\begin{aligned} x &\equiv (280+1125+378) \mod (9\cdot 7\cdot 5) \\ x &\equiv 1783 \mod 315. \end{aligned}$$

Porém,

$$1783 \equiv 208 \mod 315$$

Logo:

$$x \equiv 208 \mod 315 \implies x = 315w + 208; \quad w \in \mathbb{Z}.$$

(b)As soluções do sistema são as soluções da congruência $x \equiv 208 \mod 315$. Logo queremos saber se o sistema de congruências:

$$\begin{cases} x \equiv 208 \mod 315 \\ x \equiv 926 \mod 3. \end{cases}$$

Possui solução. Suponhamos que existe $w \in \mathbb{Z}$ que satisfaz o sistema, isto é, existem $y, z \in \mathbb{Z}$ tais que $w - 208 = 315y$ *e* $w - 926 = 3z$. Subtraindo as equações, temos $718 = 315y - 3z$. Como a última equação não tem solução, pois $(315, 3) = 3$ não divide 718, então o sistema não tem solução. Ou seja, nenhuma solução do item (a) é solução da equação $x \equiv 926 \mod 3$.

Exemplo 5.21. **[ENQ-2016.2]**A secretaria de educação de um município recebeu uma certa quantidade é superior a 1000, inferior a 2000, que se dividi-los entre 7 escolas sobram 4, entre 9 sobram 2 e entre 13 sobram 6. Encontre a quantidade de livros.

Solução: Seja x o número natural que satisfaça o enunciado da questão, assim:

$$\begin{cases} x \equiv 4 \mod 7 \\ x \equiv 2 \mod 9 \\ x \equiv 6 \mod 13. \end{cases}$$

Como mdc$(7, 9) =$ mdc$(7, 13) =$ mdc$(9, 13) = 1$, usaremos o Teorema Chinês dos Restos para resolvê -lo:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	E · N $\cdot(\overline{N})^{-1}$
$x \equiv 4 \mod 7$	4	117	5	3	1404
$x \equiv 2 \mod 9$	2	91	1	1	182
$x \equiv 6 \mod 13$	6	63	11	6	2268

$$\begin{aligned} x &\equiv (1404 + 182 + 2268) \mod (7 \cdot 9 \cdot 13) \\ x &\equiv 3854 \mod 819. \end{aligned}$$

Como,

$$3854 \equiv 578 \mod 819$$

Logo:

$$x \equiv 578 \mod 819 \implies x = 819w + 578; \quad w \in \mathbb{Z}.$$

Como 1000 < x < 2000, teremos somente a solução inteira quando $w = 1$, resultando

$$\begin{aligned} x &= 819 \cdot 1 + 578 \\ x &= 1397 \end{aligned}$$

Portanto, quantidade de livros é 1397.

Exemplo 5.22. [**ENQ-2018.1**]O objetivo deste problema é encontrar o número natural x, menor do que 1700 e que deixe restos 2,2,1 e 0 quando dividido por 5,6,7 e 11, respectivamente. Para tanto, faça os itens a seguir:

(a)Escreva um sistema de congruências que tenha x como uma solução.

(b)Determine a solução geral do sistema do item (a)

(c)A partir da solução geral do sistema, calcule o valor de x.

Solução: (a)Temos que $0 < x < 1700$ é uma solução do seguinte sistema de congruências:

$$\begin{cases} x \equiv \quad 2 \mod 5 \\ x \equiv \quad 2 \mod 6 \\ x \equiv \quad 1 \mod 7 \\ x \equiv \ 0 \mod 11 \end{cases}$$

(b)Como $\text{mdc}(5,6) = \text{mdc}(5,7) = \text{mdc}(5,11) = \text{mdc}(6,7) = \text{mdc}(6,11) = \text{mdc}(7,11) = 1$, usaremos o Teorema Chinês dos Restos para determinar a solução geral do sistema:

	E	N	$\overline{N}$	$(\overline{N})^{-1}$	E · N $\cdot(\overline{N})^{-1}$
$x \equiv 2 \mod 5$	2	462	2	3	2772
$x \equiv 2 \mod 6$	2	385	1	1	770
$x \equiv 1 \mod 7$	1	330	1	1	330
$x \equiv 0 \mod 11$	0	210	1	1	0

$$\begin{aligned} x &\equiv (2772 + 770 + 330 + 0) \mod (5 \cdot 6 \cdot 7 \cdot 11) \\ x &\equiv 3872 \mod 2310. \end{aligned}$$

Como,

$$3872 \equiv 1562 \mod 2310$$

Logo:

$$x \equiv 1562 \mod 2310 \implies x = 2310w + 1562; \quad w \in \mathbb{Z}.$$

(c)Temos que $x < 1700$. Então o valor de $w = 0$. Portanto a solução do sistema é 1562.

Considerações Finais

Durante todo o desenvolvimento deste Trabalho de Conclusão de Curso foram pesquisados diversos exercícios sobre o teorema chinês dos restos, utilizando várias referências bibliográficas para serem apresentadas aos alunos do ensino fundamental e médio como uma atividade a ser desenvolvida em sala de aula, ou seja, levar um assunto de graduação para nível médio e fundamental e assim auxiliar no ensino e na resolução de problemas pertinentes ao Teorema Chinês dos Restos.

Todos os exemplos de exercícios do Teorema Chinês dos Restos estão citados no capítulo 5, assim como suas técnicas de resolução. Mas antes descrevemos a respeito de Números inteiros, Equações Diofantinas Lineares e Congruências como pre requisitos na resolução dos problemas do Teorema Chinês dos Restos. Esta dissertação ficará à disposição de alunos e professores que queiram se aprofundar nas resoluções de problemas que envolvem o Teorema Chinês dos Restos

Referências Bibliográficas

[1] BOYER, C. B. *História de Matemática*. São Paulo: Blucher, 2012.

[2] DICKSON, L.E.*History of theory of numbers: Divisibility and Primality*. American Mathematical Society, 1966.

[3] DING, C. *Chinese Remainder Theorem, Applications in Computing, Coding, Cryptography* 1996.

[4] DOMINGUES, H. H. *Fundamentos de aritmética*. São Paulo: Atual, 1991.

[5] GUICHARD, D. *An Introduction to Combinatorics and Graph Theory*. San francisco, 2018.

[6] HAZZAN S. *Fundamentos de Matemática Elementar*: combinatória probabilidade, v.5, 7.ed. São Paulo: Atual, 2007.

[7] HEFEZ, A. *Aritmética*: Coleção PROFMAT. Rio de Janeiro: SBM, 2016.

[8] MARTINEZ, F. B.; et al. *Teoria dos números*: um passeio com primos e outros números familiares pelo mundo inteiro, 4.ed. Rio de Janeiro: IMPA, 2015.

[9] MORGADO A. C.; CARVALHO J. B.; CARVALHO P. C.; FERNANDEZ P. *Análise Combinatória e probabilidade*. Rio de Janeiro, 2000.

[10] MELLO H. P. *Desmistificando o Ensino de Análise Combinatória*. Rio de Janeiro, 2017.

[11] MORGADO A. C.; CARVALHO P. C. *Matemática discreta*: Coleção ProfMat. Rio de Janeiro: SBM, 2013.

[12] FRANCO T. *Princípios de Combinatória e Probabilidade*. Salvador, 2017.

[13] CARVALHO P. C. *Métodos de Contagem e Probabilidade*. Rio de Janeiro, IMPA, 2015.

[14] REVISTA DO PROFESSOR DE MATEMÁTICA. Rio de Janeiro, SBM, 2007. Edição Especial.

[15] RAMÍREZ J. P. *Função Gama*. Campinas, 2015.