Universidade Estadual do Maranhão
Centro de Ciências Exatas e Tecnologia
Pós-Graduação em Matemática
Mestrado Profissional em Matemática
PROFMAT

Aritmética modular e suas aplicações: uma experiência de atuação no Ensino Básico

Filliphe de Almeida

São Luís – MA
2019

Filliphe de Almeida

Dissertação de Mestrado:

Aritmética modular e suas aplicações: uma experiência de atuação no Ensino Básico

Dissertação submetida à Coordenação Acadêmica Institucional do Programa de Mestrado Profissional em Matemática em Rede Nacional na Universidade Estadual do Maranhão, oferecido em associação com a Sociedade Brasileira de Matemática, como requisito parcial para obtenção do grau de Mestre em Matemática.

Orientador:
Profº. Dr. João Coelho Silva Filho

São Luís – MA
2019

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Núcleo Integrado de Bibliotecas/UEMA

Almeida, Filliphe de.
Aritmética modular e suas aplicações: uma experiência de atuação no Ensino Básico / Filliphe de Almeida. – 2019.
xx f.

Orientador: Profº. Dr. João Coelho Silva Filho.
Dissertação (Mestrado) - Programa de Pós–graduação em Rede - Matemática em Rede Nacional/cit, Universidade Estadual do Maranhão, UEMA, 2019.

1. Matemática. II. Título.

FILLIPHE DE ALMEIDA

Congruência modular e suas aplicações: uma experiência de atuação no Ensino Básico.

Dissertação apresentada ao PROF-MAT/Universidade Estadual do Maranhão como requisito parcial para a obtenção do grau de Mestre em Matemática.

Aprovado em

Banca Examinadora:

Profº. Dr. João Coelho Silva Filho (Orientador)
Universidade Estadual do Maranhão (UEMA)

Profº Me. Guilherme Luiz de Oliveira Neto
Instituto Federal do Piauí (IFPI)

Profº. Dr. Luís Fernando Coelho Amaral
Universidade Federal do Maranhão (UFMA)

Dedico este trabalho a toda minha família pelo apoio e por todo amor a mim ofertado. Agradeço a Deus, em primeiro lugar, por todas as experiências pelas as quais passo e que permitem que eu amadureça e cresça espiritualmente e emocionalmente. Hoje sei que não há nada que aconteça em minha vida que não seja para meu bem. Aprendi a agradecer por tudo, pois Deus saber o que faz, abençoando de alguma forma seja ela pela vitória ou pela derrota.

Agradecimentos

Agradeço primeiramente a Deus, por ter me dado força, saúde, sabedoria e disposição para conseguir superar todos os obstáculos na busca deste sonho.

Aos meus pais, Raimundo Leitão e Antônia Alice, a minha irmã e seu esposo, Gabriela e Vinicius, que sempre torceram bastante para que eu pudesse realizar este sonho e ser um homem justo e honesto.

Ao meu filho, Luis Felipe, e ao meu enteado, Olavo Neto, por todo amor e também compreensão da minha ausência em vários em busca desse sonho.

A minha amada esposa, Adriana Leitão, por todo amor e paciência nos momentos mais difíceis dessa caminhada.

Aos meus familiares pelo apoio e torcida que me fortaleceu cada dia em busca desse sonho.

Aos meus amigos, que sempre me apoiaram em busca da realização deste sonho.

Aos meus colegas de curso, pela amizade e união que me fortaleceu nos momentos mais difíceis dessa caminhada em busca deste sonho.

Ao meu orientador Prof. Dr. João Coelho por toda dedicação, paciência e apoio.

Aos meus companheiros de lutas e viagens, Washington e Jálio, pela força e apoio nos momentos mais difíceis dessa caminha em busca deste sonho, vocês foram fundamentais para tudo isso.

À UEMA por me acolher com todos os excelentes profissionais que amam essa instituição e se dedicam como se fossem as suas casas.

À CAPES por dar oportunidade de melhorar minha vida tanto profissional como pessoal, propiciando um mestrado de excelência , como é o PROFMAT. A minha gratidão a todos!

Resumo

O foco principal do trabalho é o Teorema Chinês dos Restos, apresentando os fundamentos e aplicações elementares, mostrando as utilidades do Teorema, priorizando a aplicação na Educação Básica e a importância teórica e prática para os alunos e professores interessados num aprendizado aprofundado da Teoria dos Números. Para apresentar um melhor entendimento do Teorema Chinês dos Restos são abordados tópicos preliminares dos Números Inteiros, necessários para a construção do Teorema. As Equações Diofantinas e os Critérios de Divisibilidade são mostrados e solucionados por aplicações otimizadas das propriedades e dos resultados de Congruência. O Teorema é utilizado para resoluções de provas da OBMEP, da OBM e processos seletivos. O trabalho é um suporte para os professores e alunos que necessitam aprimorar seus estudos e pesquisas sobre os Números Inteiros e suas aplicações básicas.

Palavras-chave: Algoritmo de Euclides, Congruência Linear, Critérios de Divisibilidade Modular, Equação Diofantina, Teorema do Resto Chinês.

Abstract

The main focus of the work is the Chinese Theorem of Remnants, presented the fundamentals and elementary applications, showing the utilities of the Theorem, prioritizing the application in Basic Education and the theoretical and practical importance for students and teachers who are interested in learning more of Number Theory. To present a better understanding of the theorem Chinese of the Remains are covered preliminary topics of the Whole Numbers, necessary for the construction of Theorem. Diophantine Equations and Divisibility criteria are shown and solved by applications. optimized congruence properties and results. The theorem is used for OBMEP, OBM proof testing and selection processes. The work is a support for teachers and students who use improve their studies and research on integer numbers and their basic applications.

Keywords: Euclid's algorithm, Linear Congruence, Modular Divisibility Criteria, Diophantine Equation, Chinese Rest Theorem.

Sumário

1 Introdução

A Aritmética é o termo que deriva do grego Arithmos, que significa número, sendo reconhecida como a ciência dos números. A humanidade percorreu longos caminhos para chegar a teoria dos números. No ínicio da humanidade, para ajudar no processo de contagem, eram usados pedaços de pau, pedras e ossos para registrar certas quantidades. Daí, os números e os símbolos que representavam, passaram por grandes mudanças ao longo dos anos e chegando ao modo em que são utilizadas na atualidade.

Uma das ferramentas mais importantes na teoria dos números é a aritmética modular, pois a mesma envolve o conceito de congruência. Onde suas bases teóricas foram iniciadas pelo matemático suíço Euler, em meados de 1750, tornando-se mais acessível através das ideias do matemático alemão Carl Friedrich Gauss, publicado no livro Disquisitiones Arithmetcae, no ano de 1801, na qual simbologias, definições e conceitos foram construídos.

A motivação da escolha do tema Aritmética modular e suas aplicações: uma experiência de atuação no Ensino Básico, para esta dissertação foi o diverso problema na resolução de questões aplicadas a divisibilidade, as Equações Diofantinas Lineares e ao sistema de congruência, quando se aplica o Teorema Chinês do Resto. E com o uso da Congruência Modular, as dificuldades no processo de resolução foram diminuída.

No capítulo 2, é apresentado um estudo sobre Noções sobre Teoria dos Números, apresentando definições, teoremas, propriedades, proposições, exemplificações e demonstrações que servirão de base para fundamentar as aplicações, abordadas ao longo do trabalho.

No capítulo 3, é apresentado uma abordagem da congruência modular na divisibilidade de um modo mais específico no que refere–se a aplicação nos critérios de divisibilidade mais utilizado na educação básica, principalmente ensino fundamental e ensino médio, demonstrando e exemplificando a cada um dos critérios utilizando a congruência modular de modo mais simplificado e aplicações nos dígitos verificadores.

No capítulo 4, é feita uma apresentação da equação diofantina linear ao qual será apresentada a definição, teoremas, exemplos, resolução de equação diofantina linear por algoritmo de Euclides e também a resolução por um método mais prático que é a utilização da congruência modular, encontrando sempre a solução minimal da equação.

Logo, o capítulo 5, será apresentado o Teorema Chinês do Resto, onde primeiro será feita uma abordagem sobre congruência linear, posteriormente uma abordagem sobre sistema de congruência modular e por fim uma apresentação do Teorema Chinês do Resto tendo resolução de problemas de ensino fundamental e ensino médio, principal teorema na resolução de sistemas de congruência linear.

Por fim, nas considerações finais, será feita uma apresentação no que refere–se a aplicação de congruência modular. Sendo assim, expondo a importância da abordagem desse tema na educação básica, pois facilitará no processo de ensino–aprendizagem.

2 Teoria dos Números

Neste capítulo é definido divisibilidade entre dois inteiros quaiquer e demonstrado algumas proriedades que servirão de base para a demostração e resolução de uma Equação Diofantina Linear e posteriormente para o Teorema Chinês dos Restos. Enunciado e demostrado o Teorema de Eudoxius, que servirá para a demostração do Algoritmo da Divisão de Euclides. Também será falado sobre o máximo divisor comum e mínimo múltiplo comum entre dois inteiros quaisquer. O capítulo está fundamentado em Alencar Filho (1981), Hefez (2016), Ribenboim (2014) e Santos (2009).

2.1 Divisibilidade

Definição 2.1. *Sejam* $\mathfrak{a}$ *e* $\mathfrak{b}$ *dois inteiros, com* $\mathfrak{a} \neq 0$. *Diz-se que* $\mathfrak{a}$ *divide* $\mathfrak{b}$*, e escreve-se* $\mathfrak{a} \mid \mathfrak{b}$ *se, e somente se, exite um inteiro* $\mathfrak{q}$ *tal que*

$$\mathfrak{b} = \mathfrak{a} \cdot \mathfrak{q}. \tag{2.1}$$

Neste caso, diz-se que $\mathfrak{a}$ divide $\mathfrak{b}$, que $\mathfrak{a}$ é divisor de $\mathfrak{b}$, $\mathfrak{b}$ é um múltiplo de $\mathfrak{a}$, $\mathfrak{a}$ é um fator de $\mathfrak{b}$, ou que $\mathfrak{b}$ é divisivel por $\mathfrak{a}$. Escreve-se $\mathfrak{a} \nmid \mathfrak{b}$ para indicar que $\mathfrak{a}$ não divide $\mathfrak{b}$, significando que não existe nenhum número inteiro $\mathfrak{q}$ tal que $\mathfrak{b} = \mathfrak{a} \cdot \mathfrak{q}$.

Se $\mathfrak{a}$ é divisor de $\mathfrak{b}$, então $(-\mathfrak{a})$ também será divisor de $\mathfrak{b}$, pois por (2.1) implica que $\mathfrak{b} = (-\mathfrak{a}) \cdot (-\mathfrak{q})$, com $\mathfrak{q} \in \mathbb{Z}$, assim para qualquer inteiro existem dois a dois iguais em valor absoluto e de sinais opostos.

Exemplo 2.1. *Note que* $-6 \mid 30$*, pois* $30 = (-6) \cdot (-5)$*, e ainda que* $7 \nmid 50$*, pois não existe um* $\mathfrak{q} \in \mathbb{Z}$*, tal que* $50 = 7 \cdot \mathfrak{q}$.

Teorema 2.1. *Quaisquer que sejam os inteiros* $\mathfrak{a}$*,* $\mathfrak{b}$*,* $\mathfrak{c}$ *e* $\mathfrak{d}$*, tem–se:*

1. $\mathfrak{a} \mid 0, \quad 1 \mid \mathfrak{a} \quad e \quad \mathfrak{a} \mid \pm\mathfrak{a}$;
2. *Se* $\mathfrak{a} \mid 1$*, então* $\mathfrak{a} = \pm 1$;

3. *Se* $a \mid b \quad e \quad c \mid d$*, então* $ac \mid bd$*;*

4. *Se* $a \mid b \quad e \quad b \mid c$*, então* $a \mid c$*;*

5. *Se* $a \mid b \quad e \quad b \mid a$*, então* $a = \pm b$*;*

6. *Se* $a \mid b$ *com* $b \neq 0$*, então* $|a| \leqslant |b|$*;*

7. *Se* $a \mid b \quad e \quad a \mid c$*, então* $a \mid (bx + cy)$*, para todo* x *e* y *inteiros.*

Demonstração. (1) Pela definição, se $a \mid 0$, então existe $q_1 \in \mathbb{Z}$ tal que $0 = a \cdot q_1$, basta fazer, $q_1 = 0$, pois consequentemente $0 = a \cdot 0$; se $1 \mid a$, então existe $q_2 \in \mathbb{Z}$ tal que $a = 1 \cdot q_2$, assim $q_2 = a$ e $a = 1 \cdot a$; se $a \mid a$ então existe $q_3 \in \mathbb{Z}$ tal que $a = a \cdot q_3$, assim $q_3 = 1$ e $a = a \cdot 1$;

(2) Se $a \mid 1$, então existe um $q \in \mathbb{Z}$ tal que $1 = a \cdot q$ implicando nas seguintes possibilidades: $a = 1$ e $q = 1$ ou $a = -1$ e $q = -1$. Logo $a = \pm 1$.

(3) Se $a \mid b \quad e \quad c \mid d$, então

$$b = a \cdot q_1, \text{ com } q_1 \in \mathbb{Z}, \tag{2.2}$$

$$d = c \cdot q_2, \text{ com } q_2 \in \mathbb{Z}. \tag{2.3}$$

Multiplicando membro a membro em (2.2) e (2.3), tem–se

$$b \cdot d = (a \cdot c)(q_1 \cdot q_2) \Longrightarrow ac \mid bd.$$

(4) Se $a \mid b \quad e \quad b \mid c$, então

$$b = a \cdot q_1, \text{ com } q_1 \in \mathbb{Z}, \tag{2.4}$$

$$c = b \cdot q_2, \text{ com } q_2 \in \mathbb{Z}. \tag{2.5}$$

Multiplicando membro a membro em (2.4) e (2.5), tem–se

$$b \cdot c = (a \cdot b)(q_1 \cdot q_2) \Longrightarrow c = a(q_1 \cdot q_2) \Longrightarrow a \mid c.$$

(5) Se $a \mid b \quad e \quad b \mid a$, então

$$b = a \cdot q_1, \text{ com } q_1 \in \mathbb{Z}, \tag{2.6}$$

$$a = b \cdot q_2, \text{ com } q_2 \in \mathbb{Z}. \tag{2.7}$$

Substituindo (2.6) em (2.7),

$$a = a(q_1q_2) \Rightarrow q_1q_2 = 1 \Rightarrow q_1 \mid 1.$$

Pelo item 2 implica que $q_1 = \pm 1$ e $a = \pm b$.

(6) Se $a \mid b$ com $b \neq 0$, então existe um $q \in \mathbb{Z}$ tal que $b = a \cdot q$, aplicando o módulo em ambos os membros tem–se que

$$|b| = |a \cdot q| = |a| \cdot |q|. \tag{2.8}$$

Como $q \neq 0$ e $b \neq 0$, tem–se que $1 \leqslant |q|$. Multiplicando por $|a|$, tem–se

$$|a| \leqslant |q| \cdot |a|. \tag{2.9}$$

Logo de (2.8) e (2.9) obtem-se que $|a| \leqslant |b|$.

(7) Se $a \mid b \quad e \quad se \quad a \mid c$, então

$$b = a \cdot q_1, \text{ com } q_1 \in \mathbb{Z}, \tag{2.10}$$

$$d = c \cdot q_2, \text{ com } q_2 \in \mathbb{Z}. \tag{2.11}$$

Portanto, quaisquer que sejam os inteiros x e y, multiplicando (2.10) por x e (2.11) por y e somando membro a membro obtem–se:

$$bx + cy = aq_1x + aq_2y = a(q_1x + q_2y),$$

e $a \mid (bx + cy)$, para todo x e y inteiros. □

Exemplo 2.2. *Sejam* a *e* b *inteiro. Mostre que se* $a \mid b$ *e* $a \mid c$*, então* $a^2 \mid bc$*.*

Solução: Se $a \mid b \quad e \quad se \quad a \mid c$, então

$$b = a \cdot q_1, \text{ com } q_1 \in \mathbb{Z}, \tag{2.12}$$

$$c = a \cdot q_2, \text{ com } q_2 \in \mathbb{Z}. \tag{2.13}$$

Portanto, multiplicando ambos os membros de (2.12) e (2.13), obtem–se:

$$b \cdot c = a \cdot a \cdot (q_1 \cdot q_2) \Rightarrow b \cdot c = a^2 \cdot (q_1 \cdot q_2).$$

Logo, $a^2 \mid bc$.

Exemplo 2.3. *Prove que o número* $N = 5^{45362} - 7$ *não é divisível por* 5*.*

Solução: Suponhamos, por absurdo, que o número N seja divisível por 5. Logo, pela definição, existe um número inteiro q tal que $5^{45362} - 7 = 5 \cdot \mathsf{q}$. Logo,

$$\begin{aligned} 7 &= 5^{45362} - 5\mathsf{q} \\ &= 5 \cdot (5^{45361} - \mathsf{q}) \\ &= 5\mathsf{q}', \end{aligned}$$

com $\mathsf{q}' = 5^{45361} - \mathsf{q} \in \mathbb{Z}$, ou seja, 7 seria divisível por 5, o que é um absurdo.

Para um número inteiro $\mathfrak{a}$, $\mathrm{D}(\mathfrak{a})$ indica o conjunto de todos os divisores inteiros de $\mathfrak{a}$, ou seja,

$$\mathrm{D}(\mathfrak{a}) = \{\mathfrak{x} \in \mathbb{Z}^\star; \quad \mathfrak{x} \mid \mathfrak{a}\},$$

com $\mathbb{Z}^\star$ o conjunto dos inteiros não nulos. Como mencionado, se $\mathfrak{x}$ é divisor de $\mathfrak{a}$, então $(-\mathfrak{a})$ também é um divisor de $\mathfrak{x}$. Portanto, $\mathrm{D}(\mathfrak{a}) = \mathrm{D}(-\mathfrak{a})$, e dessa forma

$$\mathfrak{a} = \mathfrak{a} \cdot 1 = (-\mathfrak{a}) \cdot (-1).$$

Segue que 1, -1, $\mathfrak{a}$ e $-\mathfrak{a}$ são divisores de $\mathfrak{a}$, esses divisores são chamados de divisores triviais de $\mathfrak{a}$. Qualquer que seja o inteiro $\mathfrak{a}$ não nulo, se $\mathfrak{x} \mid \mathfrak{a}$, então

$$-\mathfrak{a} \leqslant \mathfrak{x} \leqslant \mathfrak{a} \quad \text{e} \quad \mathrm{D}(\mathfrak{a}) \subset [-\mathfrak{a},\ \mathfrak{a}].$$

Portanto, qualquer inteiro $\mathfrak{a} \neq 0$ tem um número finito de divisores.

Definição 2.2. *Sejam* $\mathfrak{a}$ *e* $\mathfrak{b}$ *dois inteiros e* $\mathfrak{d} \neq 0$*, chamamos de divisor comum dos inteiros* $\mathfrak{a}$ *e* $\mathfrak{b}$ *um inteiro* $\mathfrak{d}$ *tal que* $\mathfrak{d} \mid \mathfrak{a}$ *e* $\mathfrak{d} \mid \mathfrak{b}$*.*

Dizer que $\mathfrak{d}$ é divisor comum de dois inteiros $\mathfrak{a}$ e $\mathfrak{b}$ então $\mathfrak{d}$ pertence simultaneamente aos conjuntos $\mathrm{D}(\mathfrak{a})$ e $\mathrm{D}(\mathfrak{b})$, indicando por $\mathrm{D}(\mathfrak{a}, \mathfrak{b})$, ou seja:

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

pode-se afirmar ainda que $\mathrm{D}(\mathfrak{a}, \mathfrak{b}) = \mathrm{D}(\mathfrak{a}) \cap \mathrm{D}(\mathfrak{b})$.

Dois inteiros $\mathfrak{a}$ e $\mathfrak{b}$ quaisquer admite sempre -1 e 1 como divisores comuns, dessa forma segue–se que o conjunto $\mathrm{D}(\mathfrak{a}, \mathfrak{b})$ dos divisores comuns $\mathfrak{a}$ e $\mathfrak{b}$ nunca é vazio, ou seja, $\mathrm{D}(\mathfrak{a}, \mathfrak{b}) \neq \emptyset$. Em particular, se $\mathfrak{a} = \mathfrak{b} = 0$, então todo inteiro não nulo é um divisor comum de $\mathfrak{a}$ e $\mathfrak{b}$, isto é, $\mathrm{D}(\mathfrak{a}, \mathfrak{b}) = \mathbb{Z}^\star$.

Exemplo 2.4. *Determine todos os divisores comuns dos inteiros* $\mathfrak{a} = 12$ *e* $\mathfrak{b} = -18$*.*

Solução: Temos que $D(12) = \{\pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 6,\ \pm 12\}$ e $D(-18) = \{\pm 1,\ \pm 2,\ \pm 3,\ \pm 6,\ \pm 9, \pm 18\}$. Logo,

$$D(12, -18) = D(12) \cap D(-18) = \{\pm 1,\ \pm 2,\ \pm 3,\ \pm 6\}.$$

2.1.1 Algoritmo da Divisão

O Algoritmo da Divisão, conhecido também como Divisão Euclidiana, é um dos resultados mais importantes da Teoria dos Números de fácil entendimento e aplicação. É estudado desde o Ensino Fundamental, passando pelo Ensino Médio e chagando no Ensino Superior onde é abordado de forma mais geral. Esse resultado é atribuído a Euclides, que aparece no livro VII dos Elementos de Euclides, escrito por volta do ano 300 a.C.

Teorema 2.2 (Eudoxius)**.** *Considere* a *e* b *inteiros com* $b \neq 0$*. Então* a *é múltiplo de* b *ou se encontra entre dois múltiplos consecutivos de* b*, isto é, correspondendo a cada par de inteiros* a *e* $b \neq 0$ *existe um inteiro* q *tal que,*

$$qb \leqslant a < (q+1)b, \tag{2.14}$$

para $b > 0$ *e*

$$qb \leqslant a < (q-1)b, \tag{2.15}$$

para $b < 0$*.*

Demonstração. Suponha que $a > 0$ e $b > 0$. Deste modo, existem duas possibilidades:

1. Se $a = q \cdot b$, para algum $q \in \mathbb{Z}$ não há o que provar e o resultado segue;
2. Se $a \neq q \cdot b\ \forall q \in \mathbb{Z}$, existe um menor inteiro k que satisfaz a condição: $a < k \cdot b$.

Segue que $(k-1)b < a$. De fato, se $a < (k-1)b$ o que é uma contradição, pois uma vez que $a < k \cdot b$ e p é o menor inteiro em que isto ocorre. Portanto, deve-se ter $(k-1)b < a < k \cdot b$. Tomando $q = k - 1$, obtem–se

$$q \cdot b \leqslant a < (q+1)b.$$

Os casos em que $a < 0$ ou $b < 0$ podem ser demonstrados de forma análoga. □

Exemplo 2.5. *Para* $a = 17$ *e* $b = 4$*, tomando* $q = 4$*,*

$$4 \cdot 4 \leqslant 17 < (4+1) \cdot 4 \Longrightarrow 4 \cdot 4 \leqslant 17 < 5 \cdot 4.$$

Para $\mathfrak{a} = -17$ *e* $\mathfrak{b} = 4$*, escolhe–se* $\mathfrak{n} = -5$*,*

$$(-5) \cdot 4 \leqslant -17 < (-5+1) \cdot 4 \Longrightarrow (-5) \cdot 4 \leqslant -17 < (-4) \cdot 4.$$

Para $\mathfrak{a} = 25$ *e* $\mathfrak{b} = -2$*, fazendo* $\mathfrak{n} = -13$*,*

$$(-13) \cdot (-2) \leqslant 25 < (-13-1) \cdot (-2) \Longrightarrow (-13) \cdot (-2) \leqslant 25 < (-14) \cdot (-2).$$

O exemplo torna fácil e prático para abordar o Algoritmo da Divisão de Euclides.

Teorema 2.3 (Algoritmo da Divisão de Euclides)**.** *Dados dois inteiros* $\mathfrak{a}$ *e* $\mathfrak{b}$*, com* $\mathfrak{b} > 0$*, existem e são único os inteiros* $\mathfrak{q}$ *e* $\mathfrak{r}$ *tais que*

$$\mathfrak{a} = \mathfrak{q}\mathfrak{b} + \mathfrak{r}, \text{ com } 0 \leqslant \mathfrak{r} < \mathfrak{b}.$$

Os inteiros $\mathfrak{q}$ *e* $\mathfrak{r}$ *são chamados respectivamente de quociente e resto e* $\mathfrak{r} = 0$ *se, e somente se,* $\mathfrak{b}$ *é divisor de* $\mathfrak{a}$*, ou seja,* $\mathfrak{b} \mid \mathfrak{a}$*.*

Demonstração. Pelo Teorema de Eudoxius, como $\mathfrak{b} > 0$, existe um $\mathfrak{q} \in \mathbb{Z}$ satisfazendo

$$\mathfrak{q}\mathfrak{b} \leqslant \mathfrak{a} < (\mathfrak{q}+1)\mathfrak{b},$$

o que implica $0 \leqslant \mathfrak{a} - \mathfrak{q}\mathfrak{b}$ e $\mathfrak{a} - \mathfrak{q}\mathfrak{b} < \mathfrak{b}$. Desta forma, se fazer $\mathfrak{r} = \mathfrak{a} - \mathfrak{q}\mathfrak{b}$, tem–se garantida, a existência de $\mathfrak{q}$ e $\mathfrak{r}$. A fim de mostrar a unicidade, supondo a existência de outro par $\mathfrak{q}_1$ e $\mathfrak{r}_1$, verificando

$$\mathfrak{a} = \mathfrak{q}_1\mathfrak{b} + \mathfrak{r}_1 \quad \text{com} \quad 0 \leqslant \mathfrak{r}_1 < \mathfrak{b}.$$

Assim $(\mathfrak{q}\mathfrak{b} + \mathfrak{r}) - (\mathfrak{q}_1\mathfrak{b} + \mathfrak{r}_1) = 0$, isto é $\mathfrak{b}(\mathfrak{q} - \mathfrak{q}_1) = \mathfrak{r}_1 - \mathfrak{r}$, o que implica $\mathfrak{b} \mid (\mathfrak{r}_1 - \mathfrak{r})$. Mas, como $\mathfrak{r}_1 < \mathfrak{b}$ e $\mathfrak{r} < \mathfrak{b}$, temos $|\mathfrak{r}_1 - \mathfrak{r}| < \mathfrak{b}$ e, portanto, como $\mathfrak{b} \mid (\mathfrak{r}_1 - \mathfrak{r})$ tem–se $\mathfrak{r}_1 - \mathfrak{r} = 0$ o que permite concluir que $\mathfrak{r} = \mathfrak{r}_1$. Logo $\mathfrak{q}_1\mathfrak{b} = \mathfrak{q}\mathfrak{b}$ e daí $\mathfrak{q}_1 = \mathfrak{q}$, uma vez que $\mathfrak{b} \neq 0$. □

Corolário 2.1. *Se* $\mathfrak{a}$ *e* $\mathfrak{b}$ *são dois inteiros, com* $\mathfrak{b} \neq 0$*, existem e são únicos os inteiros* $\mathfrak{q}$ *e* $\mathfrak{r}$ *que satisfazem as condições:*

$$\mathfrak{a} = \mathfrak{q}\mathfrak{b} + \mathfrak{r}, \text{ com } 0 \leqslant \mathfrak{r} < |\mathfrak{b}|.$$

Demonstração. Se $\mathfrak{b} > 0$, nada há para demostrar, e se $\mathfrak{b} < 0$, então $|\mathfrak{b}| > 0$, e por conseguinte existem e são únicos os inteiros $\mathfrak{q}_1$ e $\mathfrak{r}$ tais que

$$\mathfrak{a} = \mathfrak{q}_1|\mathfrak{b}| + \mathfrak{r}, \text{ com } 0 \leqslant \mathfrak{r} < |\mathfrak{b}|,$$

ou seja, por ser $|b| = -b$, para $b < 0$:

$$a = q_1(-b) + r \Rightarrow a = (-q_1)b + r, \text{ com } 0 \leqslant r < |b|.$$

Portanto, existe e são únicos os inteiros $q = q_1$ e r tais que

$$a = qb + r, \text{ com } 0 \leqslant r < |b|.$$

□

Exemplo 2.6. *Ache o quociente* q *e o resto* r *na divisão de* $a = 53$ *por* $b = -13$ *que satisfazem às condições do algoritmo da divisão.*

Solução: Efetuando a divisão usual dos valores absolutos de a e b, obtem–se:

$$53 = 13 \cdot 4 + 1 \Rightarrow 53 = (-13) \cdot (-4) + 1,$$

onde $0 \leqslant 1 < |-13|$. Logo, o quociente $q = -4$ e o resto $r = 1$.

Exemplo 2.7. *Ache o quociente* q *e o resto* r *na divisão de* $a = -89$ *por* $b = 11$ *que satisfazem às condições do algoritmo da divisão.*

Solução: Efetuando a divisão usual dos valores absolutos de a e b, obtem–se:

$$89 = 11 \cdot 8 + 1 \Rightarrow -89 = 11 \cdot (-8) - 1.$$

Como $r = -1 < 0$ não satisfaz à condição $0 \leqslant r < |11|$, somando e subtraindo o valor de 11 de b ao segundo membro da igualdade anterior, tem–se:

$$-89 = 11 \cdot (-8) + (-11) + 11 - 1 \Rightarrow -89 = 11 \cdot (-9) + 10,$$

e $0 \leqslant 10 < 11$. Logo, o quociente $q = -8$ e o resto $r = 10$.

Dividindo por um inteiro qualquer a por $b = 2$, existem duas possibilidades para os restos: r = 0 ou r = 1. Se $r = 0$ então $a = 2q$ e é denominado par; se $r = 1$ então $a = 2q + 1$, e é denomindado ímpar.

Observe–se que

$$a^2 = (2q)^2 = 4q^2 \quad \text{ou} \quad a^2 = (2q + 1)^2 = 4(q^2 + q) + 1$$

de modo que na divisão do quadrado a^2 de um inteiro a por 4 o resto é 0 ou 1.

Exemplo 2.8. *Mostrar que o quadrado de um inteiro qualquer é da forma* $3k$ *ou* $3k + 1$.

Solução: Dado um inteiro qualquer a, temos que de acordo com o Algoritmo da Divisão:

$$a = 3q + r, \text{ com } 0 \leqslant r < 3,$$

ou seja, o número inteiro a pode assumir as seguintes formas: $a = 3q$ ou $a = 3q + 1$ ou $a = 3q + 2$.

(i). Se $a = 3q$, então, $a^2 = (3q)^2 = 9q^2 = 3 \cdot (3q^2) = 3k$, com $k = 3q^2$.

(ii). Se $a = 3q + 1$, então,

$$\begin{aligned} a^2 = (3q+1)^2 &= 9q^2 + 6q + 1 \\ &= 3 \cdot (3q^2 + 2q) + 1 \\ &= 3k + 1, \quad \text{com} \quad k = 3q^2 + 2q. \end{aligned}$$

(iii). Se $a = 3q + 2$, então,

$$\begin{aligned} a^2 = (3q+2)^2 &= 9q^2 + 12q + 4 \\ &= 9q^2 + 12q + 3 + 1 \\ &= 3 \cdot (3q^2 + 4q + 1) + 1 \\ &= 3k + 1, \quad \text{com} \quad k = 3q^2 + 4q + 1. \end{aligned}$$

Logo, a^2 terá uma das formas, $3k$ ou $3k + 1$.

Exemplo 2.9. *Mostrar que o cubo de um inteiro qualquer é de uma das formas* $9k$, $9k+1$ *ou* $9k + 8$.

Solução: Dado um inteiro qualquer a, pelo o Algoritmo da Divisão:

$$a = 3q + r, \text{ com } 0 \leqslant r < 3,$$

ou seja, o número inteiro a pode assumir as seguintes formas: $a = 3q$ ou $a = 3q + 1$ ou $a = 3q + 2$.

Para $a = 3q$, então $a^3 = (3q)^3 = 27q^3 = 9 \cdot (q^3) = 9k$.

Para $a = 3q + 1$, então

$$\begin{aligned} a^3 = (3q+1)^3 &= (3q)^3 + 3 \cdot (3q)^2 \cdot 1 + 3 \cdot (3q) \cdot 1^2 + 1^3 \\ &= 27q^3 + 27q^2 + 9q + 1 \\ &= 9 \cdot (3q^3 + 3q^2 + q) + 1 \\ &= 9k + 1. \end{aligned}$$

Se $a = 3q + 2$, então

$$\begin{aligned} a^3 = (3q+2)^3 &= (3q)^3 + 3 \cdot (3q)^2 \cdot 2 + 3(3q) \cdot 2^2 + 2^3 \\ &= 27q^3 + 54q^2 + 36q + 8 \\ &= 9 \cdot (3q^3 + 6q^2 + 4q) + 8 \\ &= 9k + 8. \end{aligned}$$

Portanto, o cubo de um inteiro qualquer é das seguintes formas: $9k$, $9k + 1$ ou $9k + 8$.

2.2 Máximo Divisor Comum

Definição 2.3. *Sejam* a *e* b *dois inteiros não conjuntamente nulos (*$a \neq 0$ *ou* $b \neq 0$*). Chamamos de máximo divisor comum de* a *e* b *o inteiro positivo* d *que satisfaz às seguintes condições:*

1. $d \mid a$ *e* $d \mid b$
2. *Se* $c \mid a$ *e* $c \mid a$*, então* $c \leqslant d$.

O máximo divisor comum de a e b é indicado por:

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

é imediato que $mdc(a, b) = mdc(b, a)$. Também é imediato os seguintes casos:

1. O $mdc(0, 0)$ não existe;
2. O $mdc(a, 1) = 1$;
3. Se $a \neq 0$, então o $mdc(a, 0) = |a|$;
4. Se $a \neq 0$, então o $mdc(a, a) = |a|$;

5. Se $a \mid b$, então o $mdc(a, b) = |a|$.

Em particular, é imediato verificar que:

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

Teorema 2.4. *Seja* d *o máximo divisor comum entre* a *e* b*, então existem inteiros* x *e* y *tais que*

$$mdc(a, b) = ax + by, \tag{2.16}$$

isto é, o $mdc(a, b)$ *é uma combinação linear de* a *e* b*.*

Demonstração. Considere S o conjunto de todas as combinações lineares $ma + nb$ onde m e n são inteiros, isto é,

$$S = \{ma + nb \mid am + nb > 0 \text{ e } m, n \in \mathbb{Z}\}.$$

Este conjunto $S \neq \emptyset$ pois, existem números negativos, positivos e também o zero. Escolhendo m_0 e n_0 tais que $c = m_0a + n_0b$ seja o menor inteiro positivo pertencente ao conjunto S. Como $d = mdc(a, b)$, pelo Teorema Algoritmo da Divisão de Euclides, existem q e r tais que

$$a = qc + r \quad \text{com} \quad 0 \leqslant r < c.$$

Assim,

$$r = a - qc = a - q(m_0a + n_0b) = (1 - qm_0)a + (-qn_0)b,$$

isto é, o resto r é uma combinação linear de a e b. Isto mostra que $r \in S$, pois $(1 - qm_0)$ e $(-qn_0)$ são inteiros, como $0 \leqslant r < c$ e $c > 0$ é o elemento mínimo de S, então $r = 0$ e $a = qc$, ou seja, $c \mid a$.

De forma análoga se prova que $c \mid b$, logo, c é um divisor comum positivo de a e b. Por outro lado d também é um divisor comum positivo de a e b, então existem inteiros k_1 e k_2 tais que $a = k_1d$ e $b = k_2d$ e, portanto,

$$\begin{aligned} c &= m_0a + n_0b \\ &= m_0(k_1d) + n_0(k_2d) \\ &= d(m_0k_1 + n_0k_2), \end{aligned}$$

ou seja, $d \mid c$ e $c > 0$, tem-se $d \leqslant c$, visto que se $d < c$ não é possível, isto é, d é o maior

divisor comum positivo de a e b, conclui-se que $d = c$, logo,

$$d = mdc(a, b) = m_0 a + n_0 b.$$

□

A demostração desse teorema mostra que o mdc(a,b) é o menor inteiro positivo da forma ax + by, isto é que pode ser expresso como combinação linear de a e b. Mas essa combinação linear não é única pois,

$$mdc(a, b) = d = a(x + bt) + b(y - at)$$

para qualquer que seja o inteiro t.

Note que, se

$$d = ax_0 + by_0 \tag{2.17}$$

para algum par de inteiro x_0 e y_0, então d não é necessariamente o $mdc(a, b)$. Assim, se

$$mdc(a, b) = ax + by,$$

então

$$t \cdot mdc(a, b) = t \cdot (ax) + t \cdot (by),$$

para todo inteiro t, mostrado na expressão (2.17), com $d = t \cdot mdc(a, b)$ e $x_0 = tx$ e $y_0 = ty$.

Exemplo 2.10. *Dados os inteiros* $a = 18$ *e* $b = 6$*, tem-se que*

$$mcd(18, 6) = 6 \Rightarrow 18x + 6y = 6. \tag{2.18}$$

Tomando $x_0 = 1$ *e* $y_0 = -2$ *tem–se* $18 \cdot 1 + 6 \cdot (-2) = 6$*. Em geral, todos os pares de inteiros* (x_0, y_0) *que satisfazem a equação (2.18) pode ser obtido por:*

$$x = 1 + k \quad e \quad y = -2 - 3k,$$

com $k \in \mathbb{Z}$*, nota-se que* $18(1 + k) + 6(-2 - 3k) = 6$*. Este assunto será entendido com mais detalhes na seção de equações diofantinas lineares.*

2.3 Algoritmo de Euclides

Lema 2.1. *Se* $a = bq + r$*, então* $mdc(a, b) = mdc(b, r)$.

Demonstração. Se o $\mathtt{mdc}(a, b) = d$, então pela definição de Máximo Divisor Comum $d \mid a$ e $d \mid b$, o que implica $d \mid (a - bq)$ ou $d \mid r$, isto é, d é um divisor comum de b e r, pois $d \mid b$ e $d \mid r$.

Por outro lado, se c é um divisor comum qualquer de b e r, ou seja, $c \mid b$ e $c \mid r$, então $c \mid (bq + r)$ ou $c \mid a$, isto é, c um divisor comum de a e b, o que segue que $c \leqslant d$, pois $\mathtt{mdc}(a, b) = d$. Logo, desse modo $\mathtt{mdc}(b, r) = d$. □

Sejam a e b dois inteiros tais que $a \neq 0$ ou $b \neq 0$ cujo máximo divisor comum se deseja determinar, segue de imediato da definição que $\mathtt{mdc}(a, b) = \mathtt{mdc}(|a|, |b|)$, tomando a e b inteiros positivos distintos, se a > b, tais que b não divide a, isto é, $b \nmid a$. Dessa forma, aplicando repetidas vezes o algoritmo da divisão obtem–se as igualdades:

$$\begin{aligned}
a &= bq_1 + r_1, \quad \text{com} \quad 0 < r_1 < b;\\
b &= r_1q_2 + r_2, \quad \text{com} \quad 0 < r_2 < r_1;\\
r_1 &= r_2q_3 + r_3, \quad \text{com} \quad 0 < r_3 < r_2;\\
r_2 &= r_3q_4 + r_4, \quad \text{com} \quad 0 < r_4 < r_3;\\
\vdots &= \vdots
\end{aligned}$$

Todos os restos r_1, r_2, r_3, r_4, ..., são todos inteiros positivos tais que

$$b > r_1 > r_2 > r_3 > r_4 > \ldots$$

e existem apenas $b - 1$ inteiros positivos menores que b, necessariamente se chega a uma divisão cujo resto $r_{n+1} = 0$, ou seja:

$$\begin{aligned}
r_{n-2} &= r_{n-1}q_n + r_n, \quad \text{com} \quad 0 < r_n < r_{n-1}\\
r_{n-1} &= r_nq_{n+1} + r_{n+1}, \quad \text{com} \quad r_{n+1} = 0
\end{aligned}$$

Se o resto $r_n \neq 0$ que aparece nas expressões acima é o máximo divisr comum de a e b, isto é, $\mathtt{mdc}(a, b) = r_n$. Pelo Lema (2.1) tem–se que

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

Esse processo de calcular o máximo divisor comum de dois inteiros positivos a e b é denominado Algoritmo de Euclides. Podemos representar esse procedimento ainda da seguinte forma:

	q_1	q_2	q_3		q_n	q_{n+1}
a	b	r_1	r_2	$\ldots$	r_{n-1}	r_n
r_1	r_2	r_3	r_4		0	

O Algoritmo de Euclides também é usado para se encontrar os inteiros x e y tal que $\mathtt{mdc}(a, b) = r_n$ como combinação linear de a e b.

Exemplo 2.11. *Usando o algoritmo de Euclides, ache os inteiros* x *e* y *que satisfaz a seguinte igualdade:*

$$\mathtt{mdc}(56, 72) = 56x + 72y.$$

Solução: Usando o Algoritmo de Euclides

	1	3	2
72	56	16	8
16	8	0	

Dessa forma escrevendo–se cada divisão da seguinte maneira:

$$\begin{aligned} 72 &= 56 \cdot 1 + 16 && (2.19)\\ 56 &= 16 \cdot 3 + 8 && (2.20)\\ 16 &= 8 \cdot 2 + 0. \end{aligned}$$

Assim, pelo Lema (2.1),

$$\mathtt{mdc}(72, 56) = \mathtt{mdc}(56, 16) = \mathtt{mdc}(16, 8) = 8.$$

Como o $\mathtt{mdc}(56, 72) = 8$ e a sua expressão como combinação linear de 72 e 56, isolando os restos 16 e 8 nas equações (2.19) e (2.20) respectivamente, temos:

$$\begin{aligned} 16 &= 72 - 56 \cdot 1 && (2.21)\\ 8 &= 56 - 16 \cdot 3. && (2.22) \end{aligned}$$

Substituindo (2.21) em (2.22),

$$\begin{aligned} 8 &= 56 - (72 - 56 \cdot 1) \cdot 3\\ &= 56 - 72 \cdot 3 + 56 \cdot 3\\ &= 56 \cdot 4 + 72 \cdot (-3). \end{aligned}$$

Logo,

$$\mathtt{mdc}(56, 72) = 8 = 56\mathtt{x} + 72\mathtt{y},$$

onde $\mathtt{x} = 4$ e $\mathtt{y} = -3$. Lembrando que a combinação linear não é única.

Exemplo 2.12. *Ache os inteiros* $\mathtt{x}$ *e* $\mathtt{y}$ *que satisfaz a seguinte igualdade:*

$$78\mathtt{x} + 32\mathtt{y} = 2.$$

Solução: A equação afimar que $\mathtt{mdc}(78, 32) = 2$, deve–se comprovar a verdade. Usando o Algoritmo de Euclides tem–se:

	2	2	3	3
78	32	14	4	2
14	4	2	0	

Dessa forma, escrever–se cada divisão da seguinte maneira:

$$\begin{aligned} 78 &= 32 \cdot 2 + 14 && (2.23)\\ 32 &= 14 \cdot 2 + 4 && (2.24)\\ 14 &= 4 \cdot 3 + 2 && (2.25)\\ 4 &= 2 \cdot 2 + 0. \end{aligned}$$

Pelo Lema (2.1),

$$\mathtt{mdc}(78, 32) = \mathtt{mdc}(32, 14) = \mathtt{mdc}(14, 4) = \mathtt{mdc}(4, 2) = 2.$$

É verdade de que $\mathtt{mdc}(78, 32) = 2$ e a sua expressão como combínação linear de 78 e 32, isolando os restos 14, 4 e 2 nas expressões (2.23), (2.24) e (2.25) respectivamente, tem–se:

$$\begin{aligned} 14 &= 78 - 32 \cdot 2 && (2.26)\\ 4 &= 32 - 14 \cdot 2 && (2.27)\\ 2 &= 14 - 4 \cdot 3. && (2.28) \end{aligned}$$

Substituindo (2.26) em (2.27) depois em (2.28), tem-se

$$\begin{aligned} 2 &= \Big(78-32\cdot 2\Big)-\Big(32-14\cdot 2\Big)\cdot 3 \\ &= \Big(78-32\cdot 2\Big)-\Big[32-(78-32\cdot 2)\cdot 2\Big]\cdot 3 \\ &= 78\cdot 7+32\cdot(-17). \end{aligned}$$

Logo,

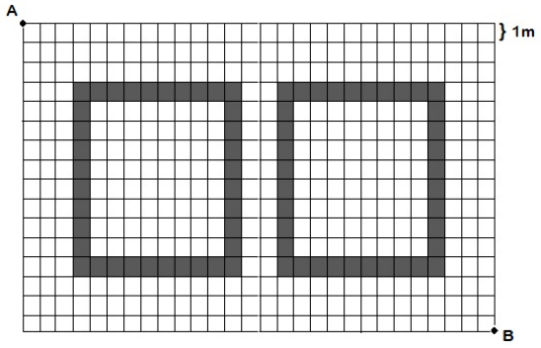
$$\mathtt{mdc}(78,32)=2=78\mathtt{x}+32\mathtt{y},$$

onde $\mathtt{x}=7$ e $\mathtt{y}=-17$. A combinação linear não é única.

Problema 2.1 (Colégio Militar do Rio de Janeiro)**.** *O judô, luta japonesa que surgiu do jiu-jitsu, tornou-se nas Olimpíadas de Londres 2012 o esporte individual que mais trouxe medalhas olímpicas para o Brasil, ultrapassando a então líder vela. A área de lutas do judô, denominada Dojô, é um conjunto de placas quadradas (tatames) de 1m de lado.*

Abaixo, temos um Dojô com duas áreas de luta de mesmas dimensões, delimitadas por tatames mais escuros e cercadas por uma região de segurança, para evitar a queda de atletas em piso desprotegido.

Figura 1: Dojô Com Duas Áreas



Fonte: CMRJ.

Os tatames que compõem o Dojô em questão foram transportados de um depósito para área de competições em pequenos caminhões, todos com as mesmas quantidades. Sabendo que a razão entre as quantidades de tatames escuros e claros é a mesma em todos os caminhões, qual o maior número possível de caminhões que podem ter sido utilizados na tarefa, obedecendo às condições citadas, se cada um fez uma única viagem?

A) 2

B) 4

C) 6

D) 8

E) 10

Solução: Contabilizando a quantidade total de tatames: $28 \cdot 16 = 448$ tatames. Já a quantidade de tatames da cor preta é de 72 tatames. Assim a quantidade de tatames claros, $448 - 72 = 376$. Portanto calculando o $\mathtt{mdc}(376, 72)$ usando o Algoritmo de Euclides, tem–se:

	5	4	2
376	72	16	8
16	8	0	

Logo o $\mathtt{mdc}(376, 72) = 8$, dessa forma a quantidade de caminhões a ser utilizados é 8. Resposta D.

3 Aritmética Modular

Neste capítulo é apresentado alguns conceitos e/ou definições que serão utilizados nos próximos capítulos. Todas essas definições e resultados apresentados posteriormente aqui podem ser encontrados em Alencar Filho (1981), Hefez (2016), Ribenboim (2014) e Santos (2009).

Definição 3.1. *Seja* m *um número inteiro diferente de zero. Diremos que dois números inteiros* a *e* b *são congruentes módulo* m *se os restos de sua divisão euclidiana por* m *são iguais. Quando os inteiros* a *e* b *são congruentes módulo* m*, escreve-se*

$$a \equiv b (\mathrm{mod}\ m).$$

Exemplo 3.1. $11 \equiv 3(\mathrm{mod}\ 2)$*, pois os restos da divisão de* 11 *e de* 3 *por* 2 *são iguais a* 1.

Agora se resto das divisão de dois inteiros a e b por m não for iguais, diremos que a e b não são congruentes, ou que são incongruentes, módulo m. Escreveremos, neste caso, $a \not\equiv b(\mathrm{mod}\ m)$.

De fato é imadiato como resto da divisão de um número inteiro qualquer por l é sempre nulo, temos que $a \equiv b(\mathrm{mod}\ l)$, quaisquer que sejam a e b inteiros. Dessa forma, consideraremos sempre m > 1.

Pela Definição 3.1., se verifica se dois números inteiros são congruentes módulo m, mas não é necessário efetuar a divisão euclidiana de ambos por m para depois comparar os seus restos. Temos o seguinte resultado.

Proposição 3.1. *Suponha que* a*,* b *inteiros são tais que* $b \geqslant a$*. Tem-se que* $a \equiv b(\mathrm{mod}\ m)$ *se, e somente se,* $m | (b - a)$.

Demonstração. Sejam $a = mq + r$, com $r < m$ e $b = mq' + r'$, com $r' < m$, as divisões

euclidianas de a e b por m, respectivamente. Logo,

$$b - a = \begin{cases} m(q' - q) + (r' - r), & \text{se } r' \geqslant r \\ m(q' - q) + (r' - r), & \text{se } r \geqslant r' \end{cases}$$

onde $r' - r < m$, ou $r - r' < m$. Portanto, $a \equiv b (\mathrm{mod}\ m)$ se, e somente se, $r = r'$, o que é equivalente a dizer que $m | (b - a)$. □

Proposição 3.2. *Se a e b são inteiros, então $a \equiv b (\mathrm{mod}\ m)$ se, e somente se, existir um inteiro k tal que $a = b + km$.*

Demonstração. ($\Longrightarrow$) Se $a \equiv b (\mathrm{mod}\ m)$, então $m \mid (a - b)$. O que implica na existência de um k inteiro tal que $a - b = km$, daí $a = b + km$.

($\Longleftarrow$) Se $a = b + km$, então $a - b = km$ sendo k inteiro, isto é, $m \mid (a - b)$. Assim, $a \equiv b (\mathrm{mod}\ m)$. □

Proposição 3.3. *Se a, b, m e d são inteiros, com $m > 1$, as seguintes sentenças são verdadeiras:*

1. $a \equiv a (\mathrm{mod}\ m)$.
2. *Se* $a \equiv b (\mathrm{mod}\ m)$, *então* $b \equiv a (\mathrm{mod}\ m)$.
3. *Se* $a \equiv b (\mathrm{mod}\ m)$ *e* $b \equiv d (\mathrm{mod}\ m)$, *então* $a \equiv d (\mathrm{mod}\ m)$.

Demonstração. (1). Como $m \mid 0$, tem-se que $m \mid (a - a)$. O que implica em $a \equiv a (\mathrm{mod}\ m)$.

(2). Se $a \equiv b (\mathrm{mod}\ m)$, então $m \mid (a - b)$ isto é $a = b + mk$, sendo k inteiro. Dai segue que $b = a - mk$ o que implica em $b - a = -mk$, isto é, $b - a = m(-k)$ onde $b \equiv a (\mathrm{mod}\ m)$. (Proposição 3.2).

(3). Se $a \equiv b (\mathrm{mod}\ m)$, então $a - b = mk_1$, k_1 inteiro, dai

$$a = b + mk_1 \tag{3.1}$$

e se $b \equiv d (\mathrm{mod}\ m)$, então $b - d = mk_2$ com k_2 inteiro, dai

$$b = d + mk_2. \tag{3.2}$$

Somando (3.1) e (3.2) tem–se,

$$a + b = b + d + (k_1 + k_2)m$$

o que implica em $a = d + (k_1 + k_2)m$, sendo $k_1 + k_2$ inteiro, e assim $a \equiv d(\mathrm{mod}\ m)$. □

Esta proposição monstra que a relação de congruência definida no conjunto dos inteiros, é uma relação de equivalência, pois é valido as propriedades Reflexiva, Simétrica e Transitiva.

Teorema 3.1. *Se* a, b, c *e* m *são inteiros, com* $m > 0$, *tem-se que* $a \equiv b(\mathrm{mod}\ m)$, *então:*

1. $a + c \equiv b + c(\mathrm{mod}\ m)$;
2. $a - c \equiv b - c(\mathrm{mod}\ m)$;
3. $ac \equiv bc(\mathrm{mod}\ m)$.

Demonstração. (1) Como $a \equiv b(\mathrm{mod}\ m)$ então $a - b = mk$, com k inteiro. E, portanto pode-se escrever $a - b = (a + c) - (b + c)$, assim $(a + c) - (b + c) = mk$. Assim,

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

e $a + c \equiv b + c(\mathrm{mod}\ m)$.

(2) Como $a - b = (a - c) - (b - c)$ e por hipótese $(a - b) = mk$, tem-se $(a - c) - (b - c) = mk$, daí $a - c \equiv b - c(\mathrm{mod}\ m)$.

(3) Como $a - b = mk$, tem-se $ac - bc = mkc$, assim, $ac \equiv bc(\mathrm{mod}\ m)$. □

Teorema 3.2. *Se* a, b, c *e* m *são inteiros tais que* $a \equiv b(\mathrm{mod}\ m)$ *e* $c \equiv d(\mathrm{mod}\ m)$, *então:*

1. $a + c \equiv b + d(\mathrm{mod}\ m)$;
2. $a - c \equiv b - d(\mathrm{mod}\ m)$;
3. $ac \equiv bd(\mathrm{mod}\ m)$.

Demonstração. (1) Se $a \equiv b(\mathrm{mod}\ m)$ e $c \equiv d(\mathrm{mod}\ m)$, então $a - b = mk_1$ e $c - d = mk_2$. Somando ambos os membros tem–se que,

$$(a - b) + (c - d) = m(k_1 + k_2)$$

o que implica em

$$(a + c) + (-b - d) = m(k_1 + k_2),$$

assim, $(a+c)-(b+d) = m(k_1+k_2)$ o que implica em $a+c \equiv b+d(\mathrm{mod}\ m)$.

(2) Como da hipótese

$$a-b = mk_1 \tag{3.3}$$

e

$$c-d = mk_2, \tag{3.4}$$

subtraindo (3.3) de (3.4) tem-se que

$$(a-b)-(a-c) = m(k_1-k_2)$$

o que implica em $(a-c)-(b-d) = m(k_1-k_2)$, logo $a-c \equiv b-d(\mathrm{mod}\ m)$.

(3) Da hipótese tem-se que, $a-b = mk_1$ e $c-d = mk_2$, multiplicando ambos os membros por c na primeira igualdade e ambos os membros por b na segunda igualdade, tem-se:

$$ac-bc = mk_1c \tag{3.5}$$

e

$$bc-bd = mk_2b. \tag{3.6}$$

Somando (3.5) e (3.6), tem–se que:

$$ac-bc+bc-bd = m(k_1c+k_2b),$$

o que implica em $ac-bd = m(k_1c+k_2b)$, logo $ac \equiv bd(\mathrm{mod}\ m)$. □

Teorema 3.3. *Se* a, b, c *e* m *são inteiros e* $ac \equiv bd(\mathrm{mod}\ m)$, *então* $a \equiv b\left(\mathrm{mod}\ \frac{m}{d}\right)$, *onde* $d = mdc(c,m)$.

Demonstração. De $ac \equiv bd(\mathrm{mod}\ m)$ temos $ac-bc = mk$, com k inteiro, o que implica em $c(a-b) = mk$. Dividindo ambos por d, tem–se:

$$\left(\frac{c}{d}\right)(a-b) = m\left(\frac{k}{d}\right) \Longrightarrow \left(\frac{c}{d}\right)(a-b) = k\left(\frac{m}{d}\right).$$

Portanto, $\frac{m}{d}$ divide $\left(\frac{c}{d}\right)(a-b)$, como $mdc\left(\frac{m}{d},\frac{c}{d}\right) = 1$, então $\frac{m}{d}$ divide $(a-b)$.

Daí $a \equiv b\left(\mathrm{mod}\frac{m}{d}\right)$ sendo $d = mdc(c,m)$. □

Proposição 3.4. *Se* a, b, k *e* m *são inteiros com* $k > 0$ *e* $a \equiv b(\mathrm{mod}\ m)$, *então* $a^k \equiv b^k(\mathrm{mod}m)$.

Demonstração. A demonstração segue, imediatamente, da identidade:

$$a^k - b^k = (a - b) \cdot (a^{k-1} + a^{k-2} \cdot b + \ldots + a \cdot b^{k-2} + b^{k-1}),$$

como $m \mid (a - b)$ o que implica em $a - b = mq$, com q inteiro, então $m \mid (a^k - b^k)$, logo $a^k \equiv b^k (\mathrm{mod}\ m)$. □

Exemplo 3.2. *Determinar o resto da divisão de* 2^{3528} *por* 13.

Solução: Calcular a potência 2^{3528}, para depois dividir o resultado por 13, é um caminho árduo, observe por congruência modular. Veja,

$$2^8 = 256 \equiv (-4)(\mathrm{mod}\ 13),$$

pela Proposição 3.4 temos $2^{3528} \equiv (-4)^{441}(\mathrm{mod}\ 13)$. Como $(-4)^3 = -64 \equiv 1(\mathrm{mod}\ 13)$, tem-se $(-4)^{441} \equiv 1^{411}(\mathrm{mod}\ 13)$. Portanto $2^{3528} \equiv 1(\mathrm{mod}\ 13)$, logo, 2^{3528} deixa resto 1 na divisão por 13.

Exemplo 3.3. *Determinar o resto da divisão de* 5^{21} *por* 127.

Solução: Certamente fazer a potência 5^{21} e depois dividir por 127 não é o melhor caminho. De um modo mais econômico, veja que:

$$5^3 = 125 \equiv -2(\mathrm{mod}\ 127)$$

o que implica em $(5^3)^7 \equiv (-2)^7(\mathrm{mod}\ 127)$ e $(-2)^7 = -128 \equiv -1(\mathrm{mod}\ 127)$, que por sua vez $-1 \equiv 126(\mathrm{mod}\ 127)$. Assim, o resto da divisão de 5^{21} por 127 é 126.

Exemplo 3.4. *Determine o resto da divisão de* 12^{12} *por* 5.

Solução: Note que $12^2 = 144 \equiv -1(\mathrm{mod}\ 5)$, daí $12^2 \equiv -1(\mathrm{mod}\ 5)$, o que implica em $(12^2)^6 \equiv (-1)^6(\mathrm{mod}\ 5)$, logo $12^{12} \equiv 1(\mathrm{mod}\ 5)$. Assim, o resto da divisão de 12^{12} por 5 é 1.

Problema 3.1. *O calendário é congruência módulo 7, seja o mês de agosto de 2019, cujos dias estão descritos abaixo:*

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Observe que em cada coluna (dia da semana) encontramos números congruentes entre se módulo 7. Na coluna do domingo determinamos números congruentes a 4, ou seja, $4 \equiv k_1 (\mathrm{mod}\ 7)$ com $k_1 \in \mathbb{Z}$, na segunda–feira os congruentes a 5, isto é, $5 \equiv k_2 (\mathrm{mod}\ 7)$ com $k_2 \in \mathbb{Z}$ e assim por diante. Perceba que o dia 31 de agosto de 2019 é um sábado, consequentemente dia 1º de setembro será um domingo, dia 2 é uma segunda-feira, dia 3 é uma terça-feira, dia 4 é uma quarta-feira, dia 5 é uma quinta-feira, dia 6 é uma sexta-feira, dia 7 é um sábado. Como determinar o dia da semana que corresponde a 26 de setembro de 2019.

Para isto, precisamos determinar um inteiro k, onde $1 \leqslant k \leqslant 7$, congruente a 26 módulo 7. Ora, como

$$26 \equiv k (\mathrm{mod}\ 7) \Longrightarrow 26 = 7 \cdot 3 + k,$$

segue que $k = 5$, ou seja, como 5 de setembro corresponde a quinta–feira, concluímos que o dia 26 de setembro de 2019 também refere-se a uma quinta–feira.

Problema 3.2 (PROFMAT – Exame de Qualificação (2012–2))**.** *Mostre que nenhum número natural da forma* $4n + 3$ *pode ser escrito como o quadrado ou a soma de dois quadrados de números naturais.*

Solução: Suponha que existam $x,\ y,\ z \in \mathbb{N}$ tais que $z^2 = 4n+3$ ou que $x^2+y^2 = 4n+3$. Teríamos então que $z^2 = 3(\mathrm{mod}\ 4)$ ou que $x^2+y^2 = 3(\mathrm{mod}\ 4)$. Sendo, para todo $a \in \mathbb{N}$, $a \equiv 0(\mathrm{mod}\ 4)$, $a \equiv 1(\mathrm{mod}\ 4)$, $a \equiv 2(\mathrm{mod}\ 4)$, ou $a \equiv 3(\mathrm{mod}\ 4)$, segue que

$$a^2 \equiv 0(\mathrm{mod}\ 4) \quad \text{ou} \quad a^2 \equiv 1(\mathrm{mod}\ 4).$$

Logo $z^2 \not\equiv 3(\mathrm{mod}\ 4)$ e $x^2 + y^2 \not\equiv 3(\mathrm{mod}\ 4)$, o que é uma contradição.

3.1 Critérios de Divisibilidade

Nessa seção é mencionado alguns critérios de divisibilidade, utilizando as definições, propriedades e resultados de congruência modular. A ideia é mostrar os critérios de

divisibilidade e estabelecer regras que permitam determinar se um dado número inteiro, é ou não divisível por um outro número inteiro n, a um custo menor do que efetuar a divisão.

Será representado um número inteiro na base 10, da seguinte forma:

$$a = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \ldots + a_1 \cdot 10 + a_0.$$

3.1.1 Divisibilidade por 2

Um numero inteiro n é divisível por 2 quando o último algarismo é par ou é zero. Utilizando a noção de congruência, note que: $10 \equiv 0(\mathrm{mod}\ 2)$, assim $10^i \equiv 0(\mathrm{mod}\ 2)$. Assim,

$$n_i \cdot 10^i \equiv 0(\mathrm{mod}\ 2),\ \text{para } i \geqslant 1.$$

Portanto, dado um número n, tem–se que:

$$n = n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + \ldots + n_1 \cdot 10 + n_0 \equiv 0 + 0 + \ldots + 0 + n_0 = n_0(\mathrm{mod}\ 2),$$

assim $n \equiv n_0(\mathrm{mod}\ 2)$. Assim, n é divisível por 2 se, e somente se, n_0 é divisível por 2, ou seja, se n_0 é par.

Exemplo 3.5. *Verifique se o número 3416 é divisível por 2.*

Solução: Veja que:

$$3416 = 3 \cdot 10^3 + 4 \cdot 10^2 + 1 \cdot 10 + 6 \equiv 0 + 0 + 0 + 6 = 6(\mathrm{mod}\ 2),$$

mas, $6 \equiv 0(\mathrm{mod}\ 2)$, por transitividade $3416 \equiv 0(\mathrm{mod}\ 2)$. O que confirma que 3416 é divisível por 2 já que 6 é um número par e é divisível por 2.

Exemplo 3.6. *Verifique se o número 4783 é divisível por 2.*

Solução: Veja que:

$$4783 = 4 \cdot 10^3 + 7 \cdot 10^2 + 8 \cdot 10 + 3 \equiv 0 + 0 + 0 + 3 = 3(\mathrm{mod}\ 2),$$

mas, $3 \equiv 1(\mathrm{mod}\ 2)$, por transitividade $4783 \equiv 1(\mathrm{mod}\ 2)$. O número 4783 não é divisível por 2, pois o algarismo da unidades, que é 3, não é divisível por 2.

3.1.2 Divisibilidade por 3

Um número inteiro n é divisível por 3 se, e somente se, a soma de seus algarismos for um número divisível por 3. Utilizando a noção de congruência e o Teorema 3.2, note que: $10 \equiv 1(\mathrm{mod}\ 3)$, por outro lado, $10^2 \equiv 10 \cdot 10 \equiv 1 \cdot 1 \equiv 1(\mathrm{mod}\ 3)$, ou ainda, $10^3 \equiv 10^2 \cdot 10 \equiv 1 \cdot 1 \equiv 1(\mathrm{mod}\ 3)$, assim, $10^i \equiv 1(\mathrm{mod}\ 3)$. Daí,

$$n_i \cdot 10^i \equiv 1(\mathrm{mod}\ 3),\ \text{para } i \geqslant 1.$$

Assim,

$$\begin{aligned} n_0 &\equiv n_0(\mathrm{mod}\ 3) \\ n_1 \cdot 10 &\equiv n_1(\mathrm{mod}\ 3) \\ n_2 \cdot 10^2 &\equiv n_2(\mathrm{mod}\ 3) \\ &\vdots \\ n_r \cdot 10^r &\equiv n_r(\mathrm{mod}\ 3) \end{aligned}$$

Somando membro a membro, tem–se que:

$$\Big(n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + \ldots + n_1 \cdot 10 + n_0\Big) \equiv \Big(n_r + n_{r-1} + \ldots + n_1 + n_0\Big)(\mathrm{mod}\ 3),$$

assim temos que $n \equiv (n_r + n_{r-1} + \ldots + n_1 + n_0)(\mathrm{mod}\ 3)$. Assim n é divisível por 3 se, e somente se, $(n_r + n_{r-1} + \ldots + n_1 + n_0)$ é divisível por 3, ou seja, se a soma de todos os algarismo for divisível por 3, em outras palavras,

$$n_r + n_{r-1} + \ldots + n_1 + n_0 \equiv 0(\mathrm{mod}\ 3).$$

Exemplo 3.7. *Verifique se o número 3363 é divisível por 3.*

Solução: Veja que:

$$3363 = 3 \cdot 10^3 + 3 \cdot 10^2 + 6 \cdot 10 + 3 \equiv 3 + 3 + 6 + 3 = 18(\mathrm{mod}\ 3),$$

mas, $18 \equiv 0(\mathrm{mod}\ 3)$, por transitividade tem–se que $3363 \equiv 0(\mathrm{mod}\ 3)$. Isso diz que o número 3363 é divisível por 3, pois a soma do seus algarismo também é divisível por 3.

Exemplo 3.8. *Verifique se o número 6694 é divisível por 3.*

Solução: Veja que:

$$6694 = 6 \cdot 10^3 + 6 \cdot 10^2 + 9 \cdot 10 + 4 \equiv 6 + 6 + 9 + 4 = 25(\mathrm{mod}\ 3).$$

Mas $25 \equiv 1(\mathtt{mod}\ 3)$, por transitividade, $6694 \equiv 1(\mathtt{mod}\ 3)$. Isso nos diz que o número 6694 não é divisível por 3, pois a soma dos seus algarismos não é divisível por 3.

3.1.3 Divisibilidade por 4

Um número inteiro $\mathtt{n}$ é divisível por 4 se, e somente se, quando termina em 00 ou quando os dois últimos algarismos da direita for divisível por 4. Como $10 \equiv 2(\mathtt{mod}\ 4)$, por outro lado, $10^2 = 10 \cdot 10 \equiv 2 \cdot 2 = 0(\mathtt{mod}\ 4)$. Daí,

$$\mathtt{n}_\mathtt{i} \cdot 10^\mathtt{i} \equiv 0(\mathtt{mod}\ 4), \text{ para } \mathtt{i} > 1.$$

Assim,

$$\begin{aligned} \mathtt{n} &\equiv \mathtt{n}_\mathtt{r} \cdot 10^\mathtt{r} + \mathtt{n}_{\mathtt{r}-1} \cdot 10^{\mathtt{r}-1} + \ldots + \mathtt{n}_1 \cdot 10 + \mathtt{n}_0(\mathtt{mod}\ 4) \\ \mathtt{n} &\equiv 0 + 0 + \ldots + \mathtt{n}_1 \cdot 10 + \mathtt{n}_0(\mathtt{mod}\ 4) \\ \mathtt{n} &\equiv \mathtt{n}_1 \cdot 10 + \mathtt{n}_0(\mathtt{mod}\ 4) \end{aligned}$$

Logo, $\mathtt{n}$ é divisível por 4 se, e somente se, $\mathtt{n}_1\mathtt{n}_0$ é divisível por 4.

Exemplo 3.9. *Verifique se o número 6324 é divisível por 4.*

Solução: Veja que:

$$6324 = 6 \cdot 10^3 + 3 \cdot 10^2 + 2 \cdot 10 + 4 \equiv 0 + 0 + 20 + 4 = 24(\mathtt{mod}\ 4),$$

mas, $24 \equiv 0(\mathtt{mod}\ 4)$, por transitividade $6324 \equiv 24(\mathtt{mod}\ 4)$. Logo 24 é divisível por 4, portanto 6324 é divisível por 4.

Exemplo 3.10. *Verifique se o número 715 é divisível por 4.*

Solução: Veja que:

$$715 = 7 \cdot 10^2 + 1 \cdot 10 + 5 \equiv 0 + 10 + 5 = 15(\mathtt{mod}\ 4),$$

daí, $15 \equiv 3(\mathtt{mod}\ 4)$. Logo 15 não é divisível por 4, portanto 715 não é divisível por 4.

3.1.4 Divisibilidade por 5

Um número inteiro n é divisível por 5 quando o último algarismo for 0 ou 5. Utilizando a noção de congruência, note que: $10 \equiv 0(\mathrm{mod}\ 5)$, dessa forma $10^i \equiv 0(\mathrm{mod}\ 5)$. Daí,

$$n_i \cdot 10^i \equiv 0(\mathrm{mod}\ 5),\ \text{para}\ i \geqslant 1.$$

Portanto, dado um número $n = n_r n_{r-1} \ldots n_0$, na base 10, tem–se que:

$$n = n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + \ldots + n_1 \cdot 10 + n_0 \equiv 0 + 0 + \ldots + 0 + n_0 = n_0(\mathrm{mod}\ 5),$$

assim $n \equiv n_0(\mathrm{mod}\ 5)$. Assim, n é divisível por 5 se, e somente se, n_0 é divisível por 5, ou seja, se n_0 for 0 ou 5.

Exemplo 3.11. *Verifique se o número 2570 é divisível por 5.*

Solução: Veja que:

$$2570 = 2 \cdot 10^3 + 5 \cdot 10^2 + 7 \cdot 10 + 0 \equiv 0 + 0 + 0 + 0 = 0(\mathrm{mod}\ 5),$$

mas, $0 \equiv 0(\mathrm{mod}\ 5)$, por transitividade $2570 \equiv 0(\mathrm{mod}\ 5)$. Logo 2570 é divisível por 5 já que o número termina em 0.

Exemplo 3.12. *Verifique se o número 4465 é divisível por 5.*

Solução: Veja que:

$$4465 = 4 \cdot 10^3 + 4 \cdot 10^2 + 6 \cdot 10 + 5 \equiv 0 + 0 + 0 + 5 = 5(\mathrm{mod}\ 5),$$

mas, $5 \equiv 0(\mathrm{mod}\ 5)$, por transitividade $4465 \equiv 0(\mathrm{mod}\ 5)$. Portanto 4465 é divisível por 5 pois o número termina em 5.

Exemplo 3.13. *Verifique se o número 5791 é divisível por 5.*

Solução: Veja que:

$$5796 = 5 \cdot 10^3 + 7 \cdot 10^2 + 9 \cdot 10 + 6 \equiv 0 + 0 + 0 + 6 = 6(\mathrm{mod}\ 5),$$

mas, $6 \equiv 1(\mathrm{mod}\ 5)$, por transitividade $5796 \equiv 1(\mathrm{mod}\ 5)$. O número 5796 não é divisível por 5, pois o número não tem em sua unidade o algarismo 0 ou 5.

3.1.5 Divisibilidade por 7

Um número inteiro $n = n_r n_{r-1} \dots n_0$, na base 10 é divisível por 7 se, e somente se, $n_r \cdot 10^{r-1} + n_{r-1} \cdot 10^{r-2} + \dots + n_2 \cdot 10 + n_1 \equiv 2 \cdot n_0 (\mathrm{mod}\ 7)$, ou seja:

$$7 \Big| \Big[\big(n_r \cdot 10^{r-1} + n_{r-1} \cdot 10^{r-2} + \dots + n_2 \cdot 10 \big) - 2 \cdot n_0 \Big], \tag{3.7}$$

De fato, se n é divisível por 7 existe $k \in \mathbb{Z}$ tal que $n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + \dots + n_1 \cdot 10 + n_0 = 7 \cdot k$, daí,

$$\begin{aligned} n_0 &= 7 \cdot k - \Big(n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + \dots + n_2 \cdot 10^2 + n_1 \cdot 10 \Big) \\ n_0 &= 7 \cdot k - 10 \cdot \Big(n_r \cdot 10^{r-1} + n_{r-1} \cdot 10^{r-2} + \dots + n_2 \cdot 10 + n_1 \Big) \end{aligned} \tag{3.8}$$

Em, $n_r \cdot 10^{r-1} + n_{r-1} \cdot 10^{r-2} + \dots + n_2 \cdot 10 - 2 \cdot n_0$, substituindo n_0 de (3.8), temos:

$$\begin{aligned} & n_r \cdot 10^{r-1} + n_{r-1} \cdot 10^{r-2} + \dots + n_2 \cdot 10 - 2 \Big\{ 7 \cdot k - 10 \cdot \Big(n_r \cdot 10^{r-1} + n_{r-1} \cdot 10^{r-2} + \dots + n_2 \cdot 10 + n_1 \Big) \Big\} \\ &= n_r \cdot 10^{r-1} + n_{r-1} \cdot 10^{r-2} + \dots + n_2 \cdot 10 - 14 \cdot k + 20 \cdot \Big(n_r \cdot 10^{r-1} + n_{r-1} \cdot 10^{r-2} + \dots + n_2 \cdot 10 + n_1 \Big) \\ &= 21 \cdot \Big(n_r \cdot 10^{r-1} + n_{r-1} \cdot 10^{r-2} + \dots + n_2 \cdot 10 + n_1 \Big) - 14 \cdot k \\ &= 7 \cdot \Big\{ 3 \cdot \Big(n_r \cdot 10^{r-1} + n_{r-1} \cdot 10^{r-2} + \dots + n_2 \cdot 10 + n_1 \Big) - 2 \cdot k \Big\} \end{aligned}$$

Dessa forma $7 \Big| \Big[(n_r \cdot 10^{r-1} + n_{r-1} \cdot 10^{r-2} + \dots + n_2 \cdot 10) - 2 \cdot n_0 \Big]$.

Se, suponhamos que $7 \Big| \Big[(n_r \cdot 10^{r-1} + n_{r-1} \cdot 10^{r-2} + \dots + n_2 \cdot 10) - 2 \cdot n_0 \Big]$, então existe $k \in \mathbb{Z}$ tal que

$$n_r \cdot 10^{r-1} + n_{r-1} \cdot 10^{r-2} + \dots + n_2 \cdot 10 - 2 \cdot n_0 = 7 \cdot k$$

Mas,

$$\begin{aligned} n_r \cdot 10^r + \dots + n_1 \cdot 10 + n_0 &= 10 \cdot (n_r \cdot 10^{r-1} + n_{r-1} \cdot 10^{r-2} + \dots + n_1 \cdot 10) + n_0 \\ &= 10 \cdot (7 \cdot k + 2 \cdot n_0) + n_0 \\ &= 70 \cdot k + 20 \cdot n_0 + n_0 \\ &= 7 \cdot (10 \cdot k + 3 \cdot n_0) \end{aligned}$$

Logo $7|\mathfrak{n}$.

Exemplo 3.14. *Verifique se o número* 511 *é divisível por* 7.

Solução: Veja que:

$$51 - 2 \cdot 1 = 51 - 2 = 49$$

como $49 \equiv 0(\mathfrak{mod}\ 7)$, ou seja, $7|49$, por transitividade tem–se que $511 \equiv 0(\mathfrak{mod}\ 7)$. Assim 511 é divisível por 7.

3.1.6 Divisibilidade por 8

Um número inteiro $\mathfrak{n}$ é divisível por 8 se, e somente se, quando termina em 000 ou quando os três últimos algarismos da direita for divisível por 8. Como $10 \equiv 2(\mathfrak{mod}\ 8)$, por outro lado, $10^3 = 10 \cdot 10 \cdot 10 \equiv 2 \cdot 2 \cdot 2 = 0(\mathfrak{mod}\ 8)$. Daí,

$$\mathfrak{n}_\mathfrak{i} \cdot 10^\mathfrak{i} \equiv 0(\mathfrak{mod}\ 8),\ \text{para}\ \mathfrak{i} > 2.$$

Assim,

$$\begin{aligned}
\mathfrak{n} &\equiv \mathfrak{n}_\mathfrak{r} \cdot 10^\mathfrak{r} + \mathfrak{n}_{\mathfrak{r}-1} \cdot 10^{\mathfrak{r}-1} + \ldots + \mathfrak{n}_2 \cdot 10^2 + \mathfrak{n}_1 \cdot 10 + \mathfrak{n}_0(\mathfrak{mod}\ 8) \\
\mathfrak{n} &\equiv 0 + 0 + \ldots \mathfrak{n}_2 \cdot 10^2 + \mathfrak{n}_1 \cdot 10 + \mathfrak{n}_0(\mathfrak{mod}\ 8) \\
\mathfrak{n} &\equiv \mathfrak{n}_2 \cdot 10^2 + \mathfrak{n}_1 \cdot 10 + \mathfrak{n}_0(\mathfrak{mod}\ 8)
\end{aligned}$$

Logo, $\mathfrak{n}$ é divisível por 8 se, e somente se, $\mathfrak{n}_2\mathfrak{n}_1\mathfrak{n}_0$ é divisível por 8.

Exemplo 3.15. *Verifique se o número 36536 é divisível por 8.*

Solução: Veja que:

$$36536 = 3 \cdot 10^4 + 6 \cdot 10^3 + 5 \cdot 10^2 + 3 \cdot 10 + 6 \equiv 0 + 0 + 500 + 30 + 6 = 536(\mathfrak{mod}\ 8),$$

mas, $536 \equiv 0(\mathfrak{mod}\ 8)$, por transitividade $36536 \equiv 536(\mathfrak{mod}\ 8)$. Logo 536 é divisível por 8, portanto 36536 é divisível por 8.

Exemplo 3.16. *Verifique se o número 70121 é divisível por 8.*

Solução: Veja que:

$$70121 = 7 \cdot 10^4 + 0 \cdot 10^3 + 1 \cdot 10^2 + 2 \cdot 10 + 1 \equiv 0 + 0 + 100 + 20 + 1 = 121(\mathfrak{mod}\ 8),$$

daí, $121 \equiv 1(\mathfrak{mod}\ 8)$. Logo 121 não é divisível por 8, portanto 70121 não é divisível por 8.

3.1.7 Divisibilidade por 9

Um número inteiro n é divisível por 9 se, e somente se, a soma de seus algarismos for um número divisível por 9. Utilizando a noção de congruência e o Teorema 3.2, note que: $10 \equiv 1(\mathrm{mod}\ 9)$, por outro lado, $10^2 \equiv 10 \cdot 10 \equiv 1 \cdot 1 \equiv 1(\mathrm{mod}\ 9)$, ou ainda, $10^4 \equiv 10^2 \cdot 10^2 \equiv 1 \cdot 1 \equiv 1(\mathrm{mod}\ 9)$, assim, $10^i \equiv 1(\mathrm{mod}\ 9)$. Daí,

$$n_i \cdot 10^i \equiv 1(\mathrm{mod}\ 9),\ \text{para } i \geqslant 1.$$

Assim,

$$\begin{aligned} n_0 &\equiv n_0(\mathrm{mod}\ 9) \\ n_1 \cdot 10 &\equiv n_1(\mathrm{mod}\ 9) \\ n_2 \cdot 10^2 &\equiv n_2(\mathrm{mod}\ 9) \\ &\vdots \\ n_r \cdot 10^r &\equiv n_r(\mathrm{mod}\ 9) \end{aligned}$$

Somando membro a membro, tem–se que:

$$n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + \ldots + n_1 \cdot 10 + n_0 \equiv n_r + n_{r-1} + \ldots + n_1 + n_0(\mathrm{mod}\ 9),$$

assim $n \equiv n_r + n_{r-1} + \ldots + n_1 + n_0(\mathrm{mod}\ 9)$. Assim n é divisível por 9 se, e somente se, $(n_r + n_{r-1} + \ldots + n_1 + n_0)$ é divisível por 9, em outras palavras,

$$n_r + n_{r-1} + \ldots + n_1 + n_0 \equiv 0(\mathrm{mod}\ 9).$$

Exemplo 3.17. *Verifique se o número 18135 é divisível por 9.*

Solução: Veja que:

$$18135 = 1 \cdot 10^4 + 8 \cdot 10^3 + 1 \cdot 10^2 + 3 \cdot 10 + 5 \equiv 1 + 8 + 1 + 3 + 5 = 18(\mathrm{mod}\ 9),$$

mas, $18 \equiv 0(\mathrm{mod}\ 9)$, por transitividade tem–se que $18135 \equiv 0(\mathrm{mod}\ 9)$. Portanto, a soma dos algarismos do número 18135 é um número divisível por 9, logo o número 18135 é divisível por 9.

Exemplo 3.18. *Verifique se o número 514045 é divisível por 9.*

Solução: Veja que:

$$514045 = 5 \cdot 10^5 + 1 \cdot 10^4 + 4 \cdot 10^3 + 0 \cdot 10^2 + 4 \cdot 10 + 5 \equiv 5 + 1 + 4 + 0 + 4 + 5 = 19(\mathrm{mod}\ 9),$$

mas $19 \equiv 1(\mathtt{mod}\ 9)$, por transitividade, $514045 \equiv 1(\mathtt{mod}\ 9)$. Isso nos diz que o número 514045 não é divisível por 9, pois a soma dos seus algarismos não é divisível por 9.

3.1.8 Divisibilidade por 11

Um número inteiro n é divisível por 11 se, e somente se, quando a diferença não negativa entre a soma dos algarismos de ordem ímpar (I) e a soma dos algarismos de ordem par (P) for um número divisível por 11. Utilizando a noção de congruência, a Proposição 3.4 e o Teorema 3.2, note que: $10 \equiv (-1)(\mathtt{mod}\ 11)$, por outro lado, $10^2 \equiv 10 \cdot 10 \equiv (-1)\cdot(-1) \equiv 1(\mathtt{mod}\ 11)$, ou ainda, $10^3 \equiv 10\cdot 10\cdot 10 \equiv (-1)\cdot(-1)\cdot(-1) \equiv (-1)(\mathtt{mod}\ 11)$, assim, $10^{2i} \equiv 1(\mathtt{mod}\ 11)$ e $10^{2i+1} \equiv (-1)(\mathtt{mod}\ 11)$, com $i = 0, 1, 2, \ldots, r$. Portanto, dado um número $n = n_r n_{r-1} \ldots n_0$, na base 10, temos que:

$$\begin{aligned}
n_0 &\equiv n_0(\mathtt{mod}\ 11)\\
n_1 \cdot 10 &\equiv -n_1(\mathtt{mod}\ 11)\\
n_2 \cdot 10^2 &\equiv n_2(\mathtt{mod}\ 11)\\
n_3 \cdot 10^3 &\equiv -n_3(\mathtt{mod}\ 11)\\
n_4 \cdot 10^4 &\equiv n_4(\mathtt{mod}\ 11)\\
&\vdots\\
n_r \cdot 10^r &\equiv (-1)^r \cdot n_r(\mathtt{mod}\ 11).
\end{aligned}$$

Somando, membro a membro as congruências acima obtem–se:

$$n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + \ldots + n_1 \cdot 10 + n_0 \equiv n_0 - n_1 + n_2 - n_3 + \ldots + (-1)^r \cdot n_r(\mathtt{mod}\ 11),$$

assim $n \equiv n_0 - n_1 + n_2 - n_3 + \ldots + (-1)^r \cdot n_r(\mathtt{mod}\ 11)$. Assim n é divisível por 11 se, e somente se, $(n_0 - n_1 + n_2 - n_3 + \ldots + (-1)^r \cdot n_r)$ é divisível por 11.

Exemplo 3.19. *Verifique se o numero* 4520835 *é divisível por* 11.

Solução: Veja que:

$$4520835 = 4{\cdot}10^6{+}5{\cdot}10^5{+}2{\cdot}10^4{+}0{\cdot}10^3{+}8{\cdot}10^2{+}3{\cdot}10{+}5 \equiv 4{-}5{+}2{-}0{+}8{-}3{+}5 = 11(\mathtt{mod}\ 11),$$

mas, $11 \equiv 0(\mathtt{mod}\ 11)$, por transitividade tem–se que $4520835 \equiv 0(\mathtt{mod}\ 11)$. Portanto o número 4520835 é divisível por 11, pois a diferença entre a soma dos algarismos de ordem ímpar e a soma dos algarismos de ordem par é um número divisível por 11.

Exemplo 3.20. *Verifique se o número* 18135 *é divisível por* 11.

Solução: Veja que:

$$81135 = 8 \cdot 10^4 + 1 \cdot 10^3 + 1 \cdot 10^2 + 3 \cdot 10 + 5 \equiv 8 - 1 + 1 - 3 + 5 = 10 (\mathtt{mod}\ 11),$$

mas, $10 \equiv (-1) (\mathtt{mod}\ 11)$, por transitividade tem–se que $81135 \equiv (-1) (\mathtt{mod}\ 11)$. Portanto o número 81135 não é divisível por 11, pois a diferença entre a soma dos algarismos de ordem ímpar e a soma dos algarismos de ordem par não é um número divisível por 11.

Problema 3.3 (PROFMAT (2015.2))**.** *Determine* **TODOS** *os valores possíveis para os algarismos* $\mathtt{x}$, $\mathtt{y}$, $\mathtt{z}$ *e* $\mathtt{t}$ *de modo que os números abaixo, representados na base 10, tenham a propriedade mencionada:*

(a) $3\mathtt{x}90586\mathtt{y}$ *é divisível por* 60*.*

(b) $72\mathtt{z}41\mathtt{t}$ *é divisível por* 99*.*

Solução: (a) $3\mathtt{x}90586\mathtt{y}$ é divisível por $60 = 2^2 \cdot 3 \cdot 5$ se, e somente se, é divisível simultaneamente por 4, 3 e 5.

(i) $3\mathtt{x}90586\mathtt{y}$ é divisível por 5 se, e somente se, $\mathtt{y} = 0$ ou $\mathtt{y} = 5$.

(ii) $3\mathtt{x}90586\mathtt{y}$ é divisível por 4 se, e somente se, $6\mathtt{y}$ é divisível por 4. Pelo item anterior, $\mathtt{y} = 0$, pois 65 não é divisível por 4.

(iii) $3\mathtt{x}905860$ é divisível por 3 se, e somente se, $3 + \mathtt{x} + 9 + 0 + 5 + 8 + 6 + 0 = 31 + \mathtt{x}$ é divisível por 3. Os possíveis valores para $\mathtt{x}$ são: 2, 5, 8.

Resposta: 32905860, 35905860 ou 38905860.

(b) $72\mathtt{z}41\mathtt{t}$ é divisível por $99 = 9 \cdot 11$ se, e somente se, é divisível simultaneamente por 9 e 11.

(i) $72\mathtt{z}41\mathtt{t}$ é divisível por 9 se, e somente se, $7 + 2 + \mathtt{z} + 4 + 1 + \mathtt{t} = 14 + \mathtt{z} + \mathtt{t}$ é divisível por 9. Então $\mathtt{z} + \mathtt{t} = 4$ ou $\mathtt{z} + \mathtt{t} = 13$.

(ii) $72\mathtt{z}41\mathtt{t}$ é divisível por 11 se, e somente se, $\mathtt{t} - 1 + 4 - \mathtt{z} + 2 - 7 = \mathtt{t} - \mathtt{z} - 2$ é divisível por 11. Então $\mathtt{t} - \mathtt{z} = -9$ ou $\mathtt{t} - \mathtt{z} = 2$.

Primeiro caso: $\begin{cases} \mathtt{z} + \mathtt{t} = 4 \\ \mathtt{t} - \mathtt{z} = -9 \end{cases}$, sem solução inteira. Segundo caso: $\begin{cases} \mathtt{z} + \mathtt{t} = 4 \\ \mathtt{t} - \mathtt{z} = 2 \end{cases} \iff \mathtt{z} = 1$ e $\mathtt{t} = 3$.

Terceiro caso: $\begin{cases} \mathtt{z} + \mathtt{t} = 13 \\ \mathtt{t} - \mathtt{z} = -9 \end{cases} \iff \mathtt{z} = 11$ e $\mathtt{t} = 2$. Quarto caso: $\begin{cases} \mathtt{z} + \mathtt{t} = 13 \\ \mathtt{t} - \mathtt{z} = 2 \end{cases}$, sem solução inteira.

Logo, 721413 é o número encontrado.

3.2 Dígito verificador

Atualmente a aplicação da conguência modular é bem ampla, uma delas é na "Criptografia", que estuda métodos para modificar as informações gerando mais segurança, o dígito verificador é uma importante ferramenta em validação e autenticação de documentos importantes, como por exemplo CPF, título de eleitor, cartões de créditos, ISBN, código de barra entre outros, tem como base uma sequências numéricas.

3.2.1 CPF

O Cadastro de Pessoa Física (CPF) é o documento que identifica o contribuinte perante a Receita Federal. Cada contribuinte pessoa física possui um Cartão CPF, ou simplesmente CPF, que comprova o cadastro. Ele contém um número identificador que não muda. Não é obrigatório portar o cartão, mas o número do CPF é exigido em várias situações, principalmente em operações financeiras, como abertura de contas em bancos.[1]

O cadrasto possui 11 dígitos, dos quais os nono dígito identifica o estado brasileito de emissão da pessoa conforme a tabela 1, já o ultimo dois ultimos dígitos são os verificadores.

[1] `http://www.caixa.gov.br/cadastros/cpf/Paginas/default.aspx`

Tabela 1: Dígito idetificador do estado

9º dígito	**Estados emissor**
0	RS
1	DF, GO, MS, MT, TO
2	AC, AM, AP, PA, RO, RR
3	CE, PI, MA
4	AL, PB, PE, RN
5	BA, SE
6	MG
7	ES, RJ
8	SP
9	PR, SC

Para determinar os dois dígitos verificadores, tomamos a sequência dos dígitos que compõe o CPF: $a_1a_2a_3a_4a_5a_6a_7a_8a_9 - a_{10}a_{11}$. O primeiro digíto verificador a_{10} é determinado pela seguinte congruência:

$$a_{10} \equiv S \pmod{11},$$

onde $S = \sum_{i=1}^{9} i \cdot a_i$.

Já o segundo dígito verificador a_{11} é determinado pela seguinte congruência:

$$a_{11} \equiv P \pmod{11},$$

onde $P = \sum_{i=1}^{10} (i-1) \cdot a_i$.

Figura 2: Cadastro de Pessoa Física - CPF

Fonte: Municipio Bento Goncalves - Cadastro de Pessoa Física - CPF

Exemplo 3.21. *Determine os dígitos verificadores do seguinte número fictício de CPF:* **467.539.150**–$a_{10}a_{11}$.

Solução: Vamos determinar o primeiro dígito calculando a seguinte soma

$$\begin{aligned} S &= \sum_{i=1}^{9} i \cdot a_i \\ S &= 1 \cdot 4 + 2 \cdot 6 + 3 \cdot 7 + 4 \cdot 5 + 5 \cdot 3 + 6 \cdot 9 + 7 \cdot 1 + 8 \cdot 5 + 9 \cdot 0 \\ S &= 4 + 12 + 21 + 20 + 15 + 54 + 7 + 40 + 0 \\ S &= 173 \end{aligned}$$

assim, tem-se

$$a_{10} \equiv S \pmod{11} \Longrightarrow a_{10} \equiv 173 \pmod{11} \Longrightarrow a_{10} \equiv 8 \pmod{11},$$

logo $a_{10} = 8$. Da mesma forma o a_{11} é

$$\begin{aligned} P &= \sum_{i=1}^{10} (i-1) \cdot a_i \\ P &= 0 \cdot 4 + 1 \cdot 6 + 2 \cdot 7 + 3 \cdot 5 + 4 \cdot 3 + 5 \cdot 9 + 6 \cdot 1 + 7 \cdot 5 + 8 \cdot 0 + 9 \cdot 8 \\ P &= 0 + 6 + 14 + 15 + 12 + 45 + 6 + 35 + 0 + 72 \\ P &= 205 \end{aligned}$$

daí resulta a seguinte congruência

$$a_{11} \equiv P \pmod{11} \Longrightarrow a_{11} \equiv 205 \pmod{11} \Longrightarrow a_{11} \equiv 7 \pmod{11},$$

portanto $a_{11} = 7$. Logo temos que o número do CPF é 467.539.150 - 87. Pois, além disso $4 + 6 + 7 + 5 + 3 + 9 + 1 + 5 + 0 + 8 + 7 = 40 \equiv 0 (\mathrm{mod}\ 11)$.

3.2.2 Cartão de crédito

O surgimento do cartão de crédito foi por volta de 1950 onde Frank MacNamara estava com executivos financeiros em um restaurante na cidade de Nova York e percebeu que tinha esquecido seu dinheiro e seu talão de cheques para pagar a conta. E teve a ideia de criar um cartão em que contivesse o nome do dono. Após um tempo, o dono do cartão pudesse pagar a conta, começando assim a história do cartão de crédito. Essa criação chegou ao Brasil somente em 1956 por o "Diners". Inicialmente funcionava como um cartão de compra e não um cartão de crédito. Alguns anos depois, em 1968, foi lançado o primeiro cartão de crédito de banco o "Credicard".

No Brasil os cartões de crédito possuem 16 dígitos, sendo que os primeiros quinze dígitos determinam a bandeira emissora e dados do cliente, somente o último dígito será o

dígito verificador. Para determinar esse dígito verificador usaremos o Algoritmo de Luhn, criado por Hans Peter Luhn em 1954.

Para determinar o dígito verificador consideramos a seguinte sequência dos dígitos de um cartão de crédito:

$$a_1a_2a_3a_4 \ . \ a_5a_6a_7a_8 \ . \ a_9a_{10}a_{11}a_{12} \ . \ a_{13}a_{14}a_{15}a_{16}$$

Para deteminar o dígito verificador a_{16} devemos primeiro tomamos os dígitos com índice ímpares e calculamos o k_i, da seguinte forma: $k_i = \begin{cases} 2 \cdot a_i & \text{se } 2 \cdot a_i \leqslant 9 \\ 2 \cdot a_i - 9 & \text{se } 2 \cdot a_i > 9 \end{cases}$. Calculamos agora a soma S pelo somatório desses k_i com o somatório dos a_i de índice par, dado por:

$$S = \sum_{i=1}^{8} k_{2i-1} + \sum_{i=1}^{8} a_{2i},$$

logo o dígito verificador a_{16} resulta da seguinte congruência:

$$a_{16} \equiv -S \pmod{10}.$$

Exemplo 3.22. *Determine o dígito verificador do cartão de credito fictício, cujo os primeiros quizes dígitos é dado por:* $2134.5678.9012.345a_{16}$.

Solução: Vamos determinar os k_i

$$\begin{aligned}
k_1 &= 2 \cdot a_1 = 2 \cdot 2 = 4 \leqslant 9 \implies k_1 = 4 \\
k_3 &= 2 \cdot a_3 = 2 \cdot 3 = 6 \leqslant 9 \implies k_3 = 6 \\
k_5 &= 2 \cdot a_5 = 2 \cdot 5 = 10 > 9 \implies k_5 = 2 \cdot a_5 - 9 \Longrightarrow k_5 = 1 \\
k_7 &= 2 \cdot a_7 = 2 \cdot 7 = 14 > 9 \implies k_7 = 2 \cdot a_7 - 9 \Longrightarrow k_7 = 5 \\
k_9 &= 2 \cdot a_9 = 2 \cdot 9 = 18 > 9 \implies k_9 = 2 \cdot a_9 - 9 \Longrightarrow k_9 = 9 \\
k_{11} &= 2 \cdot a_{11} = 2 \cdot 1 = 2 \leqslant 9 \implies k_{11} = 2 \\
k_{13} &= 2 \cdot a_{13} = 2 \cdot 3 = 6 \leqslant 9 \implies k_{13} = 6 \\
k_{15} &= 2 \cdot a_{15} = 2 \cdot 5 = 10 > 9 \implies k_{15} = 2 \cdot a_{15} - 9 \Longrightarrow k_{15} = 1
\end{aligned}$$

Aplicando o algoritmo temos

$$\begin{aligned} S &= \sum_{i=1}^{8} k_{2i-1} + \sum_{i=1}^{8} a_{2i} \\ S &= (4+6+1+5+9+2+6+1) + (1+4+6+8+0+2+4) \\ S &= 34+25 \\ S &= 59, \end{aligned}$$

usando a congruência

$$a_{16} \equiv -S \pmod{10} \Rightarrow a_{16} \equiv -59 \pmod{10} \Rightarrow a_{16} = 9.$$

Logo, temos que, o dígito verificador $a_{16} = 9$, portanto o cartão de crédito tem a seguinte númeração: 2134.5678.9012.3459

4 Equações Diofantinas Lineares

Nesse capítulo é abordado as Equações Diofantinas Lineares. Será utilizado o Algoritmo de Euclides como resolução e demostração de alguns fatos. Será abordado também problemas e exemplos que permitirá alcança um novo modo de resolução de questões no vasto universo da matemática. Equações Diofantinas são equações polinomiais com coeficientes inteiros duas ou mais variáveis que admitem apenas soluções inteiras. Segundo FILHO (1984) e SANTOS (2009):

4.1 Método do Algarismo de Euclides

Definição 4.1. *Uma equação diofantina linear é qualquer equação polinomial com coeficientes inteiros com uma ou mais incógnitas, uma equação do tipo*

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b, \tag{4.1}$$

com, a_1,a_2, ..., a_n *inteiros dados, chamados coeficientes,* b *que também é um inteiro dado, é chamado termo constante e* x_1,x_2, ..., x_n *são as incógnitas.*

Exemplo 4.1. *Alguns exemplos de Equações Diofantinas:*

i) $256x + 127y = 12$*;*

ii) $5x + 9y = 17$*;*

iii) $2x + 3y + 5z = 11$*;*

iv) $3x + 6y + 18z = 18$*;*

O tipo mais simples de equação diofantina linear abordado é para um caso particular quando $n = 2$, ou seja, é uma equação diofantina linear com duas incógnitas x e y, isto é:

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

onde a, b e c são inteiros dados, sendo $ab \neq 0$.

Todo par de inteiros x_0 e y_0 é dito solução inteira da equação quando:

$$ax_0 + by_0 = c$$

Exemplo 4.2. *Resolvendo a equação diofantina lineaar com duas incógnitas:*

$$14x + 22y = 50.$$

Tem–se

$$\begin{aligned} 14 \cdot 2 + 22 \cdot 1 &= 50 \\ 14 \cdot 13 + 22 \cdot (-6) &= 50 \\ 14 \cdot 46 + 22 \cdot (-27) &= 50 \\ 14 \cdot (-9) + 22 \cdot 8 &= 50 \\ 14 \cdot (-20) + 22 \cdot 15 &= 50. \end{aligned}$$

Portanto, os pares de inteiros: 2 *e* 1, 13 *e* -6, 46 *e* -27, -9 *e* 8, -20 *e* 15 *são soluções da equação* $14x + 22y = 50$.

Entretanto existem equações lineares com duas incógnitas que não admitem soluções. Observe que a equação diofantina linear:

$$2x + 8y = 7,$$

não têm solução, pois não existe um x e y que, quando substituido na equação resulte em 7, ou seja, $2x + 8y$ resulta num número par para quaisquer valores de x e y, onde 7 é um inteiro ímpar. Dessa forma não existe x e y que satisfaz a equação diofantina linear $2x + 8y = 7$.

Teorema 4.1. *A Equação Diofantina Linear* $ax + by = c$ *tem solução se e, somente se,* d *divide* c*, sendo que* $d = mdc(a, b)$.

Demonstração. ($\Longrightarrow$) Suponha que x_0 e y_0 seja uma solução para a equação Diofantina linear $ax + by = c$, assim:

$$ax_0 + by_0 = c.$$

Como o $mdc(a, b) = d$, existem inteiros r e s tais que $a = dr$ e $b = ds$, e temos:

$$c = ax_0 + by_0 = drx_0 + dsy_0 = d(rx_0 + sy_0).$$

Assim $rx_0 + sy_0$ é inteiro, logo temos que d divide c, ou seja, $d \mid c$.

($\Longleftarrow$) Suponha que d divide c, ou seja, $d \mid c$, assim existe t inteiro tal que

$$c = dt. \tag{4.3}$$

Como o mdc(a,b) = d, existem inteiros x_0 e y_0 tais que

$$d = ax_0 + by_0. \tag{4.4}$$

Multiplicando a equação (4.4) por t temos:

$$d \cdot t = (ax_0 + by_0) \cdot t \quad \Longrightarrow \quad c = a(tx_0) + b(ty_0).$$

De (4.3) $t = \dfrac{c}{d}$, isto é, o par de inteiro

$$x = tx_0 = \left(\frac{c}{d}\right) \cdot x_0 \quad \text{e} \quad y = ty_0 = \left(\frac{c}{d}\right) \cdot y_0$$

é uma solução para a equação $ax + by = c$. □

Teorema 4.2. *Se* d *divide* c*, sendo* $d = mdc(a, b)$ *e se o par de inteiros* x_0 *e* y_0 *é uma solução particular da equação diofantina linear* $ax + by = c$*, então todas as outras soluções desta equação são dadas pela fórmula:*

$$x = x_0 + \left(\frac{b}{d}\right) \cdot t \quad e \quad y = y_0 - \left(\frac{a}{d}\right) \cdot t,$$

com t *um inteiro qualquer.*

Demonstração. Suponha que x_0 e y_0 inteiros seja uma solução particular para a equação diofantina linear $ax + by = c$, e seja x_1 e y_1 outra solução qualquer da mesma equação. Então

$$\begin{aligned} x_0 + by_0 = \quad & c \quad = ax_1 + by_1 \\ & \Downarrow \\ a(x_1 - x_0) \quad = \quad & b(y_0 - y_1). \end{aligned} \tag{4.5}$$

Como o $mdc(a, b) = d$, existem inteiros r e s tais que $a = dr$ e b = ds, com r e s primos entre si, substituindo em (4.5) tem–se:

$$(dr)(x_1 - x_0) = (ds)(y_0 - y_1) \Longrightarrow r \cdot (x_1 - x_0) = s \cdot (y_0 - y_1)$$

Assim $r \mid s(y_0 - y_1)$, e sabendo que o $mdc(r, s) = 1$ implica que $r \mid (y_0 - y_1)$. Dessa

forma para qualquer número t inteiro teremos:

$$y_0 - y_1 = rt \quad \text{e} \quad x_1 - x_0 = st.$$

Como $a = dr \Rightarrow r = \dfrac{a}{d}$ e $b = ds \Rightarrow \dfrac{b}{d}$, temos as fórmulas:

$$x_1 = x_0 + \left(\frac{b}{d}\right)\cdot t \quad \text{e} \quad y_1 = y_0 - \left(\frac{a}{d}\right)\cdot t.$$

□

Os valores de x_1 e y_1 satisfazem qualquer equação da forma $ax+by = c$, para qualquer inteiro t. Observe que:

$$\begin{aligned} c &= ax_1 + by_1 \\ &= a\left[x_0 + \left(\frac{b}{d}\right)\cdot t\right] + b\left[y_0 - \left(\frac{a}{d}\right)\cdot t\right] \\ &= \left(ax_0 + by_0\right) + \left(\frac{ab}{d} - \frac{ab}{d}\right)\cdot t \\ &= c + 0 \cdot t \\ &= c. \end{aligned}$$

Portanto, se $\mathtt{mdc}(a, b) = d$ e $d \mid c$, então para qualquer equação diofantina da forma $ax+by = c$ existiram uma infinidade de soluções, uma para cada valor do inteiro arbitrário t.

Para encontrar uma solução particular existe duas formas, a primeira é por tentativas e a outra forma é pelo Algoritmo de Euclides. Nos dois caso a solução geral é obtida usando o Teorema (4.2).

Exemplo 4.3. *Determine todas as soluções da equaçõa diofantina linear*

$$56x + 72y = 40. \tag{4.6}$$

Solução: Primeiro deve–se encontrar o $\mathtt{mdc}(56, 72)$, pelo Algoritmo de Euclides.

	1	3	2
72	56	16	8
16	8	0	

Portanto o $\mathtt{mdc}(56, 72) = 8$ e como $8 \mid 40$, segue que a equação (4.6) tem solução.

Dessa forma escreve–se cada divisão da seguinte maneira:

$$\begin{aligned} 72 &= 56 \cdot 1 + 16 && (4.7)\\ 56 &= 16 \cdot 3 + 8 && (4.8)\\ 16 &= 8 \cdot 2 + 0. \end{aligned}$$

Isolando os restos 8 e 16 nas expressões (4.8) e (4.7) respectivamente, temos:

$$\begin{aligned} 16 &= 72 - 56 \cdot 1 && (4.9)\\ 8 &= 56 - 16 \cdot 3. && (4.10) \end{aligned}$$

Substituindo (4.9) em (4.10), obtem–se:

$$\begin{aligned} 8 &= 56 - \Big(72 - 56 \cdot 1\Big) \cdot 3\\ &= 56 \cdot 4 + 72 \cdot (-3). \end{aligned}$$

Logo, o par de inteiros $\mathtt{x}_0 = 4$ e $\mathtt{y}_0 = -3$ é uma solução particular para a equação (4.6). E todas as outras soluções são dadas pelas fórmulas:

$$\begin{aligned} \mathtt{x} = 4 + \left(\frac{72}{8}\right) \cdot \mathtt{t} &\implies \mathtt{x} = 4 + 9 \cdot \mathtt{t}\\ \mathtt{y} = -3 - \left(\frac{56}{8}\right) \cdot \mathtt{t} &\implies \mathtt{y} = -3 - 7 \cdot \mathtt{t}, \end{aligned}$$

com $\mathtt{t}$ um inteiro qualquer.

Exemplo 4.4. *Determine todas as soluções inteiras e positivas da equação diofantina linear*

$$5\mathtt{x} - 11\mathtt{y} = 29. \tag{4.11}$$

Solução: Determinamos primeiramente o $\mathtt{mdc}(5, 11)$, pelo Algoritmo de Euclides tem–se:

	2	5
11	5	1
1	0	

Portanto o $\mathtt{mdc}(5, 11) = 1$ e como $1 \mid 29$, segue que a equação (4.11) tem solução. Dessa forma exprimir 1 como combinação linear de 5 e 11, assim podemos escrever cada

divisão da seguinte maneira:

$$\begin{aligned} 11 &= 5 \cdot 2 + 1 \\ 5 &= 1 \cdot 5 + 0. \end{aligned} \tag{4.12}$$

Pela expressão (4.12) tem–se que:

$$1 = 11 - 5 \cdot 2 \Rightarrow 5 \cdot (-2) - 11 \cdot (-1) = 1 \Rightarrow 5 \cdot (-58) - 11 \cdot (-29) = 29.$$

Logo, o par de inteiros $\mathtt{x}_0 = -58$ e $\mathtt{y}_0 = -29$ é uma solução particular para a equação (4.11). E todas as outras soluções são dadas pelas fórmulas:

$$\begin{aligned} \mathtt{x} = -58 + \left(\frac{-11}{1}\right) \cdot \mathtt{t} &\implies \mathtt{x} = -58 - 11 \cdot \mathtt{t} \\ \mathtt{y} = -29 - \left(\frac{5}{1}\right) \cdot \mathtt{t} &\implies \mathtt{y} = -29 - 5 \cdot \mathtt{t}, \end{aligned}$$

com $\mathtt{t}$ um inteiro qualquer.

Escolhendo um $\mathtt{t}$ para que as soluções inteiras e positivas, basta que satisfaça as seguintes desigualdades:

$$-58 - 11 \cdot \mathtt{t} > 0 \quad \text{e} \quad -29 - 5 \cdot \mathtt{t} > 0.$$

Assim,

$$-58 - 11 \cdot \mathtt{t} > 0 \Rightarrow \mathtt{t} < -\frac{58}{11} \Rightarrow \mathtt{t} < -5\frac{3}{11} \Rightarrow \mathtt{t} \leqslant -6,$$

e

$$-29 - 5 \cdot \mathtt{t} > 0 \Rightarrow \mathtt{t} < -\frac{29}{5} \Rightarrow \mathtt{t} < -6\frac{1}{5} \Rightarrow \mathtt{t} \leqslant -6.$$

Se tomarmos $\mathtt{t} = -6$ tem–se:

$$\begin{aligned} \mathtt{x} = -58 - 11 \cdot (-6) \Rightarrow \mathtt{x} = 8. \\ \mathtt{y} = -29 - 5 \cdot (-6) \Rightarrow \mathtt{y} = 1. \end{aligned}$$

Logo, existe solução inteira e positiva quando $\mathtt{t} \leqslant -6$.

Exemplo 4.5. *Determine todas as soluções da equaçõa diofantina linear*

$$57\mathtt{x} - 99\mathtt{y} = 77. \tag{4.13}$$

Solução: O $\mathtt{mdc}(57, 99) = 3$, mas 3 não divide 77, ou seja $3 \nmid 77$, dessa forma a equação (4.13) não possui solução inteiras.

Problema 4.1 (OBMEP)**.** *Para fazer várias blusas iguais, uma costureira gastou* R$ $2,99$ *para comprar botões de* 4 *centavos e laços de* 7 *centavos. Ela usou todos os botões e laços que comprou. Quantas blusas ela fez?*

A) 2

B) 5

C) 10

D) 13

E) 23

Solução: Chamando de $\mathtt{x}$ o número de laços e $\mathtt{y}$ o número de botões, temos:

$$0,07\mathtt{x} + 0,04\mathtt{y} = 2,99.$$

Mulplicando a equação por 100, obtemos:

$$7\mathtt{x} + 4\mathtt{y} = 299. \tag{4.14}$$

Pelo Algoritmo de Euclides temos:

	1	1	3
7	4	3	1
3	1	0	

Portanto o $\mathtt{mdc}(7,4) = 1$ e como $1 \mid 299$, segue que a equação (4.14) tem solução. Dessa forma exprimir 1 como combinação linear de 7 e 4, assim escrever–se cada divisão da seguinte maneira:

$$\begin{aligned} 7 &= 4 \cdot 1 + 3 && (4.15)\\ 4 &= 3 \cdot 1 + 1 && (4.16)\\ 3 &= 1 \cdot 3 + 0. \end{aligned}$$

Isolando os restos 1 e 3 nas expressões (4.16) e (4.15) respectivamente, tem–se:

$$\begin{aligned} 3 &= 7 - 4 \cdot 1 && (4.17)\\ 1 &= 4 - 3 \cdot 1. && (4.18) \end{aligned}$$

Substituindo (4.17) em (4.18), obtem–se:

$$\begin{aligned} 1 &= 4-\left(7-4\cdot 1\right)\cdot 1 \\ &= 7\cdot(-1)+4\cdot 2. \end{aligned} \tag{4.19}$$

Multiplicando (4.19) por 299, obtem–se:

$$7\cdot(-299)+4\cdot 598 = 299.$$

Logo, o par de inteiros $x_0 = -299$ e $y_0 = 598$ é uma solução particular para a equação (4.14). E todas as outras soluções são dadas pelas fórmulas:

$$\begin{aligned} x = -299+\left(\frac{4}{1}\right)\cdot t &\implies x = -299+4\cdot t \\ y = 598-\left(\frac{7}{1}\right)\cdot t &\implies y = 598-7\cdot t, \end{aligned}$$

com t um inteiro qualquer.

Escolhendo um t para que as soluções sejam inteiras e positivas, basta que satisfaça as seguintes desigualdades:

$$-299+4\cdot t > 0 \quad \text{e} \quad 598-7\cdot t > 0.$$

Assim,

$$-299+4\cdot t > 0 \Rightarrow t > \frac{299}{4} \Rightarrow t > 74\frac{3}{4} \Rightarrow t \geqslant 75,$$

e

$$598-7\cdot t > 0 \Rightarrow t < \frac{598}{7} \Rightarrow t < 85\frac{3}{7} \Rightarrow t \leqslant 84.$$

Tem–se uma solução inteira e positiva basta tomar $75 \leqslant t \leqslant 84$. Se tomar $t = 78$ tem–se:

$$\begin{aligned} x = -299+4\cdot 78 \Rightarrow x = 13, \\ y = 598-7\cdot 78 \Rightarrow y = 52. \end{aligned}$$

O número de botões deve ser múltiplo do número de laços, pois suponhamos que em cada blusa existirá um laço e a mesma quantidade de botões por blusa. Dessa forma como $x = 13$ laços tem–se 13 blusas. Resposta será a letra D).

4.2 Congruências Lineares

Definição 4.2. *Sejam* a *e* b *inteiros quaisquer e* m *um inteiro positivo, define–se congruência linear toda equação da forma:*

$$ax \equiv b(\mathrm{mod}\ m). \tag{4.20}$$

Para todo inteiro x_0 que satisfaz a equação (4.20) tal que

$$ax_0 \equiv b(\mathrm{mod}\ m)$$

diz–se que x_0 é uma solução para a congruência linear. Daí, também temos $m \mid (ax_0 - b)$, ou seja, existe um inteiro y_0 tal que

$$ax_0 - b = my_0 \Rightarrow ax_0 - my_0 = b. \tag{4.21}$$

Dessa forma o problema é encontra todas soluções inteiras que satisfazem a Equação Diofantina Linear (4.21). Perceba que o inteiro x_0 é uma solução particular da congruência linear $ax \equiv b(\mathrm{mod}\ m)$, onde podemos construir uma infinidade de outras soluções, todas mutuamente congruentes módulo m.

Se a equação (4.20) possui duas soluções quaisquer x_1 e x_2 que são congruentes módulo m, ou seja, $ax_1 \equiv x_2(\mathrm{mod}\ m)$, essas soluções não são consideradas distintas, o interessante é determinar as soluções duas a duas mutamente incongruentes módulo m, as quais são chamadas de sistema completo de soluções incongruentes da congruência.

Portanto uma congruência linear definida como: $ax \equiv b(\mathrm{mod}\ m)$. Pode ter apenas uma solução ou ter varias soluções ou não existir solução.

Teorema 4.3. *A congruência linear* $ax \equiv b(\mathrm{mod}\ m)$ *tem solução se e somente se* d *divide* b*, sendo* $d = \mathrm{mdc}(a, m)$*.*

Demonstração. ($\Longrightarrow$) Suponhamos que a congruência linear adimita solução e seja o inteiro x_0 sua solução, então

$$ax_0 \equiv b(\mathrm{mod}\ m).$$

Existe um inteiro y_0, tal que

$$\begin{aligned} ax_0 - b &= my_0 \\ &\Downarrow \\ ax_0 - my_0 &= b. \end{aligned}$$

Pelo Teorema 2.4 existe um inteiro d tal que $d \mid a$ e $d \mid m$, porque $d = mdc(a, m)$, segue que $d \mid (ax_0 - my_0)$ e, logo, $d \mid b$.

($\Longleftarrow$) Se $d \mid b$, isto e, existe inteiro k tal que $b = dk$. Como o $d = mdc(a, m)$, da mesma forma pelo Teorema 2.4, existem inteiros x_0 e y_0 tal que

$$ax_0 + my_0 = d, \tag{4.22}$$

multiplicando ambos os membros a igualdade (4.22) por k, temos:

$$a(x_0 \cdot k) + m(y_0 \cdot k) = d \cdot k = b \Rightarrow a(x_0 \cdot k) - b = m(y_0 \cdot k) \Rightarrow a(x_0 \cdot k) \equiv b(mod\ m).$$

Portanto, o inteiro $(k \cdot x_0)$ é uma solução da congruência linear: $ax \equiv b(mod\ m)$. □

Teorema 4.4. *Sejam a, b e m inteiros e $d \mid b$. Se x_0 é uma solução da congruência $ax \equiv b(mod\ m)$, então*

$$x_0, \quad x_0 + \frac{m}{d}, \quad x_0 + 2 \cdot \frac{m}{d}, \quad x_0 + 3 \cdot \frac{m}{d}, \quad \ldots, \quad x_0 + (d-1) \cdot \frac{m}{d},$$

onde $d = mdc(a, m)$, forma um sistema completo de solulções da congruência, duas a duas incongruentes módulo m.

Demonstração. Todas solução x da congruência $ax \equiv b(mod\ m)$ é congruente módulo m, a $x_0 + i \cdot \frac{m}{d}$ para algum $0 \leqslant i < d$, então:

$$ax \equiv ax_0(mod\ m),$$

e, portanto, pelo Teorema 3.3,

$$x \equiv x_0 \left(mod\ \frac{m}{d} \right)$$

Logo, $x - x_0 = \frac{km}{d} \Rightarrow k = \frac{(x - x_0)d}{m}$, onde k é inteiro. Pela divisão euclidiana, existe

$0 \leqslant i < d$ tal que $k = qd + i$ e, portanto,

$$\begin{aligned} \frac{(x - x_0)d}{m} &= qd + i \\ x - x_0 &= qm + i \cdot \frac{m}{d} \\ x - \left(x_0 + i \cdot \frac{m}{d}\right) &= qm, \end{aligned}$$

daí temos que $x \equiv x_0 + i \cdot \frac{m}{d} \left(\mod m\right)$

Reciprocamente, os números $x_0 + i \cdot \frac{m}{d}$, com $0 \leqslant i < d$, são soluções da congruência $ax \equiv b (\mod m)$, pois,

$$a\left(x_0 + i \cdot \frac{m}{d}\right) = ax_0 + i \cdot \frac{a \cdot m}{d} \equiv ax_0 \equiv b (\mod m).$$

Finalmente, esses números são dois a dois incongruentes módulo m, pois se, $0 \leqslant i, j < d$,

$$x_0 + i \cdot \frac{m}{d} \equiv x_0 + j \cdot \frac{m}{d} (\mod m),$$

então

$$i \cdot \frac{m}{d} \equiv j \cdot \frac{m}{d} (\mod m).$$

Como $0 \leqslant i, j < d$, entaão $0 \leqslant i \cdot \frac{m}{d}, j \cdot \frac{m}{d} < m$, e como m divide $\left| i \cdot \frac{m}{d} - j \cdot \frac{m}{d} \right|$, segue–se que $i \cdot \frac{m}{d} = j \cdot \frac{m}{d} \Rightarrow i = j$. □

Foi visto até agora que se uma congruência linear $ax \equiv b (\mod m)$ é equivalente a uma Equação Diofantina Linear, ou seja, $ax - my = b$, no qual admite solução se, e somente se, $d \mid b$ onde $d = mdc(a, m)$. Além disso pelo Teorema 4.2, todas as outras soluções para uma Equação Diofantina Linear são dadas pela fórmula:

$$x = x_0 + \left(\frac{b}{d}\right) \cdot t \quad \text{e} \quad y = y_0 - \left(\frac{a}{d}\right) \cdot t$$

onde t é um inteiro qualquer.

Dessa fórmula se atribuimos a t os valores: 0, 1, 2, 3, ..., $d - 1$, ou seja, d inteiros:

$$x_0, \quad x_0 + \frac{m}{d}, \quad x_0 + 2 \cdot \frac{m}{d}, \quad x_0 + 3 \cdot \frac{m}{d}, \quad \ldots, \quad x_0 + (d - 1) \cdot \frac{m}{d},$$

Vamos mostrar que estes d inteiros são mutuamente incongruentes módulo m e que todos os outros inteiros dados da forma $x = x_0 + \left(\frac{b}{d}\right) \cdot t$ são congruêntes módulo m a

algum d inteiro. Diante disso enunciaremos o seguinte corolário.

Corolário 4.1. *Se* d *divide* b*, sendo* $d = mdc(a, m)$*, então a congruência linear*

$$ax \equiv b(mod\ m)$$

tem precisamente d *soluções mutuamente incongruentes módulo* m*.*

Demonstração. Suponhamos que x_0 seja solução para a congruência linear, então todas as soluções x são da forma $x = x_0 + \left(\frac{b}{d}\right)\cdot t$, com t é um inteiro qualquer. Se

$$x_1 = x_0 + \left(\frac{m}{d}\right)\cdot t_1 \quad \text{e} \quad x_2 = x_0 + \left(\frac{m}{d}\right)\cdot t_2$$

são soluções, e se $x_1 \equiv x_2(mod\ m)$, então

$$\begin{aligned} x_0 + \left(\frac{m}{d}\right)\cdot t_1 &\equiv x_0 + \left(\frac{m}{d}\right)\cdot t_2 (mod\ m) \\ t_1 &\equiv t_2 \left(mod\ \frac{m}{(m, \frac{m}{d})}\right) \\ t_1 &\equiv t_2 (mod\ d) \end{aligned}$$

visto que o $mdc\left(m, \frac{m}{d}\right) = \frac{m}{d}$ e $0 \leqslant t_1 < t_2 \leqslant d - 1$. Isso nos diz que $d \mid (t_2 - t_1)$, o que é impossível, isto é, $0 < t_2 - t_1 < d$.

Dessa forma para qualquer inteiro $x_0 + \left(\frac{m}{d}\right)\cdot t$ é congruente módulo m para algum d. Logo, duas soluções x_1 e x_2 são mutuamente incongruente módulo m se, e somente se, t_1 e t_2 são incongruente módulo d, então existem d soluções mutuamente incongruentes. □

Exemplo 4.6. *Resolva a conguência linear* $3x \equiv 6(mod\ 15)$

Solução: Temos que $mdc(3, 6) = 3$ e como $3 \mid 15$, a congruência dada tem exatamete 3 soluções mutuamente incongruentes módulo 15. Dessa forma $x_0 = 2$ é uma solução para a congruência linear $3x \equiv 6(mod\ 15)$, e por conseguinte as suas 3 soluções, são dadas pela fómula:

$$x = 2 + \left(\frac{15}{3}\right)\cdot t = 2 + 5t,$$

onde $t = 0,\ 1,\ 2$.

Logo,

$$x = 4,\ 7,\ 12.$$

Como foi demonstrado, a equação diofantina linear $ax + by = c$ admite solução se e somente se $d \mid c$, onde $d = mdc(a, b)$. Nessas condições dizer que x_0 e y_0 é uma solução

particular para qualquer equação, então:

$$ax_0 + by_0 = c \quad \Longrightarrow \quad ax_0 - c = -b_0,$$

o que nos implica

$$ax_0 \equiv c(\mathrm{mod}\ b) \qquad \text{ou} \qquad by_0 \equiv c(\mathrm{mod}\ a).$$

Assim para se obter uma solução particular da equação diofantina linear da forma $ax + by = c$, basta determinar uma solução para a congruência linear $ax_0 \equiv c(\mathrm{mod}\ b)$, se x_0 é uma solução, basta substituir esse valor em x na equação diofantina.

Exemplo 4.7. *Resolva por congruência linear a equação diofantina linear:* $9x+16y = 35$.

Solução: Como o $\mathrm{mdc}(9, 16) = 1$, a equação em questão admite solução, assim determinar uma solução para a equação diofantina, basta determinar uma solução para a equação

$$16y \equiv 35(\mathrm{mod}\ 9).$$

O $\mathrm{mdc}(16, 35) = 1$ e como $1 \mid 9$, a congruência dada tem exatamente uma solução mutuamente incongruentes módulo 9. Dessa forma $y_0 = 5$ é uma solução para a congruência linear $16y \equiv 35(\mathrm{mod}\ 9)$, e por conseguinte as suas soluções, são dadas pela fórmula:

$$y = 5+\left(\frac{9}{1}\right)\cdot t = 5 + 9t,$$

onde $t \in \mathbb{Z}$. Substituindo esse valor encontrado de y na equação diofantina linear dada, obtém–se

$$9x + 16 \cdot (5 + 9t) = 35 \Longrightarrow x = -5 - 16t.$$

Logo, todas as outras soluções para a equação diofantina linear $9x + 16y = 35$ são dadas pelas fórmulas:

$$x = -5 - 16t \qquad \text{e} \qquad y = 5 + 9t,$$

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

Exemplo 4.8. *Demonstrar que se* $d = \mathrm{mdc}(a, m)$ *e se* $d \mid b$*, então as congruênci as lineares:*

$$ax \equiv b(\mathrm{mod}\ m) \qquad e \qquad \left(\frac{a}{d}\right)x \equiv \left(\frac{b}{d}\right)\left(\mathrm{mod}\ \frac{m}{d}\right)$$

têm precisamente as mesma soluções.

Solução: Seja

$$\begin{aligned} ax \equiv b(\mathrm{mod}\ m) &\implies ax - my = b \\ &\implies \left(\frac{a}{d}\right)x - \left(\frac{m}{d}\right)y = \left(\frac{b}{d}\right) \\ &\implies \left(\frac{a}{d}\right)x \equiv \left(\frac{b}{d}\right)\left(\mathrm{mod}\ \frac{m}{d}\right). \end{aligned}$$

Portanto, as duas equações são equivalentes. O que leva a concluir que têm as mesmas soluções.

Definição 4.3. *Seja* y *um inteiro. Chama–se inverso de* y *módulo* m *um inteiro* $y^\star$ *tal que*

$$y \cdot y^\star \equiv 1(\mathrm{mod}\ m).$$

Teorema 4.5. *Se o* $\mathrm{mdc}(y, m) = 1$*, então* y *tem um único inverso módulo* m*.*

Demonstração. Como $\mathrm{mdc}(y, m) = 1$, então a congruência linear: $y \cdot x \equiv 1(\mathrm{mod}\ m)$. Tem um única solução $x_0(\mathrm{mod}\ m)$, isto é:

$$y \cdot x_0 \equiv 1(\mathrm{mod}\ m),$$

de modo que o inteiro y tem um único inverso módulo m: $y^\star = x_0$. □

Exemplo 4.9. *Achar o inverso de 3 módulo 7.*

Solução: Tem–se que a congruência linear:

$$3 \cdot y^\star \equiv 1(\mathrm{mod}\ 7) \implies y^\star = 5.$$

4.3 Classe Residuais

Introduziremos agora o conceito de classe residual módulo m. Veremos que o conjunto dos números inteiros poderá ser repartido em m subconjuntos, onde cada um deles é formado por todos os números inteiros que possuem o mesmo resto quando dividido por m.

Dado um inteiro positivo $m > 1$, repartiremos o conjunto $\mathbb{Z}$, dos números inteiros, em subconjuntos, onde cada um deles é formado por números inteiros que deixam o mesmo resto quando dividido por m. Esse conjunto é representado da seguinte forma:

$$\overline{0} = \{x \in \mathbb{Z} | \quad x \equiv 0 \pmod{m}\}$$

$$\overline{1} = \{x \in \mathbb{Z} | \quad x \equiv 1 \pmod{m}\}$$

$$\overline{2} = \{x \in \mathbb{Z} | \quad x \equiv 2 \pmod{m}\}$$

$$\vdots$$

$$\overline{m-1} = \{x \in \mathbb{Z} | \quad x \equiv m-1 \pmod{m}\}.$$

Segue-se que $\overline{m} = \overline{0}$, $\overline{m+1} = \overline{1}$ e assim por diante, assim o conjunto

$$\overline{a} = \{x \in \mathbb{Z} | \quad x \equiv a \pmod{m}\},$$

é chamado de classe residual módulo m do elementos a de $\mathbb{Z}$. O conjunto de todas as classes residuais módulo m será representado por $\mathbb{Z}_m$. Logo,

$$\mathbb{Z}_m = \{\overline{0},\ \overline{1},\ \overline{2},\ \ldots,\ \overline{m-1}\}.$$

Se $m = 2$, temos $\mathbb{Z}_2 = \{\overline{0},\ \overline{1}\}$, onde $\overline{0} = \{x \in \mathbb{Z} | \quad x \equiv 0 \pmod{2}\} = \{x \in \mathbb{Z} | \quad x = 2k,\ \text{com } k \in \mathbb{Z}\}$, ou seja, $\overline{0} = \{x \in \mathbb{Z} | \quad x \text{ é par}\}$. Analogamente temos $\overline{1} = \{x \in \mathbb{Z} | \quad x \equiv 1 \pmod{2}\} = \{x \in \mathbb{Z} | \quad x \text{ é ímpar}\}$. Logo,

$$\overline{a} = \begin{cases} \overline{0}, & \text{se e somente, se } a \text{ é par} \\ \overline{1}, & \text{se e somente, se } a \text{ é ímpar} \end{cases}.$$

Se $m = 3$, então tem-se que

$$\overline{a} = \begin{cases} \overline{0}, & a \text{ é múltiplo de 3} \\ \overline{1}, & a \text{ tem resto 1 quando dividido por 3} \\ \overline{2}, & a \text{ tem resto 2 quando dividido por 3} \end{cases}$$

tendo o conjunto das classes residuais módulo 3 é $\mathbb{Z}_3 = \{\overline{0},\ \overline{1},\ \overline{2}\}$. Se define também as seguintes operações em $\mathbb{Z}_m$:

Adição: $\overline{a} + \overline{b} = \overline{a+b}$;

Multiplicação: $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

Essas operações gozam das seguintes propriedades. Para todos $\overline{a},\ \overline{b},\ \overline{c} \in \mathbb{Z}_m$, temos

Propriedades da Adição.

A_1) Associatividade: $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$;

A_2) Comutatividade: $\overline{a} + \overline{b} = \overline{b} + \overline{a}$;

A_3) Existência de zero: $\overline{a} + \overline{0} = \overline{a}$ para todo $\overline{a} \in \mathbb{Z}_m$;

A_4) Existência de simétrico: $\overline{a} + \overline{-a} = \overline{0}$;

Propriedades da Multiplicação.

M_1) Associatividade: $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$;

M_2) Comutatividade: $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$;

M_3) Existência de unidade: $\overline{a} \cdot \overline{1} = \overline{a}$;

AM) Distributividade: $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$.

Todas as demonstrações das propriedades acima estão listadas em HEFEZ (2016). Logo, $\mathbb{Z}_m$, com as operações e gozando das propriedades acima é chamado *anel das classes residuais módulo* m. Definido anel das classes residuais, as tabelas da adição e da multiplicação em $\mathbb{Z}_2 = \{\overline{0},\ \overline{1}\}$, $\mathbb{Z}_3 = \{\overline{0},\ \overline{1},\ \overline{2}\}$ e $\mathbb{Z}_4 = \{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3}\}$ ficaram da seguinte forma:

Tabela 2: Adição e Multiplicação em $\mathbb{Z}_2$.

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Tabela 3: Adição e Multiplicação em $\mathbb{Z}_3$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Tabela 4: Adição e Multiplicação em $\mathbb{Z}_4$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

A classes residual tem uma importante característica que é a transformação a congruência $a \equiv b \pmod{m}$ gera uma igualdade $\overline{a} = \overline{b}$. Assim, ela permite resolver uma congruência $aX \equiv b \pmod{m}$ reduzindo a resolver em $\mathbb{Z}_m$ a seguinte equação:

$$\overline{a}Z = \overline{b}.$$

Exemplo 4.10. *Determine* P *múltiplo de* 4*, que possui quatro algarismos. Dividindo* P *por* 5 *encontramos resto igual a* 3*. Determine o menor valor de* P*.*

Solução: Temos que $\mathsf{P} = 4 \cdot \mathsf{x}$. Resolver a congruência em questão, equivale a resolver em $\mathbb{Z}_5$ a equação

$$[4] \cdot \mathsf{Z} = [3]. \tag{4.23}$$

Observe que $\overline{4} \cdot \overline{4} = \overline{1}$, logo $\overline{4}$ é invertível em $\mathbb{Z}_5$ com inverso $\overline{4}$. Portanto, multiplicando ambos os membros da equação (4.23) por $\overline{4}$ obtemos

$$\begin{aligned} \overline{4} \cdot \overline{4} \cdot \mathsf{Z} &= \overline{3} \cdot \overline{4} \\ \overline{1} \cdot \mathsf{Z} &= \overline{2} \\ \mathsf{Z} &= \overline{2} \end{aligned}$$

Portanto, $\overline{2}$ em $\mathbb{Z}_5$ é o conjunto dos números inteiros que dividido por 5 deixam resto 2, então são da forma $\mathsf{x} = 2 + 5\mathsf{t}$, com $\mathsf{t} \in \mathbb{Z}$. Como $\mathsf{P} \geqslant 1000 \Rightarrow 4\mathsf{x} \geqslant 1000 \Rightarrow \mathsf{x} \geqslant 250$, daí temos

$$2 + 5\mathsf{t} \geqslant 250 \Rightarrow 5\mathsf{t} \geqslant 248 \Rightarrow \mathsf{t} \geqslant 49,6,$$

logo $\mathsf{t} = 50$, assim $\mathsf{x} = 2 + 5 \cdot 50 = 252$. Portanto $\mathsf{P} = 4 \cdot 252 = 1008$.

5 Teorema Chinês dos Restos

A história relata que, na antiguidade os generais chineses logo depois de uma guerra, sempre contavam–se suas tropas para saber a quantidade de homens mortos em combate, fazendo isso da seguinte forma: ordenava em várias colunas com um certo padrão de tamanho, e repetia esse processo repetidas vezes com variados tamanhos, depois, contavam as tropas que restavam, assim o problema resultava no total de perdas.

Suponhamos que um general chinês possuísse 1800 soldados para uma determinada batalha. Ao fim do confronto, o general mandou que os soldados se pusessem em linha para fazer a contabilidade os soldados mortos, dessa forma ordenou que se alinhassem de 5 em 5 tropas, e sobrou 1 tropa. Quando alinhou de 6 em 6 e verificou que sobraram 3. E quando alinhou de 7 em 7 sobrou apenas 2 tropas. Depois diz outro alinhamento de 13 em 13, não sobrando nenhuma tropa. Quantas tropas o general tinha?

Para se resolver esse problema que aparentemente é simples é necessário utilizar–se a feramenta de congruência, vamos usar o Teorema Chinês dos Restos, do qual o problema mencionado acima é uma aplicação do mesmo.

Teorema 5.1 (Teorema Chinês dos Restos)**.** *Sejam* $m_1,\ m_2, \ldots,\ m_r$ *inteiros positivos primos entre si dois a dois, isto é, tais que* $mdc(m_i, m_j) = 1$ *se* $i \neq j$*. Nestas condições, o sistema de congruência lineares:*

$$\begin{cases} x \equiv a_1 (\mathrm{mod}\ m_1) \\ x \equiv a_2 (\mathrm{mod}\ m_2) \\ x \equiv a_3 (\mathrm{mod}\ m_3) \\ \vdots \qquad\qquad \vdots \\ x \equiv a_r (\mathrm{mod}\ m_r) \end{cases}$$

tem uma única solução

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 + \ldots + a_r M_r y_r (\mathrm{mod}\ M)$$

onde $M = m_1 \cdot m_2 \cdots m_r$, $M_k = \dfrac{M}{m_k}$ *e* y_k *é tal que* $M_k y_k \equiv 1 (\mathrm{mod}\ m_k)$ *com* $k = 1,\ 2, \ldots,\ r$, *ou seja,* y_k *é o inverso multiplicativo de* M_k *módulo* m_k.

Demonstração. Para cada $k = 1,\ 2,\ 3,\ \ldots,\ r$, ou seja:

$$M_k = \frac{M}{m_k} = m_1 \cdot m_2 \cdots m_{k-1} \cdot m_{k+1} \cdots m_r$$

isto é, M_k é o produto de todos os inteiros m_i com o fator m_k omitido. Por hipótese, os m_i são primos entre si doi a dois, de modo que o $mdc(M_k, m_k) = 1$ e, portanto, a congruência linear:

$$M_k \cdot y_k \equiv 1 (\mathrm{mod}\ m_k) \tag{5.1}$$

tem uma única solução y_k.

Posto isso, vamos demostrar que o inteiro:

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 + \ldots + a_r M_r y_r (\mathrm{mod}\ M)$$

satisfazendo cada um das congruências do sistema considerado, ou seja, que x é uma solução deste sistema.

Assim, se $i \neq k$, então $m_k \mid M_i$ e $M_i \equiv 0 (\mathrm{mod}\ m_k)$, o que implica:

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 + \ldots + a_r M_r y_r \equiv a_k M_k y_k (\mathrm{mod}\ M)$$

E como y_k é um solução para a congruência (5.1), temos

$$M_k \cdot y_k \equiv 1 (\mathrm{mod}\ m_k) \Longrightarrow x \equiv a_k \cdot 1 \equiv a_k (\mathrm{mod}\ m_k)$$

e isso porva que x é uma solução do sistema de congruência linear considerado. □

Para demostra a unicidade desta solução, suponhamos que x_1 é uma outra solução qualquer do sistema de congruência. Então

$$x \equiv a_k \equiv x_1 (\mathrm{mod}\ m_k),$$

com $k = 1,\ 2,\ 3,\ \ldots,\ r$, de modo que $m_k \mid (x - x_1)$ para cada valor de k. E como o $mdc(m_i, m_j) = 1$, segue–se que $m_1 \cdot m_2 \cdots m_r \mid (x - x_1)$, isto é,

$$m \mid (x - x_1) \qquad \text{e} \qquad x \equiv x_1 (\mathrm{mod}\ m).$$

Para resolver o problema inicial do general chinês, temos que organizar as informações.

Seja x o número de tropas resultante, dessa forma:

$$\begin{cases} x \equiv 1(\mathrm{mod}\ 5) \\ x \equiv 3(\mathrm{mod}\ 6) \\ x \equiv 2(\mathrm{mod}\ 7) \\ x \equiv 0(\mathrm{mod}\ 13) \end{cases}.$$

Como 5, 6, 7 e 13 são inteiros positivos primos entre si dois a dois. Aplicando o Teorema Chinês do Resto tem–se que: $a_1 = 1$, $a_2 = 3$, $a_3 = 2$, $a_4 = 0$, $m_1 = 5$, $m_2 = 6$, $m_3 = 7$ e $m_4 = 13$. Dessa forma,

$$M = 5 \cdot 6 \cdot 7 \cdot 13 = 2730,$$

daí, $M_1 = \dfrac{M}{m_1} = \dfrac{2730}{5} = 546$, $M_2 = \dfrac{M}{m_2} = \dfrac{2730}{6} = 455$, $M_3 = \dfrac{M}{m_3} = \dfrac{2730}{5} = 390$ e $M_4 = \dfrac{M}{m_4} = \dfrac{2730}{13} = 210$.

Agora vamos encontra todos os inversos multiplicativos de M_k módulo m_k. Como

$$\mathrm{mdc}(M_1, m_1) = \mathrm{mdc}(M_2, m_2) = \mathrm{mdc}(M_3, m_3) = \mathrm{mdc}(M_4, m_4) = 1,$$

temos as congruências lineares:

$$\begin{aligned} M_1 \cdot y_1 &\equiv 1(\mathrm{mod}\ m_1) \Longrightarrow 546 \cdot y_1 \equiv 1(\mathrm{mod}\ 5); \\ M_2 \cdot y_2 &\equiv 1(\mathrm{mod}\ m_2) \Longrightarrow 455 \cdot y_2 \equiv 1(\mathrm{mod}\ 6); \\ M_3 \cdot y_3 &\equiv 1(\mathrm{mod}\ m_3) \Longrightarrow 390 \cdot y_3 \equiv 1(\mathrm{mod}\ 7); \\ M_4 \cdot y_4 &\equiv 1(\mathrm{mod}\ m_4) \Longrightarrow 210 \cdot y_4 \equiv 1(\mathrm{mod}\ 13). \end{aligned}$$

Por outro lado temos que 546 deixa resto 1 quando dividido por 5, 455 deixa resto 5 quando dividido por 6, 390 deixa resto 5 quando dividido por 7 e 210 deixa resto 2 quando dividido por 13, ou seja,

$$\begin{aligned} 546 &\equiv 1(\mathrm{mod}\ 5) \Longrightarrow 1 \cdot y_1 \equiv 1(\mathrm{mod}\ 5); \\ 455 &\equiv 5(\mathrm{mod}\ 6) \Longrightarrow 5 \cdot y_2 \equiv 1(\mathrm{mod}\ 6); \\ 390 &\equiv 5(\mathrm{mod}\ 7) \Longrightarrow 5 \cdot y_3 \equiv 1(\mathrm{mod}\ 7); \\ 210 &\equiv 2(\mathrm{mod}\ 13) \Longrightarrow 2 \cdot y_4 \equiv 1(\mathrm{mod}\ 13). \end{aligned}$$

tem como solução respectivamente: $y_1 = 6$, $y_2 = 5$, $y_3 = 3$, $y_4 = 20$. Portanto,

$$\begin{aligned} x &= 1 \cdot 546 \cdot 6 + 3 \cdot 455 \cdot 5 + 2 \cdot 390 \cdot 3 + 0 \cdot 210 \cdot 20 \\ x &= 3.276 + 6.825 + 2.340 + 0 \\ x &= 12.441 \end{aligned}$$

daí,

$$x \equiv 12.441 (\mathrm{mod}\ 2.730) \Longrightarrow x \equiv 1.521 (\mathrm{mod}\ 2.730) \Longrightarrow x = 1.521 + 2730 \cdot q,$$

com q um número natural. Mas queremos que x seja maior do que 0 e menor do que 1800, tomando $q = 0$ implica que $x = 1521$. Logo, concluímos que sobraram 1521 tropas após o combate.

Exemplo 5.1. *Encontre o menor inteiro positivo* x *tal que* $x = 5 (\mathrm{mod}\ 7)$, $x = 7 (\mathrm{mod}\ 11)$ *e* $x = 3 (\mathrm{mod}\ 13)$.

Solução: Usando o teorema anterior com $m_1 = 5$, $m_2 = 7$, $m_3 = 11$, $a_1 = 5$, $a_2 = 7$ e $a_3 = 3$ podemos achar $x = 887 (\mathrm{mod}\ 1001) = 7 \cdot 11 \cdot 13$. Como a solução é única módulo m, isso significa que, dentre os números $1,\ 2,\ \ldots,\ 1001$ a menor solução positiva é 887.

Problema 5.1 (POTI)**.** *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 o número de degraus da escada. Pelos dados do problema podemos montar o seguinte sistema:

$$\begin{cases} x \equiv 1 (\mathrm{mod}\ 2) \\ x \equiv 2 (\mathrm{mod}\ 3) \\ x \equiv 3 (\mathrm{mod}\ 5) \end{cases}$$

como $mdc(2, 3) = mdc(2, 5) = mdc(3, 5) = 1$, então podemos aplicar o Teorema Chinês dos Restos. Assim, $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, $m_1 = 2$, $m_2 = 3$, $m_3 = 5$ e

$$M = m_1 \cdot m_2 \cdot m_3 = 2 \cdot 3 \cdot 5 = 30$$

dessa forma, $M_1 = \dfrac{M}{m_1} = \dfrac{30}{2} = 15$, $M_2 = \dfrac{M}{m_2} = \dfrac{30}{3} = 10$ e $M_3 = \dfrac{M}{m_3} = \dfrac{30}{5} = 6$. Agora,

vamos determinar os inteiros y_i com $i = 1,\ 2,\ 3$ tais que.

$$\begin{aligned} M_1 \cdot y_1 &\equiv 1 (\mathrm{mod}\ m_1) \Longrightarrow 15 \cdot y_1 \equiv 1 (\mathrm{mod}\ 2) \\ M_2 \cdot y_2 &\equiv 1 (\mathrm{mod}\ m_2) \Longrightarrow 10 \cdot y_2 \equiv 1 (\mathrm{mod}\ 3) \\ M_3 \cdot y_3 &\equiv 1 (\mathrm{mod}\ m_3) \Longrightarrow 6 \cdot y_3 \equiv 1 (\mathrm{mod}\ 5) \end{aligned}$$

Dessa forma $y_1 = 1$, $y_2 = 2$ e $y_3 = 3$. Logo:

$$\begin{aligned} x &= a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 + a_3 \cdot M_3 \cdot y_3 \\ x &= 1 \cdot 15 \cdot 1 + 2 \cdot 10 \cdot 2 + 3 \cdot 6 \cdot 3 \\ x &= 15 + 40 + 54 \\ x &= 109 \end{aligned}$$

daí,

$$x \equiv 109 (\mathrm{mod}\ 30) \Longrightarrow x \equiv 19 (\mathrm{mod}\ 30) \Longrightarrow x = 19 + 30 \cdot q,$$

Como x está entre 150 e 200, temos $150 < 19 + 30q < 200 \Longrightarrow 131 < 30q < 181 \Longrightarrow 4 < q < 6 \Longrightarrow q = 5$. Portanto, o número de degraus da escada é $x = 19 + 30 \cdot 5 = 169$.

Problema 5.2 (PROMAT – Exame de Qualificação (2012–1))**.** *Um truque de adivinhação de números*

(a) Ache as soluções mínimas de cada uma das seguintes congruências:

$$\begin{aligned} &\text{i.} \quad 110y \equiv 1 (\mathrm{mod}\ 9) \\ &\text{ii.} \quad 99y \equiv 1 (\mathrm{mod}\ 10) \\ &\text{iii.} \quad 90y \equiv 1 (\mathrm{mod}\ 11) \end{aligned}$$

(b) Um mágico pede a sua audiência para escolher um número natural M *de pelo menos dois algarismos e menor do que* 1000*, e de lhe revelar apenas os restos* r_9*,* r_{10} *e* r_{11} *da divisão de* M *por* 9*,* 10 *e* 11*, respectivamente. Sem nenhuma outra informação ele consegue descobrir* M*. Explique como ele consegue fazer isto.*

(c) Supondo que a plateia tenha dado as seguintes informações ao mágico: $r_9 = 7$*,* $r_{10} = 8$ *e* $r_{11} = 9$*, qual foi o valor de* M *que o mágico achou?*

Solução: (a) A congruência $110y \equiv 1 (\mathrm{mod}\ 9)$ é equivalente à congruência $2y \equiv 1 (\mathrm{mod}\ 9)$, cuja solução mínima é claramente $y_1 = 5$. A congruência $99y \equiv 1 (\mathrm{mod}\ 10)$ é equivalente à congruência $9y \equiv 1 (\mathrm{mod}\ 10)$, cuja solução mínima é claramente $y_2 = 9$. A congruência $90y \equiv 1 (\mathrm{mod}\ 11)$ é equivalente à congruência $2y \equiv 1 (\mathrm{mod}\ 11)$, cuja solução mínima é

claramente $y_3 = 6$.

(b) O mágico tem que resolver o seguinte sistema de congruências:

$$\begin{cases} M & \equiv & r_1 (\mathrm{mod}\ 9) \\ M & \equiv & r_2 (\mathrm{mod}\ 10) \\ M & \equiv & r_3 (\mathrm{mod}\ 11) \end{cases}.$$

O Teorema Chinês dos Restos nos diz que o sistema tem uma única solução módulo $9 \cdot 10 \cdot 11 = 990$, dada pela equação

$$M \equiv (10 \cdot 11) y_1 r_9 + (9 \cdot 10) y_2 r_{10} + (9 \cdot 10) y_3 r_{11} \Big(\mathrm{mod}\ (9 \cdot 10 \cdot 11) \Big),$$

em que y_1, y_2 e y_3 são as soluções das equações diofantinas do item (a). Logo

$$M \equiv 550 r_9 + 891 r_{10} + 540 r_{11} (\mathrm{mod}\ 990),$$

e só existe um valor de M satisfazendo essa equação e a restrição de que $10 \leqslant M \leqslant 999$.

(c) Temos que achar $10 \leqslant M \leqslant 999$ natural tal que

$$\begin{aligned} M &\equiv 550 \cdot 7 + 891 \cdot 8 + 540 \cdot 9 (\mathrm{mod}\ 990) \\ M &\equiv 988 (\mathrm{mod}\ 990). \end{aligned}$$

Então $M = 988$.

Problema 5.3. *Um bando de 17 piratas, ao tentar dividir igualmente entre si as moedas de uma arca, verificou que haveria uma sobra de 3 moedas. Seguiu-se uma discussão, na qual um pirata foi morto. Na nova tentativa de divisão, já com um pirata a menos, verificou-se que haveria uma sobra de 10 moedas. Nova confusão, e mais um pirata foi morto. Então, por fim, eles conseguiram dividir igualmente as moedas entre si. Qual o menor número de moedas que a arca poderia conter?"*

Solução: Seja x a quantidade de moedas. Como $mdc(17, 16) = mdc(17, 15) = mdc(16, 15) = 1$, então aplicaremos o Teorema Chinês dos Restos. Assim, $a_1 = 3$, $a_2 = 10$, $a_3 = 0$, $m_1 = 17$, $m_2 = 16$, $m_3 = 15$, então

$$\begin{cases} x & \equiv & 3 (\mathrm{mod}\ 17) \\ x & \equiv & 10 (\mathrm{mod}\ 16) \\ x & \equiv & 0 (\mathrm{mod}\ 15) \end{cases}$$

e $M = 17 \cdot 16 \cdot 15 = 4080$, dessa forma, $M_1 = \dfrac{4080}{17} = 240$ e $M_2 = \dfrac{4080}{16} = 255$. Então,

$$\begin{aligned} M_1 \cdot y_1 &\equiv 1 (\mathrm{mod}\ m_1) \Longrightarrow 240 \cdot y_1 \equiv 1 (\mathrm{mod}\ 17) \\ M_2 \cdot y_2 &\equiv 1 (\mathrm{mod}\ m_2) \Longrightarrow 255 \cdot y_2 \equiv 1 (\mathrm{mod}\ 16) \end{aligned}$$

Encontrando $y_1 = 9$ e $y_2 = 15$, logo

$$\begin{aligned} x &= a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 \\ x &= 3 \cdot 240 \cdot 9 + 10 \cdot 255 \cdot 15 \\ x &= 6480 + 38250 \\ x &= 44730 \end{aligned}$$

daí, $x \equiv 44730 (\mathrm{mod}\ 4080) \Longrightarrow x \equiv 3930 (\mathrm{mod}\ 4080) \Longrightarrow x = 3930 + 4080 \cdot q$. Para o menor valor inteiro positivo de x temos apenas um valor quando $q = 0$, Portanto, a quantidade de moedas é $x = 3930 + 4080 \cdot 0 = 3930$.

Problema 5.4 (PROFMAT MA14 (2014.2))**.** *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 na turma, com $x < 50$. Podemos montar o seguinte sistema:

$$\begin{cases} x \equiv 2 (\mathrm{mod}\ 3) \\ x \equiv 1 (\mathrm{mod}\ 4) \\ x + 1 \equiv 0 (\mathrm{mod}\ 5) \end{cases} \Longleftrightarrow \begin{cases} x \equiv 2 (\mathrm{mod}\ 3) \\ x \equiv 1 (\mathrm{mod}\ 4) \\ x \equiv 4 (\mathrm{mod}\ 5) \end{cases}$$

como $\mathrm{mdc}(3,4) = \mathrm{mdc}(3,5) = \mathrm{mdc}(4,5) = 1$, usaremos o Teorema Chinês dos Restos para resolvê-lo. Assim, $a_1 = 2$, $a_2 = 1$, $a_3 = 4$, $m_1 = 3$, $m_2 = 4$, $m_3 = 5$ e $M = 3 \cdot 4 \cdot 5 = 60$, segue que, $M_1 = \dfrac{60}{3} = 20$, $M_2 = \dfrac{60}{4} = 15$ e $M_3 = \dfrac{60}{5} = 12$. Agora, vamos determinar os inteiros y_i com i = 1,2,3 tais que:

$$\begin{aligned} M_1 \cdot y_1 &\equiv 1 (\mathrm{mod}\ m_1) \Longrightarrow 20 \cdot y_1 \equiv 1 (\mathrm{mod}\ 3) \\ M_2 \cdot y_2 &\equiv 1 (\mathrm{mod}\ m_2) \Longrightarrow 15 \cdot y_2 \equiv 1 (\mathrm{mod}\ 4) \\ M_3 \cdot y_3 &\equiv 1 (\mathrm{mod}\ m_3) \Longrightarrow 12 \cdot y_3 \equiv 1 (\mathrm{mod}\ 5) \end{aligned}$$

Dessa forma $y_1 = 2$, $y_2 = 3$ e $y_3 = 3$, logo

$$\begin{aligned} x &= a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 + a_3 \cdot M_3 \cdot y_3 \\ x &= 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 4 \cdot 12 \cdot 3 \\ x &= 80 + 45 + 144 \\ x &= 269 \end{aligned}$$

daí,

$$x \equiv 269(\mathrm{mod}\ 60) \Longrightarrow x \equiv 29(\mathrm{mod}\ 60) \Longrightarrow x = 29 + 60 \cdot q,$$

Portanto, a quantidade de alunos na turma é $x = 29 + 60 \cdot 0 = 29$.

6 Considerações Finais

A finalidade deste trabalho apresentado é proporcionar aos alunos da graduação e futuros professores da Educação Básica, um maior contato com a aritmética no que diz respeito a Teoria dos Números, mostrando alguns dispositivos práticos como, o Algoritmo de Euclides, estudada de maneira superficial no Ensino Fundamental e que raramente são abordados na forma de problemas em anos subsequentes. Fazendo referência a Euclides e seu dispositivo prático para determinação do $\mathtt{mdc}$ de dois números inteiros quaisquer que não é mencionado nem trabalhados nos livros didáticos.

O estudo sobre Equação Diofantina pode ser entendido como mais uma oportunidade de aprendizagem, pois não acreditamos no, "quanto mais exercícios, melhor", mas "quanto melhores os exercícios, melhor". Devemos manter nossos alunos em contato com a aritmética e a álgebra (a pele que segura todas as lindas penas da matemática) durante todo o Ensino Básico.

Durante todo o trabalho foram pesquisados diversos exercícios dentre eles provas de olimpíadas (OBMEP e OBM), Exame Nacional de Acesso ao mestrado profissional PROFMAT (ENA) e Exames Nacional de Qualificação (ENQ) sobre o Teorema Chinês do Resto, de forma a ser apresentado a alunos da Educação Básica, o foco é proporcionar tanto aos alunos quanto professores um assunto da graduação podendo ser transmitida para o Ensino Fundamental e Ensino Médio, de forma que auxilie os mesmos a resolução de problemas pertinentes ao Teorema Chinês do Resto.

Antes de chegar aos exemplos e problemas do Teorema Chinês do Resto citado no capítulo anterior, descrevemos a respeito de Números Inteiros e suas propriedades, divisibilidade, Máximo Divisor Comum, Algoritmo de Euclides, Congruência Modular, aplicação da congruência modular em dígitos verificadores, Equação Diofantina Lineares, classes residuais, como pré-requisito para resolução dos problemas do Teorema Chinês do Resto. Logo, desejamos que este trabalho estimule os professores da Educação Básica fazendo com que esse incentivo rompa as barreiras existentes e faça de sua sala de aula um novo universo ainda mais diversificado e dinâmico.

Referências

ALENCAR FILHO, Edgar de. – *Teoria Elementar dos números*. 2ª Ed. São Paulo: Nobel, 1981.

A História do Cartão de Crédito. Disponivel em: `https://www.conciliadora.com.br/blog/a-historia-do-cartao-de-credito/`. Acesso em: 08 de Dez. 2019.

Cadastro de Pessoas Fisicas (CPF). Disponivel em: `http://www.bentogoncalves.rs.gov.br/cidadao/cidadania/cadastro-de-pessoa-fisica-cpf`. Acesso em: 08 de Dez. 2019.

CPF - Cadrasto Social - Caixa. Disponivel em: `http://www.caixa.gov.br/cadastros/cpf/Paginas/default.aspx`. Acesso em: 08 de Dez. 2019.

LEITE, Kalama Guimarães - *EQUAÇÃO DIOFANTINA LINEAR: APLICAÇÕES NO ENSINO MÉDIO*. Dissertação de mestrado PROFMAT: Universidade Federal do Amapá Unifap. Macapá - AP, 2014.

OLIVEIRA, Rafael Américo de - *Explorando o universo do números primos* / Rafael Américo de Oliveira. - Rio Claro, 2015. 61 f. : il. Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas.

Silva, Rivanildo Garcia da. - *Congruências e Equações diofantinas [manuscrito]: algumas aplicações* / Rivanildo Garcia da Silva. - 2018. 77 p. Digitado. Dissertação (Mestrado em Profissional em Matemática em Rede Nacional) - Universidade Estadual da Paraíba, Pró-Reitoria de Pós-Graduação e Pesquisa, 2019.

LEOPOLD, Guilherme Liegel - *Congruência e Aplicações*. Dissertação (Mestrado em Profissional em Matemática em Rede Nacional) - Universidade Estadual de Maringá, 2015.

GIOIA, Anthony A. - *The theory of numbers an introduction*. Originally published: Chicago: Markham Pub, Co, 2970.

GLÓRIA, Walace da Silva. - *Teorema Chinês Dos Restos: Ensino e Aplicações*. Dissertação (Mestrado em Profissional em Matemática em Rede Nacional) - Universidade Federal do Amazonas, 2019.

GUSMAI, Daniel Martins. - *Calculadora das Classes Residuais*. Dissertação (Mestrado em Profissional em Matemática em Rede Nacional) - Universidade Federal do ABC, Centro De Matemática, Computação e Cognição, 2018.

NASCIMENTO, Adriano Sales. - *Teorema Chinês Do Resto: Sua aplicação no Ensino Médio*. Dissertação (Mestrado em Profissional em Matemática em Rede Nacional) - Universidade Federal de Mato Grosso, 2014.

SANTOS, José Plínio de Oliveira. – *Introdução à Teoria dos Números*, 3ª Ed. Rio de Janeiro: IMPA, 2009.

SILVA, Luis Henrique Pereira da. - *Uma Aplicação da Congruência na Determinação de Critérios de Divisibilidade*. Dissertação (Mestrado em Profissional em Matemática em Rede Nacional) - Universidade Federal de Goiás, Instituto de Matemática e Estatística (IME), 2015.

OBM. – *Provas e Soluções*. Disponível em <`http://www.obm.org.br/`>. Acesso em 04 dez. 2018.

OBMEP. – *Provas e Soluções*. Disponível em <`http://www.obmep.org.br/`>. Acesso em 04 dez. 2018.

PINZ, Carla Rejane Fick. *Dígitos Verificadores e Detecção de Erros*. Dissertação (Mestrado em Profissional em Matemática em Rede Nacional) - Universidade Federal do Rio Grande - FURG, 2013.

PROFMAT. – *Provas e Soluções*. Disponível em <`http://www.profmat-sbm.org.br/`> Acesso em 14 fev. 2019.

HEFEZ, Abramo. – *Aritmética*. Coleção PROFMAT. Rio de Janeiro: SBM, 2016.

HEFEZ, Abramo. – *Elementos de Aritmética*. Textos Universitarios. Rio de Janeiro: SBM, 2016.

K. I. Oliveira, A. J. Corcho – *Iniciação à Matemática: um curso com problemas e soluções*, SBM, 2012.