UNIVERSIDADE DA INTEGRAÇÃO INTERNACIONAL DA LUSOFONIA AFRO-BRASILEIRA
INSTITUTO DE CIÊNCIAS EXATAS E DA NATUREZA
CURSO DE LICENCIATURA EM MATEMÁTICA

ANTONIO JANDERSON DE ALMEIDA SAMPAIO

SISTEMAS DE CONGRUÊNCIAS LINEARES E APLICAÇÕES NA EDUCAÇÃO BÁSICA

REDENÇÃO
2021

ANTONIO JANDERSON DE ALMEIDA SAMPAIO

SISTEMAS DE CONGRUÊNCIAS LINEARES E APLICAÇÕES NA EDUCAÇÃO BÁSICA

Monografia apresentada ao Curso de Licenciatura em Matemática do Instituto de Ciências Exatas e da Natureza da Universidade da Integração Internacional da Lusofonia Afro-Brasileira, como parte dos requisitos necessários para a obtenção do título de Licenciado em Matemática. Área de concentração: Matemática.

Orientador: Prof. Dr. Joserlan Perote da Silva

REDENÇÃO

2021

Universidade da Integração Internacional da Lusofonia Afro-Brasileira
Sistema de Bibliotecas da UNILAB
Catalogação de Publicação na Fonte.

Sampaio, Antonio Janderson de Almeida.

S181s

SISTEMAS DE CONGRUÊNCIAS LINEARES E APLICAÇÕES NA EDUCAÇÃO BÁSICA / Antonio Janderson de Almeida Sampaio. - Redenção, 2021.
53f: il.

Monografia - Curso de Matemática, Instituto De Ciências Exatas E Da Natureza, Universidade da Integração Internacional da Lusofonia Afro-Brasileira, Redenção, 2021.

Orientador: Prof. Dr. Joserlan Perote da Silva.

1. Matemática - Divisibilidade. 2. Números primos. 3. Equações lineares. 4. Teorema Chinês do Resto. 5. Aplicações. I. Título

CE/UF/Dsibiuni CDD 510

ANTONIO JANDERSON DE ALMEIDA SAMPAIO

SISTEMAS DE CONGRUÊNCIAS LINEARES E APLICAÇÕES NA EDUCAÇÃO BÁSICA

Monografia apresentada ao Curso de Licenciatura em Matemática do Instituto de Ciências Exatas e da Natureza da Universidade da Integração Internacional da Lusofonia Afro-Brasileira, como parte dos requisitos necessários para a obtenção do título de Graduado em Matemática. Área de Concentração: Matemática.

Aprovada em: 13/04/2021.

BANCA EXAMINADORA

Joserlan Perote da Silva

Prof. Dr. Joserlan Perote da Silva (Orientador)
Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)

Rafael Jorge Pontes Diógenes

Prof. Dr. Rafael Jorge Pontes Diógenes
Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)

Kelma Gomes de melo.

Prof.ª Ma. Kelma Gomes de Melo
Secretaria de Educação do Ceará (SEDUC)

Dedico este trabalho a todas as pessoas que contribuíram direta ou indiretamente com a sua realização. De forma especial a minha mãe que sempre me apoiou em todo o processo de construção desse trabalho e também em cada momento de minha vida, e aos meus familiares, minha namorada e amigos que me apoiaram para a conclusão desta etapa acadêmica.

AGRADECIMENTOS

Primeiramente agradeço a Deus por sua misericórdia e cuidado em todos os dias de minha vida, especialmente neste período de elaboração do presente trabalho.

Faço um agradecimento especial a meus familiares, minha namorada e meus amigos que estiveram comigo nos momentos difíceis e me encorajaram a seguir em frente. Gratidão por todo o apoio, paciência e compreensão que cada um de vocês tiveram para comigo ao longo desse ciclo formativo.

Aqui reconheço o empenho, paciência, compreensão e também o apoio do Prof. Dr. Joserlan Perote da Silva e agradeço também pela excelente orientação. Na qual, esteve sempre ensinando e sugerindo caminhos a serem seguidos, na tentativa de proporcionar uma melhor construção dos saberes que constituem o presente trabalho.

Aos demais professores dessa instituição que colaboraram para minha formação acadêmica, minha gratidão e reconhecimento por tão bem cumprirem o ofício que lhes foi confiado.

Agradeço também ao Prof. Dr. Rafael Jorge Pontes Diógenes e à Prof. Ma. Kelma Gomes de Melo pelo aceite ao convite de colaborar com este estudo, trazendo sugestões e correções de maneira a enriquecer os conhecimentos e resultados que aqui serão apresentados.

Obrigado a esta instituição por me possibilitar experiências tão preciosas para minha vida profissional e também pelos auxílios financeiros fornecidos que proporcionaram minha permanência no curso. Manifesto um agradecimento especial ao PIBIC - UNILAB e ao PIBIC - CNPq pelas possibilidades de crescimento intelectual e pelas bolsas de fomento, disponibilizadas no decorrer do período que colaborei para a pesquisa de iniciação científica.

"Não há nenhum ramo da Matemática que por mais abstrato que seja, que não possa ser aplicado a fenômenos do mundo real"
Nikolai Lobachersky

RESUMO

O presente trabalho objetiva apresentar soluções para os problemas que abordam, mesmo que implicitamente, congruências lineares e que possivelmente estão presentes em avaliações direcionadas aos estudantes do ensino médio. Para isto, é realizada uma fundamentação teórica sobre o assunto onde é apresentada uma breve revisão sobre divisibilidade, máximo divisor comum, mínimo múltiplo comum e números primos, e uma investigação sobre o comportamento modular de um número usando os conceitos de divisão euclidiana. Assim, busca-se aqui desenvolver bases fundamentadas para a resolução de problemas trazidos em olímpiadas de Matemática de forma que seja possível obter um sistema de congruências lineares e aplicar o teorema do resto chinês para encontrar sua solução. Essa estratégia de resolução pode ser adequada e utilizada por estudantes da rede pública e privada do ensino médio proporcionando-lhes êxito em avaliações externas e em processos seletivos que os permitam ingressar no ensino superior que lhes seja exigido um conhecimento concreto sobre a estrutura e operações com números inteiros.

Palavras-chave: Divisibilidade. Números primos. Equações Lineares. Teorema Chinês do Resto. Aplicações.

ABSTRACT

This paper aims to present solutions to problems that address even implicitly linear congruence and that are possibly present in assessments directed to high school students. For this, a theoretical foundation on the subject is performed where a brief review of divisibility, maximum common divisor, minimum common multiple and prime numbers is presented, and an investigation of the modular behavior of a number using the concepts of Euclidean division. Thus, we seek here to develop a foundation for solving problems brought up in Mathematics Olympiads in such a way that it is possible to obtain a system of linear congruences and apply the Chinese remainder theorem to find its solution. This resolution strategy can be adequate and used by public and private high school students, providing them with success in external evaluations and in selection processes that allow them to enter higher education, where a concrete knowledge about the structure and operations with integers is required.

Keywords: Divisibility. Prime numbers. Linear Equations. Chinese Remainder Theorem. Aplications.

SUMÁRIO

1 INTRODUÇÃO

Resolver um sistema de congruências lineares exige conhecimentos prévios por vezes, oriundos ainda do ensino fundamental. Para isto, este trabalho vem explorar competências necessárias para compreender e utilizar as estratégias de resolução de um sistema dado, formulando significados eficazes para a aplicabilidade desses resultados na escola ou nas mais diversas situações do cotidiano.

O presente estudo é dividido em capítulos onde seguem uma sequência gradativa de saberes de maneira a possibilitar ao leitor uma melhor visualização e assimilação do processo que constitui as instruções aqui apresentadas.

No segundo capítulo é explorado sobre a divisão sendo possível reconhecer seu algoritmo e alguns critérios para obtenção de divisores de um inteiro qualquer. Este proporciona ainda, o conhecimento sobre inteiros primos, enuncia o Teorema Fundamental da Aritmética e apresenta as equações diofantinas que, assim como Silva (2018), explicita a clara relação de decomposição de um inteiro composto com números primos e como estes podem ajudar na resolução de equações lineares.

O terceiro capítulo que tem como base o livro de Alencar Filho (1981), vem apresentar o conceito de congruências apontando suas características e propriedades de maneira, que sejam formalizadas as estratégias de resolução e significados das congruências lineares, aplicando-as principalmente em sistemas compostos por estas.

Desta forma, buscando solidificar os conhecimentos que estão sendo formados, o quarto capítulo traz situações onde se é possível reafirmar estes saberes sobre sistemas de congruências lineares através de aplicações no cotidiano expressas como situações-problema presentes em olímpiadas de matemática.

Portanto, esse estudo possibilita uma ampliação e ressignificação dos saberes matemáticos, de forma a proporcionar aos educandos do ensino básico e aos profissionais da educação a estarem em constante formação.

2 PRELIMINARES

O conceito de divisibilidade no conjunto dos números inteiros é um tema essencial para a teoria dos números e consequentemente, para o estudo aqui desenvolvido. Neste capítulo, será apresentada uma fundamentação teórica com base na desenvolvida por Moreira, Martínez e Saldanha (2012) dos saberes essenciais que colaboram para a formalização dos conceitos e resultados deste trabalho.

2.1 NÚMEROS INTEIROS

O conjunto dos números inteiros ($\mathbb{Z}$) é dado por

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

onde os elementos não-nulos pertencentes a esse conjuntos são positivos ou negativos.

Definição 2.1 *(Príncipio da boa ordenação) Todo conjunto não-vazio X de inteiros não negativos possui elemento mínimo, ou seja:*

$$\forall X \subset \mathbb{N}, X \neq \emptyset \Rightarrow \exists \min A.$$

Exemplo 2.1 *O conjunto $X = \{1, 3, 5, 7, \cdots\}$ dos inteiros positivos ímpares é um subconjunto não-vazio de $\mathbb{N}$. Pelo Príncipio da boa ordenação, X possui elemento mínimo ($\min X = 1$).*

Teorema 2.1 *(Indução matemática) Seja $P(n)$ uma proposição associada a cada inteiro positivo n e que satisfaz as seguintes condições:*

1. *$P(1)$ é verdadeira;*
2. *para todo inteiro positivo k, se $P(k)$ é verdadeira, então $P(k+1)$ também é verdadeira*

Nestas condições, a proposição $P(n)$é verdadeira para todo inteiro positivo n.

Demonstração: Seja S o conjunto dos inteiros positivos n, para os quais $P(n)$ é verdadeira, ou seja:

$$S = \{n \in \mathbb{Z}_+; P(n) \text{ é verdadeira}\}.$$

Pela primeira condição, $P(1)$ é verdadeira, e assim $1 \in S$. Pela segunda condição, para todo inteiro positivo k, se $k \in S$ então $k+1 \in S$. Fazendo isto repetidas vezes, verificamos que $\forall k, k+1 \in S$ ou seja $S = \mathbb{Z}_+$. ∎

As próximas subseções abordarão os significados da divisão e critérios de divisibilidade, que juntos, fundamentam as bases essenciais do presente estudo.

2.2 DIVISÃO NOS NÚMEROS INTEIROS

Como a divisão de um inteiro por outro nem sempre é possível, ou seja, expressar essa possibilidade através da divisibilidade. Então quando não existir uma relação de divisibilidade entre dois números inteiros, veremos que ainda será possível efetuar uma divisão com um pequeno resto, chamada de divisão euclidiana.

2.2.1 Divisibilidade

Definição 2.2 *Dizemos que um número a é divisível por b, ou seja, b é um dos divisores de a, quando existir um número k tal que $a = k \cdot b$, com $a, b, k \in \mathbb{Z}$.*

Exemplo 2.2 *A seguir, temos alguns exemplos de divisibilidade:*

- *63 é divisível por 7, pois* $7 \cdot 9 = 63$.
- *32 é divisível por 8, pois* $8 \cdot 4 = 32$.
- *18 não é divisível por 7, pois não existe* $a \in \mathbb{Z}$, *onde* $7a = 18$.

Observação 2.1 *Quando b é um divisor de a, podemos afirmar que b divide a, onde denotaremos por $b \mid a$. Caso contrário, denotaremos por $b \nmid a$.*

Observação 2.2 *Seja b divisível por a, isto equivale a afirmar que b é múltiplo de a.*

Proposição 2.1 *Se $d \mid a$ e $d \mid b$, então $d \mid ax + by$ para quaisquer x e y inteiros.*

Demonstração: Se $d \mid a$ e $d \mid b$ então existem q_1 e q_2 inteiros onde $a = dq_1$ e $b = dq_2$. Dessa forma,

$$ax + by = dq_1x + dq_2y = d(q_1x + q_2y)$$

onde x, y são inteiros. Como $q_1x + q_2y \in \mathbb{Z}$ então $d \mid ax + by$. ∎

Proposição 2.2 *Se $d \mid a$ então $a = 0$ ou $\mid d \mid \leq \mid a \mid$.*

Demonstração: Admitindo $d > 0$, quando $a = d$ temos que $d \mid a$. Dessa forma, $d \mid a - a$, o que implica $d \mid 0$. Se $a = 0$, então $d \mid a$. Seja $a > 0$, resta-nos mostrar que $\mid d \mid \leq \mid a \mid$. Como $d \mid a$, então existe q_1 onde $a = dq_1$. Dessa forma,

$$\mid a \mid = \mid d \mid \cdot \mid q_1 \mid .$$

Disso temos que $\mid d \mid \leq \mid a \mid$. ∎

Proposição 2.3 *Se $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração: Sejam $q_1, q_2 \in \mathbb{Z}$ de forma que $b = aq_1$ e $c = bq_2$. Assim,

$$c = bq_2 = aq_1q_2.$$

Dessa forma, $a \mid c$. ∎

Exemplo 2.3 *Determine todos os pares (m, n) de inteiros positivos para os quais $\dfrac{n^3+1}{mn-1}$ é inteiro.*

Solução: Busquemos aqui reduzir o grau em n utilizando os conceitos e propriedades da divisibilidade acima apresentados. Inicialmente note que devemos ter $mn > 1$. Assim,

$$mn - 1 \mid n^3 + 1 \Rightarrow mn - 1 \mid (n^3 + 1) \cdot m - (mn - 1) \cdot n^2$$

$$\Longleftrightarrow mn - 1 \mid n^2 + m.$$

De modo análogo,

$$mn - 1 \mid n^2 + m \Rightarrow nm - 1 \mid (n^2 + m) \cdot m - (mn - 1) \cdot n$$

$$\Longleftrightarrow mn - 1 \mid m^2 + n.$$

Finalmente,

$$mn - 1 \mid m^2 + n \Rightarrow mn - 1 \mid (m^2 + n)m - (mn - 1)$$

$$\Longleftrightarrow mn - 1 \mid m^3 + 1.$$

Assim, voltamos a expressão inicial se trocarmos m por n. Dessa forma, há uma solução simétrica em m e n e as divisibilidades são todas equivalentes entre si, ou seja, $mn - 1 \mid m^3 + 1$. Portanto, podemos admitir que $m \geq n$. Pela proposição 2.2, se $d \mid a$ então $a = 0$ ou $\mid d \mid \leq \mid a \mid$. Assim:

$$mn - 1 \mid n^2 + m \Rightarrow mn - 1 \leq n^2 + m \Leftrightarrow m(n - 1) \leq n^2 + 1.$$

Se $n = 1$ então $m - 1 \mid n - 1 \Rightarrow n - 1 \mid m + 1 - (m - 1) = 2 \Rightarrow m = 2$ *ou* $m = 3$. Se $n > 1$, então $m \leq \dfrac{n^2+1}{n-1} = n + 1 + \dfrac{2}{n-1}$. Como admitimos que $m \geq n$, temos então duas possibilidades onde $n \geq 4$ ou $m = n + 1$. Vamos analisar aqui esses dois casos.

- se $m \geq n = 2$ devemos ter $2m - 1 \mid 2^2 + m \Rightarrow 2m - 1 \mid 2(m + 4) - (2m - 1) \Leftrightarrow 2m - 1 \mid 9 \Leftrightarrow m = 2$ ou $m = 5$, em ambos os casos temos solução para o problema;
- se $m \geq n = 3$ teremos $3m - 1 \mid 3^2 + m \Rightarrow 3m - 1 \mid 3(m + 9) - (3m - 1) \Leftrightarrow 3m - 1 \mid 28 \Leftrightarrow m = 5$, que nos dá soluções para o problema;
- se $m = n \geqslant 4$ devemos ter

$$n^2 - 1 \mid n^2 + n \Leftrightarrow n - 1 \mid n$$

$$\Rightarrow n - 1 \mid n - (n - 1) \Longleftrightarrow n - 1 \mid 1$$

Pela proposição 2.2 chegamos a uma contradição, pois $n \geq 4$. Portanto as soluções (m, n) são

$$(1, 2), (2, 1), (1, 3), (3, 1), (2, 2), (2, 5), (5, 2), (3, 5), (5, 3).$$

■

2.2.2 Divisão euclidiana

Sejam $a, b \in \mathbb{Z}$, onde $0 \leq b \leq a$ existem únicos inteiros q *e* r que satisfazem as condições:

$$a = bq + r$$

e

$$0 \leq r < b.$$

Euclides em seu livro Elementos mostra que sempre é possível efetuar a divisão de a por b com resto. Isto será bastante utilizado no estudo que está sendo aqui desenvolvido.

2.3 ALGORITMO DE EUCLIDES

Nesta seção, que tem como referência Hefez (2004), serão apresentados conceitos e estratégias que possibilitarão resolver problemas sobre divisibilidade de inteiros, de forma a operar com seus múltiplos e divisores comuns.

2.3.1 Máximo divisor comum

Definição 2.3 *Sejam $a, b \in \mathbb{Z}^*$, o máximo divisor comum será um inteiro positivo d tal que*
1. $d \mid a$ e $d \mid b$;
2. Se $c \mid a$ e $c \mid b$, onde $c \in \mathbb{Z}$, então $c \leq d$.
Onde existe $x, y \in \mathbb{Z}$ tal que

$$ax + by = d.$$

Denotaremos o máximo divisor comum de a e b usando a seguinte notação

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

Exemplo 2.4 *Determine o $mdc(12, 30)$.*
Solução: Primeiramente vamos listar os divisores naturais de 12, onde aqui esse conjunto será representado por $D(12)$. Assim,

$$D(12) = \{1, 2, 3, 4, 6, 12\}.$$

Agora façamos o mesmo para o número 30 onde denominaremos o conjunto de seus divisores naturais por $D(30)$. Assim,

$$D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}.$$

Veja que $1, 2, 3, 4, 6$ são divisores comuns de 12 e 30. Listados os divisores comuns, basta observar o maior destes apresentados. Dessa forma, temos que 6 é o máximo divisor comum de 12 e 30. ■

Não será sempre necessário listar todos os divisores naturais de dois números para obter o maior deles. Existe um algoritmo que muito nos ajudará nesse procedimento. Veja a seguir:

2.3.2 Algoritmo de Euclides

O algoritmo de Euclides é um dos métodos mais antigos que se destaca por sua eficiência para se obter o máximo divisor comum de dois números.

Proposição 2.4 *Se $a = bq + r$, então o $mdc(a, b) = mdc(b, r)$.*
Demonstração: Seja $d = mdc(a, b)$. Dessa forma, $d \mid a$ e $d \mid b$. Assim, $d \mid a - qb = r$, o que implica d ser divisor comum de b e r.
Admitindo $c \in \mathbb{Z}$, onde $c \mid b$ e $c \mid r$. Assim

$$c \mid (bq + r) = a,$$

ou seja, c é um divisor comum de a e b.
Como $d = mdc(a, b)$ temos que $d \geq c$. Daí têm-se que

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

■

Sejam $a, b \in \mathbb{Z}$. Já é possível concluir que

1. se $a \neq 0$, então $mdc(a, 0) = a$;

2. se $a \neq 0$, então $mdc(a, a) = a$;

3. se $b \mid a$, então $mdc(a, b) = b$

Admitindo $a \neq b$, onde $a > b$ e $b \nmid a$, assim

$$a > b > 0.$$

O uso repetido do algoritmo da divisão fornece as seguintes igualdades:

$$a = bq_1 + r_1,\ 0 < r_1 < b$$

$$b = r_1 q_2 + r_2,\ 0 < r_2 < r_1$$

$$r_1 = r_2 q_3 + r_3,\ 0 < r_3 < r_2$$

$$r_2 = r_3 q_4 + r_4,\ 0 < r_4 < r_3$$

Como $r_i > 0,\ \forall i = 1, \cdots, n$ temos que:

$$b > r_1 > r_2 > \cdots r_n$$

e existem apenas $b - 1$ inteiros positivos menores que b. Assim, $r_{n+1} = 0$, e implica

$$r_{n-2} = r_{n-1} q_n + r_n,\ 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n q_{n+1} + r_{n+1},\ e\ r_{n+1} = 0.$$

Assim, r_n é o máximo divisor comum de a e b procurado.
Portanto,

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

Este processo para obter-se o Máximo divisor comum de dois inteiros positivos é denominado algoritmo de euclides.

Exemplo 2.5 *Usando o algoritmo de Euclides determine* $mdc(60, 98)$.
Solução: Temos que:

$$98 = 60 \cdot 1 + 38$$

$$60 = 38 \cdot 1 + 22$$

$$38 = 22 \cdot 1 + 16$$

$$22 = 16 \cdot 1 + 6$$

$$16 = 6 \cdot 2 + 4$$

$$6 = 4 \cdot 1 + 2$$

$$4 = 2 \cdot 2.$$

Assim, o $mdc(60, 98) = 2$. ■

2.3.3 Mínimo múltiplo comum

Definição 2.4 *Dados* $a, b \in \mathbb{Z}^*$, *o mínimo múltiplo comum de* a *e* b *será um inteiro positivo* m *que obedece as seguintes condições:*

1. $a \mid m$ *e* $b \mid m$;

2. Se $a \mid c$ *e* $b \mid c$, *com* $c > 0$, *então* $m \leq c$.

Assim, m *é múltiplo comum de* a *e* b *e é menor que todo múltiplo qualquer de* a *e* b.

Proposição 2.5 *Sejam* $a, b \in \mathbb{Z}$, *temos que*

$$mdc(a,b) \cdot mmc(a,b) = ab.$$

Demonstração: Seja $mdc(a,b) = d$ e $mmc(a,b) = m$. Veja que $a \mid a \cdot \frac{b}{d}$ e $b \mid b \cdot \frac{a}{d}$. Assim, $\frac{ba}{d}$ é um múltiplo comum de a e b.
Dessa forma, existe k tal que

$$\frac{ab}{d} = mk, \ k \in \mathbb{N}.$$

Assim,

$$\frac{a}{d} = \frac{m}{b}k \ e \ \frac{b}{d} = \frac{m}{a}k.$$

Com efeito, k é um divisor comum de $\frac{a}{d}$ e $\frac{b}{d}$ e pela definição, estes não têm divisores comuns.
Logo $k = 1$, daí $\frac{ab}{d} = m \Rightarrow ab = dm$.
Portanto,

$$ab = mdc(a,b) \cdot mmc(a,b).$$

■

Exemplo 2.6 *Calcule o* $mmc(60, 45)$.
Solução: Primeiramente calculemos o $mdc(60, 45)$. Pelo algoritmo de Euclides:

$$60 = 45 \cdot 1 + 15$$

$$45 = 15 \cdot 3$$

Portanto, $mdc(60, 45) = 15$. Assim,

$$mmc(60, 45) = \frac{60 \cdot 45}{15} = 180.$$

■

2.4 EQUAÇÕES DIOFANTINAS

Chama-se equação diofantina toda equação polinomiual independente da quantidade de incógnitas, onde o tipo mais simples, e também o que será utilizado nesse estudo é

$$ax + by = c$$

onde $a, b \in \mathbb{Z}$ e $ab \neq 0$.

Proposição 2.6 *Uma equação diofantina terá solução em* $\mathbb{Z}$ *se e somente se* $mdc(a, b) \mid c$.
Demonstração: Admitindo que $ax + by = c$ tem solução, assim existem x_0, y_0 tal que

$$ax_0 + by_0 = c.$$

Seja $d = mdc(a, b),\ \exists r, s \in \mathbb{Z}$ onde $a = dr$ e $b = ds$, temos que

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

Veja que $rx_0 + sy_0 \in \mathbb{Z}$ e d divide c $(d \mid c)$.
Reciprocamente, admita que $d = mdc(a, b) \mid c$,daí $\exists t \in \mathbb{Z}$ onde $c = dt$. Como $mdc(a, b) = d$, $\exists x_0, y_0 \in \mathbb{Z}$ de forma que

$$d = ax_0 + by_0.$$

Assim,

$$c = dt = (ax_0 + by_0)t = a(tx_0) + b(ty_0).$$

Portanto, tx_0, ty_0 é uma solução da equação $ax + by = c$. ∎

Proposição 2.7 *Se* $d \mid c$, *onde* $d = mdc(a, b)$ *e* x_0, y_0 *uma solução particular da equação diofantina linear* $ax + by = c$, *as demais soluções são dadas por*

$$x = x_0 + \frac{b}{d}t,$$

e

$$y = y_0 - \frac{a}{d}t$$

para $t \in \mathbb{Z}$ *arbitrário.*
Demonstração: Admitindo que x_0, y_0 é uma solução particular de $ax + by = c$. Seja x_1, y_1 outra solução desta equação. Então, temos:

$$ax_0 + by_0 = ax_1 + by_1.$$

Daí,

$$a(x_1 - x_0) = b(y_0 - y_1).$$

Como $mdc(a, b) = d,\ \exists\ r, s \in \mathbb{Z}$ onde,

$$a = dr\ e\ b = ds,$$

com $mdc(r, s) = 1$.
Assim,

$$r(x_1 - x_0) = s(y_0 - y_1). \tag{1}$$

Disso temos, que $r \mid (y_0 - y_1)$. Portanto, $\exists t \in \mathbb{Z}$ onde,

$$y_0 - y_1 = rt. \tag{2}$$

Da equação 1 e da equação 2, temos

$$x_1 - x_0 = st,$$

Isto implica que:

$$x_1 = x_0 + st = x_0 + (\frac{b}{d}) \cdot t$$

e

$$y_1 = y_0 - rt = y_0 - (\frac{a}{d}) \cdot t.$$

Os valores x_1, y_1 satisfazem a equação $ax + by = c,\ \forall t \in \mathbb{Z}$.
Note que: $ax_1 + by_1 = a[x_0 + \frac{b}{d} \cdot t] + b[y_0 - \frac{a}{d} \cdot t] = (ax_0 + by_0) + (\frac{ab}{b} - \frac{ab}{b})t = c + 0 \cdot t = c$.
Logo, d divide c.

Assim, $ax + by = c$, admite infinitas soluções, e uma para cada t. ∎

Exemplo 2.7 *Determinar todas as soluções inteiras da seguinte equação diofantina linear*

$$56x + 72y = 40$$

Solução: Usando o algoritmo de Euclides, para determinar $mdc(56, 72)$.

$$72 = 56 \cdot 1 + 16$$

$$56 = 16 \cdot 3 + 8$$

$$16 = 8 \cdot 2 + 0$$

Assim, $mdc(56, 72) = 8$. Veja que $8 \mid 40$, logo a equação diofantina tem solução. Com

efeito

$$8 = 56 - 16 \cdot 3 = 56 - (72 - 56) \cdot 3 = 56 \cdot 4 - 72 \cdot 3 = 56 \cdot 4 + 72 \cdot (-3).$$

Disso temos,

$$56 \cdot 4 + 72 \cdot (-3) = 8.$$

Multiplicando por 5 ambos os lados da equação acima obtemos

$$56 \cdot 20 + 72 \cdot (-15) = 40.$$

Portanto, $x_0 = 20$, e $y_0 = -15$ é uma solução particular da equação proposta. Todas as demais soluções são dadas por

$$x = 20 + 9t$$

e

$$y = -15 - 7t,$$

onde t é um inteiro arbitrário.

■

2.5 TEOREMA FUNDAMENTAL DA ARITMÉTICA

Definição 2.5 *Um inteiro positivo $p > 1$ é um número primo, quando somente 1 e p são seus divisores positivos. Um número maior que 1 não-primo é denominado composto.*
Aqui são apresentados alguns números pertencentes ao conjunto dos números primos

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

Definição 2.6 *Sejam $a, b \in \mathbb{Z}^*$, a e b são primos entre si se $mdc(a, b) = 1$.*
Observação 2.3 *Um primo p e um inteiro k são ditos primos entre si se $p \nmid k$.*
Observação 2.4 *Seja p, k e q inteiros, com p primo. Se $p \mid kq$ então $p \mid k$ ou $p \mid q$, para quaisquer $k, q \in \mathbb{Z}$.*
Teorema 2.2 *(Teorema fundamental da aritmética) Todo inteiro x maior que 1 pode ser representado por uma única decomposição, ao menos de ordem, como produto de fatores primos.*
Demonstração: Seja a_1 ($a_1 > 1$) o menor divisor de x. Supondo que a_1 não seja primo, então existe b_1, tal que $2 \leqslant b_1 < a_1$ e $b_1 \mid a_1$. Temos que $a_1 \mid x$, e por transitividade $b_1 \mid x$. Dessa forma, chegamos a uma contradição, pois inicialmente foi escolhido a_1 o menor divisor de x. Portanto, a_1 é primo.

Como $a_1 \mid x$, existe p_1, tal que $x = a_1 \cdot p_1$. Se $p_1 = 1$, x é primo, já que a_1 é um primo como verificamos acima.
Se $p_1 > 1$, teremos de modo análogo, a_2 o menor divisor de p_1. Seja p_2 tal que $p_1 = a_2 \cdot p_2$, com a_2 primo. Assim,

$$x = a_1 \cdot a_2 \cdot p_2$$

com $a_1 \cdot a_2$ primos e $1 \leqslant p_2 < a_1$. Se $p_2 = 1$, então $x = a_1 \cdot a_2$. Se $p_2 < a_1$, chegamos a uma contradição, o que obriga $p_2 = 1$ ou p_2 ser primo. Realizando esse processo repetidas vezes, obteremos, $a_1, a_2, ..., a_n$ e uma sequência de números naturais $p_1 > p_2 > ... > p_n \geqslant 1$. Sempre que $p_n \neq 1$, poderemos obter uma decomposição em fatores primos de p_n. E quando $p_n = 1$,

$$x = a_1 \cdot a_2, ... \cdot a_n$$

onde, $\forall a_i$, com $i = 1, 2, ..., n$; a_i é primo.
Supondo que $x \in \mathbb{Z}$ tenha duas decomposições distintas. Sejam elas

$$x = p_1 p_2 \cdots p_n$$

$$x = q_1 q_2 \cdots q_n$$

onde p_i, q_i são primos $\forall i \in [1, n]$. Dessa forma,

$$p_1 \cdots p_n = x = q_1 \cdots q_n.$$

Disso podemos verificar que p_1 divide algum q_i. Chega-se aqui a uma contradição, pois q_i é primo fazendo isso para todo p_i verifica-se que $p_i = q_i$. Assim verifica-se que um inteiro maior que 1 admite única decomposição em fatores primos.

■

Teorema 2.3 *Se n é um inteiro natural composto, então n tem um divisor p tal que $p \leq \sqrt{n}$.*
Demonstração: Se o inteiro n é composto então, existem $b, c \in \mathbb{Z}$ tais que

$$n = bc,$$

onde $1 < b < n$ e $1 < c < n$.
Supondo que $b \leq c$, teremos:

$$b^2 \leq bc = a \Rightarrow b \leq \sqrt{n}.$$

Como $b > 1$, pelo Teorema Fundamental da Aritmética b tem pelo menos um divisor primo p, de forma que

$$p \leq b \leq \sqrt{n}.$$

Sabendo que $p \mid b$ e $b \mid n$, isto implica que $p \mid n$. Ou seja, p é um inteiro primo $p \leq \sqrt{n}$, divisor de n.

■

A decomposição de um inteiro $n > 1$ pode ser feita da seguinte maneira:

- divide-se o número n pelo seu menor divisor primo (digamos, p_1);
- divide-se o quociente obtido a_1 pelo seu menor divisor primo p_2;
- divide-se o quociente obtido a_2 pelo seu menor divisor primo p_3;
- realiza-se esse processo repetidasvezes até se obter um quociente igual a 1;

Os números são colocados em duas colunas :

- na coluna da esquerda ficam os quociente obtidos, que aparecem abaixo do número a ser fatorado;
- na coluna da direita são inseridos os divisores primos, do menor para o maior estando ao lado do número ao qual ele divide;

Dessa forma

$$\begin{array}{r|l} n & p_1 \\ a_1 & p_2 \\ a_2 & p_3 \\ \vdots & \vdots \\ a_i & p_j \\ a_j & a_j \\ 1 & \end{array}$$

Portanto, a decomposição de n em fatores primos é dada da seguinte maneira:

$$n = p_1 p_2 p_3 \cdots p_j a_j.$$

Exemplo 2.8 *Obtenha a decomposição em fatores primos do número* 100.

Para obter a decomposição em fatores primos será usada a fatoração. Assim

$$\begin{array}{r|l} 100 & 2 \\ 50 & 2 \\ 25 & 5 \\ 5 & 5 \\ 1 & \end{array}$$

Disso temos que

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2.$$

Exemplo 2.9 *Obtenha a decomposição em fatores primos do número 1120.*
Para obter a decomposição em fatores primos será usada a fatoração. Assim

$$\begin{array}{r|l} 1120 & 2 \\ 560 & 2 \\ 280 & 2 \\ 140 & 2 \\ 70 & 2 \\ 35 & 5 \\ 7 & 7 \\ 1 & \end{array}$$

Disso temos que

$$1120 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \cdot 7 = 2^5 \cdot 5 \cdot 7.$$

2.6 CRITÉRIOS DE DIVISIBILIDADE

Para alguns divisores existem regras que permitem conferir a divisibilidade sem se efetuar a divisão euclidiana. Essas estratégias são denominadas critérios de divisibilidade. Usando-os, será possível mais facilmente realizar as operações que serão apresentadas no decorrer deste estudo.

2.6.1 Divisibilidade por 2

Proposição 2.8 *Um número é divisível por* 2 *se, e somente se, o algarismo das unidades é um número divisivel por* 2.

Demonstração: ($\Longrightarrow$)Seja x um número inteiro. Podemos escrever sua decomposição

da seguinte maneira:

$$x = a_n 10^n + \cdots a_2 10^2 + a_1 10 + a_0.$$

Admitindo $b = a_n 10^n + \cdots a_2 10^2 + a_1 10$, temos que

$$b = 10(a_n 10^{n-1} + \cdots + a_1) = 2 \cdot 5(a_n 10^{n-1} + \cdots + a_1).$$

Portanto, $2 \mid b$.
Admitindo que $2 \mid x$ e $2 \mid b$ isto implica que $2 \mid x - b = a_0$. Assim, para que a_0 seja divisível por 2, $a_0 = 0, 2, 4, 6, 8$.
($\Longleftarrow$)Sabendo que $2 \mid a_0$ e $2 \mid b$, daí

$$x = a_0 + b \Rightarrow 2 \mid x.$$

Portanto, quando o algarismo das unidades for divisível por 2 o número x também será.

$$\therefore 2 \mid x \Leftrightarrow 2 \mid a_0$$

■

Exemplo 2.10 $2 \mid 1046$*, pois* $2 \mid 6$*;*

Exemplo 2.11 $2 \nmid 793$*, pois* $2 \nmid 3$*;*

2.6.2 Divisibilidade por 3

Proposição 2.9 *Um número será divisível por 3 se, e somente se, a soma de seus algarismos for divisível por 3.*
Demonstração: Seja $x \in \mathbb{Z}$ múltiplo de 3, tal que seus algarismos sejam a_i, onde $i = 1, \cdots, n$. Isto implica que x pode ser escrito da seguinte maneira:

$$x = a_1 \cdot 10^0 + a_2 \cdot 10^1 + a_3 \cdot 10^2 + \cdots + a_n \cdot 10^{n-1}.$$

Um número será divisível por 3 quando puder ser escrito da forma $3n$, com $n \in \mathbb{Z}$. Temos que $3 \nmid 10$, pois não existe n, tal que $3 \cdot n = 10$. Mas, temos que existe n, tal que $3n + 1 = 10$.
Por indução, tentemos verificar que para 10^k, existe n tal que $3n + 1 = 10^k$, com $k \in \mathbb{Z}^*$
Para $k = 1$, existe $n = 3$ tal que $3n + 1 = 10$. Por hipótese indutiva, vamos admitir que para $k = r$, existe n_1 onde

$$10^r = 3n_r + 1.$$

Quando o expoente for $r+1$, têm-se que:

$$10^{r+1} = 10^r \cdot 10 = (3n_r + 1) \cdot (3n + 1) = 9n_1 n + 3n_1 + 3n + 1 = 3(3n_1 n + n + n_1) + 1.$$

Admitindo $n_{r+1} = 3(3n_1 n + n + n_1)$, $10^{r+1} = 3n_{k+1} + 1$. Portanto, para cada $k \in \mathbb{N}$, existe $n \in \mathbb{Z}$ onde $10^k = 3n + 1$. Assim, podemos escrever x da seguinte forma:

$$x = a_1 + a_2(3b_1 + 1) + a_3(3b_2 + 1) + \cdots + a_n(3b_{n-1}),$$

com $b \in \mathbb{Z}$.
Ou ainda:

$$x = (a_1 + a_2 + \cdots + a_n) + 3(a_2 b_1 + \cdots + a_n b_{n-1}).$$

Seja $a = (a_1 + a_2 + \cdots + a_n)$ e $b = 3(a_2 b_1 + \cdots + a_n b_{n-1})$, temos que $x = a + b$. Suponha que $3 \mid x$. Como $3 \mid b$ segue que

$$3 \mid (x - b) \Rightarrow x \mid a.$$

Reciprocamente, suponha que $3 \mid a$. Como $3 \mid b$, então $3 \mid a + b = x$.
Portanto,

$$3 \mid x \Longleftrightarrow 3 \mid a$$

■

Exemplo 2.12 *75 é divisível por* 3, *pois* $7 + 5 = 12$, *e* $3 \mid 12$.

Exemplo 2.13 *64 não é divisível por* 3, *pois* $6 + 4 = 10$ *e* $3 \nmid 10$.

2.6.3 Divisibilidade por 5

Proposição 2.10 *Um número é divisível por* 5 *se, e somente se, o algarismo das unidades for divisível por* 5.

Demonstração: Seja x um inteiro que possa ser escrito da seguinte forma:

$$x = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots a_n \cdot 10^n$$

Seja $B = a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots a_n \cdot 10^n$, verifica-se que

$$B = 10(a_1 + \cdots a_n \cdot 10^{n-1}).$$

Reciprocamente, suponha que $5 \mid a_0$. Como $5 \mid B$ então $5 \mid B + a_0 = x$.

$$\therefore \ 5 \mid x \Leftrightarrow 5 \mid a_0.$$

■

Exemplo 2.14 85 *é divisível por* 5, *pois* $5 \mid 5$.

Exemplo 2.15 94 *não é divisível por* 5, *pois* $5 \nmid 4$.

2.6.4 Divisibilidade por 7

Denotaremos um número $x \in \mathbb{N}$ que possui n algarismos onde $a_i = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ da seguinte maneira:

$$x = a_n a_{n-1} \cdots a_2 a_1.$$

Proposição 2.11 *Um número natural* $x = a_n a_{n-1} ... a_1 a_0$ *é divisível por 7 se, e somente se, a diferença entre o número* $y = a_n a_{n-1} ... a_2 a_1$ *e o dobro de* a_0 *é divisível por 7.*

Demonstração:

($\Longrightarrow$)Seja $x = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1 10^1 + a_0$, onde x é divisível por 7, logo $\exists q \in \mathbb{Z}$ tal que $x = 7q$.

Considerando $k = a_n 10^{n-1} + a_{n-1} 10^{n-2} + \cdots + a_2 10 + a_1 - 2a_0$. Vamos provar que k é divisível por 7.

De fato,

$$k = 10^{-1}(a_n 10^n + a_{n-1} 10^{n-1} + \cdots a_2 10^2 + a_1 10^1) - 2a_0.$$

Assim:

$$k = 10^{-1}(7q - a_0) - 2a_0$$

$$= 10^{-1} \cdot 7q - a_0(10^{-1} + 2)$$

$$= 7 \cdot 10^{-1} q - a_0 \cdot 21 \cdot 10^{-1}$$

$$= 7(10^{-1} q - a_0 \cdot 3 \cdot 10^{-1}.$$

Portanto, $7 \mid k$.

($\Longleftarrow$) Seja $k = a_n 10^{n-1} + a_{n-1} 10^{n-2} + \cdots + a_2 10 + a_1 - 2a_0$ onde $7 \mid k$ e $\exists p \in \mathbb{Z}$ tal que $k = 7p$.

Logo,

$$k = 10^{-1}(a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_2 10^2 + a_1 10^1) - 2a_0 = 10^{-1}(x - a_0) - 2a_0.$$

Ou seja,

$$7p = 10^{-1}x - a_0 \cdot 21 \cdot 10^{-1} \Rightarrow 7(p + 3a_0 10_{-1}) = 10^{-1} \cdot x$$

$$\Rightarrow 7(10p + 3a_0) = x.$$

Portanto, $7 \mid x$. ∎

Exemplo 2.16 *91 é divisível por 7, pois* $7 \mid (9 - 2 \cdot 1) = 7$.

Exemplo 2.17 *102 não é divisível por 7, pois* $7 \nmid 10 - 2 \cdot 2 = 4$.

2.6.5 Divisibilidade por 11

Proposição 2.12 *Um número é divisível por* 11 *se, e somente se, a soma dos algarismos de ordem par subtraídos da soma dos de ordem ímpar resultar em um número divisível por* 11.

Demonstração: ($\Longrightarrow$) Seja $x \in \mathbb{Z}$, tal que $11 \mid x$. Dessa forma existe $p \in \mathbb{Z}$ tal que $11p = x$. Então, temos que x pode ser escrito da seguinte maneira:

$$x = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0.$$

Temos que
$10 = 11 \cdot 1 - 1$, fazendo $y = 1$, temos que

$$10 = 11y - 1.$$

Assim, $100 = 10^2 = (11y - 1)^2 = 121y^2 - 22y + 1 = 11(11y^2 - 2y) + 1$. Veja que quando o expoente é ímpar a potência de base pode ser escrita como $11p - 1$ e quando for par poderá ser escrito como $11p + 1$, onde $p \in \mathbb{Z}$. Tentemos mostrar que para todo n, existe $q \in \mathbb{Z}$, onde $10^n = 11q + 1$, quando n for par. Sendo n par, então existe $p \in \mathbb{Z}$ tal que $n = 2k$. Vamos usar o Príncipio da Indução Finita para provar isto. De fato, quando $k = 1$ é válida a igualdade acima.
Seja $n = 2k$ por hipótese de indução

$$10^{2k} = 11q + 1,$$

onde $q \in \mathbb{Z}$.
Seja $n = 2k + 2$, obtemos:

$$10^{2k+2} = 10^{2k} \cdot 10^2 = (11q+1) \cdot (11p+1) = 121pq + 11p + 11q + 1 = 11(11pq + p + q) + 1.$$

De modo análogo, seja agora n ímpar temos que n pode ser escrito da seguinte maneira:

$$n = 2k + 1.$$

Para $n = 2k+1$ temos que é válido o que queremos aqui mostrar. Por hipótese de indução

$$10^{2k+1} = 11r - 1.$$

Para $n = 2k + 3$ temos:

$$10^{2n+3} = 10^{2n+1} \cdot 10^2 = (11r-1) \cdot (11p+1) = 121pr + 11r - 11p - 1 = 11(11pr + r - p) - 1.$$

Daí podemos reescrever x assim:
Consideremos aqui n par,e $p_i \in \mathbb{Z}$ onde $i = 1, \cdots, n$. Com efeito:

$$x = a_n(11p_n + 1) + a_{n-1}(11p_{n-1} - 1) + \cdots + a_1(p_1 - 1) + a_0.$$

Seja $b = 11(a_n p_n + \cdots + a_1 p_1)$ e $c = (a_n + a_{n-2} + \cdots + a_0) - (a_{n-1} + \cdots + a_1)$. Temos que $x = b + c$. Admitindo que $11 \mid x$ temos que $11 \mid x - b = c$.
Agora consideremos n ímpar, assim

$$x = a_n(11p_n - 1) + a_{n_1}(11p_{n-1} + 1) + \cdots + a_1(11p + 1) + a_0$$

Seja $b = 11(a_n p_n + \cdots + a_1 p_1)$ e $d = (a_{n_1} + a_{n-2} + \cdots + a_1) - (a_n + \cdots + a_1)$. Sabendo que $x = b + d$, assim $11 \mid x - b = d$. Portanto, em ambos os casos temos que a condição necessária é satisfeita.
($\Longleftarrow$) Seja $x = b + c$ ou $x = b + d$ como 11 divide b, c e d então $11 \mid x$.

■

Exemplo 2.18 *2948 é divisível por 11, pois* $11 \mid 9 + 8 - 2 - 4 = 11$.

Exemplo 2.19 *2568 não é divisível por 11, pois* $11 \nmid 5 + 8 - 2 - 6 = 5$.

3 SISTEMA DE CONGRUÊNCIAS LINEARES

No presente capítulo, serão consolidados os saberes básicos para se obter o significado de congruências, onde os principais resultados tiveram como base o estudo desenvolvido por Santos (2009).

3.1 CONGRUÊNCIAS

Definição 3.1 *Sejam $a, b \in \mathbb{Z}$, e m um inteiro positivo fixado. Assim, a é congruente a b módulo m se $m \mid (a-b)$. Logo, existe $K \in \mathbb{Z}$, tal que*

$$a - b = k \cdot m$$

Notação: $a \equiv b \mod m$

Exemplo 3.1 $32 \equiv 4 \mod 7$, *pois* $7 \mid (32-4)$

Exemplo 3.2 $10 \equiv 1 \mod 3$, *pois* $3 \mid (10-1)$

Teorema 3.1 *Dois inteiros a e b são congruentes módulo m, se e somente se a e b deixam o mesmo resto quando divididos por m.*

Demonstração: Inicialmente, suponhamos que $a \equiv b \mod m$, assim existe $k \in \mathbb{Z}$, tal que

$$a - b = km.$$

Seja r o resto da devisão de b por m. Pelo algoritmo da divisão, o resto deverá ser sempre maior ou igual que zero e menor que o divisor.

Assim, temos $b = mq + r$ e $0 \leq r < m$. Consequentemente, $a = km + b = km + mq = (k+q)m + r$.

Isto significa que r é o resto da divisão de a por m. Assim verifica-se que a e b divididos por m deixam resto r.

Respectivamente, supondo que a e b divididos por m deixam resto r. Assim, existem q_1, q_2 tais que

$$a = mq_1 + r$$

e

$$b = mq_2 + r,$$

sendo $0 \leq r < m$.

Disso, podemos concluir

$$a - b = mq_1 + r - (mq_2 + r) = mq_1 - mq_2 = m(q_1 - q_2).$$

Portanto, $m \mid (a-b)$ se e somente se $a \equiv b \mod m$. ∎

Proposição 3.1 *Seja $m \in \mathbb{Z}_+$ e $a, b, c \in \mathbb{Z}$. Temos as seguintes propriedades:*

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

Demonstração: A prova da proposicão 3.1 será realizada em partes, observando a ordem das propriedades apresentadas.

Primeiramente, vamos mostrar a propriedade 1.
Tem-se que, $m \cdot 0 = 0$, logo $m \mid 0$. Sendo $0 = a - a$, $m \mid (a - a)$. Portanto, $a \equiv a \mod m$.

Agora, vamos mostrar a propriedade 2.
Com efeito, se $a \equiv b \mod m$, então $a - b = km$ com $k \in \mathbb{Z}$,
Assim,

$$b - a = -(km) = -km.$$

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

Por fim, vamos mostrar a propriedade 3.
Se $a \equiv b \mod m$ e $b \equiv c \mod m$, $\exists n, k \in \mathbb{Z}$ tais que

$$a - b = mn$$

e

$$b - c = mk.$$

Disso temos,

$$a = mn + b$$

e

$$c = -mk + b.$$

Assim,

$$a - c = (mn + b) - (-mk + b) = mn + b + mk + b = m(n + k).$$

Desde que $(n + k) \in \mathbb{Z}$ concluímos que:

$$a \equiv c \mod m.$$

■

Proposição 3.2 *Seja* $m \in \mathbb{Z}_+$ *fixado e* $a, b \in \mathbb{Z}$ *, se* $a \equiv b \mod m$ *e se* $n \mid m$, *então* $a \equiv b \mod n$.

Demonstração: Por certo,

$$a \equiv b \mod m \Rightarrow m \mid (a - b) \; e \; a - b = km.$$

Sabendo que $n \mid m$, deve existir $p \in \mathbb{Z}$ tal que

$$m = np.$$

Assim,

$$a - b = km = knp \Rightarrow n \mid a - b \; e \; a \equiv b \mod n.$$

■

Proposição 3.3 *Se* $a \equiv b \mod m$ *e se* $c > 0$*, então* $ac \equiv bc \mod mc$
Demonstração: De fato,

$$a \equiv b \mod m \Rightarrow a - b = km.$$

Multiplicando cada elemento da igualdade acima por c, obtém -se:

$$ac - bc = kmc.$$

Disso temos,

$$ac \equiv bc \mod mc.$$

■

Proposição 3.4 *Se* $a \equiv b \mod m$ *e se* a, b, m *são todos divisíveis por* $d \in \mathbb{Z}_+$*, então* $\frac{a}{d} \equiv \frac{b}{d} \mod \frac{m}{d}$,
Demonstração: Sabendo que $a \equiv b \mod m$, isto implica que

$$a - b = km.$$

Multiplicando por $\frac{1}{d}$ a igualdade acima, obtém-se:

$$\frac{a}{d} - \frac{b}{d} = k \, \frac{m}{d}$$

o que implica

$$\frac{a}{d} \equiv \frac{b}{d} \mod \frac{m}{d}.$$

■

Proposição 3.5 *Se* $ac \equiv bc \mod m$ *e se o* $mdc(c, m) = 1$*, então* $a \equiv b \mod m$.
Demonstração: Se $ac \equiv bc \mod m$ então $\exists p \in \mathbb{Z}$ onde

$$ac - bc = pm.$$

Isto implica que:

$$c(a-b) = pm.$$

Como o $mdc(c,m) = 1$, então $c \nmid m$. Dessa forma, c divide p. Assim, existe $p_1 \in \mathbb{Z}$ tal que $p_1 = \dfrac{p}{c}$, onde

$$a - b = p_1 m \Rightarrow a \equiv b \mod m.$$

■

3.2 CONGRUÊNCIAS LINEARES

Definição 3.2 *Chama-se congruência linear toda equação da forma*

$$ax \equiv b \mod m,$$

onde a e b são dois inteiros quaisquer e m um inteiro positivo.

Teorema 3.2 *A congruência linear $ax \equiv b \mod m$ tem solução se, e somente se, d divide b, sendo*

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

Demonstração:

($\Longrightarrow$) Seja x_1 uma solução da congruência linear

$$ax \equiv b \mod m.$$

Para isto, existe y_1, onde

$$ax_1 - b = my_1 \Rightarrow ax - my_1 = b$$

e como $d \mid a$ e $d \mid m$, pois $d = mdc\,(a,m)$, temos que:

$$d \mid (ax_1 - mx_1).$$

Portanto, pelo verificado acima,

$$d \mid b.$$

($\Longleftarrow$) Sabemos que $d \mid b$, ou seja, $\exists k \in \mathbb{Z}$, tal que

$$b = dk.$$

Sabendo que $mdc(a, m) = d$, existem x_1 e y_1 tais que

$$ax_1 + my_1 = d.$$

Multiplicando a igualdade acima por k, obtemos

$$akx_1 + mky_1 = dk.$$

Disso temos

$$akx_1 + mky_1 = b.$$

Assim,

$$a(kx_1) \equiv b \mod m.$$

Pelo que verificamos, kx_1 é uma solução da congruência linear $ax \equiv b \mod m$. ∎

Teorema 3.3 *Se d divide b, sendo $d = mdc(a, m)$, então a congruência linear*

$$ax \equiv b \mod m$$

tem precisamente d soluções incongruentes módulo m.

Demonstração: É sabido que há uma equivalência da congruência $ax \equiv b \mod m$ com a equação diofantina $ax - my = b$, e esta possui solução se e somente se $mdc(a, m)$ dividir b. Seja x_0, y_0 uma solução particular da equação diofantina $ax - my = b$, as demais soluções são dadas por:

$$x = x_0 + \frac{m}{d}\, t$$

e

$$y = y_0 + \frac{a}{d}\ \ t,$$

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

Pelo que verificamos acima, podemos listar as soluções para x atribuindo valores a t. Sendo S o conjunto de soluções para x quando $t \in [0, d-1]$, ou seja, quando t pertencer aos primeiros d inteiros não-negativos, temos que:

$$S = \{x_0,\ x_0 + 2\frac{m}{d},\ x_0 + 3\frac{m}{d}, \cdots,\ x_0 + (d-1)\frac{m}{d}\}.$$

Visto isso, vamos verificar que essas soluções são incongruentes módulo m, e que todos

os inteiros dados pela fórmula $x = x_0 + \frac{m}{d}t$ são congruentes módulo m a algum deses inteiros.
Sejam t_1 e t_2 tais que

$$0 \leq t_1 < t_2 \leq d - 1$$

e suponha que

$$\frac{m}{d}t_1 \equiv \frac{m}{d}t_2 \mod m.$$

Visto que o $mdc(\frac{m}{d}, m) = \frac{m}{d}$, podemos dividir por $\frac{m}{d}$ cada fator da congruência acima. Assim, obtém-se

$$t_1 \equiv t_2 \mod d.$$

Isto implica, que $\exists n \in \mathbb{N}^*$ tal que

$$t_1 - t_2 = d \cdot n.$$

Logo,

$$d \mid t_1 - t_2.$$

Mas, aqui chegamos a um absurdo, pois $t_1 - t_2 < d$.
Qualquer outro inteiro $x_0 + \frac{m}{d}t$ é congruente módulo m, a algum dos d inteiros acima apresentados. Pelo algoritmo da divisão

$$t = dq + r,$$

onde

$$0 \leq r \leq d - 1.$$

Portanto,

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

isto é,

$$x_0 + \frac{m}{d}t \equiv \ x_0 + \frac{m}{d}r \mod m,$$

onde $x_0 + \frac{m}{d}r$ é um dos inteiros selecionados.
Portanto, quando há solução há exatamente d soluções incongruentes de $ax \equiv b \mod m$.

■

Exemplo 3.3 *Obtenha as soluções da congruência linear a seguir:*

$$6x \equiv 21 \mod 8.$$

Solução: Temos que o $mdc(6, 8) = 2$. Sabe-se que $2 \nmid 21$, então a congruência não tem solução inteira. ■

Exemplo 3.4 *Obtenha as soluções da congruência linear a seguir:*

$$30x \equiv 12 \mod 54.$$

Solução: Temos que $mdc(30, 54) = 6$, e $6 \mid 12$, logo a congruência tem precisamente 6 soluções mutuamente incongruentes módulo 54.
Sabe-se que:

$$6 \cdot 5x \equiv 6 \cdot 2 \mod \frac{54}{6}$$

o que implica:

$$5x \equiv 2 \mod 9.$$

Mas, temos que $2 \equiv 20 \mod 9$, logo:

$$5x \equiv 20 \mod 9.$$

Dividindo a congruência acima por 5, obtém-se:

$$x \equiv 4 \mod 9.$$

As seis soluções são dadas pela fórmula:

$$x = 4 + \frac{54}{6}t = 4 + 9t,$$

onde $t = 0, 1, 2, 3, 4, 5$.
Portanto, as soluções dessa congruência são os inteiros: $4, 13, 22, 31, 40$ *e* 49.

■

3.3 RESOLUÇÃO DE EQUAÇÕES DIOFANTINAS LINEARES POR CONGRUÊNCIAS

Uma equação diofantina $ax+by = c$, tem solução se, e somente se, $mdc(a, b) \mid c$.
Seja x_0, y_0 uma solução particular qualquer desta equação, então:

$$ax_0 + by_0 = c,$$

e

$$ax_0 - c = -by_0,$$

o que implica:

$$ax_0 \equiv c \mod b.$$

Para obter uma solução particular, basta determinar uma solução qualquer onde $x = x_0$ da congruência linear:

$$ax \equiv c \mod b$$

substituimos o valor de x_0 na equação para encontrar o valor y_0 tal que $ax_0 + by_0 = c$.

Exemplo 3.5 *Resolver por congruências a equação diofantina linear:*

$$48x + 7y = 17.$$

Solução: Como o $mdc(7, 48) = 1$, a equação tem solução. Precisamos encontrar uma solução particular desta equação. A solução particular buscada dessa equação é obtida encontrando uma solução geral da congruência a seguir:

$$48x \equiv 17 \mod 7.$$

Sabe-se que $48x \equiv -x \mod 7$, disso têm-se que:

$$-x \equiv 17 \mod 7$$

Sabendo que $17 \equiv 3 \mod 7$, assim:

$$-x \equiv 3 \mod 7.$$

Logo,

$$x \equiv -3 \mod 7.$$

Sabendo que $-3 \equiv 4 \mod 7$, obtemos:

$$x \equiv 4 \mod 7$$

Agora, substituindo $x = 4$ na equação diofantina dada, teremos:

$$48 \cdot 4 + 7y = 17 \Rightarrow 7y = 17 - 48 \cdot 4 \Rightarrow y = \frac{17 - 192}{7} = -\frac{175}{7} = -25.$$

Então, assim obtém-se uma solução particular para a equação diofantina dada. Para obter as demais soluções basta atribuir a t um valor inteiro, nas fórmulas a seguir:

$$x = 4 + 7t,$$

e

$$y = -25 - 48t.$$

■

3.4 INVERSO DE UM NÚMERO

Definição 3.3 *Seja $a \in \mathbb{Z}$, denominamos inverso de a módulo m um inteiro a^{-1} tal que*

$$aa^{-1} \equiv 1 \mod m.$$

Teorema 3.4 *Seja $a \in \mathbb{Z}$, a tem único inverso módulo m, se $mdc(a, m) = 1$.*
Demonstração: Como o $mdc(a, m) = 1$, a congruência linear $ax \equiv 1 \mod m$, terá única solução. Seja x_0 a solução dessa congruência, têm-se então:

$$ax_0 \equiv 1 \mod m.$$

Pelo que podemos verificar acima, x_0 é o inverso de a. Portanto, existe um único a^{-1} quando $mdc(a, m) = 1$. ■

Exemplo 3.6 *Ache os inversos de 4 e 8 módulo 9.*
Solução: Primeiramente vamos encontrar o inverso de 4. Seja x_1 o inverso de 4 módulo 9, devemos ter:

$$4x_1 \equiv 1 \mod 9.$$

Como o $mdc(4, 9) = 1$ logo existe um único elemento inverso. Sabendo que $4 \mid 28$ e $28 \equiv 1$ mod 9. Dessa forma,

$$4x_1 = 28 \Rightarrow x_1 = 7.$$

Portanto, 7 é o inverso de 4 módulo 9.
Seja x_2 o inverso de 8 módulo 9. Assim,

$$8 \cdot x_2 \equiv 1 \mod 9.$$

Como o $mdc(8,9) = 1$, logo existe um único elemento inverso. Sabendo que $8 \mid 64$ e $64 \equiv 1 \mod 9$. Dessa forma,

$$8 \cdot x_2 = 64 \Rightarrow x_2 = 8.$$

Portanto, 8 é o inverso de 8 módulo 9. ∎

3.5 TEOREMA CHINÊS DO RESTO

Quando temos um grupo de congruências lineares, onde se deseja obter uma solução que as satisfaz, temos um sistema de congruências lineares. Um sistema de duas ou mais congruências lineares não tem necessariamente uma solução, mesmo que cada uma das congruências do sistema, isoladamente, tenha solução. Usando o Teorema chinês do resto somos capazes de facilmente obter sua solução, quando as exigências deste são satisfeitas.

Teorema 3.5 (Teorema chinês do resto) *Sejam $m_1, m_2, \cdots, m_r$ números naturais onde $mdc(m_i, m_j) = 1$, quando $i \neq j$. O sistema de congruências lineares :*

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \vdots \\ x \equiv a_r \mod m_r \end{cases}$$

tem única solução módulo $m = m_1 m_2 \cdots m_r$.

Demonstração: Seja $m = m_1 m_2 \cdots m_r$ e $M_k = \dfrac{m}{m_k} = m_1 m_2 \cdots m_{k-1} m_{k+1} \cdots m_r$. Assim, M_k é o produto de todos os m_i, com exceção de m_k. Sabendo que $mdc(m_i, m_j) = 1$, têm-se que a congruência

$$M_k x \equiv 1 \mod m_k,$$

admite única solução x_k, pois $mdc(M_k, n_k) = 1$.

Mostremos que o número inteiro $x = a_1 M_1 x_1 + a_2 M_2 x_2 + \cdots + a_r M_r x_r$ é solução de cada uma das congruências do sistema dado.

Se $i \neq k$, temos que $m_k \mid M_i$, assim:

$$M_i \equiv 0 \mod m_k.$$

Isto implica que:

$$x = a_1M_1x_1 + a_2M_2x_2 + \cdots + a_rM_rx_r \equiv a_kM_kx_k \mod m_k.$$

Sabendo que x_k é solução da congruência

$$M_kx \equiv 1 \mod m_k,$$

têm-se que

$$M_kx_k \equiv 1 \mod m_k.$$

Portanto,

$$x \equiv a_k \cdot 1 \equiv a_k \mod m_k$$

é uma solução linear do sistema de congruências dado.
Agora, será verificado se há outra solução para o sistema. Supondo que x_1 seja uma solução arbitrária tal que $x_1 \neq x$. Desta forma, deve-se ter

$$x \equiv a_k \equiv x_1 \mod m_k,$$

onde $k = 1, \cdots, r$.
Disso temos

$$m_k \mid (x - x_1)\ \forall k \in 1, \cdots, r.$$

Sabendo que $\forall i, j$ onde $i \neq j$ onde $i, j = 1, \cdots, r$

$$m \mid (x - x_1)$$

e

$$x \equiv x_1 \mod m.$$

Chegamos assim a um absurdo, pois $x = x_1$. Mostra-se assim a unicidade da solução do sistema de congruências lineares dado. ∎

Exemplo 3.7 *Achar um inteiro que deixa restos 3, 5 e 7 quando dividido por 5, 7 e 11 respectivamente.*

Solução: Vamos escrever as congruências para obter o inteiro que satisfaz as condições acima:

$$\begin{cases} x \equiv 3 \mod 5 \\ x \equiv 5 \mod 7 \\ x \equiv 7 \mod 11 \end{cases}$$

Temos aqui um sistema de congruências lineares, e sabe-se que

$$mdc(5,7) = mdc(5,11) = mdc(7,11) = 1.$$

Usando o teorema do resto chinês o sistema tem única solução módulo $m = 5 \cdot 7 \cdot 11 = 385$. Assim,

$$M_1 = \frac{385}{5} = 77,$$
$$M_2 = \frac{385}{7} = 55,$$

e

$$M_3 = \frac{385}{11} = 35.$$

Assim, obtemos as congruências lineares a seguir:

$$\begin{cases} 77x_1 \equiv 1 \mod 5 \\ 55x_2 \equiv 1 \mod 7 \\ 35x_3 \equiv 1 \mod 11 \end{cases}$$

Vamos encontrar a solução de cada congruência acima

$$77x_1 \equiv 1 \mod 5$$

Sabe-se que $1 \equiv 231 \mod 5$ assim:

$$77x_1 \equiv 231 \mod 5.$$

Portanto,

$$x_1 \equiv 3 \mod 5.$$

Prosseguindo, para

$$55x_2 \equiv 1 \mod 7$$

sabe-se que $1 \equiv 15 \mod 7$, disso temos que:

$$55x_2 \equiv 15 \mod 7.$$

Assim,

$$11x_2 \equiv 3 \mod 7.$$

Sabendo que $3 \equiv 66 \mod 7$, implica:

$$11x_2 \equiv 66 \mod 7,$$

$$\Rightarrow x_2 \equiv 6 \mod 7.$$

Por fim, para

$$35x_3 \equiv 1 \mod 11 \equiv 45 \mod 11$$

$$\Rightarrow 7x_3 \equiv 9 \mod 11$$

$$7x_3 \equiv 42 \mod 11 \Rightarrow x_3 \equiv 6 \mod 11.$$

Assim o inteiro x é dado por:

$$x = 3 \cdot 77 \cdot 3 + 5 \cdot 55 \cdot 6 + 7 \cdot 35 \cdot 6 = 693 + 1650 + 1470 = 3813.$$

Têm-se que

$$3813 \equiv 348 \mod 385.$$

Assim, $x \equiv 348 \mod 385$ é a única solução do sistema de congruências dado e o número 348 é um número que atende as exigências propostas. ■

Teorema 3.6 *Sejam $m_1, \cdots, m_r$ inteiros primos entre si dois a dois, ou seja, $mdc(m_i, m_j) = 1$ quando $m_i \neq m_j$ e $i, j = 1, \cdots, n$ e a_k inteiro tal que*

$$mdc(a_k, m_k) = 1 \text{ para } k = 1, \cdots, r.$$

Temos que, o sistema de congruências lineares:

$$\begin{cases} a_1x \equiv b_1 \mod m_1 \\ a_2x \equiv b_2 \mod m_2 \\ \vdots \\ a_rx \equiv b_r \mod m_r \end{cases} \tag{3}$$

tem solução única $m = m_1 \cdots m_r$.

Demonstração: Visto que o $mdc(a_k, m_k) = 1$, a congruência linear

$$a_kx \equiv 1 \mod m_k$$

possui solução única módulo $m_k : a_k^*$ onde:

$$a_ka_k^* \equiv 1 \mod m_k.$$

Assim, a conguência $a_kx \equiv b_k \mod m_k$ é equivalente a seguinte congruência:

$$x \equiv b_ka_k^* \mod m_k.$$

E assim o sistema 3 é equivalente a:

$$\begin{cases} x \equiv b_1a_1^* \mod m_1 \\ x \equiv b_2a_2^* \mod m_1 \\ \vdots \\ x \equiv b_ra_r^* \mod m_r \end{cases}$$

Pelo teorema chinês dos restos terá uma única solução módulo $m = m_1 \cdots m_r$.

■

Exemplo 3.8 *Encontre a solução do sistema de congruências a seguir:*

$$\begin{cases} 2x \equiv 1 \mod 5 \\ 3x \equiv 9 \mod 6 \\ 4x \equiv 1 \mod 7 \end{cases} \tag{4}$$

Solução: Os módulos 5, 6 e 7 das congruências do sistema são primos entre si. Ou seja:

$$mdc(5, 6) = mdc(5, 7) = mdc(6, 7) = 1.$$

Pelo teorema chinês do resto, o sistema dado tem única solução módulo $m = 5 \cdot 6 \cdot 7 = 210$. Vamos encontrar as soluções a_i^* das congruências lineares:

Para a primeira

$$2x \equiv 1 \mod 5,$$

nota-se que

$$1 \equiv 6 \mod 5 \Rightarrow 2x \equiv 6 \mod 5 \Rightarrow x \equiv 3 \mod 5.$$

Para a segunda

$$3x \equiv 9 \mod 6 \Rightarrow x \equiv 3 \mod 6.$$

Por fim, para a terceira

$$4x \equiv 1 \mod 7$$

tem-se que

$$1 \equiv 36 \mod 7 \Rightarrow 4x \equiv 36 \mod 7 \Rightarrow x \equiv 9 \mod 7 \Rightarrow x \equiv 2 \mod 7.$$

As soluções são $a_1^* = 3$, $a_2^* = 3$ e $a_3^* = 2$. O sistema 4 é equivalente a:

$$\begin{cases} x \equiv 3 \mod 5 \\ x \equiv 3 \mod 6 \\ x \equiv 2 \mod 7 \end{cases}$$

Seguindo o algoritmo do Teorema chinês do resto tem-se

$$M_1 = \frac{210}{5} = 42,\ M_2 = \frac{210}{6} = 35 \ e \ M_3 = \frac{210}{7} = 30.$$

Assim, para a congruência

$$42x \equiv 1 \mod 5$$

temos que

$$1 \equiv 21 \mod 5 \Rightarrow 42x \equiv 21 \mod 5 \Rightarrow 2x \equiv 1 \mod 5.$$

Dado que $1 \equiv 6 \mod 5$ temos que

$$2x \equiv 6 \mod 5 \Rightarrow x \equiv 3 \mod 5.$$

Para a congruência

$$35x \equiv 1 \mod 6,$$

tem-se

$$1 \equiv 175 \mod 6 \Rightarrow 35x \equiv 175 \mod 6 \Rightarrow x \equiv 5 \mod 6.$$

Por fim, para a congruência

$$30x \equiv 1 \mod 7$$

tem-se

$$1 \equiv 50 \mod 7 \Rightarrow 30x \equiv 50 \mod 7 \Rightarrow 3x \equiv 5 \mod 7.$$

Dados que $5 \equiv 12 \mod 7$ concluímos que

$$x \equiv 4 \mod 7$$

Assim,

$$x = 3 \cdot 42 \cdot 3 + 3 \cdot 5 \cdot 35 + 30 \cdot 2 \cdot 4 = 1173.$$

Disso temos:

$$x \equiv 1173 \mod 210.$$

É sabido que $1173 \equiv 93 \mod 210$. Portanto

$$x \equiv 93 \mod 210$$

é a solução procurada. ■

4 APLICAÇÕES

Vamos utilizar as estratégias de obtenção de uma solução de um sistema de congruências lineares para resolver alguns problemas trazidos de olímpiadas de matemática.

4.1 PROBLEMA SOBRE SATÉLITES

Três satélites passarão sobre o Rio de Janeiro à noite. O primeiro à 1h da madrugada, o segundo às 4h e o terceiro às 8h da manhã. Cada satélite tem um período diferente. O primeiro leva 13h para completar uma volta em torno da Terra, o segundo 15h e o terceiro 19h. Determine quantas horas decorrerão, a partir da meia-noite, até que os três satélites passem ao mesmo tempo sobre o Rio de Janeiro.

Solução: Para resolver esse problema, deve-se identificar a incógnita e as operações descritas. Sabendo que o primeiro satélite passa a cada 13h a partir de 1h da madrugada. Seja x_1 o horário em que o este está sobre o Rio de Janeiro, têm-se que:

$$x_1 = 1 + 13t,$$

onde $t \in \mathbb{N}$, o que equivale dizer que

$$x_1 \equiv 1 \mod 13.$$

Já o segundo satélite passa a primeira vez às 4h da manhã e leva 15h para passar novamente. Seja x_2 em horas o momento em que esse satélite está sobre o Rio de Janeiro e pode ser obtido:

$$x_2 = 4 + 15t$$

onde $t \in \mathbb{N}$.
Isto equivale dizer que

$$x_2 \equiv 4 \mod 15.$$

O terceiro satélite passa a primeira vez às 8h e leva 19h para completar uma volta. Assim, o momento x_3 em horas em que o satélite está sobre o Rio de Janeiro é descrito da seguinte forma:

$$x_3 = 8 + 19t,$$

onde $t \in \mathbb{N}$.
Isto equivale dizer que

$$x_3 \equiv 8 \mod 19.$$

O momento x em que ios satélites passarão juntos sobre o Rio de Janeiro ocorre quando

$$x = x_1 = x_2 = x_3$$

Assim, podemos descrever um sistema usando as congruências obtidas acima:

$$\begin{cases} x \equiv 1 \mod 13 \\ x \equiv 4 \mod 15 \\ x \equiv 8 \mod 19 \end{cases}$$

Usando o teorema chinês do resto, e sabendo que 13, 15 e 19 são primos entre si, isso nos assegura que o sistema terá única solução módulo $m = 13 \cdot 15 \cdot 19 = 3705$, onde

$$M_1 = \frac{3705}{13} = 285;\ M_2 = \frac{3705}{15} = 247\ e\ M_3 = \frac{3705}{19} = 195$$

Vamos determinar as soluções das seguintes congruências:

- $285x \equiv 1 \mod 13$

Note que $285x \equiv 12x \mod 13$, isto implica

$$12x \equiv 1 \mod 13.$$

Desde que $1 \equiv 14 \mod 13$, assim:

$$12x \equiv 14 \mod 13 \Rightarrow 6x \equiv 7 \mod 13$$

Dado que, $7 \equiv 72 \mod 13$. Isto implica que $6x \equiv 72 \mod 13$. Portanto

$$x \equiv 12 \mod 13$$

- $247x \equiv 1 \mod 13$

Sabe-se que $247x \equiv 7x \mod 15$. Dessa forma, $7x \equiv 1 \mod 15$. Como $1 \equiv 91 \mod 15$ por transição $7x \equiv 91 \mod 15$, disso temos

$$x \equiv 13 \mod 15$$

- $195x \equiv 1 \mod 19$

Sabe-se que $195 \equiv 5 \mod 19$, o que implica $5x \equiv 1 \mod 19$. Como $1 \equiv 20 \mod 19$, tem-se que

$$x \equiv 4 \mod 19.$$

Assim, x será:

$$x = 285 \cdot 1 \cdot 12 + 247 \cdot 4 \cdot 13 + 195 \cdot 8 \cdot 4 = 22504$$

Dado que $22504 \equiv 274 \mod 3705$, temos:

$$x \equiv 274 \mod 5.$$

Portanto, os satélites estarão simultaneamente sobre o Rio de Janeiro após 274 horas ou seja após 11 dias e dez horas após meia-noite. ■

4.2 PROBLEMA DO CAMPONÊS E OS OVOS

Um camponês tem um certo número de ovos; quando divide por 3, sobra-lhe 1; quando divide por 4 sobram 2 ovos; e quando os divide por 5, sobram 3. Quantos ovos tem o camponês?

Solução: Para obter o número x de ovos deve-se determinar a solução do sistema a seguir:

$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 2 \mod 4 \\ x \equiv 3 \mod 5 \end{cases}$$

A primeira congruência nos dá que $\exists y_1 \in \mathbb{Z}$ tal que

$$x = 1 + 3y_1. \tag{5}$$

Usando o resultado da equação 5 na segunda congruência dada, obtém-se

$$1 + 3y_1 \equiv 2 \mod 4 \Rightarrow 3y_1 \equiv 1 \mod 4. \tag{6}$$

Pela congruência 6, temos que

$$y_1 \equiv 3 \mod 4.$$

Seja $y_2 \in \mathbb{Z}$ tal que $y_1 = 3 + 4y_2$, assim

$$x = 1 + 3(3 + 4y_2) = 10 + 12y_2.$$

Substituindo esse valor na terceira congruência do sistema, verifica-se

$$10 + 12y_2 \equiv 3 \mod 5,$$

o que implica

$$12y_2 \equiv -7 \mod 5.$$

Sabendo que $-7 \equiv 3 \mod 5$ e $3 \equiv 48 \mod 5$, assim

$$12y_2 \equiv 48 \mod 5 \Rightarrow y_2 \equiv 4 \mod 5. \tag{7}$$

O resultado da congruência 7 nos dá que $\exists y_3 \in \mathbb{Z}$, tal que

$$y_2 = 4 + 5y_3.$$

Assim, x é dado por

$$x = 10 + 12y_2 = 10 + 12(4 + 5y_3) = 58 + 63y_3.$$

A equação descrita acima pode ser representada pela congruência linear $x \equiv 58 \mod 63$,

obrigando $y_3 = 0$. Portanto, 58 é o número de ovos do camponês. ■

4.3 PROBLEMA DA REPOSIÇÃO SALARIAL

Uma empresa tem três cargos: Junior, Office e Sênior. A cada três anos o cargo Junior tem reposição salarial, o cargo Office tem reposição salarial a cada 4 anos e o cargo Sênior a cada 5 anos. Se o cargo Junior teve aumento a primeira vez em 2002, o Office em 2003 e o Sênior em 2004. Qual o primeiro ano que acontecerá reposição para os três cargos, e de quanto em quanto tempo terão reajustes juntos?

Solução: Usando o teorema chinês do resto, é possível obter o sistema a seguir:

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

A solução desse problema terá módulo $m = 3 \cdot 4 \cdot 5 = 60$, onde $M_1 = 20$, $M_2 = 15$, e $M_3 = 12$. Agora, vamos obter a solução de cada congruência a seguir:

$$\begin{cases} 20x \equiv 1 \mod 3 \\ 15x \equiv 1 \mod 4 \\ 12x \equiv 1 \mod 5 \end{cases} \tag{8}$$

Sabendo que $1 \equiv 40 \mod 3$, por transição $20x \equiv 40 \mod 3$, isto implica

$$x \equiv 2 \mod 3.$$

Veja que $1 \equiv 225 \mod 4$, assim, $15x \equiv 225 \mod 4$ implicando $x \equiv 15 \mod 4$. Mas, $15 \equiv 3 \mod 4$, assim

$$x \equiv 3 \mod 4.$$

Da última congruência dada no sistema 8, pode-se verificar que $1 \equiv 36 \mod 5$. Desta forma,

$$12x \equiv 36 \mod 5 \Rightarrow x \equiv 3 \mod 5.$$

A solução x buscada é dada por

$$x = 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 4 \cdot 12 \cdot 3 = 359. \tag{9}$$

Da equação 9, pode-se afirmar que

$$x \equiv 359 \mod 60 \Rightarrow x \equiv 59 \mod 60.$$

Assim, a solução mínima é 59 e as demais são dadas por

$$x = 59 + 60t,$$

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

Portanto, o primeiro ano que haverá reajuste para os três cargos será 2059 e esse evento acontecerá a cada 60 anos. ■

5 CONCLUSÃO

O presente estudo fundamentou-se em apresentar como a Matemática está presente em nossa realidade e de forma ainda mais precisa como a Aritmética pode ser contextualizada em exercícios para os educandos do ensino fundamental e médio.

Para isto, foram aqui apresentados conteúdos programáticos da educação básica a fim de solidificar os saberes que estiveram sendo formados neste trabalho. As revisões e acentuações de conhecimentos de teoria dos números inteiros consistiram em estratégias para justificar o processo constituinte do propósito desta temática.

Este aprendizado torna eficaz a compreensão mais profunda de operações com números inteiros, e assim, a fundamentação do teorema chinês do resto pode ser melhor visualizada e significada em olímpiadas de Matemática. Com efeito, os estudantes e professores utilizam deste na contextualização de situações do cotidiano que podem ser expressas através de um sistema de congruências lineares.

Portanto, sabendo que os conhecimentos matemáticos sempre estão colaborando para possibilitar uma transformação da realidade, é possível afirmar que o estudo cá apresentado, buscou justificar conhecimentos do ensino superior utilizando as bases do ensino básico. De forma, que este possa ser aplicado possibilitando aos profissionais da educação e aos educandos que desejarem ingressar em curso de Matemática a estarem em constante formação seja como educador ou como discente do ensino superior.

REFERÊNCIAS

ALENCAR FILHO, Edgard de. **Teoria Elementar dos Números**. São Paulo: Nobel, 1981.

HERFEZ, A. **Elementos de Aritmética**. Rio de Janeira: SBM, 2004.

MOREIRA, Carlos Gustavo T. de A.; MARTÍNEZ, Fabio E. B.; SALDANHA, Nicolau C. **Tópicos de Teoria dos Números**. Rio de Janeira: SBM, 2012.

SANTOS, J. P. O. **Introdução à Teoria dos Números**. 3. ed. Rio de Janeiro: IMPA, 2009.

SILVA, Rivanildo Garcia da. **Congruências e Equações diofantinas: algumas aplicações.** Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Universidade Estadual da Paraíba, Campina Grande, 2018.