UNIVERSIDADE DO ESTADO DO AMAZONAS

ESCOLA NORMAL SUPERIOR

LICENCIATURA EM MATEMATICA

KELLYANE RIBEIRO PEREIRA

TEOREMA DO RESTO CHINÊS E SUAS APLICAÇÕES.

MANAUS, FEVEREIRO

2023

KELLYANE RIBEIRO PEREIRA

TEOREMA DO RESTO CHINÊS E SUAS APLICAÇÕES

Trabalho de Conclusão do Curso elaborado junto às disciplinas TCC I e TCC II do Curso de Licenciatura em Matemática da Universidade do Estado do Amazonas para a obtenção do grau de licenciado em Matemática.

Orientador: Prof. Dr. Almir Cunha da Graça Neto.

MANAUS, FEVEREIRO
2023

TERMO DE APROVAÇÃO

TERMO DE APROVAÇÃO DE TRABALHO DE CONCLUSÃO DO CURSO DE LICENCIATURA EM MATEMÁTICA DA UNIVERSIDADE DO ESTADO DO AMAZONAS

Ata de Defesa do Trabalho de Conclusão de Curso em Licenciatura em Matemática da Escola Normal Superior-UEA de **KELLYANE RIBEIRO PEREIRA.**

Em 16 de março de 2023, às 18:30h, na Sala Maria Clara Dantas da Escola Normal Superior da UEA na presença da Banca Examinadora composta pelos professores: Dr. Almir Cunha da Graça Neto, Me. Alessandro Monteiro de Menezes e Me. Alexandra Salerno Pinheiro, a aluna **KELLYANE RIBEIRO PEREIRA** apresentou o Trabalho de Conclusão do Curso intitulado: "**TEOREMA DO RESTO CHINÊS E SUAS APLICAÇÕES.**" A Banca Examinadora deliberou e decidiu pela APROVAÇÃO do referido trabalho, com o conceito 9,5 divulgando o resultado ao aluno e demais presentes.

Manaus, 16 de março de 2023.

Presidente da banca examidadora

Orientador (a)

Avaliador 1

Avaliador 2

Aluno

AGRADECIMENTOS

Agradeço primeiramente ao meu Deus e criador, por me permitir concluir essa etapa tão desafiadora, mas necessária para a minha formação acadêmica.

À minha irmã gêmea, Kellyana Ribeiro, que me apoia, orienta e até mesmo me auxilia, da melhor maneira possível, sem ela nada do que sou hoje seria possível.

Ao meu amor, Leandro Gomes por me apoiar e acreditar em mim, mais do que eu mesma, e por estar sempre ao meu lado.

Aos meus amigos Gustavo Silva e Pamela Bianca por sempre me ajudarem quando precisei e mesmo quando achei que não precisava, eles estavam lá para me apoiar.

Aos meus avós, Rita Maria e Raimundo Nonato, que fizeram o possível e o impossível para que eu pudesse concluir essa etapa. E ao bebê que salvou a minha vida, meu primo Elias, obrigado por me permitir ver o futuro como algo bom, e mesmo sem saber você mudou a minha vida.

E ao meu orientador Prof. Dr. Almir Neto, que aceitou me orientar nesse processo, além de um ótimo professor é uma grande inspiração para mim.

Resumo

Esta pesquisa foi realizada com o objetivo de demonstrar o Teorema do Resto Chinês, com o intuito de simplificar e auxiliar algumas aplicações que envolvessem sistemas de congruências lineares. O teorema apresenta aplicações tanto no Ensino Básico quanto no superior, e dessa forma este trabalho pôde contribuir com as aplicações do Teorema do Resto Chinês. A fim de obter êxito na pesquisa, será explorado o contexto histórico da Teoria aritmética dos números e do Teorema do Resto Chinês, para compreender a origem do problema que originou o Teorema. Além do aspecto histórico, foi necessário o estudo e explanação de conceitos de Divisibilidade, Equações Diofantinas, Congruências e Congruências lineares para o embasamento das demonstrações feitas, e como consequência na utilização das aplicações apresentadas neste trabalho. Em relação aos resultados obtidos, eles foram favoráveis, visto que foi possível demonstrar e resolver aplicações do Teorema do Resto Chinês. O trabalho é fundamentado nos conceitos apresentados pelos autores Filho (1981); Rosen (2011); Glória (2019); Santos (2020).

Palavras-Chave: Sistema de congruência lineares. Teorema do Resto Chinês. Congruência lineares.

SUMÁRIO

LISTA DE ABREVIATURA E SIGLAS

TRC – Teorema do Resto Chinês.

PROFMAT – Mestrado Profissional em Matemática em Rede Nacional.

ENQ – Exame Nacional de Qualificação.

OBM – Olimpíada Brasileira de Matemática.

OBMEP- Olimpíada Brasileira de Matemática das Escolas Públicas.

INTRODUÇÃO

Imaginemos o seguinte questionamento: “Em uma cesta contendo ovos, na contagem de dois em dois, de três em três, de quatro em quatro e de cinco em cinco, sobram 1,2,3 e 4 ovos, respectivamente. Qual é a menor quantidade de ovos que a cesta pode ter?”, esse e vários problemas, tanto em nível básico como em nível superior, podem ser resolvidos através de um sistema de congruências lineares, e visto que um sistema pode não ter solução, mesmo que cada congruência linear apresente uma solução, faz-se necessária a utilização de um resultado importante que é o Teorema do Resto Chinês, para auxiliar na resolução de um sistema de congruências lineares com determinadas características.

Dessa forma, é evidente que o Teorema do Resto Chinês contribui de forma significativa na resolução de diversas aplicações, que podem ser vistas até mesmo no cotidiano do aluno, tornando assim mais interessante a utilização do Teorema.

Nesse contexto, o objetivo geral da pesquisa é demonstrar de forma detalhada o Teorema do Resto Chinês, pois, como a demonstração é utilizada no processo de resolução das aplicações, faz-se bastante útil que ela seja demonstrada e explorada. E como consequência desse resultado, serão mostradas as aplicações tanto da OBMEP, OBM quanto do PROFMAT, por exemplo. E para satisfazer essa demonstração e as devida aplicações, é necessário definir Divisibilidade e suas propriedades, visto que o teorema é aplicado em determinadas circunstâncias, assim como, definir Congruências e Congruências Lineares.

A pesquisa está estruturada da seguinte forma: O capítulo 1 é destinado a fundamentação teórica onde aborda-se os aspectos históricos da Teoria Aritmética dos números e do Teorema do Resto Chinês, além disso são destacados os conceitos de Divisibilidade essenciais para futuras demonstrações e soluções apresentadas no trabalho, como o Máximo divisor comum, Algoritmo da divisão e inteiros primos entre si. Em seguida, destaca-se o conceito de inteiros congruentes, bem como as propriedades de congruência e as equações diofantinas lineares, posteriormente são apresentadas as definições de Congruências Lineares.

No capítulo 2, aborda-se a metodologia da pesquisa, com a abordagem quantitativa e a estratégia adotada foi a exploratória, e como procedimento técnico, a fim de seguir o rigor matemático, a pesquisa bibliográfica. Na apresentação e análise dos resultados enuncia-se o Teorema do Resto Chinês e sua respectiva demonstração detalhada, assim como as aplicações

nas olímpiadas e no exame nacional de qualificação do mestrado profissional em matemática em Rede Nacional (PROFMAT).

CAPÍTULO 1

FUNDAMENTAÇÃO TEÓRICA

1. Aspectos históricos

Neste capítulo será apresentado o aspecto histórico da Teoria aritmética dos números e do Teorema do Resto Chinês, de acordo com Boyer (1996), Eves (2011), Rosen (2011) e Pei; Salomaa; Ding; (1996)

1.1. Teoria dos Números

O que se conhece hoje da teoria dos números é resultado de muitas contribuições valiosas feitas por diversos matemáticos e estudiosos da antiguidade. Assim como eles contribuíram de forma tão significativa na construção do que conhecemos hoje como sendo a teoria dos números, esses resultados contribuem em diversos teoremas, demonstrações e aplicações.

Segundo Eves (2011, p.99) uma das primeiras contribuições para o desenvolvimento do que conhecemos da teoria dos números, se deu por Pitágoras com os números amigáveis, no mesmo segmento que o de Pitágoras temos Pierre de Fermat, que também encontrou um par de números amigáveis, porém esse par já havia sido encontrado por um árabe. O filósofo René Descartes também deu sua contribuição com um novo par de números amigáveis. Além dos números amigáveis é atribuído aos pitagóricos os números perfeitos, deficientes e abundantes (EVES, 2011).

Outra contribuição essencial foi feita por Euclides de Alexandria através do livro *Os elementos*. Euclides era conhecido por sua habilidade de ensinar, logo de expor os seus conhecimentos, sendo essa a chave para o sucesso de *os elementos.* Pelo contrário do que acreditam *os elementos* traziam uma ideia elementar não só de geometria, mas também de aritmética, no sentido da teoria dos números (BOYER,1996).

Os teoremas dos livros VII, VIII e IX (os elementos) trazem muito conhecimento de teoria dos números. O Livro VII traz duas proposições importantes para a teoria dos números, conhecido como “algoritmo de Euclides”.

O matemático Sun Zi também contribuiu com um livro que se assemelha muito ao livro *Nove Capítulos sobre a Arte da Matemática.* Nesse livro temos um marco importante que será explorado neste trabalho, o Teorema do Resto Chinês.

1.2. Teorema do Resto Chinês.

A primeira aparição do Teorema do Resto Chinês, foi no livro intitulado Sun Zi Suanjing, que significa Manual de Aritmética do sol, do matemático Sun Zi da china antiga, que apresenta três volumes, sendo o problema 26 do vol.3 o livro que mostra o problema que deu origem ao Teorema do Resto Chinês. Não se sabe a data exata da publicação deste livro.

No livro, a primeira ideia do TRC, é introduzida através de um problema: "Temos várias coisas, mas não sabemos exatamente quantas. Se os contarmos por três, temos dois sobrando. Se contarmos por cinco, temos três sobrando. Se contarmos por sete, temos dois sobrando. Quantas coisas existem?" (DING, 1996). Esse problema busca os restos de um número quando dividido por 3,5, e 7, sucessivamente, o livro até apresenta a resposta correta para esses restos, porém não foi possível fazer uma generalização de maneira correta dessa ideia.

Os exemplos dados por Sun Zi são simplesmente numéricos sem uma ideia geral, sendo assim Qin Jiushao (1202-1261) contribuiu com a forma geral para resolver os problemas do Teorema do Resto Chinês.

Nos dias atuais o Teorema do Resto Chinês é enunciado da seguinte maneira, "Sejam $m_1, m_2, \ldots, m_r$ inteiros positivos relativamente primos dois a dois. Então o sistema de congruências:

$$x \equiv a_1 (mod\ m_1)$$
$$x \equiv a_2 (mod\ m_2)$$
$$.$$
$$.$$
$$.$$
$$x \equiv a_r (mod\ m_r)$$

tem uma solução única módulo $M = m_1 m_2 \ldots m_r$ (ROSEN, 2011, p.162)

1.3. Divisibilidade

Neste capítulo serão apresentados tópicos de divisibilidade[1], que são a base para auxiliar demonstrações futuras.

[1] Todas as definições, teoremas e corolários desta seção estão de acordo com Filho (1981) em sua obra: Teoria Elementar dos Números.

Definição 1.3.1. (Divisibilidade em $\mathbb{Z}$) Sejam $u\ e\ v$ inteiros, com $u \neq 0$. Onde u divide v (denotado por $u|\ v$), se somente se existir um inteiro q, tal que $v = u \cdot q$. Se u divide v, então u é divisor de v. Caso contrário se u não divide v, então denotamos por $u \nmid v$. Essa relação "u divide v" é a relação de divisibilidade em $\mathbb{Z}$.

Exemplo:

I. Com $u = 3$ e $v = 21$, então $3|21$, pois $21 = 3 \cdot (7)$

II. Com $u = 6$ e $v = 30$, então $6|30$, pois $30 = 6 \cdot (5)$

III. Como podemos notar pelo exemplo (I) e (II), u é um divisor de v, então $-u$ é um divisor de v, pois a igualdade $v = u \cdot q$ implica $v = (-u) \cdot (-q)$.

Proposição 1. Se os inteiros $u, v\ e\ q, u|v$ e $v \mid q$, então $u \mid q$.

Exemplo: Dados $u = 12, v = 24$ e $q = 72, 12|24$ e $24|72$, então $12|72$.

Teorema 1. Para todos os inteiros, sendo u, v e c, tem-se as seguintes propriedades:

I. $u \mid 0$, $1 \mid u$ e $u|u$

II. Se $u \mid 1$, então $u = \pm 1$

III. Se $u \mid v$ e se $c|\ d$, então $u \cdot\ c \mid v \cdot d$

IV. Se $u \mid v$ e se $v|\ c$, então $u|\ c$

V. Se $u \mid v$ e se $v \mid u$, então $u = \pm\, v$

Demonstração:

I. Com efeito: $0 = u \cdot 0$; $u = 1 \cdot u$; $u = u \cdot 1$.

II. Com efeito: Se $u \mid 1$, então $1 = u \cdot q$ onde $q \in \mathbb{Z}$, implica em $u = 1$ e $q = 1$ ou $u = -1$ e $q = -1, isto$ é: $u = \pm 1$.

III. Com efeito: $u \mid v \Rightarrow v = u \cdot q$ com $q \in \mathbb{Z}$, $c \mid d \Rightarrow d = c \cdot q_1$ com $q_1 \in \mathbb{Z}$. Com isso $v \cdot d = (u \cdot c) \cdot (q \cdot q_1) \Rightarrow u \cdot c \mid v \cdot d$.

IV. Com efeito: $u \mid v \Rightarrow v = u \cdot q$, com $q \in \mathbb{Z}, v|\ c \Rightarrow c = v \cdot q_1$, com $q_1 \in \mathbb{Z}$. Portanto $c = u \cdot (q \cdot q_1) \Longrightarrow u|c$.

V. Com efeito:

$u \mid v \Rightarrow v$ com $q \in \mathbb{Z}$

$v \mid c \Rightarrow c = v \cdot q_1$, com $q_1 \in \mathbb{Z}$

Portanto: $u = v \cdot (q \cdot q_1) \Rightarrow q \cdot q_1 = 1 \Rightarrow q_1|\ 1 \Rightarrow q_1 = \pm 1 \Rightarrow u = \pm\, v$.

Teorema 2. (Algoritmo da Divisão) Dados dois inteiros $u\ e\ v$, com $v \neq 0$, então existem e são únicos os inteiros $q\ e\ r$ que satisfazem: $u = v.q + r\ e\ 0 \leq r < v$.

Corolário 1. Com dois inteiros u e v, com $v \neq 0$, existem e são únicos os inteiros q e r que satisfazem as condições: $u = v.q + r$ e $0 \leq r < |v|$.

Exemplo: Encontrar o quociente q e o resto r na divisão de $u = 40$ por $v = -12$, que torna as condições do algoritmo da divisão possíveis: $40 = 12 \cdot 3 + 4 \Longrightarrow 40 = (-12) \cdot (-3) + 4$ e $0 \leq 4 < |-12|$. Logo, o quociente $q = -3$ e o resto $r = 4$.

Exemplo: Encontrar o quociente q e o resto r na divisão de $u = 18$ por $v = 6$, de modo que sejam únicos. Efetuando a divisão usual dos valores absolutos de u e v, teremos: $u = v.q + r \Rightarrow 18 = 6 \cdot 3 + 0$.

Definição 1.3.2. (Máximo Divisor Comum) Sejam u e v dois inteiros não conjuntamente nulos ($u \neq 0$ ou $v \neq 0$). Chama-se máximo divisor comum de u e v o inteiro positivo d ($d \geq 0$) que satisfaz às condições:

I. $d|\, u\ e\ d|\, v$

II. se $c|\, u$ e se $c|\, v$, então $c \leq d$.

Notação do máximo divisor comum: $mdc(u, v)$.

É imediato que o $mdc(u, v) = mdc(v, u)$. Em particular:

i. o $mdc\ (0, 0) = 0$

ii. o $mdc\ (u, 1) = 1$

iii. se $u \neq 0$, então o $mdc(u, 0) = |u|$

iv. se $u|\, v$, então $o\ mdc(u, v) = |u|$

Teorema 3. Se u e v são dois inteiros não conjuntamente nulos ($u \neq 0\ ou\ v \neq 0$), então existe e é único o $mdc\ (u, v)$; além disso, existem inteiros x e y tais que $mdc\ (u, v) = u \cdot x + v \cdot y$, isto é, o $mdc\ (u, v)$ é uma combinação linear de u e v.

Definição 2.2.3. (Inteiros primos entre si) Sejam u e v dois inteiros, não conjuntamente nulos. Diz-se que u e v são primos entre si, se e somente se, o $mdc\ (u, v) = 1$.

Assim, por exemplo, são primos entre si os inteiros: 2 e 5, -9 e 16, -27 e -35, cujo $mdc\ (2,5) = mdc\ (-9, 16) = mdc\ (-27, -35) = 1$. Dois inteiros u e v primos entre si admitem como únicos divisores comuns 1 e -1.

Corolário 2. Se o $mdc\ (u, v) = d$, então $o\ mdc\ (u/d, v/d) = 1$.

1.4. Congruências

Nesta seção, serão abordados alguns resultados importantes que auxiliarão no desenvolvimento da demonstração do Teorema do Resto Chinês. A maioria desses resultados sobre congruências foram introduzidos por Gauss (1777-1855). Serão explorados definições, teoremas e corolários sobre Congruências[2] e Congruências Lineares.

Definição 2.3.1. (Inteiros congruentes) Sejam u e v dois inteiros quaisquer e seja m um inteiro positivo fixo. Diz-se que u é congruente a v módulo m se e somente se m divide a diferença $u - v$. Em outros termos, u é congruente a v módulo m, se e somente se, existe um inteiro k tal que $u - v = k \cdot m$.

Notação: $u \equiv v\,(mod\, m)$, indica-se que u é congruente a v módulo m. Portanto, simbolicamente:

$u \equiv v\,(mod\, m) \Leftrightarrow m|\,(u - v)$ ou seja: $u \equiv v\,(mod\, m) \Leftrightarrow \exists\, k \in \mathbb{Z} \mid u - v = k \cdot m$.

Exemplos:

I. $10 \equiv 26\,(mod\ 2)$, porque $2|\,(10 - 26)$

II. $-30 \equiv 51 (mod 3)$, porque $3|\,(-30 - 51)$

III. $-11 \equiv 17\,(mod\ 7)$, porque $7|\,(-11 - 17)$

IV. $85 \equiv 22\,(mod\ 9)$, porque $9|\,(85 - 22)$

Dado um m que não divide a diferença $u - v$, então diz-se que u é incongruente a v módulo m, o que se indica pela notação: $u \not\equiv v\,(mod\, m)$.

Teorema 5. (Caracterização de Inteiros Congruentes). Dois inteiros u e v são congruentes módulo m se, e somente se, u e v deixam o mesmo resto quando divididos por m.

Demonstração:

($\Rightarrow$) Suponhamos que $u \equiv v\,(mod\, m)$. Então, por definição: $u - v = k \cdot m$, com $k \in \mathbb{Z}$. Seja r o resto da divisão de v por m; então, pelo algoritmo da divisão: $v = m \cdot q + r$, onde $0 \leq r < m$. Portanto: $u = k \cdot m + v = k \cdot m + m \cdot q + r = (k + q)\, m + r$ e isto significa que r é o resto da divisão de u por m, isto é, os inteiros u e v divididos por m deixam o mesmo resto r.

---

[2] Todas as definições, teoremas e corolários desta seção estão de acordo com (FILHO,1981) em sua obra Teoria Elementar dos Números.

($\Longleftarrow$) Reciprocamente, suponhamos que u e v divididos por m deixam o mesmo resto r. Então, podemos escrever: $u = m \cdot q_1 + r \, e \, u = m \cdot q_2 + r, onde \, 0 \leq r < m$. Portanto, temos que $u - v = (q_1 - q_2)\, m \Rightarrow m | (u - v) \Rightarrow u \equiv v \, (mod \, m)$.

Exemplos: Sejam os inteiros 10 e 26, pelo algoritmo da divisão, $10 = 2 \cdot (5) + 0 \, e \, 26 = 2 \cdot (13) + 0$, isto é, 10 e 26 divididos por 2 deixam o mesmo resto 0. Logo, pelo teorema anterior: $10 \equiv 26 \, (mod \, 2)$. Agora, dois inteiros que deixam o mesmo resto quando divididos por 3 são -30 e 51. Tem-se a congruência: $-30 \equiv 51 \, (mod. 3)$, também pelo teorema anterior, -30 e 51 divididos por 3 deixam o mesmo resto 0. Pelo algoritmo da divisão, $-30 = 3 \cdot (10) + 0$ e $51 = 3 \cdot (17) + 0$.

Teorema 6. (Propriedades das congruências). Seja m um inteiro positivo fixo $(m > 0)$ e sejam $u, v \, e \, c$ inteiros quaisquer. Subsistem as seguintes prioridades:

I. $u \equiv u \, (mod \, m)$.
II. Se $u \equiv v \, (mod \, m)$, então $v \equiv u \, (mod \, m)$
III. Se $u \equiv v \, (mod \, m) \, e$ se $v \equiv c \, (mod \, m)$, então $u \equiv c \, (mod \, m)$.

Demonstração:

I. Com efeito: $m \mid 0 \, ou \, m \mid (u - u) \Rightarrow u \equiv u \, (mod \, m)$
II. Com efeito, se $u \equiv v \, (mod \, m)$, então $u - v = k \cdot m$, com $k \in \mathbb{Z}$. Portanto: $u - v = -(km) = (-k)\, m \Rightarrow v \equiv u \, (mod \, m)$.
III. Com efeito, se $u \equiv v \, (mod \, m)$ e se $v \equiv c \, (mod \, m)$, então existem inteiros h e $k \in \mathbb{Z}$ tais que $u - v = h \cdot m \, e \, v - c = k \cdot m$. Portanto: $u - c = (u - v) + (v - c) = h \cdot m + k \cdot m = (h + k)\, m$ e isto significa que $u \equiv c \, (mod \, m)$.

E, consoante este teorema, a relação R no conjunto $\mathbb{Z}$ dos inteiros definida por $uRv \Leftrightarrow u \equiv v \, (mod \, m)$ é reflexiva, simétrica e transitiva, ou seja, R é uma relação de equivalência em $\mathbb{Z}$. Esta relação de equivalência R em $\mathbb{Z}$ é denominada "congruência módulo m".

Teorema 7. Seja m um inteiro positivo fixo $(m > 0)$ e sejam u e v dois inteiros quaisquer. Subsistem as seguintes propriedades:

I. Se $u \equiv v \, (mod \, m)$ e se $n | \, m$, com $n > 0$, então $u \equiv v \, (mod \, n)$.
II. Se $u \equiv v \, (mod \, m)$ e se $c > 0$, então $u \cdot c \equiv v \cdot c \, (mod \, mc)$.

III. Se $u \equiv v\ (mod\ m)$ se u, v e m são todos divisíveis pelo inteiro $d > 0$, então $u/d \equiv v/d\ (mod\ m/d)$.

Exemplos:

I. $85 \equiv 22\ (mod\ 9) \implies 85 \equiv 22\ (mod\ 3)$

II. $6 \equiv 2\ (mod\ 2) \implies 12 \equiv 8\ (mod\ 4)$

III. $6 \equiv 4\ (mod\ 2) \implies 3 \equiv 2\ (mod\ 1)$

Teorema 8. Seja m um inteiro positivo fixo $(m > 0)$ e sejam u, v, c e d inteiros quaisquer. Subsistem as seguintes propriedades:

1. Se $u \equiv v\ (mod\ m)$ e se $c \equiv d\ (mod\ m)$, então $u + c \equiv v + d\ (mod\ m)$ e $u \cdot c \equiv v \cdot d\ (mod\ m)$.
2. Se $u \equiv v\ (mod\ m)$, então $u + c \equiv v + c\ (mod\ m)$ e $u \cdot c \equiv v \cdot c\ (mod\ m)$
3. Se $u \equiv v\ (mod\ m)$, então $u^n \equiv v^n\ (mod\ m)$ para todo inteiro positivo n.

Teorema 9. Se $u \cdot c \equiv v \cdot c\ (mod\ m)$ e se o $mdc\ (c, m) = d$, então $u \equiv v\ (mod\ m/d)$, $m > 1$.

Demonstração: Com efeito, se $u \cdot c \equiv v \cdot c\ (mod\ m)$, então: $uc - vc = (u - v)\ c = km$, com $k \in \mathbb{Z}$.

E se o $mdc\ (c, m) = d$, existem inteiros r e s tais que $c = d \cdot r$ e $m = d \cdot s$, onde r e s são primos entre si. Portanto: $(u - v)\ d \cdot r = k \cdot d \cdot s\ ou\ (u - v) = k \cdot s$. Logo, $u - v = k \cdot \frac{m}{d}$

Corolário 3. Se $u \cdot c \equiv v \cdot c\ (mod\ m)$ e se o $mdc\ (c, m) = 1$, então $u \equiv v\ (mod\ m)$. Com essa propriedade é fácil ver que é permitido *cancelar* fatores de ambos os membros de uma congruência que são primos com o módulo.

Corolário 4. Se $u \cdot c \equiv v \cdot c (mod\ p)$, com p primo, e se p não divide c $(p \nmid c)$, então $u \equiv v\ (mod\ p)$.

Demonstração: Com efeito, as condições, p não divide c $(p \nmid c)$ e p é primo, implicam que $mdc\ (c, p) = 1$.

1.5. Equações Diofantinas Lineares

Equação com mais de uma variável onde tem-se soluções inteiras, são conhecidas como equações diofantinas lineares da forma:

$$ux + vy = c$$

onde $u, v\ e\ c$ são inteiros, sendo $uv \neq 0$.

Todo par de inteiros $x_o\ e\ y_o$, onde $ux_o + vy_o = c$, chama-se solução inteira da equação $ux + vy = c$.

Teorema 10. A equação diofantina linear $ux + uy = c$ tem solução se e somente se d divide c, sendo $d = mdc\ (u, v)$.

Teorema 11. Se d divide c, onde $d = mdc\ (u, v)$, sendo $x_o\ e\ y_o$ um par de solução particular da equação diofantina linear $ux + vy = c$, então todas as outras soluções desta equação diofantina são dadas pelas seguintes fórmulas:

$$x = x_o + (v/d)t, y = y_0 - (u/d)t$$

onde t é um inteiro qualquer.

Exemplo[3]: Determinar todas as soluções da equação diofantina linear

$$172x + 20y = 1000.$$

Resolvendo o $mdc\ (172, 20)$ pelo algoritmo de *EUCLIDES:*

$$172 = 20 \cdot 8 + 12$$
$$20 = 12 \cdot 1 + 8$$
$$12 = 8 \cdot 1 + 4$$
$$8 = 4 \cdot 2 + 0$$

Logo, o $mdc(172, 20) = 4$ e como $4|1000$ então a equação tem solução de acordo com o resultado anterior.

Sendo assim, agora se faz necessário obter uma expressão do inteiro 4 como combinação linear de 172 e 20:

$$4 = 12 - 8 = 12 - (20 - 12) = 12 \cdot 2 - 20$$
$$= (172 - 20 \cdot 8) - 20 = 172 \cdot 2 - 20 \cdot 16 - 20$$
$$= 172 \cdot 2 - 20(16 + 1) = 172 \cdot 2 - 20 \cdot 17$$

Isto é:

$$4 = 172 \cdot 2 + 20 \cdot (-17).$$

Multiplicando ambos os membros da igualdade por 250, obtemos:

$$1000 = 172 \cdot 500 + 20(-4250)$$

Portanto, o par de inteiros $x_0 = 500$ e $y_0 = -4250$ é uma solução particular da equação proposta, e todas as outras soluções são dadas pelas fórmulas:

---

[3] Exemplo conforme Filho (1981)

$$x = 500 + (20/4)t = 500 + 5t, e$$

$y = -4250 - (172/4)t = -4250 - 43t$, onde t é um inteiro qualquer.

1.6. Congruências Lineares

Definição 5. Chama-se congruência linear toda equação da forma

$$ux \equiv v\ (mod\ m)$$

onde u e v são dois inteiros quaisquer e m um inteiro positivo.

Todo inteiro x_o tal que $ux_o \equiv v\ (mod\ m)$ diz-se que é uma solução da congruência linear.

É importante notar que, se x_o é uma solução da congruência $ux_o \equiv v\ (mod\ m)$, então todos os inteiros $x_o + km$ (1), onde k é um inteiro arbitrário, isto é, os inteiros:

$$\ldots, x_o - 2m, x_o - m, x_o + m, x_o + 2m, \ldots$$

também são soluções da congruência linear (1), pois, temos:

$$u(x_o + m) \equiv u.x_o \equiv v\ (mod\ m).$$

Exemplo:

$$3x \equiv 9\ (mod\ 12) \qquad (2)$$

Como $3.3 \equiv 9\ (mod\ 12)$, segue-se que $x_o = 3$ é uma solução desta congruência linear, e por conseguinte todos os inteiros $3 + 12k$, isto é, os inteiros:

$$\ldots, -33, -21, -9, 15, 27, 39, \ldots$$

Como se vê, obtida uma solução particular x_o de uma congruência linear $ux \equiv v(mod\ m)$ podemos imediatamente construir uma infinidade de outras soluções, todas mutuamente congruentes módulo m.

Duas soluções quaisquer da congruência, x_o e x_1 que são congruentes módulo m, isto é, tais que $x_o \equiv x_1\ (mod\ m)$, não são consideradas soluções distintas, isto é, o número de soluções da congruência linear é dado pelo número de soluções mutuamente incongruentes módulo m que a satisfazem.

Teorema 12. A congruência linear $ux \equiv v\ (mod\ m)$ tem solução, se e somente se, d divide $v\ (d \mid v)$, sendo $d = mdc\ (u, m)$.

Demonstração:

($\Longrightarrow$) Suponhamos que a congruência linear $ux \equiv v\ (mod\ m)$ tem como solução o inteiro x_o **,** isto é, que $ux_o \equiv v\ (mod\ m)$. Então, existe um inteiro y_o tal que

$$u \cdot x_o - v = m \cdot y_o \text{ ou } u \cdot x_o - m \cdot y_o = v$$

e como $d|\, u\ e\ d|\, m$, porque $d = mdc\,(u,m)$, segue-se que $d|\,(u \cdot x_o - m \cdot y_o)$ e, portanto, $d|\, v$.

($\Longleftarrow$) Reciprocamente, suponhamos que $d|\, v$, isto é, que $v = d \cdot k$, onde k é um inteiro.

Como o $mdc\,(u,m) = d$, existem inteiros $x_o e\, y_o$ tais que $ux_o + my_o = d$ ou multiplicando ambos os membros desta igualdade por k: $u\,(k \cdot x_o) + m\,(k \cdot y_o) = d \cdot k = v$ ou $u\,(k \cdot x_o) - v = m\,(-k \cdot y_o)$ o que implica: $u(k \cdot x_o) \equiv v\,(mod\, m)$

Portanto, o inteiro kx_oé uma solução da congruência linear $ux \equiv v\,(mod\, m)$.

Teorema 13. Se d divide v $(d \mid v)$, sendo $d = mdc\,(u,m)$, então a congruência linear $ux \equiv v\,(mod\, m)$ tem precisamente d soluções mutuamente incongruentes módulo m.

Corolário 5. Se o $mdc\,(u,m) = 1$, então a congruência linear $ux \equiv v\,(mod\, m)$ tem uma única solução módulo m.

Exemplo[4]: Resolver a congruência linear

$$18x \equiv 30\,(mod\ 42).$$

O $mdc\,(18{,}42) = 6$ e como $6|30$, a congruência dada tem exatamente 6 soluções *mutuamente incongruentes módulo* 42.

Como $18 \cdot 4 \equiv 30\,(mod\ 42)$, uma solução de congruência dada é $x_o = 4$, e por conseguinte as suas 6 soluções mutuamente incongruentes módulo 42 são dadas pela fórmula: $x = 4 + (42/6)t = 4 + 7\,t$, onde $t = 0{,}1{,}\ldots{,}5$, isto é, são os inteiros: $x = 4{,}11{,}18{,}25{,}32{,}39$.

Exemplo[5]: Resolver a congruência linear $36x \equiv 53\,(mod\ 131)$.

O $mdc\,(36{,}131) = 1$ e, portanto, a congruência dada tem uma única solução módulo 131.

Como $53 \equiv -78\,(mod\ 131)$, temos:

$$36x \equiv -78\,(mod\ 131)$$

$$6.6x \equiv 6(-13)\,(mod\ 131)$$

ou seja, por ser o $mdc\,(6{,}131) = 1$:

$$6x \equiv -13\,(mod\ 131)$$

Como $-13 \equiv -144\,(mod\ 131)$, temos:

---

[4] Exemplo de acordo com Filho (1981)

[5] Exemplo de acordo com Filho (1981)

$$6x \equiv -144\ (mod\ 131)$$

$$6x \equiv 6(-24)\ (mod\ 131)$$

ou seja, por ser o $mdc\ (6{,}131) = 1$:

$$x \equiv -24 \equiv 107\ (mod\ 131).$$

Teorema 14. Seja o $mdc\ (u, m) = 1$. Então u tem um único inverso módulo m.

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

$$ux \equiv 1(mod\ m)$$

Tem uma única solução $x_o\ (mod\ m)$, isto é:

$$ux_o \equiv 1\ (mod\ m)$$

De modo que o inteiro u tem um *único inverso módulo m:*

$$u^* = x_o.$$

Exemplo: Por ser $6 \cdot 6 = 36 \equiv 1(mod\ 5)$, com isso o inverso de 6 módulo 5 é o próprio 6.

CAPÍTULO 2

2. METODOLOGIA DA PESQUISA

Este trabalho tem como finalidade, enunciar, demonstrar e aplicar o Teorema do Resto Chinês, a fim de resolver questões tanto de ensino básico como da OBMEP e OBM, quanto a nível de mestrado como o PROFMAT.

2.1. Abordagem Metodológica

Quanto à abordagem adotada para a realizar a pesquisa é a quantitativa, a fim de explorar Teorema do Resto Chinês através da demonstração e como consequência do teorema as suas aplicações, assim contribuindo com a pesquisa cientifica em matemática pura.

E a fim de ter uma maior afinidade e familiaridade com o problema adotou-se como estratégia a pesquisa exploratória, pois segundo Gil (2002) pesquisas com essa estratégia objetivam proporcionar maior familiaridade com o problema, a fim de torná-lo mais explícito ou a constituir hipóteses. Com isso buscou-se o detalhamento das demonstrações necessárias para provar o Teorema do Resto Chinês e com isso as variações de aplicações do Teorema.

Com o objetivo de seguir o rigor matemático que é necessário, a pesquisa bibliográfica é a que mais se encaixa de acordo com Gil (2002).

Sendo assim a pesquisa baseou-se no procedimento técnico a pesquisa bibliográfica, que de acordo com Gil (2002):

> A pesquisa bibliográfica é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos. Embora em quase todos os estudos seja exigido algum tipo de trabalho dessa natureza, há pesquisas desenvolvidas exclusivamente a partir de fontes bibliográficas. (GIL, 2002, p. 44)

Sendo assim o levantamento bibliográfica como afirma Gil (2002) baseado em livros, artigos científicos, teses e dissertações, foi utilizado nas demonstrações e aplicações do Teorema. Os principais autores que fundamentam a pesquisa bibliográfica são. As contribuições feitas por estes autores são fundamentais para explorar o tema desta pesquisa, assim possibilitando manter a rigorosidade matemática necessária para trabalhar o Teorema do Resto Chines e suas aplicações.

2.2. Etapas da pesquisa

Descrever as etapas referentes ao desenvolvimento das seções da fundamentação teórica que deverão ser desenvolvidas, destacando quais as principais definições, teoremas e exemplos que deverão ser apresentados.

A primeira etapa se dará através de uma pesquisa bibliográfica, utilizando os autores Boyer (1996), Eves (2011), Ding (1996), Filho (1981), Rosen (2011) e Glória (2019) para embasar e direcionar o estudo e a escrita dos conceitos matemáticos a serem explorados durante a pesquisa.

Partindo da pesquisa bibliográfica que foi feita na primeira etapa, serão desenvolvidas as demonstrações do Teorema do Resto Chinês, e a partir daí aplicar o Teorema principal nas questões de olímpiadas e da pós-graduação.

CAPÍTULO 3

3. Teorema do Resto Chinês

Teorema (do Resto Chinês). Sejam $m_1, m_2, m_3, \ldots, m_r$ inteiros positivos, tais que $mdc\ (m_i, m_j) = 1\ se\ i \neq j$. Então, o sistema de congruências lineares:

$$x \equiv u_1 (mod\ m_1)$$
$$x \equiv u_2 (mod\ m_2)$$
$$\vdots$$
$$x \equiv u_r (mod\ m_r)$$

tem solução única módulo M $= m_1 m_2 m_3 \ldots m_r$.

Demonstração:

Para cada $k = 1,2,\ldots,r$, seja:

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

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

$$M_k x \equiv 1 (mod\ m_k)$$

tem uma única solução x_k, módulo m_k.

Posto isto, vamos demonstrar que o inteiro:

$$X = u_1 M_1 x_1 + u_2 M_2 x_2 + \ldots + u_r M_r x_r$$

satisfaz cada uma das congruências do sistema considerado, ou seja, que X é uma solução deste sistema.

Temos que, se $i \neq k$, então $m_k | M_i$, ou seja, $M_i \equiv 0\ (mod\ m_k)$, logo $u_i M_i x_i \equiv 0\ (mod\ m_k)$ e, portanto

$$\sum_{i=1}^{r} u_i M_i x_i \equiv u_k M_k x_k\ (mod\ m_k), isto\ é,$$

$$X \equiv u_k M_k x_k\ (mod\ m_k),$$

ou seja,

$$X \equiv u_k \ (mod\ m_k), 1 \leq k \leq r.$$

Para demonstrar a unicidade desta solução, suponhamos que X_1 seja uma outra solução qualquer do sistema de congruências considerado. Então:

$$X = u_k \equiv X_1 (mod\ m_k), k = 1,2,\ldots,r,$$

de modo que $m_k|(X - X_1)$ para cada valor de k, e como $mdc(m_i, m_j) = 1$, temos que $m_1 m_2 \ldots m_r|(X - X_1)$, isto é, $M|(X - X_1)$ e $X \equiv X_1 (mod\ M)$. Sendo assim, está provado o Teorema do Resto Chinês.

3.1. Aplicações do Teorema do Resto Chinês

APLICAÇÃO 1 (OBM 2009) Sejam m e n dois inteiros positivos primos entre si. O Teorema Chines dos Restos afirma que, dados inteiros i e j com $0 \leq i < m$ e $0 \leq j < n$, existe exatamente um inteiro a, com $0 \leq a < mn$, tal que o resto da divisão de a por m é igual a i e o resto da divisão de a por n é igual a j. Por exemplo, para $m = 3$ e $n = 7$, temos que 19 é o único número que deixa restos 1 e 5 quando dividido por 3 e 7, respectivamente. Assim, na tabela a seguir, cada número de 0 a 20 aparecera exatamente uma vez.

	0	1	2	3	4	5	6
0		A				B	
1				C			D
2		E			F		

Qual a soma dos números das casas com as letras A, B, C, D, E e F?

Solução:

Dado que $mdc\ (m,n) = 1$, onde $m = 3$ e $n = 7$, de acordo com os dados do problema, temos o seguinte sistema de congruência linear:

$$a \equiv i(mod\ 3)$$

$$a \equiv j(mod\ 7)$$

Onde i e j são resto da divisão de a por m e n respectivamente. Usando o Teorema do Resto Chinês, **para encontrar o valor de (A):**

$$a \equiv 0(mod\ 3)$$

$$a \equiv 1(mod\ 7)$$

Onde $M = 3 \cdot 7 = 21$ e $M_1 = \frac{3 \cdot 7}{3} = 7, M_2 = \frac{3 \cdot 7}{7} = 3$, obtendo um novo sistema de congruências:

$$7a \equiv 1(mod\ 3) => a \equiv 1(mod\ 3)$$

$$3a \equiv 1(mod\ 7) => a \equiv 5(mod\ 7)$$

Sendo assim, $X = a_1 M_1 x_1 + a_2 M_2 x_2 + \cdots + a_r M_r x_r$ é solução do problema:

$$X = 0 \cdot 7 \cdot 1 + 1 \cdot 3 \cdot 5 = 15$$

$$A = 15$$

Utilizando o Teorema do Resto Chinês, **para encontrar o valor de (B):**

$$a \equiv 0 \ (mod\ 3)$$

$$a \equiv 5 \ (mod\ 7)$$

Onde $M = 3 \cdot 7 = 21$ e $M_1 = \frac{3 \cdot 7}{3} = 7$, $M_2 = \frac{3 \cdot 7}{7} = 3$, obtendo um novo sistema de congruências:

$$7a \equiv 1(mod\ 3) => a \equiv 1(mod\ 3)$$

$$3a \equiv 1(mod\ 7) => a \equiv 5(mod\ 7)$$

Sendo assim, $X = a_1 M_1 x_1 + a_2 M_2 x_2 + \cdots + a_r M_r x_r$ é solução do problema:

$$X = 1 \cdot 7 \cdot 1 + 5 \cdot 3 \cdot 5 = 75 \equiv 12 \ (mod\ 21)$$

$$B = 12$$

Utilizando o Teorema do Resto Chinês, **para encontrar o valor de (C):**

$$a \equiv 1(mod\ 3)$$

$$a \equiv 3(mod\ 7)$$

Onde $M = 3 \cdot 7 = 21$ e $M_1 = \frac{3 \cdot 7}{3} = 7, M_2 = \frac{3 \cdot 7}{7} = 3$, obtendo um novo sistema de congruências:

$$7a \equiv 1(mod\ 3) \Longrightarrow a \equiv 1(mod\ 3)$$

$$3a \equiv 1(mod\ 7) \Longrightarrow a \equiv 5(mod\ 7)$$

Sendo assim, $X = a_1 M_1 x_1 + a_2 M_2 x_2 + \cdots + a_r M_r x_r$ é solução do problema:

$$X = 1 \cdot 7 \cdot 1 + 3 \cdot 3 \cdot 5 = 52 \equiv 10 \ (mod\ 21)$$

$$C = 10$$

Utilizando o Teorema do Resto Chinês, **para encontrar o valor de (D):**

$$a \equiv 1(mod\ 3)$$

$$a \equiv 6(mod\ 7)$$

Onde $M = 3 \cdot 7 = 21$ e $M_1 = \frac{3 \cdot 7}{3} = 7, M_2 = \frac{3 \cdot 7}{7} = 3$, obtendo um novo sistema de congruências:

$$7a \equiv 1(mod\ 3) \Longrightarrow a \equiv 1(mod\ 3)$$

$$3a \equiv 1(mod\ 7) \Longrightarrow a \equiv 5(mod\ 7)$$

Sendo assim, $X = a_1 M_1 x_1 + a_2 M_2 x_2 + \cdots + a_r M_r x_r$ é solução do problema:

$$X = 1 \cdot 7 \cdot 1 + 6 \cdot 3 \cdot 5 = 97 \equiv 13\ (mod\ 21)$$

$$D = 13.$$

Utilizando o Teorema do Resto Chinês, **para encontrar o valor de (E):**

$$a \equiv 2(mod\ 3)$$

$$a \equiv 1(mod\ 7)$$

Onde $M = 3 \cdot 7 = 21$ e $M_1 = \frac{3 \cdot 7}{3} = 7, M_2 = \frac{3 \cdot 7}{7} = 3$, obtendo um novo sistema de congruências:

$$7a \equiv 1(mod\ 3) \Longrightarrow a \equiv 1(mod\ 3)$$

$$3a \equiv 1(mod\ 7) \Longrightarrow a \equiv 5(mod\ 7).$$

Sendo assim, $X = a_1 M_1 x_1 + a_2 M_2 x_2 + \cdots + a_r M_r x_r$ é solução do problema:

$$X = 2 \cdot 7 \cdot 1 + 1 \cdot 3 \cdot 5 = 29 \equiv 8\ (mod\ 21)$$

$$E = 8.$$

Utilizando o Teorema do Resto Chinês, **para encontrar o valor de (F):**

$$a \equiv 2(mod\ 3)$$

$$a \equiv 4(mod\ 7)$$

Onde $M = 3 \cdot 7 = 21$ e $M_1 = \frac{3 \cdot 7}{3} = 7, M_2 = \frac{3 \cdot 7}{7} = 3$, obtendo um novo sistema de congruências:

$$7a \equiv 1(mod\ 3) \Longrightarrow a \equiv 1(mod\ 3)$$

$$3a \equiv 1(mod\ 7) \Longrightarrow a \equiv 5(mod\ 7)$$

Sendo assim, $X = a_1 M_1 x_1 + a_2 M_2 x_2 + \cdots + a_r M_r x_r$ é solução do problema:

$$X = 2 \cdot 7 \cdot 1 + 4 \cdot 3 \cdot 5 = 74 \equiv 11\ (mod\ 21)$$

$$F = 11$$

Com isso A+B+C+D+E+F= 15+12+10+13+8+11=69.

APLICAÇÃO 2 (OBMEP- 2016) - Juca possui menos do que 800 bolinhas de gude. Ele gosta de separar as bolinhas em grupinhos com a mesma quantidade de bolinhas. Ele percebeu que se formar grupinhos com 3 bolinhas cada, sobram exatamente 2 bolinhas. Se ele formar grupinhos de 4 bolinhas, sobram 3 bolinhas. Se ele formar grupinhos de 5 bolinhas, sobram 4 bolinhas. E, finalmente, se ele formar grupinhos com 7 bolinhas cada, sobram 6 bolinhas.

a) Juca possui quantas bolinhas de gude?

b) Se Juca formasse grupinhos com 20 bolinhas cada, quantas bolinhas sobrariam?

Solução:

De acordo com os dados do problema, temos o seguinte sistema de congruências lineares:

$$x \equiv 2(mod\ 3)$$
$$x \equiv 3(mod\ 4)$$
$$x \equiv 4(mod\ 5)$$
$$x \equiv 6(mod\ 7)$$

a) Como o $mdc\,(3,4) = mdc\,(5,7) = mdc\,(3,5) = mdc\,(3,7) = mdc\,(4,7) = 1$, podemos aplicar o Teorema do Resto Chinês para resolver o problema. Para encontrar o número de bolinhas que Juca possui, precisamos resolver o sistema de congruências, e como os m_i são primos dois a dois então o sistema possui solução e é única módulo $M = 3 \cdot 4 \cdot 5 \cdot 7 = 420$. Sejam, $M_1 = \frac{3\cdot4\cdot5\cdot7}{3} = 140$, $M_2 = \frac{3\cdot4\cdot5\cdot7}{4} = 105$, $M_3 = \frac{3\cdot4\cdot5\cdot7}{5} = 84$ *e* $M_4 = \frac{3\cdot4\cdot5\cdot7}{7} = 60$. e

Obtemos um novo sistema de congruências, equivalente ao primeiro:

$$140x \equiv 1(mod\ 3)$$
$$105x \equiv 1(mod\ 4)$$
$$84x \equiv 1(mod\ 5)$$
$$60x \equiv 1(mod\ 7).$$

Resolvendo as congruências:

I. $140x \equiv 1(mod\ 3) \Longrightarrow 2x \equiv 1\ (mod\ 3) \Longrightarrow x \equiv 2\ (mod\ 3)$

II. $105x \equiv 1(mod\ 4) \Longrightarrow x \equiv 1(mod\ 4)$

III. $84x \equiv 1(mod\ 5) \Longrightarrow 4x \equiv 1(mod\ 5) \Longrightarrow x \equiv 4(mod\ 5)$

IV. $60x \equiv 1(mod\ 7) \Longrightarrow 4x \equiv 2(mod\ 7) \Longrightarrow x \equiv 2(mod\ 7)$

A solução geral é dada por $X = u_1M_1x_1 + u_2M_2x_2 + u_3M_3x_3 + u_4M_4x_4$, sendo assim

$$X = 2 \cdot 140 \cdot 2 + 3 \cdot 105 \cdot 1 + 4 \cdot 84 \cdot 4 + 6 \cdot 60 \cdot 2 = 2939.$$

A solução geral é dada por: $x(t) = 2939 + 420t, t \in \mathbb{Z}$. Como o número de bolinhas é menor que 800, teremos a inequação $2939 + 420t < 800$, onde $t < -5$. Portanto, para $t = -6$, obtemos

$$x(t) = 2939 + 420 \cdot (-6) = 419$$

Logo, Juca possui 419 bolinhas de gude.

b) Se Juca formasse grupinhos com 20 bolinhas cada, quantas bolinhas sobrariam?

Solução:

Como Juca tem no total 419 bolinhas, $419 = 20 \cdot 20 + 19$, ou seja, formando grupos com 20 bolinhas de gude, sobrariam 19.

APLICAÇÃO 3: Um general chinês possuía 2000 soldados para uma batalha. Após o confronto ele precisou verificar suas baixas. Assim alinhou de 7 em 7 e sobraram 5. Quando alinhou de 9 em 9 sobraram 4. E quando alinhou de 10 em 10 sobrou apenas 1. Quantos soldados havia na formatura, sabendo que há mais de 1500 indivíduos na formatura?

Solução: Seja *h* a quantidade de soldados, onde $1500 < h < 2000$, temos o seguinte sistema de congruências:

$$h \equiv 5\ (mod\ 7)$$

$$h \equiv 4\ (mod\ 9)$$

$$h \equiv 1\ (mod\ 10).$$

Como $mdc\ (7,9) = \ mdc\ (9,10) = mdc\ (7,10) = 1$, então pelo Teorema do Resto Chinês tal sistema tem solução única módulo $\mathrm{M} = 7 \cdot 9 \cdot 10 = 630$. Sejam $\mathrm{M}_1 = 90$, $\mathrm{M}_2 = 70$, $\mathrm{M}_3 = 63$.

$$90h \equiv 1\ (mod\ 7) \Longrightarrow h \equiv 6\ (mod\ 7)$$

$$70h \equiv 1\ (mod\ 9) \Longrightarrow h \equiv 4\ (mod\ 9)$$

$$63h \equiv 1\ (mod\ 10) \Longrightarrow h \equiv 7\ (mod\ 10)$$

Então:

$$X = 5 \cdot 90 \cdot 6 + 4 \cdot 70 \cdot 4 + 1 \cdot 63 \cdot 7 = 4261 \equiv (mod\ 630)$$

Porém,

$$4261 \equiv 481(mod\ 630) \Longrightarrow h \equiv 481(mod\ 630)$$

Sendo assim, $h = 630q + 481;\ q \in \mathbb{Z}$.

Porém como $1500 < h < 2000$, então $q = 2$, obtendo assim $h = 630 \cdot 2 + 481 = 1741$. Então havia 1741 soldados.

APLICAÇÃO 4 (PROFMAT-MA14-2011) Dispomos de uma quantidade de x reais menor do que 3000. Se distribuirmos essa quantidade entre 11 pessoas, sobra um real, se distribuirmos entre 12 pessoas, sobram dois reais, e se distribuirmos entre 13 pessoas, sobram três reais. De quantos reais dispomos?

Solução: Seja x a quantidade em dinheiro que dispomos, tal que $x < 3000$, logo:

$$x \equiv 1(mod\ 11)$$
$$x \equiv 2(mod\ 12)$$
$$x \equiv 3(mod\ 13)$$

Como o $mdc\ (11,12) = mdc\ (12,13) = mdc\ (11,13) = 1$ então, pelo Teorema do Resto Chinês, tal sistema tem solução única módulo $M = 11 \cdot 12 \cdot 13 = 1.716$. Sejam $M_1 = 12 \cdot 13 = 156$, $M_2 = 11 \cdot 13 = 143$, $M_3 = 11 \cdot 12 = 132$, então temos um novo sistema de congruências

$$156x \equiv 1(mod\ 11)$$
$$132x \equiv 1(mod\ 13)$$
$$143x \equiv 1(mod\ 12).$$

Resolvendo as congruências

I. $156x \equiv 1(mod\ 11) \Longrightarrow 2x \equiv 1\ (mod\ 11) \Longrightarrow x \equiv 6\ (mod\ 11)$

II. $143x \equiv 1(mod\ 12) \Longrightarrow x \equiv 11\ (mod\ 12)$

III. $132x \equiv 1(mod\ 13) \Longrightarrow 2x \equiv 1\ (mod\ 13) \Longrightarrow x \equiv 7\ \ (mod\ 13)$

Com isso $X = 1 \cdot 156 \cdot 6 + 2 \cdot 143 \cdot 11 + 3 \cdot 132 \cdot 7 = 6854 \equiv 1.706\ (mod\ 1716)$, ou seja, $x \equiv 1706\ (mod\ 1716)$ sendo $x = 1706 + 1716q$. Como x < 3000, teremos somente a solução inteira quando $q = 0$, resultando em $x = 1706 + 1716 \cdot 0.\ Logo, x = 1706\ reais$.

APLICAÇÃO 5 (ENQ-2015.1) Considere o seguinte sistema de congruências

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

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

Solução:

a) Como $mdc\ (9,7) = mdc\ (9,5) = mdc\ (7,5) = 1$, então o sistema tem solução, pelo Teorema do Resto Chinês, e é única módulo $M = 9 \cdot 7 \cdot 5 = 315$. Com $M_1 = 35$, $M_2 = 45, M_3 = 63$. Assim têm-se as congruências lineares:

$$35x \equiv 1(mod\ 9) \Longrightarrow x \equiv 8\ (mod\ 9)$$
$$45x \equiv 1(mod\ 7) \Longrightarrow x \equiv 5\ (mod\ 7)$$
$$63x \equiv 1(mod\ 5) \Longrightarrow x \equiv 2\ (mod\ 5)$$

Portanto

$$X = 35 \cdot 8 \cdot 1 + 45 \cdot 5 \cdot 5 + 63 \cdot 2 \cdot 3 = 1783 + q \cdot 315$$

Como se pede na questão o menor número natural, então $1783 + q \cdot 315 > 0$ para $q \in \mathbb{Z}$.

$$1783 + q \cdot 315 > 0 \Leftrightarrow q > \frac{-1783}{315} \Leftrightarrow q \geq -5.$$

Com isso, a menor solução é 208.

APLICAÇÃO 6 (ENQ-2014.2) Em uma cesta contendo ovos, na contagem de dois em dois, de três em três, de quatro em quatro e de cinco em cinco, sobram 1,2,3 e 4 ovos, respectivamente. Qual é a menor quantidade de ovos que a cesta pode ter?

Solução:

$$x \equiv 1\ (mod\ 2)$$
$$x \equiv 2\ (mod\ 3)$$
$$x \equiv 3\ (mod\ 4)$$
$$x \equiv 4\ (mod\ 5)$$

Como o $mdc\ (3{,}4)\ =\ mdc\ (3{,}5)\ =\ mdc\ (4{,}5)\ =\ 1$, pelo TRC o sistema tem solução única módulo $M = 3 \cdot 4 \cdot 5 = 60$, $M_1 =\ 20, M_2 =\ 15, M_3 = 12$. Onde $y_1 = 2, y_2 = 3, y_3 =\ 3$ são soluções das congruências $20y_1 \equiv 1\ (mod\ 3), 15y_2 \equiv 1\ (mod\ 4)\ e\ 12y_3 \equiv 1\ (mod\ 5)$. Logo, a solução é dada por

$$X = M_1 y_1 c_1 + M_2 y_2 c_2 + M_3 y_3 c_3 =\ 20 \cdot 2 \cdot 2 + 15 \cdot 3 \cdot 3 + 12 \cdot 3 \cdot 4 = 359.$$

As soluções do sistema se dão por $x = 359 + 60t$, onde $t \in \mathbb{Z}$. Sendo assim a menor solução é 59, quando $t = -5$.

3.2. Versão estendida do Teorema do Resto Chinês.

Teorema. Sejam $m_1, m_2, \dots, m_r$ inteiros positivos primos entre si, dois a dois, isto é, o $mdc\,(m_i, m_j) = 1$, para todo $i \neq j$, e sejam $u_1, u_2, \dots, u_r$ inteiros tais que o $mdc\,(u_k, m_k) = 1$ para $k = 1,2, \dots, r$.

Então, o sistema de congruências lineares:

$$u_1 x \equiv v_1 (mod\ m_1)$$
$$u_2 x \equiv v_2 (mod\ m_2)$$
$$\dots\dots\dots\dots\dots\dots$$
$$u_r x \equiv v_r (mod\ m_r)$$

tem solução única módulo M = $m_1 m_2 \dots m_r$.

Demonstração:

Como $mdc\,(u_k, m_k) = 1$, então a congruência linear

$$u_k x \equiv 1 (mod\ m_k)$$

tem solução única módulo m_k, digamos, $u^*{}_k$, de modo que

$$u_k u^*{}_k \equiv 1 (mod\ m_k)$$

Portanto, a congruência $u_k x \equiv v_k (mod\ m_k)$ é equivalente à congruência:

$$x \equiv v_k u^*{}_k\ (mod\ m_k).$$

Como consequência, o sistema dado é equivalente ao sistema de congruências lineares:

$$x \equiv v_1 u^*{}_1 (mod\ m_1)$$
$$x \equiv v_2 u^*{}_2 (mod\ \ m_2)$$
$$\dots\dots\dots\dots\dots\dots$$
$$x \equiv v_r u^*{}_r (mod\ m_r).$$

Como foi apresentado no resultado anterior, pelo "Teorema do Resto Chinês", terá uma única solução módulo $M = m_1 m_2 \dots m_r$.

Exemplo[6]: Resolver o sistema de congruências lineares:

[6] Exemplo retirado do livro de Filho (1981).

$$2y \equiv 1(mod\ 5)$$

$$3y \equiv 2(mod\ 7)$$

$$4y \equiv 3(mod\ 11)$$

Solução:

Como $mdc\ (5,7) = mdc\ (5,11) = mdc\ (7,11) = 1$, então pelo teorema do resto chinês, tem solução única módulo $M = 5 \cdot 7 \cdot 11 = 385$.

As congruências lineares:

$$2y \equiv 1(mod\ 5), 3y \equiv 1(mod\ 7), 4y \equiv 1(mod\ 11)$$

tem as seguintes soluções: ${u_1}^* = 3, {u_2}^* = 5,\ {u_3}^* = 3$, sendo assim o sistema é equivalente a:

$$y \equiv 3(mod\ 5)$$

$$y \equiv 10(mod\ 7)$$

$$y \equiv 9(mod\ 11)$$

para o qual $X \equiv 108\ (mod\ 385)$ é a *única solução.*

CONSIDERAÇÕES FINAIS

Com esta pesquisa, fica evidente a importância do Teorema do Resto Chinês para a resolução de sistemas de congruências lineares, para Teoria dos Números e para a Matemática, visto sua ampla gama de aplicações.

Vale salientar, que para resolvermos sistemas de congruências lineares, utilizando o Teorema do Resto Chinês, faz-se necessário atentar-se a algumas importantes condições: sendo $m_1, m_2, \dots m_r$ primos dois a dois, o sistema de congruências lineares vai possuir uma e somente uma solução módulo $M = m_1 m_2 \dots m_r$. Ademais, as soluções são dadas por $X = u_1 M_1 x_1 + u_2 M_2 x_2 + \dots + u_r M_r x_r$, sendo $M_k = m/m_k$ e x_k é solução de $M_k x_k \equiv 1 \ (mod\ m_k), \forall\ k = 1, \dots, r$.

No cotidiano, problemas como o citado na aplicação 6 e muitos outros encontram solução através do TRC, resolvendo a deficiência de conceitos matemáticos capazes de encontrar soluções eficientes, utilizadas desde o ensino médio, em provas de olímpiadas estudantis até as provas de pós-graduação, como as do ENQ-PROFMAT.

Com isso, os objetivos foram alcançados e este trabalho poderá contribuir com pesquisas e estudos futuros, visto que esse trabalho é apenas um recorte do que muito pode vir a ser explorado trazendo luz ao tema.

REFERÊNCIAS

BOYER, C. B. **História da matemática**. 2. Ed. São Paulo: Blucher, 1996.

SANTOS, J. P. **Introdução à Teoria dos Números**. 3. Ed. Rio de Janeiro: IMPA, 2020.

FILHO, E. A. **Teoria elementar dos números**. São Paulo: Nobel, 1981.

EVES, H. **Introdução à história da matemática**. 5. Ed. São Paulo: Editora Unicamp, 2011.

ROSEN, K. H. **Elementary Number Theory and its Applications**. 6 Ed. Boston: person, 2011.

PEI, D. SALOMAA, A. DING, C. **Chinese Remainder Theorem, Applications in Computing, Coding, Cryptography**. World Scientific Publishing Company,1996.

GUERRA, E. L de A. **Manual de pesquisa qualitativa**. Belo Horizonte: Grupo Anima Educação, 2014.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. Ed. São Paulo: Atlas S.A, 2002.

GLÓRIA, W. S. **Teorema Chinês dos Restos: Ensino e aplicações**. 2019. Dissertação. Mestrado Profissional em Matemática em Rede Nacional - Universidade Federal do Amazonas.