Universidade Federal do Oeste da Bahia - UFOB
Campus Reitor Edgard Santos
Centro das Ciências Exatas e das Tecnologias
Mestrado Profissional em Matemática

TEOREMA CHINÊS DOS RESTOS: UMA PROPOSTA DE ABORDAGEM TEÓRICA COM IMPLEMENTAÇÃO COMPUTACIONAL

Diandra Chisa Tanaka

BARREIRAS
2021

Diandra Chisa Tanaka

TEOREMA CHINÊS DOS RESTOS: UMA PROPOSTA DE ABORDAGEM TEÓRICA COM IMPLEMENTAÇÃO COMPUTACIONAL

Dissertação apresentada ao Programa de Pós-Graduação em Nível de Mestrado Profissional em Matemática - PROFMAT da Universidade Federal do Oeste da Bahia, como requisito parcial à obtenção do título de mestre.
Orientador: Prof. Dr. Edvaldo Elias de Almeida Batista

BARREIRAS
2021

FICHA CATALOGRÁFICA

T161 Tanaka, Diandra Chisa

Teorema Chinês dos Restos: uma proposta de abordagem teórica com implementação computacional. / Diandra Chisa Tanaka. – 2021.

55f.: il

Orientador: Prof. Dr. Edvaldo Elias de Almeida Batista

Dissertação – PROFMAT – Mestrado Profissional em Matemática em Rede Nacional, Universidade Federal do Oeste da Bahia. Centro das Ciências Exatas e das Tecnologias - Barreiras, BA, 2021.

1. Matemática – Estudo e Ensino. 2. Programação de Computadores. I. Batista, Edvaldo Elias de Almeida. II. Universidade Federal do Oeste da Bahia – Centro das Ciências Exatas e das Tecnologias. III. Título.

CDD 510.7

Biblioteca Universitária de Barreiras – UFOB

Diandra Chisa Tanaka

TEOREMA CHINÊS DOS RESTOS: UMA PROPOSTA DE ABORDAGEM TEÓRICA COM IMPLEMENTAÇÃO COMPUTACIONAL

Dissertação apresentada ao Programa de Pós-Graduação em Nível de Mestrado Profissional em Matemática - PROFMAT da Universidade Federal do Oeste da Bahia, como requisito parcial à obtenção do título de mestre.

Aprovada em 18 de outubro de 2021.

Banca Examinadora

Orientador: Dr. Edvaldo Elias de Almeida Batista
Universidade Federal do Oeste da Bahia

Prof. Dr. Bruno Trindade Reis
Universidade Federal do Oeste da Bahia

Prof. Dr. Tibério Bittencourt de Oliveira Martins
Universidade Federal de Mato Grosso

Agradecimentos

A Deus, que é meu consolo e fortaleza.

Aos meus pais. Ao Yukio, meu pai, exemplo de honestidade, simplicidade e pleno amor à família. À Yolanda Magali, minha mãe e eterna amiga, modelo materno de amor e perdão incondicional. Amo-os profundamente.

Aos meus irmãos, Samuel e Rodrigo, motivos de orgulho para meus pais e para mim. Não poderia ter pessoas melhores para me inspirar. Obrigada pelos momentos de descontração e pelo apoio sempre que precisei.

Ao meu esposo, Felipe, que me desperta o desejo de ser cada vez melhor, agradeço por todo o amor e cuidado devotados. Agradeço também à sua família pela consideração e momentos partilhados.

Aos colaboradores da UFOB: Docentes, técnicos em administração e terceirizados.

Agradeço, especialmente, ao meu Orientador Prof. Edvaldo, sem o qual esse trabalho jamais seria possível. Estou certa de que não poderia ter recebido mais zelosa orientação. Obrigada pelo tempo empenhado, paciência e conhecimento compartilhado.

Meu agradecimento vai, em particular, para outros professores: Profa. Marília, mulher admirável, que de modo tão generoso me incentivou em muitos momentos, Prof. Juarez e Prof. Elier por, desde a graduação, me encorajarem diante de desafios no mundo acadêmico.

A todos os meus colegas do curso de mestrado, a minha gratidão.

Resumo

O Teorema Chinês dos Restos foi uma ferramenta utilizada, historicamente, para resolver um problema sobre contagem de soldados. Trata-se, basicamente, de uma relação de equivalência entre restos. Nos dias de hoje, além de fazer parte do estudo da Aritmética, é utilizado na criptografia e partilha de senhas, por exemplo. Considerando o atual contexto, no qual cada vez mais tecnologias são utilizadas no processo de ensino, o propósito deste trabalho é tornar a didática sobre o Teorema Chinês dos Restos mais lúdica. Para isso, elabora-se um algoritmo que elenca o passo a passo para solucionar problemas de sistemas de congruências lineares e, em seguida, implementa-se um programa capaz de executar esse roteiro e gerar um arquivo com o registro dos cálculos. Para compor o referencial teórico, abordam-se os conceitos de divisibilidade, números primos e congruências, apresentando as definições relacionadas e resolução de exemplos. Em seguida, apresentamos o Teorema Chinês dos Restos, o algoritmo proposto e demonstramos a sua eficácia por meio da resolução de problemas com a implementação computacional.

Palavras-chave: Teorema Chinês dos Restos, Congruências, Programação.

Abstract

The Chinese Remainder Theorem was a tool used, historically, to solve a problem about counting soldiers. It is basically an equivalence relationship between remainders. Nowadays, in addition to being part of the study of Arithmetic, it is used in encryption and password sharing, for example. Considering the current context, in which more and more technologies are used in the teaching process, the purpose of this work is to make the didactic about the Chinese Theorem of Remains more playful. For this, an algorithm is developed that lists the step by step to to solve problems of linear congruence systems and, then, a program capable of executing this script and generating a file with the registration of the calculations is implemented. To compose the theoretical framework, the concepts of divisibility, prime numbers and congruence are addressed, presenting the related definitions and solving examples. Then, we present the Chinese Remainder Theorem, the proposed algorithm, and demonstrate its effectiveness by solving problems with the computational implementation.

Key-words: Chinese Remainder Theorem, Congruences, Programming.

Lista de ilustrações

Sumário

1 Introdução

A congruência é uma relação de equivalência de restos e, por sua vez, um sistema de congruências é composto por n congruências. O Teorema Chinês dos Restos propõe uma importante metodologia para resolução desses sistemas.

A depender da quantidade de congruências que compõe o sistema ou do seu nível de dificuldade, a resolução do problema pode se tornar pouco atrativa e, muitas vezes, cansativa para o aluno. Nesse sentido, o trabalho do professor em manter o interesse do discente nesse conteúdo pode ser um desafio.

É fato que a abordagem digital nessa era sempre desperta mais interesse do estudante. Diante dessa ótica, o presente trabalho objetiva tornar o ensino sobre o Teorema Chinês dos Restos mais didático, aplicando o assunto por meio de um programa que coleta os dados do problema e proporciona ao usuário acompanhar todas as etapas da solução. Também é apresentado um algoritmo que roteiriza um passo a passo para resolução desse tipo de exercício, o que é uma valiosa ferramenta de fixação, podendo, oportunamente, ser implementada em outras linguagens de programação.

São escassos os trabalhos que versam sobre o Teorema Chinês dos Restos, sendo que eles, na sua maioria, discutem somente o ensino desse conteúdo em escolas ou sua aplicabilidade. Souto Filho (2015) [11] escreveu sobre o histórico do teorema e apresentou-o, com a resolução de muitos exercícios. Nascimento (2014) [8] propôs um minicurso com ênfase na resolução de problemas e aplicou-o para alunos do ensino médio, concluindo que, apesar da dificuldade com algumas nomenclaturas e simbologia, observou-se que o assunto motivou a aprendizagem, sendo útil na solução de vários exercícios. Glória (2019) [5] apresentou o Teorema Chinês dos Restos, além de diversos exemplos e sugere que seu trabalho possa servir de base para alunos e professores que buscam atividades relacionadas com o tema. Com o mesmo intuito, Santos (2017) [10] aborda assuntos importantes na revisão bibliográfica que embasam o teorema e resolve muitos exemplos. Bomfim (2021) [2] ministrou para um grupo de alunos diversos assuntos, incluindo o Teorema Chinês dos Restos, e constatou que houve adesão por mais da metade dos estudantes, que utilizaram a ferramenta na resolução dos testes aplicados.

Como aplicações já abarcadas em trabalhos, podemos citar a criptografia que é uma espécie de codificação de mensagens [1], além da partilha de senhas [9] que é uma maneira de distribuir uma chave entre várias pessoas, de modo que nenhuma delas tenha posse da senha inteira, mas que não sejam necessárias todas as chaves para reconstruir a senha.

Entretanto, além de tratar do referencial teórico indispensável para o tema, esta dissertação tem como diferencial a pretensão de apresentar um novo recurso para o docente, com enfoque sob um ponto de vista mais lúdico e atraente para os alunos. Dessa forma, podem ser desenvolvidos e explorados novos conhecimentos para o professor e, posteriormente, para o estudante, gerando dinamismo nas aulas, fator tão primordial no aprendizado.

O trabalho está estruturado da seguinte maneira: no capítulo 2, apresentamos um relevante histórico acerca do Teorema Chinês dos Restos, mencionando aquele que se acredita ser o primeiro problema da história envolvendo sistemas de congruências e como, naquele momento, foi solucionado.

No capítulo 3, tratamos sobre a divisão de números inteiros, sendo evidenciados os conceitos de divisibilidade, algoritmos de um modo geral, algoritmo de Euclides, equações diofantinas lineares, máximo divisor comum e mínimo múltiplo comum.

No capítulo 4, abordamos o conceito de números primos e o Teorema Fundamental da Aritmética e no capítulo 5 estudamos as congruências lineares e seus sistemas.

No sexto capítulo, é enunciado e demonstrado o Teorema Chinês dos Restos e, em seguida, propõe-se um algoritmo computacional e um fluxograma para ele.

O capítulo 7 exemplifica com exercícios o funcionamento do programa proposto, além de expor o arquivo gerado por ele com o valor das variáveis calculadas e o resultado final. No último capítulo, são discutidas as conclusões.

2 Histórico: Teorema Chinês dos Restos

Segundo Matkovic (1988), o registro mais antigo sobre o problema dos restos é do matemático chinês Sun-Tsu, no século IV. O referido autor escreveu a obra: "Sun-Tsu Suan-Ching", que significa: Aritmética Clássica de Sun-Tsu, composta por três volumes. No terceiro volume, problema 26, ele relatou:
"Nós temos um número desconhecido de objetos, se nós os contarmos de três em três, deixa resto dois; se nós os contarmos de cinco em cinco, deixa resto três; se nós os contarmos de sete em sete, o resto é dois. Quantos são os objetos?"
Em seguida, o matemático fornece a resposta: 23, e descreve o método utilizado no cálculo:

Para cada unidade que sobra quando se conta de três em três, considere 70.
Logo, se você conta a cada três e tem resto dois, tome 140.
Para cada unidade que sobra quando se conta de cinco em cinco, considere 21.
Logo, se você conta a cada cinco e tem resto três, tome 63.
Para cada unidade que sobra quando se conta de sete em sete, considere 15.
Logo, se você conta a cada sete e tem resto dois, tome 30.
Se a soma for 106 ou mais, subtraia múltiplos de 105 (resultado da multiplicação entre 3, 5, 7) e você terá o resultado.
No exemplo, tem-se 140+63+30 = 233.
Daí, subtraia 2x105 = 210 e você tem o resultado. [3]

Utilizando os símbolos da Álgebra Moderna, o problema em estudo pode ser representado da seguinte forma:

$$N \equiv 2 \mod 3$$

$$N \equiv 3 \mod 5$$

$$N \equiv 2 \mod 7$$

Resolução:

$$70 \equiv 1 \mod 3 \Rightarrow 140 \equiv 2 \mod 3$$

$$21 \equiv 1 \mod 5 \Rightarrow 63 \equiv 3 \mod 5$$

$$15 \equiv 1 \mod 7 \Rightarrow 30 \equiv 2 \mod 7$$

$$\mathrm{N} = 140 + 63 + 30 - \mathrm{n}.105 = 23$$

Embora o cálculo acima tenha se apresentado de forma mais direta, no decorrer dos próximos capítulos, serão abordados conteúdos importantes para a resolução de problemas desse tipo e resolvidos mais exemplos de modo detalhado.

O fato é que através desse problema, a intenção por trás do Teorema Chinês dos Restos estava estabelecida. Vale lembrar que existem infinitas soluções, de acordo com o valor assumido por n, mas, no caso, Sun-Tsu estava procurando pela menor solução positiva, assim, n assume o valor 23. Em seu livro, não há a generalização do Teorema, tampouco sua prova. [7]

No decorrer do tempo, os chineses deram vários nomes para o Teorema Chinês dos Restos ou Teorema dos Restos Chinês. Os diferentes nomes vinham dos métodos computacionais ou das diferentes aplicações dadas ao teorema por cada autor. [7]

3 Divisibilidade

Compreender a definição e propriedades da divisibilidade é um passo primordial, pois é um conceito básico que será constantemente utilizado no decorrer deste trabalho. Neste capítulo serão abordados a Divisão Euclidiana, o Máximo Divisor Comum e suas propriedades, o Algoritmo de Euclides, Equações Diofantinas Lineares e o Mínimo Múltiplo Comum.

Definição 3.1. *Considerando dois números inteiros* a *e* b, a *divide* b *(representa-se:* $a|b$*), quando existe* $c \in \mathbb{Z}$*, tal que,* $b = ca$*. No caso, pode-se dizer também que* a *é divisor ou um fator de* b *ou que* b *é um múltiplo de* a *ou que* b *é divisível por* a.

A notação $a|b$ não representa uma operação em $\mathbb{Z}$. Trata-se de uma sentença que afirma ser verdade que existe c inteiro tal que $b = ca$. A negação dessa sentença é representada por $a \nmid b$ isto é, não existe nenhum inteiro c tal que $b = ca$.

Exemplo 1. *Pela Definição 3.1, ficam claros os exemplos a seguir:*

- $1|0$ *, pois* $0 = 0 \cdot 1$.
- $2|8$ *, pois* $8 = 4 \cdot 2$.
- $3 \nmid 5$ *, pois nenhum número inteiro multiplicado por 3 resulta em 5.*

Abaixo são apresentadas algumas propriedades importantes da divisibilidade:

Proposição 3.1. *Sejam* $a, b, c, d, x, y \in \mathbb{Z}$*, tem-se:*

(i) $1|a, \quad a|a$ *e* $a|0$.

(ii) se $a|b$ *e* $b|c$*, então,* $a|c$.

(iii) $a|b$ *e* $c|d \Rightarrow ac|bd$.

(iv) se $a|b$ *e* $a|c$*, então* $a|(xb + yc), \quad \forall x, y \in \mathbb{Z}$.

(v) Considerando $b \neq 0$*, então,* $a|b \Rightarrow |a| \leqslant |b|$.

Demonstração. Serão demonstradas, respectivamente, cada uma das propriedades. Vale lembrar que todas as incógnitas pertencem ao conjunto dos números inteiros:

(i) $1|a, \quad a|a$ e $a|0$, pois, por definição, se $a|b$, então $b = ca$. Assim: $a = a \cdot 1, \quad a = 1 \cdot a, \quad 0 = 0 \cdot a$.

(ii) $a|b \Rightarrow \exists f \in \mathbb{Z}$ tal que $b = fa$ e $b|c \Rightarrow \exists g \in \mathbb{Z}$ tal que $c = gb$. Substituindo o valor de b obtido da primeira equação nessa última, tem-se:
$c = g(fa) \Rightarrow c = (gf)a$
O que significa que $a|c$.

(iii) $a|b \Rightarrow \exists f \in \mathbb{Z}$ tal que $b = fa$ e $c|d \Rightarrow \exists g \in \mathbb{Z}$ tal que $d = gc$. Multiplicando entre si os membros das equações, tem-se: $bd = (fa)(gc) = (fg)(ac)$.
Portanto, $ac|bd$.

(iv) Se $a|b$ e $a|c$, tem-se que $\exists f, g \in \mathbb{Z}$ tal que $b = fa$ e $c = ga$, respectivamente. Daí,
$xb + yc = x(fa) + y(ga) = a(xf) + a(yg) = a(xf + yg)$.
Portanto, como $xb + yc = a(xf + yg)$, então $a|(xb + yc)$.

(v) Se $a|b \Rightarrow \exists c \in \mathbb{Z}$ tal que $b = ca$. Em módulo, $|b| = |c||a|$. Como $|b| \neq 0$, tem-se que $|c| \neq 0$. Consequentemente, $1 \leqslant |c|$ e, portanto, $|a| \leqslant |a||c| = |b|$.

□

Pelas proposições supracitadas, tornam-se imediatas resoluções como as apresentadas a seguir:

Exemplo 2. *Se* $9|27$ *e* $27|162$, *então* $9|162$.

Exemplo 3. *Se* $3|9$ *e* $6|12$, *então* $(3 \cdot 6)|(9 \cdot 12) \Rightarrow 18|108$.

Como consequência de algumas dessas proposições, destaca-se que a relação de divisibilidade em $\mathbb{N} \cup \{0\}$ é uma relação de ordem, pois é:

(i) reflexiva: $\forall a \in \mathbb{N}, \quad a|a$. Proposição 3.1 (i)

(ii) transitiva: se $a|b$ e $b|c$, logo, $a|c$. Proposição 3.1 (ii)

(iii) antissimétrica: se $a|b$ e $b|a$, logo, $a = b$. Proposição 3.1 (v)

3.1 Divisão Euclidiana

Preliminarmente, é interessante enunciar o Princípio da Indução e o Princípio da Boa Ordenação, pois este será utlizado na demonstração da Divisão Euclidiana.

O Princípio da Indução Matemática é um valioso instrumento para provar teoremas. Nesta seção, ele será utilizado na demonstração do Princípio da Boa Ordenação.

Axioma 1 (Axioma de Indução)**.** *Seja S um subconjunto de $\mathbb{N}$ tal que*

(i) $0 \in S$

(ii) S *é fechado com respeito à operação de "somar 1"a seus elementos, ou seja,*

$$\forall n, \quad n \in S \Rightarrow n+1 \in S$$

Então $S = \mathbb{N}$.

Desse Axioma, segue o Princípio de Indução Matemática:

Teorema 3.1 (Princípio da Indução Matemática)**.** *Seja $a \in \mathbb{N}$ e seja $p(n)$ uma sentença aberta em n. Suponha que:*

(i) $p(a)$ *é verdade, e que*

(ii) $\forall n \geqslant a, p(n)$ *é verdade* $\Rightarrow p(n+1)$ *é verdade,*

então $p(n)$ *é verdade para todo* $n \geqslant a$.

Demonstração. Seja $v = \{n \in \mathbb{N}; p(n) \ \ verdade\}$; ou seja, v é o subconjunto de $\mathbb{N}$ para os quais $p(n)$ é verdade.
Considere o conjunto

$$S = \{m \in \mathbb{N}; a + m \in v\},$$

que verifica trivialmente $a + S \subset v$.
Como, pela condição (i), tem-se que $a + 0 = a \in v$, segue-se que $0 \in S$.
Por outro lado, se $m \in S$, então $a + m \in v$ e, por (ii), tem-se que $a + m + 1 \in v$; logo $m + 1 \in S$. Assim, pelo Axioma 1, $S = \mathbb{N}$. Portanto,

$$\{m \in \mathbb{N}; m \geqslant a\} = a + \mathbb{N} \subset v,$$

o que prova o resultado.

□

Teorema 3.2 (Princípio da Boa Ordenação)**.** *Todo subconjunto não vazio $S \subset \mathbb{N}$, possui um menor elemento, isto é, existe $a \in S$ tal que $a \leqslant x, \forall x \in S$.*

Demonstração. A demonstração será feita por absurdo, utilizando o Princípio da Indução Matemática (teorema 3.1). Seja S um subconjunto não vazio de $\mathbb{N}$ e suponha, por absurdo, que S não possui um menor elemento. Portanto, o que se quer mostrar é que S é vazio, o que seria uma contradição.
Considere o conjunto T complementar de S em $\mathbb{N}$. Deve-se mostrar que $T = \mathbb{N}$. Dado o conjunto:

$$I_n = \{k \in \mathbb{N}; k \leqslant n\},$$

considerando a sentença aberta:

$$p(n) : I_n \subset T.$$

Como $0 \leqslant n, \quad \forall n$, segue que $0 \in T$, pois, caso contrário, 0 seria um menor elemento de S. Portanto, $p(0)$ é verdade.
Supondo agora que $p(n)$ seja verdade. Se $n + 1 \in S$, como nenhum elemento de I_n está em S, $n + 1$ seria um menor elemento de S, o que não é permitido. Assim, $n + 1 \in T$, daí

$$I_{n+1} = I_n \cup \{n + 1\} \subset T,$$

o que prova que $\forall n, I_n \subset T$; portanto $\mathbb{N} \subset T \subset \mathbb{N}$, consequentemente, $T = \mathbb{N}$.

□

A Divisão Euclidiana consiste na divisão de um número por outro, obtendo um quociente q como resultado e um resto r.

Teorema 3.3 (Divisão Euclidiana)**.** *Dados dois inteiros* a *e* $b, b \neq 0$, *existe um único par de inteiros* q *e* r *tais que:*

$$a = qb + r, \quad com \quad 0 \leqslant r < |b|$$

Se $b|a, r = 0$.

Demonstração. Se $a < b$, tome $q = 0$ e $r = a$. Se $a = b$, tome $q = 1$ e $r = 0$.

Suponha que $a > b$ e considere os números:

$$a, a - b, a - 2b, ..., a - nb, ...$$

Pelo Princípio da Boa Ordenação (teorema 3.2), o conjunto S, formado pelos elementos acima, tem um menor elemento $r = a - qb$. Deve-se provar que r tem a propriedade requerida, isto é, que $r < b$.

Se $b|a$, então $r = 0$ e nada tem de ser provado.

Por outro lado, se $b \nmid a$, então $r \neq b$ e, portanto, basta mostrar que não pode ocorrer $r > b$. De fato, se isso ocorresse, existiria um natural $c < r$ tal que $r = c + b$. Consequentemente, $r = c + b = a - qb$, daí:

$c = a - qb - b \Rightarrow c = a - (q+1)b \in S$, com $c < r$, o que é uma contradição com o fato de r ser o menor elemento de S. Portanto, $a = bq + r$ com $r < b$, o que prova a existência de q e r.

Para provar a unicidade, note que, dados dois elementos distintos de S, a diferença entre o maior e o menor desses elementos, sendo um múltiplo de b é, pelo menos, b. Logo, se $r = a - bq$ e $r' = a - bq'$, com $r < r' < b$, teria que $r' - r \geqslant b$, o que acarretaria $r' \geqslant r + b \geqslant b$, que é um absurdo. Portanto $r = r'$.

Daí segue que $a - bq = a - bq'$, o que implica que $bq = bq'$, portanto, $q = q'$. □

A Divisão Euclidiana pode ser aplicada em diversas situações, como as representadas a seguir:

Exemplo 4. *Na divisão do número 16 por 3, qual é o quociente e qual o resto?*
Pelo Divisão Euclidiana, tem-se que:

$$16 = q \cdot 3 + r$$

Uma maneira de resolver esse problema é por tentativa e erro. Isto é, atribuindo, mentalmente, números para q *até encontrar o maior deles tal que* $0 \leqslant r < 3$. *Assim:*
Para $q = 5, r = 16 - 5 \cdot 3 = 1$
Para $q = 6, r = 16 - 6 \cdot 3 = -2$
Mas $0 \leqslant r < 3$, *portanto,* $q = 5, r = 1$.

Exemplo 5. *Qual o resto da divisão de 297 por 4?*
Pelo Divisão Euclidiana, obtem-se:

$$297 = q \cdot 4 + r$$

De forma semelhante ao que foi feito no exemplo anterior, procura-se o maior q *tal que* $0 \leqslant r < 4$.
Para $q = 74, r = 297 - 74 \cdot 4 = 1$
Para $q = 75, r = 297 - 75 \cdot 4 = -3$
Como o resto não pode ser negativo, $q = 74$.

3.2 O Máximo Divisor Comum

Dados dois inteiros a e b, distintos ou não, um número inteiro d será um divisor comum de a e b se $d|a$ e $d|b$.

Exemplo 6. *Tomando os números 8 e 24, tem-se que* ± 1 , ± 2 , ± 4 *e* ± 8 *são divisores comuns.*

Definição 3.2. *Na obra Os Elementos de Euclides, o autor, essencialmente, define que o inteiro* $d \geqslant 0$ *é o máximo divisor comum (mdc) de* a *e* b *se atender às propriedades:*

(i) d *é um divisor comum de* a *e* b, *e*

(ii) d *é divisível por todo divisor comum de* a *e* b

Notação: $d = mdc(a, b)$ *ou, simplesmente,* $d = (a, b)$.

Exemplo 7. *Para encontrar o mdc de 8 e 24, pode-se pensar da seguinte forma:*
Sabe-se que ± 1 , ± 2 , ± 4 *e* ± 8 *são divisores comuns, isto é, atendem à primeira propriedade. Contudo, entre esses, somente o número 8 é positivo e divisível por todo divisor comum de 8 e 24 (segunda propriedade), pois* ± 1 , ± 2 , ± 4 *dividem 8. Portanto, o mdc de 8 e 24 é 8, em notação:* $(8, 24) = 8$.

De forma simplificada, o máximo divisor comum de dois ou mais números inteiros é o maior divisor inteiro comum a todos eles.

Exemplo 8. *Observe o raciocínio para determinar o mdc de 20 e 30:*
Sabe-se que ± 1 , ± 2 , ± 4 , ± 5 , ± 10 *e* ± 20 *são divisores de 20 e* ± 1 , ± 2 , ± 3 , ± 5 , ± 6 , ± 10 , ± 15 *e* ± 30 *são dividores de 30. Logo, o maior divisor comum de 20 e 30 é 10. A mesma resposta pode ser obtida por meio da fatoração em números primos, na qual se escolhe(m) o(s) fator(es) comum(ns) de menor expoente:*
$20 = 2 \cdot 2 \cdot 5 = 2^2 \cdot 5$
$30 = 2 \cdot 3 \cdot 5$
$(20, 30) = 2 \cdot 5 = 10$

É importante ressaltar que o mdc de dois ou mais números é único.

Para demonstrar a existência do mdc de qualquer par de números inteiros não nulos, Euclides utilizou o seguinte resultado:

Lema 3.1. *Sejam* $a, b, n \in \mathbb{Z}$. *Se existe* $(a, b-na)$, *então* (a, b) *existe e* $(a, b) = (a, b-na)$.

Demonstração. Seja $d = (a, b-na)$. Como $d|a$ e $d|(b-na)$, então, d divide $b = b-na+na$ (Proposição 3.1 (iv)). Isto é, d é um divisor comum de a e b. Supondo que c seja divisor comum de a e b, então, c é um divisor comum de a e $b-na$ (Proposição 3.1 (iv)) e, portanto, $c|d$. Isso prova que $d = (a, b)$.

□

O Lema 3.1 é fundamental para estabelecer o Algoritmo de Euclides, que será estudado na Seção 3.4.

3.3 Algoritmos

Um algoritmo é qualquer procedimento computacional bem definido, que toma um valor ou conjunto de valores como entrada e produz algum valor ou conjunto de valores como saída [4]. Contudo, o conceito de algoritmo não foi criado para satisfazer às necessidades da computação. Pelo contrário, a programação é apenas um dos campos da aplicação dos algoritmos.

Algoritmos iterativos estão associados ao conceito de iteração ou aproximação sucessiva. Caracterizam-se por envolver os seguintes passos:

1. Inicialização
   Consiste em coletar os dados iniciais e estabelecer as condições do problema.

2. Passo Iterativo
   Repetição sucessiva de um determinado processo.

3. Critério de Parada (ou teste de paragem)
   Instrumento por meio do qual o passo iterativo é finalizado.

Na próxima seção consta a aplicação desses passos no Algoritmo de Euclides.

3.4 Algoritmo de Euclides

O Algoritmo de Euclides aplica sucessivas vezes a Divisão Euclidiana para encontrar o máximo divisor comum de dois naturais.

Definição 3.3 (Algoritmo de Euclides)**.** *O Algoritmo de Euclides consiste nos três passos a seguir:*

1. *Inicialização*
   Dados $a, b \in \mathbb{N}$.
   Se $a < b$, *o resultado é imediato:* $q = 0$ *e* $r = a$.
   Para o caso $b \leqslant a$, *segue:*
   Defina $r_0 = a, \quad r_1 = b$ *e tome* $k = 2$.

2. *Critério de Parada*
   Se $r_{k-1} | r_{k-2}$, *então está atendido o critério de parada, tendo* $(a, b) = r_{k-1}$. *Se não, vá para o passo iterativo.*

3. *Passo Iterativo*

   Sejam $r_k, q_k \in \mathbb{N}$, *faça:*

$$r_{k-2} = r_{k-1}q_k + r_k, \quad 0 < r_k < r_{k-1}$$

   Verifique o critério de parada com $k+1$ *em vez de* k.

A referida condição é garantida, pois, caso contrário, haveria uma sequência de números naturais $b > r_1 > r_2 > ...$ sem menor elemento, o que contraria o Princípio da Boa Ordenação (teorema 3.2).

Na prática, utiliza-se o Algoritmo de Euclides posicionando os resultados de cada etapa em uma tabela. Inicialmente, tem-se: $a = bq_1 + r_1$, de forma que cada número assume sua posição na tabela:

	q_1	
a	b	
r_1		

Em seguida: $b = r_1q_2 + r_2$, posicionando esses números seguindo a mesma tabela:

	q_1	q_2	
a	b	r_1	
r_1	r_2		

Generalizando:

	q_1	q_2	q_3	...	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	...	r_{n-2}	r_{n-1}	$r_n = (a, b)$
r_1	r_2	r_3	r_4	...	r_n	0	

Para aplicar o método, segue um exemplo.

Exemplo 9. *Calcule o mdc de 372 e 162.*

Como $372 > 162$, *tem-se que:* $372 = 2.162 + 48$. *A tabela é preenchida da seguinte forma:*

	2	
372	162	
48		

$162 = 3.48 + 18$.

	2	3	
372	162	48	
48	18		

$48 = 2.18 + 12$.

	2	3	2	
372	162	48	18	
48	18	12		

$18 = 1.12 + 6$.

	2	3	2	1	
372	162	48	18	12	
48	18	12	6		

$12 = 2.6 + 0$.

	2	3	2	1	2	
372	162	48	18	12	6	
48	18	12	6	0		

Portanto, $(372, 162) = 6$.

3.5 Propriedades do mdc

A partir de agora serão explanadas propriedades relevantes do mdc.

Sejam $a, b \in \mathbb{Z}$, inicialmente, define-se o conjunto:

$$I(a, b) = \{xa + yb; x, y \in \mathbb{Z}\}.$$

A seguir, será utilizada a notação:

$$d\mathbb{Z} = \{ld; l \in \mathbb{Z}\}.$$

Teorema 3.4. *Sejam* $a, b \in \mathbb{Z}$ *não ambos nulos. Se* $d = min\ I(a,b) \cap \mathbb{N}$, *então:*

(i) d *é o mdc de* a *e* b *e*

(ii) $I(a,b) = d\mathbb{Z}$.

Demonstração. (i) Suponha que c divida a e b, logo, c divide todos os números naturais da forma $xa + yb$, portanto, c divide todos os elementos de $I(a,b)$ e, consequentemente, $c|d$.
Para mostrar que d divide todos os elementos de $I(a,b)$, considere $z \in I(a,b)$ e suponha, por absurdo, que $d \nmid z$. Logo, pela divisão euclidiana,

$$z = dq + r, \text{ com } 0 < r < d.$$

Como $z = xa + yb$ e $d = ma + nb$, para alguns $x, y, n, m \in \mathbb{Z}$, segue-se que:

$$z = dq + r \Rightarrow r = z - dq \Rightarrow r = xa + yb - (ma + nb)q$$
$$\Rightarrow r = xa - qma + yb - qmb \Rightarrow r = (x - qm)a + (y - qn)b \in I(a,b) \cap \mathbb{N},$$

o que é um absurdo, pois $d = \min I(a,b) \cap \mathbb{N}$ e $r < d$. Particularmente, $d|a$ e $d|b$. Assim, fica provado que d é o mdc de a e b.

(ii) Dado que todo elemento de $I(a,b)$ é divisível por d, tem-se que $I(a,b) \subset d\mathbb{Z}$. Por outro lado, para todo $ld \in d\mathbb{Z}$, tem-se que

$$ld = l(ma + nb) = (lm)a + (ln)b \in I(a,b)$$

e, portanto, $d\mathbb{Z} \subset I(a,b)$. Em conclusão, tem-se que $I(a,b) = d\mathbb{Z}$.

□

O Teorema 3.4 dá mais uma demonstração da existência do mdc de dois números a e b e da existência de inteiros m e n, de modo que

$$(a,b) = ma + nb.$$

Diferente do Algoritmo de Euclides, aqui não há uma forma prática de encontrar o mdc de dois números, tampouco os inteiros m e n.

Corolário 1. *Para quaisquer* $a, b \in \mathbb{Z}$, *não ambos nulos, e* $n \in \mathbb{N}$, *tem-se:*

$$(na, nb) = n(a,b)$$

Demonstração. Note que

$$I(na, nb) = nI(a, b)$$

O resultado segue do teorema anterior e do fato:

$$\min(nI(a, b) \cap \mathbb{N} = n \min(I(a, b) \cap \mathbb{N}).$$

□

Corolário 2. *Dados* $a, b \in \mathbb{Z}$, *não ambos nulos, tem-se que*

$$\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1.$$

Demonstração. Pelo Corolário 1, tem-se

$$(a, b)\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = ((a, b)\left(\frac{a}{(a, b)}, (a, b)\frac{b}{(a, b)}\right) = (a, b)$$

Provando o resultado. □

Aplica-se o Corolário 2 no exemplo abaixo, a fim de facilitar sua compreensão.

Exemplo 10. *Considerando a=6 e b=8, sabe-se que (6,8)=2. Daí*

$$\left(\frac{6}{2}, \frac{8}{2}\right) = (3, 4) = 1.$$

Conforme enunciado no referido Corolário.

Proposição 3.2. *Dois números inteiros* a *e* b *são primos entre si se, e somente se, existem números inteiros* m *e* n *tais que* $ma + nb = 1$.

Demonstração. Suponha que a e b sejam primos entre si. Logo, $(a, b) = 1$. Como pelo Teorema 3.4, tem-se que existem números inteiros m e n tais que $ma + nb = (a, b) = 1$, segue a primeira parte da proposição. Reciprocamente, suponha que existam números inteiros m, n tais que $ma + nb = 1$. Se $d = (a, b)$, temos que $d|(ma + nb)$, o que mostra que $d|1$ e, portanto, $d = 1$.

□

Essa proposição estabelece uma relação fundamental entre estruturas aditiva e multiplicativa dos números naturais, o que permitirá provar, entre outros resultados, o importante Lema de Gauss:

Teorema 3.5 (Lema de Gauss)**.** *Sejam* a, b, c *números inteiros. Se* $a|bc$ *e* $(a, b) = 1$, *então* $a|c$.

Demonstração. Se $a|bc$, então existe $e \in \mathbb{Z}$ tal que $bc = ae$.
Se $(a, b) = 1$, então, pela proposição anterior, existem $m, n \in \mathbb{Z}$ tais que

$$ma + nb = 1.$$

Multiplicando por c ambos os lados da igualdade acima:

$$c = mac + nbc.$$

Substituindo bc por ae nesta última igualdade, tem-se:

$$c = mac + nae = a(mc + ne).$$

Portanto, $a|c$.

□

Exemplo 11. $4|(27 \cdot 20)$, *logo* $4|20$, *uma vez que* $(4, 27) = 1$.

3.6 Equações Diofantinas Lineares

Estima-se que Diofanto de Alexandria tenha vivido no século III d.C.. Do autor são conhecidas duas obras: sobre números poligonais e Aritmética. Dessa última, restam somente seis livros (segundo o prefácio, o total de livros seria treze). A obra se trata de uma coletânia de problemas, a maioria indeterminados, para cuja resolução, Diofanto utilizava métodos algébricos consideravelmente diferentes da matemática grega clássica.[6]

Hoje, recebem o nome de equações diofantinas todas aquelas equações polinomiais, com coeficientes inteiros, sempre que se trata de procurar suas possíveis soluções, também nos inteiros.

Nesta seção, serão apresentadas equações diofantinas lineares, especialmente de duas incógnitas. Considere a equação:

$$ax + by = c$$

onde $a, b \in \mathbb{Z}$, não simultaneamente nulos. Uma solução é $(x_0, y_0) \in \mathbb{Z}X\mathbb{Z}$ para qual $ax_0 + by_0 = c$ é verdade.

Proposição 3.3. *Uma equação diofantina* $ax+by = c$, *em que* a *e* b *não são simultaneamente nulos, admite solução se, e somente se,* $d = (a, b)$ *divide* c.

Demonstração. $\Rightarrow$) Se $(x_0, y_0) \in \mathbb{Z}X\mathbb{Z}$ é solução, vale: $ax_0 + by_0 = c$. Como $d|a$ e $d|b$ então $d|c$.
$\Leftarrow$) Como $d = (a, b)$, $d = ax_0 + by_0$ para um conveniente par $(x_0, y_0) \in \mathbb{Z}X\mathbb{Z}$. Mas, por hipótese, $d|c$, logo: $c = dt$, para algum $t \in \mathbb{Z}$. Assim:

$$c = dt = (ax_0 + by_0)t = a(x_0 t) + b(y_0 t)$$

O que mostra que $(x_0 t, y_0 t)$ é solução.

□

Proposição 3.4. *Seja* (x_0, y_0) *uma particular solução da equação diofantina* $ax + by = c$, *onde* $a \neq 0$ *e* $b \neq 0$. *Então essa equação admite infinitas soluções, sendo seu conjunto:*

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

onde $d = (a, b)$.

Demonstração. Tomando (x', y') como soluções genéricas de $ax + by = c$ então:

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

Supondo $a = dr$ e $b = ds$:

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

onde $(r, s) = 1$.
Pela igualdade anterior, $r|s(y_0 - y')$, então $s|r(y_0 - y')$ e, portanto, $y_0 - y' = rt$ para algum $t \in \mathbb{Z}$. Daí:

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

Substituindo um resultado no outro:

$$r(x' - x_0) = s(y_0 - y') = s(y_0 - y_0 + rt) = srt$$
$$\Rightarrow r(x' - x_0) = srt$$
$$\Rightarrow x' = x_0 + st = x_0 + \frac{b}{d}t$$

Portanto, a solução da equação dada é:

$$\left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t \right)$$

□

Essa proposições serão aplicadas no exemplo que segue.

Exemplo 12. *Encontre as soluções de* $172x + 20y = 1000$.
Ao dividir todos os coeficientes da equação por 4, obtem-se: $43x + 5y = 250$.

$$43 = 5 \cdot 8 + 3$$
$$5 = 3 \cdot 1 + 2$$
$$3 = 2 \cdot 1 + 1$$

Tem-se que:
$1 = 3 - 2 \cdot 1 = 3 - (5 - 3 \cdot 1) = 3 \cdot 2 + 5 \cdot (-1) = (43 - 5 \cdot 8) \cdot 2 + 5 \cdot (-1) = 43 \cdot 2 + 5 \cdot (-17)$, *portanto,*

$$(x_0, y_0) = (2, -17)$$

Logo, $(250x_0, 250y_0) = (500, -4250)$ *é uma solução particular. A solução geral é:*

$$x = 500 + 5t$$
$$y = -4250 - 43t$$

onde $t \in \mathbb{Z}$

A resolução de equações diofantinas linerares será ferramenta importante para solucionar congruências lineares que serão vistas no Capítulo 5.

3.7 Mínimo Múltiplo Comum

Elucidadas algumas das propriedades principais do mdc, nesta seção, será apresentado o conceito de mínimo múltiplo comum, encerrando o capítulo sobre Divisibilidade.

Um número inteiro é um múltiplo comum de dois números inteiros se ele é, simultaneamente, múltiplo de ambos. Em qualquer caso, os números ab e 0, são sempre múltiplos de a e b.

Exemplo 13. *Considerando* $a = 5$ *e* $b = 12, ab = 60$. *Então* $ab = 60$ *e 0 são dois múltiplos comuns de* a *e* b.

Exemplo 14. *Considerando* $a = 4$ *e* $b = 6$, *os números* $12, 24, 36, 132$ *são alguns dos múltiplos comuns de* a *e* b.

Definição 3.4. $n \geqslant 0$ *é um mínimo múltiplo comum (mmc) dos números inteiros* a *e* b, *se atender às seguintes condições:*

(i) n *é múltiplo comum de* a *e* b, *e*

(ii) se c *é múltiplo comum de* a *e* b, *então* $n|c$.

Denota-se o múltiplo comum de a e b por $[a, b]$.

Exemplo 15. *Considerando* $a = 2$ *e* $b = 9$. *O número 36 é múltiplo comum de* a *e* b, *mas não é um mmc deles. O número 18 é um mmc de 2 e 9, pois atende às condições: é múltiplo comum de 2 e 9, e* $18|36$.

De modo simplificado, o mínimo múltiplo comum entre dois ou mais números é representado pelo menor valor comum pertecente aos múltiplos dos números.

Exemplo 16. *Para determinar o mmc de 20 e 30, encontramos os mútiplos de 20:* $0, 20, 40, 60, 80, ...$ *e os múltiplos de 30:* $0, 30, 60, 90, ...$. *É fácil observar que o menor múltiplo comum é 60. Outra forma calcular o mmc é por meio da fatoração em números primos, na qual devemos selecionar os fatores comuns e não comuns de menor expoente:* $20 = 2 \cdot 2 \cdot 5 = 2^2 \cdot 5$
$30 = 2 \cdot 3 \cdot 5$
$[20, 30] = 2^2 \cdot 3 \cdot 5 = 60$

Proposição 3.5. *O mínimo múltiplo comum, se existe, é único.*

Demonstração. Se n e n' são dois mínimos múltiplos comuns de a e b, então, de (ii) da definição supracitada, tem-se que $n|n'$ e $n'|n$. Sendo n e n' inteiros não negativos, só pode ser que $n = n'$.

□

Para efeito do cálculo do mmc de dois números, supõe-se que sempre são não negativos.

Proposição 3.6. $[a, b] = 0 \Leftrightarrow a = 0 \quad ou \quad b = 0$.

Demonstração. Se $[a, b] = 0$, então 0 divide ab que é um múltiplo comum de a e b, portanto, $ab = 0$, logo, $a = 0$ ou $b = 0$. Por outro lado, se $a = 0$ ou $b = 0$, o único múltiplo comum de a e b é 0, assim, $[a, b] = 0$.

□

A próxima porposição tem um resultado interessante, pois relaciona o cálculo do mmc com o Algoritmo de Euclides.

Proposição 3.7. *Dados dois números inteiros* a *e* b, *afirma-se que* $[a, b]$ *existe e* $[a, b](a, b) = |ab|$.

Demonstração. Se $a = 0$ ou $b = 0$, a igualdade acima é trivialmente satisfeita, pois $[0, 0] = 0$, daí $0 \cdot (0, 0) = 0 = |0 \cdot 0|$.
Sem perda de generalidade, supõe-se $a, b \in \mathbb{N}$. Tome $m = \dfrac{ab}{(a, b)}$. Como

$$m = a\frac{b}{(a, b)} = b\frac{a}{(a, b)},$$

tem-se que $a|m$ e $b|m$, logo, m é múltiplo comum de a e b.
Seja c um múltiplo comum de a e b, assim, $c = na = n'b$. Segue que

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

Pelo Corolário 2, $\dfrac{a}{(a, b)}$ e $\dfrac{b}{(a, b)}$ são primos entre si, segue do Teorema 3.4, que $\dfrac{a}{(a, b)}$ divide n' e, portanto, $m = \dfrac{a}{(a, b)}b$ divide $n'b$ que é igual a c .

□

Isso significa que, para encontrar o mmc de dois inteiros ambos não nulos, basta dividir o módulo do produto dos dois números pelo seu mdc.

Exemplo 17. *Considerando* $a = 45$ *e* $b = 27$. *Será calculado o mdc pelo Algoritmo de Euclides, para, em seguida, encontrar o mmc pela Proposição 3.5.*

$45 = 1.27 + 18$

	1	
45	27	
18		

$27 = 1.18 + 9$

	1	1	
45	27	18	
18	9		

$18 = 2.9 + 0$

	1	1	2	
45	27	18	9	
18	9	0		

Logo, $(45, 27) = 9$. *Como* $[a, b](a, b) = |ab|$:

$$[a, b] = \frac{|ab|}{(a, b)} \Rightarrow [45, 27] = \frac{|45 \cdot 27|}{9} \Rightarrow [45, 27] = 135 \ .$$

Portanto, o mmc de 45 e 27 é 135.

4 Números Primos

O conceito de números primos será indispensável no estudo do Teorema Chinês dos Restos. Por esse motivo, vale a pena abordar objetivamente o assunto, com suas aplicações.

Definição 4.1. *Um número inteiro* $n, (n > 1)$, *que possui somente dois divisores positivos, sendo eles:* n *e* 1, *é chamado primo. Caso possua mais divisores,* n *é dito composto.*

Exemplo 18. *O número 23 é primo, pois seus únicos divisores positivos são 1 e 23. Já o número 14 é composto, pois pode ser dividido por 1, 2, 7, 14.*

Dois números são primos entre si, quando o máximo divisor comum é 1.

Exemplo 19. *Os números 41 e 22 são primos entre si, pois o único inteiro positivo que divide ambos é 1.*

Dados dois números primos p e q e um número inteiro a qualquer. Pelo exposto, decorrem as seguintes afirmativas:

(i) Se $p|q$, então $p = q$.

Demonstração. Como $p|q$ e sendo q primo, decorre que $p = 1$ ou $p = q$. Todavia, como p é primo, isto é $p > 1$, logo, $p = q$. □

(ii) Se $p \nmid a$, então $(p, a) = 1$.

Demonstração. Se $(p, a) = d$, então $d|p$ e $d|a$. Já que p é primo, então $d = p$ ou $d = 1$. Como $p \nmid a$, logo, $d \neq p$. Por conseguinte, $d = 1$.

□

A próxima proposição estabelece mais um resultado de Euclides:

Proposição 4.1 (Lema de Euclides)**.** *Sejam* $a, b, p \in \mathbb{Z}$, *com* p *primo. Se* $p|ab$, *então* $p|a$ *ou* $p|b$.

Demonstração. Basta provar que se $p|ab$ e $p \nmid a$, então $p|b$. Mas, se $p \nmid a$, tem-se que $(p, a) = 1$, pelo Lema de Gauss (Teorema 3.4), então $p|b$.

□

Exemplo 20. *Seja* $a = 14, b = 5, p = 7$, *logo* $ab = 70$. *Como* $7|70$, p *divide* a *ou* b. *No caso,* $p|a$.

4.1 Teorema Fundamental da Aritmética

Do ponto de vista da estrutura multiplicativa dos naturais, os números primos são, certamente, os mais simples, contudo, são suficientes para gerar todos os números naturais. Esse fato é estabelecido pelo conhecido Teorema Fundamental da Aritmética, enunciado nesta seção.

Teorema 4.1. *Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração. O teorema será provado por indução. Supondo o resultado válido para todo número natural menor do que n, deve-se provar que vale para n. Se n é primo, nada precisa ser demonstrado, por esse motivo, considere n composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução (suposição de que todo número menor que n se escreve como produto de números primos), tem-se que existem números primos $p_1, ..., p_r$ e $q_1, ..., q_s$ tais que $n_1 = p_1...p_r$ e $n_2 = q_1...q_s$, por conseguinte, $n = p_1...p_r q_1...q_s$.
Deve-se provar a unicidade da escrita (exceto pela ordem dos fatores). Suponha, agora, $n = p_1...p_r = q_1...q_s$, novamente, com p_i e q_j primos. A unicidade fica provada se for mostrado que $s = r$ e que cada parcela p_i é igual a algum q_j. Como $p_1|q_1...q_s$, ele divide, ao menos, um dos fatores de q_j. Sem perda de generalidade, supõe-se que $p_1|q_1$, mas se eles são primos, então $p_1 = q_1$. Assim,

$$p_2...p_r = q_2...qs$$

Como $p_2...p_r < n$, pela hipótese de indução, $r = s$ e os p_i e q_j são iguais aos pares.

□

A escrita de um número através de números primos é chamada de decomposição em fatores primos. Dados $n, m \in \mathbb{N}$ com $n > 1$ e $m > 1$ quaisquer, é possível escrever

$$n = p_1^{\alpha_1}...p_r^{\alpha_r} \text{ e } m = p_1^{\beta_1}...p_r^{\beta_r},$$

usando o mesmo conjunto de números primos, mas permitindo que os expoentes variem em $\mathbb{N} \cup \{0\}$.

Exemplo 21. *A decomposição dos números 30 e 69 utilizando o mesmo conjunto de números primos pode ser da seguinte maneira:*

$$30 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 23^0 \text{ e } 69 = 2^0 \cdot 3^1 \cdot 5^0 \cdot 23^1 \ .$$

Exemplo 22. *A decomposição dos números 20 e 70 utilizando o mesmo conjunto de números primos pode ser da seguinte maneira:*

$$20 = 2^2 \cdot 5^1 \cdot 7^0 \text{ e } 70 = 2^1 \cdot 5^1 \cdot 7^1 \ .$$

5 Congruência

A aritmética com os restos da Divisão Euclidiana (vista na Seção 3.1) por um número fixado é uma das noções introduzidas por Gauss no livro Disquisitiones Arithmeticae, de 1801 [6].

Nesse capítulo será definida a congruência entre números inteiros módulo $\mathfrak{m} > 1$, além de suas propriedades mais importantes.

Definição 5.1. *Sejam* $\mathfrak{a}, \mathfrak{b}, \mathfrak{m}$ *números inteiros,* $\mathfrak{m} > 1$. *Diz-se que* $\mathfrak{a}$ *é côngruo a* $\mathfrak{b}$, *módulo* $\mathfrak{m}$, *se* $\mathfrak{a}$ *e* $\mathfrak{b}$ *deixam o mesmo resto quando divididos por* $\mathfrak{m}$.
Notação: $\mathfrak{a} \equiv \mathfrak{b}(\ \mathit{mod}\ \mathfrak{m})$.

Exemplo 23. *A seguir alguns exemplos para melhor compreensão do conceito:*

(i) $7 \equiv 9$ *mod* 2, *pois* 7 *e* 9, *quando divididos por* 2, *deixam o mesmo resto que é* 1.

(ii) $26 \equiv 10$ *mod* 4, *pois* 26 *e* 10 *deixam o mesmo resto* 2 *ao serem divididos por* 4.

(iii) $13 \equiv 41$ *mod* 7, *pois ao dividir* 13 *por* 7 *e* 41 *por* 7, *obtém-se o mesmo resto que é* 6.

Na definição anterior foi considerado $\mathfrak{m} > 1$, pois, como o resto da divisão de um número inteiro por 1 é sempre nulo, ou seja $\mathfrak{a} \equiv \mathfrak{b} \bmod \mathfrak{m}$ para quaisquer $\mathfrak{a}, \mathfrak{b} \in \mathbb{Z}$, torna-se trivial a aritmética dos restos módulo 1.

Quando a relação $\mathfrak{a} \equiv \mathfrak{b} \bmod \mathfrak{m}$ for falsa, diz-se que $\mathfrak{a}$ e $\mathfrak{b}$ não são congruentes (ou incongruentes) módulo $\mathfrak{m}$. Em notação: $\mathfrak{a} \not\equiv \mathfrak{b} \bmod \mathfrak{m}$.

Nota-se, imediatamente, que congruência é uma relação de equivalência. Valendo, portanto, as proposições a seguir:

Proposição 5.1. *Seja* $\mathfrak{m} \in \mathbb{N}$. *Para todos* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \in \mathbb{Z}$, *tem-se que:*

(i) $\mathfrak{a} \equiv \mathfrak{a}$ *mod* $\mathfrak{m}$,

(ii) se $\mathfrak{a} \equiv \mathfrak{b}$ *mod* $\mathfrak{m}$, *então* $\mathfrak{b} \equiv \mathfrak{a}$ *mod* $\mathfrak{m}$,

(iii) se $\mathfrak{a} \equiv \mathfrak{b}$ *mod* $\mathfrak{m}$ *e* $\mathfrak{b} \equiv \mathfrak{c}$ *mod* $\mathfrak{m}$, *então* $\mathfrak{a} \equiv \mathfrak{c}$ *mod* $\mathfrak{m}$.

Mas não será preciso sempre dividir $\mathfrak{a}$ e $\mathfrak{b}$ por $\mathfrak{m}$ a fim de comparar seus restos para verificar se existe congruência entre eles. Basta aplicar o resultado que segue:

Proposição 5.2. *Suponha que* $a, b, m \in \mathbb{Z}$, *com* $m > 1$. *Tem-se que* $a \equiv b$ *mod* m *se, e somente se,* $m|b - a$.

Demonstração. Sejam $a = mq + r$, com $0 \leqslant r < m$ e $b = mq' + r'$, com $0 \leqslant r' < m$, as divisões euclidianas de a e b por m, respectivamente. Logo:

$$b - a = mq' + r' - mq - r = m(q' - q) + (r' - r)$$

Portanto, $a \equiv b$ mod m se, e somente se, $r = r'$, o que acarretaria: $m|b - a$, já que $|r - r'| < m$.

□

Exemplo 24. *Reanalisando as mesmas congruências do exemplo passado, agora, tem-se:*

(i) $7 \equiv 9$ *mod* 2, *pois* $2|(9 - 7)$.

(ii) $26 \equiv 10$ *mod* 4, *pois* $4|(10 - 26)$.

(iii) $13 \equiv 41$ *mod* 7, *pois* $7|(41 - 13)$.

Perceba que todo número inteiro é congruente módulo m ao seu resto pela divisão euclidiana por m e, por conseguinte, é congruente módulo m a um dos números: $0, 1, ..., m - 1$, que são os possíves restos. É claro que dois desses números distintos não são congruentes módulo m.

Exemplo 25. *Na divisão euclidiana de* 11 *por* 5, *obtem-se resto* 1. *Note que* $11 \equiv 1$ *mod* 5.

Denomina-se sistema completo de resíduos módulo m todo conjunto de números inteiros cujos restos pela divisão por m são os números $0, 1, ..., m - 1$, sem repetições e numa ordem qualquer. Portanto, um sistema completo de resíduos módulo m possui m elementos.

Exemplo 26. *Se* $m = 3$, *as classes que formam o sistema completo de resíduos módulo* 3 *são:*
$\{..., -9, -6, -3, 0, 3, 6, 9, ...\}$, *formado pelos números que deixam resto 0 na divisão por 3.*
$\{..., -8, -5, -2, 1, 4, 7, 10, ...\}$ *formado pelos números que deixam resto 1 na divisão por 3.*
$\{..., -7, -4, -1, 2, 5, 8, 11, ...\}$ *formado pelos números que deixam resto 2 na divisão por 3.*
Dessa maneira, para construir um sistema completo de resíduos módulo 3, *basta escolher um representante de cada classe, por exemplo:* $\{-9, 1, -4\}$.
Em particular, o conjunto formado por números consecutivos também será um sistema completo de resíduos módulo 3 : $\{3, 4, 5\}$.

A escolha conveniente de um elemento em cada uma das classes para representá-la, em muitas oportunidades, poderá facilitar os cálculos.

Lema 5.1. *Dados* p *primo e* a *inteiro de tal modo que* $(p, a) = 1$ *e dado o conjunto* $A = \{an; \forall n \in \mathbb{N} \ \ com \ \ n < p\}$. *O conjunto dos restos das divisões dos elementos de* A *por* p *forma um sistema completo de resíduos módulo* p.

Demonstração. Como n é diferente de zero e estritamente menor do que p, então tem-se exatamente $p - 1$ valores possíveis. Agora, suponha que haja dois múltiplos de a : ia e ja que tenham o mesmo resto quando divididos por p : $ia \equiv ja \mod p$.
Subtraindo ja de ambos os lados:

$$ia \equiv ja \mod p \Rightarrow ia - ja \equiv ja - ja \mod p \Rightarrow a(i - j) \equiv 0 \mod p.$$

Isto é, p divide $a(i - j)$, logo, se divide o produto de dois números, ele deve, pelo menos, dividir um deles. Mas como a não é divisível por p, daí p deve dividir $i - j$.

Mas i e j são ambos menores que p, portanto, a diferença deles deve estar estritamente entre $-p$ e p. O único múltiplo de p estritamente entre $-p$ e p é zero, então $i - j = 0$, isto é, $i = j$.

Isso significa que a única maneira de ter $ia \equiv ja \mod p$ é se $i = j$. Mostrando, assim, que todos os múltiplos de a a partir dele mesmo até $(p - 1)a$ possuem diferentes restos quando divididos por p.

Finalmente, uma vez que existem exatamente $p - 1$ múltiplos não nulos de a no conjunto e $p - 1$ possíveis restos não nulos mod p, conclui-se que cada resto aparece exatamente uma vez. Provando assim que o conjunto dos restos das divisões dos elementos de A por p se configura como um sistema completo de resíduos módulo p.

□

Havendo duas congruências de mesmo módulo, é possível fazer operações entre elas, conforme proposições abaixo:

Proposição 5.3. *Sejam* $a, b, c, d, m \in \mathbb{Z}$, *com* $m > 1$.

(i) Se $a \equiv b$ *mod* m *e* $c \equiv d$ *mod* m, *então* $a + c \equiv b + d$ *mod* m.

(ii) Se $a \equiv b$ *mod* m *e* $c \equiv d$ *mod* m, *então* $ac \equiv bd$ *mod* m.

Demonstração. Suponha que $a \equiv b \mod m$ e $c \equiv d \mod m$. Logo, temos que $m|b - a$ e $m|d - c$.

(i) Basta observar que $m|(b - a) + (d - c)$ e, portanto, $m|(b + d) - (a + c)$, o que prova essa parte do resultado.

(ii) Basta notar que $bd - ac = d(b - a) + a(d - c)$ e concluir que $m|bd - ac$.

□

Exemplo 27. *Considerando as congruências:*

$$2 \equiv 9 \text{ mod } 7 \text{ e } 6 \equiv 13 \text{ mod } 7.$$

Então, $2 + 6 \equiv 9 + 13$ *mod* $7 \Rightarrow 8 \equiv 22$ *mod* 7.
Também é verdade que $2 \cdot 6 \equiv 9 \cdot 13$ *mod* $7 \Rightarrow 12 \equiv 117$ *mod* 7.

A proposição a seguir diz que, para as congruências, vale o cancelamento de parcelas com relação à adição:

Proposição 5.4. *Sejam* $a, b, c, m \in \mathbb{Z}$, *com* $m > 1$. *Tem-se que*

$$a + c \equiv b + c \text{ mod } m \Leftrightarrow a \equiv b \text{ mod } m.$$

Demonstração. Se $a \equiv b$ mod m, segue-se imediatamente da Proposição 5.3 (i) que $a + c \equiv b + c$ mod m, pois $c \equiv c$ mod m.

Reciprocamente, se $a + c \equiv b + c$ mod m, então $m|b + c - (a + c)$, o que implica que $m|b - a$ e, consequentemente, $a \equiv b$ mod m.

□

É importante ressaltar que o mesmo vale para a subtração.

Exemplo 28. *Como* $7 \equiv 12$ *mod* 5, *então é verdade que:*

$$7 - 3 \equiv 12 - 3 \text{ mod } 5 \Rightarrow 4 \equiv 9 \text{ mod } 5$$
$$7 + 11 \equiv 12 + 11 \text{ mod } 5 \Rightarrow 18 \equiv 23 \text{ mod } 5$$

O cancelamento multiplicativo não vale da mesma maneira, embora ainda seja possível fazer a seguinte equivalência:

Proposição 5.5. *Sejam* $a, b, c, m \in \mathbb{Z}$, *com* $m > 1$. *Temos que*

$$ac \equiv bc \text{ mod } m \Leftrightarrow a \equiv b \text{ mod } \frac{m}{(c, m)}.$$

Demonstração. Como $\frac{m}{(c, m)}$ e $\frac{c}{(c, m)}$ são coprimos, temos que

$$ac \equiv bc \bmod m \Leftrightarrow m|(b-a)c \Leftrightarrow \frac{m}{(c,m)}|(b-a)\frac{c}{c,m} \Leftrightarrow \frac{m}{(c,m)}|b-a$$
$$\Leftrightarrow a \equiv b \bmod \frac{m}{(c,m)}.$$

□

Corolário 3. *Sejam* $a, b, c, m \in \mathbb{Z}$, *com* $m > 1$ *e* $(c, m) = 1$. *Tem-se que*

$$ac \equiv bc \text{ } mod \text{ } m \Leftrightarrow a \equiv b \text{ } mod \text{ } m.$$

Exemplo 29. *Tem-se que:*

$$10 \equiv 22 \text{ } mod \text{ } 4 \Rightarrow 5 \cdot 2 \equiv 11 \cdot 2 \text{ } mod \text{ } 4 \Rightarrow 5 \equiv 11 \text{ } mod \frac{4}{2} \Rightarrow 5 \equiv 11 \text{ } mod \text{ } 2.$$

A próxima proposição fornece uma maneira de encontrar outros sistemas completos de resíduos a partir de um já definido.

Proposição 5.6. *Sejam* $a, k, m \in \mathbb{Z}$, *com* $m > 1$ *e* $(k, m) = 1$. *Se* $a_1, ..., a_m$ *é um sistema completo de resíduos módulo* m, *então*

$$a + ka_1, ..., a + ka_m$$

também é um sistema completo de resíduos módulo m.

Demonstração. Como, do corolário acima, para $i, j = 0, ..., m-1$, tem-se que

$$a + ka_i \equiv a + ka_j \bmod m \Leftrightarrow ka_i \equiv ka_j \bmod m \Leftrightarrow a_i \equiv a_j \bmod m \Leftrightarrow i = j.$$

Isso mostra que $a + ka_1, ..., a + ka_m$ são, dois a dois, não congruentes módulo m e, portanto, formam um sistema completo de resíduos módulo m.

□

É válido, ainda, observar propriedades adicionais das congruências, relacionadas com multiplicação:

Proposição 5.7. *Sejam* $a, b \in \mathbb{Z}$ *e* $m, n, m_1, ..., m_r$ *inteiros maiores do que* 1. *Tem-se*

(i) se $a \equiv b$ *mod* m *e* $n|m$, *então* $a \equiv b$ *mod* n;

(ii) $a \equiv b$ *mod* $m_i, \forall i = 1, ..., r \Leftrightarrow a \equiv b$ *mod* $[m_1, ..., m_r]$;

(iii) se $a \equiv b$ *mod* m, *então* $(a, m) = (b, m)$.

Demonstração. (i) Se $a \equiv b \bmod m$, então $m|b-a$. Como $n|m$, segue que $n|b-a$. Logo, $a \equiv b \bmod n$.

(ii) Se $a \equiv b \bmod m_i, i = 1, ..., r$, então $m_i | b - a$, para todo i. Sendo $b - a$ um múltiplo de cada m_i, segue-se que $[m_1, ..., m_r] | b - a$, o que prova que $a \equiv b \bmod [m_1, ..., m_r]$. Por outro lado, tem-se que $a \equiv b \bmod [m_1, ..., m_r]$ e $m_i | [m_1, ..., m_r], i = 1, ..., r$, logo, pela proposição anterior, $a \equiv b \bmod m_i$.

(iii) Se $a \equiv b \bmod m$, então $m | b - a$ e, portanto, $b = a + tm$ com $t \in \mathbb{Z}$. Logo, pelo Lema 3.1:

$$(a, m) = (a + tm, m) = (b, m)$$

□

5.1 Congruência Linear

Vistas todas essas propriedades, é possível resolver as chamadas congruências lineares ou congruências de primeiro grau, que são do tipo:

$$ax \equiv b \bmod m$$

onde $a, b, m \in \mathbb{Z}, a \neq 0, m > 0$ e x é uma variável também em $\mathbb{Z}$.

Exemplo 30. *Dada a congruência de primeiro grau* $2x \equiv 3$ *mod* 5, *tem-se como uma solução* $x = 4$. *Mas, na realidade, todos os elementos do conjunto* $\{4 + 5t, t \in \mathbb{Z}\}$ *são representações da mesma solução.*

Exemplo 31. *Encontre o menor múltiplo positivo de 7 que deixa resto 1 quando dividido por 2, 3, 4, 5 e 6. [6]*

Solucionar o problema equivale a resolver às seguintes congruências lineares:

$$7X \equiv 1 \ mod\ 2$$
$$7X \equiv 1 \ mod\ 3$$
$$7X \equiv 1 \ mod\ 4$$
$$7X \equiv 1 \ mod\ 5$$
$$7X \equiv 1 \ mod\ 6$$

Pela Proposição 5.7 (ii), essas congruências lineares têm a mesma solução que

$$7X \equiv 1 \ mod\ [2, 3, 4, 5, 6].$$

Logo, deve-se achar a solução positiva mínima u *de:* $70X \equiv 1$ *mod* 60. *Transformando essa congruência em equação diofantina (assunto visto na Seção 3.6), tem-se:* $7X - 60Y = 1$.
Pelo algoritmo de euclides: $60 = 7 \cdot 8 + 4$
$7 = 4 \cdot 1 + 3$
$4 = 3 \cdot 1 + 1$
Portanto,

$$1 = 4 - 3 \cdot 1 = 4 - (7 - 4) = 2 \cdot 4 - 7 = 2(60 - 7 \cdot 8) - 7 = 7 \cdot (-17) - 60 \cdot (-2)$$

$x_0 = -17$ *e* $y_0 = -2$ *é uma solução particular da equação diofantina, sendo a solução geral* $x = -17 + 60t$ *e* $y = -2 - 7t, t \in \mathbb{Z}$.
Portanto, o menor valor positivo para u de modo que exista v *para os quais* u, v *é uma solução de* $7X - 60Y = 1$ *é* $u = -17 + 1 \cdot 660 = 43$. *Substituindo na congruência de interesse:*

$$7 \cdot 43 \equiv 1 \text{ mod } 60 \Rightarrow 301 \equiv 1 \text{ mod } 60.$$

5.2 Sistemas de Congruências

Nessa seção, serão estudados sistemas formados por congruências lineares simultâneas. Genericamente, os sistemas são do tipo:

$$\begin{cases} a_1 x \equiv b_1 \mod m_1 \\ a_2 x \equiv b_2 \mod m_2 \\ \ldots \\ a_n x \equiv b_n \mod m_n \end{cases}$$

Uma solução do sistema é o inteiro x_0 que é solução de cada uma das congruências que pertencem ao sistema. Ou seja, se uma das congruências não tem solução, por conseguinte, todo o sistema não possui solução.

Exemplo 32. *Solucione o sistema de congruências:*

$$\begin{cases} 3x \equiv 1 \mod 5 \\ 2x \equiv 3 \mod 9 \end{cases}$$

Uma das soluções da primeira congruência é 2 e da segunda é 6. Daí, as soluções gerais são:

$$x = 2 + 5t, t \in \mathbb{Z} \text{ para a primeira equação}$$
$$x = 6 + 9s, s \in \mathbb{Z} \text{ para a segunda equação}$$

Em congruências, tem-se:

$$x \equiv 2 \mod 5$$
$$x \equiv 6 \mod 9$$

Substituindo a solução geral $x = 2 + 5t$ *da primeira congruência na segunda:*

$$2 + 5t \equiv 6 \ mod\ 9$$
$$\Rightarrow 5t \equiv 4 \ mod\ 9$$

Sendo $t_0 = 8$ *uma solução particular. Então,* $t = 8 + 9k$ *é uma solução geral. Daí:*

$$x = 2 + 5t = 2 + 5(8 + 9k) = 42 + 45k, (k \in \mathbb{N})$$
ou
$$x \equiv 42 \ mod\ 45$$

é a solução do sistema.

Como foi executado no exemplo anterior, toda equação linear pode ser transformada em outra equivalente com coeficiente 1. Portanto, a partir de agora, neste trabalho, serão estudados exclusivamente os sistemas com os coeficientes de x iguais a 1.

Proposição 5.8. *Um sistema*

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

admite solução se, e somente se, $a_1 - a_2$ *é divisível por* $d = (m_1, m_2)$. *Neste caso, se* x_0 *é uma solução particular do sistema e se* $m = [m_1, m_2]$, *então* $x \equiv x_0$ *mod* m *é sua solução geral.*

Demonstração. $\Rightarrow$) Se x_0 é solução particular do sistema, então existe $t \in \mathbb{Z}$ tal que

$$x_0 = a_1 + m_1 t \text{ e } a_1 + m_1 t \equiv a_2 \mod m_2$$
$$\Rightarrow m_1 t \equiv a_2 - a_1 \text{ mod } m_2$$

Logo, $d|(a_2 - a_1)$
$\Leftarrow$) Como, por hipótese, $d|(a_2 - a_1)$, então

$$m_1 y \equiv a_2 - a_1 \text{ mod } m_2$$

admite uma solução y_0. Daí,

$$a_1 + m_1 y_0 \equiv a_2 \text{ mod } m_2$$

Como

$$a_1 + m_1 y_0 \equiv a_1 \text{ mod } m_1$$

então $a_1 + m_1 y_0$ é solução do sistema.
Se x_0 é solução particular e x é geral, então $x_0 \equiv a_1 \bmod m_1$ e $x \equiv a_1 \bmod m_1$. Assim,

$$x \equiv x_0 \bmod m_1$$

isto é $m_1|(x - x_0)$. Analogamente, $m_2|(x - x_0)$. Então $m|(x - x_0)$, o que é equivalente a

$$x \equiv x_0 \bmod m$$

□

Será dedicado todo o Capítulo 6 para abordar o Teorema Chinês dos Restos, tema principal desse trabalho, que é uma das formas de resolver sistemas de congruências.

6 Teorema Chinês dos Restos

Acredita-se que, na antiguidade, os generais chineses contavam os soldados mortos nas guerras da seguinte forma: agrupavam as tropas em grupos de diferentes tamanhos, formando colunas, e depois contavam quantos soldados sobravam. E repetiam algumas vezes para tamanhos diferentes de grupos. [5]

Supondo que um general inicia uma batalha com 2000 soldados e, ao seu término, ele precise verificar quantos homens não retornaram. Com esse propósito, ele alinha os soldados em colunas de 7, sobrando 5 deles. Quando os organiza em grupos de 9, restam 4. E quando os alinha em grupos de 10, sobra apenas 1. Sabendo que retornaram mais de 1500 indivíduos dessa batalha, quantos sobreviveram e quantos morreram? [5]

Para solucionar problemas dessa natureza, pode-se fazer uso do conhecimento acerca de congruências (abordadas no Capítulo 5) e sistemas de congruências.

Nesse sentido, o Teorema Chinês dos Restos propõe uma maneira de encontrar respostas para tais sistemas. No presente capítulo, o teorema é enunciado e demonstrado e, em seguida, será apresentado um algoritmo, elaborado pela autora, que roteiriza a resolução de sistemas com n equações.

Serão abordados sistemas de n congruências da seguinte forma:

$$\begin{aligned} X &\equiv a_1 \mod m_1 \\ X &\equiv a_2 \mod m_2 \\ &\dots \\ X &\equiv a_n \mod m_n \end{aligned}$$

Teorema 6.1 (Teorema Chinês dos Restos)**.** *Para que tal sistema possua solução, é suficiente que* m_i *e* m_j *sejam primos entre si, isto é* $(m_i, m_j) = 1$*, para todo par* m_i, m_j *com* $i \neq j$*. A solução será única módulo* $z = m_1 m_2 ... m_r$ *como segue:*

$$S = a_1 x_1 y_1 + ... + a_n x_n y_n$$

onde $x_i = z/m_i$ *e* y_i *é solução de* $x_i y_i \equiv 1$ *mod* m_i*,* $\quad i = 1, ..., n$.

Demonstração. Vamos provar que S é solução simultânea do sistema de congruências. Como $m_i | z$, e $x_i y_i \equiv 1 \mod m_i$ segue que:

$$S = a_1 x_1 y_1 + ... + a_n x_n y_n \equiv a_i x_i y_i \equiv a_i \mod m_i$$

Portanto, a solução existe e tem essa forma. Provaremos, por absurdo, que ela é única. Considerando que S' é outra diferente solução para o sistema, então:

$$S \equiv a_i \mod m_i$$
$$S' \equiv a_i \mod m_i$$

Ou seja:

$$S \equiv S' \mod m_i, i = 1, ..., n.$$

Como $(m_i, m_j) = 1$ para $i \neq j$, segue que $[m_1, ..., m_n] = m_1 ... m_n = z$ portanto, $S \equiv S' \mod z$, o que é um absurdo. Logo, a solução é única. □

O enunciado do Teorema Chinês dos Restos traz informações que roteirizam o cálculo para encontrar a solução do sistema. A partir dos exemplos a seguir, fica claro a linha de raciocínio a ser seguida.

Exemplo 33. *Solucione o sistema de congruências:*

$$X \equiv 2 \ mod \ 3$$
$$X \equiv 3 \ mod \ 5$$
$$X \equiv 2 \ mod \ 7$$

Como $3, 5, 7$ *são primos entre si, o sistema tem solução.*
Cálculo de z:
$z = 3 \cdot 5 \cdot 7 = 105$
Cálculo de x_1, x_2, x_3 :
$x_1 = \frac{105}{3} = 35; x_2 = \frac{105}{5} = 21; x_3 = \frac{105}{7} = 15$
Cálculo de y_1, y_2, y_3 :
$35y_1 \equiv 1 \ mod \ 3 \Rightarrow y_1 = 2$
$21y_2 \equiv 1 \ mod \ 5 \Rightarrow y_2 = 1$
$15y_3 \equiv 1 \ mod \ 7 \Rightarrow y_3 = 2$
Cálculo de S:
$S = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \ mod \ 105$
Dessa forma, tem-se que 23 é uma solução e qualquer outra solução é da forma:
$x = 23 + 105k, k \in \mathbb{Z}$

Exemplo 34. *Solucione o sistema de congruências:*

$$X \equiv 1 \ mod \ 5$$
$$X \equiv 2 \ mod \ 7$$
$$X \equiv 3 \ mod \ 11$$

Como $5, 7, 11$ *são primos entre si, o sistema tem solução.*
Cálculo de z:
$z = 5 \cdot 7 \cdot 11 = 385$
Cálculo de x_1, x_2, x_3 :
$x_1 = \frac{385}{5} = 77; x_2 = \frac{385}{7} = 55; x_3 = \frac{385}{11} = 35$

Cálculo de y_1, y_2, y_3 :
$77y_1 \equiv 1$ *mod* $5 \Rightarrow y_1 = 3$
$55y_2 \equiv 1$ *mod* $7 \Rightarrow y_2 = 6$
$35y_3 \equiv 1$ *mod* $11 \Rightarrow y_3 = 6$
Cálculo de S:
$S = 1 \cdot 77 \cdot 3 + 2 \cdot 55 \cdot 6 + 3 \cdot 35 \cdot 6 = 1521 \equiv 366$ *mod* 385
Dessa forma, tem-se que 366 é uma solução e qualquer outra solução é da forma:
$x = 366 + 385k, k \in \mathbb{Z}$

6.1 Algoritmo

A proposta de algoritmo, a seguir, foi elaborada pela autora, para aplicação do Teorema Chinês dos Restos na resolução de sistemas de congruências. Trata-se de um algoritmo com muitos passos iterativos, todavia, a fim de simplificar, ocultou-se as iterações para obter os dados de entrada da inicialização e do item 4.

1. Inicialização
   a) Entrar com número n;
   b) Solicitar valores para $a_1, ..., a_n$ e $m_1, ..., m_n$
   c) Verificar se $(m_i, m_j) = 1$, para i $\neq$ j;
   d) Cálculo de $z = m_1 m_2 ... m_n$;
   e) i=1;
2. Passo iterativo
   Faça:
   a) Cálculo de $x_i = \dfrac{z}{m_i}$;
   b) Cálculo de w_i = resto de x_i dividido por m_i;
   c) Cálculo de y_i ;
      i. Inicialização
      $t = 1$.
      ii. Passo Iterativo
      Faça: $\dfrac{(w_i \cdot t)}{m_i}$
      iii. Critério de Parada
      Se o resto da divisão for 1, então o critério de parada está atendido e $y_i = t$.
      Se não, volte ao passo iterativo com $t + 1$ em vez de t.

3. Critério de Parada
   Se $i = n$, o critério de parada está atendido. Senão, volte para o passo iterativo com $i + 1$ em vez de i.

4. Cálculo de S $= a_1 x_1 y_1 + ... + a_n x_n y_n$;

5. Cálculo de R, resto de S divido por z;

6. Mostra na tela resultado final: $x = R + z \cdot k$, onde k é natural.

onde:
n é o número de congruências que formarão o sistema;
a_n, m_n são os números que compõe as congruências;

Na Figura 1 é apresentado o fluxograma que ilustra as etapas dos cálculos que serão realizados.

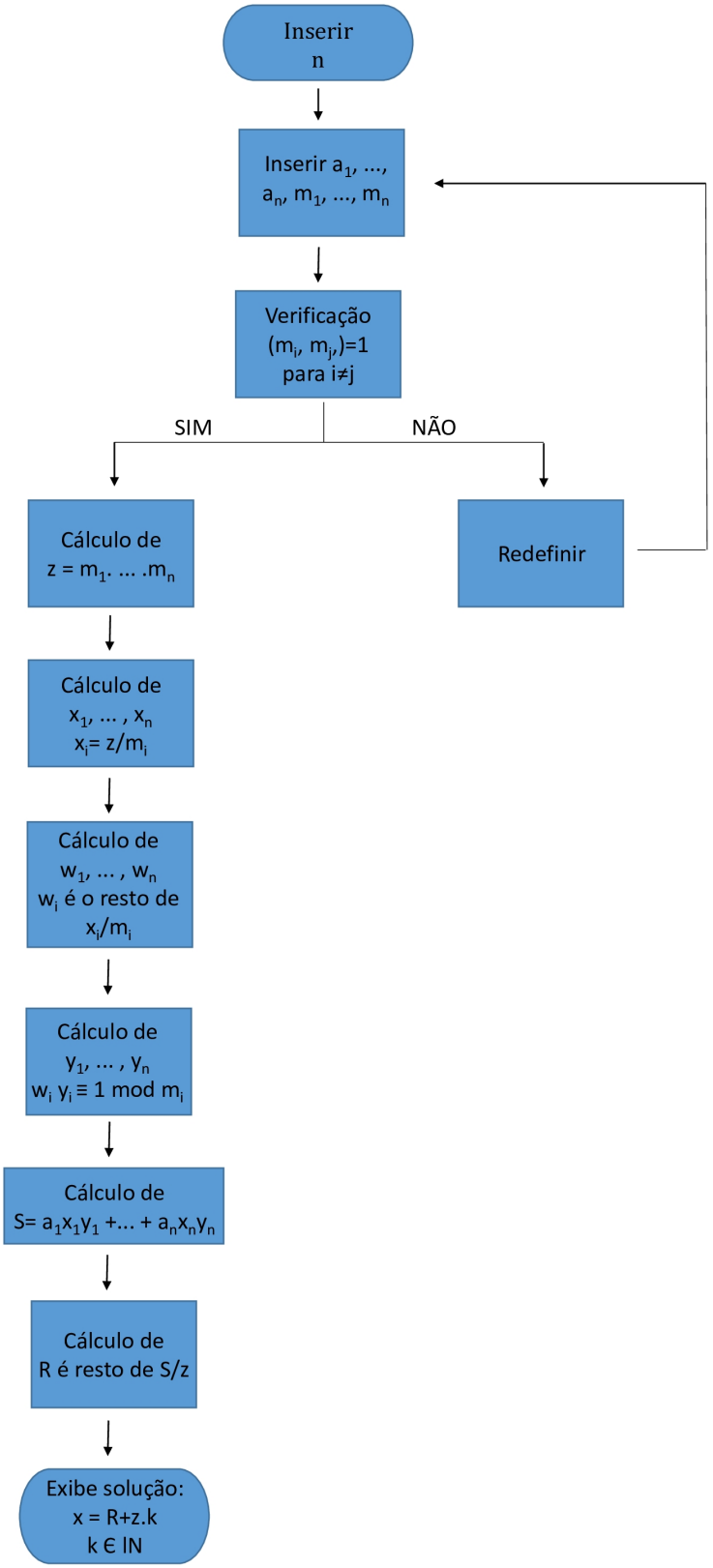

Figura 1 – Fluxograma para resolução de sistemas de congruências pelo Teorema Chinês dos Restos

7 Aplicações com uso de software

Neste trabalho, propõe-se implementar o algoritmo explanado no capítulo anterior em linguagem C de computação, a fim de se obter um programa com extensão .exe que gere, além do resultado, um arquivo de texto com as etapas de cálculo. É importante mencionar que o programa foi executado em computador com sistema operacional windows 7 ultimate de 64 bits.

O referido arquivo de texto aparecerá automaticamente no computador do usuário, após o encerramento do programa, dentro da mesma pasta onde o ele está salvo, e estará nomeado da seguinte forma: "Resultados TCR". A cada exercício que se for resolvendo, o arquivo será sobrescrito com os novos resultados.

No presente capítulo, o programa será submetido à resolução de exemplos e os produtos de cada um deles (resultado e arquivos de texto) estarão expostos a seguir.

Refazendo o Exemplo 33 no programa, observam-se os seguintes resultados, conforme ilustrado nas figuras a seguir.

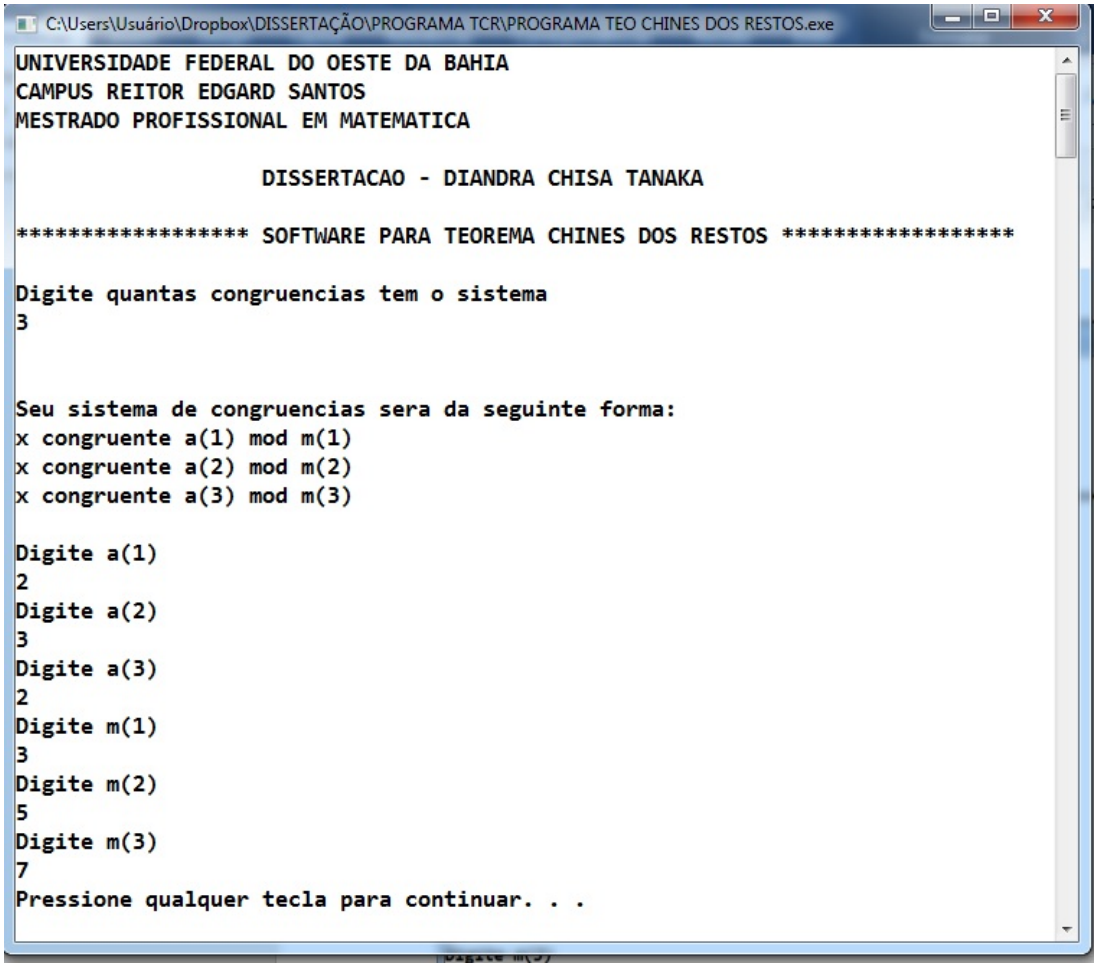

Figura 2 – Captura de tela do programa para resolução do Exemplo 33 (Parte 1)

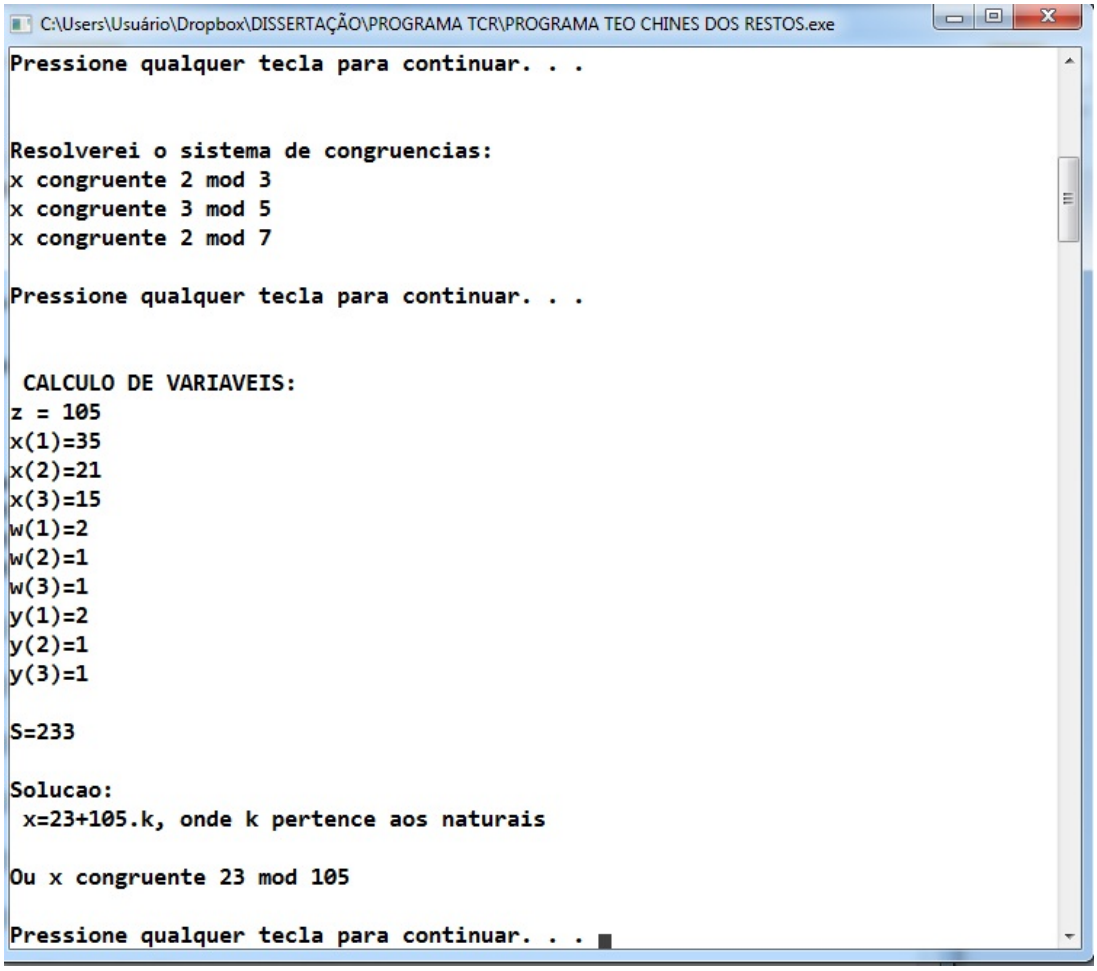

Figura 3 – Captura de tela do programa para resolução do Exemplo 33 (Parte 2)

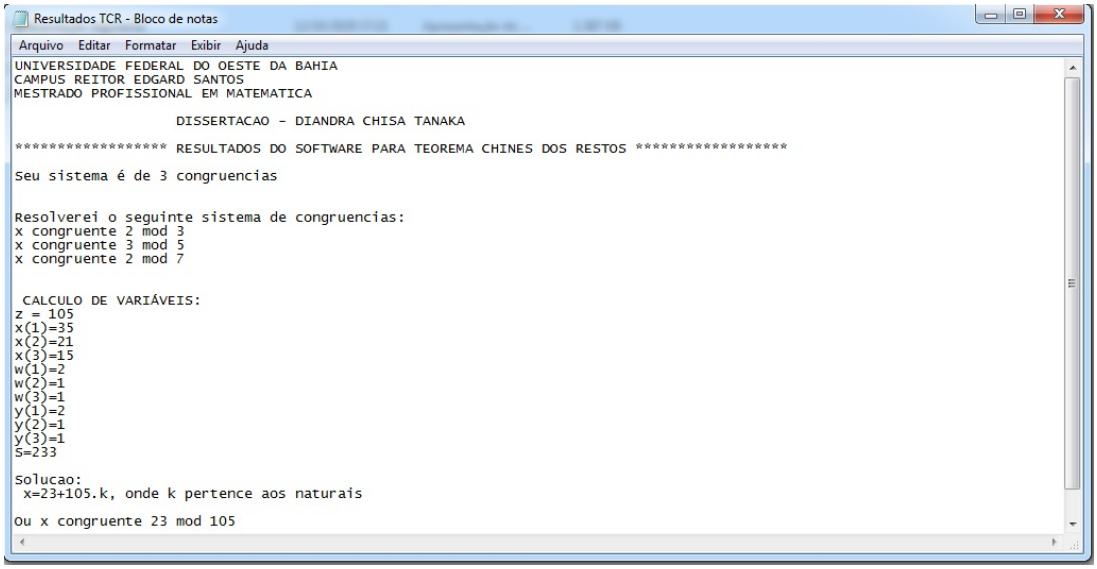

Figura 4 – Captura de tela arquivo de texto gerado para resolução do Exemplo 33

Nota-se que os resultados obtidos foram os mesmos de quando o problema foi resolvido de forma manual, embora, agora, em poucos segundos.

Os próximos exemplos de sistemas de congruências foram extraídos da lista de exercícios do site do Portal da OBMEP, no módulo referente a Teorema Chinês dos Restos.

Exemplo 35. *Encontre as soluções do sistema:*

$$X \equiv 1 \ mod\ 3$$
$$X \equiv 2 \ mod\ 5$$
$$X \equiv 3 \ mod\ 7$$

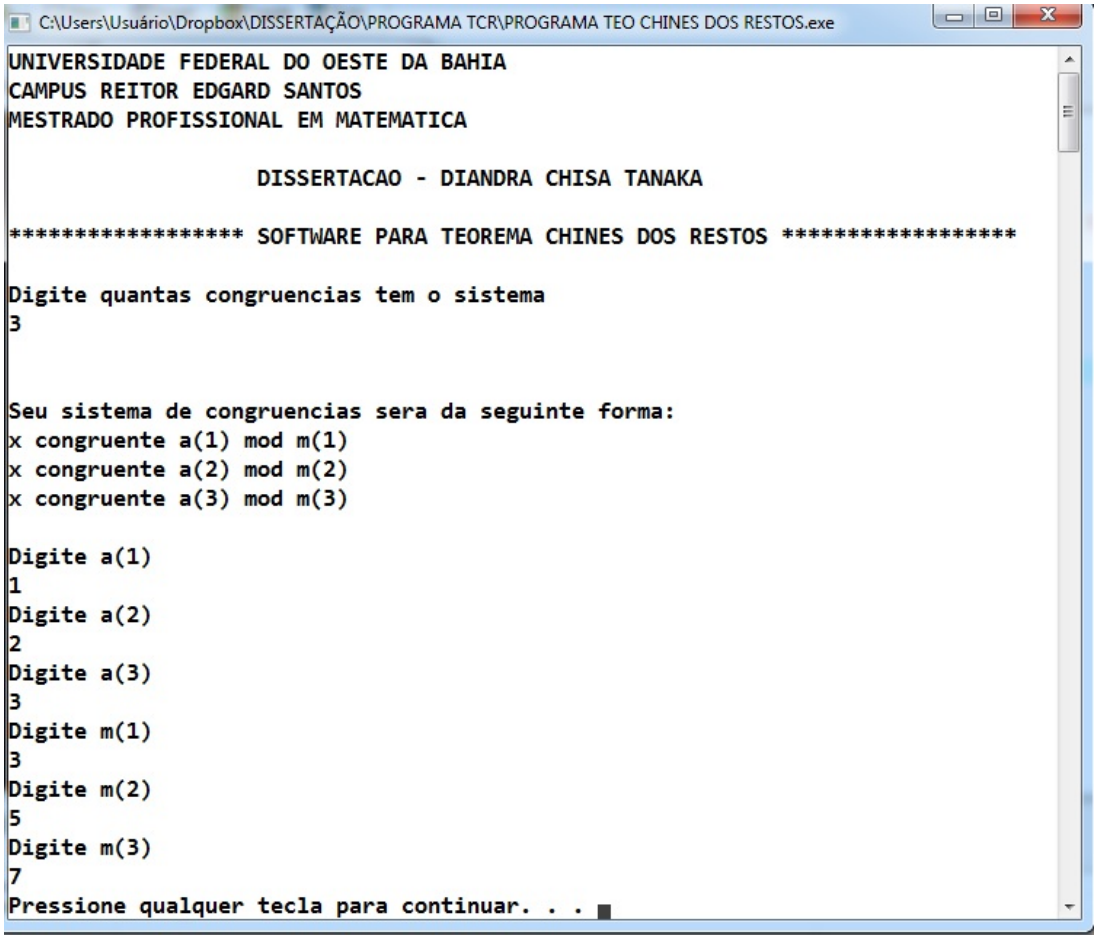

Figura 5 – Captura de tela do programa para resolução do Exemplo 35 (Parte 1)

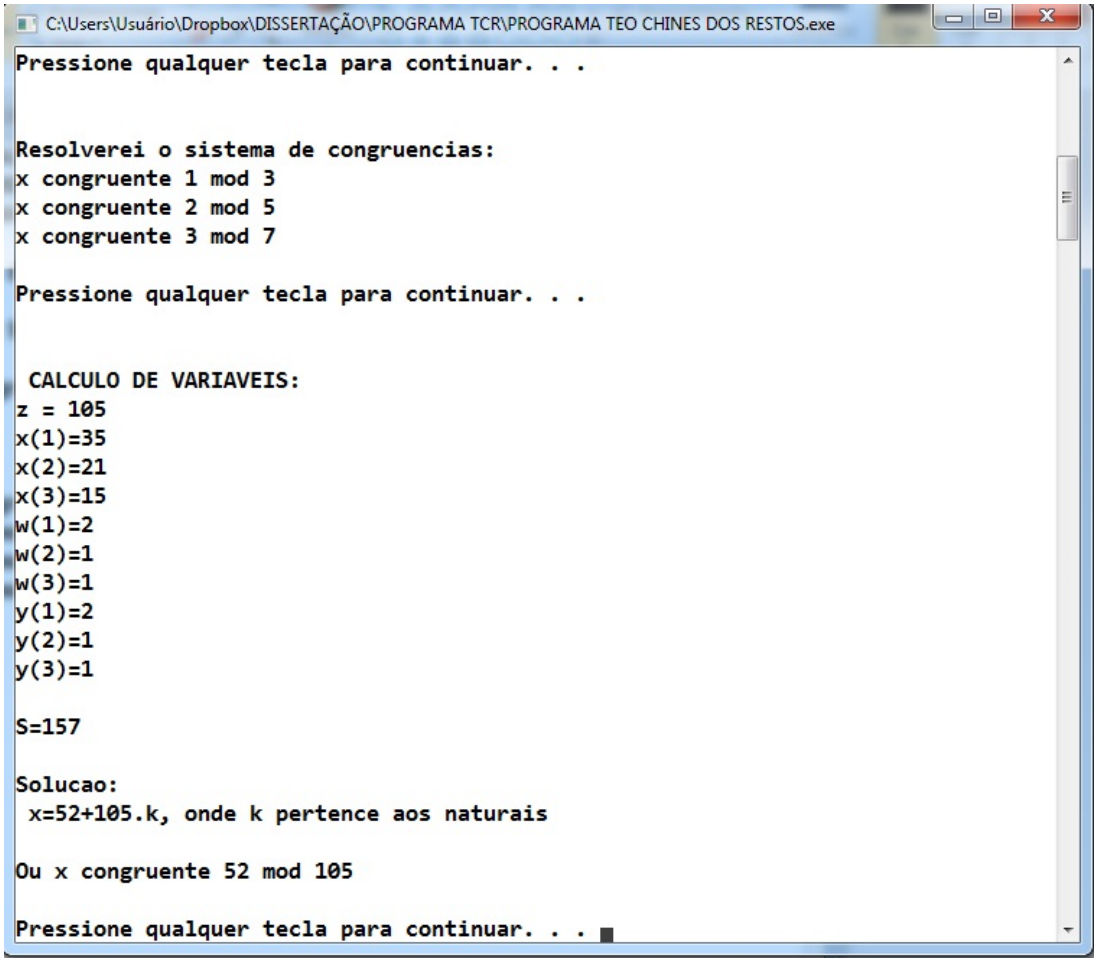

Figura 6 – Captura de tela do programa para resolução do Exemplo 35 (Parte 2)

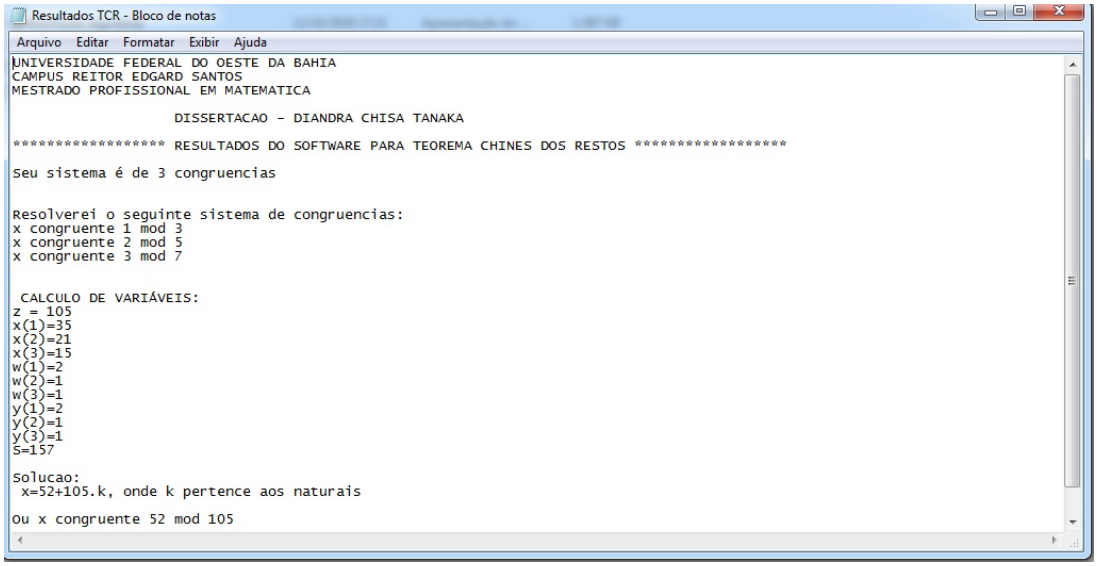

Figura 7 – Captura de tela arquivo de texto gerado para resolução do Exemplo 35

Exemplo 36. *Encontre as soluções do sistema:*

$$X \equiv 1 \ mod \ 3$$

$$X \equiv 2 \ mod \ 5$$
$$X \equiv 3 \ mod \ 11$$

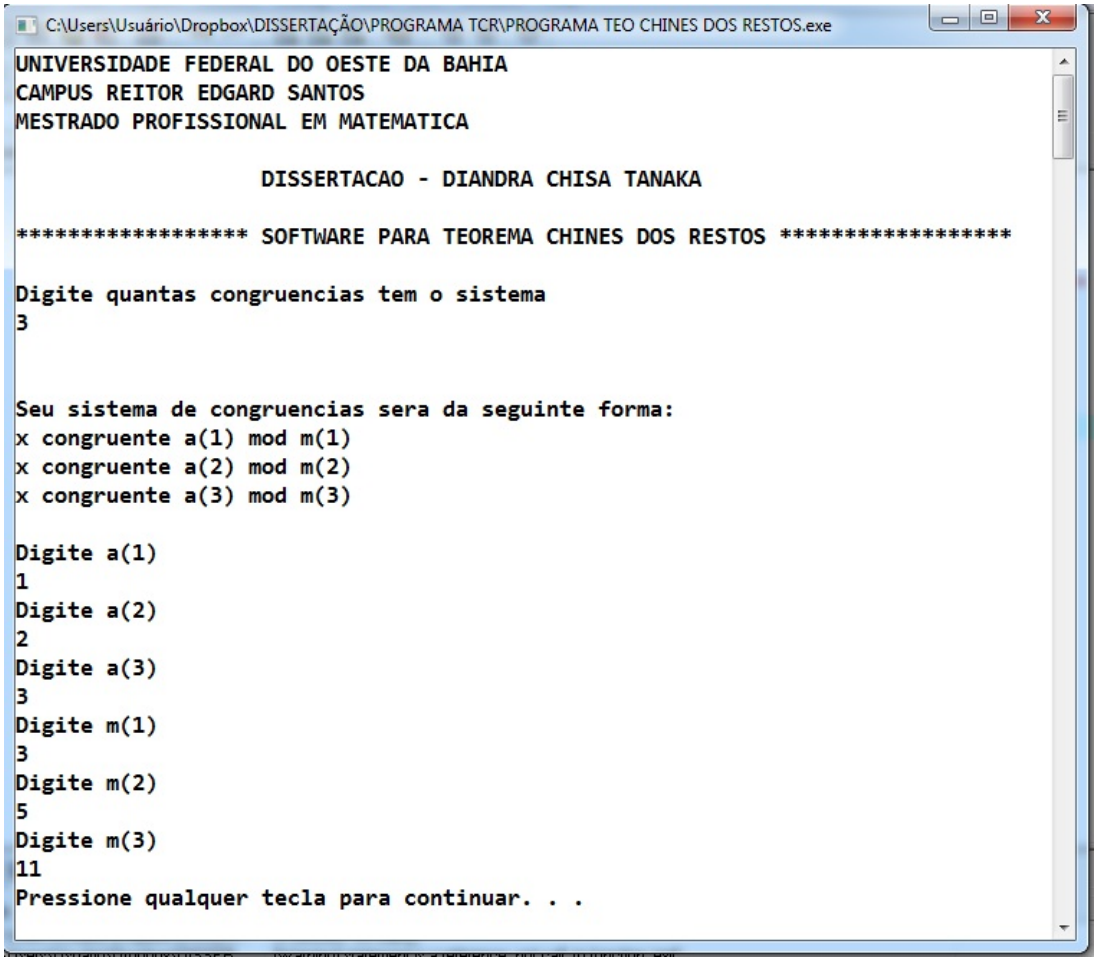

Figura 8 – Captura de tela do programa para resolução do Exemplo 36 (Parte 1)

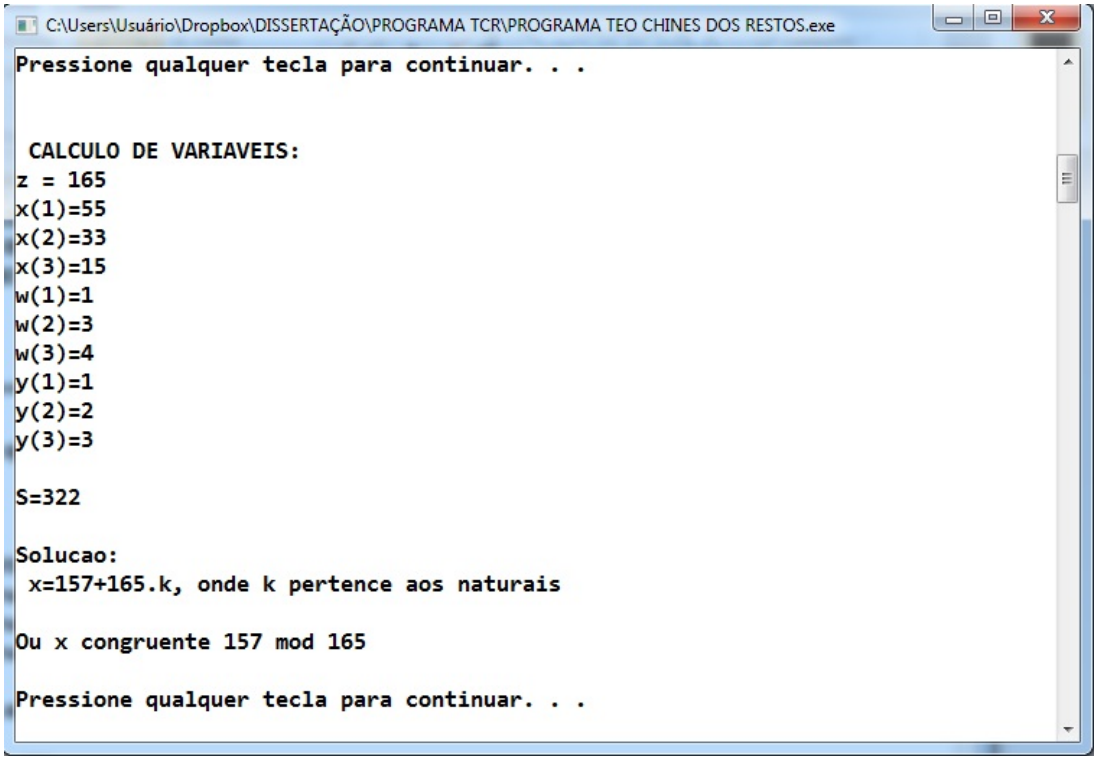

Figura 9 – Captura de tela do programa para resolução do Exemplo 36 (Parte 2)

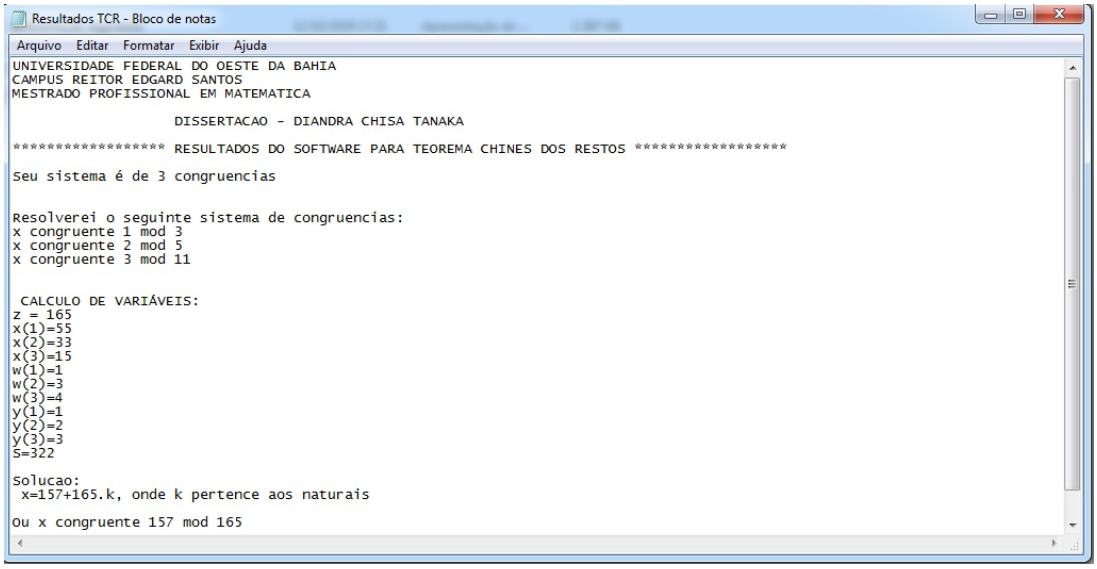

Figura 10 – Captura de tela arquivo de texto gerado para resolução do Exemplo 36

Exemplo 37. *Encontre as soluções do sistema:*

$$X \equiv 2 \ mod \ 10$$
$$X \equiv 7 \ mod \ 11$$
$$X \equiv 5 \ mod \ 13$$

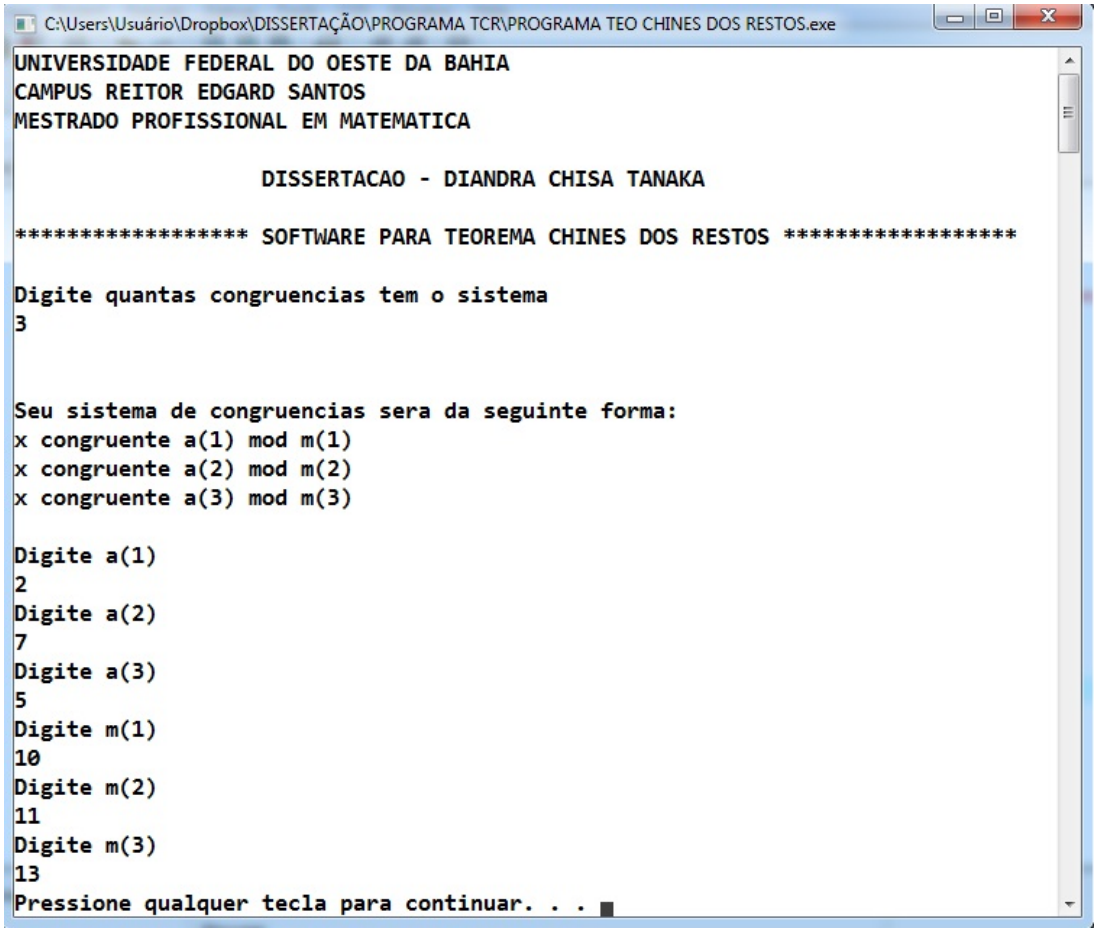

Figura 11 – Captura de tela do programa para resolução do Exemplo 37 (Parte 1)

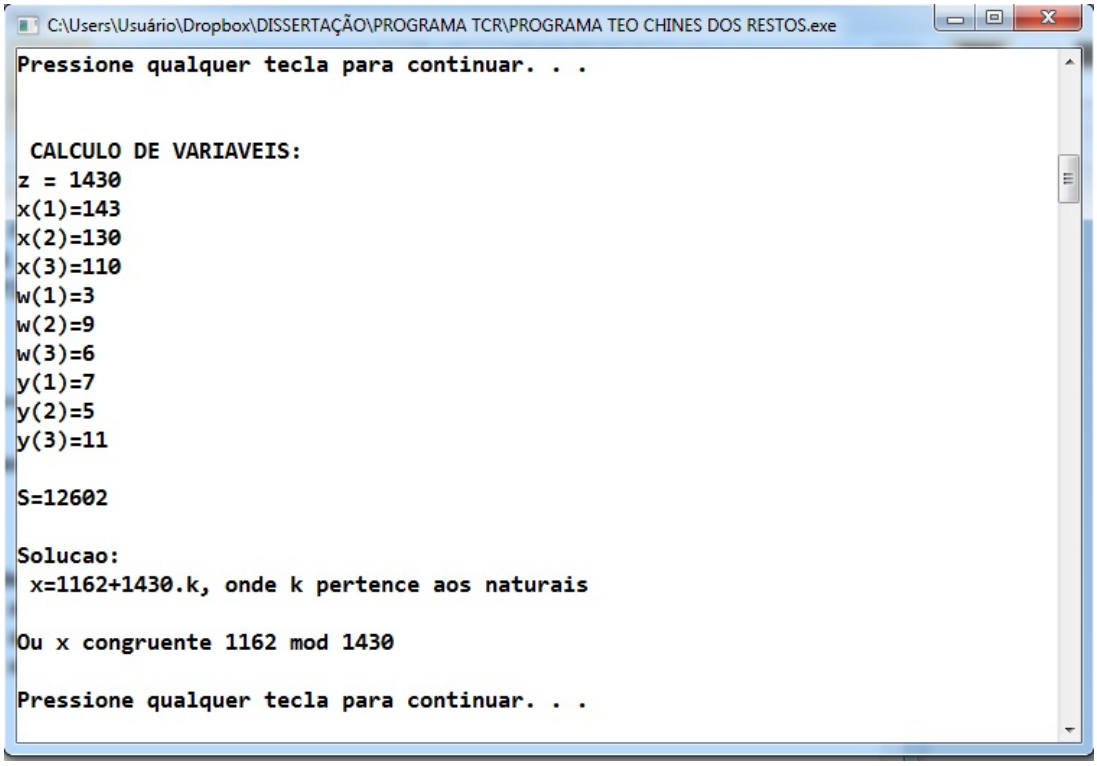

Figura 12 – Captura de tela do programa para resolução do Exemplo 37 (Parte 2)

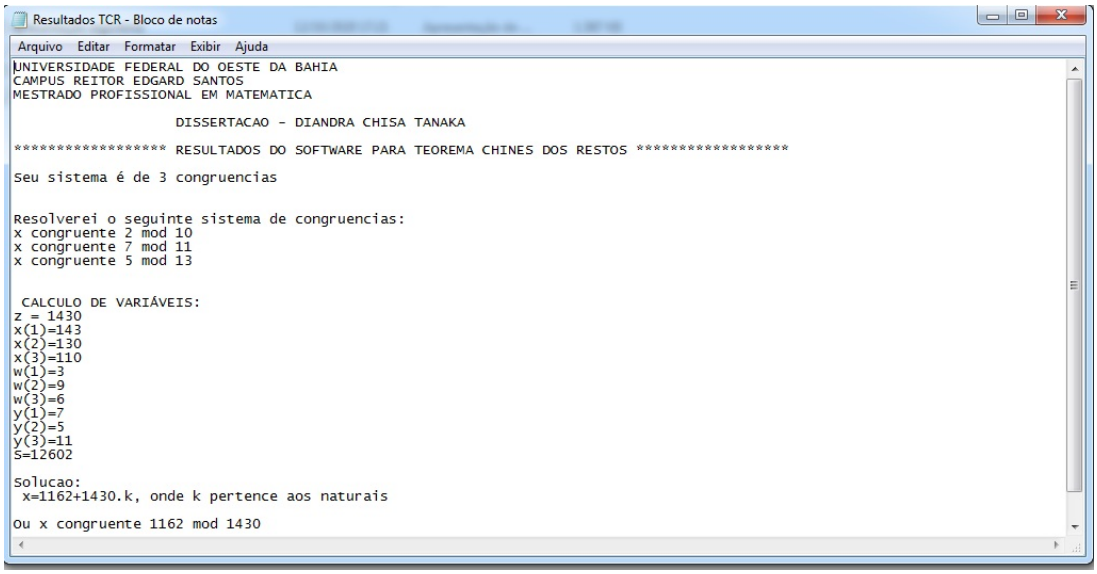

Figura 13 – Captura de tela arquivo de texto gerado para resolução do Exemplo 37

Após conferência, percebe-se que o programa forneceu todos os resultados de forma correta. É válido ressaltar que, durante todos os processos de resolução, há a verificação pelo próprio programa da condição imposta no Teorema Chinês dos Restos, de que os números atribuídos a m_i tem de ser primos entre si. Caso os números não atendam à condição, é solicitado ao usuário que digite novamente os dados do sistema de congruências. Para demonstrar, será feito o teste com o Exemplo 38:

Exemplo 38. *Encontre as soluções do sistema:*

$$X \equiv 2 \ mod \ 12$$
$$X \equiv 7 \ mod \ 8$$
$$X \equiv 5 \ mod \ 13$$

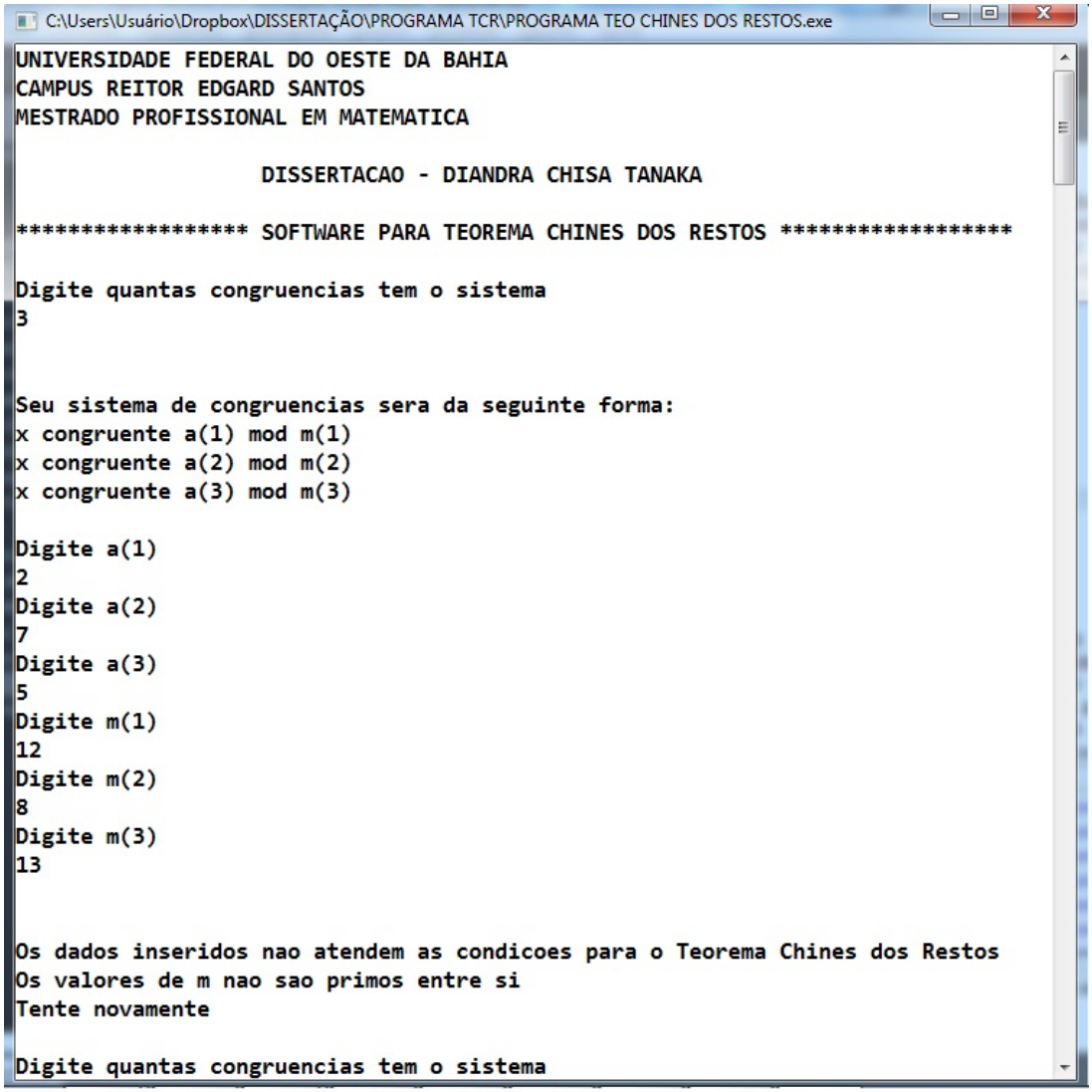

Figura 14 – Captura de tela do programa para Exemplo 38

Fica demonstrado que o programa faz as verificações relativas ao Teorema Chinês dos Restos e que, caso os dados inseridos não se enquadrem, é solicitado que o usuário digite novamente.

O programa fica disponível para download clicando abaixo:

Programa Teorema Chinês dos Restos

8 Conclusões

O algoritmo proposto neste trabalho foi eficiente na sua implementação, originando um programa que resolveu corretamente sistemas de congruências. Como produto da utilização do programa, é gerado automaticamente um arquivo de texto com o registro do resultado de cada variável, além do resultado final.

É disparadamente maior o tempo gasto para resolver manualmente questões desse tipo, quando se compara com o programa elaborado, visto que, em poucos segundos o resultado já é exibido na tela do usuário. Isso pode tornar a didática para este conteúdo mais dinâmica, agregando mais uma ferramenta de ensino para o professsor.

Considerando a progressiva utilização de tecnologias em sala de aula, o mesmo algoritmo pode ser traduzido para outras linguagens de programação, como as que atendem aplicativos para celulares ou tablets, tornando-se ainda mais acessível e atrativo para todos os públicos.

É importante salientar que é imprescindível lapidar no estudante a capacidade de interpretação dos problemas e o discernimento para determinar qual a estratégia será aplicada, a fim de resolver dos problemas de matemática. Novas ferramentas, como softwares, vem para agregar o processo de aprendizagem, contribuindo para interação entre aluno e professor.

Referências

[1] BATISTA JÚNIOR, Claudenildo Castro **O Teorema Chinês dos Restos: uma abordagem voltada para olimpíadas de Matemática com aplicações em Criptografia RSA**. 81f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade Federal Rural de Pernambuco, Recife, 2020. 9

[2] BOMFIM, Luciane Souza **Subsunçores para Resolução de Problemas de Divisão de Números Inteiros: o Caso do Teorema Chinês do Resto**. 35f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade Estadual de Maringá, Maringá, 2021. 9

[3] CHANG, I-Chen. **The ancient Chinese pearl in number theory: the Chinese remainder theorem**. International Journal of Mathematical Education and Science Technology, Vol. 11, No. 4, p. 545-556, 1980. 11

[4] CORMEN, Thomas H et al. **Algoritmos: teoria e prática**. 239 p. Rio de Janeiro: Elsevier, 2002. 19

[5] GLÓRIA, Walace da Silva. **Teorema Chinês dos Restos: Ensino e Aplicações**. 72f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade Federal do Amazonas, Manaus, 2019. 9, 42

[6] HEFEZ, Abramo. **Aritmética**. 298 p. Rio de Janeiro: SBM, 2016. 24, 33, 38

[7] MATKOVIC, David J. **The Chinese Remainder Theorem: A Historical Account**. Pi Mu Epsilon Journal, Vol. 8, No. 8, p. 493-502, 1988. 12

[8] NASCIMENTO, Adriano Sales **Teorema Chinês do Resto: Sua aplicação no ensino médio**. 63f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade Federal do Mato Grosso, Cuiabá, 2014. 9

[9] PRAZERES, Sidmar Bezerra dos **O Teorema Chinês dos Restos e a Partilha de Senhas**. 71f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade Federal Rural de Pernambuco, Recife, 2014. 9

[10] SANTOS, Audemir dos **Teorema Chinês dos Restos e Aplicações**. 79f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade Federal do Amazonas, Manaus, 2017. 9

[11] SOUTO FILHO, Antônio Luís de **O Teorema Chinês dos Restos**. 37f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade Federal do Maranhão, São Luís, 2015. 9