INSTITUTO FEDERAL DA PARAÍBA
CAMPUS CAJAZEIRAS
CURSO DE LICENCIATURA EM MATEMÁTICA

Marcos Lopes de Farias

DÍGITOS VERIFICADORES: ARITMÉTICA MODULAR E TEORIA DOS GRUPOS APLICADAS À DETECÇÃO DE ERROS EM SISTEMAS NUMÉRICOS COTIDIANOS

CAJAZEIRAS

2024

MARCOS LOPES DE FARIAS

DÍGITOS VERIFICADORES: ARITMÉTICA MODULAR E TEORIA DOS GRUPOS APLICADAS À DETECÇÃO DE ERROS EM SISTEMAS NUMÉRICOS COTIDIANOS

Monografia apresentada junto ao **Curso de Licenciatura em Matemática** do **Instituto Federal da Paraíba**, como requisito à obtenção do título de **Licenciado em Matemática**.

Orientador:

Prof. Dr. Vinicius Martins Teodósio Rocha

Cajazeiras

2024

MARCOS LOPES DE FARIAS

DÍGITOS VERIFICADORES: ARITMÉTICA MODULAR E TEORIA DOS GRUPOS APLICADAS À DETECÇÃO DE ERROS EM SISTEMAS NUMÉRICOS COTIDIANOS

Monografia apresentada ao programa de **Curso de Licenciatura em Matemática** do **Instituto Federal da Paraíba**, como requisito à obtenção do título de **Licenciado em Matemática**.

Data de aprovação: 09/10/2024

Banca Examinadora:

Documento assinado digitalmente
gov.br VINICIUS MARTINS TEODOSIO ROCHA
Data: 11/10/2024 08:37:25-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Vinicius Martins Teodósio Rocha
Instituto Federal da Paraíba - IFPB

Documento assinado digitalmente
gov.br MARCIO ALISSON LEANDRO COSTA
Data: 10/10/2024 14:29:14-0300
Verifique em https://validar.iti.gov.br

Prof(a). Me. Marcio Alisson Leandro Costa
Instituto Federal da Paraíba - IFPB

Documento assinado digitalmente
gov.br NIWLANDES DE FARIAS ARAUJO
Data: 11/10/2024 12:04:46-0300
Verifique em https://validar.iti.gov.br

Prof(a). Me. Niwlandes de Farias Araújo
ECI EST EM Otaviano L da Silva

IFPB / Campus Cajazeiras
Coordenação de Biblioteca
Biblioteca Prof. Ribamar da Silva
Catalogação na fonte: Cícero Luciano Félix CRB-15/750

F224d Farias, Marcos Lopes de.
Dígitos verificadores : aritmética modular e teoria dos grupos aplicadas à detecção de erros em sistemas numéricos cotidianos / Marcos Lopes de Farias. – 2024.
67f. : il.

Trabalho de Conclusão de Curso (Licenciatura em Matemática) - Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, Cajazeiras, 2024.

Orientador(a): Prof. Dr. Vinicius Martins Teodósio Rocha.

1. Dígitos verificadores. 2. Aritmética modular. 3. Teoria dos grupos. 4. Sistema numérico. I. Instituto Federal de Educação, Ciência e Tecnologia da Paraíba. II. Título.

IFPB/CZ CDU: 51(043.2)

Dedico este trabalho à minha família, pelo apoio incondicional e pelo incentivo constante durante toda minha jornada acadêmica. Aos amigos, pela compreensão nos momentos mais difíceis e por estarem sempre ao meu lado. E, finalmente, a todos os professores que me inspiraram e me guiaram durante esse caminho.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, pela saúde e força para concluir essa etapa da minha vida.

Aos professores do curso de Licenciatura em Matemática do IFPB, que me proporcionaram uma formação sólida e inspiradora. Cada ensinamento contribuiu para o meu crescimento acadêmico e pessoal.

À minha família, especialmente a minha mãe e a minha avó, pelo carinho, suporte e por sempre acreditarem nos meus sonhos. Sem o amor e incentivo de vocês, essa conquista não seria possível.

Por fim, a todos que, direta ou indiretamente, contribuíram para a realização deste trabalho. Minha gratidão eterna a cada um.

"A matemática é o alfabeto com o qual Deus escreveu o universo."

Galileu Galilei

RESUMO

Este trabalho aborda a aplicação de dígitos verificadores em sistemas numéricos cotidianos, utilizando conceitos de aritmética modular e teoria dos grupos para detecção de erros. A pesquisa examina como esses métodos matemáticos são empregados em diversos contextos, como em CPF, ISBN, cartões de crédito e códigos de barras, com o objetivo de garantir a confiabilidade das informações. São explorados os métodos de Verhoeff, Damm e os tradicionais módulo 10 e módulo 11, destacando suas diferentes abordagens na correção de erros de transposição, digitação e outras falhas comuns em sistemas numéricos. O estudo também avalia a eficácia de cada método em termos de complexidade, praticidade e precisão, mostrando que, enquanto a aritmética modular oferece simplicidade, os algoritmos baseados em teoria dos grupos proporcionam maior robustez e segurança em sistemas críticos.

Palavras-chave: dígitos verificadores, aritmética modular, teoria dos grupos, detecção de erros, sistemas numéricos.

ABSTRACT

This work addresses the application of check digits in everyday numerical systems, using concepts of modular arithmetic and group theory for error detection. The research examines how these mathematical methods are employed in various contexts, such as in CPF, ISBN, credit cards and barcodes, with the aim of ensuring the reliability of the information. Verhoeff's and Damm's methods are explored, as well as the traditional module 10 and module 11, highlighting their different approaches to correcting transposition errors, typing, and other common flaws in number systems. The study also evaluates the effectiveness of each method in terms of complexity, practicality, and accuracy, showing that while modular arithmetic offers simplicity, algorithms based on group theory provide greater robustness and safety in critical systems.

Keywords: check digits, modular arithmetic, group theory, error detection, numerical systems.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ISBN	International Book Number
CPF	Cadastro de Pessoa Física
DF	Distrito Federal
GO	Goiás
MS	Mato Grosso do Sul
MT	Mato Grosso
TO	Tocantins
AC	Acre
AM	Amazonas
AP	Amapá
PA	Pará
RO	Rondônia
RR	Roraima
CE	Ceará
MA	Maranhão
PI	Piauí
AL	Alagoas
PB	Paraíba
PE	Pernambuco
RN	Rio Grande do Norte
BA	Bahia
SE	Sergipe
MG	Minas Gerais
ES	Espírito Santo
RJ	Rio de Janeiro
SP	São Paulo
PR	Paraná
SC	Santa Catarina
RS	Rio Grande do Sul
TSE	Tribunal Superior Eleitoral

LISTA DE SÍMBOLOS

$\mid$	Divide
$\nmid$	Não Divide
$<$	Menor
$>$	Maior
$\leq$	Menor ou igual
$\geq$	Maior ou igual
$\Longleftrightarrow$	Se e somente se
$\Longrightarrow$	Implica
$\cap$	Intersecção
$=$	Igual
$\mathbb{Z}$	Conjunto dos números inteiros
$\in$	Pertence
$\equiv$	Congruente
$\not\equiv$	Incongruente
$\neq$	Diferente
(a, b)	mdc entre a e b

SUMÁRIO

1 INTRODUÇÃO

A relação entre matemática e tecnologia é conhecida antes mesmo do surgimento do primeiro computador.

Mas desde a utilização em massa de dados por meio das redes têm-se buscado métodos para tornar seguro e confiável o uso das informações digitais. Os dígitos verificadores surgiram para esta finalidade como caracteres numéricos adicionados a um número principal ou código para tornar possível verificar rápida e corretamente a precisão dos dados. Segundo (HEFEZ; VILLELA, 2017), eles participam do nosso cotidiano de diversas formas, estando presente, por exemplo, quando fazemos uso de informações digitalizadas como CPF, Código de Barras de produtos, Título de eleitor e outros.

Tendo sido projetados para utilizar conceitos matemáticos para fins práticos, com a utilização de operações aritméticas e teoria dos números, é possível, por meio dos dígitos verificadores, detectar erros na digitação, na transposição de números e até mesmo possíveis falsificações. Estando eles, assim, presentes em aspectos da nossa vida digital, têm o propósito de promover melhorias e segurança nas informações que necessitam de confiabilidade em sua utilização e transmissão.

Foi visando a isso que, ainda nas décadas de 1950 e 1960, o matemático holandês Jacobus Koss Verhoeff (VERHOEFF, 1975) se destacou por desenvolver, em sua tese de doutorado, um estudo sobre o tema. Naquela época, a presença do computador e o enorme volume de dados não eram considerados tão importantes e gigantescos como na atualidade. Em sua pesquisa, com cerca de 12.000 erros, ele categorizou os erros cometidos, elencando os principais tipos existentes na transmissão de dados, bem como sua frequência, proporcionando uma base sólida para entender a importância dos dígitos verificadores como resposta.

Tabela 1.1 – Tipos e frequências de erros segundo Verhoeff

Tipo de erro	**Formato**	**Frequência em %**
Erros Individualizados	..a..→..b..	79,10
Transposição Adjacente	..ab..→..ba..	10,20
Transposição Alternada	..abc..→..cba..	0,80
Gêmeos Adjacentes	..aa..→..bb..	0,50
Gêmeos Alternados	..aca..→..bcb..	0,30
Fonéticos	..1a..→..a0..,a>1	0,50
Outros		8,60

Esse estudo foi fundamental para a inovação de métodos como o do próprio holandês no mesmo trabalho chamado de Algoritmo de Verhoeff e posteriormente o algoritmo de Damm.

A importância de métodos como esses se torna ainda mais evidente em um mundo onde o tempo é um recurso escasso e as distrações são constantes, especialmente nas tarefas cotidianas, em que as pessoas realizam atividades nos computadores que envolvem muitos números, como compras, transações bancárias, votações e registros de documentos.

Segundo (GOULART, 2023), ao usar um aparelho como o computador há uma interação entre o equipamento e a pessoa e essa interação está próxima da existente entre duas pessoas sendo importante levar em consideração os aspectos humanos como limitações e erros.

Diante desse cenário, este trabalho tem como objetivo analisar e demonstrar a importância dos dígitos verificadores na detecção de erros em sistemas de numeração, destacando suas aplicações práticas em diferentes contextos e a fundamentação matemática por trás dos principais algoritmos utilizados. Para isso, é explicado o funcionamento dos métodos mais comuns como o que faz uso da aritmética modular e os algoritmos de Damm e de Verhoeff com uma abordagem detalhada sobre sua fundamentação matemática, demonstrado, por meio de exemplos práticos, a aplicação dos dígitos verificadores em sistemas de numeração como ISBN, CPF, Título de Eleitor e códigos de barras e avaliada a eficácia dos diferentes algoritmos de dígitos verificadores na detecção de erros comuns, e de transposição de dígitos adjacente presentes na digitação.

A organização deste trabalho é descrita a seguir. No Capítulo 1, lembramos subsídios teóricos necessários para que o leitor compreenda alguns resultados posteriormente apresentados a respeito dos dígitos verificadores. São utizadas como referências principalmente as obras (SANTOS, 2020), (YARTEY, 2017), (SAVóIS, 2014), (SOUZA, 2015), (LIMA, 2011) e (CANçADO, 2016). No capítulo 2, destacamos a importância dos dígitos verificadores através de exemplos práticos como o código de barras e o CPF apresentando também métodos diferentes como o algoritmo de Verhoeff e o de Damm utilizados para garantia da integridade das informações. Demonstramos, neste capítulo também, como cada método funciona e quais conceitos matemáticos são usados para cada caso. No capítulo 3, analisamos a capacidade dos métodos que utilizam a aritmética modular, o algoritmo de Verhoeff e o de Damm frente aos principais tipos de erros como os erros simples e os de transposição adjacente e sob quais condições esses erros são ou

não detectáveis.

2 CONCEITOS PRELIMINARES

Neste capítulo são apresentados conceitos algébricos preliminares e algumas demonstrações necessários para o embasamento das próximas partes a respeito dos dígitos verificadores. Para isto, tomaremos como base teórica (SANTOS, 2020), (YARTEY, 2017), (SAVóIS, 2014), (SOUZA, 2015), (LIMA, 2011) e (CANçADO, 2016).

2.1 DIVISIBILIDADE

Através da definição formal de divisibilidade entre números inteiros, veremos como um número pode ser expresso como múltiplo de outro. Além disso, nesta seção, serão apresentadas proposições fundamentais, como a transitividade da divisibilidade. Os resultados aqui expostos serão de imensa ajuda para construção dos demais como a compreensão do Algoritmo da Divisão.

Definição 1. *Dados dois números inteiros a e b, dizemos que a divide b se exite um c inteiro tal que $b = a \cdot c$. denotaremos por $a|b$.*

Definição 2. *Caso o contrário aconteça, ou seja, a não divida b, denotaremos por $a \nmid b$.*

Proposição 1. *Se a, b e c são inteiros, $a|b$ e $b|c$, então $a|c$.*

Demonstração. Como $a|b$ e $b|c$, existem inteiros k_1 e k_2 tais que $b = k_1 a$ e $c = k_2 b$. Substituindo o valor de b na equação $c = k_2 b$ teremos $c = k_2 k_1 a$ o que implica $a|c$. □

Exemplo 1. *Como $3|12$ e $12|48$, então $3|48$. Como não existem inteiros c satisfazendo $15 = 4c$, então $4 \nmid 15$.*

Proposição 2. *Se $a|b$ e $a|c$, então $a|(xb+yc)$, para todo $x, y \in \mathbb{Z}$.*

Demonstração. Se $a|b$ e $a|c$, então existem $m, n \in \mathbb{Z}$, tais que $b = ma$ e $c = na$, dessa forma, para todo $x, y \in \mathbb{Z}$, temos $xb + yc = x(ma) + y(na) = a(xm + yn)$. Como $xm + yn \in \mathbb{Z}$ segue que $a|xb + yc$. □

2.2 TEOREMA DE EUDOXIUS

O Teorema de Eudoxius estabelece uma importante relação entre inteiros e seus múltiplos. Este Teorema afirma que, dado um número inteiro e um divisor positivo, esse número será múltiplo desse divisor ou estará entre dois múltiplos consecutivos. Essa propriedade é fundamental para compreender a estrutura dos números inteiros, sendo uma ferramenta chave na análise de divisibilidade.

Teorema 1. *Dados a e b inteiros, com $b>0$, então a é múltiplo de b ou está localizado entre dois múltiplos consecutivos de b. De outro modo, dados a e b inteiros, com $b>0$, então existe q inteiro tal que*

$$bq \leq a < b(q+1).$$

Demonstração. Suponha que $a \geq 0$ (o caso $a<0$ pode ser tratado de forma análoga) e considere o número racional $\frac{a}{b}$.

O fato de o conjunto dos números naturais ser ilimitado superiormente assegura a existência de um natural maior que $\frac{a}{b}$. Dentre todos esses naturais, há um o qual é o menor possível, chame-o de n. Então, $\frac{a}{b} < n$ é verdade, mas a minimalidade de n garante que $\frac{a}{b} < n-1$ é falso. Dessa forma, $\frac{a}{b} \geq n-1$, de modo que

$$n-1 \leq \frac{a}{b} < n.$$

Chamando $n-1$ de q, temos $n = q+1$. Assim,

$$q \leq \frac{a}{b} < q+1,$$

e multiplicando as desigualdades acima por b, obtemos:

$$bq \leq a < b(q+1).$$

□

2.3 ALGORITMO DA DIVISÃO

O Algoritmo da Divisão é um dos resultados mais fundamentais da aritmética. Sendo assim, os resultados aqui apresentados têm propriedades centrais para muitas operações em teoria dos números e cálculos relacionados à divisibilidade que veremos a seguir.

Teorema 2. *Dados dois inteiros a e b, $b>0$, existe um par único de inteiros q e r tais que*

$$a = qb + r, \ com\ 0 \leq r < b \qquad (r = 0 \iff b|a)$$

(q é chamado de quociente e r de resto da divisão de a por b)

Demonstração. Pelo Teorema de Eudoxius, como $a > b$, existe q tal que: $qb \leq a < (q+1)b$ o que implica $0 \leq a - qb$ e $a - qb < b$. Desta forma, se definirmos $r = a - qb$, teremos, garantida, a existencia de q e r. A fim de mostrarmos a unicidade vamos supor a existência de outro par de números q_1 e r_1 verificando:

$$a = q_1 b + r_1 \text{ com } 0 \leq r_1 < b.$$

Disto temos que $(qb+r) - (q_1 b + r_1) = 0$ implica $b(q - q_1) = r_1 - r$, o que acarreta $b|(r_1 - r)$. Mas, como $r_1 < b$ e $r < b$, temos $|r_1 - r| < b$ e, portanto, como $b|(r_1 - r)$ devemos ter $r_1 - r = 0$ o que implica $r = r_1$. Logo $q_1 b = qb$ nos diz que $q_1 = q$ uma vez que $b \neq 0$. □

2.4 MÁXIMO DIVISOR COMUM (MDC)

Máximo Divisor Comum (MDC) é o maior número inteiro que divide outros dois inteiros simultaneamente. O cálculo do MDC é importante para resolver equações diofantinas e garantir a divisibilidade de sistemas numéricos.

Definição 3. *O máximo divisor comum de dois inteiros a e b (a ou b diferentes de zero), denotado por (a,b), é o maior inteiro que divide a e b ao mesmo tempo.*

Exemplo 2. *Considere os números inteiros 5 e 15 e os conjuntos A e B como sendo os conjuntos dos divisores positivos de 5 e 15 respectivamente. $A = \{1;5\}$ e $B = \{1;3;5;15\}$ como $(5,15)$ é o maior inteiro que divide 5 e 15, isso equivale a dizer que $(5,15)$ é o maior inteiro pertencente à intersecção de A e B e denotaremos por $A \cap B$.*

Como $A \cap B = \{1,5\}$, $(5,15) = 5$.

2.5 NÚMEROS PRIMOS

Nesta parte, exploraremos a definição dos números primos juntamente com algumas das suas propriedades. Também abordaremos a ideia de coprimos, que são números inteiros cujo MDC é 1.

Definição 4. *Um número inteiro $n > 1$ possuindo somente dois divisores positivos, n e 1, é chamado primo.*

Definição 5. *Se $n > 1$ não é primo, dizemos que n é composto.*

Considerando a definição anterior acerca dos números primos, consideramos dois primos p_1 e p_2 e $n \in \mathbb{Z}$, disso ocorre que:

(1) Se $p_1|p_2$, então $p_1 = p_2$;

(2) Se $p_1 \nmid n$, então $(p_1, n) = 1$

Demonstração. 1. Se $p_1|p_2$, sendo p_2 primo, então $p_1 = 1$ ou $p_1 = p_2$. Como p_1 e p_2 são primos, por hipótese, temos que $p_1 > 1$. portanto $p_1 = p_2$.

2. Tome $(p_1, n) = t$, $t \in \mathbb{Z}$, segue que, pela Definição 3 e Exemplo 2, $t|p_1$ e $t|n$. Como p_1 é primo, segue que $t = 1$ ou $t = p_1$. Como temos, por hipótese $p_1 \nmid n$, segue que $t \neq p_1$. Portanto $t = 1$.

□

Definição 6. *Dizemos também que se $(a, b) = 1$, os números a e b são primos entre si ou diz-se apenas que a e b são coprimos.*

2.6 CONGRUÊNCIA

Nesta Seção, iremos definir os conceitos de Congruência e apresentar o Teorema de Bézout. Congruência é uma relação bastante conhecida na teoria dos números. Ela permite comparar números inteiros quanto ao seu comportamento em divisões por um número fixo chamado módulo. Através de exemplos e proposições, exploraremos as propriedades fundamentais de congruência módulo m.

O Teorema de Bézout afirma que o maior divisor comum de dois números inteiros pode ser expresso como uma combinação linear desses números. Este teorema é um resultado essencial para este trabalho, tendo várias aplicações especialmente na resolução de equações diofantinas e na análise de divisibilidade.

Definição 7. *Se a e b são inteiros dizemos que a é congruente a b módulo m $(m > 0)$ se $m|(a-b)$. Denotamos isto por $a \equiv b \pmod{m}$. Se $m \nmid (a-b)$ dizemos que a é incongruente a b módulo m e denotaremos por $a \not\equiv b \pmod{m}$.*

Exemplo 3. $11 \equiv 3 \pmod{2}$ *pois* $2|(11-3)$. *Como* $5 \nmid 6$ *e* $6 = 17-11$ *temos que* $17 \not\equiv 11 \pmod{5}$.

Proposição 3. *Se a e b são inteiros, temos que $a \equiv b \pmod{m}$ se, e somente se, existir um inteiro k tal que $a = b + km$.*

Demonstração. Sejam $a, b \in \mathbb{Z}$, $a \equiv b$ (mod m) implica que $m|(a-b)$, deste fato, pelo Teorema 2, segue que existe $k \in \mathbb{Z}$, tal que $a - b = km$, dessa maneira, $a = b + km$.

Sejam $a, b, k \in \mathbb{Z}$, tais que $a = b + km$, temos que $km = a - b$. Deste modo segue $a - b$ é um múltiplo de m, ou seja, $m|(a-b)$, então, pela Definição 7, $m|(a-b)$, concluimos que $a \equiv b \pmod{m}$. □

Proposição 4. *Se a, b, m e d são inteiros, $m > 0$, as seguintes sentenças são verdadeiras*

1. $a \equiv a \pmod{m}$*;*

2. Se $a \equiv b \pmod{m}$*, então* $b \equiv a \pmod{m}$*;*

3. Se $a \equiv b \pmod{m}$ *e* $b \equiv d \pmod{m}$*, então* $a \equiv d \pmod{m}$*.*

Demonstração. (1) Como $m|0$, então $m|(a-a)$, o que implica $a \equiv a \pmod{m}$.

(2) Se $a \equiv b \pmod{m}$, então $a = b + k_1 m$ para algum inteiro k_1. Logo $b = a + (-k_1)m$, o que implica, pela Proposição 3, $b \equiv a \pmod{m}$.

(3) Se $a \equiv b \pmod{m}$ e $b \equiv d \pmod{m}$, então existem inteiros k_1 e k_2 tais que $a - b = k_1 m$ e $b - d = k_2 m$. Somando-se, membro a membro, estas últimas equações, obtemos $a - d = (k_1 + k_2)m$, o que implica $a \equiv d \pmod{m}$. □

Proposição 5. *Sejam* $m \in \mathbb{Z}^+$ *e* $a, b, c, d \in \mathbb{Z}$ *tais que* $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$*, então*

1. $a + c \equiv b + d \pmod{m}$

2. $a \cdot c \equiv b \cdot d \pmod{m}$

3. $a - c \equiv b - d \pmod{m}$

Demonstração. (1) Dado que, por hipótese, $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, temos que $m|(a-b)$ e $m|(c-d)$. Dessa forma, pela Proposição 2, $m|(a-b)+(c-d) = (a+c)-(b+d)$. Portanto, $a + c \equiv b + d \pmod{m}$.

(2) Como, por hipótese, $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, segue que $m|(a-b)$ e $m|(c-d)$. Dai, $m|c(a-b)$ e $m|b(c-d)$. Dessa forma, $m|c(a-b)+b(c-d) = ac - bc + bc - bd$. Sendo assim, $m|ac - bd$, o que implica $ac \equiv bd \pmod{m}$.

(3) Pela Proposição 4, sabemos que $a \equiv a \pmod{m}$. Em particular, isso implica que $-1 \equiv -1 \pmod{m}$.

Agora, pela Proposição 5, caso (2), se $c \equiv d \pmod{m}$, então temos que

$$-1c \equiv -1d \pmod{m}, c, d \in \mathbb{Z}$$

ou seja,

$$-c \equiv -d \pmod{m}.$$

Finalmente, pela Proposição 5, caso (1), podemos adicionar a ambos os lados da congruência e obter:

$$a + (-c) \equiv b + (-d) \pmod{m}$$

o que equivale a:

$$a - c \equiv b - d \pmod{m}.$$

□

Proposição 6. *Sejam $m \in \mathbb{Z}^+$ e $a, b, c, d \in \mathbb{Z}$ tais que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então*

1. $a + c \equiv b + d \pmod{m}$

2. $a \cdot c \equiv b \cdot d \pmod{m}$

3. $a - c \equiv b - d \pmod{m}$

Demonstração. (1) Dado que, por hipótese, $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, temos que $m|(a-b)$ e $m|(c-d)$. Dessa forma, pela Proposição 2, $m|(a-b)+(c-d) = (a+c)-(b+d)$. Portanto, $a + c \equiv b + d \pmod{m}$.

(2) Como, por hipótese, $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, segue que $m|(a-b)$ e $m|(c-d)$. Dai, $m|c(a-b)$ e $m|b(c-d)$. Dessa forma, $m|c(a-b)+b(c-d) = ac-bc+bc-bd$. Sendo assim, $m|ac-bd$, o que implica $ac \equiv bd \pmod{m}$.

(3) Pela Proposição 4, sabemos que $a \equiv a \pmod{\text{m}}$. Em particular, isso implica que $-1 \equiv -1 \pmod{\text{m}}$.

Agora, pela Proposição 5, caso (2), se $c \equiv d \pmod{\text{m}}$, então temos que

$$-1c \equiv -1d \pmod{\text{m}}, c, d \in \mathbb{Z}$$

ou seja,

$$-c \equiv -d \pmod{m}.$$

Finalmente, pela Proposição 5, caso (1), podemos adicionar a ambos os lados da congruência e obter:

$$a+(-c) \equiv b+(-d) \pmod{m}$$

o que equivale a:

$$a-c \equiv b-d \pmod{m}.$$

□

Definição 8. *(Relação de Equivalência): Uma relação sobre um conjunto A é dita de equivalência se a relação entre elementos de A são:*

- *Reflexiva: Dado $a \in A$ e uma relação $\sim$, $a \sim a$, $\forall a \in A$.*
- *Transitiva: Dados a, b e $c \in A$, $a \sim b$ e $b \sim c \Rightarrow a \sim c$, $\forall a, b, c \in A$.*
- *Simétrica: Dados a e $b \in A$, $a \sim b \Rightarrow b \sim a$.*

Desta forma, note que, pela Proposição 4, nos inteiros módulo m há uma relação de equivalência. Pois ficou provado que ela é reflexiva, simétrica e transitiva.

Definição 9. *(Classes de Equivalência): Para todo número inteiro a, o conjunto dos inteiros que são congruentes a a módulo m é conhecido como a classe de equivalência de a em relação à congruência módulo m, representado por $\overline{a}$. Logo, por definição*

$$\overline{a} := \{b \in \mathbb{Z} \,|\, b \equiv a \pmod{m}\}$$

Definição 10. *(Sistema de resíduos módulo m): Um sistema completo de resíduos módulo m é um conjunto de inteiros que contém exatamente um representante de cada classe de equivalência de inteiros em relação à congruência módulo m.*

Por exemplo, um sistema completo de resíduos módulo $m = 5$ pode ser $0, 1, 2, 3, 4$, pois esses números representam todas as classes de equivalência dos inteiros sob a relação de congruência módulo 5.

Em geral, para um número inteiro m , um sistema completo de resíduos pode ser qualquer conjunto de m inteiros tais que qualquer inteiro é congruente a um, e apenas um, elemento desse conjunto módulo m .

Proposição 7. *Para todo inteiro positivo t, (ta, tb) = t(a, b). Demonstração em (SANTOS, 2020, p. 6)*

Proposição 8. *Se $c > 0$ e a e b são divisíveis por c, então $(\frac{a}{c}, \frac{b}{c}) = \frac{1}{c}(a,b)$*

Demonstração. Como a e b são divisíveis por c, temos que $(\frac{a}{c},\ \frac{b}{c}) \in \mathbb{Z}$. Pela Proposição 7, $(\frac{a}{c},\frac{b}{c}) = \frac{1}{c}(a,b)$ é equivalente a $\frac{1}{c}(a,b)$. □

Corolário 1. *Se $(a,b) = d$, temos que $(\frac{a}{d},\frac{b}{d}) = 1$*

Demonstração. Como $d = (a,b)$ segue que $d|a$ e $d|b$, pela Proposição 8, $(\frac{a}{d},\frac{b}{d}) = \frac{1}{d}(a,b)$, mas como $(a,b) = d$, temos $\frac{1}{d}(a,b) = \frac{1}{d}d = 1$. □

Proposição 9. *Sejam $a,b,c \in \mathbb{Z}^*$, tem-se que*

Se $c|b$, então $c|ab$.

Demonstração. Como $c|b$, segue que $b = ck$ para algum $k \in \mathbb{Z}$. Como $a \in \mathbb{Z}$, segue que $ab = c(ka)$, então $c|ab$. □

Teorema 3. *(Teorema de Bézout): Se $d = (a,b)$, então existem $x,y \in \mathbb{Z}$ de modo que $ax + by = d$.*

Demonstração. Como $d = (a,b)$, temos que $d \mid a$ e $d \mid b$. Pela Proposição 2, $d \mid (ax + by)$, o que implica que existe $k \in \mathbb{Z}$ tal que $ax + by = dk$.

Considere o conjunto $\mathbb{S} = \{ax + by \mid x,y \in \mathbb{Z} \text{ e } ax + by > 0\}$. $\mathbb{S}$ é notoriamente não vazio pois basta que tomemos $x = a$ e $y = 0$ o que implica $a^2 > 0$. E pelo Princípio da Boa Ordem, $\mathbb{S}$ tem um elemento mínimo. Sendo assim, tome o menor elemento de $\mathbb{S}$ $ax_0 + by_0$. Esse elemento é múltiplo de d, já que d divide todos os elementos de $\mathbb{S}$, e, então, $ax_0 + by_0 = dk_0$, com $k_0 \in \mathbb{Z}$.

Vamos provar que $dk_0 \mid a$ e $dk_0 \mid b$. Suponha, por absurdo, que $dk_0 \nmid a$. Pelo Teorema 2, isso implica que $a = d_0q + r$, onde $0 < r < dk_0$. Então,

$$a = d_0q + r$$

$$r = a - d_0q$$

$$r = a - (ax_0 + by_0)q$$

$$r = a(1 - qx_0) + (-qy_0)b.$$

Considere $(1-qx_0)=x_1$ e $-qy_0=y_1$, com $x_1,y_1\in\mathbb{Z}$. Desta forma, $r=ax_1+by_1$, o que nos diz que $r\in\mathbb{S}$ e, assim, $r\geq dk_0$, pois dk_0 é o menor elemento de $\mathbb{S}$. O que é um absurdo, já que $0<r<dk_0$. Logo, $dk_0\mid a$. De maneira análoga, prova-se que $dk_0\mid b$.

Como $dk_0\mid a$ e $dk_0\mid b$, dk_0 é um divisor comum de a e b, e $d=(a,b)$ é o maior deles. Disso, temos então que $dk_0\leq d$.

Ficou provado também que $dk_0\in\mathbb{S}$ e, então, $dk_0>0$. E como $d>0$, segue que $k_0>0$, e, portanto, $dk_0=d$, logo $k_0=1$.

Desta forma, $ax_0+by_0=dk_0$, o que implica que $ax_0+by_0=d$. Logo, existem $x,y\in\mathbb{Z}$, onde $x=x_0$ e $y=y_0$, tais que $d=ax+by$.

□

Exemplo 4. *Tome os inteiros 12 e 20 e $d=(12,20)=4$. Este teorema nos garante que existem $x,y\in\mathbb{Z}$ tais que $12x+20y=4$. E de fato, basta tomarmos $x=2$ e $y=-1$ e então $12\cdot 2+20\cdot(-1)=4$,*

2.6.1 Equação Diofantina

Uma equação diofantina, $ax+by=c$, é um tipo de equação fundamental na teoria dos números, onde as soluções inteiras são buscadas. Os resultados aqui apresentados serão de suma importância para o entendimento e construção dos resultados acerca de congruência linear.

Definição 11. *Uma equação da forma $ax+by=c$, onde $a,b,c\in\mathbb{Z}$ é chamada de equação diofantina linear.*

Proposição 10. *Se $a,b,c\in\mathbb{Z}$ são tais que $(a,b)\nmid c$, então a equação diofantina $ax+by=c$ não possui solução inteira.*

Demonstração. Suponha, por absurdo, que existem $x,y\in\mathbb{Z}$, tais que $ax+by=c$. Como $ax+by=c$, com $x,y\in\mathbb{Z}$ e $d=(a,b)$, segue que $d|a$ e $d|b$ o que nos diz, pela Proposição 2, que $d|ax+by=c$, o que é uma contradição, já que, por hipótese, $d\nmid c$. □

Proposição 11. *Se $a,b,c\in\mathbb{Z}$ são tais que $d=(a,b)|c$, então a equação diofantina $ax+by=c$ possui soluções inteiras.*

Demonstração. Ora, como $d|c$, segue que $c=dk$, $k\in\mathbb{Z}$ e como $d=(a,b)$, $d|a$ e $d|b$. Disso segue, pela Proposição 2, que existem z_1 e $z_2\in\mathbb{Z}$, tais que $d|az_1+bz_2$. Logo, como $c=kd$, $c=k(az_1+bz_2)=kaz_1+kbz_2$ e assim, temos a solução $x=kz_1$ e $y=kz_2$. □

Exemplo 5. *Tome as equações diofantinas lineares* $2x+14y=5$ *e* $2x+3y=7$.

Temos que $2x+14y=17$ *não terá soluções inteiras, pois* $(2,14)=2$ *e* $2\nmid 5$. *Por outro lado,* $2x+3y=7$ *terá soluções inteiras, já que* $(2,3)=1$ *e* $1|7$.

Teorema 4. *Seja* $x=x_0$ *e* $y=y_0$ *uma solução da equação diofantina* $ax+by=c$ *e* $d=(a,b)$. *Então existem infinitas soluções todas da forma* $x=x_0+\frac{b}{d}k$, $y=y_0-\frac{a}{d}k$.

Demonstração. Seja $x=x_1$ e $y=y_1$ outra solução de $ax+by=c$. Então temos que

$$ax_0+by_0=c \tag{1}$$

e

$$ax_1+by_1=c \tag{2}$$

Subtraindo essas equações obtemos $ax_1-ax_0+by_1-by_0=c-c$

$$a(x_1-x_0)=b(y_1-y_0) \tag{3}$$

Como $d=(a,b)$, temos que $\frac{a}{d}$ e $\frac{b}{d}$ são inteiros. Além disso, pelo Corolário 1, $(\frac{a}{d},\frac{b}{d})=1$.

Assim, da equação 3,

$$\frac{a}{d}(x_1-x_0)=\frac{b}{d}(y_0-y_1) \tag{4}$$

de onde segue que $\frac{b}{d}$ divide x_1-x_0. Portanto, existe $k\in\mathbb{Z}$, tal que $x_1-x_0=k\frac{b}{d}$. Logo, $x_1=x_0+k\frac{b}{d}$.

Substituindo na equação 4,

$$\frac{a}{d}k\frac{b}{d}=\frac{b}{d}(y_0-y_1)$$

$$\frac{a}{d}k=y_0-y_1$$

$$y_1=y_0-k\frac{a}{d}.$$

□

2.6.2 Congruência Linear

A congruência linear se trata de uma extensão da congruência simples que fora apresentada neste trabalho. Na congruência linear busca-se encontrar soluções inteiras para equações congruentes, utilizando métodos específicos baseados em divisibilidade e no algoritmo de Euclides.

Será apresentada a condição necessária e suficiente para a existência de soluções inteiras para essa classe de equações, bem como o número de soluções possíveis.

Definição 12. *Chamamos de congruência linear em uma variável a uma congruência da forma* $ax \equiv b \pmod{m}$ *onde* x *é uma incógnita.*

Teorema 5. *Sejam* $a,b,c,m \in \mathbb{Z}$ *tais que* $ac \equiv bc \pmod{m}$. *Então* $a \equiv b \ (mod\frac{m}{d})$, *onde* $d = (c,m)$.

Demonstração. Pela definição de congruência, temos que $ac \equiv bc \pmod{m}$ implica que $m|(ac-bc)$. Logo, $(a-b)c = mq$, para algum $q \in \mathbb{Z}$. Como $d = (c,m)$, temos que $\frac{c}{d}$ e $\frac{m}{d}$ são inteiros. Assim, $(a-b)\frac{c}{d} = \frac{m}{d}q$ implica que $\frac{m}{d}$ divide $(a-b)\frac{c}{d}$.

Como, Pelo Corolário 1, $(\frac{m}{d}, \frac{c}{d}) = 1$, segue que $\frac{m}{d}$ divide $(a-b)$, e isso, pela Definição 7 implica que $a \equiv b \pmod{\frac{m}{d}}$. □

Proposição 12. *Sejam* $a,b \in \mathbb{Z}$ *e* $d = (a,m)$. $ax \equiv b \ (mod\ m)$ *possui solução inteira quando* $d|b$.

Demonstração. Por definição, $ax \equiv b \pmod{m}$ implica que $m|(ax-b)$ e, segundo a Definição 1, existe y inteiro tal que $ax - b = my$, o que é equivalente a $ax - my = b$ que é uma equação diofantina. Pela Proposição 11, essa equação tem solução inteira apenas quando $(a,m)|b$.

Ainda, segundo a Proposição 10, essa equação diofantina linear e consequentemente a congruência linear $ax \equiv b \pmod{m}$ não possui solução inteira quando $d \nmid b$. □

Teorema 6. *Sejam* a,b,m *inteiros tais que* $m > 0$ *e* $d = (a,m)$. *No caso em que* $d \nmid b$ *a congruência* $ax \equiv b \pmod{m}$ *não possui nenhuma solução e quando* $d|b$, *possui exatamente* d *soluções incongruentes módulo* m.

Demonstração. Pela Proposição 12, sabemos que o inteiro x é solução de $ax \equiv b \pmod{m}$, se $d|b$ e que ela não possui nenhuma solução quando $d \nmid b$. Pelo Teorema 4 , sabemos que se $d|b$ existem infinitas soluções dadas por $x = x_0 - (\frac{m}{d})k$ e $y = y_0 - (\frac{a}{d})k$, onde o par (x_0, y_0)

é uma solução particular de $ax - my = b$. Logo, a congruência $ax \equiv b \pmod{m}$ possui infinitas soluções dadas por $x = x_0 - (\frac{m}{d})k$. Como estamos interessados em saber o número de soluções incongruentes, vamos tentar descobrir sob quais condições $x_1 = x_0 - (\frac{m}{d})k_1$ e $x_2 = x_0 - (\frac{m}{d})k_2$ são congruentes módulo m.

Se x_1 e x_2 são congruentes, então $x_0 - (\frac{m}{d})k_1 \equiv x_0 - (\frac{m}{d})k_2 \pmod{m}$. O que, pela Proposição 6, equivale a $x_0 - x_0 - (\frac{m}{d})k_1 \equiv x_0 - x_0 - (\frac{m}{d})k_2 \pmod{m}$ o que resulta em $-(\frac{m}{d})k_1 \equiv -(\frac{m}{d})k_2 \pmod{m}$ e isso implica que $(\frac{m}{d})k_1 \equiv (\frac{m}{d})k_2 \pmod{m}$. Como $(\frac{m}{d})|m$, temos que $(\frac{m}{d}, m) = \frac{m}{d}$, o que, segundo o Teorema 5, nos permite o cancelamento de $\frac{m}{d}$ resultando em $k_1 \equiv k_2 \pmod{d}$. Observe que m foi substituído por $d = \frac{m}{\frac{m}{d}}$. Isto mostra que soluções incongruentes serão obtidas ao tomarmos $x = x_0 - \frac{m}{d}k$ onde k percorre um sistema completo de resíduos módulo d, o que conclui a demonstração. □

Definição 13. *Soluções incongruentes módulo m de uma congruência linear são soluções inteiras distintas que não são equivalentes entre si sob o módulo m .*

Exemplo 6. $2x \equiv 4$*(mod 6).*

Como $(2,6) = 2$*, segue que existem exatamente duas soluções incongruentes módulo 6. Essas soluções podem ser* $x = 2$ *e* $x = 5$*, pois:*

$2 \cdot 2 = 4 \equiv 4 \pmod{6}$ *e* $2 \cdot 5 = 10 \equiv 4 \pmod{6}$*. Essas duas soluções são incongruentes entre si, pois:*

$2 \not\equiv 5 \pmod{6}$.

Em resumo, as soluções incongruentes são aquelas que representam todas as soluções possíveis da congruência linear sem repetição dentro do intervalo do módulo m.

Corolário 2. *Se* $(a, m) = 1$*, assim a congruência linear* $ax \equiv b \pmod{m}$ *Possui uma única solução módulo m.*

2.7 GRUPOS

Um grupo é um conjunto de elementos, juntamente com uma operação binária que combina dois elementos para formar um terceiro, obedecendo a certas propriedades, como fechamento, associatividade, existência de um elemento neutro e existência de inversos.

Será apresentada a definição formal de grupo, discutindo as propriedades necessárias que caracterizam essa estrutura algébrica.

Definição 14. *Seja G um conjunto não vazio e esteja definida nele uma operação binária* $\cdot$*, isto é*

$$\cdot : G \times G \to G$$

Dizemos que $(G, \cdot)$ é um grupo se o seguinte acontecer:

- G_1*: Existe um elemento $e \in G$ tal que, para todo $g \in G$, $g \cdot e = g = e \cdot g$;*
- G_2*: Para quaisquer $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;*
- G_3*: Para todo $g \in G$, existe $h \in G$ tal que $g \cdot h = e = h \cdot g$.*

Exemplo 7. *Considere o conjunto dos números inteiros $\mathbb{Z}$ com a operação usual de soma $+$. Temos que $(\mathbb{Z}, +)$ é um grupo, pois*

- *a soma de 2 inteiros é um inteiro, logo $+$ é uma operação binária em $\mathbb{Z}$;*
- *a soma é associativa, pois*

$$x + (y + z) = (x + y) + z, \quad \forall x, y, z \in \mathbb{Z};$$

- *o elemento neutro é 0, pois*

$$x + 0 = 0 + x = x, \quad \forall x \in \mathbb{Z};$$

- *o inverso de x é $-x$, pois*

$$x + (-x) = (-x) + x = 0, \quad \forall x \in \mathbb{Z}.$$

Definição 15. *Um grupo G é chamado de grupo abeliano, ou comutativo, se a operação $\cdot$ for comutativa, ou seja*

$$a \cdot b = b \cdot a \text{ , para todo } a \text{ e } b \in G.$$

Exemplo 8. $(\mathbb{Z}, +)$ *é um grupo abeliano, pois*

$$x + y = y + x, \quad \forall x, y \in \mathbb{Z}.$$

Definição 16. *Considere um grupo $(H, \times)$. Para que este grupo seja não-abeliano, é necessário que existam elementos $a, b \in \mathbb{H}$ tais que $a \times b \neq b \times a$.*

Exemplo 9. *Seja o grupo das matrizes $n \times n$ com a operação usual de multiplicação entre matrizes. No geral, este grupo é não-abeliano.*
Considere as matrizes $A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ e $B = \begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix}$. A multiplicação $A \times B$ é dada por:

$$A \times B = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} (2\times 1+1\times 2) & (2\times 3+1\times 2) \\ (1\times 1+1\times 2) & (1\times 3+1\times 2) \end{pmatrix}$$

$$= \begin{pmatrix} 4 & 8 \\ 3 & 5 \end{pmatrix}$$

Agora, calculemos $B \times A$:

$$B \times A = \begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix} \times \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} (1\times 2+3\times 1) & (1\times 1+3\times 1) \\ (2\times 2+2\times 1) & (2\times 1+2\times 1) \end{pmatrix}$$

$$= \begin{pmatrix} 5 & 4 \\ 6 & 4 \end{pmatrix}$$

Como $A \times B \neq B \times A$, a multiplicação de matrizes não é comutativa.

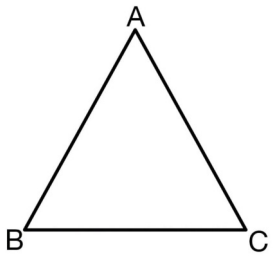
2.8 GUPOS DIEDRAIS

Nesta seção, iremos explorar os conceitos dos grupos de simetria e dos grupos diedrais. Os fatos e resultados aqui explorados serão de grande utilidade para compreensão do algoritmo de Verhoeff 3.2.10.

Uma permutação de um conjunto consiste em reordenar seus elementos, trocando suas posições, ou seja, levando um elemento para a posição do outro sem que nenhum deles seja removido ou adicionado ao conjunto. Sendo assim, considere o conjunto $\{A, B, C\}$ representando os vértices de um triângulo equilátero. Podemos reorganizar esses elementos de diferentes formas.

Considere uma função que mapeia cada elemento para outro. Por exemplo $f(A) = A$, $f(B) = B$, $f(C) = C$ que representa o próprio triângulo sem qualquer alteração. Essa é a função identidade.

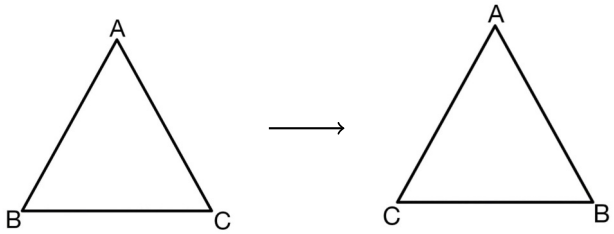
Figura 2.1 – Triângulo ABC



Fonte: O Autor

Outro exemplo seria $f(A) = A$, $f(B) = C$, $f(C) = B$ onde os vértices B e C trocam de lugar, enquanto A permanece em sua posição original. Este tipo de movimentação não altera o formato do triângulo, apenas a disposição dos vértices.

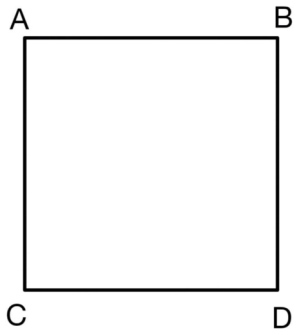
Figura 2.2 – f aplicada no triângulo equilátero



Fonte: O Autor

Podemos realizar nos vértices de um quadrado algo exatamente análogo ao que foi feito nos vértices do triângulo. Considere o conjunto $\{A, B, C, D\}$, que representa os vértices de um quadrado. A função $f(A) = A$, $f(B) = B$, $f(C) = C$ e $f(D) = D$ representa a posição inicial dos vértices, ou seja, a função identidade.

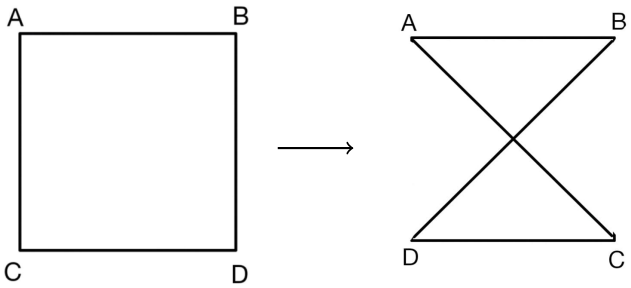
Figura 2.3 – Quadrado



Fonte: O Autor

Agora, considere $f(A) = A$, $f(B) = B$, $f(C) = D$ e $f(D) = C$

Figura 2.4 – f aplicada no Quadrado



Fonte: O Autor

Note que esse fato, Figura 2.4, faz com que a estrutura do polígono seja alterada causando uma deformação.

Neste trabalho, ao se falar de simetria estaremos considerando os movimentos rígidos realizados em uma figura plana. Esses movimentos preservam a estrutura da figura de forma que ela não seja deformada. Por exemplo, uma simetria de um triângulo equilátero seria uma cópia deste triângulo com a mesma estrutura original, mas com os vértices ou lados trocados de lugar.

Considerando $n \geq 3$ como sendo os lados de um polígono regular, o grupo diedral D_n é o grupo formado pelo conjunto das simetrias do polígono com as operações correspondentes. Denotado por $(D_n, \circ)$ e com ordem de $2n$, o grupo representa n rotações de $k\frac{2\pi}{n}$ em torno do baricentro, onde $0 \leq k \leq n-1$ e n reflexões em relação aos eixos de simetria do polígono.

O Grupo Diedral D_n, ou Grupo de Simetrias, pode ser visto como um grupo de permutações, pois existe uma bijeção

$f : D_n \to D_n$ e as rotações e reflexões de D_n são representadas por permutações

Proposição 13. *D_n é um grupo não abeliano com a composição de funções.*

Demonstração em (CANçADO, 2016, p. 44).

2.9 TABELA DE CAYLEY

Quando o grupo G é finito podemos descrever sua operação através de uma tabela, chamada de Tabela de Cayley, onde as linhas e colunas têm todos os elementos de G de forma que o elemento da linha correspondente ao elemento g e a coluna correspondente ao elemento h é o elemento $g \circ h$

Tabela 2.1 – Tabela de Cayley

$\circ$	e	...	h	...
e				
$\vdots$				
g			$g \circ h$	
$\vdots$				

Exemplo 10. *Tome o grupo M , $M = \{1, -1\}$ com a operação de multiplicação usual. Temos o segunte:*

Tabela 2.2 – Tabela de Cayley grupo M

$\times$	1	-1
1	1	-1
-1	-1	1

3 SISTEMAS DE DÍGITOS VERIFICADORES

Neste capítulo são descritos os principais métodos utilizados para cálculo dos dígitos verificadores. Os métodos mais utilizados, segundo (SOUZA et al., 2013), são os que fazem uso da aritmética modular para o cálculo dos dígitos verificadores (dv´s). Esses levam em consideração os resultados módulo m, $m \in \mathbb{N}$.

Outros métodos utilizados são o método de Verhoeff, que utiliza a teoria dos grupos, e o algoritmo de Damm, que utiliza os quadrados latinos. Todos esses serão detalhados mais adiante.

Consideramos um número de identificação como sendo aquele formado pela parte principal e pelos seus dígitos verificadores. Para todos os casos a seguir consideramos um número de identificação formado por algarismos decimais, isto é, cada algarismo, individualmente, que o compõe varia de 0 a 9. A parte principal é utilizada para definição dos dígitos verificadores.

A exemplo, o número de identificação 3937638-4 pode ser dividido em duas partes. A primeira parte é a principal e a segunda os dígitos verificadores. Parte principal: 3937638. Dígito verificador: 4.

3.1 MÉTODOS

3.1.1 Aritmética Modular

Considerando um número com n dígitos, o método que utiliza a aritmética modular utiliza a parte principal $a_1a_2a_3\ldots a_{n-1}$ para que o dígito verificador a_n seja gerado através de uma operação, que consiste em multiplicar da esquerda para a direita os a_i por pesos p_i bem definidos, $1 \leq i \leq n-1$, sendo os resultados dessa multiplicação somados

$$a_n \stackrel{\text{def}}{=} a_1p_1 + a_2p_2 + \ldots + a_{n-1}p_{n-1} \tag{5}$$

a_n será dito o dígito verificador e é determinado calculando o resto dessa soma quando dividida por um número m.

Para simplificação deste fato, considere $a_1 \cdot p_1 + a_2 \cdot p_2 + \ldots + a_{n-1} \cdot p_{n-1} = k, k \in \mathbb{Z}^+$.

Como demonstrado no Teorema 2, temos que $k = mq + r$, onde q é o quociente e r o resto da divisão de k por m.

$$\begin{cases} \text{Se } r = 0, m|k \\ \text{Se } 0 < r < m, m \nmid k \end{cases} \tag{6}$$

Isso implica, pela Proposição 3, que como $k - r = mq$, $m|k - r$, ou seja $k \equiv r \pmod{m}$. Portanto $r = a_n$. Deste fato segue o que vemos na equação 7.

Para os nossos casos práticos a seguir, consideramos os dois resultados que seguem.

$$a_1p_1 + a_2p_2 + ... + a_{n-1}p_{n-1} \pmod{m} = a_n \tag{7}$$

e

$$a_1p_1 + a_2p_2 + ... + a_{n-1}p_{n-1} + a_n \equiv 0 \pmod{m}. \tag{8}$$

A equação 7 chamamos de equação do sistema direto ou completa e a equação 8 de equação por complemento.

3.2 APLICAÇÃO PRÁTICA DOS MÉTODOS

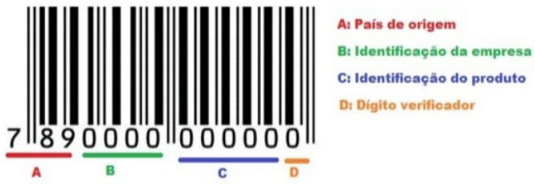
Nesta parte, abordaremos os casos onde os dígitos verificadores ganham aplicação com foco na verificação de números de identificação em processos que necessitam de validação de dados. Para todos os resultados que seguem, consideramos $m \geq 10$ sendo vistos os casos de $m = 10$ e $m = 11$ para os casos práticos. Para os casos onde $m = 10$ é utilizado um dígito verificador como no código de barras, Cartão de crédito e ISBN. Casos onde existem dois dígitos verificadores é utilizado $m = 11$ como no cálculo dos dígitos verificadores do CPF, Título de eleitor e da agência e conta do banco do Brasil.

3.2.1 Módulo 10

Código de Barras

O código de barras, comumente necessário em mercados, é usado para identificar produtos e é formado por barras verticais, para leitura via leitor ou scanner, e números que podem ser digitados manualmente em casos onde o leitor ou scanner não funcione corretamente.

Figura 3.1 – Código de barras



Fonte: (CERQUEIRA et al., 2015, p. 28)

Esse código carrega consigo informações que remetem desde o país de origem do produto até o dígito verificador responsável pela detecção de possíveis erros na digitação manual desse código. Podendo ser dividido em partes e sendo o tipo mais usado o European Article Numbering (EAN - 13) ele contém 13 dígitos, distribuídos da seguinte maneira.

Na primeira parte, os três primeiros dígitos representam o país de onde o produto é originário. Cada país tem sua própria numeração e no caso do Brasil, é 789;

Na segunda parte, os quatro dígitos seguintes referem-se à identificação da empresa a qual fabricou o produto;

Na terceira parte, os próximos 5 dígitos são os referentes ao próprio produto;

E na quarta e última parte um único dígito que representa o dígito verificador.

Esse é calculado da seguinte forma: Utilizando a equação por complemento, considere o código 7 898708731394 como exemplo. Multiplica-se os dígitos de forma alternada pelos pesos 1 e 3:

$$\begin{array}{cccccccccccc} & 7 & 8 & 9 & 8 & 7 & 0 & 8 & 7 & 3 & 1 & 3 & 9 \\ \times & & & & & & & & & & & & \\ & 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 \\ \hline & 7 & 24 & 9 & 24 & 7 & 0 & 8 & 21 & 3 & 3 & 3 & 27 \end{array}$$

Somando-se os resultados das multiplicações $7+24+9+24+7+0+8+21+3+3+3+27=136$.

Como utiliza-se a equação por complemento, segue que $136+dv \equiv 0 \pmod{10}$

$\Rightarrow dv = 4$, pois $136+4 \equiv 0 \pmod{10}$.

3.2.2 Cartão de Crédito

O cartão de crédito é muito usado para compras onde se quer ou precisa evitar o uso de dinheiro físico e é muito presente na vida de todos. Formado por 16 dígitos, o cartão de crédito carrega consigo informações sobre seu titular, a empresa emitente do cartão entre outras.

O primeiro número representa a bandeira do cartão, por exemplo, um cartão iniciado com o número 4 representa a bandeira VISA;

Os próximos cinco números representam a instituição emissora do cartão;

Os nove números seguintes referem-se às informações do proprietário do cartão como conta e agência;

E finalmente o último número é o dígito verificador.

Figura 3.2 – Cartão de Crédito

Fonte: https://vivaocredito.com.br/significado-dos-numeros-do-cartao-de-credito/

Para determinação do dígito verificador é utilizado um método criado por Hans Peter Luhn, (LUHN, 1960), método esse conhecido como algoritmo de Luhn.

Utilizando a equação por complemento módulo 10 e os pesos 1 e 2, multiplicam-se os dígitos das posições ímpares por 2 e os das posições pares por 1. Considere o número 1234 5678 9012 3452.

$$
\begin{array}{cccccccccccccccc}
 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 0 & 1 & 2 & 3 & 4 & 5 \\
\times & & & & & & & & & & & & & & & \\
 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 \\
\hline
 & 2 & 2 & 6 & 4 & 10 & 6 & 14 & 8 & 18 & 0 & 2 & 2 & 6 & 4 & 10
\end{array}
$$

Se algum dos resultados da multiplicação for maior que 9, realizamos uma operação chamada "noves fora", ou seja, subtraímos 9.

Como 10, 14 e 18 são maiores que 9, o número resulta agora em

$$2\ 2\ 6\ 4\ 1\ 6\ 5\ 8\ 9\ 0\ 2\ 2\ 6\ 4\ 1$$

Agora somando os números temos $2+2+6+4+1+6+5+8+9+0+2+2+6+4+1=58$.

Como nesse caso utilizamos a equação por complemento, segue que $58+dv \equiv 0 \pmod{10}$.

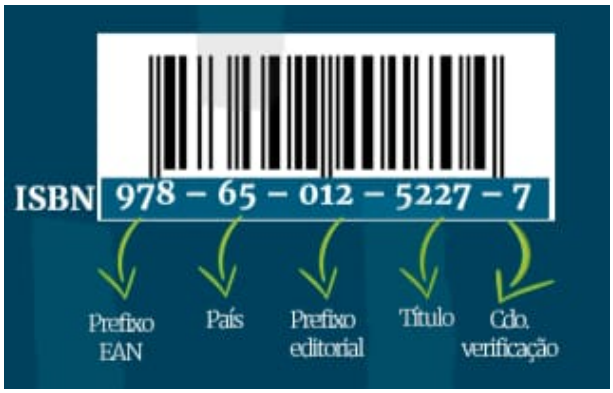
E portanto $dv = 2$, pois $58+2 \equiv 0 \pmod{10}$.

3.2.3 ISBN

O International Standard Book Number, Padrão Internacional de Numeração de Livro , ou apenas ISBN é o número de identificação numérico utilizado principalmente para livros. Esse número é o identificador de obras reconhecido internacionalmente com o intuito de que cada obra tenha um número único e que isso facilite a identificação e checagem das obras, além de evitar erros humanos na utilização, pois nele é utilizado o sistema de dígito verificador.

Em resposta ao crescente número de publicações, a partir de 1 de janeiro de 2007 utiliza-se o ISBN-13. Composto por 13 dígitos esse número carrega consigo informações que indicam o título, o autor, o país, a editora e a edição de uma obra.

Figura 3.3 – ISBN



Fonte: https://editorialpaco.com.br/o-que-e-isbn/

Utilizando exatamente o mesmo método do código de barras, é possível checar a veracidade do número de uma obra através de seu número de identificação.

Dado o ISBN 978 85 24401 69 5, verifiquemos o processo para definição do seu dígito verificador

$$\begin{array}{cccccccccccc} & 9 & 7 & 8 & 8 & 5 & 2 & 4 & 4 & 0 & 1 & 6 & 9 \\ \times & & & & & & & & & & & & \\ & 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 \\ \hline & 9 & 21 & 8 & 24 & 5 & 6 & 4 & 12 & 0 & 0 & 6 & 27 \end{array}$$

Resultando em $9+21+8+24+5+6+4+12+0+3+6+27 = 125$. Utilizando a equação por complemento, segue que

$$125 + d_v \equiv 0 \pmod{10}$$

$$\Rightarrow dv = 5.$$

3.2.4 Módulo 11

Como visto anteriormente, no caso de utilização do módulo 10, conseguimos escrever o dígito verificador, dv, como sendo um número entre 0 e 9, $0 \leq dv \leq 9$, pois eles são os possíveis restos na divisão por 10. Para o módulo 11 existe o detalhe de que os possíveis restos na divisão por 11 variam de 0 a 10 e como o dígito verificador é um número compreendido entre 0 e 9, resta o problema de quando esse resto resulta exatamente em 10. Para esses casos temos como solução adotar a nomenclatura do módulo 11 completo e do módulo 11 restrito.

Para o módulo 11 completo é utilizado o caractere especial X para representar o resto 10 na divisão por 11.

Já no caso do módulo 11 restrito utiliza-se o 0 para representar o 10 como resto nessa divisão.

3.2.5 CPF

O Cadastro de Pessoas Físicas (CPF) é algo aparentemente simples. É um documento composto por 11 algarismos gerenciado pela Receita Federal do Brasil (RFB).

Figura 3.4 – CPF

Fonte:
https://www.gov.br/mre/pt-br/embaixada-managua/servicosconsulares/cadastro-de-pessoas-fisicas-cpf

Comumente utilizado e com ampla necessidade para tarefas do dia a dia, o CPF é usado, por exemplo, para identificação dos cidadãos brasileiros perante órgãos governamentais e instituições privadas, e carrega diversas informações referente a cada pessoa e seu número de inscrição.

Esses 11 dígitos são definidos utilizando métodos que garantem que um mesmo número nunca se repita e obedeça a critérios bem definidos. Para isso, a Receita Federal divide o nosso país em dez regiões que são chamadas regiões fiscais e tem relação tanto com os estados quanto com o número do CPF.

Tabela 3.1 – Regiões Fiscais

Região Fiscal	Dígito Correspondente	Estados
1	1	DF, GO, MS, MT e TO
2	2	AC, AM, AP, PA, RO e RR
3	3	CE, MA e PI
4	4	AL, PB, PE e RN
5	5	BA e SE
6	6	MG
7	7	ES e RJ
8	8	SP
9	9	PR e SC
10	0	RS

O nono dígito do documento carrega consigo a informação de qual região fiscal uma determinada pessoa informou para o cadastramento inicial. Por exemplo, uma pessoa que informa sua região fiscal como sendo o estado da Paraíba tem em seu CPF o nono dígito sendo o algarismo 4.

Este documento tem como característica a utilização de dois dígitos verificadores que são calculados separadamente utilizando a equação por complemento.

Quando o resto da divisão por 11 é 0 ou 1, o dígito verificador é 0;

Se o resto da divisão por 11 for maior que 2 e menor que 11, $2 < r < 11$, o dígito verificador é dado pelo complemento, ou seja $dv = 11$ - r.

Dado o número 111 256 244-34 o cálculo é dado da seguinte forma: Utilizando os pesos (10, 9, 8, 7, 6, 5, 4, 3 e 2) aplicados aos 9 primeiros dígitos, conseguimos calcular o primeiro dígito verificador.

$$\begin{array}{cccccccccc} & 1 & 1 & 1 & 2 & 5 & 6 & 2 & 4 & 4 \\ \times & & & & & & & & & \\ & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 \\ \hline & 10 & 9 & 8 & 14 & 30 & 30 & 8 & 12 & 8 \end{array}$$

Resultando em $10+9+8+14+30+30+8+12+8 = 129$

$$\Rightarrow 129 + dv \equiv 0 \pmod{11}$$

E de fato $dv = 3$ pois $129+3 \equiv 0 \pmod{11}$.

Em posse do primeiro dígito podemos calcular o segundo, utilizando os mesmos pesos e desconsiderando o primeiro dígito do número do CPF

$$\begin{array}{cccccccccc} & 1 & 1 & 2 & 5 & 6 & 2 & 4 & 4 & 3 \\ \times & & & & & & & & & \\ & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 \\ \hline & 10 & 9 & 16 & 35 & 36 & 10 & 16 & 12 & 6 \end{array}$$

Resultando em $10+9+16+35+36+10+16+12+6 = 150$

$$\Rightarrow 150 + dv_2 \equiv 0 \pmod{11}$$

Confirmando que $dv_2 = 4$ pois $150+4 \equiv 0 \pmod{11}$.

3.2.6 Titulo de Eleitor

Usado pelo cidadão brasileiro principalmente para fazer a escolha de seus representantes políticos, o título eleitoral é emitido pelo Tribunal Superior Eleitoral (TSE) e é usado de forma direta nas eleições.

Figura 3.5 – Título de eleitor.

Fonte: https://www.conjur.com.br/2010-dez-29/eleitor-quinta-justificar-ausencia-segundo-turno/

Usado em todo o país é formado por 12 dígitos, com exceção dos estados de São Paulo e Minas Gerais que diferem dos demais contendo 1 dígito a mais, carrega em sua composição informações específicas.

Os oito primeiros dígitos identificam o eleitor, os próximos dois dígitos referem-se à unidade federativa e os dois últimos são ditos os dígitos verificadores.

Utilizando o módulo 11 restrito, o método de cálculo e verificação desse número utiliza duas etapas.

Para a primeira utilizam-se os pesos (2, 3, 4, 5, 6, 7, 8 e 9) aplicados aos primeiros 8 dígitos para o cálculo do primeiro dígito verificador.

Para o cálculo do segundo dígito, na segunda etapa, são utilizados os pesos (7, 8 e 9) aplicados aos próximos 3 dígitos que inclui o primeiro dígito verificador calculado na primeira etapa.

Sendo assim, para o título eleitoral de número 1023 8501 06 - 71 o cálculo é feito da seguinte forma:

Primeira etapa:

$$\begin{array}{cccccccccc} & 1 & 0 & 2 & 3 & 8 & 5 & 0 & 1 & \\ \times & & & & & & & & & \\ & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \\ \hline & 2 & 0 & 8 & 15 & 48 & 35 & 0 & 9 & \end{array}$$

Resultando em $2+0+8+15+48+35+0+9=117$.

Como é utilizada a equação do sistema direto ou completa com o módulo 11 restrito, segue que $117 \equiv dv \pmod{11}$ e portanto $dv = 7$, pois $117 \equiv 7 \pmod{11}$.

Em posse do primeiro dígito verificador, segue-se para a segunda etapa que utiliza os pesos 7, 8 e 9 para determinação do segundo dígito verificador.

$$\begin{array}{rccc} & 0 & 6 & 7 \\ \times & & & \\ & 7 & 8 & 9 \\ \hline & 0 & 48 & 63 \end{array}$$

Resultando em $0 + 48 + 63 = 111$

$$\Rightarrow 111 \equiv dv_2 \pmod{11}$$

Portanto $dv_2 = 1$ pois $111 \equiv 1 \pmod{11}$.

3.2.7 Banco do Brasil

Comum em vários municípios brasileiros atendendo clientes para os mais diversos tipos de operações bancárias, o Banco do Brasil também utiliza a aritmética modular para determinação e checagem dos números de suas agências e para o número da conta de cada cliente.

Com a possível utilização de um caractere especial, o Banco do Brasil faz uso do módulo 11 completo e pode considerar o X como dígito verificador.

Sendo duas informações distintas, a agência é responsável por localizar a conta dentro da rede do Banco, enquanto o número da conta identifica única e exclusivamente aquela conta em específico. O número da agência é composto por 5 dígitos, incluindo o dígito verificador, enquanto o número da conta corrente pode ter entre 6 e 8 dígitos, dependendo da época em que a conta foi criada e da agência. Para o nosso exemplo vamos adotar, sem perda de generalidade, uma conta com 6 dígitos incluindo o de verificação.

Figura 3.6 – Agência e Conta Banco do Brasil

Fonte:https://pontospravoar.com/cartao-banco-do-brasil-ourocard-visa-gold-analise/

Os pesos aplicados são distintos para checagem.

Os pesos 5, 4, 3 e 2 são aplicados para cálculo do dígito de verificação da agência. Sendo assim, considerando a agência 2644-1 teremos o seguinte

$$\begin{array}{cccccc} & 2 & 6 & 4 & 4 \\ \times & & & & \\ & 5 & 4 & 3 & 2 \\ \hline & 10 & 24 & 12 & 8 \end{array}$$

Resultando em $10+24+12+8=54$.

Como o dígito verificador será dado pelo complemento, ou seja, $54+dv \equiv 0 \pmod{11}$.

De fato, $dv=1$, pois $54+1 \equiv 0 \pmod{11}$.

Os pesos 6, 5, 4, 3, 2 , são aplicados para cálculo do dígito de verificação da conta. Considere a conta 32717-4, o cálculo para checagem será

$$\begin{array}{cccccc} & 3 & 2 & 7 & 1 & 7 \\ \times & & & & & \\ & 6 & 5 & 4 & 3 & 2 \\ \hline & 18 & 10 & 28 & 3 & 14 \end{array}$$

Resultando em $18+10+28+3+14=73$.

Sendo assim, $73+dv \equiv 0 \pmod{11}$ e $dv=4$ pois $73+4 \equiv 0 \pmod{11}$.

3.2.8 Verhoeff

Verhoeff, em sua tese de doutorado, propôs e utilizou a aritmética modular e o grupo diedral para evitar ou detectar erros e também para analisar a eficácia de métodos para a detecção de erros em números de identificação que utilizam para isso dígitos verificadores.

3.2.9 Módulo 10

Utilizando permutações e o módulo 10 para calcular o dígito verificador, este método utiliza uma tabela de permutação fixa para determinar como os dígitos do número original devem ser permutados.

Tabela 3.2 – Permutações de esquema de Verhoeff

x	0	1	2	3	4	5	6	7	8	9
$f_0(x)$	5	8	1	3	6	9	7	0	4	2
$f_1(x)$	5	0	6	1	7	2	3	9	8	4
$f_2(x)$	0	1	8	7	5	9	6	4	2	3
$f_3(x)$	1	8	6	9	0	4	2	3	5	7
$f_4(x)$	5	0	4	8	2	9	3	6	1	7
$f_5(x)$	0	1	7	5	6	8	9	4	3	2
$f_6(x)$	5	8	0	9	7	4	2	6	3	1
$f_7(x)$	5	0	9	2	3	8	4	7	1	6
$f_8(x)$	0	1	4	9	6	2	3	5	7	8
$f_9(x)$	1	8	3	4	2	5	7	0	9	6

Em posse dessa tabela, cada algarismo do número original é multiplicado pelo valor bem específico que ali consta em relação à permutação. Após essa multiplicação, os resultados são somados e o resultado é considerado módulo 10.

Dessa forma, um número $a_1a_2a_3\ldots a_{n-1}$ tem seu dígito verificador calculado da seguinte forma:

$$dv = f_0(a_1) + f_1(a_2) + \ldots + f_{n-2}(a_{n-1}) \pmod{10}$$

Sendo assim, aplicando o método para determinar o dígito verificador do número 3215774621 segue que

$$dv = f_0(3) + f_1(2) + f_2(1) + f_3(5) + f_4(7) + f_5(7) + f_6(4) + f_7(6) + f_8(2) + f_9(1) \pmod{10}.$$

Resultando em 3+6+1+4+6+4+7+4+4+8=47, como $47 \equiv dv \pmod{10}$ segue que dv=7, pois $47 \equiv 7 \pmod{10}$.

É notória a semelhança também entre o papel desempenhando entre f_i e os pesos p_i dos casos anteriores. como mostrado na tabela 3.3 a seguir.

Tabela 3.3 – Multiplicação por pesos

x	0	1	2	3	4	5	6	7	8	9
0·	0	0	0	0	0	0	0	0	0	0
1·	0	1	2	3	4	5	6	7	8	9
2·	0	2	4	6	8	0	2	4	6	8
3·	0	3	6	9	2	5	8	1	4	7
4·	0	4	8	2	6	0	4	8	2	6
5·	0	5	0	5	0	5	0	5	0	5
6·	0	6	2	8	4	0	6	2	8	4
7·	0	7	4	1	8	5	2	9	6	3
8·	0	8	6	4	2	0	8	6	4	2
9·	0	9	8	7	6	5	4	3	2	1

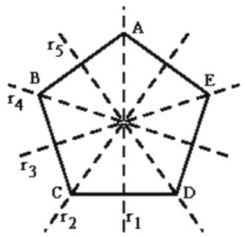
Segundo (SOUZA et al., 2013), este método de Verhoeff que utiliza o módulo 10 é detentor da melhor média de detecção de erros dentre todos os métodos módulo 10 mais utilizados.

De fato, ao compararmos as tabelas 3.2 e 3.3, as semelhanças entre as permutações e os pesos se limitam à sua estrutura inicial. Note que há uma diferença significativa no comportamento dos dois métodos quando considerados módulo 10. Os pesos , ao serem aplicados diretamente em operações módulo 10, podem gerar valores congruentes, ou seja, diferentes números podem produzir o mesmo resultado final, o que pode levar a duplicidades e reduzir a eficácia na detecção de erros. Por outro lado, as permutações geram valores únicos, o que torna esse método mais robusto para evitar colisões de valores e, portanto, se mostra mais eficaz na identificação de erros.

3.2.10 Método de Verhoeff: Teoria dos Grupos

Além do método utilizando a aritmética modular, (VERHOEFF, 1975) encontrou na teoria dos grupos e mais precisamente no pentágono regular uma maneira de checagem.

Figura 3.7 – Pentágono regular



Fonte:

Ela consiste em considerar as composições das simetrias desse polígono. Essas simetrias são movimentos rígidos que preservam a estrutura do polígono e nesse caso são consideradas as rotações em torno do centro e os espelhamentos em relação às retas que passam pelos vértices. Estas simetrias com a operação $*$ formam um grupo chamado de grupo diedral, $(D, *)$.

Ao todo são consideradas 5 rotações e 5 reflexões que são representadas em uma tabela de composição que considera essas simetrias.

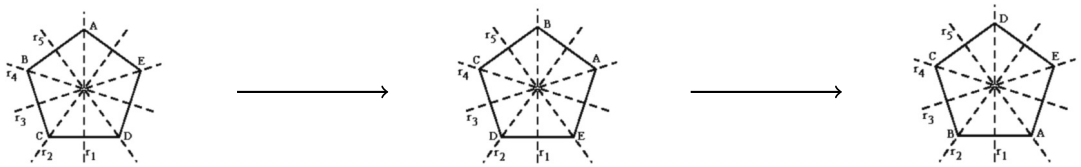
As rotações são denotadas por 0, 1, 2, 3 e 4. Já as reflexões, que são os espelhamentos, por 5, 6, 7, 8 e 9.

Tabela 3.4 – Simetrias

0	Identidade rotação de ângulo de 0
1	Rotaçao de ângulo $\frac{2\pi}{5}$
2	Rotaçao de ângulo $\frac{4\pi}{5}$
3	Rotaçao de ângulo $\frac{6\pi}{5}$
4	Rotaçao de ângulo $\frac{8\pi}{5}$
5	Reflexão em relação à reta r_1
6	Reflexão em relação à reta r_2
7	Reflexão em relação à reta r_4 r_3
8	Reflexão em relação à reta r_4
9	Reflexão em relação à reta r_5 r_5

A exemplo, operar ou compor 4 com 8 é o mesmo que aplicarmos a simetria associada a 4, ou seja, realizarmos uma rotação de $\frac{8\pi}{5}$ e após isso a simetria associada a 8 que é a reflexão em relação à reta r_4 . Sendo assim, o processo realizado no pentágono pode ser visto na Figura 3.8.

Figura 3.8 – Simetrias aplicadas no polígono ABCDE



Um caminho direto para isso seria o que leva [ABCDE] em [DCBAE], (4*8), e isso é o que acontece e é mostrado na tabela de Cayley deste grupo.

Tabela 3.5 – Tabela de Cayley do Grupo Diedral D_5

$*$	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0

O processo para checagem de números por este método é o de aplicar potências de uma permutação $\sigma \in D_5$ com a característica de que $a * \sigma(b) \neq b * \sigma(a)$ para $a \neq b$ em cada algarismo em uma ordem pré-estabelecida.

Sendo assim, dado o número $a_1 a_2 \dots a_{n-2} a_{n-1}$, considerando a permutação σ, esse identificador tem o seu dígito verificador dado pela seguinte forma

$$\sigma^{n-1} a_1 * \sigma^{n-2} a_2 \dots * \sigma a_{n-1} * dv = 0.$$

Para o nosso caso consideramos a permutação $\sigma = (32)(41)(67895)$ e a operação $*$ dada pela tabela de Cayley do grupo D_5. A exemplo, o número de identificação 245016 tem seu dígito verificador dado da seguinte maneira

$$\begin{aligned} 0 &= \sigma^6(2) * \sigma^5(4) * \sigma^4(5) * \sigma^3(0) * \sigma^2(1) * \sigma(6) * dv \\ &= 2 * 1 * 9 * 0 * 1 * 7 * dv \\ &= 3 * 9 * 0 * 1 * 7 * dv \\ &= 7 * 0 * 1 * 7 * dv \\ &= 7 * 1 * 7 * dv \\ &= 6 * 7 * dv \\ &= 4 * dv \end{aligned}$$

Portanto $dv = 1$ pois $4 * 1 = 0$.

3.2.11 Algoritmo de Damm

O algoritmo de Verhoeff foi durante muito tempo considerado a maneira mais completa e segura para evitar problemas na utilização e transmissão de informações via dígito verificador, mas em sua dissertação de doutorado H. Michael Damm (DAMM, 2004) criou e utilizou um outro método.

O algoritmo que carrega seu nome é um método de detecção de erros que utiliza uma estrutura algébrica chamada quasigrupo. Um quasigrupo é um conjunto Q com uma operação binária $\circ$ que é fechada, ou seja, para todos os elementos $a, b \in Q$, $a \circ b$ está em Q, e além disso satisfaz a propriedade de que para cada par de elementos $(a, b) \in Q$ existem elementos únicos x e y em Q tais que $a \circ x = b$ e $y \circ a = b$.

Neste algoritmo, o quasigrupo é representado por uma matriz (10×10), onde os elementos são dígitos de 0 a 9, e a operação $\circ$ é a indexação na matriz que é construída de forma a garantir que seja um quadrado latino, ou seja, que cada elemento de Q apareça uma e somente uma vez em cada linha e em cada coluna da tabela.

Tabela 3.6 – Quadrado Latino Damm

∘	0	1	2	3	4	5	6	7	8	9
0	0	3	1	7	5	9	8	6	4	2
1	7	0	9	2	1	5	4	8	6	3
2	4	2	0	6	8	7	1	3	5	9
3	1	7	5	0	9	8	3	4	2	6
4	6	1	2	3	0	4	5	9	7	8
5	3	6	7	4	2	0	9	5	8	1
6	5	8	6	9	7	2	0	1	3	4
7	8	9	4	5	3	6	2	0	1	7
8	9	4	3	8	6	1	7	2	0	5
9	2	5	8	1	4	3	6	7	9	0

O algoritmo funciona da seguinte forma: Cada dígito do número é mapeado para uma posição na tabela de permutação. Em seguida, são realizadas as permutações seguindo uma regra específica baseada nos dígitos do número. Uma vez concluídas as permutações, o resultado final é o dígito de verificação.

Formalmente, cada dígito do número é combinado com o resultado acumulado até aquele ponto. Dado o número de identificação $a_1 a_2 a_3 \ldots a_{n-1}$, o dígito verificador será dado pela equação

$(...((0 \circ a_1) \circ a_2) \circ a_3) \circ ...) \circ a_{n-1}$ e o resultado será o dígito verificador, ou seja,

$$(...((0 \circ a_1) \circ a_2) \circ a_3) \circ ...) \circ a_{n-1} = dv.$$

Sendo assim, o número $201918794-dv$, tem, segundo o método de Damm, o dígito verificador dado pela seguinte forma:

$$\begin{aligned}
\text{dv} &= (\ldots((0\circ 2)\circ 0)\circ 1)\circ 9)\circ 1)\circ 8)\circ 7)\circ 9)\circ 4 \\
&= (\ldots((1\circ 0)\circ 1)\circ 9)\circ 1)\circ 8)\circ 7)\circ 9)\circ 4 \\
&= (\ldots((7\circ 1)\circ 9)\circ 1)\circ 8)\circ 7)\circ 9)\circ 4 \\
&= (\ldots((9\circ 9)\circ 1)\circ 8)\circ 7)\circ 9)\circ 4 \\
&= (\ldots((0\circ 1)\circ 8)\circ 7)\circ 9)\circ 4 \\
&= (\ldots((3\circ 8)\circ 7)\circ 9)\circ 4 \\
&= (\ldots((2\circ 7)\circ 9)\circ 4 \\
&= (3\circ 9)\circ 4 \\
&= 6\circ 4 \\
\text{dv} &= 7
\end{aligned}$$

4 MÉTODOS E A DETECÇÃO DE ERROS

O presente trabalho se dedicou até o momento a determinar ou confirmar o dígito de checagem de números como o do cartão de crédito ou do código de barras de um produto.

Mas quando se faz uso dos números de identificação, sejam eles de produtos ou de pessoas, o dígito verificador já é conhecido e está incluso, sendo -nesse caso- sua existência de total aplicabilidade já que é nesse momento que ele garante a integridade e a validade do identificador. Para todos os métodos a maneira de checagem é a de refazer o caminho de forma inversa, ou seja, verificando se a equação ou método usado para a definição do dígito tem solução com o número fornecido.

A maneira é semelhante à de procurar solução ou soluções de uma equação, quando estamos determinando o dígito, e a de testar valores para verificar se satisfazem ou não a equação, quando utilizando o número de identificação completo. Por exemplo, a equação

$$2x + 3 = 5$$

Possui 1 como solução, pois

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

E

$$x^2 = 4$$

que possui 2 e (-2) como soluções, pois $2^2 = 4$ assim como $(-2)^2 = 4$.

No caso do método que utiliza a aritmética modular com a equação por complemento, $a_1p_1 + a_2p_2 + \ldots + a_{n-1}p_{n-1} + dv \equiv 0 \pmod{m}$ define o dígito de checagem dv. O computador em posse do número completo verifica se há ou não erro analisando.

Se

$$a_1p_1 + a_2p_2 + \ldots + a_{n-1}p_{n-1} + dv \equiv 0 \pmod{m}.$$

Caso isso não ocorra, ou seja,

$$a_1p_1 + a_2p_2 + \ldots + a_{n-1}p_{n-1} + dv \not\equiv 0 \pmod{m}.$$ Um erro foi cometido.

Ainda observando as semelhanças, note que não é interessante que um mesmo método aceite dois valores distintos como solução para a mesma equação, como no caso de uma equação do segundo grau com delta maior que zero. Nessa situação, existirão dois valores diferentes que, se trocados, resultarão em erro na digitação, mas, embora cometido, não seria identificado, pois a equação ainda seria solucionada, tornando a sentença verdadeira.

Em resumo, é isso que todos os métodos buscam: identificar todos os tipos de erros que possam ser cometidos. No entanto, é necessário que cada equação tenha solução única, já que qualquer erro acarretaria na não veracidade da sentença e, consequentemente, na detecção de erros, pois a equação não seria solucionada.

Um método perfeito seria aquele capaz de identificar todos os tipos de erros. Mas, caso isso não ocorra, ele deve identificar pelo menos os erros simples, caracterizados pela troca de a por b e os de transposição adjacente que são os que resultam da troca de ab por ba pois esses dois tipos - segundo a Tabela 1.1- representam aproximadamente 90% dos casos.

Sendo assim, neste capítulo será analisada a capacidade dos principais métodos usados para detecção dos dois principais tipos de erros catalogados.

4.1 MÉTODOS QUE UTILIZAM ARITMETICA MODULAR

Neste trabalho os métodos que fazem uso da aritmética modular representam todas as aplicações práticas.

4.1.1 Erro Simples

Um erro simples consiste na troca de a_i por b, com $a_i \neq b$. Sendo assim, quando cometido um erro desse tipo teremos

$$S = (p_1a_1) + (p_2a_2) + \ldots + (p_ia_i) + (p_{i-1}a_{i=1}) + \ldots + (p_{n-2}a_{n-2}) + (p_{n+1}a_{n+1}) + dv \equiv 0 \pmod{m}$$

Onde S representa a ausência de erro. Ocorrendo o erro teríamos

$$M = (p_1a_1) + (p_2a_2) + \ldots + (p_ib) + (p_{i-1}a_{i=1}) + \ldots + (p_{n-2}a_{n-2}) + (p_{n+1}a_{n+1}) + dv \equiv 0 \pmod{m}$$

Para que o erro não seja percebido, basta apenas que S e M deixem o mesmo resto na divisão por m. Sendo assim, pela Proposição 5,

$$(p_1a_1)+(p_2a_2)+\ldots+(p_ia_i)+(p_{i-1}a_{i=1})+\ldots+(p_{n-2}a_{n-2})+(p_{n-1}a_{n-1})+dv-[(p_1a_1)+(p_2a_2)+\ldots+(p_ib)+(p_{i-1}a_{i=1})+\ldots+(p_{n-2}a_{n-2})+(p_{n-1}a_{n-1})+dv]\equiv 0-0 \pmod{m}$$

$$\Rightarrow (p_1a_1)+(p_2a_2)+\ldots+(p_ia_i)+(p_{i-1}a_{i=1})+\ldots+(p_{n-2}a_{n-2})+(p_{n-1}a_{n-1})+dv-(p_1a_1)-(p_2a_2)-\ldots-(p_ib)-(p_{i-1}a_{i=1})-\ldots-(p_{n-2}a_{n-2})-(p_{n-1}a_{n-1})-dv\equiv 0 \pmod{m}$$

$$\Rightarrow (p_ia_i)-(p_ib)\equiv 0 \pmod{m}$$

$$\Rightarrow p_i(a_i-b)\equiv 0 \pmod{m}.$$

Note que $p_i(a_i-b)\equiv 0 \pmod{m}$ pode ser reescrita como uma congruência linear da forma $ax\equiv b \pmod{m}$, com $p_i=a$.

Como estamos interessados em encontrar uma solução única, já que qualquer duplicidade de soluções acarreta na não detecção de erros, temos que a congruência $p_i(a_i-b)\equiv 0 \pmod{m}$ deve ter uma e somente uma solução. O que acontece, segundo o Teorema 6 e o Corolário 2, quando $(p_i,m)=1$.

Portanto, todo erro deste tipo será detectado quando

$$(p_i,m)=1.$$

Exemplo 11.

Considere o número de identificação 337182-0, os pesos 1 e 2 e a equação por complemento módulo 10.

Agora considere que na ocorrência de um erro simples o novo número foi digitado como $387182-0$.

$$\begin{array}{cccccccc} & 3 & 8 & 7 & 1 & 8 & 2 \\ \times & & & & & & & \\ & 1 & 2 & 1 & 2 & 1 & 2 \\ \hline & 3 & 16 & 7 & 2 & 8 & 4 \end{array}$$

Como $40+0\equiv 0 \pmod{10}$ o erro não seria detectado.

Considere agora o número de identificação é 337182-4, mas com os pesos 1 e 3 e a equação por complemento.

Considere que na ocorrência de um erro simples o novo número foi digitado como $387182-4$.

$$\begin{array}{cccccccc} & 3 & 8 & 7 & 1 & 8 & 2 \\ \times & & & & & & & \\ & 1 & 3 & 1 & 3 & 1 & 3 \\ \hline & 3 & 24 & 7 & 3 & 8 & 6 \end{array}$$

Como $3+24+7+3+8+6+4=55$, mas $55 \not\equiv 0 \pmod{10}$ o erro seria detectado.

4.1.2 Erro de Transposição Adjacente

De maneira análoga, um erro de transposição adjacente ocorre na troca de $a_j a_i$ por $a_i a_j$ sendo necessário também para uma não detecção que da troca ainda resulte um valor que satisfaça a sentença. Considerando que N representa ausência de erro e L a presença, temos o seguinte

$$N = (p_1a_1)+(p_2a_2)+\ldots+(p_ia_i)+(p_{i+1}a_{i+1})+\ldots+(p_{n-2}a_{n-2})+(p_{n-1}a_{n-1})+dv \equiv 0 \pmod{m}$$

e

$$L = (p_1a_1)+(p_2a_2)+\ldots+(p_ia_{i+1})+(p_{i+1}a_i)+\ldots+(p_{n-2}a_{n-2})+(p_{n-1}a_{n-1})+dv \equiv 0 \pmod{m}.$$

Note que também podemos calcular a diferença, pela Proposição 5, o que nos daria

$$(p_ia_i)+(p_{i-1}a_{i-1})-[(p_ia_{i=1})+(p_{i-1}a_i)]$$

$$\Rightarrow (p_i-p_{i-1})(a_i-a_{i-1}).$$

Sendo assim, esse erro não seria detectado quando

$$(p_i-p_{i-1})(a_i-a_{i-1}) \equiv 0 \pmod{m}, \text{ ou seja, } m|(p_i-p_{i-1})(a_i-a_{i-1}).$$

Considerando o resultado anterior, podemos reescrever o resultado acima $(p_i-p_{i-1})(a_i-a_{i-1}) \equiv 0 \pmod{m}$ como uma congruência linear da forma $ax \equiv b \pmod{m}$ com$(p_i-p_{i-1}) = a$ o que, segundo o Teorema 6 e o Corolário 2, possui solução única quando $((p_i-p_{i-1}), m) = 1$

Portanto, todo erro deste tipo será detectado quando

$$(p_i - p_{i-1}, m) = 1.$$

Como visto no caso anterior, no qual as propriedades são as mesmas.

Por estes fatos, note que no caso em que m é um número primo, como no caso de $m = 11$, há uma vantagem em relação a $m = 10$, já que 11 é primo e com isso qualquer $0 < p_i < 10$ será coprimo com m.

Exemplo 12.

Considere o número de identificação $54249 - 6$, os pesos 2 e 4 e a equação por complemento módulo 10.

Agora considere a ocorrência de um erro de Transposição Adjacente e o novo número foi digitado como $54294 - 6$.

$$\begin{array}{cccccc} & 5 & 4 & 2 & 9 & 4 \\ \times & & & & & \\ & 2 & 4 & 2 & 4 & 2 \\ \hline & 10 & 16 & 4 & 36 & 8 \end{array}$$

Como $74 + 6 \equiv 0 \pmod{10}$ o erro não seria detectado.

Considere agora o número de identificação $54249 - 8$, mas com os pesos 1 e 2 e a equação por complemento.

Sendo cometido um erro de forma que o novo número seja $54294 - 8$, segue que

$$\begin{array}{cccccc} & 5 & 4 & 2 & 9 & 4 \\ \times & & & & & \\ & 1 & 2 & 1 & 2 & 1 \\ \hline & 5 & 8 & 2 & 18 & 4 \end{array}$$

Mas como $37 + 8 \not\equiv 0 \pmod{10}$ o erro seria detectado.

4.2 MÉTODO DE VERHOEFF

4.2.1 Erro Simples

Para que o método do Holandês baseado na teoria dos grupos não identifique um erro simples que ocorre da troca de a por b, com $a \neq b$, segue que o seguinte deve acontecer

$$\sigma^{m-1}a_1 * \sigma^{m-2}a_2 \ldots * \sigma a_{m-1} * dv = \sigma^{m-1}a_1 * \sigma^{m-2}b \ldots * \sigma a_{m-1} * dv$$

$$\Rightarrow \sigma^{m-2}a_2 = \sigma^{m-2}b$$

Como σ é uma permutação, para que $a_2 * \sigma(b) = \sigma(a_2) * b$ é necessário que $a_2 = b$, mas como $a_2 \neq b$ segue que $a_2 * \sigma(b) \neq \sigma b * (a_2)$.

Note também que, pela Proposição 13, D_5 é não-abeliano, ou seja, é não comutativo. Sendo assim observa-se que $a * \sigma(b) \neq b * \sigma(a)$, para a e b pertencentes a D_5. Isso nos garante que um erro simples é sempre identificado.

Exemplo 13.

Tome o número de identificação 245016-4 corretamente verificado pelo Algoritmo de Verhoeff.

Após a ocorrência de um erro simples resultando em 265016-4.

$$\sigma^6(2) * \sigma^5(6) * \sigma^4(5) * \sigma^3(0) * \sigma^2(1) * \sigma(6) * 4 =$$

$$= 2 * 6 * 9 * 0 * 1 * 7 * 4$$

$$= 8 * 9 * 0 * 1 * 7 * 4$$

$$= 4 * 0 * 1 * 7 * 4$$

$$= 4 * 1 * 7 * 4$$

$$= 0 * 7 * 4$$

$$= 7 * 4$$

$$= 8.$$

Como $8 \neq 0$, o erro seria detectado.

4.2.2 Erro de Transposição Adjacente

Como σ representa a permutação aplicada aos elementos de D, segue que por D ser um grupo, σ^k, $k \in \mathbb{N}$, também pertence a D. Daí temos que o método detecta os erros

de transposição adjacente pois

$$\sigma^k(a) * \sigma^{k+1}(b) \neq \sigma^k(b) * \sigma^{k+1}(a)$$

que pode ser escrito como

$$\sigma^k(a) * \sigma^k(\sigma(b)) \neq \sigma^k(b) * \sigma^k(\sigma(a))$$

e como $\sigma^k(a) \neq \sigma^k(b)$, de fato erros deste tipo são detectados e assim este método detecta todos os erros simples e todos os erros de transposição adjacente.

Exemplo 14.

Considere novamente o número 245016-4 corretamente verificado, mas por ocorrer um erro de transposição adjacente foi digitado como 240516-4.

Após este fato, segue que

$$\sigma^6(2) * \sigma^5(4) * \sigma^4(0) * \sigma^3(5) * \sigma^2(1) * \sigma(6) * 4 =$$

$$= 2 * 1 * 0 * 8 * 1 * 7 * 4$$

$$= 3 * 0 * 8 * 1 * 7 * 4$$

$$= 3 * 8 * 1 * 7 * 4$$

$$= 6 * 1 * 7 * 4$$

$$= 5 * 7 * 4$$

$$= 3 * 4$$

$$= 2$$

Como $2 \neq 0$, o erro seria detectado.

4.3 ALGORITMO DE DAMM

4.3.1 Erro Simples

Considerando um número de n dígitos $a_1a_2a_3 \ldots a_n$, no qual a_n é o dígito verificador dv, e a Tabela 3.6 , um número é considerado válido por este método se

$$(\ldots((0 \circ a_1) \circ a_2) \ldots \circ dv = 0$$

mas se

$$(\ldots((0 \circ a_1) \circ a_2)\ldots \circ dv \neq 0$$

o método o considera inválido, o que indica que houve um erro.

Vamos considerar um erro simples onde um dígito a_i é incorretamente substituído por b, com $a_i \neq b$.

Para que o método detecte o erro, devemos mostrar que o valor final do número com erro processado via agoritmo após a troca não será zero.

Considere o número $a_1a_2a_3\ldots a_{n-1}dv$ e

$$VC = (\ldots((0 \circ a_1) \circ a_2)\ldots \circ dv = 0$$

onde VC, pelo algoritmo, é válido e foi calculado corretamente.

Agora considere que a_i foi substituído erroneamente por b resultando no número $a_1a_2\ldots a_{i-1}ba_{i+1}\ldots a_{n-1}dv$ e então

$$VE = (\ldots((0 \circ a_1) \circ a_2) \circ a_3) \circ \ldots) \circ b) \circ a_{i+1}) \circ \ldots) \circ dv.$$

Precisamos mostrar que $VE \neq 0$.

Note que até a posição a_{i-1} VC e VE apresentam o mesmo valor que denotaremos por p, com p variando de 0 a 9.

Mas a partir daí, teremos

$$VC : (\ldots(p \circ a_i) \circ a_{i+1}) \circ dv$$

e

$$VE : (\ldots(p \circ b) \circ a_{i+1}) \circ dv$$

Como consideramos a Tabela 3.6, que representa um quasigrupo totalmente antissimétrico, (DAMM, 2004, p. 106) e um quasigrupo antissimétrico é um tipo de estrutura algébrica em que a operação binária satisfaz a propriedade de antissimetria, isso significa que para quaisquer elementos a e b no quasigrupo, $p \circ a_i \neq p \circ b$.

Esse valor $p \circ b$ propagará o erro nos cálculos subsequentes, uma vez que a sequência de operações subsequentes será diferente da original, resultando em um valor $VE \neq 0$.

Portanto, se a_i é trocado por b, o valor final VE não será zero. Isso prova que o algoritmo de Damm detecta qualquer erro simples, pois a substituição de qualquer dígito

a_i por um valor diferente b inevitavelmente resulta em um valor final diferente de zero, invalidando o número.

Exemplo 15.

O número 201918794-7 é considerado válido pelo Algoritmo de Damm. Considere um erro simples que deu origem ao número 201918784-7.

$$(\dots((0\circ 2)\circ 0)\circ 1)\circ 9)\circ 1)\circ 8)\circ 7)\circ 8)\circ 4)\circ 7 =$$

$$= (\dots((1\circ 0)\circ 1)\circ 9)\circ 1)\circ 8)\circ 7)\circ 8)\circ 4)\circ 7$$

$$= (\dots((7\circ 1)\circ 9)\circ 1)\circ 8)\circ 7)\circ 8)\circ 4)\circ 7$$

$$= (\dots((9\circ 9)\circ 1)\circ 8)\circ 7)\circ 8)\circ 4)\circ 7$$

$$= (\dots((0\circ 1)\circ 8)\circ 7)\circ 8)\circ 4)\circ 7$$

$$= (\dots((3\circ 8)\circ 7)\circ 8)\circ 4)\circ 7$$

$$= (\dots((2\circ 7)\circ 8)\circ 4)\circ 7$$

$$= ((3\circ 8)\circ 4)\circ 7$$

$$= (2\circ 4)\circ 7$$

$$= 8\circ 7$$

$$= 2$$

Como $2 \neq 0$, o erro seria detectado.

4.3.2 Erro de Transposição Adjacente

Um erro de transposição adjacente ocorre quando da troca de $a_i a_{i+1}$ por $a_{i+1}a_i$.

Considerando o número de n dígitos, $a_1a_2a_3\dots a_n$, no qual a_n é o dígito verificador dv, pelo método, este número será válido se

$$(\dots((0\circ a_1)\circ a_2)\dots)\circ a_i)\circ a_{i+1})\dots a_{n-1})\circ dv = 0$$

Caso contrário, o método considera o número inválido indicando que há um erro na digitação. Considere

$$VC = (\ldots((0 \circ a_1) \circ a_2)\ldots) \circ a_i) \circ a_{i+1})\ldots a_{n-1}) \circ dv$$

como sendo o número correto e sem erro, $VC = 0$.

Agora considere um erro de transposição adjacente, troca de $a_i a_{i+1}$ por $a_{i+1} a_i$, com $a_i \neq a_{i+1}$ resultando em

$$VT = (\ldots((0 \circ a_1) \circ a_2)\ldots) \circ a_{i+1}) \circ a_i)\ldots a_{n-1}) \circ dv$$

Este método detectarà o erro se $VT \neq 0$

Note que até a posição a_{i-1}, VC e VT têm o mesmo valor que denotaremos por s, com s variando de 0 até 9.

Desta forma, teremos

$$VC : s \circ a_i) \circ a_{i+1})\ldots a_{n-1}) \circ dv$$

e

$$VT : s \circ a_{i+1}) \circ a_i)\ldots a_{n-1}) \circ dv$$

Como $VC = 0$, devemos mostrar que $VT \neq 0$.

Devido à propriedade de antissimetria do quasigrupo, sabemos que:

$$s \circ a_i \neq s \circ a_{i+1}$$

e

$$s \circ a_{i+1} \circ a_i \neq s \circ a_i \circ a_{i+1}.$$

Essa diferença se propagará nos cálculos subsequentes, resultando em $VT \neq 0$.

Portanto, se os dígitos a_i e a_{i+1} são transpostos, o valor final VT não será zero. Isso prova que o algoritmo de Damm detecta qualquer erro de transposição adjacente, pois a troca de quaisquer dígitos adjacentes inevitavelmente resulta em um valor final diferente de zero, invalidando o número.

Exemplo 16.

Considere o número 201918794-7 que foi processado pelo Algoritmo de Damm e não apresenta erro e após a ocorrência de um erro de Transposição Adjacente o novo número seja 201918749-7.

$$(\ldots((0\circ 2)\circ 0)\circ 1)\circ 9)\circ 1)\circ 8)\circ 7)\circ 4)\circ 9)\circ 7 =$$

$$= (\ldots((1\circ 0)\circ 1)\circ 9)\circ 1)\circ 8)\circ 7)\circ 4)\circ 9)\circ 7$$

$$= (\ldots((7\circ 1)\circ 9)\circ 1)\circ 8)\circ 7)\circ 4)\circ 9)\circ 7$$

$$= (\ldots((9\circ 9)\circ 1)\circ 8)\circ 7)\circ 4)\circ 9)\circ 7$$

$$= (\ldots(0\circ 1)\circ 8)\circ 7)\circ 4)\circ 9)\circ 7$$

$$= (\ldots((3\circ 8)\circ 7)\circ 4)\circ 9)\circ 7$$

$$= (\ldots((2\circ 7)\circ 4)\circ 9)\circ 7$$

$$= ((3\circ 4)\circ 9)\circ 7$$

$$= (9\circ 9)\circ 7$$

$$= 0\circ 7$$

$$= 6$$

Como $6 \neq 0$, o erro seria detectado.

CONSIDERAÇÕES FINAIS

Indiscutivelmente a presença da matemática é notada em vários aspectos da sociedade e um deles é na tecnologia. Presente e aplicável no cotidiano, a matemática por meio dos dígitos verificadores se tornou indispensável.

Este trabalho destacou a relevância dos dígitos verificadores como ferramentas fundamentais para garantir a integridade de informações em sistemas numéricos cotidianos, como CPF, ISBN, cartões de crédito e códigos de barras. Através da aplicação da aritmética modular e da teoria dos grupos, métodos como os algoritmos de Verhoeff e Damm se mostraram robustos para detectar erros comuns, como os de transposição e digitação.

A aritmética modular, ainda que eficiente em muitos casos, apresenta limitações na detecção de erros, enquanto os algoritmos baseados na teoria dos grupos, sem aplicações práticas, proporcionam maior robustez e precisão, especialmente em contextos onde a segurança dos dados é primordial.

Dessa forma, com o crescimento da demanda por segurança e confiabilidade nas informações digitais, espera-se que o uso de métodos mais sofisticados continue a se expandir, proporcionando soluções mais eficazes para a proteção de dados.

REFERÊNCIAS

CANçADO, Ana Paula. **Grupo Diedral: o estudo de grupos de simetrias em polígonos regulares**. Dissertação (Trabalho de Conclusão de Curso) — Universidade Federal de São João del-Rei, São João del Rei, MG, 2016. Orientadora: Profa. Ma. Lorena Mara Costa Oliveira.

CERQUEIRA, Luciana Mota et al. Aritmética modular nos códigos de barras. Universidade Federal do Recôncavo da Bahia, 2015.

DAMM, H. Michael. **Total anti-symmetrische Quasigruppen**. Tese (Dissertation) — Philipps-Universität Marburg, Marburg, jul. 2004. Página 44.

GOULART, Ione Ferrarini. Interação humano-computador. 2023.

HEFEZ, Abramo; VILLELA, Maria Lúcia T. **Códigos Corretores de Erros**. 2nd. ed. Rio de Janeiro, Brazil: IMPA, 2017.

LIMA, Lucas Fabiano. Grupos de simetria i. **Isomorfismos, UFSCar, Sao Carlos**, 2011.

Hans Peter Luhn. **Computer for Verifying Numbers**. 1960. 2,950,048. Filed January 6, 1954.

SANTOS, José Plínio de Oliveira. **Introdução à Teoria dos Números**. 3ª. ed. [S.l.]: IMPA, 2020. 128 p. ISBN 978-85-244-0496-2.

SAVóIS, Josias Neubert. **Método para resolver equações diofantinas com coeficientes no conjunto dos números racionais**. 95 p. Dissertação (Dissertação (Mestrado)) — Universidade Federal do Rio Grande, Rio Grande, 2014. Mestrado Profissional em Matemática em Rede Nacional.

SOUZA, Natália Pedroza de et al. Uma análise dos esquemas de dígitos verificadores usados no brasil. Universidade do Estado do Rio de Janeiro, 2013.

SOUZA, Rodrigo Luiz de. Permutações, grupos e simetrias. **Ciência e Natura**, Universidade Federal de Santa Maria, v. 37, n. 3, p. 289–307, 2015.

VERHOEFF, J. **Error Detecting Decimal Codes**. 2nd printing. ed. Amsterdam: Mathematical Centre, 1975.

YARTEY, Joseph Nee Anyah. **Álgebra II**. Salvador, BA: Universidade Federal da Bahia, Instituto de Matemática e Estatística; Superintendência de Educação a Distância, 2017. 244 p. ISBN 978-8292-144-9.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
Campus Cajazeiras - Código INEP: 25008978
Rua José Antônio da Silva, 300, Jardim Oásis, CEP 58.900-000, Cajazeiras (PB)
CNPJ: 10.783.898/0005-07 - Telefone: (83) 3532-4100

Documento Digitalizado Restrito

TCC

Assunto:	TCC
Assinado por:	Marcos Farias
Tipo do Documento:	Anexo
Situação:	Finalizado
Nível de Acesso:	Restrito
Hipótese Legal:	Informação Pessoal (Art. 31 da Lei no 12.527/2011)
Tipo do Conferência:	Cópia Simples

Documento assinado eletronicamente por:

- **Marcos Lopes de Farias**, **ALUNO (201912020018) DE LICENCIATURA EM MATEMÁTICA - CAJAZEIRAS**, em 11/10/2024 16:53:48.

Este documento foi armazenado no SUAP em 11/10/2024. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1275140
Código de Autenticação: 4f0f9b302a