



Universidade do Estado do Rio de Janeiro
Centro de Tecnologia e Ciências
Instituto de Matemática e Estatística

Tancredo Ramos Duarte

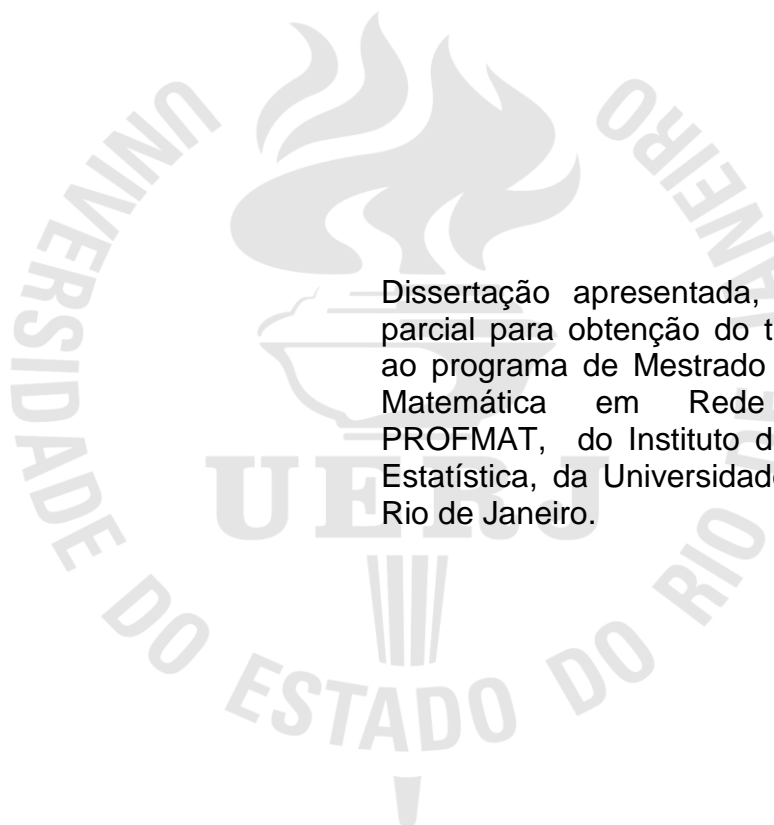
Algumas aplicações das congruências

Rio de Janeiro

2017

Tancredo Ramos Duarte

Algumas Aplicações das Congruências.



–Dissertação apresentada, como requisito parcial para obtenção do título de mestre, ao programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, do Instituto de Matemática e Estatística, da Universidade do Estado do Rio de Janeiro.

Orientador : Prof. Dr. Roberto Alfonso Olivares Jara

Rio de Janeiro

2017

CATALOGAÇÃO NA FONTE
UERJ / REDE SIRIUS / BIBLIOTECA CTC-A

D812 Duarte, Tancredo Ramos.
Algumas aplicações das congruências / Tancredo Ramos Duarte. –
2017.
74f. : il.

Orientador: Roberto Alfonso Olivares Jara.
Dissertação (Mestrado profissional em Matemática em Rede Nacional
- PROFMAT) - Universidade do Estado do Rio de Janeiro, Instituto de
Matemática e Estatística.

1. Congruências e restos - Teses. 2. Aritmética - Teses. I. Jara,
Roberto Alfonso Olivares. II. Universidade do Estado do Rio de Janeiro.
Instituto de Matemática e Estatística. III. Título.

CDU 512.533.2

Autorizo para fins acadêmicos e científicos, a reprodução total ou parcial
desta dissertação, desde que citada a fonte.

Assinatura

Data

Tancredo Ramos Duarte

Algumas Aplicações das congruências

Dissertação apresentada, como requisito parcial para obtenção do título de mestre, ao programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, do Instituto de Matemática e Estatística, da Universidade do Estado do Rio de Janeiro.

Aprovada em 07 de fevereiro de 2017.

Banca Examinadora:

Prof. Dr. Roberto Alfonso Olivares Jara (Orientador)
Instituto de Matemática e Estatística - UERJ

Prof. Dr. Helvécio Rubens Crippa
Instituto de Matemática e Estatística – UERJ

Prof. Dr. André Luiz Martins Pereira
Universidade Federal Rural do Rio de Janeiro

Rio de Janeiro

2017

DEDICATÓRIA

Dedico esse trabalho aos meus familiares e amigos, pelo apoio recebido.

AGRADECIMENTOS

Gostaria de agradecer, primeiramente, a Deus por esta oportunidade e por ter me dado força nos momentos mais difíceis. Aos meus pais, Anita e Donaciano, pela educação dada e pelas orações que fizeram. A minha irmã Giselda pelo companheirismo. A minha esposa Márcia e aos meus filhos Renan, Elisa e Jéssica que souberam entender a minha ausência por causa das obrigações que tinha com este trabalho. Ao meu professor e orientador Roberto Alfonso que esteve presente durante todo o processo de construção do mesmo. A todos os professores do Profmat por garantirem um curso de qualidade e, em especial, ao professor Sergio Luis, coordenador do curso. À secretária do curso Isabella pelo seu pronto atendimento, quando solicitada. À professora de Letras Luciana Romão que me orientou na coesão e coerência do texto. Ao programa Profmat pela oportunidade de crescimento e ao Capes pelo incentivo financeiro. A todos os colegas do curso que sempre me incentivaram. A todos aqueles que, de alguma forma, contribuíram para que esse objetivo fosse alcançado.

RESUMO

DUARTE, Tancredo Ramos. *Algumas aplicações das congruências*. 2017. 74f. Dissertação (Mestrado Profissional em matemática em Rede Nacional) - Instituto de Matemática e Estatística, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2017.

Este trabalho foi realizado visando mostrar que a matemática pode ser aplicada a situações relacionadas ao cotidiano e que algumas investigações inovadoras podem nos dar resultados, a princípio, inesperados. Inicialmente, apresentamos noções básicas sobre a divisibilidade mostrando as principais propriedades das congruências. Nessa pesquisa, abordamos o tema dígitos verificadores com ênfase nos principais documentos utilizados pelo cidadão brasileiro. Posteriormente, fizemos um estudo sobre o triângulo aritmético mostrando sua relação com o binômio de Newton e de que forma esse triângulo pode ser utilizado no cálculo das probabilidades. Além disso, foi dada uma nova configuração aplicada ao triângulo aritmético módulo m . Verificamos que suas principais propriedades continuam válidas em qualquer módulo e . Por fim, realizamos uma proposta pedagógica sobre o tema dígitos verificadores do RG e do CPF que podem ser inseridos no processo de ensino aprendizagem de forma lúdica, fazendo com que o aluno seja protagonista desse processo, realizando um paralelo com o cotidiano do mesmo.

Palavras-chave: Dígitos verificadores. Triângulo aritmético. Congruência.

ABSTRACT

DUARTE, Tancredo Ramos. *Some applications of congruences*. 2017. 74 f .
Dissertation (Professional Master Course on Mathematics in National Network) -
Institute of Mathematics and Statistics, State University of Rio de Janeiro, Rio de
Janeiro, 2017.

This work was carried out aiming to show that mathematics can be applied to situations related to daily life and that some innovative investigations can give us unexpected results in the beginning. First, we introduced the basic notions of divisibility showing the main properties of congruences. In this research, we approached the verifying digits theme with emphasis on the main documents used by the Brazilian citizen. After that, we developed a study on the arithmetic triangle showing its relation to Newton's binomial and how this triangle can be used in the calculation of probabilities. Furthermore, a new configuration was given to the arithmetic triangle module. We verified that its main properties remain valid in any module and, finally, we made a pedagogical proposition on the subject verifying digits of the RG and the CPF, that can be inserted in the process of teaching learning in a playful way, making the student a protagonist of this process, making a parallel with the daily life of the same student.

Keywords : Digits checkers . Arithmetical triangle. Congruence.

LISTA DE FIGURAS

Figura 1	–	Triângulo aritmético binomial.....	41
Figura 2	–	Triângulo aritmético.....	42
Figura 3	–	Triângulo aritmético genérico.....	51
Figura 4	–	Triângulo aritmético (mod 5).....	51
Figura 5	–	Triângulo aritmético (mod 7).....	52
Figura 6	–	Triângulo aritmético (mod 9).....	52
Figura 7	–	Triângulo aritmético (mod 10).....	53
Figura 8	–	Triângulo aritmético genérico (mod m).....	53
Figura 9	–	Triângulo aritmético (mod 2) com código de cores.....	57
Figura 10	–	Triângulo aritmético (mod 3) com código de cores.....	58
Figura 11	–	Triângulo aritmético (mod 5) com código de cores.....	58
Figura 12	–	Foto grupo 1 apresentando trabalho.....	65
Figura 13	–	Foto grupo 2 apresentando trabalho.....	65
Figura 14	–	Foto grupo 3 apresentando trabalho.....	66
Figura 15	–	Foto grupo 4 apresentando trabalho.....	66

LISTA DE ABREVIATURAS E SIGLAS

AC	Acre
AL	Alagoas
AM	Amazonas
AP	Amapá
BA	Bahia
CE	Ceará
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CNH	Carteira Nacional de Habilitação
CPF	Cadastro de Pessoa Física
DETRAN	Departamento Estadual de trânsito
DF	Distrito Federal
DENATRAN	Departamento Nacional de Trânsito
ENEM	Exame Nacional do Ensino Médio
ES	Espírito Santo
GO	Goiás
IBGE	Instituto Brasileiro de Geografia e Estatística
MA	Maranhão
MDC	Máximo Divisor Comum
MERCOSUL	Mercado Comum do sul
MG	Minas Gerais
MRP	Machine Readable Passport
MS	Mato Grosso do Sul
MT	Mato Grosso
OACI	Organização de Aviação Civil Internacional

PA	Pará
PB	Paraíba
PCN	Parâmetros curriculares Nacionais
PE	Pernambuco
PI	Piauí
PR	Paraná
RENAVAM	Registro Nacional de Veículos Automotores
RG	Registro geral
RIC	Registro de Identidade Civil
RJ	Rio de Janeiro
RN	Rio Grande do Norte
RO	Rondônia
RR	Roraima
RS	Rio Grande do Sul
SC	Santa Catarina
SE	Sergipe
SP	São Paulo
SPC	Serviço de proteção ao Crédito
TO	Tocantins
TSE	Tribunal Superior Eleitoral

SUMÁRIO

	INTRODUÇÃO	13
1	RESULTADOS PRELIMINARES	15
1.1	Os números inteiros	15
1.2	Divisibilidade nos inteiros	16
1.3	Algoritmo da divisão de Euclides	17
1.4	Máximo divisor comum	17
1.5	Teorema fundamental da aritmética	18
1.6	Congruências módulo m	19
1.7	Classes residuais	21
2	DÍGITOS VERIFICADORES	24
2.1	Dígitos verificadores dos documentos utilizados pelo cidadão em nosso país	25
2.2	Registro geral do estado do Rio de Janeiro	25
2.3	Cadastro de pessoa física	26
2.4	Passaporte	28
2.5	Carteira nacional de habilitação	29
2.6	Título eleitoral	31
2.7	Certidão de nascimento/casamento/óbito	33
2.8	Unicidade dos dígitos verificadores	35
2.9	A importância dos dígitos verificadores do CPF	36
3	ALGUMAS APLICAÇÕES DO TRIÂNGULO DE PASCAL	40
3.1	Fatorial	40
3.2	Números binomiais	40
3.3	Triângulo de Pascal	41
3.4	Binômio de Newton e o triângulo aritmético	46
3.5	O triângulo aritmético como ferramenta para o cálculo de probabilidades	49
3.6	A congruência módulo m no triângulo aritmético	50
3.7	Outras propriedades do triângulo aritmético	57
4	PROPOSTA PEDAGÓGICA	61
4.1	Descrição geral	61
	CONCLUSÃO	67

REFERÊNCIAS	68
APÊNDICE – Plano de aula	70

INTRODUÇÃO

A congruência é uma ferramenta de extrema importância quando queremos dar ênfase ao resto da divisão. Nesse trabalho, apresentamos algumas aplicações das congruências. Nosso foco é mostrar uma abordagem dos dígitos verificadores nos principais documentos utilizados pelos cidadãos brasileiros, apresentando toda a matemática envolvida na determinação desses dígitos. Realizamos também um enfoque diferenciado da congruência módulo m no triângulo aritmético, verificando que as propriedades do triângulo aritmético são válidas em qualquer módulo aplicado ao triângulo.

Nos dias atuais, devemos apresentar nossos conteúdos em sala de aula de forma contextualizada a situações do cotidiano do aluno. Como parte dos alunos do sexto ano possui RG e CPF, apresentamos uma proposta pedagógica para o estudo dos dígitos verificadores nessas turmas que terão, não apenas a oportunidade de verificar toda a matemática envolvida nesse processo, mas também a de trabalhar a questão da cidadania que está diretamente relacionada à obtenção desses documentos.

De forma geral, o triângulo aritmético possui aplicações consideráveis na matemática. Diante disso, apesar de não ser o foco principal desse trabalho daremos alguns exemplos das aplicações desse triângulo no desenvolvimento do binômio de Newton e no cálculo de algumas probabilidades.

Os objetivos desse trabalho são: Definir e apresentar os dígitos verificadores com ênfase nos documentos utilizados pelos cidadãos brasileiros; apresentar as propriedades do triângulo aritmético, verificando a validade das mesmas na congruência módulo m ; despertar a autonomia e incentivar o interesse dos alunos no processo de construção do conhecimento; perceber a matemática como ciência voltada à solução de problemas da atualidade.

Diante da dificuldade de trabalhar alguns conteúdos matemáticos inseridos na realidade dos alunos, o tema dígitos verificadores do RG e do CPF terá um papel importante na vida deles como cidadãos, pois os mesmos fizeram uma pesquisa na unidade escolar para saber a porcentagem dos alunos que possuem esses documentos e, posteriormente, foram protagonistas desse processo, onde ratificaram a importância desses na vida do cidadão e apresentaram para os demais alunos da unidade escolar a matemática envolvida na determinação desses dígitos.

Para o desenvolvimento desse trabalho, foram utilizadas pesquisas bibliográficas visando dar embasamento teórico ao mesmo. Foi realizada uma proposta pedagógica com uma turma do sexto ano da Escola Municipal de Formação Profissional Governador Portela, onde os alunos foram os atores principais do processo de ensino aprendizagem, apresentando o estudo sobre dígitos verificadores para as outras turmas da escola. Em relação à congruência no triângulo aritmético, não foi encontrada nenhuma referência bibliográfica que falasse especificamente desse assunto. Diante disso, os resultados obtidos foram produzidos pelo autor do trabalho com a supervisão do orientador.

1 RESULTADOS PRELIMINARES

Neste capítulo abordaremos alguns conceitos e resultados relacionados aos números inteiros. Dentre eles, a divisibilidade e a aritmética modular, para justificar o uso dessas ferramentas nos capítulos seguintes deste trabalho.

1.1 Os números inteiros

Vamos admitir que o leitor esteja familiarizado com o conjunto dos números inteiros.

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

Juntamente com as operações de adição $(a, b) \rightarrow a + b$ e de multiplicação $(a, b) \rightarrow ab$ (denotaremos ab por $a \cdot b$, ou ainda $a \times b$) que possuem as seguintes propriedades para quaisquer $a, a', b, b', c \in \mathbb{Z}$:

i) A adição e multiplicação são bem definidas:

Se $a = a'$ e $b = b'$, então $a + b = a' + b'$ e $ab = a'b'$.

ii) A adição e a multiplicação são comutativas:

$$a + b = b + a \text{ e } ab = ba.$$

iii) A adição e a multiplicação são associativas:

$$(a + b) + c = a + (b + c) \text{ e } (ab)c = a(bc).$$

iv) A adição e a multiplicação possuem (únicos) elementos neutros.

$$a + 0 = a \text{ e } a \cdot 1 = a.$$

v) A adição possui elementos simétricos:

Existe $b = -a$ tal que $a + b = 0$

vi) A multiplicação é distributiva com relação à adição.

$$a(b + c) = ab + ac.$$

Além disso, a operação de adição mais a existência de simétricos permitem definir a operação subtração, como a seguir:

Para qualquer par de inteiros a e b , o inteiro b menos a , denotado por $b - a$ é dado por:

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

O conjunto \mathbb{Z} possui um destacado subconjunto: O conjunto dos números naturais.

$$\mathbb{N} = \{1, 2, 3, \dots\}.$$

Admitiremos também que \mathbb{Z} tem as seguintes propriedades:

vii) Fechamento de \mathbb{N} : para todos $a, b \in \mathbb{N}$, tem-se que $a + b \in \mathbb{N}$, $ab \in \mathbb{N}$ e $0|a \nexists$.

viii) Tricotomia: Dados $a, b \in \mathbb{Z}$, uma e apenas uma, das seguintes possibilidades é verdadeira:

1) $a = b$ 2) $a < b$ 3) $a > b$.

ix) Princípio da Boa Ordenação: Se S é um subconjunto não vazio de \mathbb{Z} e limitado inferiormente, então S possui um menor elemento.

x) Propriedade Arquimediana: Dados $a, b \in \mathbb{Z}$, com $b \neq 0$. Então existe $n \in \mathbb{Z}$ tal que $nb > a$.

1.2 Divisibilidade nos inteiros

Dados a e $b \in \mathbb{Z}$, com $b \neq 0$, dizemos que b divide a , e escrevemos $b|a$ se existir $c \in \mathbb{Z}$ tal que $a = bc$. Caso b não divida a , escrevemos $b \nmid a$.

Como ilustração, $8|56$, pois $56 = 8 \cdot 7$

Seja b um número inteiro não nulo. Se b dividir a , dizemos que b é um divisor de a , que a é divisível por b ou ainda que a é múltiplo de b . Note que todo inteiro não nulo é um divisor de si mesmo e de zero.

Exemplo: $a|0$ pois $0 = a \cdot 0$ e $a|a$ pois $a = a \cdot 1$

Veremos agora, uma proposição que estabelece propriedades básicas da relação de divisibilidade.

Proposição 1.2.1: Sejam a, b e c inteiros não nulos e x e y inteiros quaisquer. Então:

(i) se $b|a$ e $a|b$, então $a = \pm b$.

(ii) se $c|b$ e $b|a$, então $c|a$.

(iii) se $c|a$ e $c|b$, então $c|(ax + by)$.

(iv) se $b|a$, então $|b| \leq |a|$.

(v) se $c|b$, então $c|ab$.

(vi) se $b|a$, então $bc|ac$.

Demonstração:

(i) se a' e b' são inteiros tais que $a = ba'$ e $b = ab'$, então $a = (ab')a' = a(a'b')$ e, daí, $a'b' = 1$. Logo, $a' = \pm 1$, donde segue que $a = \pm b$.

(ii) se $a = ba'$ e $b = cb'$, com $a', b' \in \mathbb{Z}$, então $a = (cb')a' = c(a'b')$, com $a'b' \in \mathbb{Z}$. Logo, $c|a$.

(iii) sejam $a = ca'$ e $b = cb'$, com $a', b' \in \mathbb{Z}$. Então $ax + by = ca'x + cb'y = c(a'x + b'y)$, com $a'x + b'y \in \mathbb{Z}$. Logo $c|(ax + by)$.

(iv) se $a = ba'$, com $a' \in \mathbb{Z}$, então $a \neq 0 \Rightarrow a' \neq 0$ e, daí, $|a'| \geq 1$. Logo $|a| = |ba'| = |b||a'| \geq |b|$.

(v) se $b = cb'$, com $b' \in \mathbb{Z}$, então $ab = c(ab')$, com $ab' \in \mathbb{Z}$. Logo $c|ab$

(vi) se $a = ba'$, com $a' \in \mathbb{Z}$, então $ac = (bc)a'$ e, daí, $bc|ac$.

1.3 Algoritmo da divisão de Euclides

Se um inteiro $b \neq 0$ não divide o inteiro a , é possível ainda efetuar a divisão de a por b , com resto. Esse resultado que demonstramos a seguir é um dos resultados mais importantes da teoria dos números inteiros.

Teorema 1.3.1: Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, existem únicos $q, r \in \mathbb{Z}$ tais que $a = bq + r$, com $0 \leq r < |b|$.

Os números inteiros q e r são respectivamente, o quociente e o resto da divisão de a por b .

Demonstração:

Suponha primeiramente que $b > 0$. Pela propriedade Arquimediana (propriedade (x) em 1.1), existe inteiro q tal que $q(-b) \geq -a$, logo $qb \leq a$. Pelo Princípio da boa Ordenação (propriedade (ix) em 1.1) podemos supor que q seja o maior inteiro tal que $bq \leq a$. Então $bq \leq a < b(q+1)$, de modo que $0 \leq a - bq < b$ e basta definir $r = a - bq$. Se $b < 0$, então $-b > 0$, donde existem q e $r \in \mathbb{Z}$ tais que $a = (-b)q + r$, com $0 \leq r < -b$. Daí, $a = b(-q) + r$, com $0 \leq r < -b = |b|$.

Para provar a unicidade, suponha, agora, que $a = bq + r = bq' + r'$, onde $q, q', r, r' \in \mathbb{Z}$ e $0 \leq r, r' < |b|$, então $|r - r'| < |b|$ e $b(q - q') = r' - r$. Se $q \neq q'$ então $|q - q'| \geq 1$, de modo que $|b| \leq |b| \cdot |q - q'| = |r' - r| < |b|$, uma contradição. Portanto, $q = q'$ e, daí $r = r'$.

1.4 Máximo divisor comum

Definição: Sejam a e b dois números inteiros. chama-se máximo divisor comum (*mdc*) de a e b o inteiro d com $d > 0$, que satisfaz as seguintes condições:

(i) $d|a$ e $d|b$.

(ii) se d' é um inteiro tal que $d'|a$ e $d'|b$, então $d'|d$, ou seja, todo divisor comum de a e b é também divisor de d .

Usaremos como notação $\text{mdc}(a, b) = d$.

Exemplo: Se $a = 18$ e $b = 12$, e se $D(m)$ é o conjunto dos divisores do inteiro m , então

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

$D(18) \cap D(12) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$. Portanto $d = \text{mdc}(18, 12) = 6$

Proposição 1.4.1 Sejam c e m dois números inteiros não ambos nulos. Se $\text{mdc}(c, m) = 1$, então existem inteiros x e y tais que $cx + my = 1$

Proposição 1.4.2 Se m , a e b são inteiros tais que $\text{mdc}(m, a) = 1$ e $m|ab$, então $m|b$.

(HEFEZ, 2013, P.96)

1.5 Teorema fundamental da aritmética

Definição: Um número $p \in \mathbb{Z}$ é dito primo se satisfaz as seguintes condições:

(i) $p > 1$.

(ii) Os únicos divisores de p são ± 1 e $\pm p$.

Logo, um número inteiro é primo quando possui exatamente dois divisores positivos distintos: 1 e ele próprio.

Um número maior do que 1 que não é primo, é dito composto.

Exemplo:

$D_+(2) = \{1, 2\} \Rightarrow 2$ é primo.

$D_+(3) = \{1, 3\} \Rightarrow 3$ é primo.

$D_+(4) = \{1, 2, 4\} \Rightarrow 4$ é composto.

$D_+(5) = \{1, 5\} \Rightarrow 5$ é primo.

$D_+(6) = \{1, 2, 3, 6\} \Rightarrow 6$ é composto.

Teorema 1.5.1: Todo número inteiro $a > 1$ é, um número primo ou pode ser escrito de maneira única como produto de números primos, ou seja, $a = p_1 \cdot p_2 \cdot \dots \cdot p_r$, com $p_1 \leq p_2 \leq \dots \leq p_r$ números primos.

(CAMINHA, 2013, P.35)

1.6 Congruências módulo m

Nesta unidade iremos abordar alguns conceitos e propriedades básicas das congruências. Conceitos esses, que terão grande relevância no desenvolvimento desse trabalho.

Definição: (Aritmética dos Restos)

Seja m um número natural. Diremos que dois números naturais a e b são congruentes módulo m se os restos de sua divisão Euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m , escreve-se:

$$a \equiv b \pmod{m}$$

Exemplo: $10 \equiv 26 \pmod{8}$ pois ambos 10 e 26 deixam o mesmo resto 2 ao serem divididos por 8 . Analogamente, $27 \equiv 15 \pmod{6}$, pois os restos da divisão de 27 e 15 por 6 , são iguais 3 .

Caso o número a não seja congruente ao número b módulo m , escrevemos $a \not\equiv b \pmod{m}$

Proposição 1.6.1: Sejam a , b e m números inteiros, com $m > 1$. Tem-se que:

$$a \equiv b \pmod{m} \text{ se, e somente se, } m|a - b.$$

Demonstração:

Suponha que $a \equiv b \pmod{m}$. Pelo algoritmo euclidiano temos, $a = q_1 \cdot m + r$ e $b = q_2 \cdot m + r$; com q_1 e $q_2 \in \mathbb{Z}$ e $0 \leq r < m$. Note que $a - b = (q_1 - q_2)m$. Logo $m|a - b$.

Reciprocamente, se $m|a - b$, então $a - b = q \cdot m$, com $q \in \mathbb{Z}$. Pelo algoritmo euclidiano temos $a = q_1 \cdot m + r_1$ e $b = q_2 \cdot m + r_2$; com $q_1, q_2 \in \mathbb{Z}$ e $0 \leq r_1, r_2 < m$. Como $a - b = q \cdot m$, $q_1 \cdot m + r_1 - (q_2 \cdot m + r_2) = qm$. Logo $m|r_1 - r_2$ com $0 \leq r_1, r_2 < m$. Daí $r_1 - r_2 = 0$, $r_1 = r_2$ e portanto $a \equiv b \pmod{m}$.

Observe que no exemplo acima vimos que $27 \equiv 15 \pmod{6}$. Agora, $27 - 15 = 12$ e como $6|12$, segue pela proposição 1.6.1 que $27 \equiv 15 \pmod{6}$.

A congruência é uma ferramenta poderosa para calcularmos o resto da divisão entre dois números inteiros, notoriamente para dividendos muito grandes. Em particular todo número é congruente módulo m ao resto de sua divisão por m e, portanto, é congruente módulo m a um dos números $0, 1, 2, 3, \dots, m - 1$.

Exemplo: 19 dividido por 3 deixa resto 1, pois $19 = 3 \cdot 6 + 1$. Logo podemos escrever que $19 \equiv 1 \pmod{3}$.

Proposição 1.6.2: (Propriedades das congruências) Sejam a, b, c, d e m números inteiros, com $m > 1$. Valem as seguintes propriedades:

- (i) $a \equiv a \pmod{m}$.
- (ii) se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.
- (iii) se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.
- (iv) se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$.
- (v) se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $ac \equiv bd \pmod{m}$.
- (vi) se $a \equiv b \pmod{m}$, então $a + c \equiv b + c \pmod{m}$.
- (vii) se $a \equiv b \pmod{m}$, então $ac \equiv bc \pmod{m}$.
- (viii) se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$, para $n \in \mathbb{N}$.
- (ix) se $a \equiv b \pmod{m}$ e $n|m$, então $a \equiv b \pmod{n}$.
- (x) se $\text{mdc}(c, m) = 1$ e $ac \equiv bc \pmod{m}$, então $a \equiv b \pmod{m}$.

Demonstração:

- (i) como $m|0$, então $m|a - a$, portanto $a \equiv a \pmod{m}$.
- (ii) se $a \equiv b \pmod{m}$, temos que $m|a - b$, logo $\exists k \in \mathbb{Z}$ tal que $a - b = mk$, multiplicando a última igualdade por (-1) , temos que $-(a - b) = -mk$, assim $b - a = m(-k)$, portanto $b \equiv a \pmod{m}$.
- (iii) se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então existem inteiros k e k' tais que: $a - b = mk$ e $b - c = mk'$, somando as duas igualdades membro a membro segue que $(a - b) + (b - c) = mk + mk' \Rightarrow a - c = m(k + k')$. Portanto temos que $m|(a - c)$, ou seja, $a \equiv c \pmod{m}$.
- (iv) se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então existem inteiros k e k' tais que: $a - b = mk$ e $c - d = mk'$, somando as duas igualdades membro a membro segue que $(a - b) + (c - d) = mk + mk' \Rightarrow (a + c) - (b + d) = m(k + k')$. Portanto temos que $m|[(a + c) - (b + d)]$, ou seja, $a + c \equiv b + d \pmod{m}$.
- (v) suponhamos que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$. Logo, $m|b - a$ e $m|d - c$. Basta notar que $bd - ac = d(b - a) + a(d - c)$ e, portanto $m|(bd - ac)$, ou seja, $ac \equiv bd \pmod{m}$.
- (vi) se $a \equiv b \pmod{m}$, temos que $a - b = mk$. Somando e substituindo c no primeiro membro da igualdade, temos: $a - b + c - c = mk \Rightarrow (a + c) - (b + c) = mk$. Portanto temos que $a + b \equiv b + c \pmod{m}$.

(vii) se $a \equiv b \pmod{m}$, temos que $a - b = mk$. Multiplicando ambos os lados da igualdade por c temos: $ac - bc = mkc$, Portanto $ac \equiv bc \pmod{m}$.

(viii) se $a \equiv b \pmod{m}$, então $m|a - b$. Sabendo que $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})$. como $m|a - b$, então $m|a^n - b^n$. Portanto $a^n \equiv b^n \pmod{m}$.

(ix) se $a \equiv b \pmod{m}$, então $m|a - b$. Como $n|m$, então $n|a - b$. Portanto $a \equiv b \pmod{n}$.

(x) se $ac \equiv bc \pmod{m} \Rightarrow m|(b - a)c \Rightarrow m|(b - a)$, pois $(c, m) = 1 \Rightarrow a \equiv b \pmod{m}$.

As três primeiras propriedades acima correspondem às propriedades reflexiva, simétrica e transitiva, respectivamente. Segue que a noção de congruência é uma relação de equivalência e as propriedades (iv) e (v) mostram que tal relação é compatível com as operações de adição e multiplicação nos inteiros. A seguir vamos determinar suas classes de equivalência.

1.7 Classes residuais

Dado um número inteiro $m > 1$. Vamos repartir o conjunto \mathbb{Z} dos números inteiros em subconjuntos, onde cada um deles é formado por todos os números inteiros que possuem o mesmo resto quando divididos por m . Logo temos a seguinte partição de \mathbb{Z} :

$$[0] = \{x \in \mathbb{Z}; x \equiv 0 \pmod{m}\}$$

$$[1] = \{x \in \mathbb{Z}; x \equiv 1 \pmod{m}\}$$

⋮

$$[m - 1] = \{x \in \mathbb{Z}; x \equiv m - 1 \pmod{m}\},$$

Note que $[m] = [0]$, $[m + 1] = [1]$, ...

O conjunto $[a] = \{x \in \mathbb{Z}; x \equiv a \pmod{m}\}$ é chamado classe residual módulo m do elemento a de \mathbb{Z} . O conjunto de todas as classes residuais módulo m será representado por \mathbb{Z}_m . Portanto $\mathbb{Z}_m = \{[0], [1], \dots, [m - 1]\}$

Proposição 1.7.1: As classes residuais possuem as seguintes propriedades:

- (i) $[a] = [b]$ se, e somente se, $a \equiv b \pmod{m}$;
- (ii) Se $[a] \cap [b] \neq \emptyset$, então $[a] = [b]$;
- (iii) $\bigcup_{a \in \mathbb{N}} [a] = \mathbb{Z}$.

Demonstração:

É imediata do fato que as congruências são uma relação de equivalência nos inteiros.

Proposição 1.7.2: Para cada $a \in \mathbb{Z}$ existe um, e somente um, $r \in \mathbb{Z}$, com $0 \leq r < m$, tal que $[a] = [r]$.

Demonstração:

De fato, tome r como sendo o resto da divisão euclidiana de a por m . Logo r é unicamente determinado e $a \equiv r \pmod{m}$. Portanto $[a] = [r]$.

Como para cada $0 \leq i, j \leq m - 1$, com $i \neq j$, tem-se $[i] \neq [j]$, existem exatamente m classes residuais distintas módulo m , a saber, $[0], [1], \dots, [m - 1]$.

Isto é, $\bigcup_{0 \leq i \leq m-1} [i] = \mathbb{Z}$.

Aritmética de \mathbb{Z}_m .

Podemos definir as seguintes operações em \mathbb{Z}_m :

Adição: $[a] + [b] = [a + b]$

Multiplicação: $[a] \cdot [b] = [a \cdot b]$.

Ambas estão bem definidas, devido as propriedades (iv) e (v) da Proposição 1.6.2. Além disso, gozam das seguintes propriedades:

Teorema 1.7.3: Para quaisquer que sejam $[a], [b], [c] \in \mathbb{Z}_m$, tem-se

(i) $([a] + [b]) + [c] = [a] + ([b] + [c])$. (Associatividade da adição)

(ii) $[a] + [b] = [b] + [a]$. (Comutatividade da adição)

(iii) $[a] + [0] = [a]$. ($[0]$ é o neutro da adição)

(iv) $[a] + [-a] = [0]$. ($[-a]$ é o inverso aditivo de $[a]$)

(v) $([a] \cdot [b]) \cdot [c] = [a] \cdot ([b] \cdot [c])$. (Associatividade da multiplicação)

(vi) $[a] \cdot [b] = [b] \cdot [a]$. (Comutatividade da multiplicação)

(vii) $[a] \cdot [1] = [a]$. ($[1]$ é o neutro da multiplicação)

(viii) $[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c]$. (Distributividade da multiplicação)

Demonstração:

Como propriedades análogas são válidas em \mathbb{Z} , usando-as nos inteiros, juntamente com a adição e multiplicação de \mathbb{Z}_m , prova-se facilmente todas essas propriedades.

O Teorema 1.7.3 mostra que \mathbb{Z}_m com as operações acima definidas é um anel comutativo com identidade. No caso de m ser um primo tem-se o seguinte resultado.

Teorema 1.7.4: \mathbb{Z}_m é corpo se, e somente se, m é um número primo.

Demonstração:

Suponhamos que m é primo. Então, dado um inteiro $1 < a \leq m - 1$ temos que $\text{mdc}(a, m) = 1$. Assim, pela Proposição 1.4.1, existem inteiros x, y tais que $ax + my = 1$. Logo, $[a].[x] = [a].[x] + [y].[m] = [a.x] + [y.m] = [ax + ym] = [1]$. O que mostra que qualquer elemento $\mathbb{Z}_m - \{[0]\}$ é invertível. Portanto \mathbb{Z}_m é corpo.

Reciprocamente, suponhamos que \mathbb{Z}_m é corpo. Para mostrar que m é primo, basta mostrar que m não é divisível pelos elementos do conjunto $\{2, 3, \dots, m - 1\}$. Assim, consideremos $a \in \{2, 3, \dots, m - 1\}$, Temos que $[a] \neq [0]$. Como \mathbb{Z}_m é corpo existe $[x] \in \mathbb{Z}_m - \{[0]\}$ tal que $[a].[x] = [1]$. Logo $ax - 1$ é divisível por m . Então existe $y \in \mathbb{Z}$ tal que $ax + my = 1$. Logo $\text{mdc}(a, m) = 1$. Portanto a não divide m , onde concluímos que m é primo.

Para maiores esclarecimentos, os assuntos deste capítulo podem ser encontrados em Caminha (2013), Hefez (2013),

2 DÍGITOS VERIFICADORES

Os dígitos verificadores são fundamentais no universo tecnológico. Estão presentes em incontáveis informações que são armazenadas e enviadas, especialmente, no contexto comercial. Sem esses códigos, as informações não seriam confiáveis em decorrência, principalmente, de erros humanos na digitação.

Dígitos verificadores são um ou mais caracteres acrescentados a uma cadeia de caracteres (numérica ou alfanumérica) original, que certifica e ou a corrige, dando maior segurança contra fraudes, erros de digitação ou leitura. Esses dígitos são formulados através de algoritmos, que podem ser públicos ou não.

Tais dígitos são utilizados em códigos de barra de produtos, números de conta corrente, documentos de identidade, CPF, CNPJ etc e têm grande importância no mundo comercial, na identificação civil, arrecadação de tributos, instituições financeiras e muitas outras áreas.

Os esquemas utilizados no Brasil têm como base teórica a aritmética modular. Denominamos sistema de dígito verificador de módulo n ao esquema de atribuição de um dígito a um identificador composto por m dígitos $a_1 a_2 a_3 \dots a_{m-1} a_m$ tal que seja atribuído um peso P_i para a posição a_i do identificador e o dígito verificador a_{m+1} é calculado para satisfazer a equação $\sum(P_i a_i) \pm a_{m+1} \equiv 0 \pmod{n}$, com $1 \leq i \leq m$, $0 \leq a_{m+1} < n$. A variação do sinal está relacionada ao documento que está sendo calculado o dígito verificador.

O objetivo da abordagem desse tema é analisar os esquemas de dígitos verificadores dos documentos utilizados pelo cidadão em nosso país e apresentar os esquemas na determinação dos dígitos do CPF e da identidade em turmas do sexto ano, uma vez que a maioria desses alunos já possui esses documentos. Além disso, apresentar toda a matemática envolvida nesses esquemas que é realizada por operações básicas estudadas nesse período, motivando nossos alunos e mostrando que a matemática de sala de aula pode ser contextualizada aos dígitos dos documentos que são utilizados por eles.

2.1 Dígitos verificadores dos documentos utilizados pelo cidadão em nosso país

O cidadão brasileiro utiliza vários documentos que são úteis em seu dia a dia e esse tema será abordado como divulgação. A idéia é mostrar de que forma ele pode ser trabalhado nas escolas, onde os alunos terão a possibilidade de verificar toda a matemática envolvida na determinação desses números, bem como o motivo pelo qual isso é feito visando evitar possíveis fraudes. Além disso, terão a oportunidade de saber qual a importância desses documentos no cotidiano.

2.2 Registro geral do estado do Rio de Janeiro

O registro geral – RG ou carteira de identidade é um documento de extrema importância para todo cidadão brasileiro. Ele é o principal documento de identificação do país e tem a finalidade de provar a identidade de uma pessoa, além de ser necessário para solicitação de outros documentos. Sem o RG não é possível abrir conta em banco, prestar concurso público, entre tantas outras coisas. Não há uma idade mínima para tirar o documento, que pode ser feito a qualquer tempo. Hoje as pessoas estão tirando o documento de identidade cada vez mais cedo. Os pais podem fazer o documento de seus filhos pela facilidade de transportá-los, pela exigência na compra de antibióticos, para cadastro em centros de saúde, para matrículas escolares, para obtenção do plano de saúde, para viagens ao exterior, entre outras coisas. Essa medida pode ajudar muito no caso de desaparecimento da criança, pois através das digitais ela pode ser identificada mais rápido e facilmente. As digitais do bebê são formadas durante a gestação, por isso não há necessidade de esperar muito tempo após o nascimento.

O correto seria que todos os cidadãos a cada 10 anos renovassem sua carteira de identidade, pelo fato de alteração na escrita e na foto. Há várias situações em que o RG não é aceito com data de expedição superior a 10 anos, como por exemplo, viagem para o exterior (ex. Argentina, Uruguai).

Determinação do Dígito de Verificador do RG.

O dígito verificador do RG é determinado através da aritmética modular (mod 10), ou seja, resto da divisão por dez, mas há também mais algumas operações matemáticas envolvidas nesse esquema.

A identidade é composta por nove dígitos, sendo os oito primeiros algarismos do identificador e o último é o dígito verificador. Nessa variante, após os algarismos do identificador serem multiplicados pelos pesos 1 e 2 alternadamente, em cada produto se $p_i a_i > 9$, digamos $p_i a_i = c_0 c_1$, onde $c_0 = 1$ e $c_1 \in \{0, 2, 4, 6, 8\}$, o número resultante do produto $p_i a_i$ deve ser substituído pela soma $c_0 + c_1$ de seus algarismos antes da aplicação do módulo.

Considerando os algarismos do identificador, como sendo $a_1, a_2, a_3, a_4, a_5, a_6, a_7$, e a_8 respectivamente, podemos definir a equação para o cálculo do dígito verificador a_9 como sendo: $(1a_1 + 2a_2 + 1a_3 + 2a_4 + 1a_5 + 2a_6 + 1a_7 + 2a_8) \pmod{10} = r$, onde o complemento de r para 10, ou seja, $(10 - r) = a_9$ que é o dígito verificador procurado.

Exemplo: Utilizaremos o número de identidade 09613435 – 8. Inicialmente multiplicamos todos os algarismos pelo seu peso correspondente:

$$\begin{array}{r}
 0 \quad 9 \quad 6 \quad 1 \quad 3 \quad 4 \quad 3 \quad 5 \\
 \times 1 \quad 2 \quad 1 \quad 2 \quad 1 \quad 2 \quad 1 \quad 2 \\
 \hline
 0 \quad 18 \quad 6 \quad 2 \quad 3 \quad 8 \quad 3 \quad 10
 \end{array}$$

Substituímos 18, obtendo $1 + 8 = 9$ e a 10, obtendo $1 + 0 = 1$ e a soma dos resultados é $0 + 9 + 6 + 2 + 3 + 8 + 3 + 1 = 32$. Como $32 \equiv 2 \pmod{10}$ temos como dígito verificador o complemento de 2 para 10, ou seja, 8 e assim fica determinado o dígito verificador da identidade. Caso o resto seja zero, o algarismo 0 será o dígito verificador.

2.3 Cadastro de pessoa física

Todo cidadão brasileiro tem um código que o identifica na Receita Federal, é o cadastro de pessoa física (CPF). O CPF é de grande importância na vida de todos nós, pois é através dele que estamos cadastrados na Receita Federal e sabemos que todos os anos temos que fazer a declaração de imposto de renda, declarando bens materiais e pagando uma taxa que varia de acordo com os ganhos anuais de cada um, e para que possamos colocar nossos filhos como dependentes na declaração de imposto de renda é necessário que o mesmo possua CPF. Para que as crianças de 0 a 18 anos sejam titulares de um plano de saúde, é exigido o

número do CPF. Logo, podemos notar sua importância desde os primeiros dias de nascimento de uma criança.

Além disso, quando vamos realizar compras em uma loja, o lojista pode consultar o número do CPF para verificar se o nosso nome está no SPC (serviço de proteção ao crédito), e então autorizar ou não a venda. Podemos ter também multas de trânsitos cadastradas em nosso CPF, quando as mesmas não são cadastradas no número do RENAVAM (registro nacional de veículos automotores) ou para o registro de nossa CNH (carteira nacional de habilitação). Como podemos ver, o CPF é um documento que devemos ter e conservá-lo, pois é de grande serventia em nossa vida. Como são muitos os CPFs no território nacional na intenção de evitar fraudes, os dígitos de verificação são obtidos por meio de operações matemáticas.

Temos ainda a informação que o nono dígito (da esquerda para direita) representa a região onde o CPF foi emitido. Observe a lista abaixo:

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

Determinação dos dígitos Verificadores do CPF.

Os dígitos verificadores do CPF são determinados através da aritmética modular (mod 11), ou seja, resto de divisão por onze, caso o resto da divisão por 11 seja 10 utilizamos o dígito 0, mas há também mais algumas operações matemáticas envolvidas nesse esquema.

O CPF é composto por onze dígitos, sendo os oito primeiros algarismos identificadores do contribuinte, o nono identifica o estado brasileiro onde ele é registrado e os dois últimos são os dígitos verificadores. Nessa variante, após os algarismos do identificador serem multiplicados pelos pesos 1, 2, 3, 4, 5, 6, 7, 8 e 9 respectivamente (para obtenção do primeiro dígito verificador) e pelos pesos 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9 (para obtenção do segundo dígito verificador).

Considerando os primeiros nove algarismos como sendo $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8$ e a_9 respectivamente, podemos definir a equação para o cálculo do dígito verificador como sendo: $(1a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9) \pmod{11} = a_{10}$, onde a_{10} é o primeiro dígito verificador procurado. Para o cálculo do segundo dígito verificador consideramos o ultimo dígito encontrado e podemos

escrever a equação $(0a_1 + 1a_2 + 2a_3 + 3a_4 + 4a_5 + 5a_6 + 6a_7 + 7a_8 + 8a_9 + 9a_{10}) \pmod{11} = a_{11}$, onde a_{11} é o segundo dígito verificador procurado.

Exemplo: Utilizaremos o número do CPF 028925257-13. Inicialmente multiplicamos cada algarismo pelo seu respectivo peso para obtenção do primeiro dígito verificador que é dado por:

$$\begin{array}{r} 0 \quad 2 \quad 8 \quad 9 \quad 2 \quad 5 \quad 2 \quad 5 \quad 7 \\ \times 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \\ \hline 0 \quad 4 \quad 24 \quad 36 \quad 10 \quad 30 \quad 14 \quad 40 \quad 63 \end{array}$$

A soma das parcelas é $0 + 4 + 24 + 36 + 10 + 30 + 14 + 40 + 63 = 221$.

Como $221 \equiv 1 \pmod{11}$, temos que o primeiro dígito verificador é 1. Agora multiplicamos cada algarismo pelo seu respectivo peso e o primeiro dígito verificador encontrado fará parte desse processo para obtenção do segundo dígito verificado que é dado por:

$$\begin{array}{r} 0 \quad 2 \quad 8 \quad 9 \quad 2 \quad 5 \quad 2 \quad 5 \quad 7 \quad 1 \\ \times 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \\ \hline 0 \quad 2 \quad 16 \quad 27 \quad 8 \quad 25 \quad 12 \quad 35 \quad 56 \quad 9 \end{array}$$

A soma das parcelas é $0 + 2 + 16 + 27 + 8 + 25 + 12 + 35 + 56 + 1 = 190$.

Como $190 \equiv 3 \pmod{11}$, temos que o segundo dígito verificador é 3. E assim temos determinado os dois dígitos verificadores.

2.4 Passaporte

O passaporte é um documento de extrema importância para o cidadão, pois o mesmo é obrigatório quando queremos viajar para o exterior, cujo destino não seja países do MERCOSUL. O número do passaporte no Brasil utiliza o padrão internacional MRP (Machine Readable Passport) definido pela OACI (organização de Aviação Civil Internacional)

Esse padrão consiste em duas linhas, cada uma com quarenta e quatro caracteres, onde a primeira contém somente informações sobre o passageiro. Utilizam-se as letras maiúsculas de A a Z e os dígitos de 0 a 9. No padrão existem campos de livre preenchimento que cada país pode adotar ou não. Além disso, os tamanhos dos identificadores podem variar dentro de certos limites. O símbolo < é usado como espaço vazio para levar em conta essas diferenças.

A primeira linha não possui nenhum esquema de dígitos verificadores. Na segunda linha os nove primeiros caracteres representam o identificador do passaporte, que é a informação onde vamos focar. Outros campos nessa linha são associados à nacionalidade do passageiro (BRA no caso dos brasileiros), data de nascimento, sexo, data de expedição do passaporte, campos livres e mais três dígitos verificadores associados a esses últimos dados descritos.

Determinação do dígito Verificador do Passaporte.

Para o cálculo do dígito verificador, é utilizada a equação direta e os pesos 7, 3 e 1. Sendo que os caracteres que podem ser alfanuméricos devem ser convertidos para o cálculo, através de um mapeamento das letras para números. A letra A é mapeada para 10, a letra B para 11 e assim sucessivamente e o caractere < é mapeado para 0. Vamos detalhar apenas a obtenção do dígito verificador do identificador.

Após as conversões alfanuméricas necessárias e considerando os primeiros nove algarismos como sendo $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8$ e a_9 respectivamente, podemos definir a equação para o cálculo do dígito verificador como sendo: $(7a_1 + 3a_2 + 1a_3 + 7a_4 + 3a_5 + 1a_6 + 7a_7 + 3a_8 + 1a_9) \pmod{10} = a_{10}$, onde a_{10} é o dígito verificador procurado.

Exemplo: Utilizaremos o passaporte F964114F<3. Inicialmente converte-se F para 15 e < para 0. Em seguida aplicam-se os pesos, somando os resultados do produto e o dígito verificador será o resto da divisão desse número por 10, pois é utilizado a aritmética modular (mod 10).

$$\begin{array}{r}
 15 \quad 9 \quad 6 \quad 4 \quad 1 \quad 1 \quad 4 \quad 15 \quad 0 \\
 \times 7 \quad 3 \quad 1 \quad 7 \quad 3 \quad 1 \quad 7 \quad 3 \quad 1 \\
 \hline
 105 \quad 27 \quad 6 \quad 28 \quad 3 \quad 1 \quad 28 \quad 45 \quad 0
 \end{array}$$

Os resultados são somados, obtendo-se $105 + 27 + 6 + 28 + 3 + 1 + 28 + 45 + 0 = 243$. Como $243 \equiv 3 \pmod{10}$ segue que o dígito verificador é 3.

2.5 Carteira nacional de habilitação

A CNH (carteira nacional de habilitação) emitida pelos DETRANS (Departamentos Estaduais de Trânsito) sob a orientação do DENATRAN (Departamento Nacional de Trânsito) é de extrema importância para o cidadão que

deseja conduzir veículo automotor, pois a mesma é obrigatória para condução de veículo automotor em via pública.

A CNH é dividida em várias categorias: Categoria ACC para condução de veículos de duas rodas, abaixo de 50 cilindradas; categoria A para condução de veículos automotores e elétricos, de duas ou três rodas, com ou sem carro lateral; categoria B para condução de veículos automotores e elétricos de quatro rodas cujo peso bruto total não exceda a três mil e quinhentos quilogramas e cujo lotação não exceda a oito lugares, excluído a do motorista; categoria AB para condução de veículos que englobam as categorias A e B simultaneamente; categoria C para condução de veículos automotores e elétricos utilizados em transporte de carga, cujo peso bruto total exceda a três mil e quinhentos quilogramas e não exceda a seis mil quilogramas, abrangendo ainda todos os veículos da categoria B; categoria D para condução de veículos automotores e elétricos utilizados no transporte de passageiros, cuja lotação exceda a oito lugares e todos os veículos abrangidos nas categorias B e C; categoria E para condução de combinação de veículos automotores e elétricos, em que a unidade tratora se enquadre nas categorias B, C ou D e ainda cuja unidade acoplada tenha seis mil quilogramas de peso bruto total ou mais.

Para obtenção da CNH é necessário que o cidadão já possua 18 anos completos e a formação do condutor compreende a realização de curso teórico técnico e de prática de direção veicular desenvolvidos em curso de formação de condutores.

Determinação dos Dígitos Verificadores da CNH.

Os dígitos verificadores da CNH são determinados através da aritmética modular (mod 11), ou seja, resto da divisão por 11, mas há algumas outras operações matemáticas envolvidas nesse esquema. Neste caso o identificador é constituído por onze dígitos, onde os dois últimos são os dígitos verificadores. Para o cálculo do primeiro dígito verificador são utilizados os pesos 9, 8, 7, 6, 5, 4, 3, 2 e 1 e do segundo os pesos 1, 2, 3, 4, 5, 6, 7, 8 e 9, existindo uma particularidade no cálculo desse segundo dígito, explicada adiante. No caso do resultado do resto da divisão ser 10 o primeiro dígito verificador será transformado em 0.

Considerando os primeiros nove algarismos como sendo $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8$ e a_9 respectivamente, podemos definir a equação para o cálculo do primeiro dígito verificador como sendo: $(9a_1 + 8a_2 + 7a_3 + 6a_4 + 5a_5 + 4a_6 + 3a_7 + 2a_8 +$

$1a_9) \pmod{11} = a_{10}$, onde a_{10} é o primeiro dígito verificador procurado. Para o cálculo do segundo dígito verificador podemos escrever a equação $(1a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9) \pmod{11} = r$, onde r representa o resto da divisão por 11.

O valor de a_{11} depende do resultado de r e do cálculo inicial de a_{10} .

- Se $a_{10} \neq 10$ e $r = 10$, então $a_{11} = 0$.
- Se $a_{10} \neq 10$ e $r \neq 10$, então $a_{11} = r$.
- Se $a_{10} = 10$ e $r \leq 2$, então $a_{11} = r$.
- Se $a_{10} = 10$ e $r > 2$, então $a_{11} = r - 2$.

Exemplo: Utilizaremos a carteira nacional de habilitação número 00275125796, inicialmente multiplicamos os nove primeiros dígitos pelos seus respectivos pesos, somamos os resultados e o resto da divisão por 11 será o primeiro dígito verificador.

$$\begin{array}{r} 0 \ 0 \ 2 \ 7 \ 5 \ 1 \ 2 \ 5 \ 7 \\ \times 9 \ 8 \ 7 \ 6 \ 5 \ 4 \ 3 \ 2 \ 1 \\ \hline 0 \ 0 \ 14 \ 42 \ 25 \ 4 \ 6 \ 10 \ 7 \end{array}$$

Os resultados são somados, obtendo-se $0 + 0 + 14 + 42 + 25 + 4 + 6 + 10 + 7 = 108$. Como $108 \equiv 9 \pmod{11}$, segue que o primeiro dígito verificador é 9.

O cálculo do segundo dígito verificador é dado por:

$$\begin{array}{r} 0 \ 0 \ 2 \ 7 \ 5 \ 1 \ 2 \ 5 \ 7 \\ \times 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \\ \hline 0 \ 0 \ 6 \ 28 \ 25 \ 6 \ 14 \ 40 \ 63 \end{array}$$

Os resultados são somados, obtendo-se $0 + 0 + 6 + 28 + 25 + 6 + 14 + 40 + 63 = 182$. Como $182 \equiv 6 \pmod{11}$, temos que $a_{10} \neq 10$ e $r \neq 10$, então $a_{11} = r$. Onde concluímos que o dígito verificador é 6, que foi o valor encontrado para r .

2.6 Título Eleitoral

O título eleitoral é emitido pelo TSE (tribunal superior eleitoral). O documento é necessário para que o brasileiro vote e participe da vida política do país, o mesmo pode ser obtido a partir dos 16 anos de forma facultativa até os 18 anos incompletos, mas após completar 18 anos todo cidadão deve adquirir seu título eleitoral, sujeito à multa caso não o faça. O voto é facultativo para os eleitores que já completaram 70 anos.

É exigida a quitação eleitoral do servidor público na hora da contratação, para tirar ou renovar o passaporte entre outros.

O número do título eleitoral é composto por 12 dígitos (13 no caso dos estados de SP e MG). Os oito primeiros são sequenciais e identificam o eleitor, os dois seguintes são referentes à unidade de federação de origem da inscrição e os dois últimos constituem os dígitos verificadores, determinados com base na aritmética modular (mod 11), ou seja, resto da divisão por 11.

Determinação dos Dígitos Verificadores do Título Eleitoral.

Para o cálculo do primeiro dígito verificador são utilizados os pesos 2, 3, 4, 5, 6, 7, 8 e 9 nos primeiros oito dígitos do identificador e, para o segundo dígito verificador, são utilizados os pesos 7, 8 e 9 nos dígitos a_9 , a_{10} e a_{11} respectivamente.

Considerando os primeiros oito algarismos como sendo $a_1, a_2, a_3, a_4, a_5, a_6, a_7$ e a_8 respectivamente, podemos definir a equação para o cálculo do primeiro dígito verificador como sendo: $(2a_1 + 3a_2 + 4a_3 + 5a_4 + 6a_5 + 7a_6 + 8a_7 + 9a_8) \pmod{11} = a_{11}$, onde a_{11} é o primeiro dígito verificador procurado, caso o resto da divisão seja 10 o primeiro dígito verificador será transformado em 0. Para o cálculo do segundo dígito verificador podemos escrever a equação $(7a_9 + 8a_{10} + 9a_{11}) \pmod{11} = a_{12}$, que é o segundo dígito verificador procurado.

Exemplo: Utilizaremos o título de eleitor número 0798 1719 0302. Inicialmente multiplicamos os oito primeiros dígitos pelos seus respectivos pesos, somamos os resultados e o resto da divisão por 11 será o primeiro dígito verificador.

$$\begin{array}{r} 0 \quad 7 \quad 9 \quad 8 \quad 1 \quad 7 \quad 1 \quad 9 \\ \times \underline{2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9} \\ 0 \quad 21 \quad 36 \quad 40 \quad 6 \quad 49 \quad 8 \quad 81 \end{array}$$

Os resultados são somados, obtendo-se $0 + 21 + 36 + 40 + 6 + 49 + 8 + 81 = 241$. Como $241 \equiv 10 \pmod{11}$, temos que o primeiro dígito verificador é 0, pois o resto 10 é transformado em 0.

O cálculo do segundo dígito verificador é dado por:

$$\begin{array}{r} 0 \quad 3 \quad 0 \\ \times \underline{7 \quad 8 \quad 9} \\ 0 \quad 24 \quad 0 \end{array}$$

Os resultados são somados, obtendo-se $0 + 24 + 0 = 24$. Como $24 \equiv 2 \pmod{11}$, portanto o segundo dígito verificador é 2.

2.7 Certidões de nascimento/casamento/óbito

A certidão de nascimento é um documento de extrema importância, sendo o primeiro passo para o pleno exercício da cidadania. Sem ela, o indivíduo deixa de ser percebido pelo estado e não pode exercer seus direitos civis, políticos, econômicos e sociais, não estando apto a obter a documentação básica para cadastrar-se em programas sociais, matricular-se em escolas, entre outras limitações. No caso das crianças, a falta de registro aumenta a vulnerabilidade ao trabalho infantil, à exploração sexual, ao aliciamento para atividades criminosas e ao tráfico de crianças.

A certidão de casamento é o documento onde fica registrado os dados relativos à união matrimonial. Na certidão ficam lavrados diversos dados como a data do casamento, o nome dos noivos, suas profissões, entre outros.

A certidão de óbito, da mesma forma que a de nascimento, exige seu registro na serventia de registro civil de pessoas naturais, sendo também obrigatório, ao morrer, que o registro seja feito, encerrando assim a personalidade civil da pessoa. Com base nessas informações apresentadas pelo cartório, o Instituto Brasileiro de Geografia e Estatística (IBGE) levanta estimativas de causas de mortalidade infantil, números de homicídios, expectativas de vida, entre outros para fundamentar políticas públicas a serem adotadas.

Essas certidões são instituídas pelo Ministério da Justiça a partir de 2010 e são compostas por 32 dígitos, onde o primeiro grupo de 6 dígitos identifica o cartório, o segundo grupo de 2 dígitos identifica o acervo, o terceiro grupo de 2 dígitos identifica o serviço do registro civil das pessoas naturais, o quarto grupo de 4 dígitos identifica o ano de registro, o quinto grupo de 1 dígito identifica o tipo do livro de registro, o sexto grupo de 5 dígitos identifica o número do livro, o sétimo grupo de 3 dígitos identifica o número da folha do livro e o oitavo grupo de 7 dígitos identifica o número de registro. Finalmente o nono grupo de 2 dígitos correspondem aos dígitos verificadores.

Determinação dos Dígitos Verificadores da Certidão de Nascimento/Casamento/Óbito.

Os dígitos verificadores dessas certidões são determinados através da aritmética modular (mod 11), ou seja, resto da divisão por 11, mas há outras operações matemáticas envolvidas nesse processo. Nesta variante os trinta

primeiros dígitos são multiplicados pelos pesos 2, 3, 4, 5, 6, 7, 8, 9, 10, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9, somamos os resultados e encontramos o resto da divisão por 11.

Considerando os trinta primeiros algarismos como sendo $a_1, a_2, a_3, \dots, a_{30}$ respectivamente, podemos definir a equação para o cálculo do primeiro dígito verificador como sendo $(2a_1 + 3a_2 + 4a_3 + 5a_4 + 6a_5 + 7a_6 + 8a_7 + 9a_8 + 10a_9 + 0a_{10} + 1a_{11} + 2a_{12} + 3a_{13} + 4a_{14} + 5a_{15} + 6a_{16} + 7a_{17} + 8a_{18} + 9a_{19} + 10a_{20} + 0a_{21} + 1a_{22} + 2a_{23} + 3a_{24} + 4a_{25} + 5a_{26} + 6a_{27} + 7a_{28} + 8a_{29} + 9a_{30}) \pmod{11} = a_{31}$ que é o primeiro dígito verificador. Caso o resto da divisão seja 10 utilizaremos 1 como sendo o dígito verificador.

Para o cálculo do segundo dígito verificador consideramos o último dígito encontrado e podemos utilizar a equação $(1a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 + 10a_{10} + 0a_{11} + 1a_{12} + 2a_{13} + 3a_{14} + 4a_{15} + 5a_{16} + 6a_{17} + 7a_{18} + 8a_{19} + 9a_{20} + 10a_{21} + 0a_{22} + 1a_{23} + 2a_{24} + 3a_{25} + 4a_{26} + 5a_{27} + 6a_{28} + 7a_{29} + 8a_{30} + 9a_{31}) \pmod{11} = a_{32}$ que é o segundo dígito verificador procurado. Caso o resto da divisão seja 10 utilizaremos 1 como sendo o dígito verificador.

Exemplo: Utilizaremos a certidão de Casamento número: 090530 01 55 2011 2 00014 096 0003117 65. Inicialmente multiplicamos cada algarismo pelo seu respectivo peso para obtenção do primeiro dígito.

$$\begin{array}{r}
 0 \ 9 \ 0 \ 5 \ 3 \ 0 \ 0 \ 1 \ 5 \ 5 \ 2 \ 0 \ 1 \ 1 \ 2 \ 0 \ 0 \ 0 \ 1 \ 4 \ 0 \ 9 \ 6 \ 0 \ 0 \ 0 \ 3 \\
 1 \ 1 \ 7 \\
 \times \underline{2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 10 \ 0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 10 \ 0 \ 1 \ 2 \ 3 \ 4 \ 5} \\
 \hline
 6 \ 7 \ 8 \ 9 \\
 0 \ 27 \ 0 \ 25 \ 18 \ 0 \ 0 \ 9 \ 50 \ 0 \ 2 \ 0 \ 3 \ 4 \ 10 \ 0 \ 0 \ 0 \ 9 \ 40 \ 0 \ 9 \ 12 \ 0 \ 0 \ 0 \ 18 \\
 7 \ 8 \ 63
 \end{array}$$

Somando as parcelas obtemos: $0 + 27 + 0 + 25 + 18 + 0 + 0 + 9 + 50 + 0 + 2 + 0 + 3 + 4 + 10 + 0 + 0 + 0 + 9 + 40 + 0 + 9 + 12 + 0 + 0 + 0 + 18 + 7 + 8 + 63 = 314$. Como $314 \equiv 6 \pmod{11}$, portanto o primeiro dígito verificador é 6.

O segundo dígito verificador é dado por:

0 9 0 5 3 0 0 1 5 5 2 0 1 1 2 0 0 0 1 4 0 9 6 0 0 0 3
 1 1 7 6
~~x~~ 1 2 3 4 5 6 7 8 9 10 0 1 2 3 4 5 6 7 8 9 10 0 1 2 3 4 5
 6 7 8 9
 0 18 0 20 15 0 0 8 45 50 0 0 2 3 8 0 0 0 8 36 0 0 6 0 0 0 15
 6 7 56 54

Somando as parcelas obtemos: $0 + 18 + 0 + 20 + 15 + 0 + 0 + 8 + 45 + 50 + 0 + 0 + 2 + 3 + 8 + 0 + 0 + 0 + 8 + 36 + 0 + 0 + 6 + 0 + 0 + 0 + 15 + 6 + 7 + 56 + 54 = 357$. Como $357 \equiv 5 \pmod{11}$, portanto o segundo dígito verificador é 5.

Observação: Registro de Identidade Civil.

Vale ressaltar que está sendo implantado no Brasil o registro de identidade civil (RIC) um cartão com chip que conterà os números do RG, CPF, título de eleitor, e ainda, informações do biótipo. O identificador será um número de onze dígitos, sendo o último o dígito verificador, que será calculado utilizando a aritmética modular (mod 11), com a utilização dos pesos 9, 8, 7, 6, 5, 4, 3, 2, 9 e 8. Isso caso não mudem nada até a implantação do sistema.

2.8 Unicidade dos dígitos verificadores

Os dígitos verificadores são unicamente determinados. Neste trabalho apresentamos a unicidade dos dígitos verificadores do CPF e do RG. De forma análoga, a unicidade dos dígitos verificadores dos outros documentos podem ser verificada.

Unicidade do dígito verificador do RG.

O dígito verificador de qualquer RG do estado do Rio de Janeiro é unicamente determinado. De fato, suponha por absurdo que exista um número a do RG cujos oito primeiros algarismos identificadores sejam a_1, a_2, \dots, a_8 e que tenha dois dígitos verificadores distintos, digamos $a = a_1 a_2 \dots a_8 - a_9$ e $a = a_1 a_2 \dots a_8 - b_9$, com $a_9 \neq b_9$. Logo, por definição segue que:

$10 - a_9 \equiv 1a_1 + 2a_2 + 1a_3 + 2a_4 + 1a_5 + 2a_6 + 1a_7 + 2a_8 \pmod{10}$ e
 $10 - b_9 \equiv 1a_1 + 2a_2 + 1a_3 + 2a_4 + 1a_5 + 2a_6 + 1a_7 + 2a_8 \pmod{10}$. Logo, pelas propriedades (ii) e (iii) da proposição 1.6.2, segue que $10 - a_9 \equiv 10 - b_9 \pmod{10}$, e, portanto $a_9 \equiv b_9 \pmod{10}$, como $0 \leq a_9, b_9 \leq 9$, temos que $a_9 = b_9$. Esta

contradição mostra que de fato o dígito verificador de qualquer RG é unicamente determinado.

Observação: Ressaltamos que caso $p_i a_i > 9$, ou seja, $p_i a_i = c_0 c_1$, utilizaremos o número $(c_0 + c_1)$ antes de aplicar o módulo aos produtos $(1a_1, 2a_2, 1a_3, 2a_4, 1a_5, 2a_6, 1a_7, 2a_8)$, como já explicado anteriormente.

Unicidade dos Dígitos de Verificação do CPF.

Os dígitos verificadores de qualquer número de CPF são unicamente determinados. De fato, suponha que exista um número a de CPF, cujos nove primeiros algarismos sejam a_1, a_2, \dots, a_9 (onde os oito primeiros a_1, a_2, \dots, a_8 são os identificadores do contribuinte e a_9 indica a estado do Brasil onde foi obtido) e que tenha dois possíveis pares de dígitos verificadores, digamos $a = a_1 a_2 \dots a_9 - a_{10} a_{11}$ e $a = a_1 a_2 \dots a_9 - b_{10} b_{11}$. Logo, por definição segue que:

$$a_{10} \equiv 1a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 \pmod{11} \text{ e,}$$

$1a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 \equiv b_{10} \pmod{11}$. Logo, pelas propriedades (ii) e (iii) da proposição 1.6.2, segue que $a_{10} \equiv b_{10} \pmod{11}$. E como $0 \leq a_{10}, b_{10} \leq 9$, $a_{10} = b_{10}$. Analogamente, como por definição

$$a_{11} \equiv 0a_1 + 1a_2 + 2a_3 + 3a_4 + 4a_5 + 5a_6 + 6a_7 + 7a_8 + 8a_9 + 9a_{10} \pmod{11} \text{ e,}$$

$$0a_1 + 1a_2 + 2a_3 + 3a_4 + 4a_5 + 5a_6 + 6a_7 + 7a_8 + 8a_9 + 9a_{10} \equiv b_{11} \pmod{11},$$

novamente pelas propriedades (ii) e (iii) da proposição 1.6.2, segue que $a_{11} \equiv b_{11} \pmod{11}$ e como $0 \leq a_{11}, b_{11} \leq 9$, tem-se a igualdade $a_{11} = b_{11}$. Isto mostra que, de fato, os dígitos verificadores de qualquer número de CPF são unicamente determinados.

2.9 A importância dos dígitos verificadores do CPF

Abordaremos aqui a importância dos dígitos verificadores do CPF no caso de erro na digitação de algum algarismo.

O erro de digitação ocorreu apenas em um algarismo

Seja $a = a_1 a_2 \dots a_9 - a_{10} a_{11}$ um número válido de CPF. Se uma pessoa digitar errado um dos 11 algarismos do CPF, esse CPF não será válido. De fato, vejamos os seguintes casos:

Caso 1: O erro foi em um dos dígitos verificadores a_{10} ou a_{11} .

Pela unicidade destes dígitos verificadores, esse novo CPF não será válido.

Caso 2: O erro ocorreu em qualquer um dos nove primeiros dígitos de a . Digamos em vez de digitar $a_1 a_2 \dots a_9$ foi digitado $a_1 a_2 \dots a_{i-1} b_i a_{i+1} \dots a_9$, com $b_i \neq a_i$ ($0 < i < 10$). Então teremos $1a_1 + 2a_2 + \dots + 9a_9 \equiv a_{10} \equiv 1a_1 + 2a_2 + \dots + ib_i + \dots + 9a_9 \pmod{11}$. Logo, pela propriedade (iii) da proposição 1.6.2, segue que $1a_1 + 2a_2 + \dots + 9a_9 \equiv 1a_1 + 2a_2 + \dots + ib_i + \dots + 9a_9 \pmod{11} \Rightarrow ia_i \equiv ib_i \pmod{11}$ e como $\text{mdc}(i, 11) = 1$, pela propriedade (x) da proposição 1.6.2, segue que $a_i \equiv b_i \pmod{11}$ e portanto $a_i = b_i$, o que é um absurdo, ou seja, se um dos nove primeiros algarismos for digitado errado, o algarismo verificador a_{10} também mudará e, mais uma vez, a unicidade do dígito verificador a_{10} será fundamental para invalidar o CPF neste caso.

O erro de digitação ocorreu em dois algarismos.

Seja $a = a_1 a_2 \dots a_9 - a_{10} a_{11}$ um número válido de CPF. Se uma pessoa digitar errado dois dos 11 algarismos do CPF, esse CPF não será válido. De fato, vejamos os seguintes casos:

Caso 1: O erro foi na digitação de um ou nos dois dígitos verificadores. Pela unicidade destes dígitos, o novo número de CPF não será válido.

Caso 2: O erro foi na digitação de dois dígitos dentre os nove primeiros dígitos. Digamos que em vez de digitar $a = a_1 a_2 \dots a_9 - a_{10} a_{11}$ foi digitado $b = a_1 a_2 \dots b_i \dots b_j \dots a_9 - a_{10} a_{11}$ com $b_i \neq a_i$ e $b_j \neq a_j$. Então $1a_1 + 2a_2 + \dots + ia_i + \dots + ja_j + \dots + 9a_9 \equiv a_{10} \equiv 1a_1 + 2a_2 + \dots + ib_i + \dots + jb_j + 9a_9 \pmod{11} \Rightarrow$

$$ia_i + ja_j \equiv ib_i + jb_j \pmod{11} \text{ (A)}$$

Note que $ia_i - ib_i + ja_j - jb_j \equiv 0 \pmod{11}$, então $i(a_i - b_i) + j(a_j - b_j) \equiv 0 \pmod{11}$, segue que $i(a_i - b_i) + j(a_j - b_j) = 11k$ com $k \in \mathbb{Z}$. O que nos mostra que caso haja erro de digitação de dois algarismos entre os nove primeiros, há possibilidades de que o primeiro dígito verificador seja satisfeito.

Exemplo: Utilizaremos o CPF válido 150691907-33 para ilustrar duas possibilidades em que o fato ocorre.

1ª possibilidade: em vez de digitar 1 e 5 foram digitados 6 e 8.

6	8	0	6	9	1	9	0	7
1	2	3	4	5	6	7	8	9
6	16	0	24	45	6	63	0	63

A soma das parcelas é $6 + 16 + 0 + 24 + 45 + 6 + 63 + 0 + 63 = 223$. Como $223 \equiv 3 \pmod{11}$, temos que o primeiro dígito verificador foi satisfeito.

$$i(a_i - b_i) + j(a_j - b_j) = 11k \Rightarrow 1(1 - 6) + 2(5 - 8) = -11. \text{ Temos } k = -1.$$

2ª possibilidade: Em vez de digitar 6 e 1 foram digitados 7 e 4.

$$\begin{array}{r} 1 \quad 5 \quad 0 \quad 7 \quad 9 \quad 4 \quad 9 \quad 0 \quad 7 \\ \times 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \\ \hline 1 \quad 10 \quad 0 \quad 28 \quad 45 \quad 24 \quad 63 \quad 0 \quad 63 \end{array}$$

A soma das parcelas é $1 + 10 + 0 + 28 + 45 + 24 + 63 + 0 + 63 = 234$. Como $234 \equiv 3 \pmod{11}$, temos que o primeiro dígito verificador foi satisfeito.

$i(a_i - b_i) + j(a_j - b_j) = 11k \Rightarrow 4(6 - 7) + 6(1 - 4) = -22$. Temos $k = -2$. Por outro lado,

$$\begin{aligned} 0a_1 + 1a_2 + 2a_3 + \dots + 9a_{10} &\equiv a_{11} \equiv 0a_1 + 1a_2 + 2a_3 + \dots + (i-1)b_i + \dots + \\ &(j-1)b_j + \dots + 9a_{10} \\ \pmod{11} &\Rightarrow (i-1)a_i + (j-1)a_j \equiv (i-1)b_i + (j-1)b_j \pmod{11} \end{aligned}$$

$$(ia_i + ja_j) - (a_i + a_j) \equiv (ib_i + jb_j) - (b_i + b_j) \pmod{11} \quad (\text{B})$$

De A e B segue que:

$$a_i + a_j \equiv b_i + b_j \pmod{11} \text{ e } a_i - b_i \equiv -(a_j - b_j) \pmod{11} \Rightarrow$$

$$i(a_i - b_i) \equiv -i(a_j - b_j) \pmod{11} \quad (\text{C})$$

Alem disso, de (A) tem-se que:

$$i(a_i - b_i) \equiv -j(a_j - b_j) \pmod{11} \quad (\text{D})$$

De (C) e (D) obtemos:

$-i(a_j - b_j) \equiv -j(a_j - b_j) \pmod{11}$. Agora, como $|a_j - b_j| < 11 \Rightarrow (a_j - b_j, 11) = 1$ e portanto $i \equiv j \pmod{11}$ e como $|i - j| < 11 \Rightarrow 11|i - j| \Leftrightarrow i = j$. E temos uma contradição. Isto mostra que se houver erro de digitação em dois dos nove primeiros algarismos, o primeiro dígito verificador poderá com muita sorte ser satisfeito, mas o segundo dígito não. Com isso, temos que os dígitos verificadores devem ser diferentes e, portanto, o CPF número $b = a_1 a_2 \dots b_i \dots b_j \dots a_9 - a_{10} a_{11}$ será inválido.

Para erros de três ou mais dígitos não é garantido que tais erros sejam detectados.

Os dígitos verificadores possuem relevância considerável principalmente no universo tecnológico, dando maior confiabilidade a uma série de informações evitando fraudes e erros humanos na digitação, entre outros.

Para maiores esclarecimentos, os assuntos desse capítulo podem ser encontrados em <http://www.cin.ufpe.br/~gdcc/matdis/aulas/binomial>, acessado em 21 de março de 2016, Souza (2013). Com exceção dos itens 2.8 Unicidade dos dígitos verificadores e 2.9 A importância dos dígitos verificadores do CPF, pois os mesmos foram produzidos pelo autor e seu orientador.

3 ALGUMAS APLICAÇÕES DO TRIÂNGULO DE PASCAL

Neste capítulo abordaremos o triângulo de Pascal apresentando suas principais propriedades. Mostraremos também o cálculo de algumas probabilidades com a utilização do triângulo aritmético e sua aplicação no desenvolvimento do binômio de Newton, mas o foco principal é mostrar que o triângulo aritmético escrito em qualquer módulo não invalida as propriedades verificadas no triângulo original, ou seja, mostraremos que aplicando a aritmética modular módulo m , as propriedades do triângulo aritmético continuam válidas. Primeiramente, apresentaremos as definições de fatorial e dos números binomiais.

3.1 Fatorial

Definição: Dado um número inteiro não negativo n , chamamos fatorial de n ou n fatorial o número $n!$ definido por:

$$0! = 1, \text{ para } n = 0$$

$$1! = 1, \text{ para } n = 1 \text{ e,}$$

$$n! = n(n-1)! = n(n-1)(n-2) \cdots 3 \cdot 2 \cdot 1, \text{ para } n \geq 2.$$

3.2 Números Binomiais

Definição: É chamado de número binomial o número $\binom{n}{k}$, com n e k inteiros não negativos, $n \geq k$, definido por $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ (n representa a ordem e k é a classe do número binomial).

Exemplo: $\binom{5}{3} = \frac{5!}{3!(5-3)!} = \frac{5 \cdot 4 \cdot 3!}{3! \cdot 2 \cdot 1} = 10.$

Como consequência imediata da definição acima, dado um número natural n temos que:

$$\binom{n}{0} = \binom{n}{n} = \frac{n!}{0!n!} = 1 \text{ e } \binom{n}{1} = \frac{n!}{1!(n-1)!} = \frac{n(n-1)!}{1(n-1)!} = n, \text{ para } n \geq 1.$$

Exemplo: $\binom{5}{0} = \frac{5!}{0!(5-0)!} = \frac{5!}{0! \cdot 5!} = 1.$

Exemplo: $\binom{5}{5} = \frac{5!}{5!(5-5)!} = \frac{5!}{5! \cdot 0!} = 1.$


```

1
1  1
1  2  1
1  3  3  1
1  4  6  4  1
1  5 10 10 5  1

```

Triângulo retângulo

```

          1
         1  1
        1  2  1
       1  3  3  1
      1  4  6  4  1
     1  5 10 10 5  1

```

Triângulo isóscele

Figura 2 – Triângulo aritmético até a nona linha

```

          1
         1  1
        1  2  1
       1  3  3  1
      1  4  6  4  1
     1  5 10 10 5  1
    1  6 15 20 15 6  1
   1  7 21 35 35 21 7  1
  1  8 28 56 70 56 28 8  1
 1  9 36 84 126 126 84 36 9  1

```

.....

Fonte: <http://www.cin.ufpe.br/~gdcc/matdis/aulas/binomial>

Observação: Por motivos práticos a contagem das linhas começará sempre da linha zero. Desta forma, a linha zero corresponde a $n = 0$, a linha um corresponde a $n = 1$ e assim por diante.

Propriedades do Triângulo Aritmético.

1ª propriedade: Toda linha começa e termina por 1.

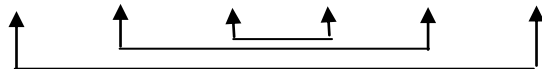
Demonstração:

De fato, para qualquer inteiro não negativo n , o primeiro elemento da linha n é $\binom{n}{0} = \frac{n!}{0!n!} = 1$ e, o último elemento dessa linha é $\binom{n}{n} = \frac{n!}{0!n!} = 1$.

Exemplo: linha 5 \rightarrow 1 5 10 10 5 1

2ª propriedade: Em uma mesma linha, os coeficientes binomiais equidistantes dos extremos são iguais.

Exemplo: Linha 5 \rightarrow $\binom{5}{0}$ $\binom{5}{1}$ $\binom{5}{2}$ $\binom{5}{3}$ $\binom{5}{4}$ $\binom{5}{5}$
 1 5 10 10 5 1


Demonstração:

Sejam $\binom{n}{k}$ e $\binom{n}{n-k}$ dois coeficientes equidistantes dos extremos. Têm-se que:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!(n-n+k)!} = \frac{n!}{k!(n-k)!} = \binom{n}{n-k} \text{ e, portanto, segue o resultado.}$$

Dois coeficientes binomiais equidistantes dos extremos são chamados de coeficientes binomiais complementares.

3ª propriedade: Relação de Stifel.

Somando quaisquer dois elementos consecutivos de uma mesma linha obtemos o elemento da linha seguinte, posicionado entre os dois elementos que foram somados.

Exemplo: Observe, no triângulo isóscele acima, que

$$\binom{6}{3} + \binom{6}{4} = 20 + 15 = 35 = \binom{7}{4}$$

Esta propriedade é considerada a propriedade mais importante do triângulo aritmético, pois nos permite construí-lo sem a necessidade de se calcular todos os coeficientes binomiais.

Demonstração:

Devemos demonstrar que se n e k são inteiros tais que $n > k \geq 0$, então

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}. \text{ De fato:}$$

$$\begin{aligned} \binom{n}{k} + \binom{n}{k+1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k-1)!} = \frac{n!}{k!(n-k-1)!} \left(\frac{1}{n-k} + \frac{1}{k+1} \right) = \frac{n!}{k!(n-k-1)!} \frac{n+1}{(n-k)(k+1)} \\ &= \frac{(n+1)!}{(n-k)!(k+1)!} = \binom{n+1}{k+1}, \text{ como queríamos demonstrar.} \end{aligned}$$

4ª propriedade: Teorema da soma das linhas.

A soma dos elementos da linha n é igual a 2^n .

Exemplo:

Linha 0	1					$\rightarrow 2^0$						
Linha 1		1	1			$\rightarrow 2^1$						
Linha 2			1	2	1	$\rightarrow 2^2$						
Linha 3				1	3	3	1	$\rightarrow 2^3$				
Linha 4					1	4	6	4	1	$\rightarrow 2^4$		
Linha 5						1	5	10	10	5	1	$\rightarrow 2^5$

Triângulo isóscele até a quinta linha

Demonstração:

Devemos provar que se n é inteiro tal que $n \geq 0$, então

$$S_n = \sum_{i=0}^n \binom{n}{i} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{n} = 2^n. \text{ De fato, temos que:}$$

Como $S_m = \binom{m}{0} + \sum_{i=1}^{m-1} \binom{m}{i} + \binom{m}{m}$, aplicando a relação de Stifel ao termo geral do somatório, concluímos que:

$$\begin{aligned} S_m &= \binom{m}{0} + \sum_{i=1}^{m-1} \binom{m-1}{i-1} + \sum_{i=1}^{m-1} \binom{m-1}{i} + \binom{m}{m} = \binom{m-1}{0} + \sum_{i=1}^{m-1} \binom{m-1}{i-1} \\ &+ \sum_{i=1}^{m-1} \binom{m-1}{i} + \binom{m-1}{m-1} = \sum_{i=1}^m \binom{m-1}{i-1} + \sum_{i=0}^{m-1} \binom{m-1}{i} = \sum_{i=0}^{m-1} \binom{m-1}{i-1} + \\ &\sum_{i=0}^{m-1} \binom{m-1}{i} \end{aligned}$$

fazendo a mudança de variável em um dos somatórios, concluímos que: $S_m = \sum_{i=0}^{m-1} \binom{m-1}{i} + \sum_{i=0}^{m-1} \binom{m-1}{i} = 2S_{m-1}$. Daí fazendo $m = 1, 2, 3, \dots, n$ no resultado acima, chegamos às equações:

$$S_1 = 2S_0$$

$$S_2 = 2S_1$$

$$S_3 = 2S_2$$

$$S_{n-1} = 2S_{n-2}$$

$$S_n = 2S_{n-1}$$

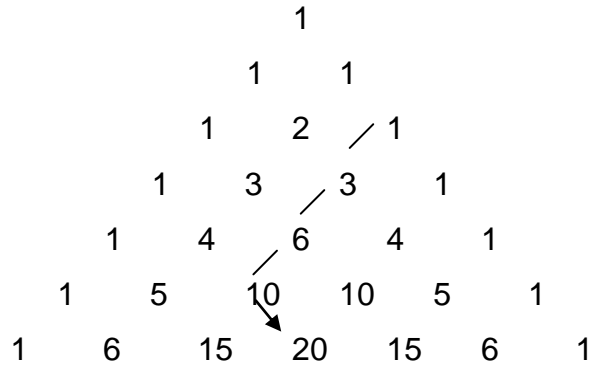
Assim aplicando o produto telescópico, ou seja, multiplicando (membro a membro) as n equações acima e eliminando os fatores comuns em ambos os membros, concluímos que:

$$S_n = 2^n S_0 \text{ e, como } S_0 = \sum_{i=0}^0 \binom{0}{i} = \binom{0}{0} = 1, \text{ segue que } S_n = 2^n.$$

5ª propriedade: Teorema da soma das diagonais.

Somando os elementos de uma mesma diagonal (que no caso de um triângulo retângulo seria de uma mesma coluna), iniciando pelo primeiro elemento da diagonal, obtemos o elemento situado abaixo e à direita da última parcela. Conforme ilustração abaixo.

Exemplo: $1 + 3 + 6 + 10 = 20$



Triângulo isósceles até a sexta linha

Demonstração:

Devemos provar que se n e k são inteiros tais que $n \geq 0$ e $k \geq 0$, então, $\sum_{i=0}^n \binom{k+i}{k}$
 $= \binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \dots + \binom{k+n}{k} = \binom{k+n+1}{k+1}$. De fato, Considerando
 $S_k = \sum_{i=0}^n \binom{k+i}{k}$, para $k \geq 0$, temos que: $S_k = \binom{k}{k} + \sum_{i=1}^n \binom{k+i}{k}$, e aplicando a
 relação de Stifel ao termo geral do somatório, concluímos que:

$$S_k = \binom{k}{k} + \sum_{i=1}^n \binom{k+i+1}{k+1} - \sum_{i=1}^n \binom{k+i}{k+1} = \binom{k+1}{k+1} + \sum_{i=1}^n \binom{k+i+1}{k+1} - \sum_{i=1}^n \binom{k+i}{k+1} = \sum_{i=0}^{n-1} \binom{k+i+1}{k+1} + \binom{k+n+1}{k+1} - \sum_{i=1}^n \binom{k+i}{k+1} = \sum_{i+1=1}^n \binom{k+i+1}{k+1} + \binom{k+n+1}{k+1} - \sum_{i=1}^n \binom{k+i}{k+1},$$

e ainda fazendo a mudança de variável em um dos somatórios, segue que:

$$S_k = \sum_{i=1}^n \binom{k+i}{k+1} + \binom{k+n+1}{k+1} - \sum_{i=1}^n \binom{k+i}{k+1} = \binom{k+n+1}{k+1},$$

como queríamos mostrar.

3.4 Binômio de Newton e o triângulo aritmético

O triângulo aritmético está diretamente relacionado aos coeficientes do desenvolvimento do binômio de Newton, ou seja, podemos utilizá-lo para auxiliar no desenvolvimento do binômio.

Binômio de Newton

Obteremos a fórmula para o desenvolvimento do binômio $(a + b)^n$, conhecido como binômio de Newton. Vale ressaltar que, para qualquer que seja o inteiro n tal que $n > 0$ podemos calcular o desenvolvimento do binômio como sendo: $(a + b)^n = (a + b)(a + b) \cdots (a + b)$, onde o termo $(a + b)$ será multiplicado por ele mesmo n vezes. Usando a propriedade distributiva da multiplicação temos que:

$$\text{Se } n = 0, (a + b)^0 = 1$$

$$\text{Se } n = 1, (a + b)^1 = a + b$$

$$\text{Se } n = 2, (a + b)^2 = a^2 + 2ab + b^2$$

$$\text{Se } n = 3, (a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

$$\text{Se } n = 4, (a + b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4, \text{ e assim por diante.}$$

À medida que o expoente n aumenta o desenvolvimento de $(a + b)^n$, torna-se mais complexo e as contas ficam mais trabalhosas. Daí surge a necessidade de generalização do desenvolvimento do binômio através de uma fórmula conhecida como o Teorema do Binômio de Newton. Alguns padrões podem ser observados nos desenvolvimentos realizados anteriormente.

- O desenvolvimento $(a + b)^n$ possui $n + 1$ elementos;
- Os coeficientes do desenvolvimento de $(a + b)^n$ são os elementos da linha n do triângulo aritmético;
- Os termos do desenvolvimento de $(a + b)^n$ são formados, além dos coeficientes, por $a^i b^j$ com $i = 0, 1, 2, \dots, n - 1, n$ e $j = n, n - 1, \dots, 2, 1, 0$.

Desse modo, podemos conjecturar a fórmula do binômio de Newton, conhecida como Teorema Binomial, apresentada a seguir.

Proposição 3.4.1: Se a e b são números reais e n é um inteiro não negativo, então:

$$(a + b)^n = a^n + \sum_{i=1}^{n-1} \binom{n}{i} a^{n-i} b^i + b^n = \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n-1} a^{n-(n-1)} b^{n-1} + b^n$$

Demonstração:

Considerando $S_m = \sum_{i=0}^m \binom{m}{i} a^{m-i} b^i$ para $m \geq 0$, temos que:

$S_m = \binom{m}{0} a^m + \sum_{i=1}^{m-1} \binom{m}{i} a^{m-i} b^i + \binom{m}{m} b^m$, e aplicando a relação de Stifel ao termo geral do somatório, concluímos que:

$$S_m = \binom{m}{0} a^m + \sum_{i=1}^{m-1} \binom{m-1}{i-1} a^{m-i} b^i + \sum_{i=1}^{m-1} \binom{m-1}{i} a^{m-i} b^i + \binom{m}{m} b^m = \binom{m-1}{0} a^m + \sum_{i=1}^{m-1} \binom{m-1}{i-1} a^{m-i} b^i + \sum_{i=1}^{m-1} \binom{m-1}{i} a^{m-i} b^i + \binom{m-1}{m-1} b^m = \sum_{i=1}^m \binom{m-1}{i-1} a^{m-i} b^i + \sum_{i=0}^{m-1} \binom{m-1}{i} a^{(m-1)-i} b^{i+1} + a \sum_{i=0}^{m-1} \binom{m-1}{i} a^{(m-1)-i} b^i$$
, e ainda, fazendo a mudança de variável em um dos somatórios, segue que:

$$S_m = b \sum_{i=0}^{m-1} \binom{m-1}{i} a^{(m-1)-i} b^i + a \sum_{i=0}^{m-1} \binom{m-1}{i} a^{(m-1)-i} b^i = b S_{m-1} + a S_{m-1} = (a+b) S_{m-1}$$
. Daí, fazendo $m = 1, 2, \dots, n$ no resultado obtido acima, chegamos às equações:

$$S_1 = (a+b) S_0$$

$$S_2 = (a+b) S_1$$

$$S_3 = (a+b) S_2$$

$$S_{n-1} = (a+b) S_{n-2}$$

$$S_n = (a+b) S_{n-1}$$

Assim, aplicando o produto telescópico, ou seja, multiplicando (membro a membro) as n equações acima e eliminando os fatores comuns em ambos os membros, concluímos que:

$S_n = (a+b)^n S_0$, como $S_0 = \sum_{i=0}^0 \binom{0}{i} a^i b^i = \binom{0}{0} a^0 b^0 = 1$, segue que

$S_n = (a+b)^n$, como queríamos mostrar.

Relação entre o Triângulo Aritmético e o Binômio de Newton.

Utilizando o teorema do binômio de Newton, façamos o desenvolvimento $(a+b)^n$, para $n = 0, 1, 2, 3, 4$ e 5 .

$$(a + b)^0 = \binom{0}{0} a^0 b^0$$

$$(a + b)^1 = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1$$

$$(a + b)^2 = \binom{2}{0} a^2 b^0 + \binom{2}{1} a^1 b^1 + \binom{2}{2} a^0 b^2$$

$$(a + b)^3 = \binom{3}{0} a^3 b^0 + \binom{3}{1} a^2 b^1 + \binom{3}{2} a^1 b^2 + \binom{3}{3} a^0 b^3$$

$$(a + b)^4 = \binom{4}{0} a^4 b^0 + \binom{4}{1} a^3 b^1 + \binom{4}{2} a^2 b^2 + \binom{4}{3} a^1 b^3 + \binom{4}{4} a^0 b^4$$

$$(a + b)^5 = \binom{5}{0} a^5 b^0 + \binom{5}{1} a^4 b^1 + \binom{5}{2} a^3 b^2 + \binom{5}{3} a^2 b^3 + \binom{5}{4} a^1 b^4 + \binom{5}{5} a^0 b^5,$$

Triângulo isóscele do Teorema binomial até a quinta linha

Calculando os coeficientes binomiais acima temos:

$$(a + b)^0 = 1$$

$$(a + b)^1 = 1a + 1b$$

$$(a + b)^2 = 1a^2 + 2ab + 1b^2$$

$$(a + b)^3 = 1a^3 + 3a^2b + 3ab^2 + 1b^3$$

$$(a + b)^4 = 1a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + 1b^4$$

$$(a + b)^5 = 1a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + 1b^5$$

Triângulo isóscele dos coeficientes binomiais até a quinta linha

$$\begin{array}{cccccc}
 & & & & & & 1 \\
 & & & & & & & 1 & & 1 \\
 & & & & & & 1 & & 2 & & 1 \\
 & & & & & & & 1 & & 3 & & 3 & & 1 \\
 & & & & & & & & 1 & & 4 & & 6 & & 4 & & 1 \\
 & & & & & & & & & 1 & & 5 & & 10 & & 10 & & 5 & & 1
 \end{array}$$

Triângulo isoscele aritmético até a quinta linha

Podemos observar que os coeficientes do desenvolvimento do binômio são iguais a sua respectiva linha no triângulo aritmético, ou seja, o triângulo aritmético é uma ferramenta que poderá ser utilizado para facilitar a determinação dos coeficientes do desenvolvimento do binômio de Newton, não sendo necessário o cálculo dos números binomiais correspondentes.

3.5 O triângulo aritmético como ferramenta para cálculo de probabilidades

Os números que formam esse curioso triângulo estão diretamente relacionados à análise combinatória, binômio de Newton e probabilidades. Já vimos anteriormente que a soma de qualquer linha desse triângulo é uma potência de base 2, logo os problemas de contagem ou probabilidades, em que cada experimento tenha apenas duas opções de escolha (masculino ou feminino, cara ou coroa, verdadeiro ou falso, etc), podem ter nesse triângulo um poderoso auxílio. Para ilustrar vamos realizar alguns exemplos:

Exemplo: Uma mulher pretende ter quatro filhos ou filhas. Quantas são as possibilidades desse experimento?

Solução: São $2^4 = 16$ que corresponde ao somatório da quarta linha do triângulo aritmético.

Exemplo: Quantas são as possibilidades para que essa mulher tenha quatro filhos do sexo masculino?

Solução: 1 possibilidade que corresponde ao primeiro número da quarta linha do triângulo aritmético.

Exemplo: Quantas são as possibilidades de que essa mulher tenha 3 filhos e 1 filha?

Solução: 4 possibilidades que correspondem ao segundo elemento da quarta linha.

Exemplo: Quantas são as possibilidades de que essa mulher tenha 2 filhos e 2 filhas?

Solução: 6 possibilidades que correspondem ao terceiro elemento da quarta linha.

Exemplo: Quantas são as possibilidades de que essa mulher tenha 1 filho e 3 filhas?

Solução: 4 possibilidades que correspondem ao quarto elemento da quarta linha.

Exemplo: Quantas são as possibilidades de que essa mulher tenha 4 filhas?

Solução: 1 possibilidade que corresponde ao último elemento da quarta linha.

Exemplo: Se essa mulher teve realmente quatro filhos, qual é a probabilidade de que seus filhos sejam 2 de cada sexo?

Solução: $\frac{6}{16} = \frac{3}{8} = 0,375 = 37,5\%$ Linha 4 \rightarrow 1 4 6 4 1

Relacionando os problemas acima com o binômio de Newton e considerando 'a' como sendo o nascimento de filhos e 'b' de filhas, temos:

$(a + b)^4 = 1a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + 1b^4$, note que o coeficiente 1 do termo a^4 corresponde a 4 filhos do sexo masculino, o coeficiente 4 do termo a^3b corresponde

a 3 filhos do sexo masculino e 1 do sexo feminino, o coeficiente 6 do termo a^2b^2 corresponde a 2 filhos do sexo masculino e 2 do sexo feminino, o coeficiente 4 do termo ab^3 corresponde a 1 filho do sexo masculino e 3 filhos do sexo feminino e o coeficiente 1 do termo b^4 corresponde a 4 filhos do sexo feminino.

Exemplo: No lançamento de cinco moedas distintas e não viciadas, qual é a probabilidade de se obter 3 caras e 2 coroas?

Solução: Vamos utilizar como auxílio para a solução desse problema a linha 5 do triângulo aritmético.

Linha 5 \rightarrow 1 5 10 10 5 1 $\rightarrow 2^5$

Número de caras \rightarrow 0 1 2 3 4 5

O coeficiente correspondente à opção 3 caras e 2 coroas é igual a 10, como o número de elementos do espaço amostral é igual a $2^5 = 32$, a probabilidade procurada é igual a $\frac{10}{32} = \frac{5}{16} = 0,3125 = 31,25\%$

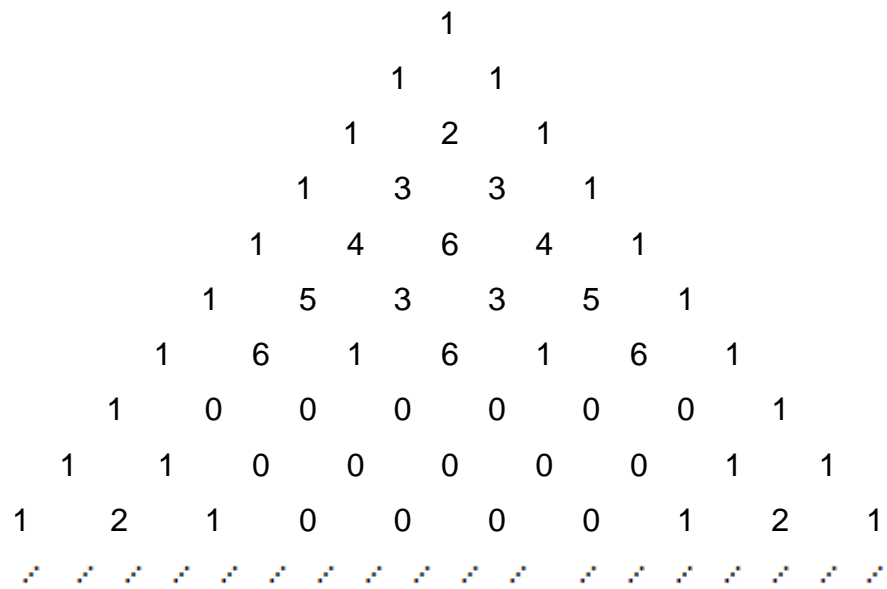
3.6 A congruência módulo m no triângulo aritmético

Abordaremos a congruência no triângulo aritmético, ou seja, apresentaremos o triângulo aritmético em alguns módulos e observaremos que todas as propriedades citadas anteriormente continuam válidas. Nosso objetivo principal é mostrar que essas propriedades são válidas no módulo m . Lembramos que no triângulo aritmético escrito no módulo 2, teremos apenas os algarismos 0 e 1, que são os possíveis restos na divisão por 2. Já no triângulo aritmético escrito no módulo 3, teremos apenas os algarismos 0, 1 e 2 que são os possíveis restos na divisão por 3, e assim por diante.

Apresentaremos também os triângulos escritos, de forma que cada resto represente uma cor, para que seja possível observarmos algum padrão nesse processo.

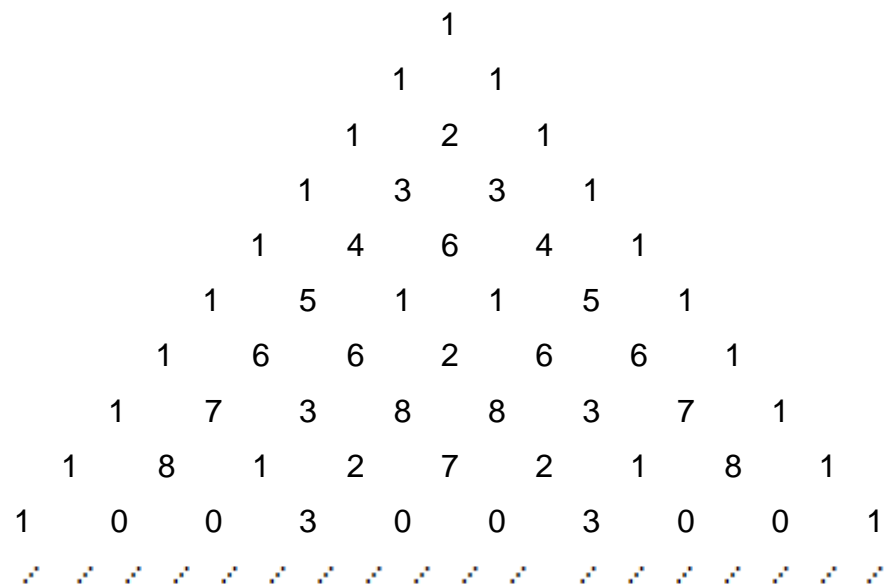
Denotaremos por A_{nk} ao elemento da linha n e da coluna k , do triângulo aritmético. Logo $A_{nk} = \binom{n}{k}$, para cada par de inteiros n e k tais que $n \geq k \geq 0$. Assim temos:

Figura 5 – Triângulo aritmético (mod 7)



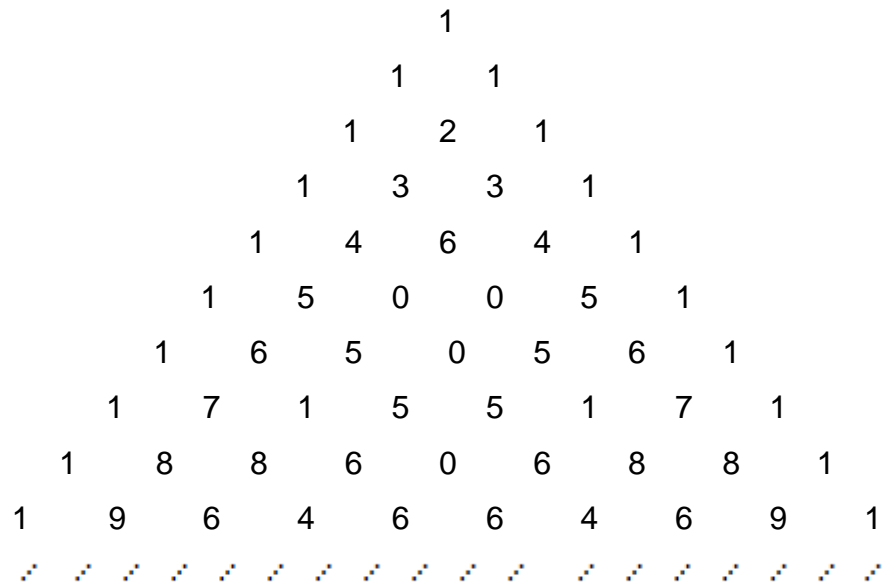
Fonte: O autor, 2016

Figura 6 – Triângulo aritmético (mod 9)



Fonte: O autor, 2016

Figura 7 – Triângulo aritmético (mod 10)

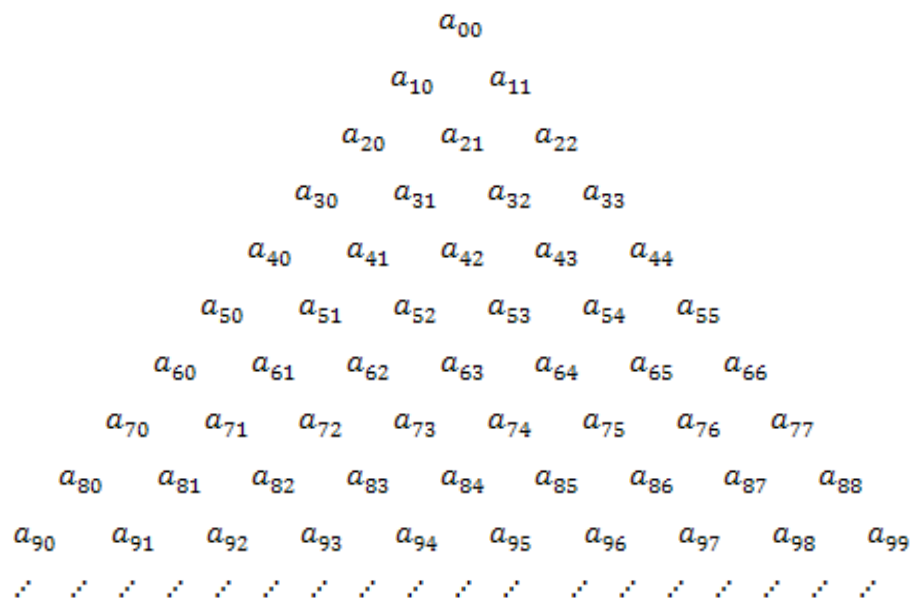


Fonte: O Autor, 2016

Triângulo Aritmético Módulo m .

Primeiramente, vamos definir o triângulo aritmético genérico módulo m , onde m é qualquer inteiro maior que um.

Definição: O triângulo aritmético módulo m consiste dos elementos a_{nk} tais que $A_{nk} \equiv a_{nk} \pmod{m}$, onde a_{nk} representa o resto da divisão de A_{nk} por m . Logo, tal triângulo é obtido substituindo os A_{nk} do triângulo genérico pelos restos a_{nk} .

Figura 8 – Triângulo aritmético genérico (mod m)

Fonte: O Autor, 2016

Já vimos que no triângulo aritmético temos várias propriedades. Nos livros didáticos usuais, este assunto é apresentado sem maiores desdobramentos. Aqui mostraremos outra abordagem envolvendo congruências. Partiremos do triângulo aritmético original e, em seguida, veremos as novas configurações deste triângulo, ao aplicarmos diferentes módulos. Verificaremos se nestes novos triângulos as propriedades aqui analisadas continuam válidas. Vejamos agora o que acontece com o triângulo aritmético módulo m .

Inicialmente, verificaremos a validade módulo m das cinco propriedades anteriormente estudadas.

1ª Propriedade: $(\text{mod } m). a_{n0} \equiv a_{nn} \equiv 1 \pmod{m}$ para qualquer inteiro $m > 1$.

Demonstração:

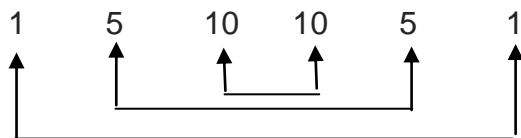
É imediata, pois pela primeira propriedade sabemos que $A_{n0} = A_{nn} = 1$, logo tomando congruência módulo m obtemos o resultado.

2ª Propriedade: $(\text{mod } m). a_{nk} \equiv a_{n(n-k)} \pmod{m}$ para qualquer inteiro $m > 1$.

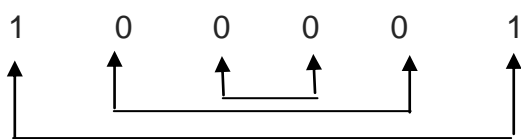
Demonstração:

É imediata da segunda propriedade, pois $A_{nk} = A_{n(n-k)}$, tomando congruência módulo m segue o resultado.

Exemplo:



Linha 5



Linha 5 (mod 5)

3ª Propriedade: $(\text{mod } m). a_{nk} + a_{n(k+1)} \equiv a_{(n+1)(k+1)} \pmod{m}$

Demonstração: É imediata, pois pela terceira propriedade sabe-se que $A_{nk} + A_{n(k+1)} = A_{(n+1)(k+1)}$. Logo, tomando congruência módulo m em ambos os lados, segue o resultado.

Exemplo:

$$\begin{array}{cccccc}
 & & & & & & 1 \\
 & & & & & & 1 & 1 \\
 & & & & & & 1 & 2 & 1 \\
 & & & & & & 1 & \underline{3} & \underline{3} & 1 \\
 & & & & & & 1 & 4 & \underline{6} & 4 & 1 \\
 & & & & & & 1 & 5 & 10 & 10 & 5 & 1
 \end{array}$$

Triângulo isóscele original

$$\begin{array}{cccccc}
 & & & & & & 1 \\
 & & & & & & 1 & 1 \\
 & & & & & & 1 & 2 & 1 \\
 & & & & & & 1 & \underline{3} & \underline{3} & 1 \\
 & & & & & & 1 & 0 & \underline{2} & 0 & 1 \\
 & & & & & & 1 & 1 & 2 & 2 & 1 & 1
 \end{array}$$

Triângulo isóscele (mod 4)

4ª Propriedade: (mod m). Para qualquer inteiro $m > 1$ tem-se que $a_{n0} + a_{n1} + \dots + a_{nn} \equiv 2^n \pmod{m}$.

Demonstração:

Pela quarta propriedade temos que $A_{n0} + A_{n1} + \dots + A_{nn} = 2^n$ e, pela definição do triângulo aritmético módulo m temos que $A_{ni} \equiv a_{ni} \pmod{m}$ para cada $i = 0, 1, 2, \dots, n$. Logo $2^n = A_{n0} + A_{n1} + \dots + A_{nn} \equiv a_{n0} + a_{n1} + \dots + a_{nn} \pmod{m}$ e temos provada a propriedade.

Exemplo:

Linha 0	1					$\rightarrow 2^0$	
Linha 1	1	1				$\rightarrow 2^1$	
Linha 2	1	2	1			$\rightarrow 2^2$	
Linha 3	1	3	3	1		$\rightarrow 2^3$	
Linha 4	1	4	6	4	1	$\rightarrow 2^4$	
Linha 5	1	5	10	10	5	1	$\rightarrow 2^5$

Triângulo isóscele original

Linha 0		1				$\rightarrow 2^0$		
Linha 1		1	1			$\rightarrow 2^1$		
Linha 2		1	2	1		$\rightarrow 2^2$		
Linha 3		1	3	3	1	$\rightarrow 2^1$		
Linha 4		1	4	0	4	1	$\rightarrow 2^2$	
Linha 5		1	5	4	4	5	1	$\rightarrow 2^1$

Triângulo isóscele (mod 6)

5ª Propriedade: (mod m). Se n e k são inteiros tais que $n \geq k \geq 0$, então $a_{kk} + a_{(k+1)k} + a_{(k+2)k} + \dots + a_{(k+n)k} \equiv a_{(k+n+1)(k+1)} \pmod{m}$.

Demonstração:

Pela quinta propriedade sabemos que se n e k são inteiros tais que $n \geq k \geq 0$, então $A_{kk} + A_{(k+1)k} + A_{(k+2)k} + \dots + A_{(k+n)k} = A_{(k+n+1)(k+1)}$. Como $A_{(k+i)k} \equiv a_{(k+i)k} \pmod{m}$ para cada $i \in \{0, 1, 2, \dots, n\}$ e, $A_{(k+n+1)(k+1)} \equiv a_{(k+n+1)(k+1)} \pmod{m}$, então $a_{kk} + a_{(k+1)k} + a_{(k+2)k} + \dots + a_{(k+n)k} \equiv A_{kk} + A_{(k+1)k} + A_{(k+2)k} + \dots + A_{(k+n)k} = A_{(k+n+1)(k+1)} \equiv a_{(k+n+1)(k+1)} \pmod{m}$. Isto prova a propriedade.

Exemplo:

			1				
			1	1			
		1	2	1	/		
	1	3	3	/	1		
	1	4	6	/	4	1	
	1	5	10	↘	10	5	1

Triângulo isóscele original

			1				
			1	1			
		1	2	1	/		
	1	3	3	/	1		
	1	4	6	/	4	1	
	1	5	2	↘	2	5	1

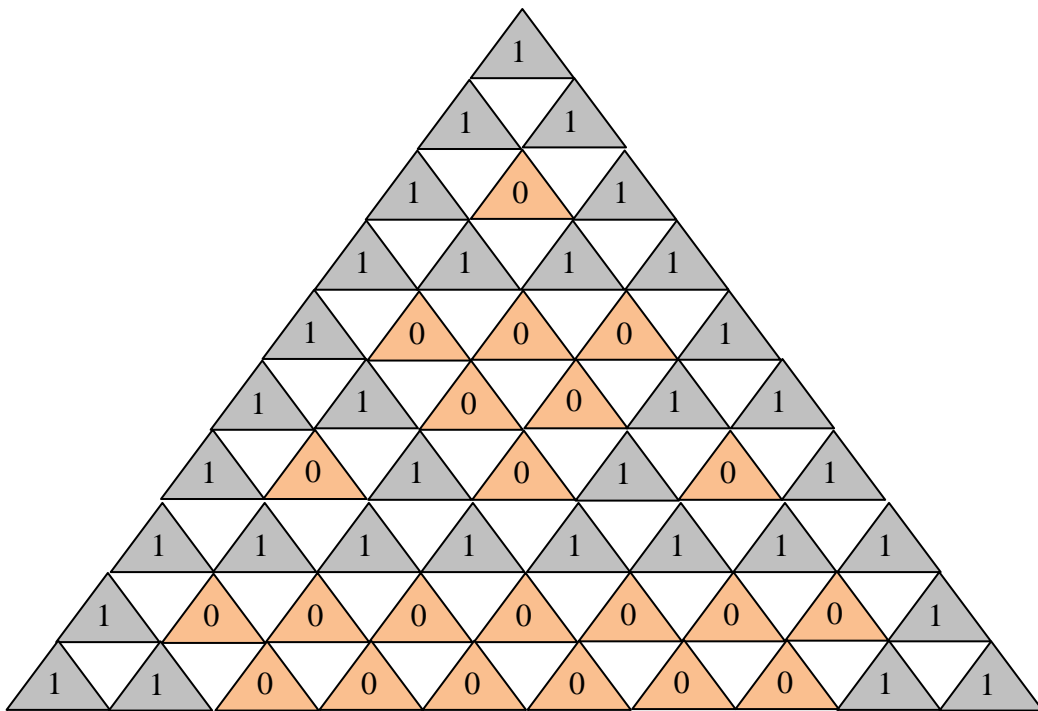
Triângulo isóscele (mod 8)

3.7 Outras propriedades do triângulo aritmético

Além das propriedades mostradas na seção 3.6 foram observadas outras propriedades nas linhas desses triângulos no caso em que $m = p$ é um número primo. Para evidenciar essas relações veremos agora a configuração de alguns triângulos aritméticos aplicando um código de cores nos restos.

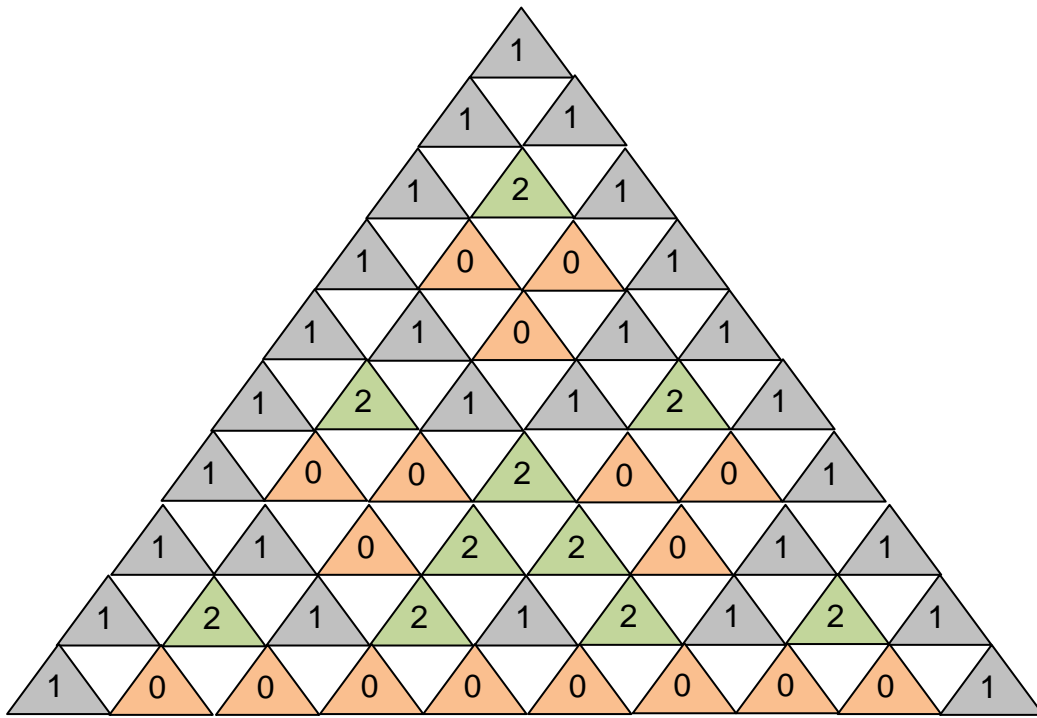
Triângulos aritméticos coloridos para $p = 2, 3$ e 5 .

Figura 9 – Triângulo aritmético (mod 2) com código de cores



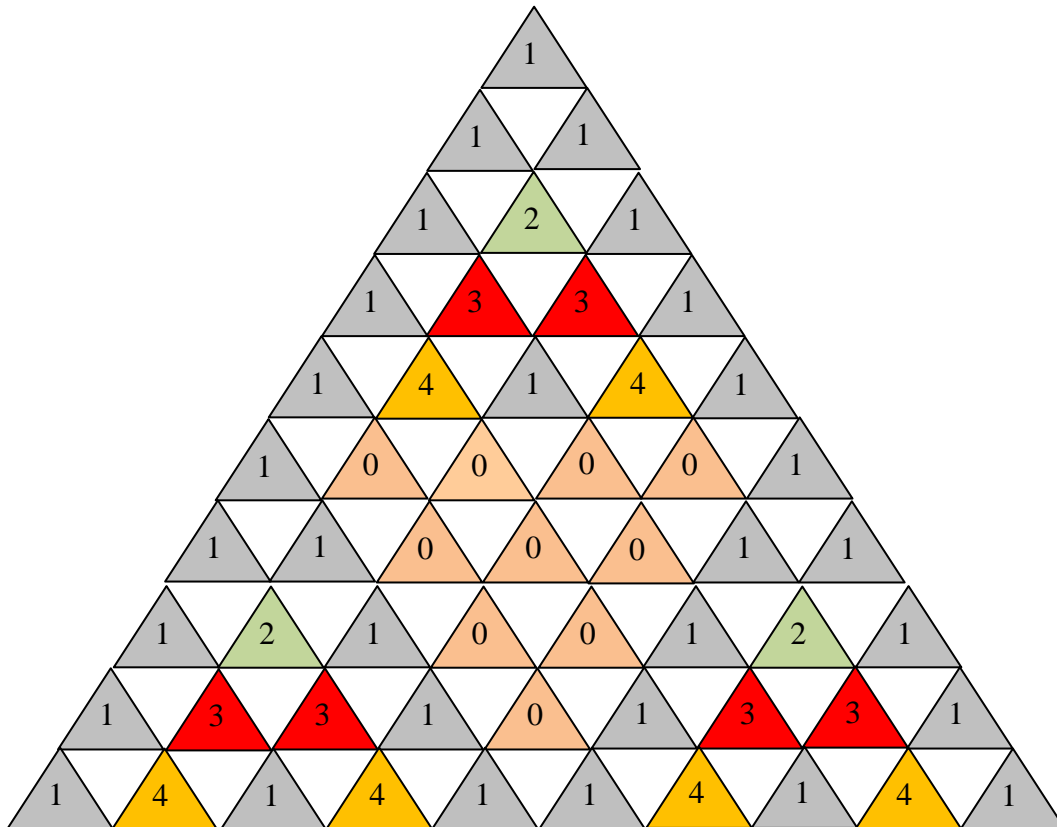
Fonte: O autor, 2016

Figura 10 – Triângulo aritmético (mod 3) com código de cores



Fonte: O Autor, 2016

Figura 11 – Triângulo aritmético (mod 5) com código de cores



Fonte: O Autor, 2016

No triângulo módulo 2, olhando as linhas 2, 2^2 e 2^3 pode-se observar que todos os elementos são zero exceto o primeiro e último. No triângulo módulo 3, olhando as linhas 3 e 3^2 pode-se observar que todos os elementos são zero exceto o primeiro e último. Analogamente no triângulo módulo 5, também se verifica que na linha 5 todos os elementos são zero com exceção do primeiro e último termo. Isso irá conjecturar a seguinte propriedade: $A_{p^i k} \equiv 0 \pmod{p}$, para cada $k \in \{1, 2, \dots, p^i - 1\}$. Iremos provar que isto de fato é verdadeiro para qualquer primo p .

Proposição 3.7.1 se p é um número primo e k é um inteiro tal que $0 < k < p^i$, então $A_{p^i k} \equiv 0 \pmod{p}$.

Demonstração:

Basta demonstrar que $p | A_{p^i k}$ ou equivalentemente que $p | \binom{p^i}{k}$. Primeiramente vamos provar que $p | \binom{p}{k}$. De fato,

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)(p-2)\dots(p-k+1)(p-k)!}{k!(p-k)!},$$
 daí temos que $k! \binom{p}{k} = p(p-1)\dots(p-k+1)$, note que $p | p(p-1)\dots(p-k+1)$, pois é múltiplo de p . Como $p \nmid k!$ e $\text{mdc}(p, k!) = 1$, logo pela Proposição 1.4.2 segue que $p | \binom{p}{k}$.

Considere agora os elementos $A_{p^i k}$, $0 < k < p^i$, da linha p^i , com $i > 1$. Neste caso tem-se que
$$\binom{p^i}{k} = \frac{p^i!}{k!(p^i-k)!} = \frac{p^i(p^i-1)(p^i-2)\dots(p^i-k+1)(p^i-k)!}{k!(p^i-k)!} = \frac{p^i(p^i-1)\dots[p^i-(k-1)]}{k!}.$$
 Observe que, como $i > 1$ e $0 < k < p^i$, k pode ser maior que p e nesse caso $p | k!$ e $\text{mdc}(p, k!) \geq p$.

Afirmção: se o expoente da maior potência de p que divide k é r , $r \geq 0$, então $\binom{p^i}{k}$ é divisível por p^{i-r} .

Demonstração da afirmação:

Seja sp^j um múltiplo de p tal que $0 < sp^j < k$ com $\text{mdc}(s, p) = 1$. Logo $k! = k(k-1)\dots sp^j \dots 2.1$ e portanto temos uma potência de p , independente da potência p^r de k . Mas, no numerador de $\frac{p^i(p^i-1)\dots[p^i-(k-1)]}{k!}$ temos o fator $p^i - sp^j = p^j(p^{i-j} - s)$ onde também aparece a mesma potência p^j . Simplificando, do numerador e denominador o termo p^j eliminamos esse fator. Repetindo esse

processo para Cada potência de p que aparece em $(k-1)!$ tem-se que $\binom{p^i}{k} = \frac{p^i}{p^r} \cdot t$ com $\text{mdc}(t, p) = 1$. Logo $p^{i-r} | \binom{p^i}{k}$. Desta afirmação segue a proposição 3.7.1.

Note que na demonstração acima foi provado um resultado mais forte do que o enunciado da proposição 3.7.1. Na verdade provamos que: Se i e k são inteiros positivos tais que $0 < k < p^i$ e $k! = p^r t$, com $\text{mdc}(t, p) = 1$, então $A_{p^i, k} \equiv 0 \pmod{p^{i-r}}$.

Outros resultados podem ser obtidos a partir dos triângulos aritméticos quando m for um número primo p . Por exemplo, olhando os triângulos aritméticos coloridos acima observa-se o seguinte:

Proposição 3.7.2 se a e b são números inteiros e p é um número primo, então $(a+b)^p \equiv a^p + b^p \pmod{p}$.

Demonstração:

pela proposição 3.7.1 sabe-se que $\binom{p}{i} \equiv 0 \pmod{p}$, para cada $i \in \{1, 2, \dots, p-1\}$, e pela proposição 3.4.1 (Teorema binomial) tem-se que $(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \dots + \binom{p}{p-1}ab^{p-1} + b^p$. Tomando congruência módulo p , segue $(a+b)^p \equiv a^p + 0a^{p-1}b + \dots + 0ab^{p-1} + b^p \equiv a^p + b^p \pmod{p}$.

O pequeno Teorema de Fermat afirma o seguinte: $c^p \equiv c \pmod{p}$ para qualquer inteiro c e primo p .

Exercício: Use o pequeno Teorema de Fermat para demonstrar a proposição 3.7.2.

Solução: Pelo Pequeno Teorema de Fermat, temos que $a^p \equiv a \pmod{p}$ e $b^p \equiv b \pmod{p}$. Pela propriedade (iv) da proposição 1.6.2, segue que $a^p + b^p \equiv a + b \pmod{p}$. Como $a + b \equiv (a+b)^p \pmod{p}$, segue pela propriedade (iii) da proposição 1.6.2 que $a^p + b^p \equiv (a+b)^p \pmod{p}$ e pela propriedade (ii) da proposição 1.6.2 concluímos que $(a+b)^p \equiv a^p + b^p \pmod{p}$.

Para maiores esclarecimentos, os assuntos deste capítulo podem ser encontrados em Caminha (2012), Caminha (2013), Hefez (2013), Silva (2015). Com exceção dos itens 3.6 A congruência módulo m no triângulo aritmético e 3.7 Outras propriedades do triângulo aritmético, pois o mesmo foram produzidos pelo autor e seu orientador.

4 PROPOSTA PEDAGÓGICA

Os parâmetros curriculares nacionais (PCN's) elaborados pelo Ministério da Educação e do Desporto nos comunicam uma referência para o trabalho dos professores do Ensino Fundamental e Médio. Eles têm por objetivo garantir às crianças e jovens brasileiros os conhecimentos necessários para o exercício da cidadania. Embora não seja uma diretriz obrigatória, orientam as reflexões dos envolvidos no processo educativo, em especial no professor norteando as ações do cotidiano escolar. Tendo-os por base e destacando alguns dos objetivos neles propostos, elaboramos uma sequência de ações pedagógicas buscando levar o tema “dígitos verificadores” da Carteira de identidade e do CPF” para ser aplicado em turmas do sexto ano do Ensino Fundamental.

Essa proposta pedagógica tem como público alvo os estudantes do sexto ano do Ensino Fundamental, levando a esses alunos a oportunidade de aplicar conhecimentos matemáticos adquiridos em sala de aula em situações do cotidiano.

A maioria dos alunos do sexto ano já possui os documentos de identidade e CPF, mas não sabe qual é a verdadeira finalidade e importância deles. Nessa proposta, além de mostrar a importância e finalidade desses documentos, queremos também apresentar aos nossos alunos toda a matemática envolvida na determinação de alguns dígitos desses documentos (dígitos verificadores), fazendo um paralelo com as operações estudadas nessa fase e tornando as aulas mais atrativas.

Através das aplicações que mostraremos aqui, pretendemos fazer com que os alunos tenham mais interesse e curiosidade sobre o assunto e que percebam a presença da matemática em seu cotidiano, às vezes de maneira bem sutil e de fácil entendimento. Neste sentido, vamos detalhar a sequência de ações que compõem nossa proposta pedagógica.

4.1 Descrição geral

Pretende-se desenvolver esse trabalho em turmas do sexto ano do Ensino Fundamental, que será dividido em 5 etapas com duração aproximada de 90 minutos cada.

Primeira etapa: Aula Dialogada.

Inicia-se a aula com uma conversa informal, abordando o assunto “documentos utilizados pelos brasileiros no cotidiano” e instigando a participação dos estudantes.

Queremos detectar se os alunos conhecem os documentos que são utilizados por seus pais, destacando aqueles que julguem mais importantes e acrescentando alguns, caso não sejam citados, através desse dialogo perguntar sobre a importância desses documentos e sua finalidade. Após esse debate, indagar se eles possuem esses documentos e se em algum momento já o utilizaram e, caso afirmativo, deixar que expliquem em que momento isso aconteceu.

Orientá-los para que façam uma pesquisa sobre os algoritmos que aparecem nesses documentos, como eles são determinados e quando são exigidos, dividindo a turma em grupos de forma que apresentem os resultados de sua pesquisa.

Segunda etapa: Apresentação da Pesquisa.

Inicialmente, cada grupo fará sua apresentação no tempo de 5 a 8 minutos. Após as apresentações, mediar um debate sobre o assunto, onde o professor possa explicar toda a importância desses documentos na vida dos alunos, para que servem e em que momentos eles serão exigidos, levando-os a entender que aqueles que ainda não possuem devem providenciar o mais breve possível.

Levantar a questão dos dígitos verificadores através de uma explicação por parte do professor, mostrando qual sua relevância e dando alguns exemplos de sua utilização, inclusive exemplos que não se relacione apenas aos documentos, como no caso dos códigos de barras dos produtos. Finalmente, abrir uma discussão sobre o processo de determinação desses dígitos, explicando aos alunos a determinação dos dígitos verificadores do RG e do CPF, utilizando um RG e um CPF como exemplos. Perguntar quais operações matemáticas estudadas em sala de aula estão envolvidas nesse processo, abordando a importância da matemática no cotidiano.

Pedir para que tragam na próxima aula seus RGs e CPFs e, aqueles que não possuem esses documentos, deverão anotar e trazer o número dos mesmos de um de seus respectivos responsáveis.

Terceira etapa: Aplicação de algoritmos para cálculos dos dígitos verificadores.

Os alunos de porte de seus documentos, e utilizando os conhecimentos adquiridos na última aula, farão uma verificação se os dígitos verificadores dos mesmos foram determinados de forma correta. Em um segundo momento, os alunos

serão divididos em grupo e será lançado um desafio no qual cada grupo irá separar um RG e um CPF com apenas os dígitos identificadores que serão entregues para outro grupo e aquele que descobrir primeiro os dígitos verificadores desses documentos, de forma correta, será o vencedor do desafio.

Propor a resolução de exercícios do ENEM e de concursos públicos que abordem o assunto. (sugestão no plano de aula em anexo)

Quarta etapa: Sensibilização dos alunos da Escola

Os alunos do sexto ano do Ensino Fundamental farão uma pesquisa na escola realizando um levantamento da quantidade de alunos que não possuem esses documentos e posteriormente, serão os protagonistas explicando a importância dos mesmos em suas vidas, motivando assim, o corpo discente a providenciar tais documentos, pois os mesmos são obrigatórios em diversas situações para o exercício de cidadania. Além disso, farão também uma apresentação abordando o tema dígitos verificadores do RG e do CPF, onde explicarão resumidamente a importância desses dígitos para evitar fraudes e detectar possíveis erros de digitação e como os mesmos são determinados, justificando o motivo pelo qual o assunto foi abordado pelo professor de matemática da turma.

Quinta etapa: avaliação das atividades desenvolvidas

A proposta de trabalhar a determinação dos dígitos verificadores do CPF e do RG na turma 601 da Escola Municipal de Formação Profissional Governador Portela localizada no município de Miguel Pereira – RJ, foi analisada como positiva, pois os alunos tiveram a oportunidade de aprender a importância desses documentos na vida do cidadão. O tema dígitos verificadores foi apresentado de forma clara e objetiva, mostrando sua relevância no universo tecnológico, levando o aluno a refletir que sem esses dígitos, as informações sobre os documentos do cidadão ficariam mais vulneráveis.

Os discentes levaram alguns números de RG e de CPF para sala de aula e após serem divididos, em grupos, aprenderam toda a matemática envolvida na determinação desses dígitos. Posteriormente, cada grupo anotou um número de RG e um de CPF sem os dígitos verificadores e foi lançado um desafio entre eles, de modo que cada grupo deveria descobrir os dígitos verificadores dos documentos que foram passados por outro grupo. Aquele que encontrasse primeiro, corretamente, era considerado vencedor do desafio.

Após os conhecimentos adquiridos sobre o tema e com os grupos já formados, cada qual ficou responsável por duas turmas da escola, sendo uma no turno da manhã e outra no turno da tarde. A primeira etapa realizada foi uma pesquisa que consistia de quatro perguntas, as quais seriam feitas nas outras turmas: 1 – Você possui CPF? 2 – Você possui RG? 3 – Sabe qual a finalidade desses documentos? 4 – Sabe o que são dígitos verificadores? Na pesquisa realizada nas oito turmas da escola, totalizando 100 alunos, verificou-se que 68% deles possuem CPF, 70% possuem RG, 67% sabiam a importância desses documentos e 10% alegaram ter conhecimento sobre o que são dígitos verificadores.

Com as pesquisas realizadas cada grupo confeccionou cartazes informativos sobre a importância desses documentos, o que eram dígitos verificadores, sua finalidade e de que forma esses dígitos verificadores são determinados.

A culminância dessa proposta pedagógica foi elaborada de forma que cada equipe deveria apresentar cartazes para as suas respectivas turmas, expondo a importância da obtenção desses documentos que estão diretamente relacionados à cidadania de cada indivíduo na sociedade, uma vez que eles são exigidos em diversas situações do dia a dia. A abordagem dos dígitos verificadores mostrou como a matemática está presente no cotidiano, ratificando que essas operações matemáticas dão maior segurança a esses códigos, na intenção de evitar fraudes, erros de digitação etc.

O trabalho proporcionou interatividade entre as turmas da escola, levando os alunos à reflexão sobre o tema da cidadania que está diretamente relacionado à obtenção desses documentos. Tornando-os conhecedores de seus direitos e deveres.

Figura 12 – Foto grupo 1 apresentando trabalho



Fonte: O autor, 2016

Figura 13 – Foto grupo 2 apresentando trabalho



Fonte: O autor, 2016

Figura 14 – Foto grupo 3 apresentando trabalho



Fonte: O autor, 2016

Figura 15 – Foto grupo 4 apresentando trabalho



Fonte: O autor, 2016

CONCLUSÃO

Vimos que a aritmética modular é uma ferramenta de extrema relevância na determinação do resto da divisão. De fato, nesse trabalho, a utilizamos para apresentar algumas aplicações das congruências, com foco na determinação dos dígitos verificadores e para uma abordagem diferenciada aplicada ao triângulo aritmético.

A nossa proposta de trabalhar os dígitos verificadores mostra como a matemática está presente em situações do cotidiano. Assim, aplicamos o tema em sala de aula, desenvolvendo uma atividade para os alunos do sexto ano do Ensino Fundamental com enfoque para o RG e o CPF. O resultado nos levou a concluir que houve um aumento acentuado no interesse do educando, potencializando um aprendizado individual e coletivo, pois os alunos foram atores na construção do conhecimento divulgando o estudo realizado nas outras turmas da escola. Notamos uma interatividade que proporcionou aprimoramentos na área da matemática e na questão relativa à cidadania diretamente relacionada à obtenção desses documentos.

O triângulo aritmético tem aplicação em diversos ramos da matemática, entre eles, destacamos o binômio de Newton e o estudo das probabilidades. O nosso trabalho apresenta uma abordagem intrigante, onde produzimos o triângulo aritmético módulo m , mostrando que suas principais propriedades continuam preservadas e, desta forma, concluímos que esse estudo pode ainda ser aprofundado em outro momento, visando aplicações relevantes em nossa área de ensino, através de padrões que podem ser observados e até uma aplicação no Teorema de Fermat.

Esperamos que esse trabalho contribua de forma significativa como instrumento facilitador na busca de inovações no estudo da matemática, proporcionando maior interesse por parte dos discentes. Ressaltamos que o tema, dígitos verificadores, pode ser inserido no Ensino Fundamental na disciplina em questão, podendo ser trabalhado de forma interdisciplinar principalmente nos assuntos relacionadas à cidadania do indivíduo.

REFERÊNCIAS

BIGODE, Antônio José Lopes; GIMENEZ, Joaquim. Metodologia para o ensino da aritmética: Competência numérica no cotidiano. São Paulo: FTD, 2009.

CAMINHA, A. Tópicos de Matemática Elementar, Volume 4: Combinatória. Sociedade Brasileira de Matemática, 2012.

CAMINHA, A. Tópicos de matemática Elementar, Volume 5: Teoria dos Números. Sociedade Brasileira de Matemática, 2013.

DOMINGUES, Hygino H. Fundamentos de Aritmética. São Paulo: Atual, 1991.

HEFEZ, A. Aritmética – Rio de Janeiro: SBM, 2013. (coleção profmat)

HEFEZ, A. Curso de Álgebra. Volume 1. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, CNPQ 1993.

HEFEZ, A. Elementos da Aritmética. (Série textos universitários, Sociedade Brasileira de Matemática) ISBN. 978-85-85818-25-8

HEFEZ, A. Iniciação a Aritmética. (programa de Iniciação Científica OBMEP, Sociedade Brasileira de Matemática)

IEZZI, G. ET al. Matemática. Volume único. São Paulo: Atual 2011.

<http://www.cin.ufpe.br/~gdcc/matdis/aulas/binomial>, acessado em 21 de março de 2016

<http://www.dicasdeprogramacao.com.br/algorithmo-para-validar-CPF/>, acessado em 03 de maio de 2016

<http://www.qualityrioplanosdesaude.com.br/documentos-necessarios-para-contratar-plano-de-saude/>, acessado em 14 de março de 2016.

MAIER, Rudol R. Teoria dos Números, Disponível em <http://www.mat.unb.br/~maierr/tnotas.pdf>

MEC, Parâmetros curriculares nacionais – terceiro e quarto ciclos, 1998.

MOURA, Rafael Nogueira de. Congruências modulares e algumas aplicações para educação básica. 2015. Dissertação (Mestrado Profissional em Matemática em rede Nacional – PROFMAT) – Universidade Federal do Ceará, Fortaleza. 2015.

SOUZA, Natália Pedrosa de. Uma Análise dos Esquemas de Dígitos Verificadores Usados no Brasil/Natália Pedrosa de Souza Universidade do Rio de Janeiro.2013.

SILVA, Márcio Rebouças da. Números Binomiais: Uma Abordagem Combinatória para o Ensino Médio. 2015. Dissertação (Mestrado profissional em Matemática em rede Nacional – PROFMAT) – Universidade Federal do Ceará, Fortaleza. 2015.

APÊNDICE

Planejamento de aula

Escola: Escola Municipal de Formação Profissional Governador Portela. **Turno:**

Tarde

Professor: Tancredo Ramos Duarte

Data:

Turma: 601

Série: 6º ano

Horário: 12: 30 – 14:00

Data: 05/07; 06/07; e 07/07 de 2016

TEMA:

- Dígitos verificadores do RG e do CPF

Objetivos:

- Despertar a autonomia e incentivar o interesse no processo de construção do conhecimento;
- Saber informa-se, comunicar-se, argumentar, compreender informações, aguçar sua criatividade e seu espírito investigativo;
- Verificar quais as utilidades dos documentos utilizados pelos brasileiros no cotidiano;
- Utilizar os recursos disponíveis para pesquisa;
- Participar, socialmente, de forma prática e solidária;
- Utilizar algoritmos para determinar dígitos verificadores;
- Perceber a matemática como ciência voltada à solução de problemas da atualidade.

Conteúdos:

- Adição de números naturais;
- Multiplicação de números naturais;
- Divisão de números naturais;
- Aritmética dos restos;
- Dígitos verificadores.

Recursos:

- Giz e apagador;
- Quadro negro;
- Data show;
- Exercícios para discussão.

Introdução:

Os parâmetros curriculares nacionais (PCN's), elaborados pelo Ministério da Educação e do Desporto, nos comunicam uma referência para o trabalho dos professores do Ensino Fundamental e Médio. Eles têm por objetivo garantir às crianças e jovens brasileiros os conhecimentos necessários para o exercício da cidadania. Embora não seja uma diretriz obrigatória, orientam as reflexões dos envolvidos no processo educativo, em especial no professor, norteando as ações do cotidiano escolar. Tendo-os por base e destacando alguns dos objetivos neles propostos, elaboramos uma sequência de ações pedagógicas buscando levar o tema “dígitos verificadores” do RG e do CPF para serem aplicados em turmas do sexto ano do Ensino Fundamental.

Essa proposta pedagógica tem como público alvo os estudantes do sexto ano do Ensino Fundamental, levando a esses alunos a oportunidade de aplicarem conhecimentos matemáticos adquiridos em sala de aula e nas situações do cotidiano.

A maioria dos alunos do sexto ano já possui os documentos de RG e CPF, mas não sabe qual é a verdadeira finalidade e importância dos mesmos. Nessa proposta, além de mostrar a importância e finalidade desses documentos, queremos também apresentar aos nossos alunos toda a matemática envolvida na determinação dos dígitos verificadores, fazendo um paralelo com as operações matemáticas estudadas nessa fase e tornando as aulas mais atrativas.

O intuito é, através das aplicações que mostraremos aqui, fazer com que os alunos tenham mais interesse e curiosidade sobre o assunto em questão e percebam que a matemática está presente no seu cotidiano, às vezes de maneira bem sutil e de fácil entendimento. Neste sentido, vamos detalhar a sequência de ações que compõem nossa proposta pedagógica.

Desenvolvimento:

- Iniciar a aula com uma conversa informal, abordando o assunto “documentos utilizados pelos brasileiros no cotidiano”, instigando a participação dos estudantes.
- Queremos detectar se os alunos conhecem os documentos que são utilizados por seus pais, destacando aqueles que julguem mais importantes e acrescentando alguns, caso não sejam citados. Através desse diálogo, perguntar sobre a importância dos mesmos e sua finalidade. Após esse

debate, indagar se eles possuem esses documentos e se em algum momento já o utilizaram, caso afirmativo, deixar que expliquem em que momento isso aconteceu. Orientar para que façam uma pesquisa sobre os algarismos que aparecem nesses documentos e como eles são determinados, dividindo a turma em grupos de forma que terão que apresentar os resultados de sua pesquisa.

- Inicialmente, cada grupo fará sua apresentação no tempo de 5 a 8 minutos. Após as apresentações, mediar um debate sobre o assunto, onde o professor possa mostrar toda a importância desses documentos na vida do aluno, para que servem e em que momentos eles serão exigidos, levando-os a entender que aqueles que ainda não possuem devem providenciar o mais breve possível. Levantar a questão dos dígitos verificadores através de uma explicação por parte do professor explicando o que são e qual sua relevância, dando alguns exemplos de sua utilização, inclusive exemplos que não se prendam apenas aos documentos. Finalmente, promover uma discussão sobre o processo de determinação desses dígitos, explicando para os alunos a determinação dos mesmos no RG e CPF, através de alguns exemplos de documentos, indagar quais operações matemáticas aprendidas em sala de aula estão envolvidas nesse processo, abordando a importância da matemática no cotidiano.
- Pedir aos alunos que tragam para próxima aula seus RGs e CPFs e aqueles, que não possuírem esses documentos, deverão anotar o número dos mesmos de um de seus respectivos responsáveis.
- Os alunos de porte de seus documentos, e juntamente com os conhecimentos adquiridos na última aula, farão uma análise se os dígitos verificadores foram determinados de forma correta. Em um segundo momento, os alunos serão divididos em grupo onde cada qual, irá separar dois CPFs com apenas os nove primeiros dígitos que serão entregues para outro grupo e, aquele que determinar primeiro os dígitos verificadores desses documentos de forma correta, será o vencedor do desafio.
- Propor a resolução de exercícios do ENEM e de concursos públicos que abordem o assunto

- Os alunos do sexto ano do Ensino Fundamental farão uma pesquisa na escola realizando um levantamento da quantidade de alunos que não possuem esses documentos e, posteriormente, serão os protagonistas explicando a importância dos mesmos. Assim, estaremos motivando que providenciem seus próprios documentos, pois os mesmos, são obrigatórios em diversas situações para o exercício de cidadania. Farão também uma apresentação abordando o tema dígitos verificadores do RG e do CPF, onde explicarão, resumidamente, a importância desses dígitos para evitar as fraudes, detectar possíveis erros de digitação e como os mesmos são determinados, justificando o motivo pelo qual o assunto foi abordado pelo professor de matemática da turma.
- Realizar um processo de investigação para saber qual foi a receptividade por parte dos alunos e, após as etapas realizadas, incentivar a divulgação em outras escolas como uma proposta de ampliação para outras turmas do sexto ano do Ensino Fundamental.

Sugestão de exercícios:

1) ENEM (2005) Os números de identificação utilizados no cotidiano (de contas bancárias, de CPF, de carteira de identidade, etc) usualmente possuem um dígito de verificação, normalmente representado após o hífen, como em 17326 – 9. Esse dígito adicional tem a finalidade de evitar erros no preenchimento ou digitação de documentos. Um dos métodos utilizados para gerar esse dígito utiliza os seguintes passos:

- Multiplicar o último algarismo por 1, o penúltimo por 2, o antepenúltimo por 1 e assim por diante, sempre alternando multiplicações por 1 e 2;
- Soma-se 1 a cada um dos resultados dessas multiplicações que forem maior do que ou igual 10;
- Somam-se os resultados obtidos;
- Calcula-se o resto da divisão dessa soma por 10, obtendo-se assim o dígito verificador.

O dígito de verificação fornecido pelo processo acima para o número 24685 é:

- a) 1 b) 2 c) 4 d) 6 e) 8

Gabarito: e

2) ENEM (2009) Para cada indivíduo, a sua inscrição no cadastro de pessoa física (CPF) é composto por um número de 9 algarismos e outro número de dois algarismos, na forma d_1 e d_2 , em que os dígitos d_1 e d_2 são denominados dígitos verificadores. Os dígitos verificadores são calculados, a partir da esquerda, da seguinte maneira. Os 9 primeiros algarismos são multiplicados pela sequência 10, 9, 8, 7, 6, 5, 4, 3, 2 (o primeiro por 10, o segundo por 9, e assim sucessivamente) em seguida, calcula-se o resto r da divisão da soma dos resultados por 11, e se esse resto for 0, ou 1 d_1 é zero, caso contrário $d_1 = (11 - r)$. o dígito d_2 é calculado pela mesma regra, na qual os números a serem multiplicados pela sequência dada são contados a partir do segundo algarismo, sendo d_1 o último algarismo, isto é, d_2 é zero se o resto s da divisão por 11 das somas das multiplicações for 0 ou 1, caso contrário, $d_2 = (11 - s)$.

Suponha que João tenha perdido seus documentos, inclusive o cartão do CPF e, ao dar queixa da perda na delegacia, não conseguisse lembrar quais eram os dígitos verificadores, recordando-se apenas que os 9 primeiros algarismos eram 123.456.789. Neste caso, os dígitos verificadores d_1 e d_2 esquecidos são respectivamente:

- a) 0 e 9 b) 1 e 4 c) 1 e 7 d) 9 e 1 e) 0 e 1

Gabarito: a

Conclusão:

Os trabalhos construídos pelos alunos foram apresentados no mês de setembro de 2016 para as respectivas turmas de acordo com a separação dos grupos. Os resultados encontram-se no corpo do trabalho.