REVISTA FACISA ON-LINE (ISSN 2238-8524) | vol. 10 | n. 1 | p. 187-198
jan. – jul. de 2021 | BARRA DO GARÇAS - MT

CALCULANDO DÍGITOS VERIFICADORES UTILIZANDO O RESTO DA DIVISÃO EUCLIDIANA

Adilson Antônio Berlatto[1]
Jhonattan Pinto Barbosa[2]
Valdiego Siqueira Melo[3]

RESUMO: Este trabalho aborda o conceito de congruências modulares e tem o propósito de utilizar operações aritméticas básicas - adição, multiplicação e divisão com resto - para aplicar tal conceito ao cálculo de dígitos verificadores em documentos como CPF e CNH. Para isso, foi desenvolvida uma pesquisa exploratória e aplicada, com levantamentos bibliográficos envolvendo tópicos como aritmética modular, produto interno e sistemas de identificação modulares, baseando-se em Coutinho (2003) e Hefez (2013), além de Barbosa (2015). Foram utilizados exemplos visando uma melhor compreensão dos conceitos apresentados. Identificou-se que é possível aplicar o conceito de congruências modulares em sistemas de identificação para determinar dígitos verificadores em documentos como CPF e CNH utilizando-se apenas conceitos amplamente conhecidos da Matemática, como adição, multiplicação e divisão com resto.

Palavras-chave: Divisão Euclidiana. Congruências Modulares. Profmat.

COMPUTING CHECK DIGITS USING THE REMAINDER OF THE EUCLIDEAN DIVISION

ABSTRACT: This paper addresses the concept of modular congruences and the use of basic arithmetic operations - addition, multiplication and division with remainder - to apply this concept to calculating check digits in documents such as CPF and CNH. For this, an exploratory and applied research was developed, with bibliographic surveys involving topics such as modular, internal product and modular identification systems, based on Coutinho (2003) and Hefez (2013), besides Barbosa (2015). Examples were used to better understand the concepts presented. It was identified that it is possible to apply the concept of modular congruences in identification systems to determine the verifier codes in documents such as CPF and CNH, using only the automatically known concepts of Mathematics such as addition, multiplication and division with remainder.

Keywords: Euclidean Division. Modular Congruences. Profmat.

[1] Doutor em Matemática pela UnB, docente do Instituto de Ciências Exatas e da Terra no campus da UFMT de Barra do Garças, e-mail: berlatto@ufmt.br;
[2] Mestre em Matemática pela UFMT, docente no curso de Engenharia Civil do Centro Universitário Cathedral - UniCathedral, e-mail: jhonattan.barbosa@hotmail.com;
[3] Mestre em Matemática pela UnB, docente no curso de Engenharia Civil do Centro Universitário Cathedral - UniCathedral e docente dos cursos de Agronomia e Engenharia Civil da UNEMAT, campus de Nova Xavantina, e-mail: prof.valdiego@gmail.com.

INTRODUÇÃO

É evidente que a Matemática possui uma importante participação na criação de novas tecnologias, bem como em aplicações nas mais variadas áreas de conhecimento. Para entender e aplicar conceitos matemáticos que possibilitem resultados importantes é necessário algum tempo de estudo, pois é preciso estudar novas definições e se habituar com diferentes notações do assunto. Normalmente, esse entendimento, ocorre apenas no ensino superior, certas vezes superficialmente, e é comum não ficar evidente que os conceitos utilizados em novas teorias são simples e conhecidos. Um assunto que possui muita aplicabilidade é o de Congruências Modulares. Por exemplo, esse conceito é de fundamental importância em criptografia (algoritmo RSA), dígitos verificadores em documentos e em guias de pagamento, identificação de livros (ISSN), sistemas de identificação e códigos de barras. Com o desenvolvimento de computadores e celulares, tem sido muito utilizado em programação e jogos. Embora as congruências modulares não sejam de conhecimento de grande parte da população, mesmo entre acadêmicos, elas estão fundamentadas em algo bastante conhecido: o resto da divisão de números inteiros.

As aplicações da divisão acima citadas, geralmente, ficam restritas ao conhecimento de nível superior. No entanto, é possível abordá-las na educação básica com o conhecimento de algumas operações. A ideia inicial deste estudo surgiu da tentativa de inserir o trânsito como tema transversal no ensino de Matemática na educação básica, tentando sair do lugar comum dos gráficos ou da estatística. No Brasil, muitos acidentes e mortes ocorrem diariamente no trânsito.

Este trabalho é baseado em Barbosa (2015), dissertação de mestrado apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional – Profmat – em 2015. Ao se abordar este tema na escola, é possível auxiliar na educação para o trânsito, formando pessoas mais comprometidas com a ética e a cidadania, bem como inserir a Matemática como ferramenta no dia a dia do cidadão.

DESENVOLVIMENTO

Aritmética Modular

O conceito de congruência modular foi introduzido em 1801, por Carl Friederich Gauss, em seu livro Disquisitiones Arithmeticae, considerado como o “tratado mais amplo e importante desde Os Elementos de Euclides” (SINGH, 2004). Tal conceito se fundamenta na

aritmética dos números inteiros, mais precisamente, nos restos da divisão euclidiana de dois inteiros não nulos.

Muitas são as aplicações práticas desta teoria. Dentre elas estão: numeração universal de livros (ISBN); códigos de barras; garantia de numeração única de documentos, como CPF, CNPJ e CNH (BARBOSA, 2015); teoria dos códigos e criptografia (COUTINHO, 2003). Convém lembrar que esta última é um capítulo a parte de tudo isso. É graças a ela que transações financeiras podem ser feitas com segurança pela internet, utilizando-se a criptografia RSA (RIVEST; SHAMIR; ADLEMAN, 1978). A evolução dos computadores no século XX foi um dos principais motivadores do desenvolvimento da aritmética modular e da teoria dos números.

Exemplo 1: Em uma segunda-feira, antes de ir para a escola, um aluno assiste a um telejornal, que exibe uma reportagem com imagens de um eclipse ocorrido no dia anterior e dizendo que o próximo eclipse na cidade ocorrerá em 250 dias. Como o estudante só tem folga aos finais de semana, ele fica curioso em saber se poderá ver o eclipse. Sabendo que de 7 em 7 dias é uma segunda-feira, ele obtém que em $245 = 7 \cdot 35$ dias será a segunda-feira mais próxima dos 250 dias. Ainda, como 250 = 245 + 5, o eclipse acontecerá 5 dias após a tal segunda, ou seja, no sábado. O conceito empregado é simples: $250 = 35 \cdot 7 + 5$, isto é, 5 é o resto da divisão de 250 por 7 e fornece a resposta para a questão. Em geral, problemas que envolvem fatores que ocorrem, periodicamente, no tempo (como os meses de um ano ou as horas de um dia) podem ser resolvidos com esse tipo de raciocínio.

Dado um inteiro $m > 1$, dizemos que dois inteiros a e b são congruentes módulo m se os restos de suas divisões por m são iguais. Escreve-se $a \equiv b \pmod{m}$. Algumas operações básicas que se estendem das propriedades da adição e multiplicação de inteiros para essas congruências, como por exemplo: somar, subtrair ou multiplicar em ambos os lados de uma congruência e somar ou multiplicar membro a membro duas congruências, como pode ser visto em Hefez (2013). Ainda, se r é o resto da divisão de a por m, então $a \equiv r \pmod{m}$ e $a \equiv r - m \pmod{m}$. Além disso, assim como a igualdade entre números inteiros, a relação de congruência módulo m é transitiva.

Algumas formas de critérios de divisibilidade são dedutíveis a partir de congruências. O método consiste em escrever um número inteiro na base decimal e encontrar congruências das potências de 10. Seja

$$N = a_n\, 10^{n-1} + a_{n-1}\, 10^{n-2} + \ldots + a_2\, 10 + a_1 \quad (1)$$

a representação do número inteiro N na base decimal, onde $a_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ e $i \in \{1, 2, \ldots, n\}$. Como $10 \equiv 1 \pmod{3}$, segue que $10^k \equiv 1 \pmod{3}$, para todo $k \in \mathbb{N}$. Dessa forma, obtém-se que

$$N \equiv a_n + a_{n-1} + \ldots + a_2 + a_1 \pmod 3;$$

ou seja, o resto das divisões de N por 3 e de $a_n + a_{n-1} + \ldots + a_2 + a_1$ por 3 são iguais. Na divisão por 11 um fato análogo ocorre:

$$N \equiv (-1)^{n+1} a_n + (-1)^n a_{n-1} + \ldots - a_2 + a_1 \pmod{11}.$$

Com isso, o resto da divisão de N por 11 é o mesmo que o resto da divisão da soma dos algarismos de N, alternando-se os sinais, por 11.

Produto Interno

O Produto Interno é um dos objetos de estudo da Álgebra Linear, mas tem utilidade em várias outras áreas da Matemática. Ele permite calcular ângulos, distâncias e projeções, conceitos fundamentais para a Física e engenharias. Suas aplicações vão desde a Estatística até áreas de tecnologia, como por exemplo no estudo de códigos, como pode ser visto em Hefez (2002, p. 88).

Dados dois vetores $u = (a_1, a_2, \ldots, a_n)$ e $v = (b_1, b_2, \ldots, b_n)$ em $\mathbb{R}^n$, o produto interno entre u e v é o número real

$$\langle u, v \rangle = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n.$$

Esta definição pode ser útil para a abordagem geral dos critérios de divisibilidade. Considerando a representação de $N \in \mathbb{Z}$ na base decimal descrita em (1), pode-se escrever

$$\begin{aligned} N &= a_n 10^{n-1} + a_{n-1} 10^{n-2} + \ldots + a_2 10 + a_1 \\ &= \langle (a_n, a_{n-1}, \ldots, a_2, a_1), (10^{n-1}, 10^{n-2}, \ldots, 10, 1) \rangle . \end{aligned}$$

Observamos que, no critério de divisibilidade por 3, foi obtido que

$$N \equiv \langle (a_n, a_{n-1}, \ldots, a_2, a_1), (1, 1, \ldots, 1, 1) \rangle \pmod 3$$

e, no critério de divisibilidade por 11,

$$N \equiv \langle (a_n, a_{n-1}, \ldots, a_2, a_1), ((-1)^{n+1}, (-1)^n, \ldots, -1, 1) \rangle \pmod{11}.$$

De modo geral, tratando-se da divisibilidade de N por um algum número inteiro positivo, mantém-se o vetor $(a_n, a_{n-1}, \ldots, a_2, a_1)$ e encontra-se um vetor específico para se efetuar o produto interno. Tal vetor é encontrado observando-se os restos dos componentes do vetor $(10^{n-1}, 10^{n-2}, \ldots, 10, 1)$ pelo número que se quer dividir. Agora um exemplo.

Exemplo 2**:** Considere o número inteiro $M = 1234567$. Para verificar se M é divisível por 3, são usados os vetores $M = (1, 2, 3, 4, 5, 6, 7)$ e $P = (1, 1, 1, 1, 1, 1, 1)$. Calculando o produto interno, obtemos

$$\langle \overline{M}, P \rangle = 1 \cdot 1 + 2 \cdot 1 + 3 \cdot 1 + 4 \cdot 1 + 5 \cdot 1 + 6 \cdot 1 + 7 \cdot 1 = 28.$$

Como 28 não é divisível por 3, M também não é. Ainda, o resto de 28 por 3 é 1, assim como o resto da divisão de M por 3. Para saber o resto da divisão de M por 11, os vetores utilizados são $\overline{M}$ e $P = (1, -1, 1, -1, 1, -1, 1)$, donde

$$\langle \overline{M}, P \rangle = 1 \cdot 1 + 2 \cdot (-1) + 3 \cdot 1 + 4 \cdot (-1) + 5 \cdot 1 + 6 \cdot (-1) + 7 \cdot 1 = 4.$$

Com isso, o resto obtido é 4.

Como o raciocínio acima pode ser empregado, por exemplo, para se criar um critério de divisibilidade por 7? Para isso, vamos considerar a expansão de N como em (1). Calculando as potências de 10 módulo 7, obtém-se que:

$$10^0 \equiv 1 \pmod 7$$
$$10 \equiv 3 \pmod 7$$
$$10^2 \equiv 2 \pmod 7$$
$$10^3 \equiv -1 \pmod 7$$
$$10^4 \equiv -3 \pmod 7$$
$$10^5 \equiv -2 \pmod 7$$
$$10^6 \equiv 1 \pmod 7$$

Na sexta potência de 10, um padrão é estabelecido, determinando o vetor

$$P = (\ldots, 2, 3, 1, -2, -3, -1, 2, 3, 1),$$

onde P possui n coordenadas. Voltando ao exemplo, temos que

$$\langle \overline{M}, P \rangle = \langle (1, 2, 3, 4, 5, 6, 7), (1, -2, -3, -1, 2, 3, 1) \rangle$$
$$= 1 \cdot 1 + 2 \cdot (-2) + 3 \cdot (-3) + 4 \cdot (-1) + 5 \cdot 2 + 6 \cdot 3 + 7 \cdot 1 = 19$$

e, com isso, M não é divisível por 7. Observe que o número 111.111.222.222.333.333 é divisível por 7.

O caso da divisão por 6 é ainda mais simples. Como $10^n \equiv 4 \pmod 6$, para todo $n \geq 1$, o vetor que obtemos é $P = (4, 4, \ldots, 4, 4, 4, 1)$. Desse modo, um número $N = a_n 10^{n-1} + a_{n-1} 10^{n-2} + \ldots + a_2 10 + a_1 \in \mathbb{Z}$, escrito como em (1), é divisível por 6 se, e somente se, o número

$$\langle (a_n, a_{n-1}, \ldots, a_4, a_3, a_2, a_1), (4, 4, \ldots, 4, 4, 4, 1) \rangle$$

é divisível por 6.

Esse método se aplica a qualquer inteiro positivo e constitui uma abordagem diferente para se tratar de critérios de divisibilidade na educação básica. De certo modo, apenas utilizando o conceito de divisão euclidiana com resto, o método permite que o estudante use sua criatividade, ao tentar desenvolver um critério de divisibilidade.

Sistemas de Identificação Modulares

Desde a antiguidade o homem sentia a necessidade de se diferenciar dos demais, de se identificar. Era comum distinguir sua moradia fixando na entrada decalques em argila de desenhos palmares, juntamente com cabeças de animais dissecados ou até mesmo de inimigos vencidos em combate. Para identificação pessoal, era comum a utilização de dentes de animais presos às orelhas, lábios e nariz, bem como desenhos pelo corpo, como pode ser visto em Matias (2004).

Com o passar do tempo, vários métodos de identificação foram desenvolvidos, dada a necessidade de se identificar precisamente uma pessoa, um objeto ou um animal: era necessário saber se uma pessoa era realmente quem ela dizia ser ou verificar a procedência ou especificações de um objeto.

Com a crescente capacidade de processamento de informações dos computadores, os sistemas de informações tiveram uma grande evolução. Atualmente, surgiram os sistemas de Identificação Automática e Captura de Dados (AIDC, sigla proveniente de Automatic Identification and Data Capture), que identificam automaticamente objetos e lançam seus dados em sistemas de computador. Tais sistemas começaram a ser produzidos no final dos anos 40 e são desenvolvidos até os dias de hoje.

De modo geral, um sistema de identificação é um método no qual se identifica ou confere a autenticidade de um determinado item. Por exemplo: verificar se há erro na digitação de um número de documento, como o número do CPF; obter o preço de um produto verificando seu código de barras; restringir o acesso via reconhecimento óptico (retina) ou impressão digital, entre outros.

Os Sistemas de Identificação Modulares são os sistemas de identificação que utilizam a aritmética modular. Dado um inteiro $k > 1$, um número de identificação num sistema de identificação módulo k é da forma $a_1\ a_2 \ldots a_{n-1}\ d$, onde $a_1, a_2, \ldots, a_{n-1}, d$ são números entre 0 e $k - 1$ e d é o dígito verificador. Para determinar o valor de d, é escolhido no sistema um vetor $P = (p_1, p_2, \ldots, p_n)$, cujas componentes pertencem ao conjunto $\{0, 1, 2, \ldots, k - 1\}$ de modo que

$$\langle (a_1, a_2, \ldots, a_{n-1}, d), (p_1, p_2, \ldots, p_{n-1}, p_n) \rangle \equiv 0 \text{ (mod k)}.$$

Geralmente, o número p_n é escolhido sendo 1 para facilitar o cálculo de d. Para entender melhor, vejamos alguns exemplos.

Exemplo 3: Em uma determinada escola, será aplicada uma prova para os alunos do 1º, 2º e 3º ano do ensino médio. Ao se inscreverem, os alunos recebem um cartão de acesso

com uma numeração, para fins de registro e identificação. Essa numeração é composta por quatro números $a_1a_2a_3-a_4$ onde:

1. a_1 representa o número da fileira onde o aluno irá sentar no dia da prova, de modo que as fileiras são numeradas da esquerda para a direita. As salas possuem seis fileiras, cada uma com seis carteiras.
2. a_2 representa a numeração da carteira a que se sentará o aluno na fileira, onde as carteiras de cada fileira são numeradas da frente para o fundo.
3. a_3 representa a série em que o aluno está cursando; este dígito será 1 se o aluno cursar o 1º ano do ensino médio, 2 se tiver cursando o 2º ano e 3 se estiver no 3º ano.
4. a_4 é um dígito verificador, utilizado para verificar se não há fraude. Esse dígito é o menor número positivo que somado à $4a_1 + 3a_2 + 2a_3$ seja divisível por 7. Ou seja:

$$4a_1 + 3a_2 + 2a_3 + a_4 \equiv 0 \pmod 7.$$

E, assim, a_4 é o resto da divisão de $\langle (a_1, a_2, a_3), (3, 4, 5) \rangle$ por 7.

Um determinado aluno desta escola cursa o 1º ano do ensino médio e, após a inscrição, é informado que irá sentar-se na 4ª carteira da 3ª fileira. Qual será seu número de identificação? Com essas informações, sabemos que os três primeiros dígitos do seu registro são 341. Para calcular o dígito verificador, basta observar que o resto da divisão de $\langle (3, 4, 1), (3, 4, 5) \rangle = 3 \cdot 3 + 4 \cdot 4 + 1 \cdot 5 = 30$ por 7 é 2. Portanto, o seu número de identificação é $341-2$.

No dia da prova, um aluno estava com dois cartões de acesso, um com o número $232-0$ e outro com $352-2$. Como podemos saber qual cartão é válido? Podemos observar que $\langle (2, 3, 2), (3, 4, 5) \rangle = 28$, que deixa resto 0 na divisão por 7. Logo o cartão de acesso com numeração $232-0$ é válido. Por outro lado, temos que $\langle (3, 5, 2), (3, 4, 5) \rangle = 39$, deixando resto 4 na divisão por 7. Desse modo, o número de identificação $352-2$ não existe e, portanto esse cartão de acesso é falso.

Cadastro De Pessoa Física - CPF

O Cadastro de Pessoa Física foi instituído por meio do Decreto-lei número 401, no dia 30 de dezembro de 1968. Nesse momento, era portador de CPF apenas quem declarasse Imposto de Renda. Atualmente, o CPF é um documento de uso cotidiano de todo cidadão brasileiro. A figura 1 mostra um dos modelos deste documento.

Figura 1: Modelo de cartão de CPF.

Fonte: LIMA, 2015.

O CPF utiliza o sistema de identificação módulo 11, ou seja, o número do CPF consiste de 11 dígitos na forma $a_1a_2a_3a_4a_5a_6a_7a_8a_9 - a_{10}a_{11}$, sendo os dois últimos dígitos verificadores e $a_i \in \{0, 1, 2, \ldots, 9\}$, para $i = 1, 2, \ldots, 11$. Como o sistema de identificação é módulo 11, os dígitos verificadores podem assumir o valor 10. No caso de isso ocorrer, utiliza-se o dígito 0 no lugar do dígito 10. Para o cálculo de a_{10}, os vetores utilizados são $V_1 = (a_1, a_2, \ldots, a_{10})$ e $P_1 = (10, 9, 8, \ldots, 2, 1)$, de acordo com a equação $\langle V_1, P_1 \rangle \equiv 0 \pmod{11}$, ou seja,

$$\langle (a_1, a_2, \ldots, a_{10}), (10, 9, 8, \ldots, 2, 1) \rangle \equiv 0 \pmod{11}.$$

Com isso,

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

$$a_{10} \equiv \sum_{i=1}^{9} (i - 11) \cdot a_i \ (mod\ 11).$$

Como $(i - 11) \equiv i \ (mod\ 11)$, temos que

$$a_{10} \equiv \sum_{i=1}^{9} i \cdot a_i \ (mod\ 11),$$

donde

$$a_{10} \equiv \langle (a_1, a_2, \ldots, a_9), (1, 2, \ldots, 9) \rangle \ (mod\ 11).$$

Isso significa que a_{10} nada mais é do que o resto da divisão de $\langle (a_1, a_2, \ldots, a_9), (1, 2, \ldots, 9) \rangle$ por 11, sendo que o valor é trocado para 0 no caso de que o resto seja 10.

Agora, tendo encontrado o primeiro dígito verificador, é preciso encontrar o segundo, a_{11}. Nesse caso, são utilizados os vetores $V_2 = (a_1, a_2, \ldots, a_{10}, a_{11})$ e $P_2 = (11, 10, 9, 8, \ldots, 2, 1)$, de modo que a_{11} satisfaça a equação $\langle V_2, P_2 \rangle \equiv 0 \pmod{11}$. De modo

análogo ao cálculo de a_{10}, encontramos que

$$a_{11} \equiv \sum_{i=1}^{10} (i-1) \cdot a_i \ (mod\ 11).$$

Com isso, obtém-se que a_{11} é o resto da divisão de $\langle (a_1, a_2, \ldots, a_{10}), (0, 1, 2, \ldots, 9) \rangle$ por 11, valendo a mesma observação no caso de ocorrer resto 10.

De acordo com o raciocínio acima, fica claro que o cálculo para se encontrar os dígitos verificadores de um número de CPF pode ser feito utilizando-se apenas as operações de adição e multiplicação de números inteiros (que é o produto interno) e calculando restos da divisão por 11. Portanto, esse tipo de exemplo prático pode ser abordado em conteúdos da educação básica, sem exigir notações complicadas nem cálculos exagerados durante a aula. Vejamos como fazer isso em um exemplo fictício.

Exemplos 4**:** Os nove primeiros dígitos de um CPF são 063.210.421. O número completo é da forma $063.210.421 - a_{10}\ a_{11}$. Como

$$\langle (0, 6, 3, 2, 1, 0, 4, 2, 1), (1, 2, 3, 4, 5, 6, 7, 8, 9) \rangle$$
$$= 0 \cdot 1 + 6 \cdot 2 + 3 \cdot 3 + 2 \cdot 4 + 1 \cdot 5 + 0 \cdot 6 + 4 \cdot 7 + 2 \cdot 81 \cdot 9 = 87$$

e o resto da divisão de 87 por 11 é 10, temos que $a_{10} = 10$ e, como comentado anteriormente, o primeiro dígito verificador a_{10} é igual a 0. Até o momento, o CPF é $063.210.421 - 0a_{11}$.

Agora, como

$$\langle (0, 6, 3, 2, 1, 0, 4, 2, 0), (0, 1, 2, 3, 4, 5, 6, 7, 8, 9) \rangle = 68$$

e o resto da divisão de 68 por 11 é 2, segue que $a_{11} = 2$. Portanto, o número completo do CPF é 063.210.421 − 02.

Carteira Nacional De Habilitação - CNH

A Carteira Nacional de Habilitação (CNH) é o documento que confere ao cidadão o direito de dirigir carros, motocicletas e caminhões (de acordo com as habilidades do condutor). Ela possui um Número de Registro Nacional (veja o campo onde aparece o número fictício 22222222222, na figura 2), que é gerado pelo sistema informatizado da Base Índice Nacional de Condutores (BINCO), de acordo com a Resolução 192, de 30 de março de 2006.

A CNH, assim como o CPF, também utiliza o sistema de identificação módulo 11. Seu número de registro nacional é composto de nove caracteres $a_1, a_2, \ldots, a_9$ e de dois dígitos verificadores a_{10} e a_{11}. O cálculo é feito do mesmo modo que o do CPF. A única diferença é a disposição dos dígitos verificadores: o resultado é colocado na forma $a_1a_2a_3a_4a_5a_6a_7a_8a_9 - a_{11}a_{10}$.

Exemplo 5: Considerando uma CNH cujo número de registro inicia-se com os números 063210421, vimos no exemplo anterior que $a_{10} = 0$ e que $a_{11} = 2$. Com isso, seu número de registro é 06321042120.

Figura 2: Modelo de CNH.

Fonte: Detran/RS

Registro Nacional de Veículos Automotores (RENAVAM)

A sigla RENAVAM significa Registro Nacional de Veículos Automotores. Trata-se de um banco de dados que registra toda a vida de um veículo, desde quando o fabricante ou importador registra seus dados originais, passando pelo emplacamento, troca de propriedade, mudança de estado, mudanças de características até quando o mesmo sai de circulação.

O código RENAVAM é composto por 11 dígitos numéricos da forma $a_1a_2a_3 \ldots a11$, sendo a_{11} um dígito numérico verificador, que é calculado de modo a satisfazer

$$\langle (a_1, a_2, a_3, \ldots, a_{11}), (3, 2, 9, 8, 7, 6, 5, 4, 3, 2, 1) \rangle \equiv 0 \pmod{11}$$

Reescrevendo, a_{11} é o resto da divisão do número $\langle (a_1, a_2, \ldots, a_{10}), (8, 9, 2, 3, 4, 5, 6, 7, 8, 9) \rangle$ por 11, sendo substituído por 0 no caso do resto ser 10.

Exemplo 6: Vamos calcular o dígito verificador a_{11} de um Código Renavam formado, inicialmente, pelos números 0364801252. Veja que

$$\langle (0,3,6,4,8,0,1,2,5,2),(8,9,2,3,4,5,6,7,8,9)\rangle = 161$$

e, como o resto de 161 por 11 é 7, segue que o número completo do RENAVAM é 03648012527.

CONSIDERAÇÕES FINAIS

As aplicações tratadas aqui são utilizadas atualmente e, em muitos casos, conhecidas por grande parte da população. Outro assunto que pode ser abordado com este enfoque é a criptografia RSA, utilizada, atualmente, para segurança de dados na internet. Por exemplo, grande parte das compras e das operações bancárias feitas via internet utilizam essa criptografia. E ela está baseada no mesmo assunto: o resto da divisão de dois inteiros.

Embora o estudo de congruências modulares não faça parte dos temas abordados na educação básica da maioria dos centros educacionais, a divisão de números inteiros com resto sempre é. Desse modo, é possível abordar alguns temas atuais do cotidiano das pessoas utilizando conceitos básicos de Matemática já conhecidos, como adição, multiplicação e divisão de números inteiros.

REFERÊNCIAS

BARBOSA, Jhonattan. P. **Sistemas de identificação modulares em documentos do DETRAN:** uma forma alternativa de relacionar matemática e trânsito. Barra do Garças - MT: UFMT, 2015.

COUTINHO, Severino C. **Números Inteiros e Criptografia RSA**. Série de Computação e Matemática. Rio de Janeiro: IMPA, 2003.

DEPARTAMENTO ESTADUAL DE TRÂNSITO DO RIO GRANDE DO SUL. **Detran/RS emite novo modelo da Carteira Nacional de Habilitação**. Rio Grande do Sul, 29 de junho de 2006. Disponível em: <https://detran.rs.gov.br/detran-rs-emite-novo-modelo-dacarteira-nacional-de-habilitacao>. Acesso em: 20 jun. 2015.

HEFEZ, Abramo. **Aritmética**. Coleção Profmat. Rio de Janeiro: SBM, 2013.

_____. VILLELA, Maria L. T. **Códigos Corretores de Erros**. Série de Computação e Matemática. Rio de Janeiro: IMPA, 2002.

LIMA, Ronaldo F. **Checagem de CPF em C**. Ribeirão Preto, 31 de maio de 2015. Disponível em: <https://medium.com/dev-interior/checagem-de-cpf-em-C-a64fe7a386f5>. Acesso em: 20 jun. 2015.

MATIAS, Caio R. S. **Protótipo de um Sistema de Identificação do(s) Delta(s) e Núcleo em Impressões Digitais Utilizando Redes Neurais Artificiais**. 2004. 82 p. Monografia (Bacharelado em Ciências da Computação) - Centro de Ciências Exatas e Naturais, Universidade Regional de Blumenau, Blumenau, 2004. Disponível em: <bluehttp://dsc.inf.furb.br/arquivos/tccs/monografias/2004-2caiorsmatiasvf.pdf>. Acesso em: 04 out. 2014.

RIVEST, Ronald L.; SHAMIR, Adi e ADLEMAN, Leonard M. **Method for Obtaining Digital Signatures and PublicKey Cryptosystems**. Communications of the ACM 21 (2), p. 120-126, 1978.

SINGH, Simon. **O Último Teorema de Fermat**. Rio de Janeiro: Editora Record, 2004.