UNIVERSIDADE FEDERAL DE MATO GROSSO
INSTITUTO DE CIÊNCIAS EXATAS E DA TERRA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

JHONATTAN PINTO BARBOSA

SISTEMAS DE IDENTIFICAÇÃO MODULARES EM DOCUMENTOS DO DETRAN: UMA FORMA ALTERNATIVA DE RELACIONAR MATEMÁTICA E TRÂNSITO

BARRA DO GARÇAS - MT
2015

JHONATTAN PINTO BARBOSA

SISTEMAS DE IDENTIFICAÇÃO MODULARES EM DOCUMENTOS DO DETRAN: UMA FORMA ALTERNATIVA DE RELACIONAR MATEMÁTICA E TRÂNSITO

Dissertação apresentada ao programa de Pós-Graduação em Matemática em Rede Nacional - PROFMAT, da Universidade Federal de Mato Grosso, como requisito para a obtenção do título de Mestre em Ensino de Matemática.

Orientador: Prof. Dr. Adilson Antônio Berlatto

Barra do Garças - MT
2015

Dados Internacionais de Catalogação na Fonte.

B238s Barbosa, Jhonattan Pinto.
Sistemas de identificação modulares em documentos do DETRAN: uma forma alternativa de relacionar matemática e trânsito / Jhonattan Pinto Barbosa. -- 2015
85 f. : il. color. ; 30 cm.

Orientador: Adilson Antônio Berlatto.
Dissertação (mestrado profissional) - Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação em Matemática, Cuiabá, 2015.
Inclui bibliografia.

1. Aritmética Modular. 2. Sistemas de Identificação Modulares. 3. Matemática e o Trânsito. I. Título.

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Permitida a reprodução parcial ou total, desde que citada a fonte.

MINISTÉRIO DA EDUCACÃO
UNIVERSIDADE FEDERAL DE MATO GROSSO
PRÓ-REITORIA DE ENSINO DE PÓS-GRADUACÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL - PROFMAT
Avenida Fernando Corrêa da Costa, 2367 - Boa Esperança - Cep: 78060900 -Cuiabá/MT
Tel : (65) 3615-8713/8710 - Email : geraldo@ufmt.br

FOLHA DE APROVAÇÃO

TÍTULO : "Sistemas de identificação modulares em documentos do DETRAN: uma forma alternativa de relacionar matemática e trânsito"

AUTOR : Jhonattan Pinto Barbosa

defendida e aprovada em 23/02/2015.

Composição da Banca Examinadora:

Presidente Banca / Orientador Doutor(a) Adilson Antônio Berlatto
Instituição : UNIVERSIDADE FEDERAL DE MATO GROSSO

Examinador Interno Doutor(a) Juan Elmer Villanueva Zevallos
Instituição : UNIVERSIDADE FEDERAL DE MATO GROSSO

Examinador Externo Pós-Doutor(a) Ricardo Nunes de Oliveira
Instituição : Universidade Federal de Goiás - UFG

BARRA DO GARÇAS,23/02/2015.

AGRADECIMENTOS

Ao Deus todo poderoso, seu Filho Jesus Cristo e ao Espirito Santo por me auxiliar nesta tarefa, me sustentando e guiando em todo tempo.

Ao meu orientador, Prof. Dr. Adilson Antônio Berla tto, que acreditou neste projeto e soube encaminhar os trabalhos de forma que alcançássemos os objetivos traçados, sempre com uma palavra de encorajamento e apoio.

Em especial queria agradecer a minha esposa, Rosany que não mediu esforços para auxiliar-me neste projeto, tendo paciência e me incentivando nos momentos em que o desânimo aparecia, sendo companheira, amável, fiel, dedicada, isto é, simplesmente essencial.

A minha mãe, que acreditou em meus sonhos e sonhou junto comigo. Não desanimou, nem esmoreceu, apoiando em todo o tempo.

Aos meus amigos Max, Vinícius e principalmente Valdiego, que foi deveras importante para a conclusão desta dissertação.

Aos meus colegas de trabalho, em especial a Comissão Permanente para Análise de Licença para Formação profissional do Detran/MT, pela liberação nos dias de aula e ao Hewerton Sousa Ribeiro que me ajudou na criação do site que é uma das contribuições principais desta dissertação.

A todos os meus irmãos de fé, pelas orações e palavras de incentivo, em especial aos pastores Elcio e Edimar.

Enfim, a todos que de alguma forma contribuíram para a realização desta dissertação e ao curso como um todo o meu muito obrigado!

"*Tudo tem um tempo determinado,*
e há tempo para todo propósito
debaixo do céu."

(Bíblia Sagrada, Eclesiastes 3.1)

RESUMO

Esta dissertação tem como objetivo principal, ser um instrumento facilitador na tarefa de relacionar a matemática com a temática do trânsito. Para isso, utilizaremos os conceitos de Aritmética Modular existentes nos Sistemas de Identificação Modulares que encontram-se aplicados à guias e documentos do Departamento Estadual de Trânsito de Mato Grosso (Detran/MT), pois entendemos que o educando ao ingressar as séries finais do ensino fundamental e consequentemente o ensino médio já possui as ferramentas necessárias para a compreensão de tais conceitos devido a sua natureza elementar e aplicabilidade ao cotidiano do estudante. Entretanto, antes de abordarmos esse assunto apresentamos alguns conceitos preliminares, que sustentam os resultados utilizados. Além disso, no último capítulo apresentamos uma atividade que pode ser aplicada as séries finais do ensino fundamental e também no ensino médio, com o intuito de demonstrar a real possibilidade de abordar o tema trânsito nas aulas de matemática, sem que haja a necessidade de se utilizar tabelas, gráficos ou dados sobre acidentes de trânsito, números da frota de veículos, ou quaisquer outros indicadores estatísticos.

Palavras-chave: Aritmética Modular, Sistemas de Identificação Modulares, Matemática e o Trânsito.

ABSTRACT

This dissertation has the main aim, be a facilitator instrument on the task to relate the math with the transit theme. For this, we will use the Modular Arithmetic concepts existing on the Modular Identification Systems that were applied to guides and documents from Detran/MT, because we understand that the pupil when come into the final series from the elementary school and consequently high school already has the necessary instruments to the comprehension of such concepts due to their elemental nature and applicability to student's everyday. However, before we approach this subject we presented some preliminaries concepts, that sustain the utilized results. Furthermore, on the last chapter we present one activity that can be applied on final series from the elementary school and on the high school too, with the intuit to demonstrat the real possibility to approach the traffic theme on the math classes, without the necessity to use the tables, graphics or data about traffic acidentes, numbers from the vehicle fleet, or other statistical indicators.

Keywords: Modular Arithmetic, Modular Identification Systems, Math and the Transit.

Lista de Figuras

Lista de Tabelas

Sumário

INTRODUÇÃO

Quando vemos hoje os modernos sistemas de identificação, como por exemplo os sistemas biométricos ou os sistemas por rádio frequência (RFID), nem nos damos conta que o isso tudo teve seu início na mais remota antiguidade. Historiadores afirmam que os trogloditas já demonstravam interesse na identificação de suas moradias e também usavam em seu corpo vários adereços e desenhos, a fim de serem identificados pelos outros (APPOL apud MATIAS, 2004, on-line).

Entretanto, apenas nas últimas décadas com a criação e crescente capacidade de processamento dos computadores foi que os processos de identificação tiveram grande avanço. Entre esses sistemas de identificação destacaremos neste trabalho os sistemas de identificação modulares que são baseados na aritmética modular desenvolvida principalmente por Carl Friedrich Gauss em seu livro *Disquisitiones Arithmeticae*, publicado em 1801.

Os números de identificação do sistema são palavras $a_1a_2a_3\ldots a_n$ definidas em A que verificam

$$(p_1, p_2, p_3, \ldots, p_n) \cdot \big(\varphi(a_1), \varphi(a_2), \varphi(a_3), \ldots, \varphi(a_n)\big) \equiv 0 \pmod{k}$$

ou seja,

$$[p_1\varphi(a_1) + p_2\varphi(a_2) + p_3\varphi(a_3) + \cdots + p_n\varphi(a_n)] \equiv 0 \pmod{k},$$

onde A é um conjunto de cardinal k e φ uma função definida de A em $\mathbb{Z}_k$ ($\varphi : A \to \mathbb{Z}_k$) e uma n-upla $(p_1, p_2, p_3, \ldots, p_n)$ construído por inteiros não nulos. Além disso, a soma $p_1\varphi(a_1) + p_2\varphi(a_2) + p_3\varphi(a_3) + \cdots + p_n\varphi(a_n)$ é chamada de soma de controle. Dessa forma, os sistemas desse tipo serão denominados sistemas de identificação módulo k.

As aplicações desses sistemas são muito variadas, como o catálogo de livros, de revistas, periódicos, partituras musicais, e de outros produtos através do código de barras (EAN e UPC). Temos ainda aplicações em diversos documentos, como carteira

de identidade, passaporte, CPF, CNPJ, título de eleitor entre outros.

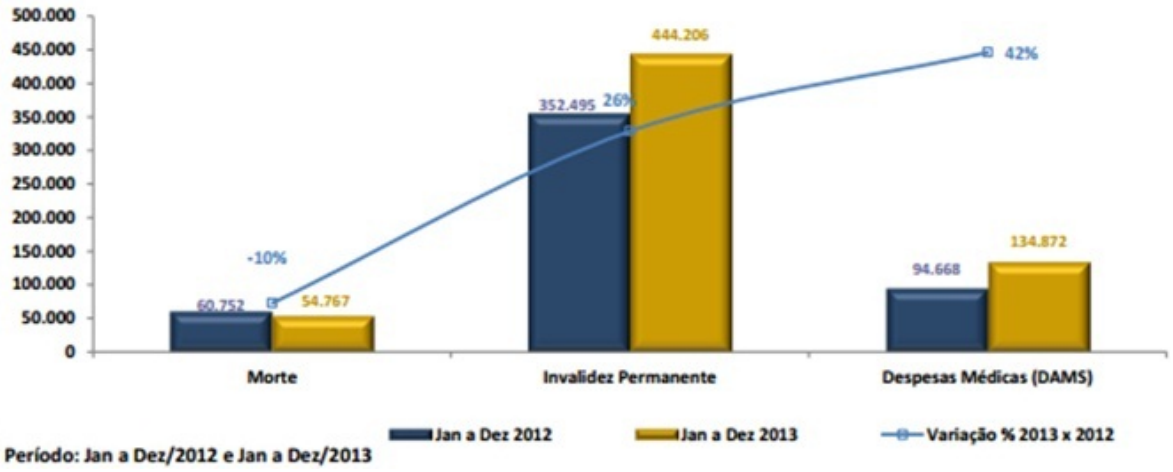
Neste trabalho, utilizaremos as aplicações destes sistemas de identificações modulares nos documentos e guias emitidos pelo Departamento Estadual de Trânsito do Estado do Mato Grosso a fim de oferecer uma forma alternativa de relacionar a matemática e o trânsito em sala de aula.

Uma questão que se levanta é: "Por que trabalhar trânsito em sala de aula?"

Primeiramente, por que a lei determina, através do Código de Trânsito Brasileiro (CTB), Lei n. 9.503, de 23 de setembro de 1997, onde em seu Capítulo VI, compreendido do art.74 ao art.79, afirma que a educação para o trânsito deverá ser promovida em todos os níveis educacionais, por meio de planejamento e ações coordenadas entre órgãos e entidades que compõe o Sistema Nacional de Trânsito.

Outro fator que nos leva a trabalhar o trânsito em sala de aula é o entendimento de que somente por meio da educação poderemos formar cidadãos responsáveis que compreendem e respeitam ativamente às normas e os princípios que os regem, e evitar que situações tão terríveis como as demonstradas pela gráfico abaixo continuem a acontecer:

Figura 1 – Evolução das indenizações pagas por natureza.



Fonte: Seguradora Líder DPVAT.

Este gráfico da evolução das indenizações pagas aos que foram vítimas de acidente de trânsito, mostra que apenas nos dois últimos anos mais de 115 mil pessoas tiveram suas vidas ceifadas em acidentes de trânsito e quase 800 mil nesse mesmo período ficaram com sequelas graves para toda a vida.

Deste modo, vemos que inserir o trânsito não é apenas necessário, mas uma questão de urgência. Entretanto, para que haja sucesso não se deve inserir o trânsito no currículo escolar como uma nova disciplina, mas ele deve ser incluído como um tema transversal, uma vez que os temas transversais não pertencem a nenhuma disciplina

específica, mas "atravessam" todas elas como se a todas fossem pertinentes, expressando conceitos e valores básicos à democracia e cidadania e obedecendo a questões importantes e urgentes à sociedade contemporânea. (KRASILCHIK & MARANDINO, 2004)

Assim sendo, entendendo que o conceito de congruência pode ser uma definição de fácil assimilação por parte do aluno, tendo em vista que os alunos já trabalham os conceitos de divisão exata e divisão com resto pequeno desde o princípio de sua vida na escola, decidimos apresentar uma proposta ao professor de matemática como alternativa para relacionar o trânsito em suas aulas, utilizando os sistemas de identificação modulares presentes nos documentos e guias do Detran/MT.

Dessa forma, para que o leitor possa compreender a nossa proposta, dividimos esta dissertação em quatro capítulos. No primeiro capítulo, são abordados os conceitos de Divisibilidade, Máximo Divisor Comum, Congruência e Classes Residuais, os quais são imprescindíveis, para a compreensão dos sistemas de identificação e aplicação da proposta. No segundo capítulo, tratamos sobre os diversos tipos de sistemas de identificação e mostramos algumas aplicações. O terceiro capítulo mostra as aplicações dos sistemas de identificação modulares nos documentos e guias do Detran/MT. E finalizamos, com o quarto capítulo apresentando uma proposta de atividade que proporciona aos alunos uma aprendizagem significativa tanto dos conceitos matemáticos, quanto dos conceitos relacionados ao trânsito.

CAPÍTULO 1

CONCEITOS PRELIMINARES

Este capítulo apresenta definições e resultados importantes para a compreensão do nosso objeto de estudo, que são as aplicações dos sistemas de identificações modulares em documentos do DETRAN. Estas definições e resultados aqui abordados foram obtidas com base em Alencar Filho (1987), Gomes e Silva (2008) e Hefez (2011, 2012).

Assim sendo, iniciaremos esse capítulo com um simples, porém crucial conceito, que é o conceito de divisibilidade.

1.1 Divisibilidade

Considerando o conjunto dos números inteiros $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, temos que a divisão de um número inteiro por outro nem sempre é possível, quando for possível diremos que há uma relação de divisibilidade.

Definição 1.1. Sejam a e b dois inteiros, com $a \neq 0$. Diz-se que a *divide* b se e somente se existe um inteiro c tal que $b = ac$. De maneira equivalente, se a *divide* b dizemos que a é um *divisor* de b, ou ainda que, a é um *fator* de b. Além disso, se a *divide* b temos que b é *divisível* por a, ou semelhantemente, b é *múltiplo* de a. Denotaremos $a \mid b$ para dizer que $a \neq 0$ *divide* b e, portanto, $a \nmid b$ significa que $a \neq 0$ *não divide* b.

Exemplo 1.2. Hallowen, ou dia das bruxas, é uma tradição dos países de língua inglesa onde no dia 31 de outubro, as crianças andam de casa em casa em sua vizinhança pedindo guloseimas, com a frase: "Gostosuras ou travessuras?". Neste ano, a fim de evitar que sua casa seja alvo das travessuras das crianças, Beth adquiriu 204 doces para a festividade tendo a intenção de distribuir 4 deles a cada criança que bater a sua

porta. Sabendo que existem 50 crianças na vizinhança de Beth, podemos dizer que a quantidade de doces que Beth comprou será suficiente? A resolução desse problema está alicerçada no conceito de divisibilidade, ou seja, queremos saber se existe um número inteiro q, tal que $4 \cdot q = 204$. De fato existe tal inteiro, basta que $q = 51$ para $4 \cdot 51 = 204$, isto é, Beth poderá agradar a 51 crianças, sendo assim ela comprou balinhas em quantidade suficiente.

Exemplo 1.3. Um famoso banco da capital decidiu renegociar as dívidas de seus clientes a fim de não ficar com um prejuízo tão grande e ofereceu ao cliente a oportunidade de pagamento do valor devido em 9 prestações iguais sem acréscimo de juros. Sabendo que um saldo negativo em conta de $R\$\,783,00$. Quanto deve ser o valor de cada parcela paga pelo cliente? Novamente, precisaremos do conceito de divisibilidade agora aplicado a valores negativos, pois se considerarmos que o débito figura como valor negativo, temos que encontrar um q tal que:

$$9 \cdot q = -783$$

logo, $q = -87$, ou seja, o valor da parcela deverá ser de $R\$\,87,00$. Além disso, o sinal negativo interpreta-se pelo fato de representar valor devido a cada parcela.

Exemplo 1.4. Em alguns shoppings podemos encontrar poltronas que massageiam aqueles que nelas sentam, desde que os mesmos coloquem num lugar específico da poltrona uma cédula que corresponde ao pagamento pelos serviços de massagem. Assim sendo, sabendo que uma poltrona dessas aceita apenas notas de $R\$\,2,00$ reais e um indivíduo possui $R\$\,37,00$ reais. Podemos dizer que ele conseguirá gastar todo seu dinheiro nessa poltrona? Para que a resposta a essa questão seja verdadeira, precisamos encontrar q inteiro tal que $2 \cdot q = 37$, o que é impossível, já que $2 \nmid 37$. Logo, temos que essa pessoa não conseguirá gastar todo o seu dinheiro nessa poltrona.

As proposições e teoremas que apresentaremos em seguida são propriedades fundamentais da divisibilidade nos inteiros.

Proposição 1.5. *Se $a \in \mathbb{Z}$, então:*

(i) $a \mid 0$

(ii) $1 \mid a \quad e \quad -1 \mid a$

(iii) $a \mid a \quad e \quad -a \mid a$

Demonstração.

(i) Como $0 = a \cdot 0$, temos que $a \mid 0$.

(ii) Temos que $a = 1 \cdot a$ e $a = (-1) \cdot (-a)$, dessa forma, $1 \mid a$ e $-1 \mid a$.

(iii) Observamos ainda que, $a = a \cdot 1$ e $a = (-a) \cdot (-1)$, assim obtemos que $a \mid a$ e $-a \mid a$.

■

Proposição 1.6. *Se $a \mid b$ então:*

(i) $-a \mid b$,

(ii) $a \mid -b$,

(iii) $-a \mid -b$,

(iv) $|a| \mid |b|$.

Demonstração. Como $a \mid b$, temos que $b = a \cdot c$, e como $a \neq 0$, segue-se que $-a \neq 0$ e $|a| \neq 0$. Dessa forma:

(i) $b = (-a) \cdot (-c)$

(ii) $-b = a \cdot (-c)$

(iii) $-b = (-a) \cdot c$

(iv) $|b| = |a \cdot c| = |a| \cdot |c|$

Com isso provamos os itens (i), (ii), (iii) e (iv).

■

Teorema 1.7. *Sejam a e b dois inteiros.*

(i) Se $a \mid 1$, então $a = 1$ ou $a = -1$.

(ii) Se $a \mid b$ e se $b \mid a$, então $a = b$ ou $a = -b$.

(iii) Se $a \mid b$, com $b \neq 0$, então $|a| \leq |b|$.

Demonstração.

(i) Sabemos que 1 e -1 são divisores de 1. Sendo assim, suponhamos que $a \mid 1$, logo, existe $c \in \mathbb{Z}$ tal que $1 = a \cdot c$ e, assim, $1 = |a \cdot c| = |a| \cdot |c|$. De modo que $|a| \neq 0$ e $|c| \neq 0$, ou seja, $|a| \geq 1$ e $|c| \geq 1$. Porém se $|a| > 1$, então $|a| \cdot |c| > |c| \geq 1$, dessa forma, $|a| \cdot |c| > 1$ o que é impossível. Logo, $|a| = 1$, isto é, $a = 1$ ou $a = -1$.

(ii) Temos que se $a \mid b$ e se $b \mid a$, então $b = ac$ e $a = bd$, onde $c, d \in \mathbb{Z}$. Logo $b = ac = bdc$, assim, $cd = 1$. Dessa forma, $d \mid 1$. Portanto $d = 1$ ou $d = -1$. Assim sendo, $a = b$ ou $a = -b$.

(iii) Observamos que se $a \mid b$, com $b \neq 0$, então $b = ac$, com $c \neq 0$. Logo, $|c| \geq 1$ e $|b| = |a||c| \geq |a|$. Assim sendo, $|a| = |b|$ se e somente se $a = \pm b$.

■

Corolário 1.8. *Todo inteiro $a \neq 0$ tem somente um número finito de divisores.*

Demonstração. Seja x um divisor de a, logo $x \mid a$, então $|x| \leq |a|$, ou seja, $-a \leq x \leq a$. Logo o número de divisores é finito.

■

Teorema 1.9. *Sejam a, b, c e d inteiros.*

(i) Se $a \mid b$ e se $c \neq 0$, então $ac \mid bc$.

(ii) Se $ac \mid bc$, então $a \mid b$.

(iii) Se $a \mid b$ e se $c \mid d$, então $ac \mid bd$.

(iv) Se $a \mid b$ e se $b \mid c$, então $a \mid c$.

(v) Se $a \mid b$ e se $a \mid c$, então $a \mid (bx \pm cy)$, onde $x, y \in \mathbb{Z}$.

Demonstração.

(i) Como $a \neq 0$, por definição e $c \neq 0$ por hipótese, temos que $ac \neq 0$. Por outro lado, se $a \mid b$, então $b = at$, onde $t \in \mathbb{Z}$. Logo, $bc = (ac)t$. Daí, $ac \mid bc$.

(ii) Como $ac \neq 0$, temos que $a \neq 0$ e $c \neq 0$. De outro modo, se $ac \mid bc$, então $bc = act$, com $t \in \mathbb{Z}$. Consequentemente, $b = at$ e disto temos que $a \mid b$.

(iii) Se $a \mid b$ e se $c \mid d$, então $b = at$ e $d = cs$, onde $t, s \in \mathbb{Z}$. Logo, $bd = atcs = acts$, daí, $ac \mid bd$.

(iv) Temos que se $a \mid b$ e se $b \mid c$, então $b = at$ e $c = bs$, onde $t, s \in \mathbb{Z}$. Assim, $c = ats$. Logo, $a \mid c$.

(v) Observamos que se $a \mid b$ e se $a \mid c$, então $b = at$ e $c = as$, onde $t, s \in \mathbb{Z}$. Dessa forma, sejam $x, y \in \mathbb{Z}$, temos que $bx \pm cy = atx \pm asy = a(tx \pm sy)$. De onde obtemos que $a \mid (bx \pm cy)$.

■

Exemplo 1.10. Dispondo de 72 laranjas, João decide vender suas laranjas em pacotes que cabiam uma dúzia, ou seja, 12 laranjas. Porém ao perceber que sua clientela reclamavam que havia muitas laranjas em um mesmo pacote, decidiu colocar as laranjas

em pacotes menores com 4 laranjas cada. Mas, neste instante lhe surgiu uma dúvida, será que a nova disposição em pacotes com 4 laranjas acomodará perfeitamente as 72 laranjas que possui? Sabemos que $4 \mid 12$ e que $12 \mid 72$, logo pelo item (iv) do Teorema 1.9, temos que $4 \mid 72$. Assim sendo, João pode ficar tranquilo que os pacotes com 4 laranjas acomodarão perfeitamente as suas 72 laranjas.

1.2 Algoritmo da Divisão

Apresentaremos a seguir um algoritmo que garante a existência e a unicidade de um quociente q e um resto r que permite efetuar a divisão entre dois números inteiros, onde um deles não é necessariamente um múltiplo do outro. Para isso, primeiramente enunciaremos um axioma denominado Princípio da Boa Ordenação, pois ele é fundamental para a demonstração do algoritmo.

Axioma 1.11 (Princípio da Boa Ordenação)**.** *Todo subconjunto não vazio $A \subseteq \mathbb{N}$ possui elemento menor que todos os outros elementos deste, ou seja, existe $a \in A$ tal que $a \leq n$ para todo $n \in A$.*

Teorema 1.12 (Algoritmo da Divisão)**.** *Se a e b são dois inteiros, com $b > 0$, então existem únicos inteiros q e r tais que:*

$$a = bq + r \quad e \quad 0 \leq r < b.$$

Demonstração. Consideremos o conjunto:

$$S = \{a - bx; x \in \mathbb{Z}, a - bx \geq 0\}.$$

Observamos que este conjunto é não vazio, pois, para $x = -|a|$, temos, $a - bx = a + b|a|$. Por outro lado, como $b \geq 1$, $b|a| \geq |a|$ e $a + b|a| \geq a + |a| \geq 0$. Deste modo provamos que S contém o inteiro $a + b|a|$, ou seja, S é não vazio. Assim, pelo Princípio da Boa Ordenação, existe o elemento mínimo r de S tal que, $r \geq 0$ e $r = a - bq$, com $q \in \mathbb{Z}$, isto é:

$$a = bq + r \quad \text{e} \quad 0 \leq r.$$

Além de que, o inteiro $r < b$, porque, se caso contrário teríamos $r \geq b$, onde $r - b \geq 0$ e como $r - b = a - b(q + 1)$. Logo $r - b \in S$. Porém, $r - b < r$, o que seria uma contradição, pois r é o elemento mínimo de S. Assim,

$$a = bq + r \quad \text{e} \quad 0 \leq r < b.$$

Passemos agora à prova da unicidade de q e r. Suponhamos que $a = bq + r = bq' + r'$,

onde $q, q', r, r' \in \mathbb{Z}$, $0 \leq r < b$ e $0 \leq r' < b$. Logo, $r' - r = b(q' - q)$, ou seja, $r' - r$ é múltiplo de b, porém, $-b < -r \leq r' - r < b$. Assim $r' - r = 0$, pois é único múltiplo de b em $(-b, b)$. Deste modo, $r = r'$ e consequentemente $b(q' - q) = 0$, logo, $q = q'$.

■

O exemplo abaixo mostra uma aplicação simples do Teorema 1.12.

Exemplo 1.13. Um estudante de álgebra leva todos os dias para a aula 7 folhas de papel para anotar tópicos que achar relevante. Ao contar suas folha restantes, verifica que dispõe de 53 folhas, à quantas aulas ele conseguirá levar essa mesma quantidade de papel? Neste exemplo vamos encontrar o quociente q e o resto r da divisão de 53 por 7. Como $53 = 7 \cdot 7 + 4$, temos que $q = 7$ e $r = 4$ satisfazem as condições do Teorema 1.12, ou seja, o estudante assistirá 7 aulas portando como de costume 7 folhas e lhe restará ainda 4 folhas.

O teorema a seguir aborda de forma generalizada a divisão entre dois inteiros a e b, onde garante que para a existência de únicos q e r, basta que $b \neq 0$.

Teorema 1.14 (Forma generalizada do algoritmo da divisão)**.** *Se a e b são dois inteiros, com $b \neq 0$, então existem e são únicos os inteiros q e r que satisfazem às condições:*

$$a = bq + r \quad e \quad 0 \leq r < |b|.$$

Demonstração. Observemos primeiramente que se $b > 0$, pelo Teorema 1.12, já temos o que queremos. Portanto, consideremos $b < 0$, assim $|b| > 0$ e consequentemente, pelo Teorema 1.12, existem únicos q' e r tais que $a = |b|q' + r$ e $0 \leq r < |b|$. Porém, $|b| = -b$, pois $b < 0$ e tomando $q = -q'$, obtemos:

$$a = bq + r \quad \text{e} \quad 0 \leq r < |b|.$$

■

Exemplo 1.15. Encontremos o quociente q e o resto r da divisão euclidiana de $a = 16$ por $b = -6$. Temos pelo Teorema 1.14, que q e r devem satisfazer

$$16 = (-6)q + r \quad \text{e} \quad 0 \leq r < |-6|.$$

Assim sendo, os únicos q e r que satisfazem tais condições são $q = -2$ e $r = 4$, pois,

$$16 = (-6)(-2) + 4 \quad \text{e} \quad 0 \leq 4 < |-6|.$$

1.3 Máximo Divisor Comum (M.D.C.)

Nesta seção, abordaremos a definição e algumas propriedades do máximo divisor comum, um tema que será muito útil para definição de critérios para a detecção de erros em sistemas de identificação modulares. Entretanto, iniciaremos essa seção recordando o conceito de divisor comum, para que posteriormente apresentemos o tema central desta seção.

Definição 1.16. Dados dois números inteiros a e b, não simultaneamente nulos, $d \in \mathbb{Z}$ é um divisor comum de a e b se $d \mid a$ e $d \mid b$.

Exemplo 1.17. No Exemplo 1.10 temos que $4 \mid 12$ e $4 \mid 72$, logo 4 é um divisor comum de 12 e 72.

Definição 1.18 (M.D.C.)**.** Sejam a e b dois inteiros não conjuntamente nulos. Chama-se máximo divisor comum de a e b o inteiro positivo d $(d > 0)$ que satisfaz às condições:

(i) $d \mid a$ e $d \mid b$, ou seja, d é divisor comum de a e b.

(ii) Se $c \mid a$ e se $c \mid b$, então $c \mid d$.

Portanto, se d é um mdc de a e b e c é um divisor comum desses números, então $|c|$ divide d e, portanto, $c \leq |c| \leq d$. Isto nos mostra que o máximo divisor comum de dois números é efetivamente o maior dentre todos os divisores comuns desses números. O máximo divisor comum de a e b indica-se pela notação $mdc(a, b)$.

A definição do $mdc(a, b)$ é, obviamente, simétrica em relação aos inteiros a e b, de modo que $mdc(a, b) = mdc(b, a)$. Em particular:

(i) Temos que $mdc(0, 0)$ não existe.

(ii) O $mdc(a, 1) = mdc(a, -1) = 1$.

(iii) Se $a \neq 0$, então $mdc(a, 0) = |a| = mdc(a, a)$.

(iv) O $mdc(a, 0) = 1$ se e somente se $a = \pm 1$.

(v) Se $a \mid b$, então o $mdc(a, b) = |a|$.

Exemplo 1.19. Em detrimento das definições acima é fácil ver que:

1. $mdc(5, 1) = mdc(5, -1) = 1$.
2. $mdc(-6, 0) = |-6| = 6$, pois $-6 \neq 0$.
3. $mdc(-4, 8) = |-4| = 4$, pois $-4 \mid 8$.

Definição 1.20. Sejam a e b dois inteiros. Chama-se combinação linear de a e b todo inteiro n da forma $n = ax + by$, onde x e y são inteiros quaisquer. Dessa forma temos que:

$$46 = 12 \cdot 5 + 7 \cdot (-2)$$

ou seja, 46 é uma combinação linear dos inteiros 12 e 7.

Mostraremos agora um teorema que, segundo Carneiro (2009, on-line), infelizmente é omitido no ensino do máximo divisor comum no ensino fundamental, que é o fato notável de que o máximo divisor comum de dois inteiros pode ser expresso como uma combinação linear desses dois números. Além disso, essa propriedade do M.D.C. é tão importante em Aritmética que alguns autores a chamam de Teorema Fundamental da Teoria dos Números, mais usualmente conhecido como Teorema de Bézout.

Teorema 1.21 (Forma linear do M.D.C. ou Teorema de Bézout)**.** *Se a e b são dois inteiros não conjuntamente nulos, então existem inteiros x e y tais que o $mdc(a, b) = ax + by$, isto é, o $mdc(a, b)$ é uma combinação linear de a e b.*

Demonstração. Seja S o conjunto de todos os inteiros positivos da forma $au + bv$, onde u e v são inteiros, ou seja:

$$S = \{au + bv;\ au + bv > 0 \text{ e } u, v \in \mathbb{Z}\}.$$

Temos que S é não vazio, pois, se $a \neq 0$, suponhamos $a > 0$, então $a = a \cdot 1 + b \cdot 0 > 0$ pertence a S. Suponhamos agora $a < 0$, então $-a = a \cdot (-1) + b \cdot 0 > 0$ pertence a S. Logo S é não vazio.

Disto temos que pelo Principio da Boa Ordenação, existe e é único o elemento mínimo d de S. Assim sendo, $d = \min S$, logo existem inteiros x e y tais que $d = ax+by$.

Destarte, provemos agora que $d = mdc(a, b)$. Aplicando o algoritmo da divisão aos inteiros a e d, temos:

$$a = dq + r, \quad \text{onde} \quad 0 \leq r < d.$$

Assim,

$$r = a - dq = a - (ax + by)q = a(1 - qx) + b(-qy)$$

ou seja, o resto r é uma combinação linear de a e b. Dessa forma, se $r > 0$, então r pertence a S, o que é impossível, posto que $0 \leq r < d$ e $d > 0$ é o elemento mínimo de S. Portanto, $r = 0$ e $a = dq$, isto é, $d \mid a$. De maneira análoga se conclui que $d \mid b$, ou seja, d é um divisor comum de a e b.

Enfim, se c é um divisor comum positivo de a e b, então $c \mid (ax + by)$. Logo $c \mid d$ e $c \leq d$, ou seja, d é maior divisor comum positivo de a e b.

Dessa forma, $mdc(a,b) = d = ax + by,\ x, y \in \mathbb{Z}$, como queríamos demonstrar.

■

Observação 1.22. Pelo Teorema 1.21 o $mdc(a,b) = d$, e como d é o elemento mínimo do conjunto S, segue-se que o $mdc(a,b)$ existe e é único. Além disso, o $mdc(a,b)$ é o menor inteiro positivo da forma $ax+by$, ou seja, que pode ser escrito como combinação linear de a e b.

Observação 1.23. A representação do $mdc(a,b)$ como combinação linear de a e b não é única, pois, temos:

$$mdc(a,b) = d = ax + by = a(x + bt) + b(y - at).$$

Quaisquer que seja o inteiro t.

Dentre as várias aplicações do Teorema de Bézout, destacaremos na próxima proposição a possibilidade de que para determinarmos que dois números a e b são primos entre si, basta que existam inteiros m e n tais que $an + bm = 1$.

Proposição 1.24. *Dois números inteiros a e b são primos entre si se, e somente se, existem inteiros m e n tais que $an + bm = 1$. De fato, primeiramente suponhamos que a e b sejam primos entre si, ou seja, $mdc(a,b) = 1$. Mas, pelo teorema de Bézout temos que existem m e n inteiros tais que $an + bm = 1$. Por outro lado, se existem m e n tais que $an + bm = 1$ e $d = mdc(a,b)$, temos que $d \mid a$ e $d \mid b$, logo $d \mid (an + bm)$, ou seja, $d \mid 1$. O que implica necessariamente que $d = mdc(a,b) = 1$.*

Teorema 1.25. *Se a e b são dois inteiros não conjuntamente nulos, então o conjunto de todos os múltiplos do $mdc(a,b) = d$ é*

$$T = \{ax + by;\ x, y \in \mathbb{Z}\}.$$

Demonstração. Temos que $d \mid (ax + by)$, para quaisquer inteiros x e y, pois $d \mid a$ e $d \mid b$. Logo, todo elemento de T é um múltiplo de d. Por outro lado, existem inteiros x_0 e y_0 tais que $d = ax_0 + by_0$, de modo que todo múltiplo kd de d é da forma:

$$kd = k(ax_0 + by_0) = a(kx_0) + b(ky_0).$$

Ou seja, kd é uma combinação linear de a e b e, assim, kd é elemento do conjunto T.

■

Teorema 1.26. *Se a e b são dois inteiros não conjuntamente nulos, então o*

$$mdc(a,b) = mdc(a + kb, b)$$

para todo inteiro k.

Demonstração. Sejam $d = mdc(a, b)$ e $d' = mdc(a + kb, b)$, para provarmos o resultado desejado provemos os dois itens abaixo:

(i) $d \mid d'$

Sabemos que $d \mid a$ e $d \mid b$, logo $d \mid (a + kb)$. Assim, como $d \mid (a + kb)$ e $d \mid b$, temos que $d \mid d'$.

(ii) $d' \mid d$

Como $d' \mid b$, então $d' \mid (-kb)$, onde $k \in \mathbb{Z}$. Disto e do fato que $d' \mid (a+kb)$, temos que $d' \mid (a + kb + (-kb))$, ou seja $d' \mid a$. Assim sendo, $d' \mid a$ e $d' \mid b$, logo $d' \mid d$.

Dessa forma por (i) e (ii) temos $d = d'$.

■

1.4 Algoritmo de Euclides

Forneceremos agora um processo prático para calcular o M.D.C. de dois inteiros positivos a e b denominado Algoritmo de Euclides ou processo das divisões sucessivas. Segundo Hefez (2011), esse processo foi enunciado por Euclides em sua obra, Os Elementos, em Alexandria, por volta do ano 300 A.C. e é até hoje o método mais eficiente para o cálculo do máximo divisor comum de dois inteiros. No entanto, antes de passarmos ao método, provaremos um lema que é essencial para estabelecermos o Algoritmo de Euclides.

Lema 1.27 (Lema de Euclides)**.** *Se $a = bq + r$, então o $mdc(a, b) = mdc(b, r)$.*

Demonstração. Sejam $d = mdc(a, b)$ e $d' = mdc(b, r)$, disto temos que $d \mid a$ e $d \mid b$, logo $d \mid (a - bq)$, ou seja, $d \mid r$. Assim, $d \mid d'$. Por outro lado, se $d' \mid b$ então $d' \mid bq$, consequentemente $d' \mid (a - bq + bq)$, isto é, $d' \mid a$. Dessa forma, $d' \mid d$. Como $d \mid d'$ e $d' \mid d$, temos que $d = d'$.

■

Algoritmo de Euclides ou Processo das Divisões Sucessivas

Sejam a e b dois inteiros não conjuntamente nulos cujo mdc se deseja determinar. Discutiremos aqui apenas o caso onde a e b são inteiros positivos distintos tais que b não divide a, pois os demais casos são tratados acima ou são análogos devido ao fato de que $mdc(a, b) = mdc(-a, b) = mdc(a, -b) = mdc(-a, -b)$. Além disso, admitiremos sem perda de generalidade que $a > b$.

Iniciamos dividindo a por b, como $b \nmid a$ podemos escrever

$$a = bq_1 + r_1,$$

onde $r_1, q_1 \in \mathbb{Z}$ e $0 < r_1 < b$. Pelo Lema 1.27,

$$mdc(a, b) = mdc(b, r_1).$$

Dividindo b por r_1, se $r_1 \mid b$ então $mdc(b, r_1) = r_1 = mdc(a, b)$. Caso contrário podemos escrever

$$b = r_1q_2 + r_2,$$

onde $r_2, q_2 \in \mathbb{Z}$ e $0 < r_2 < r_1$. Pelo Lema 1.27,

$$mdc(b, r_1) = mdc(r_1, r_2).$$

Agora, dividindo r_1 por r_2, $r_2 \mid r_1$ então

$$mdc(r_1, r_2) = r_2 = mdc(b, r_1) = mdc(a, b).$$

Caso contrário, podemos escrever

$$r_1 = r_2q_3 + r_3,$$

onde $r_3, q_3 \in \mathbb{Z}$ e $0 < r_3 < r_2$. Pelo Lema 1.27,

$$mdc(r_1, r_2) = mdc(r_2, r_3).$$

Este procedimento não pode continuar indefinidamente, pois teríamos uma sequência de números naturais $b > r_1 > r_2 > \cdots$ que não possui menor elemento, o que não é possível pelo Princípio da Boa Ordenação. Logo para algum n, temos $r_n \mid r_{n-1}$ o que implica que $mdc(a, b) = r_n$.

Podemos sistematizar o procedimento da seguinte forma:

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

Exemplo 1.28. Em uma transportadora, haviam dois tipos de objetos os perecíveis e os não perecíveis que eram acomodados em caixas. Tendo que efetuar uma entrega de 252 objetos perecíveis e 54 objetos não perecíveis, com a menor quantidade de caixas

possível, com caixas de mesmo tamanho, ou seja, que caibam a mesma quantidade de objetos e sem que os objetos estejam misturados dentro das caixas. Qual será a quantidade de objetos em cada caixa? E quantas caixas serão utilizadas ao todo? Para a resolução deste exemplo será necessária a aplicação do conceito de *mdc*, sendo assim, vamos calcular o $mdc(54, 252)$ utilizando o procedimento acima, logo temos que

	4	1	2
252	54	36	$18 = mdc(54, 252)$
36	18		

Assim sendo, observamos que $mdc(54, 252) = 18$, isto é, temos que cada caixa conterá 18 objetos e o número de caixas com objetos perecíveis será de 14, uma vez que $18 \cdot 14 = 252$ e que o número de caixas com objetos não perecíveis será 3, pois, $18 \cdot 3 = 54$. Deste modo, temos que ao todo serão necessárias $14 + 3 = 17$ caixas.

1.5 Congruência Módulo m

Veremos nesta seção um dos conceitos mais importantes da Teoria de Números introduzidos por Carl Friedrich Gauss em seu livro *Disquisitiones Arithmeticae*, o conceito de congruência modular ou congruência módulo m.

Uma particularidade interessante desta definição é que ela está intimamente ligada a divisibilidade e aos restos de uma divisão de números inteiros o que torna sua abordagem no Ensino Fundamental e Médio uma possibilidade tangível e de certo modo necessária. Haja vista que, podemos observar as várias aplicações dessa aritmética em nosso dia-a-dia como, por exemplo: nos relógios analógicos e digitais, na criptografia, em eventos cíclicos, na otimização de rede de computadores, nos sistemas de identificação modulares (CPF, CNPJ, códigos de barra, ISBN, EAN, ...) que é o tema principal deste trabalho, entre outras.

Deste modo, passemos agora a essa imprescindível definição:

Definição 1.29. Sejam a e b dois números inteiros e m um número inteiro maior que 1. Diremos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Usamos a notação $a \equiv b \pmod{m}$ para representar o fato de que a é congruente a b módulo m. Caso contrário, diremos que a não é congruente a b módulo m ou que a é incongruente a b módulo m e usamos a notação $a \not\equiv b \pmod{m}$.

A proposição que se segue nos mostra um fato importante: que não é necessário sempre dividir a por m e b por m e comparar os restos para que $a \equiv b \pmod{m}$, basta que $m \mid (b - a)$ para que tenhamos que $a \equiv b \pmod{m}$.

Proposição 1.30. *Suponha que $a, b, c \in \mathbb{Z}$, com $m > 1$. Tem-se que $a \equiv b \pmod{m}$ se, e somente se, $m \mid (b - a)$.*

Demonstração. Sejam $a = mq + r$, com $r < m$ e $b = mq' + r'$, com $r' < m$, as divisões euclidianas de a e b por m, respectivamente. Dessa forma,

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

Portanto, $a \equiv b \pmod{m}$ se, e somente se, $r = r'$, ou seja, $a \equiv b \pmod{m}$ se, e somente se, $m \mid (b - a)$.

■

Proposição 1.31. *Se $a, m \in \mathbb{Z}$, com $m > 1$ e r é o resto da divisão euclidiana de a por m, então $a \equiv r \pmod{m}$.*

Demonstração. Pelo Algoritmo da Divisão Euclidiana, existe um número inteiro q tal que $a = mq + r$. Daí, tem-se $a - r = mq$. Logo, $m \mid (a - r)$ que pela proposição anterior é equivalente a $a \equiv r \pmod{m}$.

■

As proposições a seguir apresentam propriedades fundamentais para as aplicações de congruências que serão efetuadas ao longo deste trabalho.

Proposição 1.32. *Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m>1$ obtemos que*

(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) $a \equiv b \pmod{m}$ se, se somente se, $a + c \equiv b + c \pmod{m}$,

(vi) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $ac \equiv bd \pmod{m}$.

Demonstração.

(i) Temos que $m \mid (a - a)$, daí do resultado desejado.

(ii) Como $a \equiv b \pmod{m}$, temos que $m \mid (b - a)$, mas pela Proposição 1.6, item (ii), obtemos que $m \mid -(b - a)$, ou seja, $m \mid (a - b)$, de onde obtemos o resultado desejado.

(iii) Por hipótese temos que $m \mid (b-a)$ e $m \mid (b-c)$, então pelo Teorema 1.9, item (v), temos que $m \mid [(b-a)-(b-c)]$, logo $m \mid (c-a)$ o que é equivalente a $a \equiv c \pmod{m}$.

(iv) Basta observar que pelo Teorema 1.9, item (v), obtemos que $m \mid [(b-a)+(d-c)]$ e, portanto, $m \mid (b+d)-(a+c)$, o que prova o resultado.

(v) Ao observarmos que $a \equiv b \pmod{m}$ e $c \equiv c \pmod{m}$, segue do item anterior que $a+c \equiv b+c \pmod{m}$. Reciprocamente, se $a+c \equiv b+c \pmod{m}$, então $m \mid [(b+c)-(a+c)]$, de onde obtemos que $m \mid (b-a)$ e, consequentemente, $a \equiv b \pmod{m}$.

(vi) Como $m \mid (b-a)$ e $m \mid (d-c)$, pelo Teorema 1.9, item (v), temos que $m \mid [d(b-a)+a(d-c)]$, ou seja, $m \mid (bd-ac)$. Assim obtemos o resultado desejado.

■

Proposição 1.33. *Sejam $a, b, c, m \in \mathbb{Z}$, com $c \neq 0$ e $m > 1$. Temos que*

$$ac \equiv bc \ (mod\, m) \iff a \equiv b \ \left(mod \frac{m}{mdc(c,m)}\right).$$

Demonstração. Temos que

$$ac \equiv bc \pmod{m} \iff m \mid (b-a)c \iff \frac{m}{mdc(c,m)} \mid (b-a)\frac{c}{mdc(c,m)}.$$

como o $mdc\left(\frac{m}{mdc(c,m)}, \frac{c}{mdc(c,m)}\right) = 1$, então,

$$\frac{m}{mdc(c,m)} \mid (b-a)$$

o que implica que

$$a \equiv b \ \left(\mod \frac{m}{mdc(c,m)}\right).$$

■

Uma importante aplicação das proposições apresentadas acima são os critérios de divisibilidade que podem ser encontrados em Esquinca (2013, on-line) e Hefez (2012).

As próximas seções foram baseadas em Hefez (2011) e Araujo (2009, on-line) e são indispensáveis para a compreensão dos sistemas de identificações modulares, pois estão ligadas ao cálculo não só do dígito verificador, mas também dos outros dígitos, caso seja necessário.

1.6 Congruências Lineares

Definição 1.34. Chamamos de congruência linear a toda equação do tipo $aX \equiv b \pmod{m}$, onde $a, b, m \in \mathbb{Z},\ m > 1$.

Proposição 1.35. *Dados $a, b, m \in \mathbb{Z}$, com $m > 1$, a congruência $aX \equiv b \pmod{m}$ possui solução se, e somente se, $mdc(a, m) \mid b$.*

Demonstração. Suponhamos que a congruência $aX \equiv b \pmod{m}$ tenha uma solução x; logo, temos que $m \equiv ax - b$, ou seja, existe y tal que $ax - b = my$, ou equivalentemente, $ax - my = b$. Assim, como $mdc(a, m) \mid a$ e $mdc(a, m) \mid m$, logo $mdc(a, m) \mid (ax - my)$ e consequentemente $mdc(a, m) \mid b$.

Reciprocamente, suponhamos agora que $d = mdc(a, m) \mid b$. Daí, pelo Teorema 1.21, existem inteiros u e v tais que $d = au - mv$. Por outro lado, como $d \mid b$, existe n tal que $b = nd$. Agora multiplicando n aos dois membros da equação $au - mv = d$, temos $a(un) - m(vn) = nd$, o que mostra que os números $x = un$ e $y = vn$ formam uma solução para a equação $aX - mY = b$. Disto temos que $ax - my = b$, ou seja, $ax - b = my$, isto é, $m \mid (ax - b)$ ou equivalentemente, x é solução da congruência $aX \equiv b \pmod{m}$.

■

Teorema 1.36. *Sejam $a, b, m \in \mathbb{Z}$, com $m > 1$ e $(a, m) \mid b$. Se x_0 é uma solução da congruência $aX \equiv b \pmod{m}$, então*

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d},$$

onde $d = mdc(a, m)$, formam um sistema completo de soluções incongruentes da congruência.

Demonstração. Primeiramente, sabemos pela proposição anterior que a congruência admite solução. Passaremos então agora a mostrar que os números $x_0 + i\frac{m}{d}$, com $i \in \mathbb{N}$, são soluções. Observemos que

$$a\left(x_0 + i\,\frac{m}{d}\right) = ax_0 + i\,\frac{a}{d}\,m \equiv ax_0 \equiv b \pmod{m}.$$

Além disso, esse números são dois a dois incongruentes módulo m. Pois, temos que se, para $i, j < d$,

$$x_0 + i\,\frac{m}{d} \equiv x_0 + j\,\frac{m}{d} \pmod{m},$$

então

$$i\,\frac{m}{d} \equiv j\,\frac{m}{d} \pmod{m}.$$

Logo, pela Proposição 1.33 e ainda pelo fato de que $mdc\left(\frac{m}{d}, m\right) = \frac{m}{d}$, onde $d = mdc(a, m)$, temos que

$$i \equiv j \pmod{d}.$$

O que implica que $i = j$.

Para finalizar, seja x uma solução qualquer da congruência, logo $ax \equiv ax_0 \pmod{m}$, e assim novamente pela Proposição 1.33, temos que

$$x \equiv x_0 \pmod{\frac{m}{d}}.$$

Dessa forma, $x - x_0 = k\frac{m}{d}$. Pela divisão euclidiana, existe $i < d$ tal que $k = qd + i$ e, portanto,

$$x = x_0 + qm + i\,\frac{m}{d} \equiv x_0 + i\,\frac{m}{d} \pmod{m}.$$

■

Corolário 1.37. *Se $mdc(a, m) = 1$, então a congruência $aX \equiv b \pmod{m}$ possui uma única solução módulo m.*

A congruência $aX \equiv 1 \pmod{m}$, com $mdc(a, m) = 1$, admite solução única módulo m. Esta solução será chamada de inverso multiplicativo de a módulo m. E será representada por a^{-1}.

1.7 Sistema Completo de Restos

Definição 1.38. Seja m um inteiro positivo fixo. Chama-se sistema completo de restos módulo m todo conjunto $S = \{r_1, r_2, \ldots, r_m\}$ de m inteiros tal que qualquer a é congruente módulo m a um único elemento de S.

Proposição 1.39. *O conjunto $S = \{0, 1, 2, \ldots, m-1\}$ é um sistema completo de restos módulo m.*

Demonstração. Mostraremos que todo inteiro a é congruente módulo m a exatamente um dos valores $0, 1, 2, \ldots, m-1$. Seja $a \in \mathbb{Z}$. Pelo algoritmo da divisão de a por m, existem únicos inteiros q e r tais que $a = mq + r$ com $a \leq r \leq m-1$. Logo, $a - r = mq$ e $a \equiv r \pmod{m}$. Pela unicidade de r, obtemos o resultado. ■

1.7.1 Classes Residuais

Definição 1.40. Seja m um inteiro positivo fixo. Se a é um inteiro qualquer então a classe residual módulo m de a, denotada por $\overline{a}$ (ou $[a]_m$ ou a_m), consiste do conjunto

formado por todos os inteiros que são congruentes ao inteiro a módulo m, isto é,

$$\overline{a} = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\} = \{x \in \mathbb{Z} : m \mid x - a\} = \{a + km : k \in \mathbb{Z}\}.$$

Observação 1.41. As classes residuais módulo m também são denominadas inteiros módulo m ou classes de restos módulo m ou classes de congruência módulo m.

Exemplo 1.42. Seja $m = 9$. Temos:

- $\overline{4} = \{x \in \mathbb{Z} : x \equiv 4 \pmod{9}\} = \{x \in \mathbb{Z} : 9 \mid x - 4\} = \{4 + 9k : k \in \mathbb{Z}\} = \{\ldots, -14, -5, 4, 13, \ldots\}$.
- $\overline{22} = \{x \in \mathbb{Z} : x \equiv 22 \pmod{9}\}$. Como $22 \equiv 4 \pmod{9}$ então $x \equiv 22 \pmod{9}$ se, e somente se, $x \equiv 4 \pmod{9}$. Logo, $\overline{22} = \{x \in \mathbb{Z} : x \equiv 4 \pmod{9}\} = \overline{4}$.

Proposição 1.43. *Seja m um inteiro positivo fixo e sejam $\overline{a}$ e $\overline{b}$ as classes residuais módulo m de dois inteiros quaisquer a e b. Então:*

(i) $\overline{a} = \overline{b} \iff a \equiv b \,(mod\, m)$

(ii) $\overline{a} \cap \overline{b} = \emptyset$ *ou* $\overline{a} = \overline{b}$*, ou seja, se* $\overline{a} \cap \overline{b} \neq \emptyset$*, então* $\overline{a} = \overline{b}$

Demonstração.

(i) Seja $\overline{a} = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\}, \overline{b} = \{x \in \mathbb{Z} : x \equiv b \pmod{m}\}$ e $\overline{a} = \overline{b}$, logo existe $y \in \mathbb{Z}$, tal que $y \in \overline{a}$ e $y \in \overline{b}$. Disto temos que, $y \equiv a \pmod{m}$ e $y \equiv b \pmod{m}$, daí tem-se $a \equiv b \pmod{m}$.

Por outro lado, seja $t \in \overline{a}$, logo $t \equiv a \pmod{m}$, como $a \equiv b \pmod{m}$ temos que, $t \equiv b \pmod{m}$, ou seja, $t \in \overline{b}$, daí temos que $\overline{a} \subset \overline{b}$. Em contrapartida, seja $w \in \overline{b}$, logo $w \equiv b \pmod{m}$, como $a \equiv b \pmod{m}$ temos que, $w \equiv a \pmod{m}$, ou seja, $w \in \overline{a}$, daí temos que $\overline{b} \subset \overline{a}$, e consequentemente $\overline{a} = \overline{b}$.

(ii) Se $\overline{a} \cap \overline{b} \neq \emptyset$, temos que existe $y \in \mathbb{Z}$, tal que, $y \in \overline{a}$ e $y \in \overline{b}$, ou seja, $y \equiv a \pmod{m}$ e $y \equiv b \pmod{m}$, daí tem-se $a \equiv b \pmod{m}$ e assim pelo item (i) segue que $\overline{a} = \overline{b}$.

■

1.7.2 O Conjunto das Classes Residuais

O conjunto formado por todas as classes residuais módulo m, ou seja, $\{\overline{a} : a \in \mathbb{Z}\}$ é indicado por $\mathbb{Z}_m$.

Proposição 1.44. *O conjunto $\mathbb{Z}_m$ tem exatamente m elementos.*

Demonstração. Primeiramente mostraremos que $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$. De fato, pois temos obviamente que $\{\overline{0}, \overline{1}, \ldots, \overline{m-1}\} \subset \mathbb{Z}_m$. Além disso, seja $\overline{a} \in \mathbb{Z}_m$, onde $a \in \mathbb{Z}$. Pelo algoritmo da divisão de a por m, existem inteiros q e r tais que $a = mq + r$, $0 \leq r \leq m-1$. Assim $a - r = mq$, ou seja, $m \mid a - r$. Logo $a \equiv r \pmod{m}$ e pela Proposição 1.43, temos que $\overline{a} = \overline{r}$. Como $0 \leq r \leq m-1$ então $\overline{a} = \overline{r} \in \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$. Dessa forma, temos que $\mathbb{Z}_m \subset \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$, o que implica necessariamente que $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$. Suponhamos agora que $\overline{r} = \overline{s}$, onde $r, s \in \mathbb{Z}$ tais que $0 \leq r < s \leq m-1$. Novamente, pela Proposição 1.43 temos que $r \equiv s \pmod{m}$. Assim $s \equiv r \pmod{m}$ e $m \mid s - r$. Mas isto é um absurdo, pois $0 < s - r < m$. Portanto $\{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ tem exatamente m elementos. ∎

Uma vantagem das classes residuais é que transformam a congruência $a \equiv b \pmod{m}$ na igualdade $\overline{a} = \overline{b}$.

Definição 1.45 (Adição e Multiplicação em $\mathbb{Z}_m$)**.**

(i) Dadas duas classes $\overline{a}$ e $\overline{b} \in \mathbb{Z}_m$, chama-se soma $\overline{a} + \overline{b}$ a classe $\overline{a+b}$ (que é única, independentemente do representante tomado para $\overline{a}$ ou para $\overline{b}$).

$$\begin{array}{rccc} + : & \mathbb{Z}_m \times \mathbb{Z}_m & \longrightarrow & \mathbb{Z}_m \\ & (\overline{a}, \overline{b}) & \longmapsto & \overline{a} + \overline{b} = \overline{a+b} \end{array}$$

(ii) Dadas duas classes $\overline{a}$ e $\overline{b} \in \mathbb{Z}_m$, chama-se produto $\overline{a} \cdot \overline{b}$ a classe $\overline{ab}$ (que é única, independentemente do representante tomado para $\overline{a}$ ou para $\overline{b}$).

$$\begin{array}{rccc} \cdot : & \mathbb{Z}_m \times \mathbb{Z}_m & \longrightarrow & \mathbb{Z}_m \\ & (\overline{a}, \overline{b}) & \longmapsto & \overline{a} \cdot \overline{b} = \overline{ab} \end{array}$$

Definidas dessa forma as operações acima gozam das seguintes propriedades:

(a) Associatividade da soma: $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$

(b) Comutatividade da soma: $\overline{a} + \overline{b} = \overline{b} + \overline{a}$

(c) Elemento neutro para a soma: $\overline{a} + \overline{0} = \overline{a}$

(d) Elemento simétrico para a soma: $\overline{a} + \overline{m-a} = \overline{0}$

(e) Associatividade do produto: $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$

(f) Comutatividade do produto: $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$

(g) Elemento neutro para o produto: $\overline{a} \cdot \overline{1} = \overline{a}$

(h) Distributividade da multiplicação em relação à adição: $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$

Um elemento $\overline{a} \in \mathbb{Z}_m$ será dito invertível quando existir $\overline{b} \in \mathbb{Z}_m$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$. Neste caso, diremos que $\overline{b}$ é o inverso de $\overline{a}$.

Proposição 1.46. *$\overline{a} \in \mathbb{Z}_m$ é simetrizável para a multiplicação, ou seja, admite inverso multiplicativo se, e somente se, $mdc(a, m) = 1$.*

Demonstração. Primeiramente observemos que se $\overline{a} \in \mathbb{Z}_m$ admite inverso multiplicativo, então existe $\overline{b} \in \mathbb{Z}_m$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$, ou seja, $ab \equiv 1 \pmod{m}$. Disto temos que $m \mid ab - 1$, logo existe $q \in \mathbb{Z}$ tal que $ab - 1 = mq$ e assim temos que $ab + m(-q) = 1$, isto é, $mdc(a, m) = 1$. Por outro lado, se $mdc(a, m) = 1$, existem $x, y \in \mathbb{Z}$, tal que $ax + my = 1$, daí obtemos $ax - 1 = (-y)m$, logo temos que $m \mid ax - 1$, ou seja, $ax \equiv 1 \pmod{m}$, ou equivalentemente, $\overline{a} \cdot \overline{x} = \overline{1}$, isto é, $\overline{a}$ admite inverso multiplicativo.

■

Assim resolver uma congruência $aX \equiv b \pmod{m}$ se reduz a resolver em $\mathbb{Z}_m$ a seguinte equação:

$$\overline{a}X = \overline{b}.$$

Exemplo 1.47. Resolver a congruência $9X \equiv 5 \pmod{11}$ equivale a resolver em Z_{11} a equação

$$\overline{9}X = \overline{5}.$$

Sabemos que em Z_{11}, $\overline{5} \cdot \overline{9} = \overline{1}$, logo temos que

$$\overline{5} \cdot \overline{9}X = \overline{5} \cdot \overline{5} = \overline{3}$$

ou seja, $X = \overline{3}$. Portanto as soluções de $9X \equiv 5 \pmod{11}$ são $x = 3 + 11t$, onde $t \in \mathbb{Z}$.

No capítulo a seguir faremos um estudo de alguns sistemas de identificação, com ênfase aos sistemas de identificação modulares.

CAPÍTULO 2

SISTEMAS DE IDENTIFICAÇÃO

Historiadores, arqueólogos e exploradores afirmam que a história da identificação humana tem seu início desde a longínqua antiguidade, onde trogloditas usavam diversos sinais para marcarem suas moradias. Um método de identificação bastante utilizado para distinguir a sua moradia das demais, era o de decalcar em argila desenhos palmares, colori-los e fixa-los em sua moradas juntamente com cabeças dessecadas de animais ou até mesmo de inimigos abatidos em combate. Além disso, para sua "identificação pessoal", usavam dentes de animais preso as orelhas, lábios e nariz, além de vários desenhos pelo corpo (APPOL apud MATIAS, 2004, on-line).

Com o passar do tempo foram desenvolvidos vários métodos de identificação, pois era cada vez maior a necessidade de se identificar precisamente uma pessoa, um objeto, um animal e etc.... Afinal era necessário saber se uma pessoa era realmente quem ela dizia ser, ou ainda, saber a origem e as especificações de um determinado objeto. Mais do que isso, os sistemas de identificação passaram a proporcionar qualidade de vida às pessoas. Como exemplo podemos mencionar o sistema de identificação de cores para daltônicos "ColorAdd" (para maiores detalhes, ver Neiva (2014, on-line)). Entretanto, apenas nas últimas décadas com a criação dos computadores e sua crescente capacidade de processamento de informações foi que os sistemas de identificação tiveram uma grande evolução.

Essa evolução deve-se principalmente ao surgimento dos sistemas de identificação automática (Automatic Identification and Data Capture - AIDC, Identificação Automática, Auto-ID ou ainda, Captura Automática de Dados), que são métodos de identificação automática de objetos e pessoas que coletando dados sobre eles conseguem adiciona-los diretamente a sistemas de computador, ou seja, sem interferência humana. (WIKIPÉDIA, 2014, on-line).

Segundo Moura (2006, on-line), o grande benefício dos AIDC é a precisão e velocidade na abstração da informação, pois com isso evita-se erros ligados a atividade humana. Além disso, ele destaca que nesses sistemas as informações recolhidas são disponibilizadas em um breve espaço de tempo a todos os utilizadores do sistema, o que torna essa ferramenta muito atrativa e útil.

Dentre outros sistemas de identificação, podemos citar os de identificação: por intermédio do reconhecimento óptico de caracteres (Optical Character Recognition - OCR), mediante a apresentação de cartões inteligentes (Smart Card), por rádio frequência (Radio-Frequency IDentification - RFID), através de dados biométricos (impressões digitais, veias, retina, voz, íris entre outros), por meio do código de barras.

As próximas seções, tomando por base Lourenço (2011), Picado (2001) e Milies (2008, 2009), apresentaram a definição de sistemas de identificação modulares, algumas aplicações e como detectar possíveis erros de leitura e escritas mais comuns nestes sistemas.

2.1 Sistemas de Identificação Modulares

Segundo Picado (2001), a grande evolução dos sistemas automáticos tornou-os relativamente baratos, rápidos e confiáveis. Com isso, a utilização destes sistemas para a leitura de números, fez com que a justaposição de um algarismo aos números de identificação de uma dada coleção de objetos, com o objetivo de detectar os erros de leitura e escrita mais comuns tornasse uma prática comum.

É interessante observar que estes sistemas não corrigem os erros automaticamente, apenas informam ao operador a existência de um erro, sem entretanto, precisar em qual posição do número ocorreu o erro. Dessa forma, os operadores são forçados a reescrever todo o número inserido no sistema. Ainda assim, os sistemas de identificação modulares se tornaram muito atrativos e bastante utilizados.

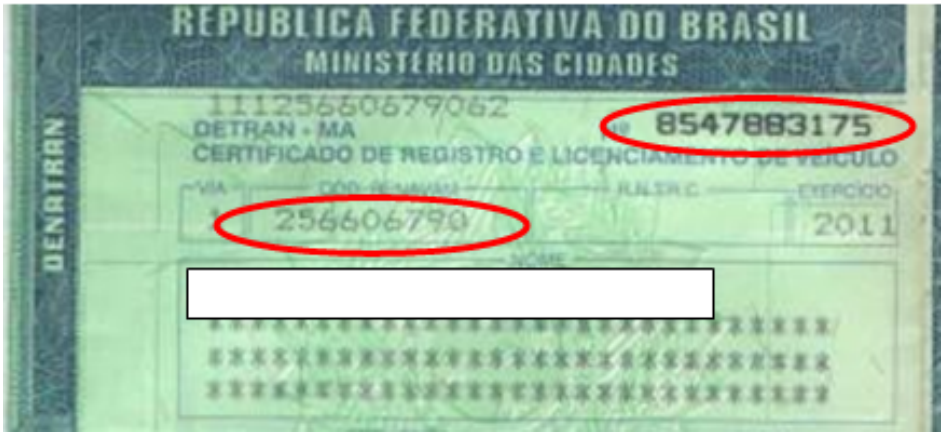
Citaremos aqui alguns exemplos de aplicações destes sistemas: o sistema ISBN (International Standard Book Number) para o catálogo de livros, o sistema ISMN (International Standard Music Number) para publicações de pautas musicais, o ISSN (International Standard Serial Number) para publicações periódicas, os sistemas UPC (Universal Product Code) e EAN (European Article Numbering) utilizado nos códigos de barras. Além desses, existem diversos outros sistemas que utilizam-se de dígitos verificadores e que não possuem uma nomenclatura específica e podem ser encontrados em cartões de crédito, contas bancárias, cheques, bilhetes de avião, passaportes, documentos de identidade, carteira de habilitação, guias de arrecadação, documentos de veículos, cadastros de pessoas físicas e jurídicas, título eleitoral, entre outros.

Exemplo 2.1. Imagens de algumas das aplicações acima citadas:

Figura 2.1 – Número do Cadastro de Pessoas Físicas.

Fonte: AGÊNCIA BRASIL, 2011.

Figura 2.2 – Número do Espelho do Certificado de Registro e Licenciamento de Veículo e Código Renavam.



Fonte: http://autos.culturamix.com/dicas/documentacao-de-veiculos-usados

Figura 2.3 – Código de barras com utilização do Sistema EAN-13.

Fonte: GB Network & Print, 2014.

Figura 2.4 – Código de barras com utilização do Sistema ISBN-13.

Fonte: http://www.esquemafacil.com.br/livros-tecnicos/televisores/livro-fly-back-s-tirando-duvidas-ref-5537-isbn-978-85-7036-139-4.html

Apresentaremos a seguir a Definição 2.2 que estabelece o produto entre os algarismos que serão inseridos pelo usuário e os respectivos pesos que serão associados a cada um desses algarismos.

Definição 2.2. Dados as n-uplas $(x_1, x_2, x_3, \ldots, x_n)$ e $(y_1, y_2, y_3, \ldots, y_n)$, onde $x_1, x_2, x_3, \ldots, x_n, y_1, y_2, y_3, \ldots, y_n \in \mathbb{Z}$, definimos o produto $(x_1, x_2, x_3, \ldots, x_n) \cdot (y_1, y_2, y_3, \ldots, y_n)$ como o número inteiro $x_1y_1 + x_2y_2 + x_3y_3 + \cdots + x_ny_n$.

Exemplo 2.3. O produto entre $(1, 3, 2, 4, 6, 8)$ e $(9, 5, 7, 4, 2, 1)$ é $1 \cdot 9 + 3 \cdot 5 + 2 \cdot 7 + 4 \cdot 4 + 6 \cdot 2 + 8 \cdot 1 = 74$.

Com os conceitos do Capítulo 1 e a Definição 2.2, podemos apresentar as características comuns dos diversos sistemas de identificação modulares e ainda analisá-los de forma geral e sistemática, por meio da Definição 2.4 que se segue.

Definição 2.4. Sejam A um conjunto de cardinal k e φ uma função definida de A em $\mathbb{Z}_k$ ($\varphi : A \to \mathbb{Z}_k$) e uma n-upla $(p_1, p_2, p_3, \ldots, p_n)$ construído por inteiros não nulos. Designamos esta n-upla por vetor de verificação de algarismos do sistema e aos seus elementos p_i, $i = 1, \ldots, n$, por pesos.

Os números de identificação do sistema são palavras $a_1a_2a_3 \ldots a_n$ definidas em A que verificam

$$(p_1, p_2, p_3, \ldots, p_n) \cdot \big(\varphi(a_1), \varphi(a_2), \varphi(a_3), \ldots, \varphi(a_n)\big) \equiv 0 \pmod{k}$$

ou seja,

$$[p_1\varphi(a_1) + p_2\varphi(a_2) + p_3\varphi(a_3) + \cdots + p_n\varphi(a_n)] \equiv 0 \pmod{k}$$

Denominamos os sistemas desse tipo por sistemas de identificação módulo k e à soma $p_1\varphi(a_1) + p_2\varphi(a_2) + p_3\varphi(a_3) + \cdots + p_n\varphi(a_n)$ por soma de controle.

Exemplo 2.5. Ao analisarmos o EAN-13 podemos perceber que:

$k = 10,\ \ A = \{0, 1, \ldots, 9\},\ \ \varphi(a) = a\ \ \text{e}\ \ (p_1, p_2, \ldots, p_n) = (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1).$

Além disso, temos que a soma de controle é

$$[p_1\varphi(a_1) + p_2\varphi(a_2) + p_3\varphi(a_3) + \cdots + p_n\varphi(a_n)] = \sum_{i=0}^{6} a_{2i+1} + 3\sum_{i=1}^{6} a_{2i} = \cdots$$

$$\cdots = a_1 + 3a_2 + a_3 + 3a_4 + a_5 + 3a_6 + a_7 + 3a_8 + a_9 + 3a_10 + a_11 + 3a_12 + a_13.$$

Ou seja, o dígito verificador a_{13} será

$$a_{13} \equiv -\left(\sum_{i=0}^{5} a_{2i+1} + 3\sum_{i=1}^{6} a_{2i}\right) \pmod{10}$$

Observação 2.6. Para não sobrecarregarmos muito a notação cometeremos o abuso, daqui em diante, de identificar $\varphi(a)$ com a.

2.2 Detectando erros mais comuns em Sistemas de Identificação Modulares

Passaremos agora a discorrer de forma sucinta sobre os erros mais comuns que ocorrem na escrita dos números de identificação.

Definição 2.7. Consideremos $a_1a_2a_3\ldots a_n$ um número de identificação de comprimento n.

- Um erro singular acontece quando um dos caracteres do número é alterado para um diferente valor $(\ldots a_i \ldots \to \ldots a_i' \ldots)$;
- Referimo-nos a um erro de transposição de algarismos adjacentes quando existe uma troca entre dois algarismos adjacentes $(\ldots a_ia_j \ldots \to \ldots a_ja_i \ldots)$;
- Designamos por erro de transposição intercalada, quando ocorre a troca entre dois algarismos que têm exatamente um a intercalá-los $(\ldots a_ia_ka_j \ldots \to \ldots a_ja_ka_i \ldots)$;
- Os erros gêmeos sucedem quando dois caracteres consecutivos iguais são mudados para um outro par de caracteres iguais $(\ldots aa \ldots \to \ldots a'a' \ldots)$;
- Designam-se por erros gêmeos intercalados quando sucede uma modificação de dois caracteres iguais, separados por um terceiro caractere, por um outro par de caracteres iguais $(\ldots aa_ka \ldots \to \ldots a'a_ka' \ldots)$;

- Existem também os erros gêmeos generalizados que consistem na alteração de dois caracteres iguais por um outro par de caracteres iguais, independentemente da posição que ocupam ($\ldots a \ldots a \ldots \to \ldots a' \ldots a' \ldots$).

Os restantes dos erros, abrangidos pelas outras categorias, podem ser agregados todos na classe dos erros aleatórios e fonéticos.

Tão importante quanto saber quais são os tipos de erros é saber a frequência relativa de cada um deles, a fim de que se possa construir um sistema que possa identificar tais erros. A Tabela 2.1 mostra essa frequência relativa:

Tabela 2.1 – Tipos de erros e suas frequências relativas.

Tipos de Erros	Forma	Frequência Relativa
Singulares	$\ldots a_i \ldots \to \ldots a'_i \ldots$	79,1%
Transposições de algarismos adjacentes	$\ldots a_i a_j \ldots \to \ldots a_j a_i \ldots$	10,2%
Transposições intercaladas	$\ldots a_i a_k a_j \ldots \to \ldots a_j a_k a_i \ldots$	0,8%
Gêmeos	$\ldots aa \ldots \to \ldots a'a' \ldots$	0,5%
Gêmeos intercalados	$\ldots aa_k a \ldots \to \ldots a'a_k a' \ldots$	0,3%
Aleatórios e fonéticos		9,1%

Fonte: LOURENÇO, 2011.

Estes estudos estatísticos também nos dizem que caso seja observado a ocorrência de algum desses erros, a ocorrência de mais do que um é muito pouco provável (PICADO, 2001).

Agora de posse das definições 2.4 e 2.2, juntamente com os dados da Tabela 2.1 podemos determinar quando os erros mais comuns (singulares e de transposição) são detectáveis:

Proposição 2.8. *Consideremos um número $a_1a_2a_3 \ldots a_n$ de um sistema de identificação módulo k e com vetor de verificação de algarismos $(p_1, p_2, p_3, \ldots, p_n)$. Temos que:*

(i) Um erro singular $\ldots a_i \ldots \to \ldots a'_i \ldots$ na i-ésima posição é detectável se e só se $p_i(a_i - a'_i) \not\equiv 0 \pmod{k}$.

(ii) Uma transposição dos algarismos a_i e a_j nas posições i e j é detectável se e só se $(p_i - p_j)(a_i - a_j) \not\equiv 0 \pmod{k}$.

Demonstração.

(i) Seja S a soma de controle com os algarismos corretos e S' a soma de controle com a troca de um algarismo $(\ldots a_i \ldots \to \ldots a_i' \ldots)$ caracterizando o erro singular. Temos por definição de soma de controle que $S \equiv 0 \pmod{k}$ e $S' \equiv 0 \pmod{k}$ se o erro não for detectado ou $S' \not\equiv 0 \pmod{k}$ se o erro for detectado. Verifiquemos o valor da diferença entre S e S'.

$$\begin{aligned} S - S' = & \ (p_1a_1 + p_2a_2 + \cdots + p_ia_i + \cdots + p_na_n) \\ & -(p_1a_1 + p_2a_2 + \cdots + p_ia_i' + \cdots + p_na_n) \\ = & \ p_ia_i - p_ia_i' \\ = & \ p_i(a_i - a_i'). \end{aligned}$$

Assim, obtemos que o erro é detectável somente se $p_i(a_i - a_i') \not\equiv 0 \pmod{k}$.

(ii) Neste caso a diferença entre a soma de teste correta e a soma de teste errada é

$$\begin{aligned} S - S' = & \ (p_1a_1 + p_2a_2 + \cdots + p_ia_i + \cdots + p_ja_j + \cdots + p_na_n) \\ & -(p_1a_1 + p_2a_2 + \cdots + p_ia_j + \cdots + p_ja_i + \cdots + p_na_n) \\ = & \ p_ia_i + p_ja_j - p_ia_j - p_ja_i \\ = & \ p_i(a_i - a_j) + p_j(a_j - a_i) \\ = & \ p_i(a_i - a_j) - p_j(a_i - a_j) \\ = & \ (p_i - p_j)(a_i - a_j) \end{aligned}$$

Portanto o erro só será detectado se e só se $(p_i - p_j)(a_i - a_j) \not\equiv 0 \pmod{k}$.

■

Exemplo 2.9. Seja $k = 7$, $(p_1, p_2, \ldots, p_n) = (1, 2, 3, 4, 5, 6)$, $\varphi(a) = a$ e $A = \{0, 1, 2, 3, 4, 5, 6\}$, temos que este sistema detecta todos os erros singulares, pois como k é primo, então para que o erro não fosse detectado teríamos obrigatoriamente que $k \mid p_i$ ou $k \mid (a_i - a_i')$ o que não acontece, pois $p_i \in \{1, 2, 3, 4, 5, 6\}$ e $1 \leq (a_i - a_i') \leq 6$.

Exemplo 2.10. Seja $k = 10$, $(p_1, p_2, \ldots, p_n) = (1, 2, 3, 4, 5, 6, 7)$, $\varphi(a) = a$ e $A = \{0, 1, 2, \ldots, 9\}$. Caso p_i seja par e $(a_i - a_i') = 5$, ou ainda, se $p_i = 5$ e $(a_i - a_i')$ for par, um erro singular não será detectado por esse sistema. Por exemplo: seja o número de identificação $123456 - 7$ e o operador digitasse equivocadamente $173456 - 7$, o erro não seria detectado, uma vez que $1 \cdot 1 + 7 \cdot 2 + 3 \cdot 3 + 4 \cdot 4 + 5 \cdot 5 + 6 \cdot 6 + 7 \cdot 7 \equiv 0 \pmod{10}$.

Exemplo 2.11. Seja $k = 7$, $(p_1, p_2, \ldots, p_n) = (1, 2, 3, 4, 5, 6)$, $\varphi(a) = a$ e $A = \{0, 1, 2, 3, 4, 5, 6\}$, temos que este sistema detecta todos os erros de transposição, pois como k é primo, então para que o erro não fosse detectado teríamos obrigatoriamente que $k \mid (p_i - p_j)$ ou $k \mid (a_i - a_i')$ o que não acontece, pois $1 \leq (p_i - p_j) \leq 5$ e $1 \leq (a_i - a_i') \leq 6$.

Exemplo 2.12. Seja $k = 10$, $(p_1, p_2, \ldots, p_n) = (1, 2, 3, 4, 5, 6, 7)$, $\varphi(a) = a$ e $A = \{0, 1, 2, \ldots, 9\}$. Caso $(p_i - p_j)$ seja par e $(a_i - a_i') = 5$, ou ainda, se $(p_i - p_j) = 5$ e $(a_i - a_i')$ for par, o erro de transposição não será detectado por esse sistema. Por exemplo: seja o número de identificação $135723 - 6$ e o operador digitasse equivocadamente $335721 - 6$, o erro de transposição não seria detectado, uma vez que $3 \cdot 1 + 3 \cdot 2 + 5 \cdot 3 + 7 \cdot 4 + 2 \cdot 5 + 1 \cdot 6 + 6 \cdot 7 \equiv 0 \pmod{10}$.

Destarte, passemos agora as condições para que os pesos p_i assegurem a detecção de todos os erros de um determinado tipo.

Corolário 2.13. *Um sistema de identificação módulo k com vetor de verificação de algarismos $(p_1, p_2, p_3, \ldots, p_n)$ detecta:*

(i) Os erros singulares na posição i se e só se $mdc(p_i, k) = 1$;

(ii) As transposições de algarismos nas posições i e j se e só se $mdc(p_i - p_j, k) = 1$.

Demonstração.

(i) Sejam $a_i, a_i' \in \{0, 1, \ldots, k-1\}$ com $a_i \neq a_i'$, onde a_i representa o algarismo correto que foi substituído por um algarismo errado, a_i', dando assim origem a um erro singular na posição $i(\ldots a_i \ldots \to \ldots a_i' \ldots)$.

Como vimos no item (i) da Proposição 2.8, o sistema detecta todos os erros singulares na i-ésima posição se e só se $p_i(a_i - a_i') \not\equiv 0 \pmod{k}$ para quaisquer $a_i, a_i' \in \{0, 1, \ldots, k-1\}$ com $a_i \neq a_i'$.

Verifiquemos que, de fato, $p_i(a_i - a_i') \not\equiv 0 \pmod{k}$ é equivalente a $mdc(p_i, k) = 1$.

Provemos que se $p_i(a_i - a_i') \not\equiv 0 \pmod{k}$ então $mdc(p_i, k) = 1$.

Suponhamos que $mdc(p_i, k) = d$ com $d > 1$. Então $p_i = dd_1$ e $k = dd_2$ com $d_1, d_2 \in \{1, 2, \ldots, k-1\}$.

Fazendo $a_i = d_2$ e $a_i' = 0$, chegamos a um absurdo, pois

$$p_i(a_i - a_i') = p_i(d_2 - 0) = p_i d_2 = dd_1 d_2 = d_1 dd_2 = d_1 k \equiv 0 \pmod{k}.$$

Portanto $d = 1$, ou seja, $mdc(p_i, k) = 1$.

Provemos que se $mdc(p_i, k) = 1$ então $p_i(a_i - a_i') \not\equiv 0 \pmod{k}$.

Suponhamos que $mdc(p_i, k) = 1$. Então não existe $d \neq 1$ tal que $d \mid p_i$ e $d \mid k$.

Se existissem diferentes $a_i, a_i' \in \{0, 1, \ldots, k-1\}$ tais que $k \mid p_i(a_i - a_i')$ teríamos $k \mid (a_i - a_i')$, porque $k \nmid p_i$ (pois $mdc(p_i, k) = 1$), o que é também um absurdo pois $|a_i - a_i'| \in \{1, 2, \ldots, k-1\}$.

Portanto $p_i(a_i - a_i') \not\equiv 0 \pmod{k}$.

(ii) Pelo item (ii) da Proposição 2.8, sabemos que o sistema detecta todas as transposições dos algarismos a_i e a_j nas posições i e j se e só se para quaisquer $a_i, a_j \in \{0, 1, \ldots, k-1\}$, com $a_i \neq a_j$ se tem $(p_i - p_j)(a_i - a_j) \not\equiv 0 \pmod{k}$. Pela demonstração do item anterior, temos que $(p_i - p_j)(a_i - a_j) \not\equiv 0 \pmod{k}$ é equivalente a $mdc(p_i - p_j, k) = 1$, pois o módulo da diferença entre os algarismos a_i e a_j é um número pertencente a $\{1, 2, \ldots, k-1\}$.

■

Exemplo 2.14. Seja $k = 7$, $(p_1, p_2, \ldots, p_n) = (1, 2, 3, 4, 5, 6)$, $\varphi(a) = a$ e $A = \{0, 1, 2, 3, 4, 5, 6\}$, temos que este sistema detecta todos os erros singulares, pois $mdc(1, 7) = mdc(2, 7) = mdc(3, 7) = mdc(4, 7) = mdc(5, 7) = mdc(6, 7) = 1$. Além disso, como $1 \leq (p_i - p_j) \leq 5$, temos que $mdc(p_i - p_j, 7) = 1$, portanto este sistema também detecta todos os erros de transposição.

Exemplo 2.15. Seja $k = 10$, $(p_1, p_2, \ldots, p_n) = (1, 2, 3, 4, 5, 6, 7)$, $\varphi(a) = a$ e $A = \{0, 1, 2, \ldots, 9\}$. Como $mdc(p_2 = 2, 10) = mdc(p_4 = 4, 10) = mdc(p_6 = 6, 10) = 2$ e $mdc(p_5 = 5, 10) = 5$, temos que este sistema não detecta todos os erros singulares. Além disso, se $(p_i - p_j) = 2$, $(p_i - p_j) = 4$ ou $(p_i - p_j) = 5$, temos que $mdc(p_i - p_j, 10) \neq 1$, ou seja, este sistema não detecta todos os erros de transposição.

Analogamente podemos fazer o mesmo relativamente aos outros tipos de erros, obtendo a Tabela 2.2:

Tabela 2.2 – Tipos de erros e condições.

Tipos de Erros	Forma	Condições
Singulares	$\ldots a_i \ldots \to \ldots a'_i \ldots$	$mdc(p_i, k) = 1$
Transposições	$\ldots a_i \ldots a_j \ldots \to \ldots a_j \ldots a_i \ldots$	$mdc(p_i - p_j, k) = 1$
Gêmeos	$\ldots aa \ldots \to \ldots a'a' \ldots$	$mdc(p_i + p_{i+1}, k) = 1$
Gêmeos intercalados	$\ldots aa_k a \ldots \to \ldots a'a_k a' \ldots$	$mdc(p_i + p_{i+2}, k) = 1$
Gêmeos generalizados	$\ldots a \ldots a \ldots \to \ldots a' \ldots a' \ldots$	$mdc(p_i + p_j, k) = 1$

Fonte: PICADO, 2001.

Assim, de posse da Tabela 2.2, torna-se mais fácil a construção de sistemas de identificação modulares que detectem determinados tipos de erros, o que possibilita uma aplicação mais eficaz destes sistemas.

Além disso, ela mostra porque os sistemas com $k = 11$ são os mais utilizados. Já que para os sistemas que usam $k < 10$ não é possível que todos os erros singulares e todas as transposições sejam detectados caso não se obrigue que todos os algarismos variem entre 0 e $k - 1$, o que torna o sistema pouco útil e extremamente limitado. No caso $k = 10$ a primeira condição e a segunda condição da Tabela 2.2 são incompatíveis, pois, para que $mdc(p_i, 10) = 1$, se e somente se, os pesos p_i são ímpares, porém nesse

caso o $mdc(p_i - p_j, 10) = 2$ o que faz com que o sistema não identifique todos os erros de transposição o que torna-o menos eficiente.

Quando analisamos o caso em que $k > 10$, o problema surge na necessidade de se utilizar mais do que um algarismo de teste ou, alternativamente, de introduzir caracteres não numéricos para os algarismos de teste. Pois, os restos nestes casos são mais numerosos que o sistema decimal, o que pode ocasionar problemas técnicos e aumentar os custos de produção de sistemas automáticos de leitura e escrita. A fim de evitar isso a maioria dos sistemas módulo 11 em utilização, ou não usam os números de identificação cujo algarismo de teste é superior a 9, ou atribuem o algarismo de teste igual a 0 no caso em que deveria ser 10. Mesmo assim, os sistemas módulo 11 são mais eficientes que os sistemas módulo 10 sob mesmas condições (PICADO, 2001).

No próximo capítulo abordaremos a aplicação dos sistemas de identificação modulares em documentos e guias de arrecadação do Departamento Estadual de Trânsito de Mato Grosso (DETRAN/MT).

CAPÍTULO 3

SISTEMAS DE IDENTIFICAÇÃO MODULARES EM DOCUMENTOS E GUIAS DE ARRECADAÇÃO DO DETRAN/MT

Abordaremos inicialmente um pouco da história do Departamento Estadual de Trânsito de Mato Grosso (DETRAN/MT), para isso nos baseamos em Vasconcelos (apud PIMENTEL, 2002a, 2002b, on-line) e DETRAN/MT (2014, on-line). Posteriormente, passaremos a análise dos sistemas de identificação presentes em documentos e guias emitidos por esse departamento.

3.1 Breve história do DETRAN/MT

O primeiro automóvel a circular pelo estado, segundo Vasconcelos (apud PIMENTEL, 2002a, on-line), foi um caminhão Orion, de fabricação italiana, modelo 1903-1908. Transportado por navio, foi descarregado em Várzea Grande em 1912, depois de adquirido pelo comerciante e coronel Arthur Borges. Ele chegou a Mato Grosso com a missão de viabilizar o transporte de mercadorias e a abertura de estradas. A partir daí o número de veículos passou a ser cada vez maior e foi quando, com o aumento da frota, surgiram também o trânsito e suas complicações e já nos anos 20 aconteceu o primeiro acidente de trânsito, no cruzamento entre as ruas Dom Aquino e Dom Bosco.

Devido a essas situações, é criada em 1927, pelo então Governador do Estado Dr. Mário Correa da Costa, a primeira inspetoria de veículos, encarregada de

regulamentá-los. Nasce neste momento, mesmo que não com o nome atual, o Departamento de Trânsito de Mato Grosso.

Essa nomenclatura é apenas utilizada a partir do Primeiro Código de Trânsito do Brasil sancionado pelo Decreto Lei Nº 3.671 em 25 de setembro de 1941, que abordava uma legislação unificada sobre trânsito em todo o país, o qual estabelecia que em cada Estado deveria criar um Departamento de Trânsito, específico para regular e direcionar a matéria. Como no Estado de Mato Grosso existia a Inspetoria de Veículos ela foi adaptada aos termos da nova lei, passando a partir de então a ser Departamento Estadual de Trânsito, acompanhando e adaptando-se à legislação vigente.

Com o passar dos anos, o DETRAN/MT foi adequando-se as mudanças na lei como por exemplo a que estabeleceu através da Lei nº 5.108 de 21/09/66, o Código Nacional de Trânsito e sua regulamentação através do Decreto Nº 62.127 de 16/01/68, o Regulamento do Código Nacional de Trânsito.

Atualmente, a competência do DETRAN/MT, assim como suas atribuições são definidas pelo atual Código de Trânsito Brasileiro, Lei Federal Nº 9.503 de 23 de setembro de 1997, e suas alterações. Os serviços da autarquia são prestados em mais de 120 postos de atendimento em todo o Mato Grosso, por meio das Circunscrições Regionais de Trânsito (CIRETRANS), Agências Municipais de Trânsito e Agências VIP, ou ainda, através do site: www.detran.mt.gov.br.

Dentre outras serviços, cabe ao DETRAN a confecção e entrega da Carteira Nacional de Habilitação, do Certificado de Registro de Veículo e do Certificado de Registro e Licenciamento de Veículo aos respectivos proprietários. Estes documentos são regulamentados pelo Código de Trânsito Brasileiro (CTB), Conselho Nacional de Trânsito (Contran) e Departamento Nacional de Trânsito (Denatran) por meio de resoluções, deliberações e portarias.

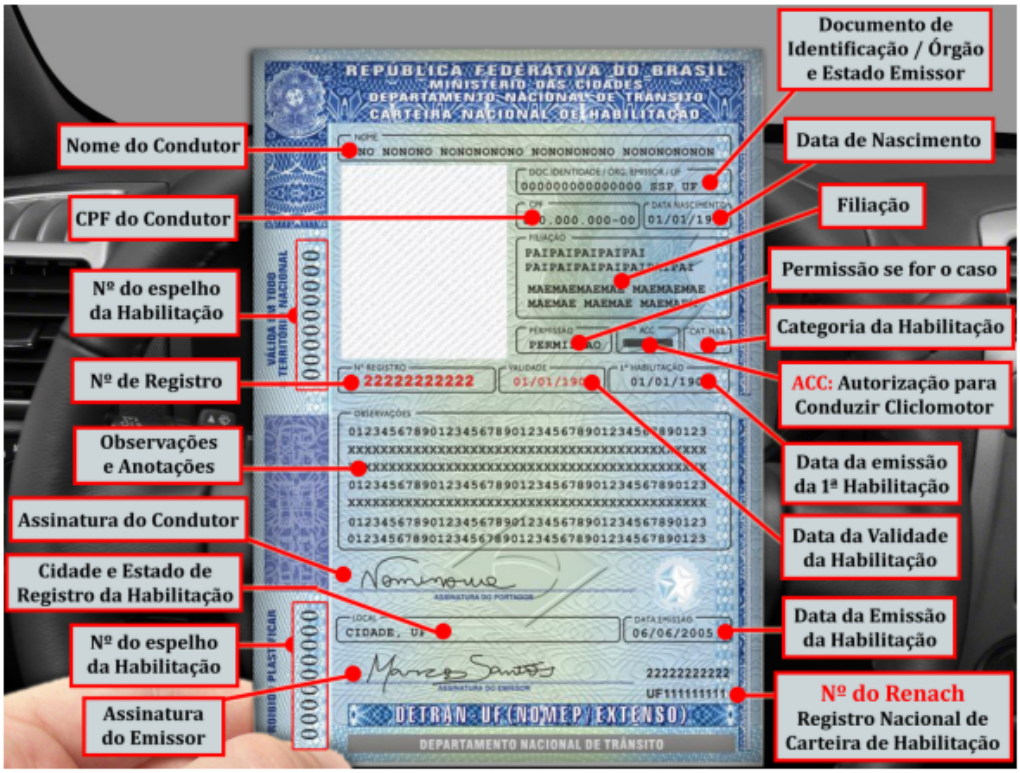
Nas próximas seções serão abordados de forma sucinta a utilização e a definição dos documentos acima listados e as aplicações dos sistemas de identificação modulares neles presentes.

Além disso, devido à escassez de exemplos na bibliografia sobre o tema e também a fim de preservar os dados dos usuários e das instituições, foram utilizados exemplos com números fictícios. Vale ainda ressaltar que até a confecção deste, os números de identificação ou eram de domínio público ou não estavam atribuídos a nenhuma pessoa física ou jurídica, exceto alguns de propriedade do autor.

3.2 Carteira Nacional de Habilitação

Começaremos nossa abordagem primeiramente observando a Figura 3.1:

Figura 3.1 – Carteira Nacional de Habilitação.



Fonte: www.detran.sp.gov.br

Esta figura mostra uma Carteira Nacional de Habilitação (CNH), com seus respectivos campos. Este é um documento é regulamentado pelo CTB e seu modelo segue a resolução 192 de 30 de março de 2006, ele é de porte obrigatório e assegura que a pessoa discriminada no documento está apta a conduzir veículos nas vias públicas.

Abordaremos a seguir a utilização de sistemas de identificação modulares neste documento, para isso utilizaremos os campos que se referem a:

- Cadastro de Pessoa Física (CPF) do Condutor
- Número de Registro
- Número do Registro Nacional de Carteira de Habilitação (Renach)
- Número do Espelho da Habilitação

3.2.1 Cadastro de Pessoa Física (CPF)

Em 30 de dezembro de 1968 é instituído por meio do Decreto-lei nº 401 o Cadastro de Pessoas Físicas. O qual versava que o Registro de Pessoas Físicas criado pelo artigo 11 da Lei número 4.862 de 29 de novembro de 1965 é transformado no Cadastro

de Pessoas Físicas (CPF) e que o mesmo alcançaria as pessoas físicas, contribuintes ou não do imposto de renda e seria de responsabilidade do Ministério da Fazenda.

Segundo a Receita Federal, o contribuinte que apresentou declaração de rendimentos do exercício de 1969, ano-calendário de 1968, recebeu, no início de 1970, juntamente com o Manual de Orientação e formulários, duas vias do Cartão de Identificação do Contribuinte (CIC), emitidos eletronicamente e com prazo de validade. Os cartões emitidos até a década de 1970 tinham prazo e eram renovados quando esse expirava.

A partir disto, a declaração de rendimentos do imposto de renda das pessoas físicas passou a ter um campo para indicação do número de inscrição no Cadastro das Pessoas Físicas. Com o passar do tempo, o CPF ultrapassou os limites do imposto de renda e tornou-se um documento de suma importância no cotidiano do brasileiro.

A Figura 2.1 do Capítulo 2 é exemplo de CPF em formato plástico que deixou de ser impresso nesse formato a partir de 06 de junho de 2011.

O CPF possui 11 caracteres, sendo que 2 deles se referem a dígitos de verificação. Com base em Ghiorzi (2014, on-line), Goulart (2014, on-line) e Sá (2014, on-line) estes dígitos de verificação são gerados por sistemas de identificação modulares e calculados da seguinte forma:

Seja o CPF do Condutor um número $a_1a_2a_3\ldots a_{10}a_{11}$, onde $a_1, a_2, a_3, \ldots, a_{10}$, $a_{11} \in \{0, 1, \ldots, 9\}$ e a_{10} e a_{11} são os dígitos verificadores. Primeiramente calculamos a_{10}, ele deve satisfazer a seguinte soma teste:

$$\begin{aligned} S = &\ (a_1, a_2, a_3, \ldots, a_{10}) \cdot (10, 9, 8, \ldots, 1) \equiv 0 \pmod{11} \\ = &\ 10a_1 + 9a_2 + 8a_3 + 7a_4 + 6a_5 + 5a_6 + 4a_7 + 3a_8 + 2a_9 + a_{10} \equiv 0 \pmod{11} \end{aligned}$$

ou seja,

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

Depois de encontrado a_{10}, passamos agora ao cálculo de a_{11} que deverá satisfazer a soma teste:

$$\begin{aligned} S = &\ (a_1, a_2, a_3, \ldots, a_{10}, a_{11}) \cdot (11, 10, 9, 8, \ldots, 1) \equiv 0 \pmod{11} \\ = &\ 11a_1 + 10a_2 + 9a_3 + 8a_4 + 7a_5 + 6a_6 + 5a_7 + 4a_8 + 3a_9 + 2a_{10} + a_{11} \equiv 0 \pmod{11} \end{aligned}$$

ou seja,

$$a_{11} \equiv -\sum_{i=1}^{10}(12 - i) \cdot a_i \pmod{11}.$$

Observação 3.1. Em todos os sistemas que aqui abordarmos, quando ocorrer que $a_i \equiv 10 \pmod{11}$, teremos que $a_i = 0$, ou seja, ao invés de inserirmos o dígito "10

(dez)", será inserido o dígito 0 (zero).

Exemplo 3.2. Seja o número de um CPF $063210421a_{10}a_{11}$, temos que o algarismo a_{10} será:

$$a_{10} \equiv -\sum_{i=1}^{9}(11-i)\cdot a_i \,(\mathrm{mod}\, 11). \tag{3.1}$$

Expandindo a soma em (3.1) e substituindo os valores de $a_1, a_2, \ldots, a_9$, obtemos:

$$a_{10} \equiv -(10\cdot 0 + 9\cdot 6 + 8\cdot 3 + 7\cdot 2 + 6\cdot 1 + 5\cdot 0 + 4\cdot 4 + 3\cdot 2 + 2\cdot 1) \,(\mathrm{mod}\, 11).$$

Equivalentemente,

$$a_{10} \equiv -(0 + 54 + 24 + 14 + 6 + 0 + 16 + 6 + 2) \,(\mathrm{mod}\, 11),$$

ou seja,

$$a_{10} \equiv -122 \,(\mathrm{mod}\, 11).$$

Como $-122 \equiv -1 \,(\mathrm{mod}\, 11)$ e $-1 \equiv 10 \,(\mathrm{mod}\, 11)$, por transitividade, segue que

$$a_{10} \equiv 10 \,(\mathrm{mod}\, 11).$$

Logo, pela Observação 3.1, temos que $a_{10} = 0$.

Calculando a_{11} obtemos:

$$a_{11} \equiv -\sum_{i=1}^{10}(12-i)\cdot a_i \,(\mathrm{mod}\, 11). \tag{3.2}$$

Expandindo a soma em (3.2) e substituindo os valores de $a_1, a_2, \ldots, a_{10}$, obtemos:

$$a_{11} \equiv -(11\cdot 0 + 10\cdot 6 + 9\cdot 3 + 8\cdot 2 + 7\cdot 1 + 6\cdot 0 + 5\cdot 4 + 4\cdot 2 + 3\cdot 1 + 2\cdot 0) \,(\mathrm{mod}\, 11),$$

isto é,

$$a_{11} \equiv -(0 + 60 + 27 + 16 + 7 + 0 + 20 + 8 + 3 + 0) \,(\mathrm{mod}\, 11).$$

Assim,

$$a_{11} \equiv -141 \,(\mathrm{mod}\, 11).$$

Como $-141 \equiv -9 \,(\mathrm{mod}\, 11)$ e $-9 \equiv 2 \,(\mathrm{mod}\, 11)$, segue que

$$a_{11} \equiv 2 \,(\mathrm{mod}\, 11).$$

Logo, $a_{11} = 2$ e o número do CPF é 063.210.421-02.

3.2.2 Número do Registro Nacional

De acordo com a Resolução 192 de 30 de março de 2006, o Registro Nacional, será gerado pelo sistema informatizado da Base Índice Nacional de Condutores - BINCO, o qual será composto de 9 (nove) caracteres mais 2 (dois) dígitos verificadores de segurança, sendo único para cada condutor e o acompanhará durante toda a sua existência como condutor, não sendo permitida a sua reutilização para outro condutor.

O cálculo dos dígitos verificadores é feito pelo mesmo processo utilizado para o cálculo do CPF a única diferença é que ao término dos cálculos de a_{10} e a_{11}, inserimos os resultados da seguinte forma $a_1a_2a_3a_4a_5a_6a_7a_8a_9 - a_{11}a_{10}$, sendo este o número do Registro Nacional calculados a partir $a_1a_2a_3a_4a_5a_6a_7a_8a_9$.

Utilizando o exemplo acima o Número de Registro que inicia-se em 321654987 teria os dígitos $a_{10} = 0$ e $a_{11} = 2$, porém o Número de Registro desta CNH seria 06321042120.

3.2.3 Número do Registro Nacional de Carteira de Habilitação (RENACH)

Segundo o DENATRAN, o RENACH armazena toda a vida do condutor de veículo, desde o seu "nascimento" como candidato até a sua habilitação, controlando as mudanças de categoria, imposições de penalidades, suspensões do direito de dirigir e ainda mudança de domicílio e transferência de estado. O RENACH controla ainda a emissão da CNH e da PID - Permissão Internacional para Dirigir, que é o documento necessário para que um brasileiro possa dirigir no exterior (nos países signatários da Convenção de Viena). Este número do formulário RENACH identificará a Unidade da Federação onde o condutor foi habilitado ou realizou alterações de dados no seu prontuário pela última vez.

Regulamentado também pela Resolução 192 de 30 de março de 2006, o número de identificação estadual será o número do formulário RENACH composto, obrigatoriamente, por 11 (onze) caracteres, sendo as duas primeiras posições formadas pela sigla da Unidade de Federação expedidora, facultada a utilização da última posição como dígito verificador de segurança. Vale salientar que no Mato Grosso na última posição é utilizado dígito verificador.

O número conforme descrito acima é disposto da seguinte forma:

$$UFa_1a_2a_3a_4a_5a_6a_7a_8a_9$$

Para calcularmos o dígito verificador do Renach recorreremos a soma teste que

se segue:

$$\begin{aligned} S = &\ (a_1, a_2, a_3, \ldots, a_8, a_9) \cdot (9, 8, 7, \ldots, 2, 1) \equiv 0 \pmod{11} \\ = &\ 9a_1 + 8a_2 + 7a_3 + 6a_4 + 5a_5 + 4a_6 + 3a_7 + 2a_8 + a_9 \equiv 0 \pmod{11} \end{aligned}$$

isto é,

$$a_9 \equiv -\sum_{i=1}^{8} (10 - i) \cdot a_i \pmod{11}$$

Exemplo 3.3. Se um condutor é domiciliado no estado de Mato Grosso e ao ingressar o processo de renovação de sua CNH possui seu número Renach com os 8 primeiros algarismos 14725836. Então o dígito verificador dessa sequência será:

$$a_9 \equiv -\sum_{i=1}^{8} (10 - i) \cdot a_i \pmod{11}. \tag{3.3}$$

Expandindo a soma em (3.3) e substituindo os valores de $a_1, a_2, \ldots, a_8$, obtemos:

$$a_9 \equiv -(9 \cdot 1 + 8 \cdot 4 + 7 \cdot 7 + 6 \cdot 2 + 5 \cdot 5 + 4 \cdot 8 + 3 \cdot 3 + 2 \cdot 6) \pmod{11}.$$

Daí, segue que

$$a_9 \equiv -(9 + 32 + 49 + 12 + 25 + 32 + 9 + 12) \pmod{11}.$$

Assim,

$$a_9 \equiv -180 \pmod{11}.$$

Como $-180 \equiv -4 \pmod{11}$ e $-4 \equiv 7 \pmod{11}$, por transitividade, temos que

$$a_9 \equiv 7 \pmod{11}.$$

Portanto $a_9 = 7$ e o Número Renach é MT147258367.

3.2.4 Número do Espelho da CNH

O Número do Espelho da CNH é formado por 9 caracteres, onde 1 deles é o dígito verificador. Este número é regulamentado pela Resolução 192 de 30 de março de 2006 e seu cálculo é apresentado a seguir.

Seja $a_1a_2a_3a_4a_5a_6a_7a_8a_9$ o número do espelho de uma CNH, onde $a_1, a_2, \ldots, a_9 \in \{0, 1, \ldots, 9\}$ e a_9 é o dígito verificador. Temos que escolher a_9 de modo que:

$$a_9 \equiv -a_1a_2a_3a_4a_5a_6a_7a_8 \pmod{11}.$$

Observação 3.4. Neste caso, $a_1a_2a_3a_4a_5a_6a_7a_8$ formam um só número com oito algarismos e não a multiplicação entre os algarismos de a_1 à a_8.

Para melhor compreensão observemos o exemplo que se segue.

Exemplo 3.5. Uma pessoa que possua uma CNH cujo o espelho inicia-se com 12345678 deverá possuir obrigatoriamente o dígito verificador 7, pois

$$a_9 \equiv -12345678 \pmod{11}$$

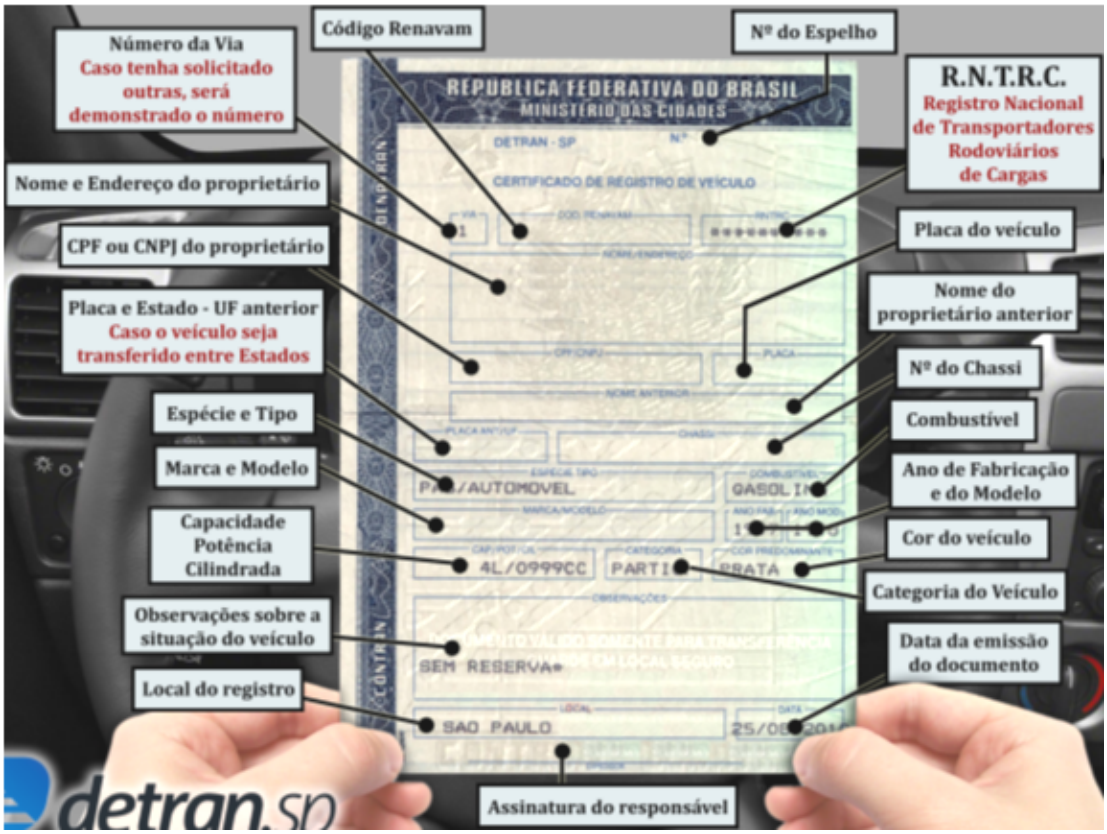
e como $-12345678 \equiv -4 \pmod{11}$ e $-4 \equiv 7 \pmod{11}$, temos que

$$a_9 \equiv 7 \pmod{11}.$$

3.3 Certificado de Registro de Veículo (CRV) e Certificado de Registro e Licenciamento de Veículo (CRLV)

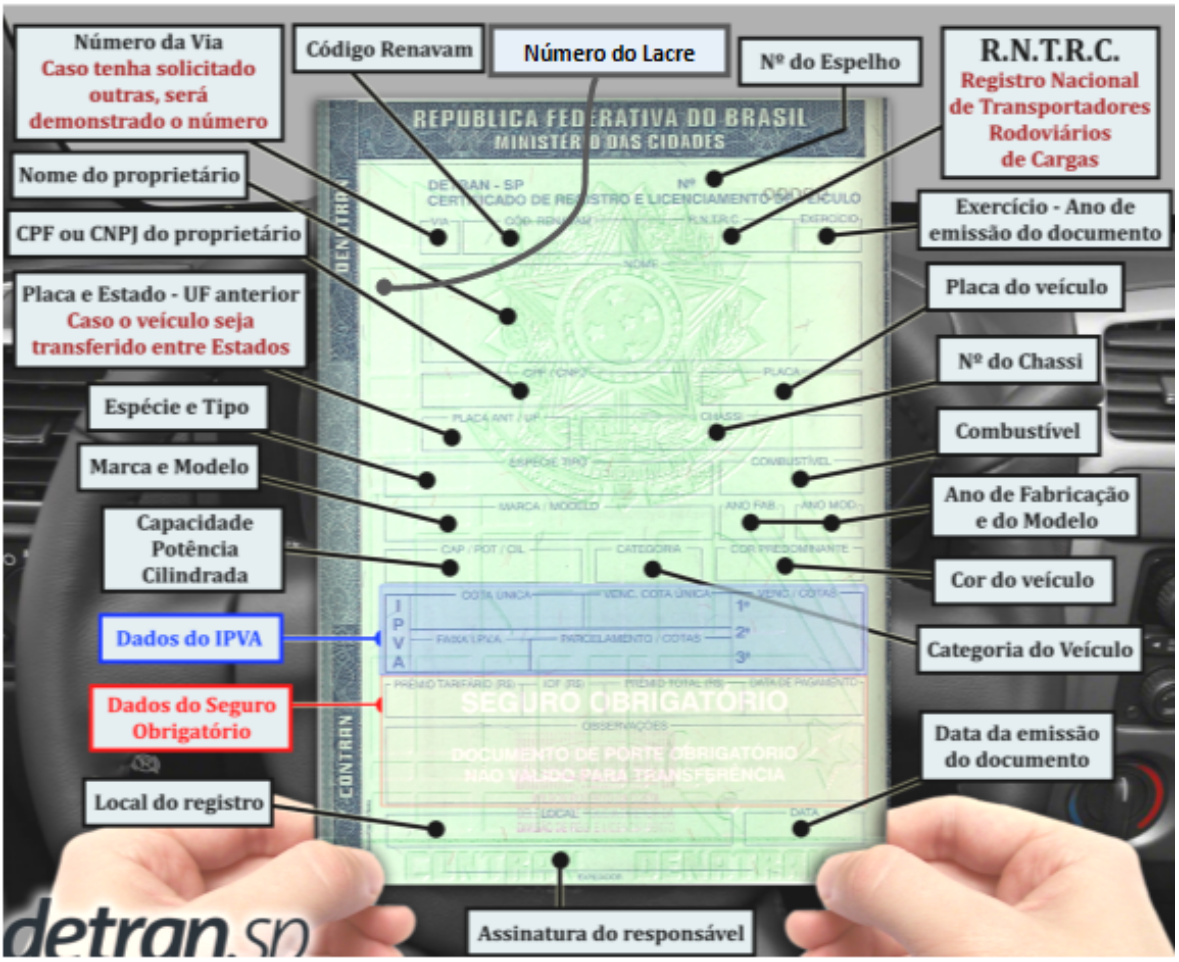
De maneira análoga à utilizada na seção anterior apresentaremos logo em seguida imagens dos documentos que serão nosso objeto de estudo nesta seção.

Figura 3.2 – Certificado de Registro de Veículo.



Fonte: www.detran.sp.gov.br

Figura 3.3 – Certificado de Registro e Licenciamento de Veículo.



Fonte: www.detran.sp.gov.br

A Figura 3.2 refere-se a um Certificado de Registro de Veículo (CRV) regulamentado pelas Resoluções 310/2009, 187/2006 e 16/1998, conforme Glossário DETRAN-RJ este documento é pelo Detran e define a propriedade de um veículo a pessoa física ou jurídica. Por meio dele, o vendedor formaliza a autorização para a transferência de propriedade. O certificado também é necessário nos processos em que há alteração de características do veículo ou de qualquer dado de seu proprietário. Além disso, este documento sempre é emitido em conjunto com o CRLV.

A Figura 3.3 refere-se a um Certificado de Registro e Licenciamento de Veículo (CRLV) que é normatizado pelas Resoluções 187/2006 e 16/1998 o qual segundo glossário DETRAN-MG é emitido anualmente pelo Detran, que atesta a compatibilidade de veículo com as exigências legais determinadas pelo órgão legislador de trânsito. que é emitido anualmente e atesta a compatibilidade de veículo com as exigências legais determinadas pelo órgão legislador de trânsito.

Nestes dois certificados podemos encontrar algumas aplicações dos sistemas de identificação modular, para a visualização de tais sistemas estaremos analisando os

seguintes campos:

- Número do Espelho do CRV/CRLV
- Código do Registro Nacional de Veículos Automotores (RENAVAM)
- Número do Lacre
- Número do CPF/CNPJ

3.3.1 Número do Espelho do CRV/CRLV

De acordo com a Resolução do Contran nº 16/98 alterada pela Deliberação do DENATRAN nº 125 de 24 de abril de 2012 o Número do Espelho do CRV/CRLV tem a função de identificar a cédula e possui 12 dígitos, sendo 11 dígitos numéricos e um dígito numérico verificador e para o cálculo do dígito verificador será utilizado o módulo onze, com peso de 2 a 9, voltando ao 2, a partir da mais baixa ordem, ou seja, da direita para a esquerda. Matematicamente:

$$S = (a_1, a_2, a_3, \ldots, a_{12}) \cdot (4, 3, 2, 9, 8, 7, 6, 5, 4, 3, 2, 1) \equiv 0 \pmod{11}$$

$$S = \left[\sum_{i=1}^{3} (5 - i) \cdot a_i + \sum_{i=4}^{12} (13 - i) \cdot a_i \right] \equiv 0 \pmod{11}$$

Logo,

$$a_{12} \equiv - \left[\sum_{i=1}^{3} (5 - i) \cdot a_i + \sum_{i=4}^{11} (13 - i) \cdot a_i \right] \pmod{11}.$$

É importante observar que o número do espelho CRLV muda anualmente devido ao licenciamento obrigatório, uma vez que é impresso novo documento, porém o número do espelho do CRV permanece o mesmo, já que não há troca de CRV nesse procedimento. Mas, convém ainda ressaltar que tendo a mesma numeração ou não, ambos seguirão o padrão acima estabelecido para determinação do dígito verificador.

3.3.2 Registro Nacional de Veículos Automotores (RENAVAM)

De acordo com o DENATRAN, RENAVAM é o Registro Nacional de Veículos Automotores. Trata-se de um grande banco de dados que registra toda a vida do veículo, desde seu "nascimento" (quando o fabricante ou importador registra seus dados originais), passando pelo emplacamento, troca de propriedade, mudança de estado, mudanças de características até sua "morte" quando este sai de circulação.

Em virtude da Portaria DENATRAN nº 27/2013, desde 1º de abril de 2013, o código RENAVAM passou a ser composto de 11 dígitos numéricos, sendo um deles

dígito numérico verificador. A numeração anterior regulamentada pela Portaria DENATRAN nº 03/1986 possuía 9 dígitos sendo um deles de verificação e terão acrescidos zeros à esquerda e não serão alterados. A forma de cálculo é semelhante ao Número do Espelho do CRV/CRLV a diferença está apenas no número de caracteres. Sendo assim, para o código RENAVAM $a_1a_2a_3\ldots a_{11}$ temos que,

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

ou seja,

$$a_{11} \equiv -\left[\sum_{i=1}^{2}(4-i)\cdot a_i + \sum_{i=3}^{10}(12-i)\cdot a_i\right] \pmod{11}.$$

3.3.3 Lacre Eletrônico

O lacre eletrônico foi criado pela Portaria DENATRAN nº 272 de 21 de dezembro de 2007, devido a necessidade de que os lacres aplicados nas placas de veículos automotores fossem fiscalizados quanto a origem de fabricação, distribuição, aplicação e descarte, o que possibilitaria agregar maior segurança e reduziria, ainda mais, a possibilidade de fraude. O DETRAN do Estado de Mato Grosso por meio da Portaria n° 010/2010/GP/DETRAN/MT foi um dos primeiros a implementar o lacre eletrônico. Este apresenta uma numeração sequencial de 10 dígitos, onde um deles é um dígito verificador, seguidos da sigla MT e tem sua aplicação registrada em sistema de controle informatizado próprio, de forma a fazer constar o número do lacre utilizado no cadastro do Veículo, e no Certificado de Registro e Licenciamento do Veículo (CRLV). Assim o número do Lacre tem este formato:

$$a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}UF$$

Figura 3.4 – Número do Lacre de um veículo.

Fonte: elaborado pelo autor, 2014.

O cálculo do dígito verificador a_{10} é semelhante aos já apresentados, diferenci-

ando apenas quanto a quantidade de caracteres, ou seja,

$$a_{10} \equiv -\left[2a_1 + \sum_{i=2}^{9}(11-i)\cdot a_i\right] \pmod{11}$$

Exemplo 3.6. Na figura de um lacre eletrônico apresentado na Figura 3.4, podemos observar a seguinte numeração 0018210392MT, ou seja, $a_{10} = 2$. Confiramos se esta numeração é valida. De fato, pois

$$a_{10} \equiv -[2\cdot 0 + 9\cdot 0 + 8\cdot 1 + 7\cdot 8 + 6\cdot 2 + 5\cdot 1 + 4\cdot 0 + 3\cdot 3 + 2\cdot 9] \pmod{11},$$

isto é,

$$a_{10} \equiv -[0 + 0 + 8 + 56 + 12 + 5 + 0 + 9 + 18] \pmod{11},$$

assim,

$$a_{10} \equiv -108 \pmod{11}$$

e como $-108 \equiv -9 \pmod{11}$ e $-9 \equiv 2 \pmod{11}$, logo

$$a_{10} \equiv 2 \pmod{11}.$$

Sabemos que o CRV e o CRLV podem ser impressos em nome de pessoa física por meio do CPF ou pessoa jurídica através do CNPJ, porém como já falamos sobre o CPF neste capítulo, abordaremos em seguida o CNPJ.

3.3.4 Cadastro Nacional de Pessoas Jurídicas (CNPJ)

Segundo a Receita Federal, o Cadastro Nacional da Pessoa Jurídica (CNPJ), foi instituído em 1998, em substituição ao antigo Cadastro Geral de Contribuintes (CGC). Surgiu como uma proposta de racionalização de recursos e procedimentos dos diversos cadastros existentes e previa a adesão de todas as administrações tributárias estaduais e municipais, com posterior integração nacional do cadastro tributário. Possui 14 caracteres, sendo 2 deles para verificação.

Com base em Ghiorzi (2014, on-line) e Goulart (2014, on-line), podemos encontrar os dígitos verificadores da seguinte forma:

Seja $a_1a_2a_3\ldots a_{13}a_{14}$ o número de um CNPJ, onde a_{13} e a_{14} são dígitos verificadores. Primeiramente obtemos a_{13} como segue:

$$a_{13} \equiv -\left[\sum_{i=1}^{4}(6-i)\cdot a_i + \sum_{i=5}^{12}(14-i)\cdot a_i\right] \pmod{11}$$

E posteriormente, de posse de a_{13}, temos que a_{14} será:

$$a_{14} \equiv -\left[\sum_{i=1}^{5}(7-i)\cdot a_i + \sum_{i=6}^{13}(15-i)\cdot a_i\right] \ (\text{mod}11)$$

Finalizamos este capítulo apresentando uma análise dos sistemas de identificação presentes nas guias de recolhimento emitidas no DETRAN/MT.

3.4 Guias de Arrecadação Emitidas pelo DETRAN/MT

Estaremos analisando as guias necessárias para a renovação do CRLV, ou seja, as guias do Imposto sobre a Propriedade de Veículos Automotores (IPVA), do Licenciamento Obrigatório e do Seguro de Danos Pessoais Causados por Veículos Automotores de Via Terrestre (Seguro DPVAT), por terem características comum as demais guias emitidas pelo DETRAN/MT. Nestas guias, além dos casos já citados neste capítulo, podemos encontrar sistemas de identificação modulares nas representações numéricas do código de barras.

Essas guias de arrecadação seguem o padrão estabelecido pela Federação Brasileira de Bancos (Febraban), em seu manual número 04 de utilização do código de barras vigente desde 01/04/2005, disponível em http://www.febraban.org.br.

A Figura 3.5 mostra o modelo de código de barras que é utilizado nas guias de arrecadação emitidas pelo DETRAN/MT.

Figura 3.5 – Código de barras.

Fonte: www.febraban.org.br

Analisaremos nos códigos de barras apenas a sua representação numérica que encontra-se localizada logo acima do código de barras. Essa representação numérica é composta por 4 boxes, onde dentro de cada box existem 11 posições, acrescido de 1 dígito verificador, módulo-10 ou módulo-11 de acordo com o código de moeda escolhido. Como os dígitos verificadores são usados para detectar possíveis erros de digitação, logo, não estão representados nas barras que compõe o código.

A Tabela 3.1 mostra como será o conteúdo do código.

Tabela 3.1 – Conteúdo de um código de barras.

Posição	**Tamanho**	**Conteúdo**
01-01	1	Identificação do Produto
02-02	1	Identificação do Segmento
03-03	1	Identificação do valor real ou referência
04-04	1	Dígito verificador geral (módulo 10 ou 11)
05-15	11	Valor
16-19	4	Identificação da Empresa/Órgão
20-44	25	Campo livre de utilização da Empresa/Órgão
16-23	8	CNPJ / MF
24-44	21	Campo livre de utilização da Empresa/Órgão

Fonte: www.febraban.org.br

A Tabela abaixo se refere a função dos campos específicos no código de barra.

Tabela 3.2 – Função dos campos específicos no código de barra.

Campo Específico	**Função**
Identificação do Produto	Constante "8" para identificar arrecadação
Identificação do Segmento	Identificará o segmento e a forma de identificação da Empresa/Órgão: 1. Prefeituras; 2. Saneamento; 3. Energia Elétrica e Gás; 4. Telecomunicações; 5. Órgãos Governamentais; 6. Carnês e Assemelhados ou demais Empresas/Órgãos que serão identificadas através do CNPJ; 7. Multas de trânsito; 9. Uso exclusivo do banco.

(continua)

Tabela 3.2 – Função dos campos específicos no código de barra. (continuação)

Campo Específico	**Função**
Identificador de Valor Efetivo ou Referência	Este campo será: "6" – Valor a ser cobrado efetivamente em reais com código verificador calculado pelo módulo 10 na quarta posição do código de barras e valor com 11 posições sem qualquer alteração; "7" – Quantidade de moeda Zeros – somente na impossibilidade de utilizar o valor Valor a ser reajustado por um índice com dígito verificador calculado pelo módulo 10 na quarta posição do Código de Barras e valor com 11 posições; "8" – Valor a ser cobrado em reais com dígito verificador calculado pelo módulo 11 na quarta posição do Código de Barras e valor com 11 posições sem qualquer alteração; "9" – Quantidade de moeda Zeros – somente na impossibilidade de utilizar o valor; Valor a ser reajustado por um índice com dígito verificador calculado pelo módulo 11 na quarta posição do Código de Barras e valor com 11 posições.
Dígito Verificador	Dígito de auto conferência dos dados nos Códigos de Barras.
Valor Efetivo ou Valor de Referência	Se o campo "03 – Código de Moeda" indicar valor efetivo, este campo deverá conter o valor a ser cobrado. Se o campo "03 – Código de Moeda" indicar valor de referência, neste campo poderá conter uma quantidade de moeda, zeros, ou um valor a ser reajustado por um índice, etc.
Identificação da Empresa/Órgão	O campo identificação da Empresa/Órgão terá uma condição especial para cada segmento: – Será um código de quatro posições atribuído e controlado pela Febraban, ou as primeiras oito posições do cadastro geral de contribuintes do Ministério da Fazenda. – Se for utilizado o CNPJ para identificar a Empresa/Órgão, haverá uma redução no seu campo livre que passará a conter 21 posições. – No caso de uso do Segmento 9, este campo deverá conter o código de compensação do mesmo, com quatro dígitos. É através desta informação que o banco identificará a quem repassar as informações e o crédito. Cada Banco definirá a forma de identificação da empresa a partir da 20ª posição.
Campo Livre	Este campo é de uso exclusivo da Empresa/Órgão e será devolvido inalterado. Se existir data de vencimento no campo livre, ela deverá vir em primeiro lugar e em formato AAAAMMDD.

Fonte: www.febraban.org.br

Logo a seguir apresentamos dois tipos de dígito verificadores que compõe a representação numérica: o dígito verificador geral, que constará na 4ª posição do código de barras e o dígito verificador específico para cada agrupamento de 11 posições (box) que será inserido após cada um desses agrupamentos.

Deste modo, existe a necessidade de primeiramente obtermos o dígito verificador geral para posteriormente encontrarmos os outros dígitos verificadores que compõe apenas a representação numérica do código de barras.

A representação numérica do código de barras será da seguinte forma:

$$a_1a_2a_3a_4\ldots a_{11}d_1a_{12}a_{13}\ldots a_{22}d_2a_{23}a_{24}\ldots a_{33}d_3a_{34}a_{35}\ldots a_{44}d_4$$

onde, $a_1, a_2, a_3, a_5, \ldots, a_{44}$ são caracteres do código de barras, $d_1, \ldots, d_4$ são os dígitos verificadores específicos e a_4 é caractere do código de barras e dígito verificador geral. Além disso, temos que $a_1 = 8$, $a_2 \in \{1, 2, \ldots, 7, 9\}$, $a_3 \in \{6, 7, 8, 9\}$ e $a_4, \ldots, a_{44}, d_1, \ldots, d_4 \in \{0, 1, \ldots, 9\}$.

Para o cálculo dos dígitos verificadores é necessário que se observe a 3ª posição do código, ou seja, a_3 que representa o "Código de Moeda", pois é ele quem determinará se os dígitos verificadores serão obtidos pelo módulo 10 ou pelo módulo 11.

Se $a_3 = 6$ ou $a_3 = 7$ calcular-se-á os dígitos verificadores pelo módulo 10 da seguinte forma:

– Dígito verificador geral:

Seja S a soma de todos os algarismos dos números $2a_1, a_2, 2a_3, a_5, 2a_6, a_7, 2a_8, \ldots, a_{43}, 2a_{44}$. Assim sendo, o dígito verificador geral será:

$$a_4 \equiv -\mathsf{S} \pmod{10}$$

– Dígitos verificadores específicos:

Seja $\mathsf{S_1}$ a soma de todos os algarismos dos números $2a_1, a_2, 2a_3, a_4, \ldots, 2a_{11}$. Temos que

$$d_1 \equiv -\mathsf{S_1} \pmod{10}$$

Seja $\mathsf{S_2}$ a soma de todos os algarismos dos números $2a_{12}, a_{13}, 2a_{14}, \ldots, 2a_{22}$. Temos que

$$d_2 \equiv -\mathsf{S_2} \pmod{10}$$

Seja $\mathsf{S_3}$ a soma de todos os algarismos dos números $2a_{23}, a_{24}, 2a_{25}, \ldots, 2a_{33}$. Temos que

$$d_3 \equiv -\mathsf{S_3} \pmod{10}$$

Seja $\mathsf{S_4}$ a soma de todos os algarismos dos números $2a_{34}, a_{35}, 2a_{36}, \ldots, 2a_{44}$. Temos que

$$d_4 \equiv -\mathsf{S_4} \pmod{10}$$

Se $a_3 = 8$ ou $a_3 = 9$ calcular-se-á os dígitos verificadores pelo módulo 11 da seguinte forma:

– Dígito verificador geral:

$$a_4 \equiv -\left[\sum_{i=1)}^{3}(5-i)a_i + \sum_{i=5}^{12}(14-i)a_i + \sum_{i=13}^{20}(22-i)a_i + \sum_{i=21}^{28}(30-i)a_i + \sum_{i=29}^{36}(38-i)a_i + \sum_{i=37}^{44}(46-i)a_i\right] \pmod{11}$$

ou equivalentemente,

$$a_4 \equiv -\left[\sum_{i=1}^{3}(5-i)a_i + \sum_{i=1}^{5}\big(9a_{8i-3} + 8a_{8i-2} + 7a_{8i-1} + 6a_{8i} + 5a_{8i+1} + 4a_{8i+2} + 3a_{8i+3} + 2a_{8i+4}\big)\right] \pmod{11}$$

– Dígitos verificadores específicos:

$$d_1 \equiv -\left[\sum_{i=1}^{3}(5-i)a_i + \sum_{i=4}^{11}(13-i)a_i\right] \pmod{11}$$

$$d_2 \equiv -\left[\sum_{i=12}^{14}(16-i)a_i + \sum_{i=15}^{22}(24-i)a_i\right] \pmod{11}$$

$$d_3 \equiv -\left[\sum_{i=23}^{25}(27-i)a_i + \sum_{i=26}^{33}(35-i)a_i\right] \pmod{11}$$

$$d_4 \equiv -\left[\sum_{i=34}^{36}(38-i)a_i + \sum_{i=37}^{44}(13-i)a_i\right] \pmod{11}$$

Para que a visualização das aplicações dos conceitos abordados nessa seção nas guias do DETRAN/MT seja facilitada, estaremos introduzindo a seguir subseções que versarão respectivamente sobre as guias de Licenciamento, IPVA e Seguro DPVAT.

3.4.1 Guia de Licenciamento de Veículo

A Figura 3.6 ilustra o modelo uma guia referente a taxa de licenciamento do veículo, o valor desta guia é divido entre o DETRAN/MT para custear as despesas do órgão com a emissão do CRLV e a Secretaria de Segurança Pública que investe nas

mais diversas áreas de sua competência. Sua emissão pode ser efetuada através do site www.detran.mt.gov.br com o código RENAVAM e a placa do veículo ou em um posto de atendimento do DETRAN/MT.

Figura 3.6 – Guia de arrecadação da taxa de licenciamento do veículo.


2ª Via Contribuinte

GOVERNO DO ESTADO DE MATO GROSSO
SECRETARIA DE ESTADO DE FAZENDA
DOCUMENTO DE ARRECADAÇÃO – DAR – MODELO 1 - AUT

03 - RESERVADO
Nº T.P.A.R. | SEQUÊNCIA
04 – RESERVADO AO SELO FISCAL
OBRIGATÓRIO O USO DO SELO FISCAL NA SAÍDA PARA OUTRA U.F.

01 – NOME DO CONTRIBUINTE
05 - CNPJ OU CPF
02 – ENDEREÇO COMPLETO
06 – INSCRIÇÃO ESTADUAL
07 – RESERVADO AO Nº DO SELO FISCAL
08 – Nº PARCELA
09 – NUMERO DA N.A.I. / RENAVAM
10 – NOME DO MUNICÍPIO: BARRA DO GARÇAS
00 – COD. MUNIC.: 65005
00 – PERIODO REF.: 01/03/2014
22 – DATA VENCTO.: 31/03/2014
23 – INF. COMPLEMENTARES: Controle: 6841325927
24 – ESPECIFICAÇÃO DA RECEITA: TAXAS DETRAN
25 - CÓDIGO: 6335
26 - VALOR: 100,00
32 – INFORMAÇÕES PREVISTAS EM INSTRUÇÕES
CORREÇÃO MONETÁRIA
27 – VALOR: 0,00
MULTA
28 – VALOR: 0,00
JUROS
29 – VALOR: 0,00
T.S.E.
30 – VALOR: 0,00
TOTAL A RECOLHER
31 – VALOR: 100,00
33 - VALOR A RECOLHER POR ESTADO
CEM REAIS
40 – AUTENTICAÇÃO MECÂNICA

Modelo aprovada pela Portaria nº 085/2002 – SEFAZ

85830000001-7 00000123201-0 40331633500-2 06841325927-6

Fonte: elaborado pelo autor, 2014.

Ao observarmos a representação numérica do código de barras desta guia podemos notar que:

$a_1 = 8$, pois trata-se de uma guia de arrecadação

$a_2 = 5$, pois refere-se à órgãos governamentais (DETRAN/MT)

$a_3 = 8$, por se tratar de valor a ser cobrado efetivamente em reais e os dígitos verificadores devem ser calculados pelo módulo 11.

$a_4 = 3$ é o digito verificador geral, pois

$$a_4 \equiv -\left[\sum_{i=1}^{3}(5-i)a_i + \sum_{i=5}^{12}(14-i)a_i + \sum_{i=13}^{20}(22-i)a_i + \sum_{i=21}^{28}(30-i)a_i \right.$$

$$\left. + \sum_{i=29}^{36}(38-i)a_i + \sum_{i=37}^{44}(46-i)a_i\right] \pmod{11}.$$

Retirando os somatórios obtemos,

$$[4a_1 + 3a_2 + 2a_3 + 9a_5 + 8a_6 + 7a_7 + 6a_8 + 5a_9 + 4a_{10} + 3a_{11} + 2a_{12} +$$

$$+9a_{13} + 8a_{14} + 7a_{15} + 6a_{16} + 5a_{17} + 4a_{18} + 3a_{19} + 2a_{20}+$$

$$+9a_{21} + 8a_{22} + 7a_{23} + 6a_{24} + 5a_{25} + 4a_{26} + 3a_{27} + 2a_{28}+$$

$$+9a_{29} + 8a_{30} + 7a_{31} + 6a_{32} + 5a_{33} + 4a_{34} + 3a_{35} + 2a_{36}+$$

$$+9a_{37} + 8a_{38} + 7a_{39} + 6a_{40} + 5a_{41} + 4a_{42} + 3a_{43} + 2a_{44}].$$

Logo,

$$a_4 \equiv -(32 + 15 + 16 + 3 + 5 + 8 + 9 + 4 + 8 + 28 + 15 + 12 + 3 + 12 + 27 + 24 + 35+$$

$$+18 + 16 + 36 + 8 + 21 + 12 + 25 + 36 + 6 + 14) \pmod{11}$$

Ou seja,

$$a_4 \equiv -448 \equiv -8 \equiv 3 \pmod{11}$$

$$a_4 \equiv 3 \pmod{11}$$

$a_5, \ldots, a_{15} = 00000010000$ representam o valor da guia, onde $a_{14}a_{15}$ são os centavos. Assim esta guia é de R$ 100,00.

$a_{16}, \ldots, a_{19} = 0123$, número que identifica a quem deve ser depositado (DETRAN/MT)

$a_{20}, \ldots, a_{28} = 20140331$, é a Data de vencimento no formato AAAAMMDD.

$a_{29}, \ldots, a_{32} = 6335$, código que se refere a taxa do DETRAN/MT.

$a_{33}, \ldots, a_{44} = 0006841352927$, são números de controle de uso exclusivo do órgão.

$d_1 = 7$, $d_2 = 0$, $d_3 = 2$ e $d_4 = 6$ são os dígitos verificadores específicos calculados da seguinte forma:

$d_1 \equiv -(32 + 15 + 16 + 27 + 2) \equiv -92 \equiv -4 \equiv 7 \pmod{11}$,

$d_2 \equiv -(7 + 12 + 15 + 8 + 2) \equiv -44 \equiv 0 \pmod{11}$,

$d_3 \equiv -(16 + 6 + 27 + 8 + 42 + 18 + 15 + 20) \equiv -152 \equiv -9 \equiv 2 \pmod{11}$ e

$d_4 \equiv -(18 + 16 + 36 + 8 + 21 + 12 + 25 + 36 + 6 + 14) \equiv -192 \equiv -5 \equiv 6 \pmod{11}$.

Dessa forma, conseguimos verificar cada dígito verificador e ainda obter a partir do número do código de barras vários dados, como por exemplo, a data de vencimento e o valor.

A seguir apresentaremos o conceito e destinação do IPVA e ainda mostraremos o modelo de guia utilizado para seu recolhimento.

3.4.2 Guia do Imposto sobre a Propriedade de Veículos Automotores (IPVA)

O Imposto sobre a Propriedade de Veículos Automotores (IPVA), é um imposto cuja arrecadação é anual e obrigatória a todos que possuem veículos automotores. E seu pagamento é requisito obrigatório para obtenção do CRLV. A receita do IPVA é partilhada entre o Estado (50%) e o Município (50%) de domicílio do proprietário e destina-se ao financiamento de serviços básicos à população como saúde, educação, transporte, segurança, habitação, etc., não sendo portanto obrigatória sua destinação para melhoria das vias. A fim de não tornar a leitura maçante e por se tratar de processos de formação inteiramente análogos aos da guia de licenciamento estaremos apenas apresentando o modelo da guia de IPVA.

Figura 3.7 – Guia de arrecadação do IPVA.


2ª Via Contribuinte

GOVERNO DO ESTADO DE MATO GROSSO
SECRETARIA DE ESTADO DE FAZENDA
DOCUMENTO DE ARRECADAÇÃO – DAR – MODELO 1 - AUT

03 - RESERVADO
Nº T.P.A.R.
SEQUÊNCIA
04 – RESERVADO AO SELO FISCAL
OBRIGATÓRIO O USO DO SELO FISCAL NA SAÍDA PARA OUTRA U.F.

01 – NOME DO CONTRIBUINTE
05 - CNPJ OU CPF
02 – ENDEREÇO COMPLETO
06 – INSCRIÇÃO ESTADUAL
07 – RESERVADO AO Nº DO SELO FISCAL
08 – Nº PARCELA
09 – NUMERO DA N.A.I. / RENAVAM
10 – NOME DO MUNICÍPIO: BARRA DO GARÇAS
00 – COD. MUNIC.: 65005
00 – PERIODO REF.: 2014
22 – DATA VENCTO.: 30/06/2014
23 – INF. COMPLEMENTARES: Controle: 183248712
24 – ESPECIFICAÇÃO DA RECEITA: IPVA / DATA EMISSÃO: 10/06/2014
25 - CODIGO: 6114
26 - VALOR: 85,14
32 – INFORMAÇÕES PREVISTAS EM INSTRUÇÕES
CORREÇÃO MONETÁRIA
27 – VALOR: 0,00
MULTA
28 – VALOR: 0,00
JUROS
29 – VALOR: 0,00
T.S.E.
30 – VALOR: 59,57
TOTAL A RECOLHER
31 – VALOR: 144,71
33 - VALOR A RECOLHER POR ESTADO
CENTO E QUARENTA E QUATRO REAIS E SETENTA E UM CENTAVOS
40 – AUTENTICAÇÃO MECANICA

Modelo aprovada pela Portaria nº 085/2002 – SEFAZ

85850000001-0 44710117201-1 40630018324-5 87120650059-9

Fonte: elaborado pelo autor, 2014.

Esta guia pode ser emitida pela internet no www.sefaz.mt.gov.br com o código renavam ou com o NIV (Número de Identificação Veicular) também conhecido como chassi, ou ainda, em qualquer posto de atendimento do DETRAN/MT.

Finalizando este capítulo, mostraremos agora como é a representação numérica do código de barras de uma guia de Seguro DPVAT e como são aplicados os recursos desse seguro.

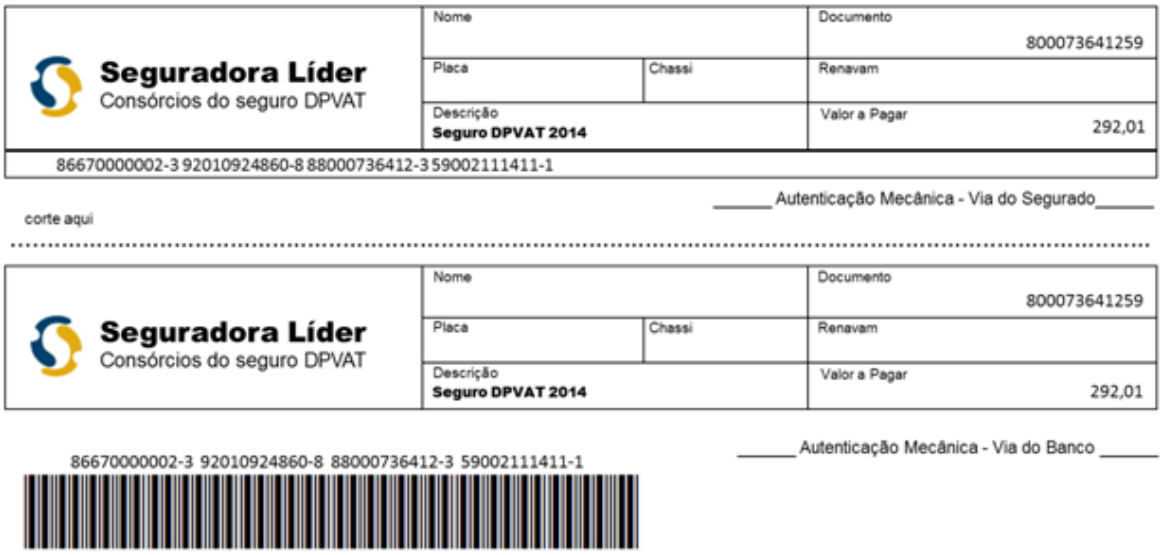
3.4.3 Guia do Seguro DPVAT

Nesta seção será analisada a guia de recolhimento do Seguro de Danos Pessoais Causados por Veículos Automotores de Via Terrestre (Seguro DPVAT), que tem 50% de seu valor destinado ao pagamento de indenizações e a manutenção do Seguro DPVAT em todo o Brasil, e os outros 50% são destinados ao Fundo Nacional de Saúde (45%) que custeia despesas médico-hospitalares de acidentados no trânsito e ao DENATRAN (5%), para desenvolvimento de programas de prevenção de acidentes no trânsito. Esta guia pode ser emitida pelos sites:
http://www.detran.mt.gov.br ou http://www.dpvatsegurodotransito.com.br/index.aspx

Ou se o usuário preferir pode ir até uma CIRETRAN ou Agência de Trânsito de sua cidade.

A Figura 3.8 mostra um modelo de guia de Seguro DPVAT:

Figura 3.8 – Guia de Seguro DPVAT.



Fonte: elaborado pelo autor, 2014.

Quando analisamos a representação numérica do código de barra desta guia apresentada na Figura 3.8 podemos averiguar que:

$a_1 = 8$, pois trata-se de uma guia de arrecadação.

$a_2 = 6$, neste caso, temos uma empresa a Seguradora Líder dos Consórcios do Seguro DPVAT, ou simplesmente, Seguradora Líder DPVAT.

$a_3 = 6$, por se tratar de valor a ser cobrado efetivamente em reais e todos os dígitos verificadores devem ser calculados pelo módulo 10.

$a_4 = 7$ é o digito verificador geral, pelo fato de que como,

$2a_1 = 16$	$a_2 = 6$	$2a_3 = 12$	$a_5 = 0$	$2a_6 = 0$
$a_7 = 0$	$2a_8 = 0$	$a_9 = 0$	$2a_{10} = 0$	$a_{11} = 2$
$a_{12} = 18$	$a_{13} = 2$	$2a_{14} = 0$	$a_{15} = 1$	$2a_{16} = 0$
$a_{17} = 9$	$2a_{18} = 4$	$a_{19} = 4$	$2a_{20} = 16$	$a_{21} = 6$
$2a_{22} = 0$	$a_{23} = 8$	$2a_{24} = 16$	$a_{25} = 0$	$2a_{26} = 0$
$a_{27} = 0$	$2a_{28} = 14$	$a_{29} = 3$	$2a_{30} = 12$	$a_{31} = 4$
$2a_{32} = 2$	$a_{33} = 2$	$2a_{34} = 10$	$a_{35} = 9$	$2a_{36} = 0$
$a_{37} = 0$	$2a_{38} = 4$	$a_{39} = 1$	$2a_{40} = 2$	$a_{41} = 1$
$2a_{42} = 8$	$a_{43} = 1$	$2a_{44} = 2$		

$$S = (1+6+6+1+2+2+1+8+2+1+9+4+4+1+6+6+8+1+6+1+$$

$$+4+3+1+2+4+2+2+1+0+9+4+1+2+1+8+1+2)$$

$S = 123$.

Logo,

$$a_4 \equiv -123 \equiv -3 \equiv 7 \pmod{10}.$$

$a_5, \ldots, a_{15} = 00000029201$ representam o valor da guia, onde $a_{14}a_{15}$ são os centavos. Assim esta guia é de R$ 292,01.

$a_{16}, \ldots, a_{23} = 09248608$ são os primeiros algarismos do CNPJ 09.248.608/0001-04 da Seguradora Líder DPVAT que identificam a quem deve ser depositado.

$a_{24}, \ldots, a_{44} = 800073641259002111411$, são números de controle de uso exclusivo da empresa.

$d_1 = 3$, $d_2 = 8$, $d_3 = 3$ e $d_4 = 1$ são os dígitos verificadores específicos cuja confirmação mostra-se através de:

$d_1 \equiv -(1+6+6+1+2+7+4) \equiv -27 \equiv 3 \pmod{10}$,

$d_2 \equiv -(1+8+2+1+9+4+4+1+6+6) \equiv -42 \equiv 8 \pmod{10}$,

$d_3 \equiv -(1+6+8+7+6+6+8+1+4) \equiv -47 \equiv 3 \pmod{10}$ e

$d_4 \equiv -(1+9+4+1+2+1+8+1+2) \equiv -29 \equiv 1 \pmod{10}$.

Assim sendo, conseguimos verificar pela análise tão somente da representação numérica do código de barras das guias de Seguro DPVAT, não apenas cada dígito verificador, mas devido o padrão estabelecido pela FEBRABAN, temos acesso ao oito primeiros números do CNPJ da empresa arrecadadora, o valor e sabemos que a guia não possui uma data de vencimento.

No próximo capítulo veremos como utilizar em sala de aula os conceitos até aqui abordados e como essas ferramentas matemáticas podem proporcionar um ambiente para a aprendizagem sobre temas relacionados ao trânsito.

CAPÍTULO 4

ABORDANDO O TRÂNSITO EM SALA DE AULA A PARTIR DO ESTUDO DOS DÍGITOS VERIFICADORES

4.1 Os Temas Transversais e o Trânsito

A Seguradora Líder, empresa responsável pelo pagamento das indenizações, divulgou em seu boletim ANO 03, volume 04, dentre outras informações, a seguinte:

Tabela 4.1 – Indenizações Pagas.

Quantidades					
Natureza da Indenização	Jan a Dez 2012	%	Jan a Dez 2013	%	Jan a Dez 2013 x Jan a Dez 2012
Morte	60.752	12%	54.767	9%	-10%
Invalidez Permanente	352.495	69%	444.206	70%	26%
Despesas Médicas (DAMS)	94.668	19%	134.872	21%	42%
Total	507.915	100%	633.845	100%	25%

Período: Jan a Dez/2012 e Jan a Dez/2013

Fonte: Seguradora Líder DPVAT.

Esta tabela mostra as indenizações pagas nos anos de 2012 e 2013, e apresenta ainda uma comparação entre eles. Podemos notar que o número de mortes reduziu cerca de 10% para ainda alarmantes 54767 mortos que ainda é superior ao número de 50108 mortos em homicídios (ONU, 2014, on-line). Enquanto o número de vítimas por invalidez cresceu 26% e o número de solicitações de indenizações por gastos com

despesas médicas aumentou impressionantes 42% chegando a 134872 atendimentos.

Este boletim ainda mostra que a faixa etária entre 18 e 34 anos representam 50,9% do total e que os homens representam cerca de 78,7% das vítimas nesta faixa etária.

Entendendo a urgência do tema e acreditando que por meio da educação será possível reduzir o número de mortos e feridos em acidentes de trânsito e construir uma cultura de paz no espaço público, faz-se necessário ações comprometidas com a educação para o trânsito, pois por dela podemos formar cidadãos com valores ligados à ética e à cidadania. (BRASIL, 2009, on-line).

Neste aspecto, o Código de Trânsito Brasileiro versa em seu art. 1 §2º que o trânsito, em condições seguras, é um direito de todos e dever dos órgãos e entidades componentes do Sistema Nacional de Trânsito (SNT). Além disso, o Capítulo VI do CTB, compreendido do art.74 ao art.79, determina que a educação para o trânsito deverá ser promovida em todos os níveis educacionais, por meio de planejamento e ações coordenadas entre órgãos e entidades que compõe o SNT.

Entretanto, a Lei de Diretrizes e Bases da Educação Nacional (BRASIL, 1996) não contempla o estudo do trânsito em sua base nacional comum. Da mesma forma, os Referenciais Curriculares Nacionais da Educação Infantil (RCNEI) e os Parâmetros Curriculares Nacionais do Ensino Fundamental e Médio (PCN) não indicam o trânsito sequer como tema transversal, apenas como tema local.

Quando observamos os Parâmetros Curriculares Nacionais (BRASIL, 1997) encontramos a seguinte definição de transversalidade:

> Transversalidade diz respeito à possibilidade de se estabelecer na prática educativa, uma relação entre aprender na realidade e da realidade de conhecimentos teoricamente sistematizados (aprender sobre a realidade) e as questões da vida real (aprender na realidade e da realidade).

Dessa forma, os temas transversais têm por objetivo trazer à tona, em sala de aula, questões sociais que possibilitem a construção da democracia e da cidadania.

Entretanto, quando comparamos a definição de transversalidade e os pré-requisitos observados para que um tema possa ser considerado um tema transversal, verifica-se facilmente que o trânsito atende a todos os requisitos e não somente pode, como deve ser inserido de forma transversal em todas as disciplinas. Pois, trata-se de um tema inerente à realidade de todas as pessoas, em todos os tempos, em todos os lugares, além de ser um tema de urgência social, abrangência nacional, que possibilita sua abordagem nas diversas etapas do processo de aprendizagem e ainda fornece mecanismos para a compreensão da realidade e participação social.

Convém ressaltar que qualquer ação educativa direcionada as instituições de ensino (escolas, universidades, etc.) não deve ter como objetivo primordial formar futuros motoristas, uma vez que, o trânsito é formado por diversos componentes, entre eles o motorista é apenas uma peça desse imenso quebra-cabeças. Dessa forma, estas ações devem levar os alunos a analisar, refletir e debater sobre temas comuns a todos como:

- O respeito às leis de trânsito e ao espaço público;
- A convivência entre pessoas pelas ruas da cidade, baseada na cooperação;
- Tolerância, igualdade de direitos, responsabilidade, solidariedade e tantos outros valores imprescindíveis para um trânsito mais humano.

4.2 A Matemática e o Trânsito

Segundo os PCN (BRASIL, 1997) a matemática é indispensável à vida em sociedade, haja vista que não há como separar a compreensão e a tomada de decisões diante de questões políticas e sociais da capacidade de analisar informações expressas em dados estatísticos ou índices. De outra forma, podemos dizer que para exercer a cidadania, todo cidadão deve ser capaz de saber calcular, medir, raciocinar, argumentar, tratar informações estatisticamente, etc.

Vista assim, a matemática torna-se um instrumento indissociável da vida cotidiana de todas as pessoas: comprar, pagar, receber, ou seja, é de suma importância compreender as diferentes abordagens matemáticas como gráficos, tabelas, esquemas e etc.

Quando pensamos em inserir o trânsito na matemática encontramos algumas orientações, como as que o DENATRAN propõe por meio da portaria 147/2009:

> O trânsito pode ser inserido na Matemática a partir de dados numéricos, representados em tabelas ou gráficos, relacionados à frota veicular, ao número de acidentes, ao número de vítimas fatais e não-fatais, à densidade demográfica, à extensão territorial, entre outros indicadores.
>
> Estudar e debater sobre o número de acidentes; estabelecer relações entre o aumento populacional e o aumento da frota veicular; pesquisar as causas das mortes em acidentes de trânsito; identificar a faixa etária das vítimas do trânsito; identificar os veículos que mais se envolvem em acidentes, entre outras atividades, produzirá aprendizagens significativas sobre o tema. A elaboração e o levantamento de dados também podem sugerir a construção de gráficos, de tabelas, de esquemas, incentivando a produção de linguagens matemáticas.

> A resolução de problemas também pode partir de situações ocorridas no trânsito. Assim, os alunos poderão calcular valores atribuídos a multas, pontuações referentes às infrações cometidas, etc.

Ou ainda, segundo Minas Gerais (2003) que sugere que essa transversalidade do trânsito na matemática possa ser efetuada por meio de: resoluções de problemas, jogos, elaboração e análise de esquemas, tabelas e gráficos com dados estatísticos ou ainda por meio da geometria. Utilizando os mais diversos recursos como: livros, jornais, revistas, sites, fotos, filmes e etc....

Porém, todas essas possibilidades de integrar matemática e o trânsito estão de alguma forma ligadas a utilização de dados estatísticos ou a geometria, o que sem dúvidas é deveras proveitoso. Entretanto, apresentaremos a seguir uma proposta alternativa, que tem por finalidade proporcionar a interação entre matemática e trânsito de uma forma pouco convencional, valendo-se dos conceitos matemáticos da aritmética modular presentes nos sistemas de identificação modulares com dígitos verificadores usados em documentos e guias emitidos pelo DETRAN/MT.

Dessa forma, esperamos que o aluno possa vivenciar a matemática de maneira concreta, a fim de que possa participar do processo de ensino-aprendizagem.

Apresentaremos a seguir uma proposta alternativa, que tem por finalidade proporcionar a interação entre matemática e trânsito, valendo-se dos conceitos matemáticos presentes nos sistemas de identificação modulares com dígitos verificadores usados em documentos e guias emitidos pelo DETRAN/MT. Dessa forma, esperamos que o aluno possa vivenciar a matemática de maneira concreta, a fim de que possa participar do processo de ensino-aprendizagem.

4.3 Atividade Proposta

O modelo a seguir foi baseado em Silva (2013, on-line).

Atividade: Matemática e trânsito ligados pelos dígitos.

Ano de escolaridade: 6º ao 9º do Ensino Fundamental e do 1º ao 3º ano do Ensino Médio.

Unidade de ensino: Divisibilidade/ Divisão Euclidiana/ Produto Escalar/ Congruência.

Recursos: Xerox da CNH, CRLV e Guias de Licenciamento, Seguro DPVAT e IPVA.

Estratégias: Utilizar documentos e guias de arrecadação do DETRAN/MT com a ausência dos dígitos verificadores em alguns campos.

Objetivos específicos:

- Determinar os dígitos verificadores dos códigos que são formados por sistemas de identificação modulares;
- Verificar se a representação numérica de um código de barras de uma guia está correta ou não;
- Reconhecer a importância da prevenção e do autocuidado no trânsito para a preservação da vida;
- Analisar fatos relacionados ao trânsito, considerando preceitos da legislação vigente e segundo seu próprio juízo de valor;
- Manifestar opiniões, ideias, sentimentos e emoções a partir de experiências pessoais no trânsito;

Primeiramente, o aluno é levado a resolver situações problema que envolvem os conceitos de divisibilidade e divisão euclidiana:

Exemplo 4.1. Hallowen, ou dia das bruxas, é uma tradição dos países de língua inglesa onde no dia 31 de outubro, as crianças andam de casa em casa em sua vizinhança pedindo guloseimas, com a frase: "Gostosuras ou travessuras?". Neste ano, a fim de evitar que sua casa seja alvo das travessuras das crianças, Beth adquiriu 200 doces para a festividade tendo a intenção de distribuir 4 deles a cada criança que bater a sua porta. Sabendo que existem 50 crianças na vizinhança de Beth, podemos dizer que a quantidade de doces que Beth comprou será suficiente?

A resolução desse problema está alicerçada no conceito de divisibilidade, ou seja, queremos saber se existe um número inteiro q, tal que $4 \cdot q = 200$. De fato, existe tal inteiro, basta que $q = 50$ para $4 \cdot 50 = 200$, isto é, Beth poderá agradar a 50 crianças. Assim sendo, podemos dizer que Beth comprou balinhas em quantidade suficiente.

O exemplo a seguir foi adaptado de Esquinca (2013, on-line).

Exemplo 4.2. Durante o curso de Licenciatura em Matemática, quatro amigos, Jhonattan, Max, Valdiego e Vinicíus, decidem criar um grupo de estudo o qual foi denominado G4. Certo dia ao se reunirem decidiram comprar uma coleção de livros de matemática. Observando que o total da compra era de R$ 375,00 decidiram que o pagamento seria feito através de um depósito em dinheiro no caixa eletrônico e que todos deviam pagar um mesmo valor. Sabendo que não é permitido colocar moedas no envelope, qual será o valor a ser depositado por cada um, de modo que essa quantia seja a menor quantia necessária para o pagamento dos livros? Caso haja troco quanto será?

Para resolvermos esse problema basta que efetuemos a divisão euclidiana do valor do débito que é de R$ 375,00, por 4 e obteremos:

$$-375 = -94 \cdot 4 + 1.$$

Dessa forma, a menor quantia necessária para o pagamento dos livros que cada um irá depositar é de R$ 94,00 e haverá R$ 1,00 de troco.

Depois é apresentado ao aluno o conceito e a notação de congruência mostrando que congruência está baseado no resto da divisão euclidiana, pois, pela Definição 1.29, se os restos de dois números inteiros a e b de sua divisão euclidiana por m são iguais, então a e b são congruentes módulo m, onde m é um número inteiro maior que 1, e denotaremos $a \equiv b \,(\mathrm{mod}\, m)$. Caso contrário, $a \not\equiv b \,(\mathrm{mod}\, m)$, ou seja, a não é congruente a b módulo m.

Exemplo 4.3. Sabemos que:
$18 = 1 \cdot 12 + 6$ e $6 = 0 \cdot 12 + 6$, ou seja, tanto o 18, quanto o 6, deixam resto 6 na divisão por 12. Assim temos que $18 \equiv 6 \pmod{12}$. Uma aplicação deste fato pode ser visualizado em relógios digitais que marcam as horas em formato de 24 horas, isto é, 18:00 é equivalente a 6 horas da tarde e 06:00 é equivalente a 6 horas da manhã.

Exemplo 4.4. Observemos que:
$4 = 0 \cdot 7 + 4,\ 11 = 1 \cdot 7 + 4,\ 18 = 2 \cdot 7 + 4,\ 25 = 3 \cdot 7 + 4$, disto temos que $4, 11, 18$ e 25 possuem os mesmos restos na divisão por 7. Sendo assim, temos que

$$11 \equiv 4 \,(\mathrm{mod}\, 7),\ 18 \equiv 4 \,(\mathrm{mod}\, 7),\ 25 \equiv 4 \,(\mathrm{mod}\, 7).$$

Esse fato nos fornece uma interessante aplicação, pois se observarmos um calendário, supondo que dia 4 do mês foi por exemplo terça-feira, então por congruência temos que os dias 11, 18 e 25 também serão terça-feira.

No entanto, o conceito de congruência também deve ser apresentado ao aluno mostrando a relação entre congruência e divisibilidade, pois pela Proposição 1.30 temos que dados dos inteiros a e b, se $b - a$ é divisível por m, então a e b são congruentes módulo m, onde m é um número inteiro maior que 1.

Exemplo 4.5. Sergio ao chegar em casa depois de uma aula de matemática sobre congruência decidiu verificar se a sua quantidade de bolinhas azuis e amarelas que possuía eram congruentes módulo 6, como ele possui 27 bolinhas azuis e 39 bolinhas amarelas, fez o seguinte cálculo $(39 - 27) = 12$ e como 12 é divisível por 6, soube que a quantidade de bolinhas era congruente, isto é, $39 \equiv 27 \pmod{6}$. Porém, por achar o procedimento muito simples, decidiu tirar a prova fazendo a divisão de cada quantidade

por 6 e obteve que $39 = 6 \cdot 6 + 3$ e $27 = 4 \cdot 6 + 3$, ou seja, as duas quantidades de bolinhas possuíam o mesmo resto. Logo, são congruentes módulo 6.

Exemplo 4.6. Se hoje é 1 de maio quinta-feira, posso afirmar com certeza que dia 22 de maio será quinta-feira? Por que?
Neste caso como $22 - 1 = 21$ e 21 é divisível por 7 que é a quantidade de dias da semana então podemos afirmar que com certeza que dia 22 de maio será quinta-feira.

É importante apresentar ao aluno algumas propriedades de congruências, como as listadas na Proposição 1.32, pois elas são imprescindíveis para a compressão dos diversos fenômenos que envolvem congruências. O próximo exemplo é um modelo de problema que pode ser aplicado para mostrar que o uso de congruência pode facilitar problemas que pareciam insolúveis.

Exemplo 4.7. Temos visto que a cada dia há uma necessidade cada vez maior por espaço para o armazenamento de dados, supondo que exista a necessidade de se guardar um arquivo da ordem de $(3^{100} + 3^{40})$ bytes em 10 servidores espalhados pelo mundo, é possível saber se essa divisão será exata nos inteiros?

Ao ler o problema entendemos que trata-se de algo relativamente simples, pois a solução está baseada em dividir $(3^{100} + 3^{41})$ por 10. Entretanto, essa divisão é extremamente trabalhosa e demandaria um tempo enorme para concluí-la. Mas por meio de congruência podemos resolver essa questão de forma rápida e fácil.

Primeiramente, observemos que:

$$\begin{aligned}
3 &\equiv 3 \pmod{10} \\
3^2 = 9 &\equiv 9 \pmod{10} \\
3^3 = 27 &\equiv 7 \pmod{10} \\
3^4 = 81 &\equiv 1 \pmod{10} \\
3^5 = 243 &\equiv 3 \pmod{10} \\
3^6 = 729 &\equiv 9 \pmod{10} \\
3^7 = 2187 &\equiv 7 \pmod{10} \\
3^8 = 6561 &\equiv 1 \pmod{10} \\
&\vdots
\end{aligned}$$

Desse modo, observamos que existe um padrão onde os números que são escritos como $3^{4k} \equiv 1 \pmod{10}$, $3^{(4k+1)} \equiv 3 \pmod{10}$, $3^{(4k+2)} \equiv 9 \pmod{10}$ e $3^{(4k+3)} \equiv 7 \pmod{10}$, ou seja, basta que dividamos o expoente da potência de 3 por 4 e vejamos o resto, para saber a que número é congruente a potência de 3. Temos que: $100 = 25 \cdot 4 + 0$, ou seja, resto 0. Assim, $3^{100} \equiv 1 \pmod{10}$, por outro lado, $41 = 10 \cdot 4 + 1$, disto temos

que o resto é 1 e assim $3^{41} \equiv 3 \pmod{10}$. Logo,

$$(3^{100} + 3^{41}) \equiv 1 + 3 \equiv 4 \,(\mathrm{mod}\, 10).$$

Dessa forma observamos que a divisão não será exata pois restará 4 bytes.

Em seguida, ensinamos ao aluno já utilizando a notação de congruência a calcular o dígito verificador de números de identificação com poucos caracteres e posteriormente apresentam-se as guias e documentos do DETRAN/MT e logo em seguida os sistemas de identificação modulares neles presentes.

Exemplo 4.8. Na Escola Carl Friedrich Gauss, os alunos ao serem matriculados recebiam uma numeração para fins de identificação. Essa numeração era composta por quatro números $a_1a_2a_3a_4$ onde:

- a_1 representa a fileira onde o aluno estará sentado, de modo que as fileiras são numeradas da esquerda para a direita. Assim, que o aluno que sentar-se na 2ª fileira terá obrigatoriamente que possuir seu número de identificação iniciado em 2.

- a_2 representa a numeração da cadeira a que se encontra o aluno na fileira, onde as cadeiras de cada fileira são numeradas da frente para o fundo. Dessa forma, o aluno que sentar-se por exemplo na 4ª cadeira da fileira, terá obrigatoriamente o número $a_14a_3a_4$.

- 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.

- a_4 é um dígito verificador. Esse dígito é o menor número positivo que somado à $4a_1 + 3a_2 + 2a_3$ seja divisível por 7. Ou seja:

$$4a_1 + 3a_2 + 2a_3 + a_4 \equiv 0 \ (mod\ 7)$$

Deste modo, temos que o aluno que está cursando o 1º ano do ensino médio e senta-se na 2ª cadeira, da 1ª fileira qual será seu número de registro? Um menino que chegue ao portão desta escola o número 232–8, poderá entrar? Por quê? E um menino com o número 241–5 entrará?

Exemplo 4.9. O Código Renavam é um exemplo de sistema de identificação que está presente no CRV/CRLV, o qual é composto de 11 dígitos numéricos $a_1a_2a_3 \ldots a_{11}$, onde a_{11} é o dígito verificador calculado pela seguinte expressão:

$$S = (a_1, a_2, a_3, \ldots, a_{11}) \cdot (3, 2, 9, 8, 7, 6, 5, 4, 3, 2, 1) \equiv 0 \ (\mathrm{mod}\ 11)$$

ou seja,

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

Assim sendo, se um Código Renavam é formado pelos números 0364801252, temos que a_{11} será? Podemos resolver esse exemplo de várias formas, deixaremos a cargo do professor escolher a que melhor se adaptar à realidade de seus alunos.

Solução 1

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

Substituindo os valores de $a_1, a_2, a_3, \ldots, a_{10}$ obtemos:

$$3 \cdot 0 + 2 \cdot 3 + 9 \cdot 6 + 8 \cdot 4 + 7 \cdot 8 + 6 \cdot 0 + 5 \cdot 1 + 4 \cdot 2 + 3 \cdot 5 + 2 \cdot 2 + a_{11} \equiv 0 \pmod{11},$$

ou seja, $180 + a_{11} \equiv 0 \pmod{11}$, isto é, $a_{11} \equiv -180 \equiv -4 \equiv 7 \pmod{11}$. Logo, $a_{11} = 7$.

Solução 2
Para calcularmos o valor do dígito verificador:

1º) Obtemos a soma dos valores dos outros dígitos com seus respectivos pesos:

$$3 \cdot 0 + 2 \cdot 3 + 9 \cdot 6 + 8 \cdot 4 + 7 \cdot 8 + 6 \cdot 0 + 5 \cdot 1 + 4 \cdot 2 + 3 \cdot 5 + 2 \cdot 2 = 180$$

2º) Verificamos qual seria o menor número inteiro positivo que adicionado a soma torná-la-ia divisível por 11. Este número será o dígito verificador.

Neste caso, temos que o dígito verificador será 7, pois $180 + 7 = 187$ é divisível por 11.

Solução 3
Para encontrar o dígito verificador devemos:

1º) Dividir o valor positivo da soma dos outros dígitos com seus respectivos pesos por 11 e observar o valor do resto:

$$3 \cdot 0 + 2 \cdot 3 + 9 \cdot 6 + 8 \cdot 4 + 7 \cdot 8 + 6 \cdot 0 + 5 \cdot 1 + 4 \cdot 2 + 3 \cdot 5 + 2 \cdot 2 = 180$$

deixa resto 4 quando divido por 11.

2º) O dígito verificador será 11 menos esse resto observado, ou de forma análoga, quanto falta ao resto observado para chegar a 11.

Temos que $11 - 4 = 7$. Dessa forma, 7 será o dígito verificador.

Solução 4

1º) Dados os pesos e os dígitos, inserimos os dados na seguinte expressão:

$$(11 - p_1)a_1 + (11 - p_2)a_2 + \cdots + (11 - p_{n-1})a_{n-1}.$$

Neste exemplo, temos:

$$(11-3)0+(11-2)3+(11-2)6+(11-3)4+(11-4)8+(11-5)0+(11-6)1+(11-7)2+$$

$$+(11-8)5+(11-9)2.$$

Logo

$$8 \cdot 0 + 9 \cdot 3 + 2 \cdot 6 + 3 \cdot 4 + 4 \cdot 8 + 5 \cdot 0 + 6 \cdot 1 + 7 \cdot 2 + 8 \cdot 5 + 9 \cdot 2 = 161.$$

2º) O dígito verificador será o resto da divisão do resultado da expressão acima com 11. Temos que $161 = 14 \cdot 11 + 7$. Assim temos que 7 é o dígito verificador.

Temos que $161 = 14 \cdot 11 + 7$. Assim temos que 7 é o dígito verificador.

Observação 4.10. As soluções apresentadas são válidas não somente para o Exemplo 4.9, mas também para todos os sistemas de identificação modulares apresentados nesta dissertação, desde que devidamente adaptados.

Além disso, a fim de fornecer um agente facilitador para o estudo dos dígitos verificadores abordados nesta dissertação, foi desenvolvido o site *www.sistemadigito.site90.com* em parceria com Hewerton Sousa Ribeiro[1]. Neste site o professor poderá abordar o significado e utilidade dos códigos existentes nos documentos do DETRAN e também mostrar como são efetuados os cálculos dos seus respectivos dígitos verificadores.

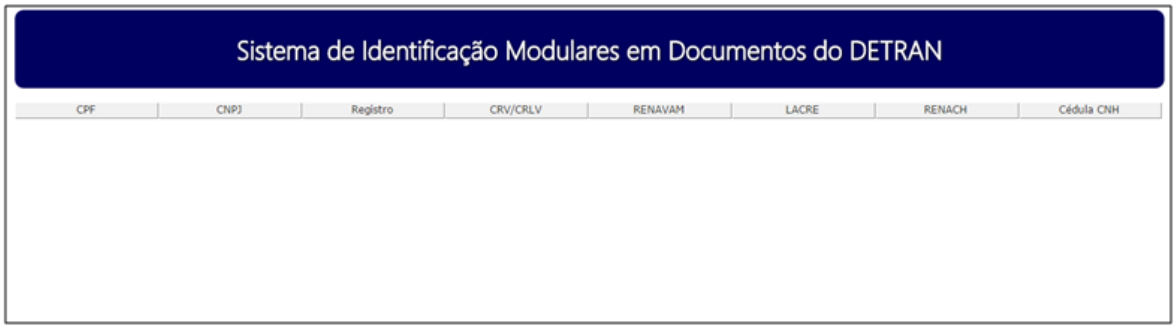
A Figura 4.1 mostra o layout do site, que fornecerá ao professor e, consequentemente, ao aluno, a possibilidade de escolher entre:

- CPF
- CNPJ
- Registro

[1]Bacharel em Ciência da Computação pela Universidade Federal de Mato Grosso – UFMT

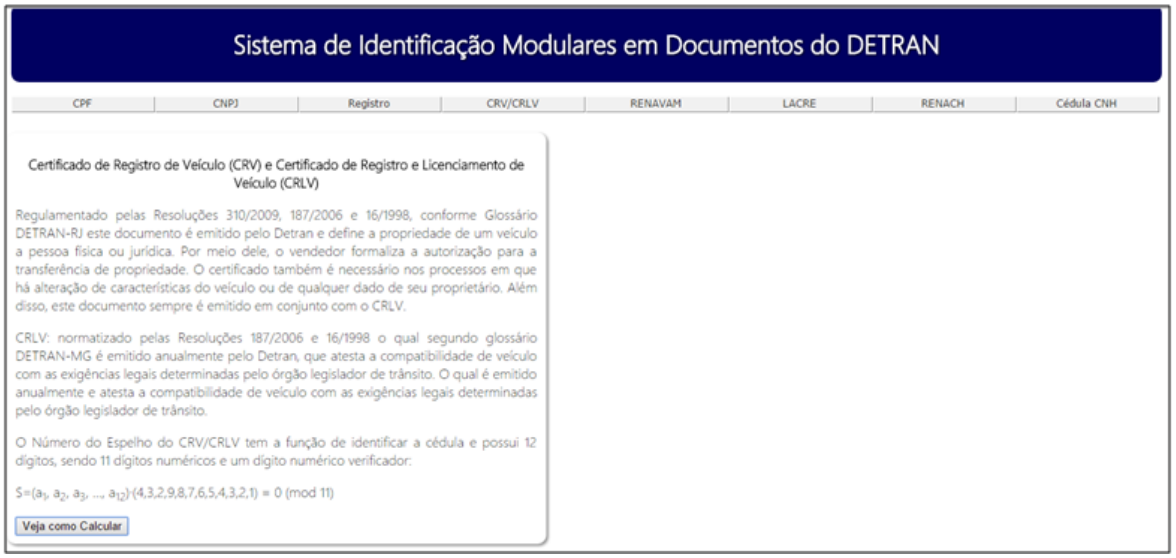
- CRV/CRLV
- RENAVAM
- LACRE
- RENACH
- Cédula CNH

Figura 4.1 – Layout do Site.



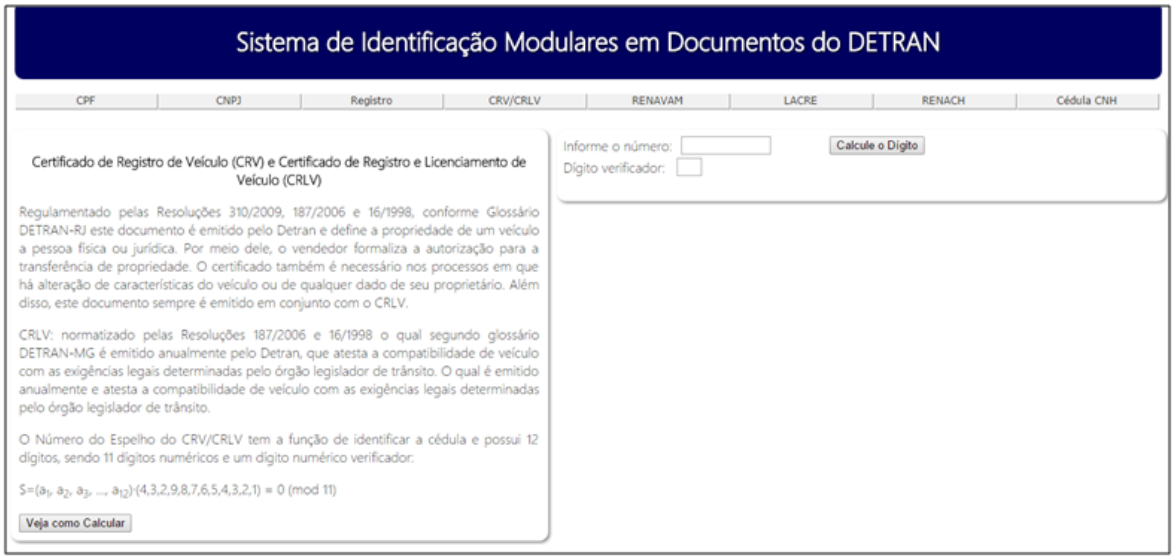
Ao clicar sobre uma dessas opções abrirá logo abaixo uma janela que fornecerá informações sobre o código/documento escolhido e sua forma de cálculo, conforme Figura 4.2. Além disso, o aluno encontrará um ícone chamado "Veja como Calcular".

Figura 4.2 – Informações sobre o código/documento escolhido.



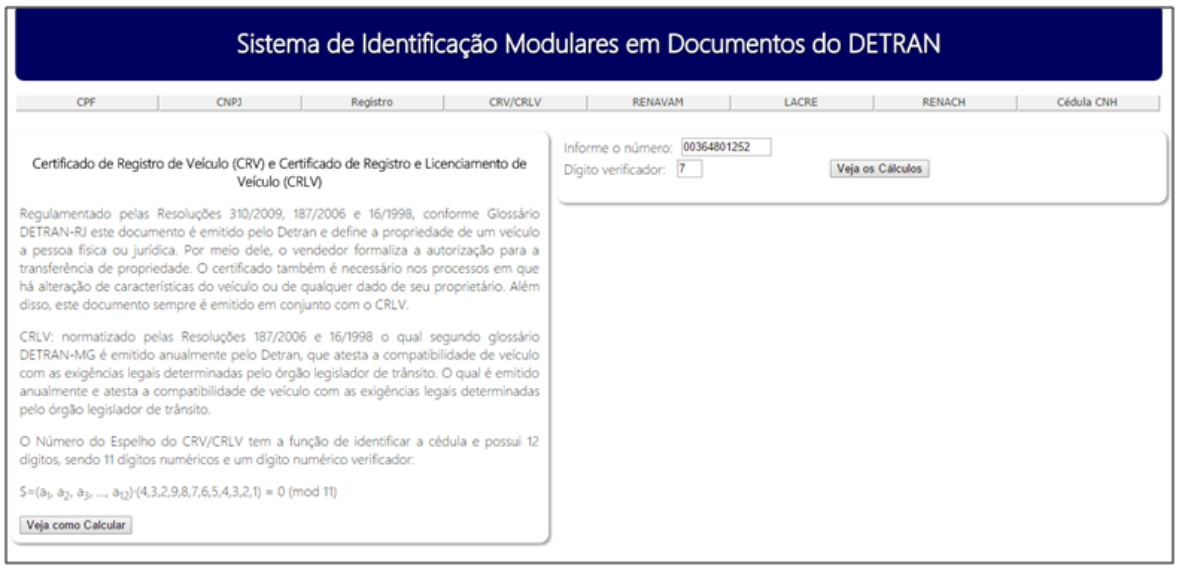
Clicando sobre ícone "Veja como Calcular" abrirá uma janela a direita, na qual aparecerão um ícone chamado "Calcule o Dígito" e dois campos: um para que o aluno possa fornecer os dígitos do código sem o dígito verificador e outro que fornecerá o dígito verificador calculado a partir dos dígitos inseridos pelo aluno. (Ver Figura 4.3)

Figura 4.3 – Campos “Informe o número” e “Dígito verificador” e ícone “Calcule o Dígito”.



Após o aluno inserir os dígitos do código sem o dígito verificador e clicar em “Calcule o Dígito”, o site fornecerá no campo “Dígito Verificador” o valor do dígito verificador, como pode ser observado na Figura 4.4. Com isso, o aluno poderá conferir se o resultado que ele fez em seu caderno é igual ao fornecido pelo site.

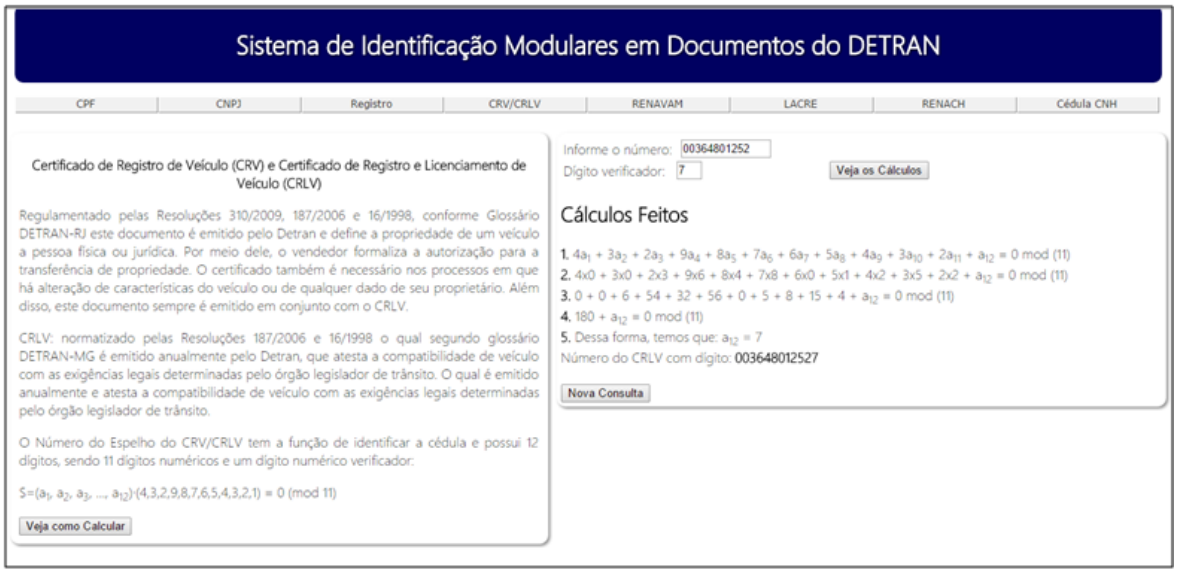
Figura 4.4 – Valor do dígito verificador.



Em seguida, além de fornecer o valor do dígito verificador, o site apresentará um ícone denominado “Veja os Cálculos” (Figura 4.5). Ao clicar sobre este ícone, o aluno terá a possibilidade de conferir passo a passo o cálculo do dígito verificador e com isso conferir se sua resolução está igual à fornecida pelo site. Com isso, o aluno

que por ventura errou a questão poderá encontrar seu erro conferindo linha a linha a solução apresentada.

Figura 4.5 – Passo a passo para os cálculos do dígito verificador.



Após isso, será fornecido o código completo com os dígitos fornecidos pelo aluno e o respectivo dígito calculado, além de disponibilizar o ícone "Nova Consulta", que oferece a oportunidade de fazer novos cálculos.

Nesse momento, espera-se que os alunos já estejam familiarizados não somente com os sistemas de identificação modulares, mas também com algumas definições dos códigos trabalhados nos documentos do DETRAN, pois a partir disso o professor irá propor questões para um debate sobre alguns temas relacionados ao trânsito, como CRV/CRLV, CNH e Guias de Arrecadação utilizados em exemplos anteriores.

Exemplo 4.11. Sugestões de questões para debate:

- O que faz o DETRAN?
- Para que serve o CRLV e por que ele tem que ser atualizado anualmente?
- Qual(is) a(s) finalidade(s) da Taxa de Licenciamento, do Seguro DPVAT e do IPVA?
- Em sua opinião a finalidade dos recursos tem sido efetivamente cumprida? Por quê?
- Para que serve a CNH? Ela precisa ser renovada? Por quê?
- Por que a CNH e o CRLV são documentos de porte obrigatório?

- A pessoa que aprende a dirigir sozinha ou com a ajuda de um amigo está habilitada a dirigir nas vias? Por quê?
- Só quem possui CNH tem responsabilidade para um trânsito consciente?
- Uma pessoa tem um veículo emplacado em seu nome, ela pode dirigir seu próprio veículo, mesmo que não possua CNH?

Dessa forma, poderemos proporcionar um importante momento para que o aluno possa analisar e refletir sobre as informações obtidas, oportunizadas pelo debate e a manifestação de opiniões a respeito do tema, onde cálculos e operações matemáticas serão ferramentas facilitadoras no processo de compreensão do tema.

CONSIDERAÇÕES FINAIS

Como vimos, um trânsito seguro é direito de todos e somente pela educação teremos cidadãos mais conscientes e, consequentemente, menos acidentes. Além disso, observamos que o trânsito pode e deve ser abordado nas diversas fases do aprendizado, ou seja, da pré-escola ao ensino superior. Outro fator importante observado, decorrente da transversalidade do tema trânsito, é a possibilidade de abordagem na disciplina de matemática.

Dentre as diversas possibilidades dentro da matemática, trabalhamos com congruência por se tratar de um dos conceitos mais importantes da Aritmética e possuir diversas aplicações de fácil compreensão e que fazem parte do cotidiano dos alunos. Como exemplo, temos os sistemas de identificação modulares, que estão presentes em códigos de barra, documentos pessoais, documentos do Detran, entre outros que pudemos ver no decorrer desta dissertação. Ademais, por ser uma definição fundamentada em divisão euclidiana e divisibilidade, sua aplicação torna-se tangível aos alunos do ensino médio e das séries finais do ensino Fundamental.

Além disso, a partir do conceito de congruência e sua aplicação em sistema de identificação modulares, mostramos mais uma possibilidade de falar de trânsito nas aulas de matemática e com isso oferecer a oportunidade de propiciar um debate que será um agente facilitador na formação de um cidadão mais crítico e comprometido com seu papel na sociedade.

Dessa forma, espere-se que esta dissertação seja um agente motivador para que mais professores de matemática possam abordar o trânsito em sala de aula de forma alternativa e interessante.

REFERÊNCIAS BIBLIOGRÁFICAS

AGÊNCIA BRASIL. *Mulheres podem tirar CPF de graça.* São Paulo, 09 março 2011. Disponível em: <http://www.clmais.com.br/informacao/17245/mulheres-podem-tirar-cpf-de-gra%C3%A7a>. Acesso em: 12 março 2014.

ALENCAR FILHO, E. de. *Aritmética dos Inteiros.* São Paulo: Nobel, 1987.

ARAUJO, M. J. V. C. de. *Introdução à Álgebra.* Notas de Aulas. 2009. Disponível em: <http://www.ufjf.br/carlos_soares/files/2010/08/Apostila-%C3%81lgebra.pdf>. Acesso em: 12 abril 2014.

BRASIL. Departamento Nacional de Trânsito. *Diretrizes Nacionais da Educação para o Trânsito no Ensino Fundamental.* Brasília: Ministério das Cidades, 2009. Disponível em: <http://www.denatran.gov.br/download/portarias/2009/portaria_denatran_147_09_anexo_ii_diretrizes_ef.pdf>. Acesso em: 12 set. 2014.

_____. Lei nº 9394, de 20 de dezembro de 1996. Estabelece as diretrizes e bases da educação nacional. *Lei de Diretrizes e Bases da Educação - LDB.* Brasília, 1996.

_____. Ministério da Educação (MEC), Secretaria de Educação do Ensino Médio. *Parâmetros Curriculares Nacionais para o Ensino Médio (PCNEM):* Ciências da Natureza, Matemática e suas Tecnologias. Brasília: MEC, 2000.

_____. Ministério da Educação (MEC), Secretaria de Educação Fundamental (SEF). *Parâmetros Curriculares Nacionais (PCN)*: Apresentação dos Temas Transversais, Ética. Brasília: MEC/SEF, 1997.

CARNEIRO, J. P. Q. *Dispositivo prático para expressar o MDC.* Revista do Professor de Matemática, n. 37. Rio de Janeiro: Sociedade Brasileira de Matemática, 2009. Disponível em: <http://www.feg.unesp.br/~anachiaradia/Material/FAM%20-%20Dispositivo%20pratico%20para%20expressar%20o%20mdc.pdf>. Acesso em: 04 out. 2014.

DEPARTAMENTO ESTADUAL DE TRÂNSITO DE MATO GROSSO. Histórico do DETRAN. Disponível em: <http://www.detran.mt.gov.br/institucional/1088/1176/historico-do-detran->. Acesso em: 14 fev. 2014.

DEPARTAMENTO ESTADUAL DE TRÂNSITO DE SÃO PAULO. Disponível em: <http://www.detran.sp.gov.br/>. Acesso em: 22 jun. 2014.

FEBRABAN - Federação Brasileira dos Bancos. *"Layout" Padrão de Arrecadação / Recebimento com Utilização do Código de Barras.* Versão 04. Disponível em: <http://www.febraban.org.br>. Acesso em: 15 abril 2014.

DOCUMENTAÇÃO de Veículos Usados. Disponível em: <http://autos.culturamix.com/dicas/documentacao-de-veiculos-usados>. Acesso em: 22 março 2014.

ESQUINCA, J. C. P. *Aritmética: Códigos de Barras e Outras Aplicações de Congruências.* 2013. 63 p. Dissertação (Mestrado Profissional em Matemática) - Universidade Federal de Mato Grosso do Sul, Campo Grande, MS, 2013. Disponível em: <http://bit.profmat-sbm.org.br/xmlui/bitstream/handle/123456789/371/2011_00238_JOSIANE_COLOMBO_PEDRINI_ESQUINCA.pdf?sequence=1>. Acesso em: 01 dez. 2013.

GB Network & Print. *Código de Barras GTIN GS1 EAN-13.* Disponível em: <http://gbnet.com.br/v2/new_barcodes_ean13.html>. Acesso em: 19 fev. 2014.

GHIORZI, T. *Dígitos Verificadores - CGC / CPF / Título Eleitoral.* Disponível em: <http://www.jalucrei.com.br/calculo_dv_cpf_cgc.htm>. Acesso em: 05 de abril de 2014.

GOMES, O. R.; SILVA, J. C. *Estruturas Algébricas para Licenciatura:* Introdução à Teoria dos Números. Brasília: Ed. do Autor, 2008.

GOULART, A. *Cálculo do Digito Verificador para CPF e CGC.* Disponível em: <http://www.goulart.pro.br/cbasico/Calculo_dv.htm>. Acesso em: 05 abril 2014.

HEFEZ, A. *Elementos de Aritmética.* Rio de Janeiro: Sociedade Brasileira de Matemática, 2011.

HEFEZ, A. *Iniciação à Aritmética.* Programa de Iniciação Científica OBMEP. Rio de Janeiro: Sociedade Brasileira de Matemática, 2012.

KRASILCHIK, M.; MARANDINO, M. *Ensino de Ciências e Cidadania.* São Paulo: Moderna, 2004.

LIVRO Fly Back's Tirando Dúvidas! LOJA Virtual Esquemafácil. Disponível em: http://www.esquemafacil.com.br/livros-tecnicos/televisores/livro-fly-back-s-tirando-

duvidas-ref-5537-isbn-978-85-7036-139-4.html. Acesso em: 19 fev. 2014.

LOURENÇO, P. J. P. *Aplicações da Aritmética Modular*. 2011. 123 p. Dissertação (Mestrado em Matemática) - Universidade de Coimbra, Coimbra, Portugal, 2011. Disponível em: <http://sistemaidentificacao.no.sapo.pt/ficheiros/Relatorio-Arit%20Modular.pdf>. Acesso em: 27 jan. 2014.

MATIAS, C. 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: <http://dsc.inf.furb.br/arquivos/tccs/monografias/2004-2caiorsmatiasvf.pdf>. Acesso em: 04 out. 2014.

MILIES, C. P. *A Matemática dos Códigos de Barra.* Revista do Professor de Matemática, n. 65. Rio de Janeiro: Sociedade Brasileira de Matemática (SBM), 2008. p. 46-53.

_____. *A Matemática dos Códigos de Barra:* detectando erros. Revista do Professor de Matemática, n. 68, Rio de Janeiro: Sociedade Brasileira de Matemática (SBM), 2009. p. 38-42.

MINAS GERAIS. Polícia Civil do Estado de Minas Gerais, Departamento de Trânsito de Minas Gerais, Coordenação de Educação de Trânsito. *Trânsito - Aprender para a Vida*. Belo Horizonte: O Lutador, 2003.

MOURA, B. do C. *Logística:* conceitos e tendências. Lisboa: Centro Atlântico, 2006. Disponível em: <http://books.google.com.br/books?id=uIReFI6gzugC&pg=PA260&lpg=PA260&dq=sistemas+de+identifica%C3%A7%C3%A3o&source=bl&ots=UqtL0vSgH5&sig=-O4ppMgldgzDPFLS3C9AU6JNRZU&hl=pt-BR&sa=X&ei=26Y9VMT8E4XJgwTZxILYBA&ved=0CDMQ6AEwBDgo#v=onepage&q=sistemas%20de%20identifica%C3%A7%C3%A3o&f=false>. Acesso em: 12 out. 2014.

NEIVA, Miguel. *Color Identification System for Colorblind People*. Disponível em: <http://www.coloradd.net/>. Acesso em: 28 out. 2014.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *ONU: 50 mil pessoas foram assassinadas no Brasil em 2012. Isto equivale a 10% dos homicídios no mundo*. 10 de abril de 2014. Disponível em: <http://www.onu.org.br/onu-50-mil-pessoas-foram-assinadas-no-brasil-em-2012-isto-equivale-a-10-dos-homicidios-no-mundo/>. Acesso em: 13 out. 2014.

PICADO, J. *A Álgebra dos Sistemas de Identificação:* da aritmética modular aos grupos diedrais. Boletim da Sociedade Portuguesa de Matemática. Coimbra - Portugal: 2001. v. 44, p. 39-73.

PIMENTEL, C. Um passeio pela história – de carro: Pesquisa mostra como foi a

chegada dos primeiros modelos em Mato Grosso e a reação da população. *Diário de Cuiabá.* Cuiabá, 20 jan. 2002. Edição nº 10183. Disponível em: <http://www.diariodecuiaba.com.br/detalhe.php?cod=85225>. Acesso em: 02 set. 2014.

_____. Ritmo imposto pelos motores obrigou cidade a se adaptar. *Diário de Cuiabá.* Cuiabá, 20 jan. 2002. Edição nº 10183. Disponível em: <http://www.diariodecuiaba.com.br/detalhe.php?cod=85228>. Acesso em: 02 set. 2014.

SÁ, I. P. de. *Aritmética modular e algumas de suas aplicações.* Disponível em: <http://www.magiadamatematica.com/diversos/eventos/20-congruencia.pdf>. Acesso em: 01 dez. 2013.

SILVA, V. A. R. da. *Propostas de Utilização de Códigos de Barra como Recurso Didático para o Ensino da Matemática.* 2013. 44 p. Dissertação (Mestrado Profissional em Matemática) - Universidade Federal Rural do Rio de Janeiro, Seropédica - Rio de Janeiro, 2013. Disponível em: <http://bit.profmat-sbm.org.br/xmlui/bitstream/handle/123456789/520/2011_00418_VALESKA_APARECIDA_RODRIGUES_DA_SILVA.pdf?sequence=1>. Acesso em: 01 dez. 2013.

WIKIPÉDIA - a enciclopédia livre. *Identificação Automática e Captura de Dados.* Flórida: Wikimedia Foundation, 2013. Disponível em: <http://pt.wikipedia.org/w/index.php?title=Identifica%C3%A7%C3%A3o_autom%C3%A1tica_e_captura_de_dados&oldid=35163331>. Acesso em: 12 out. 2014.