UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO

MATEMÁTICA EM REDE NACIONAL

MESTRADO PROFISSIONAL

JOSIANE COLOMBO PEDRINI ESQUINCA

ARITMÉTICA: CÓDIGOS DE BARRAS E OUTRAS APLICAÇÕES DE CONGRUÊNCIAS

CAMPO GRANDE - MS

Abril de 2013

UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO

MATEMÁTICA EM REDE NACIONAL

MESTRADO PROFISSIONAL

JOSIANE COLOMBO PEDRINI ESQUINCA

ARITMÉTICA: CÓDIGO DE BARRAS E OUTRAS APLICAÇÕES DE CONGRUÊNCIAS

Orientadora: Prof.ª Dr. ª Elisabete Sousa Freitas

Trabalho de Conclusão de Curso apresentado ao Programa de Pós-Graduação em Matemática em Rede Nacional do Centro de Ciências Exatas e Tecnologia – CCET/UFMS, como parte dos requisitos para obtenção do título de Mestre.

Campo Grande - MS

Abril de 2013

ARITMÉTICA: CÓDIGO DE BARRAS E OUTRAS APLICAÇÕES DE CONGRUÊNCIAS

JOSIANE COLOMBO PEDRINI ESQUINCA

Trabalho de Conclusão de Curso submetido ao Programa de Pós-Graduação em Matemática em Rede Nacional, Centro de Ciências Exatas e Tecnologia, da Universidade Federal de Mato Grosso do Sul, como parte dos requisitos para obtenção do título de Mestre.

Aprovado pela Banca Examinadora:

Prof. Dr. Claudemir Aniz - UFMS
Prof. ª Dr. ª Elisabete Sousa Freitas - UFMS
Prof. ª Dr. ª Anamaria Gomide - UNICAMP

Campo Grande - MS

Abril de 2013

Dedico aos meus pais, José Antônio e Edma, que compreenderam minha ausência. Agradeço por aceitarem minha falta, durante minha busca por novos conhecimentos, concedendo-me a chance de crescer ainda mais.

Epígrafe

A engenhosidade humana não pode arquitetar uma escrita secreta que a própria engenhosidade humana não possa resolver.

Edgar Allan Poe

AGRADECIMENTOS

Agradeço em primeiro lugar a Deus, por essa oportunidade e por me dar forças nos momentos em que mais precisei.

Ao meu esposo Rogério Esquinca, por estar sempre ao meu lado, me ajudando em tudo o que precisasse.

Aos meus pais, que por tantas vezes deixei de vê-los, por causa das obrigações que tinha para com este trabalho, pelo amor e por todas as orações que fizeram. Ao meu irmão, Leandro, pelo companheirismo durante essa caminhada.

A minha professora e Orientadora, Elisabete, por toda dedicação e paciência, por ser para mim hoje, um exemplo de pessoa e de professora a serem seguidos.

Ao professor e coordenador do curso, Claudemir Aniz, pelo empenho e atenção destinados aos alunos e professores do Profmat e por toda preocupação em garantir um curso de boa qualidade.

Ao programa Profmat, pela oportunidade de crescimento profissional.

A Capes, pelo incentivo e financiamento do curso.

A todos os colegas de turma, pelas trocas de conhecimento que fizemos, principalmente a Hellen pelos dias e noites de estudo.

Aos meus colegas de trabalho, em especial, Rosimeire, Oscar, Daiane, Clener, Márcia, Hélio, Rosinete, Abegail e Marilene, pela compreensão, incentivo e ajuda, nos momentos em que precisei.

Enfim, agradeço a todos que contribuíram de alguma forma, para que esse objetivo fosse alcançado.

Resumo

O presente trabalho tem por objetivo ser um instrumento de auxílio para o professor de matemática da Educação Básica, no desenvolvimento de aulas de *Aritmética.* Contém algumas aplicações de *congruência*, presentes no dia-a-dia, sendo elas: Critério de Divisibilidade, A Prova dos Noves, Código de Barras e Sistema de Identificação ISBN. Antes das aplicações, foi feito um embasamento teórico sobre *Aritmética Modular*. As aplicações aqui expostas não costumam estar presentes nos atuais livros didáticos da Educação Básica. No entanto, podem ser úteis para o aprendizado dos alunos, no sentido de servirem como novas ferramentas de cálculo, trazendo agilidade e simplicidade na resolução de problemas matemáticos. Além dessas aplicações serem interessantes aos olhos dos alunos, a *Aritmética Modular* é utilizada na solução de diversos problemas da atualidade.

Palavras-chave: Aritmética. Divisão Euclidiana. Congruência.

Abstract

This paper aims to be a tool to aid the math teacher of Basic Education in developing lessons *Arithmetic*. Contains some *congruence* applications, present in the day by day, namely: Divisibility Criterion, The Proof of Nines, Barcoding and Identification System ISBN. Before the application was made on a theoretical basis *Modular Arithmetic*. The applications presented here are usually not present in current textbooks of Basic Education. However, it may be useful for student learning, to serve as new calculation tools, bringing speed and simplicity in solving mathematical problems. Besides these applications are interesting in the eyes of the students, the *Modular Arithmetic* is used in solving various problems of today.

Keywords: Arithmetic. Euclidean Division. Congruence.

Sumário

Capítulo 1

Introdução

A *Teoria dos Números* é o ramo da matemática que estuda propriedades dos números em geral. Ela pode ser dividida em vários campos, sendo um deles chamado *Teoria Elementar dos Números,* que estuda propriedades dos números inteiros.

Uma das ferramentas importantes da *Teoria Elementar dos Números* é a *Aritmética Modular,* que envolve o estudo de congruências no conjunto dos números inteiros.

A principal motivação para a escolha do tema "*Aritmética Modular*" para esse trabalho foi a sua pertinência na solução de diversos problemas atuais. Muitos desses problemas estão relacionados ao crescente uso das tecnologias de comunicação, principalmente a internet, e vêm sendo resolvidos com o auxílio da *Aritmética Modular*. Duas importantes aplicações da *Aritmética Modular* são a Criptografia e os Códigos de Barras. A primeira faz a codificação de senhas ou de outros conteúdos que necessitem de sigilo absoluto, proporcionando-lhes a proteção necessária. Já os códigos de barras são usados pelo mundo todo para a identificação de produtos, o que facilita muito a organização de estoques, além de agilizar o processo de compras e vendas. Além disso, existem vários problemas da matemática, os quais podem ter a sua resolução agilizada se usarmos em sua solução propriedades da *Aritmética Modular*.

O objetivo principal deste trabalho é o de servir como uma ferramenta para o planejamento de aulas de matemática, para professores do ensino básico, principalmente os do ensino médio, que estejam dispostos a utilizar no decorrer de suas aulas, as aplicações de *Aritmética Modular* aqui contidas, mostrando aos seus alunos que essa *Aritmética* está presente no dia-a-dia e o quanto são importantes as suas aplicações.

A utilização de aplicações em forma de exemplos, principalmente na introdução de alguns conteúdos matemáticos, tem sempre como meta, torná-los menos abstratos e mais interessantes para os alunos, permitindo-lhes reconhecê-los como algo real, aplicável, que pode ser usado por eles em situações do cotidiano, e não só dentro da sala de aula, durante as aulas de matemática.

É esperado ainda que, a partir deste trabalho, muitos outros possam surgir, para completá-lo e enriquecê-lo ainda mais, com outras aplicações de *Aritmética Modular* que possam ser adequadamente utilizadas nas aulas ministradas por professores de matemática da Educação Básica.

Capítulo 2

Aritmética Modular

2.1 Um Pouco da História

Muitos problemas, tratados em *Teoria dos Números,* têm o enunciado de fácil interpretação, porém existem vários problemas deste tipo em aberto, isto é, que continuam sem solução.

Para exemplificar, pode-se citar a *Conjectura de Golbach*, formulada em 1746:

"*Todo número par maior do que 2 pode ser escrito como soma de dois números primos*".

Um teorema famoso, conhecido como " *O Último Teorema de Fermat",* enunciado por Pierre de Fermat no século XVII, só foi provado em 1995.

Embora não fosse um matemático por profissão, Pierre de Fermat (França, 1601-1665) dedicava parte do seu tempo para estudar matemática e muito contribuiu para o desenvolvimento da *Teoria dos Números.* Além disso, Fermat também deu contribuições importantes ao Cálculo Diferencial e Integral e à Geometria, por exemplo. Ele costumava propor diversos desafios para matemáticos da época, os quais se empenhavam em solucioná-los. Seu último desafio, o "*Último Teorema de Fermat*", logo abaixo, é um exemplo de enunciado muito fácil de se entender:

Teorema: A equação $x^n + y^n = z^n$, não possui solução inteira, não trivial, para n natural,

$n \geq 3$.

Observação: Uma solução é chamada trivial se $x \cdot y \cdot z = 0$.

Fermat costumava fazer anotações sobre seus estudos nas margens de seus livros e o único indício deixado por ele sobre a prova deste teorema é uma observação feita em 1637 na sua cópia do livro "*Aritmética*", do grego Diofanto.

Na margem do Problema 8 do Livro 2 Fermat Escreveu:

"Eu descobri uma demonstração verdadeiramente maravilhosa disto, que toda via esta margem não é suficientemente grande para cabê-la"[7].

A partir daí, o *Último Teorema de Fermat* se tornou objeto de estudo de muitos matemáticos que tentaram por muitos anos demonstrá-lo. Até mesmo, prêmios em dinheiro foram oferecidos àquele que conseguisse tamanha façanha. As tentativas foram muitas, mas conseguiam no máximo provar o teorema para casos particulares.

Enfim, em 1995, o *Último Teorema de Fermat* foi demonstrado pelo matemático inglês Andrew Wiles. Andrew utilizou como base a conjectura Taniyama-Shimura, feita pelos matemáticos Yutaka Taniyama e Goro Shimura. Andrew tinha interesse no teorema desde os dez anos de idade, porém só aprofundou seus estudos, secretamente, sete anos antes da descoberta. Como recompensa Andrew recebeu um prêmio de $50.000 libras da *Fundação Wolfskhel*.

O livro "*O Último Teorema de Fermat*" de Simon Singh, conta toda a história do teorema.

Mesmo após o feito de Andrew Wiles, os matemáticos tentam até hoje desvendar o mistério de como seria a demonstração original de Fermat.

Apesar do "*Último Teorema de Fermat*" não ter aplicações imediatas, na tentativa de demonstrá-lo foram desenvolvidas muitas ideias e ferramentas matemáticas que tomaram rumo próprio e encontraram aplicações práticas. Uma aplicação importante é o uso dessas ferramentas em Criptografia.

2.2 Principais Conceitos e Teoremas

"*Determinar quantas vezes uma parte cabe em outra*", "*dividir uma quantidade em partes iguais*", são frases muito comuns nos livros didáticos de matemática da Educação Básica, nos capítulos que tratam sobre divisão de números inteiros. Na verdade, essas frases fazem parte de uma das principais propriedades dos números inteiros, a *Divisão Euclidiana*.

2.2.1 Algoritmo da Divisão

Neste trabalho, considera-se os conjuntos $\mathbb{Z}$ dos números inteiros e $\mathbb{N}$ dos números naturais, com suas operações de multiplicação $(\cdot)$ e adição $(+)$ e a relação de ordem $\leq$, com suas propriedades já conhecidas. Além disso, considera-se o inteiro 0 como número natural e o *Princípio da Boa Ordenação* em $\mathbb{N}$.

Observação: *Princípio da Boa Ordenação.*

Todo subconjunto não vazio X do conjunto $\mathbb{N}$ dos números naturais, tem um menor elemento, isto é, existe $m_0 \in X$ tal que $m_0 \leq x$ para todo $x \in X$.

Proposição 1. (*Divisão Euclidiana em* $\mathbb{N}$) Dados dois números naturais quaisquer, a e b, com $a > 0$, existem dois únicos números naturais q e r, com $0 \leq r < a$, tais que, $b = qa + r$.

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

Demonstração:

(Existência)

Caso $a > b$, tem-se $q = 0$ e $r = b$, ou seja, $b = 0 \cdot a + b$, em que $0 \leq b < a$.

Caso $b = a$, tem-se $q = 1$ e $r = 0$, ou seja, $b = 1 \cdot a + 0$, em que $0 \leq 0 < a$.

Caso $a \leq b$, considere a seguinte lista de números, enquanto todas as diferenças forem números naturais:

$$b, b - a, b - 2a, b - 3a, ..., b - na, ... \qquad (1)$$

Essa lista de números naturais é decrescente, logo finita, portanto a lista (1) possui um menor elemento. Chamando de r o menor elemento da lista (1), então existirá um número natural q, tal que $r = b - qa$.

$$b, b-a, b-2a, b-3a, ..., b-qa \text{ (último número natural da lista).}$$

Como r é um número natural, $0 \leq r$. Agora basta verificar que $r < a$.

Suponha que $r \geq a$, então existe um número natural c, com $c < r$, tal que $r = c+a$. Daí,

$$r = c + a = b - qa \Rightarrow c = b - qa - a \Rightarrow c = b - (q+1)a.$$

Mas, se $c = b - (q+1)a$, então c é um elemento da lista (1) menor do que r. O que contradiz a hipótese, pois r é o menor elemento da lista (1), com $r = b - qa$.

Portanto, $b = aq + r$ com $0 \leq r < a$, o que prova a existência de q e r.

(Unicidade)

Sejam $b = qa + r$ e $b = q'a + r'$, com $0 \leq r < a$ e $0 \leq r' < a$. Suponha, sem perda de generalidade, que $r \leq r'$, tem-se que:

$$r \leq r' \Rightarrow 0 \leq r' - r = -q'a + qa = (q - q')a \text{ e}$$

$$0 \leq r \leq r' < a \Rightarrow 0 \leq r' - r < a.$$

Daí,

$$0 \leq (q - q')a < a \Rightarrow 0 \leq q - q' < 1 \Rightarrow q' - q = 0 \Rightarrow q = q'$$

Logo, $r = r'$.

Portanto, r e q são únicos tais que $b = qa + r$, com $0 \leq r < a$.

■

Exemplo 1. Escreva a lista (1) para os seguintes valores de a e b:

(i) $a = 3$ e $b = 10$.

Tem-se a seguinte sequência:

$$10,\ 10 - 3,\ 10 - (2 \text{ x } 3),\ 10 - (3 \text{ x } 3);$$

$$10,\ 7,\ 4,\ 1$$

Assim, $10 = 3 \cdot 3 + 1$, ou seja, $q = 3$ e $r = 1$.

(ii) $a = 10$ e $b = 3$.

Neste caso, como $b < a$, tem-se:

$3 = 0 \cdot 10 + 3$, ou seja, $q = 0$ e $r = 3$.

(iii) $a = 2$ e $b = 22$.

A sequência será:

$$22,\ 22 - 1 \cdot 2,\ 22 - 2 \cdot 2,\ 22 - 3 \cdot 2,\ 22 - 4 \cdot 2,\ 22 - 5 \cdot 2,\ 22 - 6 \cdot 2,\ 22 - 7 \cdot 2,\ 22 - 8 \cdot 2,\ 22 - 9 \cdot 2,\ 22 - 10 \cdot 2,\ 22 - 2 \cdot 11$$

ou seja,

$$22,\ 20,\ 18,\ 16,\ 14,\ 12,\ 10,\ 8,\ 6,\ 4,\ 2,\ 0.$$

Resultando em $22 = 11 \cdot 2 + 0$, o que dá, $q = 11$ e $r = 0$.

Sempre que $r = 0$, isto é, $b = qa$, diz-se que b é múltiplo de a ou que b é divisível por a.

Pode-se estender o algoritmo anterior para o conjunto dos números inteiros, conforme mostra a seguinte proposição:

Proposição 2. (Algoritmo da Divisão) Sejam a e b números inteiros com $a > 0$, então existem únicos r e q, inteiros, tais que:

$$b = qa + r,\ 0 \leq r < a,$$

em que r é o resto e q é o quociente da divisão de b por a.

Demonstração:

(Existência)

O caso de b ser um número natural já foi estudado na proposição 1. Analisa-se agora, como ficariam o quociente e o resto, para a divisão de um número inteiro negativo. Suponha que $b < 0$, logo, $-b > 0$.

Da proposição 1, tem-se que existem únicos q' e r' tais que $-b = q'a + r'$, em que $0 \leq r' < a$. Daí,

$$-b = q'a + r' \Rightarrow b = -q'a - r' \Rightarrow b = -q'a - a + a - r' \Rightarrow$$

$$b = (-q' - 1)a + a - r',\ 0 \leq a - r' < a$$

Dessa forma, $q = (-q' - 1)$, cumpre o papel do quociente, enquanto que $r = a - r'$ representa o resto da divisão de, b por a.

(Unicidade)

Devido a unicidade de q' e de r' provada na proposição 1, fica garantida a unicidade de q e r.

■

Exemplo 2. Ana, Beto e Carlos, possuem uma conta em conjunto com saldo devedor de 550 reais. Eles querem dividir o valor igualmente e pagar essa dívida através de um depósito em dinheiro no caixa eletrônico. Sabendo que não é permitido colocar moedas no envelope, qual será o saldo da conta após os três terem depositado o mesmo valor, sendo este valor a menor quantia necessária para quitar a divida?

Solução:

Fazendo a divisão euclidiana da dívida de 550 reais, por 3, tem-se:

$$-550 = (-184) \cdot 3 + 2$$

Portanto, Ana, Beto e Carlos irão depositar 184 reais cada um e sobrarão 2 reais de saldo positivo na conta.

Observação: (Definição de número par e de número ímpar)

Seja $a \in \mathbb{Z}$. Considere a divisão euclidiana de a por 2. Tem-se que $a = 2q + r$ em que $r = 0$ ou $r = 1$.

Dessa forma, diz-se que um número natural é par se deixa resto zero na divisão por 2 e é ímpar se deixa resto 1 na divisão por 2. Assim,

$$\mathbb{Z} = \{2q; q \in \mathbb{Z}\} \cup \{2q + 1; q \in \mathbb{Z}\} = \{\textit{números pares}\} \cup \{\textit{números ímpares}\}.$$

Exemplo 3. Prove que o produto de dois números inteiros consecutivos é sempre par.

Solução:

Considere dois números inteiros consecutivos, n e $n + 1$. Tem-se que $n = 2q$ ou $n = 2q + 1$. Donde $n(n + 1) = 2q(2q + 1)$ ou $n = (2q + 1)(2q + 2) = 2(2q + 1)(q + 1)$.

Portanto, o produto de dois números inteiros consecutivos é sempre par.

2.2.2 Divisibilidade

Definição 1. Sejam a, $b \in \mathbb{Z}$. Diz-se que a *divide* b quando existe $q \in \mathbb{Z}$, tal que $b = qa$.

Notação:

Caso a divida b, escreve-se: $a \mid b$ (lê-se: a divide b, ou a é um divisor de b ou b é um múltiplo de a).

Caso a não divida b, escreve-se: $a \nmid b$ (lê-se: a não divide b).

Exemplo 4. Tem-se que $5 \mid 35$, pois $35 = 7{\cdot}5$.

Observação: Se $b \neq 0$ e $a \mid b$, o inteiro q nas condições da definição é único e é denominado *quociente* de b por a, indicado por $q = \frac{b}{a}$. De fato, se $b = a \cdot q = a \cdot q'$ então $a \cdot (q - q') = 0$, em que $a \neq 0$, e daí $q = q'$.

Quando $a = 0$ divide b, tem-se que $b = 0$ e neste caso $0 = 0 \cdot q$, para todo q inteiro.

Assim, pela definição, $\frac{0}{0}$ é uma indeterminação.

Exemplo 5. Tem-se que $5 \mid 35$ e $7 = \frac{35}{5}$.

Proposição 3. Sejam a, b, c e d números inteiros quaisquer. Então valem:

(i) $1 \mid a$, $a \mid a$ e $a \mid 0$.

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

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

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

(v) Se $a \mid b$ então para todo $m \in \mathbb{Z}$, tem-se que $a \mid (mb)$.

(vi) Se $a \mid b$ e $a \mid c$, então para todos m, $n \in \mathbb{Z}$, tem-se que $a \mid (mb + nc)$.

(vii) $a|b \Leftrightarrow a \mid -b \Leftrightarrow -a \mid b \Leftrightarrow -a \mid -b$.

$(viii)$ Se $a \mid b$ e $b \neq 0$, então $|a| \leq |b|$.

(ix) Se $b \mid a$ e $a \mid b$, então $a = \pm b$.

(x) Se $a \mid 1$, então $a = \pm 1$.

Demonstração:

(i) Tem-se que, $1 \mid a$ pois $a = 1 \cdot a$, $a \mid a$ pois $a = 1 \cdot a$ e por fim, $a \mid 0$ pois $0 = 0 \cdot a$.

(ii) Se $a \mid b$ e $b \mid c$, então existem números inteiros q_1 e q_2, tais que $b = q_1 a$ e $c = q_2 b$, substituindo a primeira equação na segunda tem-se, $c = (q_2 q_1)a$, logo, $a \mid c$.

(iii) Se $a \mid b$ e $c \mid d$, então existem números inteiros q_1 e q_2, tais que $b = q_1 a$ e $d = q_2 c$, multiplicando ordenadamente a primeira e a segunda equação tem-se, $bd = (q_2 q_1)ac$, logo, $ac \mid bd$.

(iv) Se $a \mid b$ e $a \mid c$, então existem números inteiros q_1 e q_2, tais que $b = q_1 a$ e $c = q_2 a$, somando membro a membro as duas equações tem-se, $b + c = q_1 a + q_2 a = (q_2 + q_1)a$, logo, $a \mid (b + c)$.

(v) Se $a \mid b$ então existe um número inteiro q, tal que $b = qa$, multiplicando a equação anterior por um número inteiro m, tem-se que $mb = (qm)a$, logo, para todo m, tem-se que $a \mid mb$.

(vi) Se $a \mid b$ e $a \mid c$, então existem números inteiros q_1 e q_2, tais que $b = q_1 a$ e $c = q_2 a$, multiplicando a primeira equação por m e a segunda por n, sendo m e n inteiros, tem-se: $mb = q_1 ma$ e $nc = q_2 na$, em seguida, somando membro a membro as duas últimas equações, obtêm-se $mb + nc = q_1 ma + q_2 na = (q_1 m + q_2 n)a$, logo $a \mid (mb + nc)$.

(vii)

$a \mid b \Leftrightarrow b = qa,\ q \in \mathbb{Z} \Leftrightarrow -b = (-q)a,\ (-q) \in \mathbb{Z} \Leftrightarrow b = (-q)(-a),\ (-q) \in \mathbb{Z} \Leftrightarrow -b = q(-a),\ q \in \mathbb{Z}$.

$(viii)$ Se $a \mid b$ com $b \neq 0$, então existe um inteiro $q \neq 0$ tal que $b = qa$, logo,

$$|b| = |qa| = |q| \cdot |a| \geq |a|.$$

(ix) Suponha que $b \mid a$ e $a \mid b$. Se $a = 0$ ou $b = 0$, tem-se, $a = b = 0$. No caso $a, b \neq 0$, tem-se, pelo item $(viii)$ desta proposição, $|a| \leq |b|$ e $|a| \geq |b|$ logo, $|a| = |b|$, ou seja, $a = \pm b$.

(x) Suponha que $a \mid 1$. Do item (i) desta proposição, $1 \mid a$ para todo a inteiro. Logo, pelo item anterior (ix), tem-se que $a = \pm 1$.

■

Proposição 4. Sejam a, b, $c \in \mathbb{Z}$, tais que $a \mid (b + c)$. Então

$$a \mid b \Leftrightarrow a \mid c.$$

Demonstração:

Suponha que $a \mid (b+c)$. Então, existe um número inteiro q, tal que $b+c=qa$.

($\Rightarrow$)

Suponha ainda, que $a \mid b$, então existe q_1 tal que $b = aq_1$. De $b+c=qa$ e de $b=aq_1$, tem-se que $aq_1+c=aq$. Daí, $c=a(q-q_1)$, como $q-q_1 \in \mathbb{Z}$, pode-se concluir que $a \mid c$.

A demonstração da recíproca é análoga.

■

Exemplo 6. Sejam a, $b \in \mathbb{Z}$ *e* $n \in \mathbb{N}$. Tem-se que $(a-b) \mid (a^n - b^n)$.

Solução:

Pode-se escrever,

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}).$$

Logo, $(a-b) \mid (a^n - b^n)$.

Exemplo 7. Sejam a, $b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Tem-se que $(a+b) \mid (a^{2n+1} + b^{2n+1})$.

Solução:

Pode-se escrever,

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

Segue do exemplo anterior que:

$$a-(-b) \mid (a^{2n+1} - (-b)^{2n+1}) \Rightarrow a+b \mid (a^{2n+1} + b^{2n+1}).$$

Portanto, $(a+b) \mid (a^{2n+1} + b^{2n+1})$.

Exemplo 8. Sejam a, $b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Tem-se que $a+b \mid (a^{2n} - b^{2n})$.

Solução:

Escrevendo, $a+b = a-(-b)$. Tem-se, do exemplo 6 que:

$$a-(-b) \mid (a^{2n} - (-b^{2n}) \Rightarrow a+b \mid (a^{2n} - b^{2n}).$$

Portanto, $a+b \mid (a^{2n} - b^{2n})$.

Exemplo 9. (OBM) Prove que se n é ímpar, então 8 divide $n^2 - 1$.

Solução:

Suponha n ímpar, isto é, $n = 2k+1$, $k \in \mathbb{Z}$. Daí,

$$n^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k + 1 - 1 = 4k(k+1).$$

Como, k e $k+1$, são números consecutivos, tem-se do exemplo 3, que $4k(k+1) = 4 \cdot 2t = 8t$, $t \in \mathbb{Z}$.

Portanto, 8 divide $n^2 - 1$.

Exemplo 10. Mostre que $13 \mid 2^{70} + 3^{70}$.

Solução:

Escrevendo,

$$2^{70} + 3^{70} = (2^2)^{35} + (3^2)^{35} = 4^{35} + 9^{35}.$$

Pelo exemplo 7, $(a+b) \mid (a^{2n+1} + b^{2n+1})$. Assim, fazendo $a = 4$, $b = 9$ e $n = 17$, segue que:

$$4+9 \mid (4^{35} + 9^{35}) \Rightarrow 13 \mid 2^{70} + 3^{70}.$$

2.2.3 Máximo Divisor Comum

Seja a um número inteiro. Indica-se por $D(a)$ o conjunto dos divisores de a. Por exemplo:

$$D(18) = \{-1, 1, -2, 2, -3, 3, -6, 6, -9, 9, -18, 18\}.$$

Observe que para qualquer inteiro $a \neq 0$, tem-se que $D(a)$ é finito.

Seja m um número inteiro. Indica-se por $\mathbb{Z}m$ o conjunto dos múltiplos de m. Assim,

$$\mathbb{Z}m = \{0, -m, m, -2m, 2m, -3m, 3m, ...\}$$

que pode ser representado por

$$\mathbb{Z}m = \{x \cdot m; x \in \mathbb{Z}\}.$$

Por exemplo:

$$\mathbb{Z} \cdot 2 = \{x \cdot 2; x \in \mathbb{Z}\} = \{0, -2, 2, -4, 4, -6, 6, ...\}.$$

Definição 2. Um inteiro d é dito um divisor comum de a e b se $d \,|\, a$ e $d \,|\, b$.

Indica-se por $D(a, b)$ o conjunto dos divisores comuns de a e b.

Observação: Se a e b não são simultaneamente nulos, o conjunto $D(a, b)$ é finito. De fato, $D(a, b) = D(a) \cap D(b)$, onde pelo menos um dos conjuntos é finito.

Definição 3. Sejam a e b inteiros, não simultâneamente nulos. Chama-se *máximo divisor comum de a e b*, indicado por $mdc(a\,,\,b)$, o maior de seus divisores comuns. Assim,

$$mdc(a, b) = MaxD(a, b)$$

Observações:

1. Como $a \neq 0$ ou $b \neq 0$, $D(a,b)$ é finito, assim sempre possui um maior elemento e $mdc(a,b) \geq 1$.
2. Da definição, segue que $mdc(a\,,\,b) = mdc(b\,,\,a)$.

Exemplo 11. Encontre os divisores comuns e o máximo divisor comum de:

16 e 24

Primeiramente, determina-se os divisores de 16 e de 24 separadamente:

$D(16) = \{-1, -2, -4, -8, -16, 1, 2, 4, 8, 16\}$.

$D(24) = \{-1, -2, -3, -4, -6, -8, -12, -24, 1, 2, 3, 4, 6, 8, 12, 24\}$.

Em seguida, toma-se os divisores comuns.

$D(16, 24) = \{-1, -2, -4, -8, 1, 2, 4, 8\}$.

Portanto, $mdc(16, 24) = 8$

Observação: Entre todos os divisores comuns a 16 e a 24 os dois que possuem o maior módulo, -8 e 8, têm a propriedade de ser múltiplo de todos os outros divisores comuns a 16 e a 24.

Exemplo 12. Encontre os divisores comuns e o máximo divisor comum de:

15 e 45

Os divisores de 15 e de 45 são:

$D(15) = \{-1, -3, -5, -15, 1, 3, 5, 15\}$.

$D(45) = \{-1, -3, -5, -15, -45, 1, 3, 5, 15, 45\}$.

Os divisores comuns a 15 e 45 são:

$D(15, 45) = \{-1, -3, -5, -15, 1, 3, 5, 15\}$.

Portanto, $mdc(15, 45) = 15$.

Observação: Entre todos os divisores comuns a 15 e a 45 os dois que possuem o maior módulo, -15 e 15, têm a propriedade de ser múltiplo de todos os outros divisores comuns a 15 e a 45.

A seguir algumas propriedades do máximo divisor comum, $d = mdc(a\,,\,b)$, de dois números naturais a e b, não simultaneamente nulos, as quais são consequências imediatas da definição de mdc.

- Se d é o máximo divisor comum de a e b, então d também é o máximo divisor comum de a e -b, -a e b, e -a e -b.
- Se $a \neq 0$, então $mdc(a\,,\,0) = a$;
- $mdc(a\,,\,1) = 1$;
- $a \mid b \Leftrightarrow mdc(a\,,\,b) = a$.

Proposição 5. Considere m um inteiro e $\mathbb{Z}m$ o conjunto dos múltiplos de m. Tem-se que:

(i) Se α, $\beta \in \mathbb{Z}m$, então $\alpha + \beta \in \mathbb{Z}m$.

(ii) Se $\alpha \in \mathbb{Z}m\, e\, a \in \mathbb{Z}$, então $\alpha \cdot a \in \mathbb{Z}m$.

Demonstração:

(i) De fato, se α, $\beta \in \mathbb{Z}m$, existem x e y, números inteiros, tais que $\alpha = xm$ e $\beta = ym$, assim, $\alpha + \beta = xm + ym = (x + y)m$. Portanto, $\alpha + \beta \in \mathbb{Z}m$.

(ii) De $\alpha \in \mathbb{Z}m$, existe um número inteiro x tal que $\alpha = xm$. Multiplicando, α por a tem-se:

$$\alpha \cdot a = xma = xam.$$

Portanto, $\alpha \cdot a \in \mathbb{Z}m$.

■

Definição 4. Sejam m e n números inteiros. O conjunto indicado por $\mathbb{Z}m + \mathbb{Z}n$ é definido do seguinte modo:

$$\mathbb{Z}m + \mathbb{Z}n := \{x + y;\ x \in \mathbb{Z}m, y \in \mathbb{Z}n\}.$$

Exemplo 13. Observe que $m = 1 \cdot m + 0 \cdot n$, $n = 0 \cdot m + 1 \cdot n$,$-m = (-1) \cdot m + 0 \cdot n$, $-n = 0 \cdot m + (-1) \cdot n$, portanto $m, n, -m, -n \in \mathbb{Z}m + \mathbb{Z}n$.

Proposição 6. Sejam m e n números inteiros. Tem-se que:

(i) Se α, $\beta \in \mathbb{Z}m + \mathbb{Z}n$, então $\alpha + \beta \in \mathbb{Z}m + \mathbb{Z}n$

(ii) Se $\alpha \in \mathbb{Z}m + \mathbb{Z}n\, e\, a \in \mathbb{Z}$, então $\alpha \cdot a \in \mathbb{Z}m + \mathbb{Z}n$

Demonstração:

(i) Suponha que α, $\beta \in \mathbb{Z}m + \mathbb{Z}n$, então existem x, y, z e w, números inteiros, tais que $\alpha = xm + yn$ e $\beta = zm + wn$. Assim,

$$\alpha + \beta = xm + yn + zm + wn = (x + z)m + (y + w)n.$$

Portanto, $\alpha + \beta \in \mathbb{Z}m + \mathbb{Z}n$.

(ii)De $\alpha \in \mathbb{Z}m + \mathbb{Z}n$ exitem números inteiros x e y tais que $\alpha = xm + yn$. Multiplicando, α por a tem-se:

$$\alpha \cdot a = (xm + yn)a = xam + yan.$$

Portanto, $\alpha \cdot a \in \mathbb{Z}m + \mathbb{Z}n$.

■

Teorema 1. Sejam m e n inteiros não simultaneamente nulos. Então existe um inteiro $d > 0$ tal que $\mathbb{Z}m + \mathbb{Z}n = \mathbb{Z}d$.

Demonstração:

Considere o conjunto, indicado por J^+ definido do seguinte modo:

$$J^+ = \{x \in \mathbb{Z}m + \mathbb{Z}n; x > 0\}.$$

Como $m, n, -m, -n \in \mathbb{Z}m + \mathbb{Z}n$, tem-se que J^+ não é um conjunto vazio.

Para provar que $\mathbb{Z}m + \mathbb{Z}n = \mathbb{Z}d$, considere $d \in J^+$ tal que d é o menor elemento de J^+. Tem-se que $d > 0$ e existem inteiros r e s tais que $d = rm + sn$.

Tomando um elemento qualquer de $\mathbb{Z}d$, o qual é da forma $xd = x(rm + sn) = (xr)m + (xs)n$, logo também um elemento de $\mathbb{Z}m + \mathbb{Z}n$. Portanto $\mathbb{Z}d \subset \mathbb{Z}m + \mathbb{Z}n$.

Por outro lado, tome $a \in \mathbb{Z}m + \mathbb{Z}n$. Considere a divisão euclidiana de a por d,

$$a = qd + r, \text{ em que } 0 \leq r < d.$$

Suponha $r > 0$. Como a, $d \in \mathbb{Z}m + \mathbb{Z}n$ tem-se pela proposição 6 que $r = a - dq \in \mathbb{Z}m + \mathbb{Z}n$ e daí, $r \in J^+$. Uma contradição pois $r < d$ e d é o menor elemento de J^+. Concluindo assim que $r = 0$ e daí $a \in \mathbb{Z}d$. Mostrando assim, que $\mathbb{Z}m + \mathbb{Z}n \subset \mathbb{Z}d$ e a demonstração está concluída.

■

Proposição 7. Se m e n são inteiros, não simultaneamente nulos e $\mathbb{Z}m + \mathbb{Z}n = \mathbb{Z}d$, onde $d > 0$, então $d = mdc(m, n)$.

Demonstração:

Como $m, n \in \mathbb{Z}d = \mathbb{Z}m + \mathbb{Z}n$, d é um divisor comum de m e n. Além disso, como $d \in \mathbb{Z}d = \mathbb{Z}m + \mathbb{Z}n$, $d = rm + sn$, donde todo divisor comum, d', de m e n divide d, portanto d é o maior dos divisores comuns de m e n.

■

Corolário 1. (*Teorema de Bézout*) Se $d = mdc(m\,,\,n)$, então existem números inteiros x e y, tais que $d = mx + ny$.

.

Corolário 2. (*Caracterização do mdc(a,b)*) Sejam a e b números inteiros não simultaneamente nulos, $d > 0$ é o máximo divisor comum de a e b, se, e somente se:

(i) $d \,|\, a$ e $d \,|\, b$

(ii) Se d' é um número inteiro tal que $d' \,|\, a$ e $d' \,|\, b$, então $d' \,|\, d$.

A caracterização do *mdc* dada pelo corolário anterior, era utilizada por Euclides como definição para o *mdc*.

Lema 1. (Lema de Euclides) Sejam a, b, $n \in \mathbb{Z}$. Então, $mdc(a\,,\,b) = mdc(a\,,\,b - na)$.

Demonstração:

Considerando $mdc(a\,,\,b - na) = d$, segue que $d \,|\, a$ e $d \,|\, b - na$. Donde $d \,|\, na$, e $d \,|\, b - na + na$. Assim, $d \,|\, a$ e $d \,|\, b$.

Se d' é um divisor comum de a e b, então d' divide a e $b - na$ logo, d' divide d.

Portanto, $mdc(a\,,\,b) = d$.

■

O algoritmo apresentado a seguir, foi usado por Euclides a mais de dois milênios e continua sendo até hoje, uma ótima ferramenta para encontrar o máximo divisor comum de dois números inteiros.

2.2.4 Algoritmo de Euclides

Como $mdc(a, b) = mdc(a, -b) = mdc(-a, b) = mdc(-a, -b)$, vamos considerar $a, b > 0$.

Para determinar o máximo divisor comum de dois números inteiros $a, b > 0$, deve-se primeiramente efetuar a divisão euclidiana de b por a. Assim, existem únicos q_1 e r_1 inteiros tais que $b = aq_1 + r_1$, $0 \leq r_1 < a$.

Em seguida, efetua-se a divisão de a por r_1. Novamente, existem únicos q_2 e r_2 inteiros tais que $a = r_1q_2 + r_2$, $0 \leq r_2 < r_1$.

Observe que esse processo de divisão é finito, pois a lista de restos é estritamente decrescente e está contida no conjunto dos números naturais. O processo continua, até que se tenha $r_n = 0$. Como o primeiro resto ($0 \leq r_1 < a$) é menor do que a, não haverá nessa sequência mais do que a termos. Assim,

$$b = aq_1 + r_1,\ 0 \leq r_1 < a$$

$$a = r_1q_2 + r_2,\ 0 \leq r_2 < r_1$$

$$r_1 = r_2q_3 + r_3,\ 0 \leq r_3 < r_2$$

$$\vdots$$

$$r_{n-4} = r_{n-3}q_{n-2} + r_{n-2},\ 0 \leq r_{n-2} < r_{n-3}$$

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1},\ 0 \leq r_{n-1} < r_{n-2}$$

$$r_{n-2} = r_{n-1}q_n + r_n,\ 0 \leq r_n < r_{n-1}$$

Ilustrando essas divisões sucessivas, tem-se a seguinte tabela:

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

Tabela 2.1: Algoritmo de Euclides

Como $r_n = 0$, tem-se que $r_{n-1} \mid r_{n-2}$, e assim o $mdc(r_{n-2}, r_{n-1}) = r_{n-1}$.

Considerando o Lema de Euclides, conclui-se que:

$$mdc(a\,,\,b) = mdc(a\,,\,r_1) = mdc(r_1\,,\,r_2) = mdc(r_2\,,\,r_3) = \cdots = mdc(r_{n-2}\,,\,r_{n-1}) = r_{n-1}$$

Definição 5. Diz-se que dois números naturais a e b, são primos entre si, se o $mdc(a\,,\,b) = 1$.

Exemplo 14. Cálculo de máximos divisores comuns.

a)$mdc(14\,,\,35) = mdc(14\,,\,21 = 35 - 14) = mdc(14\,,\,7 = 21 - 14) = mdc(7 = 14 - 7\,,\,7) = 7$

b) $mdc(81\,,\,64) = mdc(17\,,\,64) = mdc(17\,,\,13) = 1$

c) $mdc(-1\,,\,8) = 1$

d) $mdc(4a\,,\,7a) = mdc(4a\,,\,3a) = mdc(a\,,\,3a) = mdc(a\,,\,0) = a$.

Proposição 8. Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros r e s tais que $ra + sb = 1$.

Demonstração:

($\Rightarrow$)

Sejam a e b dois inteiros primos entre si, ou seja, $mdc(a\,,\,b) = 1$. Assim, pelo *Teorema de Bézout,* existem r, s, números inteiros, tais que $ra + sb = 1$.

($\Leftarrow$)

Seja $d = mdc(a\,,\,b)$, então $d \mid a$ e $d \mid b$, implica que $d \mid (ra + sb)$, ou seja, $d \mid 1$.

Portanto, $d = 1$.

■

2.2.5 Números Primos

"*Números: eles desempenham um papel análogo ao dos átomos na estrutura da matéria. Todos os outros números podem ser obtidos através de produtos dos números primos.*"(Francisco Cesar Polcino Milies e Sónia Pitta Coelho).

Definição 6. Um número $p \in \mathbb{N}$ é chamado *número primo* se:

(i) $p > 1$ e

(ii) os únicos divisores naturais de p são 1 e p.

Proposição 9. Dados dois primos p e q e um número inteiro a qualquer, tem-se que:

(i) Se $p \,|\, q$ então $p = q$.

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

Demonstração:

(i) De q ser primo tem-se que seus únicos divisores positivos são 1 e q. Como $p \,|\, q$ segue que $p = 1$ ou $p = q$, mas p é primo, logo $p = q$.

(ii) Seja $d = mdc(p\,,\, a)$, então $d \,|\, p$ e $d \,|\, a$. De p ser primo e de $d \,|\, p$, tem-se que $d = p$ ou $d = 1$, mas por hipótese $p \nmid a$, então $d = 1$.

■

Curiosidade: Existem 168 números primos menores do que 1000. São eles:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557,

563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991 e 997.

Definição 7. Um número natural é *composto,* se for maior do que um e não for *primo.*

Portanto, se um número n é composto, existirá um divisor n_1 de n, tal que $n_1 \neq 1$ e $n_1 \neq n$. Segue que existirá um n_1 e existirá um n_2, tal que:

$$n = n_1 \cdot n_2, \text{ com } 1 < n_1 < n \text{ e } 1 < n_2 < n.$$

Proposição 10. O menor divisor maior do que 1 de qualquer número natural, $n > 1$, é necessariamente um número primo.

Demonstração:

Sejam $n \in \mathbb{N}$, $n > 1$ e d o menor divisor, maior do que 1, de n.

Se d fosse composto, então teria um divisor n' tal que, $1 < n' < d$. Daí, $n' \mid n$, o que contraria a escolha de d.

■

O primeiro matemático a produzir uma tabela de números primos foi *Eratóstenes*, no terceiro século a.C.. Para construir tal tabela, ele escrevia inicialmente uma lista com todos os números, de 1, até o maior número, n, que desejasse alcançar. Em seguida, escolhia o primeiro primo, 2, e eliminava da lista todos os seus múltiplos. Passava ao número seguinte que não fora eliminado e procedia também eliminando todos os seus múltiplos, esse procedimento se repetia até que fossem eliminados todos os múltiplos dos primos p, com $p^2 \leq n$. No final desse procedimento aparecia a tabela de primos. Este procedimento estabelecido por Eratóstenes, passou a ser chamado de *Crivo de Eratóstenes.*

O *Crivo de Eratóstenes* é baseado no seguinte Lema:

Lema 2. Todo número composto $a > 1$, admite um divisor primo p tal que $p^2 \leq a$.

Demonstração:

Suponha $a > 1$ um número composto. Seja p o menor divisor de a, maior do que 1, logo p é primo.

Escrevendo $a = p \cdot m$. Tem-se $p \leq m$ e daí $p^2 \leq pm = a$.

■

Este lema nos diz que:

Se um número $a > 1$ não for divisível por nenhum primo p, $p^2 \leq a$, então ele é primo.

Como exemplo, para elaborar uma tabela de todos os primos inferiores a 120, procede-se da seguinte forma:

- Escrevem-se todos os números de 2 a 120.
- A seguir, risca-se todos os múltiplos de 2, acima de 2, pois nenhum deles é primo. O segundo número não riscado, é o 3, que é primo.
- Risca-se então, todos os múltiplos de 3, acima de 3, pois nenhum deles é primo. O terceiro número não riscado, é o 5, que é primo.
- Risca-se então, todos os múltiplos de 5, acima de 5, pois nenhum deles é primo. O quarto número não riscado, é o 7, que é primo.
- Risca-se todos os múltiplos de 7, acima de 7, pois nenhum deles é primo. O quinto número não riscado, é o 11, que é primo.

Pronto, já se tem todos os primos inferiores a 120, sem que seja preciso continuar o procedimento.

De fato, como $11^2 = 121 > 120$, os possíveis números compostos nesta tabela, teriam como divisores, pelo menos um número primo p, $p < 11$, ou seja, 2, 3, 5 ou 7.

	2	3	4	5	6	7	8	9	10	Números Primos
11	12	13	14	15	16	17	18	19	20	2;3;5;7;11;13;17;
21	22	23	24	25	26	27	28	29	30	19;23;29;31;37;
31	32	33	34	35	36	37	38	39	40	41;43;47;53;59;
41	42	43	44	45	46	47	48	49	50	61;67;71;73;79;
51	52	53	54	55	56	57	58	59	60	83;89;97;101;
61	62	63	64	65	66	67	68	69	70	103;107;109;113
71	72	73	74	75	76	77	78	79	80	
81	82	83	84	85	86	87	88	89	90	
91	92	93	94	95	96	97	98	99	100	
101	102	103	104	105	106	107	108	109	110	
111	112	113	114	115	116	117	118	119	120	

Tabela 2.2: Crivo de Eratóstenes

Proposição 11. Sejam $a,\ b,\ c \in \mathbb{Z}$. Se $a \mid bc$ e $mdc(a,b) = 1$, então $a \mid c$.

Demonstração:

Suponha que $a \mid bc$ e $mdc(a,b) = 1$. Segue que existem inteiros r e s tais que $ra + sb = 1$, donde $rac + sbc = c$. Como $a \mid a$ e $a \mid bc$, tem-se que $a \mid c$.

Proposição 12. (*Propriedade fundamental dos números primos*) Sejam $a,\ b \in \mathbb{Z}$ e p um número primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Demonstração:

Suponha que $p \nmid a$. Então, pela proposição 9, item (ii), $mdc(p\,,\,a) = 1$, assim, pela proposição anterior, tem-se que $p \mid b$.

■

A proposição anterior aparece no livro *"Os Elementos VII"*, de *Euclides*.

Proposição 13. Sejam $n, d \in \mathbb{N}$. Se $d > 1$ e $d \,|\, n$ então $d \nmid n + 1$.

Demonstração:

De fato, se $d \,|\, n+1$, como $d \,|\, n$, teria-se $d \,|\, 1$. Isto não é possível pois $d > 1$.

■

Teorema 2. Existem infinitos números primos.

Demonstração:

Sejam $p_1, p_2, p_3, \ldots, p_s$, os s primeiros primos, $s \in \mathbb{N}^\star$. Considere o número natural

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_s + 1 > 1.$$

Seja p o menor divisor de n, maior do que 1, logo p é primo.

Como $p \,|\, p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_s + 1$, usando a proposição 13, tem-se que $p \nmid p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_s$. Logo, $p \neq p_i$, para todo $i = 1, 2, ..., s$.

Portanto existem infinitos números primos.

■

2.2.6 Congruência Módulo m

Certamente este é o ponto principal da organização de conteúdos deste trabalho. O conceito de *congruência* será muito importante para o desenvolvimento das aplicações contidas no Capítulo 3, pois além de fazer parte delas, apresenta propriedades essenciais para o estudo da *Aritmética Modular* ou *Aritmética dos Restos*, a qual é presente, de maneira fundamental, nas aplicações que serão apresentadas no próximo capítulo.

Definição 8. Sejam $a, b, m \in \mathbb{Z}$ com $m > 1$, diz-se que a é *congruente* a b *módulo* m e denota-se por $a \equiv b \, mod \, m$, se a e b possuírem o mesmo resto ao serem divididos por m.

Exemplo 15. Como $78 = 5 \cdot 15 + 3$ e $-78 = 5 \cdot (-16) + 2$, tem-se que:

$$78 \equiv 3 \, mod \, 5 \text{ e } -78 \equiv 2 \, mod \, 5.$$

Observação: Segue do Algoritmo da Divisão que todo inteiro a é congruente módulo m a um inteiro r, tal que $0 \leq r < m$.

De fato, considerando $a \in \mathbb{Z}$ e a divisão euclidiana de a por m, tem-se:

$$a = qm + r, \text{ onde } 0 \leq r < m.$$

Como $0 \leq r < m$, o resto da divisão de r por m é exatamente r.

Portanto $a \equiv r \, mod \, m$.

Observação: Se $0 \leq r_1, r_2 < m$ e $r_1 \equiv r_2 \, mod \, m$ então $r_1 = r_2$.

Exemplo 16. $16 \equiv 8 \ mod \ 4$.

De fato, pois 16 e 8 deixam resto zero quando divididos por 4.

Exemplo 17. $12 \equiv -8 \ mod \ 10$

Como $-8 = -1 \cdot 10 + 2$, tem-se que 12 e -8 deixam resto 2 quando divididos por 10.

Exemplo 18. $30 \not\equiv 10 \ mod \ 6$

De fato, pois na divisão por 6, 30 deixa resto zero, enquanto que 10 deixa resto 4.

A proposição seguinte traduz congruência módulo m como divisibilidade por m.

Proposição 14. Dados a, b, $m \in \mathbb{Z}$ com $m > 1$ tem-se que $a \equiv b \, mod \, m$, se, e somente se, $m \,|\, (b - a)$.

Demonstração:

($\Rightarrow$)

Suponha que $a \equiv b \, mod \, m$, então pela definição de congruência, tem-se que a e b deixam o mesmo resto, r, quando divididos por m. Segue que, existem inteiros q_1 e q_2, tais que:

$$a = q_1 m + r \text{ e } b = q_2 m + r, \, 0 \leq r \leq m - 1$$

Daí,

$$b - a = q_2 m + r - (q_1 m + r) = q_2 m - q_1 m = (q_2 - q_1)m \Rightarrow b - a = (q_2 - q_1)m \Rightarrow m|(b - a).$$

($\Leftarrow$)

Suponha agora que $m \,|\, (b - a)$.

Considerando a divisão euclidiana, tem-se $a = q_1 m + r_1$ e $b = q_2 m + r_2$ com $0 \leq r_1, r_2 \leq m - 1$. Daí,

$$b - a = q_2 m + r_2 - (q_1 m + r_1) = (q_2 - q_1)m + r_2 - r_1$$

Como $m \,|\, (b - a)$ e $m \,|\, (q_2 - q_1)m$, tem-se que $m \,|\, r_2 - r_1$.

Supondo sem perda de generalidade que $r_1 \leq r_2$ e observando que $0 \leq r_2 - r_1 \leq m - 1$, conclui-se que $r_2 - r_1 = 0$.

Portanto $r_2 = r_1$, donde $a \equiv b \, mod \, m$.

■

As proposições 3 (Divisibilidade) e 14 estabelecem as propriedades da *congruência módulo m*.

Proposição 15. Sejam a, b, c, d, m e r, números inteiros, com $m > 1$ e $r \geq 1$. Então:

(i) $a \equiv a \, mod \, m$.

(ii) Se $a \equiv b \, mod \, m$, então $b \equiv a \, mod \, m$.

(iii) Se $a \equiv b \, mod \, m$ e $b \equiv c \, mod \, m$, então $a \equiv c \, mod \, m$.

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

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

(vi) Se $a \equiv b \, mod \, m$, então $a^r \equiv b^r \, mod \, m$.

$(vii)(a + c) \equiv (b + c) \; mod \, m$ se, e somente, se $a \equiv b \, mod \, m$.

$(viii)$ Se $ab \equiv ac \, mod \, m$ e $mdc(a\,,\, m) = 1$, então $b \equiv c \, mod \, m$.

Demonstração:

(i) Basta observar que $m \,|\, (a - a) = 0$.

(ii) Se $a \equiv b \, mod \, m$, então $m \,|\, (b - a)$, donde $m \,|\, (a - b)$, o que implica que $b \equiv a \, mod \, m$.

(iii) Suponha que $a \equiv b \, mod \, m$ e $b \equiv c \, mod \, m$. Daí, $m \,|\, (a-b)$ e $m \,|\, (c-b)$, donde $m \,|\, (a-c)$.

Portanto $a \equiv c \, mod \, m$.

(iv) Suponha que $a \equiv b \, mod \, m$ e $c \equiv d \, mod \, m$. Tem-se que $m \,|\, (b - a)$ e $m \,|\, (d - c)$, donde:

$$m \,|\, ((b - a) + (d - c)) = b + d - (a + c).$$

Portanto, $a + c \equiv b + d \, mod \, m$.

(v) Suponha que $a \equiv b \, mod \, m$ e $c \equiv d \, mod \, m$. Tem-se que $m \,|\, (b-a)$ e $m \,|\, (d-c)$, donde $m \,|\, d(b-a)$ e $m \,|\, a(d-c)$. Daí, $m \,|\, (d(b-a) - a(d-c))$, ou seja, $m|(ac-bd)$.

Portanto, $ac \equiv bd \, mod \, m$.

(vi) Suponha que $a \equiv b \, mod \, m$. Aplicando o item (v) desta proposição $r-1$ vezes:

$$r \, congruências \begin{cases} a \equiv b \, mod \, m \\ a \equiv b \, mod \, m \\ \quad \vdots \\ a \equiv b \, mod \, m \end{cases} \Rightarrow a^r \equiv b^r \, mod \, m.$$

(vii) $a + c \equiv b + c \, mod \, m \Leftrightarrow m \,|\, (a + c - (b + c)) \Leftrightarrow m \,|\, (a - b) \Leftrightarrow a \equiv b \, mod \, m$.

$(viii)$ Suponha que $ab \equiv ac \, mod \, m$. Então,

$$m \,|\, (ac - ab) \Rightarrow m \,|\, a(c - b)$$

Como $mdc(a\,,\, m) = 1$, tem-se necessariamente que $m \,|\, (c - b)$.

Portanto, $b \equiv c \, mod \, m$.

■

2.2.7 Aritmética dos Restos

As propriedades das congruências podem facilitar muito o cálculo do resto de uma divisão de dois números inteiros. A determinação do resto da divisão de 20 por 7 não intimida em nada, mas e se a tarefa for descobrir o resto da divisão de 7^{50} por 11 por exemplo? O que parecia simples, pode tomar proporções gigantescas de dificuldade, se não forem utilizadas, para a solução deste problema, algumas das propriedades supracitadas.

Exemplo 19. Encontre o resto da divisão de 7^{50} por 11.

Solução:

Comece analisando algumas congruências módulo 11.

$$\begin{cases} 7 \equiv 7\, mod 11 & (1) \\ 7^2 = 49 \equiv 5\, mod 11 & (2) \\ 7^3 \equiv 35 \equiv 2\, mod 11 & (3) \\ 7^4 \equiv 5^2 \equiv 25 \equiv 3\, mod 11 & (4) \\ 7^5 \equiv 21 \equiv 10 \equiv -1\, mod 11 & (5) \\ 7^{10} \equiv (-1)^2 \equiv 1\, mod 11 & (6) \end{cases}$$

Repare que a congruência (6) pode ser obtida da congruência (5) utilizando-se o item (vi) da proposição 15, elevando-a ao quadrado.

Agora basta elevar a congruência (6) a quinta potência,

$$(7^{10})^5 \equiv 1^5 mod 11 \Leftrightarrow 7^{50} \equiv 1\, mod 11.$$

Portanto, o resto da divisão de 7^{50} por 11 é 1.

Exemplo 20. Encontre o resto da divisão de 5^{21} por 127.

Solução:

Tem-se que:

$$5^3 \equiv 125 \equiv -2\, mod 127.$$

Do item (vi) da proposição 15 e da congruência acima, tem-se que:

$$(5^3)^7 \equiv (-2)^7 \equiv -128 \equiv -1 \equiv 126\, mod 127.$$

Portanto, o resto da divisão de 5^{21} por 127 é 126.

Exemplo 21. Determine o resto da divisão do número $10^{10} + 10^{10^2} + 10^{10^3} + \cdots + 10^{10^{100}}$ por 7.

Sabe-se que:

$$10 \equiv 3\, mod\, 7 \Rightarrow 10^2 \equiv 9 \equiv 2\, mod\, 7 \Rightarrow 10^{10} \equiv 32 \equiv 4\, mod\, 7 \text{ e}$$

$$\begin{cases} 4 \equiv -3\, mod\, 7 \\ 4^2 \equiv 2\, mod\, 7 \\ 4^4 \equiv 4\, mod\, 7 \\ 4^5 \equiv 2\, mod\, 7 \\ 4^{10} \equiv 4\, mod\, 7 \end{cases}$$

Dessa forma,

$$10^{10} \equiv 4^{10} \equiv 4\, mod\, 7$$

$$10^{10^2} = (10^{10})^{10} \equiv 4^{10} \equiv 4\, mod\, 7.$$

Continuando tem-se que:

$$10^{10} \equiv 10^{10^2} \equiv 10^{10^3} \equiv \cdots \equiv 10^{10^{100}} \equiv 4\, mod\, 7.$$

Logo,

$$10^{10} + 10^{10^2} + 10^{10^3} + \cdots + 10^{10^{100}} \equiv \underbrace{4 + 4 + 4 + \cdots + 4}_{100\, parcelas} \equiv 400 \equiv 1\, mod\, 7.$$

Portanto, o resto da divisão de $10^{10} + 10^{10^2} + 10^{10^3} + \cdots + 10^{10^{100}}$ por 7 é 1.

Exemplo 22. Qual é o algarismo das unidades do número $2^{100} + 13^{16}$?

Solução:

Para encontrar o algarismo das unidades de qualquer número, basta encontrar o resto da divisão desse número por 10. Por isso, usa-se a congruência módulo 10, para encontrar o algarismo das unidades de $2^{100} + 13^{16}$.

$$\begin{cases} 2 \equiv 2\, mod 10 & (1) \\ 2^2 \equiv 4\, mod 10 & (2) \\ 2^5 \equiv 2\, mod 10 & (3) \\ 2^{10} \equiv 4\, mod 10 & (4) \end{cases} \text{e} \begin{cases} 4^2 \equiv 6\, mod 10 & (5) \\ 4^4 \equiv 6\, mod 10 & (6) \\ 4^5 \equiv 4\, mod 10 & (7) \\ 4^{10} \equiv 6\, mod 10 & (8) \end{cases}.$$

Daí,

$$(2^{10})^{10} \equiv\ 4^{10}\ \equiv\ 6\, mod\, 10 \Rightarrow 2^{100} \equiv\ 6\, mod\, 10.\ (9)$$

Agora,

$$\begin{cases} 13 \equiv 3\, mod 10 & (10) \\ 13^2 \equiv 9\, mod 10 & (11) \\ 13^4 \equiv 1\, mod 10 & (12) \\ 13^{16} \equiv 1\, mod 10 & (13) \end{cases}$$

Repare que ficou muito fácil determinar as congruências (11), (12) e (13), já que bastou para isso, elevá-las uma a uma ao quadrado para encontrar a seguinte.

Finalmente, basta usar o item (iv) da proposição 15 nas congruências (9) e (13) para obter que:

$$2^{100} + 13^{16} \equiv\ 6 + 1\ \equiv\ 7\, mod\, 10.$$

Portanto, o algarismo das unidades do número $2^{100} + 13^{16}$ é o 7.

Capítulo 3

Aplicações de Congruência Para o Ensino Básico

"*O assunto, além de ser intrinsecamente interessante, tem a virtude de mesclar conceitos e técnicas importantes de Álgebra com aplicações imediatas na vida real*" (Abramo Hefez e Maria Villela).

Cada uma das aplicações de *Aritmética Modular* que serão citadas neste capítulo tem sua importância, seja ela por colaborar com a solução de algum problema da atualidade, seja agilizando o processo de resolução de determinados problemas da matemática do ensino básico.

Citaremos aqui aplicações de *Aritmética Modular* que poderão ser utilizadas por professores de matemática da Educação Básica, principalmente para aqueles que atuam no ensino médio, como forma de contextualizar a matemática com as necessidades do dia-a-dia.

3.1 Critério de Divisibilidade

Os critérios de divisibilidade que são encontrados atualmente nos livros didáticos da Educação Básica, consistem de diversas regras, que quando aplicadas a um número inteiro,

permitem determinar se o número é ou não divisível por um determinado número. A questão é, as regras são tantas, que se torna mais fácil o aluno realizar o cálculo do que ter que decorar todas aquelas regras.

A proposta feita aqui, é que seja usada congruência (*Aritmética dos Restos*) para a dedução das regras ou simplesmente a aplicação da *Aritmética Modular* em cada caso particular, sem se preocupar com as regras.

Dados dois números inteiros, a e b, como pode-se decidir sobre a divisibilidade destes números, ou seja, se $a \mid b$ ou se $a \nmid b$? Veja um exemplo bem simples.

Exemplo 23. Verifique se 38 é divisível por 6, usando congruências (*Aritmética dos Restos*).

Solução:

Para que o 6 divida 38, deve-se ter o resto da divisão de 38 por 6 igual a zero.

Pode-se escrever, $38 = 3 \cdot 10 + 8$.

Tem-se que, $3 \equiv 3 \, mod \, 6$.

Multiplicando essa congruência por 10 tem-se, $30 \equiv 0 \, mod \, 6$.

Somando 8 a esta última congruência, tem-se, $38 \equiv 8 \equiv 2 \, mod \, 6$.

Portanto, o resto da divisão de 38 por 6 é 2, logo $6 \nmid 38$.

Exemplo 24. Verifique se 230 é divisível por 2.

Solução:

Veja que pode-se escrever 230 da seguinte forma:

$$230 = 2 \cdot 10^2 + 3 \cdot 10 + 0.$$

Aplicando propriedades de congruências, tem-se:

$$2 \cdot 10^2 + 3 \cdot 10 + 0 \equiv 0 \, mod \, 2.$$

Portanto, 230 é divisível por 2.

Exemplo 25. Generalizando o exemplo anterior. Considere $a = a_n a_{n-1} \dots a_1 a_0$ escrito na representação decimal.

Assim, $a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, $n \in \mathbb{N}$. Tem-se que:

$$\begin{cases} 10 \equiv 0 \, mod \, 2 \\ 10^2 \equiv 0 \, mod \, 2 \\ 10^3 \equiv 0 \, mod \, 2 \\ \cdots\cdots\cdots\cdots \\ 10^n \equiv 0 \, mod \, 2 \end{cases}$$

Multiplicando uma a uma as congruências acima, por $a_1, a_2, \cdots, a_n$, respectivamente, tem-se que:

$$\begin{cases} a_1 \cdot 10 \equiv 0 \, mod 2 \\ a_2 \cdot 10^2 \equiv 0 \, mod 2 \\ a_3 \cdot 10^3 \equiv 0 \, mod 2 \\ \cdots\cdots\cdots\cdots \\ a_n \cdot 10^n \equiv 0 \, mod 2. \end{cases}$$

Além disso, $a_0 \equiv a_0 \mod 2$. Agora somando, todas essas congruências, obtêm-se que:

$$a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n \equiv a_0 \, mod \, 2$$

ou seja,

$$a \equiv a_0 mod \, 2.$$

Assim, um número inteiro $a = a_n a_{n-1} \dots a_1 a_0$, é divisível por dois se, e somente se, a_0 for divisível por dois, passando a ser este um critério de divisibilidade por dois.

Exemplo 26. Verifique se 36127 é divisível por 3.

Solução:

Pode-se escrever 36127 da seguinte maneira:

$$36127 = 3 \cdot 10^4 + 6 \cdot 10^3 + 1 \cdot 10^2 + 2 \cdot 10 + 7$$

Aplicando a congruência módulo 3 e observando que $10 \equiv 1 \, mod \, 3$, tem-se que:

$$32127 \equiv 3 + 6 + 1 + 2 + 7 \equiv 1 \, mod \, 3.$$

Portanto, 36127 não é divisível por 3 pois deixa resto 1.

Exemplo 27. Generalizando o exemplo anterior.

Considere $a = a_n a_{n-1} \ldots a_1 a_0 = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, $n \in \mathbb{N}$. Neste caso, $10 \equiv 1 \, mod \, 3$ e daí, usando as propriedades das congruências, tem-se que:

$$a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n \equiv a_0 + a_1 + a_2 + \cdots + a_n mod \, 3.$$

ou seja,

$$a \equiv a_0 + a_1 + a_2 + \cdots + a_n \ mod \ 3.$$

Portanto, $a = a_n a_{n-1} \ldots a_1 a_0$ é divisível por 3 se, e somente se, $a_0 + a_1 + a_2 + \cdots + a_n$ é divisível por 3.

Veja mais dois exemplos, agora para encontrar o critério de divisibilidade por 11 e uma vez mais, mostra-se que qualquer critério pode ser determinado usando um único método.

Exemplo 28. Verifique se 234 é divisível por 11.

Solução:

Tem-se que:

$$234 = 2 \cdot 10^2 + 3 \cdot 10 + 4.$$

Aplicando congruência módulo 11 e observando que $10 \equiv -1 \, mod \, 11$, obtêm-se que:

$$234 \equiv 2 - 3 + 4 \equiv 3 \, mod \, 11.$$

Portanto, 234 não é divisível por 11 pois deixa resto 3.

Exemplo 29. Generalizando o exemplo anterior.

Dado $a = a_n a_{n-1} \ldots a_1 a_0 = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, $n \in \mathbb{N}$. Tem-se, neste caso que $10 \equiv -1 \, mod \, 11$. Aplicando as propriedades das congruências, segue que:

$$a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n mod \, 11.$$

ou seja,

$$a \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n \ mod \ 11.$$

Portanto, $a = a_n a_{n-1} \ldots a_1 a_0$ é divisível por 11 se, e somente se, $a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n$ é divisível por 11.

Dessa forma, conclui-se que, para determinar se um número inteiro a é divisível por um número inteiro m, uma boa saída pode ser estudar a *congruência módulo m.*

3.2 A Prova dos Noves

A *"prova dos noves"* ou *"regra dos noves fora"*, é um método para identificar erros em operações com números naturais. É um exemplo bem simples de aplicação das propriedades de congruências.

Primeiramente, "*tirar os noves fora*"de um número natural n, significa encontrar o resto da divisão de n por 9.

Por exemplo, para $n = 739571$, tem-se:

$$739571 = 7{\cdot}10^6{+}3{\cdot}10^5{+}9{\cdot}10^4{+}5{\cdot}10^3{+}7{\cdot}10^2{+}1 \equiv 7{+}3{+}9{+}5{+}7{+}1 \equiv 1{+}0{+}4 \equiv 5\, mod\, 9.$$

Outro exemplo,

$$75932 \equiv 7+5+9+3+2 \equiv 3+0+5 \equiv 8\, mod\, 9.$$

Considere a seguinte conta $737 \cdot 246 = 181302$. A regra é a seguinte:

Tire os noves fora dos números envolvidos. Assim,

737 "noves fora"8

246 "noves fora"3

Multiplique $8 \cdot 3$ e tire os "noves fora" obtendo $24 \equiv 6\, mod\, 9$.

Se a conta estiver correta ao tirar os "noves fora"do resultado, deve ser encontrado também o número 6.

De fato, 181302 "noves fora"é igual a 6.

Resumindo,

$$\begin{array}{ccc} 737 & \equiv & 8 \\ \underline{246} & \equiv & \underline{3} \\ \underbrace{181302}_{\equiv 6} & = & \underbrace{24}_{\equiv 6} \end{array}$$

Isto é apenas um indício de que o resultado está correto pois, se fossem trocados dois algarismos, por exemplo, 181203 ao invés de 181302, teríamos depois "dos noves fora" também o número 6.

Considere que a conta foi feita dando o resultado: "$737 \cdot 246 = 181402$".

Aplicando a regra:

737"noves fora"8

246 "noves fora"3

3.8 "noves fora"6

181.402 "noves fora "7

Resumindo,

$$\begin{array}{ccc} 737 & \equiv & 8 \\ \underline{246} & \equiv & \underline{3} \\ \underbrace{1813402}_{\equiv 7} & \neq & \underbrace{24}_{\equiv 6} \end{array}$$

Podemos afirmar com certeza que a conta está errada.

A regra é explicada, usando as propriedades das congruências.

De fato:

Se $a \equiv a' mod\, m$ e $b \equiv b' mod\, m$ então $ab \equiv a' \cdot b' \, mod\, m$.

Voltando ao exemplo onde $737 \cdot 246 = 181402$

Como $737 \equiv 8\, mod\, 9$ e $246 \equiv 3\, mod\, 9$, tem-se que $737 \cdot 246 \equiv 3 \cdot 8\, mod\, 9$.

Neste exemplo, $181402 \equiv 3 \cdot 8\, mod\, 9$, e daí $7 \equiv 6\, mod\, 9$, o que mostra que a conta está errada.

3.3 Código de Barras

Uma das aplicações importantes e interessantes da *Aritmética Modular* é aquela que explica os misteriosos códigos de barras, encontrados por exemplo, nos produtos de um supermercado.

Numa definição técnica, o código de barras é uma representação gráfica de dados. Ele permite uma rápida captação de dados, proporciona velocidade nas transações, precisão nas informações e admite atualização em tempo real e tudo isso implica em maior controle, diminuição de erros, gerenciamento remoto, garantindo velocidade no atendimento de pedidos e clientes, além da significativa redução nos custos.

Tendo em vista todas as vantagens proporcionadas pela inserção dos códigos de barras, principalmente na área comercial, fica evidente a motivação para trabalhar tal assunto em sala de aula, pois é um bom exemplo da aplicação de *Aritmética Modular*.

Os códigos de barras são hoje utilizados no mundo todo e servem para fazer identificações em diversas áreas como, indústria, comércio, bancos, bibliotecas, hospitais, bancos de sangue, correios, transportes, controles de acesso entre outros.

Os primeiros estudos realizados com intuito de criar códigos que facilitassem e agilizassem os processos de comercialização de produtos foram feitos em 1952 por Joseph Woodland e Bernard Silver. Os códigos criados por Woodland e Silver eram formados por circunferências concêntricas de espessura variável.

O código de barras, no formato de listras verticais alternadas nas cores preta e branca e com um número colocado abaixo das listras, da forma como conhecemos hoje, foi elaborado pela primeira vez por George J. Laurer já na década de setenta. O código apresentado por Laurer consistia de 12 dígitos (número colocado abaixo das listras) e foi aceito em 1973 quando recebeu o nome de Código Universal de Produtos "UPC" (*Universal Product Code*). Estados Unidos e Canadá foram os países que adotaram o código UPC.

Figura 3.3.1: UPC

Em 1976, Laurer acrescentou um dígito ao código, para que dessa forma, fosse possível identificar também o país de origem dos produtos classificados com o código de barras. O novo código, com treze dígitos, recebeu o nome de EAN-13 (European Article Numbering system).

Figura 3.3.2: EAN-13

Neste trabalho, serão explicados como são feitos a leitura, o cálculo do dígito verificador e a detecção de erros, para os códigos de barras EAN-13 e UPC.

3.3.1 Entendendo as Barras

O código de barras é uma representação do número no formato de barras, de forma que uma leitora óptica leia e interprete qual é o número representado.

Os códigos de barras são formados por sequências de barras verticais de cores alternadas, pretas e brancas, com larguras que variam entre, fina, média, grossa, ou muito grossa, que identificam o número que aparece abaixo das barras. A leitura das barras é feita através da tabela a seguir, que define como deve-se ler ou interpretar cada uma das barras.

Listras	Finas	Médias	Grossas	Muito Grossas
Branca	0	00	000	0000
Preta	1	11	111	1111

Tabela 3.1: Significado das listras

Os códigos EAN-13 possuem três blocos de barras um pouco mais compridas que as outras, cada bloco contendo três barras, os quais servem de delimitadores e não são interpretados como números.

Os códigos de barras UPC, possuem os mesmos delimitadores que o EAN-13, representados por barras mais compridas, com a diferença que o primeiro e o último dígito estão codificados com barras do mesmo comprimento das dos delimitadores.

3.3.2 Entendendo os Números e as Barras no UPC e no EAN-13

Considere primeiramente os códigos UPC. Inicialmente é feita a leitura referente a espessura e a cor das barras, com auxilio da tabela 3.1, sendo que, a cada quatro barras

será associada uma sequência de 7 dígitos entre zeros e uns. Cada dígito de $0; 1; 2; ...; 9$ é representado por uma sequência de zeros e uns, conforme a tabela abaixo. O numero representado pelas sequências será lido por um leitor óptico, respeitando a posição, esquerda ou direita de cada dígito.

Dígito	Lado Esquerdo	Lado Direito
0	0001101	1110010
1	0011001	1100110
2	0010011	1101100
3	0111101	1000010
4	0100011	1011100
5	0110001	1001110
6	0101111	1010000
7	0111011	1000100
8	0110111	1001000
9	0001011	1110100

Tabela 3.2: UPC

Exemplo 30. O número $\underbrace{036000}_{lado\,esquerdo} - \underbrace{291452}_{lado\,direito}$ será escrito como:

0001101 - 0111101 - 0101111 - 0001101 - 0001101 - 0001101 - 1101100 - 1110100 - 1110010 - 1011100 - 1001110 - 1101100

e representado graficamente:

Figura 3.3.3: UPC

A principal diferença entre os códigos UPC e EAN-13, está na quantidade de dígitos, já que o UPC possuí 12 algarismos, enquanto que o EAN-13, possui 13.

Para o sistema EAN-13, o mais usado atualmente, deve-se ter a seguinte interpretação: os primeiros dois ou três dígitos são usados na identificação do país de origem. No Brasil por exemplo são três dígitos, 789, que identificam a origem dos produtos fabricados aqui. Os próximos quatro ou cinco dígitos servem para identificar a empresa, enquanto que os cinco números seguintes representam o código do produto, e por fim, o último dígito é o digito verificador, conforme ilustra a figura a seguir retirada de [18].

Figura 3.3.4: Código de Barras - EAN-13

Como no sistema UPC, no sistema EAN-13 cada dígito é representado por uma sequência de zeros e uns. Para que uma mesma leitora possa ser usada nos dois sistemas,

o primeiro dígito que aparece no sistema EAN-13 é determinado pelos 6 dígitos seguintes. Para que isso possa ser feito, é acrescentada mais uma representação para cada dígito do lado esquerdo, conforme a tabela abaixo.

Dígito	Lado Esquerdo (Ímpar)	Lado Esquerdo (Par)	Lado Direito
0	0001101	0100111	1110010
1	0011001	0110011	1100110
2	0010011	0011011	1101100
3	0111101	0100001	1000010
4	0100011	0011101	1011100
5	0110001	0111001	1001110
6	0101111	0000101	1010000
7	0111011	0010001	1000100
8	0110111	0001001	1001000
9	0001011	0010111	1110100

Tabela 3.3: EAN-13

Ao iniciar a interpretação das barras do lado esquerdo do código, de acordo com a tabela 3.1, tem-se que, a cada quatro barras, uma sequência de sete dígitos será formada com zeros e uns. Caso tal sequência tenha uma quantidade ímpar de uns, então deve-se procurar na tabela 3.3 o algarismo correspondente a tal sequência, na coluna referente ao lado esquerdo (ímpar), caso contrário, procura-se na coluna lado esquerdo (par). O restante da leitura, feita do lado direito das barras, é análoga a feita pra o sistema UPC.

Exemplo 31. O número que aparece na figura 3.2.2 (código EAN-13) é 4-891668-326689.

Tem-se, segundo a tabela 3.1, as seguintes sequências de dígitos:

Lado Esquerdo		Lado Direito	
1º	8↔0110111 (quantidade ímpar de uns)	7º	3↔1000010
2º	9↔0010111 (quantidade par de uns)	8º	2↔1101100
3º	1↔0011001 (quantidade ímpar de uns)	9º	6↔1010000
4º	6↔0101111 (quantidade ímpar de uns)	10º	6↔1010000
5º	6↔0000101 (quantidade par de uns)	11º	8↔1001000
6º	8↔0001001 (quantidade par de uns)	12º	9↔1110100

A paridade da quantidade de números uns que aparecem na representação dos seis primeiros dígitos, determinará o primeiro dígito, conforme a tabela abaixo.

Dígito Inicial	1º	2º	3º	4º	5º	6º
0	Ímpar	Ímpar	Ímpar	Ímpar	Ímpar	Ímpar
1	Ímpar	Ímpar	Par	Ímpar	Par	Par
2	Ímpar	Ímpar	Par	Par	Ímpar	Par
3	Ímpar	Ímpar	Par	Par	Par	Ímpar
4	Ímpar	Par	Ímpar	Ímpar	Par	Par
5	Ímpar	Par	Par	Ímpar	Ímpar	Par
6	Ímpar	Par	Par	Par	Ímpar	Ímpar
7	Ímpar	Par	Ímpar	Par	Ímpar	Par
8	Ímpar	Par	Ímpar	Par	Par	Ímpar
9	Ímpar	Par	Par	Ímpar	Par	Ímpar

Tabela 3.4: Ordem de codificação EAN-13

No exemplo anterior a sequência encontrada foi:

ímpar, par, ímpar, ímpar, par, par

e de acordo com a tabela 3.4, o dígito inicial é o 4, o que realmente ocorre.

Observação: Nos dois sistemas, UPC e EAN-13, os dígitos têm codificações diferentes dependendo do lado que se encontram, se estiverem do lado esquerdo, iniciam com zeros, se estiverem do lado direito, iniciam com uns. Isso permite que a leitura mesmo sendo feita de cabeça para baixo, produzirá o mesmo número.

3.3.3 O Dígito de Verificação

Quando algum problema impedir a leitura do código, por exemplo, alguma imperfeição na figura das barras, o operador terá que digitar a sequência de números do código e pode ser que ocorram erros. O dígito de verificação é um recurso para a detecção de alguns erros.

Considere $a_1, a_2, ..., a_{12}, a_{13}$ a sequência de dígitos de um determinado código de barras EAN-13. Como já foi dito, os primeiros doze dígitos servem para identificar o país de origem, o fabricante, além de especificar o produto, ou seja, esses dígitos já são pré estabelecidos. Nos dois sistemas, EAN-13 e UPC, o último dígito, ou dígito de verificação, será determinado pelos primeiros dígitos, os doze primeiros, no caso do sistema EAN-13 e pelos onze primeiros dígitos, no caso do sistema UPC.

Considere o sistema EAN-13. Chamando de X o décimo terceiro dígito e escrevendo a sequência de dígitos em forma de vetor, tem-se $\alpha = (a_1, a_2, \cdots, a_{12}, X)$

O sistema EAN-13, utiliza um vetor fixo, ω, chamado vetor de pesos, dado por:

$$\omega = (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1).$$

Calculando o "produto escalar" de ambos vetores, tem-se:

$$\alpha \cdot \omega = (a_1, a_2, ..., a_{12}, X).(1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1) = a + 3a_2 + \cdots + 3a_{12} + X.$$

O dígito de verificação, $X \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, é tal que $\alpha \cdot \omega \equiv 0 \ mod \ 10$.

Caso o código seja um UPC, ou seja, tenha 12 dígitos, então a única modificação será no vetor de pesos que terá uma coordenada a menos e começará com 3:

$$\omega = (3,\ 1,\ 3,\ 1,\ 3,\ 1,\ 3,\ 1,\ 3,\ 1,\ 3,\ 1).$$

Exemplo 32. Considere o número do código de barras da figura 3.3.4 em que X é o dígito de verificação. Determine o valor de X.

Solução:

Seja então, 489166832668X o número referente ao código de barras da figura 3.3.4. Colocando os dígitos do código na primeira linha de uma tabela, o vetor de pesos na segunda linha da mesma tabela e efetuando o produto da primeira pela segunda linha, tem-se:

Dígitos do código de barras	4	8	9	1	6	6	8	3	2	6	6	8	X
Vetor de Pesos EAN-13	1	3	1	3	1	3	1	3	1	3	1	3	1
Resultado do produto	4	24	9	3	6	18	8	9	2	18	6	24	X

Deve-se ter $\alpha \cdot \omega = 4+24+9+3+6+18+8+9+2+18+6+24+X \equiv 0\, mod\, 10$.

Que é o mesmo que $\underbrace{6+24+6+24+18+2}_{\equiv 0\, mod 10}+4+3+8+9+9+18+X \equiv 0\, mod\, 10$.

Daí,

$$4+8+9+9+18+3+X = \underbrace{12+18}_{\equiv 0\, mod 10}+18+3+X \equiv 0\, mod\, 10 \Rightarrow 21+X \equiv 0\, mod\, 10$$

O valor do dígito de verificação $X \in \{0,1,2,3,4,5,6,7,8,9\}$ deve ser tal que,

$$(21+X) \equiv 0\, mod\, 10.$$

Logo, $X = 9$ é o dígito de verificação para o código de barras da figura 3.2.4, e isso realmente ocorre.

3.3.4 Erros Detectáveis e Não Detectáveis

Caso, durante a leitura do código de barras, ocorra algum problema com o leitor óptico, ou um outro problema que impeça a leitura óptica do código, será necessário que o

operador realize a leitura manualmente, ou seja, ele terá que digitar os algarismos localizados logo abaixo do código de barras. Nesse momento, poderá ocasionalmente, ocorrer uma "falha humana" e o número digitado pode não corresponder exatamente ao número contido no código de barras. Se algum dos algarismos for inserido incorretamente ou fora da ordem certa, é bem provável que o resultado da verificação não seja um número congruente a zero módulo dez e então o processador emitirá um sinal sonoro alertando o erro de digitação. Cabe aqui ressaltar, que a possibilidade de que uma falha na digitação ocorra e não seja detectada é muito pequena. Veja a seguir em quais situações isso acontece.

Se o operador digitar um único algarismo errado, comete um erro chamado de erro singular, certamente o produto $\alpha \cdot \omega$, não será congruente a zero módulo dez e então o erro será detectado. Caso o operador digite dois ou mais algarismos de modo errado, há possibilidade dos erros se compensarem uns aos outros e o resultado de $\alpha \cdot \omega$ ser congruente a zero módulo dez. Nesse caso o erro não será detectado.

Além dos erros citados acima, podem ocorrer outros tipos de erros, como por exemplo a troca da posição dos algarismos digitados, chamados erros de transposição. Um erro de transposição muito comum, é o erro de transposição adjacente, que ocorre quando a ordem de dois números consecutivos é trocada. Nesse caso, o erro pode ou não ser detectado.

Exemplo 33. Considere o número 4891668326689 do código de barras da figura 3.3.4. Verifique em cada caso, se o erro seria detectado, caso o número fosse digitado das seguintes formas:

a) $48916683266\underbrace{98}$

Como o código é um EAN-13, o vetor de pesos utilizado será:

$$\omega = (1,\ 3,\ 1,\ 3,\ 1,\ 3,\ 1,\ 3,\ 1,\ 3,\ 1,\ 3,\ 1).$$

Além disso, $\alpha = (4, 8, 9, 1, 6, 6, 8, 3, 2, 6, 6, 9, 8)$. Assim,

$$\alpha \cdot \omega = 4 + 24 + 9 + 3 + 6 + 18 + 8 + 9 + 6 + 6 + 18 + 9 + 24 = 144.$$

Como $144 \not\equiv 0 \, mod \, 10$, o erro será detectado.

b) $489\underbrace{61}68326689$

Neste caso $\alpha = (4, 8, 9, 6, 1, 6, 8, 3, 2, 6, 6, 8, 9)$. Assim,

$$\alpha \cdot \omega = 4 + 24 + 9 + 18 + 1 + 18 + 8 + 9 + 2 + 18 + 6 + 24 + 9 = 150.$$

Como $150 \equiv 0 \, mod \, 10$, o erro não será detectado.

Para as proposições a seguir, basta serem feitas demonstrações para o sistema EAN-13, pois para o sistema UPC, as demonstrações seriam análogas.

Proposição 16. Uma transposição adjacente é detectada pelo EAN-13 e pelo UPC, se e somente se, $|a_i - a_{i+1}| \neq 5$.

Demonstração:

Seja $a_1, a_2, ..., a_i, a_{i+1}, \ldots, a_{12}, a_{13}$, uma sequência de dígitos pela qual um determinado produto está identificado no sistema EAN-13. Tem-se que:

$$a_1 + 3a_2 + ... + 3a_i + a_{i+1} + \ldots + 3a_{12} + a_{13} \equiv 0 \, mod \, 10 \qquad (1)$$

Suponha que essa sequência tenha sido erroneamente digitada da seguinte forma:

$$a_1, a_2, ..., a_{i+1}, a_i, \ldots, a_{12}, a_{13}.$$

O erro de transposição não será detectado, se, e somente se:

$$a_1 + 3a_2 + ... + 3a_{i+1} + a_i + \ldots + 3a_{12} + a_{13} \equiv 0 \, mod \, 10 \qquad (2)$$

Fazendo (2) - (1) tem-se,

$$2a_i - 2a_{i+1} \equiv 0 \, mod \, 10 \Leftrightarrow 2\,(a_i - a_{i+1}) \equiv 0 \, mod \, 10$$

Observe que sempre $|a_i - a_{i+1}| \leq 9$, já que a_i e a_{i+1}são números entre zero e 9. Daí,

$$2\,(a_i - a_{i+1}) \equiv 0\, mod\, 10 \Leftrightarrow |a_i - a_{i+1}| = 5$$

Portanto, conclui-se que o erro por transposição adjacente será detectado se, e somente se, $|a_i - a_{i+1}| \neq 5$.

■

Proposição 17. Uma transposição não adjacente do tipo,

$$..., a_i, a_{i+1}, a_{i+2} \ldots \longmapsto ..., a_{i+2}, a_{i+1}, a_i \ldots$$

não é detectada pelos sistemas EAN-13 e UPC.

Demonstração:

Considere $a_1, a_2, ..., a_i, a_{i+1}, a_{i+2}, \ldots, a_{12}, a_{13}$, uma sequência de dígitos pela qual um determinado produto está identificado no sistema EAN-13. Tem-se que:

$$a_1 + 3a_2 + ... + a_i + 3a_{i+1} + a_{i+2} + \ldots + 3a_{12} + a_{13} \equiv 0\, mod\, 10.$$

Realizando a verificação de erro em um código que sofreu uma transposição não adjacente do tipo da do enunciado, tem-se a mesma soma:

$$a_1 + 3a_2 + ... + a_{i+2} + 3a_{i+1} + a_i + \ldots + 3a_{12} + a_{13} \equiv 0\, mod\, 10.$$

Portanto, os códigos UPC e EAN-13, não são capazes de identificar erros de transposição não adjacente das do tipo do enunciado.

■

Do fato que $\alpha = (a_1, a_2, \cdots, a_{12}, a_{13})$ e $\omega = (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$, para o sistema EAN-13, e $\alpha = (a_1, a_2, \cdots, a_{12})$ e $\omega = (3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$, para o sistema UPC, tem-se que, se a_i e a_j são dois dígitos quaisquer, de um dos dois sistemas, caso a

diferença $i-j$ seja par, a_i e a_j terão o mesmo peso, um ou três. Caso a diferença $i-j$ seja ímpar, a_i e a_j não terão o mesmo peso, ou seja, um terá peso um, e o outro terá peso três. Com isto, para a demonstração do resultado a seguir, basta considerar um dos dois sistemas, pois para o outro será análogo.

Proposição 18. Um erro de transposição em que dois dígitos não adjacentes a_i e a_j são trocados, não pode ser detectado pelos sistemas UPC e EAN-13, se a diferença $i-j$ for par.

Demonstração:

Ao realizar o produto escalar $\alpha \cdot \omega$, tem-se que os algarismos da posição par no sistema EAN-13 (ou respectivamente ímpar no sistema UPC) são multiplicados por 3, enquanto que os outros algarismos são multiplicados por 1. Portanto, se a variação de i para j é par, o fator de multiplicação, 1 ou 3, não muda. Logo, o resultado final não se altera.

■

Proposição 19. Um erro de transposição em que dois dígitos não adjacentes a_i e a_j são trocados, com a diferença $i-j$ ímpar, será detectado pelos sistemas EAN-13 e UPC, se e somente se, $|a_i - a_j| \neq 5$.

Demonstração.

Considere $a_1, a_2, ..., a_i, ...a_j, \ldots, a_{12}, a_{13}$, uma sequência de dígitos pela qual um determinado produto está identificado no sistema EAN-13. Tem-se que:

$$a_1 + 3a_2 + \cdots + a_i + \cdots + 3a_j + \cdots + 3a_{12} + a_{13} \equiv 0 \, mod \, 10 \qquad (3)$$

Sabe-se que ao realizar o produto escalar $\alpha \cdot \omega$, tem-se que no sistema EAN-13, os algarismos da posição par, são multiplicados por 3, enquanto que os algarismos na posição ímpar, são multiplicados por 1. Portanto, se a variação de i para j é ímpar, o fator de multiplicação, 1 ou 3, muda. Dessa forma, se um código sofreu uma transposição não adjacente dos algarismos a_i *e* a_j (sendo $i-j$ ímpar), tal erro será detectado, se, e somente se:

$$a_1 + 3a_2 + \cdots + a_j + \cdots 3a_i + \ldots + 3a_{12} + a_{13} \equiv 0 \, mod \, 10 \qquad (4)$$

Fazendo (3) - (4) tem-se,

$$a_i - a_j + 3a_j - 3a_i \equiv 0\, mod\, 10 \Leftrightarrow 2(a_i - a_j) \equiv 0\, mod\, 10$$

Observe novamente, que sempre $|a_i - a_j| \leq 9$, já que a_i *e* a_j são números entre zero e 9. Daí,

$$2(a_i - a_j) \equiv 0\, mod\, 10 \Leftrightarrow |a_i - a_j| = 5$$

Portanto, conclui-se que o erro por transposição não adjacente, com a diferença $i-j$ ímpar, será detectado se, e somente se, $|a_i - a_j| \neq 5$.

■

Foram mostrados alguns erros detectáveis e outros não detectáveis, envolvendo a digitação de código de barras dos sistemas EAN-13 e UPC. Outros tipos de erros e sua possível detecção podem ser encontrados em [12] e [5].

3.4 Sistema de Identificação ISBN

"*Uma lista de números é transmitida e guardada com mais eficiência do que uma lista de nomes. Além disso, as listas de números transpõem a barreira da língua e dos vários alfabetos da comunidade internacional (pense na facilidade com que podemos encomendar um livro de um editor japonês sem ter que especificar o título do livro em japonês!*)". [16]

O sistema ISBN (International Standard Book Number), criado em 1969 para a identificação numérica de livros, CD-Roms e publicações em braille, talvez seja um dos pioneiros na utilização de um dígito de verificação ao final de cada código capaz de resolver o problema dos erros singulares e de transposição. [14]

Assim como os códigos de barras, o ISBN também é uma representação gráfica de dados reconhecida mundialmente. Ele proporciona às bibliotecas, às editoras e principalmente

aos leitores, utilizarem, onde quer que estejam, uma única linguagem (a de números), não importando de que país seja o livro ou a origem da pessoa que o solicitará.

Conhecer um sistema tão grandioso como o ISBN, saber como funciona, calcular o dígito de verificação, ser capaz de detectar um erro de digitação, certamente será uma rica experiência para os alunos do Ensino Básico, principalmente porque a ciência que está por trás de tudo isso é a Matemática, matéria esta, que necessita de conteúdos que prendam a atenção dos alunos.

Os códigos ISBN de livros lançados entre 1969 e 2007 possuem dez dígitos, os quais denominamos ISBN-10, já para as publicações feitas após 1 de janeiro de 2007, os códigos receberam um acréscimo de três dígitos, sendo chamados agora de ISBN-13.

A seguir será mostrado como é feito o cálculo do dígito de verificação e a detecção de erros dos ISBN-10, já que para o ISBN-13 os resultados são os mesmos que foram apresentados anteriormente para os códigos de barras, EAN-13.

3.4.1 O Dígito de Verificação

No sistema ISBN-10 o décimo dígito, da esquerda para a direita, é o dígito de verificação, enquanto que os outros nove algarismos fazem a identificação do livro. Esses nove algarismos são divididos em três partes e o número de dígitos em cada parte pode variar. Da esquerda para a direita, a primeira parte identifica um grupo nacional ou geográfico de editores, no Brasil por exemplo, esse número é o 85. A segunda parte, determina especificamente, uma editora desse grupo, a FTD por exemplo, possui o número 322 para sua identificação. Por fim, a terceira parte, identifica um título específico, o livro "Matemática Fazendo a Diferença, de Bonjorno & Ayrton, para o $7^{\underline{o}}$ ano, traz o número 5867 como identificação da obra.

O vetor de pesos do ISBN-10 é $\omega = (10, 9, 8, 7, 6, 5, 4, 3, 2, 1)$.

Para determinar o dígito de verificação de um código ISBN-10, $\alpha = (a_1, a_2, a_3, \ldots, X)$, em que $X \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ representa o dígito de verificação, deve-se calcular a soma S:

$$S = \alpha \cdot \omega = (a_1, a_2, a_3, \ldots, X) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) = 10a_1 + 9a_2 + \cdots + X,$$

e esta soma deve ser congruente a zero módulo onze. Ou seja,

$$10a_1 + 9a_2 + \cdots + X \equiv 0 \, mod \, 11$$

Observação: No sistema ISBN-10, se o dígito de verificação encontrado for o número dez, este será representado pela letra x.

Exemplo 34. Encontre o dígito de verificação de um livro cujo os primeiros nove dígitos do ISBN-10 são: 85-7056-046.

Solução:

Tem-se, $\alpha = (8, 5, 7, 0, 5, 6, 0, 4, 6, X)$. Daí,

$$S = \alpha \cdot \omega = (8, 5, 7, 0, 5, 6, 0, 4, 6, X) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) = \\ 80 + 45 + 56 + 0 + 30 + 30 + 0 + 12 + 12 + X.$$

Daí,

$$S \equiv -8 + 1 + 1 + 0 - 3 - 3 + 0 + 1 + 1 + X \equiv -6 - 6 + 2 + X \equiv 1 + X \, mod \, 11.$$

Como, $S \equiv 1 + X \, mod \, 11$, então, para que se tenha, $S \equiv 0 \, mod \, 11$, deve-se ter $X = 10$.

Neste caso, o ISBN-10 desse livro é 85-7056-x.

Exemplo 35. Seja X o dígito verificador do livro cujo o ISBN-10 é 85-322-5867-X. Determine o valor de X.

Solução:

Neste caso, $\alpha = (8, 5, 3, 2, 2, 5, 8, 6, 7, X)$. Daí,

$$S = \alpha \cdot \omega = (8, 5, 3, 2, 2, 5, 8, 6, 7, X) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) \Rightarrow$$

$$\Rightarrow S = 80 + 45 + 24 + 14 + 12 + 25 + 32 + 18 + 14 + X.$$

Daí,

$$S \equiv -8 + 1 + 2 + 3 + 1 + 3 - 1 - 4 + 3 + X \equiv 2 - 2 \equiv 0 \, mod \, 11$$

Como $S \equiv 0 \, mod \, 11$, conclui-se que $X = 0$.

3.4.2 Detecção de Erros

Assim como nos sistemas de códigos de barras, no ISBN, há uma grande preocupação com a detecção de possíveis erros. As duas proposições a seguir, mostrarão que erros singulares e de transposição serão detectados durante a leitura de códigos do sistema ISBN-10.

Lembrando que erros singulares, são aqueles em que ocorre erro na digitação de um único dígito. Enquanto que o erro de transposição, ocorre quando há a troca na posição de dois dígitos.

Proposição 20. Se ocorrer na leitura de um código ISBN-10 um erro singular, então o erro será detectado.

Demonstração:

Seja $\alpha = (a_1, a_2, a_3, \ldots, a_{10})$, um código ISBN-10. Tem-se:

$$S = (a_1, a_2, \cdots, a_i, \ldots, a_{10}) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) = 10a_1 + 9a_2 + \cdots + (11 - i)\, a_i + \cdots + a_{10}.$$

Suponha que o código tenha sido digitado errado e que no lugar de a_i, digitou-se um outro algarismo, a_i', $1 \leq i \leq 10$. Neste caso,

$$S' = (a_1, a_2, \cdots, a_i', \ldots, a_{10}) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) = 10a_1 + 9a_2 + \cdots + (11 - i)\, a_i' + \cdots + a_{10}.$$

Fazendo $S - S'$ tem-se:

$$S - S' = (11 - i)\, a_i - (11 - i)\, a_i' = (11 - i)\, (a_i' - a_i)$$

Se o erro não fosse detectado, então, $S' \equiv 0\, mod\, 11$. Daí, de S' e S serem múltiplos de 11, a sua diferença, $S - S' = (11 - i)\, (a_i' - a_i)$ também seria múltiplo de 11, ou seja, $11 \mid (11 - i)\, (a_i' - a_i)$. Como 11 é primo, pela propriedade fundamental, $11 \mid (11 - i)$ ou $11 \mid (a_i' - a_i)$. O que não pode ocorrer, já que $(11 - i)$ não é múltiplo de 11, pois está compreendido entre 1 e 10 e nem $(a_i' - a_i)$, é múltiplo de 11, pois está compreendido entre -9 e 9.

Portanto, o erro será detectado.

■

Proposição 21. Se ocorrer na leitura de um código ISBN-10 um erro de transposição, então o erro será detectado.

Demonstração:

Seja $\alpha = (a_1, a_2, ..., a_i, \ldots, a_j, ..., a_{10})$, um código ISBN-10. Tem-se:

$$S = (a_1, a_2, ..., a_i, \ldots, a_j, ..., a_{10}) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) =$$
$$10a_1 + 9a_2 + \cdots + (11 - i)\, a_i + \cdots + (11 - j)\, a_j + \cdots + a_{10}.$$

Suponha que o código tenha sido digitado errado e que no lugar de a_i, digitou-se a_j e no lugar de a_j, digitou-se, a_i, $1 \leq i, j \leq 10$. Neste caso,

$$S' = (a_1, a_2, ..., a_j, \ldots, a_i, ..., a_{10}) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) =$$
$$10a_1 + 9a_2 + \cdots + (11 - i)\, a_j + \cdots + (11 - j)\, a_i + \cdots + a_{10}.$$

Fazendo $S - S'$, tem-se:

$$S - S' = (11 - i)\, a_i - (11 - i)\, a_j + (11 - j)\, a_j - (11 - j)\, a_i = (i - j)\, (a_i - a_i).$$

Usando o mesmo argumento da proposição anterior, necessariamente $S' \not\equiv 0 \, mod \, 11$.

De fato, se o erro não for detectado, ou seja, $S' \equiv 0 \, mod \, 11$, tem-se S' e S múltiplos de 11, logo a sua diferença, $S - S' = (i - j)(a_i - a_i)$ também será múltiplo de 11. Mas, de 11 ser primo, pela propriedade fundamental, isso não pode ocorrer, já que $(i - j)$ não é múltiplo de 11, pois está compreendido entre e -9 e 9 e nem $(a_j - a_i)$ é múltiplo de 11, pois também está compreendido entre -9 e 9.

Portanto, o erro será detectado.

■

Capítulo 4

CONSIDERAÇÕES FINAIS

Conclui-se que, por meio da *Aritmética Modular* (*congruências*), certos problemas de matemática poderão ser resolvidos de forma ágil e eficaz.

Esta ferramenta permitirá ao aluno, fazer investigações matemáticas, como por exemplo: os critérios de divisibilidade. O aluno será capaz de estabelecer se um número inteiro a é divisível por um número inteiro m, através do estudo da *congruência módulo m,* sem precisar decorar regras.

Com a *Prova dos Noves*, o aluno poderá estabelecer cálculos mentais com facilidade, para verificar a veracidade dos resultados obtidos em operações envolvendo números naturais.

Apresentados como uma aplicação da *Aritmética Modular,* no contexto social, os código de barras e o ISBN poderão despertar o interesse do aluno em aprender tal teoria.

Professores de matemática, que atuem principalmente no ensino médio, poderão utilizar este trabalho, como um instrumento para o desenvolvimento de aulas de *Aritmética.* Para tanto, buscou-se, durante a elaboração da redação, utilizar uma linguagem simples e objetiva. Além disso, o principal objetivo foi colocar aqui aplicações de *Aritmética Modular*, pouco aproveitadas até então nas salas de aula, de modo a serem interessantes aos olhos dos alunos, para que os mesmos ficassem curiosos e interessados em aprender mais sobre os assuntos das aulas de matemática. Acredita-se também, que motivados por este, outros trabalhos nessa linha, possam vir a sugerir outras aplicações interessantes da *Matemática*

que poderão ser também aproveitadas na Educação Básica.

Referências Bibliográficas

[1] ANRADE, Doherty. O nove misterioso. RPM 09. Presidente Prudente-SP.

[2] BUESCU, Jorge. O mistério do Bilhete de Identidade e outras histórias. Lisboa: Gradiva, 2001.

[3] CARDOSO, Celso. Dissertação de Mestrado, Fatoração de números inteiros usando curvas elíticas, Universidade Federal de Mato Grosso do Sul.

[4] COUTINHO, S.C . Criptografia. (Programa de Iniciação Científica OBMEP, Sociedade Brasileira de Matemática).

[5] DIAS, Eduardo Marques. Código de barras. Universidade Católica de Brasília. Departamento de Matemática.

[6] DOMINGUES, Hygino H. e IEZZI, Gelson . Álgebra Moderna. Editora Atual, 1982.

[7] HEFEZ, A. Elementos de Aritmética. (Série Textos Universitários, Sociedade Brasileira de Matemática). ISBN:978-85-85818-25-8

[8] HEFEZ, A. Iniciação à Aritmética. (Programa de Iniciação Científica OBMEP, Sociedade Brasileira de Matemática).

[9] HERNSTEIN, I.N. Topics in Algebra, 1964. ISBN: 9780471010906

[10] JÚNIOR, Porfírio Azevedo dos Santos. A Matemática dos Códigos de Barras - UPC. Departamento de Matemática. Universidade Federal de Goiás/Campus Catalão.

[11] LOURENÇO, Paulo Jorge Pais, dissertação de mestrado. Aplicações de Aritmética.

[12] MILIES, César Polcino. A matemática dos códigos de barras. 19 f. São Paulo, SP. IME/USP - Departamento de Matemática, SP.

[13] MILIES, Francisco Cesar Polcino e COELHO, Sónia Pitta . Números: Uma Introdução à Matemática.

[14] MELLO, José Luiz Pastore . RPM 48. Aritmética modular e sistemas de identificação.

[15] OLIVEIRA, Krerley Irraciel Martins e FERNANES, Adán José Corcho. Iniciação à Matemática: um curso com problemas e soluções. SBM-2010. ISBN:978-85-85818-46-3

[16] PICADO, Jorge. A álgebra dos sistemas de identificação: da aritmética modular aos grupos diedrais, Boletim da Sociedade Portuguesa de Matemática, nº 44, abril/2001.

[17] RODRIGUES, Flávio Wagner . A prova dos nove. RPM 14, IME-USP.

[18] http://www.gs1-ean13.com.br/80973298613287498769652834756/entenda_o_codigo_de_barras.htm, acessado em 14/01/2013.

[19] http://msdn.microsoft.com/pt-br/library/cc580676.aspx, acessado em 14/01/2013.

[20] http://pt.wikipedia.org/wiki/N%C3%BAmero_primo, acessado em 22/01/2013.

[21] http://www.ime.unicamp.br/~calculo/history/fermat/fermat.html, acessado em 24/03/2013.