UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

Congruências modulares e aplicações no ensino básico

Janayna Mara Rezende Barbosa

Dissertação de Mestrado do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT)

ICMC USP
SÃO CARLOS

Janayna Mara Rezende Barbosa

Congruências modulares e aplicações no ensino básico

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestra em Ciências – Mestrado Profissional em Matemática em Rede Nacional. *VERSÃO REVISADA*

Área de Concentração: Mestrado Profissional em Matemática em Rede Nacional

Orientadora: Profa. Dra. Katia Andreia Gonçalves de Azevedo

USP – São Carlos
Novembro de 2017

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados fornecidos pelo(a) autor(a)

Rezende Barbosa, Janayna Mara
R467c Congruências modulares e aplicações no ensino básico / Janayna Mara Rezende Barbosa; orientadora Katia Andreia Gonçalves Azevedo. -- São Carlos, 2017.
112 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2017.

1. Teoria dos Números. 2. Congruências. 3. Código de barras. I. Azevedo, Katia Andreia Gonçalves, orient. II. Título.

Janayna Mara Rezende Barbosa

Modular congruence and applications in basic education

Master dissertation submitted to the Institute of Mathematics and Computer Sciences – ICMC-USP, in partial fulfillment of the requirements for the degree of Mathematics Professional Master's Program. *FINAL VERSION*

Concentration Area: Professional Master Degree Program in Mathematics in National Network

Advisor: Profa. Dra. Katia Andreia Gonçalves de Azevedo

USP – São Carlos
November 2017

Aos meus pais que sempre me incentivaram a estudar e a lutar pelos meus sonhos.

AGRADECIMENTOS

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

Aos meus pais, que não mediram esforços para facilitar que eu chegasse até aqui, pelo amor e por todas as orações que fizeram.

Às minhas filhas, Maria Clara e Maria Luísa, que compreenderam a minha ausência em vários momentos para realizar esse trabalho.

Ao meu irmão, Junior, pelo companheirismo durante essa caminhada.

À minha professora e orientadora, Prof. Dra. Katia Andrea Gonçalves de Azevedo, por toda dedicação e paciência, por ter acreditado no meu potencial, incentivando a seguir em frente sempre.

A todos os professores do Profmat, polo de Ribeirão Preto, pelo empenho e atenção destinados aos alunos e por toda preocupação em garantir um curso de boa qualidade.

Ao programa Profmat, pela oportunidade de crescimento profissional.

À Capes, pelo incentivo e financiamento do curso.

A todos os colegas de turma, pelas trocas de conhecimento que fizemos, principalmente à Priscila e ao Talles, por serem também companheiros das idas e vindas ao curso e ao amigo Rafael a quem agradeço imensamente todo o apoio para a digitação deste trabalho.

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

“Fiz a escalada da montanha da vida,
removendo pedras e plantando flores”
(Cora Coralina)

RESUMO

BARBOSA, J. M. **Congruências modulares e aplicações no ensino básico**. 2017. 112 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2017.

O presente trabalho inicia-se com uma breve história sobre a evolução da Teoria dos Números, destacando os estudiosos que tiveram grande importância para o reconhecimento dessa parte da Matemática. Logo após, é feita uma fundamentação teórica dos principais tópicos da Teoria dos Números, ressaltando alguns teoremas e apresentando exemplos de aplicações em várias áreas da Matemática. É apresentado um estudo a respeito dos diversos sistemas de codificação que fazem o uso do dígito verificador, com o objetivo de motivar o aluno a entender um pouco sobre o conceito de aritmética modular, de maneira fácil, rápida e simples. Para finalizar são apresentados relatos de atividades realizadas com alunos do ensino básico, envolvendo códigos de barras, visando ressaltar a importância de entender a aplicabilidade das congruências nos dias de hoje.

Palavras-chave: Teoria dos números, Congruências e Códigos de barras.

ABSTRACT

BARBOSA, J. M. **Modular congruence and applications in basic education**. 2017. 112 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2017.

His work starts by describing a brief history on the development of Numbers Theory, highlighting the ones who had great importance for the recognition of this part of Mathematics. Next, a theoretical framework of the main topics of Numbers Theory is made, emphasizing some theorems and presenting examples of applications in several areas of Mathematics. A survey is done about several coding systems that use check digit, in order to motivate the student to understand the concept of modular arithmetic, in an easy, fast and simple way. Finally, we present reports of activities carried out with students of basic education, involving bar codes, in order to highlight the importance of understanding the applicability of congruences nowadays.

Keywords: Theory of Numbers, Congruences and Barcodes.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

CAPÍTULO

1

INTRODUÇÃO

A Teoria dos Números é um ramo da Matemática que estuda as propriedades dos números em geral. Ela é dividida em vários campos, sendo um deles dedicado ao estudo das propriedades dos números inteiros.

Uma das ferramentas importantes da Teoria dos Números é a congruência modular, que envolve o estudo de congruências no conjunto dos números inteiros.

A principal motivação para escolha do tema Congruências Modulares e Aplicações no Ensino Básico para esse trabalho, foi que, fazendo o uso das novas tecnologias, juntamente com conceitos aplicáveis dessa parte da Matemática, podemos compreender melhor o mundo de informações que nos cerca.

O professor de Matemática, com o objetivo de proporcionar aos alunos o desenvolvimento de competências e habilidades que garantam a formação do cidadão, frente a um novo perfil de profissional, pode fazer o uso em sala de aula de atividades diversas, e neste trabalho propomos aplicações de congruências modulares.

Uma destas aplicações é relativa aos sistemas de codificações, ressaltando os códigos de barras. Estes são usados pelo mundo todo para a identificação de produtos, facilitando a organização e contagem de estoques, além de agilizar o processo de entrada e saída dos produtos.

Além disso, em diversos campos da Matemática, temos problemas que podem ter a sua resolução facilitada se usarmos os teoremas e propriedades da Teoria dos Números.

O objetivo deste trabalho é ainda mostrar como conceitos da Teoria dos Números estão presentes no nosso dia-a-dia e o quanto é importante a aplicação de seus conceitos para resolução de problemas diversos.

No capítulo II é feito um levantamento do contexto histórico da evolução dos estudos relacionados à Teoria dos Números, tentando ressaltar os grandes matemáticos que contribuíram de alguma forma para o reconhecimento e estudo dessa parte da Matemática.

No capítulo III é apresentada uma fundamentação teórica, com estudos dos principais teoremas e conceitos que serão usados ao longo do trabalho e nas aplicações.

No capítulo IV, primeiramente, é contada um pouco da história dos códigos de barras. A seguir, é feito um estudo sobre sua estrutura e a obtenção do dígito verificador. É mostrado também como é possível ou não detectar um erro ao se digitar os algarismos de um código de barras. Além do código de barras, o trabalho também faz o estudo de outros sistemas de codificações que fazem o uso do dígito verificador. É apresentado relato de atividades que foram trabalhadas com alunos do 9^{o}ano do ensino básico, relativo ao tema, em uma escola pública do estado de Minas Gerais.

É esperado que, a partir desse trabalho muitos outros possam surgir para completá-lo e enriquecê-lo com outras aplicações de congruências modulares que possam ser adequadamente utilizadas nas aulas ministradas por professores de Matemática na educação básica, procurando sempre motivar os alunos e desenvolver competências e habilidades necessárias para sua formação e atuação na sociedade em que vivemos.

CAPÍTULO

2

UM POUCO DA HISTÓRIA DA TEORIA DOS NÚMEROS

A forma de compreender e representar os números, respondendo a uma necessidade do homem de representar quantidades, foram evoluindo ao longo da história.

Embora os números inteiros positivos compõem o sistema matemático mais simples, o estudo de suas propriedades exerce grande fascínio na mente humana desde a antiguidade, desafiando inúmeros estudiosos através de seus conceitos e propriedades que vão além de qualquer simplicidade.

Os sumérios, por volta de 2500 a.C., já possuíam um calendário e faziam o uso da base sexagesimal. Já desenvolviam algum tipo de aritmética no estudo da astronomia.

No Antigo Egito encontra-se o Papiro de Rhind ou Papiro de Ahmes. Esse documento egípcio é datado de 1650 a.C., onde um escriba de nome Ahmes detalha a solução de 85 problemas de aritmética, frações, cálculo de áreas, volumes e progressões. É um dos documentos antigos mais famosos que descreve registros onde é possível perceber como a Matemática era praticada naquela época.

A Teoria dos Números é um ramo da Matemática que se preocupa com as propriedades dos números inteiros e com os problemas que surgiram naturalmente do estudo dos números inteiros. A Teoria dos Números também já foi chamada de Aritmética Superior. Esse termo caiu em desuso.

A primeira abordagem científica da Teoria dos Números é atribuída aos gregos, por volta de 450 a.C. Pitágoras e seus seguidores, chamados de pitagóricos, foram os primeiros a classificar os números em pares, ímpares e primos.

Entre os problemas da Teoria dos Números abordados pelos gregos antigos, podemos citar o cálculo do máximo divisor comum de dois números, a determinação dos números primos

menores que um inteiro dado e a demonstração de que há uma infinidade de números primos.

Podemos citar também Euclides de Alexandria (330-275 a.C.). Ele, a pedido do imperador Ptolomeu I, organizou a obra "Os Elementos", composta de 13 livros. Destes, os livros VII, VIII e IX são dedicados à Teoria dos Números onde encontramos conceitos numéricos expressos em linguagem geométrica. Outro matemático de destaque é Diofanto de Alexandria, (nascido entre 201 e 214 e falecido entre 284 e 298). Sua obra Arithmetica, escrita por volta de 250 d.C., trata principalmente da solução de equações indeterminadas com coeficientes inteiros.

Embora a Matemática tenha sido continuadamente estudada por outros autores gregos e posteriormente, por árabes, indianos e europeus, a parte da Teoria dos Números ficou esquecida até o início do século XVII.

Em 1612, Bachet (1581-1638), outro grande matemático de destaque na Teoria dos Números, publicou o texto original em grego de Diofanto incluindo uma tradução latina. Entre 1621 e 1632 o francês Pierre de Fermat (1601-1665), adquiriu a cópia do livro de Bachet, fazendo um estudo e anotando nas margens as ideias que lhe ocorriam. Essas anotações posteriormente serviram de base para importantes resultados.

Naquela época, a Matemática era exercida como profissão por poucas pessoas. A comunicação entre os estudiosos era precária e se dava através de cartas e por pessoas que serviam de difusores das novas ideias. Uma das pessoas que se destacou nesse papel foi Marin Mersenne (1588-1648). Ele mantinha correspondência com alguns dos maiores matemáticos da época, como Descartes, Pascal e Fermat.

Nessa época, existia a República das Letras, que era uma espécie de sociedade informal de estudiosos, professores, bibliotecários, jornalistas, inventores, historiadores e artistas. Mersenne comunicava as novidades matemáticas que chegavam ao seu conhecimento à essa República.

Depois da morte de Pierre de Fermat, em 1665, coube a Samuel Fermat, seu filho, coletar e publicar a obra de seu pai. Dessas anotações, a parte de maior destaque foi o Último Teorema de Fermat.

O sucessor de Fermat foi o suiço Leonhard Euler (1707-1783). Euler publicou uma imensa obra Matemática, contribuindo para quase todas as áreas da Matemática pura e aplicada existentes no século XVIII. Este esteve ligado a academias científicas na Alemanha e na Rússia, que eram instituições de pesquisas que passaram a publicar atas com as contribuições científicas de seus membros.

Christian Goldbach (1690-1764) era um professor da Academia das Ciências de São Petesburgo. Goldbach escreveu vários documentos relacionados a teorias matemáticas e ficou conhecido pela conjectura de Goldbach e foi contemporâneo de Euler.

Em 1729, em uma de suas correspondências a Euler, Goldbach mencionou o seguinte questionamento: " Você conhece a observação de Fermat de que todos os números da forma

$2^{2^n} + 1$ são primos?".

Euler não demonstrou muito interesse e só em 1730, começou finalmente a ler a obra de Fermat. Nos anos seguintes, este provou grande parte dos resultados enunciados por Fermat, resolvendo inclusive a questão proposta por Goldbach.

Euler foi responsável pela popularização da Teoria dos Números, mas o estudo de forma sistematizada, ou seja, de forma metodológica, visando a elaboração do conhecimento, iniciou-se somente com a obra *Disquisitiones Arithmeticae*, do alemão Carl Friedrich Gauss (1777-1855), publicada em 1801.

Gauss foi um matemático, astrônomo e físico alemão que contribuiu muito em diversas áreas da ciência, dentre elas a Teoria dos Números, Estatística, Análise Matemática, Astronomia e Óptica. Alguns se referem a ele como "Príncipe da Matemática". Ele considerava a Matemática como rainha das ciências.

A Teoria dos Números, desde então, busca descobrir relações que diferentes tipos de números podem estabelecer.

CAPÍTULO

3

PRINCIPAIS CONCEITOS E TEOREMAS

Neste capítulo, apresentamos alguns resultados importantes para o entendimento e desenvolvimento do trabalho.

3.1 Princípio da Boa Ordenação

Adotaremos aqui o Princípio da Boa Ordenação, que é uma propriedade do conjunto dos Números Inteiros, como axioma e, como consequência deste, o Princípio de Indução Finita.

Alguns livros, como por exemplo em [9], adota o Princípio de Indução Finita como axioma e deste enuncia o Princípio da Boa Ordenação. Já em [8], é adotado o Princípio da Boa Ordenação e deste obtém-se o Princípio de Indução Finita como faremos aqui. Começamos, primeiramente, com uma definição.

Definição 1. Dizemos que um subconjunto S de $\mathbb{Z}$ é limitado inferiormente, se existir $c \in \mathbb{Z}$ tal que $c \leq x$ para todo $x \in S$. Dizemos que $a \in S$ é um menor elemento de S, se $a \leq x$ para todo $x \in S$.

Note que um menor elemento de S, se existir, é único, pois se a e a' são menores elementos de S, temos $a \leq a'$ e $a' \leq a$, o que acarreta $a = a'$.

Os conjuntos $\mathbb{Z}$ e $-\mathbb{N}$ não são limitados inferiormente e nem possuem um menor elemento. Já $\mathbb{N}$ é limitado inferiormente e possui 1 como menor elemento.

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

Este axioma diferencia os números inteiros dos racionais e reais. Note que, o intervalo $(0,1)$, tanto em $\mathbb{Q}$ quanto em $\mathbb{R}$ é limitado inferiormente, mas não possui um menor elemento.

A seguir, serão listadas algumas propriedades dos números inteiros que podem ser demonstradas com o uso do Princípio da Boa Ordenação.

Proposição 1. Não existe nenhum número inteiro n tal que $0 < n < 1$.

Demonstração. Suponha por absurdo que exista n com essa propriedade. Logo, o conjunto $S = \{x \in \mathbb{Z}; 0 < x < 1\}$ é não vazio, além de ser limitado inferiormente. Portanto, S possui um menor elemento a com $0 < a < 1$. Multiplicando esta última desigualdade por a, obtemos $0 < a^2 < a < 1$. Logo $a^2 \in S$ e $a^2 < a$, uma contradição. Portanto, $S = \emptyset$. □

Corolário 1. Dado um número inteiro n qualquer, não existe nenhum número inteiro m tal que $n < m < n+1$.

Demonstração. Suponha, por absurdo, que exista um número inteiro m satisfazendo as desigualdades $n < m < n+1$, logo $0 < m-n < 1$, o que contradiz a Proposição 1. □

Definição 2. Dizemos que um subconjunto T de $\mathbb{Z}$ é limitado superiormente, se existir $d \in \mathbb{Z}$ tal que $d \geq x$ para todo $x \in T$. Dizemos que um elemento $b \in \mathbb{Z}$ é o maior elemento de T, se $b \geq x$ para todo $x \in T$.

É imediato verificar que o maior elemento de um conjunto, se existir, é único.

Uma das mais importantes consequências do Princípio da Boa Ordenação é o Princípio de Indução Finita.

Teorema 3.1. Sejam S um subconjunto de $\mathbb{Z}$ e $a \in \mathbb{Z}$ tais que

(i) $a \in S$

(ii) S é fechado com respeito à operação de "somar 1"a seus elementos, ou seja, $\forall n, n \in S \Rightarrow n+1 \in S$.

Então, $\{x \in \mathbb{Z};\ x \geq a\} \subset S$.

Demonstração. Ponhamos $S' = \{x \in \mathbb{Z};\ x \geq a\}$ e suponhamos por absurdo que $S' \not\subset S$, logo $S' \backslash S \neq \emptyset$. Como esse conjunto é limitado inferiormente por a, existe um menor elemento c em $S' \backslash S$. Pelo fato de $c \in S'$ e $c \notin S$, temos que $c > a$. Portanto $c-1 \in S'$ e $c-1 \in S$. Pela hipótese sobre S, temos que $c = (c-1)+1 \in S$. Como $c \in S'$, obtemos uma contradição com o fato de $c \in S' \backslash S$. □

A proposição demonstrada acima aplica-se para verificar a validade geral de fórmulas ou propriedades que envolvem números inteiros. E é conhecida como um dos Axiomas de Giuseppe Peano (1858-1932).

Segue-se do Princípio de Indução Finita, o seguinte instrumento para provar teoremas.

Uma sentença Matemática aberta em n, são expressões que quando n é substituído por um número inteiro ela se torna uma sentença verdadeira ou falsa.

Teorema 3.2. Seja $a \in \mathbb{Z}$ e seja $p(n)$ uma sentença aberta em n. Suponha que

(i) $p(a)$ é verdadeiro,

(ii) $\forall n \geq a$, $p(n)$ é verdadeiro $\Rightarrow p(n+1)$ é verdadeiro.

Então, $p(n)$ é verdadeiro para todo $n \geq a$.

Demonstração. Seja $V = \{n \in \mathbb{Z}; p(n)\}$ verdadeiro, ou seja, V é o subconjunto dos elementos de $\mathbb{Z}$ para os quais $p(n)$ é verdadeiro.

Como por (i) $a \in V$ e por (ii)

$$\forall n, n \in V \Rightarrow n+1 \in V$$

segue-se do Princípio de Indução Finita que $\{x \in \mathbb{Z}; x \geq a\} \subset V$.

□

A comparação entre o Princípio de Indução Finita e um jogo de dominós ajuda na compreensão deste (Ver [5]). Consideremos um jogo de dominós, já enfileirados. Empurrando o primeiro, veremos eles caírem continuadamente. Ao empurrarmos o primeiro vemos este empurrar o segundo, este empurrar o terceiro, e assim por diante.

Para o estudo em questão substituíremos os dominós por uma sequência infinita de proposições definidas pelos inteiros.

Admita que seja possível provar que

(A) A proposição inicial seja verdadeira;

(B) Sendo uma proposição, diferente da proposição inicial, verdadeira, isso implica que a proposição próxima também seja verdadeira.

Assim, todas as proposições da sequência ficam provadas como verdadeiras.

A parte (A) é chamada de Base da Indução ou passo básico e a parte (B) é o passo indutivo.

Para fazer o uso do método de indução devemos:

- Não considerarmos a proposição como fato isolado, mas como uma sequência infinita de proposições semelhantes;
- Provar a primeira proposição da sequência, chamada de base da indução ou passo básico;

- Deduzimos a segunda proposição da primeira, a terceira da segunda, e assim por diante. Esse é o passo indutivo.

  A partir disso, podemos chegar a qualquer das proposições da sequência, partindo da base de indução. Assim todas elas serão aceitas como verdadeiras.

Através de alguns exemplos veremos como usar o Princípio de Indução Finita para provar alguns resultados.

Exemplo 3.1. Queremos determinar uma fórmula para a soma dos n primeiros números naturais. Conta a história que o matemático alemão Carl Friedrich Gauss (1777-1885), quando ainda garoto, estava em sua sala de aula, e o professor para aquietar a turma, mandou os alunos calcularem a soma de todos os números naturais de 1 a 100. Para sua surpresa, pouco tempo depois, o menino deu a resposta 5050, aparentemente sem cálculos. Indagado como tinha descoberto tão rapidamente o resultado, Gauss então com nove anos de idade, descreveu um método que posteriormente foi sistematizado da seguinte forma:

Sendo $S_n = 1+2+...+n$, o objetivo é encontrar uma fórmula fechada para S_n.

Somando a igualdade acima, membro a membro, com ela mesma, só que a segunda com as parcelas em ordem invertida, temos que:

$$S_n = 1+2+...+(n-1)+(n-2)+n$$

$$S_n = n+(n-1)+(n-2)+...+2+1$$

obtendo

$$2S_n = (n+1)+(n+1)+...+(n+1) = n(n+1)$$

Com isso temos que $S_n = \dfrac{n(n+1)}{2}$.

É necessário ser crítico em relação à fórmula encontrada. Ela parece já satisfazer o problema proposto. Mas, é preciso saber se a fórmula é válida para todo n. Para isso, usamos o Princípio de Indução Finita:

Considerando a sentença S_n sobre os naturais e $n_0 = 1$ temos

1^{o}) Para a base de indução, sendo $n_0 = 1$:

$$S(1) = \frac{1.(1+1)}{2} = \frac{1.2}{2} = \frac{2}{2} = 1.$$

Portanto, para $n_0 = 1$, S_{n_0} é verdadeira.

2º) Considerando como hipótese de indução que S_n seja verdadeira e provaremos para S_{n+1}:

$$S_n = 1+2+3+...+n = \frac{n(n+1)}{2}$$

$$S_{n+1} = 1+2+3+...+n+(n+1) = \frac{n(n+1)}{2}+n+1$$

$$S_{n+1} = \frac{n(n+1)+2(n+1)}{2}$$

$$S_{n+1} = \frac{n^2+n+2n+2}{2} = \frac{n^2+3n+2}{2}$$

$$S_{n+1} = \frac{(n+1)(n+2)}{2}$$

$$S_{n+1} = \frac{(n+1)[(n+1)+1]}{2}.$$

Isto torna a proposição válida para todo $n \in \mathbb{N}$.

O Princípio de Indução Finita é usado para estabelecer verdades matemáticas, válidas para subconjuntos de $\mathbb{Z}$. Não é o caso de mostrar que uma sentença aberta vale para um grande número de casos, mas mostrar que determinada sentença aberta é verdadeira para todo número inteiro maior ou igual do que um a, tal que $a \in \mathbb{Z}$.

O Princípio de Indução Finita admite uma variante, chamada de Princípio da Indução Completa, ou Segunda Forma do Princípio de Indução.

Teorema 3.3. Seja $p(n)$ uma sentença aberta tal que

(i) $p(a)$ é verdadeiro,

(ii) $\forall n$, $p(a)$ e $p(a+1)$ e ...e $p(n)$ é verdadeiro $\Rightarrow p(n+1)$ é verdadeiro.

Então, $p(n)$ é verdadeiro para todo $n \geq a$.

Demonstração. Considere o conjunto $V = \{n \in a+\mathbb{N}; p(n) verdadeiro\}$. Queremos provar que o conjunto $W = (a+\mathbb{N})\backslash V$ é vazio. Suponha, por absurdo, que vale o contrário. Logo, pelo Princípio da Boa Ordenação, W teria um menor elemento k, e, como sabemos de (i) que $a \notin W$, segue-se que existe n tal que $k = a+n > a$. Portanto, $a, a+1, ..., k-1 \notin W$; logo $a, a+1, ..., k-1 \in V$. Por (ii) conclui-se que $k = k-1+1 = (a+n-1)+1 \in V$, o que contradiz o fato de $k \in W$. □

Na prática, para provar uma propriedade utilizando a segunda forma de indução, devemos provar que $n_0 \in T$, sendo T um subconjunto de $\mathbb{Z}$, e a seguir, dado um n qualquer, maior do que n_0, admitir que n e todos os números entre n_0 e n, inclusive, estão em T e provar que $n+1$ também pertence a T.

Problema 1 (Propriedades da sequência de Fibonacci)

Leonardo Fibonacci, como era conhecido, nasceu em 1170 e morreu em 1240. Foi um grande matemático da Europa Cristã Medieval. Ele representou papel importante, fazendo contribuições relevantes.

Foi Fibonacci quem descobriu a sequência $(1,1,2,3,5,8,...)$. Nessa sequência cada termo, a partir do terceiro, equivale à soma dos dois termos imediatamente anteriores.

Determine o próximo número na sequência $1,1,2,3,5,8,13,...$ e prove que o seu termo de posição n é sempre menor que $(7/4)^n$.

Solução:

Como dito anteriormente, cada termo, a partir do terceiro, é a soma dos dois termos imediatamente anteriores

$$2 = 1+1$$
$$3 = 2+1$$
$$5 = 3+2, \text{ e assim por diante.}$$

Pode-se concluir então que o próximo termo da sequência proposta no problema é 21, pois $8+13 = 21$.

Essa sequência pode ser definida da seguinte maneira recursiva

$$\begin{cases} F_1 = F_2 = 1 \\ F_{n+1} = F_{n-1} + F_n, \forall n \geq 2, n \in \mathbb{N} \end{cases}$$

Utilizando a segunda forma do Princípio da Indução Finita, ou forma completa, podemos provar que $\forall n \in \mathbb{N}$, $F_n < (7/4)^n$.

Para $n = 1$ e $n = 2$, a proposição é verdadeira, pois

$$F_1 = F_2 = 1 < (7/4)^1 = 7/4.$$

Seja $n \geq 2$ um natural e vamos supor que para todo natural m com $1 \leq m \leq n$, vale que $F_m < (7/4)^m$. Vamos mostrar que $F_{n+1} < (7/4)^{n+1}$:

$$F_{n+1} = F_{n-1} + F_n < (7/4)^{n-1} + (7/4)^n = (7/4)^n.(7/4)^{-1} + (7/4)^n$$

$$= (7/4)^n.(4/7) + (7/4)^n$$
$$= (7/4)^n.(\tfrac{4}{7} + 1)$$
$$= (7/4)^n.\tfrac{11}{7}$$

Como $(7/4)^n.\frac{11}{7} < (7/4)^n.7/4 = (7/4)^{n+1}$, então, $F_{n+1} < (7/4)^{n+1}$.

Logo, a proposição está demonstrada.

3.2 Divisibilidade

Vejamos agora o importante conceito de divisibilidade.

Definição 3. Sejam a, $b \in \mathbb{Z}$. Diz-se que a divide b, escrevendo $a|b$, quando existir $q \in \mathbb{Z}$, tal que $b = qa$. Quando $a|b$, diremos também que a é um divisor ou um fator de b, ou ainda, que b é múltiplo de a ou que b é divisível por a.

Caso a não divida b, escreve-se $a \nmid b$ e lê-se a não divide b.

Exemplo 3.2. Sabe-se que $3|27$, pois $27 = 3.9$.

Teorema 3.4. Sejam a, b, c e d números inteiros quaisquer. Então as seguintes proposições são verdadeiras

(1) $1|a$, $a|a$ e $a|0$;

(2) Se $a|b$ e $b|c$, então $a|c$;

(3) Se $a|b$ e $c|d$, então $(ac)|(bd)$;

(4) Se $a|b$ e $a|c$, então $a|(b+c)$;

(5) Se $a|b$ então para todo $m \in \mathbb{Z}$, tem-se que $a|(mb)$;

(6) Se $a|b$ e $a|c$, então para todo m, $n \in \mathbb{Z}$, tem-se que $a|(mb+nc)$;

(7) $a|b \Leftrightarrow a|-b \Leftrightarrow -a|b \Leftrightarrow -a|-b$;

(8) Se $a|b$ e $b \neq 0$, então $|a| \leq |b|$;

(9) Se $b|a$ e $a|b$, então $a = \pm b$;

(10) Se $a|1$, então $a = \pm 1$.

Demonstração. (1) Tem-se que, $1|a$, pois $a = 1.a$; $a|a$ pois $a = 1.a$; e $a|0$ pois $0 = 0.a$.

(2) Se $a|b$ e $b|c$, então existem números inteiros q_1 e q_2, tais que $b = q_1.a$ e $c = q_2.b$. Substituindo o valor de b na segunda obtemos $c = (q_1q_2).a$. Logo, $a|c$.

(3) Se $a|b$ e $c|d$, então existem números inteiros q_1 e q_2 tais que $b = q_1a$ e $d = q_2c$. Multiplicando a primeira pela segunda temos que $bd = (q_1q_2)ac$. Logo, $ac|bd$.

(4) Se $a|b$ e $a|c$, então existem números inteiros tais que $b = q_1a$ e $c = q_2a$. Somando as duas equações membro a membro temos que $b+c = q_1a+q_2a = (q_1+q_2)a$. Logo, $a|(b+c)$.

(5) Se $a|b$ então existe um número q, tal que $b = qa$. Multiplicando a equação anterior por m, tem-se que $mb = (qm)a$, logo, para todo m, tem-se que $a|mb$.

(6) Se $a|b$ e $a|c$, então existem números inteiros q_1 e q_2, tais que $b = q_1a$ e $c = q_2a$. Multiplicando a primeira e a segunda equação por m e n, inteiros, respectivamente, tem-se que, $mb = mq_1a$ e $nc = nq_2a$. Somando-as membro a membro, obtêm-se que $mb+nc = q_1ma+q_2na = (q_1m+q_2n)a$, logo $a|(mb+nc)$.

(7) $a|b$ então $b = qa$, $q \in \mathbb{Z}$. Multiplicando ambos os lados por (-1) obtêm-se que $(-b) = (-q)a$, $(-q) \in \mathbb{Z}$ ou ainda que $(-b) = q(-a), q \in \mathbb{Z}$. Partindo de $b = qa$, $q \in \mathbb{Z}$, podemos escrever que $b = (-q)(-a)$, $(-q) \in \mathbb{Z}$, e seguem as equivalências.

(8) Se $a|b$ com $b \neq 0$, então existe um número inteiro $q \neq 0$ tal que $b = qa$, logo, $|b| = |qa| = |q|.|a| \geq |a|$.

(9) Suponha que $b|a$ e $a|b$. Se $a = 0$ ou $b = 0$, tem-se $a = b = 0$. No caso de $a, b \neq 0$, tem-se pelo item (8) que $|a| \leq |b|$ e $|b| \leq |a|$. Logo $|a| = |b|$, ou seja, $a = \pm b$.

(10) Se $a|1$ pelo item (1), sabe-se que $1|a$ para todo a inteiro. Logo, pelo item anterior tem-se que $a = \pm 1$.

□

Teorema 3.5. Sejam a, b e $c \in \mathbb{Z}$, tais que $a|(b+c)$. Então $a|b \Leftrightarrow a|c$.

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

Suponha ainda que $a|b$. Então existe q_1 tal que $b = aq_1$. De $b+c = qa$ e $b = aq_1$ podemos escrever que $aq_1 + c = aq$. Disso, tem-se que $c = a(q-q_1) \in \mathbb{Z}$. Então $a|c$. A demonstração de $a|c \Rightarrow a|b$ é análoga.

□

Exemplo 3.3. Prove que se n é ímpar, então 8 divide $n^2 - 1$.

Como n é ímpar, podemos escrever que $n = 2k+1$, para algum $k \in \mathbb{Z}$. Com isso temos que

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

Como k e $k+1$ são números consecutivos, um deles é par. E um número par multiplicado por 4 será sempre um múltiplo de 8. Portanto, $n^2 - 1$ é múltiplo de 8, para todo n ímpar.

Teorema 3.6. Sejam a, b, $n \in \mathbb{N}$, com $a > b > 0$. Temos que $a-b$ divide $a^n - b^n$.

Demonstração. Vamos provar por indução sobre n.

É óbvio a afirmação para $n = 1$, pois $a-b$ divide $a^1 - b^1 = a-b$. Suponhamos, agora, que $a-b|a^n - b^n$ e provemos que $a-b|a^{n+1} - b^{n+1}$. Então, podemos escrever que

$$a^{n+1} - b^{n+1} = a^n a - b^n b = a^n a - ba^n + ba^n - b^n b = a^n(a-b) + b(a^n - b^n).$$

Como $a-b|a-b$ e por hipótese $a-b|a^n - b^n$, pelo item 6 do Teorema 3.4, podemos afirmar que $a-b|a^{n+1} - b^{n+1}$, para todo $n \in \mathbb{N}$. □

Teorema 3.7. Sejam a, b, $n \in \mathbb{N}$, com $a + b \neq 0$. Então temos que $a+b$ divide $a^{2n+1} + b^{2n+1}$.

Demonstração. Esse resultado também será provado por indução.

Para $n = 1$, temos que $a^{2n+1} + b^{2n+1} = a^3 + b^3$.

Como $a^3 + b^3$ pode ser escrito na forma $(a+b)(a^2 - ab + b^2)$ então $a+b|a^3 + b^3$.

Suponhamos, agora, que $a+b|a^{2n+1} + b^{2n+1}$ e provemos que $a+b|a^{2(n+1)+1} + b^{2(n+1)+1}$.

Temos que

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

Como $a+b|a^2 - b^2$, pois $a^2 - b^2 = (a-b)(a+b)$ e, por hipótese $a+b|a^{2n+1} + b^{2n+1}$, podemos afirmar que para todo $n \in \mathbb{N}$, $a+b|a^{2(n+1)+1} + b^{2(n+1)+1}$. □

Teorema 3.8. Sejam a, b, $n \in \mathbb{N}$, com $a \geq b > 0$. Temos que $a+b$ divide $a^{2n} - b^{2n}$.

Demonstração. Novamente, usando indução sobre n provaremos a afirmação acima.

Para $n = 1$, temos que $a+b|a^2 - b^2$, pois $a^2 - b^2 = (a-b)(a+b)$.

Como hipótese de indução consideremos que $a+b|a^{2n} - b^{2n}$ e provemos que $a+b|a^{2(n+1)} - b^{2(n+1)}$.

Podemos escrever que

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

Como $a+b|a^2 - b^2$ e, por hipótese $a+b|a^{2n} - b^{2n}$, decorre das igualdades acima que $a+b|a^{2(n+1)} + b^{2(n+1)}$, estabelecendo assim o resultado para todo $n \in \mathbb{N}$. □

A seguir, temos exemplos de aplicação dos teoremas anteriores.

Exemplo 3.4. Mostre que para todo $n \in \mathbb{N}$,

$$8|3^{2n}-1.$$

A expressão $3^{2n}-1$ pode ser escrita da seguinte forma

$$(3^2)^n-1^n=9^n-1^n.$$

Como 8 é $9-1$, então

$$9-1|9^n-1^n$$

pelo Teorema 3.6.

A potência 1^n, para todo $n\in\mathbb{N}$, será sempre 1. Então,

$$9-1|9^n-1$$

$$8|9^n-1$$

$$8|(3^2)^n-1$$

$$8|3^{2n}-1 \text{ para todo } n\in\mathbb{N}.$$

Exemplo 3.5. Demonstre que $13|2^{70}+3^{70}$.

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

Como 13 é igual a $4+9$, temos que

$$4+9|4^{35}+9^{35}.$$

Pelo Teorema 3.7 sabemos que $a+b|a^{2n+1}+b^{2n+1}$. Note que 35 é da forma $2n+1=2.17+1$. E considerando $a=4$ e $b=9$, podemos afirmar que $13|2^{70}+3^{70}$.

Exemplo 3.6. Prove que $53|7^{4n}-2^{4n}$, para todo $n\in\mathbb{N}$.

A expressão $7^{4n}-2^{4n}$ pode ser reescrita na forma $(7^2)^{2n}-(2^2)^{2n}=49^{2n}-4^{2n}$. Como 53 é $49+4$, a afirmação dada pode ser reescrita como

$$49+4|49^{2n}-4^{2n}.$$

Pelo Teorema 3.8, temos que $a+b|a^{2n}-b^{2n}$. Considerando $a=49$ e $b=4$, então podemos afirmar que $53|7^{4n}-2^{4n}$, para todo $n\in\mathbb{N}$.

3.2.1 Divisão Euclidiana

Mesmo que um número natural a não divida o número b, podemos efetuar essa divisão obtendo um quociente "q" e um resto r, sendo estes únicos.

Teorema 3.9. Sejam a e b dois números naturais com $0 < a \leq b$. Existem dois únicos números naturais q e r tais que

$$b = aq + r, \text{ com } 0 \leq r < a.$$

Demonstração. Suponha que $b > a$ e considere os números, pertencentes a $\mathbb{N}$,

$$b, b-a, b-2a,...,b-na,...$$

Pela Propriedade da Boa Ordem, o conjunto S formado pelos elementos acima tem um menor elemento $r = b - qa$.

Vamos provar que $r < a$.

Se $a|b$ então $r = 0$ e nada temos a provar.

Se, por outro lado, $a \nmid b$, então $r \neq 0$, e portanto, basta mostrar que não ocorre $r \geq a$.

De fato, se isso ocorresse, existiria um número natural $c < r$ tal que $r = c + a$.

Consequentemente, sendo $r = c + a = b - qa$, teríamos $c = b - qa - a \Rightarrow c = b - (q+1)a \in S$, com $c < r$ contradizendo o fato de r ser o menor elemento de S.

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

Para provarmos a unicidade, observe que, dados dois elementos distintos de S, a diferença entre o maior e o menor desses elementos, sendo um múltiplo de a, é pelo menos a.

Logo, se $r = b - aq$ e $r' = b - aq'$, com $r < r' < a$, teríamos $r' - r \geq a$, o que acarretaria $r' \geq r + a \geq a$, absurdo. Portanto, $r = r'$.

Disso segue-se que $b - aq = b - aq'$, o que implica que $aq = aq'$ e, portanto, $q = q'$. □

Exemplo 3.7. Mostre que o resto da divisão de 10^n por 9 é sempre 1, qualquer que seja o número natural n.

Por indução, para $n = 0$, temos que

$$10^0 = 9.0 + 1.$$

Portanto, o resultado vale.

Suponha agora, que o resultado seja válido para um dado n, isto é $10^n = 9q + 1$ e provemos para $n + 1$.

Considere a igualdade

$10^{n+1} = 10.10^n = (9+1).10^n = 9.10^n + 10^n = 9.10^n + 9q + 1 = 9(10^n + q) + 1.$

Com isso, prova-se que o resultado vale para $n+1$ e portanto, vale para todo $n \in \mathbb{N}$.

3.2.2 Paridade

A ideia de paridade é uma poderosa ferramenta na resolução de problemas matemáticos envolvendo números inteiros.

Definição 4. Denominamos números pares aos inteiros $..., -6, -4, -2, 0, 2, 4, ...$, ou seja, todos os inteiros da forma $2q$, para $q \in \mathbb{Z}$. E denominamos números ímpares aos inteiros $..., -3, -1, 1, 3, 5, ...$, ou seja, todos os inteiros da forma $2q+1$, para $q \in \mathbb{Z}$.

Dizemos que dois números inteiros têm a mesma paridade quando, e só quando, ou ambos forem pares, ou ambos forem ímpares.

Teorema 3.10. A soma de dois números pares é par.

Demonstração. De fato, dois números pares podem ser escritos na forma $2q$ e $2q'$ cuja soma é $2q + 2q' = 2(q + q')$. Logo, a soma de dois pares é par. □

Teorema 3.11. A soma de dois números ímpares é par.

Demonstração. Representando os dois números ímpares nas formas $2q+1$ e $2q'+1$, temos que $(2q+1) + (2q'+1) = 2(q+q') + 2$. Logo, a soma de dois números ímpares é par. □

Teorema 3.12. A soma de um número par com um número ímpar é ímpar.

Demonstração. Seja o número par representado por $2q$ e o número ímpar representado por $2q'+1$. Para a soma destes termos temos $2q + 2q' + 1 = 2(q+q') + 1$. Logo, a soma de um número par com um número ímpar é ímpar. □

Teorema 3.13. O produto de dois números pares é par.

Demonstração. Consideremos os números pares na forma $2q$ e $2q'$. Efetuando o produto temos que $2q.2q' = 2(2qq')$. Logo, o produto de dois números pares é múltiplo de 4 e portanto, é par. □

Teorema 3.14. O produto de um número par por um número ímpar é par.

Demonstração. Considere um número par na forma $2q$ e o número ímpar na forma $2q'+1$, efetuando o produto, obtemos $2q.(2q'+1) = 2(2qq'+q)$. Logo, o produto de um número par por um número ímpar é par. □

Teorema 3.15. O produto de dois números ímpares é ímpar.

Demonstração. Sendo um dos números ímpares na forma $2q+1$ e o outro na forma $2q'+1$ e efetuando o produto obtemos $(2q+1)(2q'+1) = 4qq' + 2q + 2q' + 1 = 2(2qq' + q + q') + 1$. Logo, o produto de dois números ímpares é ímpar. □

Vejamos a seguir alguns exemplos de uso da paridade na resolução de exercícios.

Em [4], página 5, encontramos o seguinte enunciado:

Exemplo 3.8. Onze engrenagens estão colocadas em um plano, arrumadas em uma cadeia como ilustrado na figura a seguir. Todas as engrenagens podem rodar simultaneamente?

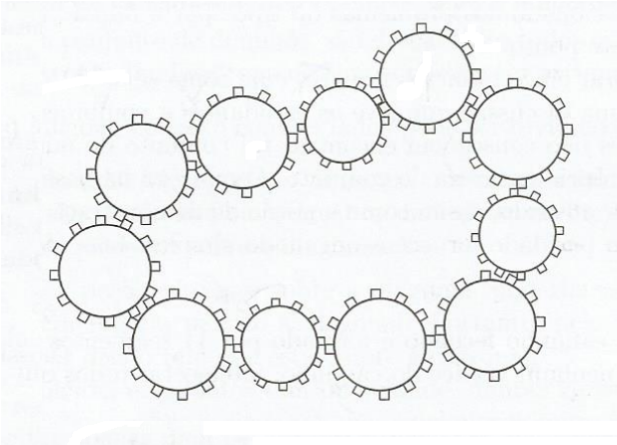


Figura 1: Engrenagens.

Suponha que o sentido de rotação da primeira seja horário. Então a segunda tem que girar no sentido contrário, ou seja, anti-horário, a terceira no sentido horário novamente, a quarta no sentido anti-horário. Mas, então, a primeira e a décima primeira engrenagem tem que girar no mesmo sentido, o que é uma contradição. Portanto a resposta é não.

Exemplo 3.9. Pergunta-se: O resultado de 20^{10} x 11^{200} + 21^{19} é par ou ímpar?

Para sabermos a paridade desse número não precisamos efetuar as contas indicadas. Basta pensarmos que, como 20 é par, multiplicando por ele mesmo 10 vezes, resultará um número também par, como 11 é ímpar, multiplicado por ele mesmo 200 vezes, resultará em um número ímpar, o mesmo ocorre com 21, que é ímpar, e ao ser multiplicado por ele mesmo 19 vezes, também resultará em um número ímpar. Agora basta pensarmos nas seguintes operações: (par x ímpar + ímpar) e veremos que o resultado será ímpar.

3.2.3 Máximo Divisor Comum

Segundo a definição de divisibilidade, ao observar o fato de que se um número inteiro a é divisor de um inteiro b, então $-a$ também divide b. Assim, podemos determinar o conjunto dos divisores inteiros de um número inteiro b, representado por $D(b)$.

Exemplo 3.10. a) $D(6) = \{\pm1, \pm2, \pm3, \pm6\}$.

b) $D(15) = \{\pm1, \pm3, \pm5, \pm15\}$.

c) $D(40) = \{\pm1, \pm2, \pm4, \pm5, \pm8, \pm10, \pm20, \pm40\}$.

d) $D(48) = \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm8, \pm12, \pm16, \pm24, \pm48\}$.

Observando os conjuntos dos divisores de 40 e de 48, verifica-se que estes apresentam números comuns, que são: $\{\pm1, \pm2, \pm4, \pm8\}$. Este fato motiva a seguinte definição:

Definição 5. Sejam $a, b \in \mathbb{Z}$ dois números, sendo pelo menos um deles diferente de zero. O máximo divisor comum entre a e b, denotado por $mdc(a,b)$, é o número natural d, $d > 0$, que é divisor comum de a e b e possui as propriedades a seguir:

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

b) Se algum $c \in \mathbb{N}$ dividir simultaneamente, a e b, então temos que $c|d$.

No exemplo apresentado anteriormente, temos $mdc(40,48) = 8$.

Observação:

a) $mdc(a,1) = 1$;

b) $mdc(a,0) = |a|$, com $a \neq 0$;

c) Se a é divisor de b, então $mdc(a,b) = a$;

d) Se $mdc(a,b) = 1$, então a e b são denominados primos entre si ou coprimos.

Exemplo 3.11. a) $mdc(1894,1) = 1$;

b) $mdc(17,0) = 17$;

c) $mdc(28,14) = 14$, pois 14 é divisor de 28;

d) $mdc(13,14) = 1$, então 13 e 14 são primos entre si ou coprimos.

Teorema 3.16. Um número d é divisor comum de a e de b, não ambos nulos, se e somente se, ele é um divisor comum de a e de $b-a$.

Demonstração. Se $d|a$ e $d|b$ então existem q_1 e q_2, tais que $a = dq_1$ e $b = dq_2$. Subtraindo a segunda da primeira obtemos $b-a = d(q_2-q_1)$. Logo, $d|(b-a)$.

Reciprocamente, se $d|a$ e $d|b-a$ então existem q_3 e q_4, tais que $a = dq_3$ e $b-a = dq_4$. Somando a primeira com a segunda obtemos $a+b-a = b = d(q_3+q_4)$. Logo, $d|b$.

□

Exemplo 3.12. Pelo Teorema anterior, temos que 6 é um divisor comum de 42 e 30, pois $6|42$, $6|12$ e $6|42-30$.

Para provar a existência do máximo divisor comum, Euclides utilizou-se basicamente do lema abaixo.

Lema 1. (Lema de Euclides) Sejam a, b, $n \in \mathbb{N}$, com $a < na < b$. Se existe $mdc(a, b-na)$, então existe $mdc(a,b)$ e

$$mdc(a,b) = mdc(a, b-na).$$

Demonstração. Seja $d = mdc(a, b-na)$. Como $d|a$ e $d|(b-na)$, pelo Teorema 3.16, segue que d divide $b = b-na+na$. Logo, d é um divisor comum de a e b. Suponha agora que c seja um divisor comum de a e b. Logo, c é um divisor comum de a e $b-na$ e, portanto, $c|d$. Isso prova que $d = mdc(a,b)$.

□

Usando a mesma técnica na demonstração do Lema de Euclides, pode-se provar que, para todos a, b, $n \in \mathbb{N}$

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

ou que, se $na > b$, então

$$mdc(a,b) = mdc(a, na-b).$$

O Lema de Euclides é efetivo para calcular *mdc* e será fundamental para estabelecermos o algoritmo de Euclides, que permite, com eficiência, calcular o *mdc* de dois números naturais quaisquer.

Pelo Lema de Euclides podemos encontrar o $mdc(42,30)$ da seguinte maneira:

como $12 = 42 - 1.30$, então $mdc(42,30) = mdc(30,12)$. Como $6 = 30 - 2.12$, então $mdc(30,12) = mdc(12,6)$. Como $0 = 12 - 2.6$, então $mdc(12,6) = mdc(6,0) = 6$.

Logo, $mdc(42,30) = 6$.

Uma outra aplicação do Lema de Euclides enunciado anteriormente pode ser apresentado no problema a seguir.

Exemplo 3.13. Determine os valores de a e n para os quais $a+1$ divide $a^{2n}+1$.

Note inicialmente que

$$a+1|a^{2n}+1 \Leftrightarrow mdc(a+1, a^{2n}+1) = a+1.$$

Como $a^{2n}+1 = (a^{2n}-1)+2$ e como visto em divisibilidade, Teorema 3.8, que $a+1|a^{2n}-1$, assim podemos escrever que, para todo n, temos

$$a+1 = mdc(a+1, a^{2n}+1) = mdc(a+1, (a^{2n}-1)+2) = mdc(a+1, 2).$$

Portanto, $a+1 | a^{2n}+1$, para algum $n \in \mathbb{N}$, se e somente se, $a+1 = mdc(a+1,2)$, o que ocorre se, e somente se $a = 0$ ou $a = 1$.

Exemplo 3.14. Dona Maria, costureira do bairro, dispõe de duas fitas de tamanhos diferentes. Com as mãos, ela mediu as fitas: a primeira de 24 palmos e a segunda de 32 palmos. Ela pretende cortar as duas fitas de modo a obter pedaços do mesmo tamanho e que seja o maior possível. Quanto medirá cada fita?

Como $8 = 32 - 1.24$, então $mdc(32,24) = mdc(24,8)$. Como $0 = 24 - 3.8$, então $mdc(24, 8) = mdc(8,0) = 8$.

Portanto, cada pedaço deverá medir 8 palmos para que Dona Maria obtenha todos do mesmo tamanho e de maior medida possível. Como $24 : 8 = 3$ e $32 : 8 = 4$, ela conseguirá obter 7 pedaços.

Observe que dados $a, b \in \mathbb{Z}$, se existir o $mdc(a,b)$ de a e b, então

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

Assim, para efeito do cálculo do *mdc* de dois números, podemos sempre supô-los não negativos.

Apresentaremos agora a prova construtiva da existência do *mdc* dada por Euclides (Ver [6]). Esse método, que recebeu o nome de algoritmo de Euclides, é muito usado na área computacional e pouco foi aperfeiçoado em mais de dois milênios.

Como os restos formam uma sequência estritamente decrescente, o algoritmo eventualmente termina quando atingimos o resto 0.

Dados a, $b \in \mathbb{N}$, podemos supor $a \leq b$. Se $a = 1$ ou $a = b$, ou ainda $a|b$ sabe-se que $mdc(a,b) = a$.

Suponha então, que $1 < a < b$ e que $a \nmid b$. Logo, pelo algoritmo geral da divisão podemos escrever

$$b = aq_1 + r_1, \text{ com } r_1 < a.$$

Assim, temos duas possibilidades:

1º) $r_1 | a$.

Pelo Lema de Euclides, teríamos que $r_1 = mdc(a, r_1) = mdc(a, b - q_1 a) = mdc(a,b)$, terminando assim o algoritmo.

2º) $r_1 \nmid a$

Nesse caso, podemos efetuar a divisão de a por r_1, obtendo

$$a = r_1.q_2 + r_2, \text{ com } r_2 < r_1.$$

Com isso temos duas possibilidades novamente

a) $r_2 | r_1$.

Neste caso, novamente pelo Lema de Euclides, temos

$r_2 = mdc(r_1, r_2) = mdc(r_1, a - q_2 r_1) = mdc(r_1, a) = mdc(b - q_1 a, a) = mdc(b, a) = mdc(a, b)$.

Terminando assim o algoritmo.

b) $r_2 \nmid r_1$.

Ao efetuarmos a divisão de r_1 por r_2, obtemos

$$r_1 = r_2 q_3 + r_3, \text{ com } r_3 < r_2.$$

Se esse processo continuasse indefinidamente, teríamos uma sequência de números naturais $a > r_1 > r_2 > ...$ que não possui menor elemento, o que não é possível pelo Princípio da Boa Ordem que nos garante que o conjunto dos números naturais, possui um menor elemento. Logo, para algum n, temos que $r_n | r_{n-1}$, e assim $mdc(a, b) = r_n$.

Com isso mostramos a existência do $mdc(a, b)$.

Vamos mostrar agora a unicidade. Para isso, admitamos que $mdc(a, b) = d$ e $mdc(a, b) = d'$. Assim, tanto d como d' são divisores comuns de a e b. Então, $d | d'$ e $d' | d$ e como d e d' são ambos positivos segue que $d = d'$, provando assim a unicidade do $mdc(a, b)$.

O algoritmo acima pode ser sintetizado e realizado na prática, através das divisões sucessivas, utilizando o que é conhecido pelos alunos como "jogo da velha ampliado".

Inicialmente, efetuamos a divisão $b = aq_1 + r_1$ e colocamos os números envolvidos no seguinte diagrama

	q_1	
b	a	
r_1		

A seguir, continuamos efetuando a divisão $a = r_1 q_2 + r_2$ e colocamos os números envolvidos no diagrama

	q_1	q_2	
b	a	r_1	
r_1	r_2		

Ao prosseguirmos enquanto for possível, teremos

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

Podemos ilustrar o algoritmo de Euclides com o seguinte exemplo:

Dona Marta, costureira do bairro, dispõe de duas peças de tecidos de tamanhos diferentes. A primeira peça tem 372 cm e a segunda 162 cm. Ela pretende cortar os dois tecidos de modo a obter pedaços iguais e que sejam do maior comprimento possível. Quanto medirá cada pedaço do tecido?

Pelo diagrama apresentado anteriormente podemos escrever que

	2	3	2	1	2		
372	162	48	18	12	6		
48	18	12	6	0			

Pelo método do diagrama fica fácil perceber que o *mdc* dos dois números em questão é o último resto não nulo do processo das divisões sucessivas. Portanto, cada pedaço do tecido deverá ter 6 cm.

No exemplo acima, podemos perceber que o Algoritmo de Euclides nos fornece

$$\begin{aligned} 6 &= 18 - 1.12 \\ 12 &= 48 - 2.18 \\ 18 &= 162 - 3.48 \\ 48 &= 372 - 2.162. \end{aligned}$$

Portanto,

$$\begin{aligned} 6 &= 18 - 1.12 \\ &= 18 - 1.(48 - 2.18) \\ &= 3.18 - 48 \\ &= 3(162 - 3.48) - 48 \\ &= 3.162 - 10.48 \end{aligned}$$

$$= 3.162 - 10(372 - 2.162)$$
$$= 23.162 - 10.372.$$

Temos então que

$$mdc(372, 162) = 6 = 23.162 - 10.372.$$

Através das divisões sucessivas do Algoritmo de Euclides conseguimos escrever 6 como a diferença entre um múltiplo de 162 e um múltiplo de 372.

Essa é uma propriedade do *mdc* que será demonstrada a seguir, que é chamada relação de Bézout. É uma ferramenta que pode ser usada para encontrar o *mdc* entre dois números através de uma combinação linear destes. O resultado foi provado pela primeira vez por Claude-Gaspard Bachet de Méziriac (1581-1638) e algum tempo depois generalizado por Etienne Bézout (1730-1783).

Proposição 2. (Relação de Bézout) Sejam a, $b \in \mathbb{Z}$ ambos não nulos e seja $d = mdc(a,b)$. Então existem x_1, $y_1 \in \mathbb{Z}$ tais que

$$ax_1 + by_1 = d.$$

Demonstração. O caso $a = 0$ ou $b = 0$ é trivial, pois $mdc(0,a) = a$ e $mdc(0,b) = b$. Nos outros casos, considere o conjunto S, composto de todas as combinações lineares de a e b,

$$S = \{ax + by, x, y \in \mathbb{Z}, \text{ e } ax + by > 0\}.$$

Considere $a \neq 0$. Então, $a \in S$, pois $a = a.1 + b.0 > 0$ se $a > 0$ e $-a$ pertence a S, pois $-a = a(-1) + b.0 > 0$ se $a < 0$. Logo, $S \neq \emptyset$.

Seja $a = 0$. Se $b > 0$, então $a.0 + b.1 > 0$ e se $b < 0$, então $a.0 + b(-1) > 0$. Logo, $S \neq \emptyset$.

Pelo princípio da Boa Ordem, existe um $d \in S$ minimal.

Como $d \in S$, temos $d > 0$ e existem x_1 e $y_1 \in \mathbb{Z}$ tais que $d = ax_1 + by_1$.

Afirmamos que d é o $mdc(a,b)$.

Dividindo a por d, então $\exists\, q, r \in \mathbb{Z}$ tais que $a = dq + r$ e $0 \leq r < d$. Assim, $r = a - qd = a - q(ax_1 + by_1) = a - aqx_1 - bqy_1 = a(1 - qx_1) + b(-qy_1)$.

Se fosse $r > 0$, poderíamos concluir que $r \in S$, o que claramente é um absurdo já que $r < d$ e d é o elemento mínimo de S.

Logo, $r = 0$ e $a = qd$, o que significa que $d|a$.

Da mesma forma mostra-se que $d|b$.

Como $d|a$ e $d|b$, logo d é divisor comum de a e b.

Seja $c \in \mathbb{N}$ tal que $c|a$ e $c|b$. Pelo Teorema 3.4 (6) concluímos que $c|ax_1 + by_1$ e $c|d$. Logo, $d = mdc(a,b)$.

□

A proposição demonstrada acima nos fornece o *mdc* de dois números, como combinação linear destes, mas não é construtiva como o Algoritmo de Euclides, que nos fornece um meio prático para achar o *mdc* de dois números.

Proposição 3. Sejam a, $b \in \mathbb{Z}$, não ambos nulos e seja $d = mdc(a,b)$. Então,

$$\{ax + by | x, y \in \mathbb{Z}\} = \{dz | z \in \mathbb{Z}\}.$$

Em palavras: As combinações lineares inteiras de a e b são exatamente os múltiplos do $mdc(a,b)$.

Demonstração. Abreviemos $T = \{ax + by | x, y \in \mathbb{Z}\}$ e $R = \{dz | z \in \mathbb{Z}\}$. Pela Relação de Bézout, existem x_1, $y_1 \in \mathbb{Z}$ com $d = ax_1 + by_1$. Para todo $z \in \mathbb{Z}$ segue $dz = a(x_1 z) + b(y_1 z) \in T$. Logo, $R \subseteq T$. Como $d|(ax + by)$ para qualquer $ax + by \in T$, segue também $T \subseteq R$. Logo, $T = R$. □

Com a Relação de Bézout e o fato de que dados dois números naturais a e b serem ditos primos entre si, ou coprimos, se $mdc(a,b) = 1$, ou seja, se o único divisor comum de ambos é 1, podemos estabelecer o seguinte corolário.

Corolário 2. Dois números a, $b \in \mathbb{Z}$ não ambos nulos, são primos entre si, se e somente se existem x_1, $y_1 \in \mathbb{Z}$ tais que

$$ax_1 + by_1 = 1.$$

Este resultado estabelece relações entre as estruturas aditivas e multiplicativas dos números naturais, permitindo provar a proposição a seguir.

Proposição 4. Sejam a, b e c números naturais. Se $a|b.c$ e $mdc(a,b) = 1$ então $a|c$.

Demonstração. Se $a|b.c$, então existe $l \in \mathbb{N}$ tal que $bc = al$. Se $mdc(a,b) = 1$, então pelo corolário anterior, temos que existem m, $n \in \mathbb{N}$ tais que

$$na + mb = 1.$$

Multiplicando por c ambos os lados da igualdade acima, temos que

$$c = nac + cmb.$$

Substituindo bc por al nesta última igualdade, temos que

$$c = nac + mal = a(nc + ml)$$

e portanto, $a|c$. □

Proposição 5. Sejam $a, b \in \mathbb{Z}$, ambos não nulos e $d = mdc(a,b)$. Então,

$$mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

(Observamos que $\frac{a}{d}$ e $\frac{b}{d}$ são números inteiros).

Demonstração. De $ax + by = d$ para certos $x, y \in \mathbb{Z}$, segue que $\frac{a}{d}x + \frac{b}{d}y = 1$. Pelo Corolário 2 concluímos a afirmação. □

3.2.4 Mínimo Múltiplo Comum

Definição 6. Sejam $a, b \in \mathbb{Z}$ dois números ambos não nulos. O mínimo múltiplo comum entre a e b é o número natural $m = mmc(a,b)$ definido pelas propriedades

a) $a|m$ e $b|m$ (isto é, m é múltiplo comum de a e b).

b) Se $a|c$ e $b|c$ para algum $c \in \mathbb{N}$, então temos também $m|c$.

Se c é um mínimo múltiplo comum de a e b, então pela Definição 5, item b, temos que $m|c$ e, portanto, $m \leq c$, o que nos diz que o mínimo múltiplo comum, se existir, é único e é o menor dos múltiplos de a e b.

Vale lembrar que o número $a.b$ é sempre um múltiplo comum de a e b.

A proposição enunciada a seguir, conecta o *mdc* e o *mmc* de dois números inteiros e pode ser utilizada, juntamente com o Algoritmo de Euclides, para o cálculo de *mmc*.

Proposição 6. Sejam a e b dois números inteiros. Então $mdc(a,b).mmc(a,b) = a.b$.

Demonstração. Se $a = 0$ ou $b = 0$, a igualdade acima é trivialmente satisfeita. É também fácil verificar que a igualdade é verificada para a e b se, e somente se, ela é verificada para $\pm a$ e $\pm b$. Então, sem perda de generalidade, podemos supor $a, b \in \mathbb{N}$.

Consideremos $m = \dfrac{ab}{mdc(a,b)}$.

Podemos escrever $m = a\dfrac{b}{mdc(a,b)} = b\dfrac{a}{mdc(a,b)}$.

Assim, $a|m$ e $b|m$. Portanto m é um múltiplo comum de a e b.

Seja c um múltiplo comum de a e b; logo, $c = na = n'b$. Segue que

$$n\frac{a}{mdc(a,b)} = n'\frac{b}{mdc(a,b)}.$$

Pela Proposição 5, $mdc\left(\frac{a}{mdc(a,b)}, \frac{b}{mdc(a,b)}\right) = 1$.

Pela Proposição 4, temos que $\frac{a}{mdc(a,b)}$ divide n', e, portanto, $m = \frac{a}{mdc(a,b)}b$ divide $n'b$, que é igual a c.

□

Segue um exemplo de aplicação de *mmc*.

Exemplo 3.15. Seja $n \in \mathbb{N}$ e $n \neq 0$. Calcule $mmc(n^2+1, n+1)$.

$n^2+1 = (n+1)(n-1)+2$. Logo, $mdc(n^2+1, n+1) = mdc(n+1, n^2+1) = mdc(n+1, (n+1)(n-1)+2)$ e pelo Lema de Euclides, $mdc(n+1, (n+1)(n-1)+2) = mdc(n+1, 2)$.

Se n é par, $n+1$ é ímpar e $mdc(n+1, 2) = 1$ e daí,

$mmc(n^2+1, n+1).mdc(n^2+1, n+1) = (n^2+1)(n+1) \Rightarrow mmc(n^2+1, n+1) = (n^2+1)(n+1)$.

Se n é ímpar, $n+1$ é par e $mdc(n+1, 2) = 2$ e daí,

$mmc(n^2+1, n+1).mdc(n^2+1, n+1) = (n^2+1)(n+1) \Rightarrow mmc(n^2+1, n+1) = \frac{(n^2+1)(n+1)}{2}$.

3.2.5 Equações Diofantinas

Nesta seção definiremos as equações diofantinas lineares, estudaremos a condição para que existam soluções de uma equação diofantina linear e mostraremos como resolver equações deste tipo aplicando *mdc*, através do Algoritmo de Euclides.

Uma equação diofantina é linear se ela tiver a forma

$$a_1x_1 + a_2x_2 + ... + a_nx_n = c,$$

onde as incógnitas são $x_1, x_2, ..., x_n \in \mathbb{Z}$.

Tais equações são chamadas equações diofantinas lineares em homenagem a Diofanto de Alexandria (aproximadamente 300 d.C.).

Diofanto foi um matemático e filósofo grego e é considerado o maior algebrista grego, verdadeiro precursor da moderna teoria dos números e considerado por alguns como pai da álgebra, devido à sua inovação com notações, e por ser o primeiro a usar símbolos na resolução de problemas algébricos. Mostrou interesse por uma grande variedade de equações indeterminadas que admitem infinitas soluções.

Nesse trabalho, faremos o estudo em particular das equações diofantinas lineares do tipo

$$ax + by = c \text{ com } a, b, c \in \mathbb{Z}.$$

A resolução de muitos problemas de aritmética depende da resolução desses tipos de equação, onde a, b e c são números inteiros dados e x e y são incógnitas a serem determinadas em $\mathbb{Z}$.

Nem sempre estas equações possuem soluções. É portanto necessário estabelecer condições para que tais equações possuam soluções e, caso tenham, como determiná-las.

Para isso estabeleceremos duas proposições a seguir.

Proposição 7. Sejam $a, b, c \in \mathbb{Z}$ e a e b não ambos nulos e $d = mdc(a,b)$. A equação diofantina

$$ax + by = c$$

admite pelo menos uma solução $x, y \in \mathbb{Z}$ se, e somente se, $d|c$.

Demonstração. Como $d|a$ e $d|b$ temos também que $d|c$ para qualquer possível solução $(x,y) \in \mathbb{Z} \times \mathbb{Z}$, de $ax+by=c$. Logo, $d|c$ é uma condição necessária para que haja a solução de $ax+by=c$.

Reciprocamente, seja $d|c$, digamos $dl = c$ para algum $l \in \mathbb{Z}$. Pelo Teorema de Bézout sabemos que existem x_1 e $y_1 \in \mathbb{Z}$ com $d = ax_1 + by_1$. Segue $c = a(lx_1) + b(ly_1)$ e vemos que (lx_1, ly_1) é uma solução particular de $ax+by=c$.

□

Usando a mesma notação da proposição anterior, temos

Proposição 8. Suponha $d|c$ e seja (x_0, y_0) uma solução particular de $ax+by=c$. Então a solução geral, isto é, o conjunto de todas as soluções de $ax+by=c$ é dada por

$$\begin{cases} x = x_0 + \frac{b}{d}t \\ y = y_0 - \frac{a}{d}t \end{cases} \quad \text{com } t \in \mathbb{Z}$$

Demonstração. Seja (x_0, y_0) uma solução particular e $t \in \mathbb{Z}$. Provamos primeiro que qualquer par de números

$$\begin{cases} x = x_0 + \frac{b}{d}t \\ y = y_0 - \frac{a}{d}t \end{cases}$$

satisfaz a equação também.

De fato, $ax+by = a\left(x_0+\frac{b}{d}t\right)+b\left(y_0-\frac{a}{d}t\right) = ax_0+\frac{b}{d}at+by_0-\frac{b}{d}at = ax_0+by_0 = c$.

Reciprocamente, seja (x,y) uma solução qualquer de $ax+by=c$. Temos então $ax_0+by_0 = c = ax+by$ e daí

$$a(x-x_0) = b(y_0-y).$$

Existem r, $s \in \mathbb{Z}$ tais que $a = rd$ e $b = ds$ e vale $mdc(r,s) = mdc(\frac{a}{d},\frac{b}{d}) = 1$.

Segue que $dr(x-x_0) = ds(y_0-y)$ e daí

$$r(x-x_0) = s(y_0-y),$$

pois $d \neq 0$.

Podemos supor $a \neq 0$. Concluímos $r|s(y_0-y)$ e daí $r|y_0-y$ pois $mdc(r,s)=1$.

Logo, existe $t \in \mathbb{Z}$ tal que $rt = y_0-y$ de onde vem $y = y_0-rt = y_0-\frac{a}{d}t$.

Segue que $r(x-x_0) = s(y_0-y) = srt$ e então $x-x_0 = st$, pois $r \neq 0$. Isto dá $x = x_0+st = x_0+\frac{b}{d}t$.

Logo, temos

$$\begin{cases} x = x_0+\frac{b}{d}t \\ y = y_0-\frac{a}{d}t \end{cases}$$

para algum $t \in \mathbb{Z}$, como afirmado.

□

Exemplo 3.16. Analisar se existem soluções inteiras da equação

$$12x+5y = 7$$

Nota-se que o $mdc(12,5) = 1$ e $1|7$. Portanto, essa equação diofantina linear admite solução.

Pelo algoritmo de Euclides podemos escrever 1 como combinação linear de 12 e 5

$1 = 5-2.2 = 5-2(12-2.5) = 5-2.12+4.5 = 5.5-2.12 = 12(-2)+5(5) = 1.$

Multiplicando ambos os lados por 7, obtemos

$$12(-14)+5(35) = 7.$$

Concluímos então que $(-14,35)$ é uma solução particular de $12x+5y=7$. Dessa forma, as soluções desta equação são dadas por

$$x = -14+5t,\ y = 35-12t, \text{ com } t \in \mathbb{Z}.$$

3.2.6 Pequeno Teorema de Fermat e Números Especiais

Faremos o estudo dos números primos, que desempenham papel importante dentro da teoria dos números e de toda a Matemática. A estes números estão associados problemas cujas soluções têm resistido as tentativas de várias gerações de matemáticos, como visto em [14].

Definição 7. Um número $p \in \mathbb{N}$ é denominado primo, se $p > 1$ e seus únicos divisores são p e 1. Indicamos por $P = \{p \in \mathbb{N} | p \text{ é } primo\}$ o conjunto de todos os números primos.

Podemos dizer que

$$p \in P \Leftrightarrow (\forall a, b \in \mathbb{N} : p = ab \Rightarrow a = p \; e \; b = 1 \; ou \; a = 1 \; e \; b = p).$$

Um número $n > 1$ é dito composto se ele não é primo. Assim, n é composto, se existem $r, s \in \mathbb{N}$, $1 < s \leq r < n$ com $n = rs$.

Por exemplo, $2, 3, 5, 7, 11$ e 13 são números primos, enquanto $4, 6, 8, 9, 10$ e 12 são compostos.

Com o Lema de Euclides podemos estabelecer a seguinte propriedade fundamental dos números primos.

Proposição 9. Sejam a, b, $p \in \mathbb{N}$, com p primo. Se $p|ab$, então $p|a$ ou $p|b$.

Demonstração. Suponhamos $p|ab$ e $p \nmid a$. Agora se $p \nmid a$, então $mdc(p, a) = 1$ e portanto, pela Proposição 4, segue que $p|b$. □

Observamos que com esta proposição os números primos ficam caracterizados totalmente, pois se $n = rs$ é composto $(1 < s \leq r < n)$, podemos ter $n|rs$. Porém $n \nmid r$ e $n \nmid s$.

Por exemplo, se $7|ab$, sabemos que um dos fatores a ou b (ou ambos) é múltiplo de 7. Mas, temos que $4|36 = 2.18$, porém nem $4 \nmid 2$ e nem $4 \nmid 18$.

Desde aproximadamente, 500 anos antes de Cristo, os chineses já sabiam que se p é um número primo, então $p|2^p - 2$. Pierre de Fermat, no século XVII, generalizou este resultado, através de um pequeno, mas notável teorema.

Para demonstrar o Pequeno Teorema de Fermat faremos o uso do lema a seguir.

Primeiramente se p e i são dois números naturais, nesse caso com $0 < i < p$, chama-se número binomial de classe i ao número $\binom{p}{i}$ dado por

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p(p-1)(p-2)...(p-i+1)(p-i)!}{i!(p-i)!} = \frac{p(p-1)...(p-i+1)}{i!}.$$

Lema 2. Seja p um número primo. Os números $\binom{p}{i}$, onde $0 < i < p$, são todos divisíveis por p.

Demonstração. O resultado vale trivialmente para $i = 1$, pois $\binom{p}{1} = p$ e $p|p$. Podemos, então, supor $1 < i < p$. Neste caso $i!|p(p-1)...(p-i+1)$. Como $(i!, p) = 1$, decorre que $i!|(p-1)...(p-i+1)$, e o resultado se segue, pois como visto anteriormente:

$$\binom{p}{i} = \frac{p(p-1)...(p-i+1)}{i!}.$$

Teorema 3.17. (**Pequeno Teorema de Fermat**) Dado um número primo p, tem-se que p divide o número $a^p - a$, para todo $a \in \mathbb{N}$.

Demonstração. Vamos provar o resultado por indução sobre a. O resultado vale para $a = 1$, pois $p|0$. Supondo o resultado válido para a, iremos provar para $a+1$. Pela fórmula do Binômio de Newton,

$$(a+1)^p - (a+1) = a^p - a + \binom{p}{1}a^{p-1} + ... + \binom{p}{p-1}a.$$

Pelo lema anterior e pela hipótese de indução, o segundo membro da igualdade acima é divisível por p.

□

Como consequência do Pequeno Teorema de Fermat, podemos escrever o seguinte corolário.

Corolário 3. Se p é um número primo e se a é um número natural não divisível por p, então p divide $a^{p-1} - 1$.

Demonstração. Como, pelo Pequeno Teorema de Fermat, $p|a(a^{p-1} - 1)$ e como $(a, p) = 1$, segue, imediatamente, que p divide $a^{p-1} - 1$. □

O interessante é observar que o Pequeno Teorema de Fermat nos serve como um teste de não primalidade.

Dado $m \in \mathbb{N}$, com $m > 1$, se existir algum $a \in \mathbb{N}$, com $mdc(a, m) = 1$, e $m \nmid a^{m-1} - 1$, então m não é primo.

Porém, é interessante salientar que se um número, $m > 1$, atender a condição de $m|a^{m-1} - 1$, esse número não é necessariamente primo. Isso pode ser visto no exemplo abaixo.

Exemplo 3.17. Seja $a \in \mathbb{N}$ tal que $mdc(a, 3) = mdc(a, 11) = mdc(a, 17) = 1$. Isso é equivalente a $mdc(a, 561) = 1$, pois $3.11.17 = 561$.

Por outro lado,

$$mdc(a^{280}, 3) = mdc(a^{56}, 11) = mdc(a^{35}, 17) = 1.$$

Pelo Pequeno Teorema de Fermat, 3 divide $(a^{280})^2 - 1 = a^{560} - 1$, 11 divide $(a^{56})^{10} - 1 = a^{560} - 1$ e 17 divide $(a^{35})^{16} - 1 = a^{560} - 1$. Daí segue que 561 divide $a^{560} - 1$, para todo a tal que $mdc(a, 561) = 1$, sem que 561 seja primo.

Apresentaremos agora algumas propriedades de alguns números primos.

Primos de Fermat e de Mersenne

Nessa parte será feito o estudo de alguns números primos, como números de Fermat em homenagem a Pierre de Fermat (1601-1665), que após Euclides e Eratóstenes, foi considerado o primeiro matemático a contribuir para o desenvolvimento da Teoria dos Números.

Proposição 10. Sejam a e n números naturais maiores do que 1. Se $a^n + 1$ é primo, então a é par e $n = 2^m$, com $m \in \mathbb{N}$.

Demonstração. Suponhamos que $a^n + 1$ seja primo, onde $a > 1$ e $n > 1$. Logo, a tem que ser par, pois, caso contrário, $a^n + 1$ seria par e maior do que dois, o que contraria o fato de ser primo.

Se n tivesse um divisor primo p, diferente de 2, teríamos $n = n'p$ com $n' \in \mathbb{N}$, e $n' \neq 0$.

Portanto, pelo Teorema 3.7, $a^{n'} + 1$ dividiria $(a^{n'})^p + 1 = a^n + 1$, contradizendo o fato desse último número ser primo. Isto implica que n é da forma 2^m.

□

Os números de Fermat são os números da forma $F_n = 2^{2^n} + 1$, $n = 0, 1, ...$

Em 1640, Fermat afirmou que acreditava que todos os números dessa forma eram primos, baseando-se no fato de que $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ são primos.

Mas em 1732, Leonard Euler, provou que $F_5 = 2^{2^5} + 1 = 641$ x 6700417, portanto um número composto. Até hoje, não se sabe se existem outros números de Fermat além dos cinco primeiros, que são chamados de primos de Fermat.

Proposição 11. Sejam a e n números naturais maiores do que 1. Se $a^n - 1$ é primo, então $a = 2$ e n é primo.

Demonstração. Suponhamos que $a^n - 1$ seja primo, com $a > 1$ e $n > 1$. Suponhamos, por absurdo, que $a > 2$. Logo $a - 1 > 1$ e $a - 1 | a^n - 1$ pelo Teorema 3.6 e, portanto, $a^n - 1$ não é primo, assim temos uma contradição. Consequentemente $a = 2$.

Por outro lado, suponhamos, por absurdo, que n não é primo. Temos que $n = rs$ com $r > 1$ e $s > 1$. Como $2^r - 1$ divide $(2^r)^s - 1 = 2^n - 1$, novamente considerando o Teorema 3.6, contradiz o fato de $2^n - 1$ ser primo. Portanto, n é primo.

□

Os números de Mersenne são os números da forma $M_p = 2^p - 1$, onde p é um número primo.

Para p pertencente ao intervalo $2 \leq p \leq 5000$ os números de Mersenne que são primos são chamados de primos de Mersenne e correspondem aos seguintes valores de p : $2, 3, 5, 7, 13, 19, 31, 61, 89, 107, 127, 521, 607, 1279$, $2203, 3217, 4253$ e 4423.

Em Janeiro de 2016, o pesquisador estadunidense Curtis conseguiu calcular o maior número primo de Mersenne até o momento. Este número é formado por mais de 22 milhões de dígitos, e é da forma $2^{74207281} - 1$. Vale lembrar que esse tipo de sequência numérica é um componente importante para os sistemas de encriptação usados em computadores (Ver [15]).

3.2.7 Teorema Fundamental da Aritmética

Teorema 3.18. (Teorema Fundamental da Aritmética) Todo número $1 < n \in \mathbb{N}$ ou é primo ou se escreve como produto de números primos, de forma única (a menos da ordem dos fatores).

Demonstração. Usando a segunda forma do Princípio de Indução, podemos escrever que

1^o) Se $n = 2$, o resultado é óbvio.

2^o) Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos, então, n composto.

Logo, existem números naturais n_1 e n_2 tais que $n = n_1.n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, ..., p_r$ e $q_1, ..., q_s$ tais que $n_1 = p_1...p_r$ e $n_2 = q_1...q_s$. Portanto, $n = p_1...p_r q_1...q_s$.

Para provar a unicidade da escrita suponhamos, agora que, $n = p_1...p_r = q_1...q_s$, onde os p_i e q_j são números primos. Como $p_1 | q_1...q_s$, concluímos, aplicando-se repetidas vezes a Proposição 9, que p_1 tem que dividir alguns dos fatores $q_1, q_2, ..., q_s$. Logo existe $k (1 \leq k \leq s)$ com $p_1 | q_k$. Como p_1 e q_k são primos, temos $p_1 = q_k \geq q_1$. Da mesma forma, $q_1 | p_l$ para algum $l (1 \leq l \leq r)$ e segue $q_1 = p_l \geq p_1$. Assim, $p_1 = q_1$. Agora, de $p_1.p_2...p_r = q_1.q_2...q_s$ segue que

$$p_2...p_r = q_2....q_s.$$

Portanto, por indução, concluímos $r - 1 = s - 1$, isto é, $r = s$ e $p_2 = q_2$, $p_3 = q_3$,...,$p_r = q_r$ que junto com $p_1 = q_1$ fica provado o que queríamos demonstrar.

□

Agrupando no Teorema Fundamental da Aritmética, os fatores primos repetidos, se necessário, e ordenando os números primos em ordem crescente podemos enunciar o seguinte teorema.

Teorema 3.19. Para todo número $1 < n \in \mathbb{N}$ existem únicos primos distintos $p_1, p_2, ..., p_r$ (os quais podemos supor em ordem natural $p_1 < ... < p_r$) e únicos números $a_1, a_2, ..., a_r \in \mathbb{N}$ de tal maneira que

$$n = p_1^{a_1}.p_2^{a_2}...p_r^{a_r} = \prod_{k=1}^{r} p_k^{a_k}.$$

O produto $\prod_{k=1}^{r} p_k^{a_k}$ chama-se decomposição primária de n.

É interessante notar que um número natural $n > 1$, escrito na forma $n = p_1^{a_1}...p_r^{a_r}$ é um quadrado perfeito, se, e somente se, cada expoente a_i é par.

Ao estudarmos os números primos, nos vem a ideia se o conjunto formado pelos números primos é finito ou não. Essa duvida foi respondida por Euclides de Alexandria em 300 a.C. no livro IX dos Elementos. Ele provou usando redução ao absurdo, pela primeira vez em Matemática, sendo esta prova considerada uma das pérolas em Matemática.

Teorema 3.20. Existem infinitos números primos.

Demonstração. Suponhamos que os números primos formassem um conjunto finito, representado por $P = \{p_1, p_2, ..., p_r\}$. Consideremos um número natural $n = p_1.p_2....p_r + 1$. Pelo Teorema Fundamental da Aritmética, este $n > 1$ é divisível por algum primo q. Pela suposição, $q = p_k$ para algum $k \in \{1, 2, ..., r\}$ e, consequentemente, esse q divide o produto $p_1p_2...p_r$. Mas, isto implica também que q divide 1, o que é um absurdo. Logo, nenhum conjunto finito pode conter todos os primos.

□

Ao saber da infinitude dos números primos, nos perguntamos, se é possível obter uma lista que contenha números primos até uma dada ordem.

Será apresentado a seguir, um dos métodos mais antigos para obter uma tabela de números primos, chamado de Crivo de Eratóstenes, devido ao matemático grego Eratóstenes, que viveu por volta de 230 anos antes de Cristo. Esse método, descrito em [13] e [16], permite determinar todos os números primos até a ordem que se desejar, mas não é muito eficiente para ordens elevadas.

Para se obter os números primos até uma certa ordem n, escreva os números de 2 até n em uma tabela.

O primeiro desses números, o 2, é primo. Risque todos os demais múltiplos de 2 na tabela, pois não são primos.

O próximo número não riscado é o 3, que também é primo. Risque todos os múltiplos de 3 na tabela, pois esses não são primos.

O seguinte número não riscado é o 5 que é um número primo. Risque os demais múltiplos de 5 na tabela.

Seguindo, temos que o próximo número não riscado é o 7, que também é primo. Risque os demais múltiplos de 7 na tabela.

Note que o procedimento segue da mesma maneira enquanto dado um número primo p, $p^2 \leq n$. Isso se deve a uma consequência dada pelo próprio Eratóstenes.

Faremos como exemplo o resultado para $n = 150$. Para esse caso, o procedimento termina quando chegarmos no número primo 11, visto que para o próximo primo 13, quando elevado ao quadrado resulta em 169 que é maior que 150.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
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
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150

Tabela 1: Crivo de Eratóstenes.

Ao término desse procedimento, os números não riscados são todos primos menores ou iguais a n.

Lema 3. Se um número natural $n > 1$ não é divisível por nenhum número primo p tal que $p^2 \leq n$, então ele é primo.

Demonstração. Suponhamos, por absurdo, que n não seja divisível por nenhum número primo p tal que $p^2 \leq n$ e que não seja primo. Seja q o menor número primo que divide n; então, $n = qn_1$, com $q \leq n_1$. Segue daí que $q^2 \leq qn_1 = n$. Logo, n é divisível por um número primo q tal que $q^2 \leq n$, absurdo. □

Note que o Lema acima descrito também nos fornece um teste de primalidade, pois, para verificar se um certo número n é primo, basta verificar que não é divisível por nenhum primo p que não supere $\sqrt{n}$.

Exemplo 3.18. Para mostrar que o número 221 é composto basta testar se ele é múltiplo de algum dos números primos $p = 2, 3, 5, 7, 11$ e 13 já que o próximo primo 17 é tal que $17^2 = 289 > 221$.

Fazendo esse procedimento obtemos que 221 é divisível por 13 $(221 = 13 \text{ x } 17)$, portanto não é primo.

A distribuição dos números primos dentro dos naturais ainda é algo desconhecido e está ligada a muitos problemas em estudos.

Pela tabela acima, nota-se que existem pares de números primos que diferem de duas unidades. Podemos listar alguns deles: $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, $(59,61)$, $(71,73)$ entre outros.

Esses pares de primos consecutivos são chamados de primos gêmeos e eles diferem de 2 unidades.

Definição 8. Um par de números $(p, p+2)$ é denominado um gêmeo de primos se ambos, p e $p+2$ são primos.

É interessante citar que até o presente momento os matemáticos ainda não sabem dizer se os pares de primos gêmeos formam um conjunto finito ou infinito.

Um outro problema matemático, ainda em aberto, é a conjectura de Goldbach (lembrando que o termo Conjectura, em uma linguagem mais coloquial significa palpite, chute).

O matemático prussiano Christian Goldbach, numa certa carta de 7 de junho de 1742 endereçada a Leonard Euler, um dos maiores matemáticos, propôs que se provasse que todo número natural maior do que 5 pode ser escrito como soma de três números primos:

Por exemplo: $6 = 2+2+2$, $7 = 3+2+2$, $8 = 3+3+2$, $9 = 5+2+2$, $10 = 5+3+2$, e assim por diante.

Euler, por sua vez, respondeu que acreditava na conjectura, mas que prová-la era equivalente a mostrar que todo número par maior ou igual a 4 era soma de dois números primos.

Por exemplo: $4 = 2+2$, $6 = 3+3$, $8 = 5+3$, $10 = 3+7$ etc.

Em 1937, o matemático russo Ivan Vinogradov, demonstrou o difícil teorema que garante que todo número natural ímpar, suficientemente grande, pode ser escrito como soma de, no máximo, três números primos.

Muitos problemas ainda por resolver estão relacionados com a distribuição dos números primos dentro da sequência dos números naturais.

3.3 Congruências

Realizaremos agora um estudo da aritmética com os restos da divisão euclidiana por um número dado.

Definição 9. Seja $n \in \mathbb{N}$, com $n \neq 0$, um número fixo. Dois números a, $b \in \mathbb{Z}$ chamam-se congruentes módulo n, se os restos de sua divisão euclidiana por n são iguais. Quando os inteiros a e b são congruentes módulo n, escreve-se:

$$a \equiv b \ (mod\ n).$$

Proposição 12. Suponha que $a, b \in \mathbb{N}$ são tais que $b \geq a$. Tem-se que $a \equiv b \ (mod\ n)$ se, e somente se, $n|b-a$.

Demonstração. Sejam $a = nq + r$, com $r < n$ e $b = nq' + r'$, com $r' < n$ as divisões euclidianas de a e b por n, respectivamente. Logo,

$$b - a = \begin{cases} n(q'-q) + (r'-r), \ se\ r' \geq r \\ n(q'-q) - (r-r'), \ se\ r \geq r' \end{cases}$$

Portanto, $a \equiv b \ (mod\ n)$ se, e somente se $r = r'$, o que em vista da igualdade acima, é equivalente a dizer que $n|b-a$, já que $|r-r'| < n$.

Por exemplo, $22 \equiv 7 \ (mod\ 5)$, pois os restos da divisão de 22 e de 7 por 5 são iguais a 2.

Quando a e b não possuírem o mesmo resto na divisão por n, dizemos que a relação $a \equiv b \ (mod\ n)$ é falsa. Nesse caso, escrevemos $a \not\equiv b \ (mod\ n)$.

Como o resto da divisão de um número natural qualquer por 1 é sempre zero, temos que $a \equiv b \ (mod\ 1)$, para quaisquer $a, b \in \mathbb{N}$. Portanto, consideremos sempre $n > 1$.

Todo número inteiro é congruente módulo n ao seu resto pela divisão euclidiana por n, e portanto, é congruente módulo n a um dos números $0, 1, ..., n-1$. E dentre esses números, dois deles não são congruentes módulo n entre si.

Chamaremos de sistema completo de resíduos módulo n a todo conjunto de números inteiros cujos restos pela divisão por n são os números $0, 1, ..., n-1$, em qualquer ordem e sem repetições.

Exemplo 3.19. Para $n = 7$, temos que $\{0, 1, 2, 3, 4, 5, 6\}$ é o conjunto dos menores restos não-negativos módulo 7. E que $\{-23, 15, 70, -47, 83, -4, 36\}$ é um sistema completo de resíduos módulo 7, pois $-23 \equiv 5$, $15 \equiv 1$, $70 \equiv 0$, $-47 \equiv 2$, $83 \equiv 6$, $-4 \equiv 3$, $36 \equiv 4 \ (mod\ 7)$.

Portanto, um sistema de resíduos completo módulo n possui n elementos.

O que tornam as congruências tão úteis em problemas de divisibilidade e compatível com as operações de adição e multiplicação nos inteiros é o fato de ser uma relação de equivalência.

Como visto em [11] podemos estabelecer as seguintes propriedades.

Teorema 3.21. (Propriedades Fundamentais das Congruências). Seja $n \in \mathbb{N}$, a, b, c, $d \in \mathbb{Z}$. Temos:

1) (Reflexividade): $a \equiv a \ (mod\ n)$.

Demonstração. $a \equiv a \ (mod\ n)$ pois $n|a-a=0$. □

2) (Simetria): Se $a \equiv b \ (mod\ n)$, então $b \equiv a \ (mod\ n)$.

Demonstração. Se $n|a-b$, então $n|-(a-b) \Leftrightarrow n|b-a$. □

3) (Transitividade): Se $a \equiv b \ (mod\ n)$ e $b \equiv c \ (mod\ n)$, então $a \equiv c \ (mod\ n)$.

Demonstração. Se $n|a-b$ e $n|b-c$, então $n|(a-b)+(b-c) \Leftrightarrow n|a-c$. □

4) (Compatibilidade com a soma e diferença): Pode-se somar e subtrair membro a membro

$$\begin{cases} a \equiv b \ (mod\ n) \\ c \equiv d \ (mod\ n) \end{cases} \Rightarrow \begin{cases} a+c \equiv b+d \ (mod\ n) \\ a-c \equiv b-d \ (mod\ n) \end{cases}$$

Demonstração. Se $n|a-b$ e $n|c-d$, então $n|(a-b)+(c-d)$.

Como $(a-b)+(c-d)$ pode ser escrito da forma $(a+c)+(-b-d)=(a+c)-(b+d)$, então $n|(a+c)-(b+d)$. O outro caso é análogo.

Como consequência disso, temos que se $a \equiv b \ (mod\ n)$, então $ka \equiv kb \ (mod\ n)$ para todo $k \in \mathbb{Z}$. □

5) (Compatibilidade para o produto): Pode-se multiplicar membro a membro em uma congruência

$$\begin{cases} a \equiv b \ (mod\ n) \\ c \equiv d \ (mod\ n) \end{cases} \Rightarrow \quad ac \equiv bd \ (mod\ n)$$

Demonstração. $n|(a-b)-(c-d) \Leftrightarrow n|(a-b)+(-c+d) \Leftrightarrow n|(a-c)+(d-b) \Leftrightarrow n|(a-c)-(b-d)$ e $n|(a-b)c+(c-d)b \Leftrightarrow n|ac-bd$.

Em particular, se $a \equiv b \ (mod\ n)$, então $a^k \equiv b^k \ (mod\ n)$ para todo $k \in \mathbb{N}$. □

6) (Cancelamento): Se $mdc(c,n)=1$, então

$$ac \equiv bc \ (mod\ n) \Leftrightarrow a \equiv b \ (mod\ n).$$

Demonstração. Como $mdc(c,n) = 1$ temos que $n|ac - bc \Leftrightarrow n|(a-b)c \Leftrightarrow n|a-b$ pela Proposição 4. □

Vejamos alguns exemplos:

1) Demonstrar que $31|20^{15} - 1$.

Isso equivale a mostrar que $20^{15} \equiv 1\ (mod\ 31)$. Para isso, podemos notar que

$$20 \equiv -11\ (mod\ 31)$$

e assim $20^2 \equiv (-11)^2 (mod\ 31) \Leftrightarrow 20^2 \equiv 121\ (mod\ 31)$.

Como $121 \equiv -3\ (mod\ 31)$ temos que

$$20^2 \equiv -3\ (mod\ 31).$$

Multiplicando

$$\begin{cases} 20 \equiv -11\ (mod\ 31) \\ 20^2 \equiv -3\ (mod\ 31) \end{cases} \quad \text{membro a membro}$$

obtemos $20^3 \equiv 33\ (mod\ 31)$ e como $33 \equiv 2\ (mod\ 31)$ temos,

$$20^3 \equiv 2 (mod\ 31).$$

Elevando a 5, temos que $20^{15} \equiv 2^5 = 32$ e como $32 \equiv 1\ (mod\ 31)$, obtemos $20^{15} \equiv 1\ (mod\ 31)$, como desejado.

2) Se $a \equiv b\ (mod\ 4)$, mostre que $a \equiv b\ (mod\ 2)$.

Para resolver esse exercício faz-se o uso da seguinte proposição.

Proposição 13. Sejam $a, b \in \mathbb{N}$, $m, n \in \mathbb{N}\backslash\{0,1\}$. Temos que se $a \equiv b\ (mod\ m)$ e $n|m$ então $a \equiv b\ (mod\ n)$.

Demonstração. Se $a \equiv b\ (mod\ m)$ então $m|(b-a)$. Como $n|m$, segue que $n|(b-a)$. Logo, $a \equiv b\ (mod\ n)$. □

Como no exercício temos $a \equiv b\ (mod\ 4)$ e $2|4$, então $a \equiv b\ (mod\ 2)$.

Em congruências ainda podemos estabelecer a seguinte definição

Definição 10. Dado $n \in \mathbb{N}$. Uma congruência linear é uma congruência da forma

$$ax \equiv b\ (mod\ n)$$

onde $a, b \in \mathbb{Z}$ são dados e as soluções $x \in \mathbb{Z}$ são procuradas.

Exemplo 3.20. $2x \equiv 5\ (mod\ 6)$.

Essa congruência linear não tem solução. Podemos escrever $2x-5 \equiv 0\ (mod\ 6)$. Para isso, precisamos de um número ímpar, $2x-5$, que dividido por um número par, no caso 6, resulte em uma divisão exata, o que é impossível.

Primeiramente, vamos dar um critério para estabelecer se tais congruências admitem ou não soluções.

Proposição 14. Dados $n \in \mathbb{N}$, e a, $c \in \mathbb{Z}$, com $n > 1$, a congruência $ax \equiv c\ (mod\ n)$ possui solução se e somente se, $mdc(a,n)|c$.

Demonstração. Suponha que a congruência $ax \equiv c\ (mod\ n)$ tenha uma solução x, logo, temos que $n|c-ax$ ou $n|ax-c$, o que equivale a existência de y tal que $c-ax = ny$ ou $ax-c = ny$. Portanto, pelo menos uma das seguintes equações $ny+ax = c$ ou $ax-ny = c$ admite solução. Logo, pela Proposição 7, $mdc(a,n)|c$.

Reciprocamente, suponha que $mdc(a,n)|c$. Logo, em virtude da Proposição 7, a equação $ax-ny = c$ admite uma solução x, y. Portanto, $ax = c+ny$ e, consequentemente, x é solução da congruência pois, $ax \equiv c\ (mod\ n)$. □

Se x_0 é solução da congruência $ax \equiv c\ (mod\ n)$, então todo x tal que $x \equiv x_0\ (mod\ n)$ é também solução da congruência pois,

$$ax \equiv ax_0 \equiv c\ (mod\ n).$$

Com isso toda solução particular, determina, automaticamente, uma infinidade de soluções da congruência, congruentes entre si.

O interesse é determinar uma coleção completa de soluções duas a duas incongruentes módulo n, as quais serão chamadas de sistema completo de soluções incongruentes da congruência.

Proposição 15. Sejam $n \in \mathbb{N}$ e $a,b \in \mathbb{Z}$ e seja $d = mdc(a,n)$. Se $d|b$, então $ax \equiv b\ (mod\ n)$ possui exatamente d soluções incongruentes entre si módulo n. Se $x_0 \in \mathbb{Z}$ é uma solução particular (chamada de solução minimal), então d soluções incongruentes são obtidas por

$$x_0,\ x_0+\tfrac{n}{d},\ x_0+\tfrac{2n}{d},\ x_0+\tfrac{3n}{d},\ldots,\ x_0+(d-1)\tfrac{n}{d}.$$

Demonstração. Seja $d|b$ e seja $x_0 \in \mathbb{Z}$ com $ax_0 \equiv b\ (mod\ n)$, isto é, $ax_0+ny_0 = b$ para algum $y_0 \in \mathbb{Z}$. Pela Proposição 8, toda solução de $ax \equiv b\ (mod\ n)$ é então da forma $x = x_0+\frac{n}{d}t$, com $t \in \mathbb{Z}$.

Escrevendo-se $t = qd+k$, com q, $k \in \mathbb{Z}$ e com $0 \leq k \leq d-1$ temos

$$x = x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}(qd+k) = x_0 + qn + k\frac{n}{d} \equiv x_0 + k\frac{n}{d}\ (mod\ n).$$

Mostramos portanto que toda solução é congruente módulo n a um dos números indicados.

Mais ainda, de $x_0 + j\frac{n}{d} \equiv x_0 + k\frac{n}{d}\ (mod\ n)$, com $0 \leq j, k \leq d-1$ segue que

$$j\tfrac{n}{d} \equiv k\tfrac{n}{d}\ (mod\ n).$$

Assim,

$$j\tfrac{n}{d} = k\tfrac{n}{d} + ln, \text{ com } l \in \mathbb{Z}.$$

Dividindo-se por $\frac{n}{d}$, segue $j = k + ld \equiv k\ (mod\ d)$.

De $0 \leq |j-k| \leq d-1$, concluímos $l = 0$ e $j = k$.

Isto mostra que as d soluções indicadas são incongruentes módulo n. □

Exemplo 3.21. A aplicação de congruência a seguir nos conta algo interessante. Em 1969, D. J. Lewis afirmou que a equação $x^3 - 117y^3 = 5$ tem no máximo 18 soluções inteiras. Dois anos depois, R Finkelstein e H.Lodon, usando métodos de Teoria Algébrica dos Números, provaram que essa equação não possuía nenhuma solução. Mas em 1973, F. Halter-Koche e V.St.Udresco conseguiram enxergar uma prova mais simples para esse caso, que é descrita abaixo.

Queremos mostrar que a equação $x^3 - 117y^3 = 5$ não possui soluções inteiras. Observamos que como 117 é múltiplo de 9, qualquer solução inteira deve satisfazer

$$x^3 - 117y^3 \equiv 5\ (mod\ 9) \Leftrightarrow x^3 \equiv 5\ (mod\ 9).$$

Porém, x só pode deixar resto $0, 1, ..., 8$ na divisão por 9. Analisando estes 9 casos, temos

$x\ (mod\ 9)$	0	1	2	3	4	5	6	7	8
$x^3\ (mod\ 9)$	0	1	8	0	1	8	0	1	8

Ou seja, x^3 só pode deixar resto 0, 1 ou 8 na divisão por 9. Logo, $x^3 \equiv 5\ (mod\ 9)$ é impossível e a equação não possui soluções inteiras.

Exemplo 3.22. Resolver a equação $8x \equiv 4\ (mod\ 12)$.

Como $d = mdc(8,12) = 4$ e $4|4$, a congruência tem 4 soluções módulo 12.

Por tentativa, obtém-se, $x_0 = 2$ como solução minimal. Portanto, as soluções módulo 12 são

$$2, 2+\tfrac{12}{4}, 2+2\tfrac{12}{4}, 2+3\tfrac{12}{4} = 2, 5, 8, 11.$$

Pela Proposições 13 e 14 podemos estabelecer o seguinte resultado.

Corolário 4. Sejam $n \in \mathbb{N}$, e $a, x, y \in \mathbb{Z}$ com $d = mdc(a,n)$. Então,

$$ax \equiv ay \ (mod\ n) \Rightarrow x \equiv y \ (mod\ \tfrac{n}{d}).$$

Demonstração. Como $d = mdc(a,n)$, temos que $a = d.a'$ e $n = d.n'$ e que $mdc(a',n') = 1$. Assim,

$ax \equiv ay \ (mod\ n) \Leftrightarrow n|ax - ay \Leftrightarrow n|a(x-y) \Leftrightarrow dn'|da'(x-y) \Leftrightarrow n'|a'(x-y) \Leftrightarrow \frac{n}{d} = n'|(x-y) \Leftrightarrow x \equiv y \ (mod\ \frac{n}{d})$.

□

Portanto, numa congruência módulo n um fator comum pode ser cancelado, desde que se observe que a nova congruência só é válida módulo $\frac{n}{d}$.

Consideremos $a, n \in \mathbb{N}$ com $n > 1$ e $d = mdc(a,n)$. Quando $d = 1$, temos o seguinte resultado.

Lema 4. Se $mdc(a,n) = 1$, então existe x inteiro tal que $ax \equiv 1 \ (mod\ n)$. Tal inteiro é único módulo n. Se $mdc(a,n) > 1$ não existe tal inteiro.

Demonstração. Se $mdc(a,n) = 1$, pelo Teorema de Bézout, existem $x, y \in \mathbb{Z}$ com $ax + ny = 1$, mas $ax + ny \equiv ax \ (mod\ n)$; logo $ax \equiv 1 \ (mod\ n)$.

Se $x' = x \ (mod\ n) \Rightarrow ax' \equiv ax \equiv 1 \ (mod\ n)$.

Se $aZ \equiv 1 \ (mod\ n) \Rightarrow aZ \equiv 1 \equiv ax \ (mod\ n) \Rightarrow n|aZ - ax = a(Z-x)$.

Como $mdc(a,n) = 1 \Rightarrow n|Z - x \Rightarrow Z \equiv x \ (mod\ n)$.

Se $mdc(a,n) = d > 1$ e $ax \equiv 1 \ (mod\ n) \Rightarrow n|1 - ax \Rightarrow \exists\, y; 1 - ax = ny \Rightarrow ax + ny = 1$.

$$\left.\begin{array}{l} d|a \Rightarrow d|ax \\ d|n \Rightarrow d|ny \end{array}\right\} \Rightarrow d|ax + ny = 1,$$ o que é um absurdo, pois 1 não pode ser múltiplo de $d > 1$.

□

A solução de $ax \equiv 1 \ (mod\ n)$, com $mdc(a,n) = 1$ é única e será chamada de inverso multiplicativo módulo n.

Exemplo 3.23. Encontre $x \in \mathbb{Z}$, tal que $x \equiv 1 \ (mod\ 11)$ e $x \equiv 2 \ (mod\ 7)$:

Solução: Se $x \equiv 1 \ (mod\ 11) \Rightarrow x = 11k + 1$, $k \in \mathbb{Z}$.

Como $x \equiv 2 \ (mod\ 7)$ podemos escrever que:

$$11k+1 \equiv 2\ (mod\ 7) \Leftrightarrow 11k \equiv 1\ (mod\ 7) \Leftrightarrow 4k \equiv 1\ (mod\ 7).$$

Como $mdc(4,7) = 1$, essa congruência possui solução, que é o inverso multiplicativo de 4 módulo 7.

Quando fazemos 4.2 encontramos 8, que quando dividido por 7 resta 1. Então,

$$k \equiv 2\ (mod\ 7) \Leftrightarrow k = 7r+2,\ r \in \mathbb{Z}.$$

Substituindo k em x, obtemos que

$$x = 11(7r+2)+1 = 77r+23,\ r \in \mathbb{Z},\ \text{são soluções.}$$

A possibilidade de associar a divisão euclidiana à congruência modular nos permite utilizá-la para trabalhar com polinômios (Ver [12]).

Exemplo 3.24. Calcular o resto da divisão de $P(x) = x^5 + x + 1$ por $x^3 - 1$.

Sabe-se que $x^3 - 1 \equiv 0\ (mod\ x^3 - 1)$.

Somando 1 a ambos os lados da congruência, tem-se

$$x^3 \equiv 1\ (mod\ x^3 - 1).$$

Multiplicando ambos os lados da congruência por x^2, obtemos

$$x^3.x^2 \equiv 1.x^2\ (mod\ x^3 - 1)$$

$$x^5 \equiv x^2\ (mod\ x^3 - 1).$$

Podemos somar $x+1$ a ambos os lados, pois $x+1 \equiv x+1\ (mod\ x^3 - 1)$.

Com isso,

$$x^5 + x + 1 \equiv x^2 + x + 1\ (mod\ x^3 - 1).$$

Ou seja, o resultado da divisão de $x^5 + x + 1$ por $x^3 - 1$ é igual a $x^2 + x + 1$.

Exemplo 3.25. Provar que $P(x) = x^{999} + x^{888} + x^{777} + ... + x^{111} + 1$ é divisível pelo polinômio $D(x) = x^9 + x^8 + x^7 + ... + x^1 + 1$.

Podemos escrever $x^{10} - 1$ como $(x-1)(x^9 + x^8 + x^7 + ... + x^1 + 1)$.

Utilizando-se da notação de congruência podemos escrever que $x^{10} - 1 \equiv 0\ (mod\ x^9 + x^8 + x^7 + ... + 1)$, ou ainda que

$$x^{10} \equiv 1\ (mod\ x^9 + x^8 + x^7 + ... + 1).$$

Com isso, todas as potências x^{10} no $P(x)$ podem ser substituídas por 1.

$P(x) = x^{999} + x^{888} + x^{777} + ... + x^{111} + 1 \Rightarrow P(x) = x^9(x^{10})^{99} + x^8(x^{10})^{88} + x^7(x^{10})^{77} + ... + x(x^{10})^{11} + 1 \equiv x^9 + x^8 + ... + x + 1 \equiv 0 \ (mod\ x^9 + x^8 + x^7 + ... + x + 1)$.

Logo, $P(x)$ é divisível por $D(x)$.

A vantagem de usarmos congruência é que podemos substituir as potências grandes de x por outros termos que correspondem ao resto da divisão dessas potências pelo módulo dado no exercício.

Apresentaremos agora um algoritmo para resolver sistemas de congruências lineares. Como visto em [3], esse algoritmo é muito antigo e foi inventado pelos chineses e pelos gregos para resolver problemas de astronomia.

Esse método recebe o nome de Algoritmo Chinês do resto porque um dos primeiros lugares em que aparece é no livro Manual de Aritmética do Mestre Sun, escrito entre 287 d.C. e 473 d.C. O mesmo também é mencionado na Aritmética de Nicômaco de Gerasa.

Teorema 3.22. (**Teorema Chinês dos Restos**)

Sejam $m_1, m_2, ..., m_r$, inteiros positivos primos entre si, dois a dois, isto é, $mdc(m_i, m_j) = 1$ sempre que $i \neq j$, e sejam $a_1, a_2, ..., a_r$ inteiros quaisquer. Então o sistema de congruências

$$\begin{aligned} x &\equiv a_1 \ (mod\ m_1) \\ x &\equiv a_2 \ (mod\ m_2) \\ &\vdots \\ x &\equiv a_r \ (mod\ m_r) \end{aligned}$$

admite uma solução x. Além disso, as soluções são únicas módulo m, sendo $m = m_1.m_2....m_r$.

Demonstração. Seja $m = m_1.m_2....m_r$.

Temos que $M_j = \frac{m}{m_j} \equiv 0 \ (mod\ m_i)$, $\forall j \neq i$ e $mdc(\frac{m}{m_j}, m_j) = 1$, logo $\exists\ b_j \in \mathbb{Z}$ tal que $\frac{m}{m_j}.b_j \equiv 1 \ (mod\ m_j)$, pelo Lema 4.

Considere

$$x = a_1.\frac{m}{m_1}.b_1 + a_2.\frac{m}{m_2}.b_2 + ... + a_r.\frac{m}{m_r}.b_r.$$

Temos $x \equiv a_i.\frac{m}{m_i}.b_i \ (mod\ m_i)$.

Assim, $\frac{m}{m_i}.b_i \equiv 1 \ (mod\ m_i) \Rightarrow x \equiv a_i.1 \equiv a_i \ (mod\ m_i)\ \forall i \leq r$, isto é, x é solução do sistema.

Imaginemos que exista outra solução $y \in \mathbb{Z}$.

Temos $y \equiv a_i \ (mod\ m_i), \forall_i \leq r \Leftrightarrow y \equiv x \ (mod\ m_i), \forall_i \leq r \Leftrightarrow m_i | y - x, \forall_i \leq r \Leftrightarrow m_1.m_2...m_r | y - x \Leftrightarrow y \equiv x \ (mod\ m_1.m_2...m_r)$.

□

Uma aplicação do Teorema Chinês do Resto seria na astronomia. Veja um exemplo que ilustra esse fato, visto em [3].

Três satélites passarão sobre o Rio esta noite. O primeiro à 1 hora da madrugada, o segundo às 4 horas e o terceiro às 8 horas da manhã. Cada satélite tem um período diferente. O primeiro leva 13 horas para completar uma volta em torno da Terra, o segundo 15 horas e o terceiro 19 horas. Determine quantas horas decorrerão, a partir da meia-noite, até que os três satélites passem ao mesmo tempo sobre o Rio.

Para resolvermos este problema usando o Teorema Chinês dos Restos, chamaremos de x o número de horas contadas a partir da meia-noite de hoje, quando os três satélites passarão juntos sobre o Rio. O primeiro satélite passa sobre o Rio a cada 13 horas, a contar da 1 da madrugada. Logo, precisamos ter que $x = 1 + 13t$, para algum t inteiro positivo, o que é equivalente a congruência $x \equiv 1 \ (mod\ 13)$. As equações correspondentes aos outros dois satélites são

$$x \equiv 4 \ (mod\ 15) \quad \text{e} \quad x \equiv 8 \ (mod\ 19).$$

Como os módulos são diferentes não podemos somar ou subtrair. Para resolver usaremos o Teorema Chinês dos Restos, descrito anteriormente.

1º) Escrevendo $m = m_1.m_2.m_3$, temos $m = 13.15.19 = 3705$.

2º) Encontrar os M_j, que são da forma $M_j = \frac{m}{m_j}$.

$M_1 = \dfrac{13.15.19}{13} = 285$;

$M_2 = \dfrac{13.15.19}{15} = 247$;

$M_3 = \dfrac{13.15.19}{19} = 195$.

3º) Encontrar os b_j, que é o inverso multiplicativo M_j, módulo m_j, ou seja, $M_j.b_j \equiv 1 \ (mod\ m_j)$.

b_1:

$$285b_1 \equiv 1 \ (mod\ 13).$$

Correspondendo a uma equação diofantina temos que

$$285b_1 - 13t = 1, \text{com } t \in \mathbb{Z}.$$

Através do algoritmo de Euclides, obtemos

	21	1	12
285	13	12	1
12	1	0	

$$1 = 13 - 12.1$$
$$1 = 13 - (285 - 13.21).1$$
$$1 = 13 - 285 + 13.21$$
$$1 = (-1).285 + 13.22$$

Então $b_1 = -1$.

b_2:

$$247b_2 \equiv 1 \ (mod\ 15).$$

Correspondendo a uma equação diofantina, temos que

$$247b_2 - 15t = 1, \text{ com } t \in \mathbb{Z}.$$

Através do algoritmo de Euclides, obtemos

	16	2	7
247	15	7	1
7	1	0	

$$1 = 15 - 7.2$$
$$1 = 15 - (247 - 15.16).2$$
$$1 = 15 - 2.247 + 32.15$$
$$1 = 33.15 - 2.247$$

Então $b_2 = -2$.

b_3:

$$195b_3 \equiv 1 \ (mod\ 19).$$

Correspondendo a uma equação diofantina, temos que

$$195b_3 - 19t = 1, \text{ com } t \in \mathbb{Z}.$$

Através do algoritmo de Euclides, obtemos

	10	3	1	4
195	19	5	4	1
5	4	1	0	

$$1 = 5 - 4.1$$
$$1 = 5 - 1(19 - 3.5).1$$
$$1 = 1.5 - 1.19 + 3.5$$
$$1 = 4.5 - 1.19$$
$$1 = 4(195 - 19.10) - 1.19$$
$$1 = 4.195 - 40.19 - 1.19$$
$$1 = 4.195 - 41.19.$$

Então $b_3 = 4$.

A solução é única e da forma

$$x = \frac{m}{m_1} b_1.a_1 + \frac{m}{m_2} b_2.a_2 + \frac{m}{m_3} b_3.a_3.$$

$$x = \frac{3705}{13}(-1).1 + \frac{3705}{15}.(-2).4 + \frac{3705}{19}.4.8.$$

$$x = -285 - 1976 + 6240$$

$$x = 3979.$$

Como $3979 \equiv 274 \ (mod\ 3705)$, segue-se que 274 é a solução minimal única módulo 3705 e qualquer outra solução é da forma $274 + 3705\lambda$, com $\lambda \in \mathbb{N}$.

Portanto, os satélites passarão novamente juntos sobre o Rio após 274 horas, que corresponde a 11 dias e 10 horas.

Uma outra aplicação do Teorema Chinês do Resto por ser usada em uma brincadeira que pode ser proposta por um professor em sala de aula, como consta em [7].

O professor pede ao aluno que escolha um número menor que 1001 e que diga os restos r_7, r_{11}, r_{13} desse número quando dividido por $7, 11$ e 13, respectivamente. Sem nenhuma outra informação dada pelo aluno, o professor pode adivinhar o número escolhido pelo aluno.

Seja x um número natural e sejam r_7, r_{11} e r_{13} os seus restos pela divisão por 7,11 e 13, respectivamente.

Tem-se então que

$x \equiv r_7 \ (mod 7)$

$x \equiv r_{11}\ (mod 11)$

$x \equiv r_{13}\ (mod 13)$

Pelo Teorema Chinês do Resto, temos que

1º) $m = m_1.m_2.m_3 = 7.11.13 = 1001.$

2º) Encontrando os M_j obtemos

$$M_1 = \frac{m}{m_1} = \frac{1001}{7} = 143.$$

$$M_2 = \frac{m}{m_2} = \frac{1001}{11} = 91.$$

$$M_3 = \frac{m}{m_3} = \frac{1001}{13} = 77.$$

3º) Encontrar os b_j, que é o inverso multiplicativo M_j, módulo m_j:

b_1:

$$143b_1 \equiv 1\ (mod\ 7).$$

Correspondendo a equação diofantina temos que

$$143b_1 - 7t = 1, \text{ com } t \in \mathbb{Z}.$$

Através do algoritmo de Euclides, obtemos

	20	2	3
143	7	3	1
3	1	0	

$$1 = 7 - 3.2$$
$$1 = 7 - (143 - 7.20).2$$
$$1 = 7 - 2.143 + 7.40$$
$$1 = (-2).143 + 41.7$$

Então $b_1 = -2$.

b_2:

$$91b_2 \equiv 1\ (mod\ 11).$$

Correspondendo à equação diofantina temos que

$$91b_2 - 11t = 1, \text{ com } t \in \mathbb{Z}.$$

Através do algoritmo de Euclides, obtemos

	8	3	1	2
91	11	3	2	1
3	2	1	0	

$$1 = 3 - 2.1$$
$$1 = 3 - (11 - 3.3).1$$
$$1 = 3 - 11 + 3.3$$
$$1 = 4.3 - 1.11$$
$$1 = 4.(91 - 11.8) - 1.11$$
$$1 = 4.91 - 32.11 - 1.11$$
$$1 = 4.91 - 33.11$$

$$b_2 = 4.$$

b_3:

$$77b_3 \equiv 1 \ (mod\ 13).$$

Correspondendo a equação diofantina temos que

$$77b_3 - 13t = 1, \text{ com } t \in \mathbb{Z}.$$

Através do Algoritmo de Euclides, obtemos

	5	1	12
77	13	12	1
12	1	0	

$$1 = 13 - 12.1$$
$$1 = 13 - (77 - 13.5).1$$
$$1 = 13 - 77 + 13.5$$
$$1 = 6.13 - 77.1$$

$$b_3 = -1.$$

Logo, o sistema tem por solução x, que pode ser representado por

$$143.r_7(-2) + 91.r_{11}.4 + 77.r_{13}(-1) \equiv x \ (mod\ 1001)$$

$$= -286r_7 + 364r_{11} - 77r_{13} \equiv x \ (mod\ 1001).$$

De fato, o número que o aluno escolheu é o resto da divisão de $-286r_7 + 364r_{11} - 77r_{13}$ por 1001.

O professor poderá adaptar essa atividade para outros números contanto que observe que os números escolhidos para serem os divisores devem ser primos entre si e que o número deve ser menor que o produto destes.

3.3.1 Classes Residuais

Considere um número inteiro positivo qualquer $m > 1$. Dividiremos o conjunto dos números inteiros $\mathbb{Z}$ em subconjuntos, cada um formado pelos números inteiros que deixam o mesmo resto quando dividimos por m.

Assim, podemos definir classes residuais da seguinte maneira:

Definição 11. Seja m um número inteiro positivo fixo. Se a é um inteiro qualquer então a classe residual módulo m de a, denotada por $\overline{a}$ (ou $[a]$), consiste do conjunto formado por todos os inteiros que são congruentes ao inteiro módulo m, isto é,

$$\overline{a} = \{x \in \mathbb{Z};\ x \equiv a\ (mod\ m)\} = \{x \in \mathbb{Z};\ m|(x-a)\} = \{a + km;\ k \in \mathbb{Z}\}.$$

Observação:

1ª) Se $m = 1$ e $a \in \mathbb{Z}$ temos $\overline{a} = \{x \in \mathbb{Z};\ 1|(x-a)\} = \mathbb{Z}$.

2ª) As classes residuais módulo m também são denominadas inteiros módulo m ou classes de restos módulo m ou ainda, classes de congruência ou equivalência módulo m.

3ª) Se $a \in \mathbb{Z}$, então $\overline{a} \neq \emptyset$, pois como $a \equiv a(mod\ m)$ temos que $a \in \overline{a}$.

Podemos obter os subconjuntos:

$\overline{0} = \{x \in \mathbb{Z};\ x \equiv 0\ (mod\ m)\}$;

$\overline{1} = \{x \in \mathbb{Z};\ x \equiv 1\ (mod\ m)\}$;

$\vdots$

$\overline{m-1} = \{x \in \mathbb{Z};\ x \equiv m-1\ (mod\ m)\}$.

Paramos em $m-1$ pois, a partir daqui teremos repetições, pois $\overline{m} = \overline{0}$, $\overline{m+1} = \overline{1}$ e assim por diante. Em particular, $\overline{0}$ é o conjunto dos múltiplos de m.

Para ilustrar, é apresentado um exemplo de uso de classe residual para solucionar um problema de paridade (Ver [16]).

Exemplo 3.26. Seja $m = 2$. Então,

$$\overline{0} = \{x \in \mathbb{Z};\ x \equiv 0\ (mod\ 2)\} = \{x \in \mathbb{Z};\ x \text{ é par }\}.$$

$\overline{1} = \{x \in \mathbb{Z};\ x \equiv 1\ (mod\ 2)\} = \{x \in \mathbb{Z};\ x \text{ é ímpar }\}$.

Temos, portanto, que $\overline{a} = \overline{0}$ se, e somente se, a é par e $\overline{a} = \overline{1}$ se, e somente se, a é ímpar.

Proposição 16. Seja m um inteiro positivo fixo e sejam $\overline{a}$ e $\overline{b}$ as classes residuais módulo m de a e b. Então:

1) $\overline{a} = \overline{b} \Leftrightarrow a \equiv b\ (mod\ m)$.

2) $\overline{a} \cap \overline{b} = \emptyset$ ou $\overline{a} = \overline{b}$.

Demonstração. 1) Suponhamos que $\overline{a} = \overline{b}$.

Seja $x \in \overline{a} = \overline{b}$, então $a \equiv x\ (mod\ m)$ e $x \equiv b\ (mod\ m)$, pela propriedade da transitividade obtém-se que

$$a \equiv b\ (mod\ m).$$

Portanto, $\overline{a} = \overline{b} \Rightarrow a \equiv b\ (mod\ m)$.

Reciprocamente, suponha que $a \equiv b\ (mod\ m)$ e seja $x \in \overline{a}$.

Então,

$\begin{cases} a \equiv b\ (mod\ m) \\ x \equiv a\ (mod\ m) \end{cases}$. Pela transitividade, temos que $x \equiv b\ (mod\ m)$, e assim, $x \in \overline{b}$.

A mesma análise é feita supondo $x \in \overline{b}$. Logo, $\overline{a} = b$.

2) Se considerarmos $\overline{a} \cap \overline{b} \neq \emptyset$, então existe $x \in \overline{a}$ e $x \in \overline{b}$, isto é, $x \equiv a\ (mod\ m)$ e $x \equiv b\ (mod\ m)$. Assim, $a \equiv b\ (mod\ m)$ e pelo item anterior , $\overline{a} = \overline{b}$.

Daí concluímos que se $\overline{a} \cap \overline{b} \neq \emptyset$, então todo elemento de $\overline{a}$ pertence a $\overline{b}$, ou seja, $\overline{a} = \overline{b}$. □

O conjunto de todas as classes residuais módulo m será representada por

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, ..., \overline{m-1}\}.$$

Proposição 17. O conjunto $\mathbb{Z}_m$ tem exatamente m elementos.

Demonstração. Sabemos que $\{\overline{0}, \overline{1}, ..., \overline{m-1}\} \subset Z_m$.

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, $a - r = mq \Rightarrow m|(a-r)$.

Logo, $a \equiv r(mod\ m)$ e, pela Proposição 16 item 1, temos $\overline{a} = \overline{r}$.

Como $0 \leq r \leq (m-1)$ então $\overline{a} = \overline{r} \in \{\overline{0}, \overline{1}, ..., \overline{m-1}\}$.

Portanto, $\mathbb{Z}_m \subset \{\overline{0}, \overline{1}, ..., \overline{m-1}\}$ e concluímos que $\mathbb{Z}_m = \{\overline{0}, \overline{1}, ..., \overline{m-1}\}$.

Suponha que $\overline{r} = \overline{s}$, onde $r, s \in \mathbb{Z}$ tais que $0 \leq r < s \leq m-1$. Pela Proposição 16 item 1 temos que $r \equiv s \ (mod\ m)$ e $m|(s-r)$ mas isto é um absurdo, pois $0 < s-r < m$. Logo, $r = s$ e $\{\overline{0}, \overline{1}, ..., \overline{m-1}\}$ tem exatamente m elementos. □

Corolário 5. As classes $\overline{0}, \overline{1}, ..., \overline{m-1}$ são duas a duas distintas.

A demonstração deste segue da demonstração da proposição anterior e da unicidade do resto, visto em Divisão Euclidiana.

Como poderíamos pensar na representação do $\mathbb{Z}_m$?

Imaginemos uma reta horizontal e marquemos m pontos equidistantes, começando de 0 até $m-1$. Imaginemos agora, que enrolamos esta reta no contorno de uma circunferência, fazendo com que m coincida com o ponto 0. Como a reta é infinita, continuaremos a enrolá-la de modo que os múltiplos de m coincidam com o ponto 0, obtendo a classe de equivalência $\overline{0}$, os pontos que coincidirem com 1, pertencerão à classe $\overline{1}$, os pontos que coincidirem com 2, pertencerão à classe $\overline{2}$ e assim sucessivamente.

O conjunto de m representantes, um de cada uma das classes residuais $\overline{0}, \overline{1}, ..., \overline{m-1}$ é um sistema completo de resíduos módulo m.

Temos as seguintes operações definidas em $\mathbb{Z}_m$.

1) Adição e Multiplicação

Seja m um inteiro positivo fixo. Iremos agora definir as operações de adição e multiplicação no conjunto $\mathbb{Z}_m$ das classes residuais módulo m. Sejam $\overline{a}, \overline{x}, \overline{y}, \overline{b} \in \mathbb{Z}_m$.

Temos que $\overline{a} = \overline{x}$ e $\overline{b} = \overline{y}$. Então,

$$\begin{cases} a \equiv x \ (mod\ m) \\ b \equiv y \ (mod\ m) \end{cases} \Rightarrow \begin{cases} a+b \equiv x+y \ (mod\ m) \\ a.b \equiv x.y \ (mod\ m) \end{cases}$$

Consequentemente,

$$\overline{a+b} = \overline{x+y} \quad \text{e} \quad \overline{ab} = \overline{xy}.$$

Isso torna verdadeiras as definições a seguir.

Definição 12. Dadas duas classes, $\overline{a}, \overline{b} \in \mathbb{Z}_m$, chama-se soma $\overline{a} + \overline{b}$ à classe $\overline{a+b}$ (que é única, independente do representante tomado para $\overline{a}$ ou para $\overline{b}$). Ou seja,

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

Definição 13. Dadas duas classes, $\overline{a}, \overline{b} \in \mathbb{Z}_m$, chama-se produto $\overline{a}.\overline{b}$ à classe $\overline{ab}$ (que é única, independente do representante tomado para $\overline{a}$ ou para $\overline{b}$). Ou seja,

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

Observamos que as operações em $\mathbb{Z}_m$ foram definidas a partir das operações de seus representantes. Assim, como em [16], podemos enunciar as propriedades abaixo para as operações em $\mathbb{Z}_m$.

Propriedades da Adição

Dados $\overline{a}, \overline{b}$ e $\overline{c} \in \mathbb{Z}_m$, temos:

1º) Associatividade: $(\overline{a}+\overline{b})+\overline{c} = \overline{a}+(\overline{b}+\overline{c})$.

2º) Comutatividade: $\overline{a}+\overline{b} = \overline{b}+\overline{a}$.

3º) Existência do zero: $\overline{a}+\overline{0} = \overline{a}, \forall\, \overline{a} \in \mathbb{Z}_m$.

4º) Existência do simétrico: $\overline{a}+(-\overline{a}) = \overline{0}$.

Propriedades da Multiplicação

1º) Associatividade: $(\overline{a}.\overline{b}).\overline{c} = \overline{a}.(\overline{b}.\overline{c})$.

2º) Comutatividade: $\overline{a}.\overline{b} = \overline{b}.\overline{a}$.

3º) Existência da unidade: $\overline{a}.\overline{1} = \overline{a}$.

4º) Distributividade: $\overline{a}(\overline{b}+\overline{c}) = \overline{a}.\overline{b}+\overline{a}.\overline{c}$.

A demonstração de cada um destes itens é relativamente simples, pois utilizamos a validade destas propriedades em $\mathbb{Z}$.

Observação: O elemento $-\overline{a}$ é chamado de o simétrico de $\overline{a}$ para a operação de soma, exatamente como no caso dos inteiros.

Definição 14. Um conjunto com as operações de adição e de multiplicação com as propriedades descritas acima é chamado de anel.

Logo, $\mathbb{Z}_m$ com as operações acima é um anel, chamado anel das classes residuais módulo m, ou anel dos inteiros módulo m.

Para ilustrarmos, em $\mathbb{Z}_6$ temos as seguintes tabelas de soma e produto.

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

Tabela 2: Soma em $\mathbb{Z}_6$.

.	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Tabela 3: Multiplicação em $\mathbb{Z}_6$.

2) Divisão

Veremos agora como calcular divisões em $\mathbb{Z}_m$. Pensando nos números reais a e b, a frase dividir a por b é equivalente a multiplicar a por $1/b$. O número real $1/b$ é conhecido como inverso multiplicativo de b, com $b \neq 0$. Agora vamos transpor isso para $\mathbb{Z}_m$. Digamos que $\overline{a} \in \mathbb{Z}_m$. Diremos que a classe $\overline{\alpha} \in \mathbb{Z}_m$ é o inverso de $\overline{a}$ se a equação $\overline{a}.\overline{\alpha} = \overline{1}$ é verificada em $\mathbb{Z}_m$.

Em $\mathbb{Z}_m$, $\overline{0}$ não possui inverso. De fato,

$0.\overline{\alpha} = (\overline{0}+\overline{0}).\overline{\alpha} = \overline{0}.\overline{\alpha} + \overline{0}.\overline{\alpha}$

$\overline{0}.\overline{\alpha} + (-\overline{0}.\overline{\alpha}) = 0.\overline{\alpha} + (\overline{0}.\alpha - \overline{0}.\overline{\alpha})$

$\overline{0} = \overline{0}.\overline{\alpha}.$

É preciso observar que em $\mathbb{Z}_m$ pode haver outros elementos sem inverso, além da classe $\overline{0}$, veja por exemplo, a tabela acima obtida para $\mathbb{Z}_6$.

Para determinarmos esse inverso faremos o uso de equação diofantina , como veremos a seguir.

$\overline{a}.\overline{\alpha} = \overline{1}$ corresponde a dizer que $a\alpha - 1$ é divisível por m, isto é,

$$a\alpha + km = 1, \text{ para algum } k \text{ inteiro.}$$

Esta equação implica que $mdc(a,m) = 1$, como visto nas equações diofantinas. Portanto, o inverso de $\overline{a}$ só existe se $mdc(a,m) = 1$.

Com isso, como visto em [16], podemos enunciar as seguintes definição e proposição.

Definição 15. Um elemento $\overline{a} \in \mathbb{Z}_m$ será dito invertível quando existir $\overline{\alpha} \in \mathbb{Z}_m$ tal que $\overline{a}.\overline{\alpha} = \overline{1}$.

Proposição 18. Um elemento $\overline{a}$ de $\mathbb{Z}_m$ é invertível se, e somente se, $mdc(a,m) = 1$.

A demonstração vista anteriormente, nos diz que para calcular o inverso, quando ele existe, basta usar o algoritmo euclidiano estendido, como nas equações diofantinas.

Quanto à existência de inverso, ainda temos a seguinte definição:

Definição 16. Um anel onde todo elemento não nulo possui um inverso multiplicativo é chamado de corpo.

E depois de conhecida essa definição, temos o seguinte corolário:

Corolário 6. $\mathbb{Z}_m$ é um corpo se, e somente se, m é primo.

Vamos denotar o subconjunto de $\mathbb{Z}_m$, cujos elementos possuem inverso multiplicativo por $U(m) = \{\overline{a} \in \mathbb{Z}_m; mdc(a,m) = 1\}$.

Segue o seguinte exemplo

$$U(8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}.$$

$$\overline{7}.\overline{5} = \overline{3} \quad \overline{3}.\overline{7} = \overline{5}.$$

Digamos que $\overline{a}$ tem inverso $\overline{\alpha}$ e $\overline{b}$ tem inverso $\overline{\beta}$ em $\mathbb{Z}_m$. O inverso de $\overline{a}.\overline{b}$ será $\overline{\alpha}.\overline{\beta}$, pois

$$(\overline{a}.\overline{b}).(\overline{\alpha}.\overline{\beta}) = (\overline{a}.\overline{\alpha}).(\overline{b}.\overline{\beta}) = \overline{1}.\overline{1} = \overline{1}.$$

Esse conjunto que denotamos por $U(m)$ é chamado de sistema reduzido de resíduos módulo m.

Podemos usar o que foi estudado nessa seção para resolvermos congruências lineares em $\mathbb{Z}_m$.

Considere uma congruência linear do tipo $ax \equiv b(mod\ m)$, com a, $b \in \mathbb{Z}$. Para resolvê-la, podemos isolar o x, dividindo a equação por a. Se $mdc(a,m) = 1$, existe $\alpha \in \mathbb{Z}$ tal que $\alpha.a \equiv 1\ (mod\ m)$.

Multiplicando a equação acima por α, obtemos $\alpha.ax \equiv \alpha.b\ (mod\ m)$. Como $\overline{\alpha}$ é o inverso de $\overline{a}$ em $\mathbb{Z}_m$ esta equação se reduz a

$$x \equiv \alpha.b \ (mod\ m).$$

Exemplo 3.27. Resolver a congruência $7x \equiv 3\ (mod 15)$.

Primeiramente, como $mdc(7,15) = 1$, então existe solução.

Então, precisamos multiplicar a equação pelo inverso de $\overline{7}$ em $\mathbb{Z}_{15}$. Como $15 - 2.7 = 1$, o inverso de $\overline{7}$ é $-\overline{2} = \overline{13}$. Multiplicando por 13, temos

$$13.7.x \equiv 3.13(mod 15).$$

$$x \equiv 39 \equiv 9(mod 15).$$

Com isso, fica resolvida a congruência dada.

Exemplo 3.28. Qual a paridade do número

$$20^{10}.11^{200} + 21^{19}?$$

Podemos decidir a paridade de um a expressão envolvendo produtos e somas de inteiros lembrando que $\overline{0}$ corresponde aos números pares e $\overline{1}$, aos números ímpares.

Com isso, podemos estabelecer as seguintes tabelas que regem a paridade das somas e produtos dos números inteiros.

+	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

.	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Então, para sabermos a paridade do número acima, basta substituir o número 20 por $\overline{0}$, por ser par; e os números 11 e 21 por $\overline{1}$, por serem ímpares.

Assim, obtemos a expressão

$$\overline{0}^{10}.\overline{1}^{200} + \overline{1}^{19},$$

que nos dá como resultado $\overline{1}$. Portanto, o número dado é ímpar.

CAPÍTULO

4

SISTEMAS DE CODIFICAÇÃO

Hoje em dia os códigos fazem parte da nossa vida. Já na maternidade recebemos uma identificação e daí por diante, os códigos se tornam cada vez mais presentes: Registro de Certidão de Nascimento, Registro de Identidade (RG), Cadastro de Pessoa Física (CPF), Carteira Profissional, Título de Eleitor e outros documentos utilizados para identificação.

Além disso, nas farmácias, nos supermercados, nas bancas de revistas, nas livrarias os produtos são acompanhados de etiquetas com seu código. Nosso Código de Endereçamento Postal (CEP), nossa agência bancária, a conta corrente possuem seu código de identificação.

Os números de identificação são gerados por sistemas capazes de detectar a maioria dos erros cometidos durante a sua leitura, digitação ou transmissão. Esses sistemas utilizam um ou mais algarismos acrescentados ao número de identificação que permitem alertar o operador da ocorrência de um erro e é conhecido como dígito verificador. O dígito verificador é obtido por algoritmos que utilizam conceitos de Teoria dos Números, mais especificamente a Congruência Modular.

4.1 Estudo de Alguns Sistemas de Codificação

Esse capítulo apresenta um estudo sobre os códigos de barras e alguns outros códigos numéricos de acordo com [10].

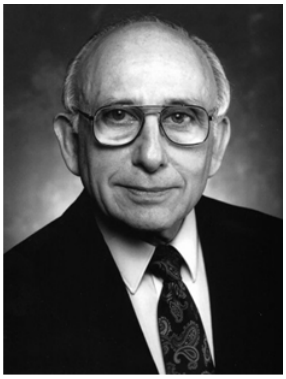
4.1.1 Códigos de Barras

Na maior parte do século XX, os supermercados precisavam fechar suas portas por um dia para realizar o balanço, que era a contagem manual dos produtos por mais de uma vez e por mais de um funcionário. Tal procedimento acarretava perda da venda do dia e ainda havia erros.

Pela necessidade de contabilizar automaticamente a entrada e saída de produtos, o

presidente de uma cadeia de mercados solicitou ao diretor do Instituto de Tecnologia da Filadélfia, nos Estados Unidos, que tentasse criar algo para sanar essa exigência do mercado.

Depois de alguns estudos, um aluno da graduação Bernard Silver e o professor Norman Joseph Woodland produziram as primeiras ideias sobre os modernos códigos de barra (Ver [10]).

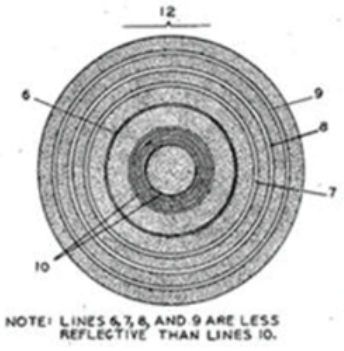


(a) Norman J. Woodland (1921-2012).

(b) Bernard Silver (1924-1963).

Figura 2: Woodland e Silver

Os estudos iniciais resultaram em um sistema de linhas e círculos que depois foi substituído por um padrão de circunferências concêntricas de largura variável (Figura 3). Silver e Woodland registraram uma patente para o seu sistema de codificação em 20 de outubro de 1949, porém receberam a concessão desta apenas em 1952. O invento era classificado como "classificação de artigos através de identificação de padrões", como visto em [10].



(a) Código de barras.

(b) Código de Barras.

Figura 3: Modelo do Primeiro Código de Barras.

Por volta de 1970, uma firma de assessoria, a Mc Kinsey & Co., junto com a Uniform Grocery Product Code Council, definiu um formato numérico para identificar produtos e pediu a diversas companhias que elaborassem um código adequado.

Na elaboração de um código adequado, das companhias contactadas, a que apresentou a melhor proposta foi a IBM, e o autor desse código foi George J. Laurer (Figura 4).

Figura 4: George J. Laurer.

O código proposto só foi aceito formalmente em 1973, passando a ser conhecido como código UPC (Universal Product Code), adotado nos Estados Unidos e no Canadá.

Assim, na manhã em 06 de junho de 1974, no estado de Ohio, Estados Unidos, uma funcionária que trabalhava em uma rede de supermercados Marshs passou uma caixa de chicletes por um scanner e foi lido o código de barras do primeiro produto vendido com esse tipo de codificação.

Ele consistia de uma sequência de 12 dígitos, traduzidos para barras brancas e pretas, seguindo padrões estabelecidos.

Figura 5: Exemplo de códigos de barras UPC.

Existem algumas versões posteriores do UPC, com pequenas modificações. Posteriormente foi solicitado, a Laurer que ampliasse o código, de modo a identificar também o país de origem de cada produto classificado.

Baseado no UPC, ele acabou criando um novo código, com 13 dígitos (Figura 6), que foi adotado em dezembro de 1976 com o nome EAN (European Article Numbering System).

Mais tarde, constatou-se a eficiência desse tipo de código e sua utilização foi estendida rapidamente para o Brasil em 1983. O Brasil deu um grande passo à frente de outros países da América Latina, aderindo ao sistema de código de barras na maioria das cidades e estados.

Figura 6: Exemplo de códigos de barras EAN-13.

4.1.2 Estrutura do Código de Barras

O código de barras é uma forma de representação gráfica, no formato de barras, que através de uma leitura por meio óptico informa dados de um determinado objeto.

Os códigos de barras são formados por sequências de barras verticais de cores brancas e pretas, com larguras variáveis: fina, média, grossa ou muito grossa.

Cada espessura e cor de uma listra podem ser interpretados de acordo com a tabela abaixo:

Espessura / Cor	Fina	Média	Grossa	Muito Grossa
Branca	0	00	000	0000
Preta	1	11	111	1111

Tabela 4: Cor e espessura das listras.

Esses dados também são representados por uma sequência numérica que aparece abaixo das barras. A cada número lhe é atribuído um espaço de espessura fixa que corresponde sempre a uma sequência de sete dígitos iguais a 1 ou 0.

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

Os códigos de barras UPC, também 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.

Comecemos o estudo dos códigos de barras pelos códigos do tipo UPC.

A leitura distingue a direita da esquerda, já que o produto pode ser passado em uma direção ou outra, porque os dígitos são codificados de maneira diferente quando estão do lado direito ou lado esquerdo do código de barras, conforme a tabela a seguir:

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 5: Codificação para código UPC.

Note que a codificação de um dado número, à direita, se obtém da sua codificação à esquerda, trocando cada 0 por 1 e reciprocamente. O mecanismo de reconhecimento da máquina consiste em notar que cada sequência do lado esquerdo tem um número ímpar de dígitos iguais a 1, e consequentemente, cada uma das que estão à direita tem um número par. Então, pela paridade de cada sequência a máquina detecta de que lado está lendo o código.

A elaboração do código EAN se deparou com a necessidade de adicionar um dígito à cada código, para permitir a identificação do país de origem do produto, mas de tal forma que a máquina leitora pudesse ler ambos os códigos.

Para isso os países que utilizavam o código UPC, EUA e Canadá, são identificados com um 0 na frente, e o resto da codificação é feito utilizando-se o sistema anterior. Para outros países, como era necessário adicionar um dígito e também manter o mesmo padrão de tamanho do código de barras, para não ter que modificar todos os leitores, não foi modificada a codificação do lado direito (permitindo assim que as leitoras continuassem a identificar o lado correspondente). Mas, a codificação do lado esquerdo varia dependendo do dígito inicial. Um dígito do lado esquerdo pode ser codificado com um número par ou ímpar de dígitos iguais a 1, de acordo com a tabela a seguir.

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 6: Codificação EAN-13.

Assim, para cada dígito inicial escolhe-se uma alternância diferente de pares e ímpares de acordo com o seguinte critério:

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 7: Codificação do lado esquerdo do código EAN-13.

É interessante observar que, para o sistema EAN-13, o primeiro dígito não é apresentado em barras. Ele fica implícito na ordem da codificação dos próximos seis algarismos.

Exemplo 4.1. Um pacote de macarrão instantâneo, produzido e cadastrado no Brasil, é identificado pelo código 7891079001523.

A sequência começa com 789, de modo que o primeiro dígito é 7.

Consequentemente, de acordo com a tabela anterior deve-se usar, no lado esquerdo, a seguinte ordem de codificação:

ímpar, par, ímpar, par, ímpar, par.

Consultando a tabela de codificação do EAN-13, obtemos:

$$8 \to 0110111 \quad 9 \to 0010111 \quad 1 \to 0011001$$
$$0 \to 0100111 \quad 7 \to 0111011 \quad 9 \to 0010111$$

Para os dígitos do lado direito não temos que nos preocupar com a paridade, então obtemos:

$$0 \to 1110010 \quad 0 \to 1110010 \quad 1 \to 1100110$$
$$5 \to 1001110 \quad 2 \to 1101100 \quad 3 \to 1000010$$

Então o código de barras correspondente, de modo que o primeiro dígito estará implícito na codificação dos demais, é:

Figura 7: Código de Barras de um macarrão instantâneo.

Em ambos os sistemas, UPC e EAN-13, os dígitos têm codificações diferentes dependendo do lado que se encontram. Se estiverem do lado esquerdo, iniciam com zeros (barras brancas), se estiverem do lado direito, iniciam com uns (barras pretas).

Isso permite que a leitura, mesmo sendo feita de cabeça para baixo, produza o mesmo número.

Para o sistema EAN-13, que é mais usado atualmente, deve-se ter a seguinte interpretação: os primeiros dois ou três dígitos identificam o país de origem (país onde foi cadastrado o produto), os próximos quatro ou cinco dígitos servem para identificar a empresa, já os cinco números seguintes, representam o código do produto, e por fim, o último dígito é o dígito verificador, conforme ilustra a Figura 8.

Esse último dígito, chamado dígito verificador, é adicionado no final da sequência de elaboração do código, de acordo com um algoritmo que se obtém a partir dos dígitos anteriores, obedecendo ao padrão do sistema adotado, como veremos posteriormente. Esse dígito não faz parte da sequência dos dígitos que contém as informações sobre o produto e tem a finalidade de certificar a validade do código numérico.

Figura 8: Estrutura do Código de Barras.

Quando por algum motivo o leitor óptico não conseguir efetuar a leitura do código de barras, o operador terá que digitar a sequência numérica do código, podendo assim ocorrer erros.

O dígito verificador é um recurso para ajudar a máquina a detectar alguns erros.

Considere $a_1, a_2, a_3, ..., a_{13}$ a sequência de dígitos de um determinado código de barras EAN-13. Como foi dito anteriormente, os 12 primeiros dígitos já são pré-estabelecidos. O último dígito, que é o dígito verificador, será determinado por um algoritmo que envolve os primeiros dígitos, os doze primeiros no caso do EAN-13 e pelos onze primeiros dígitos, no caso do sistema UPC.

A utilização de um dígito verificador não permite a correção automática do erro. Contudo, permite que o sistema alerte o operador sobre a ocorrência deste e consequentemente da necessidade de reescrever os números.

Considerando o sistema EAN-13, chamaremos de x o décimo terceiro dígito. A sequência numérica dos 12 primeiros dígitos do código pode ser representada por:

$$(a_1, a_2, a_3, ..., a_{12}).$$

Efetua-se o produto dos números da sequência ordenadamente por:

$$(1, 3, 1, 3, ..., 1, 3).$$

Observa-se que cada dígito pertencente a uma ordem ímpar, multiplica-o por 1, e cada dígito pertencente a uma ordem par, multiplica-o por 3.

Somando-se os produtos obtidos temos:

$$a_1.1 + a_2.3 + a_3.1 + a_4.3 + a_5.1 + a_6.3 + a_7.1 + a_8.3 + a_9.1 + a_{10}.3 + a_{11}.1 + a_{12}.3.$$

O dígito verificador, que chamaremos de x, é determinado de tal forma que a soma obtida acima somada com x, seja um múltiplo de 10, ou seja:

$$a_1.1 + a_2.3 + a_3.1 + a_4.3 + ... + a_{10}.3 + a_{11}.1 + a_{12}.3 + x \equiv 0 \ (mod\ 10).$$

Se a leitura estiver correta, o resultado desse cálculo é igual ao do dígito verificador. O interessante do assunto código de barras para esse trabalho, é que para o cálculo do dígito verificador, o algoritmo usado é uma congruência módulo 10.

Exemplo 4.2. Considere o código de barras da Figura 7 e chamemos o dígito verificador, no caso 3, de x.

Seja então $789107900152x$ o número referente ao código de barras da Figura 8.

Multiplicando esses algarismos ordenadamente por $(1,3,1,3,1,3,1,3,1,3,1,3,1)$, obtém-se:

$7.1+8.3+9.1+1.3+0.1+7.3+9.1+0.3+0.1+1.3+5.1+2.3+x.1$ que resulta em $87+x$.

Para descobrirmos x é preciso que a soma $87+x$ seja um múltiplo de 10. Usando as congruências modulares podemos escrever que:

$$87+x \equiv 0 \ (mod\ 10).$$

Logo, $x = 3$.

4.1.3 Erros detectáveis e Erros não detectáveis

Como dito anteriormente, caso durante a leitura do código de barras, ocorra um problema com o leitor óptico ou um problema que impeça a leitura óptica do código, será necessário que o operador digite os algarismos localizados logo abaixo do código de barras.

Nesse momento, podem ocorrer erros de digitação, onde o resultado não seja congruente a zero módulo 10 e então o processador emitirá um sinal sonoro alertando que houve um erro de digitação.

Se o operador digitar um único algarismo errado, comete um erro denominado único. Certamente, a soma encontrada não será congruente a zero módulo 10, sendo o erro sempre detectado, como veremos adiante.

Caso o operador digite dois ou mais algarismos errados, há uma possibilidade dos números digitados se compensarem uns aos outros e o resultado da soma obtida ser congruente a zero módulo dez, não sendo possível a máquina detectar o erro nesse caso.

Ainda pode ocorrer de dois algarismos consecutivos serem digitados em posições trocadas, chamado de erro de transposição adjacente.

Nesse caso, o erro pode ou não ser detectado, o que será detalhado posteriormente.

Quando os erros não são detectados, o produto é registrado pelo leitor óptico como outro. É por isso, que algumas vezes, ao conferirmos uma compra feita em um supermercado, por

exemplo, exista na nota entregue ao consumidor produtos que não foram levados ou divergências no valor observado pelo consumidor.

Segundo [10], autores como D.F.Beckley e J.Verhoeff investigaram sistematicamente esses erros e a pesquisa apontou como mais frequentes:

- O erro único $(...a... \to ...b...)$, com 79% de ocorrência;
- O erro de transposição adjacente $(...ab... \to ...ba...)$, com $10,2\%$.

Os $10,8\%$ restantes correspondem a erros com frequências menores de 1% cada.

Para uma melhor compreensão desses erros serão apresentados exemplos a seguir.

Exemplo 4.3. Considere o código de barras abaixo:

Figura 9: Código de Barras de um Medicamento.

Suponha que houve um erro de digitação no dígito da posição a_9, e que o código tenha sido transmitido da seguinte forma: 7898495**1**5007.

O computador detectaria o erro, pois:

$7.1 + 8.3 + 9.1 + 8.3 + 4.1 + 9.3 + 5.1 + 6.3 + 1.1 + 5.3 + 0.1 + 0.3 + 7.1 = 141 \not\equiv 0 \ (mod\ 10)$.

Imagine que a troca tenha ocorrido com um algarismo, a_n, que ocupa uma ordem ímpar, que é multiplicado por 1. E que S representa a soma de todos os outros algarismos que ocupam ordem ímpar e foram multiplicados por 1 com todos os algarismos que ocupam ordem par e foram multiplicados por 3. Então teríamos que:

$$S + a_n \equiv 0 \ (mod\ 10).$$

Sabemos que a_n só pode assumir um valor dentre os algarismos $0,1,2,3,4,5,6,7,8,9$.

Considerando as classes residuais, esse conjunto de algarismos é denominado sistema completo de resíduos módulo 10, que é composto pelos restos possíveis em uma divisão por 10. Como estudado anteriormente, pela unicidade do resto, duas classes residuais não podem ser iguais.

Assim existe um único valor para a_n que quando somado com S resultará em um múltiplo de 10.

O mesmo ocorre para a troca de um algarismo a_n, que ocupa uma ordem par e é multiplicado por 3. Se S representa a soma de todos os algarismos que ocupam ordem ímpar e foram multiplicados por 1 com todos os outros algarismos que ocupam ordem par e foram multiplicados por 3. Então, temos que

$$S + 3a_n \equiv 0 \ (mod\ 10).$$

Se o sistema completo de resíduos módulo 10, que é de onde sai o valor de a_n, for multiplicado por 3, obtemos: $(0,3,6,9,12,15,18,21,24,27)$ que nos retorna os possíveis restos em uma divisão por 10: $(0,3,6,9,2,5,8,1,4,7)$ que é o próprio sistema completo de resíduos módulo 10, de onde apenas um valor quando somado com S resultará em um múltiplo de 10.

Portanto se o erro é único, esse erro será sempre detectado, independente de sua posição.

Além do erro único, 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 chamado de transposição adjacente, que é quando troca-se a ordem de dois algarismos consecutivos. Nesse caso o erro pode ou não ser detectado, como pode ser observado nos exemplos a seguir.

Exemplo 4.4. Para os casos a seguir, vamos considerar o código de barras de uma embalagem de um leite condensado

Figura 10: Código de Barras de um Leite Condensado.

1º Caso: Imagine que a operadora do caixa, digitou o número e ocorreu um erro de digitação em que dois destes números ficaram em posições trocadas, ficando a sequência numérica da seguinte forma:

$$789\mathbf{26}59412762.$$

Como o código é um EAN-13, os algarismos de ordem ímpar devem ser multiplicados por 1 e os algarismos de ordem par devem ser multiplicados por 3, obtendo-se

$$7.1 + 8.3 + 9.1 + 2.3 + 6.1 + 5.3 + 9.1 + 4.3 + 1.1 + 2.3 + 7.1 + 6.3 + 2.1 = 122.$$

Como $122 \not\equiv 0\ (mod\ 10)$, a máquina irá detectar o erro.

2º Caso: Para este 2º caso, suponhamos que existiu uma troca entre os algarismos a_7 e a_8 e o número digitado fosse o seguinte:

$$7896254912762.$$

Como foi feito no 1º caso, devemos multiplicar a sequência numérica acima por $1,3,1,3,1,3,1,3,1,3,1,3,1$, obtendo:

$$7.1+8.3+9.1+6.3+2.1+5.3+4.1+9.3+1.1+2.3+7.1+6.3+2.1=140.$$

Como $140 \equiv 0\ (mod\ 10)$, o erro não será detectado.

Através desses dois casos estudados acima, observamos que um erro de transposição adjacente pode ou não ser detectado. Então, quando será detectado ou não?

Seja $a_1,a_2,a_3,...,a_i,a_{i+1},...,a_{12},a_{13}$ uma sequência de dígitos de um código de barras no sistema EAN-13. Multiplicando os algarismos de ordem ímpar por 1 e os que estão na ordem par por 3 obtemos:

$$a_1+3a_2+a_3+...+3a_i+a_{i+1}+...+3a_{12}+a_{13} \equiv 0\ (mod\ 10). \quad (1)$$

Suponhamos que tenha ocorrido um erro e que essa sequência tenha sido digitada da seguinte forma:

$$a_1,a_2,a_3,...,a_{i+1},a_i,...,a_{12},a_{13}.$$

O erro não será detectado se, e somente se:

$$a_1+3a_2+a_3+...+3a_{i+1}+a_i+...+3a_{12}+a_{13} \equiv 0\ (mod\ 10). \quad (2)$$

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

$(a_1+3a_2+a_3+...+3a_{i+1}+a_i+...+3a_{12}+a_{13})-(a_1+3a_2+...+3a_i+a_{i+1}+...+3a_{12}+a_{13}) \equiv 0\ (mod\ 10)$.

$$3a_{i+1}-a_{i+1}+a_i-3a_i \equiv 0\ (mod\ 10)$$

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

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

Como os dígitos da sequência $a_1, a_2, a_3, ..., a_{12}, a_{13}$ são números entre 0 e 9, podemos escrever que $|a_{i+1} - a_i| \leq 9$.

Então para que $2(a_{i+1} - a_i)$ seja congruente a zero módulo dez é preciso que

$$|a_{i+1} - a_i| = 5.$$

Com essa demonstração, podemos enunciar a seguinte proposição.

Proposição 19. Uma transposição adjacente é detectada pelo sistema EAN-13 e pelo sistema UPC, se e somente se, $|a_{i+1} - a_i| \neq 5$.

Podem ocorrer também erros de troca de algarismos que não sejam consecutivos, que são chamados de transposição não adjacente.

Exemplo 4.5. Consideremos ainda o código de barras do leite condensado 7896259412762.

1º Caso: Para esse caso, vamos considerar que o termo a_5 foi digitado no lugar de a_8 e vice-versa, obtendo assim a seguinte sequência

$$7896\mathbf{4}59\mathbf{2}12762.$$

Ao multiplicarmos os algarismos de ordem ímpar por 1 e os algarismos de ordem par por 3, temos como resultado

$$7.1 + 8.3 + 9.1 + 6.3 + 4.1 + 5.3 + 9.1 + 2.3 + 1.1 + 2.3 + 7.1 + 6.3 + 2.1 = 126.$$

$$126 \not\equiv 0 \ (mod\ 10).$$

Então, nesse caso, o erro será detectado.

2º Caso: Agora, imaginemos trocar o termo a_3 com o a_{11}. Com isso, a sequência a considerar será:

$$78\mathbf{7}6259412\mathbf{9}62.$$

Fazendo a multiplicação por $1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1$, tem-se que

$$7.1 + 8.3 + 7.1 + 6.3 + 2.1 + 5.3 + 9.1 + 4.3 + 1.1 + 2.3 + 9.1 + 6.3 + 2.1 = 130.$$

$$130 \equiv 0 \ (mod\ 10).$$

Para esse caso, o erro já não será detectado.

Após analisarmos os dois casos anteriores, percebemos que no 1º caso, ao trocarmos o termo a_5 com o termo a_8, a diferença entre as ordens, ou seja $8-5=3$, é um número ímpar, portanto o erro foi detectado. Já para o 2º caso, ao trocarmos o termo a_3 com o termo a_{11}, a diferença entre as ordens, ou seja, $11-3=8$, é um número par, e nessas condições o erro não foi detectado.

Então podemos enunciar a seguinte proposição:

Proposição 20. 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 da sequência numérica de um código de barras do sistema UPC ou EAN-13 por $1,3,1,3,1,3,...,1,3$ percebemos que os algarismos de ordens ímpares são multiplicados por 1 e os algarismos de ordens pares são multiplicados por 3. Portanto, se a troca for entre dois algarismos:

- ambos de ordem par: o fator de multiplicação, que é 3, não muda. Com isso, ao serem trocados, ambos continuam sendo multiplicados por 3, não alterando a soma final. Por isso, o erro não será detectado.

- ambos de ordem ímpar: o fator de multiplicação, que é 1, não muda. Com isso, ao serem trocados, ambos continuam sendo multiplicados por 1, não alterando a soma final. Assim, o erro também não será detectado.

- um de ordem par e outro de ordem ímpar: o fator de multiplicação do algarismo de ordem ímpar é 1 e o de ordem par é 3. Com isso, ao serem trocados, o algarismo de ordem ímpar, agora ocupa uma ordem par e será multiplicado por 3 e o algarismo, antes de ordem par, agora estará na ordem ímpar e será multiplicado por 1, alterando assim a soma final. Com isso, o erro será detectado.

□

Agora, analisaremos um último caso, ainda referente ao código de barras do Exemplo 4.4.

3º Caso: Para esse caso, ainda considerando a sequência numérica 7896259412762, referente ao leite condensado, trocaremos agora o termo a_1 com o termo a_{10}. De acordo com a proposição anterior, como a diferença entre as ordens $10-1=9$ é um número ímpar, então o erro poderia ser detectado.

Vejamos então:

Fazendo o produto da seguinte sequência **2**896259417762 por $1,3,1,3,1,3,1,3,1,3,1,3,1$, obtemos:

$$2.1+8.3+9.1+6.3+2.1+5.3+9.1+4.3+1.1+7.3+7.1+6.3+2.1=140$$

$$140 \equiv 0\ (mod\ 10).$$

Como 140 é múltiplo de 10, então o erro não será detectado.

O que ocorreu é que o módulo da diferença entre os termos é 5, ou seja $|2-7|=5$. Portanto, se a diferença entre as ordens dos termos trocados for um número ímpar, o erro só será detectado se o módulo da diferença dos termos trocados for diferente de 5.

Com isso, podemos enunciar mais uma proposição.

Proposição 21. Um erro de transposição não adjacente, em que os termos 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, $|a_j - a_i| \neq 5$.

Demonstração. Considere a seguinte sequência numérica de um código de barras de um determinado produto pelo sistema EAN-13, $a_1, a_2, a_3, ..., a_i,$
$..., ...a_j, ..., a_{12}, a_{13}$.

Ao multiplicarmos essa sequência por $1,3,1,3,1,3,1,3,1,3,1,3,1$ temos como resultado

$$a_1+3a_2+...+a_i+...+3a_j+...+3a_{12}+a_{13} \equiv 0\ (mod\ 10). \quad (3)$$

Ao realizar esse produto, sabe-se que os algarismos de ordem par são multiplicados por 3, enquanto os algarismos na posição ímpar, são multiplicados por 1. Portanto, se a variação de i para j é ímpar, o fator de multiplicação, seja 1 ou 3, vai mudar. Dessa forma, se um código sofreu uma transposição não adjacente dos algarismos a_i e a_j, sendo $i-j$ um número ímpar, ao efetuarmos o produto obteremos:

$$a_1+3a_2+...+3a_i+...+a_j+...+3a_{12}+a_{13} \equiv 0\ (mod\ 10). \quad (4)$$

Se fizermos (3)-(4), tem-se que

$(a_1+3a_2+...+a_i+...+3a_j+...+3a_{12}+a_{13})-(a_1+3a_2+...+3a_i+...+a_j+...+3a_{12}+a_{13}) \equiv 0\ (mod\ 10)$.

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

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

$$2(a_j-a_i) \equiv 0\ (mod\ 10).$$

Como já visto, sempre $|a_j - a_i| \leq 9$, visto que a_i e a_j são números entre zero e nove.

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

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

Foram analisados aqui alguns erros de maior ocorrência, dentre eles erros detectáveis e outros não detectáveis, envolvendo a digitação de códigos de barras dos sistemas EAN-13 e UPC.

4.1.4 QR Code

Já existe no mercado hoje, uma variação do código de barras UPC e EAN-13, que são os QR Codes.

Como o código de barras possui uma série de limitações quanto às informações do produto devido à baixa capacidade de armazenamento, os QR Codes foram criados na intenção de suprir essa necessidade.

O termo QR deriva de Quick Response, que na língua portuguesa significa resposta rápida; e code, traduzido para o português significa código.

O QR Code foi inventado no Japão em 1994 pela Denso Wave, uma empresa do grupo Toyota, com a finalidade de identificar peças de carros, e agilizar o processo de logística.

Contudo, a popularização deste se deu há pouco tempo e hoje em dia é usado para transmitir informações rápidas e precisas a dispositivos móveis. Assim, passou a fazer parte de embalagens de produtos em supermercados e também são encontrados em outdoors e anúncios.

O QR Code é um código de barras bidimensional que contém informações através de texto, imagem, páginas da internet, videos, cartões de visitas, entre outras.

Com uma câmera de celular e um aplicativo gratuito pode se fazer a leitura da imagem do QR Code e decodificar o conteúdo presente nesse código.

A capacidade de armazenamento de dados de um QR Code pode variar de acordo com o tipo de dado armazenado. Veja a tabela a seguir:

Tipo de caracter	Quantidade máxima de caractéres
Numéricos	7089
Alfa-numéricos	4296
Binário	2953
Kanji \ Kame (alfabeto japonês)	1817

Tabela 8: Capacidade de armazenamento de um QR Code.

Cada região do código QR tem sua própria função, tais como posicionamento, alinhamento, versão da informação e outras voltadas para segurança.

Veja uma imagem de um QR Code:

Figura 11: QR Code (a).

Os quadrados maiores e que estão presentes em três dos quatro cantos servem para facilitar a localização, tamanho e inclinação.

O quadrado encontrado próximo ao quarto canto, que é um pouco menor que os quadrados dos cantos e maior que os demais quadrados interiores, tem a função de alinhamento para que o código possa ser lido e processado.

Os quadrados menores, chamados de módulos, representam as informações contidas no código. Esses módulos trabalham em conjunto, formando um grupo a cada oito módulos. Cada um desses grupos pode ser chamado de bytes.

A primeira versão do QR Code tem formatação de 21x21 módulos. Hoje, são conhecidas um pouco mais de 40 versões diferentes, sendo a última formatação de 177x177 módulos.

Um sistema de correção de erros, que utiliza o algoritmo de Reed-Solomon, pode recuperar informação de uma etiqueta que esteja danificada de acordo com a taxa de restauração que flutua de 7% a 30%. Quanto maior o nível de correção de erros, menor a capacidade de armazenamento da etiqueta. A informação contida no código é protegida contra erros através de um código BCH.

É importante pensar que o novo formato do código de barras quebra o paradigma de servir apenas para identificação.

Ele funciona como uma etiqueta dinâmica, trazendo muitas vezes ao consumidor até mesmo o mecanismo de produção do produto que este está levando para a sua residência.

Interessante também comentar que qualquer pessoa pode criar um QR Code. Para isso precisa apenas de um serviço online.

4.1.5 Outros Códigos Numéricos

Além dos códigos de barras, existem muitos outros códigos de identificação que também possuem um sistema de segurança controlado por dígitos de verificação.

Nesta seção serão apresentados alguns deles.

1) Cadastro de Pessoas Físicas (CPF)

No Brasil o sistema de identificação usado para o cadastramento de pessoas físicas é o CPF, emitido pela Receita Federal. O CPF é outro exemplo importante de sistema de identificação que faz o uso do dígito verificador.

Este número é constituído de 11 dígitos, sendo um primeiro bloco composto de nove algarismos e um segundo, com mais dois algarismos, que formam o dígito verificador, que são obtidos também através da congruência modular.

A principal diferença entre o CPF e os códigos de barras UPC e EAN-13 é que este primeiro tem como dígito verificador dois algarismos.

O primeiro deles é o resultado de uma congruência módulo 11, obtido por um algoritmo com os 9 primeiros dígitos. E o segundo é determinado, incluindo-se o 1^{o} dígito verificador encontrado com os 9 primeiros algarismos, através de um algoritmo módulo 11.

Podemos então estruturar o CPF da seguinte maneira:

Sejam $a_1a_2a_3...a_{10}a_{11}$ os dígitos de um CPF, então

- $a_1a_2a_3a_4a_5a_6a_7a_8$ são chamados de número base;
- a_9 representa a unidade da federação onde a pessoa fez o registro;
- $a_{10}a_{11}$ são dígitos verificadores.

A Tabela 9 apresenta o dígito a_9 que deve ser usado para o registro em cada estado brasileiro.

Como dito anteriormente, a verificação do número do CPF deve ser feita em duas etapas, que serão mostradas a seguir usando como exemplo os dígitos do CPF $054703796-12$.

1ª etapa: Considera-se os nove primeiros dígitos do código $(a_1a_2a_3a_4a_5a_6a_7a_8a_9)$ e multiplica-se ordenadamente por $1,2,3,4,5,6,7,8,9$ e soma-se os produtos obtidos. Essa soma deve ser congruente ao dígito a_{10} módulo 11

$$a_1.1+a_2.2+a_3.3+a_4.4+a_5.5+a_6.6+a_7.7+a_8.8+a_9.9 \equiv a_{10}\ (mod\ 11).$$

Para o número do CPF citado acima podemos escrever que

Brasil	
Tipo de caracter	Quantidade máxima de caractéres
0	Rio Grande do Sul
1	Distrito Federal, Goiás, Mato Grosso. Mato Grosso do Sul e Tocantins
2	Acre, Amapá, Amazonas, Pará, Rondônia e Roraima
3	Ceará, Maranhão e Piauí
4	Alagoas, Paraíba, Pernambuco e Rio Grande do Norte
5	Bahia e Sergipe
6	Minas Gerais
7	Espírito Santo e Rio de Janeiro
8	São Paulo
9	Paraná e Santa Catarina

Tabela 9: Dígito da federação.

$$0.1+5.2+4.3+7.4+0.5+3.6+7.7+9.8+6.9 \equiv a_{10} \ (mod\ 11)$$

$$243 \equiv a_{10} \ (mod\ 11).$$

Como $243 \equiv 1 \ (mod\ 11)$, então o primeiro dígito verificador é 1.

2ª etapa: Para essa etapa, deve-se considerar os nove primeiros dígitos juntamente com o primeiro dígito de controle encontrado anteriormente, ou seja, $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}$. Efetua-se o produto de cada um desses algarismos ordenadamente por $0,1,2,3,4,5,6,7,8,9$ e soma-se os produtos obtidos.

A soma resultante deve ser congruente ao dígito a_{11} módulo 11

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

Para o CPF usado como exemplo temos

$$0.0+5.1+4.2+7.3+0.4+3.5+7.6+9.7+6.8+1.9 \equiv a_{11} \ (mod\ 11)$$

$$211 \equiv a_{11} \ (mod\ 11)$$

Como $211 \equiv 2 \ (mod\ 11)$, então o último dígito verificador é 2.

Então se $a_{10} = 1$ e $a_{11} = 2$, os dígitos verificadores desse CPF são 1 e 2, o que prova a sua veracidade.

Se caso a soma encontrada for congruente a 10, deve-se considerar o zero para o dígito procurado, visto que estes devem estar entre 0 e 9.

De acordo com [1] a partir de Janeiro deste ano a Receita Federal alterou o modelo de Cadastro de Pessoas Físicas (CPF). Os novos documentos passarão a ter, no verso, um QR Code, com a finalidade de facilitar a comprovação da autenticidade do documento e reduzir o risco de fraudes.

2) Número do Cartão de Crédito

Hoje grande parte dos consumidores utiliza-se do cartão de crédito para fazer suas compras.

Os principais números de cartões de crédito no Brasil possuem uma sequência de 16 dígitos. Os 6 primeiros referem-se a instituição emissora, sendo que o primeiro desses 6 dígitos caracteriza a bandeira do cartão. Se, por exemplo, for Visa começa com 4 e se for Mastercard começa com 5. Os nove dígitos seguintes identificam o cliente e o último dígito representa o dígito verificador.

Veja o esquema representado a seguir:

Figura 12: Partes que compõem o número do Cartão de Crédito.

O dígito verificador do cartão de crédito pode ser calculado por uma fórmula denominada Algoritmo de Luhn. Essa fórmula recebeu esse nome em homenagem ao cientista Hans Peter Luhn (1896-1964), um engenheiro da International Business Machines, IBM, que em 1960 recebeu a patente referente à invenção da técnica para este cálculo.

Hoje em dia esse algoritmo é de domínio público, sendo utilizado por bancos e demais instituições financeiras para validar cartões de crédito e débito. É denominado módulo 10 IBM.

A verificação da autenticidade do número de um cartão se dá da seguinte maneira:

Seja $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}a_{12}a_{13}a_{14}a_{15}a_{16}$ os dígitos de uma sequência numérica de um cartão. Os dígitos de ordem ímpar devem ser multiplicados por 2 e os dígitos de ordem par devem ser multiplicados por 1.

Ao multiplicar os dígitos de ordem ímpar por 2, deve-se considerar:

$$2a_i = \begin{cases} 2a_i, \ se \ 2a_i < 10; \\ 2a_i - 9, \ se \ 2a_i \geq 10. \end{cases}$$

Depois, soma-se todos os produtos obtidos. Essa soma deve ser congruente a zero módulo 10, ou seja,

$$2a_1 + a_2 + 2a_3 + a_4 + 2a_5 + a_6 + 2a_7 + a_8 + 2a_9 + a_{10} + 2a_{11} + a_{12} + 2a_{13} + a_{14} + 2a_{15} + a_{16} \equiv 0 \ (mod\ 10).$$

Para ilustrar esse algoritmo apresentaremos os exemplos a seguir.

Exemplo 4.6. Nesse exemplo verificaremos a autenticidade dos dígitos do seguinte cartão de crédito:

Figura 13: Número de um Cartão de Crédito.

Primeiramente multiplicaremos os algarismos das ordens ímpares por 2 e os de ordem par por 1. Logo depois, deve-se somar os produtos obtidos, lembrando que antes, se algum dos produtos obtidos for maior ou igual a 10 devemos subtrair 9 destes.

$$4.2 + 5.1 + 9.2 + 3.1 + 6.2 + 0.1 + 0.2 + 0.1 + 0.2 + 9.1 + 6.2 + 8.1 + 9.2 + 0.1 + 6.2 + 0.1 \equiv 0 \ (mod\ 10)$$

$$8 + 5 + (18 - 9) + 3 + (12 - 9) + 0 + 0 + 0 + 0 + 9 + (12 - 9) + 8 + (18 - 9) + 0 + (12 - 9) + 0 \equiv 0 \ (mod\ 10)$$

$$60 \equiv 0 \ (mod\ 10).$$

Portanto, os dígitos estão corretos, pois a somatória obtida é congruente a zero módulo 10.

Exemplo 4.7. Já para esse 2º exemplo, consideremos que seja necessário verificar o dígito verificador de um cartão.

Consideremos para isso um número de cartão fictício encontrado na internet (Figura 14).

Pelo algoritmo apresentado anteriormente devemos multiplicar os algarismos de ordens ímpares por 2 e os algarismos de ordem par por 1. Se o produto for maior ou igual a 10, lembrar que devemos subtrair 9 destes e depois somar os valores obtidos.

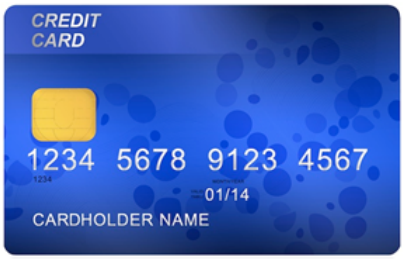


Figura 14: Cartão fictício da Internet.

Para esse caso chamaremos o dígito verificador de C. Então podemos escrever que

$$1.2+2.1+3.2+4.1+5.2+6.1+7.2+8.1+9.2+1.1+2.2+3.1+4.2+5.1+6.2+C \equiv 0\ (mod\ 10)$$

$$2+2+6+4+(10-9)+6+(14-9)+8+(18-9)+1+4+3+8+5+(12-9)+C \equiv 0\ (mod\ 10)$$

$$67+C \equiv 0\ (mod\ 10).$$

Então o dígito verificador nesse cartão deveria ser 3 e não 7 como se apresenta.

O último dígito do número do cartão, o dígito verificador, previne a digitação errada da sequência de números do cartão e também que hackers gerem números de cartão que funcionem. Essa última função é reforçada pelo código de segurança que fica no verso do cartão. Este é gerado pela própria instituição e é calculado pela criptografia do número do cartão e sua data de validade.

4.1.6 Relação entre pesos e módulo

Fizemos o estudo de três sistemas de codificação: códigos de barras, cadastro de pessoas físicas (CPF) e o número do cartão de crédito.

Para os códigos de barras foi feito um levantamento e estudo, dentre os erros que mais ocorrem, de situações em que os erros são ou não detectáveis.

Sabemos que o dígito verificador também é encontrado nos números de processos judiciais, nos códigos para catalogação de livros, ISBN, no título eleitoral, no código de endereçamento postal entre muitos outros.

Todos esses sistemas citados utilizam-se da congruência modular para obter o número do dígito verificador ou verificar a autenticidade da sequência numérica do documento.

Nesses sistemas que utilizam a congruência modular um número de identificação é da forma

$$a_1a_2a_3...a_nC,$$

onde C é o algarismo de controle ou dígito verificador. O valor de C é determinado pela congruência

$$p_1a_1 + p_2a_2 + p_3a_3 + ... + p_na_n + C \equiv 0 \ (mod\ k),$$

onde os elementos $\{p_1, p_2, p_3, ..., p_n\}$ são previamentes escolhidos e podem ser chamados de pesos.

Os sistemas desse tipo são chamados de sistema módulo k e a soma $p_1a_1 + p_2a_2 + p_3a_3 + ... + p_na_n + C$ pode ser designada por S.

Utiliza-se o zero nesta congruência embora qualquer outro valor inteiro entre 0 e $k-1$ pode ser usado.

Essa escolha do zero se deve à vantagem de que, se $S \equiv 0 \ (mod\ k)$, temos que $k|S$ e portanto essa soma, utilizada para verificar a autenticidade de um documento, é múltipla de k.

Ao criar um sistema de codificação, a escolha do módulo e dos pesos é o que determinará a capacidade de um sistema detectar um número maior de erros únicos e de transposição.

Isso será demonstrado em dois teoremas a seguir, como visto em [2].

Teorema 4.1. Um sistema de identificação módulo k, com pesos $\{p_1, p_2, ..., p_n\}$ detecta todo erro único, $a_i \to a_i'$, na i-ésima posição se e somente se, $mdc(p_i, k) = 1$.

Demonstração. Considere um número $a_1a_2a_3...C$ de um sistema de identificação módulo k, cujo dígito de verificação é C e a soma é S. Sabe-se que $S \equiv 0 \ (mod\ k)$. Representaremos por S' a soma com a troca $a_i \to a_i'$ na i-ésima posição. Apesar de S' representar uma soma incorreta podemos ter $S' \equiv 0 \ (mod\ k)$ ou $S' \not\equiv 0 \ (mod\ k)$, para caso em que o erro não foi detectado e para quando o erro é detectado, respectivamente.

Calculando a diferença $S' - S$, temos

$S' - S = (p_1a_1 + p_2a_2 + ... + p_ia_i' + ... + p_nC) - (p_1a_1 + p_2a_2 + ... + p_ia_i + ... + p_nC) = p_1a_1 + p_2a_2 + ... + p_ia_i' + ... + p_nC - p_1a_1 - p_2a_2 - ... - p_ia_i - ... - p_nC = p_ia_i' - p_ia_i = p_i(a_i' - a_i)$.

Dessa forma, um erro $a_i \to a_i'$ na i-ésima posição é detectável se, e somente se,

$$p_i(a_i' - a_i) \not\equiv 0 \ (mod\ k), \text{ para } a_i, a_i' \in \{0, 1, 2, ..., k-1\} \text{ e } a_i \neq a_i'.$$

E esta condição é equivalente a $mdc(p_i, k) = 1$ pelo teorema a seguir.

Teorema 4.2. Sejam p e k números inteiros. Então $pb \not\equiv 0 \ (mod\ k)$, para todo $b \in \{1, ..., k-1\}$ se, e somente se, $mdc(p, k) = 1$.

Demonstração. Suponha que $mdc(p,k) = d > 1$. Então $d|p$ e $d|k$, e assim $p = dd_1$ e $k = dd_2$ com $d_2 \in \{1,...,k-1\}$. Fazendo $b = d_2$ temos que

$$pb = pd_2 = dd_1d_2 = d_1dd_2 = d_1k \equiv 0 \ (mod\ k).$$

Como $pb \not\equiv 0 \ (mod\ k)$ temos um absurdo. Portanto, $d = 1$, ou seja, $mdc(p,k) = 1$.

Reciprocamente, como $mdc(p,k) = 1$ temos que $k \nmid p$. Seja $b \in \{1,....k-1\}$ tal que $pb \equiv 0 \ (mod\ k)$. Logo $k|pb$ e $mdc(p,k) = 1$. Segue que $k|b$, absurdo, pois $0 < b \leq k-1$. Portanto, $pb \not\equiv 0 \ (mod\ k)$. □

Assim, um sistema modular de identificação vai detectar todo erro único se, e somente se, $mdc(p_i,k) = 1$. □

Teorema 4.3. Um sistema de identificação módulo k, com pesos $\{p_1, p_2, ..., p_n\}$, detecta todos os erros de transposição dos algarismos a_i e a_j nas posições i e j se, e somente se, $mdc(p_i - p_j, k) = 1$.

Demonstração. Neste caso, a diferença entre a soma com os algarismos trocados e a soma correta é

$$S' - S = (p_1a_1 + ... + p_ia_j + ... + p_ja_i + ... + p_nC) - (p_1a_1 + ... + p_ia_i + ... + p_ja_j + ... + p_nC)$$

$$= p_1a_1 + ... + p_ia_j + ... + p_ja_i + ... + p_nC - p_1a_1 - ... - p_ja_j - ... - p_nC$$

$$= p_ia_j + p_ja_i - p_ia_i - p_ja_j = p_ia_j - p_ia_i + p_ja_i - p_ja_j = p_i(a_j - a_i) - p_j(a_j - a_i) = (p_i - p_j)(a_j - a_i).$$

Portanto, o sistema detecta todas as transposições de algarismos nas posições i e j, se e somente se, para quaisquer $a_i, a_j \in \{0,1,2,...,k\}$ com $a_i \neq a_j$, se tem $(p_i - p_j)(a_j - a_i) \not\equiv 0 \ (mod\ k)$, que é equivalente a $mdc(p_i - p_j, k) = 1$, pelo Teorema 4.2.

□

A maior utilização do módulo 11 se justifica pela facilidade de encontrar pesos primos com 11, usando apenas um algarismo para dígito de verificação. A desvantagem do módulo 11 é que no conjunto de dígitos de 0 a 9 não existe nenhum símbolo que represente o número 10 (resto possível nas divisões por 11). Em geral utiliza-se para sua representação o algarismo romano X ou utiliza-se o dígito 0 para representar o 10.

No caso de sistemas módulo 10, os Teoremas 4.1 e 4.3 trabalhados anteriormente podem ser incompatíveis, dependendo dos pesos adotados.

Portanto, um sistema módulo k pode ter 100% de eficiência na detecção de erros únicos e não detectar os erros de transposição.

Ao se construir um sistema de identificação ou codificação modular é essencial que se conheça os Teoremas 4.1 e 4.3 anteriores, para assim fazer uma boa escolha dos pesos e do módulo que será usado.

4.2 Aplicação em sala de aula

Diante das dificuldades relacionadas à aprendizagem de conceitos matemáticos, que acabam desmotivando o aluno, o professor precisa investir na busca de novas formas de aprimorar as atividades de ensino. Nessa direção, os recursos de ensino constituídos por novas tecnologias, como a internet, o computador e os celulares tem-se apresentados como fortes recursos que desempenham esse papel. Esta seção apresenta uma proposta de sequências de atividades de autoria própria, abordando conteúdos matemáticos do Ensino Fundamental, relacionando aos códigos estudados na seção anterior deste trabalho.

Assim, as atividades aqui propostas buscam ser motivadoras e levam à construção do conhecimento pelo próprio aluno.

Essas atividades foram desenvolvidas com alunos do 9ºano/8ª série do Ensino Fundamental, de uma escola pública. Estas podem ser adaptadas e trabalhadas em outras séries do Ensino Fundamental e do Ensino Médio.

Para desenvolvê-las os alunos precisam dominar as operações básicas com números naturais e ter um conhecimento básico de informática.

O material necessário para realização das atividades foi o uso da sala de informática da escola, celulares dos próprios alunos e embalagens de produtos que os alunos trouxeram de casa. O tempo para realização da atividade depende do envolvimento e empenho dos alunos. Em cada etapa é importante que o professor auxilie e incentive seus alunos na realização dos registros dos resultados obtidos, para análise posterior.

1ª etapa: Conhecendo os QR codes.

Primeiramente, foi exibido aos alunos uma imagem de um QR code e questionado a eles se já haviam visto imagem parecida em algum produto ou em anúncios. A maioria dos alunos presentes, afirmaram já terem visto, porém não sabiam a função deste. Foi explicado aos alunos sobre o que é esse código, um pouco de sua história e sua principal função, que é o armazenamento de informações.

Para ilustrar a aula, os alunos foram levados para a sala de vídeo da escola e assistiram ao vídeo do link:https://www.youtube.com/watch?v=1ipMnFLjxdQ. Nesse vídeo, os alunos puderam ver a grande aplicabilidade dos QR codes e como eles já estão espalhados pelo mundo todo.

Figura 15: Alunos na sala de vídeo.

Logo após, os alunos fizeram uso do celular, conectados à internet, para baixar um leitor de QR code, o Barcode (existem muitos outros aplicativos de leitura de um QR code que podem ser baixados gratuitamente). Como atividade, os alunos foram divididos em grupos e receberam o QR code da imagem abaixo.

Figura 16: Imagem de um QR code com atividade Matemática.

Cada grupo decodificou a imagem usando o aplicativo baixado. O conteúdo da imagem era o seguinte link:http://professoraju-mat.blogspot.com.br/2010/06/enigmas-da-ju-aranha-e-sua-teia.html, que os direcionava para a página do Blog de uma professora, onde continha um exercício de Matemática. Cada grupo resolveu o exercício proposto e explicou o método adotado.

2ª etapa:

Nessa parte do desenvolvimento do trabalho, foi explicado aos alunos como criar um QR code. Foi mostrado a eles, que existem diversos sites que fazem essa criação gratuitamente, como por exemplo:

- http://www.qr-code-generator.com/.
- http://e-lemento.com/gerador-qr-code.
- https://www.invertexto.com/qrcode.

Cada grupo foi para a sala de informática, e começou a fazer tentativas para criar seus próprios QR codes. Nesse ponto do trabalho, é interessante salientar que o interesse dos alunos nessa parte do desenvolvimento do trabalho foi surpreendente. Criaram vários QR codes com links, com imagens, com texto, com figuras, fazendo o uso das formas mais criativas possíveis. A escola preparava-se para uma Feira do Conhecimento. Então, cada grupo, aproveitou-se da nova forma de informar para criar QR codes voltados para o tema que cada grupo apresentaria no dia dessa feira. A escola ficou tomada de QR codes pelos corredores. A seguir, alguns QR codes criados pelos alunos:

(a) QR code criado pelo grupo 2.

(b) QR code criado pelo grupo 5.

Figura 17: QR codes criados pelos alunos.

Um aluno de cada grupo ficou responsável de informar os visitantes da escola no dia da Feira do Conhecimento sobre o que era o QR code e como fazer a leitura deste. Despertou a curiosidade até mesmo de outros professores que quiseram se aprofundar no assunto para também fazer uso do QR code em suas aulas.

3ª etapa:

Ao fazer o estudo do QR code, foi informado aos alunos que este poderia algum dia substituir o código de barras convencional, encontrados nos produtos. Então, na terceira etapa, foi realizado com os alunos, o estudo do código de barras tradicional.

Primeiramente, foi contado um pouco da história e evolução do código de barras. Já na sala de informática foi proposto aos alunos que visitassem a página da internet: http://gizmodo.uol.com.br/a-historia-nao-contada-da-origem-dos-codigos-de-barras/, onde existe o relato da criação e evolução dos códigos de barra no decorrer dos anos.

Em outro momento, na sala de aula, os alunos tiveram uma aula expositiva sobre a estrutura dos números do código de barras, composto por 13 algarismos, para entenderem o que cada parte do código representa e também foi falado sobre a existência do dígito verificador e sua função. Ao final dessa aula, foi pedido aos alunos que levassem embalagens de produtos com códigos de barras para a próxima aula.

Com as embalagens que os alunos trouxeram, foi pedido que estes analisassem as diferenças entre os códigos das embalagens presentes. Espera-se que com essa parte da atividade os alunos identifiquem: a parte da sequência que seja igual em mais de um produto e a quantidade de dígitos presente. A sala foi separada em grupos novamente e cada grupo foi até a frente na sala de aula, mostrou a embalagem, o significado de cada parte do código, criando na lousa uma tabela para representar o código do país onde o produto foi cadastrado, código do fabricante, código do produto e dígito verificador.

Para finalizar esta etapa, foi exposto aos alunos como determinar um dígito verificador do código de barras da seguinte maneira: deve-se considerar os 12 primeiros dígitos, da esquerda para a direita, e multiplicar os algarismos de ordem ímpar por 1 e de ordem par por 3, somando os produtos obtidos. Para determinar o dígito verificador basta descobrir qual número devemos acrescentar a essa soma obtida para termos um múltiplo de 10. Esse número é o dígito verificador.

Figura 18: Alunos expondo embalagem e a estrutura de um código de barras (a).

Figura 19: Alunos expondo embalagem e a estrutura de um código de barras (b).

Figura 20: Alunos expondo embalagem e a estrutura de um código de barras (c).

O comentário geral é que a atividade foi muito interessante, pois sempre iam aos supermercados com os pais e nunca imaginavam que aquele código tinha uma estrutura e um cálculo matemático envolvido nele.

É importante salientar que nessa atividade os alunos utilizaram-se de cálculos da aritmética do dia-a-dia, mas futuramente, quando tiverem contato com as congruências modulares e classes residuais ficará mais fácil entender os conceitos usados. Foi interessante também ao trabalhar códigos de barras a oportunidade de rever, no 9º ano, critérios de divisibilidade, divisão euclidiana e operações matemáticas fundamentais.

4ª etapa:

Para finalizar, foi exposto aos alunos que existem muitos outros números, usados por eles, no dia-a-dia, que também fazem uso do dígito verificador. Foi citado como exemplo, o número do cartão de crédito, o número do título de eleitor, o número de CPF, entre outros.

Dentre esses números existentes, foi escolhido o número de CPF (cadastro de pessoas físicas) para a realização da última atividade.

Primeiramente foi informado a eles que o CPF é o registro de um cidadão na Receita Federal e que esse documento é necessário em várias situações, como abertura de contas em bancos, emissão de passaporte, entre outras.

Foi ressaltado também que o CPF difere do código de barras, pois este tem nove dígitos de identificação e dois dígitos verificadores. Foi exibido a eles que o nono dígito do CPF representa a unidade federativa em que a pessoa registrou-se, e ilustrada em sala de aula pela tabela a seguir.

Brasil	
Tipo de caracter	Quantidade máxima de caracteres
0	Rio Grande do Sul
1	Distrito Federal, Goiás, Mato Grosso. Mato Grosso do Sul e Tocantins
2	Acre, Amapá, Amazonas, Pará, Rondônia e Roraima
3	Ceará, Maranhão e Piauí
4	Alagoas, Paraíba, Pernambuco e Rio Grande do Norte
5	Bahia e Sergipe
6	Minas Gerais
7	Espírito Santo e Rio de Janeiro
8	São Paulo
9	Paraná e Santa Catarina

Tabela 10: Dígito da federação.

Para que os alunos entendessem como se determina os dígitos verificadores do CPF, foi feito um exemplo do cálculo na lousa, explicando da seguinte maneira: considera-se os nove primeiros dígitos, da esquerda para a direita, do CPF, multiplicando-os por $1,2,3,4,5,6,7,8,9$, nesta ordem; depois soma-se os produtos obtidos, dividindo essa soma por 11; o resto obtido é o 10^{o} dígito, ou seja, o primeiro algarismo do dígito verificador. Para determinar o segundo dígito verificador, deve-se novamente considerar os nove primeiros dígitos, da esquerda para a direita, juntamente com o primeiro dígito verificador obtido anteriormente, multiplicando-os por $0,1,2,3,4,5,6,7,8,9$, nesta ordem; depois, soma-se os produtos obtidos e divide essa soma novamente por 11; o resto obtido é o 11^{o} dígito, ou seja, o segundo algarismo do dígito verificador.

Após ouvirem esta explicação, foi pedido aos alunos que para próxima aula trouxessem o CPF para a aula com os algarismos do dígito verificador tampados, com fita adesiva, para realização de uma atividade em grupo. Essa atividade foi realizada em duplas e consistia de que os alunos trocassem de CPF, já estando esse com os dois últimos dígitos tampados. O aluno de posse do CPF do colega deveria usar o algoritmo exposto na aula anterior para descobrir os algarismos que compunham o dígito verificador do colega.

Figura 21: Alunos determinando o dígito verificador do CPF.

Ao terminar, cada aluno, já com seu próprio CPF em mãos novamente, tirava a fita adesiva e verificava se o colega havia encontrado os dois algarismos corretamente.

Foi uma atividade produtiva, pois usou-se de operações matemáticas e ao mesmo tempo, constitui-se numa atividade lúdica, pois o fato de descobrir o número corretamente tornou-se um desafio.

Espera-se que com atividades como essas a Matemática, que constitui ferramenta fundamental para a formação de cidadãos, possa ser vista como algo que proporciona um ambiente investigativo e criativo, onde é possível fazer conexões entre diversas formas de pensamentos com outras áreas do saber e com aplicações na atualidade.

REFERÊNCIAS

[1] CORREIO. *CPF terá QR Code e dados poderão ser atualizados na receita federal.* Disponível em:http://www.correiobraziliense.com.br/app/noticia/brasil/2017/01/12/internas_-polbraeco,564690/cpf-tera-qr-code-e-dados-poderao-ser-atualizados-no-site-da-receita-fe.shtml. Acesso em 03 de Março de 2017. Citado na página 98.

[2] COSTA, F.R.A. *Sistemas de Identificação Modular: uma aplicação no ensino fundamental.* TCC - PROFMAT- UFSJ, 2014. Citado na página 101.

[3] COUTINHO, S.C. *Números inteiros e Criptografia RSA.* Rio de Janeiro: IMPA, 2014. Citado nas páginas 65 e 66.

[4] FORMIN, D. *Círculos Matemáticos.* Rio de Janeiro: IMPA, 2012. Citado na página 39.

[5] FREIRE, B.T.V. *Notas de Aula: Teoria dos Números.* Citado na página 29.

[6] HEFEZ, A. *Aritmética.* Rio de Janeiro: SBM, 2014. Citado na página 42.

[7] HEFEZ, A. *Elementos de Aritmética.* Rio de Janeiro: SBM, 2005. Citado na página 68.

[8] MAIER, R.R. *Teoria dos Números. Notas de aula* 2005. Citado na página 27.

[9] MARTINEZ, F.B. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro.* 2. ed. Rio de Janeiro: IMPA, 2013. Citado na página 27.

[10] MILIES, C.P. *A Matemática dos Códigos de Barras.* 19 f. São Paulo, SP.IME/USP- Departamento de Matemática. Citado nas páginas 79, 80 e 88.

[11] MOREIRA, C.G.T.A. *Tópicos de Teoria dos Números.* Rio de Janeiro: SBM, 2012. Citado na página 59.

[12] MOREIRA, F.R.S. *Congruências Lineares.* ITA, 2006. Citado na página 64.

[13] Ribenboim, P. *Números Primos. Velhos mistérios e novos recordes.* 1. ed. Rio de Janeiro: IMPA, 2014. Citado na página 55.

[14] SAUTOY, M.D. *A Música dos Números Primos: A História de um Problema não Resolvido na Matemática.* Rio de Janeiro: Zahar, 2007. Citado na página 51.

[15] VEJA *Cientistas descobrem o maior número primo.* Disponível em http://veja.abril.com.br/ciencia/cientistas-descobrem-o-maior-numero-primo-e-ele-tem-mais-de-22-milhoes-de-digitos/. Acesso em 05 de Fevereiro de 2017. Citado na página 54.

[16] WALL, E.S. *Teoria dos Números para professores do ensino fundamental.* Porto Alegre: AMGH, 2014. Citado nas páginas 55, 71, 74 e 76.


ICMC
USP
SÃO CARLOS