Universidade Federal de Mato Grosso
Instituto de Ciências Exatas e da Terra
Departamento de Matemática

A aritmética como conteúdo extracurricular no ensino médio

Rosângela Ferreira Domingues

Mestrado Profissional em Matemática: PROFMAT/SBM

Orientador: **Prof. Dr. Tibério Bittencourt de Oliveira Martins**

Trabalho financiado pela Capes

Barra do Garças/MT

Abril de 2017

A aritmética como conteúdo extracurricular no ensino médio

Este exemplar corresponde à redação final da dissertação, devidamente corrigida e defendida por Rosângela Ferreira Domingues e aprovada pela comissão julgadora.

Barra do Garças, 04 de maio de 2017.

Prof. Dr. Tibério Bittencourt de Oliveira Martins
Orientador

Banca examinadora:

Prof. Dr. Tibério Bittencourt de Oliveira Martins
Prof. Dr. Márcio Lemes de Sousa
Prof. Dr. Romildo da Silva Pina

Dissertação apresentada ao curso de Mestrado Profissional em Matemática – PROFMAT, da Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título **de Mestre em Matemática**.

Dados Internacionais de Catalogação na Fonte.

D671a Domingues, Rosângela Ferreira.
A aritmética como conteúdo extracurricular no ensino médio / Rosângela Ferreira Domingues. -- 2017
xiii, 72 f. : il. ; 30 cm.

Orientador: Tibério Bittencourt de Oliveira Martins.
Dissertação (mestrado profissional) - Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação em Matemática, Cuiabá, 2017.
Inclui bibliografia.

1. Aritmética. 2. Oficinas de aprendizagem. 3. Ensino médio. I. Título.

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

MINISTÉRIO DA EDUCACÃO
UNIVERSIDADE FEDERAL DE MATO GROSSO
PRÓ-REITORIA DE ENSINO DE PÓS-GRADUACÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL - PROFMAT
Av. Fernando Corrêa da Costa, 2367 - Boa Esperança – 78.060-900 – Cuiabá/MT
Tel : (65) 3615-8576 - Email : profmat@ufmt.br

FOLHA DE APROVAÇÃO

TÍTULO : "A aritmética como conteúdo extracurricular no ensino médio"

AUTOR : Rosângela Ferreira Domingues

defendida e aprovada em 28/04/2017.

Composição da Banca Examinadora:

Presidente Banca / Orientador Doutor Tibério Bittencourt de Oliveira Martins
Instituição : Universidade Federal de Mato Grosso

Examinador Interno Doutor Márcio Lemes de Sousa
Instituição : Universidade Federal de Mato Grosso

Examinador Externo Doutor Romildo da Silva Pina
Instituição : Universidade Federal de Goiás

BARRA DO GARÇAS, 28/04/2017.

À minha família, em especial ao meu esposo Antonio Carlos de O. Machado e meus filhos Karine Domigues Machado e Kairo Domingues Machado.

Agradecimentos

Agradeço primeiramente a Deus por todas as graças alcançadas, pois creio que sempre posso contar com Sua proteção. Aos meus pais, Valdeci Ferreira Domingues e Pedro José Domingues, que me criaram e me proporcionaram todas as condições necessárias aos meus estudos e sempre estiveram ao meu lado quando precisei. Ao meu esposo, Antonio Carlos, que em nenhum momento deixou de acreditar que eu conseguiria, por ser o meu grande incentivador a continuar com meus estudos, foi meu alicerce em todos os momentos de dificuldade e proporcionou aos nossos filhos toda a atenção que eu não pude dar nesses dois anos, principalmente durante a minha ausência física por conta das viagens (mais de 60 000 quilômetros percorridos). Aos meus filhos, Kairo e Karine, por terem a paciência e compreensão ao verem meu tempo e atenção dividida com os estudos. Aos meus irmãos e demais familiares que sempre me incentivaram. Ao meu orientador, Prof. Dr. Tibério Bittencourt de Oliveira Martins, pelo apoio, colaboração e incentivo e pela competência e sabedoria. A todos os meus colegas de curso, companheiros de muitas horas de estudos, amigos que sempre vou me lembrar com um carinho muito especial, pois sem eles eu não teria conseguido chegar até aqui. Ao PROFMAT, pela oportunidade e a CAPES, pelo apoio financeiro. Enfim a todos amigos e colegas que de alguma forma me incentivaram e torceram por mim.

A mente que se abre a uma nova ideia,
jamais voltará ao seu tamanho original.

O mais incompreensível sobre o mundo,
é que seja compreensível.

Albert Einstein.

Resumo

Este trabalho apresenta uma proposta para trazer melhorias no processo de ensino e aprendizagem para os alunos do Ensino Médio através da inserção da aritmética como conteúdo extracurricular. O objetivo principal é apresentar aplicações da aritmética que podem ser inseridas como oficinas de aprendizagem durante o ano letivo. Para o desenvolvimento do trabalho foram realizadas pesquisas sobre os principais resultados dentro da teoria dos números relacionados à aritmética. Entre as aplicações da aritmética que foram pesquisadas, destacam-se os códigos de barras e a criptografia.

Palavras chave: Aritmética, oficinas de aprendizagem, ensino médio.

Abstract

This work presentes a proposal to bring improvements for the teaching and learning process for the students at High School through the insertion of arithmetic as extracurricular content. The principal objective is to present applications of arithmetic that can be inserted as learning workshops during the school year. For the development of this work, a research about the main results of number theory related to arithmetic were realized. Among the applications of this researched in arithmetics stand out the bar codes and the cryptography.

Keywords: Arithmetic, learning workshops, high school.

Sumário

Lista de Figuras

Lista de Quadros

Lista de Tabelas

Introdução

> "A Matemática é a rainha das ciências e a teoria dos números é a rainha das matemáticas."
>
> (Gauss)

A matemática sempre esteve e sempre estará presente nas diversas atividades do ser humano, por isso há a necessidade de proporcionar aos jovens um conhecimento matemático para a vida, capaz de inseri-los no mundo atual como cidadãos conscientes.

A disciplina de matemática foi introduzida no currículo escolar brasileiro no século XVIII, passando por uma reorientação curricular no século XX, a partir da década de 20. No período de 1960 a 1970, a matemática moderna reformou amplamente o currículo da matemática enfatizando a teoria dos conjuntos, as estruturas algébricas, etc. Esse novo ensino, formalizava a matemática tornando-a cada vez mais distante das questões práticas, principalmente no ensino fundamental. A partir de 1980, o destaque do ensino da matemática foi na resolução de problemas levando-se em conta aspectos sociais e cognitivos entre outros, na aprendizagem da matemática. Esses conceitos davam importância ao aluno como ser ativo na construção do conhecimento, com ênfase na resolução de problemas criados a partir do cotidiano do aluno. Apesar dessas mudanças, os problemas com a aprendizagem ainda persistiam, conforme Brasil (1998, p. 79):

> Muitos alunos têm a sensação de que a Matemática é uma matéria difícil e que seu estudo se resume em decorar uma série de fatos matemáticos, sem compreendê-los e sem perceber suas aplicações e que isso lhes será de pouca utilidade. Tal constatação os leva a assumir atitudes bastante negativas, que se manifestam no desinteresse, na falta de empenho e mesmo na pouca preocupação diante de resultados insatisfatórios ou nos sentimentos de insegurança, bloqueio e até em certa convicção de que são incompetentes para aprendê-la, o que os leva a se afastar da Matemática em situações na vida futura.

Atualmente ainda é constante a busca por novas metodologias para sanar as dificuldades em relação ao ensino de matemática. Nessa busca, o grande destaque da

Teoria dos Números: a Aritmética em conjunto com suas aplicações é uma ferramenta que pode vir a despertar no aluno um interesse investigativo pela matemática o que é algo que acrescenta muito no processo ensino aprendizagem. Segundo Coutinho (2007, p.ii):

> O que os matemáticos entendem como teoria dos números é o estudo das propriedades dos números inteiros, e não de quaisquer tipos de números. Por exemplo, questões referentes à fatoração de inteiros, ao cálculo do máximo divisor comum e ao estudo dos números primos, fazem parte desta teoria. Na verdade, juntamente com a geometria, essa é uma das áreas mais antigas da matemática.

A aritmética não tem tido muito espaço no ensino médio, apesar de que há muitas aplicações em situações que podem contextualizar os assuntos abordados nessa fase escolar. Problemas envolvendo situações do cotidiano do aluno podem facilmente ser resolvidos através da aritmética aplicando conceitos de fatoração ou critérios de divisibilidade, por exemplo. Conforme Lorensatti (2012, p. 13-14):

> A Aritmética faz parte da cultura dos povos desde os tempos antigos, tendo sido desenvolvida para atender às necessidades de comunicação e quantificação. Na história das civilizações, os povos a criaram e a recriaram sob roupagens diferentes, utilizando essencialmente os mesmos processos matemáticos modificados ao longo do tempo. Em nossos dias, as experiências de quantificação de objetos e fenômenos fazem parte da vida prática das pessoas, e o estudo da Aritmética é uma necessidade para prover a organização adequada da sociedade e oferecer oportunidades para o indivíduo desenvolver processos matemáticos inerentes à sua estrutura lógica mental.

A inserção da aritmética no ensino médio, como um componente extracurricular, visa auxiliar no processo ensino aprendizagem como um instrumento contextualizador dos conteúdos já abordados nessa etapa escolar. Pretende-se aqui desenvolver uma metodologia diferenciada com os alunos do ensino médio através das aplicações da aritmética com o intuito de despertar nesses alunos o interesse pela aprendizagem da matemática, bem como melhorar o desempenho deles nessa disciplina.

A aritmética é um assunto abordado desde o ensino fundamental, com as propriedades dos números inteiros, cálculo de máximo divisor comum, mínimo múltiplo comum e algoritmo da divisão, mas no ensino médio ela acaba sendo deixada de lado apesar de ainda ter muito a contribuir. Seus conceitos são de fácil demonstração e compreensão, pois envolve basicamente operações com números inteiros, e em muito auxiliam na aprendizagem de conteúdos dessa etapa escolar. Muitas são as aplicações da aritmética no cotidiano do aluno, ela está presente nos códigos identificadores utilizados pelo comércio, como por exemplo, os códigos de barras, nos calendários, na criptografia, dentre outros.

Com a aritmética podemos resolver problemas de olimpíadas de matemática através dos conceitos de divisibilidade e congruências entre números inteiros, por exemplo.

O objetivo desse trabalho é contribuir para a melhoria do ensino aprendizagem dos alunos do ensino médio desenvolvendo uma metodologia extracurricular utilizando a contextualização dos conteúdos de matemática através da aritmética aplicada aos códigos identificadores, à divisão euclidiana, e congruências de números inteiros. Para atingir esse objetivo principal deverá ser atingido os objetivos específicos: conhecer os conceitos básicos de aritmética como divisão euclidiana, congruência modulo m, máximo divisor comum, mínimo múltiplo comum, Teorema Fundamental da Aritmética, dentre outros; compreender quais conceitos de aritmética modular são utilizados na elaboração de um código de barras e outros códigos de identificação e criptografia; e despertar o interesse pela matemática nos alunos do ensino médio, através de problemas envolvendo os conceitos de aritmética, principalmente os de olimpíadas de matemática.

Para realização desse trabalho, inicialmente será feita uma pesquisa bibliográfica sobre os conceitos básicos de aritmética, como divisão euclidiana, congruência modulo m, máximo divisor comum, mínimo múltiplo comum, Teorema Fundamental da Aritmética, dentre outros. Em um segundo momento, será realizada pesquisa bibliográfica acerca das aplicações da aritmética nos códigos de barras, e de outros códigos de identificação, na criptografia e outras aplicações. Ao final do estudo teórico, apresentaremos uma proposta que traz a aritmética como conteúdo extracurricular no ensino médio, onde serão propostas algumas oficinas de aplicação dos conceitos de aritmética apresentados, destacando os códigos de identificação e a criptografia.

Capítulo 1

Aritmética

Neste capítulo abordaremos um pouco da história da aritmética, destacando quais os principais matemáticos que contribuíram com as descobertas nesse importante ramo da teoria dos números. Abordaremos também os principais resultados que serão utilizados nas aplicações do segundo capítulo.

1.1 A aritmética e suas origens

A aritmética, parte essencial da Teoria dos Números, é o estudo das propriedades dos números inteiros. A aritmética tem suas origens ainda nas civilizações antigas, quando se inicia o processo de contagem, de associação de objetos a números. Na Grécia antiga, ela começa a dar os primeiros sinais de aparência com a aritmética que usamos hoje, O termo aritmético vem do grego, onde *arithmos* significa número e *technes* significa ciência, assim a aritmética é a ciência dos números. Segundo Coutinho (2014, p.8):

> No que diz respeito aos inteiros, os gregos diferenciavam entre a logística, ou arte de calcular com números inteiros, e a aritmética, ou estudo das propriedades fundamentais dos números inteiros. A primeira era domínio dos comerciantes e profissionais: a segunda dos matemáticos e filósofos. A teoria dos números era herdeira da aritmética dos gregos. Ironicamente a palavra aritmética é usada hoje em dia para descrever aquilo que os gregos chamavam de logística.

Os primeiros registros da aritmética atual podem ser observados na obra *Elementos* escrita por Euclides, matemático que viveu em Alexandria por volta de 300 a.C.. Essa obra, composta por treze livros, sendo que três deles tratava de problemas relacionados à aritmética, reuniu muita coisa da escola pitagórica.

A escola pitagórica, criada na Grécia por Pitágoras por volta de 520 a.C., era um misto de escola e comunidade religiosa onde se difundia o estudo da Ciência, da Matemática e da Filosofia. Era uma espécie de sociedade secreta por isso há poucos registros das descobertas realizadas por ela. A escola pitagórica existiu por mais de dois séculos, mesmo após a morte de Pitágoras. Mesmo com poucos registros escritos, as primeiras contribuições na aritmética, como a classificação dos números pares e ímpares são atribuídas a Pitágoras, pois tudo o que era descoberto na escola pitagórica era atribuído ao chefe. Conforme Domingues (1991, p. 9):

> Não restam dúvidas que os pitagóricos viam o papel dos números de uma maneira muito especial. Daí não ser surpresa que a aritmética teórica tenha nascido com eles. Como a escola tratava a matemática de maneira muito filosófica e abstrata, desvinculada das exigências da vida prática, era natural que separassem o estudo teórico dos números que chamavam *aritmética*, dos cálculos práticos, que denominavam *logística*. Preocupando-se essencialmente com o primeiro desses aspectos.

Os números inteiros negativos tiveram a sua primeira aparição em uma obra do indiano Brahmagupta por volta de 628 d.C., onde ele considera os negativos como dívidas. Diofanto de Alexandria, que viveu no século III, foi considerado o maior algebrista grego e ele foi quem melhor operou com os números negativos, ele tratava de equações indeterminadas com coeficientes inteiros.

A aritmética só voltou a ter grande destaque no século XVII, quando o francês Pierre de Fermat, em 1621, adquiriu uma cópia da obra de Aritmética de Diofanto, cujo texto original foi publicada em grego e em uma tradução latina por Bachet de Méziriac nove anos antes. Fermat era um magistrado e não um matemático por profissão, mas se interessou pelo assunto e fez muitas anotações sobre a obra de Diofanto. Pelo que diz Groenwald et al (2005, p.95), nessa época não haviam publicações na área de matemática, mas o frade francês Marin Mersenne era muito amigos dos matemáticos da época, como Pascal, Descartes e o próprio Fermat e era o principal divulgador das descobertas destes, e a comunicação era feita através de cartas, e foi assim que boa parte da obra de Fermat ficou conhecida. Mas foi só depois de sua morte em 1665, que seu filho Samuel Fermat coletou e publicou a obra de seu pai Pierre de Fermat.

Outro grande matemático foi Leonhard Euler, nascido em 1707 e teve uma vasta obra que contribuiu não só na aritmética como em outras áreas da matemática no século XVIII. Euler tomou conhecimento da obra de Fermat em 1730, através de Christian Goldbach, matemático prussiano, nascido em 1764, que também teve algumas contribuições

para a aritmética. Leonhard Euler estendeu muitos resultados de Fermat, segundo Groenwald (2005, p.95):

> Em sua primeira carta a Euler em 1729, Goldbach acrescenta o seguinte PS: *Você conhece a observação de Fermat de que todos os números* $2^{2^n}+1$ *são primos? Ele disse que não sabia prová-la; nem ninguém conseguiu fazê-lo, que eu tenha conhecimento.* Euler reage com ceticismo e não demonstra muito interesse, mas Goldbach não desiste e volta ao assunto. Em 1730, Euler começa finalmente a ler a obra de Fermat. Nos anos seguintes ele provaria e estenderia grande parte dos resultados enunciados por Fermat, resolvendo inclusive a questão proposta por Goldbach.

Carl Friedrich Gauss, alemão, nascido em 1777, foi matemático, astrônomo e físico, considerado o príncipe da matemática, foi quem sistematizou a teoria dos números através da sua obra *Disquisitiones Arithmeticae*, publicada em 1801.

São algumas das contribuições desses grandes matemáticas que iremos estudar nas próximas seções.

1.2 Números inteiros

As referências para essa e as próximas seções são: Hefez (2006) e Hefez (2014).

Seja $\mathbb{Z}$ o conjunto dos números inteiros onde $\mathbb{Z} = \{-3, -2, -1, 0, 1, 2, 3, 4...\}$, temos definidas as operações de adição e multiplicação e uma relação de ordem. Mas antes de apresentar essas operações, vamos ver dois princípios muito utilizados nas demonstrações dos resultados que terão grande relevância nesse capítulo: o Princípio da Boa Ordenação e o Princípio da Indução Finita.

1.2.1 Princípio da Boa Ordenação

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 $x \in S$. Assim, podemos escrever:

Axioma 1.1 - Princípio da Boa Ordenação: Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então S possui um menor elemento.

Esse é um axioma que caracteriza o conjunto dos números inteiros e o diferencia de conjuntos como os racionais e os reais, pois nesses não é possível determinar um menor

elemento em um subconjunto. Se considerarmos, por exemplo, um subconjunto de $\mathbb{R}$ dado por $X = \{x|2 < x < 3\}$, não é possível determinar o menor elemento desse subconjunto.

1.2.2 Princípio da Indução Finita

Esse é um valioso instrumento para demonstrar teoremas que envolvem os números inteiros e vem sendo utilizado desde a antiguidade, mesmo que implicitamente. A indução matemática é o quarto axioma de Giuseppe Peanno (1858-1932), utilizados para caracterizar os números naturais. Eis o seu enunciado:

Teorema 1.1 - Princípio da Indução Finita - Seja 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:

Tomando $S' = \{x \in \mathbb{Z}; x \geq a\}$, vamos supor por absurdo que S' não está contido em S, logo $S'\backslash S \neq \emptyset$. Como, pelo Princípio da Boa Ordenação, esse conjunto é limitado inferiormente por a, existe um menor elemento c em $S'\backslash S$. Como $c \in S'$ e $c \notin S$, segue que $c > a$. Portanto, $c - 1 \in S'$ e $c - 1 \in S$, pois c é o menor elemento de $S'\backslash S$. Assim, pela hipótese sobre S, temos que $c = (c - 1) + 1 \in S$, e como $c \in S'$, temos uma contradição, pois $c \in S'\backslash S$. Portanto $S' \subset S$.

Seja $P(n)$ uma propriedade de um número natural n e seja $n_o \in \mathbb{N}$, o Princípio da Indução Finita consiste verificar que:

(i) $P(n_{0)}$ é verdadeira

(ii) Para todo $n \geq n_0$, se $P(n)$ é verdadeira então $P(n+1)$ também é verdadeira. Portanto $P(n)$ é válida para todo $n \in \mathbb{N}$.

Exemplo 1.1 - Provar, usando indução finita, que $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$, que é a soma dos n primeiros números naturais.

Resolução:

Queremos provar que $P(n) : 1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$ é verdadeira, para isso vamos usar indução sobre n.

(i) Tomando $n_0 = 1$, temos que $P(1) : 1 = \dfrac{1(2)}{2} = \dfrac{1(1+1)}{2} = 1$, logo $P(1)$ é válida.

(ii) Supondo que a propriedade é verdadeira para algum $n > 1$ teremos a veracidade para $n + 1$, ou seja $P(n+1) : 1 + 2 + 3 + \cdots + n + (n+1) = \dfrac{(n+1)(n+2)}{2}$ é válida.

Partindo da nossa hipótese indutiva, $P(n)$, vamos somar $(n + 1)$ em ambos os membros da igualdade, obtendo:

$1 + 2 + 3 + \cdots + n + (n+1) = \dfrac{n(n+1)}{2} + (n+1)$, isso equivale a:

$1 + 2 + 3 + \cdots + n + (n+1) = \dfrac{n(n+1) + 2(n+1)}{2}$, logo:

$1+2+3+\cdots+n+(n+1) = \dfrac{(n+1)(n+2)}{2}$, obtemos assim a $P(n+1)$. Portanto, pelo Princípio da Indução Finita, a propriedade é verdadeira para todo $n \in \mathbb{N}$.

O Princípio da Indução Finita tem uma segunda forma conhecida como Princípio da Indução Completa ou Segunda Forma do Princípio da Indução, ou ainda, Indução Forte. Essa segunda forma será descrita no próximo teorema.

Teorema 1.2 - Seja P(n) uma sentença aberta tal que:

(i) $P(n_0)$ é verdadeiro, e que

(ii) $\forall n$, $P(n_0)$ e $P(n_0 + 1)$ e $\cdots$ e $P(n) \Rightarrow P(n+1)$ é verdadeiro.

Então, P(n) é verdadeiro para todo $n \geq n_0$.

Demonstração:

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

Vamos utilizar essa forma do Princípio da Indução Finita para demonstrar o Teorema Fundamental da Aritmética na seção 1.6.1.

1.2.3 Adição, multiplicação e ordem em $\mathbb{Z}$

Sejam a, b e c números inteiros quaisquer, em $\mathbb{Z}$ são definidas as operações de adição $(+)$, multiplicação $(\cdot)$ e uma relação de ordem ($\leq$ menor do que ou igual), onde são válidas as seguintes propriedades:

A_1 - A adição é associativa: $(a+b)+c = a+(b+c)$.

A_2 - A adição é comutativa: $a+b = b+a$.

A_3 - A adição tem um elemento neutro: $a+0 = a$.

A_4 - Todo elemento de $\mathbb{Z}$ tem um elemento simétrico em relação à adição: $a+(-a) = (-a)+a = 0$.

M_1 - A multiplicação é associativa: $a.(b.c) = (a.b).c$.

M_1 - A multiplicação é comutativa: $a.b = b.a$.

M_1 - A multiplicação possui um elemento neutro: $1.a = a$.

AM - A multiplicação é distributiva com relação à adição: $a.(b+c) = a.b + a.c$.

O_1 - A relação de ordem é reflexiva: $a \leq a$.

O_2 - A relação de ordem é antissimétrica: $a \leq b$ e $b \leq a$ então $a = b$.

O_3 - A relação de ordem é transitiva: $a \leq b$ e $b \leq c$ então $a \leq c$.

O_4 - A relação de ordem é compatível e cancelativa em relação à adição: $a \leq b \Leftrightarrow a+c \leq b+c$.

Usaremos a notação $a < b$ (a menor do que b) quando na relação $a \leq b$ tivermos $a \neq b$. Usamos também as notações $b > a$ (b maior do que a) e $b \geq a$ (b maior do que ou igual a a) sempre que $a < b$ ou $a \leq b$ respectivamente.

A operação da adição nos permite definir a operação chamada subtração: dados dois números inteiros a e b, definimos o número $b-a$ (b menos a) como sendo o resultado da subtração de a de b então:

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

Outra propriedade muito importante dos números inteiros é a chamada Propriedade Arquimediana.

Corolário 1.1 - Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, então existe $n \in \mathbb{Z}$ tal que $nb > a$.

Demonstração:

Como $|b| \neq 0$ e não existe nenhum número inteiro n tal que $0 < n < 1$, temos que $|b| \geq 1$, dessa forma:

$$(|a| + 1)|b| \geq |a| + 1 > |a| \geq a.$$

Tomando:

(i) $n = |a| + 1$, se $b > 0$, logo $nb > a$; e

(ii) $n = -(|a| + 1)$, se $b < 0$.

1.2.4 Divisão em $\mathbb{Z}$

A divisão entre dois números inteiros nem sempre é possível, mas quando é possível expressamos isso com o conceito de divisibilidade. Mesmo quando a divisão não é possível, pode-se efetuá-la encontrando um "resto bem pequeno" através da chamada *divisão euclidiana*. Vejamos esses conceitos a seguir.

1.2.4.1 Divisibilidade

Sejam a e b dois números inteiros quaisquer, com $a \neq 0$, dizemos que a divide b e representamos por $a|b$ quando existir um número $c \in \mathbb{Z}$ tal que $b = ca$. Quando isso acontece podemos dizer que a é um divisor ou um fator de b, ou ainda podemos dizer que b é divisível por a ou que b é um múltiplo de a. Quando a não divide b usamos a notação $a \nmid b$.

Para quaisquer inteiros a, b e c são válidas as seguintes propriedades:

D_1: $1|a$, $a|a$ e $a|o$.

D_2: $0|a \Leftrightarrow a = 0$.

D_3: $a|b$ se, e somente se $|a| \mid |b|$

D_4 :se $a|b$ e $b|c$ então $a|c$.

As propriedades D_1 e D_2 nos dizem que todo número inteiro a é divisível por ± 1 e por $\pm a$, inclusive que $0|0$. Assim, todo número inteiro divide 0, ou seja, 0 tem infinitos divisores.

Utilizamos a notação $\frac{b}{a}$ e dizemos que $c = \frac{b}{a}$ para a, b e c inteiros, com $a \neq 0$, sempre que $b = ca$.

Proposição 1.1 - *Se $a, b, c, d \in \mathbb{Z}$, se $a|b$ e $c|d \Rightarrow ac|bd$.*

Demonstração: Se $a|b$ e $c|d$ então existem $k, y \in \mathbb{Z}$ tal que $b = ka$ e $d = yc$. Dessa forma $bd = (ka).(yc) = (ky)(ac)$, portanto $ac|bd$.

1.2.4.2 Divisão euclidiana

Em sua obra *Elementos*, Euclides já utilizava o fato de que é sempre possível efetuar a divisão de a por b deixando um resto considerado pequeno, apesar de que Euclides só tratava com números naturais.

Teorema 1.3 - Dados a, b inteiros existem dois inteiros únicos p, r tais que $a = bq + r$, com $0 \leq r < |b|$.

Demonstração:

Vamos dividir a prova em dois itens: existência e unicidade.

(i) Existência: Pela propriedade arquimediana dos inteiros $\exists\ q \in \mathbb{Z}$ tal que $-ba \geq -a$ de modo que $a - bq \geq 0$. Seja $S = \{x = a - bq; q \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$, onde x é o candidato a resto.

Pelo Princípio da Boa Ordenação, S tem um menor elemento, vamos denominá-lo r. Vamos supor que $0 \leq r < |b|$, logo temos que $r \geq 0$, pois pertence a S. Agora, vamos supor, por contradição, que $r \geq |b|$, ou seja, $r = |b| + s$ onde $s \geq 0$ e $s < r$. Vamos mostrar que $s \in S$:

Sabemos que;

$$a = bq + r = bq + |b| + s = bq \pm b + s,$$

dependendo de b então:

$$a = b(q \pm 1) + s,$$

sendo assim:

$$s = a - b(q \pm 1)$$

ou seja: $s \in S$, o que é uma contradição, pois r é o menor elemento.
Portanto,

$$r < |b|.$$

(ii) Unicidade: Para provar a unicidade vamos supor que existem q, q', r e $r' \in \mathbb{Z}$ tais que: $a = bq + r, 0 \leq r < |b|$ e $a = bq' + r', 0 \leq r' < |b|$, assim igualando as duas equações obtemos:

$$bq + r = bq' + r'$$

então:

$$0 = b(q - q') + r - r'$$

assim:

$$r' - r = b(q - q')$$

logo:

$$|r' - r| = |b|.|q - q'| \qquad (1)$$

Multiplicando a inequação $0 \leq r' < |b|$ por -1 e somando à $0 \leq r < |b|$, obtemos:

$$-|b| \leq r - r' < |b|$$

logo

$$r - r' < |b| \qquad (2)$$

Substituindo (1) em (2) obtemos:

$$|b|.|q - q'| < |b|$$

logo:

$$|q - q'| < 1$$

isso implica que:

$$|q - q'| = 0$$

Portanto $q = q'$ e, por (1),

$$r = r'.$$

Dessa forma, em uma divisão euclidiana $b = aq + r$ temos que o número b é chamado dividendo, o número a divisor, os números q e r são chamados, respectivamente, quociente e resto.

1.2.5 Múltiplos inteiros de um número

Definição 1.1 - Chamamos de múltiplo de um número inteiro a ao número ma que resulta da multiplicação do número a pelo número m.

Seja um a um número inteiro chamamos de conjunto dos múltiplos de a ao conjunto:

$$a\mathbb{Z} = \{a \times d; d \in \mathbb{Z}\}.$$

Os múltiplos de um número inteiro possuem as propriedades abaixo, considerando a e m números inteiros.

(i) 0 é múltiplo de a.

(ii) Se m é um múltiplo de a, então $-m$ é múltiplo de a.

(iii) Um múltiplo de um múltiplo de a é um múltiplo de a.

(iv) Se m e m' são múltiplos de a, então $m + m'$ e $m - m'$ são também múltiplos de a.

(v) Se m e m' são múltiplos de a, então $em + fm'$ é múltiplo de a, quaisquer que sejam os inteiros e e f.

(vi) Se $m+m'$ ou $m-m'$ é múltiplo de a e m é múltiplo de a, então m' é múltiplo de a.

1.3 Divisores de um número inteiro

Definição 1.2 - Divisor de um número inteiro a é todo número inteiro b tal que $b|a$, ou seja, a é um múltiplo de b.

O conjunto dos divisores de um inteiro a é representado por:

$D(a) = \{x \in \mathbb{Z}^*; x|a\}$, onde $\mathbb{Z}^*$ denota-se o conjunto dos inteiros não nulos.

Exemplo 1.2 - O conjunto dos divisores de 12 é $D(12) = \{1, 2, 3, 4, 6, 12\}$.

Observe que para todo $d \in \mathbb{Z}$ temos $1|d$ e $d|0$, inclusive quando $d = 0$, pois 0 é múltiplo de qualquer número. Note também que se $d|a$, então $-d|a$, $d|-a$ e $-d|-a$, para todo $a \in \mathbb{Z}$.

Observe também que se a e d são números naturais, com $a \neq 0$, e se $d|a$, então $d \leq a$. De fato, sendo a um múltiplo natural não nulo do número natural d sabemos que $a \geq d$.

Das duas propriedades acima segue que os divisores de um número inteiro formam um conjunto finito de números inteiros.

1.4 Máximo divisor comum entre dois números

Definição 1.3 - Dados dois números inteiros a e b não simultaneamente nulos é chamado de máximo divisor comum de a e b ao maior divisor comum de ambos e representado por $mdc(a, b)$ ou simplesmente por (a, b).

A definição dada por Euclides nos *Elementos* constitui-se um dos pilares de sua aritmética:

Dizemos que um número inteiro $d \geq 0$ é um máximo divisor comum (mdc) de a e b, se possui as seguintes propriedades:

(i) d é um divisor comum de a e b, e

(ii) d é divisível por todo divisor comum de a e b.

Podemos reescrever as propriedades acima como:

(i') $d|a$ e $d|b$; e

(ii') se $c|a$ então $c|d$.

Demonstração: Vamos demonstrar (i') e (ii').

Para provar (i') vamos precisar do resultado a seguir:

Lema 1.1 - Sejam $a, b, n \in \mathbb{Z}$, se existe $(a, b - na)$, então (a, b) existe e

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

Demonstração:

Seja $d = (a, b - na)$. Como $d|a$ e $d|b - na$ segue que $d|(b = b - na + na)$. Logo d é um divisor comum de a e b.

Para provar (ii') vamos supor que existe $c \in \mathbb{Z}$ que divide a e divide b então $c|d$.

De fato:

se $c|a$ e $c|b$ então $c|a-bn$, ou seja, c é um divisor comum de b e $a-bn$, logo $c|d$.

Exemplo 1.3 - Dados $a \in \mathbb{Z}$ com $a \neq 1$ e $m \in \mathbb{N}$, temos que $(\frac{a^m-1}{a-1}, a-1) = (a-1, m)$.

Resolução:

De fato, a igualdade acima é trivialmente verificada se $m = 1$ e como:

$$\frac{a^m-1}{a-1} = \frac{(a-1).(a^{m-1}+a^{m-2}.1^1+\cdots+a^0.1^{m-1})}{a-1} = a^{m-1}+a^{m-2}+\cdots+a+1$$

Então:

$$(\frac{a^m-1}{a-1}, a-1) = a^{m-1}+a^{m-2}+\cdots+a+1$$

Temos que:

$$(\frac{a^m-1}{a-1}, a-1) = (a^{m-1}-1+a^{m-2}-1+\cdots+a-1+1-1+m, a-1)$$

Logo:

$$(\frac{a^m-1}{a-1}, a-1) = (m.(a-1)+m, a-1) = (m, a-1) = (a-1, m).$$

1.4.1 Algoritmo de Euclides

Euclides, no livro VII da sua obra *Elementos* apresentou um método construtivo do cálculo do *mdc*, esse método é conhecido como *Algoritmo de Euclides*, é tido como um primor do ponto de vista computacional e não teve grandes aperfeiçoamentos em mais de dois mil anos.

Ele consiste na aplicação do algoritmo da divisão euclidiana sucessivamente até se obter o resto igual a zero, obtendo assim o *mdc*, que será o último resto não nulo.

Sejam $a, b \in \mathbb{N}$, tomemos, sem perda de generalidade, que $b \leq a$. Se $b = 1$ ou $b = a$ ou ainda $b|a$, temos que $(a, b) = a$. Suponhamos então que $1 < b < a$ e que $b \nmid a$. Assim, pela divisão euclidiana podemos escrever:

$$a = bq_1 + r_1, \text{ com } 0 < r_1 < b$$

Daí temos duas possibilidades:

(a) $r_1|b$. Nesse caso, $r_1 = (b, r_1)$ e, pelo Lema 1.1, temos que:

$$r_1 = (b, r_1) = (b, a - q_1 b) = (b, a) = (a, b),$$

e o algoritmo termina.

(b) $r_1 \nmid b$. Nesse caso, fazemos a divisão de b por r_1, obtendo:

$$b = r_1 q_2 + r_2, \text{ com } 0 < r_2 < r_1.$$

Novamente, temos duas possibilidades:

(a') $r_2 | r_1$. Nesse caso, $r_2 = (r_1, r_2)$ e, novamente, pelo Lema 1.1, temos:

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

e aqui termina o algoritmo.

(b') $r_2 \nmid r_1$. Nesse caso, efetuamos a divisão de r_1 por r_2, obtendo:

$$r_1 = r_2 q_3 + r_3, \text{ com } 0 < r_3 < r_2.$$

Esse procedimento deve ser repetido até que pare, o que certamente vai acontecer, pois caso contrário teríamos uma sequência de números naturais $b > r_1 > r_2 \ldots$ que não possui um menor elemento, contrariando o Princípio da Boa Ordenação. Logo, para algum n, temos que $r_n | r_{n-1}$, o que implica que $(a, b) = r_n$.

Podemos sintetizar essas operações no conjunto de equações a seguir:

$$\begin{gathered}
a = bq_1 + r_1, \text{ com } 0 < r_1 < b \\
b = r_1 q_2 + r_2, \text{ com } 0 < r_2 < r_1 \\
r_1 = r_2 q_3 + r_3, \text{ com } 0 < r_3 < r_2 \\
\vdots \\
r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}, \text{ com } 0 < r_{n-1} < r_{n-2} \\
r_{n-2} = r_{n-1} q_n + 0
\end{gathered}$$

Assim o mdc (a, b) é o último resto não nulo da sequência de divisões descritas acima, ou seja, $(a, b) = r_{n-1}$.

Exemplo 1.4 - Calcular o máximo divisor comum dos números 24 e 278 utilizando o algoritmo de Euclides:

Resolução:

Utilizando o algoritmo da divisão euclidiana, podemos escrever as seguintes equações:

$$278 = 24 \cdot 11 + 14$$
$$24 = 14 \cdot 1 + 10$$
$$14 = 10 \cdot 1 + 4$$
$$10 = 4 \cdot 2 + 2$$
$$4 = 2 \cdot 2 + 0$$

Assim, como o último resto não nulo é 2, temos que $(278, 24) = 2$.

Em particular, para quando esse último resto não nulo for igual a 1, temos a seguinte definição:

Definição 1.4 - Dois números a, b são ditos primos entre si ou coprimos, se $(a, b) = 1$.

1.4.2 Algoritmo de Euclides estendido

O algoritmo de Euclides estendido é uma outra versão do algoritmo de Euclides que possibilita calcular ao mesmo tempo o mdc de dois números a e b e determinar inteiros m e n tais que $(a, b) = ma + nb$.

Tomando $a \geq b$ para encontrarmos o mdc de a e b através do algoritmo estendido montamos a matriz abaixo:

$$A = \begin{bmatrix} b & 1 & 0 \\ a & 0 & 1 \end{bmatrix}$$

Para o primeiro passo de aplicação do algoritmo vamos subtrair da segunda linha q_1 vezes a primeira linha, onde q_1 é o quociente da divisão de a por b, obtemos assim a matriz:

$$A_1 = \begin{bmatrix} b & 1 & 0 \\ a - bq_1 & -q_1 & 1 \end{bmatrix} = \begin{bmatrix} b & 1 & 0 \\ r_1 & -q_1 & 1 \end{bmatrix},$$

onde r_1 como o resto da divisão de a por b.

O próximo passo consiste, na matriz A_1, subtrair da primeira linha q_2 vezes a segunda linha, onde q_2 é o quociente de b por r_1, obtendo a matriz:

$$A_2 = \begin{bmatrix} b - q_2 r_1 & 1 + q_1 q_2 & -q_2 \\ r_1 & -q_1 & 1 \end{bmatrix} = \begin{bmatrix} r_2 & 1 + q_1 q_2 & -q_2 \\ r_1 & -q_1 & 1 \end{bmatrix},$$

onde r_2 é o resto da divisão b por r_1.

O algoritmo continua reproduzindo o Algoritmo de Euclides para determinação do *mdc* de a e b, só que agora sobre as duas linhas da matriz, obtendo ao final uma matriz B que terá 0 na em uma das linhas no elemento da primeira coluna e na outra linha teremos (d, n, m), onde $d = (a, b)$ e os inteiros m, n são tais que $(a, b) = ma + nb$. Vejamos um exemplo:

Exemplo 1.5 - Calcular o máximo divisor comum dos números 273 e 126 , utilizando o algoritmo de Euclides estendido:

Para utilizar o algoritmo de Euclides estendido, temos:

$$\begin{bmatrix} 126 & 1 & 0 \\ 273 & 0 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 126 & 1 & 0 \\ 273 - 2 \times 126 & 0 - 2 \times 1 & 1 - 2 \times 0 \end{bmatrix} = \begin{bmatrix} 126 & 1 & 0 \\ 21 & -2 & 1 \end{bmatrix} \longrightarrow$$

$$\begin{bmatrix} 126 - 6 \times 21 & 1 - 6 \times (-2) & 0 - 6 \times 1 \\ 21 & -2 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 13 & -6 \\ 21 & -2 & 1 \end{bmatrix} \longrightarrow$$

Portanto $(273, 126) = 21$ e $n = -2$ e $m = 1$ logo $21 = 273 \times 1 + 126 \times (-2)$

1.5 Mínimo múltipo comum

Chamamos de mínimo múltiplo comum de dois números a e b inteiros ao menor múltiplo de ambos os números, simultaneamente, e representamos por $[a, b]$. Em outras palavras, temos a seguinte definição:

Definição 1.5 - Seja $m \in \mathbb{Z}$, com $m > 0$, dizemos que m é um *mínimo múltiplo comum* (*mmc*) dos números inteiros a e b, se possuir as seguintes propriedades:

(i) m é um múltiplo comum de a e b, e

(ii) se c é um múltiplo comum de a e b, então $m|c$

Exemplo 1.6 - Sejam os inteiros 3 e 4, temos que 24 é um múltiplo comum a ambos, mas não é o *mmc* de 3 e 4, pois temos ainda 12 que também é múltiplo de ambos e $12|24$, assim o *mmc* de 3 e 4 é 12.

Proposição 1.2 - Dados dois números inteiros a e b, temos que $[a, b]$ existe e

$$[a, b](a, b) = |a.b|$$

Demonstração:

Tomemos $m = \dfrac{ab}{(a,b)} \in \mathbb{Z}$. Observemos que $\dfrac{a}{(a,b)}$ e $\dfrac{b}{(a,b)}$ são inteiros e primos entre si, então:

(i) $m = a.\dfrac{b}{(a,b)} = \dfrac{a}{(a,b)}.b$ e isso implica que m é múltiplo comum de a e b; e

(ii) Se c é um múltiplo de a e também de b então $c = n.a = n'.b$, agora temos que provar que $m|c$.

Temos: $\dfrac{n.a}{(a,b)} = \dfrac{n'.b}{(a,b)}$, segue que: $n.\dfrac{a}{(a,b)} = n'.\dfrac{b}{(a,b)}$ e,

como $\dfrac{a}{(a,b)}$ e $\dfrac{b}{(a,b)}$ são coprimos entre si então:

$\dfrac{b}{(a,b)}|n$, o que implica que:

$n = \dfrac{b}{(a,b)}.n''$, assim fazendo uma substituição, obtemos:

$c = na = \dfrac{b}{(a,b)}n''.a = m.n''$, logo $m|c$.

Esse resultado nos permite encontrar o *mmc* através do algoritmo estendido de Euclides, pois basta encontrar o *mdc* e aplicar essa proposição.

1.6 Números primos

Definição 1.6 - Um número natural diferente de 0 e de 1 e que é apenas múltiplo de 1 e de si próprio é chamado de número primo. Um número diferente de 0 e de 1 que não é primo é chamado de número composto.

Em outras palavras, chamamos de números primos a todo número inteiro p maior que 1 que só possui dois únicos divisores positivos: 1 e o próprio número p.

Os números primos são considerados números especiais, pois desempenham um papel importante dentro da teoria dos números e, entre outras coisas, os seus produtos representam todos os números naturais, como veremos ainda nesta seção.

1.6.1 Teorema fundamental da aritmética

Agora vamos apresentar um dos mais importantes resultados da Teoria de Números:

Teorema 1.4 - **Teorema fundamental da aritmética**: Todo número natural maior do que 1 ou é primo ou se escreve de modo único (ao menos da ordem dos fatores) como um produto de números primos.

Demonstração:

Vamos usar o Princípio de Indução Completa ou Indução Forte, como também é conhecida para provar a existência do teorema.

Para $n = 2$, o resultado é obviamente verificado. Vamos supor que seja válido para todo número natural menor do que n e vamos provar que vale para n.

Se n é primo, não há nada a demonstrar, então suponhamos que n seja composto. Logo existem números naturais n_1 e n_2, tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Sabemos, pela hipótese indutiva que $n_1 = p_1.p_2.\cdots.p_r$ e $n_2 = q_1.q_2.\cdots.q_s$, onde $p_1.p_2.\cdots.p_r$ e $q_1.q_2.\cdots.q_s$ são números primos. Portanto $n = p_1.p_2.\cdots.p_r.q_1.q_2.\cdots.q_s$, logo n é formado por um produto de primos.

Agora temos que provar a unicidade da escrita. Vamos supor que tenhamos $n = p_1.p_2.\cdots.p_r = q_1.q_2.\cdots.q_s$, onde os p_i e p_j são números primos. Como $p_1|q_1$ então $p_1|q_1.q_2.\cdots.q_s$, logo $p_1 = q_j$ para algum j, digamos que $p_1 = q_1$, então $p_2.p_3.\cdots.p_r = q_2.q_3.\cdots.q_s = x$, assim $x < n+1$, logo $p(x)$ é verdadeiro por hipótese de indução, ou seja, x é fatorável de modo único como produto de números primos, ou seja, $x = p_2.p_3.\cdots.p_r = q_2.q_3.\cdots.q_s$ portanto $r = s$ para cada $p_i = q_j$ na fatoração.

1.6.2 Identificação de um número primo

Já sabemos qual é a definição de números primos, mas quantos números primos existem? É uma pergunta que Euclides respondeu no livro IX dos *Elementos*, onde deu uma prova que até hoje é utilizada e considerada uma das pérolas da matemática.

Teorema 1.5 - Existem infinitos números primos.

Demonstração:

Vamos supor que exista apenas um número finito de números primos $p_1, p_2, \cdots, p_r$. Tomemos um número natural $n = p_1 p_2 \cdots p_r + 1$ Temos que n possui um fator primo p, ou

seja, n é múltiplo de algum primo, que portanto deve ser um dos $p_1, p_2, \cdots, p_r$, digamos: p_j, então temos que $p_j|n$. Mas consequentemente, $p_j|(n - p_1.p_2.\cdots.p_r) = 1$, ou seja, p divide 1, o que é um absurdo, portanto, existem infinitos números primos.

Respondida a pergunta sobre a quantidade de primos, ainda há outro problema: como identificar um número primo? Eratóstenes, que viveu por volta de 230 anos antes de Cristo, criou o chamado Crivo de Eratóstenes, que permite determinar todos os números primos até a ordem que se desejar, mas esse método não tem muita eficiência para ordem muito elevada.

Para entendermos o Crivo de Eratóstenes vamos elaborar um quadro com números primos menores que 130.

Primeiro vamos escrever todos os números de 2 a 130 numa lista, conforme o Quadro 1.1:

Quadro 1.1: Crivo de Eratóstenes até 130

	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

Fonte: a autora, 2017

Agora vamos riscando todos os números compostos do seguinte modo:

- Risque todos os múltiplos de 2 maiores que 2, já que nenhum deles é primo.
- O segundo número não riscado é 3, que é primo. Então risque todos os múltiplos de 3, maiores que 3, pois esses não são primos.
- O terceiro número não riscado que aparece é o 5, que é primo. Então risque todos os números múltiplos de 5, maiores que 5, pois esses não são primos.
- O quarto número não riscado que agora aparece é 7, que é primo. Risque todos os números múltiplos de 7 maiores que 7, pois esses não são primos.

- O quinto número não riscado que agora aparece é 11, que é primo, repetimos o procedimento de riscar os múltiplos desse primo.

O próximo resultado nos garante que não será necessário continuar com esse procedimento até chegar 130.

Lema 1.2 - 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:

Vamos supor 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 $q^2 \leq n$, o que é um absurdo. Portanto segue a afirmação do resultado.

Assim, na nossa tabela devemos ir até alcançarmos o número primo 11, pois o próximo primo é 13 e seu quadrado supera 130. Todos os números não riscados do nosso quadro serão números primos.

Podemos utilizar o Lema 1.2 como um teste de primalidade, assim para verificar se um número é primo, basta verificar que ele não é divisível por nenhum primo p menor do que $\sqrt{n}$.

1.6.3 Pequeno Teorema de Fermat

O resultado conhecido como Pequeno Teorema de Fermat foi uma das descobertas mais importantes e simples de Fermat.

Antes de enunciarmos esse teorema, vejamos mais um resultado que auxiliará a sua prova.

Lema 1.3 - Seja p um número primo. Os números $\binom{p}{i}$, com $0 < i < p$ são todos divisíveis por p.

Demonstração:

Para $p = 1$, teremos o resultado é trivial, pois 1 é divisor de qualquer número. Supondo para $1 < i < p$, nesse caso, temos que: $i!|p(p-1)\cdots(p-i+1)$. Como $(i!, p) = 1$,

segue que $i!|(p-1)\cdots(p-i+1)$, daí como $\binom{p}{i} = p\frac{(p-1)\cdots(p-i+1)}{i!}$, logo o resultado é verdadeiro.

Agora já podemos provar esse importante teorema.

Teorema 1.6 - Pequeno Teorema de Fermat: Seja p um número primo qualquer, tem-se que p divide $a^p - a$, para todo $a \in \mathbb{Z}$.

Demonstração:

Para $p = 2$ o resultado é imediato já que $a^2 - a = a(a-1)$ é um número par, pois trata-se de um produto de dois números consecutivos. Vamos supor que p é ímpar, nesse caso basta provar para o caso $a \geq 0$, vamos fazer essa prova por indução em a.

Para $a = 0$ o resultado é evidente pois $p|0$. Vamos supor que o resultado vale para a, vamos prová-lo para $a+1$. Utilizando a fórmulda de Binômio de Newton, temos que: $(a+1)^p - (a+1) = a^p - a + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a$.

Assim, pela hipótese indutiva e pelo que vimos no Lema 1.3, temos que $a^p - a + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a$ é divisível por p, logo está demonstrado o teorema.

Em consequência ao Pequeno Teorema de Fermat, segue o próximo resultado.

Corolário 1.2 - 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:

Pelo Pequeno Teorema de Fermat temos que: $p|a(a^{p-1} - 1)$ e como $(a, p) = 1$ consequentemente segue que: $p|a^{p-1} - 1$.

O Pequeno Teorema de Fermat é também um teste de primalidade, pois dado $m \in \mathbb{N}$ com $m > 1$, se existir algum $a \in \mathbb{N}$, com $(a, m) = 1$, tal que $m \nmid a^{m-1} - 1$, então m não é primo.

1.7 Congruências

Boa parte do que veremos nessa seção foi introduzida por Gauss (1755-1855) em seu livro *Disquisitiones Arithmeticae*, publicado em 1801. Vamos agora introduzir a

grande ideia de Gauss de desenvolver uma aritmética dos restos da divisão por um certo número fixado. Essa ideia é o que chamamos de *Aritmética dos Restos* ou *Aritmética Modular*.

Definição 1.7 - Dado m um número natural, diremos que dois números inteiros a e b são congruentes módulo m, se os restos de suas divisões euclidianas por m são iguais. Representamos por $a \equiv b \ mod \ m$. Quando a relação $a \equiv b \ mod \ m$ for falsa, diremos que a e b não são congruentes módulo m, ou ainda, que a e b são incongruentes módulo m.

Exemplo 1.7 - Temos que $35 \equiv 19 \ mod \ 2$, pois ambos deixam resto 1 na divisão por 2.

A relação de congruência possui as seguintes propriedades:

Seja $m \in \mathbb{N}$. Para todos $a, b, c \in \mathbb{Z}$:

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

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

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

O resultado a seguir nos permite saber se dois números são congruentes módulo m sem precisar efetuar a divisão euclidiana e comparar os restos.

Proposição 1.3 - Dados $a, b, m \in \mathbb{Z}$, com $m > 1$, tem-se que $a \equiv b \ mod \ m$ se, e somente se, $m|b - a$.

Demosntração:

Pela divisão euclidiana, podemos escrever $a = mq + r$ com $0 \leq r < m$ e $b = mq' + r'$, com $0 \leq r' < m$, temos que: $b - a = m(q' - q) + (r' - r)$, portanto $a \equiv b \ mod \ m$ se, e somente se, $r = r'$, o que equivale a dizer que $m|b - a$, já que $|r - r'| < m$.

O que torna muito útil a relação de equivalência é o fato de ela ser compatível com as operações de adição e multiplicação nos inteiros, conforme a próxima proposição.

Proposição 1.4 - Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$, tem-se:

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

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

Demonstração:

Vamos supor que $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, logo $m|b - a$ e $m|d - c$ e assim::

(i) temos que $m|(b-a)+(d-c)$ e, portanto, $m|(b+d)-(a+c)$.

(ii) temos que $bd-ac = d(b-a)+a(d-c)$, logo $m|bd-ac$.

Também são válidos o resultado ao qual denominamos *lei do cancelamento*:

Corolário 1.3 - Sejam $a, b, c, m \in \mathbb{Z}$ com $m > 1$ temos que $a+c \equiv b+c \ mod \ m \Leftrightarrow a \equiv b \ mod \ m$.

Demonstração:

Segue da proposição 1.4 que se $a \equiv b \ mod \ m$ e $c \equiv c \ mod \ m$, então $a+c \equiv b+c \ mod \ m$. Reciprocamente, temos que se $a+c \equiv b+c \ mod \ m$, então $m|b+c-(a+c)$ o que implica que $m|b-a$, portanto $a \equiv b \ mod \ m$.

O resultado anterior nos confirmou que vale a lei do cancelamento em relação à adição. mas em relação à multiplicação nem sempre será válido, temos o seguinte resultado relacionado com o cancelamento multiplicativo.

Proposição 1.5 - Sejam $a, b, c, m \in \mathbb{Z}$ com $m > 1$ temos que $ac \equiv bc \ mod \ m \Leftrightarrow a \equiv b \ mod \ \dfrac{m}{(c,m)}$.

Demonstração:

Como $\dfrac{m}{(c,m)}$ e $\dfrac{c}{(c,m)}$ são coprimos, temos que:

$$ac \equiv bc \ mod \ m \Leftrightarrow m|(b-a)c \Leftrightarrow$$
$$\frac{m}{(c,m)}|(b-a)\frac{c}{(c,m)} \Leftrightarrow \frac{m}{(c,m)}|b-a \Leftrightarrow a \equiv b \ mod \ \frac{m}{(c,m)}.$$

Corolário 1.4 - Para todo $m \in \mathbb{N}$, com $m > 1$ e $a, b, c \in \mathbb{Z}$, se $(c, m) = 1$, então $ac \equiv bc \ mod \ m \Leftrightarrow a \equiv b \ mod \ m$.

Demonstração:

Pela proposição 1.5, temos que, como $(c, m) = 1$, então:

$$m|ac-bc \Leftrightarrow n|(a-b)c \Leftrightarrow n|a-b.$$

Com a notação de congruência, podemos reescrever o Pequeno Teorema de Fermat: Se p é um número primo e $a \in \mathbb{Z}$, então $a^p \equiv a \ mod \ p$. Além disso, se $p \nmid a$, então $a^{p-1} \equiv 1 \ mod \ p$.

1.7.1 Aplicações de congruências

Através das relações de congruência podemos saber qual o critério, ou seja, qual a característica que o número deve ter para ser divisível por um número inteiro dado. Essa é uma das aplicações de congruência muito utilizada tanto no ensino fundamental como no ensino médio, é o que chamamos de critério de divisibilidade de um número inteiro. Podemos encontrar o critério de divisibilidade para qualquer número inteiro utilizando a aritmética modular. Veremos alguns desses critérios nas próximas seções.

1.7.1.1 Critérios de divisibilidade por 3 e por 9

Como $10 \equiv 1 \ mod\ 3$ e $10 \equiv 1 \ mod\ 9$, segue que $n_i 10^i \equiv n_i \ mod\ 3$ e $n_i 10^i \equiv n_i \ mod\ 9$. Então, se n é representado na base 10 como $n_r n_{r-1} \cdots n_0$, temos:

$$n \equiv n_r + n_{r-1} + \cdots + n_0 \ mod\ 3$$

e

$$n \equiv n_r + n_{r-1} + \cdots + n_0 \ mod\ 9$$

o que prova que n é divisível por 3 ou por 9 se, e somente se, $n_r + n_{r-1} + \cdots + n_0$ é divisível, respectivamente por 3 ou por 9. Assim, basta somar os algarismos do número para saber se ele é divisível por 3 ou por 9.

1.7.1.2 Critérios de divisibilidade por 6

Vamos observar esses resultados obtidos com a utilização da definição 1.7:

$$10 \equiv 4 \ mod\ 6,$$
$$10^2 \equiv 4^2 \equiv 4 \ mod\ 6,$$
$$10^3 \equiv 10^2.10 \equiv 4.4 \equiv 4 \ mod\ 6,$$
$$10^4 \equiv 10^3.10 \equiv 4.4 \equiv 4 \ mod\ 6.$$

Assim temos que, $10^i \equiv 4 \ mod\ 6$, para todo número natural $i > 0$. Vejamos se realmente é verdadeira essa afirmação.

Se um número natural n é escrito no sistema decimal como $n_r n_{r-1} \cdots n_0$, temos que $n = (n_0 + 10n_1 + 10^2 n_2 + \cdots + 10^r n_r) \equiv (n_0 + 4n_1 + 4n_2 + \cdots 4n_r) \ mod\ 6$. Com isto, temos que o resto da divisão de n por 6 é igual ao resto da divisão de $n_0 + 4n_1 + 4n_2 + \cdots 4n_r$ por 6. Logo, provamos que: um número $n = n_r n_{r-1} \cdots n_0$ é divisível por 6 se, e somente se $n_0 + 4n_1 + 4n_2 + \cdots + 4n_r$ é divisível por 6.

1.7.1.3 Critérios de divisibilidade por 11

Temos que $10 \equiv -1 \ mod\ 11$, elevando cada membro a $2i$, obtemos que $10^{2i} \equiv 1$ mod 11 e, multiplicando membro a membro as duas congruências, pela proposição 1.4, obtemos:

$$10^{2i+1} \equiv -1 \ mod\ 11.$$

Dessa forma, sendo $n = n_r \cdots n_5 n_4 n_3 n_2 n_1 n_0$ um número escrito na base 10. Temos então:

$$n_0 \equiv n_0 \ mod\ 11$$
$$n_1 10 \equiv -n_1 \ mod\ 11$$
$$n_2 10^2 \equiv n_2 \ mod\ 11$$
$$\cdots$$

Somando membro a membro as congruências acima, pela proposição 1.4, temos que:

$$n \equiv n_0 - n_1 + n_2 - n_3 + \cdots + (-1)^r nr \ mod\ 11.$$

Portanto, n é divisível por 11 se, e somente se, é divisível por 11 o número $n_0 - n_1 + n_2 - n_3 + \cdots + (-1)^r nr$.

Veremos outras aplicações das congruências no próximo capítulo.

1.8 A função *fi de Euler*

Definição 1.8 - Dado um número inteiro m, chama-se sistema completo de resíduos módulo m ao conjunto formado por todos os restos possíveis r_i numa divisão de um número inteiro por m tal que $1 \leq r_i < m$. Esse sistema é dito reduzido módulo m quando os elementos que não são primos com m são retirados do sistema.

Denotaremos por $\varphi(m)$ o número de elementos de um sistema reduzido de resíduos módulo $m > 1$, isso corresponde à quantidade de números naturais entre 0 e $m - 1$ que são primos com m. Definindo $\varphi(1) = 1$, temos definida uma importante função:

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}$$

chamada *fi de Euler*.

Assim: $\varphi(m) := \{a \in \mathbb{N} : (a, m) = 1 \text{ e } 1 \leq a \leq m\}$.

Pela definição, temos que:

$$\varphi(m) \leq m - 1, \text{ para todo } m \geq 2.$$

Além disso, se p é primo, então $\varphi(p) = p - 1$. Assim, pelo Teorema Fundamental da Aritmética, basta sabermos calcular a função para cada uma das potências de primos.

Temos que dentre, $1, 2, \ldots, p^r$, com p primo e r natural, não são coprimos com p^r aquele que tem p como fator primo, a saber $p, 2p, 3p, \ldots, p^{r-1}p$, portanto $p^r - p^{r-1}$ são os coprimos, logo temos a fórmula:

$$\varphi(p^r) = p^r - p^{r-1} = p^r \left(1 - \frac{1}{p}\right).$$

Para $m > 1$ e sendo $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, teremos:

$$\varphi(m) = p_1^{\alpha_1} \cdots p_n^{\alpha_n} \ (1 - \frac{1}{p_1}) \cdots \ (1 - \frac{1}{p_n})$$

Para facilitar os cálculos podemos reescrever essa fórmula:

$$\varphi(p_1^{\alpha_1} \cdots p_n^{\alpha_n}) = p_1^{\alpha_1 - 1} \cdots p_n^{\alpha_n - 1}(p_1 - 1) \cdots (p_n - 1).$$

Exemplo 1.8 -- Calcular $\varphi(48)$:

Resolução:

Escrevendo o número 48 como produto de fatores primos temos $48 = 2^4.3$. Assim, calcular $\varphi(48)$ equivale a calcular $\varphi(2^4 \cdot 3)$, logo

$$\varphi(48) = 2^{4-1} \cdot 3^{1-1} \cdot (2 - 1) \cdot (3 - 1) = 8 \cdot 1 \cdot 1 \cdot 2 = 16.$$

Capítulo 2

Aplicações da aritmética

Nesse capítulo iremos estudar algumas das aplicações da aritmética onde serão aplicados muitos dos conceitos estudados no capítulo anterior.

2.1 Códigos de barras

As referências para essa seção são: Milies (2006) e Takahashi (2015).

Os códigos de barras são mundialmente utilizados e apesar disso, grande parte da população não sabe o que eles representam nem como ele são elaborados. Todos se deparam com códigos de barras diariamente, pois eles são utilizados em muitos produtos comercializados na era atual. Takahashi (2015, p.281) diz: "O código de barras é uma forma de representação gráfica que viabiliza a captura automática dos dados por meio de leitura óptica nas operações automatizadas."

Nesse capítulo vamos explicitar como são criados os códigos de barra, o que significam as barras verticais e os números representados abaixo delas, e qual a relação deles com a aritmética. Antes disso, vamos entender como foram criados.

2.1.1 História dos códigos de barras

Em 1952, Joseph Woodland e Bernard Silver patentearam o que eles chamaram de "uma classificação de artigos através de identificação de padrões", um código que consistiam em um padrão de circunferências concêntricas de espessura variável, esse foi o primeiro modelo de códigos de barras conhecido, conforme a figura abaixo:

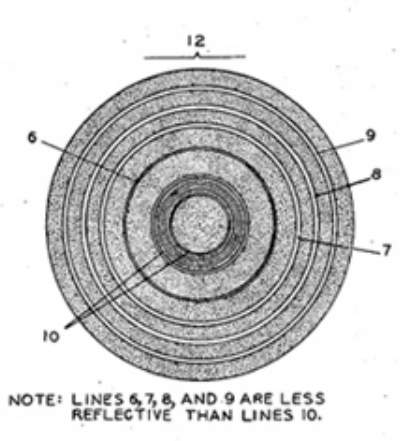

Figura 2.1: Primeiro código de barras
Fonte: USPTO Patent Drawing, 2012

Em 1973, o UPC (*Universal Product Code*) foi adotado nos Estados Unidos e Canadá. Esse código foi elaborado por George J. Laurer, através da empresa IBM (*International Business Machines*) que apresentou a proposta vencedora à solicitação de criação de um código numérico feito pela empresa de assessoria *Mc Kinsey & Co.*, junto com a *Uniform Grocery Product Code Council* que haviam definido um formato numérico para identificar produtos. Esse código possuía doze dígitos em formato de barras claras e escuras como os códigos que vemos atualmente, seguindo rigorosos padrões e ainda hoje é usado pelos Estados Unidos e Canadá.

O UPC-A, como é chamado atualmente, fez muito sucesso e diversos países da Europa também se interessaram por ter um código padrão que identificasse seus produtos e foi criado um conselho para estudar essa possibilidade e, posteriormente foi criada uma entidade sem fins lucrativos a qual deram o nome EAN (*European Article Numbering Association*). Então em 1976, Laurier ciou o EAN-13, *European Article Numbering system*, com treze dígitos que agora identificam também o país de origem do produto, mas alguns países usam esse mesmo código com um nome diferente. Esse é o código utilizado atualmente por diversos países, inclusive o Brasil.

Figura 2.2: Exemplos de códigos UPC-A e EAN-13
Fonte: GS1 Brasil, 2017

Para fazer a leitura de um código de barras, é necessário um aparelho chamado *scanner*. Um *scanner* é um aparelho de leitura ótica que permite converter imagens, fotos, ilustrações e textos em papel em um formato digital que pode ser manipulado em um computador. Há vários tipos de *scanner*, mas o princípio de funcionamento é basicamente o mesmo: o princípio da refletância da luz, que consiste em posicionar a imagem de forma que uma luz a ilumine. Um sensor capta a luz refletida pela figura, formando assim uma imagem digital. Esse sensor que capta a imagem é chamado de dispositivo de carga acoplado (CCD), é a peça principal do *scanner*. Esse tipo de sensor transforma a luz refletida em sinais elétricos que por sua vez, são convertidos em bits através de um circuito denominado conversor analógico-digital. Quanto mais forte for a luz, maior será o acúmulo de carga elétrica na placa. Todo o resto depende de um programa chamado reconhecimento óptico de caracteres (OCR) que captura a imagem no CCD, podendo assim converter o conteúdo da folha de papel em linguagem de software. Assim o *scanner* vai gerando cada caractere a partir da leitura do mapa de bits, ou bitmap.

O *scanner* que faz a leitura de códigos de barras faz a decodificação do código de barras através de um processo de emissão de uma feixe luminoso vermelho que percorre todas as barras presentes no documento. A luz é absorvida onde as barras forem escuras e refletida onde as barras forem claras, fazendo a captura das informações em poucos segundos e repassando os dados ao computador que exibirá a informação procurada.

O mercado atual tem se tornado cada vez mais exigente principalmente em relação a agilidade em que as informações são processadas, por isso, o código de barras tem sido um instrumento essencial facilitador principalmente nas transações comerciais. Criou-se uma expectativa de que os códigos de barras, além de fornecer números exclusivos de identificação, tragam mais informações como data de validade, números de série e

números de lote. Com essa nova tendência em 1994, a empresa japonesa *Denso-Wave* criou um código bidimensional QR-Code (*quick response code*) capaz de armazenar sete mil e setenta e nove caracteres numéricos, quatro mil e duzentos e noventa e seis caracteres alfa numéricos, dois mil e novecentos e cinquenta e três binários e até mil e oitocentos e dezessete caracteres japoneses. Dessa forma, são muitas as aplicações desse código e ele possui a facilidade de não precisar de um *scanner* para ser lido, isso pode ser feito através de uma câmera de celular, por exemplo.

Figura 2.3: Exemplo de um QR-Code
Fonte: Techtudo Informática, 2014

Na próxima seção vamos entender como se dá a identificação de produtos através de um código de barras do tipo UPC-A e EAN-13, que serão nossos objetos de estudos.

2.1.2 Conhecendo um código de barras

Nessa seção vamos entender o que é um código de barras, o que representam as barras verticais e os números que ficam embaixo delas. Vamos estudar com mais detalhes apenas os códigos UPC-A e EAN-13 que são os mais utilizados atualmente.

Um código de barras é um conjunto de informações representadas graficamente através de barras verticais brancas e pretas para serem lidas por um computador através de uma leitura óptica feito por um *scanner*. As barras verticais são, na verdade, listras brancas ou pretas de quatro espessuras: finas, médias, grossas e muito grossas. As listras pretas são representadas pelo algarismo *um* e as listras brancas pelo algarismo *zero*, transformando o formato de barras para o formato binário que é a linguagem computacional. A espessura da listra é representada utilizando a quantidade de um a quatro algarismos, de forma que temos os símbolos 0, 00, 000 ou 0000 para representar uma listra branca fina, branca média, branca grossa ou branca muito grossa, respectivamente. De forma análoga, temos os símbolos 1, 11, 111 ou 1111 para representar uma listra preta fina, preta média, preta grossa ou preta muito grossa, respectivamente. Há algumas listras que são

maiores que as demais, essas são chamadas de separadores e não representam números.

Cada conjunto de quatro listras, duas brancas e duas pretas formam um número do código e cada número é representado por uma sequência predefinidas de sete dígitos. Uma curiosidade é, que para qualquer número dado, o conjunto das quatro barras que o representa ocupa sempre a mesma área do código. O código é organizado para ser lido tanto iniciando pela direita como iniciando pela esquerda. Isso é possível porque quando o código é lido do lado oposto os dígitos são invertidos, ou seja, cada dígito *zero* é trocado por um dígito *um* e vice versa. Para reconhecer de qual lado está sendo lido, o computador analisa a paridade de dígitos iguais a *um*, sendo que, no código UPC-A, por exemplo, do lado esquerdo há um número ímpar e do lado direito há um número par de dígitos iguais a *um*.

Outra curiosidade é o porquê da utilização de sete dígitos para representar cada algarismo nos códigos de barras. Temos que cada algarismo precisa ser representado na linguagem de bits para que o computador processe a informação. Vamos responder a seguinte pergunta: é necessário um conjunto de quantos bits para representar os dez algarismos do nosso sistema decimal? Precisamos que cada algarismo seja representado por um mesmo número de barras pretas e brancas, de espessuras diferentes, pois o número de dígitos *um* e *zero* precisam ser de paridades diferentes. Além disso, precisamos de duas representações para cada algarismo para que eles sejam lidos de forma diferente do lado esquerdo e do direito, logo temos que ter um código com vinte representações diferentes que atendam aos requisitos citados. Vamos analisar as possibilidades:

- Se utilizarmos somente dois bits, podemos escrever quatro "palavras" (conjunto de bits), conforme o quadro abaixo, tendo no máximo duas "palavras" que utilizam o mesmo número de barras, nesse caso, duas barras, logo só poderíamos representar um único algarismo;

Quadro 2.1: "Palavras" com dois bits

00	01	10	11

Fonte: a autora, 2017

- Se utilizarmos três bits, podemos escrever oito "palavras", conforme o quadro abaixo, tendo no máximo quatro delas que utilizam um número igual de barras, sendo duas

barras, logo só poderíamos representar dois algarismos;

Quadro 2.2: "Palavras" com três bits

000	001	010	011	100	101	110	111

Fonte: a autora, 2017

- Se utilizarmos quatro bits, podemos escrever dezesseis "palavras", conforme o quadro abaixo, tendo no máximo seis "palavras"que utilizam três barras ou seis "palavras" com duas barras, logo só poderiam representar três algarismos;

Quadro 2.3: "Palavras" com quatro bits

0000	0001	0010	0011	0100	0101	0110	0111
1000	1001	1010	1011	1100	1101	1110	1111

Fonte: a autora, 2017

- Se utilizarmos cinco bits, podemos escrever trinta e duas "palavras", conforme o quadro abaixo, tendo no máximo doze "palavras" que utilizam três barras e oito que utilizam quatro barras, logo só poderiam representar quatro algarismos com um número igual de barras pretas e brancas ou seis algarismos com quantidades diferentes de barras pretas e brancas;

Quadro 2.4: "Palavras" com cinco bits

00000	00001	00010	00011	00100	00101	00110	00111
01000	01001	01010	01011	01100	01101	01110	01111
10000	10001	10010	10011	10100	10101	10110	10111
11000	11001	11010	11011	11100	11101	11110	11111

Fonte: a autora, 2017

- Se utilizarmos seis bits, podemos escrever sessenta e quatro "palavras", conforme o quadro abaixo, tendo até vinte "palavras" que utilizam três barras ou até vinte "palavras" que utilizam quatro barras, que poderiam representar dez algarismos com um número igual de barras pretas e brancas ou dez algarismos com quantidades diferentes de barras pretas e brancas. Apesar de atender quase todos os requisitos necessários, cada representação tem a mesma paridade de dígitos *um* e *zero*, logo o

computador não teria como identificar se a leitura ocorre pelo lado direito ou pelo lado esquerdo.

Quadro 2.5: "Palavras" com seis bits

000000	000001	000010	000011	000100	000101	000110	000111
001000	001001	001010	001011	001100	001101	001110	001111
010000	010001	010010	010011	010100	010101	010110	010111
011000	011001	011010	011011	011100	011101	011110	011111
100000	100001	100010	100011	100100	100101	100110	100111
101000	101001	101010	101011	101100	101101	101110	101111
110000	110001	110010	110011	110100	110101	110110	110111
111000	111001	111010	111011	111100	111101	111110	111111

Fonte: a autora, 2017

- Se utilizarmos sete bits, podemos escrever cento e vinte e oito "palavras", conforme o quadro abaixo, tendo até quarenta "palavras" que utilizam quatro barras, ou seja, quantidade suficiente para representar os dez algarismos com um número igual de barras pretas e brancas, com dígitos que tem paridades diferentes, possibilitando ao computador identificar o lado direito ou esquerdo a ser lido.

Quadro 2.6: "Palavras" com sete bits

0000000	0000001	0000010	0000011	0000100	0000101	0000110	0000111
0001000	0001001	0001010	0001011	0001100	0001101	0001110	0001111
0010000	0010001	0010010	0010011	0010100	0010101	0010110	0010111
0011000	0011001	0011010	0011011	0011100	0011101	0011110	0011111
0100000	0100001	0100010	0100011	0100100	0100101	0100110	0100111
0101000	0101001	0101010	0101011	0101100	0101101	0101110	0101111
0110000	0110001	0110010	0110011	0110100	0110101	0110110	0110111
0111000	0111001	0111010	0111011	0111100	0111101	0111110	0111111
1000000	1000001	1000010	1000011	1000100	1000101	1000110	1000111
1001000	1001001	1001010	1001011	1001100	1001101	1001110	1001111
1010000	1010001	1010010	1010011	1010100	1010101	1010110	1010111
1011000	1011001	1011010	1011011	1011100	1011101	1011110	1011111
1100000	1100001	1100010	1100011	1100100	1100101	1100110	1100111
1101000	1101001	1101010	1101011	1101100	1101101	1101110	1101111
1110000	1110001	1110010	1110011	1110100	1110101	1110110	1110111
1111000	1111001	1111010	1111011	1111100	1111101	1111110	1111111

Fonte: a autora, 2017

Os quadros apresentados acima foram construídos a partir de um algoritmo que será apresentado na seção 3.1.

2.1.2.1 Código de barras UPC-A

O código UPC-A possui doze algarismos, sendo que o primeiro algarismo representa a categoria do produto, os cinco algarismos seguintes representam o fabricante, os próximos cinco algarismos identificam o produto e o último algarismo é chamado de dígito verificador ou de controle.

Vejamos como os números são predeterminados na tabela abaixo:

Tabela 2.1: Correspondência dos dígitos no código UPC-A

Dígito	Do lado esquerdo	Do 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

Fonte: Milies, 2006

Dessa forma quando queremos representar o número *cinco* com barras devemos usar uma listra branca fina, uma listra preta média, uma listra branca grossa e uma listra preta fina, nessa ordem, para ser lido pela esquerda. Agora, o mesmo número *cinco* se for lido pela direita deverá ser representado por uma listra preta fina, uma listra branca média, uma listra preta grossa e uma listra branca fina nessa ordem. Para decodificar qual lado está sendo lido, observa-se que cada sequência do lado esquerdo tem um número impar de dígitos iguais a *um* e cada sequência do lado direito tem um número impar de dígitos iguais a *zero*. Dessa forma a máquina analisa a paridade dos números e reconhece de que lado está sendo lido. Essa codificação serve para o código UPC-A.

2.1.2.2 Código de barras EAN-13

O código EAN-13 possui treze algarismos, começando pelo lado esquerdo temos: os dois ou três primeiros identificam o país onde o produto foi fabricado, os quatro ou cinco seguintes antes das barras centrais, indicam o fabricante; do lado direito temos: os primeiros cinco algarismos logo após as barras centrais indicam o produto específico desse fabricante e o último algarismo é o disco verificador ou de controle.

O código EAN-13 foi criado com um algarismo a mais para que seja identificado o país fabricante, mas os mesmos leitores de códigos de barras conseguem reconhecer tanto o código EAN-13 como o UPC-A, pois foi acrescentado o algarismo zero ao código UPC-A para que isso fosse possível. Segundo Milies (2006, p. 5):

> Como era necessário adicionar um dígito e também manter o mesmo padrão de tamanho do código de barras, para não ter que modificar todas as leitoras, a ideia utilizada foi fazer com que o novo dígito estivesse implícito na forma de escrita de todos os outros. Para isso, 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.

Do mesmo modo que o código UPC-A, o código EAN-13, cada algarismo é formado por sete dígitos e as barras maiores separam o código em lado esquerdo e direito. Do lado esquerdo do código EAN-13, cada algarismo terá duas representações, podendo ser representado por um número par ou por um número impar de dígitos iguais a um, como podemos observar na tabela seguinte:

Tabela 2.2: Codificação do código EAN-13:

Algarismo	Do lado esquerdo ímpar	Do lado esquerdo par	Do 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

Fonte: Milies, 2006

O primeiro algarismo do código EAN-13 não vai aparecer, ou seja, não terá barras

para representá-lo. Esse primeiro algarismo tem a função de determinar a paridade de dígitos *um* que serão utilizados para representação dos demais algarismos que estão do lado esquerdo do código. Essa variação da paridade obedece os critérios da tabela a seguir:

Tabela 2.3: Codificação do algarismo inicial de acordo com a paridade de dígitos 1 de cada algarismo que aparece do lado esquerdo do EAN-13

Algarismo 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	Ímpar	Par

Fonte: Milies, 2006

Assim, quando o algarismo inicial é zero, o código EAN-13 fica idêntico ao código UPC-A, de forma que um mesmo leitor consegue ler a ambos os códigos. Tomando como exemplo um código de barras de um produto produzido no Brasil: 7896644418188, temos que o primeiro algarismo é sete, e este deverá estar implícito através da paridade de dígitos *um* na codificação dos demais seis algarismos que compõem o lado esquerdo do código, que pela tabela 2.3 nos dá: ímpar, par, ímpar, par, ímpar, par. Através da tabela 2.2, obtemos a correspondência:

Tabela 2.4: Codificação do número 7896644418188 para o código EAN-13

Algarismo	Referência (lado)	Codificação
8	Esquerdo ímpar	0110111
9	Esquerdo par	0010111
6	Esquerdo ímpar	0101111
6	Esquerdo par	0000101
4	Esquerdo ímpar	0100011
4	Esquerdo par	0011101
4	Direito	1011100
1	Direito	1100110
8	Direito	1001000
1	Direito	1100110
8	Direito	1001000
8	Direito	1001000

Fonte: a autora, 2017

Assim, o código desse produto é o código da figura 2.4:

Figura 2.4: Código de barras de um produto fabricado no Brasil
Fonte: Trio Administrador, 2013

Podemos observar que, assim como no código UPC-A, cada representação de um algarismo (conjunto de sete dígitos), representam quatro barras, cuja espessura e cor depende da repetição de *zeros* e *uns*.

Na próxima seção vamos descobrir qual a utilidade do último dígito de um código de barras EAN-13.

2.1.3 Dígito verificador de erros do código EAN-13

Já sabemos que no código EAN-13 é formado por treze dígitos, onde os dois ou três primeiros representam o país de origem do produto (no caso do Brasil é 789), os dígitos seguintes até as barras centrais representam a empresa fabricante, os cinco dígitos logo após as barras centrais, indica o produto (são escolhidos pela empresa), e o último

dígito é o dígito verificador. Esse dígito verificador é utilizado para que através dele o computador reconheça se há algum erro na digitação do código de barras.

Assim, os doze primeiros dígitos são fixos e o código verificador é determinado através de alguns cálculos de aritmética. Vamos entender como se dá esse processo no passo a passo a seguir:

1. Primeiro vamos identificar os doze dígitos iniciais como $a_1a_2a_3a_4...a_{11}a_{12}$ e vamos identificar o código verificador por x.

2. Para facilitar, vamos chamar essa sequência de $\alpha = (a_1, a_2, a_3, a_4, ..., a_{11}, a_{12}, x)$. Os códigos de barra EAN-13 utilizam uma sequência de pesos identificada por $\beta = (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$.

3. Calcula-se agora o produto entre as duas sequências de forma escalar, ou seja, o produto do primeiro item de α pelo primeiro item de β mais o produto do segundo item α pelo segundo item de β e assim sucessivamente:
   $\alpha.\beta = (a_1, a_2, a_3, a_4, ..., a_{11}, a_{12}, x).(1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$ então
   $\alpha.\beta = 1.a_1+3.a_2+1.a_3+3.a_4+1.a_5+3.a_6+1.a_7+3.a_8+1.a_9+3.a_{10}+1.a_{11}+3.a_{12}+1.x$
   logo
   $\alpha.\beta = (a_1 + a_3 + a_5 + a_7 + a_9 + a_{11} + x) + 3.(a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12})$

4. A escolha de x é feita de tal modo que o produto escalar $\alpha.\beta$ seja um múltiplo de dez, ou seja $\alpha.\beta \equiv 0 \ mod \ 10$.

Vamos ver um exemplo:

Exemplo 2.1 - Vamos descobrir através do método apresentado para o código EAN-13, qual é o dígito verificador de um código de barras cujos primeiros doze dígitos são: 7898355741001.

Tomemos $\alpha = (7, 8, 9, 8, 3, 5, 7, 4, 1, 0, 0, 1, x)$ e $\beta = (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$, logo o produto:
$\alpha.\beta = (7 + 9 + 3 + 7 + 1 + 0 + x) + 3(8 + 8 + 5 + 4 + 0 + 1)$. Assim queremos:
$\alpha.\beta = (27 + x) + 78 = 105 + x \equiv 0 \ mod \ 10$, logo temos que $x = 5$, portanto o código de barras completo é 78983557410015.

Através do dígito verificador também é possível descobrir algum número que esteja faltando no código de barras, como no próximo exemplo.

Exemplo 2.2 - Um código de barras estava com um número danificado, conforme figura abaixo. Utilizando o código verificador, vamos descobrir o número que está faltando.

Figura 2.5: Código de barras do exemplo 2.2
Fonte: Digital Song, 2009

Vamos denominar de x o número que não está visível, e procedendo como no exemplo anterior, temos:

$\alpha = (7, 8, 9, 8, 3, 5, 7, 4, 1, x, 8, 9, 2)$ e $\beta = (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$, logo

$\alpha.\beta = (7+9+3+7+1+8+2)+3.(8+8+5+4+x+9) = 139+3x \equiv 0\ mod 10.$

Assim $139 + 3x$ é um múltiplo de 10, logo o único valor para x é 7, portanto o código de barras completo é 7898357417892.

2.1.4 Dígito verificador de erros do código UPC-A

A determinação do dígito verificador no código UPC-A é feita de forma análoga ao código EAN-13, mas como o UPC-A tem um dígito a menos, a sequência de pesos fixa também tem um dígito a menos, assim $\beta = (3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$.

Exemplo 2.3 - Vamos determinar o dígito verificador no código UPC-A: 03600029145.

Chamando de y ao dígito procurado, temos:

$\alpha = (0, 3, 6, 0, 0, 0, 2, 9, 1, 4, 5, y)$ e $\beta = (3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$.

Dessa forma,

$\alpha.\beta = (3 + 0 + 0 + 9 + 4 + y) + 3.(0 + 6 + 0 + 2 + 1 + 5) \equiv 0\ mod 10.$

Assim: $16 + y + 42 = 58 + y \equiv 0\ mod 10$,

logo $y = 2$.

2.2 Outros códigos de identificação

O mundo atual é comandado por números, pois precisamos deles desde ao acordar até o adormecer. O mesmo podemos dizer sobre os códigos de identificação, pois nos deparamos com códigos no comércio, nas bibliotecas, nos hospitais, enfim em todos os lugares. A aritmética está por trás de todos esses códigos. Veremos nas próximas seções a aplicação da aritmética em mais alguns deles.

2.2.1 Cadastro de Pessoa Física: CPF

O Cadastro de Pessoa Física - CPF é um código identificador que todo cidadão brasileiro deve ter, registrado pela Receita Federal do Brasil. O CPF é composto por onze dígitos, sendo que os dois últimos são os dígitos de controle. Os oito primeiros dígitos são escolhidos aleatoriamente, mas o nono dígito é o dígito que representa o estado em que foi emitido o CPF, conforme tabela abaixo:

Tabela 2.5: Código dos estados brasileiros: nono dígito do CPF

Código	Estado
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, 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

Fonte: ACE Taboão da Serra, 2010

Para encontrar o primeiro dígito de verificação que corresponde ao décimo dígito do CPF, temos que resolver uma congruência módulo 11.

Tomemos os nove primeiros dígitos como a sequência: $a_1a_2a_3a_4a_5a_6a_7a_8a_9$ e vamos multiplicá-los pelo seu respectivo número de ordem e somar esses produtos. A essa soma chamaremos S_1, Dessa forma teremos que $S_1 \equiv x \ mod 11$, onde x é o décimo dígito do CPF.

Vejamos um exemplo:

Exemplo 2.4 - Seja o CPF 822.237.691-87. Vamos verificar se o primeiro dígito verificador está correto:

Tomemos $(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9) = (8, 2, 2, 2, 3, 7, 6, 9, 1)$, agora vamos calcular a soma S_1:

$S_1 = 8.1 + 2.2 + 2.3 + 2.4 + 3.5 + 7.6 + 6.7 + 9.8 + 1.9 = 206 \equiv x \ mod 11$.

Portanto $x = 8$ que corresponde exatamente ao décimo dígito do CPF citado.

Para encontramos o último dígito verificador que corresponde ao décimo primeiro dígito do CPF, vamos utilizar os dez primeiro dígitos representando-os pela sequência procedendo de forma análoga ao procedimento para encontrar o décimo dígito. Multiplicando os dez dígitos pelo seu respectivo número de ordem (com a posição inicial igual a zero) e somando esses produtos encontramos a soma S_2 que será congruente a y módulo onze, onde y é o dígito procurado.

Exemplo 2.5 - Retomando o exemplo 2.4, vamos conferir o décimo primeiro dígito.

Tomemos $(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9) = (8, 2, 2, 2, 3, 7, 6, 9, 1, 8, 7)$, agora vamos calcular a soma S_2:

$S_2 = 8.0 + 2.1 + 2.2 + 2.3 + 3.4 + 7.5 + 6.6 + 9.7 + 1.8 + 8.9 = 238 \equiv y \ mod 11$

Portanto $y = 7$, que corresponde exatamente ao último dígito do CPF apresentado.

2.2.2 Código ISBN

O código ISBN - *International Standard Book Number* - é um código numérico composto de treze algarismos reconhecido internacionalmente para identificar livros e publicações não periódicas. Esses treze números são dispostos de forma a identificar o título, o autor, o país, a editora e até a edição. Ele foi criado em 1967 por editores ingleses e, a partir de 1972, passou a ser aceito internacionalmente. Inicialmente possuía dez dígitos, mas em janeiro de 2007 passou a compor treze dígitos com a adoção do prefixo 978 com o objetivo de aumentar a capacidade do sistema. Para diferenciar os códigos são chamados ISBN-10 e ISBN-13.

Cada código ISBN se aplica a uma única obra e edição, não se repetindo jamais em outra. O sistema numérico é convertido em um código de barras que facilita a circulação e comercialização internacional.

O sistema é controlado pela Agência Internacional do ISBN em Berlim, na Alemanha que coordena, orienta e delega poderes às agencias nacionais. A agência brasileira é representada pela Fundação Biblioteca Nacional desde 1978 e tem a função de atribuir a numeração de identificação dos livros editados no Brasil.

Os três primeiros dígitos indicam o tipo de publicação, de um a cinco dígitos seguintes indicam o país ou a língua em que está escrito, os demais dígitos até o penúltimo indicam o livro, e o último dígito é o verificador. Os grupos são separados por hifens ou espaços.

Para encontrarmos o último algarismo de um código ISBN-10, que é o dígito verificador, vamos representar os seus algarismos por: $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}$, onde a_{10} pode ser encontrado através da congruência linear:

$$S_1 = 10a_1 + 9a_2 + 8a_3 + 7a_4 + 6a_5 + 5a_6 + 4a_7 + 3a_8 + 2a_9 + 1a_{10} \equiv 0 \ mod 11$$

No código ISBN-13, sejam os seus algarismos $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}a_{12}a_{13}$, temos que a_{13} é o dígito verificador, que pode ser encontrado através de uma congruência linear módulo *onze*:

$$S_2 = 1a_1+3a_2+1a_3+3a_4+1a_5+3a_6+1a_7+3a_8+1a_9+3a_{10}+1a_{11}+3a_{12}+a_{13} \equiv 0 \ mod 11.$$

Assim, através da aritmética modular também é possível verificar se há erros na digitação de um código ISBN.

2.3 Criptografia

Com o avanço das tecnologias e da computação, a facilidade do uso de redes de comunicação para o envio e recebimento de informações entre computadores e a preocupação com a segurança, há uma crescente necessidade de proteção dessas informações na transmissão de dados e os métodos criptográficos são cada vez mais utilizados com essa finalidade.

Criptografia é o estudo dos códigos ocultos ou secretos. A palavra tem origem grega onde *kryptós* significa esconder e *grápho* é escrita, então criptografia é escrita oculta. O objetivo da criptografia é que a mensagem apesar de ser acessível a outros receptores somente possa ser lida pelo receptor correto.

2.3.1 Tipos de criptografia

A Criptografia consiste em basicamente três passos que são: pré-codificação, codificação e decodificação. A pré-codificação é o passo que consiste em converter as letras em números usando uma tabela de conversão preestabelecida. A codificação é o processo utilizado para codificar o texto. A decodificação é a etapa que se usa para decifrar o texto, voltando-o na sua forma original.

O ramo da matemática que estuda a criptografia é conhecido por criptologia. Nesse ramo, a criptografia se classifica quanto à chave utilizada em: simétricas e assimétricas. A criptografia simétrica é o tipo que usa uma mesma chave para codificar e para descodificar a mensagem e a criptografia assimétrica usa duas chaves, uma para cada operação. A criptografia simétrica é também chamada de "chave privada", já a assimétrica é chamada de "chave pública". Chave são os elementos que codificam e decodificam a mensagem, são arquivos gerados por programas para garantir a autenticidade e a confiabilidade de uma mensagem criptografada.

Os sistemas criptográficos também são classificados quanto ao tipo de operação utilizado para codificar uma mensagem como: algoritmo de substituição, onde cada elemento textual do plano é substituído ordenadamente por outros elementos; algoritmos de transposição, quando cada elemento textual é colocado em outra posição.

Outra classificação para a criptografia é quanto à forma em que o texto normal é processado, pode-se ter uma "cifra de bloco", quando se processa a entrada de um bloco de elementos de uma vez, produzindo um bloco de saída para cada bloco de entrada. Ou pode-se ter uma "cifra de cadeia", quando se processa os elementos de entrada continuamente, produzindo na saída um elemento de cada vez.

Um código é considerado seguro quando o custo de quebrar seu sigilo é superior ao valor da informação criptografada ou o tempo necessário para quebrar o sigilo excede o tempo de vida útil da informação.

2.3.2 Código de César

A criptografia é uma ciência muito antiga e o código de César é o registro mais antigo de utilização de códigos criptografados. Júlio César, na Roma Antiga, substituiu cada letra do alfabeto pela terceira letra que a segue, conforme o quadro abaixo:

Utilizando a Cifra de César, a palavra matemática, por exemplo, passa a ser

Quadro 2.7: Cifra de César original

A	B	C	D	E	F	G	H	I	J	K	L	M
D	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*

Fonte: a autora, 2017

pdwhpdwlfd. Esse tipo de criptografia foi utilizado por muito tempo, mas ele é muito fácil de ser quebrado, pois basta fazer uma análise de frequências e tentativas sucessivas.

2.3.2.1 A matemática da Cifra de César

Basicamente o método utilizado por César consiste em *caminhar* três letras para frente no alfabeto. Outras variações desse código utilizam outros números de casas a serem deslocadas no alfabeto. Esse número será a chave ou senha do sistema criptográfico, ele deve ser conhecido apenas por que envia a mensagem e por quem a recebe para que haja mais segurança.

Outra forma de se utilizar a Cifra de César é transformando letras em números, utilizando a aritmética modular. Podemos utilizar o quadro a seguir:

Quadro 2.8: Cifra de César modificada

A = 0	B = 1	C = 2	D = 3	E = 4	F = 5	G = 6	H = 7	I = 8
J = 9	K = 10	L = 11	M = 12	N = 13	O = 14	P = 15	Q = 16	R = 17
S = 18	T = 19	U = 20	V = 21	W = 22	X = 23	Y = 24	Z = 25	

Fonte: a autora, 2017

Observando o quadro, temos que a letra codificada é obtida da letra original, somando-se 3 ao número correspondente. Por exemplo, queremos cifrar a letra O que tem valor 14, somando 3, obtemos 17, que corresponde à letra R, logo a letra O será trocada por R.

Quando o resultado ultrapassar 25, a letra codificada estará associada ao resto da divisão por 26 do número associado à letra original somado com 3, ou seja, teremos uma congruência módulo 3. Por exemplo, a letra Y corresponde originalmente ao número 24, somando-se 3, obteremos 27 e,

$$27 \equiv 1 \ mod \ 26$$

Assim Y deve ser codificado por B.

Dessa forma podemos escrever a equação da criptografia para esse sistema:

$$C \equiv (k + n) \ mod \ 26.$$

Onde:

C = Texto cifrado

k = Deslocamento

n = Texto original

Exemplo 2.6 - Cifrar a letra S:

O k é o deslocamento que pode ser o valor 3; o n é o texto original no caso, a letra S. Utilizando a equação $C \equiv (k + n) \ mod \ 26$, temos:

$$C \equiv (3 + 18) \ mod \ 26$$

Assim:

$$C \equiv 21 \ mod \ 26$$

Logo o texto cifrado é a letra V, pois no quadro temos que $21 = V$.

Para decifrar a mensagem, podemos utilizar a mesma equação, desde que se esteja de posse da chave, que é o deslocamento.

Exemplo 2.7 - Seja M uma mensagem criptografada e, sabendo que a chave, ou seja, o deslocamento é 3, decifrar a mensagem.

Utilizando a equação da criptografia: $12 \equiv (3 + n) \ mod \ 26$, somando -3 em ambos os lados da congruência, temos: $9 \equiv n \ mod \ 26$, logo: $n \equiv 9 \ mod \ 26$. Assim a letra original é J.

2.3.3 Criptografia RSA

Criptografia RSA é um sistema de chave pública, ou seja assimétrica, leva esse nome por conta do nome de seus inventores em 1978, R. L. Rivest, A. Shamir e L. M. Adelman que trabalhavam nesta época no *Massachussest Institute of Technology* (MIT). Esse não é o único sistema de chave pública existente, mas é atualmente o mais utilizado

nas transações comerciais, por ser um método quase indecifrável quando não se é o receptor legítimo da mensagem.

Para utilizar um sistema RSA precisamos de dois números primos que serão chamados parâmetros: p e q, e usaremos o produto entre eles que chamaremos de $n = p.q$ para codificar a mensagem. Então $n = p.q$ será a chave de codificação da mensagem. Essa chave será uma chave pública então cada usuário do sistema saberá essa chave, mas para decodificar a mensagem cada usuário terá sua própria chave privada constituída pelos primos p e q. Assim para se decodificar a mensagem é necessário conhecer os primos p e q, fatorando n, por isso para tornar o código seguro é necessário escolher números primos essencialmente grandes, acima de cento e cinquenta algarismos, pois tornaria a tarefa inviável mesmo com a ajuda de um computador. Segundo Andrade e Silva (2012, p. 443):

> O tempo estimado para fatorar números, por exemplo, de 308 dígitos, com os algoritmos clássicos é de aproximadamente 100 mil anos. De fato, ele mostra-se computacionalmente inquebrável com números de tais dimensões, e a sua força é geralmente quantificada com o número de bits utilizados para descrever tais números. Para um número de 100 dígitos são necessários cerca de 350 bits, e as implementações atuais superam os 512 e mesmo os 1024 bits.

De acordo com Barbosa et al (2003, p.16):

> A segurança desse método se baseia na dificuldade da fatoração de números inteiros extensos. Em 1977, os criadores do RSA achavam que uma chave de 200 bits requereriam 10^{15} anos, porém chaves com 155 bits foram atacadas em menos de 8 meses. A saída é que na medida que os algoritmos se tornem melhores e os computadores se tornem mais velozes, maiores serão as chaves. Atualmente chaves com 300 dígitos (1000 bits) nos dão uma tranquilidade por algum tempo. Em níveis críticos, chaves com 2000 bits começam a ser usadas.

O sistema RSA é dividido em três etapas: pré-codificação, codificação e decodificação que veremos nas próximas subseções.

2.3.3.1 Pré-codificação

Vamos compreender esse sistema com a utilização de um exemplo simples. Ana e Roberto querem trocar uma mensagem utilizando a criptografia. Se Ana é a emissora da mensagem, ela deve pedir para o Roberto criar a chave secreta. Roberto deve escolher os parâmetros p e q (muito grandes) e calcular o produto $n = pq$, além disso, ele deve escolher $e \in \mathbb{R}$ tal que $mdc(e, \varphi(n)) = 1$, onde $\varphi(n) = (p-1).(q-1)$. Para segurança da mensagem, Roberto deve transmitir apenas os números n e e, assim (n, e) é a chamada

chave pública, guardando secretamente os números p e q, assim (p, q) é chamada chave secreta. De posse da chave pública, Ana pode escrever a mensagem, e começar o processo de pré-codificação que consiste em substituir as letras da mensagem de acordo com a seguinte tabela de conversão:

Tabela 2.6: Conversão para o código RSA

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Fonte: Coutinho, 2014

O espaço entre as palavras deve ser substituído pelo número 99. Assim, se Ana quer escrever a frase *Quero ver você*, por exemplo, deverá converter no número $\alpha = 26301427249931142799312412 14$. O fato de a tabela usar dois algarismos para cada letra é para evitar ambiguidade, que se teria, por exemplo, se utilizasse um único algarismo para cada letra, pois se tivesse o número 13 não saberíamos se eram as letras a e c, ou a letra m, por exemplo.

Na última etapa de pré-codificação, consiste em dividir o número α, obtido por Ana, em blocos b, onde b é um número inteiro menor que n. Supondo que os parâmetros escolhidos por Roberto foram 11 e 17 (tomaremos números pequenos aqui para facilitar a compreensão), assim $n = 11.17 = 187$. Nesse caso α pode ser dividido nos seguintes blocos:

$$26 - 30 - 142 - 72 - 49 - 93 - 114 - 27 - 9 - 93 - 124 - 12 - 14$$

A forma de se escolher os blocos não é única, mas deve-se ter o cuidado de não se iniciar um bloco com zero, observe que não há uma relação dos blocos com nenhuma sílaba ou palavra o que aumenta ainda mais o sigilo, pois torna a contagem de frequência impossível.

Agora vamos ver como se dá o processo de codificação e decodificação.

2.3.3.2 Codificação e decodificação

Para a etapa de codificação precisaremos da chave de codificação que foi fornecido por Roberto a Ana: (n, e) onde n que é o produto dos números p e q, e o número e que

é um inteiro, positivo e inversível módulo $\varphi(n)$, ou seja $mdc(e, \varphi(n)) = 1$. Codificaremos cada bloco separadamente, formando assim a mensagem codificada com a sequência dos blocos já codificados, mas sem reuni-los em um só número, pois isso tornaria impossível de decodificar a mensagem, mesmo por Roberto.

Vamos chamar o bloco codificado por $C(b)$, assim para codificar b, teremos a igualdade:

$C(b)$ é igual ao resto da divisão de b^e por n, ou seja, queremos $C(b) \equiv b^e \ mod \ n$.

Retomando o nosso exemplo, onde $p = 11$, $q = 17$ e $n = 187$, teremos $\varphi(n) = 160$, para o número e tomemos 3 que é o menor número primo que não divide 160. Assim teremos:

$$C(26) \equiv 26^3 \ mod \ 187$$

Temos que :

$$26^3 \equiv 185 \ mod \ 187$$

Assim: $C(26) \equiv 26^3 \equiv 185 \ mod \ 187$.

Dessa forma temos que $C(26) = 185$ é o primeiro bloco codificado, procedendo de modo análogo com os demais blocos, obtemos os seguintes blocos codificados:

$$185 - 72 - 131 - 183 - 26 - 70 - 130 - 48 - 168 - 70 - 159 - 45 - 126$$

Esse é o método utilizado para codificar uma mensagem pela criptografia RSA. Vejamos agora como procedemos para decodificar essa mensagem. Precisamos de dois números para decodificar essa mensagem, n e o inverso de e em $\varphi(n)$, que denotaremos de d, dessa forma, teremos a chave de decodificação (n, d). Chamando o bloco da mensagem codificada de β, então $D(\beta)$ será o resultado do processo de decodificação, onde $D(\beta)$ é igual ao resto da divisão de β^d por n, ou seja, $D(\beta) \equiv \beta^d \ mod \ n$.

Como já conhecemos e e $\varphi(n)$, para encontrarmos d, basta aplicar o algoritmo euclidiano estendido. No nosso exemplo temos $n = 187$, $e = 3$ e $\varphi(n) = 160$, assim, pelo algoritmo euclidiano estendido, temos:

$$160 = 53.3 + 1 \ ,$$

donde:

$$1 = 160 + (-53).3,$$

logo vemos que -53 é o inverso de 3 módulo 160, mas como precisamos que d seja positivo temos:

$$d = 160 - 53 = 107,$$

que é o menor inteiro positivo congruente a -53 módulo 160.

Para decodificarmos o primeiro bloco, temos que encontrar:

$$D(185) \equiv 185^{107} \ mod\ 187,$$

o que já é uma tarefa muito complicada para fazer se não contarmos com a ajuda de um programa de computação algébrica, mas de fato vamos constatar que:

$$185^{107} \equiv 26 \ mod\ 187,$$

que é exatamente o primeiro bloco da mensagem original. Utilizando o mesmo procedimento para os demais blocos, Roberto decodificará a mensagem enviada por Ana.

Resumindo, para utilizar o método de criptografia RSA devemos:

- Converter as letras em números, usando uma tabela de conversão, encontrando uma sequência de números;
- Escolher dois números primos p e q muito grandes (para dificultar ou até impossibilitar uma fatoração) e para codificar a mensagem usamos $n = p.q$;
- Separar o longo número produzido pela conversão das letras em blocos menores que n, os blocos serão chamados de b e podem ser aleatórios, mas tendo o cuidado de não começar com *zero*, pois dificultaria a etapa de decodificação;
- Utilizar n e e para codificar a mensagem, onde e é inversível módulo $\varphi(n)$, assim (n, e) é a chave de codificação do sistema RSA;
- Calcular $C(b)$, que é o resto da divisão de b^n por n, para todos os blocos, obtendo assim uma nova sequência de blocos, que será a mensagem codificada;
- Calcular d, que é o inverso de e em $\varphi(n)$ e assim o par (n, d) será a chave de decodificação. Tomando cada bloco da mensagem codificada por β, temos que $D(\beta)$ igual ao resto da divisão de β^d por n, será o resultado do processo de decodificação;
- Utilizar a tabela de conversão com o bloco decodificado (igual ao original) para ler a mensagem.

2.3.3.3 O sistema de criptografia RSA sempre funciona?

Para termos a garantia de funcionamento de qualquer sistema criptográfico precisamos ter a certeza de que ao decodificarmos a mensagem ela corresponderá à mensagem original. Vamos ver porque isso sempre vai acontecer no RSA.

Vamos retomar os passos. Nesse sistema para codificar a mensagem temos que: a chave de codificação é o par (n, e), onde $n = p.q$, com p e q primos e e é tal que $(e, \varphi(n)) = 1$; $C(b)$ será a mensagem codificada, obtida através da congruência: $b^e \equiv C(b)$ $mod\ n$. Para decodificar a mensagem temos a chave de decodificação que é o par (n, d), tal que $d.e \equiv 1\ mod\ \varphi(n)$, assim para obtermos b que é a mensagem original, temos que calcular $D(\beta)$, onde $\beta = C(b)$ é a mensagem codificada, através da congruência $D(\beta) \equiv \beta^d\ mod\ n$, assim precisamos que $D(\beta) = D(C(b)) = b$ para que o sistema dê certo.

Para Coutinho (2014, p. 184):

> ... precisamos verificar que se b é um inteiro e $1 \leq b \leq n-1$ então $D(C(b)) = b$. Na verdade, vamos provar apenas que $D(C(b)) \equiv b$ $(mod\ n)$. Isto é suficiente porque tanto $D(C(b))$ quanto b estão no intervalo que vai de 1 a $n-1$, logo só podem ser congruentes módulo n se são iguais.

Por definição, temos que:

$$D(C(b)) \equiv (b^e)^d \equiv b^{ed}\ mod\ n. \tag{2.1}$$

Como $d.e \equiv 1\ mod\ \varphi(n)$ logo existe $k \in \mathbb{Z}$ tal que $ed = 1 + k.\varphi(n)$. Temos que C e D são inteiros maiores que 2 e $\varphi(n) > 0$ segue que $k > 0$. Substituindo em 2.1, temos:

$$b^{ed} \equiv b^{1+k.\varphi(n)} \equiv (b^{\varphi(n)})^k b\ mod\ n$$

Como, $n = p.q$ e $\varphi(n) = (p-1)(q-1)$, podemos reescrever a congruência:

$$b^{ed} \equiv (b^{(p-1)(q-1)})^k b\ mod\ (p.q).$$

Assim temos a congruência $mod\ p$ e $mod\ q$. O cálculo é análogo para os dois casos, logo basta fazer um deles.

$$b^{ed} \equiv (b^{(p-1)(q-1)})^k b\ mod\ p \tag{2.2}$$

Vamos analisar duas hipóteses:

(i). Se $(b, p) \neq 1$

(ii). Se $(b, p) = 1$

Em (i) temos que, como p é primo, logo p divide b e portanto $b = kp$ para um $k \in \mathbb{Z}$ daí segue que: $b \equiv 0 \ mod \ p$, logo $b^{ed} \equiv 0 \ mod \ p$ e, portanto $b^{ed} \equiv b \ mod \ p$.

Em (ii) temos que p não divide b, logo podemos usar o Pequeno Teorema de Fermat, assim $b^{p-1} \equiv 1 \ mod \ p$, substituindo em (2.2), obtemos:

$$b^{ed} \equiv (1^{(q-1)})^k b \ mod \ p$$

portanto:

$$b^{ed} \equiv b \ mod \ p.$$

De forma análoga conseguimos provar que $b^{ed} \equiv b \ mod \ q$. Em outras palavras, estamos dizendo que $b^{ed} - b$ é divisível por p e por q e, como $(p, q) = 1$, pois p e q são primos distintos, segue que pq divide $b^{ed} - b$ e como $n = pq$, podemos concluir que

$$b^{ed} \equiv b \ mod \ n.$$

Portanto o método RSA funciona sempre e, apesar de utilizar uma chave pública para criptografar uma mensagem, vamos mostrar que ele é um método muito seguro.

Como já dissemos a segurança do método parte da escolha de números primos muito grandes, acima de 100 dígitos. Sendo p e q esses primos temos $n = pq$, assim a chave pública corresponde à chave de decodificação (n, e) estará à disposição de qualquer usuário do sistema, mas a mensagem só poderá ser lida por quem possuir a chave de decodificação, que corresponde à chave privada (n, d), dessa forma o sistema só estará protegido se for muito difícil encontrar d, quando só se conhece n e e.

> Na prática, só sabemos calcular d aplicando o algoritmo euclidiano estendido a $\varphi(n)$ e e. Por outro lado, só sabemos calcular $\varphi(n)$ se soubermos fatorar n para obter p e q. Portanto, na prática, só podemos quebrar o código se conseguirmos fatorar n. Mas sabemos que, se n for grande, este é um problema muito difícil, já que não são conhecidos algoritmos rápidos de fatoração. (COUTINHO, 2014, p. 186)

Assim, a segurança do código depende da escolha dos primos utilizados que além de serem muito grandes, devem ter $|p - q|$ também grande para dificultar a fatoração por algum método já conhecido, como o *algoritmo de Fermat*, encontrado em [Coutinho 2014, capítulo 2, seção 4, p. 40-43]. Portanto com os métodos de fatoração conhecidos, com os computadores atuais e a escolha correta dos números primos, o sistema de criptografia RSA é um dos métodos mais seguros para se transmitir uma mensagem.

Capítulo 3

A aritmética como conteúdo extracurricular no ensino médio

Nesse capítulo vamos apresentar a proposta que traz a aritmética como conteúdo extracurricular no ensino médio que poderá ser aplicada aos alunos através de oficinas de aplicação dos conceitos de aritmética apresentados, destacando os códigos de identificação e a criptografia.

O ensino de aritmética é pouco explorado no ensino médio, mas é um conteúdo de suma importância e pode vir a facilitar o desenvolvimento dos discentes, principalmente quanto falamos de ampliar o raciocínio lógico dos mesmos. No capítulo 2, apresentamos algumas das aplicações da aritmética que podem vir a ser abordadas no ensino médio.

A ideia é preparar oficinas durante o ano letivo que estimulem a resolução de problemas de raciocínio lógico. Essas oficinas podem vir a ser realizadas durante o horário normal de aula, ou ainda, como atividades extraclasse em horários diferenciados visando proporcionar um melhor desempenho dos alunos do ensino médio. Cada tópico apresentado de aplicação da aritmética pode constar de uma ou mais oficinas. Nas seções a seguir, daremos exemplos de oficinas que podem ser aplicadas aos alunos desta etapa escolar.

3.1 Oficina de códigos de identificação

A oficina sobre os códigos de identificação consta de uma parte teórica sobre o assunto direcionando o conteúdo de acordo com as seções 2.1 e 2.2 desse trabalho. Após a apresentação do conteúdo deverão ser realizadas as seguintes atividades:

1. Identificar os números representados pelas barras nos códigos EAN- 13 apresentados a seguir. Observação: Como são códigos EAN-13, serão representados somente 12 dígitos, sendo que o primeiro deve ser encontrado através da tabela 2.3: representação dos dígitos pela paridade de dígitos 1.

Figura 3.1: Atividade 1, item (a)
Fonte: Revista Proteste, 2011

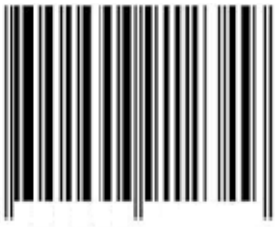

Figura 3.2: Atividade 1, item (b)
Fonte: GRAVAPAC Embalagens, 2016

Figura 3.3: Atividade 1, item (c)
Fonte: SCIELO Brasil, 1991

Figura 3.4: Atividade 1, item (d)
Fonte: Macoratti.net, 2016

2. Utilizar a aritmética modular para encontrar o dígito representado por x em cada um dos códigos de barras a seguir:

   (a) $789x456897123$

   (b) $789345789x678$

   (c) $7x89540912322$

   (d) $789544x332167$

   (e) $0234x54530029$

3. Cada aluno deverá fazer uma análise do seu CPF, verificando se está correto o dígito que representa o Estado em que o mesmo foi feito e conferindo os dígitos verificadores.

4. Os alunos trocarão entre si os números dos CPF, mas sem os dois últimos dígitos, assim cada um terá a tarefa de descobrir, através da aritmética modular, os dígitos de controle do CPF do outro.

5. Construir um quadro de "palavras" (conjuntos de bits) formadas por oito dígitos binários (*zeros* e *uns*):

Para realização da atividade 1, será necessário que o aluno compare cada conjunto de quatro barras, segundo a cor e a espessura, e represente o conjunto de sete dígitos *uns* e *zeros* para identificar quais algarismos cada conjunto de dígitos está representando, conforme a tabela 2.2, encontrando assim os 12 algarismos finais que compõe o código. Para encontrar o primeiro algarismo do código, é necessário analisar a paridade de dígitos *uns* existente na representação de cada algarismo e comparar com a tabela 2.3.

Para realização da atividade 2, os alunos deverão proceder de maneira análoga à resolução do exemplo 2.1.

Para realização da atividade 3, os alunos deverão consultar a tabela 2.5 para encontrar o Estado de confecção do documento. Tanto na atividade 3, como na atividade 4, os alunos deverão proceder como no exemplo 2.3 para resolver o que se pede.

A atividade 5 tem por objetivo incentivar o aluno a resolver problemas com algoritmos que tem regras rígidas e recorrentes, sendo necessário repetir o processo várias vezes até chegar ao resultado desejado. Para realizar essa atividade, o aluno deverá

escrever as “palavras” ordenadamente, numa sequência crescente que vai de 00000000 a 11111111. Para isso deverá ser apresentado aos alunos um algoritmo que ordena essa construção. O algoritmo funciona sempre comparando a “palavra” anterior (pode ser a primeira “palavra” para iniciar) com a “palavra” atual (que está sendo escrita). Para calcular a “palavra” atual, ela é escrita, primeiramente, igual à “palavra” anterior e então é alterada de acordo com o algoritmo. Por exemplo: iniciar com a “palavra” 00000000, e para montar a segunda “palavra”, começa afirmando que ela também é 00000000. A partir daí é que deverá modificá-la através do algoritmo, para que adquira a forma final que é 00000001. Da mesma forma, para construir a terceira “palavra”, sabendo que a segunda é 00000001, deve-se proceder da mesma forma: a terceira “palavra” assume os dígitos 00000001 e, através do algoritmo, sofre uma série de alterações até que adquira o formato final 00000010.

Esse algoritmo serve para construção de “palavras” de qualquer quantidade de bits. O algoritmo é indutivo, a primeira “palavra” já será estabelecida como 0000...0000. Então na primeira rodada, constrói-se a segunda palavra. Ela será a “palavra” atual. Após o processo do algoritmo, ela fica pronta. Então roda-se o algoritmo outra vez, mas para isso, é importante observar que a “palavra” construída anteriormente deixa de ser a “palavra” atual e passa ser a “palavra” anterior. O título de “palavra” atual passar a ser da terceira “palavra” e assim por diante.

Descrição dos passos do algoritmo para realização da atividade 5:

1. Escolha o número de dígitos de suas “palavras”.
2. Faça a primeira “palavra” ser 0000...0000.
3. Faça a “palavra” atual igual à “palavra” anterior.
4. Na “palavra” atual, da direita para a esquerda, procure pelo primeiro zero.
    - Encontrando-o, troque-o por 1.
    - À esquerda desse 1 (se tiver mais dígitos à esquerda), todos os dígitos são mantidos.
    - À direita desse 1 (se houver mais dígitos à direita), todos os dígitos são zerados.

A “palavra” atual está concluída. Parta para a próxima “palavra” reiniciando o algoritmo a partir do passo 3. Repita esse procedimento até chegar à última palavra que será 1111...1111.

Essas atividades tem o objetivo de melhor assimilação do conteúdo exposto e verificação de possíveis falhas na compreensão do mesmo.

3.2 Oficina de criptografia

A oficina sobre criptografia consta de uma parte teórica sobre o assunto direcionando o conteúdo de acordo com a seção 2.3 desse trabalho. Após a apresentação do conteúdo deverão ser realizadas as seguintes atividades:

1. Utilize a Cifra de César para escrever a mensagem: *Tirei a nota cem no exame nacional do ensino médio.*

2. Crie uma chave do sistema criptográfico apresentado na oficina para escrever nomes de três colegas da sua turma, em seguida apresente a toda sala e proponha que descubram quais são os nomes e qual foi a chave utilizada.

3. Em duplas devem combinar uma chave criptográfica, o primeiro da dupla, utilizando a chave combinada, escreve uma mensagem criptografada para o outro, que deverá conseguir descriptografá-la.

Para resolução da atividade 1, o aluno terá a escolha de utilização do quadro 2.7 para cifrar cada letra e montar a frase a partir das letras já cifradas, ou ainda utilizar o quadro 2.8 para fazer a codificação, fazendo uso da equação da criptografia apresentada na subseção 2.4.2.1.

Para resolução da atividade 2, o aluno deverá utilizar a equação da criptografia apresentada na subseção 2.4.2.1 e os demais alunos deverão fazer uso dessa mesma ferramenta para tentar descobrir quais os nomes e qual a chave utilizada.

Na atividade 3, os alunos devem escolher a chave criptográfica que vão utilizar e, em seguida, fazer uso da equação criptográfica já utilizada nas atividades anteriores, para criptografar e depois descriptografar a mensagem.

Nessas atividades será utilizada a Cifra de César para que o aluno adquira um pouco mais de familiaridade com o assunto podendo, a partir daí, avançar para a criptografia RSA que é um pouco mais complexa, mas pode ser aplicada em uma oficina específica sobre esse assunto.

3.3 Oficina da Olimpíada Brasileira de Matemática das Escolas Públicas - OBMEP

Essa oficina faz parte da proposta aqui apresentada e poderá ser aplicada aos alunos do ensino médio também com o objetivo de incentivar a participação deles nessa importante competição nacional.

Inicialmente, vamos conhecer um pouco da história da Olimpíada Brasileira de Matemática das Escolas Públicas - OBMEP e na sequência apresentamos algumas questões que podem ser resolvidas através da aritmética.

3.3.1 A Olimpíada Brasileira de Matemática das Escolas Públicas - OBMEP

Os dados aqui apresentados estão de acordo com as informações contidas no site da OBMEP.

A OBMEP foi criada em 2005 e é realizada anualmente pelo Instituto de Matemática Pura e Aplicada - IMPA, é promovida com recursos do Ministério da Ciência e Tecnologia e Inovação (MCTI) e do Ministério da Educação (MEC). É destinada a todos os alunos do ensino fundamental a partir do sexto ano das escolas públicas. Ela tem como metas estimular o estudo da Matemática e revelar talentos nessa área.

As provas da OBMEP são realizadas no segundo semestre do ano e são divididas em duas fases, sendo a primeira realizada pelos professores da unidade escolar na própria escola e os alunos concorrem somente entre si. Nessa fase a prova consta de vinte questões objetivas e é aplicada a todos os alunos inscritos da escola onde são escolhidos até cinco por cento dos alunos com maior pontuação para se classificarem para a segunda fase. A segunda fase consta de uma prova discursiva com quatro questões, sendo a mesma aplicada aos alunos classificados do município em um centro de aplicação escolhido pela

coordenação regional da OBMEP. Nessa segunda e última fase são classificados os melhores alunos que receberão premiações como, medalhas de ouro, prata e bronze, certificado de menção honrosa e bolsas de estudos em participação do Programa de Iniciação Científica JR - PIC. Além dos alunos, há premiações para professores, escolas e municípios, conforme o regulamento vigente da OBMEP.

Os alunos são separados por nível, sendo o nível 1 composto pelos alunos do $6^{\underline{o}}$ e $7^{\underline{o}}$ anos do ensino fundamental, o nível 2 é composto pelos alunos do $8^{\underline{o}}$ e $9^{\underline{o}}$ anos do ensino fundamental e o nível 3 é composto pelos alunos do $1^{\underline{o}}$, $2^{\underline{o}}$ e $3^{\underline{o}}$ anos do ensino médio. As premiações também são separadas por esses níveis.

As provas versam sobre os conteúdos de matemática divididos em três temas: análise combinatória, aritmética e geometria. Vamos resolver algumas questões dentro do tema de aritmética que é o foco principal do nosso trabalho. Abordaremos resoluções que abranjam a menor quantidade de fórmulas possíveis, através de análise e interpretação das questões com o objetivo de trabalhar o raciocínio lógico do aluno de forma a contribuir para a formação do pensamento matemático.

3.3.2 Algumas questões da OBMEP com o tema aritmética

Nessa seção vamos apresentar e resolver algumas questões com o nosso tema aritmética retiradas do banco de questões da OBMEP.

1. *Ano bissexto* - Um ano comum tem 365 dias e um ano bissexto, 366 dias. O ano bissexto, quando o mês de fevereiro tem 29 dias, ocorre a quatro anos.

   (a) Com frequência dizemos "Um ano comum tem 52 semanas". Será correta essa afirmação?

   (b) Se um ano comum inicia numa terça feira, então o ano seguinte iniciará em qual dia da semana?

   (c) Responda a pergunta anterior para um ano bissexto.

   Resolução:

   (a) Uma semana tem sete dias. Na divisão de 365 por 7 encontramos quociente 52 e resto 1. Logo, o ano comum tem 52 semanas e 1 dia. Portanto, a frase correta é "O ano comum tem cinquenta e duas semanas e um dia". Como o

ano bissexto tem 366 dias, ele possui 52 semanas e 2 dias. Portanto o correto é dizer "O ano bissexto tem sete semanas e dois dias."

(b) Se um ano comum inicia numa terça feira, então a $52^{\underline{a}}$ semana inicia numa terça e termina numa segunda, ou seja, a $52^{\underline{a}}$ semana é dada por: terça - quarta - quinta - sexta - sábado - domingo - segunda. Como esse ano tem 52 semanas e mais 1 dia, o último dia desse ano será uma terça. Logo, o ano seguinte iniciará numa quarta feira.

(c) No caso do ano bissexto, devemos considerar um dia a mais do que no item anterior. Logo, o seu último dia será uma quarta e, portanto, o ano seguinte iniciará numa quinta feira.

2. *Soma de potências* - Qual é o valor de $2^6 + 2^6 + 2^6 + 2^6 - 4^4$?

(a) 0

(b) 2

(c) 4

(d) 4^2

(e) 4^4

Resolução:

A solução correta é a alternativa (a).

Temos $2^6 + 2^6 + 2^6 + 2^6 - 4^4 = 4 \times 2^6 - 4^4$. Há várias maneiras de calcular isso.
Solução 1: $4 \times 2^6 - 4^4 = 4 \times (2^2)^3 - 4^4 = 4 \times 4^3 - 4^4 = 4^4 - 4^4 = 0$

Solução 2: $4 \times 2^6 - 4^4 = 4(2^6 - 4^3) = 4[2^6 - (2^2)^3] = 4[2^6 - 2^6] = 0$

Solução 3: $4 \times 2^6 - 4^4 = 2^2 \times 2^6 - (2^2)^4 = 2^8 - 2^8 = 0$

3. *Algarismo das unidades* - Qual é o algarismo das unidades do número $1 \times 3 \times 5 \times ... \times 97 \times 99$?

(a) 1

(b) 3

(c) 5

(d) 7

(e) 9

Resolução:

A alternativa correta é a letra (c).

O último algarismo de um múltiplo de 5 é 0 ou 5; os que terminam com 0 são pares e os que terminam com 5 são ímpares. Como $1 \times 3 \times 5 \times ... \times 97 \times 99$ é múltiplo de 5 e sendo um produto de números ímpares, também é um número ímpar; segue que o seu algarismo das unidades é 5.

4. *Potências de* 9 - Qual é o valor da soma $9^{20} + 9^{20} + 9^{20}$?

   (a) 9^{20}

   (b) 3^{66}

   (c) 9^{23}

   (d) 3^{41}

   (e) 1^{23}

   Resolução:

   A alternativa correta é a letra (d), pois:

   $9^{20} + 9^{20} + 9^{20} = 3 \times 9^{20} = 3 \times (3^2)^{20} = 3 \times 3^{40} = 3^{41}$

5. *Múltiplos de 9* - Encontre o menor múltiplo positivo de 9 que pode ser escrito apenas com os algarismo:

   (a) 0 e 1

   (b) 1 e 2

   Resolução:

   (a) Um número é divisível por 9 se a soma dos seus algarismos é um múltiplo de 9. Logo, o número deve ter 9 algarismos iguais a 1. Assim, o menor número é: 111 111 111.

   (b) Devemos usar o maior número possível de algarismos iguais a 2 que devem ficar nas casas mais à direita. Assim, o menor número é: 12 222.

6. *Divisores e fatoração* - Decomponha 96 em dois fatores inteiros positivos cuja soma dos quadrados seja 208.

   Resolução:

   Como o produto dos dois números é 96, eles são divisores de 96. Decompondo 96 em fatores primos, encontramos $96 = 2^5 \times 3$, logo seus divisores são: $1, 2, 3, 4, 6, 8, 12, 16, 24, 32, 36, 48, 96$. Os divisores $96, 48, 32, 24$ e 16 não servem pois seus quadrados já são maiores que 208. Sobram $1, 2, 3, 4, 6, 8, 12$, cujos quadrados são $1, 4, 9, 16, 36, 144$. Agora vemos que a única possibilidade é $64 + 144 = 208$. Como $8 \times 12 = 96$, os números são 8 e 12.

7. *Divisão com resto* - Quais são os números que deixam resto 5 ao dividir 2007?

   Resolução: Se um número ao dividir 2007 deixa resto 5, então esse número é um divisor de $2007 - 5 = 2002$. Logo, temos que calcular os divisores de 2002, que são: 1, 2, 7, 11, 13, 14, 22, 26, 77, 91, 143, 154, 182, 286, 1001, 2002. Logo esses são os números que deixam resto 5 ao dividirem 2007.

8. *Código secreto* - Antônio precisa descobrir um código de 3 algarismos diferentes A, B e C. Ele sabe que B é maior que A, que A é menor do que C e também que valem as igualdades seguintes:

   $BB + AA + CC = 242$

   $B \times A \times C = 360$

   Qual é o código que Antônio procura?

   Resolução:

   A única maneira de obter 360 como produto de três números de um algarismo cada um é $360 = 9 \times 8 \times 5$. Logo, a soma $AA + BB + CC$ é igual a $55 + 88 + 99$. Como A é menor do que B e do que C, temos A = 5. Logo, temos duas possibilidades para o código: 589 ou 598.

9. *O maior MDC* - Quais são os seis números de dois algarismos cujo máximo divisor comum é o maior possível?

   Resolução:

Para que o *mdc* seja o maior possível, o menor dos números deve ser igual ao próprio *mdc* e o maior dos números deve ser igual ao sêxtuplo do *mdc*. O maior múltiplo de 6 de 2 algarismos é 96. Logo, 96 é o maior dos números e o menos é $96 \div 6 = 16$. Portanto os números são: 16, 32, 48, 64, 80 e 96.

10. *Divisibilidade* - No número $6a78b$, a denota o algarismo da unidade do milhar e b denota o algarismo da unidade. Se $6a78b$ for divisível por 45, então o valor de $a+b$ é:

    (a) 5

    (b) 6

    (c) 7

    (d) 8

    (e) 9

    Resolução:

    Temos que o número é divisível por 5 e 9. Todo número divisível por 5 termina em 0 ou 5. Assim, $b = 0$ ou $b = 5$. Todo número divisível por 9 tem como a soma de seus algarismos um número múltiplo de 9. Logo, temos que $6+a+7+8+0 = 21+a$ ou $6+a+7+8+5 = 26+a$ são múltiplos de 9. Donde, $a = 6$ ou $a = 1$, respectivamente. Daí temos: $a+b = 6+0 = 6$ ou $a+b = 1+5 = 6$. Portanto a alternativa correta é a letra (b).

11. *Menor número* - Qual é o menor número de cinco algarismos divisível por 4 que se pode formar com os algarismos 1, 2, 3, 4 e 9?

    Resolução:

    O número tem que ser par, logo tem que terminar em 2 ou 4. Um número é divisível por 4 se o número formado pelos 2 últimos algarismos for divisível por 4. Assim, temos as possibilidades: 12, 24, 32, 92. Como 9 é o maior algarismo, devemos colocá-lo "o mais à direita possível". Logo 9 é o algarismo da casa das dezenas. Os outros números devem ser colocados em ordem decrescente à esquerda de 92, ou seja, o número deve iniciar com o menor algarismo que é o 1.

    Portanto, o número procurado é 13492.

12. *Divisão de números grandes* - Determine o valor de $123\ 456\ 123\ 456 \div 10\ 000\ 001$.

    Resolução:

    É claro que com números tão grandes, o objetivo da questão não é efetuar a divisão. Em vez disso, decompomos o número em partes convenientes:

    $123\ 456\ 123\ 456 = 123\ 456\ 000\ 000 + 123\ 456 = 123\ 456 \times 1\ 000\ 000 + 123\ 456 = 123\ 456\ (1\ 000\ 000 + 1)$, segue que: $123\ 456\ 123\ 456 = 123\ 456 \times 1\ 000\ 001$

    Logo, $123\ 456\ 123\ 456 \div 1\ 000\ 001 = 123\ 456$.

13. *Diferença e soma de quadrado* - Calcule:

    (a) $1678^2 - 1677^2$

    (b) $1001^2 + 1000^2$

    (c) 19999^2

    (d) $2001^2 + 2002^2 + 2003^2$

    Resolução:

    (a) Como $a^2 - b^2 = (a + b)(a - b)$, temos:

    $1678^2 - 1677^2 = (1678 + 1677)(1678 - 1677) = 3355$.

    (b) Como $(a + b)^2 = a^2 + 2ab + b^2$ temos:

    $1001^2 + 1000^2 = (1000 + 1)^2 + 1000^2 = 1000^2 + 2000 + 1 + 1000^2 = 2 \times 1000^2 + 2001 = 2\ 002\ 001$.

    (c) Como $(a - b)^2 = a^2 - 2ab + b^2$, temos:

    $19999^2 = (20000 - 1)^2 = (2 \times 10^4)^2 - 4 \times 10^4 + 1 = 4 \times 10^8 - 4 \times 10^4 + 1 = 399\ 960\ 001$.

    (d) Colocando em função de 2000, temos:

    $2001^2 + 2002^2 + 2003^2 = (2000 + 1)^2 + (2000 + 2)^2 + (2000 + 3)^2 = 3 \times 2000^2 + 12 \times 2000 + 14 = 12\ 024\ 014$.

14. *Sexta-feira treze* - Qual é o número máximo de sexta-feiras treze que podem ocorrer num ano que não é bissexto? Nesse caso, em que dia da semana cai o décimo dia do ano?

Resolução:

Como os dias da semana se repetem a cada 7 dias, a diferença entre os dias da semana é dada pelo resto ao dividir o número de dias transcorridos por 7. No Quadro 3.1, temos:

(a) Na primeira linha, o número de dias entre o dia 13 de um mês e o dia 13 do mês seguinte;

(b) Na segunda linha, o resto obtido quando dividimos esse número por 7;

(c) Na terceira linha, o resto obtido quando dividimos por 7 o número de dias entre o 13 de janeiro e o 13 do mês correspondente; assim, esse número é obtido somando os resultados obtidos na primeira linha, desde janeiro até o mês correspondente, calculando, depois, o resto da divisão por 7.

Quadro 3.1: Contagem de dias para resolução do exercício *sexta-feira treze*

J-F	F-M	M-A	A-M	M-J	J-J	J-A	A-S	S-O	O-N	N-D
31	28	31	30	31	30	31	31	30	31	30
3	0	3	2	3	2	3	3	2	3	2
3	3	6	1	4	6	2	5	0	3	5

Fonte: Banco de questões da OBMEP, 2016

Os valores iguais na última linha, significam que, nesses meses, o dia 13 caiu no mesmo dia da semana. Em particular, a última linha nos diz que 13 de fevereiro, 13 de março e 13 de novembro correspondem ao mesmo dia da semana. Assim, no máximo, temos três sextas-feiras treze. No caso de três sextas-feiras treze num mesmo ano, o 13 de janeiro ocorreu 3 dias antes de sexta-feira, isto é, numa terça-feira, e o dia 10 de janeiro aconteceu 3 dias antes disso, isto é, num sábado.

Observação: Note que uma sexta-feira treze ocorre apenas quando o primeiro dia do mês cair num domingo. Assim, uma outra maneira, talvez mais simples, de resolver o problema é determinar o número máximo de vezes em que o primeiro dia do mês caia num domingo num ano que não seja bissexto.

15. *Número ímpar* - Se n é um número inteiro qualquer, qual dos seguintes é um número ímpar?

(a) $n^2 - n + 2$

(b) $n^2 + n + 2$

(c) $n^2 + n + 5$

(d) $n^2 + 5$

(e) $n^3 + 5$

Resolução:

A opção correta é a letra (c).

Lembremos que a soma ou a diferença de números de mesma paridade é um número par:

par $\mp$ *par* = *par* e *ímpar* $\mp$ *ímpar* = *par*.

Observemos que n^2 e n^3 podem sem pares ou ímpares, portanto $n^2 + 5$ e $n^3 + 5$ podem ser ímpares ou pares, dependendo de n ser par ou ímpar. Restam as opções (a), (b) e (c).

Solução 1: Ambos $n^2 - n$ e $n^2 + n$ são soma e diferença de dois números que sempre têm a mesma paridade, portanto, esses números sempre serão pares, do mesmo modo que $n^2 - n + 2$ e $n^2 + n + 2$. Finalmente, a opção correta é (c), porque $n^2 + n + 5 = (n^2 + n) + 5$, que é soma de um par e um ímpar, sempre será um número ímpar, para todo valor inteiro de n.

Solução 2: Observemos que $n^2 - n = n(n - 1)$ e $n^2 + n = n(n + 1)$ são o produto de dois números consecutivos, portanto, são sempre pares, do mesmo modo que $n^2 - n + 2$ e $n^2 + n + 2$. Finalmente, a opção correta é a (c), $n^2 + n + 5 = (n^2 + n) + 5$ é a soma de um par com um ímpar, que é sempre ímpar, para todo valor inteiro de n.

16. *O número 119* - O número 119 tem as propriedades seguintes:

(a) A divisão por 2 deixa resto 1;

(b) A divisão por 3 deixa resto 2;

(c) A divisão por 4 deixa resto 3;

(d) A divisão por 5 deixa resto 4;

(e) A divisão por 6 deixa resto 5.

Quantos inteiros positivos menores que 2007 satisfazem essas propriedades?

Resolução:

Dados inteiros positivos d e r, dizemos que N dividido por d deixa resto r se existir um inteiro n tal $N = nd+r$. Se M dividido por d deixar o mesmo resto r, então existe um inteiro m tal que $M = md + r$. Nesse caso, se $M > N$, resulta que $m = n + p$ para algum inteiro n e, portanto, $M = md+r = (n+p)+r = nd+r+pq = N+pd$, de modo que $M - N = pd$ é um múltiplo de d. O mesmo ocorre se $M < N$. Como 119 tem todas as propriedade arroladas, decorre que se N for algum número com essas mesmas propriedades então, necessariamente $119 - N$ é um múltiplo de 2, 3, 4, 5 e 6. Como o menor múltiplo comum de 2, 3, 4, 5 e 6 é 60, N tem as mesmas propriedades de 119 se, e só se, $119 - N$ for um múltiplo de 60. Assim, os únicos inteiros N com as mesmas propriedade de 119 são da forma $N = 119 + 60 \times p$, para algum inteiro p. Para obter N positivo, precisamos tomar $p \geq -1$ e, para obter $N \leq 2007$, precisamos tomar $p \leq 31$, pois $119 + 60 \times 32 = 2039 > 2007$. Assim, os únicos números inteiros positivos e menores do que 2007 com as mesmas propriedade de divisão são $59, 119, 179, ..., 1979$ $(= 119 + 60 \times 31)$. Num total de 33 números.

17. *Números proporcionais* - Se $\frac{x}{y} = \frac{3}{z}$, então $9y^2$ é igual a:

(a) $\frac{x^2}{9}$

(b) x^3z

(c) $3x^2$

(d) x^2z^2

(e) $\frac{1}{9}x^2z^2$

Resolução:

A opção correta é (d).

Como $\frac{x}{y} = \frac{3}{z}$, então $xz = 3y$. Elevando ao quadrado ambos os membros dessa igualdade, obtemos $x^2z^2 = 9y^2$.

18. *Será que existe?* - Existe algum número inteiro N tal que valha $2008 \times N = 2222...2$?

    Resolução:

    Solução 1: Se existir esse número N, então $N = \frac{222...2}{2008} = \frac{2 \times 111...1}{2 \times 1004} = \frac{111...1}{1004}$. Logo, N não é inteiro, por ser o quociente do número ímpar 111...1 pelo número par 1004. Portanto, não existe tal N.

    Solução 2: Fatorando 2008, obtemos $2008 = 2^3 \times 251$, portanto, 2008 é divisível por 8. Se existisse um inteiro N tal que $2008 \times N = 222...2$, teríamos, então, que 8 dividiria 222...2. Por outro lado, sabemos que um número é divisível por 8 se, e somente se, o número formado pelos últimos três algarismos for divisível por 8. Mas $222 = 27 \times 8 + 6$ não é divisível por 8. Logo, não existe um número N tal que $2008 \times N = 222...2$.

19. *Soma de cubos* - Se $x + y = 1$ e $x^2 + y^2 = 2$, calcule $x^3 + y^3$.

    Resolução:

    Temos a identidade do binômio $(x+y)^2 = x^2 + 2xy + y^2$, e a do trinômio $(x+y)^3 = x^3 + 3x^2 + 3xy^2 + y^3$. Substituindo os valores de $x + y$ e $x^2 + y^2$ na identidade do binômio, obtemos $1 = 2 + 2xy$ e, portanto, $xy = \frac{-1}{2}$. Assim, pela identidade do trinômio, $x^3 + y^3 = (x + y)^3 - 3xy(x + y) = 1 - 3.(\frac{-1}{2}).1 = \frac{5}{2}$.

20. *Múltiplo de 36* - Determine o maior valor múltiplo de 36 que possui todos os algarismos pares e diferentes.

    Fatos que ajudam: A soma dos algarismos de um múltiplo de 9 é divisível por 9.

    Resolução:

    Para um número ser divisível por $36 = 4 \times 9$, deve ser divisível por 4 e por 9. Assim, a soma dos algarismos do número n procurado deve ser divisível por 9. Por outro lado, como todos os algarismos são pares, a soma dos algarismos também é par. Assim, a soma dos algarismos é no mínimo 18. Como $0 + 2 + 4 + 6 + 8 = 20$, o número n deve ser formado pelos algarismos 0, 4, 6 e 8. O maior número que podemos formar com esses algarismos, sem repetir, é 8640, o qual também é divisível por 4, assegurando que este é o número procurado.

Considerações Finais

Durante a realização da pesquisa bibliográfica, percebemos a importância que a aritmética tem para o desenvolvimento do raciocínio lógico do aluno do ensino médio, por isso ela não pode mais ser negligenciada nessa etapa escolar.

No desenvolvimento do segundo capítulo foi possível perceber o quanto a aritmética está presente no cotidiano não só dos jovens, mas como da população em geral. Conhecendo o funcionamento de um código de identificação ou até mesmo de um sistema criptográfico, nos permite vivenciar a matemática de forma integrada, contextualizada e não somente de uma maneira isolada como se dá na maioria dos conteúdos didáticos apresentados no ensino médio.

O trabalho desenvolvido durante a elaboração da proposta, no processo de pesquisa e montagem das oficinas, reforçou a compreensão do quanto a aritmética é útil como instrumento facilitador e motivador para o desenvolvimento cognitivo dos alunos do ensino médio. Trabalhando com as aplicações apresentadas, o professor conseguirá despertar no aluno dessa etapa escolar um interesse maior pela matemática, possibilitando um melhor desempenho dos mesmos nessa disciplina.

Referências Bibliográficas

ANDRADE, R. S.; SILVA, F. d. S. Algoritmo de criptografia RSA: análise entre a segurança e velocidade. **Revista Eventos Pedagógicos**, n. 3, v. 3, 2012. P. 438–457.

BARBOSA, L. A. d. M. et al. RSA criptografia assimétrica e assinatura digital. **UNICAMP- Universidade Estadual de Campinas**. 2003.

BRASIL, M. E. e. C. Introdução aos parâmetros curriculares nacionais. **Brasília: MEC - Secretaria de Educação Fundamental**. 1998.

COUTINHO, S. C. Criptografia. **Programa de Iniciação Científica da OBMEP**. Rio de Janeiro: IMPA/SBM, 2007.

COUTINHO, S. C. **Números inteiros e criptografia RSA**. 2ª ed. Rio de Janeiro: IMPA, 2014.

DOMINGUES, H. **Fundamentos da aritmética**. São Paulo: Atual, 1991.

GROENWALD, C. L. O.; SAUER, L. d. O.; FRANKE, R. F. Desenvolvendo o pensamento aritmético utilizando os conceitos da teoria dos números. **Acta Scientiae**, n. 1, v. 7, 2005. P. 93–102.

HEFEZ, A. **Elementos de aritmética**. Rio de Janeiro: SBM, 2006.

HEFEZ, A. **Aritmética - Coleção Profmat**. Rio de Janeiro: SBM, 2014.

LORENSATTI, E. J. C. Aritmética: um pouco de história. **IX ANPED Sul - Seminário de Pesquisa em Educação da Região Sul**, 2012.

MILIES, C. P. A matemática dos códigos de barras. **III Bienal da Sociedade Brasileira de Matemática - Universidade Federal de Goiás**, 2006.

OBMEP. **Banco de questões: busque por tema**. Disponivel em: <http://www.obmep.org.br/banco.htm>. Acesso em: 16 de novembro de 2016.

TAKAHASHI, C. R. d. S. Ensinando matemática através dos códigos de barras. **Ciência e Natura, Universidade Federal de Santa Maria**, n. 3, v. 37, 2015. P. 278–288.