Tópicos de criptografia para ensino médio

Marcelo Araujo Rodrigues

Marcelo Araujo Rodrigues

Tópicos de criptografia para ensino médio

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

Área de Concentração: Matemática

Orientador: Prof. Dr. Antônio Calixto de Souza Filho

USP – São Carlos

Julho de 2016

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

R696t

Rodrigues, Marcelo Araujo
Tópicos de criptografia para ensino médio / Marcelo Araujo Rodrigues; orientador Antônio Calixto Souza Filho. -- São Carlos, 2016.
82 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2016.

1. Criptografia. 2. Congruência. 3. Aritmética. 4. Divisibilidade. 5. Funções. I. Souza Filho, Antônio Calixto, orient. II. Título.

Marcelo Araujo Rodrigues

Encryption topics for high school

Master dissertation submitted to the Instituto de Ciências Matemáticas e de Computação - ICMC-USP, in partial fulfillment of the requirements for the degree of Mathematics Professional Master's Program. FINAL VERSION

Concentration Area: Mathematics

Advisor: Prof. Dr. Antônio Calixto de Souza Filho

USP – São Carlos

July 2016

À minha esposa Mirian . . .

. . . pelos diversos momentos de paciência, compreensão, amor e principalmente, incentivo.

À minha pequena Luiza . . .

. . . que da sua maneira me dá forças para continuar os meus estudos.

Agradecimentos

Primeiramente a Deus, por tudo que realiza em minha vida todos os dias da minha existência.

Às mulheres da minha vida, Mirian e Luiza, que sempre estiveram ao meu lado me encorajando e compreendendo minha ausência em muitos momentos de nossas vidas.

Aos meus pais, Benedita e José Luiz, que dedicaram suas vidas em minha formação pessoal e profissional, concedendo – me uma educação sólida e com diversas oportunidades para estudar e alcançar muitos dos meus objetivos de vida. Além deles, a minha irmã, Maria Elisângela pelo apoio para que eu pudesse concluir o curso.

Aos amigos da E.E. Professor Antônio Viana de Souza por me apoiarem desde o início do curso com conversas e palavras de encorajamento.

Ao professor Calixto pela paciência, força e ajuda nas várias tardes de orientação que tornaram possível o término deste trabalho.

Aos colegas da minha turma do PROFMAT que dividiram comigo todas as incertezas, alegrias, risadas e horas de estudos que tivemos durante nossa passagem pela EACH – USP e por me transformarem, com suas experiências, em um professor melhor.

Aos professores da EACH que nos deram aulas e transmitiram para meus colegas e eu um pouco do conhecimento que eles adquiriram durante seus anos de experiência.

Aos amigos que nesses dois anos compreenderam minha ausência.

Enfim, a todos que torceram pelo meu sucesso nesta etapa da minha vida.

"Não há nenhum ramo da Matemática, por mais abstrato que seja, que não possa um dia ser aplicado a fenômenos do mundo real."

Nicolai Lobachevsky

Resumo

Esta dissertação apresenta, aos alunos e professores do ensino Médio, uma noção elementar da criptografia, através de alguns tipos de cifras, a trinca americana e do método de criptografia RSA. Para que isso fosse possível houve a introdução de conceitos básicos entre eles, conjuntos, funções, divisibilidade, números primos, congruência, teorema de Fermat e teorema de Euler, que garantem o funcionamento de algumas dessas cifras, da trinca americana e do sistema RSA. Com relação à trinca americana, que é um sistema que permite comunicar uma troca de chave, iremos propor uma composição de cifras, para que haja uma troca de mensagens e seja um exemplo motivador que introduza o sistema de RSA. Além disso, esses conceitos básicos podem ser úteis ao serem levados à sala de aula como motivação para o aprendizado dos alunos, seja para calcular com mais agilidade e simplicidade determinados exercícios, seja para resolver uma situação – problema ou mesmo para descobrir uma nova maneira de visualizar conteúdos já vistos em sala de aula.

Palavras-Chave: Funções, Aritmética, Divisibilidade, Congruência, Criptografia.

Abstract

This dissertation presentes, to students and high school teachers, an elementary notion of cryptography through some types of cyphers, the asymmetric key algorithm and the RSA encryption method. To make this possible, we introduce basic concepts among them, set theory, functions, divisibility, primes, congruence, Fermat's theorem and Euler's theorem, which guarantee the functioning of some of these encryptions. Relating to the asymmetric key algorithm, which is a system that allows you to communicate a key exchange, we will propose a set of cyphers, so that it is possible a secure message exchange, which is also a motivating example to introduce the RSA system. In addition, these basic concepts can be useful when being taken to the classroom as the motivation for the learning of students, whether to calculate with more agility and simplicity certain exercises, whether to resolve a situation-problem or even to discover a new way to discuss subjects usually seen in the classroom.

Keywords: functions, arithmetic, divisibility, congruence, encryption.

Lista de ilustrações

Lista de tabelas

Sumário

Introdução

Acostumamos a ouvir e dizer que aprender matemática é necessário para o desenvolvimento do pensamento lógico correto, um pensamento abstrato. Vários dos seus conceitos, como os números complexos e irracionais, ou ainda geométricos como ponto e reta são abstratos e não parecem corresponder a uma experiência simples de ser entendida.

Também, atualmente, falamos muito sobre inserir um conceito matemático em um determinado contexto, pois a maioria das pessoas acham que a matemática é muito abstrata. Escutamos diversas vezes pedidos para que a Matemática seja ligada ao “dia a dia” das pessoas, tornando – a mais concreta.

Segundo Roque (2012) até mesmo o desenvolvimento do conceito de números, pelas civilizações antigas, apesar de ter sido impulsionado por necessidades concretas, implica um tipo de abstração. Ao contarmos, utilizamos a ideia do concreto, mas relacionar um número para expressar quantidades iguais de objetos diferentes é um procedimento abstrato.

Ainda, de acordo com Roque (2012) a matemática antiga não era puramente empírica nem envolvia somente problemas práticos. Ela foi evoluindo devido ao aprimoramento de suas técnicas, que permitiam ou não que determinados problemas do cotidiano fossem resolvidos.

Nos dias atuais, assim como nas civilizações antigas, o saber matemático continua em construção. Segundo os PCN’s “o conhecimento matemático é fruto de um processo de que fazem parte a imaginação, os contra – exemplos, as conjecturas, as críticas, os erros e acertos.” (BRASIL, 1997).

Assim, claramente nos vemos diante de um conflito: tornar a matemática mais “concreta” sem deixar de utilizar sua capacidade de abstração que seu aprendizado nos proporciona.

Como em outras civilizações, é possível que ao pedirmos para que a matemática possa ser vista de modo mais “concreto”, não desejamos ver só conhecimento aplicado às necessidades práticas, mas também que seus conceitos sejam vistos a partir de um contexto, algo que nos proporcione sentido.

E entre tantos contextos que hoje podemos observar em nossa sociedade está a necessidade de proteger uma informação, principalmente quando transmitida

pela internet, onde muitos computadores estão interligados e milhares de informações são transmitidas por ela em questões de segundos. E nesse momento que entra o objeto de estudo desse trabalho: a criptografia RSA.

Segundo Coutinho (2013), do grego, cryptos, que significa secreto, oculto, escondido. A criptografia estuda os métodos para deixar uma mensagem incompreensível para todos (codificação), exceto para o receptor que consegue torna – la legível (decodificação) e nela são utilizados diversos conceitos matemáticos, como por exemplo, conjuntos, funções bijetoras, números primos, fatoração de números inteiros, entre outros que são vistos no ensino fundamental e médio e, na maioria das vezes, de maneira descontextualizado sem nenhuma aplicação.

Devido a relação entre a criptografia e vários conteúdos de matemática do ensino médio, iremos propor nesse trabalho uma abordagem da Matemática envolvida na criptografia, de modo especial no *sistema RSA*, que está baseado na distribuição do que chamamos de *chaves públicas*, as quais são utilizadas para a codificação de uma mensagem e não para a decodificação. O trabalho será destinado, especialmente aos professores e alunos do Ensino Médio, mas nada impede que professores de outras áreas, outros ciclos e alunos de graduação ou pós – graduação possam usá – lo como suporte em uma pesquisa futura. Para os professores de matemática pode servir como uma ferramenta de auxílio em seus estudos e aulas, aplicando determinados conteúdos em sala de aula através de um tema atual e aos alunos um instrumento de aprofundamento em seus estudos, permitindo – lhes reconhecer que muitos conteúdos matemáticos, vistos durante as aulas de matemática, podem ser aplicados em tema atual e real. Também proporciona o contato com tecnologias, entre eles computadores e calculadoras já que resolver determinados cálculos sem o uso dessas ferramentas demandaria um enorme tempo.

Por envolver muitos conteúdos de Matemática que são vistos no Ensino Médio e outros conteúdos que são estudados mas de forma diferente da qual estamos habituados, primeiramente iremos nos deparar com uma revisão geral de determinados temas antes de tocarmos no assunto principal do trabalho.

Inicialmente, apresentaremos no capítulo 1 um panorama sobre conjuntos, suas relações e operações. Logo em seguida, no mesmo capítulo, veremos os conjuntos numéricos e a construção de alguns deles, para que possamos entender com quais conjuntos estaremos trabalhando no decorrer da dissertação.

No capítulo 2 veremos as relações e funções, com suas definições, conceitos e teoremas. Iremos definir uma relação de extrema importância que será utilizada em outra seção e que nos auxiliará na construção de um dos conjuntos vistos no primeiro capítulo. No capítulo seguinte daremos ênfase aos conceitos de divisibilidade no conjunto dos números inteiros e suas propriedades, o algoritmo de Euclides, sua extensão e os números primos, temas essenciais para a introdução da trinca americana e da criptografia RSA.

No capítulo 4 iniciaremos a Aritmética Modular, seus conceitos e definições, para que professores e alunos possam familiarizar – se com o tema e observem uma nova maneira de escrever o algoritmo de Euclides. Além disso, serão justificados o Pequeno Teorema de Fermat e o Teorema de Euler, resultados que estão intimamente ligados ao RSA. No último capítulo abordaremos a Criptografia incluindo algumas curiosidades sobre o tema e alguns tipos de cifras. Logo em seguida, apresentamos a ideia da trinca americana que consiste em uma forma de comunicar uma determinada chave secreta. Depois iremos alterar algumas ideias da trinca de maneira que possamos aproveitá – la melhor. Por fim a descrição da criptografia RSA, que reuni todos os capítulos anteriormente estudados, como funciona e por que é tão segura.

Precisamos ter em mente que os vários exemplos práticos que aparecem em cada capítulo possuem como objetivo tornar a compreensão de cada tópico mais fácil e rápida, sem deixar de manter a exatidão que cada tema exige.

1 Noções de Conjuntos

Usamos a noção de conjunto com muita frequência, por exemplo ao observar critérios de semelhança comum de dois ou mais objetos para agrupá – los, estamos formando conjuntos. Ao formar um time ou, organizar uma lista de comprar, por exemplo, estamos construindo conjuntos.

Sendo esta, uma das mais fundamentais e simples ideias matemáticas, as chamamos de noções primitivas e, segundo Lima (2012) para poder empregar os conceitos primitivos adequadamente é necessário dispor de um conjunto de regras que disciplinem sua utilização e estabeleçam suas propriedades. A estas noções primitivas damos o nome de axiomas.

A noção matemática de conjunto é a mesma que temos usualmente que seria agrupamento, coleção e, portanto, é formado por elementos. Dados um conjunto X e um elemento qualquer x, que pode ser até mesmo um outro conjunto, a principal ideia é observarmos se esse elemento x é ou não um elemento do conjunto X. Se o elemento faz parte do conjunto, dizemos que x é elemento do conjunto X e escrevemos $x \in X$ (diz – se que x pertence a X). Caso contrário, dizemos que x não é elemento do conjunto X e colocamos $x \notin X$ (x não pertence a X).

Propriedade: qualquer conjunto X tem – se a seguinte propriedade: para qualquer objeto Y ocorre que: ou $Y \in X$ ou $Y \notin X$. Esta propriedade nos mostra que existe um objeto X para o qual qualquer objeto Y é elemento de X ou não é elemento de X, ou seja, não podem ocorrer as duas coisas simultaneamente. Assim, um objeto com esta propriedade é o que conhecemos por conjunto.

Por exemplo, se X é o conjunto das vogais do nosso alfabeto, podemos dizer que a, e, i, o, u são elementos do conjunto. Este pode ser representado colocando – se os elementos entre chaves, ou seja, $X = \{a, e, i, o, u\}$. Então, observamos o que foi dito até nesse ponto, $a \in X$ e $b \notin X$.

Também podemos descrever um conjunto através de uma propriedade ou condição que caracterize os elementos. Por exemplo, seja o conjunto A , o conjunto de todos os números inteiros maiores que 1 e menores ou iguais a 3. Sua representação fica da seguinte maneira: $A = \{x \in \mathbb{Z} | \ 1 > x \geq 3\}$. Para entendermos com mais clareza a construção dos conjuntos, utilizaremos alguns dos axiomas, que por convenção já são numerados.

Axioma da Existência (A1): Existe um conjunto A, tal que, para todo objeto x, ocorre que x não é elemento de A. O conjunto A, com essas condições, é denominado *conjunto vazio* e o simbolizamos por $\emptyset$ ou $\{\}$.

Qualquer propriedade que se contradiz, define o conjunto vazio. Por exemplo, dado o conjunto $A = \{x \neq x\}$, este é vazio, pois é o conjunto dos elementos x tais que x é diferente dele mesmo. Ou ainda, o conjunto solução dos números reais x, cuja equação $x^2 < 0$ também é um conjunto vazio.

Axioma da Extensionalidade (A2): Dados dois conjuntos A e B, a igualdade $A = B$ ocorre quando as duas condições a seguir são satisfeitas: $1)$ Todos os elementos do conjunto A são elementos do conjunto B; $2)$ Todos os elementos do conjunto B são elementos do conjunto A. Através deste axioma os conjuntos $\{1,2,1,2,1,2,2,1\}$ e $\{1,2\}$ são iguais.

Outro detalhe importante, os dois primeiros axiomas garantem a seguinte afirmação: existe um único conjunto vazio.

Suponhamos que $\emptyset \neq \{\}$, pelo axioma acima, deve existir um elemento x, em um dos conjuntos, que não esteja no outro. Mas, pelo axioma $(A1)$, não ocorre que existe elemento em ambos os conjuntos. Logo, $\emptyset = \{\}$.

O próximo axioma mostra que conjuntos não vazios podem ser diferentes.

Axioma do Par (A3): Dados dois conjuntos A e B, existe o conjunto $\{A, B\}$. Este axioma pode ser visto como um construtor de novos conjuntos, a partir de conjuntos existentes.

Até o momento, existe apenas o conjunto $\emptyset$. Vamos considerar $A = B = \emptyset$. Assim, pelo axioma do Par existe o conjunto $\{\emptyset, \emptyset\}$, Pelo axioma $A2$, $\{\emptyset, \emptyset\}$=$\{\emptyset\}$, e temos assim o conjunto unitário.

Observemos que $\emptyset \neq \{\emptyset\}$, pois este último possui um elemento. Agora, considerando $A = \emptyset$ e $B = \{\emptyset\}$, pelo axioma $A3$, existe o conjunto $\{\emptyset, \{\emptyset\}\}$ e, assim, até o momento temos três conjuntos, o conjunto vazio, o unitário do vazio e o conjunto formado pelo conjunto vazio e o unitário da vazio.

Definição 1.1. Se A é um conjunto, o número de elementos do conjunto A é denominado *cardinalidade* de A e denotamos por $|A|$.Então, até o momento os conjuntos obtidos têm as seguintes cardinalidades:

- $|\emptyset| = 0$

- $|\{\emptyset\}| = 1$
- $|\{\emptyset, \{\emptyset\}\}| = 2$

A grande vantagem ao se utilizar a linguagem dos conjuntos é que existem operações, relações e propriedades, que veremos adiante, fáceis de serem manipuladas.

1.1 União de conjuntos

Estudamos os primeiros três axiomas e a partir do conjunto vazio construímos conjuntos, porém de cardinalidades 1 e 2.

Axioma da União (A4): Para qualquer conjunto A, existe o conjunto Y, tal que, os elementos de Y são exatamente os elementos dos elementos do conjunto A. Com este axioma, podemos construir conjuntos de várias cardinalidades.

Para um melhor entendimento deste axioma, suponhamos que A seja composto por $A = \{\{a, e, i, o, u\}, \{2,3,4,5\}, \{1,2,4,8\}\}$. Então, $Y = \{a, e, i, , o, u, 1,2,3,4,5,7,8\}$ e denotaremos $Y = \{a, e, i, o, u\} \cup \{2,3,4,5\} \cup \{1,2,4,8\}$.

Definição 1.2. Se A e B são conjuntos, $A \cup B$ é o conjunto formado pelos elementos de A mais os elementos de B, sendo denominado conjunto união de A e B.

O conjunto $A \cup B$ existe devido ao axioma $A4$. Ao fazermos a união entre A e B, pode ocorrer que, para todo $x \in A \cup B$, ou $x \in A$ ou $x \in B$ e, a esta condição, damos o nome de *união disjunta*.

Se o conjunto união $A \cup B$ é tal que a união não é disjunta, então deve ocorrer que A e B têm algum elemento em comum. Por exemplo, no conjunto A de vogais da palavra março e B de vogais da palavra junho, a vogal $\{o\} \in A \cup B$ e também está em cada um dos conjuntos. Neste caso, temos uma nova operação que definimos *interseção* de conjuntos.

Definição 1.3. Se A e B são conjuntos, $A \cap B$ denota o conjunto dos elementos que estão em A e em B,simultaneamente, e denominamos este conjunto de interseção de A e B.

Quando realizamos a interseção entre dois conjuntos A e B, pode ocorrer que $A \cap B = \emptyset$ ou $A \cap B \neq \emptyset$. Quando a interseção não é vazio, então deve ocorrer que A e B têm algum elemento em comum.

As duas operações anteriores podem ser vistas da seguinte forma:

- $x \in A \cup B$ significa "$x \in A$ ou $x \in B$ e;
- $x \in A \cap B$ significa "$x \in A$ e $x \in B$.

1.2 Inclusão de conjuntos

Retomemos o axioma $A2$. A condição todo o elemento do conjunto A é elemento do conjunto B será denotada por $A \subset B$ e dizemos que A é um subconjunto de B ou que A está contido em B. Assim, o axioma $A2$ equivale a seguinte sentença: $A = B$ se $A \subset B$ e $B \subset A$.

Exemplo: sejam R o conjunto de todos os retângulos e Q o conjunto de todos os quadriláteros. Todo o retângulo é quadrilátero, portanto $R \subset Q$ e a esta relação, damos o nome de *relação de inclusão*.

Quando determinado conjunto A não é subconjunto de B, escrevemos $A \not\subset B$, isto é, nem todo o elemento de A pertence B. Exemplo: dado o conjunto A como o conjunto dos números primos e o conjunto B como o conjunto dos números pares. Temos que $A \not\subset B$, pois $3 \in A$, mas $3 \notin B$.

A relação de inclusão possui algumas propriedades fundamentais. Uma delas é óbvia: dado o conjunto A, vale $A \subset A$. É claro que todo o elemento de A pertence a A. Outra propriedade diz que $\emptyset \subset A$, para qualquer que seja o conjunto A.

Suponhamos, por absurdo, que $\emptyset \not\subset A$. Teríamos que obter um elemento a, tal que $a \in \emptyset$. Como o conjunto vazio não possui elementos, chegamos a uma contradição da nossa hipótese inicial e, portanto $\emptyset \subset A$.

É possível que elementos de um determinado conjunto possam ser também conjuntos. Por exemplo, o conjunto de todos os subconjuntos de um conjunto A tem como elementos seus conjuntos.

Axioma das Partes (A6): Dado um conjunto A, existe o conjunto $\mathcal{P}(A)$, cujos elementos de $\mathcal{P}(A)$ são precisamente os subconjuntos de A. A este conjunto damos o nome de *conjuntos das partes* de A. Em símbolos, temos:

$$\mathcal{P}(A) = \{X | X \subset A\}$$

Se começarmos com o conjunto $A = \emptyset$, pelas observações anteriores temos $\mathcal{P}(A) = \{\emptyset\}$. Se $A = \{x\}$, os elementos de $\mathcal{P}(A)$ são $\emptyset$ e $\{x\}$, isto é, $\mathcal{P}(A) = \{\emptyset, \{x\}\}$. Caso o conjunto $A = \{x, y\}$, teremos de $\mathcal{P}(A) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$.

Note que o conjunto vazio e o próprio conjunto são elementos desse conjunto de subconjuntos e que repetindo este processo diversas vezes podemos demonstrar que $|\mathcal{P}(\mathrm{A})| = 2^{|\mathrm{A}|}$.

1.3 Conjuntos Numéricos

Em todo o Ensino Fundamental II os alunos se deparam com os conjuntos numéricos e suas características para que no Ensino Médio possam utilizar essas características em diversos conteúdos abordados em sala de aula. Neste tópico, apresentamos uma breve introdução da construção do conjunto dos números naturais relacionando com o que vimos até o momento.

Também veremos, mais resumido os conjuntos dos números inteiros, racionais e reais. Para uma melhor abordagem, associaremos cada conjunto com algumas equações e no final do capítulo com geometria, assuntos vistos no ensino fundamental II e assim, ter uma abordagem mais significativa da ideia de conjuntos numéricos.

1.3.1 Conjunto dos números naturais

Segundo Lima (2012) números são entes abstratos, desenvolvidos pelo homem como modelos que permitem contar e medir. Lentamente, à medida em que se civilizava, a humanidade apoderou – se desse modelo abstrato de contagem (um, dois, três, quatro, ...), sendo uma evolução demorada. E, ainda, de acordo com Lima:

> "As necessidades provocadas por um sistema social cada vez mais complexos e as longas reflexões, possíveis graças à disponibilidade de tempo trazida pelo progresso econômico, conduziram, através dos séculos, ao aperfeiçoamento do extraordinário instrumento de avaliação que é o conjunto dos números naturais." Lima (2012)

Assim, como veremos a seguir, após milhares de anos, podemos descrever precisamente esse conjunto numérico. Anteriormente, vimos que através de determinados axiomas, podemos construir conjuntos de cardinalidade 0, 1 e 2. Contudo, com o axioma $\mathrm{A4}$, obtemos conjuntos com cardinalidade maior que 2, através da seguinte sequência.

Primeiramente, dado um conjunto X, pelo axioma $\mathrm{A3}$ existe o conjunto unitário de X que simbolizamos por $\{\mathrm{X}\}$. Utilizando os conjuntos X e $\{\mathrm{X}\}$, pelo axioma $\mathrm{A3}$

existe o conjunto $A = \{X, \{X\}\}$. Com o axioma $A4$, teremos o conjunto Y, tal que $Y = X \cup \{X\}$. Então $|Y| = |X| + 1$ e, dessa maneira, podemos construir conjuntos de cardinalidade finita arbitrária.

Sendo $X = \{\emptyset\}$, então existe o conjunto $Y = \{X, \{X\}\} = \{\{\emptyset\}, \{\{\emptyset\}\}\}$. Pelo axioma $A4$, garantimos que existe $Y = \{\emptyset, \{\emptyset\}\}$ e calculamos facilmente $|X| = 1$ e $|Y| = 2$.

Retomando o processo, agora com $X = \{\emptyset, \{\emptyset\}\}$, podemos obter um conjunto $Y = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, ou seja, um conjunto de cardinalidade 3. Portanto, através dos de conjuntos e axiomas, construímos o conjunto dos números naturais.

Então, dado um conjunto X, podemos a cada conjunto $S = \{X, \{X\}\}$, com o axioma da união, associar a X o número $|X| + 1$, a partir de $X = \emptyset$.

- $\emptyset \longmapsto 1$
- $\{\emptyset\} \longmapsto 2$
- $\{\emptyset, \{\emptyset\}\} \longmapsto 3$
- $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \longmapsto 4$
- $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} \longmapsto 5$ e assim sucessivamente.

Desse modo o conjunto dos números naturais – símbolo $\mathbb{N}$ – é definido com as seguintes propriedades: $1 \in \mathbb{N}$ e se $x \in \mathbb{N}$, então $x + 1 \in \mathbb{N}$, ou seja, temos $\text{sucessor}(x) = x + 1$. Então, $\mathbb{N}$ é o conjunto que 1 e todos os sucessores a partir de 1 pertencem ao conjunto $\mathbb{N}$.

1.3.2 Conjunto dos números inteiros

Uma forma mais rápida de obter a solução da equação $x + 3 = 10$ é utilizar o conceito de *oposto* de um número, que tem como propriedade: $x + \text{oposto}(x) = 0$. Assim, $\text{oposto}(3) = -3$ e para solucionar a equação $x + 3 = 10$, podemos utilizar a técnica: $x + 3 + \text{oposto}(3) = 10 + \text{oposto}(3)$. Daí $x + 0 = 7 + 3 + \text{oposto}(3) \Longrightarrow x = 7$ e temos $S = \{7\}$.

Podemos construir o conjunto dos números inteiros – símbolo $\mathbb{Z}$ – como o conjunto $\mathbb{Z} = \mathbb{N} \cup \{\text{oposto}(n)\} \cup \{0\}$ com $n \in \mathbb{N}$.

No conjunto $\mathbb{Z}$ são definidas as operações de adição e multiplicação, além da subtração, devido a propriedade simétrico ou oposto para a adição. Para todo $x \in \mathbb{Z}$ existe $(-x) \in \mathbb{Z}$ tal que $x + (-x) = 0$. Estabelecemos que $m - n = m + (-n)$ para todos $m, n \in \mathbb{Z}$.

1.3.3 Conjunto dos números racionais

Dada a equação $2x - 3 = 0$, podemos nos perguntar em qual conjunto numérico, visto até o momento, a equação tem solução? Veremos que este conjunto não pode ser os naturais, pois com uma breve verificação temos que se $x = 1$ obteremos $2 \cdot 1 - 3 = -1$ e se $x = 2$, chegamos em $2 \cdot 2 - 3 = 1$. Assim, para $x \leq 2$ temos $2x - 3 > 0$ e a solução da equação deve ser um número tal que $1 < x < 2$, que não é uma solução presente nos conjuntos dos números naturais nem dos inteiros. Essa dificuldade é superada ao introduzirmos o conjunto dos números racionais.

Chamamos conjunto dos racionais – símbolo $\mathbb{Q}$ – o conjunto das frações $\frac{a}{b}$, tal que $a, b \in \mathbb{Z}$ com $b \neq 0$. Definiremos melhor este conjunto a partir do conceito de relação de equivalência, que será visto na seção sobre relações no capítulo 2.

O conjunto $\mathbb{Q}$ possui as mesmas operações que o conjunto $\mathbb{Z}$, além da propriedade simétrico ou inverso para a multiplicação, estabelecendo que para todo $\frac{a}{b} \in \mathbb{Q}$ e $a, b \neq 0$ existe $\frac{b}{a} \in \mathbb{Q}$ tal que $\frac{a}{b} \cdot \frac{b}{a} = 1$.

Devido essa propriedade, podemos definir em $\mathbb{Q}^*$(conjunto dos racionais não nulos) a operação de divisão, estabelecendo que $\frac{a}{b} : \frac{c}{d} = \frac{a}{b} \cdot \frac{d}{c}$ para $\frac{a}{b}$ e $\frac{c}{d}$ racionais quaisquer não nulo.

1.3.4 Conjunto dos números reais

Dado um quadrado de lado 1, pelo Teorema de Pitágoras a medida correspondente ao comprimento da sua diagonal d é $d^2 = 1^2 + 1^2 = \sqrt{2}$. Vamos mostrar que esse número não é um número racional. Suponhamos que $\sqrt{2}$ seja um número racional, ou seja, pode ser escrito na forma $\sqrt{2} = \frac{p}{q}$ com $p, q \in \mathbb{Z}$, $q \neq 0$ e sem nenhum fator comum ao serem decomposto. Então, temos $2 = \frac{p^2}{q^2} \Longrightarrow p^2 = 2q^2$. Como p^2 é o dobro de um número inteiro, ele será um número par. Já, um número ímpar elevado ao quadrado sempre é igual a um número ímpar. Logo p deve ser par. Por outro lado, $q^2 = \frac{p^2}{2}$, mas sendo p par, então p^2 é múltiplo de 4, isto é, $p^2 = 4k$. Assim, $q^2 = \frac{4k}{2} = 2k$ e concluímos que q é par. Mas, se p e q são pares então ambos são divisíveis por 2 e a fração ainda pode ser simplificada, o que contradiz nossa

suposição. Logo, $\sqrt{2}$ é um número não racional. De modo análogo, podemos mostrar que todo número primo p é tal que $\sqrt{\mathrm{p}}$ é não racional. A existência desses números fez com que os conjuntos numéricos fossem ampliados, com a introdução dos chamados *números irracionais* – símbolo $\mathbb{I}$.

E dá união entre os números irracionais e os números racionais obtemos o conjunto dos números reais – símbolo $\mathbb{R}$ – tal que $\mathbb{R} = \mathbb{Q} \cup \mathbb{I} \cup \{0\}$.

2 Relações e Funções

Neste capítulo, veremos os conceitos de relação e função, que estão relacionados com o tema principal do trabalho, a criptografia para o ensino médio. Para isso, introduziremos alguns tópicos já conhecidos desde o ensino Fundamental e outros aprendidos apenas no ensino Médio.

2.1 Par ordenado

Até o momento, estudamos os conjuntos e como são formados através de axiomas. Nesse tópico trabalharemos com um conjunto particular e para isso introduziremos diversos conceitos que para alguns serve como revisão e para outros, como um novo conceito a ser estudado.

Definição 2.1. Dizemos que (a,b) é um par ordenado se ocorrer a seguinte propriedade: se um outro par (x,y) é tal que $(x,y) = (a,b)$, então $x = a$ e $y = b$.

Um par ordenado $p = (x,y)$ é formado por um objeto x, chamado a primeira coordenada de p ou abscissa e um objeto y, chamado a segunda coordenada de p ou ordenada.

Em muitos momentos, a partir do 7ºano do ensino Fundamental II até o término do ensino Médio encontramos situações na qual a solução é determinada ao resolvermos um sistema de equações lineares com duas incógnitas. A solução nos fornece um par de números onde há a necessidade de distinguir a ordem dos elementos. Por exemplo, dado o sistema de equações, que escrevemos na forma $\begin{cases} x + y = 10 \\ x - y = 8 \end{cases}$, temos como solução do sistema, as coordenadas $x = 9$ e $y = 1$. Representamos a solução como o par ordenado $(9,1)$.

Importante observarmos que o par ordenado (x,y) não é o mesmo que o conjunto $\{x,y\}$, pois pela axioma $A2$, $\{x,y\} = \{y,x\}$ sempre. Contudo, $(x,y) = (y,x)$ somente se $x = y$.

2.2 Produto cartesiano

Dados dois conjuntos A e B podemos provar que o produto cartesiano, que simbolizaremos por $A \times B$, é um conjunto onde $A \times B = \{(a,b)$, tal que, $a \in A$ e $b \in B\}$. Neste trabalho admitiremos que $A \times B$ é um conjunto.

Sejam os conjuntos finitos $A = \{a_1, \dots, a_m\}$ e $B = \{b_1, \dots, b_p\}$. O produto cartesiano $A \times B$, com o conjunto A contendo m elementos e o conjunto B com p elementos, é finito e possui $m \cdot p$ elementos, ou seja, $|A \times B| = |A| \cdot |B|$ (cardinalidade do conjunto produto cartesiano é o produto das cardinalidades dos conjuntos).

Por exemplo, seja $A = \{1,2,3\}$ e $B = \{0,1\}$. O conjunto do produto cartesiano $A \times B = \{(1,0), (1,1), (2,0), (2,1), (3,0), (3,1)\}$. Vemos que temos 6 pares ordenados pois, $|A \times B| = |A| \cdot |B| = 3 \cdot 2 = 6$.

O produto cartesiano $A \times B$ acha – se intimamente ligado à ideia de relação, que será o assunto abordado no próximo tópico.

2.2 Relações

Uma relação, representada por R, entre os conjuntos A e B, existe se o elemento $x \in A$ está relacionado com $y \in B$ através de uma determinada propriedade.

Definição 2.2. Sejam A e B dois conjuntos. Dizemos que R é uma relação do conjunto A sobre o conjunto B se $R \subset A \times B$, isto é R é um subconjunto de $A \times B$. Neste caso, simbolizamos essa condição por $R: A \longrightarrow B$. O conjunto A será denominado *domínio* e o conjunto B de *contradomínio* da relação R.

Um exemplo rápido é a relação “maior do que” entre números reais. A condição que nos permite escrever $x > y$, com $x \in \mathbb{R}$ e $y \in \mathbb{R}$ é $x - y > 0$. Aqui, a relação é dentro do próprio conjunto.

Então, vemos que para conhecer a relação R, descrevemos a propriedade que relaciona os elementos do domínio, com os elementos do contradomínio. A notação mais comum será: $x \longmapsto y$, sendo por convenção $x \in A$, $y \in B$, seguida da propriedade que relaciona os dois conjuntos.

Exemplo 1. A relação menor: $\{-1, 1, 2, 7\} \longrightarrow \{1,2,5\}$, associa a todo elemento do domínio $x \in \{-1, 1, 2, 7\}$ elementos do contradomínio y, tais que, x seja menor que y, ou seja, $x \longmapsto y$, tal que $x < y$. Assim, $(-1,1) \in \text{menor}$, mas $(2,1) \notin \text{menor}$, pois não ocorre que $2 < 1$ e a relação menor não é verificada para o par $(2,1)$. Relacionando cada elemento do domínio com o contradomínio para a relação menor teremos o conjunto $\text{menor} = \{(-1,1), (-1,2), (-1,5), (1,2), (1,5), (2,5)\}$.

Exemplo 2. A relação reta: utilizando os conjuntos acima e a relação reta $2y = x + 3$, temos, por exemplo que $(-1) \longmapsto 2(1) = 2 = -1 + 3$. Assim, o par $(-1,1) \in \text{reta}$.

Verificando a propriedade para todo o produto cartesiano $\{-1,1,2,7\}\,\mathrm{X}\,\{1,2,5\}$, obtemos o conjunto $\mathrm{reta} = \{(-1,1),(1,2),(7,5)\}$.

Exemplo 3. A relação $\mathrm{R}: \mathbb{R} \longrightarrow \{0,1\},\ \mathrm{x} \longmapsto 1$, se $\mathrm{x}^2 < 0$, ou seja, a relação R associa 1 aos números reais cujo quadrado de qualquer número real seja negativo. Como sabemos, o quadrado de um número real é sempre positivo, então nenhum elemento de $\mathbb{R}$ associa – se ao número 1, não existindo pares ordenados para essa relação. Logo, $\mathrm{R} = \emptyset$.

Para uma melhor visualização das relações anteriores, será muito útil representar os conjuntos por pontos interiores a uma linha fechada e a relação através de flechas.

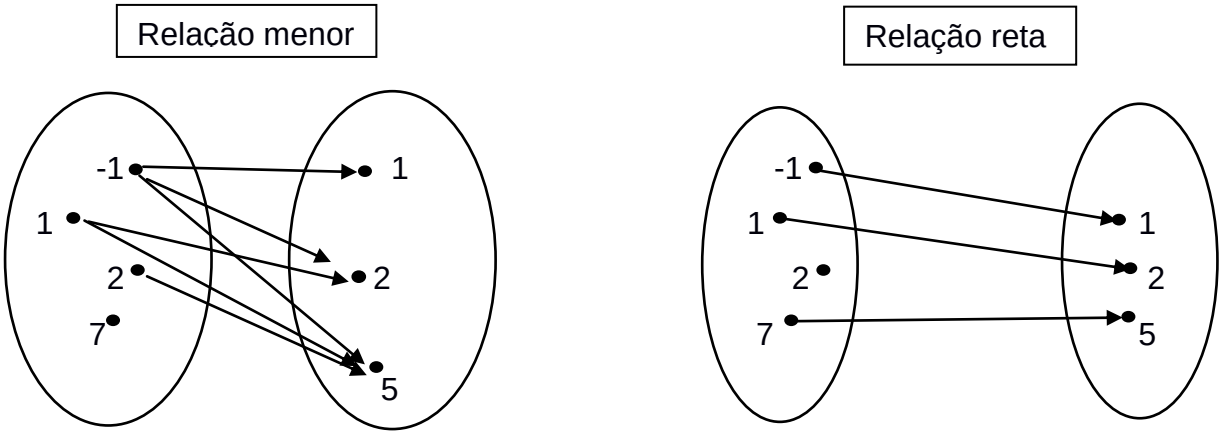

Figura 1-Diagramas de flechas das relações menor e reta

Dados A, B dois conjuntos e $\mathrm{R}: \mathrm{A} \longrightarrow \mathrm{B}$ uma relação. Como já vimos A é o domínio e B é o contradomínio. Seja $\mathrm{x} \in \mathrm{A}$ e $\mathrm{y} \in \mathrm{B}$ tal que $(\mathrm{x}, \mathrm{y}) \in \mathrm{R}$, então dizemos que y é uma *imagem* de x e denotamos isso por $\mathrm{y} = \mathrm{R}(\mathrm{x})$.

O subconjunto do contradomínio de todas as imagens de x, pela relação R, é denominado imagem de x e é denotado por $\mathrm{R}[\mathrm{x}]$, isto é, $\mathrm{R}[\mathrm{x}] = \{\mathrm{y}/(\mathrm{x}, \mathrm{y}) \in \mathrm{R} = \mathrm{R}(\mathrm{x})\}$.

Se $\mathrm{X} \subseteq \mathrm{A}$, $\mathrm{R}[\mathrm{x}] = \{\mathrm{y}/(\mathrm{x}, \mathrm{y}) \in \mathrm{R}, \mathrm{x} \in \mathrm{X}\} = \{\mathrm{R}(\mathrm{x}),$ tal que, $\mathrm{x} \in \mathrm{X}\}$ denominado conjunto imagem do subconjunto X, ou simplesmente a imagem de X e, desse modo, $\mathrm{R}[\mathrm{A}]$ é o conjunto imagem da relação.

Assim, anteriormente no primeiro exemplo, a imagem da relação menor é o conjunto $\{1, 2, 5\}$, pois todos os elementos estão associados a algum elemento do domínio. Nos outros exemplos, temos os conjuntos imagens das relações indicadas:

- reta $[\{-1, 1, 2, 7\}] = \{1,2,5\}$;
- $\mathrm{R}[\mathbb{R}] = \emptyset$.

2.2.1 Relação de equivalência

Antes de definir *relação de equivalência*, precisamos entender três propriedades que nos garantem sua existência.

Propriedade reflexiva. $R(a) = a$. Ela nos garante que dentre as possíveis imagens para um dado elemento do domínio o próprio elemento é sua imagem. A relação $R: \{1,2,3,4\} \longrightarrow \{1,2,3,4\}$, tal que $x \mapsto y$ se $x \leq y$ é reflexiva já que, por exemplo, $2 \leq 2$.

Propriedade simétrica. $R(a) = b$, então $R(b) = a$. Dado um elemento x, se y está no conjunto imagem de x, então x está no conjunto imagem y. Um exemplo de relação simétrica é a relação $A: \{4,5,6,7\} \longrightarrow \{4,5,6,7\}$, $x \mapsto y$, se x e y possuem a mesma paridade. Então, $A(4) = 6$ pois são pares e da mesma forma $A(6) = 4$.

Propriedade Transitiva. Se $R(a) = b$ e $R(b) = c$, então $R(a) = c$. Essa propriedade nos permite relacionar dois elementos que tenham em comum o fato de o primeiro ser a imagem de um certo elemento que, por sua vez, é imagem de um segundo elemento. Seja a relação $B: \mathbb{Z} \longrightarrow \mathbb{Z}$, $x \mapsto y$, se $x - y$ é um número inteiro, então $a - b$ e $b - c$ são inteiros. Desta forma $a - c = (a - b) + (b - c)$ também é um inteiro.

Definição 2.3. Uma relação $R: A \longrightarrow A$ é uma relação de equivalência se ela satisfaz as propriedades reflexiva, simétrica e transitiva.

Exemplo 4. Seja n um número inteiro positivo. A relação em $\mathbb{Z}$, que fixado n, associa ao número inteiro x, um número inteiro y, tal que $x - y$ seja um múltiplo de n, isto é, existe $k \in \mathbb{Z}$ tal que $x - y = kn$ é uma relação de equivalência. O número $x - y$ é divisível por n e, em geral, dizemos que n divide $x - y$ e denotamos por $n|x - y$. Por exemplo, se $x = 17$, $y = 9$ e $n = 4$ satisfaz a relação, pois $4|17 - 9$.

Verificaremos a seguir se a relação satisfaz as três propriedades da definição. (i) Reflexiva: $x - x = 0|n$, pois $0 = 0k$ para qualquer $k \in \mathbb{Z}$. (ii) Simétrica: $n|x - y$, pois existe $k \in \mathbb{Z}$ tal que $kn = x - y$, portanto $y - x = (-k)n$. Logo, $n|y - x$ e provamos que a relação possui a propriedade simétrica. (iii) Transitiva: se $n|x - y$ e $n|y - z$, então existe inteiros k, m tais que $x - y = kn$ e $y - z = mn$. Agora, somando as duas igualdades membro a membro teremos $x - y + (y - z) = kn + mn = x - z = (k + m)n$, isto é, $n|x - z$, confirmando que satisfaz a propriedade transitiva. Logo, fica demonstrado que o exemplo é uma relação de equivalência.

Suponhamos que exista uma relação de equivalência em um dado conjunto. Seja a um elemento particular do conjunto. O subconjunto de todos os elementos que estão relacionados com a é chamado de *classe de equivalência* de a.

Definição 2.4. Dados A um conjunto e uma relação de equivalência em A. Para cada elemento de $a \in A$, a classe de equivalência de a, representada por $\bar{a}$, é o conjunto de todos os elementos $x \in A$ tal que x está relacionado com a através da relação de equivalência.

Se voltarmos ao exemplo 4 e supormos $n = 3$, teremos $3|x - y$, ou seja, $x - y$ é divisível por 3. Portanto, para cada $a = x - y$, existirá uma classe de equivalência $\bar{a} = \{x, y \in \mathbb{Z}/3|x - y$, assim, $\bar{0} = \{x \in \mathbb{Z}$, tal que $3|x - 0\}\} = \{\ldots -6, -3, 0, 3, 6, 9, \ldots\}$.

A relação, denotada por $\sim$, que associa ao par (p, q) outro par (u, v) tal que $pv = qu$ é uma relação de equivalência. Verifiquemos se a relação satisfaz as propriedades de relação de equivalência.

(i) Reflexiva: temos que, se $p \in \mathbb{Z}$ e $q \in \mathbb{Z}^*$, $pq = qp$, portanto $(p, q) \sim (p, q)$.

(ii) Simétrica: se $p, u \in \mathbb{Z}$, $q, v \in \mathbb{Z}^*$ e $(p, q) \sim (u, v)$, então $pv = qu$, ou ainda, $uq = vp$, isto é, $(u, v) \sim (p, q)$.

(iii) Transitiva: sendo $p, u, y \in \mathbb{Z}$, $q, v, z \in \mathbb{Z}^*$, então $(p, q) \sim (u, v)$ e $(u, v) \sim (y, z)$. Sabemos que $pv = qu$. Multiplicando a igualdade por z, teremos $pvz = quz$. Também, pela relação $uz = vy$. Multiplicando essa nova igualdade por q, encontramos $uzq = vyq$. Dessa forma, $pvz = qvy$. Como $v \neq 0$, $pz = qy$, ou seja, $(p, q) \sim (y, z)$. Logo, a relação $\sim$ é uma relação de equivalência.

Podemos afirmar que o conjunto $\mathbb{Z} \times \mathbb{Z}^* = \{(p, q)/p \in \mathbb{Z}, q \in \mathbb{Z}^*\}$ não é o conjunto dos números racionais, pois sabemos que os pares $(2,3), (16,24) \in \mathbb{Z} \times \mathbb{Z}^*$ e $(2,3) \neq (16,24)$. Isso acontece, pois segundo a definição 2.1, se fossem iguais, teríamos $2 = 16$ e $3 = 24$.

Logo, a relação $\sim$ determina sobre $\mathbb{Z} \times \mathbb{Z}^*$ várias classes de equivalência. Para cada par $(p, q) \in \mathbb{Z} \times \mathbb{Z}^*$, a classe de equivalência na qual esse par pertence será indicada por $\frac{\bar{p}}{q}$. Então, $\frac{\bar{p}}{q} = \{(u, v) \in \mathbb{Z} \times \mathbb{Z}^*/(p, q) \sim (u, v)\} = \{(u, v) \in \mathbb{Z} \times \mathbb{Z}^*/pv = qu\}$. Por exemplo, $\frac{\bar{3}}{4} = \{(u, v) \in \mathbb{Z} \times \mathbb{Z}^*/3v = 4u\} = \{(3,4); (-3, -4); (6,8); (-6, -8); \ldots\}$.

O conjunto de todas as classes de equivalência determinadas por $\sim$ sobre $\mathbb{Z} \times \mathbb{Z}^*$ será o conjunto dos números racionais e designado por $\mathbb{Q}$. Logo:

$$\mathbb{Q} = \{\frac{\bar{p}}{q}/q \neq 0\} \cup \bar{0} = \{\frac{0}{k}/k \in \mathbb{Z}^*\}.$$

2.2.2 Imagem Inversa

Seja uma relação $R: A \longrightarrow B$. Se $y \in B$, o conjunto $R^{-1}[y] = \{x/(x,y) \in R\}$ é denominado *imagem inversa* do elemento y, pela relação R. Então, analogamente, temos que se $Y \subseteq B, R^{-1}[Y] = \{x/(x,y) \in R,\ y \in Y\}$

Retomando a relação menor, temos que por exemplo $\text{menor}^{-1}[2] = \{-1, 1\}$ e $\text{menor}^{-1}[\{1,2,5\}] = \{-1,1,2\}$.

Como vimos neste capítulo, até o momento, dados dois conjuntos A e B, podemos determinar as possíveis relações de um conjunto no outro. Dessas relações, existe um caso particular de especial importância que veremos no próximo tópico.

2.3 Funções

Consideremos os seguintes conjuntos $A = \{0,1,2,3\}$ e $B = \{-1,0,1,2,3\}$ e as relações entre os elementos do conjunto A e os elementos do conjunto B, formando assim os pares ordenados (x, y), com $x \in A$ e $y \in B$:

- $S = \{(x,y) \in A \text{ X } B \mid y = 2x - 1\}$
- $T = \{(x,y) \in A \text{ X } B \mid y^2 = x^2\}$
- $U = \{(x,y) \in A \text{ X } B \mid y = x\}$
- $V = \{(x,y) \in A \text{ X } B \mid y = 1\}$

Analisando cada uma das relações, temos:

- $S = \{(0,-1), (1,1), (2,3)\}$

  Para cada elemento do conjunto A, com exceção do 3, existe um só elemento $y \in Y$ tal que $(x,y) \in S$. Para o elemento $3 \in A$, não existe $y \in B$ tal que $(3,y) \in S$.

- $T = \{(0,0), (1,1), (1,-1), (2,2), (3,3)\}$

  Para cada elemento do conjunto A, com exceção do 1, existe um só elemento $y \in B$ tal que $(x,y) \in T$. Para o elemento $1 \in A$, existem dois elementos de B, que são 1 e -1, tais que $(1,1) \in T$ e $(1,-1) \in T$.

- $U = \{(0,0), (1,1), (2,2), (3,3)\}$

  Para todo elemento do conjunto A, sem exceção, existe um só elemento $y \in B$ tal que $(x,y) \in U$.

- $V = \{(0,1), (1,1), (2,1), (3,1)\}$

  Para todo elemento do conjunto A, existe um, e somente um, elemento $y \in B$

tal que $(x, y) \in V$.

As relações U e V, que possuem a seguinte característica “para todo elemento do conjunto A, sem exceção, existe um só elemento $y \in B$, tal que (x, y) pertence à relação”, recebem o nome de *função*.

Definição 2.5. Uma relação f entre os conjuntos X e Y, não vazios, recebe o nome de função se, e somente se, para cada elemento de $x \in X$, corresponde um único elemento $y \in Y$, tal que $(x, y) \in f$.

A definição acima possui duas condições para que uma relação seja função. A condição de existência (para todo elemento do conjunto X, existe um elemento do conjunto Y) e a condição de unicidade (o elemento do conjunto Y é único).

Sendo x um elemento de X, a imagem de x será um elemento de Y no qual a regra f associa com y. Devido ao fato de toda função ser uma relação, a notação para uma função f do conjunto X para o conjunto Y será a mesma. Assim, $f: X \to Y$ é uma função, sendo o conjunto X o domínio e Y o contradomínio. Se $y \in Y$ é um elemento de $x \in X$, tal que $f(x) = y$, temos que y será uma imagem de x. O conjunto de todos os elementos de Y do contradomínio que estão associados, pela função f, ao conjunto domínio chamamos de imagem, representado por $Im(f)$.

Pela definição de função o conjunto $f[x]$ será sempre unitário e, por isso, não é comum utilizar esta notação no contexto das funções.

A seguir apresentamos alguns exemplos de funções. Lembramos que, quando uma função é dada apenas por uma expressão matemática o domínio, por convenção é o maior subconjunto dos números reais para o qual a condição de existência e unicidade, de uma função f, esteja verificada e representamos este conjunto por $Dom(f)$.

- $f: A \longrightarrow B / f(x) = 2x$ é uma função que associa a cada $x \in A$ um $y \in B$
- $f: \mathbb{R}_+ \cup \{0\} \longrightarrow \mathbb{R} / f(x) = \sqrt{x}$ é uma função que corresponde cada $x \in \mathbb{R}_+ \cup \{0\}$, a um $y \in \mathbb{R}$. Notemos que $y \in \mathbb{R}$ se, e somente se, x é número real e não negativo.
- $f: \mathbb{R}^* \longrightarrow \mathbb{R} / y = \frac{1}{x}$ é uma função se, e somente se, x é um número real e diferente de zero.
- $f: \mathbb{R} \longrightarrow \mathbb{R} / f(x) = x$ é uma função que associa cada elemento de $x \in \mathbb{R}$ o próprio x.

Esta última função denominamos *função identidade* e veremos que as funções são mais comuns no que ainda iremos estudar sobre criptografia.

Antes de estudarmos detalhadamente alguns tipos de funções reais, vamos

apresentar uma técnica que obtém novas funções, a partir de funções já conhecidas, de modo semelhante aos axiomas de conjuntos que vimos no capítulo 1. Também iremos, a partir daqui, trabalhar apenas com as relações que são funções pois, são elas que utilizaremos no capítulo 5, que trata de modo básico o tema criptografia.

2.3.1 Funções compostas

Podemos obter outras funções, de modo semelhante da forma de como chegamos a outros números a partir dos números naturais. Por exemplo, seja $x \in \mathbb{R}$ e as funções reais $g(x) = -3x$ e $h(x) = x + 7$. Se, para qualquer $z \in \mathbb{R}$, tomarmos qualquer $x = g(z) = -3z$ e em seguida calcularmos $h(x) = h(-3z) = -3z + 7$, temos para qualquer $z \in Dom(g)$, tal que, $g(z) \in Dom(h)$, definida uma nova função $h(g(z)) = -3z + 7$ e a denotamos como $h \circ g$.

Definição 2.6. Sejam f, g funções, tal que, $f: A \longrightarrow B$; $g: C \longrightarrow D$, e $Im(f) \subseteq C$. Definiremos uma função $g \circ f: A \longrightarrow D / g \circ f = g(f(x))$. A esta damos o nome de *função composta*.

A composição de funções na verdade é uma operação entre funções, assim como o produto cartesiano é uma operação entre conjuntos ou a adição é uma operação entre números.

Exemplo 5. Sejam os conjuntos $A = \{0,1,2,3\}$, $B = \{0,1,2,3,4,9\}$ e $C = \{1,3,5,7,9,19\}$ e as seguintes funções:

- $f: A \longrightarrow B$ definida por $f(x) = x^2$
- $g: B \longrightarrow C$ definida por $g(x) = 2x + 1$

Pelas funções acima, podemos observar que $f(1) = 1$, $g(1) = 3$. Como $Im(f) \subseteq B$, definimos a função $g \circ f$ a partir de $g(x)$, trocando x por $f(x)$. Então, pelo exemplo $(g_o f)(x) = 2.f(x) + 1 = 2x^2 + 1$ e se calcularmos $(g_o f)(1)$, teremos $(g_o f)(1) = 2 \cdot 1^2 + 1 = 3$

Observações:

Seja X um conjunto não vazio, e as funções $f, g: X \longrightarrow X$, tal que $f(x) = x$ (função identidade) e $g(x) = 5x - 1$. Sendo $Im(f) \subseteq Dom(g)$, está definida a função $g_o f$ e $g\big(f(x)\big) = g(x) = 5x - 1$. Em particular $Im(g) \subseteq Dom(f)$ portanto, também está definida a função $f_o g$ e $f\big(g(x)\big) = f(5x - 1) = 5x - 1$. Observe que nesse exemplo

$g_o f = f \circ g$ porém, esse fato não ocorre geralmente.

Algumas vezes as funções não admitem inversas. Exemplo, sejam as funções $f: \mathbb{R}^* \longrightarrow \mathbb{R} / f(x) = \frac{1}{x}$ e $g: \mathbb{R} \longrightarrow \mathbb{R} / \ g(x) = 5x - 15$. O conjunto $\mathrm{Im}(g) = \mathbb{R} \nsubseteq \mathbb{R}^* = \mathrm{Dom}(f)$, logo a função $f \circ g$, não está definida, pois temos que $f\big(g(x)\big) = f(5x - 15) = \frac{1}{5x-15}$ e não existe $f(g(3))$, isto é, $f \circ g$ não satisfaz o critério de existência para $3 \in \mathrm{Dom}(f \circ g)$. Porém, $g \circ f$ está definida, isto é, $g\big(f(x)\big) = g\left(\frac{1}{x}\right) = \frac{5}{x} - 1$, pois $\mathrm{Dom}(f) = \mathbb{R}^*$ e, portanto $g \circ f$ é uma função.

Existem certas funções que permitem que determinadas propriedades da imagem sejam obtidas a partir do domínio. Por exemplo, a função $f(x) = -3x + 2$ permite estender a propriedade da desigualdade entre os elementos do conjunto domínio, ou seja, se tivermos $a, b \in \mathrm{Dom}(f)$ e $a \neq b$, então $f(a) \neq f(b)$. Para algumas funções essa característica pode não ocorrer, por exemplo, seja $g: \mathbb{R} \longrightarrow \mathbb{R}$ tal que $g(x) = x^2$. Temos que $-2 \neq 2 \in \mathrm{Dom}(g)$, porém $f(-2) = f(2) = 4$. As funções que possuem a característica de quando elementos diferentes do domínio correspondem a diferentes elementos da imagem denotamos função injetiva.

Definição 2.7. Uma função $f: X \longrightarrow Y$ é injetiva se, e somente se, quaisquer que sejam $a, b \in X$ se $a \neq b$, então $f(a) \neq f(b)$. Notemos que a definição é equivalente a dizer que uma função é injetiva se, e somente se, quaisquer que sejam $a, b \in X$, se $f(a) = f(b)$, então $a = b$.

Definição 2.8. Uma função $f: X \longrightarrow Y$ é sobrejetiva se, e somente se, para todo $y \in Y$ existe um $x \in X$ tal que $f(x) = y$. Notemos que $f: X \to Y$ é sobrejetiva se, e somente se, $\mathrm{Im}(f) = Y$.

A função $f: \mathbb{R} \longrightarrow \mathbb{R}_+$ tal que $f(x) = x^2$ é sobrejetiva, pois, para todo elemento de $y \in \mathbb{R}_+$ existe o elemento $x \in \mathbb{R}$ tal que $y = x^2$.

Definição 2.9. Uma função $f: X \to Y$ é bijetiva se, somente se, f é injetiva e sobrejetiva, isto é, f será bijetiva se para qualquer $y \in Y$, existe um único elemento $x \in X$ tal que $f(x) = y$.

Se retornarmos aos exemplos iniciais, veremos que a relação C, por definição, é uma função definida pela lei $f(x) = x$. Ela é sobrejetiva, pois para todo elemento de $y \in Y$, existe um elemento $x \in X$ tal que $f(x) = x$. Além disso, também é injetiva, pois para todo $x_1 \neq x_2$, temos $f(x_1) \neq f(x_2)$. Logo, a função é bijetiva.

Já a função D definida pela lei $f(x) = 1$ é sobrejetiva, pois para todo elemento de $y \in Y$ existe um elemento $x \in X$ tal que $y = 1$, mas não é injetiva, pois $x_1 \neq x_2$, temos $f(x_1) = f(x_2)$. Portanto, a função não é bijetiva.

2.3.2 Funções inversas

Definição 2.10. Uma função $f: X \longrightarrow Y$ é invertível se existe uma função $g: Y \longrightarrow X$ tal que:

(i) $f \circ g = I_Y$;

(ii) $g \circ f = I_X$.

Denotamos por I_A a função identidade do conjunto A, isto é, $I_A: x \in A \mapsto x \in A$. Neste caso, a função g é chamada função inversa de f e escrita $g = f^{-1}$.

Sejam as funções $f: \mathbb{R} \longrightarrow \mathbb{R}$ tal que $f(x) = x^3$ e $g: \mathbb{R} \longrightarrow \mathbb{R}$ tal que $g(x) = \sqrt[3]{x}$. Será que podemos dizer que essas funções são inversas uma da outra? Para responder a esta questão, utilizaremos os conceitos vistos até o momento e a definição de função inversa.

Pela definição, para verificar se f e g são inversas uma da outra, devemos determinar as compostas $f \circ g$ e $g \circ f$:

(i) $f \circ g(x) = f\big(g(x)\big) = \left(\sqrt[3]{x}\right)^3 = x$

(ii) $g \circ f(x) = g\big(f(x)\big) = \sqrt[3]{x^3} = x$

Logo, concluímos que as funções f e g são inversas uma da outra.

Exemplo 6. Seja $f: \mathbb{R} \longrightarrow \mathbb{R}$ tal que $f(x) = x - 1$. Uma inversa de f seria uma função $f^{-1}: \mathbb{R} \longrightarrow \mathbb{R}$ tal que $f^{-1} = x + 1$, pois $(f \circ f^{-1})(x) = (f^{-1} \circ f)(x) = x$.

Exemplo 7. Dada a função $f: \mathbb{R} \longrightarrow \mathbb{R}_+ \cup \{0\}$, $f(x) = x^2$. Esta não admite uma função inversa, pois considerando $g: \mathbb{R}_+ \cup \{0\} \longrightarrow \mathbb{R}$ tal que $g(x) = \sqrt{x}$ como inversa temos que $(g \circ f)(-2) = g\big(f(-2)\big) = g(4) = 2 \neq -2$. Entretanto, se $f: \mathbb{R}_+ \cup \{0\} \longrightarrow \mathbb{R}_+ \cup \{0\}$, $f(x) = x^2$, então $g(x) = \sqrt{x}$ seria uma inversa de f.

Aplicando a definição 2.9 diretamente para verificar se uma função é ou não invertível nem sempre é fácil. Por esse motivo, os conceitos de função injetiva e sobrejetiva, garantem a existência da função inversa.

Teorema 1. Seja $f: X \longrightarrow Y$, f é invertível se, e somente se, f é bijetiva.

Demonstração:

($\Longrightarrow$) Suponhamos que existe $g\colon Y \longrightarrow X$ tal que $f \circ g = I_Y$ e $g \circ f = I_X$. Tomemos $y \in Y$ e façamos $x = g(y)$. Da condição (i), $f(x) = f\big(g(y)\big) = (f \circ g)(y) = I_Y(y) = y$. Então, f é sobrejetiva. Agora, tomemos $x_1, x_2 \in X$ tais que $f(x_1) \neq f(x_2)$, logo, temos que $g \circ f(x_1) \neq g \circ f(x_2)$. Da condição (ii), segue que $I_X(x_1) \neq I_X(x_2)$. Como $x_1 \neq x_2$ a funçao f é injetiva e, portanto é bijetiva.

($\Longleftarrow$) Suponhamos que f seja bijetiva. Vamos construir uma função $g\colon Y \longrightarrow X$ satisfazendo as condições (i) e (ii) da definição anterior. Dado qualquer $y \in Y$, como f é sobrejetiva, existe algum $x \in X$ tal que $f(x) = y$ e como f é injetiva, este x é único. Assim, definimos $g(y) = x$ e a função $g\colon Y \longrightarrow X$ é uma função que associa cada $y \in Y$ o único $x \in X$ tal que $f(x) = y$, então é imediato que $g\big(f(x)\big) = I_X$ e $f\big(g(x)\big) = I_Y$ para qualquer $x \in X$ e $y \in Y$. Portanto, $f\colon X \longrightarrow Y$ é invertível. ■

3 Divisibilidade

Definição 3.1. Um número inteiro a divide um número inteiro b quando existe um m, tal que $b = a \cdot m$. Quando $a \neq 0$ (e somente neste caso), dizemos que b é *divisível* por a. Neste caso, o inteiro m é chamado de *quociente* da divisão de b por a.

Quando a divide b, denotamos por $a|b$, mas podemos dizer também que a é um divisor de b, ou que b é um múltiplo de a ou ainda, que b é divisível por a. Quando a não divide b, escrevemos $a \nmid b$.

Exemplo 1. $2|14$, pois $14 = 2 \cdot 7$; $12|60$, pois $60 = 12 \cdot 5$. Já $6 \nmid 17$, pois $6 \cdot 2 = 12$ e $6 \cdot 3 = 18$. Como $12 < 17 < 18$, vemos que não existe $a \in \mathbb{Z}$, tal que $2 < a < 3$ e, então dizemos que $6 \nmid 17$.

Proposição 3.1. Seja $a \in \mathbb{Z}$, então temos que $1|a$, $a|a$ e $a|0$

Demonstração:

Temos que, $1|a$ pois $a = 1 \cdot a$, $a|a$ pois $a = 1 \cdot a$ e $a|0$ pois $0 = 0 \cdot a$.■

Proposição 3.2. Sejam $a, b, c, d \in \mathbb{Z}$, com $a, b \neq 0$, então:

(i) Se $a|b$ e $b|c$, então $a|c$.

(ii) Se $a|b$ e $c|d$, então $a \cdot c|b \cdot d$ $(\text{quando } c \neq 0)$

Demonstração:

(i) Se $a|b$ e $b|c$, então existem $q_1, q_2 \in \mathbb{Z}$, tais que $b = q_1 \cdot a$ e $c = q_2 \cdot b$. Substituindo a primeira equação na segunda equação, temos que $c = (q_1 \cdot q_2) \cdot a$. Portanto, $a|c$.

(ii) Se $a|b$ e $c|d$, então existem $q_1, q_2 \in \mathbb{Z}$, tais que $b = q_1 \cdot a$ e $d = q_2 \cdot c$. Multiplicando ordenadamente a primeira equação pela segunda temos como resultado $bd = (q_1 \cdot q_2) \cdot ac$ e portanto, $a \cdot c|b \cdot d$. ■

Exemplo 2. Sabemos que $4|20$ e $20|100$, então pelo item i $4|100$.

Exemplo 3. Como $3|12$ e $7|35$, temos que pelo item ii, $3 \cdot 7|12 \cdot 35$ e $21|420$, pois $420 = 21 \cdot 20$.

Proposição 3.3. Sejam $a, b, c \in \mathbb{Z}$, com $a, b \neq 0$, vale:

(i) Se $a|b$ e $a|c$, então $a|b + c$.

(ii) Se $a|b$ então para todo $n \in \mathbb{Z}$, tem – se que $a|nb$.

(iii) Se $a|b$ e $a|c$, então para todos $m, n \in \mathbb{Z}$, temos que $a|mb + nc$.

(iv) $a|b \Leftrightarrow a| - b \Leftrightarrow -a|b \Leftrightarrow -a| - b$.

Demonstração:

(i) Se $a|b$ e $a|c$, então existem $q_1, q_2 \in \mathbb{Z}$ tais que $b = q_1 \cdot a$ e $c = q_2 \cdot a$. Ao somarmos as duas equações temos, $b + c = q_1 \cdot a + q_2 \cdot a = (q_2 + q_1) \cdot a$, logo, $a|(b + c)$.

(ii) Se $a|b$ então existe um número inteiro k, tal que $b = k \cdot a$. Multiplicando os dois membros da equação por um número inteiro n, temos que $n \cdot b = (n \cdot k) \cdot a$, logo, para todo n, tem-se que $a|nb$.

(iii) Se $a|b$ e $a|c$, então existem $k, q \in \mathbb{Z}$, tais que $b = k \cdot a$ e $c = q \cdot a$. Multiplicando a primeira equação por m e a segunda por n, sendo também $m, n \in \mathbb{Z}$ temos que $m \cdot b = k \cdot m \cdot a$ e $n \cdot c = q \cdot n \cdot a$. Depois somando membro a membro as duas novas equações, teremos $m \cdot b + n \cdot c = k \cdot m \cdot a + q \cdot n \cdot a = (k \cdot m + q \cdot n) \cdot a$ e, portanto, $a|(mb + nc)$.

(iv) $a|b$ temos um $k \in \mathbb{Z}$ tal que $b = k \cdot a$. Se multiplicarmos a equação por (-1), temos $(-b) = (-k) \cdot a$, com $(-k) \in \mathbb{Z}$. Multiplicando essa última equação por (-1), encontramos $b = (-k) \cdot (-a)$, com $(-k) \in \mathbb{Z}$. Por último, multiplicando novamente por (-1) a equação anterior $(-b) = k \cdot (-a)$, com $k \in \mathbb{Z}$. ■

Exemplo 4. Sabemos que $6|24$ e $6|36$. Então pelo item i da proposição anterior, $6|24 + 36 = 6|60$.

Exemplo 5. Temos que $3|24$ e $3|15$. Se $m = 4$ e $n = 5$, pelo item iii, da proposição 3.3, termos que $3|24 \cdot 4 + 15 \cdot 5 = 3|96 + 75 = 3|171$, pois $171 = 3 \cdot 57$.

Proposição 3.4. Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$. Se $a|b$ e $b \neq 0$, então $|a| \leqslant |b|$

Demonstração

Se $a \mid b$ com $b \neq 0$, então existe um inteiro $q \neq 0$ tal que $b = q \cdot a$. Logo, temos que $|b| = |qa| = |q| \cdot |a| \geq |a|$. ■

Proposição 3.5. Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$.

(i) Se $b|a$ e $a|b$, então $a = b$ ou $a = -b$.

(ii) Se $a|1$, então $a = 1$ ou $a = -1$.

Demonstração

(i) Suponha que $b|a$ e $a|b$. Se $a = 0$ ou $b = 0$, temos $a = b = 0$. No caso $a, b \neq 0$, temos, pela proposição 3.4, $|a| \leq |b|$ e $|a| \geq |b|$ logo, $|a| = |b|$, ou seja, $a = \pm b$.

(ii) Suponha que $a|1$. Do item (i) da proposição 3.1, $1|a$ para todo a inteiro. Logo, pelo item i desta proposição, temos que $a = \pm 1$. ■

Proposição 3.6. Sejam $a, b, c \in \mathbb{Z}$, tais que $a|(b + c)$. Então, $a|b \Leftrightarrow a|c$.

Demonstração:

($\Rightarrow$) Suponha que $a|(b + c)$. Então, existe número $k \in \mathbb{Z}$, tal que $b + c = k \cdot a$. Suponha ainda que $a|b$ então, existe q_1 tal que $b = a \cdot q_1$. Substituindo b na última equação temos que $a \cdot q_1 + c = k \cdot a$. Daí, $c = a \cdot (k - q_1)$ e como $k - q_1 \in \mathbb{Z}$ pode-se concluir que $a|c$. A demonstração da recíproca é análoga. ■

Antes de prosseguirmos vamos demonstrar um fato curioso, utilizando algumas proposições estudadas anteriormente. Seja n um número inteiro com $n \neq \pm 1$. Será que se somarmos dois números consecutivos, o resultado será divisível pelo menor deles? Exemplos: $8|8 + 9$? Ou $211|211 + 212$?

Dados dois números $a, b \in \mathbb{Z}$ com $a < b$, se a e b forem números consecutivos, então $a \nmid a + b$.

Demonstração:

Dados $a = n$ e $b = n + 1$ inteiros consecutivos. A soma $n + n + 1 = 2n + 1$. Pela proposição 3.3 (item i), se $n|2n$ e $n|1$, então $n|2n + 1$.

Pela proposição 3.3 (item ii), sabemos que $n|2n$. Contudo, pela proposição 3.5 (item ii),para que $n|1$, temos $n = \pm 1$, uma contradição, pois a afirmação inicial nos diz que $n \neq \pm 1$. Logo, $n \nmid 2n + 1$.■

Isto significa que qualquer número $n \in \mathbb{Z}$, com $n \neq \pm 1$, nunca divide a soma desse número com seu consecutivo.

3.1 Algoritmo da divisão de Euclides

Teorema 1. Se a e b são dois números inteiros com $a \neq 0$, então existem e são únicos os inteiros q e r tais que $b = aq + r$ e $0 \leq r < |a|$, onde q é o quociente e r o resto da divisão de b por a.

Demonstração:

Considere o conjunto $S = \{x = b - ay, y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$.

Existência: Utilizando a Propriedade Arquimediana[1], afirmamos que existe $x \in \mathbb{Z}$ tal que $n \cdot (-x) > -b$, logo $b - n \cdot x > 0$, o que mostra que $S \neq \emptyset$. Pelo Princípio da Boa Ordenação[2], tal conjunto tem um menor elemento r. Sabemos que $r \geq 0$ e vamos mostrar que $r < |a|$. Suponhamos então que $r = b - aq$ e por absurdo que $r \geq |a|$. Logo, existe um $s \in \mathbb{N} \cup \{0\}$ tal que $r = |a| + s$ e, portanto, $s < r$. Temos uma contradição, pois afirmamos que r é o menor elemento do conjunto S.

Unicidade: Suponhamos que existam q' e r', tais que $b = aq' + r'$. Se compararmos $b = aq + r$, com $b = aq' + r'$, teremos $aq + r = aq' + r'$.Reorganizando a equação anterior $aq - aq' = r' - r \Rightarrow a(q - q') = r' - r$ Logo, a divide $r' - r$. Como, $r' < a$ e $r < a$, temos $|r' - r| < a$, e, portanto, como a divide $r' - r$, devemos ter $r' - r = 0$, ou seja, $r' = r$. Desta forma, $aq = aq'$, como por hipótese $a \neq 0$, temos que $q = q'$. ■

Antes de estudarmos outros conceitos e propriedades, que estão relacionados a divisão euclidiana, resolveremos atentamente três situações nas

[1] Propriedade Arquimediana: Dados $a, b \in \mathbb{Z}$ com $a \neq 0$ então b é um múltiplo de a ou se encontra entre dois múltiplos consecutivos de a, isto é, correspondendo a cada par de inteiros $a \neq 0$ e b existe um inteiro q tal que para qualquer a $q \cdot a \leq b \leq (q \pm 1) \cdot a$.

[2] O Princípio da Boa Ordenação (PBO) nos diz que todo conjunto não vazio N de inteiros não negativos possui um menor elemento.

quais devemos dar grande importância ao quociente e ao resto da divisão de Euclides, pois são eles que determinam a solução de cada problema.

Exemplo 6. Encontre o quociente e o resto da divisão de 33 por 5.

Resolução:

$r_1 = 33 - 5 \cdot 1 = 28$

$r_2 = 33 - 5 \cdot 2 = 23$

$r_3 = 33 - 5 \cdot 3 = 18$

$r_4 = 33 - 5 \cdot 4 = 13$

$r_5 = 33 - 5 \cdot 5 = 8$

$r_6 = 33 - 5 \cdot 6 = 3$

Pelo Princípio da Boa Ordenação, o menor elemento $r = 3$ e temos $q = 6$ e podemos escrever $33 = 6 \cdot 5 + 3$.

Exemplo 7. Um caminhão, que suporta transportar até 260kg, fará uma entrega de 1000kg.

Quantas viagens, no mínimo, serão dadas para transportar toda a carga?

Não podemos esquecer que nessa questão toda a carga deve ser transportada.

Primeiramente, dividiremos 1000 por 260 para descobrir quantas viagens, com carga máxima serão dadas. Com o algoritmo da divisão, teremos:

$r_1 = 1000 - 260 \cdot 1$

$r_2 = 1000 - 260 \cdot 2$

$r_3 = 1000 - 260 \cdot 3$

Instantaneamente, diríamos que a resposta seria $q = 3$. Porém, observe que existe um $r = 220$ e esse restante de carga também deve ser transportada, mas o caminhão não irá com sua carga máxima. Então, a resposta seria 4 viagens.

Exemplo 8. (OBMEP – N1F1)[3] Guilherme começa a escrever os números naturais em figuras triangulares de acordo com o padrão abaixo:

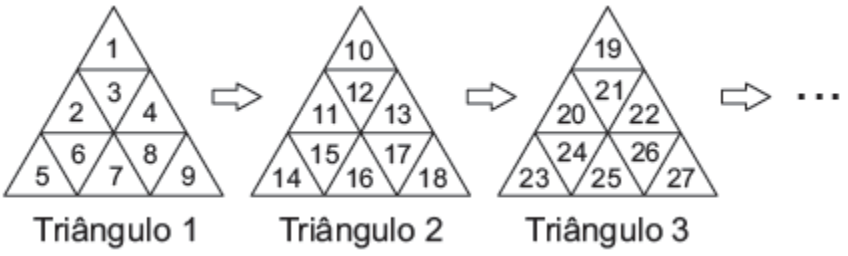

Figura 2 - Triângulos numéricos do exemplo 8

[3] A sigla OBMEP significa Olimpíadas Brasileira de Matemática das Escolas Públicas. N1F1 seria avaliação da primeira fase do nível 1, que corresponde aos 6º e 7ºanos do Ensino Fundamental II.

Nomeando as casas de cada um desses triângulos com as letras A, B, C, D, E, F, G, H e I como na figura a seguir, ele pode codificar cada número natural por meio do número do triângulo e da letra da casa em que ele aparece.

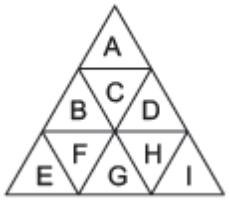

Figura 3 - Triângulo alfabético do exemplo 8

Por exemplo, o número 8 é codificado por 1H, pois aparece na casa H do triângulo 1. Já o número 22 é codificado por 3D, já que aparece na casa D do terceiro triângulo. Como Guilherme codifica o número 2014?

Para começarmos a resolução, devemos observar que em cada triângulo maior estão escritos 9 números, em triângulos menores, e que a posição de cada número corresponde ao resto da divisão desse número por 9. Por exemplo, os números 1, 10, 19 estão na mesma posição do triângulo maior e quando são divididos por 9 possuem resto 1.

Na segunda figura, a posição do número em cada triângulo é descrita por uma letra de A até I, que corresponde ao resto da divisão do número por 9, ou seja, no resto 1 a posição é A, resto 2 é B, resto 3 é C, resto 4 é D, resto 5 é E, resto 6 é F, resto 7 é G, resto 8 a posição é H e, finalmente, se o resto for 0 a posição é I.

Utilizando o algoritmo da divisão de Euclides, temos que $2014 = 223 \cdot 9 + 7$. Aqui, novamente observemos que $q = 223$ e este valor não seria a posição correta, pois ainda temos mais 7 posições, que seria o resto da divisão. Logo, 2014 está no triângulo $223 + 1 = 224$, na posição equivalente ao resto 7, ou seja, G. Portanto, Guilherme codifica 2014 como 224G.

3.2 Máximo Divisor Comum

Definição 3.2: Sejam a e b dois números inteiros não simultaneamente nulos ($a \neq 0$ ou $b \neq 0$), chamamos de *máximo divisor comum* de a e b o inteiro positivo d, indicado por $\mathrm{mdc}(a,b)$, o número que satisfaça as seguintes condições:

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

(ii) se $c|a$ e se $c|b$, então $c|d$.

Então, se d é um mdc de a e b e, c é um divisor comum desses números, $|c|$

divide d, e, portanto $c \leq |c| \leq d$,mostrando que o máximo divisor comum de dois números é o maior entre todos os divisores comuns desses números.

Por exemplo, sejam $a = 12$ e $b = 9$. Indicando por $D(x)$ o conjunto dos divisores de $x \in \mathbb{N}$, temos $D(12) = \{1,2,3,4,6,12\}$ e $D(9) = \{1,3,9\}$. Ao fazermos $D(12) \cap D(9)$, encontramos o conjunto $\{1,3\}$. Observemos que, pelo item (i) da definição anterior, $3|12$, $3|9$, $1|9$ e $1|12$; pelo item (ii) da mesma definição, se $c|12$ e $c|9$, então $c = 1$ ou $c = 3$. Portanto, temos que 3 é o máximo divisor de 12 e 9 e denotamos por $mdc(9,12) = 3$.

Alguns casos particulares é fácil verificar a existência do mdc. Por exemplo, se $b \in \mathbb{Z}$ temos claramente que $mdc(0, b) = b$, $mdc(1, b) = b$, $mdc(b, b) = b$ e ainda se $b|a$ então $mdc(a, b) = b$.

Para provar a existência do máximo divisor comum de dois inteiros não negativos utilizaremos o Lema de Euclides.

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

Demonstração:

Seja $d = mdc(a, b - na)$. Como $d|a$ e $d|(b - na)$, segue que d divide a igualdade $b = b - na + na$. Logo, d é um comum de a e b. Supondo que c seja um divisor comum de a e b. Então temos que c é um divisor comum de a e $b - na$ e, portanto $c|d$. Logo, $d = mdc(a, b)$. ■

Exemplo 9. Sejam $a = 12$ e $b = 1030$. Determine o máximo divisor comum entre esses números.

$$mdc(12, 1030) = (12, 1030 - 50 \cdot 12) = (12, 1030 - 600) = (12, 430)$$
$$= (12, 430 - 12 \cdot 20) = (12, 430 - 240) = (12, 190)$$
$$= (12, 190 - 12 \cdot 15) = (12, 190 - 180) = (12,10)$$
$$= (12,10) = (10,12) = (10,12 - 10 \cdot 1) = (10,12 - 10) = (10,2) = 2$$

Primeiramente, observamos que a definição 3.2 de máximo divisor comum ao contrário do Lema de Euclides não é construtiva, isto é, não nos fornece um meio prático para determinar o mdc de dois números.

Segundo, ao aplicar o lema 1 para descobrir o mdc entre dois números, vemos que é difícil escolher n, pois ela foi aleatória, observando apenas que $na < b$.

Dependendo de n, teremos um processo longo e cansativo. Sendo assim, usaremos o resultado a seguir que permitirá, com maior rapidez, calcular o mdc entre dois números naturais quaisquer.

3.2.1 Algoritmo de Euclides

Dados $a, b \in \mathbb{N}$, podemos supor que $a \leq b$. Seja $a|b$, $a = 1$ ou $a = b$ como já vimos $mdc(a, b) = a$. Suponhamos então, $1 < a < b$ e que $a \nmid b$. Logo, pela divisão de Euclides, podemos escrever $b = aq_1 + r_1$, com $0 < r_1 < a$.

Temos duas possibilidades:

- $r_1|a$ e, nesse caso, pelo Lema 1

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

e termina o algoritmo, ou

- $r_1 \nmid a$, e podemos dividir a por r_1, obtendo

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

Novamente, temos duas possibilidades:

- $r_2|r_1$, e, novamente pelo Lema 1,

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

e termina o algoritmo, ou

- $r_2 \nmid r_1$ e podemos dividir r_1 por r_2, obtendo

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

Pelo Princípio da Boa Ordenação, este procedimento não pode continuar infinitamente, pois teríamos uma sequência de números naturais $a, r_1, r_2, \ldots$ que não possuiria um menor elemento. Como o resto anterior é sempre menor que o seguinte e escrevendo as desigualdades dos restos $0 \leq r_n \ldots < r_3 < r_2 < r_1 < a$ teremos para algum n que $r_n|r_{n-1}$ e utilizando o Lema de Euclides $mdc(a, b) = mdc(b, r_1) = mdc(r_1, r_2) = \ldots = mdc(r_{n-1}, r_n) = r_n$.

Segundo Hefez (2011) o algoritmo de Euclides pode ser representado do seguinte modo:

	q_1	q_2	q_3	...	q_{n-1}	q_n	
b	a	r_1	r_2	...	r_{n-2}	r_{n-1}	r_n
r_1	r_2	r_3	r_4	...	r_n		

Exemplo 10. Calcular o $\mathrm{mdc}(160{,}58)$

	2	1	3	7	
160	58	44	14	2	
44	14	2			

Observe que, no exemplo, o Algoritmo de Euclides nos fornece os restos de cada divisão:

$$2 = 44 - 14 \cdot 3$$

$$14 = 58 - 44 \cdot 1$$

$$44 = 160 - 58 \cdot 2$$

Se substituirmos cada resto da divisão na expressão seguinte, teremos então, $2 = 44 - 14 \cdot 3 = 44 - 3 \cdot (58 - 44 \cdot 1) = -3 \cdot 58 + 4 \cdot 44 = -3 \cdot 58 + 4 \cdot (160 - 58 \cdot 2) =$ $= 4 \cdot 160 - 11 \cdot 58$. Então, $\mathrm{mdc}(160, 58) = 2 = 4 \cdot 160 - 11 \cdot 58$.

Utilizando o Algoritmo de Euclides de trás para frente conseguimos escrever $\mathrm{mdc}(160{,}58) = 2$ como a soma de um múltiplo de 160 e um múltiplo de 58, isto é, o algoritmo nos fornece uma forma de escrever o mdc entre dois números quaisquer, como a *combinação linear* sobre $\mathbb{Z}$.

Segundo Hefez (2013) quando utilizarmos o Algoritmo de Euclides para expressar $\mathrm{mdc}(a, b) = d$ na forma $ax + by = d$, com $x, y \in \mathbb{Z}$, o chamaremos de *algoritmo de Euclides estendido*. Por ser de grande utilidade em vários momentos nos próximos capítulos, mostraremos este outro método prático para determinar os inteiros x e y.

3.2.2 Algoritmo euclidiano estendido

É possível calcular simultaneamente o $\mathrm{mdc}(a, b)$ e os coeficientes $x, y \in \mathbb{Z}$, da igualdade $\mathrm{mdc}(a, b) = ax + by$, modificando o Algoritmo de Euclides. Segundo Hefez (2013) esse prático algoritmo foi publicado pela primeira vez em 1963.

Suponhamos $a \geq b$. Para calcular o mdc de a e b montamos a matriz

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

Primeiramente, subtraímos da segunda linha q_1 vezes a primeira linha, onde q_1 é o quociente da divisão de a por b, obtendo 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 é o resto da divisão de a por b.

Em seguida, na matriz A_1, subtraímos da primeira linha q_2 vezes a segunda linha, onde q_2 é o quociente da divisão de b por r_1,

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

onde r_2 é o resto da divisão de b por r_1.

O algoritmo prossegue e como o próprio nome indica, o algoritmo euclidiano estendido, é uma extensão do Algoritmo de Euclides para determinação do máximo divisor comum entre dois números, logo como o algoritmo original tem um fim, este também terá. Ao efetuarmos o processo sobre as duas linhas da matriz, teremos no final uma matriz B, que terá uma linha (d, y, x), onde o elemento não nulo da primeira coluna será $d = mdc(a, b)$.

A explicação desse fato é simples se interpretarmos matricialmente as operações sobre as linhas das matrizes obtidas no processo. O que fizemos foi multiplicar uma linha da matriz por um número inteiro. Porém, a linha que devemos multiplicar é aquela que contém o menor número da primeira coluna por um inteiro. Esta linha então é subtraída da outra linha de forma que resulte no menor positivo possível, ou seja, estamos dividindo o maior número da primeira coluna pelo menor e encontramos o resto da divisão. O processo se encerra quando conseguimos zerar a primeira coluna de uma das linhas.

Os valores de x e y aparecem porque, desde da primeira linha estamos escrevendo os restos como combinação linear de a e b. Por exemplo, $r_1 = a - bq_1$ e $r_2 = b - r_1 q_2 = b - (a - bq_1)q_2 = -aq_2 + b(1 + q_1 q_2)$ e, assim por diante, para todos os restos.

Teorema 2 (Teorema de Bézout). Seja $d = mdc(a, b)$, então existem inteiros x e y tais que $ax + by = d$.

Demonstração:

Seja A o conjunto de todos os números inteiros tais que cada elemento seja da seguinte forma: $A(a, b) = \{ax + by, x, y \in \mathbb{Z}\}$. Primeiramente, observemos que esse conjunto A contém números positivos, negativos e também o zero. Vamos escolher

dois números a e b tais que $c = ax + by$ seja o menor inteiro positivo que pertence ao conjunto A, que existe devido ao Princípio da Boa Ordenação.

Suponhamos então que $c \nmid a$. Pelo algoritmo da divisão de Euclides, existem q e r tais que $a = c.q + r$, com $0 < r < c$. Ao reorganizarmos a equação, teremos um $r = a - c.q = a - (a.x + b.y).q = (1 - q.x) \cdot a + (-q.y) \cdot b$. Como $(1 - q.x)$ e $(-q.y)$ são inteiros, $r \in A$, o que é uma contradição, uma vez que $0 < r < c$ e c e o menor inteiro positivo de A. Portanto, $c|a$. Analogamente, conclui – se que também $c|b$.

Como $d|a$ e $d|b$, existem m_1 e m_2 tais que $a = m_1 d$ e $b = m_2 d$. Substituindo a e b na equação $c = ax + by$, teremos $c = m_1 dx + m_2 dy = d(m_1 x + m_2 y)$, implicando que $d|c$. Da proposição 3.4 concluímos que $d \leq c$, sendo os dois números positivos. Como $d = mdc(a, b)$ não é possível que $d < c$. Portanto, $ax + by = d$. ■

Exemplo 11. Calcule $mdc(292,128)$, utilizando o algoritmo estendido de Euclides.

$$\begin{bmatrix} 128 & 1 & 0 \\ 292 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 128 & 1 & 0 \\ 292 - 2 \cdot 128 & 0 - 2 \cdot 1 & 1 - 2 \cdot 0 \end{bmatrix} = \begin{bmatrix} 128 & 1 & 0 \\ 36 & -2 & 1 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 128 - 3 \cdot 36 & 1 - 3 \cdot (-2) & 0 - 3 \cdot 1 \\ 36 & -2 & 1 \end{bmatrix} = \begin{bmatrix} 20 & 7 & -3 \\ 36 & -2 & 1 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 20 & 7 & -3 \\ 36 - 1 \cdot 20 & -2 - 1 \cdot 7 & 1 - 1 \cdot (-3) \end{bmatrix} = \begin{bmatrix} 20 & 7 & -3 \\ 16 & -9 & 4 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 20 - 1 \cdot 16 & 7 - 1 \cdot (-9) & -3 - 1 \cdot 4 \\ 16 & -9 & 4 \end{bmatrix} = \begin{bmatrix} 4 & 16 & -7 \\ 16 & -9 & 4 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 4 & 16 & -7 \\ 16 - 4 \cdot 4 & -9 - 4 \cdot 16 & 4 - 4 \cdot (-7) \end{bmatrix} = \begin{bmatrix} 4 & 16 & -7 \\ 0 & -73 & 32 \end{bmatrix}$$

Portanto, $4 = mdc(292,128) = -7 \cdot 292 + 16 \cdot 128$

Vários dos principais resultados que estudaremos no decorrer do trabalho dependem do conhecimento dos números x, y e por isso, essa mudança do algoritmo de Euclides. Segundo Coutinho (2013) o próprio método de criptografia RSA, que iremos estudar no capítulo 5, não seria possível se não existisse uma maneira eficiente de calcular os valores de x e y. Além disso, o Teorema de Bézout estabelece uma relação entre a adição e multiplicação que permitirá demonstrarmos, entre outros resultados, a proposição a seguir.

Proposição 3.7(Lema de Gauss). Sejam $a, b, c \in \mathbb{Z}$ inteiros tal que $a \neq 0$. Se $a|bc$ e $mdc(a, b) = 1$, então $a|c$.

Demonstração:

Se $a|bc$,então existe $q \in \mathbb{Z}$ tal que $bc = aq$. Sendo o $mdc(a,b) = 1$, pelo Teorema de Bézout, temos que existem $x, y \in \mathbb{Z}$ tais que $mdc(a,b) = 1 = ax + by$. Multiplicando por c ambos os lados da igualdade $c = acx + bcy$. Substituindo bc por aq na igualdade anterior chegamos em $c = acx + aqy = a(cx + qy)$ e, portanto, $a|c$. ■

Voltemos a construção dos números racionais. Com a definição de mdc podemos caracterizar os elementos das classes de equivalência do conjunto como $\frac{\bar{p}}{q}$, tal que, $mdc(p,q) = 1$ para qualquer $p, q \in \mathbb{Z}^*$. Observemos que é suficiente mostrar que cada uma dessas classes de equivalência é tal que $\frac{\bar{p}}{q} = \{\frac{kp}{kq} / k \in \mathbb{Z}^*\}$ e juntamente com $\bar{0} = \{\frac{0}{k} / k \in \mathbb{Z}^*\}$ formam o conjunto $\mathbb{Q}$. Assim:

$\mathbb{Q} = \{\frac{\bar{p}}{q}$, tal que, $p, q \in \mathbb{Z}, q \neq 0, mdc(p,q) = 1\}$.

3.3 Números primos

Definição 3.3. Um número natural $p > 1$ é um *número primo* se, e somente se, 1 e p são seus únicos divisores positivos. Um inteiro maior que 1 e que não é primo é chamado de *composto*, ou seja, se existir um divisor r de n tal que $r \neq 1$ e $r \neq n$ diremos que n é um número composto.

Lema 2. Sejam p e q números primos e a um número inteiro qualquer. Temos que:

(i) Dados p e q primos, se $p|q$, então $p = q$.

Como $p|q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Como, por hipótese, p é primo, temos que $p > 1$, o que nos leva a $p = q$.

(ii) Dados p primo e um número natural a, se $p \nmid a$, então $mdc(p,a) = 1$.

De fato, se $(p,a) = d$, temos que $d|p$ e $d|a$. Logo, como por hipótese, p é primo, temos $d = p$ ou $d = 1$. Mas $d \neq p$, pois $p \nmid a$ e, por consequência, $d = 1$.

Por exemplo, 2, 3 e 5 são números primos. Já os números 9, 10 e 12 são compostos.

Definição 3.4 Dois números inteiros a e b são ditos primos entre si quando $mdc(a,b) = 1$.

Proposição 3.8. Dois inteiros a e b, não nulos $(a \neq 0, b \neq 0)$, são primos entre si se, e somente se, existem inteiros x e y, tais que $ax + by = 1$.

Demonstração:

($\Rightarrow$) Suponha que a e b sejam primos entre si. Logo, $mdc(a,b) = 1$ e, pelo teorema de Bézout, temos que existem $x, y \in \mathbb{Z}$ tais que $ax + by = mdc(a,b) = 1$.

($\Leftarrow$) Suponha que existam $x, y \in \mathbb{Z}$ tais que $ax + by = 1$. Se, $mdc(a,b) = d$, então $d|a$ e $d|b$ e $d|(ax + by)$. Logo, $d|1$, e, portanto, $d = 1$. ■

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

Demonstração:

Observamos que $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$, pois d é um divisor comum de a e b. Se, o $mdc(a,b) = d$ então, pelo teorema de Bézout, existem x e y tais que $ax + by = d$. Dividindo – se a equação por d, temos que $\frac{ax}{d} + \frac{by}{d} = 1$, ou seja, existem inteiros x, y tais que, $\frac{a}{d}x + \frac{b}{d}y = 1$, portanto $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. ■

Proposição 3.9. Sejam $a, b \in \mathbb{Z}$ e p um número primo. Se $p|ab$, então $p|a$ ou $p|b$.

Demonstração

Se $p|a$, nada há que demonstrar. Agora, suponha que $p \nmid a$. Então, pela proposição 3.7, $mdc(p,a) = 1$ e portanto $p|b$. ■

Proposição 3.10: Se $a|c$,$b|c$ e o $mdc(a,b) = 1$, então $ab|c$.

Demonstração

Se a, b dividem c então, existem $m, n \in \mathbb{Z}$ tal que $c = am$ e $c = bn$. Como o $mdc(a,b) = 1$, pela proposição 3.8 teremos $ax + by = 1$, com $x, y \in \mathbb{Z}$. Multiplicando a igualdade por c, encontramos $acx + bcy = c$. Substituindo c nas duas parcelas do 1ºmembro da igualdade $a(bn)x + b(am)y = c \Longrightarrow ab(nx + my)$. Portanto, $ab|c$. ■

Teorema 3: (Teorema Fundamental da Aritmética) Todo número natural $n > 1$ ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como produto de números primos.

Demonstração:

Se n é primo não há o que provar, é só escrever $m = 1, p = n$. Mas, se n for um número composto, então pela definição 3.3 ele possui um divisor p_1, e escrevemos $n = p_1 \cdot n_1$ com $1 < n_1 < n$.

Caso n_1 seja primo, então a igualdade representa n como produto de fatores primos, e se, n_1 é composto, então, pela definição 3.3 possui um divisor primo p_2, isto é, $n_1 = p_2 \cdot n_2$ e $n = p_1 \cdot p_2 \cdot n_2$ com $1 < n_2 < n_1$

Se n_2 é primo, então a igualdade anterior representa n como produto de fatores primos, e se, n_2 é composto, então, pela definição 3.3 possui um divisor primo p_3, isto é, $n_2 = p_3 \cdot n_3$, e $n = p_1 \cdot p_2 \cdot p_3 \cdot n_3$, com $1 < n_3 < n_2$ e assim por diante. Logo, teremos a sequência decrescente $n > n_1 > n_2 > n_3 \ldots > 1$ e como só existe um número finito de inteiros positivos menores que n e maiores que 1, existe necessariamente um p_k que é um número primo, e por consequência:
$n = p_1 \cdot p_2 \cdot p_3 \cdots p_k$ ■

Corolário 2. A decomposição de um número inteiro positivo $a > 1$ como produto de fatores primos é única, a menos de ordem dos fatores.

Teorema 4: Existem infinitos números primos.

Demonstração:

Suponhamos, por absurdo, que exista um número finito de números primos e iremos indica – lo por $P = \{p_1, p_2, p_3 \ldots, p_k\}$ o conjunto de todos esses primos. Considere um número n tal que $n = p_1 \cdot p_2 \ldots p_k + 1$.

Agora, considere p, o menor divisor positivo de n, maior do que 1. Temos que, p é um primo e $n = p \cdot q$, com $q \in \mathbb{Z}$. Segue – se que:

$p_1 \cdot p_2 \cdots p_k + 1 = p \cdot q$

$1 = p \cdot q - p_1 \cdot p_2 \cdots p_k$

Como p pertence a P, pois p é primo, existe $1 \leq n \leq k$ tal que $p = p_n$

$1 = p_n \cdot q - p_1 \cdot p_2 \cdots p_k = p_n \cdot t$, com $t \in \mathbb{Z}$, que significa $p_n | 1$, um absurdo e,

portanto, existem infinitos números primos. ■

Com a descoberta de que existem infinitos números primos, podemos nos perguntar como obter uma lista com números primos até uma determinada ordem. A seguir, veremos um dos mais antigos métodos para elaborar tabelas com números primos, foi elaborado pelo matemático grego Eratóstenes (Hefez), que viveu por volta de 230 anos antes de Cristo. O Crivo[4] de Eratóstenes, como é chamado, permite determinarmos todos os números primos até a ordem que se desejar. Observe que o método não é muito eficiente para ordens muito elevadas. No nosso trabalho, como um exemplo elaboraremos a tabela de todos os números primos inferiores a 100.

Primeiramente, escrevemos em uma tabela todos os números naturais de 2 a 100. Riscaremos todos os números compostos da tabela, seguindo os passos a seguir. Circule o 2 e risque todos os múltiplos de 2 acima de 2, já que nenhum deles é primo. Depois, circule o 3 e risque todos os seus múltiplos. O terceiro número a ser circulado é o 5. Risque todos os múltiplos de 5. Circule o 7 e risque todos os seus múltiplos. Baseado no resultado a seguir, descoberto pelo próprio Eratóstenes, percebemos que nesse caso, não precisaremos prosseguir com o procedimento.

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

Demonstração:

Suponhamos, por absurdo, que n não seja divisível por nenhum número primo p tal que $p^2 \leq n$ e que não seja primo. Seja c o menor número primo que divide n, logo, $n = c \cdot n_1$, com $c \leq n_1$. Segue que $c^2 \leq c \cdot n_1 = n$. Portanto, n é divisível por um número c tal que $c^2 \leq n$, contradizendo a hipótese inicial. ■

Observe, que na tabela a seguir, devemos ir até o primo 7, pois o próximo primo é 11 e pelo lema 3, $11^2 > 100$.

[4] A palavra crivo significa peneira. O método consiste em peneirar os números da tabela e eliminar os que não são primos.

	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~~

Tabela 1 – Crivo de Eratóstenes com números primos menores que 100

O Lema 3 nos fornece um teste de primalidade pois, para verificar se um número n é primo basta ver se não é divisível por nenhum outro primo tal que $p \leq \sqrt{n}$.

Exemplo 13. Mostrar que 197 é um número primo.

Como $15^2 > 197$, devemos testar quais dos números primos menores que 14 são divisores de 197. Temos que:

- $2 \nmid 197$
- $3 \nmid 197$
- $5 \nmid 197$
- $7 \nmid 197$
- $11 \nmid 197$
- $13 \nmid 197$

Portanto, pelo lema 3, 197 é um número primo.

4 Aritmética dos restos

Um dos temas que fazem parte da proposta do nosso trabalho é a Aritmética dos restos e tem como objetivo, no nosso trabalho o amadurecimento dos conceitos que possui a divisão euclidiana nos naturais e inteiros e em especial o resto da divisão.

Se dois ou mais números têm como característica a de possuir o mesmo resto em uma divisão por algum número inteiro dado, é possível estabelecer certas relações entre eles. Por exemplo, os números 19 e 64, deixam resto 4 quando divididos por 5. Agora, somemos a 19 e 64 um número inteiro, por exemplo, o 8. Dividiremos novamente por 5. Teríamos como resultado da soma $19 + 8 = 27$ e $64 + 8 = 72$ e esses dois números quando divididos por 5 deixam o resto 2. Agora, se primeiramente tivéssemos feito a soma $19 + 64 = 83$ e divido por 5 encontraríamos o resto 3 que é o mesmo resto da divisão de 8 por 5.

Estas relações entre os restos de vários números e determinadas operações deu início a um novo tipo de aritmética, que na verdade, segundo Coutinho (2013) é estudada desde as civilizações mais antigas.

Mas, foi com Fermat, Euler e Gauss que esse novo ramo da matemática teve um grande impulso. Foi Carl F. Gauss que sistematizou essa teoria através do seu trabalho intitulado *Disquisitiones arithmeticae,* publicada em 1801 (Coutinho). Gauss, também conhecido como “Príncipe dos matemáticos” nasceu em 1777 e desde muito cedo foi uma criança com grande habilidade matemática.

E, segundo Boyer (1974) *Disquisitiones arithmeticae* é a principal obra responsável por desenvolver a linguagem e notação do ramo da teoria dos números conhecida como aritmética das congruências nos fornecendo um excelente exemplo de classes de equivalência.

4.1 Congruência Módulo n

Antes das principais propriedades, definições e linguagem própria, veremos alguns exemplos práticos, que nos dão breve compreensão do assunto e que podem ser desenvolvidos nas aulas durante o tanto do ensino Fundamental II quanto do ensino Médio.

Comecemos com o relógio analógico de 12 horas. Vemos que 5 horas depois das 10 horas será 3 horas da tarde. Observe que ao somarmos os números e

descobrir o resto depois de dividir por 12, teremos o horário usual. Se aplicarmos o Algoritmo da divisão de Euclides podemos observar que:

$$\begin{array}{r|l} 15 & 12 \\ \hline 3 & 1 \end{array}$$

então, $15 = 12 \cdot 1 + 3$, ou seja, o ponteiro das horas deu uma volta completa no relógio e mais 3 horas.

Agora, se pensarmos em fazer o mesmo, não com as horas, mas com o conjunto dos números inteiros e escolhermos um número inteiro $n > 0$, que será fixo, teremos o que chamamos de *módulo* ou *período*.

No caso do relógio, o número fixo seria o 12, escrevemos a soma feita no nosso exemplo como $5 + 10 \equiv 3\ (\text{módulo } 12)$ e lemos 15 congruente a 3 módulo 12.

Vamos a outro exemplo, mas agora relacionando divisão euclidiana e calendário.

Em 2014, o dia 1º de janeiro, caiu em uma quarta – feira. Supomos que essa fosse a única informação e que gostaríamos de saber em que dia da semana caiu 17 de julho. Primeiramente, montamos uma tabela para a primeira semana do ano de 2014.

Quarta	**Quinta**	**Sexta**	**Sábado**	**Domingo**	**Segunda**	**Terça**
1	**2**	**3**	**4**	**5**	**6**	**7**

Tabela 2 – Numeração da primeira semana de 2014

Vejamos, que estamos diante de outra situação de periodicidade como na questão do relógio analógico.

Segundo, precisamos saber quantos dias existem de 1 de janeiro até 17 de julho.

Janeiro	**Fevereiro**	**Março**	**Abril**	**Maio**	**Junho**	**Julho**	**Total**
31 dias	**28 dias**	**31 dias**	**30 dias**	**31 dias**	**30 dias**	**17 dias**	**198 dias**

Tabela 3 - Quantidade de dias dos meses de janeiro a julho

Agora, dividindo 198 por 7, teremos:

$$\begin{array}{r|l} 198 & 7 \\ \hline 2 & 28 \end{array}$$

Como o dia 2 de janeiro de 2014 foi uma quinta – feira, o 198º desse mesmo

ano também será e todas as demais quinta – feiras deste ano serão ocupados por números que possuem na divisão euclidiana resto 2.

Assim, dizemos que $2, 9, 16, 23, \ldots, 198$ têm a mesma congruência módulo 7, pois deixam o mesmo resto na divisão por 7. Este segundo exemplo é um problema análogo a um relógio que tivesse apenas as posições $1,2,3,4,5,6,7$.

Simbolicamente, poderemos escrever:

$$2 \equiv 9 \equiv 16 \equiv 23 \equiv \cdots \equiv 198 \pmod 7$$

Por fim, podemos aplicar outro conceito, a Progressão Aritmética, aprendido no ensino Médio e relacioná – lo à ideia de congruência. Utilizaremos uma questão da olimpíadas brasileira de matemática das escolas públicas.

(OBMEP–N3F1–2012) Um quadrado de lado $1\,\text{cm}$ roda em torno de um quadrado de lado 2cm, como na figura, partindo da posição inicial e completando um giro cada vez que um de seus lados fica apoiado em um lado do quadrado maior.

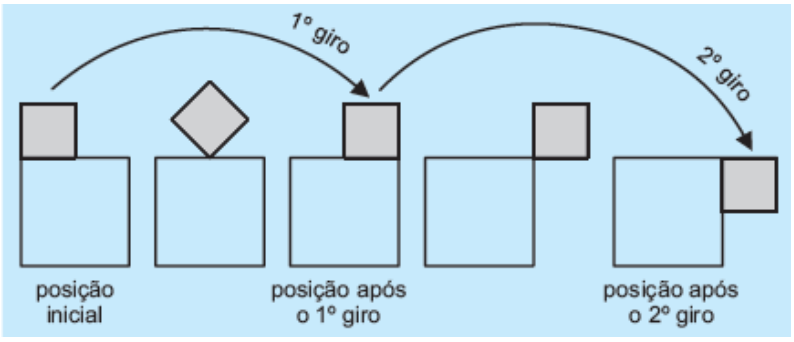

Figura 4 - Posições do quadrado de lado 1cm

Qual das figuras a seguir representa a posição dos dois quadrados após 2012º giro?

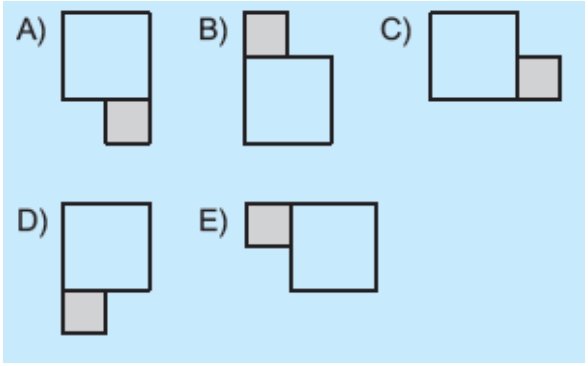

Figura 5 - Alternativas da questão sobre o giro do quadrado

Uma das formas de resolver esse exercício seria ir contando os giros até que aparecesse a 2012º posição. Convenhamos que a solução não seria tão prática e muito menos rápida.

Atentamente, verificamos que as posições se repetem a cada oito giros

sucessivos e essa periocidade faz com que os giros formem uma progressão aritmética de razão 8, isto é, aumentam de oito em oito. Agora, para facilitar o entendimento, vamos relacionar uma determinada posição a um número. A posição inicial seria 0, após o 1ºgiro seria a posição 1, após o 2ºgiro a posição 2 e, assim sucessivamente. Então, após o 7ºgiro, o quadrado menor volta para a posição inicial e o ciclo se repete. Veja o que acontece:

Posições	Posição inicial	Posição 1	Posição 2	Posição 3	Posição 4	Posição 5	Posição 6	Posição 7
	0	1	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
	...	...	...	...	...	...	...	...

Tabela 4 - Números das posições dos quadrados menores

Vejamos que a posição inicial corresponde aos números múltiplo de 8, isto é, números que divididos por 8 deixam resto zero $(8 \cdot n$, com $n \in \mathbb{N})$.

Se relacionarmos com progressão aritmética, teríamos na coluna posição inicial, uma PA de razão 8 e 1ºtermo igual a 0. A posição 1 corresponde aos números que são múltiplos de 8, mais 1, isto é, números que divididos por 8 deixam resto 1 $(8 \cdot n + 1$, com $n \in \mathbb{N})$ e assim mantemos a lógica até a coluna posição 7, definida por uma PA de razão 8 e 1º termo igual a 7.

Verifique que precisamos dividir 2012 por 8 (razão da PA), obter o resto (1ºtermo) e ver qual coluna faz parte. Temos que: $2012 = 8 \cdot 251 + 4$. Logo, após 2012ª posição, o quadrado menor terá dado 251 voltas completas no quadrado maior e mais 4 giros, parando na posição que corresponde a alternativa A.

Todos os números que estão na mesma coluna, tem uma particularidade, deixam o mesmo resto ao serem divididos por 8 e como já vimos, chamamos de congruentes módulo 8. No exemplo, podemos dizer que 2 e 26 são congruentes módulo 8, pois os dois números deixam resto 2, quando divididos por 8. Simbolicamente, podemos escrever: $26 \equiv 2 \pmod 8$.

Os exemplos anteriores nos mostram algumas situações (que envolvem repetições periódicas) onde se faz presente a noção de congruência e que estão relacionadas com os conteúdos que professores e estudantes de ensino Médio possuem familiaridade.

4.2 Definições e propriedades.

Definição 4.1 Sejam $a, b, n \in \mathbb{Z}$ tal que $n > 0$. Dois números a e b serão congruentes módulo n se, e somente se, a e b possuir o mesmo resto na divisão por n. Escreveremos $a \equiv b \pmod{n}$. Quando a e b não são congruentes módulo n, utilizamos a notação $a \not\equiv b \pmod{n}$.

Por exemplo, $11 \equiv 3 \pmod{2}$, já que os restos da divisão de 11 e 3 por 2 são iguais a 1. Já $15 \not\equiv 7 \pmod{6}$, pois 15 e 7 não deixam o mesmo resto quando divididos por 6.

Proposição 4.1 Dois números $a, b \in \mathbb{N}$ serão congruentes módulo n, com $n > 0$ se, e somente se, $n|a - b$.

Demonstração

($\Longrightarrow$) Se $a \equiv b \pmod{n}$ então $n|a - b$.

Pela hipótese, a e b são congruentes módulo n. Então, utilizando o Algoritmo de Euclides, eles possuem o mesmo resto na divisão por n, ou seja, existem q_1 e q_2 inteiros tais que $a = n \cdot q_1 + r$, com $0 \leq r < n$ e $b = n \cdot q_2 + r$, com $0 \leq r < n$. Se Subtrairmos a e b, temos $a - b = n \cdot (q_1 - q_2) + (r - r) = n \cdot (q_1 - q_2)$. Como $q_1 - q_2$ é um número inteiro, então $n|a - b$.

($\Longleftarrow$) Se $n|a - b$ então a e b são congruentes módulo n.

Dividindo a e b por n, temos pelo Algoritmo de Euclides, que existem e são únicos q_1, q_2, r_1, r_2 tais que:

(i) $a = n \cdot q_1 + r_1$, com $0 \leq r_1 < n$

(ii) $b = n \cdot q_2 + r_2$, com $0 \leq r_2 < n$

Ao subtrairmos membro a membro (i) de (ii), $a - b = n \cdot (q_1 - q_2) + (r_1 - r_2)$ com $0 \leq |r_1 - r_2| < n$. Como $n|a - b$, temos que $n|r_1 - r_2$ e daí $r_1 = r_2$.

Logo, a e b deixam o mesmo resto r na divisão por n, ou seja, $a \equiv b \pmod{n}$.

■

Exemplo 1. Temos que $32 \equiv 12 \pmod{5}$, pois $5|32 - 12 = 20$. Mas, $79 \not\equiv 8 \pmod{4}$ já que $4 \nmid 79 - 8 = 71$.

Veremos que a definição 4.1 estabelece que a congruência módulo um número inteiro n é uma relação de equivalência.

Proposição 4.2 Sejam $a, b, c \in \mathbb{Z}$ e $n \in \mathbb{N}$, com $n > 0$. Temos que:

(i) **(reflexiva):** todo número é congruente módulo n a si mesmo, ou seja, $a \equiv a \pmod{n}$;

(ii) **(simétrica):** se $a \equiv b \pmod{n}$, então $b \equiv a \pmod{n}$;

(iii) **(transitiva):** se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então $a \equiv c \pmod{n}$;

Demonstração

(i) Sabemos que $a|0$, pois utilizando a proposição 4.1 teremos que $a|(a - a)$. Logo, $a \equiv a \pmod{n}$.

(ii) Pela definição de congruência se $a \equiv b \pmod{n}$ então, $a - b = q \cdot n$ com $q \in \mathbb{Z}$. Logo, $b - a = -(q \cdot n) = (-q) \cdot n \Longrightarrow b \equiv a \pmod{n}$.

(iii) Se $a \equiv b \pmod{n}$ e se $b \equiv c \pmod{n}$, existem $q_1, q_2 \in \mathbb{Z}$ tais que $a - b = q_1 \cdot n$ e $b - c = q_2 \cdot n$. Ao somarmos as duas congruências membro a membro, teríamos $a - b + b - c = q_1 \cdot n + q_2 \cdot n \Longrightarrow a - c = n \cdot (q_1 + q_2)$.Logo, $a \equiv c \pmod{n}$ ■

Com as definições e propriedades vistas, podemos escrever muitos exemplos de congruência. Exemplos: $61 \equiv 41 \pmod{5}$ e $113 \equiv 53 \pmod{5}$. Se somarmos as duas congruências obtemos $61 + 113 \equiv 41 + 53 \pmod{5}$ e $174 \equiv 94 \pmod{5}$ é verdadeira pois, pela definição, $174 - 94 = 80 = 5 \cdot 10$.

Proposição 4.3. Sejam $a, b, c, d \in \mathbb{Z}$ e $n \in \mathbb{N}$, com $n > 0$

Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então $a + c \equiv b + d \pmod{n}$;

Demonstração

Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, existem $q_1, q_2 \in \mathbb{Z}$ tais que $a - b = q_1 \cdot n$ e $c - d = q_2 \cdot n$. Agora, somando cada igualdade membro a membro, teríamos como resultado $a - b + c - d = q_1 \cdot n + q_2 \cdot n \Longrightarrow a + c - (b + d) = n \cdot (q_1 + q_2)$ e, portanto, $a + c \equiv b + d \pmod{n}$ ■

Da mesma forma, podemos provar outras propriedades, que nos apoiará nos estudos sobre congruência e outros que virão no decorrer do trabalho.

Proposição 4.4. Sejam $a, b, c, d \in \mathbb{Z}$ e $n \in \mathbb{N}$, com $n > 0$.

(i) Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então $a \cdot c \equiv b \cdot d \pmod{n}$;

(ii) Se $a + c \equiv b + c \pmod{n} \Leftrightarrow a \equiv b \pmod{n}$;

(iii) Sejam $a \equiv b \pmod{n}$ e $k > 0$ então $a^k \equiv b^k \pmod{n}$;

(iv) Se $ab \equiv ac \pmod{n}$ e $mdc(a, n) = 1$ então $b \equiv c \pmod{n}$;

Demonstração

(i) Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, existem $q_1, q_2 \in \mathbb{Z}$ tais que $a - b = q_1 \cdot n$ e $c - d = q_2 \cdot n$. Reorganizando as equações algebricamente, temos:

$$ac = (b + q_1 n)(d + q_2 n) \Longrightarrow ac = bd + bq_2 n + dq_1 n + q_1 n q_2 n \Longrightarrow ac - bd = n(bq_2 + dq_1 + q_1 q_2 n)$$

e, portanto $ac \equiv bd \pmod{n}$.

(ii) ($\Longrightarrow$) Se $a + c \equiv b + c \pmod{n}$, então $m | b + c - (a + c)$, o que implica em $m | b - a$ e, por consequência $b \equiv a \pmod{n}$ e pelo item (ii), desta proposição, $a \equiv b \pmod{n}$.

($\Longleftarrow$) Se $a \equiv b \pmod{n}$, pela proposição 4.3 temos que $a + c \equiv b + c \pmod{n}$, pois sabemos através da proposição 4.2 (item i) que $c \equiv c \pmod{n}$

(iii) Suponhamos que $a \equiv b \pmod{n}$. Aplicando a proposição 4.4 (item i) k vezes, temos:

$$k \text{ vezes } a \equiv b \pmod{n} \begin{cases} a \equiv b \pmod{n} \\ a \equiv b \pmod{n} \\ a \equiv b \pmod{n} \\ a \equiv b \pmod{n} \\ \vdots \\ a \equiv b \pmod{n} \end{cases} \Longrightarrow a^k \equiv b^k \pmod{n}$$

(iv) Suponhamos que $ab \equiv ac \pmod{n}$. Temos que, $n | ab - ac = a \cdot (b - c)$. Como, por hipótese, $mdc(a, n) = 1 \Longrightarrow n | b - c$. Portanto $b \equiv c \pmod{n}$. ■

Observe que nesse capítulo, o conteúdo visto não é um algo novo em Matemática, mas uma notação diferente para determinados tópicos que já são conhecidos no Ensino Médio. No caso, congruência, é uma forma diferente de escrever o Algoritmo de Euclides. E ainda, se notarmos, as propriedades da divisibilidade são as mesmas de congruência, porém com outra forma de escrita.

Já sabemos que ao dividirmos um número $x \in \mathbb{Z}$ por 5, os únicos restos possíveis são 0,1, 2, 3 e 4. Além disso, vimos anteriormente que dado dois números, eles serão congruentes se possuem o mesmo resto. Vamos multiplicar por um número relativamente primo com 5, por exemplo 7, apenas pelos restos não nulos, ou seja, $7 \cdot (1)$, $7 \cdot (2)$, $7 \cdot (3)$, $7 \cdot (4)$, encontrando $7, 14, 21, 28$. Se tomarmos cada

um dos elementos desta nova sequência no módulo 5, teremos $7 \equiv 2 \pmod 5$, $14 \equiv 4 \pmod 5$, $21 \equiv 1 \pmod 5$ e $28 \equiv 3 \pmod 5$, isto é, determinamos os mesmos restos da divisão por 5 em ordem diferente.

Utilizando a proposição 4.4 (item i), temos $7 \cdot 14 \cdot 21 \cdot 28 \equiv 2 \cdot 4 \cdot 1 \cdot 3 \pmod 5$, ou ainda $7 \cdot (1) \cdot 7 \cdot (2) \cdot 7 \cdot (3) \cdot 7 \cdot 4 \equiv 2 \cdot 4 \cdot 1 \cdot 3 \pmod 5$. Reorganizando o primeiro membro da última congruência através de uma das propriedades da potenciação, temos que $7^4 \cdot (1 \cdot 2 \cdot 3 \cdot 4) \equiv 1 \cdot 2 \cdot 3 \cdot 4 \pmod 5$. Como o produto $1 \cdot 2 \cdot 3 \cdot 4 = 24$ é relativamente primo com 5, utilizando a proposição 4.4 (item iv) podemos escrever $7^4 \equiv 1 \pmod 5$.

Observando mais atentamente, independente do número a relativamente primo com o módulo p escolhido, sempre aparecerá o resultado a elevado a $p - 1$ congruente 1 módulo p.

Na verdade, essa afirmação é um corolário de um dos um dos teoremas fundamentais do nosso trabalho. Porém, antes faremos alguns comentários pertinentes que estão relacionados com a prova da nossa afirmação.

Muitos são os conceitos matemáticos que aprendemos durante o ensino Médio e destes, alguns são vistos rapidamente apenas com exemplos e exercícios práticos, sem um aprofundamento. Isso acontece algumas vezes devido ao tempo e a quantidade de conteúdo que o professor lecionar durante o ano letivo e, em outras, da dificuldade do professor com o próprio tema que ele precisa abordar.

E dois desses temas, a indução finita e o binômio de Newton, que quase não são estudados no ensino Médio auxiliam em uma das demonstrações do Teorema da afirmação anterior, que chamaremos de Pequeno Teorema de Fermat. Esses temas na maioria dos livros didáticos vêm apenas com exemplos práticos e depois exercícios de fixação.

Por esse motivo, no nosso trabalho, utilizamos uma estratégia diferente da que estamos acostumados a ver, se analisarmos diversos livros de teoria dos números. Procuramos um exemplo que chegasse a afirmação anterior pois, resolvê – lo depende apenas da divisão de Euclides (que implicitamente está relacionado a um conceito que veremos mais adiante, o *sistema completo de resíduos*) e a propriedade dos números primos.

A cronologia do teorema foi invertida devido a defasagem da habilidade de demonstração que utiliza a indução finita e conceitos do binômio de Newton. Mas em nenhum momento, o fato ocorrido impede de entendermos o teorema e seu corolário. Voltando ao exemplo, demonstraremos a afirmação anterior, que damos o

nome de *Pequeno Teorema de Fermat*.

Teorema 1. (Pequeno Teorema de Fermat). Seja p primo e $a \in \mathbb{Z}$. Se $\text{mdc}(p, a) = 1$ então $a^{p-1} \equiv 1 \pmod{p}$.

Demonstração:

Seja o conjunto de todos os restos possíveis da divisão de a por p, que são $1, 2, 3, \ldots, p-1$. Se multiplicarmos cada um dos restos da divisão por a, teremos a sequência $a \cdot 1, a \cdot 2, a \cdot 3, \ldots, a \cdot (p-1)$.Digamos então que r_1 seja o resto da divisão de $a \cdot 1$ por p, r_2 o resto de $a \cdot 2$ por p, r_3 o resto de $a \cdot 3$ por p e, assim por diante, até r_{p-1} o resto de $a \cdot (p-1)$ por p.

Se escrevermos cada divisão através de congruência, temos:

$r_1 \equiv a \cdot 1 \pmod{p}$

$r_2 \equiv a \cdot 2 \pmod{p}$

$\vdots \quad \vdots$

$r_{p-1} \equiv a \cdot (p-1) \pmod{p}$

Ao aplicarmos a proposição 4.4 (item i), $p-1$ vezes, podemos obter $r_1 \cdot r_2 \cdot r_3 \cdots r_{p-1} \equiv (a \cdot 1) \cdot (a \cdot 2) \cdot (a \cdot 3) \cdots \big(a \cdot (p-1)\big) (\text{mod } p)$. Agora se utilizarmos a propriedade da potenciação produto de mesma base, onde multiplicando potências que possuem a mesma base, podemos somar os expoentes em a, podemos escrever $r_1 \cdot r_2 \cdot r_3 \cdots r_{p-1} \equiv a^{p-1}\big(1 \cdot 2 \cdot 3 \cdots (p-1)\big)$. Como o produto $\big(1 \cdot 2 \cdot 3 \cdots (p-1)\big)$e p são relativamente primos, pela proposição 4.4 (iv), $a^{p-1} \equiv 1 \pmod{p}$. ■

Exemplo 2. Calcule o resto da divisão de 4^{363} por 41.

Sem a utilização do teorema de Fermat, teríamos um trabalho árduo para calcular tal resto. Porém, pelo Teorema de Fermat, temos que $4^{40} \equiv 1 \pmod{41}$. Utilizando a proposição 4.4 (item iii) escrevemos $(4^{40})^9 \equiv 1^9 \pmod{41}$. Sabemos que pela proposição 4.2 (item i) $4^3 \equiv 4^3 \pmod{41}$. Agora, a proposição 4.4 (item i) nos garante que $(4^{40})^9 \cdot 4^3 \equiv 1^9 \cdot 4^3 \pmod{41}$ .Com as propriedades da potenciação, teremos $4^{360} \cdot 4^3 = 4^{363} \equiv 1^9 \cdot 64 \pmod{41} \equiv 64 \equiv 23 \pmod{41}$. Logo, o resto da divisão de 4^{363} por 41 será 23.

Corolário 1. Se p é primo, então $a^p \equiv a \pmod{p}$, qualquer que seja o inteiro a.

Demonstração

Se $p|a$, então $a \equiv 0 \pmod{p}$. Pela proposição 4.4 (item iii), $a^p \equiv 0 \pmod{p}$. Logo, $a^p \equiv a \pmod{p}$.

Mas ao invés disto, $p \nmid a$, pelo Pequeno Teorema de Fermat $a^{p-1} \equiv 1 \pmod{p}$. Reescrevendo o Teorema $a^p \cdot a^{-1} \equiv 1 \pmod{p}$. Então, multiplicando por os dois membros da congruência por a, $a^p \equiv a \pmod{p}$. ■

O Pequeno Teorema de Fermat nos auxiliará nos cálculos onde os expoentes são muito grandes. Porém, como vimos o teorema nos mostra que p deve ser um número primo. Mas, e se quiséssemos calcular o resto da divisão de 122^{157} por 161, que não é primo, já que $161 = 23 \cdot 7$. Como faríamos? O resultado veremos na próxima seção, mas primeiramente apresentaremos algumas definições e proposições que auxiliam na demonstração do resultado principal do tópico a seguir.

4.3 Sistema completo de resíduos

Definição 4.2. Chama – se sistema completo de resíduos módulo n a todo conjunto de n números inteiros nos quais os restos pela divisão por n são os números $0, 1, 2, \ldots, n-1$, sem repetição e sem ordem. Vemos que um sistema completo de resíduos módulo n possui n elementos.

Assim, se $a_1, \ldots, a_n \in \mathbb{Z}$, são não congruentes módulo n, dois a dois, então eles formam um sistema completo de resíduos módulo n.

Exemplo 3. Congruência módulo 3.

O conjunto $\{0,1,2\}$ forma um sistema completo de resíduos módulo 3. Agora, observe o conjunto $\{-7, 4, 9\}$. Ele é tal que:

$-7 \equiv 2 \pmod{3}$

$4 \equiv 1 \pmod{3}$

$9 \equiv 0 \pmod{3}$

Portanto, $\{-7, 4, 9\}$ também é um sistema completo de resíduos módulo 3.

Proposição 4.5. Sejam $a, m, n \in \mathbb{Z}$, com $n > 1$ e $mdc(m, n) = 1$. Se $a_1, \ldots, a_n$ é um sistema completo de resíduos modulo n, então $a + ma_1, \ldots, a + ma_n$ também é um sistema completo de resíduos módulo n.

Demonstração:

Da definição 4.2, para determinados $i, j = 0, \ldots, n-1$, temos a seguinte congruência: $a + ma_j \equiv a + ma_i \pmod{n} \Leftrightarrow ma_j \equiv ma_i \pmod{n}$. Pela proposição, 4.2 (item ii), temos que $a_j \equiv a_i \pmod{n} \Leftrightarrow i = j$.

Assim, vemos que $a + ma_1, \ldots, a + ma_n$ são, dois a dois, não congruentes módulo n e formam um sistema completo de resíduos módulo n. ■

Agora, considere os exemplos:

Exemplo 4. Seja o conjunto $A = \{0,1,2,\ldots,10\}$, o conjunto do sistema completo de resíduos módulo 11. Para todo número $x \neq 0$, podemos admitir a propriedade na qual existe no mesmo conjunto A um número y, tal que $x \cdot y \equiv 1 \pmod{11}$, isto é, existe um $k \in \mathbb{Z}$ tal que $x \cdot y + 1 = 11 \cdot k$ ou $x \cdot y - 11 \cdot k = 1$. Exemplo, $5 \cdot 9 = 45 \equiv 1 \pmod{11}$ e $4 \cdot 3 = 12 \equiv 1 \pmod{11}$. Quando isto acontece, dizemos que 5 e 9 ou 4 e 3 são *inversos multiplicativos* módulo 11. Listando em uma tabela todos os números do conjunto com essa propriedade, teremos:

X	1	2	3	4	5	6	7	8	9	10
Y	1	6	4	3	9	2	8	7	5	10

Tabela 5 - Resíduos módulo 11

Embora exista uma forma de encontrar inversos, ela é trabalhosa para aplicá – la em um número pequeno. Por isso, determinamos esses números por tentativa. Assim, para encontrar o inverso multiplicativo de 4 módulo 7, multiplicamos por 4 todos os inteiros maiores que 2, até que achemos congruência desejada. Assim, teremos, $4 \cdot 1 = 4 \not\equiv 1 \pmod{11}$; $4 \cdot 2 = 8 \not\equiv 1 \pmod{11}$; $4 \cdot 3 = 12 \equiv 1 \pmod{11}$ e obtemos o inverso procurado.

Mas, podemos ir além da tentativa para descobrir os inversos, pois se os inteiros estão entre 1 e $n - 1$, cada um possui exatamente um inverso nesse intervalo.

Suponhamos que y' e y'' são inversos multiplicativos de x módulo n, entre 1 e $n - 1$. Logo, $x \cdot y' \equiv 1 \pmod{n}$ e $x \cdot y'' \equiv 1 \pmod{n}$. Então, chegamos a conclusão que $y'' \cdot (x \cdot y') \equiv y'' \cdot 1 \equiv y'' \pmod{n}$. Como estamos apenas multiplicando os termos em cada membro da congruência, podemos mudar a posição dos parênteses em cada um deles e teremos $(y'' \cdot x) \cdot x' \equiv 1 \cdot y' \pmod{11}$ e isso não altera o resultado da operação. Portanto, $y' \equiv y'' \pmod{n}$.

Isto significa que $y' - y''$ é divisível por n e, como, y' e y'' são menores que n, a única forma da diferença ser múltiplo de n é se for igual a zero, ou seja, $y' = y''$.

Voltando ao exemplo, como 5 e 9 são inversos um do outro módulo 11, não podem ser inversos de 4 módulo 11. Assim, procuramos pelo inverso de 4 entre os números $2, 3, 4, 6, 7, 8, 10$. Como vemos, quanto mais inversos encontramos, mais rápido completamos a tabela.

Definição 4.3. A congruência $x \cdot y \equiv 1 \pmod{n}$ admite solução módulo n. Esta solução será chamada de inverso multiplicativo de x módulo n.

Exemplo 5. Agora, sendo $B = \{0,1,2,3,4,5\}$ o conjunto que representa o sistema completo de resíduos módulo 6, vamos construir uma tabela para esse conjunto, começando pelo $1 \equiv 1 \pmod{6}$. Depois, $2 \cdot 2 = 4 \not\equiv 1 \pmod{6}$; $2 \cdot 3 = 0 \not\equiv 1 \pmod{6}$; $2 \cdot 4 = 8 \not\equiv 1 \pmod{6}$ e, por último, $2 \cdot 5 = 10 \not\equiv 1 \pmod{6}$. Assim, descobrirmos que o número 2 não possui inverso multiplicativo no módulo 6, ou seja, o conjunto não possui a propriedade descrita anteriormente, pois alguns elementos do conjunto, por exemplo o 2, não possui y tal que $2 \cdot y \equiv 1 \pmod{6}$. A seguir, temos a tabela completa dos inversos módulo 6.

X(Resíduos)	1	2	3	4	5
Y(Inverso módulo 6)	1	-	-	-	5

Tabela 6 - Resíduos módulo 6

O traço que aparece na coluna Y indica que o elemento não admite inverso módulo 6. Assim, $2,3$ e 4 não possuem inverso módulo 6. Além disso, cada um dos elementos que tem inverso módulo 6 é seu próprio inverso.

Voltando aos exemplos e suas respectivas tabelas, podemos ver que os sistemas completos de resíduos que utilizamos foram números de baixo valor e então conseguimos calcular por tentativa cada um dos inversos. Mas se quiséssemos obter os inversos multiplicativos módulo 101 ou 503? Será que existe alguma regularidade que nos permita determinar os elementos que possuem inversos e quais não possuem inverso módulo n? A primeira observação que podemos realizar é que nos parece, pelos exemplos, que todos os resíduos do módulo n sendo n ímpar têm inverso ao passo que, n par, nem todos possuem. Vejamos o que ocorre com outros módulos, por exemplo, módulo 4 e 8, montando suas respectivas tabelas.

X(Resíduos)	1	2	3
Y(Inverso módulo 4)	1	-	3

Tabela 7 - Resíduos módulo 4

X(Resíduos)	1	2	3	4	5	6	7	8
Y(Inverso módulo 9)	1	5	-	7	2	-	4	8

Tabela 8 - Resíduos módulo 9

A regularidade que supomos não é correta, pois para $n = 9$, nem todos os resíduos possuem inversos. Voltando a definição sabemos que um inteiro x tem inverso módulo n se existir y tal que $x \cdot y \equiv 1 \pmod{n}$. Com um olhar mais atento nas tabelas e nos seus números vemos que existe inverso quando não existem fatores primos comuns entre os números x e n. Em outras palavras, só existe inverso multiplicativo quando x e n são primos entre si.

Proposição 4.6. Sejam $x, n \in \mathbb{N}$, com $n > 1$. Existe um y tal que $x \cdot y \equiv 1 \pmod{n}$, isto é, x admite inverso multiplicativo módulo n, se e somente se, $mdc(x, n) = 1$.

Demonstração:

($\Longrightarrow$) Se x possui inverso multiplicativo, existe y tal que $x \cdot y \equiv 1 \pmod{n}$. Logo, existe um k tal que $x \cdot y - 1 = n \cdot k$ e podemos escrever $x \cdot y + n \cdot k = 1$ e pela proposição 3.8 $mdc(x, n) = 1$

($\Longleftarrow$) Se $mdc(x, n) = 1$, pelo Teorema de Bézout, existem inteiros y e k tal que $x \cdot y + n \cdot k = mdc(x, n)$, o que nos permite escrever $x \cdot y = 1 - n \cdot k = 1 + (-k) \cdot n$, isto é, $x \cdot y \equiv 1 \pmod{n}$. ■

Exemplo 6. Vamos construir a tabela do $x \cdot y \equiv 1 \ (mod\ 8)$

·	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

Tabela 9 – Inverso módulo 8

Para montar a tabela multiplicamos um número da primeira coluna por um número da primeira linha e escrevemos o resultado da divisão do produto por 8. Exemplo, o produto $5 \cdot 7 = 35$ e $35 = 8 \cdot 4 + 3$. Então, na posição do produto $5 \cdot 7$

temos o número 3. Por ser multiplicativa, a tabela está escrita com o sistema completo módulo 8,isto é, a tabela de todos os restos possíveis de uma divisão por 8. Logo, a posição onde resulta 1, que marcamos de vermelho, indica os pares de inversos multiplicativos módulo 8.

Podem ocorrer casos cuja tabela não é realizável, por exemplo, qual o inverso multiplicativo de 210 módulo 503, ou seja, $210 \cdot x \equiv 1\ (mod\ 503)$? Nesses casos, usamos o algoritmo estendido de Euclides.

$$\begin{bmatrix} 210 & 1 & 0 \\ 503 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 210 & 1 & 0 \\ 503-2\cdot 210 & 0-2\cdot 1 & 1-2\cdot 0 \end{bmatrix} = \begin{bmatrix} 210 & 1 & 0 \\ 83 & -2 & 1 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 210-2\cdot 83 & 1-2\cdot(-2) & 0-2\cdot 1 \\ 83 & -2 & 1 \end{bmatrix} = \begin{bmatrix} 44 & 5 & -2 \\ 83 & -2 & 1 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 44 & 5 & -2 \\ 83-44\cdot 1 & -2-1\cdot 5 & 1-1\cdot(-2) \end{bmatrix} = \begin{bmatrix} 44 & 5 & -2 \\ 39 & -7 & 3 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 44-1\cdot 39 & 5-1\cdot(-7) & -2-1\cdot 3 \\ 39 & -7 & 3 \end{bmatrix} = \begin{bmatrix} 5 & 12 & -5 \\ 39 & -7 & 3 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 5 & 12 & -5 \\ 39-7\cdot 5 & -7-7\cdot 12 & 3-7\cdot(-5) \end{bmatrix} = \begin{bmatrix} 5 & 12 & -5 \\ 4 & -91 & 38 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 5-1\cdot 4 & 12-1\cdot(-91) & -5-1\cdot 38 \\ 4 & -91 & 46 \end{bmatrix} = \begin{bmatrix} 1 & 103 & -43 \\ 4 & -91 & 46 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 1 & 103 & -43 \\ 4-4\cdot 1 & -91-4\cdot 103 & 46-4\cdot(-43) \end{bmatrix} = \begin{bmatrix} 1 & 103 & -43 \\ 0 & -503 & 218 \end{bmatrix}$$

Segue – se que $103 \cdot 210 + 503 \cdot (-43) = 1$. Assim, $210 \cdot 103 \equiv 1\ (\mathrm{mod}\ 503)$. Podemos verificar se os cálculos estão corretos através da divisão de Euclides. Temos que $210 \cdot 103 - 1 = 21629$ e $21629 : 503 = 43$.

Retomando as tabelas anteriores, observe que cada sistema completo de resíduos possui um número m de inteiros inversos. O sistema completo de resíduos módulo 11 possui 10 elementos. Já no sistema módulo 6 há 2 elementos.

Como vimos cada número possui um único inverso módulo n então, podemos fazer uma correspondência biunívoca e assim obter o número de elementos de um sistema de resíduos módulo n, que corresponde à quantidade de números naturais entre 0 e $\mathrm{n} - 1$ que são primos com n.

Definição 4.4. A função $\varphi: \mathbb{N}^* \longrightarrow \mathbb{N}$, que associa a cada $\mathrm{n} \in \mathbb{N}$ o número de elementos do conjunto $\{\mathrm{m} \in \mathbb{N}^*$ tal que $1 \leq \mathrm{m} \leq \mathrm{n}$ e $\mathrm{mdc}\,(\mathrm{m}, \mathrm{n}) = 1\}$ é chamada função (φ) fi de Euler.

Por exemplo $\varphi(9) = 6$ porque, no sistema completo de resíduos módulo 9, os números primos com 9 formam o conjunto $\{1,2,4,5,7,8\}$.

Definição 4.5. Um sistema reduzido de resíduos módulo n é um conjunto de $\varphi(n)$ inteiros $r_1, r_2, \dots, r_{\varphi(n)}$, tais que cada elemento do conjunto é relativamente primo com n, e se $i \neq j$, então $r_i \not\equiv r_j \pmod{n}$.

Podemos obter um sistema reduzido de resíduos $r_1, r_2, \dots, r_n$ módulo n, a partir de um sistema completo qualquer de resíduos $a_1, a_2, \dots, a_n$ módulo n excluindo os elementos a_i, com $i = 1,2 \dots, n$ que não são primos com n.

Exemplo 7. O conjunto $\{0,1,2,3,4,5,6,7,8\}$ representa um sistema completo de resíduos módulo 9. Logo, o conjunto $\{1, 2, 4, 5, 7, 8\}$ é um sistema de resíduos módulo 9 porque, todos os elementos do conjunto são relativamente primos com 9.

Proposição 4.7. Seja $r_1, r_2, \dots, r_{\varphi(n)}$ um sistema reduzido de resíduos módulo n e seja $a \in \mathbb{N}$ tal que $\text{mdc}(a, n) = 1$. Então, $ar_1, ar_2, \dots, ar_{\varphi(n)}$ também é um sistema reduzido de resíduos módulo n.

Demonstração

Seja $a_1, a_2, \dots, a_n$ um sistema completo de resíduos módulo n do qual foi retirado o sistema reduzido de resíduos $r_1, r_2, \dots, r_{\varphi(n)}$. Podemos observar que $\text{mdc}(ar_i, n) = 1$, para $i = 1,2,3 \dots, \varphi(n)$. Vejamos que no conjunto $\{ar_1, ar_2, \dots, ar_{\varphi(n)}\}$, não existem dois elementos congruentes módulo $\varphi(n)$. De fato, $ar_1 \equiv ar_2 \pmod{\varphi(n)}$ pelo fato de a ser relativamente primo com $\varphi(n)$, teríamos $r_1 \equiv r_2 \pmod{\varphi(n)}$, que é uma contradição. Temos então $\varphi(n)$ inteiros, primos com n e não congruentes dois a dois módulo $\varphi(n)$, pois contém representantes de todas as classes de congruência módulo n cujos elementos são primos com n. ■

Por exemplo, vimos anteriormente que o conjunto $\{1, 2, 4, 5, 7, 8\}$ é um sistema reduzido de resíduos módulo 9. Multiplicando os restos por 4, pois $\text{mdc}(4,9) = 1$ obteremos o conjunto $\{4,8,16,20,28,32\}$. Calculando módulo 9, temos $\{4,8,7,2,1,5\}$ que é o primeiro conjunto com outra ordem e deve ser assim pois, conforme ficou comprovado acima, ao multiplicarmos todos os elementos do sistema reduzido de restos por um número relativamente primo com o módulo, os produtos são incongruentes, e portanto iguais a um dos elementos $\{1, 2, 4, 5, 7, 8\}$.

Teorema 2. (Teorema de Euler). Sejam $a, n \in \mathbb{Z}$ com $n > 1$ e $\text{mdc}(a, n) = 1$, então $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Demonstração:

Seja $r_1, r_2 \ldots, r_{\varphi(n)}$ um sistema reduzido de resíduos módulo n. Se multiplicarmos o sistema por a, teremos através da proposição 4.2, que $ar_1, ar_2, \ldots, ar_{\varphi(n)}$ formam um novo sistema reduzido de resíduos módulo n. Logo, $ar_1 \cdot ar_2 \cdots ar_{\varphi(n)} = a^{\varphi(n)}\left(r_1 \cdot r_2 \cdots r_{\varphi(n)}\right) \equiv r_1 \cdot r_2 \cdots r_{\varphi(n)} (\mathrm{mod}\, n)$. Podemos cancelar, em ambos os lados da congruência, o produto $r_1 \cdot r_2 \cdots r_{\varphi(n)}$ para obter a congruência $a^{\varphi(n)} \equiv 1\ (\mathrm{mod}\, n)$. ■

Note que se n é primo $\varphi(n) = n - 1$ e se o $\mathrm{mdc}(a, n) = 1$ então, $a^{\varphi(n)} \equiv a^{n-1}\ (\mathrm{mod}\, n) \equiv 1 \equiv (\mathrm{mod}\, n)$ que é a congruência de Fermat. Assim, o Teorema de Euler é uma generalização do Pequeno Teorema de Fermat.

Lema 1. Se p primo e $a \in \mathbb{Z}_+$, então $\varphi(p^a) = p^a - p^{a-1} = p^a(1 - \frac{1}{p})$.

Demonstração

Pela definição $\varphi(n)$ sabemos que $\varphi(p^a)$ é o número de inteiros positivos inferiores a p^a e primos com p^a. Sabemos que de 1 até p^a, temos p^a números naturais. Excluindo desses os números que não são primos com p^a, isto é, os múltiplos de p que são os números $p, 2p, \ldots, (p^{n-1}.p)$, cujo número é p^{n-1}. Portanto, $\varphi(p^a) = p^a - p^{a-1}$, provando o resultado. ■

Finalmente, podemos obter a expressão de $\varphi(n)$ para qualquer $n \in \mathbb{N}$.

Teorema 3. Seja $n > 1$ e seja $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ a decomposição de n em fatores primos. Então, $\varphi(n) = p_1^{\alpha_1} \cdots p_n^{\alpha_n}\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_n}\right)$.

Demonstração

Pelo lema anterior temos $\varphi\left(p_i^{\alpha_1}\right) = p_i^{\alpha_1} - p_i^{\alpha_1 - 1} = p_i^{\alpha_1}(1 - \frac{1}{p_i})$. Portanto, o lema nos garante que

$$\varphi\left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}\right) = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) \cdot p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots\ p_r^{\alpha_r}\left(1 - \frac{1}{p_r}\right)$$

$$= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right). \blacksquare$$

Corolário 2. A função φ de Euler é multiplicativa, isto é, $\varphi(mn) = \varphi(m)\cdot\varphi(n)$ para $(m,n) = 1$.

Demonstração

Suponhamos que $m > 1$ e $n > 1$, pois o resultado é trivial para $m = n = 1$. Agora, vamos dispor os números de 1 até $m \cdot n$ em uma tabela.

1	2	$\cdots$	x	$\cdots$	n
$n+1$	$n+2$	$\cdots$	$n+x$	$\cdots$	$2n$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
$(m-1)n+1$	$(m-1)n+2$	$\cdots$	$(m-1)n+x$	$\cdots$	$m\cdot n$

Tabela 10 - Disposição dos números de 1 até mn

Para calcular $\varphi(m\cdot n)$ determinaremos os inteiros na tabela anterior que simultaneamente primos com m e n.

Os inteiros da n-ésima coluna são primos com n, se e somente se, x é primo com n. Ainda, como na primeira linha o número de inteiros que são primos com n é igual a $\varphi(n)$, segue que existe somente $\varphi(n)$ colunas formadas por números inteiros que são todos primos com n. Por outro lado, em cada uma destas $\varphi(n)$ colunas existe $\varphi(m)$ inteiros que são primos com m, pois como $mdc(m,n) = 1$ os elementos $x, x+n, 2x+n, \ldots, (m-1)n+x$ formam um sistema completo de resíduo módulo n, o número de elementos que são primos com m é igual a $\varphi(m)$. Assim, o número total de inteiros que são primos com m e n, isto é, que são primos a $m\cdot n$ e que é igual a $\varphi(m)\cdot\varphi(n)$ e portanto, nos garante que $\varphi(m\cdot n) = \varphi(m)\cdot\varphi(n)$. Quando m e n forem primos, $\varphi(m) = m-1$ e $\varphi(n) = n-1$ logo, $\varphi(m\cdot n) = (m-1)\cdot(n-1)$.

Este corolário é importantíssimo no que diz respeito ao sistema de criptografia RSA pois, escolheremos dois números primos m, n e calcularemos $\varphi(m\cdot n)$ que será um número inteiro que fará parte da codificação de mensagens.

Exemplo 8. Calcule o resto da divisão de 23^{4205} por 77.

A ideia é utilizar os teoremas estudados para resolver a questão sem calcular a potência, que é gigante, e depois efetuar a divisão.

Como $77 = 7\cdot 11$, temos $\varphi(7\cdot 11) = (7-1)\cdot(11\cdot 1) = 6\cdot 10 = 60$. Como o

$\text{mdc}(23,77) = 1$, pelo Teorema de Euler $23^{60} \equiv 1 \pmod{77}$. Realizando a divisão de $4205:60$, encontrarmos $4205 = 60 \cdot 70 + 5$. Logo, $23^{4205} = 23^{60 \cdot 70+5}$. Utilizando a proposição 4.4 (item iii) $(23^{60})^{70} \equiv 1^{70} \pmod{77}$ e com a proposição 4.4 (item i) chegamos em $(23^{60})^{70} \cdot 23^5 \equiv 1^{70} \cdot 23^5 \pmod{77}$. Se calcularmos as potências $23^3 = 12167$ e $23^2 = 529$ e em seguida, dividirmos os dois resultados pelo módulo 77, iremos encontrar $529 = 77 \cdot 6 + 67$ e $12167 = 77 \cdot 158 + 1$. Então, $23^5 \equiv 23^2 \cdot 23^3 \equiv 67 \cdot 1 \equiv 67 \pmod{77}$ e, portanto, o resto da divisão será 67.

Observemos que existe mais de uma maneira de resolver o exemplo. O mais importante é utilizar os teoremas e corolários para que o trabalho seja o menor e mais rápido possível.

4.4 Aplicações de Congruência no Ensino Médio

As aplicações mostradas nesta seção, que são direcionadas ao ensino Médio, tem sua inspiração na aritmética modular e são citadas para colaborar com a solução de algum problema da atualidade ou introduzir um novo problema como motivação para aprender matemática.

Serão três exemplos de aplicações de aritmética modular que poderão ser utilizados por professores de Matemática do ensino Médio, como forma de contextualizar o referido conteúdo com determinadas necessidades, sejam abstratas ou do nosso dia-a-dia.

Os exemplos também utilizam conceitos e teoremas novos, mas que podem ser estudados com clareza, pois já temos base com que foi estudado até o momento.

1) Cadastro das pessoas físicas na Receita Federal – CPF

Outra atividade na qual utilizamos as noções de congruência e que podemos retirar do nosso cotidiano seria os números que compõe os registros que nos identificam, por exemplo, o CPF. E a pergunta para instigar a curiosidade doa alunos seria “como uma instituição, ao precisar do nosso CPF, sabe que não digitamos um dos 11 números errado?”.

No CPF existem dois blocos de algarismos, sendo o primeiro com 9 algarismos e o segundo, com dois algarismos, que são os dígitos de controle ou de verificação, que foram criados para minimizar fraudes e que dependem dos outros

nove algarismos. A determinação desses dois dígitos é mais um caso de aplicação da noção de congruência.

Primeiramente, determinamos o décimo dígito (que é o primeiro dígito verificador) é o resultado de uma congruência módulo 11.

Seja $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9$ a sequência formada pelos primeiros dígitos de um determinado CPF. Multiplicamos essa sequência, em ordem, por $\{1,2,3,4,5,6,7,8,9\}$ e somar os produtos obtidos. O próximo dígito da sequência, que chamaremos de a_{10}, deve ser o algarismo que ao ser subtraído da soma, resulte em um número múltiplo de 11, ou seja, chamando a soma de S,temos a congruência $S - a_{10} \equiv 0 \pmod{11}$. Observe que esse número é o resto da divisão da soma por 11.

Para a determinação do segundo dígito de controle é feita de maneira semelhante, sendo que acrescentamos o décimo dígito e usamos a multiplicação dos números de 0 até 9.

Por exemplo, se o CPF de uma pessoa tem os seguintes 9 primeiros dígitos: 135 382 106. O primeiro dígito de controle será obtido da seguinte maneira:

$$S = 1 \cdot 1 + 3 \cdot 2 + 5 \cdot 3 + 3 \cdot 4 + 8 \cdot 5 + 2 \cdot 6 + 1 \cdot 7 + 0 \cdot 8 + 6 \cdot 9 = 147$$

Assim, temos: $147 \equiv 4 \pmod{11}$. Dessa forma, o primeiro dígito de verificação é o algarismo 4.

Agora, fazemos uma nova soma, incluindo o novo dígito e teremos:

$S = 1 \cdot 0 + 3 \cdot 1 + 5 \cdot 2 + 3 \cdot 3 + 8 \cdot 4 + 2 \cdot 5 + 1 \cdot 6 + 0 \cdot 7 + 6 \cdot 8 + 1 \cdot 9 = 127$. E, novamente, através de $127 \equiv 6 \pmod{11}$, chegamos ao segundo dígito de verificação que é o algarismo 6.

Concluímos que, no nosso exemplo, o CPF completo seria 135 382 106 – 46. Notamos que os dois números são os restos da divisão das somas por 11, e que, se este resto for 10, isto é, se a soma obtida fosse congruente ao 10 módulo 11, o dígito de controle será o zero.

2) Equações Diofantinas.

Muitas vezes no ensino Fundamental e Médio observamos problemas que podemos resolver através de um sistema de equações lineares e os mais presentes são os de equações do primeiro grau. Por exemplo: “Em um estacionamento há carros e motos, em um total de 20 veículos e 50 rodas. Quantos são os carros e as motos?”

Observe que nesse exemplo, sendo c o número de carros e m o número de motos, devemos satisfazer as equações $c + m = 20$ e $4c + 2m = 50$, ao mesmo tempo. Escrevendo o sistema $\begin{cases} c + m = 20 \\ 4c + 2m = 50 \end{cases}$, teremos $c = 5$ e $m = 15$.

Porém, temos muitos problemas de aritmética que dependem da resolução de equações do tipo $ax + by = c$, onde a, b e c são números inteiros dados e x e y são incógnitas a serem determinadas em $\mathbb{Z}$. Um bom exemplo seria o seguinte: "De quantos modos podemos comprar figurinhas de cinco e de três reais, de modo a gastar exatamente cinquenta reais?"

Muitos alunos usariam a ideia da tentativa e erro e perceberiam que poderíamos ter a solução 10 figurinhas de 5 reais e nenhuma de 3 reais, ou ainda, 5 figurinhas de 3 reais e 4 figurinhas de 5 reais porém, não seria o método mais adequado. Para uma resolução completa, veremos as equações diofantinas lineares.

Diofanto de Alexandria, segundo Roque (2014) introduziu uma forma de representar o valor desconhecido em um problema, designando – o com arithmos, de onde vem o nome "aritmética". Em sua principal obra que é Arithmetica, está uma coleção de problemas que ainda de acordo com Roque (2014) não se referem a uma situação real, ligada ao comércio ou agricultura mas, cada problema está ligado a uma técnica de solução que é descrita usando – se valores numéricos.

No nosso trabalho, serão estudadas as equações diofantinas lineares, de modo específico as que possuem duas incógnitas.

Teorema 4. A equação diofantina linear $ax + by = c$ admite solução se, e somente se, $\text{mdc}(a, b)|c$.

Demonstração:

($\Longrightarrow$) Suponha que a equação admita como solução o par (x_0, y_0). Então, a igualdade $ax_0 + by_0 = c$ é válida. Como o $\text{mdc}(a, b)|a$ e $\text{mdc}(a, b)|b$, também ele divide $\text{mdc}(a, b)|ax_0 + by_0$ e portanto, divide c.

($\Longleftarrow$) Agora, supondo que $\text{mdc}(a, b)|c$, isto é, $c = \text{mdc}(a, b) \cdot d$, para algum inteiro d. Sabemos que existem inteiros r e s tais que $\text{mdc}(a, b) = ar + bs$. Multiplicando a igualdade por d, obtemos $c = \text{mdc}(a, b) \cdot d = a \cdot (rd) + b \cdot (sd)$.

Portanto, a equação diofantina linear $ax + by = c$ admite pelo menos a solução $x = rd$ e $y = sd$. ■

Exemplo 10. Encontre uma solução, se existir, da equação $12x + 32y = 52$.

Primeiramente, veremos se a equação possui solução. Para isso, conforme o teorema 4, $\mathrm{mdc}(12{,}32)|52$. Utilizando o algoritmo de Euclides, teremos:

	2	1	2	
32	12	8	4	
8	4	0		

Logo, o $\mathrm{mdc}(12{,}32) = 4$ e $4|52$, pois $52 = 4 \cdot 13$

Para determinar uma solução basta usarmos o algoritmo estendido de Euclides.

$$\begin{bmatrix} 12 & 1 & 0 \\ 32 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 12 & 1 & 0 \\ 32 - 12 \cdot 2 & 0 - 1 \cdot 2 & 1 - 0 \cdot 2 \end{bmatrix} = \begin{bmatrix} 12 & 1 & 0 \\ 8 & -2 & 1 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 12 - 8 \cdot 1 & 1 - (-2) \cdot 1 & 0 - 1 \cdot 1 \\ 8 & -2 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 3 & -1 \\ 8 & -2 & 1 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 4 & 3 & -1 \\ 8 - 4 \cdot 2 & -2 - 3 \cdot 2 & 1 - (-1) \cdot 2 \end{bmatrix} = \begin{bmatrix} 4 & 3 & -1 \\ 0 & -8 & 1 \end{bmatrix}$$

Através do Teorema de Bézout (Teorema 2 do capítulo 3) podemos escrever $\mathrm{mdc}(12{,}32) = 4 = 12 \cdot 3 + 32 \cdot (-1)$. Se multiplicarmos a igualdade por 13 encontraremos $4 \cdot 13 = 52 = 12 \cdot (3 \cdot 13) + 32 \cdot \big((-1) \cdot 13\big) = 12 \cdot 39 + 32 \cdot (-13)$ e portanto, $(39, -13)$ é uma solução para a equação $12x + 32y = 52$.

O próximo resultado nos dará uma maneira de resolver a equação diofantina linear $ax + by = c$, onde $\mathrm{mdc}(a, b) = 1$, conhecida uma solução particular x_0 e y_0 da equação.

Teorema 5. Seja x_0 , y_0 uma solução particular da equação $ax + by = c$, com $\mathrm{mdc}(a, b) = 1$, então as soluções da equação são da forma $x = x_0 + tb$ e $y = y_0 - ta$, para t variando em $\mathbb{Z}$.

Demonstração:

Seja x, y uma solução qualquer da equação, temos que $ax + by = ax_0 + by_0$, então $a(x - x_0) = b(y_0 - y) = c$.

Se $a|b(y_0 - y)$ e $b|a(x - x_0)$. Como $\mathrm{mdc}(a, b) = 1$, segue que $a|(y_0 - y)$ e $b|(x - x_0)$. Assim, $y_0 - y = ta$ e $x - x_0 = sb$, para alguns inteiros t e s. Substituindo

esses valores em $a(x - x_0) = b(y_0 - y)$, obtemos $asb = bta$, o que implica que $s = t$. Logo, temos que $x = x_0 + bt$ e $y = y_0 - at$.

Reciprocamente, se $x = x_0 + bt$ e $y = y_0 - ta$, substituindo esses valores na equação $ax + by = c$, obtemos $a(x_0 + bt) + b(y_0 - at) = ax_0 + by_0 + abt - bat = ax_0 + by_0 = c$ ■

Como $t \in \mathbb{Z}$, vemos que irão existir soluções positivas, negativas e nulas porém, como na pergunta inicial inúmeras vezes é necessário resolver em $\mathbb{N} \cup \{0\}$ as equações da forma $ax + by = c$, onde $a, b, c \in \mathbb{N}$.

Para isso, definiremos o conjunto $S(a, b) = \{xa + yb; x, y \in \mathbb{N} \cup \{0\}\}$ e caracterizaremos os seus elementos.

Proposição 4.8. $c \in S(a, b)$ se, e somente se, existem $n, m \in \mathbb{N} \cup \{0\}$, com $n < b$ tais que $c = na + mb$.

Demonstração

($\Longrightarrow$) Sendo $c \in S(a, b)$, então $c = xa + yb$ com $x, y \in \mathbb{N} \cup \{0\}$. Pela divisão euclidiana $x = bq + n$, com $n < b$; logo substituindo o valor de x desta última igualdade na anterior, obtemos $c = na + mb$, onde $n < b$ e $m = aq + y$.

($\Longleftarrow$) Se $c = na + mb$, com $n, m \in \mathbb{N} \cup \{0\}$ e $n < b$ então $c \in S(a, b)$. ■

Supondo que a equação $ax + by = c$, com $mdc(a, b) = 1$, tenha solução e seja $x_0 = n$ e $y_0 = m$. As soluções x, y da equação são dadas pelas equações $x = n + tb$ e $y = m - ta$, com $t \in \mathbb{N} \cup \{0\}$ e $m - ta \geq 0$

Na questão sobre a compra das figurinhas, a equação $3x + 5y = 50$ admite a solução particular $x_0 = n = 0$ e $y_0 = m = 10$, pois $mdc(a, b) = 1$. Assim, a solução geral dessa equação é dada por $x = 0 + 5t$ e $y = 10 - 3t$.

Vemos que, para soluções não negativas, devemos ter $y = 10 - 3t \geq 0$, o que implica que $t = 0, 1, 2$ ou 3. Assim, o problema admite as seguintes soluções:

- 10 figurinhas de 5 reais.
- 5 figurinhas de 3 reais e 7 figurinhas de 5 reais.
- 10 figurinhas de 3 reais e 4 figurinhas de 5 reais.
- 15 figurinhas de 3 reais e uma figurinha de 5 reais.

Para resolvermos uma equação diofantina linear $ax + by = c$ é necessário calcular $mdc(a, b)$ e verificar se divide ou não c e então descobrir uma solução particular. A primeira parte se resolve utilizando o algoritmo de Euclides para o

cálculo do mdc. A segunda, o de determinar uma solução particular da equação, podemos usar o algoritmo de Euclides de trás para frente para determinar inteiros r e s tais que $ar + bs = mdc(a, b) = 1$, depois multiplicar ambos os membros da equação por c, obtendo $a(rc) + b(sc) = c$, e assim, a solução particular será $x_0 = rc$ e $y_0 = sc$.

3) Congruências Lineares

Neste último exemplo, a motivação será uma situação – problema, que sem o auxílio da *congruência linear*, pode resolvido por tentativa, mas chegar a solução desse problema em um tempo razoável nem sempre é possível.

Observemos a seguinte situação: “Pode o quíntuplo de um número deixar resto 3 quando dividido por 8?” Se traduzirmos a frase para a linguagem de congruência teremos, $5x \equiv 3 \pmod 8$.

Definição 4.6. Uma congruência do tipo $ax \equiv b \pmod n$ onde $a, b, n \in \mathbb{Z}$,com $n > 1$ e x uma variável em $\mathbb{Z}$, recebe o nome de congruência linear.

Então, a nossa situação resume encontrar uma ou mais soluções de uma congruência linear. Inicialmente veremos uma maneira de decidir se estas congruências têm ou não soluções.

Proposição 4.9. Dados $a, b, m \in \mathbb{Z}$,com $n > 1$, a congruência $ax \equiv b \pmod n$ possui solução se, e somente se, $mdc(a, n)|b$.

Demonstração

($\Longrightarrow$) Suponhamos que a congruência $ax \equiv b \pmod n$ tenha uma solução x. Então, teremos $n|ax - b$, isto é, existe um $y \in \mathbb{Z}$ tal que $ax - b = ny$, ou ainda, que $ax - ny = b$ admite solução pelo teorema 4 dessa mesma seção.

($\Longleftarrow$) Suponhamos que $mdc(a, n)|b$. Então, pelo teorema 4, $ax - ny = b$ admite uma solução x, y. Portanto, $ax = b + ny$ e, por consequência, x é a solução da congruência pois, $ax \equiv b \pmod n$.■

Recordemos um conceito que dará auxílio na resolução do problema. Relembrando a proposição 4.6 sobre o inverso multiplicativo, temos que existe y tal que $a \cdot y \equiv 1 \pmod n$, se e somente se, $mdc(a, n) = 1$. Ao multiplicarmos a equação $ax \equiv b \pmod n$ por y, obtemos $ayx \equiv by \pmod n$. Como y é o inverso multiplicativo

de a módulo n, esta equação é transformada em $x \equiv by \pmod{n}$. Logo, resolver uma congruência linear, caso esta tenha solução, se reduz em saber se determinado elemento possui inverso multiplicativo.

Então, para resolvermos nossa situação – problema, precisamos multiplicar a equação $5 \cdot x \equiv 3 \pmod{8}$ pelo inverso multiplicativo de 5 módulo 8. Como anteriormente montamos uma tabela de inverso multiplicativo módulo 8 (tabela 9), encontramos que o inverso de 5 é o próprio 5. Ao multiplicarmos nossa congruência por 5, temos $5 \cdot 5 \cdot x \equiv 3 \cdot 5 \pmod{8}$. Então, $x \equiv 3 \cdot 5 \equiv 15 \equiv 7 \pmod{8}$ e a solução da equação será $x = 7$.

Um item importante que podemos enxergar utilizando esse método para a resolução das congruências lineares é que se $mdc(a, n) = 1$, então a congruência $ax \equiv b \pmod{n}$ possui uma, e somente uma, solução. Ao eliminarmos a condição $mdc(a, n) = 1$, a afirmação nem sempre é verdadeira.

5 Criptografia

A criptografia é responsável por técnicas sistematizadas, chamadas de *encriptação*, que nos permitem proteger uma informação tornando um texto ilegível de maneira que apenas o receptor da mensagem possa ler. Ela também é responsável pela operação contrária, ou seja, a de “quebrar” uma mensagem que esteja codificada. A essa parte da criptografia chamamos de criptoanálise.

Uma mensagem criptografada é uma forma sistemática de colocar em ordem um conjunto de símbolos, de maneira a enviar uma informação específica. A necessidade de proteger uma informação não é atual, como poderíamos pensar, devido ao volume de transações que são feitas hoje em dia via internet. Nossos antepassados inventaram diversas formas de esconder o conteúdo de uma mensagem (Sautoy).

Na Itália do século XVI, de acordo com Sautoy (2013), o italiano Giovanni Porta descobriu que com cerca de 30 gramas de alume[5] e meio litro de vinagre, era possível conseguir uma tinta que penetrava na casca de um ovo cozido, marcava a sua clara e, ao mesmo tempo, desaparecia da casca. Ótimo para enviar mensagens secretas. Para descobrir a mensagem só era preciso descascar o ovo.

Ou ainda, segundo Carter (2007), o historiador grego Heródoto (484–425a.C), mais conhecido como o pai da História, registrou que um grego de nome Demaratus, descobriu um modo de enviar informações para fora do país. Naquele tempo, escreviam – se em tábuas de madeira cobertas com cera. Demaratus escreveu uma mensagem na tábua e depois a cobriu com cera, ocultando a mensagem. Estas são umas das diversas maneiras que pessoas pensaram para ocultar mensagens secretas.

5.1 Alguns tipos de cifras

Um dos modos mais sofisticados de ocultar uma mensagem foi desenvolvido exército espartano (século V a.C). Eles usavam um dispositivo conhecido como citale, que nada mais era que um bastão de madeira em forma de cilindro. O emissor da mensagem possuía um citale no qual enrolava uma tira de pergaminho em espiral. O remetente escrevia a mensagem secreta sobre o pergaminho ao longo

[5] Na origem, o termo "alume" se referia especificamente ao sulfato duplo de potássio e alumínio, popularmente conhecido como pedra-ume.É um adstringente e antisséptico. Os antigos gregos e romanos já o usavam como adstringente e fixador para tinturaria.

do seu comprimento e depois desenrolava a tira, que no momento parecia uma série de letras sem sentido algum. Somente ao ser enrolado novamente pelo receptor em um citale idêntico, a mensagem reaparecia. A técnica do citale consiste em uma *cifra de transposição*, ou seja, as letras do texto são misturadas como um anagrama.

Figura 6 - Citale de César

Disponível em:<https://pt.wikipedia.org/wiki/C%C3%ADtala>. Acesso em out. 2015.

Outro tipo de cifra, uma das mais simples, é chamado de *cifras de César*, em homenagem ao imperador Júlio César, que a usou para propósito militares. A cifra funciona trocando cada letra por outra, pulando o mesmo número de posições, que seria a uma espécie de *chave* do sistema para que a mensagem fosse cifrada. Por exemplo, em uma troca de cinco, o A se torna F, B se torna G, e assim por diante. Utilizando a cifra de César, cifraremos a palavra PROFMAT, deslocando o alfabeto em 5 casas para a direita. A tabela a seguir nos mostra na primeira linha o alfabeto normal e na segunda, o alfabeto deslocado em 5 casas.

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

Tabela 11 - Quadro do método de substituição utilizado por Júlio César.

Fonte: Adaptado de Singh (2010)

Ao usarmos o quadro, obteremos a seguinte palavra “UWTKRFY”. Assim, a mensagem cifrada não é legível por outra pessoa que não seja o destinatário e este, para reverter o processo deve utilizar a chave do sistema para restaurar a mensagem original a partir da mensagem cifrada.

A cifra de César é chamada *cifra de substituição monoalfabéticas*. Estas cifras, não oferecem muita segurança, pois são simples e fáceis de serem decifradas. Primeiramente, cada letra do texto original é substituída sempre pela mesma letra no texto cifrado, logo o texto possui 25 possibilidades para decifrar a mensagem.

Segundo, a frequência média com que cada letra aparece em um texto, em

determinado idioma, é mais ou menos constante. Logo, analisando a frequência de cada letra nos permite montar associações e descobrir que letras correspondem os símbolos mais frequentes. Assim, geralmente a mensagem pode ser lida por outra pessoa, sem ser o destinatário.

5.1.1 Cifra de Vigenère

De acordo com Singh (2010), a solução encontrada para a fragilidade da cifra de César, foi o desenvolvimento de uma *cifra de substituição polialfabética*, criada pelo diplomata francês Blaise Vigenère, no século XVI, baseado no trabalho sobre cifras do italiano Leon Battista Alberti e de outros, como Giovanni Porta.

A cifra de Vigenère, como ficou conhecida, utiliza uma tabela com o alfabeto escrito 26 vezes em diferentes linhas, cada uma com o alfabeto deslocado por uma posição anterior e uma palavra – chave, combinada entre o codificador e o receptor da mensagem, para cifrar e decifrar a mensagem.

Usaremos o quadro de Vigenère a seguir, a palavra – chave **PROF** e codificaremos a frase MESTRADO PROFISSIONAL.

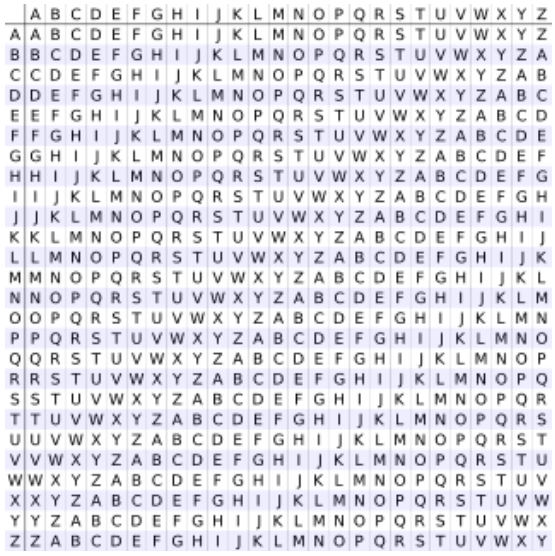

Figura 7 - Imagem da tabela de Vigenère

Disponível em:<https://pt.wikipedia.org/wiki/Cifra_de_Vigen%C3%A8re>. Acesso em out.2015

Primeiramente, escrevemos a palavra – chave quantas vezes for necessário, para que cada letra corresponda a uma letra da frase.

P	R	O	F	P	R	O	F	P	R	O	F	P	R	O	F	P	R	O	F
M	E	S	T	R	A	D	O	P	R	O	F	I	S	S	I	O	N	A	L

Tabela 12 – Quadro da Palavra – chave

Para codificar a primeira letra da frase, faremos a interseção da coluna M com a linha P (primeira letra do texto original com a primeira letra do texto cifrado), obtendo a letra B. Depois, a interseção da coluna E com a letra R, resultando a letra V e, assim por diante. A tabela mostra como fica a interseção de cada letra.

Palavra Chave	P	R	O	F	P	R	O	F	P	R	O	F	P	R	O	F	P	R	O	F
Texto Original	M	E	S	T	R	A	D	O	P	R	O	F	I	S	S	I	O	N	A	L
Texto Cifrado	B	V	G	Y	G	R	R	T	E	I	C	K	X	J	G	N	D	E	O	Q

Tabela 13 - Exemplo do uso da cifra de Vigenère.

Assim, no exemplo, a frase MESTRADO PROFISSIONAL, ficou codificada por BVGYGRRTEICKXJGNDEOQ.

Como em outros tipos de cifras, a de Vigenère também possui suas fraquezas, que no caso, de acordo com SINGH (2010), foi encontrada 300 anos depois da sua invenção, pelo oficial prussiano Friedrich Kasiski (1805-1881). Ele percebeu o fato que a chave se repete. Por exemplo, se a palavra chave for RIO, a primeira letra do texto original e depois, a cada três letras, será cifrada pela letra R. A segunda letra e a cada três, será cifrada pela letra I e a terceira letra do texto e a cada três letras, será cifrada pela letra O. Kasiski observou que se fosse possível descobrir o tamanho da palavra chave, poderia – se usar a análise de frequência em cada conjunto de letras cifradas e descobrir a mensagem ocultada.

5.1.2 Cifras em bloco

Outra maneira de dificultar a cifra de César é subdividir a mensagem em blocos de várias letras e misturarmos esses blocos. A este processo de cifrar uma mensagem chamamos de *cifra em bloco*. Por exemplo, vamos codificar a mensagem OS NÚMEROS GOVERNAM O MUNDO, seguindo os seguintes passos, que serão aplicados ao nosso exemplo:

- eliminamos os espaços e se a mensagem tenha uma quantidade ímpar de letras, completamos com um A;
  OSNÚMEROSGOVERNAMOMUNDOA

- subdividimos a mensagem em blocos de duas letras;
  OS – NU – ME – RO – SG – OV – ER – NA – MO – MU – ND - OA
- refletimos cada bloco;
  SO – UN – EM – OR – GS – VO – RE – AN – OM – UM – DN – AO
- trocamos de lugar o primeiro com o último bloco, o terceiro com o antepenúltimo, e assim por diante, deixando os outros como estão.
  AO – UN – UM – OR – AN – VO – RE – GS – OM – EM – DN – SO

E teremos a mensagem codificada

AOUNUMORANVOREGSOMEMDNSO

Os sistemas que vimos como exemplos, possuem dois problemas centrais. O primeiro se caracteriza pelo uso da mesma chave para cifrar e decifrar determinada mensagem. O segundo é deve existir uma troca dessa chave, para que cada parte (remetente e destinatário) consiga decifrar a mensagem que será enviada. Também fica o problema da chegada ao seu destinatário, de modo seguro, a chave da cifra, para que só ele possa decifrar a mensagem original.

As cifras que vimos anteriormente podem ser aplicadas em sala de aula pelos professores do ensino Médio e até mesmo do Fundamental II, em momentos que os professores acharem mais oportunos, assim os alunos podem trabalhar determinadas habilidades que quase não são exploradas durante as aulas de matemática.

5.2 A trinca americana

Segundo Sautoy (2007), antes de 1977, emissor e receptor de uma mensagem secreta, deveriam encontrar – se para decidir qual a chave secreta e o tipo cifra usariam para o método da codificação.

Agora, imagine utilizar uma dessas cifras para fazer negócios hoje em dia, através da internet. Teríamos muitos encontros ou ainda, receberíamos cartas confidenciais de cada empresa que possuísse uma página virtual, na qual quiséssemos fazer compras. Eles nos indicariam como codificar dados pessoais e bancários. Mas, dado o volume enorme de negócios feitos via internet, as chances dessas cartas serem interceptadas seriam imensas e muitos dados pessoais extraviariam – se no caminho.

Para este problema, os matemáticos inventaram uma nova geração de códigos e de acordo com Sautoy (2007), foram à base para a criação do que é

chamado de criptografia de *chave pública*, que possui esse nome, pois o processo de codificação pode ser conhecido por qualquer pessoa sem comprometer a segurança da mensagem original.

5.2.1 A ideia de trinca americana

Imagine que João é administrador de um site que vende bolsas em São Paulo. Maria, que mora em Minas Gerais, deseja comprar uma bolsa e quer mandar detalhes de seus dados pessoais como CPF e endereço. Para isso, eles devem trocar entre si uma chave secreta por algum meio de comunicação por exemplo, por celular, para que esses dados pessoais de Maria possam ser utilizado com segurança.

Eles escolhem em comum acordo um par de números naturais a e m e os tornam públicos. João e Maria devem escolher, cada um outro número natural e os manter secreto.

João que escolheu o número $\mathrm{A_J}$, irá calcular o único número $\mathrm{B_J} < m$ tal que $\mathrm{a}^{\mathrm{A_J}} \equiv \mathrm{B_J} \pmod{\mathrm{m}}$, ou seja, $\mathrm{B_J}$ é o resto da divisão de $\mathrm{a}^{\mathrm{A_J}}$ por m e o envia a Maria. Ela, que escolheu o número $\mathrm{A_M}$, faz o mesmo processo e calcula o único número $\mathrm{B_M} < m$ tal que $\mathrm{a}^{\mathrm{A_M}} \equiv \mathrm{B_M} \pmod{\mathrm{m}}$. Em seguida, João calcula $\mathrm{B_M}^{\mathrm{A_J}}$ e encontra a chave secreta A através da equação $\mathrm{B_M}^{\mathrm{A_J}} \equiv (\mathrm{a}^{\mathrm{A_M}})^{\mathrm{A_J}} \equiv \mathrm{a}^{\mathrm{A_M}\mathrm{A_J}} \equiv \mathrm{A} \pmod{\mathrm{m}}$, sendo que $\mathrm{A} < m$. Maria calcula separadamente $\mathrm{B_J}^{\mathrm{A_M}}$ e deverá encontrar a mesma chave secreta, com a equação $\mathrm{B_J}^{\mathrm{A_M}} \equiv (\mathrm{a}^{\mathrm{A_J}})^{\mathrm{A_M}} \equiv \mathrm{a}^{\mathrm{A_J}\mathrm{A_M}} \equiv \mathrm{A} \pmod{\mathrm{m}}$, com $\mathrm{A} < m$ e dessa forma está trocada a chave secreta entre João e Maria.

Portanto, são públicas as informações $\mathrm{a}, \mathrm{m}, \mathrm{B_J}, \mathrm{B_M}$ e são secretas as chaves $\mathrm{A_J}$ que apenas João conhece, $\mathrm{A_M}$ que somente Maria conhece e A que é conhecida apenas por João e Maria.

Vamos a um exemplo prático, lembrando que para efeito de cálculos iremos escolher número com valores baixos. Na prática os números escolhidos são enormes, para dificultar que outros, sem ser o receptor, decifre a mensagem.

Suponhamos que João e Maria escolheram $\mathrm{a} = 30$ e $\mathrm{m} = 41$. João escolhe como chave secreta $\mathrm{A_J} = 5$ e Maria $\mathrm{A_M} = 3$.

Agora, veremos qual a chave secreta A que João e Maria terão em comum. Primeiramente, João e Maria calculam, respectivamente, $\mathrm{B_J}$ e $\mathrm{B_M}$, através de congruência e suas propriedades.

João faz os cálculos para determinar B_J e encaminhá – o a Maria.

$30 \equiv 30 \pmod{41}$ e também $30 \equiv -11 \pmod{41}$.

$30^2 \equiv (-11)^2 \equiv 121 \equiv -2 \pmod{41}$.

$30^5 = 30 \cdot 30^2 \cdot 30^2 \equiv (-11) \cdot (-2) \cdot (-2) \equiv -44 \equiv -3 \equiv 38 \pmod{41}$

Logo, $B_J = 38$.

Maria, faz o mesmo e determina B_M para enviá – lo a João.

$30^3 = 30 \cdot 30^2 \equiv (-11) \cdot (-2) \equiv 22 \pmod{37}$. Ela encontra, $B_M = 22$

Com $B_M = 22$ e $B_J = 38$ em mãos os dois separadamente calculam a chave secreta A.

João calcula o resíduo $B_M^{A_J} = 22^5 \pmod{41}$ e determina a chave secreta A.

$22 \equiv 22 \pmod{41}$

$22^2 = 484 \equiv 33 \equiv -8 \pmod{41}$

$22^4 = (-8)^2 \equiv 64 \equiv 23 \pmod{41}$.

$22^5 \equiv 22 \cdot 22^4 \equiv 22 \cdot 23 \equiv 14 \pmod{41}$. Com esses cálculos, João encontra a chave secreta $A = 14$.

Se fizer os cálculos corretamente, Maria deverá encontrar a mesma chave secreta que para que faça sentido a troca de chaves. Maria deve obter o resíduo $B_J^{A_M} = 38^3 \pmod{41}$.

$38 \equiv 38 \equiv -3 \pmod{41}$

$38^2 \equiv (-3)^2 \equiv 9 \pmod{41}$

$38^3 = 38^2 \cdot 38 \equiv 9 \cdot (-3) \equiv -27 \equiv 14 \pmod{41}$ e como esperávamos, $A = 14$.

Para facilitar o entendimento, montaremos uma tabela com os dados do exemplo anterior.

	Público (a, m)	Secreto	Cálculos para a troca pública	Troca pública	Mensagem trocada (secreta)
João	$a = 30$, $m = 41$	$A_J = 5$	$30^5 \equiv 38 \pmod{41}$. $B_J = 38$	$B_J = 38$	$22^5 \equiv 14 \pmod{41}$ $A = 14$
Maria	$a = 30$, $m = 41$	$A_M = 3$	$30^3 \equiv 22 \pmod{41}$. $B_M = 22$	$B_M = 22$	$38^3 \equiv 14 \pmod{41}$ $A = 14$

Tabela 14 - Exemplo da trinca americana

A garantia do sucesso deste método está no fato de ser difícil descobrir qualquer uma das três chaves secretas, conhecendo apenas os dados públicos, acima citados. E, este sistema, denominado DHM, em homenagem aos seus

inventores, os cientistas Whitfield Driffie, Martin Hellman e Ralph Merkle foi o primeiro passo na direção da solução do problema da distribuição de chaves.

O que os criadores do sistema DHM pensaram foi elaborar funções matemáticas em que sua inversa seria quase impossível de ser determinada, isto é, uma função f com uma propriedade muito simples para calcular $f(x)$, mas que seja inviável na prática, através de um computador ou de outra forma, calcular sua inversa.

No entanto, observando mais atentamente, o sistema possui um grande defeito, pois serve apenas para a troca de chaves secretas entre duas pessoas de cada vez e isso em um mundo globalizado é terrível.

Então, Driffie teve a ideia de considerar sistemas onde cada usuário teria duas chaves, uma pública para a cifrar a mensagem e outra secreta para a decifra – la.

Faremos aqui um paralelo, imaginando que codificar e decodificar seja parecido com trancar e destrancar uma porta. Em uma porta comum utilizamos a mesma chave para fechar e abrir a porta. Logo, a chave deve ser mantida secreta.

No sistema de criptografia de chave pública teríamos uma porta com duas chaves diferentes. Uma chave serve para trancar a porta enquanto outra apenas para destrancar. Logo, não seria necessário manter em segredo a chave que tranca a porta. Uma empresa poderia distribui cópias dessa chave (sem comprometer a segurança) para qualquer visitante, em sua página na internet, que queira enviar uma mensagem segura, como o número de seu cartão de crédito.

Mesmo todos usando a mesma chave para codificar seus dados, ou seja, trancando a porta e guardando seus segredos, os clientes não conseguem mais acessar seus dados uma vez codificados, mas somente a empresa que possui a chave para destrancar a porta, ou seja, a chave secreta pode ler os segredos dos clienstes.

Driffie não conseguiu colocar sua ideia em prática, mas deixou de acordo com Sautoy (2007) um artigo sobre o assunto. Ainda, de acordo com Sautoy (2007) uma das pessoas inspiradas pelo artigo foi Ronald Rivest, que juntamente com Adi Shamir e Leonard Adleman, do Laboratório de Ciência da Informação do MIT (Massachusetts Institute of Technology) conseguiram implementar o sistema com duas chaves ou como pode ser chamado sistema criptográfico com chaves *assimétricas*, onde cada usuário possuiria duas chaves, uma pública para cifrar a mensagem e outra secreta para a decifragem das mensagens recebidas.

5.2.2 Composição de cifras

Antes de estudarmos um dos sistemas de criptografia com chaves assimétricas, veremos outro tipo de cifra, que também pode ser colocado nas aulas de matemática como motivador para o tema.

Para dificultar a quebra de uma mensagem, uma outra ideia seria compor uma nova cifra através de dois ou mais tipos de cifras.

Imaginemos que Maria deve enviar seu CPF (usaremos o CPF encontrado na seção 4.4) para comprar itens no site de João e que o sistema utilizado por eles dois seja uma cifra composta pela trinca americana e uma fórmula de codificação que ao serem combinados irão codificar e decodificar o CPF dela.

Vejamos que na trinca americana existe apenas a troca de uma chave secreta e esta chave seria um parâmetro para codificação, como na cifra de César, onde o número de deslocamento do alfabeto é a chave do sistema.

Precisamos definir a fórmula de codificação. No exemplo, associaremos cada número n a equação $A + n \equiv X \pmod{m}$, na condição que $A + n$ deve pertencer ao conjunto do sistema de resíduo módulo m.

Com a fórmula de codificação definida, Maria divide o número do seu CPF em blocos de dois algarismos, sem utilizar os dois dígitos finais, que são de verificação. Como o número possui 9 dígitos completamos o algarismo inicial com o zero. Todo o processo deve ser combinado antes com João para que ele saiba como decodificar o número enviado. O bloco separado fica da seguinte maneira:

$$01 - 35 - 38 - 21 - 06$$

Depois, ela aplica a congruência em cada um dos blocos, não esquecendo que cada elemento B deve pertencer ao sistema de resíduos módulo m.

$01 + 14 \equiv 15 \pmod{41}$

$35 + 14 \equiv 08 \pmod{41}$

$38 + 14 \equiv 11 \pmod{41}$

$21 + 14 \equiv 35 \pmod{41}$

$06 + 14 \equiv 20 \pmod{41}$

Então, envia a João o número 150811352046.

Para a decodificação, João deve resolver a equação $X - A \equiv n \pmod{m}$, com $n \in \mathbb{Z}_+$. Vejamos como fica a decodificação:

$15 - 14 \equiv 01 \pmod{41}$

$08 - 14 \equiv -6 \equiv 35 \pmod{41}$

$11 - 14 \equiv -3 \equiv 38 \pmod{41}$

$35 - 14 \equiv 21 \pmod{41}$

$20 - 14 \equiv 06 \pmod{41}$

E, João encontra o número 135.382.106 – 46.

Um detalhe importante, mesmo com a composição das cifras, a criptografia fica dependente da troca de uma chave segura, que codifica e decodifica a mensagem e também da fórmula de codificação e decodificação no qual os dois devem conhecer. Porém, existem criptografias que podemos denotá – las de completas, pois a chave gera também todos os códigos. Uma dessas criptografias é o sistema RSA, que veremos na próxima seção.

5.3 O Sistema RSA

Segundo Coutinho (2013) o mais conhecido e mais usado em aplicações financeiras dos métodos de criptografia de chave pública é o sistema RSA, que possui esse nome devido as iniciais dos seus inventores.

Rivest, Shamir e Adleman combinaram fatos matemáticos, entre eles Aritmética Modular, números primos, o Teorema de Euler (originado do Pequeno Teorema de Fermat) e complexidade computacional, de maneira que conseguiram gerar um algoritmo de enorme dificuldade para ser revertido, isto é, dificílimo de ser desfeito tendo apenas as chaves públicas.

Outro fato importante no sistema RSA é justamente escolher dois números primos p, q e multiplicá – los, encontrando um número inteiro n, que será a chave pública. Há um detalhe nessa escolha: esses números primos devem ser enormes, composto de 150 algarismos ou mais. Assim fatorar n para achar p, q, segundo Coutinho (2013) com os métodos atuais levaria alguns milhares de anos.

Voltando ao nosso exemplo, suponhamos que João queira implementar o sistema criptográfico RSA em seu site para que compradores, como Maria possam enviar seus dados pessoais com uma maior segurança. Ele deve proceder da seguinte maneira:

- João escolhe dois números primos distintos p e q e calcula o produto resultante de p, q. Em seguida, João irá escolher um número e tal que $\text{mdc}(e, \varphi(n)) = 1$, onde $1 \leq e \leq \varphi(n)$ e $\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$, sendo $\varphi(n)$ a função fi de Euler, como vimos no capítulo anterior. O par (n, e) será a chave pública que Maria ou qualquer outro comprador usará para codificar seus dados

no site de João.

- Para que João decodifique a mensagem enviada por Maria, ele gera a partir do par (n, e), uma chave secreta (n, d), onde $d \cdot e \equiv 1 \pmod{\varphi(n)}$ e $1 < d < \varphi(n)$. Como o $mdc(e, \varphi(n)) = 1$, o número d é o inverso multiplicativo de e módulo $\varphi(n)$.
- Maria codifica uma mensagem A utilizando a chave pública que João disponibilizou, calculando A^e e determina o seu resto módulo n, ou seja $A^e \equiv C \pmod{n}$. Logo, teremos C como a mensagem cifrada enviada à João.
- Ao receber a mensagem de Maria, ele utiliza sua chave secreta (n, d), calcula a potência C^d e determina seu resto módulo n, isto é, $C^d \equiv A \pmod{n}$ e assim encontra mensagem enviada por Maria. Este último resultado é muito importante, pois garante que a mensagem original seja recuperada.

5.4 Implementação matemática do Algoritmo RSA

Agora abordaremos o sistema RSA reunindo todos os tópicos até aqui estudados. Como o trabalho é voltado para professores e alunos do ensino Médio, faremos algumas modificações e adaptação da implementação do RSA feita por Coutinho (2007), para que tenhamos mais clareza didática.

5.4.1 Pré – codificação do RSA

Antes de codificar uma mensagem utilizando o sistema RSA é necessário converter a mensagem em uma sequência de números. Suponhamos, para simplificar nossos exemplos, que a mensagem original seja um texto apenas com palavras, ou seja, a mensagem é composta de letras e espaço.

Utilizando a tabela a seguir, Maria pode converter letras em números, para codificar qualquer texto.

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

Tabela 15 - Exemplo de pré – codificação

Aqui temos dois pontos importantes. Primeiro, a vantagem de utilizar números

com dois algarismos para cada letra é de evitar ambiguidade. Optando por uma tabela onde A corresponde ao número 1, B ao número 2, C ao 3 e assim por diante, não saberíamos se 16 representaria AG ou P, que é a 16ª letra do nosso alfabeto.

Segundo, vamos adicionar espaços em branco entre as palavras, que será substituído pelo número 99.

Imaginemos que Maria quer enviar “MINAS GERAIS”, estado onde ela reside, para João. De acordo com a tabela acima a mensagem pré – codificada ficaria da seguinte maneira:

$$A = 221823102899161427101828$$

Antes de Maria continuar, João precisa definir os números primos distintos p e q, considerando que $n = p \cdot q$. Assim, a última parte da pré – codificação, consiste em separar em blocos o texto A. Estes blocos devem ser menores que n. Por exemplo, se João escolher $p = 23$ e $q = 11$, teremos $n = 23 \cdot 11 = 253$. Maria pode quebrar a mensagem nos seguintes blocos:

$$221 - 8 - 23 - 102 - 89 - 91 - 61 - 42 - 7 - 101 - 8 - 28$$

O modo de Maria quebrar a mensagem não é única. Ela toma o cuidado para nenhum bloco começar por zero, pois no momento da decodificação haveria confusão. Por exemplo, não daria para distinguir 010 de 10, quando se está trabalhando com esses números. Outro cuidado a ser tomado é que cada bloco deve ter valor

5.4.2 Codificação do RSA

Para codificar a mensagem, Maria vai precisar da chave pública informada por João, o par (n, e), formado por n que é o produto dos primos p, q e de um número inteiro positivo e, escolhido por João tal que $mdc(e, \varphi(n)) = 1$. Calculando o valor de $\varphi(253) = (23 - 1) \cdot (11 - 1) = 220$, temos que $mdc(e, 220) = 1$. No nosso exemplo, para tornar o processo de codificação mais “rápido” João escolherá $e = 3$. Portanto, a chave pública que fica a disposição de Maria será o par $(253, 3)$.

Denotaremos cada bloco pré – codificado por A_k, onde $k = 1,2,3, \dots, 12$. Para codificá – los usaremos a expressão $C_k \equiv A_K^e \pmod{n}$, onde C_k é o bloco codificado.

Em termos de divisão Euclidiana C_k seria o resto da divisão de A_K^e por n. Por isso cada bloco deve ser um inteiro tal que $1 \leq A_K \leq n - 1$.

Considerando nosso exemplo, $n = 253$ e $e = 3$. Tomando o primeiro bloco da mensagem pré – codificada como $A_1 = 221$, teremos:

$C_1 \equiv 221^3 \pmod{253} = C_1 \equiv 221^2 \cdot 221 \equiv (48841) \cdot 221 \equiv (12) \cdot 221 \equiv 2652 \equiv 122 \pmod{253}$. Ou seja, $A_1 = 221$ foi codificado como 122.

Realizando o mesmo com os outros blocos da mensagem codificada, Maria terá o seguinte:

$C_2 \equiv 8^3 \pmod{253} = C_2 \equiv 512 \equiv 6 \pmod{253}$. $C_2 = 6$ e como $A_{11} = 8$, o bloco $C_{11} = C_2$.

$C_3 \equiv 23^3 \pmod{253} = C_3 \equiv 23^2 \cdot 23 \equiv 529 \cdot 23 \equiv (23) \cdot 23 \equiv 23 \pmod{253}$. $C_3 = 23$.

$C_4 \equiv 102^3 \pmod{253} = C_4 \equiv 102^2 \cdot 102 \equiv (10404) \cdot 102 \equiv (31) \cdot 102 \equiv 3162 \equiv 126 \pmod{253}$. $C_4 = 126$.

$C_5 \equiv 89^3 \pmod{253} = C_5 \equiv 89^2 \cdot 89 \equiv (7921) \cdot 89 \equiv (78) \cdot 89 \equiv 6942 \equiv 111 \pmod{253}$. $C_5 = 111$.

$C_6 \equiv 91^3 \pmod{253} = C_6 \equiv 91^2 \cdot 91 \equiv (8281) \cdot 91 \equiv (185) \cdot 91 \equiv 16835 \equiv 137 \pmod{253}$. $C_6 = 137$.

$C_7 \equiv 61^3 \pmod{253} = C_7 \equiv 61^2 \cdot 61 \equiv (3721) \cdot 61 \equiv (179) \cdot 61 \equiv 10919 \equiv 40 \pmod{253}$. $C_7 = 40$.

$C_8 \equiv 42^3 \pmod{253} = C_8 \equiv 42^2 \cdot 42 \equiv (1764) \cdot 42 \equiv (246) \cdot 42 \equiv 10332 \equiv 212 \pmod{253}$. $C_8 = 212$.

$C_9 \equiv 7^3 \pmod{253} = C_9 \equiv 343 \equiv 90 \pmod{253}$. $C_9 = 90$.

$C_{10} \equiv 101^3 \pmod{253} = C_{10} \equiv 101^2 \cdot 101 \equiv (10201) \cdot 101 \equiv (81) \cdot 101 \equiv 8181 \equiv 85 \pmod{253}$. $C_{10} = 85$.

$C_{12} \equiv 28^3 \pmod{253} = C_{12} \equiv 28^2 \cdot 28 \equiv (784) \cdot 28 \equiv (25) \cdot 28 \equiv 700 \equiv 194 \pmod{253}$. $C_{12} = 194$.

A mensagem codificada fica a seguinte maneira:

$$122 - 6 - 23 - 126 - 111 - 137 - 40 - 212 - 90 - 85 - 6 - 194$$

Perceba que João não poderá unir o bloco para formar um grande número pois, ele não conseguiria recuperar a mensagem original enviada por Maria, devido ao fato que não saberia em quais números aplicar corretamente a função de decodificação. Logo, os blocos devem ficar separados.

5.4.3 Decodificação do RSA

Decodificar os blocos da mensagem enviada por Maria significa encontrar uma função inversa na qual João precisará da chave secreta, o par (n, d). Apenas d é secreto, pois sabemos que n é público.

Vimos anteriormente que o valor d é o inverso multiplicativo de e módulo $\varphi(\mathrm{n})$,ou seja, $\mathrm{d} \cdot \mathrm{e} \equiv 1 \,(\mathrm{mod}\, \varphi(\mathrm{n}))$, com $1 < d < \varphi(n)$. Observe que para decodificar, além do e, precisaremos dos números primos p e q que são os fatores de n. Por isso, é extremamente importante que esses dois números sejam enormes.

Então, sendo $\mathrm{e} = 3$, $\mathrm{p} = 23$ e $\mathrm{q} = 11$ temos que $\mathrm{d} \cdot \mathrm{e} \equiv 1 \left(\mathrm{mod}\, \varphi(\mathrm{n})\right)$, ou seja, $\mathrm{d} \cdot \mathrm{e} \equiv 1\, [\mathrm{mod}\, (\mathrm{p}-1) \cdot (\mathrm{q}-1)] \Longrightarrow 3 \cdot \mathrm{d} \equiv 1 [\mathrm{mod}(22) \cdot (10)] \Longrightarrow 3 \cdot \mathrm{d} \equiv 1 \,(\mathrm{mod}\, 220)$. Pela proposição 4.6 d existe pois, o $\mathrm{mdc}(\mathrm{e}, \varphi(\mathrm{n})) = 1$. Reescrevendo a expressão anterior na forma $3 \cdot \mathrm{d} - 1 = 220 \cdot \mathrm{k}$, depois $3 \cdot \mathrm{d} - 220 \cdot \mathrm{k} = 1$ e aplicando o algoritmo estendido de Euclides, temos:

$$\begin{bmatrix} 3 & 1 & 0 \\ 220 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 1 & 0 \\ 220 - 73 \cdot 3 & 0 - 73 \cdot 1 & 1 - 73 \cdot 0 \end{bmatrix} = \begin{bmatrix} 3 & 1 & 0 \\ 1 & -73 & 1 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 3 - 1 \cdot 3 & 1 - 1 \cdot (-73) & 0 - 1 \cdot 1 \\ 1 & -73 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 74 & -1 \\ 1 & -73 & 1 \end{bmatrix}$$

Portanto, $1 = 3 \cdot (-73) + 1 \cdot 220$ e temos $(-73) \cdot 3 \equiv 1 (\mathrm{mod}\, 220)$. Como d deve ser um número inteiro e positivo, temos que $(-73) \equiv 147 \,(\mathrm{mod}\, 220)$ e então $(147) \cdot 3 \equiv 1 (\mathrm{mod}\, 220)$. Logo, $\mathrm{d} = 147$.

No primeiro bloco codificado $\mathrm{C}_1 = 122$ aplicaremos a função de decodificação $\mathrm{A} \equiv \mathrm{C}^{\mathrm{d}} \,(\mathrm{mod}\, \mathrm{n})$ e teremos $\mathrm{A}_1 \equiv 122^{147} \,(\mathrm{mod}\, 253)$. Para este cálculo, escreveremos expoente 147 na base de potência 2, ou seja, $147 = 2^7 + 2^4 + 2^1 + 1$ e então teremos $\mathrm{A}_1 \equiv 122^{2^7+2^4+2+1} \equiv (122^{2^7}) \cdot (122^{2^4}) \cdot (122^2) \cdot 122 \,(\mathrm{mod}\, 253)$. Para esse bloco, calcularemos o resto de cada potência separadamente e aplicaremos as propriedades da congruência.

$122 \equiv 122 \,(\mathrm{mod}\, 253)$.

$122^2 \equiv 14884 \equiv 210 \,(\mathrm{mod}\, 253)$.

$122^{2^2} \equiv (122^2)^2 \equiv 210^2 \equiv 44100 \equiv 78 \,(\mathrm{mod}\, 253)$.

$122^{2^3} \equiv \left(122^{2^2}\right)^2 \equiv 78^2 \equiv 6084 \equiv 12 \,(\mathrm{mod}\, 253)$.

$122^{2^4} \equiv \left(122^{2^3}\right)^2 \equiv 12^2 \equiv 144 \equiv 144 \,(\mathrm{mod}\, 253)$.

$122^{2^5} \equiv \left(122^{2^4}\right)^2 \equiv 144^2 \equiv 20736 \equiv 243 \,(\mathrm{mod}\, 253)$.

$122^{2^6} \equiv \left(122^{2^5}\right)^2 \equiv 243^2 \equiv 59049 \equiv 100 \pmod{253}$.

$122^{2^7} \equiv \left(122^{2^6}\right)^2 \equiv 100^2 \equiv 10000 \equiv 133 \pmod{253}$. Então:

$A_1 \equiv 122^{147} \equiv \left(122^{2^7}\right) \cdot \left(122^{2^4}\right) \cdot (122^2) \cdot 122 \equiv (133) \cdot (144) \cdot (210) \cdot (122) \equiv (19152) \cdot (25620) \equiv (177) \cdot (67) \equiv 11859 \equiv 221 \pmod{253}$. Portanto, $A_1 = 221$.

Agora, vamos decodificar o bloco A_9, porém ao invés de calcular as potências na base 2, iremos utilizar os recursos que aprendemos no decorrer do trabalho. Isso não significa que o resultado sairá diretamente sem alguns cálculos de potências.

Sabemos que $90^2 \equiv 8100 \equiv 4 \equiv 2^2 \pmod{253}$. Utilizando a proposição 4.4 (item iii), teremos $(90^2)^4 \equiv 90^8 \equiv (2^2)^4 \equiv 2^8 \equiv 3 \pmod{253}$. Ainda, com a proposição 4.4 (item iii) encontramos $(90^8)^5 \equiv 90^{40} \equiv 3^5 \equiv 243 \equiv -10 \pmod{253}$ e novamente, com a proposição anterior $(90^{40})^3 \equiv 90^{120} \equiv (-10)^3 \equiv -1000 \equiv 12 \pmod{253}$.

Pela proposição 4.2 (item i), temos $90 \equiv 90 \pmod{253}$. Através da proposição 4.4 (item i), calculamos $90^8 \cdot 90 \equiv 90^9 \equiv 3 \cdot 90 \equiv 270 \equiv 17 \pmod{253}$. Agora, com a proposição 4.4 (item iii), temos $(90^9)^3 \equiv 90^{27} \equiv 17^3 \equiv 106 \pmod{253}$.

Por último, teremos $90^{120} \cdot 90^{27} \equiv 90^{147} \equiv 12 \cdot 106 \equiv 1272 \equiv 7 \pmod{253}$. Portanto, $A_9 = 7$, como no bloco original. Os outros blocos ficam como exercícios, para que o leitor possa empregar todos os conceitos que vimos no trabalho até o momento.

Dos dois blocos que realizamos como exemplos, podemos fazer duas observações importantes. Primeiramente, com as propriedades de congruências e os teoremas vistos nos capítulos os anteriores os cálculos ficam menores e mais rápidos de serem realizados.

Segundo, fica claro que para João efetuar esses cálculos com papel e lápis, mesmo utilizando as propriedades, é muito demorado. Porém, usando um sistema computacional adequado, ele pode (com maior rapidez) obter os blocos numéricos da mensagem original que Maria enviou, depois utilizando a tabela da subseção 5.4.1 inversamente, trocar os números pelas letras e por fim encontrar o texto enviado por Maria, no caso o estado onde mora.

Agora, a pergunta que fica é: por que funciona? Ou seja, por que decodificando um bloco da mensagem codificada chegamos a um bloco da mensagem original? Vimos no exemplo que a decodificação de dois blocos resultaram nos blocos da mensagem original. Precisamos–nos convencer de que esse fato sempre ocorre.

5.4.4 Explicando o funcionamento do RSA

Imaginemos um sistema RSA com primos p e q, com $n = p \cdot q$. Então, os dados de codificação serão n e e, e os dados de decodificação n e d. Lembrando que a expressão para codificar um bloco é $A_k^e \equiv C_k \pmod{n}$, onde A é um bloco da mensagem original e C o bloco codificado. Dada $A_K \equiv C_K^d \pmod{n}$ a expressão para decodificação $A_K \equiv C_K^d \pmod{n}$, tomemos um bloco A qualquer e a expressão de codificação. Se elevarmos os dois membros da congruência à potência d teremos $(A^e)^d \equiv C^d \pmod{n}$, ou ainda, $A^{d\cdot e} \equiv C^d \equiv A \pmod{p \cdot q}$. Na verdade, queremos provar que $A^{d\cdot e} \equiv A \pmod{p \cdot q}$ pois, já é suficiente devido ao fato de que tanto $A^{d\cdot e}$ quanto A estão no intervalo entre 1 e $n - 1$. Logo, só podem ser congruentes módulo n se forem iguais.

Sendo p e q primos distintos, vamos calcular o resto da divisão de $A^{d\cdot e}$ por p e por q, ou em termos de congruência, encontrar a forma reduzida de $A^{d\cdot e}$ módulo p e módulo q. Como o cálculo é o mesmo para os dois primos, basta executar em um deles. Vamos achar a forma reduzida de $A^{d\cdot e}$ módulo p. Como $d \cdot e \equiv 1 \left(\mathrm{mod}\ \varphi(n)\right)$, então existe $K \in \mathbb{Z}$ tal que $d \cdot e = K \cdot \varphi(n) + 1$ e sendo $\varphi(n) = (p-1) \cdot (q-1)$ temos $d \cdot e = K \cdot (p-1)(q-1) + 1$.

Suponhamos que $p \nmid A$, então pelo pequeno teorema de Fermat teremos $A^{p-1} \equiv 1 \pmod{p}$. Elevando os dois lados da congruência a $k \cdot (q-1)$ e multiplicando por A teremos $(A^{p-1})^{k\cdot(q-1)} \cdot A = A^{[K\cdot(p-1)\cdot(q-1)+1]} = A^{d\cdot e} \equiv A \pmod{p}$.

Por outro lado supondo que $p|A$ então $A \equiv 0 \pmod{p}$ e $A^{d\cdot e} \equiv 0 \pmod{p}$. Logo, também neste caso $A^{d\cdot e} \equiv A \pmod{p}$. Portanto, não importa qual seja o inteiro A sempre teremos $A^{d\cdot e} \equiv A \pmod{p}$.

Analogamente, podemos concluir que $A^{d\cdot e} \equiv A \pmod{q}$. Isto significa que p e q dividem $A^{d\cdot e} - A$. Como $\mathrm{mdc}(p, q) = 1$, temos pela proposição 3.10 que o produto $p \cdot q$ divide $A^{d\cdot e} - A$. Sendo $n = p \cdot q$, concluímos que $A^{d\cdot e} \equiv A \pmod{n}$.

Observemos que $A^{d\cdot e} \equiv A \pmod{n}$ não é calculado diretamente para n pois, com $\mathrm{mdc}(n, A) \neq 1$ não significa necessariamente que $b \equiv 0 \pmod{n}$ já que n é um número composto.

5.4.5 A segurança do RSA

Após vermos todo o processo de pré – codificação, codificação, decodificação e o do funcionamento do sistema RSA, fica a seguinte questão: por que o RSA é tão seguro? Lembramos que essa criptografia é um método de chave pública, onde a chave de codificação (e, n) é acessível a qualquer pessoa. Então, o RSA só será seguro se for extremamente difícil calcular d (a chave de decodificação) quando se conhece n e e.

Mas, sabemos que para determinar d é só aplicar o algoritmo estendido de Euclides entre $\varphi(n)$ e e. Como n é o produto de dois números primos p, q, então o problema se resumirá em fatorar n que é um número muito grande.

Mesmo todo o processo parecendo simples de ser resolvido, é totalmente inviável, pois não existem computadores rápidos nem mesmo algoritmos eficientes o suficiente, que permitam fatorar um número inteiro tão enorme em um tempo hábil. Pode – se mostrar que o tempo que se precisa para a fatoração de um número de uns cem algarismos pelo método tradicional excede e muito a idade estimada do universo. Na verdade não existe nenhum algoritmo conhecido que seja capaz de fatorar números inteiros grandes de modo eficiente e não se sabe nem mesmo da existência de um algoritmo que realize essa fatoração (Hefez).

Atualmente, as transações comerciais que utilizam o RSA usam chaves públicas com cerca de 200 algarismos, logo decifrar uma mensagem criptografada com o sistema RSA é quase impossível.

Outro detalhe, no nosso exemplo falamos que a utilização de congruência facilitaria as “contas”. Entretanto, para uma aplicação comercial do RSA necessitaríamos calcular potências de números muito grandes, com módulos imensos e esse processo não é viável sem o uso da aritmética modular, ou seja, não é questão de facilidade mas sem essa aritmética os cálculos seriam impossíveis.

Considerações

Os Parâmetros Curriculares Nacionais para o Ensino Médio, nos dizem que o ensino de matemática deve permitir aos alunos "*compreender as ciências como construções humanas, entendendo como elas se desenvolvem por acumulação, continuidade ou ruptura de paradigmas e compreender conceitos, procedimentos e estratégias matemáticas e aplica – las a situações diversas".*

Como a criptografia tem um papel importante nos dias atuais, por exemplo, na segurança de transações eletrônicas, nos dígitos de verificação do CPF ou nos navegadores de internet, sua aplicação em sala de aula poderá despertar o interesse de alunos e professores, pois os conceitos matemáticos que estão presentes na criptografia dão ao professor a oportunidade de explorar, juntamente com os alunos, diversos conteúdos inseridos na grade curricular do ensino Médio.

A ideia apresentada neste trabalho é abordar conteúdos que os alunos têm contato durante a sua passagem pelo ensino Fundamental e Médio, mas que muitas vezes é feito de modo tradicional, ou seja, explicação do professor, exemplos e exercícios de fixação, de uma maneira que possibilite ao aluno desenvolver realmente o que os PCN'S nos indicam atualmente.

Acreditamos também que este trabalho possa motivar o professor de matemática do ensino Médio a aprimorar sua prática em sala de aula, introduzindo os conceitos que estão ligados a criptografia, incluindo o sistema RSA. Alguns desses conceitos, como números primos são vistos no ensino Fundamental II, mas somente como uma ferramenta para fatoração de números compostos e depois ficam esquecidos. Outros desses conceitos como a aritmética dos restos, congruência, equações *diofantinas* lineares e o algoritmo estendido de Euclides não estão na grade curricular do ensino Fundamental nem do Médio, mas podem ser introduzidos a fim de aguçar a curiosidade dos alunos.

Por fim, vemos que introduzir um tema atual como criptografia em sala de aula, abre um grande leque para o desenvolvimento de conceitos e estratégias matemáticas. Além disso, a forma como a criptografia foi introduzida durante o processo de desenvolvimento humano pode também ser um fator de atração da atenção do aluno, retirando a ideia de que a matemática se limita apenas ao contexto escolar.

Referências

ALMEIDA, M. F. L. B. P.; GIUDICE, M. D. **Criptografia RSA, dízimas periódicas, e o ensino de álgebra**. In: Seminário de Pesquisa em Educação Matemática do Estado do Rio de Janeiro, VI, 2008. Acesso em: 02 Mai. de 2014. Disponível em: <http://www.sbemrj.com.br>.

BOYER, Carl Benjamin. **História da matemática**. Tradução: Elza F. Gomide. São Paulo: Editora Edgard Blucher, 1974.

BRASIL. **Parâmetros Curriculares Nacionais**: Matemática, 1997. Acesso em: 12 de Ago. de 2015. Disponível em: <http://portal.mec.gov.br>.

CARTER P.J. **250 códigos de quebra cabeça**. Tradução: Martha Malvezzi. São Paulo: Editora Madras, 2007.

COUTINHO, S.C. **Números inteiros e Critografia RSA**. Série de Computação e Matemática. 2ed. Rio de Janeiro: IMPA/SBM, 2013.

COUTINHO, S.C. **Criptografia-Programa de Iniciação Científica OBMEP**. Rio de Janeiro: Editora da SBM, 2009.

DOMINGUES, Higino H. **Fundamentos de Aritmética**. São Paulo: Editora Atual, 1991.

HEFEZ, Abramo. **Aritmética**. Coleção PROFMAT. 1ªed. Rio de Janeiro: Editora da SBM, 2013.

HEFEZ, Abramo. **Elementos de Aritmética**. Coleção textos Universitários. 2ªed. Rio de Janeiro: Editora da SBM, 2011.

HEFEZ, Abramo. **Iniciação à Aritmética-Programa de Iniciação Científica OBMEP**. Rio de Janeiro: Editora da SBM, 2012.

IEZZI, Gelson. **Fundamentos de Matemática Elementar-Volume 1**. 7ªed. São

Paulo: Editora Atual, 1993.

LIMA E.L.; CARVALHO P.C.P.; WAGNER E.; MORGADO A..C. **A Matemática do Ensino Médio-Volume 1**. 10ªed. Rio de Janeiro: SBM, 2012.

LUZ, Welington Batista. **Introdução à Matemática do Criptossistema RSA**. Dissertação (Mestrado) Universidade Federal do Sergipe, São Cristóvão, 2013. Acesso em: 29 Jul. de 2014. Disponível em: <www.bit.profmat- sbm.org.br>

OKUMURA, Mirella Kiyo. **Números primos e criptografia RSA**. Dissertação (Mestrado) Universidade São Paulo (USP), São Carlos, 2014. Acesso em: 11 Jul. de 2014. Disponível em: <www.bit.profmat- sbm.org.br>

ROQUE, Tatiana. **História da Matemática**: uma visão crítica, desfazendo mitos e lendas. Rio de Janeiro: Editora Jorge Zahar, 2012.

SANTOS, José L. **A Arte de Cifrar, Criptografar, Esconder e Salvaguardar como Fontes Motivadores para Atividades de Matemática Básica**. Dissertação (Mestrado) Universidade Federal da Bahia (UFBA), Salvador, 2013. Acessado em: 02 de Mai. de 2014. Disponível em: <www.bit.profmat- sbm.org.br>

SANTOS, José Plínio de Oliveira. **Introdução à Teoria dos Números**. 3ªed. Rio de Janeiro: IMPA,2014.

SAUTOY, Marcus du. **Os Mistérios dos Números**: uma viagem pelos grandes enigmas da Matemática. Tradução: George Schlesinger. Rio de Janeiro: Editora Zahar, 2013.

SAUTOY, Marcus du. **A música dos números primos**: a história de um problema não resolvido na Matemática. Tradução: Diego Alfaro. Rio de Janeiro: Editora Jorge Zahar, 2007.

SINGH, Simon. **O Livro dos Códigos**: a ciência do sigilo – do antigo Egito à criptografia quântica. 7ªed. São Paulo: Editora Record, 2010.