UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO, DE CIÊNCIAS EXATAS E EDUCAÇÃO
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

Michel Ricardo Borchardt

Aritmética Modular com Aplicação à Criptografia RSA e Algumas Propostas de Sequências Didáticas na Educação Básica

Blumenau
2024

Michel Ricardo Borchardt

Aritmética Modular com Aplicação à Criptografia RSA e Algumas Propostas de Sequências Didáticas na Educação Básica

Dissertação submetida ao Mestrado Profissional em Matemática em Rede Nacional da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do título de Mestre em Matemática.

Orientador(a): Prof. Felipe Delfini Caetano Fidalgo, Dr.

Blumenau

2024

Ficha catalográfica gerada por meio de sistema automatizado gerenciado pela BU/UFSC.
Dados inseridos pelo próprio autor.

Borchardt, Michel Ricardo
Aritmética Modular com Aplicação à Criptografia RSA e Algumas Propostas de Sequências Didáticas na Educação Básica / Michel Ricardo Borchardt ; orientador, Felipe Delfini Caetano Fidalgo, 2024.
71 p.

Dissertação (mestrado profissional) - Universidade Federal de Santa Catarina, Campus Blumenau, Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Blumenau, 2024.

Inclui referências.

1. Matemática. 2. Criptografia. I. Fidalgo, Felipe Delfini Caetano. II. Universidade Federal de Santa Catarina. Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT. III. Título.

Michel Ricardo Borchardt

Aritmética Modular com Aplicação à Criptografia RSA e Algumas Propostas de Sequências Didáticas na Educação Básica

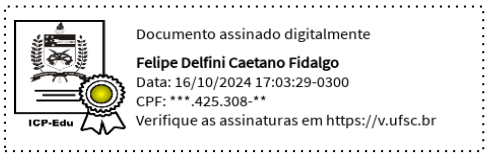
O presente trabalho em nível de Mestrado foi avaliado e aprovado, em 01 de agosto de 2024, pela banca examinadora composta pelos seguintes membros:

Prof. Felipe Delfini Caetano Fidalgo, Dr.
Universidade Federal de Santa Catarina - UFSC

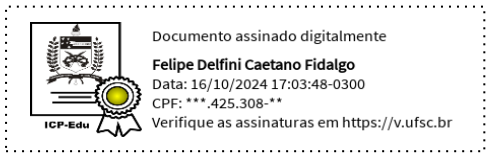
Prof. Francis Felix Cordova Puma, Dr.
Universidade Federal de Santa Catarina - UFSC

Prof.(a) Edson Donizete de Carvalho, Dr.
Universidade Estadual Paulista - UNESP

Certificamos que esta é a versão original e final do trabalho de conclusão que foi julgado adequado para obtenção do título de Mestre em Matemática.



Coordenação do Programa de Pós-Graduação



Prof. Felipe Delfini Caetano Fidalgo, Dr.
Orientador

Blumenau, 2024.

Dedico este trabalho à minha mãe, Maria Salete Klitzke, e à memória da minha Oma, Lina Krehnke Klitzke.

AGRADECIMENTOS

A conclusão deste mestrado é resultado de uma série de fatores, influenciados por muitas pessoas ao longo da minha vida. Por isso, gostaria de expressar aqui meus mais sinceros agradecimentos.

À minha mãe, Maria Salete Klitzke, que apesar de não ter tido a oportunidade de estudar além dos Anos Iniciais do Ensino Fundamental, sempre me incentivou a seguir os estudos, me mostrou o valor transformador da educação e o quanto ela poderia mudar a minha vida. Ela foi, para mim, um exemplo impecável de dedicação, esforço e doação.

À minha Oma, Lina Krehnke Klitzke, em memória, por ter cuidado de mim com tanto carinho e por transmitir valores que levo comigo diariamente, tanto na vida pessoal quanto na profissional.

À minha namorada, Rafaela Michalak, por representar a parte mais feliz dos meus dias e por me ensinar, a cada dia, a ser uma pessoa melhor.

Ao ex-colega de trabalho Nathan Lubawski, com quem compartilhei uma profunda amizade e uma rivalidade saudável, que resultou nos anos em que mais aprendi matemática. É oportuno agradecer a todos os alunos que participaram das turmas de treinamento para as Olimpíadas de Matemática, nas quais eu e Nathan lecionamos. Saibam que, além de contribuirmos para o crescimento de vocês, nós também evoluímos muito com esse trabalho.

Ao Prof. Me. Cristiano Rodolfo Tironi, cujas aulas me fizeram apaixonar pela matemática desde o Ensino Fundamental e me ajudaram a dar os primeiros passos nessa maravilhosa ciência.

À todos que contribuíram para que a OBMEP se tornasse uma realidade neste país, proporcionando oportunidades a milhares de jovens apaixonados pela matemática nas escolas públicas, assim como eu. Se não fosse por esse importante projeto, com certeza não teria alcançado as conquistas que tenho hoje. Deixo aqui um agradecimento especial à Profª. Dra. Andresa Pescador, tive a honra de participar de suas aulas no PIC – Programa de Iniciação Científica Júnior da OBMEP.

Expresso aqui minha gratidão a todo o corpo docente do PROFMAT da UFSC-Blumenau, em especial aos professores que lecionaram para a turma de 2021. Todos contribuíram significamente para o meu crescimento no campo da matemática, e cada um, com suas características únicas, me inspirou a ser um professor melhor por meio

de suas aulas excepcionais. Gostaria de fazer um agradecimento especial ao meu orientador, Dr. Felipe Delfini Caetano Fidalgo, e aos professores Dr. Francis Felix Cordova Puma (UFSC-Blumenau) e Dr. Edson Donizete de Carvalho (UNESP), por aceitarem compor a banca deste trabalho e oferecerem valiosas sugestões. Também não posso deixar de agradecer a todos que, de alguma forma, contribuíram para a construção do PROFMAT. Ter um mestrado profissional público de excelência, oferecido em Universidades Federais e outras instituições de grande renome, e organizado pelo IMPA – Instituto de Matemática Pura e Aplicada, é fundamental para um país que busca aprimorar a formação de seus professores de matemática. Sem esse programa, dificilmente teria tido a oportunidade de concluir um mestrado em uma instituição tão prestigiosa como a UFSC.

Aos meus amigos, em especial ao grande parceiro Sidnei Rodrigo dos Santos, que considero não apenas um grande amigo, mas também um ser humano admirável, dotado de um raciocínio lógico ímpar, com quem sempre tive o prazer de compartilhar conversas enriquecedoras. Quero também deixar meu agradecimento à minha colega de trabalho e amiga Daiana da Silva, que esteve sempre disposta a me ouvir, compreender e oferecer sábios conselhos nos momentos difíceis que enfrentei este ano.

Por fim, deixo meus agradecimentos a todas as inúmeras pessoas que, de alguma forma, contribuíram para a conclusão deste mestrado.

RESUMO

Este trabalho apresenta a fundamentação matemática que serve como base para a Criptografia RSA, aborda de forma breve a história da criptografia, enaltecendo sua importância desde a Antiguidade até os tempos modernos, e explica através da matemática porque a Criptografia RSA funciona. O presente trabalho possui como objetivo apresentar algumas propostas de sequências didáticas que possam ser úteis a professores de matemática da Educação Básica, envolvendo conteúdos de Aritmética, inclusive problemas envolvendo conceitos de Aritmética Modular, trazendo atividades práticas e contextualizadas que visam colocar o aluno no papel de protagonista no processo de ensino e aprendizagem e um cidadão consciente da importância da segurança da informação nos tempos modernos.

Palavras-chave: Criptografia; Aritmética Modular; Sequência Didática.

ABSTRACT

This work presents the mathematical foundation that serves as the basis for RSA Cryptography, briefly discusses the history of cryptography, highlighting its importance from Antiquity to modern times, and explains through mathematics why RSA Cryptography works. The present study aims to present some proposals for didactic sequences that may be useful to mathematics teachers in Basic Education, involving Arithmetic contents, including problems involving concepts of Modular Arithmetic, bringing practical and contextualized activities that aim to put the student in the role of protagonist in the teaching and learning process and a citizen aware of the importance of information security in modern times.

Keywords: Cryptography; Modular Arithmetic; Didactic Sequences.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Atualmente a educação matemática tem sido cada vez mais desafiada a proporcionar experiências de aprendizagens significativas e contextualizadas, que preparem os estudantes para enfrentar os desafios de um mundo em constante transformação. O modelo de ensino tradicional, sem dar a devida importância a contextualização, a utilização da tecnologia e a investigação no processo de ensino e aprendizagem se mostra pouco eficaz, pois foca apenas na memorização de técnicas e algoritmos, desencorajando o interesse dos alunos pela matéria. Segundo Pereira (2004)

> Todas as crianças chegam à escola com muitas experiências matemáticas já realizadas ainda que de forma inocente. A curiosidade em aprender, conhecer e experimentar são sentimentos naturais que não devem ser frustrados ou inibidos com aulas “mortas” nas quais se aplicam fórmulas e se treinam raciocínios e técnicas (sem grande utilidade, no entender dos mesmos). (Pereira, 2004, p.19).

Ao trabalhar com projetos ou utilizar a tecnologia em sala de aula ainda é comum ouvir expressões como “mas isto aqui não vai cair no ENEM”, “em provas oficiais não deixam usar a calculadora”. É claro que em si, estas frases não estão erradas. No entanto, ao analisarmos de forma mais ampla, o papel da escola na formação do aluno não consiste em prepará-lo para fazer uma prova no final do Ensino Médio. É preciso considerar o aluno em sua totalidade, desenvolver nele não apenas aspectos intelectuais, mas também emocionais, sociais, culturais, preparando-o assim para ser um cidadão crítico, autônomo e consciente em meio a sociedade. Segundo a Base Nacional Comum Curricular (BNCC):

> A sociedade contemporânea impõe um olhar inovador e inclusivo a questões centrais do processo educativo: o que aprender, para que aprender, como ensinar, como promover redes de aprendizagem colaborativa e como avaliar o aprendizado. (BRASIL, 2018, p. 14).

Em relação a tecnologia na sala de aula, ela tornou-se uma excelente aliada na realização de recursos e ambientes virtuais que possibilitam aos estudantes interagirem com muitos conceitos matemáticos dinâmicos e visualmente atraentes. Os

softwares, aplicativos e recursos online, como por exemplo, GeoGebra, Kahoot, PhetColorado, Poly, entre outros, além de contribuírem para o desenvolvimento de aulas mais interessantes e atrativas, despertam no estudante o interesse pela matemática, podendo ainda se revelar uma ferramenta poderosa para instigar nos alunos o espírito de investigação matemática. Ao tratar da produção científica, a tecnologia assume um papel ainda mais fundamental. O Crivo de Eratóstenes, apresentado neste trabalho como uma ferramenta para encontrar números primos, torna-se limitado para os propósitos da criptografia sem o apoio de ferramentas tecnológicas. Os maiores números primos já descobertos foram identificados por meio de algoritmos mais avançados e testes de primalidade, que só se tornaram viáveis graças à evolução tecnológica. Assim, tanto os números primos utilizados na criptografia RSA quanto os maiores já encontrados são resultado direto dos avanços tecnológicos. Segundo a Base Nacional Comum Curricular (BNCC), uma das Competências Gerais da Educação Básica é

> Compreender, utilizar e criar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais (incluindo as escolares) para se comunicar, acessar e disseminar informações, produzir conhecimentos, resolver problemas e exercer protagonismo e autoria na vida pessoal e coletiva. (BRASIL, 2018, p. 9).

Sobre a metodologia da investigação matemática, os Parâmetros Curriculares Nacionais (PCN) afirmam que

> O exercício da indução e da dedução em Matemática reveste-se de importância no desenvolvimento da capacidade de resolver problemas, de formular e testar hipóteses, de induzir, de generalizar e de inferir dentro de determinada lógica, o que assegura um papel de relevo ao aprendizado dessa ciência em todos os níveis de ensino. (BRASIL, 1998, p. 26).

Através disso, pode-se fazer a seguinte reflexão utilizando um exemplo prático de uma aula de Geometria: Qual aula apresenta uma abordagem mais eficaz pensando em obtermos uma aprendizagem significativa? Aquela em que o professor informa que a soma dos ângulos internos de um triângulo sempre é igual a 180° e passa alguns exercícios de fixação para que o aluno pratique e memorize a

propriedade mencionada, ou uma aula onde o aluno utiliza o GeoGebra e é levado a perceber que a soma dos ângulos dos triângulos que ele está desenhando, assim como a dos triângulos que seus colegas estão desenhando sempre tem o mesmo valor, onde ele acaba de fazer uma descoberta incrível, e pode começar a fazer indagações para si mesmo, colegas e professores, será que isso dará certo para todos os triângulos? Pode tentar achar um triângulo cuja soma dos ângulos dê um resultado diferente. Esta simples experiência utilizando a tecnologia e colocando o aluno no papel de protagonista no processo de ensino e aprendizagem já abre uma oportunidade para o professor abordar estes questionamentos e falar sobre a importância das demonstrações na Matemática, inclusive o professor poderia ainda utilizar o próprio GeoGebra como ferramenta auxiliar para demonstrar a seus alunos que de fato o que eles descobriram é válido para qualquer triângulo. E não para por aí,... e se pensarmos nos outros polígonos, será que a soma também será 180°? Será que terá um valor fixo?... este tipo de abordagem onde o aluno testa, faz questionamentos, realiza descobertas, precisa argumentar para defender tais descobertas, todo este processo de investigação matemática é muito mais propício para uma aprendizagem significativa do que uma simples propriedade copiada do quadro a qual o aluno acha que não serve para nada ou que a função dele ali na escola é decorar tal propriedade para a prova.

Neste contexto onde o cotidiano, a utilização da tecnologia e a investigação matemática são indispensáveis para uma aprendizagem mais significativa, o presente trabalho busca apresentar propostas de sequências didáticas que coloquem o aluno no papel de protagonista no processo de ensino e aprendizagem abordando aplicações de Aritmética e Criptografia.

Sobre Criptografia, segundo Singh (2002), um de seus objetivos ao escrever o livro *The Code Book* foi traçar a evolução dos códigos durante a história. Para ele, um código está constantemente sob ataque de decifradores. Quando os decifradores desenvolvem uma nova arma que revela a fraqueza de um código, esse código deixa de ser útil. Ele se torna extinto ou evolui para um novo código, mais forte. Por sua vez, este novo código prospera apenas até que os decifradores identifiquem sua fraqueza, e assim por diante. Dessa maneira, Singh demonstra que todas as formas de criptografia, desde as mais básicas, como a Cifra de César, até as mais avançadas, como a Criptografia RSA, desempenharam um papel crucial dentro de seus

respectivos contextos históricos. Este trabalho também apresentará um breve panorama sobre a evolução da criptografia conforme mencionada por Singh.

O presente trabalho organiza-se da seguinte forma: No capítulo 2 busca-se fundamentar a teoria matemática que sustenta a Criptografia RSA; já no capítulo 3 apresenta-se brevemente a história da Criptografia e explica-se detalhadamente a matemática que valida o sistema de Criptografia RSA; por fim, no capítulo 4, são apresentadas algumas propostas de sequências didáticas com a expectativa de que sejam úteis a professores de matemática do Ensino Básico que venham ter acesso a este estudo.

2 PRELIMINARES MATEMÁTICAS

2.1 O CONJUNTO DOS NÚMEROS NATURAIS

Com base em Ferreira (2011), o desenvolvimento do conceito de número ao longo da história é semelhante à forma como as crianças aprendem sobre números. Tanto as crianças quanto a humanidade começaram a entender os números naturais através da contagem. Os gregos antigos, na época de Euclides, consideravam como números apenas os naturais maiores que 1, com o 1 sendo visto como a unidade básica. O conceito de zero surgiu mais tarde, nos primeiros séculos da era cristã, criado pelos hindus para a numeração escrita. Para as crianças, aprender a contar só faz sentido a partir do número 2, já que elas precisam de algo concreto para contar. O entendimento do zero vem depois de alguns anos de prática com a contagem dos números “de verdade”, que acontece no começo da aprendizagem formal da numeração da escrita.

A fim de tornar o trabalho auto contido sem se tornar demasiadamente prolixo ou de se perder o foco, as demonstrações da maioria dos resultados da seção foram omitidas, mas podem ser encontradas em Ferreira (2011).

Apresentamos o Conjunto dos Números Naturais ($\mathbb{N}$) a partir dos axiomas de Peano, são eles:

1. Existe uma função injetiva $s: \mathbb{N} \to \mathbb{N}$. Chamamos a imagem $s(n)$ de cada número natural n de sucessor de n.
2. Existe um único número natural $0 \in \mathbb{N}$, tal que $0 \neq s(n)$ para todo $n \in \mathbb{N}$.

3. Se um conjunto $X \subset \mathbb{N}$ é tal que $0 \in X$ e para todo $n \in X$ temos que $s(n) \in X$, então $X = \mathbb{N}$.

O axioma 3 é conhecido como Princípio da Indução, frequentemente utilizado como uma poderosa ferramenta de demonstração de propriedades sobre os números naturais. O Princípio da Indução afirma que se uma propriedade P é válida para o número 0, e se ao supor que ela é válida para um natural n conclui-se que ela é válida para seu sucessor $s(n)$, ou seja, $P(n) \Rightarrow P(s(n))$, então a propriedade P é válida para todos os números naturais.

Intuitivamente, o axioma 3 indica que todo número natural pode ser encontrado a partir de 0, tomando-se quantas vezes forem necessárias o sucessor do número obtido: $0, s(0), s\big(s(0)\big), s\Big(s\big(s(0)\big)\Big)$... A partir disso, tomando $1 = s(0), 2 = s\big(s(0)\big), 3 = s\Big(s\big(s(0)\big)\Big)$, ... podemos estabelecer uma correspondência entre o conjunto $\mathbb{N}$ construído pelos axiomas de Peano e o conjunto usual $\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$. Além de $\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$, podemos destacar o subconjunto dos números naturais não-nulos, que será representado por $\mathbb{N}^* = \{1, 2, 3, 4, \dots\}$

O conjunto $\mathbb{N}$ dos números naturais é munido de duas operações fundamentais, a adição e a multiplicação que são definidas a seguir.

Definição 2.1.1: A operação de adição associa a cada par de números naturais (m, n) sua soma $m + n$ de forma com que

$$(i)\ m + 0 = m$$

$$(ii)\ m + s(n) = s(m + n)$$

Definição 2.1.2: Indicaremos como 1, o número natural que é sucessor de 0, ou seja, $1 = s(0)$.

Proposição 2.1.1: Para todo número natural n, temos que $s(n) = n + 1$ e $s(n) = 1 + n$.

Definição 2.1.3: A operação de multiplicação associa a cada par de números naturais (m, n) seu produto $m \cdot n$ de forma com que

$$(i)\ m \cdot 0 = 0$$

$$(ii)\ m \cdot (n + 1) = m \cdot n + m$$

Dados $m, n, p \in \mathbb{N}$, e $t \in \mathbb{N}^*$ são válidas as seguintes propriedades da adição e multiplicação de números naturais:

1. Associatividade: $(m + n) + p = m + (n + p), \quad m \cdot (n \cdot p) = (m \cdot n) \cdot p$

2. Distributividade: $m \cdot (n + p) = m \cdot n + m \cdot p$
3. Existência de Elemento Neutro: $m + 0 = m, \quad m \cdot 1 = m.$
4. Comutatividade: $m + n = n + m, \quad m \cdot n = n \cdot m$
5. Lei do Corte: $m + n = m + p \Rightarrow n = p, \quad t \cdot n = t \cdot p \Rightarrow n = p.$

Por fim, podemos estabelecer no conjunto dos números naturais a relação $m \leq n$ a partir da definição que se segue.

Definição 2.1.4: Dados $m, n \in \mathbb{N}$, dizemos que m é menor ou igual a n, escreve-se $m \leq n$ se existe $p \in \mathbb{N}$, tal que $n = m + p$. Se p for não-nulo, dizemos que m é menor do que n, ou ainda que n é maior do que m, neste caso escreve-se, respectivamente, que $m < n$ ou $n > m$.

Dados $m, n, p \in \mathbb{N}$, a relação de ordem $m \leq n$ é uma relação de ordem, pois possui as seguintes propriedades:

1. Reflexiva: Para todo $m \in \mathbb{N}$ temos que $m \leq m$.
2. Antissimétrica: Se $m \leq n$ e $n \leq m$, então $m = n$.
3. Transitiva: Se $m \leq n$ e $n \leq p$, então $m \leq p$.

Ainda, dados $m, n, p \in \mathbb{N}$, a relação $m < n$ possui as seguintes propriedades:

4. Transitiva: Se $m < n$ e $n < p$, então $m < p$.
5. Tricotomia: É válida uma, e apenas uma das três alternativas a seguir: $m = n$, $m < n$, $m > n$.
6. Monotonicidade: Se $m < n$ então, para qualquer p natural tem-se que $m + p < n + p$ e se p ainda for diferente de zero temos que $m \cdot p < n \cdot p$.

Proposição 2.1.2 (Princípio da Boa-Ordenação): Todo subconjunto não vazio de números naturais possui um menor elemento.

Demonstração: Seja S tal subconjunto de $\mathbb{N}$, consideremos o conjunto $M = \{n \in \mathbb{N}; n \leq x, \forall x \in S\}$. Claro que $0 \in M$. Como $S \neq \emptyset$, tome $s \in S$. Então $s + 1 \notin M$, pois $s + 1$ não é menor ou igual a s. Assim, $M \neq \mathbb{N}$. Como $0 \in M$ e $M \neq \mathbb{N}$, deve existir $m \in M$ tal que $m + 1 \notin M$, caso contrário, pelo Princípio de Indução, M deveria ser $\mathbb{N}$.

Afirmamos que um tal m é o menor elemento de S. Como $m \in M$, então $m \leq x, \forall x \in S$. Só falta verificar que $m \in S$. Vamos supor o contrário, que $m \notin S$. Então $m < x, \forall x \in S$. Assim, teríamos $m + 1 \leq x, \forall x \in S$, do que resultaria $m + 1 \in M$, em contradição com a escolha de m. Logo, $m \in S$.

■

2.2 CONSTRUÇÃO DOS NÚMEROS INTEIROS POR RELAÇÕES DE EQUIVALÊNCIA

Passamos, agora, a construir o conjunto dos números inteiros a partir de classes de equivalência de números naturais. Tal construção está baseada em Ferreira (2011). Antes, uma passagem teórica necessária sobre relações de equivalência baseada em Halmos (1960).

Definição 2.2.1: O par-ordenado de primeira coordenada a e segunda coordenada b é definido como $(a, b) = \{\{a\}, \{a, b\}\}$.

Definição 2.2.2: Dados dois conjuntos A e B, define-se o produto cartesiano de A por B, denotado por $A \times B$, como o conjunto $A \times B = \{(x, y); x \in A \text{ e } y \in B\}$.

Definição 2.2.3: Dados dois conjuntos A e B. Uma relação binária R é qualquer subconjunto de $A \times B$.

Seja R uma relação binária com $R \subseteq A \times B$, é comum utilizar a notação xRy para representar que $(x, y) \in R$.

Ao se tratar de relações binárias, geralmente usaremos apenas o termo relação.

Pensaremos nas relações de equivalência como sendo relações binárias em A que possuem a propriedade reflexiva, simétrica e transitiva.

Definição 2.2.4: A relação binária $\equiv$ sobre A é uma relação de equivalência se para todo $a, b, c \in A$ valem as seguintes propriedades:

1. Reflexiva: $a \equiv a$
2. Simétrica: Se $a \equiv b$, então $b \equiv a$
3. Transitiva: Se $a \equiv b$ e $b \equiv c$, então $a \equiv c$.

Definição 2.2.5: Chamamos de classe de equivalência de um elemento $a \in A$, o conjunto $\overline{(a)} = \{x \in A; x \equiv a\}$.

Definição 2.2.6: Chamamos de conjunto quociente de A, e denotamos por $A/\equiv$ o conjunto formado por todas as classes de equivalência de A.

Definição 2.2.7: Seja R uma relação binária em A. Diz-se que R é uma relação de ordem parcial não restrita se, e somente se, R é reflexiva, antissimétrica e transitiva. Diz-se ainda que R é uma relação de ordem total se além das propriedades acima citadas, para todo $x, y \in A$, temos que xRy ou yRx.

A construção do conjunto dos números inteiros irá se basear nas operações e elementos do conjunto dos números naturais.

Considere o conjunto $\mathbb{N} \times \mathbb{N}$ e sobre ele a relação $\equiv$ definida como $(a, b) \equiv (c, d)$ se, e somente se, $a + d = b + c$.

Exemplos: Note que $(4,3) \equiv (7,6)$, pois $4 + 6 = 7 + 3$. Já $(2,5) \not\equiv (3,8)$, pois $2 + 8 \neq 5 + 3$.

Observação: Intuitivamente podemos pensar que $(a, b) \equiv (c, d)$ se, e somente se, $a - b = c - d$, no entanto, formalmente não podemos utilizar a subtração, nem mesmo como soma de números negativos pois ambos ainda não foram definidos.

Proposição 2.2.1: A relação $\equiv$ é uma relação de equivalência.

Demonstração: Devemos mostrar que a relação $\equiv$ é munida das propriedades reflexiva, simétrica e transitiva.

Reflexiva: Dado $(a, b) \in \mathbb{N} \times \mathbb{N}$, pela propriedade comutativa da adição nos naturais, temos que $a + b = b + a$, logo $(a, b) \equiv (a, b)$.

Simétrica: Considere $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$. Queremos mostrar que se $(a, b) \equiv (c, d)$, então $(c, d) \equiv (a, b)$. Da hipótese temos que $(a, b) \equiv (c, d)$, logo $a + d = b + c$, novamente da propriedade comutativa nos naturais segue que $c + b = d + a$, daí $(c, d) \equiv (a, b)$.

Transitiva: Considere $(a, b), (c, d), (e, f) \in \mathbb{N} \times \mathbb{N}$. Devemos mostrar que se $(a, b) \equiv (c, d)$ e $(c, d) \equiv (e, f)$, então $(a, b) \equiv (e, f)$. Da hipótese de que $(a, b) \equiv (c, d)$ e $(c, d) \equiv (e, f)$ segue, respectivamente, que $a + d = b + c$ e $c + f = d + e$. Somando ambas as igualdades temos que $(a + d) + (c + f) = (b + c) + (d + e)$. Reorganizando a igualdade obtemos que $a + f + (c + d) = b + e + (c + d)$. Daí, pela Lei do Corte da adição segue que $a + f = b + e$, portanto $(a, b) \equiv (e, f)$.

■

Dado um elemento $(a, b) \in \mathbb{N} \times \mathbb{N}$, considere a classe de equivalência de (a, b) como sendo o conjunto $\overline{(a, b)} = \{(x, y) \in \mathbb{N} \times \mathbb{N}; (x, y) \equiv (a, b)\}$.

Definição 2.2.8: Chamamos de Conjunto dos Números Inteiros e denotamos por $\mathbb{Z}$, o conjunto quociente $\mathbb{N} \times \mathbb{N}/\equiv$ formado por todas as classes de equivalência de $\mathbb{N} \times \mathbb{N}$.

A partir da construção do conjunto dos números inteiros ($\mathbb{Z}$) pode-se definir nele as operações de adição e multiplicação como segue abaixo.

Definição 2.2.9: Dados $\alpha, \beta \in \mathbb{Z}$, com $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$. Definimos a soma $\alpha + \beta$ e o produto $\alpha \cdot \beta$, respectivamente, como

$$\alpha + \beta = \overline{(a+c, b+d)}$$

$$\alpha \cdot \beta = \overline{(ac+bd, ad+bc)}$$

Para mostrar que as operações de soma e multiplicação estão bem definidas em $\mathbb{Z}$, precisamos provar que a soma e o produto não dependem da escolha dos elementos da classe de equivalência. Para tal, seguem as demais proposições.

Proposição 2.2.2: Considere $\overline{(a,b)}, \overline{(a',b')}, \overline{(c,d)}, \overline{(c',d')} \in \mathbb{Z}$. Se $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')}$, então $\overline{(a,b)} + \overline{(c,d)} = \overline{(a',b')} + \overline{(c',d')}$.

Demonstração: Do fato de que $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')}$ temos, respectivamente, que $(a,b) \equiv (a',b')$ e $(c,d) \equiv (c',d')$, ou seja, $a + b' = b + a'$ e $c + d' = d + c'$. Somando estas equações obtemos que $(a+b') + (c+d') = (b+a') + (d+c')$. Reorganizando a ordem das parcelas temos que $(a+c) + (b'+d') = (b+d) + (a'+c')$. Daí, $(a+c, b+d) \equiv (a'+c', b'+d')$, o que implica que $\overline{(a+c, b+d)} = \overline{(a'+c', b'+d')}$ e finalmente da definição de adição segue que $\overline{(a,b)} + \overline{(c,d)} = \overline{(a',b')} + \overline{(c',d')}$.

■

Proposição 2.2.3: Considere $\overline{(a,b)}, \overline{(a',b')}, \overline{(c,d)}, \overline{(c',d')} \in \mathbb{Z}$. Se $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')}$, então $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c',d')}$.

Demonstração: Como $\overline{(a,b)} = \overline{(a',b')}$ temos que $a + b' = b + a'$. Multiplicando ambos os membros desta igualdade primeiramente por c e depois por d obtemos as seguintes igualdades,

$$\begin{cases} ca + cb' = cb + ca' \\ da + db' = db + da' \end{cases} \Rightarrow \begin{cases} ac + b'c = bc + a'c \\ bd + a'd = ad + b'd \end{cases}$$

Daí, somando os membros das equações obtemos

$$ac + bd + a'd + b'c = ad + bc + a'c + b'd$$

Mas isto implica que

$$\overline{(ac+bd, ad+bc)} = \overline{(a'c+b'd, a'd+b'c)}$$

$$\Rightarrow \overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c,d)}$$

De forma análoga, partindo do fato de que por hipótese $\overline{(c,d)} = \overline{(c',d')}$, o que implica que $c + d' = d + c'$ e multiplicando ambos os membros desta igualdade primeiramente por a' e depois por b', concluímos que

$$\overline{(a',b')} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c',d')}$$

Logo, por transitividade temos que $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c',d')}$.

■

As operações de soma e multiplicação nos inteiros estão munidas das seguintes propriedades que são apresentadas abaixo seguidas de suas respectivas demonstrações:

Proposição 2.2.4: (Propriedade Associativa da Adição): Dados $\alpha, \beta, \gamma \in \mathbb{Z}$, temos que $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.

Demonstração: Considere $\alpha = \overline{(a,b)}, \beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$. Segue que

$$(\alpha + \beta) + \gamma = \left(\overline{(a,b)} + \overline{(c,d)}\right) + \overline{(e,f)} = \overline{(a+c, b+d)} + \overline{(e,f)}$$

$$= \overline{\left((a+c)+e, (b+d)+f\right)}$$

Agora, pela propriedade associativa da adição nos naturais temos que

$\overline{\left((a+c)+e, (b+d)+f\right)} = \overline{\left(a+(c+e), b+(d+f)\right)} = \overline{(a,b)} +$

$\overline{(c+e, d+f)} = \overline{(a,b)} + \left(\overline{(c,d)} + \overline{(e,f)}\right) = \alpha + (\beta + \gamma)$.

■

Proposição 2.2.5: (Propriedade Comutativa da Adição): Dados $\alpha, \beta \in \mathbb{Z}$, tem-se que $\alpha + \beta = \beta + \alpha$.

Demonstração:

Considere $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$. Note que

$$\alpha + \beta = \overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)}$$

pela comutatividade da adição nos naturais segue que

$$\overline{(a+c, b+d)} = \overline{(c+a, d+b)} = \overline{(c,d)} + \overline{(a,b)} = \beta + \alpha$$

■

Proposição 2.2.6: (Elemento Neutro em relação a Adição): Chamamos o inteiro $0 = \overline{(0,0)}$ de elemento neutro em relação a adição, pois dado um inteiro $\alpha = \overline{(a,b)}$, temos que $\alpha + 0 = \alpha$.

Demonstração:

Note que $\alpha + 0 = \overline{(a,b)} + \overline{(0,0)} = \overline{(a+0, b+0)}$, agora como o natural 0 é elemento neutro da adição segue que $\overline{(a+0, b+0)} = \overline{(a,b)} = \alpha$.

■

Proposição 2.2.7: (Existência do Oposto): Para todo inteiro α, existe um único inteiro que chamaremos de oposto de α, e denotaremos por $-\alpha$, tal que $\alpha + (-\alpha) = 0$.

Demonstração:

(Existência): Dado o inteiro $\alpha = \overline{(a,b)}$, tome $\beta = \overline{(b,a)}$. Pela propriedade comutativa da adição em $\mathbb{N}$ temos que

$$a+b = b+a \Rightarrow (a+b)+0 = (b+a)+0 \Rightarrow (a+b, b+a) \equiv (0,0) \Rightarrow \overline{(a+b,b+a)}$$
$$= 0 \Rightarrow \overline{(a,b)} + \overline{(b,a)} = 0 \Rightarrow \alpha + \beta = 0$$

Logo, $\beta = \overline{(b,a)}$ é oposto de $\alpha = \overline{(a,b)}$.

(Unicidade): Suponha que exista um inteiro $\gamma = \overline{(e,f)}$ que seja oposto de $\alpha = \overline{(a,b)}$. Neste caso, $\overline{(a,b)} + \overline{(e,f)} = \overline{(0,0)}$. No entanto, sabemos que $\overline{(a,b)} + \overline{(b,a)} = \overline{(0,0)}$. Destas duas igualdades temos que

$$\overline{(a,b)} + \overline{(b,a)} = \overline{(a,b)} + \overline{(e,f)}$$
$$\Rightarrow \overline{(a+b,b+a)} = \overline{(a+e,b+f)}$$
$$\Rightarrow (a+b,b+a) \equiv (a+e,b+f)$$
$$\Rightarrow (b+f)+(a+b) = (a+e)+(b+a)$$
$$\Rightarrow (b+f)+(a+b) = (a+e)+(a+b)$$
$$\Rightarrow b+f = a+e$$
$$\Rightarrow (b,a) \equiv (e,f)$$
$$\Rightarrow \overline{(b,a)} = \overline{(e,f)}$$
$$\Rightarrow \overline{(e,f)} = \overline{(b,a)}$$
$$\Rightarrow \gamma = \overline{(b,a)}$$

Assim, podemos afirmar que o elemento oposto além de existir, é único.

■

Proposição 2.2.8: (Propriedade Associativa da Multiplicação): Dados $\alpha, \beta, \gamma \in \mathbb{Z}$, temos que $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.

Demonstração: Dados $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$. Temos que

$$(\alpha \cdot \beta) \cdot \gamma = \left[\overline{(a,b)} \cdot \overline{(c,d)}\right] \cdot \overline{(e,f)} = \overline{(ac+bd, ad+bc)} \cdot \overline{(e,f)}$$
$$= \overline{\big((ac+bd)\cdot e + (ad+bc)\cdot f, (ac+bd)\cdot f + (ad+bc)\cdot e\big)}$$
$$= \overline{\big(a\cdot(ce) + b\cdot(de) + a\cdot(df) + b\cdot(cf), a\cdot(cf) + b\cdot(df) + a\cdot(de) + b\cdot(ce)\big)}$$
$$= \overline{(a,b)} \cdot \overline{(ce+df, cf+de)} = \overline{(a,b)} \cdot \big(\overline{(c,d)} \cdot \overline{(e,f)}\big) = \alpha \cdot (\beta \cdot \gamma)$$

■

Proposição 2.2.9: (Propriedade Comutativa da Multiplicação): Para todo $\alpha, \beta \in \mathbb{Z}$, temos que $\alpha \cdot \beta = \beta \cdot \alpha$.

Demonstração: Sejam $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$, temos que

$$\alpha \cdot \beta = \overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac+bd, ad+bc)} = \overline{(ca+db, cb+da)} = \overline{(c,d)} \cdot \overline{(a,b)} = \beta \cdot \alpha$$

■

Proposição 2.2.10: (Propriedade Distributiva): Dados $\alpha, \beta, \gamma \in \mathbb{Z}$, temos que $\alpha \cdot (\beta + \gamma) = \alpha\beta + \alpha\gamma$.

Demonstração: Sejam $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$. Segue que

$$\begin{aligned}
\alpha \cdot (\beta + \gamma) &= \overline{(a,b)} \cdot \left(\overline{(c,d)} + \overline{(e,f)}\right) = \overline{(a,b)} \cdot \overline{(c+e, d+f)} \\
&= \overline{\left(a \cdot (c+e) + b \cdot (d+f), a \cdot (d+f) + b \cdot (c+e)\right)} \\
&= \overline{(ac + ae + bd + bf, ad + af + bc + be)} \\
&= \overline{(ac+bd, ad+bc)} + \overline{(ae+bf, af+be)} = \overline{(a,b)} \cdot \overline{(c,d)} + \overline{(a,b)} \cdot \overline{(e,f)} \\
&= \alpha\beta + \alpha\gamma
\end{aligned}$$

■

Podemos definir a relação de ordem $\leq$ entre elementos de $\mathbb{Z}$ da seguinte forma:

Definição 2.2.10: Dados $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)} \in \mathbb{Z}$, diz-se que $\alpha \leq \beta$ se $a + d \leq b + c$. Diz-se ainda que $a < b$ se $a \leq b$ e $a \neq b$. De forma análoga se definem as relações $\geq$ e $>$.

Proposição 2.2.11: A relação $\leq$ é uma relação de ordem em $\mathbb{Z}$.

Demonstração: Devemos mostrar que a relação $\leq$ é reflexiva, antissimétrica e transitiva.

(Reflexiva): Seja um inteiro $\alpha = \overline{(a,b)}$, como $a + b \leq b + a$ temos que $\alpha \leq \alpha$.

(Antissimétrica): Dados $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)} \in \mathbb{Z}$, com $\alpha \leq \beta$ e $\beta \leq \alpha$, queremos mostrar que $\alpha = \beta$. De $\alpha \leq \beta$ temos que $a + d \leq b + c$, e de $\beta \leq \alpha$ temos que $c + b \leq d + a \Rightarrow b + c \leq a + d$. Como a relação $\leq$ é antissimétrica em $\mathbb{N}$, segue que $a + d = b + c$, logo $\overline{(a,b)} = \overline{(c,d)}$, ou seja, $\alpha = \beta$.

(Transitiva): Dados $\alpha = \overline{(a,b)}, \beta = \overline{(c,d)}, \gamma = \overline{(e,f)} \in \mathbb{Z}$, queremos mostrar que se $\alpha \leq \beta$ e $\beta \leq \gamma$, então $\alpha \leq \gamma$. De $\alpha \leq \beta$ e $\beta \leq \gamma$ temos, respectivamente, que $a + d \leq b + c$ e $c + f \leq d + e$. Somando os membros destas relações temos que $a + d + c + f \leq b + c + d + e$, cancelando $d + c$ em ambos os membros da desigualdade segue que $a + f \leq b + e$. Logo, $\overline{(a,b)} \leq \overline{(e,f)}$, ou seja, $\alpha \leq \gamma$.

■

A relação de ordem $\leq$ é munida da propriedade da Monotonicidade da Adição em $\mathbb{Z}$ como mostramos na proposição a seguir.

Proposição 2.2.12: Dados $\alpha, \beta, \gamma \in \mathbb{Z}$, se $\alpha \leq \beta$ então $\alpha + \gamma \leq \beta + \gamma$.

Demonstração: Considere $\alpha = \overline{(a,b)}, \beta = \overline{(c,d)}, \gamma = \overline{(e,f)}$. Como por hipótese $\alpha \leq \beta$, temos que $a + d \leq b + c$. Daí, somando $e + f$ em ambos os lados da desigualdade obtemos

$$a + e + d + f \leq b + f + c + e$$
$$\Rightarrow \overline{(a+e, b+f)} \leq \overline{(c+e, d+f)}$$
$$\Rightarrow \overline{(a,b)} + \overline{(e,f)} \leq \overline{(c,d)} + \overline{(e,f)}$$
$$\Rightarrow \alpha + \gamma \leq \beta + \gamma$$

■

Definição 2.2.11: Dizemos que um inteiro $\alpha = \overline{(a,b)}$ é positivo se $\alpha > 0$ e negativo se $\alpha < 0$.

A partir desta definição temos os seguintes resultados:

Proposição 2.2.13: Dado um inteiro $\alpha = \overline{(a,b)}$, diz-se que α é positivo se, e somente se $a > b$. Dizemos ainda que α é negativo se, e somente se $a < b$.

Demonstração:

Por definição, α ser positivo equivale ao fato de que $\alpha > 0$. Daí,

$$\alpha > 0 \Leftrightarrow \overline{(a,b)} > \overline{(0,0)} \Leftrightarrow a + 0 > b + 0 \Leftrightarrow a > b$$

De forma análoga, se α é negativo temos por definição que $\alpha < 0$. Assim,

$$\alpha < 0 \Leftrightarrow \overline{(a,b)} < \overline{(0,0)} \Leftrightarrow a + 0 < b + 0 \Leftrightarrow a < b$$

■

Apresentamos a seguir a definição do conjunto dos inteiros positivos ($\mathbb{Z}_+$) e mostramos que ele é uma cópia do conjunto dos naturais.

Definição 2.2.12: Chamaremos de conjunto dos inteiros não-negativos o conjunto $\mathbb{Z}_+ = \{\overline{(a,0)}; a \in \mathbb{N}\}$.

Proposição 2.2.14: A função

$$\phi: \mathbb{N} \longrightarrow \mathbb{Z}_+$$
$$a \longmapsto \overline{(a,0)}$$

é bijetora.

Demonstração: Primeiramente iremos mostrar que a função é injetora. Para tanto, sejam $a, b \in \mathbb{N}$, tais que $\phi(a) = \phi(b)$, iremos mostrar que $a = b$. Por hipótese temos que

$$\phi(a) = \phi(b) \Rightarrow \overline{(a,0)} = \overline{(b,0)} \Rightarrow (a,0) \equiv (b,0) \Rightarrow a + 0 = 0 + b \Rightarrow a = b.$$

Agora mostraremos que a função é sobrejetora. Para isso, dado $\overline{(b,0)} \in \mathbb{Z}_+$, precisamos mostrar que existe $a \in \mathbb{N}$ tal que $\phi(a) = \overline{(b,0)}$. Basta tomar $a = b$. Assim, $\phi(a) = \phi(b) = \overline{(b,0)}$.

Como mostramos que a função ϕ é injetora e sobrejetora, temos que ϕ é bijetora.

■

Afim de estabelecer uma correspondência entre o conjunto $\mathbb{Z}$ construído nesta seção e a forma usual dos números inteiros $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3\}$ podemos tomar os inteiros positivos $1 = \overline{(1,0)}, 2 = \overline{(2,0)}, 3 = \overline{(3,0)}, \dots$ o elemento neutro $0 = \overline{(0,0)}$ e os inteiros negativos como sendo os opostos de cada elemento do conjunto dos inteiros positivos $-1 = \overline{(0,1)}, -2 = \overline{(0,2)}, -3 = \overline{(0,3)}\dots$ Neste sentido, destacam-se ainda os subconjuntos de $\mathbb{Z}$:

i) $\mathbb{Z}_+ = \{0, 1, 2, 3, \dots\}$

ii) $\mathbb{Z}_- = \{\dots, -3, -2, -1, 0\}$

iii) $\mathbb{Z}_+^* = \{1, 2, 3, \dots\}$

iv) $\mathbb{Z}_-^* = \{\dots, -3, -2, -1\}$

Por fim, definimos o que é um conjunto limitado inferiormente e apresentamos o Princípio da Boa Ordenação em $\mathbb{Z}$.

Definição 2.2.13: Seja X um subconjunto não vazio de $\mathbb{Z}$. Dizemos que X é limitado inferiormente se existe $\alpha \in \mathbb{Z}$ tal que $\alpha \leq x$, para todo $x \in X$. Assim, chamamos α de cota inferior de X.

Princípio da Boa-Ordenação: Seja X um subconjunto de $\mathbb{Z}$ não vazio e limitado inferiormente, então X possui um elemento mínimo.

Demonstração: Seja α uma cota inferior de X, isto é, $\alpha \leq x$ para todo $x \in X$. Consideremos $X' = \{x - \alpha; x \in X\}$. Note que $X' \subset \mathbb{N}$, portanto pelo Princípio da Boa Ordem em $\mathbb{N}$ o conjunto X' possui um elemento mínimo. Tome m' como o elemento mínimo de X', assim $m' \in X'$ e $m' \leq y$ para todo $y \in X'$. Como $m' \in X'$, temos que $m' = m - \alpha$ para algum $m \in X$. Afirmamos que $m = m' + \alpha$ é o elemento mínimo de X. Para tanto, precisamos verificar que $m \leq x$ para todo $x \in X$. No entanto, isto equivale ao fato de que $m - \alpha \leq x - \alpha$ para todo $x \in X$, ou ainda, $m' \leq x - \alpha$, o que é verdade visto que m' é o elemento mínimo de X'. Assim, de fato m é o elemento mínimo de X.

2.3 DIVISIBILIDADE

Esta seção se dedica a tratar sobre a divisibilidade no conjunto dos inteiros. As definições e proposições apresentadas aqui são de extrema importância para o desenvolvimento da teoria, fornecendo as bases essenciais para a sequência do trabalho.

Definição 2.3.1: Sejam $a, b \in \mathbb{Z}$. Diz-se que a divide b, ou que a é um divisor de b, ou ainda que b é um múltiplo de a, denotando $a|b$, se existe um inteiro c, tal que $b = c \cdot a$. Caso não exista um inteiro c que satisfaz tal condição dizemos que a não divide b e denotamos $a \nmid b$.

Proposição 2.3.1: Sejam, $a, b, c \in \mathbb{Z}$. Temos que:

i) $a|a$ e $1|a$.

ii) Se $b|a$ e $a \neq 0$, então $|b| \leq |a|$.

iii) Os únicos divisores de 1 são 1 e -1.

iv) Se $a|b$ e $b|a$, então $a = \pm b$ (a e b não nulos).

v) Se $a|b$ e $b|c$, então $a|c$.

vi) Sejam $x, y \in \mathbb{Z}$. Se $c|a$ e $c|b$, então $c|(x \cdot a + y \cdot b)$.

Demonstração:

i) Da igualdade $1 \cdot a = a \cdot 1 = a$ e da definição 2.3.1 segue que $a|a$ e $1|a$.

ii) Como $b|a$ existe um inteiro c tal que $b \cdot c = a \Rightarrow |b| \cdot |c| = |a|$. Note que $1 \leq |c|$, assim, multiplicando ambos os membros da desigualdade por $|b|$, temos que $|b| \leq |b| \cdot |c| = |a|$

iii) Seja b um divisor de 1, pelo item anterior temos que $|b| \leq 1$. Daí, como $0 \nmid 1$ segue que $b = \pm 1$.

iv) Da hipótese temos que $a|b$ e $b|a$. Assim, existem inteiros k_1, k_2, tal que $b = k_1 \cdot a$ e $a = k_2 \cdot b$. Substituindo na segunda igualdade o valor de b temos que $a = k_2 \cdot k_1 \cdot a$, como $a \neq 0$ segue que $k_1 \cdot k_2 = 1$, logo k_2 é um divisor de 1, portanto $k_2 = \pm 1$ e consequentemente $a = \pm b$.

v) Da hipótese temos que $a|b$ e $b|c$. Assim, existem inteiros k_1, k_2, tal que $b = k_1 \cdot a$ e $c = k_2 \cdot b$. Substituindo o valor de b na segunda igualdade obtemos $c = k_2 \cdot (k_1 \cdot a) = (k_1 \cdot k_2) \cdot a$. Tomando $k = k_1 \cdot k_2$ segue que $c = k \cdot a$, logo $a|c$.

vi) Da hipótese temos que $c|a$ e $c|b$. Assim, existem inteiros k_1, k_2, tal que $a = k_1 \cdot c$ e $b = k_2 \cdot c$. Multiplicando ambos os membros da primeira igualdade por x e da segunda igualdade por y, obtemos que $x \cdot a = x \cdot k_1 \cdot c$ e $y \cdot b = y \cdot k_2 \cdot c$. Daí, $x \cdot a + y \cdot b = x \cdot k_1 \cdot c + y \cdot k_2 \cdot c = (x \cdot k_1 + y \cdot k_2) \cdot c$. Tomando $k = x \cdot k_1 + y \cdot k_2$ segue que $x \cdot a + y \cdot b = k \cdot c$, logo $c|(x \cdot a + y \cdot b)$.

Enunciaremos o Teorema de Eudoxius que será utilizado para demonstrar o Teorema do Algoritmo da Divisão. O Teorema de Eudoxius traz conceitualmente a ideia de que dados dois inteiros a e b, com b não nulo, ou a é múltiplo de b ou está situado entre dois múltiplos consecutivos de b.

Teorema de Eudoxius: A cada par de inteiros a e b, com $b \neq 0$, existe um inteiro q tal que:

i) Para $b > 0$:

$$q \cdot b \leq a < (q+1) \cdot b$$

ii) Para $b < 0$:

$$q \cdot b \leq a < (q-1) \cdot b.$$

Teorema do Algoritmo da Divisão: Sejam a e b dois inteiros com $b \neq 0$. Existem dois únicos inteiros q e r, tais que:

$$a = b \cdot q + r, \qquad \text{com } 0 \leq r < |b|.$$

Denominamos q e r, respectivamente, de quociente e resto da divisão de a por b.

Demonstração:

i) (Existência): Pelo Teorema de Eudoxius, se $b > 0$ existe um inteiro q tal que $q \cdot b \leq a < (q+1) \cdot b$, isto implica que $0 \leq a - q \cdot b < b = |b|$. Já se $b < 0$ existe um inteiro q tal que $q \cdot b \leq a < (q-1) \cdot b \Rightarrow 0 \leq a - q \cdot b < -b = |b|$. Em ambos os casos se tomarmos $r = a - b \cdot q$ teremos que $a = b \cdot q + r$, com $0 \leq r < |b|$.

ii) (Unicidade): Suponha que existam dois pares de inteiros q_1, r_1 e q_2, r_2 que satisfazem as condições do teorema. Queremos mostrar que $q_1 = q_2$ e $r_1 = r_2$. Como $0 \leq r_1 < |b|$ e $0 \leq r_2 < |b|$, temos que $-|b| < -r_1 \leq r_2 - r_1 \leq r_2 < |b|$, o que implica que $|r_2 - r_1| < |b|$. Por outro lado, como $a = b \cdot q_1 + r_1 = b \cdot q_2 + r_2$, temos que $b \cdot (q_1 - q_2) = r_2 - r_1$. Assim, $|b| \cdot |q_1 -$

$q_2| = |r_2 - r_1| < |b|$. No entanto, isto só é possível se $|q_1 - q_2| = 0 \Rightarrow q_1 = q_2$, consequentemente temos $|r_2 - r_1| = 0 \Rightarrow r_1 = r_2$.

■

2.4 MÁXIMO DIVISOR COMUM (MDC) E MÍNIMO MÚLTIPLO COMUM (MMC)

A presente Seção apresenta as definições de Máximo Divisor Comum e Mínimo Múltiplo Comum, bem como vários resultados envolvendo estes elementos.

Definição 2.4.1: Considere os números inteiros $a_1, a_2, \dots, a_n$, de forma que ao menos um deles seja diferente de zero. O máximo divisor comum destes números d será o maior número inteiro que divide todos eles. Particularmente, para dois inteiros a e b (a ou b diferente de 0), diz-se que o inteiro $d \geq 0$ é o máximo divisor comum de a e b se satisfaz as seguintes condições:

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

ii) Seja $c \in \mathbb{Z}$ tal que $c|a$ e $c|b$, então $c|d$.

Utilizaremos a notação $mdc\,(a, b)$, ou ainda apenas (a, b) para se referir ao máximo divisor comum entre a e b.

Observação 2.4.1: Dados inteiros a e b temos que:

i) $(a, b) = (b, a)$

ii) $(a, 0) = |a|$

iii) $(a, 1) = a$

iv) $(a, b) = (-a, b) = (a, -b) = (-a, -b)$

Teorema de Bachet-Bézout: Dados $a, b \in \mathbb{Z}$, existem $x_0, y_0 \in \mathbb{Z}$ tais que

$$ax_0 + by_0 = (a, b)$$

Demonstração: Considere o conjunto B formado por todas as combinações lineares $\{ax + by\}$. Tome x_0 e y_0 tais que $m = ax_0 + by_0$ seja o menor inteiro positivo que pertence a B. Queremos mostrar que $m|a$ e $m|b$, como as demonstrações são análogas iremos mostrar apenas que $m|a$. Suponha por absurdo, que $m \nmid a$. Neste caso, pelo Algoritmo da Divisão existem $q, r \in \mathbb{Z}$ tais que $a = mq + r$, com $0 < r < m$. Logo, $r = a - qm = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0)$, então $r \in B$, o que é um absurdo, pois como $0 < r < m$, contradiz o fato de que m é o menor inteiro positivo que pertence a B. Assim, $m|a$ e de forma análoga se prova que $m|b$.

Agora, considere o inteiro c de forma com que $c|a$ e $c|b$. Note que a existência de c é garantida visto que 1 é divisor de qualquer inteiro. Pelo item vi) da Proposição 2.3.1 temos que $c|ax_0 + by_0$, ou seja, $c|m$.

Como m é um inteiro positivo, mostramos que $m|a$, $m|b$ e para qualquer inteiro c tal que $c|a$ e $c|b$ temos que $c|m$, pela Definição 2.4.1 segue que $m = ax_0 + by_0 = (a, b)$.

■

Observação 2.4.2: Note que na demonstração do teorema, além de mostrar que o máximo divisor comum de dois inteiros pode ser escrito como uma combinação linear entre eles, mostramos também que esta combinação linear será a de menor valor positivo dentre todas as combinações lineares.

Perceba ainda que o Teorema de Bachet-Bézout garante a existência do máximo divisor comum de quaisquer dois inteiros. A proposição a seguir mostra que além de existir, o máximo divisor comum entre dois inteiros é único.

Proposição 2.4.1 (Unicidade do Máximo Divisor Comum): Sejam $a, b \in \mathbb{Z}$. Se $d_1, d_2 \in \mathbb{Z}$ são ambos máximos divisores comuns de a e b, então $d_1 = d_2$.

Demonstração: Primeiramente iremos demonstrar o caso em que um dos inteiros a ou b é nulo. Considere, sem perda de generalidade $b = 0$. Neste caso $(a, b) = (a, 0) = |a|$, logo $d_1 = |a|$ e $d_2 = |a|$ segue que $d_1 = d_2$.

Considere agora o caso em que a e b são ambos não nulos. Como d_1 e d_2 são divisores comuns de a e b e são também os máximos divisores comuns de a e b, pelo item $ii)$ da Definição 2.4.1 temos que $d_1|d_2$ e $d_2|d_1$. Agora, pelo item $iv)$ da Proposição 2.3.1 segue que $d_1 = \pm d_2$, mas como d_1 e d_2 são ambos positivos podemos concluir que $d_1 = d_2$.

Proposição 2.4.2: Sejam $a, b, q, r \in \mathbb{Z}$, se $a = bq + r$, então $(a, b) = (b, r)$.

Demonstração: Considere $d = (a, b)$. Queremos mostrar que $d|b$, $d|r$ e para qualquer $c \in \mathbb{Z}$ tal que $c|b$ e $c|r$ temos que $c|d$. Pois bem, como $d = (a, b)$ segue de imediato que $d|b$. Agora, como $a - bq$ é uma combinação linear de a com b, pelo item $vi)$ da Proposição 2.3.1 temos que $d|a - bq$, o que implica que $d|r$. Considere agora $c \in \mathbb{Z}$ tal que $c|b$ e $c|r$, novamente pelo item $vi)$ da Proposição 2.3.1 sabemos que $c|bq + r$, ou seja, $c|a$. Como $c|a$ e $c|b$, pela Definição 2.4.1 $c|d$. Assim, podemos concluir que $(a, b) = d = (b, r)$.

■

A Proposição 2.4.2 serve como base para o Algoritmo de Euclides, cujo processo consiste em encontrar o máximo divisor comum entre dois inteiros realizando sucessivas divisões.

Teorema do Algoritmo do MDC de Euclides: Dados dois inteiros positivos a e b ($a \geq b$), pode-se aplicar sucessivas divisões que geram as seguintes igualdades:

$$\begin{cases} a = bq_1 + r_1, & 0 \leq r_1 < a \\ b = r_1 q_2 + r_2, & 0 \leq r_2 < r_1 \\ r_1 = r_2 q_3 + r_3, & 0 \leq r_3 < r_2 \\ \vdots & \\ r_{n-2} = r_{n-1} q_n + r_n, & 0 \leq r_n < r_{n-1} \\ r_{n-1} = r_n q_{n+1} + 0 & \end{cases}$$

As divisões são realizadas até encontrar uma cujo resto é 0. Encontrada tal divisão, o máximo divisor comum entre a e b é dado pelo resto encontrado na divisão anterior r_n. Caso o resto encontrado na primeira divisão seja 0, temos que $(a, b) = b$.

Demonstração: Primeiramente iremos mostrar o caso em que o resto encontrado na primeira divisão é igual a 0. Neste caso, pela Proposição 2.4.2 temos que $(a, b) = (b, 0) = |b| = b$. Se o resto da primeira divisão for diferente de zero, segue-se realizando as divisões sucessivas até encontrar a divisão cujo resto é zero. Note que isto sempre será possível após realizar um número finito de divisões visto que a sequência de números inteiros r_k, com $1 \leq k \leq n$ é estritamente decrescente e o conjunto de restos r_k está contido no conjunto $\{r \in \mathbb{Z}; 0 \leq r < a\}$. Assim, o processo para encontrar uma divisão cujo resto é 0 levará no máximo um total de a divisões. Agora, a partir das divisões realizadas, pela Proposição 2.4.2 temos que $(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \cdots = (r_{n-1}, r_n) = (r_n, 0) = |r_n| = r_n$.

■

Abaixo será descrito um exemplo numérico onde calculamos $(210{,}65)$ utilizando o Algoritmo do MDC de Euclides:

Exemplo: Para calcular $(210{,}65)$, realizamos as divisões:

$$210 = 65 \cdot 3 + 15$$

$$65 = 15 \cdot 4 + 5$$

$$15 = 5 \cdot 3 + 0$$

Assim, $(210{,}65) = 5$

A seguir, serão apresentadas mais algumas proposições e teoremas a respeito do máximo divisor comum, bem como a definição de números primos entre si.

Proposição 2.4.3: Considere $a, b \in \mathbb{Z}$. Para qualquer inteiro positivo c, temos que $(ca, cb) = c(a, b)$.

Demonstração: Pelo Teorema de Bachet-Bézout, existem $x_0, y_0 \in \mathbb{Z}$ tais que (ca, cb) pode ser descrito como a combinação linear $cax_0 + cby_0$. Inclusive sabemos que $cax_0 + cby_0$ é a combinação linear de menor valor positivo entre todas as combinações do tipo $cax + cby$. Agora, como $cax_0 + cby_0 = c(ax_0 + by_0)$ e $ax_0 + by_0$ é a combinação linear de menor valor positivo entre as combinações do tipo $ax + by$, segue que $ax_0 + by_0 = (a, b)$. Daí, $(ca, cb) = cax_0 + cby_0 = c(ax_0 + by_0) = c(a, b)$.

■

Proposição 2.4.4: Considere $a, b \in \mathbb{Z}$. Se c é um inteiro positivo tal que $c|a$ e $c|b$, então $\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c}(a, b)$.

Demonstração: Como a e b são divisíveis por c, temos que $\frac{a}{c}$ e $\frac{b}{c}$ são inteiros. Assim, pela Proposição 2.4.3 temos que $c \cdot \left(\frac{a}{c}, \frac{b}{c}\right) = \left(c \cdot \frac{a}{c}, c \cdot \frac{b}{c}\right)$, e isto implica que $c \cdot \left(\frac{a}{c}, \frac{b}{c}\right) = (a, b)$. Daí, como $c \neq 0$ podemos dividir cada membro da igualdade obtida por c, encontrando $\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c}(a, b)$.

■

Da Proposição 2.4.4, segue o seguinte Corolário:

Corolário 2.4.1: Considere $a, b \in \mathbb{Z}$. Se $(a, b) = d$, então $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demonstração: Como d é um divisor comum de a e b, pela Proposição 2.4.4 temos que $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b) = \frac{1}{d} \cdot d = 1$.

■

Teorema (Lema de Gauss): Considere $a, b, c \in \mathbb{Z}$. Se $a|bc$ e $(a, b) = 1$, então $a|c$.

Demonstração: Como $(a, b) = 1$, pelo Teorema de Bachet-Bézout existem inteiros x e y tais que $ax + by = 1$. Multiplicando ambos os membros da igualdade por c obtemos $x \cdot (ac) + y \cdot (bc) = c$. Agora, como $a|ac$ e, por hipótese, $a|bc$, pelo item $vi)$ da Proposição 2.3.1 temos que $a|c$.

Definição 2.4.2: Dados $a, b \in \mathbb{Z}$, diz-se que a e b são primos entre si, ou ainda que a e b são co-primos se $(a, b) = 1$.

Proposição 2.4.5: Dois números inteiros a e b são primos entre si se, e somente se, existirem inteiros x e y tais que $ax + by = 1$.

Demonstração: Primeiramente iremos mostrar que se a e b são primos entre si, então existem $x, y \in \mathbb{Z}$, tais que $ax + by = 1$. De fato, dados inteiros a e b, pelo Teorema de Bachet-Bézout existem inteiros x e y tais que $ax + by = (a, b)$. Daí, como $(a, b) = 1$, segue que $ax + by = 1$.

Agora queremos mostrar que dados inteiros a e b, se existem inteiros x e y tais que $ax + by = 1$, então a e b são primos entre si. Por hipótese sabemos que existem inteiros x e y tais que $ax + by = 1$. Agora, considere $d = (a, b)$, sabemos que $d|a$ e $d|b$. Assim, pelo item $vi)$ da Proposição 2.3.1 temos que $d|ax + by$, ou seja, $d|1$ o que implica que $d = 1$. Logo, a e b são primos entre si.

■

Finalizando a sessão, será apresentado a definição de Mínimo Múltiplo Comum, sua prova de existência e unicidade, e uma proposição relacionando o Máximo Divisor Comum e Mínimo Múltiplo Comum de dois inteiros.

Definição 2.4.3: Considere os inteiros não-nulos $a_1, a_2, \dots, a_n$. O Mínimo Múltiplo Comum dos números $a_1, a_2, \dots, a_n$ é o menor inteiro positivo m que é múltiplo de todos os números a_i $(1 \leq i \leq n)$. Particularmente para dois inteiros não-nulos a e b diz-se que o inteiro positivo m é o mínimo múltiplo comum de a e b se satisfazer as seguintes condições:

i) $a|m$ e $b|m$

ii) Seja $c \in \mathbb{Z}$. Se $a|c$ e $b|c$, então $m|c$.

Utilizaremos a notação $mmc\ (a, b)$, ou ainda apenas $[a, b]$ para se referir ao mínimo múltiplo comum entre a e b.

Proposição 2.4.6 (Existência e Unicidade do Mínimo Múltiplo Comum): Dados n inteiros positivos não-nulos $a_1, a_2, \dots, a_n$, o mínimo múltiplo comum de $a_1, a_2, \dots, a_n$ existe e é único.

Demonstração: Dados os inteiros $a_1, a_2, \dots, a_n$. O conjunto $M = \{m \in \mathbb{Z}_+^*; \forall i \in \mathbb{Z}, 0 \leq i \leq n, a_i|m\}$ é formado pelos inteiros positivos que são múltiplos comuns de $a_1, a_2, \dots, a_n$. Note que $M \neq \emptyset$, pois $a_1 \cdot a_2 \cdot \dots \cdot a_n \in M$. Ainda, como M é um subconjunto de $\mathbb{Z}$ limitado inferiormente, pelo Princípio da Boa Ordem ele possui um

elemento mínimo m_0. Como m_0 é um inteiro positivo e é o menor múltiplo comum de $a_1, a_2, \dots, a_n$, podemos concluir que $m_0 = [a_1, a_2, \dots, a_n]$. Além disso, pela unicidade do mínimo de um conjunto, além de existir, m_0 é único.

■

Proposição 2.4.7: Dados dois inteiros não-nulos a e b, temos que $(a,b) \cdot [a,b] = |a \cdot b|$.

Demonstração: Com o objetivo de simplificar a demonstração iremos considerar a e b inteiros positivos. Isto não trará nenhum prejuízo a prova visto que os demais casos são análogos necessitando apenas de pequenos ajustes.

Considere $d = (a,b)$ e $m = [a,b]$, queremos mostrar que $d \cdot m = a \cdot b$, ou seja, que $m = \frac{ab}{d}$.

Note que $a|\frac{ab}{d}$ e $b|\frac{ab}{d}$. Além disso, considere $m' \in \mathbb{Z}$, se $a|m''$ e $b|m''$, então existem $k_1, k_2 \in \mathbb{Z}$ tais que $m' = a \cdot k_1$ e $m' = b \cdot k_2$. Assim, temos que $a \cdot k_1 = b \cdot k_2$. Daí, dividindo ambos os membros da igualdade por d, obtém-se que $\frac{a}{d} \cdot k_1 = \frac{b}{d} \cdot k_2$. Como $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ (Corolário 2.4.1), pelo Lema de Gauss temos que $\frac{a}{d}|k_2$ e $\frac{b}{d}|k_1$. Logo, existe $k_3 \in \mathbb{Z}$ tal que $k_1 = \frac{b}{d} \cdot k_3$. Substituindo o valor de k_1 desta última igualdade em $m' = a \cdot k_1$ obtemos que $m' = \left(\frac{ab}{d}\right) \cdot k_3$. Portanto, $\frac{ab}{d}|m'$. Assim, conclui-se pela Definição 2.4.3 que $m = \frac{ab}{d}$, o que implica que $d \cdot m = a \cdot b$.

■

2.5 NÚMEROS PRIMOS

Os Números Primos ocupam posição de destaque no desenvolvimento da Teoria dos Números e também na Criptografia RSA, afinal como veremos adiante, ela se baseia na escolha de números primos extremamente grandes para garantir sua segurança.

Definição 2.5.1: Seja a um inteiro maior que 1. Diz-se que a é primo se os únicos divisores positivos de a são 1 e a. Em contrapartida, caso a não seja um número primo diz-se que a é um número composto.

A sequência dos primeiros números primos pode ser representada por $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$ Mais tarde estudaremos mais sobre esta sequência

A seguir, são apresentadas algumas proposições que decorrem da definição de número primo.

Proposição 2.5.1: Considere o inteiro a e os primos p e q. Segue que:

i) Se $p|q$, então $p = q$.

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

Demonstração:

i) Como q é um número primo, seus únicos divisores são 1 e q. Agora, note que pela hipótese p é um divisor de q, como p também é primo temos que $p \neq 1$, assim podemos concluir que $p = q$.

ii) Tome $d = (p, a)$. Como $d|p$, temos que $d = 1$ ou $d = p$. Agora, suponha por absurdo que $d = p$. Como $d = (p, a)$ temos que $d|a \Rightarrow p|a$, absurdo, pois contradiz nossa hipótese. Logo $d = (p, a) = 1$.

■

Proposição 2.5.2 (Lema de Euclides): Considere $a, b \in \mathbb{Z}$ e um número primo p. Se $p|ab$, então $p|a$ ou $p|b$.

Demonstração: Em relação a divisibilidade de a por p, só há duas possibilidades, $p|a$ ou $p \nmid a$. No caso em que $p \nmid a$, pelo item $ii)$ da Proposição 2.5.1 temos que $(p, a) = 1$ e, portanto, pelo Lema de Gauss $p|b$.

■

A seguir, será apresentado o Teorema Fundamental da Aritmética. Este teorema garante que todo número pode ser fatorado de forma única em fatores primos e é peça fundamental no sistema de Criptografia RSA.

Teorema Fundamental da Aritmética: Todo inteiro n maior que 1 pode ser escrito de forma única como

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m}$$

onde $p_1 < p_2 < \cdots < p_m$ são primos $(m \geq 1)$ e $\alpha_1, \alpha_2, \ldots, \alpha_m$ são inteiros positivos.

Demonstração: Primeiramente iremos mostrar a existência de tal fatoração e depois sua unicidade.

Existência: Note que se n é primo, temos $n = p_1$, com $\alpha_1 = 1$, o que conclui a existência nesse caso. Agora, se n é composto, como $1|n$ e $n|n$, mas n não é primo,

existe um inteiro x, com $1 < x < n$ tal que $x|n$. Logo, existe também um inteiro y tal que $n = xy$, com $1 < y < n$. Considere p_1, o menor dos divisores maiores que 1 de n. Iremos mostrar que p_1 é primo. Suponha, por absurdo, que p_1 é composto. Então, existe $x_1 \in \mathbb{Z}$ com $1 < x_1 < p_1$ tal que $x_1|p_1$, mas como $p_1|n$ isto implica que $x_1|n$. Absurdo, pois contradiz o fato de p_1 ser o menor divisor maior que 1 de n. Portanto, de fato p_1 é primo. Agora, como $p_1|n$, existe $k_1 \in \mathbb{Z}$ tal que $n = p_1 \cdot k_1$. Se k_1 é primo, a prova está completa. Já se k_1 é composto, tome p_2 como o menor divisor maior que 1 de k_1. Pelo raciocínio apresentado acima, p_2 é primo. Assim, existe $k_2 \in \mathbb{Z}$ tal que $n = p_1 \cdot p_2 \cdot k_2$. Repetindo este processo, como $k_1 = p_2 \cdot k_2$, $k_2 = p_3 \cdot k_3$, ..., $k_{r-1} = p_r \cdot k_r$, obtemos uma sequência decrescente de inteiros positivos $k_1, k_2, \dots, k_r$, logo o processo é finito. Perceba ainda, que alguns dos primos $p_1, p_2, \dots, p_r, k_r$, podem se repetir, justificando a possibilidade de existirem expoentes $\alpha_1, \alpha_2, \dots, \alpha_m$ maiores que 1.

Unicidade: Considere o conjunto B formado pelos inteiros maiores que 1 que possuem duas fatorações distintas. Suponha, por absurdo, que $B \neq \emptyset$. Assim, pelo Princípio da Boa Ordem B possui um elemento mínimo b_0, tal que $b_0 = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_m^{\alpha_m} = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \dots \cdot q_s^{\beta_s}$ são duas fatorações em primos distintas. Como $p_1|b_0$, pelo Lema de Euclides p_1 deve dividir algum dos primos q_j, com $1 \leq j \leq s$. Assim, suponha sem perda de generalidade que $p_1|q_1$. Como p_1 e q_1 são primos isto implica que $p_1 = q_1$. Agora, dividindo ambos os membros da igualdade $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_m^{\alpha_m} = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \dots \cdot q_s^{\beta_s}$ por p_1, obtemos um inteiro b, tal que $b = p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_m^{\alpha_m} = q_1^{\beta_1 - 1} \cdot q_2^{\beta_2} \cdot \dots \cdot q_s^{\beta_s}$. Note que $b \in B$ e $b < b_0$. Absurdo, pois contraria a minimalidade de b_0. Logo $B = \emptyset$.

■

Podemos escrever a fatoração em primos de n utilizando a notação de produtório, desta forma $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_m^{\alpha_m} = \prod_{i=1}^{m} p_i^{\alpha_i}$. Esta notação será utilizada em algumas proposições e observações a seguir.

Proposição 2.5.3: Existem infinitos números primos.

Demonstração: Suponha, por absurdo, que exista um número finito m de números primos, $p_1, p_2, \dots, p_m$. Considere então, o inteiro n tal que $n = p_1 \cdot p_2 \cdot \dots \cdot p_m + 1$. Pelo Teorema Fundamental da Aritmética temos que n possui um fator primo p. Note que p deve ser igual a um dos finitos primos $p_1, p_2, \dots, p_m$. Portanto, $p|p_1 \cdot p_2 \cdot \dots \cdot$

p_m e como sabemos também que $p|n$, temos que existem $k_1, k_2 \in \mathbb{Z}$ tais que $n = p \cdot k_1$ e $p_1 \cdot p_2 \cdot \ldots \cdot p_m = p \cdot k_2$. Substituindo o valor destas duas igualdades em $n = p_1 \cdot p_2 \cdot \ldots \cdot p_m + 1$ obtemos que $p \cdot k_1 = p \cdot k_2 + 1 \Rightarrow p \cdot (k_1 - k_2) = 1$. Mas, como $k_1 - k_2 \in \mathbb{Z}$, isto implica que $p|1$. Absurdo, pois p é um número primo.

■

Observação 2.5.1: Se $n = \prod_{i=1}^{m} p_i^{\alpha_i}$ representa a fatoração em primos do inteiro n, então o conjunto dos divisores positivos de n é formado por todos os números da forma $\prod_{i=1}^{m} p_i^{c_i}$, com $0 \leq c_i \leq \alpha_i$ e $i = 1,2, \ldots, m$.

Observação 2.5.2: Se escrevermos a sequência dos números primos em ordem crescente, considerando $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ..., p_n,... com p_n representando o n-ésimo número primo, então todo inteiro $n > 1$ pode ser escrito na forma $n = \prod_{i=1}^{\infty} p_i^{\alpha_i}$, com $\alpha_i \geq 0$.

Desta forma, os divisores positivos de n são todos os números que podem ser escritos na forma $\prod_{i=1}^{\infty} p_i^{c_i}$, com $0 \leq c_i \leq \alpha_i$.

Proposição 2.5.4: Considere $a, b \in \mathbb{Z}$. Se suas fatorações em primos são dadas por

$$a = \prod_{i=1}^{\infty} p_i^{\alpha_i}, \quad b = \prod_{i=1}^{\infty} p_i^{\beta_i}$$

, então

$$(a, b) = \prod_{i=1}^{\infty} p_i^{\min\{\alpha_i, \beta_i\}}$$

Demonstração: Os divisores positivos de a são todos os números que podem ser escritos na forma $\prod_{i=1}^{\infty} p_i^{c_i}$, com $0 \leq c_i \leq \alpha_i$, enquanto os divisores positivos de b são todos os que podem ser escritos na forma $\prod_{i=1}^{\infty} p_i^{c_i}$, com $0 \leq c_i \leq \beta_i$. Logo, os divisores comuns de a e b são todos os números da forma $\prod_{i=1}^{\infty} p_i^{c_i}$, com $0 \leq c_i \leq \alpha_i$ e $0 \leq c_i \leq \beta_i$. Assim, basta tomar $c_i = \min\{\alpha_i, \beta_i\}$, para se ter o maior número dentre os divisores comuns de a e b, ou seja, o máximo divisor comum de a e b.

Lema 2.5.1: Se x e y são inteiros, então $\min\{x, y\} + máx\{x, y\} = x + y$.

Demonstração: Note que se $x = y$, então $\min\{x, y\} = máx\{x, y\} = x = y$ e a igualdade é verificada. Agora, se $x \neq y$, podemos considerar, sem perda de generalidade, $x < y$. Neste caso, como $\min\{x, y\} = x$ e $máx\{x, y\} = y$, temos que $\min\{x, y\} + máx\{x, y\} = x + y$.

■

Proposição 2.5.5: Considere $a, b \in \mathbb{Z}$. Se suas fatorações em primos são dadas por

$$a = \prod_{i=1}^{\infty} p_i^{\alpha_i}, \quad b = \prod_{i=1}^{\infty} p_i^{\beta_i}$$

, então

$$[a, b] = \prod_{i=1}^{\infty} p_i^{\text{máx}\,\{\alpha_i, \beta_i\}}$$

Demonstração: Da Proposição 2.4.7 sabe-se que $(a, b) \cdot [a, b] = a \cdot b$. Substituindo nesta igualdade os valores de a, b e (a, b), por suas respectivas fatorações em primos temos

$$\prod_{i=1}^{\infty} p_i^{\min\{\alpha_i, \beta_i\}} \cdot [a, b] = \prod_{i=1}^{\infty} p_i^{\alpha_i} \cdot \prod_{i=1}^{\infty} p_i^{\beta_i}$$

o que implica que

$$\prod_{i=1}^{\infty} p_i^{\min\{\alpha_i, \beta_i\}} \cdot [a, b] = \prod_{i=1}^{\infty} p_i^{\alpha_i + \beta_i}$$

Assim, pelo Lema 2.5.1 podemos concluir que

$$[a, b] = \prod_{i=1}^{\infty} p_i^{\text{máx}\,\{\alpha_i, \beta_i\}}$$

■

A proposição abaixo mostra que na sequência dos números primos, existem sempre dois primos consecutivos cuja diferença é tão grande quanto desejarmos.

Proposição 2.5.6: Para qualquer inteiro positivo k, existem k inteiros consecutivos compostos.

Demonstração: Considere $(k+1)!$. Como $(k+1)! = (k+1) \cdot k \cdot (k-1) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$, ele é divisível por todos os k números entre 2 e $k+1$.

Assim, note que a sequência de números abaixo

$$(k+1)! + 2 = 2 \cdot \left(\frac{(k+1)!}{2} + 1 \right)$$

$$(k+1)! + 3 = 3 \cdot \left(\frac{(k+1)!}{3} + 1 \right)$$

$$\vdots$$

$$(k+1)! + k = k \cdot \left(\frac{(k+1)!}{k} + 1 \right)$$

$$(k+1)! + (k+1) = (k+1) \cdot \left(\frac{(k+1)!}{k+1} + 1 \right)$$

é formada por k números consecutivos compostos.

■

Proposição 2.5.7: Se n é composto, então ele possui um fator primo p, tal que $p \leq \sqrt{n}$.

Demonstração: Como n é composto, ele pode ser escrito como o produto de dois inteiros k_1 e k_2, com $1 < k_1 < n$ e $1 < k_2 < n$. Considere, sem perda de generalidade que $k_1 \leq k_2$. Neste caso, $k_1 \leq \sqrt{n}$, pois se não o fosse, teríamos $n = k_1 \cdot k_2 > \sqrt{n} \cdot \sqrt{n} = n$, o que é um absurdo. Ainda, pelo Teorema Fundamental da Aritmética k_1 possui algum fato primo p, consequentemente $p \leq k_1 \leq \sqrt{n}$. Como $p|k_1$ e $k_1|n$, temos que $p|n$. Logo, n possui um fator primo p, tal que $p \leq \sqrt{n}$.

A proposição 2.5.7 é bastante útil ao tentar fatorar um inteiro n em primos, visto que na tentativa de encontrar um divisor primo, basta testar números menores ou iguais que $\sqrt{n}$, se não houver nenhum primo menor ou igual que $\sqrt{n}$, então n é primo. Além disso, esta mesma proposição auxilia na criação do Crivo de Eratóstenes, segundo Coutinho (2014), o método mais antigo para achar primos.

Vamos utilizar o Crivo de Eratóstenes para encontrar os números primos de 1 até 50. Coloque em uma tabela todos os inteiros de 1 até 50. Sabemos que 1 não é primo por definição, então podemos riscar ou pintar o número 1. O próximo número é 2, que é primo, então todos os seus múltiplos maiores que 2 serão compostos, assim podemos pintar todos eles. Até o momento, teríamos uma tabela assim:

Tabela 1 – Crivo de Eratóstenes (1)

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	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Fonte: O Autor

Continuando a sequência, 3 é primo, porém todos os seus múltiplos maiores que 3 não serão, podemos pintá-los. Note que alguns já estarão pintados, pois

também são múltiplos de 2. O número 4 nem precisamos considerar, pois já está pintado, logo 4 é composto e seus múltiplos também o são e já foram pintados. Pela Proposição 15, como nosso crivo vai até 50, basta continuar o processo até eliminar os múltiplos do maior inteiro menor ou igual que a raiz quadrada de 50, ou seja, 7. Ao fim do processo, nosso Crivo estaria assim:

Tabela 2 – Crivo de Eratóstenes (2)

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	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Fonte: O Autor

Os números primos são aqueles que não foram pintados, ou seja, a sequência de todos os números primos menores que 50 é dada por $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$. Apesar de ser uma ideia muito boa para descobrir o início da sequência dos números primos, fica inviável utilizar o processo se quisermos encontrar primos extremamente grandes.

Muitos matemáticos, ao longo da história se preocuparam com este tipo de problema. A busca de números primos muito grandes ou a busca do maior número primo já encontrado. Entre eles, destaca-se Mersenne (1588-1648), ele criou uma fórmula $M_p = 2^p - 1$ que apesar de não gerar somente números primos, consegue gerar números primos extremamente grandes, entre eles o primo de Mersenne $2^{82589933} - 1$ com quase 25 milhões de dígitos descoberto em 2018.

2.6 ARITMÉTICA MODULAR

A Aritmética Modular é ferramenta base na utilização da Criptografia RSA. Durante esta seção veremos alguns resultados extremamente importantes para o funcionamento do sistema de Criptografia RSA.

Definição 2.6.1: Dados inteiros a e b e um inteiro positivo m. Diz-se que a é congruente a b, módulo m, ou ainda que b é um resíduo de a módulo m, se $m|a - b$. Neste caso, denota-se $a \equiv b\ (mod\ m)$. Caso a não seja congruente a b, módulo m, denota-se $a \not\equiv b\ (mod\ m)$.

Note que o fato de a ser congruente a b, módulo m, está intimamente relacionado ao fato de a e b terem o mesmo resto na divisão por m, como veremos na proposição a seguir.

Proposição 2.6.1: Sejam $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}_+^*$ e as divisões euclidianas de a e b por m dadas por $a = m \cdot q_1 + r_a$, com $0 \leq r_a < m$ e $b = m \cdot q_2 + r_b$, com $0 \leq r_b < m$, temos que $a \equiv b \ (mod\ m)$ se, e somente se, $r_a = r_b$.

Demonstração: Primeiramente mostraremos que se $a \equiv b \ (mod\ m)$, então $r_a = r_b$. Como $a \equiv b \ (mod\ m)$, pela Definição 2.6.1 temos que $m|a - b$. Assim, existe um inteiro k, tal que $a - b = k \cdot m$. Substituindo os valores de a e b nesta igualdade temos que $(m \cdot q_1 + r_a) - (m \cdot q_2 + r_b) = k \cdot m$, o que implica que $(q_1 - q_2) \cdot m + (r_a - r_b) = k \cdot m$. Mas, como $|r_a - r_b| < m$, comparando a igualdade obtida podemos concluir que $r_a - r_b = 0$, e finalmente, $r_a = r_b$. De forma recíproca, se $r_a = r_b$, então $r_a - r_b = 0$. Daí, $a - b = (m \cdot q_1 + r_a) - (m \cdot q_2 + r_b) = (q_1 - q_2) \cdot m + (r_a - r_b) = (q_1 - q_2) \cdot m$, e como $q_1 - q_2 \in \mathbb{Z}$ temos que $m|a - b$, logo pela Definição 2.6.1 $a \equiv b \ (mod\ m)$.

■

Decorrem diretamente da definição ainda os seguintes resultados apresentados na Proposição 2.6.2.

Proposição 2.6.2: Considere $a, b, c \in \mathbb{Z}$ e $m \in \mathbb{Z}_+^*$. Segue que:

i) (Propriedade Reflexiva) $a \equiv a \ (mod\ m)$

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

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

Demonstração:

i) Como para todo $m \in \mathbb{Z}_+^*$ tem-se que $m|0$. Seque que $m|a - a$, logo pela Definição 2.6.1 $a \equiv a \ (mod\ m)$.

ii) Como $a \equiv b \ (mod\ m)$, pela Definição 2.6.1 $m|a - b$, ou seja, existe $k \in \mathbb{Z}$ tal que $a - b = m \cdot k$. Multiplicando ambos os membros da igualdade por -1, obtemos $b - a = m \cdot (-k)$. Daí, como $-k$ também é um inteiro, temos que $m|b - a$, e novamente pela Definição 2.6.1 $b \equiv a \ (mod\ m)$.

iii) Como $a \equiv b \ (mod\ m)$ e $b \equiv c \ (mod\ m)$, decorre da definição que $m|a - b$ e $m|b - c$. Logo, $m|(a - b) + (b - c)$, o que implica que $m|a - c$. Daí, $a \equiv c \ (mod\ m)$.

■

Proposição 2.6.3: Sejam $a, b, c, d \in \mathbb{Z}$ e $m, n \in \mathbb{Z}_+^*$ tais que $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$, então as seguintes sentenças são verdadeiras:

i) $a + c \equiv b + d\ (mod\ m)$

ii) $ac \equiv bd\ (mod\ m)$

iii) $a^n \equiv b^n\ (mod\ m)$

Demonstração:

i) Como $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$, decorre da definição que $m|a - b$ e $m|c - d$. Assim, pelo item $vi)$ da Proposição 2.3.1, $m|(a - b) + (c - d)$, reorganizando a expressão temos que $m|(a + c) - (b + d)$. Novamente pela definição segue que $a + c \equiv b + d\ (mod\ m)$.

ii) Como $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$, decorre da definição que $m|a - b$ e $m|c - d$. Agora, como c e b são inteiros, pelo item $vi)$ da Proposição 2.3.1 temos que $m|(a - b) \cdot c + (c - d) \cdot b$, o que implica que $m|ac - bd$. Logo, pela definição segue que $ac \equiv bd\ (mod\ m)$.

iii) Como $a \equiv b\ (mod\ m)$, temos que $m|a - b$. Agora, note que $a^n - b^n = (a - b) \cdot (a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + a^{2b^{n-3}} + ab^{n-2} + b^{n-1})$, portanto $(a - b)|(a^n - b^n)$. Daí, como $m|a - b$ e $(a - b)|(a^n - b^n)$ temos que $m|a^n - b^n$, ou seja, $a^n \equiv b^n\ (mod\ m)$.

■

Definição 2.6.2: Sejam $a, b \in \mathbb{Z}$ e $m \in \mathbb{Z}_+^*$. Chamamos b de inverso modular de a, módulo m, se $a \cdot b \equiv 1\ (mod\ m)$.

A existência de inverso é confirmada apenas mediante a condição de a e m serem primos entre si, como veremos na proposição a seguir.

Proposição 2.6.4: Seja $a \in \mathbb{Z}$ e $m \in \mathbb{Z}_+^*$. Existe um inteiro b, tal que $a \cdot b \equiv 1\ (mod\ m)$ se, e somente se, $(a, m) = 1$.

Demonstração: Primeiramente iremos mostrar que se $a \cdot b \equiv 1\ (mod\ m)$, então $(a, m) = 1$. Como neste caso, por hipótese $a \cdot b \equiv 1\ (mod\ m)$, temos que $m|a \cdot b - 1$. Assim, existe $k \in \mathbb{Z}$ tal que $a \cdot b - 1 = k \cdot m$. Reorganizando esta equação de forma conveniente temos que $a \cdot b - m \cdot k = 1$. Logo, pela Observação 2.4.2, referente ao Teorema de Bachet-Bézout segue que $(a, m) = 1$.

Agora, mostraremos que se $(a,m)=1$, então $a\cdot b\equiv 1\,(mod\,m)$. Como $(a,m)=1$, pelo Teorema de Bachet-Bézout existem $x_0,y_0\in\mathbb{Z}$ tais que $a\cdot x_0+m\cdot y_0=1$. Reorganizando a equação temos que $a\cdot x_0-1=m\cdot(-y_0)$, e como $(-y_0)\in\mathbb{Z}$, isto implica que $m|a\cdot x_0-1$. Tome então $b=x_0$, como $m|a\cdot b-1$ segue que $a\cdot b\equiv 1\,(mod\,m)$.

■

A proposição abaixo trata sobre a Lei do Cancelamento em relação a adição e multiplicação na Aritmética Modular. Conforme será demonstrado, embora não se apresentem maiores problemas ao empregar o cancelamento na adição, na multiplicação, a validade do cancelamento é sujeita a uma importante condição.

Proposição 2.6.5: Sejam $a,b,c\in\mathbb{Z}$ e $m\in\mathbb{Z}_+^*$, as seguintes sentenças são válidas:

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

ii) Se $(c,m)=1$ e $ac\equiv bc\,(mod\,m)$, então $a\equiv b\,(mod\,m)$.

Demonstração:

i) Como $a+c\equiv b+c\,(mod\,m)$, por definição $m|(a+c)-(b+c)$, ou seja, $m|a-b$. Logo, $a\equiv b\,(mod\,m)$.

ii) Como $ac\equiv bc\,(mod\,m)$, por definição $m|ac-bc$, o que implica que $m|c\cdot(a-b)$. Daí, como $(c,m)=1$, pelo Lema de Gauss temos que $m|a-b$. Logo, $a\equiv b\,(mod\,m)$.

■

A proposição apresentada a seguir servirá como Lema para a prova do Pequeno Teorema de Fermat, apresentado em sequência.

Proposição 2.6.6: Dados $a\in\mathbb{Z}$ e p um número primo, tais que $p\nmid a$. Considere então, a sequência $(a,2a,3a,\dots,(p-1)\cdot a)$ formada por $p-1$ múltiplos de a. Pode-se afirmar que:

i) A sequência não possui múltiplos de p. Isto é, para qualquer $k\in\{1,2,3,\dots,p-1\}$ temos que $p\nmid k\cdot a$.

ii) A sequência não possui dois números congruentes entre si, módulo p. Ou seja, para quaisquer $k_1,k_2\in\{1,2,3,\dots,p-1\}$, se $k_1\neq k_2$, então $k_1\cdot a\not\equiv k_2\cdot a\,(mod\,p)$.

Demonstração:

i) Suponha, por absurdo, que exista $k \in \{1,2,3,\dots,p-1\}$ tal que $p|k \cdot a$. Note que, como $1 \leq k \leq p-1$, temos que $(k,p) = 1$. Daí, pelo Lema de Gauss, como $p|k \cdot a$ segue que $p|a$. Absurdo, pois contraria nossa hipótese.

ii) Suponha novamente por absurdo, que existam $k_1, k_2 \in \{1,2,3,\dots,p-1\}$, com $k_1 \neq k_2$ e $k_1 \cdot a \equiv k_2 \cdot a \ (mod\ p)$. Pela hipótese do Lema, como $p \nmid a$, temos que $(a,p) = 1$. Assim, pela Proposição 2.6.5 podemos efetuar o cancelamento de a na congruência $k_1 \cdot a \equiv k_2 \cdot a \ (mod\ p)$, o que implica que $k_1 \equiv k_2 \ (mod\ p)$. Mas como $k_1, k_2 \in \{1,2,3,\dots,p-1\}$, isto implica que $k_1 = k_2$. Absurdo, pois contraria o fato de $k_1 \neq k_2$.

■

Observação 2.6.1: Observe que como a sequência $(a, 2a, 3a, \dots, (p-1) \cdot a)$ é formada por $p-1$ termos, nenhum deles congruente a 0 módulo p e nenhum termo congruente a outro da própria sequência. Podemos concluir que ao analisar os resíduos r, com $1 \leq r < p$, de todos os termos da sequência, módulo p, encontraremos todos os possíveis resíduos $1, 2, 3, \dots, p-1$, não necessariamente nesta ordem.

Teorema (Pequeno Teorema de Fermat): Seja p um número primo e $a \in \mathbb{Z}$. Se $p \nmid a$, então $a^{p-1} \equiv 1 \ (mod\ p)$.

Demonstração: Considere a sequência $(a, 2a, 3a, \dots, (p-1) \cdot a)$ formada por $p-1$ múltiplos de a. Ao multiplicar todos os membros desta sequência, pela Proposição 2.6.6, juntamente com a Observação 2.6.1 temos que:

$$a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1) \cdot a \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \ \ (mod\ p)$$

$$\Rightarrow a^{p-1} \cdot (p-1)! \equiv (p-1)! \ (mod\ p)$$

Agora, como $\big((p-1)!, p\big) = 1$, pela proposição 2.7.5 conclui-se que $a^{p-1} \equiv 1 \ (mod\ p)$.

■

2.6.1 Função Totiente de Euler e o Teorema de Euler

Nesta seção apresentaremos a Função Totiente de Euler. O termo Totiente vem de “totiens”, do Latim, que significa “tantas vezes”, a função, também conhecida apenas como Função de Euler, ou apenas Função Totiente, recebe este nome porque

busca associar a um inteiro positivo m, a quantidade de inteiros positivos menores que m que são co-primos com m. Além da Função Totiente será apresentado o Teorema de Euler, que pode ser visto como uma generalização do Pequeno Teorema de Fermat.

Definição 2.6.1.1: Denomina-se função φ de Euler (lê-se função "fi" de Euler), a função que aplicada a um inteiro positivo m, retorna $\varphi(m)$, que representa a quantidade de inteiros positivos menores que m, que são relativamente primos com m. Por convenção adota-se $\varphi(1) = 1$.

Vejamos alguns exemplos:

i) $\varphi(6) = 2$, pois existem apenas dois inteiros positivos menores que 6 que são co-primos de 6, são eles 1 e 5.

ii) $\varphi(14) = 6$, pois o conjunto de números inteiros positivos menores que 14 que são co-primos com 14, $\{1, 3, 5, 9, 11, 13\}$ é formado por 6 elementos.

Perceba que apesar de não ser difícil calcular a função $\varphi(m)$, para um m pequeno, isto parece ser muito mais complicado quando tivermos valores maiores de m. Os resultados mostrados a seguir serão úteis para tal tarefa.

Proposição 2.6.1.1: Considere $p \in \mathbb{Z}$. p é primo se, e somente se, $\varphi(p) = p - 1$.

Demonstração: Primeiramente iremos mostrar que se p é primo, então $\varphi(p) = p - 1$. De fato, como p é primo, seus únicos divisores são 1 e p. Assim, p é co-primo com todos os $p - 1$ números da sequência $1,2,3, \dots, p - 1$. Logo, $\varphi(p) = p - 1$.

Agora mostraremos que se $\varphi(p) = p - 1$, então p é primo. Suponha, por absurdo, que p não é primo, isto significa que existe $k \in \mathbb{Z}$, com $1 < k < p$, tal que $k|p$. Assim, $(k, p) \neq 1$. Daí, como o conjunto $B = \{1,2,3, \dots, p - 1\}$ é formado por $p - 1$ elementos e $k \in B$, temos que $\varphi(p) \neq p - 1$. Absurdo, pois contraria a nossa hipótese.

■

Proposição 2.6.1.2: Se p é primo e k é um inteiro positivo, então $\varphi(p^k) = p^k - p^{k-1}$.

Demonstração: Queremos encontrar a quantidade de inteiros x, com $1 \leq x \leq p^k$, tal que $(x, p^k) = 1$. Repare que não há problema em considerar $x \leq p^k$, no lugar de $x \leq p^k - 1$, pois se $x = p^k$ temos $(x, p^k) \neq 1$. Agora, como p é primo x e p^k serão co-primos se, e somente se $p \nmid x$. Portanto, poderíamos calcular quantos elementos

do conjunto $B = \{1,2,3, \dots, p^k\}$ são divisíveis por p e descontar a quantia do total de p^k elementos. Considere então, o conjunto B' formado por todos os múltiplos de p que pertencem ao conjunto B, temos $B' = \{p, 2p, 3p, \dots, p^{k-1} \cdot p\}$. Note que $p^{k-1} \cdot p = p^k$. Assim, como B' possui p^{k-1} elementos, temos que $\varphi(p^k) = p^k - p^{k-1}$.

■

Definição 2.6.1.2: Dizemos que o conjunto dos inteiros $\{r_1, r_2, \dots, r_k\}$ é um sistema completo de resíduos módulo m se satisfaz as seguintes condições:

i) $r_i \neq r_j \ (mod\ m)$ para $i \neq j$

ii) para todo $n \in \mathbb{Z}$ existe um r_i tal que $n \equiv r_i \ (mod\ m)$.

Note que, por exemplo, $\{0, 1, 2, \dots, m-1\}$ é um sistema completo de resíduos módulo m.

Observação 2.6.1.1: É fácil perceber que se k inteiros $r_1, r_2, \dots, r_k$ formam um sistema completo de resíduos módulo m, então $k = m$.

Proposição 2.6.1.3: Considere $a, k, m \in \mathbb{Z}$, com m maior que 1 e $(k, m) = 1$. Se $\{a_1, a_2, \dots, a_m\}$ é um sistema completo de resíduos módulo m, então $\{a + k \cdot a_1, a + k \cdot a_2, \dots, a + k \cdot a_m\}$ também é um sistema completo de resíduos módulo m.

Demonstração: Primeiramente iremos mostrar que os elementos de $\{a + k \cdot a_1, a + k \cdot a_2, \dots, a + k \cdot a_m\}$ são, dois a dois, incongruentes entre si. Para isso, considere $i, j \in \mathbb{Z}$, com $1 \leq i, j \leq m$ e $i \neq j$. Suponha, por absurdo, que $a + k \cdot a_i \equiv a + k \cdot a_j \ (mod\ m)$, então $k \cdot a_i \equiv k \cdot a_j \ (mod\ m)$. Como, por hipótese $(k, m) = 1$, pode-se cancelar k na congruência anterior, obtendo $a_i \equiv a_j \ (mod\ m)$. Mas, como $\{a_1, a_2, \dots, a_m\}$ é um sistema completo de resíduos módulo m, isto implica que $i = j$. Absurdo, pois contraria o fato de que $i \neq j$. Por fim, como o conjunto $\{a + k \cdot a_1, a + k \cdot a_2, \dots, a + k \cdot a_m\}$ é formado por m elementos, todos incongruentes entre si, dois a dois, de fato para todo inteiro n, existe um elemento da forma $a + k \cdot a_1$, tal que $n \equiv a + k \cdot a_1 \ (mod\ m)$. Logo, $\{a + k \cdot a_1, a + k \cdot a_2, \dots, a + k \cdot a_m\}$ é um sistema completo de resíduos módulo m.

■

Proposição 2.6.1.4: Se m e n são inteiros positivos primos entre si, então $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Demonstração: Observe a tabela abaixo com os números inteiros de 1 até $m \cdot n$.

$$\begin{array}{ccccccc} 1, & 2, & \cdots & r, & \cdots & n \\ 1+n, & 2+n, & \cdots & r+n, & \cdots & 2n \\ 1+2n, & 2+2n, & \cdots & r+2n, & \cdots & 3n \\ \vdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ 1+(m-1)\cdot n, & 2+(m-1)\cdot n, & \cdots & r+(m-1)\cdot n, & \cdots & m\cdot n \end{array}$$

Note que cada linha da representa um sistema completo de resíduos módulo n. Além disso, os elementos da coluna j, com $1 \leq j < n$, são todos congruentes a j módulo n, com os elementos da coluna n sendo congruentes a 0 módulo n, pois são todos divisíveis por n. Como $(m,n) = 1$, para que um número da tabela seja primo entre si com $m \cdot n$, é necessário e suficiente que ele seja primo entre si com m, e com n. Assim, existem $\varphi(n)$ colunas com elementos que são primos entre si com n, cada uma destas colunas contendo $\varphi(m)$ elementos primos entre si com m. Logo, $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

■

Corolário 2.6.1.1: Seja $n = p \cdot q$, com p, q números primos distintos. Tem-se que $\varphi(n) = (p-1) \cdot (q-1)$.

Demonstração: Como $(p,q) = 1$, pela proposição 2.6.1.4 e proposição 2.6.1.1 tem-se que $\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$.

■

O Corolário 2.6.1.1 será utilizado diretamente na Criptografia RSA.

Proposição 2.6.1.5: Seja n um inteiro cuja fatoração em primos é dada por

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m}$$

tem-se que $\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_m}\right)$.

Demonstração: Como $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m}$, e $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_m^{\alpha_m}$ são todos primos entre si, dois a dois, pela Proposição 2.7.1.4 temos que

$$\varphi(n) = \varphi\left(p_1^{\alpha_1}\right) \cdot \varphi\left(p_2^{\alpha_2}\right) \cdot \ldots \cdot \varphi\left(p_m^{\alpha_m}\right)$$

Daí, pela Proposição 2.6.1.2

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdot \left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right) \cdot \ldots \cdot \left(p_m^{\alpha_m} - p_m^{\alpha_m - 1}\right)$$

$$\Rightarrow \varphi(n) = {p_1}^{\alpha_1} \cdot \left(1 - \frac{1}{p_1}\right) \cdot {p_2}^{\alpha_2} \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot {p_m}^{\alpha_m} \cdot \left(1 - \frac{1}{p_m}\right)$$

$$\Rightarrow \varphi(n) = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot \ldots \cdot {p_m}^{\alpha_m} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_m}\right)$$

$$\Rightarrow \varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_m}\right)$$

■

A partir da Proposição 2.6.1.5 fica mais fácil calcular o valor de $\varphi(m)$ para valores de m não tão pequenos. Observe o exemplo.

Exemplo: Calcule $\varphi(230)$.

Solução: Como $230 = 2 \cdot 5 \cdot 23$, pela Proposição 2.6.1.5 temos que

$\varphi(230) = 230 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{23}\right) = (230 - 115) \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{23}\right) =$

$115 \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{23}\right) = (115 - 23) \cdot \left(1 - \frac{1}{23}\right) = 92 \cdot \left(1 - \frac{1}{23}\right) = 92 - 4 = 88.$

A seguir, é apresentada a definição de Sistema Reduzido de Resíduos, bem como um resultado que será utilizado na demonstração do Teorema de Euler.

Definição 2.6.1.3: Um sistema reduzido de resíduos módulo m é um conjunto de $\varphi(m)$ inteiros $r_1, r_2, \ldots, r_{\varphi(m)}$, tais que cada elemento do conjunto é relativamente primo com m, e se $i \neq j$, com $1 \leq i, j \leq \varphi(m)$, então $r_i \not\equiv r_j \ (mod\ m)$, ou seja, seus elementos são, dois a dois, incongruentes entre si módulo m.

Proposição 2.6.1.6: Seja a um inteiro e m um inteiro positivo tal que $(a, m) = 1$. Se $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ é um sistema reduzido de resíduos módulo m, então $\{a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\varphi(m)}\}$ também é um sistema reduzido de resíduos módulo m.

Demonstração: Primeiramente iremos mostrar que os elementos de $\{a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\varphi(m)}\}$ são todos incongruentes entre si, dois a dois, módulo m. Dados $i, j \in \mathbb{Z}$, com $1 \leq i, j \leq \varphi(m)$, e $i \neq j$. Suponha por absurdo, que $a \cdot r_i \equiv a \cdot r_j \ (mod\ m)$. Como $(a, m) = 1$, isto implica que $r_i \equiv r_j \ (mod\ m)$. Absurdo, pois contradiz o fato de que r_i, r_j pertencem a $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$, que por hipótese, é um sistema reduzido de resíduos módulo m. Agora, note que como para todo r_i, temos que $(r_i, m) = 1$ e $(a, m) = 1$, isto implica que $(a \cdot r_i, m) = 1$, todos os $\varphi(m)$ elementos de $\{a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\varphi(m)}\}$ são primos entre si com m. Logo, $\{a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\varphi(m)}\}$ também é um sistema reduzido de resíduos módulo m.

■

Teorema de Euler: Sejam m e a inteiros, com $m > 1$ e $(a, m) = 1$. Então,

$$a^{\varphi(m)} \equiv 1 \ (mod\ m)$$

Demonstração: Considere $A = \{r_1, r_2, \dots, r_{\varphi(m)}\}$ e $B = \{a \cdot r_1, a \cdot r_2, \dots, a \cdot r_{\varphi(m)}\}$ dois sistemas reduzidos de resíduos módulo m. Ao analisar o produto de todos os membros de B módulo m, temos que

$$(a \cdot r_1) \cdot (a \cdot r_2) \cdot \dots \cdot (a \cdot r_{\varphi(m)}) \equiv r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)} \ (mod\ m)$$

$$\Rightarrow a^{\varphi(m)} \cdot (r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)}) \equiv (r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)}) \ (mod\ m)$$

Agora, como para todo r_i, com $1 \leq i \leq \varphi(m)$, temos que $(r_i, m) = 1$, então $(r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)}, m) = 1$. Assim, podemos cancelar o termo $(r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)})$ da congruência, obtendo finalmente que $a^{\varphi(m)} \equiv 1 \ (mod\ m)$.

■

3 CRIPTOGRAFIA

Este capítulo apresenta com base em Coutinho (2014), um pouco sobre a história da Criptografia, além de mostrar o processo de codificação e decodificação da Criptografia RSA e demonstrar sua validade.

A palavra Criptografia vem do grego *kryptos*, que significa secreto e *graphein,* que significa escrita. Assim, a Criptografia pode ser entendida como a arte e ciência de proteger informações por meio da transformação de dados em formatos ilegíveis para aqueles que não são os destinatários legítimos das informações.

Os principais objetivos da Criptografia são:

- Garantir que apenas as partes autorizadas possam acessar e ler os dados;

- Assegurar que os dados não foram alterados ou corrompidos durante o processo da transmissão ou armazenamento;

Um dos modelos de criptografia mais antigo e historicamente relevante é a Cifra de César. A técnica possui este nome em homenagem ao general romano Júlio César, que a utilizava para proteger suas comunicações militares. A Cifra de César é composta por um simples mecanismo de substituição, onde cada letra do alfabeto é deslocada um número fixo de posições. Por exemplo, com um deslocamento de três posições, a letra “A” seria substituída pela letra “D”, “B” seria substituída pela letra “E”, e assim por diante, como mostra o quadro abaixo.

Quadro 1 – Cifra de César com Deslocamento de Três Casas

Letra do Alfabeto Original → Letra do Alfabeto Criptografado

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

Fonte: O Autor

Assim, a mensagem “ATACAREMOS AO AMANHECER” seria criptografada como “DWDFDUHPRVDRDPDQKHFHU”, sem considerar os acentos e espaços. Ao receber a mensagem, bastava realizar o processo inverso, que neste caso é extremamente simples aos aliados sabendo a quantidade de casas deslocadas (chave de criptografia).

Note que apesar de simples, e até mesmo útil na época, basta um pouco de conhecimento em estatística e linguística às tropas inimigas, para estudar a frequência das letras do alfabeto em cada idioma, e descobrir sem muita demora qual a chave de criptografia utilizada. Descobrindo a chave de criptografia, é extremamente fácil decifrar a mensagem, pois a mensagem original poderia ser descoberta até mesmo em segundos a depender das ferramentas utilizadas.

A Cifra de César é um exemplo de criptografia simétrica, pois a chave utilizada para criptografar as mensagens – quantidade de casas deslocadas no alfabeto - é a mesma que a utilizada para descriptografar.

Atualmente, a criptografia desempenha um papel fundamental na segurança da informação moderna, visto que inúmeras informações e dados privados são transmitidos via internet. Graças a evolução da criptografia, atualmente podemos acessar um e-mail com segurança, realizar transações bancárias de forma online e até mesmo realizar compras utilizando o cartão de crédito, afinal, todas estas operações utilizam informações que precisam estar protegidas.

Em 1976, Whitfield Diffie e Martin Helmann apresentaram a criptografia assimétrica através do conceito de criptografia de chave pública. Neste modelo, a chave utilizada para criptografar uma informação, não é a mesma chave utilizada para descriptografar. Assim, a chave utilizada para criptografar pode se tornar pública, sem perda de segurança do modelo.

Para entender melhor, imagine a situação onde um banco precisa receber informações sobre transações online que são geradas em seu sistema, mas de forma

com que só ele as consiga ler. O banco gera duas chaves, uma pública (para criptografar) e uma privada, que só o banco tem acesso (para descriptografar). Qualquer transação realizada no site do banco seria criptografada com a chave pública, e qualquer um que conseguisse interceptar a transação, teria acesso as informações criptografadas e a chave pública utilizada na criptografia. No entanto, apenas o banco teria a chave privada para descriptografar guardada consigo. Assim, apenas ele consegue descriptografar as informações tornando a transação segura.

Apesar de parecer uma ideia simples e genial, a princípio não é tão simples pensar em um modelo onde o conjunto de chaves pública (criptografar) e privada (descriptografar) se relacionam de forma com que uma realize exatamente o processo inverso da outra, sem que seja óbvio, ou ao menos fácil determinar a chave privada, para descriptografar a partir da chave para criptografar, que é pública. A próxima seção abordará uma solução encontrada para este problema, a criptografia RSA.

3.1 CRIPTOGRAFIA RSA

Em 1977, os pesquisadores Ron Rivest, Adi Shamir e Leonard Adleman apresentam o modelo de Criptografia RSA, que leva as iniciais de seus nomes. A Criptografia RSA foi o primeiro modelo de criptografia assimétrica a ser implementado.

A segurança do sistema RSA se baseia na dificuldade de descobrir (em tempo hábil) a fatoração em primos de um número n formado pelo produto de dois números primos extremamente grandes p e q. Os números p e q escolhidos costumam ter centenas ou até mesmo milhares de dígitos.

3.1.1 Codificando e Decodificando uma Mensagem

Para explicar o funcionamento do modelo RSA, iremos codificar (criptografar) e depois decodificar (descriptografar) a palavra PROFMAT. O processo se dá em três partes:

1ª Parte: Pré-Codificação.

Nesta etapa, transformamos todos os caracteres da mensagem em números. Como nossa mensagem é formada apenas por letras maiúsculas, iremos utilizar o quadro abaixo.

Quadro 2 – Pré-Codificação RSA

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

Fonte: O Autor

Note que o Quadro 2 inicia transformando a letra A no número 10, não no número 1, isto ocorre para garantir que todos os caracteres sejam transformados em números com a mesma quantidade de algarismos, afim de que não haja confusão no processo de codificação e decodificação. Para uma mensagem formada por mais tipos de caracteres, poderia se tornar necessário adotar um quadro que transformasse os caracteres em números com três dígitos. É importante mencionar que o número pelo qual iniciamos o quadro não tem importância para o processo, poderíamos começar o quadro no 11 e terminar no 36, o importante é garantir a mesma quantidade de algarismos para cada número gerado.

Segundo o Quadro 2, a palavra PROFMAT será pré-codificada como 25272415221029.

2ª Parte: Codificação.

Para codificar nossa mensagem, primeiramente devemos escolher dois primos p e q que irão gerar o número $n = p \cdot q$. Os números primos p e q serão utilizados no processo de decodificação, já o número n pertence a chave de codificação, que é pública.

Como já mencionado, no sistema RSA são utilizados primos p e q com centenas, ou até mesmo milhares de algarismos, afim de impossibilitar descobrir os valores p e q a partir de n em tempo hábil. Para se ter noção do tamanho da segurança do RSA quando ele surgiu, a computação clássica levaria milhões de anos para quebrar os níveis mais fortes de segurança RSA. Com a evolução da computação quântica, surge a dúvida de até quando o sistema RSA será seguro, visto que este tipo de computação consegue fatorar número primos grandes de forma muito mais rápida. No entanto, o sistema RSA ainda é visto como seguro e vários outros sistemas de criptografia vêm sendo desenvolvidos para garantir a segurança de informações na nova era da computação que está por vir.

Para fins de exemplo e apresentação dos cálculos, iremos tomar $p = 5$ e $q = 11$. Assim, temos $n = p \cdot q = 5 \cdot 11 = 55$.

A próxima etapa consiste em separar a nossa mensagem já pré-codificada 25272415221029 em blocos. A formação dos blocos pode ser feita de várias formas desde que cada bloco b gerado seja menor que n. Neste caso, iremos separar nossa mensagem em 7 blocos, 25 – 27 – 24 – 15 – 22 – 10 – 29.

Agora, precisamos tomar um inteiro positivo λ que seja inversível módulo $\varphi(n)$. Pelo Corolário 2.6.1.1, segue que $\varphi(n) = (p-1) \cdot (q-1)$ e pela Proposição 2.6.4 conclui-se que precisamos determinar λ de forma com que $mdc(\lambda, \varphi(n)) = 1$. Para os valores de p e q tomados neste exemplo temos $\varphi(55) = (5-1) \cdot (11-1) = 4 \cdot 10 = 40$. Tomaremos então $\lambda = 3$, visto que $(3, 40) = 1$ e, portanto, 3 é inversível módulo 40. A chave pública de codificação é formada pelos números n e λ.

Para codificar nossa mensagem, cada bloco original b será codificado como um bloco a, onde $a \in \mathbb{Z}$ com $0 \leq a < n$ e $b^{\lambda} \equiv a \ (mod\ n)$.

1º Bloco: 25.

Precisamos descobrir qual o inteiro a, com $0 \leq a < n$, tal que $25^3 \equiv a \ (mod\ 55)$. Utilizando algumas propriedades da Aritmética Modular temos que

$$25^3 \equiv 25^2 \cdot 25 \equiv 625 \cdot 25 \equiv 20 \cdot 25 \equiv 500 \equiv 5 \ (mod\ 55)$$

Assim, temos $a = 5$.

2º Bloco: 27.

$$27^3 \equiv 27^2 \cdot 27 \equiv 729 \cdot 27 \equiv 14 \cdot 27 \equiv 378 \equiv 48 \ (mod\ 55)$$

3° Bloco: 24.

$$24^3 \equiv 24^2 \cdot 24 \equiv 576 \cdot 24 \equiv 26 \cdot 24 \equiv 624 \equiv 19 \ (mod\ 55)$$

4º Bloco: 15.

$$15^3 \equiv 15^2 \cdot 15 \equiv 225 \cdot 15 \equiv 5 \cdot 15 \equiv 75 \equiv 20 \ (mod\ 55)$$

5° Bloco: 22.

$$22^3 \equiv 22^2 \cdot 22 \equiv 484 \cdot 22 \equiv 44 \cdot 22 \equiv 968 \equiv 33 \ (mod\ 55)$$

6° Bloco: 10.

$$10^3 \equiv 10^2 \cdot 10 \equiv 100 \cdot 10 \equiv 45 \cdot 10 \equiv 450 \equiv 10 \ (mod\ 55)$$

7º Bloco: 29.

$$29^3 \equiv 29^2 \cdot 29 \equiv 841 \cdot 29 \equiv 16 \cdot 29 \equiv 464 \equiv 24 \ (mod\ 55)$$

Assim, a palavra PROFMAT foi codificada como 5 – 48 – 19 – 20 – 33 – 10 – 24.

3ª Parte: Decodificação.

Ao realizar o processo de decodificação do código 5 – 48 – 19 – 20 – 33 – 10 – 24 devemos encontrar a palavra PROFMAT.

A chave de decodificação, é formada por n, e pelo inteiro d, que é o inverso multiplicativo de λ módulo $\varphi(n)$. Lembrando que em nosso exemplo tomamos $\lambda = 3$ e que $\varphi(55) = (5-1)\cdot(11-1) = 40$, logo é necessário descobrir o valor de d tal que $3 \cdot d \equiv 1\ (mod\ 40)$. Não é difícil concluir que $d = 27$, visto que $3 \cdot 27 \equiv 81 \equiv 1\ (mod\ 40)$. Note a importância de se manter confidencial a informação de quais são os números p e q, pois através deles é calculado $\varphi(n)$ e, consequentemente o valor de d.

Para descriptografar nossa mensagem, cada bloco a irá gerar um bloco b', onde $b' \in \mathbb{Z}$ com $0 \leq b' < n$ e $a^d \equiv b'\ (mod\ n)$. Para que o sistema ocorra com sucesso, cada bloco b' deve ser igual ao bloco b original. Na próxima seção iremos provar este fato.

1° Bloco: 5.

$$5^{27} \equiv (5^3)^9 \equiv 125^9 \equiv 15^9 \equiv (15^2)^4 \cdot 15 \equiv 225^4 \cdot 15 \equiv 5^4 \cdot 15 \equiv 5^3 \cdot 5 \cdot 15 \equiv 15 \cdot 75 \equiv 15 \cdot 20 \equiv 300 \equiv 25\ (mod\ 55)$$

2º Bloco: 48.

$$48^{27} \equiv (-7)^{27} \equiv ((-7)^3)^9 \equiv (-343)^9 \equiv (-13)^9 \equiv ((-13)^2)^4 \cdot (-13) \equiv 169^4 \cdot (-13) \equiv 4^4 \cdot (-13) \equiv 256 \cdot (-13) \equiv 36 \cdot (-13) \equiv -468 \equiv 27\ (mod\ 55)$$

3º Bloco: 19.

$$19^{27} \equiv (19^2)^{13} \cdot 19 \equiv 361^{13} \cdot 19 \equiv 31^{13} \cdot 19 \equiv (31^2)^6 \cdot 31 \cdot 19 \equiv 961^6 \cdot 589 \equiv 26^6 \cdot 39 \equiv (26^2)^3 \cdot 39 \equiv 676^3 \cdot 39 \equiv 16^3 \cdot 39 \equiv 16^2 \cdot 16 \cdot 39 \equiv 256 \cdot 624 \equiv 36 \cdot 19 \equiv 684 \equiv 24\ (mod\ 55)$$

4º Bloco: 20.

$$20^{27} \equiv (20^2)^{13} \cdot 20 \equiv 400^{13} \cdot 20 \equiv 15^{13} \cdot 20 \equiv (15^2)^6 \cdot 15 \cdot 20 \equiv 225^6 \cdot 300 \equiv 5^6 \cdot 25 \equiv 5^3 \cdot 5^3 \cdot 25 \equiv 125 \cdot 125 \cdot 25 \equiv 15 \cdot 15 \cdot 25 \equiv 225 \cdot 25 \equiv 5 \cdot 25 \equiv 125 \equiv 15\ (mod\ 55)$$

5º Bloco: 33.

$$33^{27} \equiv (-22)^{27} \equiv ((-22)^2)^{13} \cdot (-22) \equiv 484^{13} \cdot (-22) \equiv 44^{13} \cdot (-22) \equiv (-11)^{13} \cdot (-22) \equiv ((-11)^2)^6 \cdot (-11) \cdot (-22) \equiv 121^6 \cdot 242 \equiv 11^6 \cdot 22 \equiv (11^2)^3 \cdot 22 \equiv 121^3 \cdot 22 \equiv 11^3 \cdot 22 \equiv 11^2 \cdot 11 \cdot 22 \equiv 121 \cdot 242 \equiv 11 \cdot 22 \equiv 242 \equiv 22\ (mod\ 55)$$

6º Bloco: 10.

$$10^{27} \equiv (10^2)^{13} \cdot 10 \equiv 100^{13} \cdot 10 \equiv (-10)^{13} \cdot 10 \equiv ((-10^2))^6 \cdot (-10) \cdot 10$$
$$\equiv 100^6 \cdot (-100) \equiv (-10)^6 \cdot 10 \equiv ((-10)^2)^3 \cdot 10 \equiv 100^3 \cdot 10$$
$$\equiv (-10)^3 \cdot 10 \equiv (-10)^2 \cdot (-10) \cdot (10) \equiv 100 \cdot (-100) \equiv (-10) \cdot 10$$
$$\equiv -100 \equiv 10\ (mod\ 55)$$

7º Bloco: 24.

$$24^{27} \equiv (24^2)^{13} \cdot 24 \equiv 576^{13} \cdot 24 \equiv 26^{13} \cdot 24 \equiv (26^2)^6 \cdot 26 \cdot 24 \equiv 676^6 \cdot 624 \equiv 16^6 \cdot 19$$
$$\equiv (16^2)^3 \cdot 19 \equiv 256^3 \cdot 19 \equiv 36^3 \cdot 19 \equiv (-19)^3 \equiv (-19)^2 \cdot (-19) \cdot 19$$
$$\equiv 361 \cdot (-361) \equiv 31 \cdot 24 \equiv 744 \equiv 29\ (mod\ 55)$$

Ao descriptografar o código 5 – 48 – 19 – 20 – 33 – 10 – 24, encontramos o código original 25 – 27 – 24 – 15 – 22 – 10 – 29. Utilizando o Quadro 2 temos nossa mensagem original PROFMAT.

3.1.2 Explicando por que o método de Criptografia RSA funciona

Sintetizando como funciona o sistema RSA, para criptografar uma mensagem, primeiramente realizamos uma pré-codificação transformando cada caractere da mensagem em um número e separando o código gerado em blocos.

Cada bloco b gerado deve ser menor que a chave pública n formada pelo produto dos primos p e q. A partir da escolha de λ, que é inversível módulo $\varphi(n)$, cada bloco b será codificado como um bloco a, onde $b^\lambda \equiv a\ (mod\ n)$ e $0 \leq a < n$.

No processo de decodificação será utilizado d, que é o inverso multiplicativo de λ módulo $\varphi(n)$. Cada bloco a irá gerar um bloco b', onde $a^d \equiv b'\ (mod\ n)$.

Para mostrar que o sistema funciona, ou seja, que cada bloco codificado, ao ser decodificado retorna a mensagem original, precisamos mostrar que dentre as condições do sistema RSA, qualquer bloco b' gerado na decodificação será igual ao bloco b original.

Como $b' \equiv a^d\ (mod\ n)$ e $a \equiv b^\lambda\ (mod\ n)$, temos que $b' \equiv \left(b^\lambda\right)^d\ (mod\ n)$, ou ainda $b' \equiv b^{\lambda d}\ (mod\ n)$.

Note que $\lambda d \equiv 1\ \left(mod\ \varphi(n)\right)$. Como $\varphi(n) = (p-1) \cdot (q-1)$ segue que $\lambda d \equiv 1\ (mod\ (p-1)(q-1))$. Assim, existe um inteiro k, tal que $\lambda d - 1 = k \cdot (p-1) \cdot (q-1)$, o que implica que $\lambda d = 1 + k \cdot (p-1) \cdot (q-1)$. Logo, $b^{\lambda d} = b^{1+k\cdot(p-1)\cdot(q-1)} = b \cdot b^{k\cdot(p-1)\cdot(q-1)}$.

Agora, queremos provar que $b^{\lambda d} \equiv b\ (mod\ p)$. Para isso, iremos separar o problema em dois casos.

1° Caso: $(p, b) \neq 1$.

Neste caso, como p é primo, isto implica que b é um múltiplo de p, ou seja, que $b \equiv 0\ (mod\ p)$. Daí, $b^{\lambda d} \equiv 0^{\lambda d} \equiv 0 \equiv b\ (mod\ p)$.

2° Caso: $(p, b) = 1$.

Como $(p, b) = 1$, pelo Pequeno Teorema de Fermat, temos que $b^{p-1} \equiv 1\ (mod\ p)$. Assim, $b^{\lambda d} \equiv b \cdot b^{k\cdot(p-1)\cdot(q-1)} \equiv b \cdot (b^{p-1})^{k\cdot(q-1)} \equiv b \cdot (1)^{k\cdot(q-1)} \equiv b\ (mod\ p)$.

Analogamente se prova que $b^{\lambda d} \equiv b\ (mod\ q)$.

Daí, como $b^{\lambda d} \equiv b\ (mod\ p)$ e $b^{\lambda d} \equiv b\ (mod\ q)$, existem inteiros k_1 e k_2 tais que

$$\begin{cases} b^{\lambda d} - b = k_1 \cdot p \\ b^{\lambda d} - b = k_2 \cdot q \end{cases}$$

Mas, como p e q são primos, existe um inteiro k_3, tal que

$$b^{\lambda d} - b = k_3 \cdot p \cdot q$$

$$\Rightarrow b^{\lambda d} - b = k_3 \cdot n$$

$$\Rightarrow b^{\lambda d} \equiv b\ (mod\ n)$$

Agora, lembre que $b' \equiv b^{\lambda d}\ (mod\ n)$, logo, por transitividade $b' \equiv b\ (mod\ n)$ e como ambos são inteiros não-negativos menores que n podemos concluir que $b' = b$ como queríamos demonstrar.

4 PROPOSTAS DE SEQUÊNCIA DIDÁTICA

Este capítulo busca apresentar algumas propostas de sequência didática com o objetivo de proporcionar experiências de aprendizagem significativas e contextualizadas envolvendo conceitos de Aritmética Modular e Criptografia.

Observação: O tempo estimado em cada etapa da sequência didática é apenas uma previsão, um norte. O planejamento pedagógico deve ser flexível e existem inúmeras situações que podem acontecer em sala de aula que fazem com que o professor possa ajustar o tempo de cada etapa e até mesmo reformular algumas etapas de acordo com a sua necessidade. Além disso, se houver esta possibilidade

através de projetos no contra-turno, um projeto integrado com sala e oficinas no contra-turno seria de grande valia para dividir as terefas propostas.

Sequência Didática 1: Conceitos de Aritmética Modular/Divisão Euclidiana através da Resolução de Problemas.

Ano/Série: 6° Ano do Ensino Fundamental.

Competências Gerais da BNCC:

1. Conhecimento: Valorizar e utilizar os conhecimentos historicamente construídos sobre o mundo físico, social, cultural e digital para entender e explicar a realidade, continuar aprendendo e colaborar para a construção de uma sociedade justa, democrática e inclusiva.

2. Pensamento científico, crítico e criativo: Exercitar a curiosidade intelectual e recorrer à abordagem própria das ciências, incluindo a investigação, a reflexão, a análise crítica, a imaginação e a criatividade, para investigar causas, elaborar e testar hipóteses, formular e resolver problemas e criar soluções (inclusive tecnológicas) com base nos conhecimentos das diferentes áreas.

4. Comunicação: Utilizar diferentes linguagens – verbal (oral ou visual-motora, como Libras, e escrita), corporal, visual, sonora e digital –, bem como conhecimentos das linguagens artística, matemática e científica, para se expressar e partilhar informações, experiências, ideias e sentimentos em diferentes contextos e produzir sentidos que levem ao entendimento mútuo.

9. Empatia e cooperação: Exercitar a empatia, o diálogo, a resolução de conflitos e a cooperação, fazendo-se respeitar e promovendo o respeito ao outro e aos direitos humanos, com acolhimento e valorização da diversidade de indivíduos e de grupos sociais, seus saberes, identidades, culturas e potencialidades, sem preconceitos de qualquer natureza.

Competências Específicas da Área de Matemática da BNCC:

2. Desenvolver o raciocínio lógico, o espírito de investigação e a capacidade de produzir argumentos convincentes, recorrendo aos conhecimentos matemáticos para compreender e atuar no mundo.

6. Enfrentar situações-problema em múltiplos contextos, incluindo-se situações imaginadas, não diretamente relacionadas com o aspecto prático-utilitário, expressar suas respostas e sintetizar conclusões, utilizando diferentes registros e

linguagens (gráficos, tabelas, esquemas, além de texto escrito na língua materna e outras linguagens para descrever algoritmos, como fluxogramas, e dados).

8. Interagir com seus pares de forma cooperativa, trabalhando coletivamente no planejamento e desenvolvimento de pesquisas para responder a questionamentos e na busca de soluções para problemas, de modo a identificar aspectos consensuais ou não na discussão de uma determinada questão, respeitando o modo de pensar dos colegas e aprendendo com eles.

Unidade Temática: Números.

Objetos de Conhecimento: Divisão Euclidiana.

Habilidades: Resolver problemas que possuem ciclos de repetição através do Raciocínio Lógico e Divisão Euclidiana.

Número de Aulas: 2 aulas.

Materiais Necessários: Lousa, Lápis, Caderno.

Descrição da Atividade:

Momento 1: (5 min) Dividir a turma em grupos de 3 ou 4 estudantes.

Momento 2: (40 min) Entregar os problemas abaixo para que cada grupo possa tentar resolver as questões interagindo entre os membros do grupo.

Exercício 1: Observe a sequência abaixo formada pelos símbolos

%, *, &, %, *, &, %, *, &, ...

Supondo que a sequência mantenha o padrão apresentado, responda:

a) Qual o 10° termo da sequência?

b) Qual o 30° termo da sequência?

c) Qual o 2024° termo da sequência?

Exercício 2: Uma pista circular possui uma volta com comprimento igual a 438m. Após José percorrer 2848m nesta pista, responda:

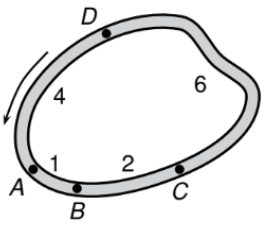
a) Quantas voltas completas José percorreu?

b) Após concluir as voltas completas, José ainda percorreu quantos metros?

Exercício 3: Questão 6 da 2ª Fase da OBMEP 2006, Nível 1.

Figura 1 – Questão OBMEP

(6) A figura representa o traçado de uma pista de corrida. Os postos *A*, *B*, *C* e *D* são usados para partidas e chegadas de todas as corridas. As distâncias entre postos vizinhos, em quilômetros, estão indicadas na figura e as corridas são realizadas no sentido indicado pela flecha.
Por exemplo, uma corrida de 17 km pode ser realizada com partida em *D* e chegada em *A*.



(a) Quais são os postos de partida e chegada de uma corrida de 14 quilômetros?
(b) E para uma corrida de 100 quilômetros, quais são esses postos?
(c) Mostre que é possível realizar corridas com extensão igual a qualquer número inteiro de quilômetros.

Fonte: Olimpíada Brasileira de Matemática das Escolas Públicas. Prova do Nível 1, questão 6, 2006.

Observações ao professor: Neste momento, espera-se que o professor primeiramente observe atentamente o trabalho de cada grupo na resolução das questões, se os mesmos estão interagindo de forma colaborativa e respeitosa. O professor ainda pode fazer alguns apontamentos e/ou provocações de acordo com a necessidade de cada grupo ou aluno.

Momento 3: (45min) Correção dos problemas com a turma. Este momento **não** deve ser um espaço onde o professor apresenta a “solução correta” de cada problema e a turma fica em silêncio copiando. Espera-se que cada grupo possa apresentar suas ideias e que a turma juntamente com os apontamentos e questionamentos do professor possa refletir sobre a solução apresentada pelos colegas, indicando pontos positivos, possíveis equívocos. É comum, pela idade em que se encontram, que os alunos queiram apenas “acertar” a questão, chegando na resposta final correta, mesmo que seja no chute. Cabe ao professor conversar com a turma e mostrar que o importante é o raciocínio desenvolvido na solução de cada questão, e que uma ideia que chega na resposta correta por mera coincidência, não possui validade lógica alguma. É possível também, que surjam soluções diferentes para o mesmo problema, é extremamente importante valorizar cada ideia apresentada, parabenizar os estudantes pela solução encontrada, e neste caso, analisar as soluções, discutir os pontos positivos e negativos de cada uma e identificar se uma se destaca sobre as demais. Todos estes levantamentos e discussões constituem um momento mágico em sala de aula, onde a turma está construindo o conhecimento sob a mediação do professor, aprendendo a argumentar com base em fundamentos lógicos.

Abaixo, encontra-se uma possível solução para cada questão e possíveis apontamentos e discussões sobre as questões e suas respectivas soluções.

Solução Exercício 1:

a) Este exercício busca identificar se o aluno conseguiu interpretar e compreender o enunciado do exercício, visto que a parte da sequência mostrada no enunciado possui 9 elementos, logo o 10° elemento seria o próximo, %.

b) É possível que alguns alunos escrevam a sequência até o 30° termo. Ao identificar isto no momento da resolução dos exercícios, o professor poderia provocar o grupo a encontrar uma solução mais "esperta", visto que apenas completar a sequência até pode ser uma forma de responder o item b), mas não é uma boa ideia para resolver o item c). Uma solução, seria identificar que a sequência se repete em blocos formados por três símbolos: %, *, &. Assim, se escrevêssemos os 30 primeiros termos da sequência, iríamos escrever exatamente 10 vezes o bloco %, *, &. Assim, o 30° símbolo da sequência é o &.

c) Escrever os 2024 primeiros símbolos da sequência seria uma tarefa "fácil", porém extremamente demorada, então parece que deve haver alguma solução mais esperta para esta questão. Como a sequência se repete a cada 3 símbolos, podemos pegar os 2024 símbolos da sequência e dividir em blocos de 3 símbolos, da Divisão Euclidiana temos que $2024 = 3 \cdot 674 + 2$, isto significa que ao dividir os 2024 símbolos em blocos de 3 símbolos (%, *, &), são gerados 674 blocos (%, *, &) e no final ainda sobram ou restam 2 símbolos. Logo, a sequência termina como

..., %, *, &, %, *

e o 2024° símbolo da sequência é o *.

Particularmente, se quisermos descobrir qual símbolo se encontra na n-ésima posição desta sequência, basta analisar o resto da divisão de n por 3. Resto 1 indica que o símbolo é %, resto 2 representa *, e o resto 0 indica que houve uma quantidade inteira de blocos de 3 símbolos, portanto o último símbolo é &.

A ideia apresentada na solução desta questão não serve apenas para descobrir o 2024° ou o n-ésimo elemento de uma sequência que se repete a cada 3 algarismos, mas sim descobrir qualquer elemento de qualquer sequência que possua um padrão de repetição. Esta discussão é extremamente importante e uma ótima ideia seria abordar outras questões análogas a esta em outras aulas.

Solução Exercício 2: Novamente aplicando os conceitos da Divisão Euclidiana, ao dividirmos os 2848 metros a serem percorridos em pedaços/voltas de 438 metros, temos que $2848 = 438 \cdot 6 + 220$. Logo, podemos perceber que José

percorreu 6 voltas completas de 438 metros e, após completar as 6 voltas andou mais 220 metros. Respostas:

a) 6 voltas.

b) 220 m.

Solução Exercício 3: Note que a distância percorrida ao dar uma volta completa na pista é de 13 km.

a) Percorrer 14 km corresponde a dar uma volta completa (13 km) e depois andar mais 1 km. Assim, basta começar a corrida no ponto A, percorrer uma volta completa, e depois terminar no ponto B.

b) Como $100 = 13 \cdot 7 + 9$, uma corrida de 100 km corresponde a uma corrida com 7 voltas completas (13 km cada) mais 9 km. Assim, o problema é equivalente a encontrar os postos de partida e chegada de uma corrida de 9 km, que são respectivamente, A e D (1km + 2km + 6km = 9 km). Logo, para uma corrida de 100 km, parte-se do posto A, dá-se 7 voltas completas, e depois termina-se a corrida no posto D.

c) Antes da solução do exercício, cabe a observação de que esta questão é uma ótima oportunidade para introduzir o conceito de “demonstração” aos alunos. Afinal, é normal que o aluno do 6° ano pense: “Como eu vou mostrar que é possível realizar qualquer corrida com um número inteiro de quilômetros, se existem infinitas possibilidades? Eu nunca vou terminar.” Cabe neste momento algumas provocações à turma: “Já que existem infinitas possibilidades, quantas eu devo mostrar que são válidas? Será que até 20 km está bom? Até 100 km? Até 1000 km? Mas e se a corrida de 1001 km não ter solução e eu não ter verificado?” Perceba que testar se é possível realizar ou não uma corrida de n quilômetros é uma estratégia boa para conhecer melhor o problema, mas apenas testar valores de n nunca será suficiente para mostrar que é possível realizar a corrida para qualquer inteiro n. É necessário além de alguns testes, reconhecer padrões, argumentar de forma lógica,...

Ao realizar alguns testes para conhecer melhor o problema, ou até mesmo por desconfiança, afinal é normal que alguns alunos pensem: “Será que funciona para qualquer valor de quilômetros mesmo?” É possível chegar aos dados apresentados no quadro a seguir.

Quadro 3 – Dados, Problema OBMEP.

Quilometragem	Posto de Partida	Posto de Chegada
1 km	A	B

2 km	B	C
3 km	A	C
4 km	D	A
5 km	D	B
6 km	C	D
7 km	D	C
8 km	B	D
9 km	A	D
10 km	C	A
11 km	C	B
12 km	B	A
13 km	A	A
14 km	A	B
15 km	B	C
16 km	A	C

Fonte: O Autor.

É importante notar que para uma corrida de 13 km ou qualquer múltiplo de 13, pode-se escolher qualquer posto de partida e de chegada, sob a condição de que ambos os postos sejam iguais, neste caso o Quadro 3 apresenta apenas uma possível solução.

Perceba que a partir dos 14 km, as soluções começam a se repetir, isto ocorre porque encontrar o posto de partida e de chegada para uma corrida de 14 km é equivalente a encontrar o posto de partida e chegada para uma corrida de 1 km. Da mesma forma, como uma corrida de 15 km corresponde a uma volta completa de 13km mais um trecho de 2 km, encontrar o posto de partida e de chegada para uma corrida de 15 km equivale a encontrar o posto de partida e de chegada para uma corrida de 2 km. Aqui, o aluno está se deparando com conceitos de Aritmética Modular sem necessariamente escrever que $14 \equiv 1\ (mod\ 13)$ e $15 \equiv 2\ (mod\ 13)$. Na verdade, encontrar os postos de partida e de chegada para uma corrida de n quilômetros, sempre será equivalente a encontrar os postos de partida e de chegada de uma corrida com um número inteiro positivo menor ou igual a 13 km, afinal se n for maior que 13, basta dar algumas voltas na pista até restar um trecho menor do que uma volta. Assim, para garantir que é possível realizar qualquer corrida com um número inteiro de quilômetros, basta garantir que é possível realizar qualquer corrida com quilometragem inteira entre 1 km e 13 km. O Quadro 3 já mostra a solução para cada um dos casos, logo o problema está resolvido.

Avaliação: A avaliação pode ocorrer através da observação, conversa com os alunos e registros no caderno, buscando identificar se os alunos:

- Demonstraram uma compreensão clara dos problemas apresentados;
- Aplicaram estratégias apropriadas para resolver os problemas;
- Demonstraram coerência no raciocínio ao longo do processo de resolução, incluindo a capacidade de reconhecer padrões, e justificar suas escolhas;
- Comunicaram suas ideias de forma clara, organizada e precisa, utilizando linguagem matemática apropriada;
- Colaboraram efetivamente com os colegas, contribuindo com ideias, ouvindo e respeitando diferentes pontos de vista e compartilhando responsabilidades.

Sequência Didática 2: Criptografia.

Ano/Série: 6° Ano do Ensino Fundamental.

Competências Gerais da BNCC:

1. Conhecimento: Valorizar e utilizar os conhecimentos historicamente construídos sobre o mundo físico, social, cultural e digital para entender e explicar a realidade, continuar aprendendo e colaborar para a construção de uma sociedade justa, democrática e inclusiva.

2. Pensamento científico, crítico e criativo: Exercitar a curiosidade intelectual e recorrer à abordagem própria das ciências, incluindo a investigação, a reflexão, a análise crítica, a imaginação e a criatividade, para investigar causas, elaborar e testar hipóteses, formular e resolver problemas e criar soluções (inclusive tecnológicas) com base nos conhecimentos das diferentes áreas.

4. Comunicação: Utilizar diferentes linguagens – verbal (oral ou visual-motora, como Libras, e escrita), corporal, visual, sonora e digital –, bem como conhecimentos das linguagens artística, matemática e científica, para se expressar e partilhar informações, experiências, ideias e sentimentos em diferentes contextos e produzir sentidos que levem ao entendimento mútuo.

9. Empatia e cooperação: Exercitar a empatia, o diálogo, a resolução de conflitos e a cooperação, fazendo-se respeitar e promovendo o respeito ao outro e aos direitos humanos, com acolhimento e valorização da diversidade de indivíduos e de grupos sociais, seus saberes, identidades, culturas e potencialidades, sem preconceitos de qualquer natureza.

Competências Específicas da Área de Matemática da BNCC:

1. Reconhecer que a Matemática é uma ciência humana, fruto das necessidades e preocupações de diferentes culturas, em diferentes momentos históricos, e é uma ciência viva, que contribui para solucionar problemas científicos e tecnológicos e para alicerçar descobertas e construções, inclusive com impactos no mundo do trabalho.

2. Desenvolver o raciocínio lógico, o espírito de investigação e a capacidade de produzir argumentos convincentes, recorrendo aos conhecimentos matemáticos para compreender e atuar no mundo.

7. Desenvolver e/ou discutir projetos que abordem, sobretudo, questões de urgência social, com base em princípios éticos, democráticos, sustentáveis e solidários, valorizando a diversidade de opiniões de indivíduos e de grupos sociais, sem preconceitos de qualquer natureza.

8. Interagir com seus pares de forma cooperativa, trabalhando coletivamente no planejamento e desenvolvimento de pesquisas para responder a questionamentos e na busca de soluções para problemas, de modo a identificar aspectos consensuais ou não na discussão de uma determinada questão, respeitando o modo de pensar dos colegas e aprendendo com eles.

Número de Aulas: 2 aulas.

Materiais Necessários: Lápis, papel, cartões (opcional).

Descrição da Atividade:

Momento 1: (15 min) Separe a turma em 5 grupos. Apresente aos alunos a seguinte proposta: Eles precisam enviar mensagens escritas entre si, de forma com que apenas seus colegas de grupo possam entender. Incentive os alunos a buscar uma solução para este problema. Talvez alguns grupos pensem em cifras de substituição.

Momento 2: (15 min) Apresente o conceito de cifra de substituição, explicando aos alunos como funciona e fornecendo alguns exemplos. Uma ótima ideia seria apresentar a Cifra de César. Peça que cada grupo crie sua própria cifra de substituição, utilizando uma chave secreta.

Momento 3: (15min) Proponha aos grupos que utilizem sua cifra de substituição para criptografar mensagens, peça que troquem mensagens entre si, mantendo o sigilo e a segurança, informe que os outros grupos tentarão decifrar suas mensagens.

Momento 4: (30 min) Peça que os grupos troquem entre si os cartões com as mensagens criptografadas e desafie-os a decifrar as mensagens de outros grupos. Após um tempo, se necessário, indique a estratégia de analisar a frequência de letras e padrões comuns em mensagens.

Momento 5: (15min) Converse com os alunos conduzindo uma discussão sobre o nível de segurança da cifra de substituição e a importância da análise de frequência das letras na quebra da cifra.

Avaliação: A avaliação pode ocorrer através da observação, conversa com os alunos e registros da atividade buscando identificar se os alunos:

- Entenderam o conceito de cifra de substituição e conseguem aplicá-lo na prática;
- Participaram de forma ativa e colaborativa durante todas as etapas da atividade em grupo;
- Utilizaram a criatividade para criptografar suas mensagens e analisaram padrões de forma lógica para quebrar a cifra dos outros grupos.

Observação: Aos professores da 1ª Série do Ensino Médio, uma boa alternativa seria elaborar uma sequência didática análoga no estudo de funções inversas e se for possível trabalhar com programação, elaborar um programa que faça a criptografia das mensagens por cifra de substituição.

Sequência Didática 3: Números Primos (Crivo de Eratóstenes).

Ano/Série: 6° Ano do Ensino Fundamental.

Competências Gerais da BNCC:

1. Conhecimento: Valorizar e utilizar os conhecimentos historicamente construídos sobre o mundo físico, social, cultural e digital para entender e explicar a realidade, continuar aprendendo e colaborar para a construção de uma sociedade justa, democrática e inclusiva.

2. Pensamento científico, crítico e criativo: Exercitar a curiosidade intelectual e recorrer à abordagem própria das ciências, incluindo a investigação, a reflexão, a análise crítica, a imaginação e a criatividade, para investigar causas, elaborar e testar hipóteses, formular e resolver problemas e criar soluções (inclusive tecnológicas) com base nos conhecimentos das diferentes áreas.

4. Comunicação: Utilizar diferentes linguagens – verbal (oral ou visual-motora, como Libras, e escrita), corporal, visual, sonora e digital –, bem como conhecimentos das linguagens artística, matemática e científica, para se expressar e partilhar informações, experiências, ideias e sentimentos em diferentes contextos e produzir sentidos que levem ao entendimento mútuo.

9. Empatia e cooperação: Exercitar a empatia, o diálogo, a resolução de conflitos e a cooperação, fazendo-se respeitar e promovendo o respeito ao outro e aos direitos humanos, com acolhimento e valorização da diversidade de indivíduos e de grupos sociais, seus saberes, identidades, culturas e potencialidades, sem preconceitos de qualquer natureza.

Competências Específicas da Área de Matemática da BNCC:

2. Desenvolver o raciocínio lógico, o espírito de investigação e a capacidade de produzir argumentos convincentes, recorrendo aos conhecimentos matemáticos para compreender e atuar no mundo.

8. Interagir com seus pares de forma cooperativa, trabalhando coletivamente no planejamento e desenvolvimento de pesquisas para responder a questionamentos e na busca de soluções para problemas, de modo a identificar aspectos consensuais ou não na discussão de uma determinada questão, respeitando o modo de pensar dos colegas e aprendendo com eles.

Unidade Temática: Números.

Objetos de Conhecimento: Números Primos e Compostos.

Habilidades: Classificar números naturais em primos e compostos.

Número de Aulas: 2 aulas.

Materiais Necessários: Lousa, lápis, caderno, tabela de números, cartolina/papel pardo, canetão, cola.

Descrição da Atividade:

Momento 1: (1 aula) O professor pode começar apresentando e discutindo com a turma o conceito de número primo e composto, apresentar alguns exemplos, elaborar uma definição junto com a turma. Após isso, pode montar no quadro o Crivo de Eratóstenes com os números de 1 a 30 (exemplo) explicando a ideia por trás do algoritmo para que os alunos percebam que de fato os números que sobram são apenas os primos. Após isso o professor pode entregar uma tabela com os números naturais de 1 até 50 para cada aluno e pedir a ele que faça o processo do Crivo afim de verificar se o aluno conseguiu assimilar o processo de construção do Algoritmo.

Momento 2 (1 aula): Dividir a turma em grupos de 3 ou 4 alunos, entregar uma cartolina ou papel pardo para cada grupo e fichas numeradas de 1 a 100. Os alunos devem colar as fichas de números de forma organizada na cartolina e em seguida aplicar o Crivo de Eratóstenes riscando os múltiplos dos números primos, para esta tarefa é interessante utilizar marcadores de cores diferentes para cada conjunto de múltiplos. Ao final da atividade cada aluno deve apresentar sua cartolina.

Avaliação: A avaliação pode ocorrer através da observação e conversa com os alunos buscando identificar se os alunos:

- Construiram o primeiro crivo de forma adequada em seu caderno;
- Participaram de forma ativa e colaborativa durante a construção do Crivo na cartolina/papel pardo;
- Apresentaram a cartolina ao final da atividade com o crivo realizado de forma correta e seguindo as instruções propostas.

Sequência Didática 4: Números Primos e Criptografia RSA.

Ano/Série: 6° Ano do Ensino Fundamental.

Competências Gerais da BNCC:

1. Conhecimento: Valorizar e utilizar os conhecimentos historicamente construídos sobre o mundo físico, social, cultural e digital para entender e explicar a realidade, continuar aprendendo e colaborar para a construção de uma sociedade justa, democrática e inclusiva.

2. Pensamento científico, crítico e criativo: Exercitar a curiosidade intelectual e recorrer à abordagem própria das ciências, incluindo a investigação, a reflexão, a análise crítica, a imaginação e a criatividade, para investigar causas, elaborar e testar hipóteses, formular e resolver problemas e criar soluções (inclusive tecnológicas) com base nos conhecimentos das diferentes áreas.

4. Comunicação: Utilizar diferentes linguagens – verbal (oral ou visual-motora, como Libras, e escrita), corporal, visual, sonora e digital –, bem como conhecimentos das linguagens artística, matemática e científica, para se expressar e partilhar informações, experiências, ideias e sentimentos em diferentes contextos e produzir sentidos que levem ao entendimento mútuo.

9. Empatia e cooperação: Exercitar a empatia, o diálogo, a resolução de conflitos e a cooperação, fazendo-se respeitar e promovendo o respeito ao outro e aos direitos humanos, com acolhimento e valorização da diversidade de indivíduos e

de grupos sociais, seus saberes, identidades, culturas e potencialidades, sem preconceitos de qualquer natureza.

Competências Específicas da Área de Matemática da BNCC:

1. Reconhecer que a Matemática é uma ciência humana, fruto das necessidades e preocupações de diferentes culturas, em diferentes momentos históricos, e é uma ciência viva, que contribui para solucionar problemas científicos e tecnológicos e para alicerçar descobertas e construções, inclusive com impactos no mundo do trabalho.

2. Desenvolver o raciocínio lógico, o espírito de investigação e a capacidade de produzir argumentos convincentes, recorrendo aos conhecimentos matemáticos para compreender e atuar no mundo.

7. Desenvolver e/ou discutir projetos que abordem, sobretudo, questões de urgência social, com base em princípios éticos, democráticos, sustentáveis e solidários, valorizando a diversidade de opiniões de indivíduos e de grupos sociais, sem preconceitos de qualquer natureza.

8. Interagir com seus pares de forma cooperativa, trabalhando coletivamente no planejamento e desenvolvimento de pesquisas para responder a questionamentos e na busca de soluções para problemas, de modo a identificar aspectos consensuais ou não na discussão de uma determinada questão, respeitando o modo de pensar dos colegas e aprendendo com eles.

Unidade Temática: Números.

Objetos de Conhecimento: Números Primos e Compostos.

Habilidades: Decompor números compostos em fatores primos.

Número de Aulas: 2 aulas.

Materiais Necessários: Lousa, lápis, caderno, folhas A4, tabela de números primos, calculadora, projetor.

Pré-Requisitos: Espera-se que o aluno já saiba a definição de número primo e composto, saiba que todo número inteiro positivo ou é primo, ou pode ser decomposto em fatores primos e saiba ao menos uma estratégia de fatoração em primos.

Descrição da Atividade:

Momento 1: (1 aula) A turma é dividida em grupos de 4 ou 5 alunos, cada grupo recebe uma tabela de números primos, pode ser até 100.

O professor escreve um número composto no quadro branco e as equipes tentam descobrir a fatoração deste número, assim que conseguir concluir a tarefa a equipe deve escrever a fatoração na folha e virá-la para baixo, para que ninguém mais possa escrever e levantar a mão indicando que terminou a tarefa. O professor estipula um tempo máximo para cada tarefa, podendo variar de acordo com a dificuldade do exercício. Ao terminar o tempo, as equipes que conseguiram resolver o exercício marcam 5 pontos e a equipe que resolveu em menos tempo ganha um bônus de 5 pontos adicionais. Após 10 exercícios ganha a equipe que fizer mais pontos.

Na próxima etapa do desafio, são escolhidos apenas números formados pela fatoração de dois números primos, no entanto, os números primos p e q que geram o número $n = p \cdot q$ são maiores, indica-se utilizar números primos entre 100 e 1000. Os grupos podem receber uma tabela com os números primos menores que 1000 ou se haver disponibilidade de um projetor em sala o professor pode projetar uma tabela com tais números. Nesta etapa os alunos podem utilizar a calculadora para efetuar os cálculos de forma mais rápida. A pontuação é a mesma da etapa anterior, após 5 exercícios ganha a equipe que fizer mais tempos. Se preferir, ao invés de estipular um ganhador por etapa o professor pode estipular um campeão geral somando os pontos obtidos em cada etapa.

Momento 2: (1 aula) Conversa sobre a competição. Espera-se que o aluno identifique que encontrar os fatores primos de um número composto nem sempre é uma tarefa muito fácil, mesmo com o auxílio de uma calculadora. Aqui o professor pode mostrar outras ferramentas tecnológicas como alguma calculadora online para fatoração em primos, provavelmente os alunos ficarão espantados com a agilidade desta ferramenta e irão pensar que podem fatorar qualquer número com ela, por maior que ele seja. No entanto, as calculadoras online também possuem uma capacidade limitada para tal tarefa, e mesmo os melhores programas disponíveis levariam centenas ou milhares de anos para fatorar um número formado pela multiplicação de dois primos com mais de 200 dígitos cada um, então o professor pode apresentar um pouco sobre a Criptografia RSA, e explicar que sua segurança se baseia neste tipo de desafio que os alunos acabaram de participar. Certamente os alunos ficarão surpreendidos com o fato de que a segurança online de vários sistemas utilizados no mundo tem relação com a matemática e com os números primos.

Avaliação: A avaliação pode ocorrer através da observação e conversa com os alunos buscando identificar se os alunos:

- Participaram de forma ativa e colaborativa durante a resolução dos problemas em grupo;
- Fatoraram corretamente os números compostos apresentados;
- Resolveram os problemas dentro do tempo estipulado;
- Refletiram sobre estratégias utilizadas e possíveis melhorias para futuras situações.
- Reconheceram a importância da fatoração de números compostos na Criptografia RSA.

5 CONCLUSÃO

Esta pesquisa explorou a construção matemática que fundamenta o Sistema de Criptografia RSA. Ao investigar a teoria por trás do sistema RSA, destacamos a importância do estudo dos números primos e Aritmética Modular. Além disso, abordamos a história da Criptografia, apresentando como ela foi importante desde suas origens antigas até o mundo moderno.

Ao compreender os princípios e aplicação prática da criptografia RSA, percebemos seu potencial como uma ferramenta valiosa na Educação Básica. As propostas de sequências didáticas apresentadas neste trabalho buscam introduzir conceitos fundamentais de matemática e segurança da informação de forma acessível e envolvente aos alunos. Através de atividades contextualizadas, os estudantes podem não apenas desenvolver habilidades matemáticas essenciais, como também compreender a importância da criptografia na proteção de dados pessoais e na segurança digital. Esperamos que as propostas de sequências didáticas apresentadas sirvam como um recurso valioso para educadores interessados em integrar conceitos de criptografia e segurança da informação em suas práticas pedagógicas, e que buscam abordar os conteúdos matemáticos, particularmente, os conceitos iniciais de Teoria dos Números de forma significativa e contextualizada.

Por fim, esperamos ainda que pesquisas futuras e práticas pedagógicas continuem a aprimorar e expandir essas iniciativas, capacitando os educadores a cultivar uma nova geração de pensadores críticos e protagonistas.

REFERÊNCIAS

BRASIL. Secretaria de Educação Fundamental. **Parâmetros Curriculares Nacionais:** Matemática. Terceiro e Quarto Ciclos do Ensino Fundamental. Brasília: MEC/SEF, 1998.

BRASIL. Ministério da Educação. **Base Nacional Comum Curricular.** Brasília: MEC, 2018.

COUTINHO, Severino Collier. **Números Inteiros e Criptografia RSA.** 2. ed. Rio de Janeiro: IMPA, 2014.

FERREIRA, Jamil. **Construção dos Números.** 2. ed. Rio de Janeiro: SBM, 2011.

HALMOS, Paul Richard. **Naive Set Theory.** Princeton, New Jersey: D. Van Nostrand Company, 1960.

HEFEZ, Abramo. **Elementos de Aritmética,** Coleção Textos Universitários. 2.ed. Rio de Janeiro: SBM, 2011.

HEFEZ, Abramo. **Aritmética,** Coleção PROFMAT. 1. ed. Rio de Janeiro: SBM, 2013.

LIMA, Elon Lages. **Análise Real, Vol.1: funções de uma variável.** 10. ed. Rio de Janeiro, IMPA, 2008

LIMA, Elon Lages. **Curso de Análise Vol.1.** 12. ed. Rio de Janeiro, IMPA, 2008.

MARTINEZ, Fabio Brochero; MOREIRA, Carlos Gustavo; SALDANHA, Nicolau; TENGAN, Eduardo. **Teoria dos Números, um passeio com primos e outros números familiares pelo mundo inteiro,** Coleção Projeto Euclides. 2.ed. Rio de Janeiro: IMPA, 2011.

PEREIRA, Magda Cristina Nunes. **As investigações matemáticas no ensino-aprendizagem das sucessões: Uma experiência com alunos do 11° ano de escolaridade.** 2004. Dissertação (Mestrado em Ensino da Matemática) – Universidade da Beira Interior, Covilhã, 2004.

SANTOS, José Plínio de Oliveira. **Introdução a Teoria dos Números.** Rio de Janeiro: IMPA, 1998.

SINGH, Simon. **The Code Book: How to make it, break it, hack it, crack it.** 1.ed. New York, New York, Delacorte Press, 2002.

OLIMPÍADA BRASILEIRA DE MATEMÁTICA DAS ESCOLAS PÚBLICAS. Disponível em:
http://www.obmep.org.br/. Acesso em: 09 jun. 2024.