UNIVERSIDADE ESTADUAL DA PARAÍBA
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UEPB

Teoria dos Números e Criptografia com Aplicações Básicas

Uelder Alves Galdino

Trabalho de Conclusão de Curso

Orientador: Prof. Dr. Vandenberg Lopes Vieira

Campina Grande - PB
Setembro/2014

G149t Galdino, Uelder Alves.
Teoria dos Números e Criptografia com aplicações básicas [manuscrito] / Uelder Alves Galdino. - 2014.
77 p.

Digitado.
Trabalho de Conclusão de Curso (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia, 2014.
"Orientação: Prof. Dr. Vandenberg Lopes Vieira, Departamento de Matemática".

1. Criptografia. 2. Método RSA. 3. Ensino de matemática. 4. Aritmética. I. Título.

21. ed. CDD 513

UNIVERSIDADE ESTADUAL DA PARAÍBA
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UEPB

Teoria dos Números e Criptografia com Aplicações Básicas

por

Uelder Alves Galdino †

Trabalho Conclusão de Curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UEPB, na modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre.

†Bolsista CAPES

Teoria dos Números e Criptografia com Aplicações Básicas

por

Uelder Alves Galdino

Trabalho de Conclusão de curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UEPB, modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre.

Aprovado por:

Prof. Dr. Bráulio Maia Júnior - UFCG

Profa. Dra. Maria Isabelle Silva - UEPB

Prof. Dr. Vandenberg Lopes Vieira - UEPB
Orientador

Universidade Estadual da Paraíba
Centro de Ciências e Tecnologia
Curso de Mestrado Profissional em Matemática em Rede Nacional

Setembro/2014

Dedicatória

A toda minha família e em especial
aos meus pais por todo incentivo.

Agradecimentos

A Deus, que sempre me acompanhou em todos os momentos de minha vida e me carregou nos momentos mais difíceis. Ele representa o maior de todos os intelectos e é o grande Matemático do Universo, por isso devo a ti Senhor, toda honra e toda glória.

Aos meus pais, Antônio e Francisca, que sempre acreditaram em meu êxito no decorrer deste curso. Em especial, ao meu pai, pelas palavras de conforto e compreensão.

À minha Esposa Ana Claudia, por entender que foi necessária a minha ausência em momentos oportunos.

Aos meus filhos Ryan e Héllen, pela enorme compreensão durante a minha ausência em circunstâncias importantes. Sem vocês não teria ânimo nas situações desfavoráveis.

Aos meus amigos, colegas de trabalho e demais familiares, de alguma forma, vocês tiveram grande importância no decorrer deste trabalho.

Às diretoras Jeane e Dalvany, pela compreensão da minha ausência nas aulas e reuniões importantes.

Aos meus colegas de mestrado, pela amizade e grande contribuição em todas as etapas deste curso. Todos vocês são especiais.

Aos professores do PROFMAT, que propiciaram o alcance de todos os objetivos necessários para culminância deste trabalho.

Ao meu orientador, o professor Dr. Vandenberg, pela confiança, paciência e grande contribuição na realização deste, além de ter sido fonte de inspiração ao tema abordado durante as aulas ministradas com todo seu competente profissionalismo.

Por fim, agradeço à Sociedade Brasileira da Matemática - SBM pelo oferecimento deste Curso em Rede Nacional e à CAPES pela concessão da bolsa.

Resumo

Este trabalho consiste numa abordagem norteadora constituída por exemplos de aplicações práticas e apresentação de importantes conceitos relativos à Teoria dos Números, confrontando a maneira atual de inserção destes no ensino básico que por muitas vezes são considerados enfadonhos e desprovidos de praticidade. Por essa razão, tem-se a Criptografia como uma ciência de grande aplicabilidade prática destes, principalmente na atualidade devido ao fluxo de importantes transações efetuadas por meio eletrônico, passíveis de interceptação por terceiros. Na ocasião foram apresentados alguns subjetivos métodos de Criptografia, com ênfase ao método RSA, um relevante sistema criptográfico de chave pública. Assim, desde os relatos históricos iniciais aos capítulos referentes à fundamentação teórica foi sempre possível perceber a importância destes temas, em particular aos processos criptográficos estudados, para uma contribuição significativa que desmistifica o ensino e proporciona um aprendizado construtivista, pois acreditamos que o aluno poderá fazer grandes descobertas como sujeito criador de suas ideias, especialmente na resolução de problemas.

Palavras Chaves: Aritmética. Criptografia. RSA.

Abstract

This work is a guiding approach consists of examples of practical applications and presentation of important concepts related to number theory, confronting the current way of inserting these in basic education which often are considered boring and devoid of practicality. For this reason, it has been Cryptography as a science of great practical applicability of these, especially nowadays due to the flow of important transactions by electronic means, subject to interception by third parties. On occasion some subjective methods of cryptography, with emphasis on the RSA method, a major public-key cryptosystem was presented. Thus, from the earliest historical accounts the chapters theoretical foundation was always possible to realize the importance of these issues, in particular the cryptographic processes studied, a significant contribution to the teaching that demystifies and provides a constructivist learning, as we believe that students can make great discoveries as creating subject of his ideas, especially in problem solving.

Keywords: Arithmetic. Cryptografy. RSA.

Sumário

Capítulo 1

Introdução

Desde os tempos mais remotos e, principalmente nos dias atuais, a necessidade de comunicar-se com segurança é imprescindível. A Teoria dos Números é a área da matemática considerada base teórica da ciência capaz de manter o sigilo da informação transmitida entre duas fontes contra terceiros, a criptografia. Que segundo o dicionário *online* Michaelis, é a arte ou processo de escrever em caracteres secretos ou em cifras.

Neste sentido, este trabalho consiste numa proposta de aplicação prática para aulas relacionadas a conteúdos curriculares do ensino da matemática na educação básica, como fonte motivadora para o processo ensino-aprendizagem. Assim, podemos encontrar na Criptografia subsídios que contemplem fortemente esse aspecto educativo de natureza singular, proporcionando novas e relevantes aplicações cotidianas para o ensino desta ciência em nível básico.

Sugerimos este trabalho aos professores interessados em melhorar seus procedimentos metodológicos de ensino, com o intuito de programar aulas dinamizadas e diferenciadas que objetivem mostrar uma real aplicação de determinados conteúdos ministrados no ensino básico. As discussões geradas sobre a falta de aplicação de situações práticas e inovadoras no ensino da Matemática em nível básico são inúmeras. De fato, como afirma os PCN's em [3]:

> *"A Matemática caracteriza-se como uma forma de compreender e atuar no mundo e o conhecimento gerado nessa área do saber como um fruto da construção humana na sua interação constante com o contexto natural, social e cultural"*.

A Teoria dos Números era considerada uma área da Matemática sem aplicações práticas até o desenvolvimento expressivo da Criptografia. No entanto, atualmente podemos envolver estes conteúdos curriculares presentes no ensino básico em aplicações diversas, proporcionando ao educando uma aprendizagem significativa.

Portanto, objetivamos com este trabalho trazer novas inspirações a professores do ensino básico que percebam a importância da aplicabilidade desses resultados na sua prática

docente. Os alunos, também poderão motivar-se para um estudo mais aprofundado sobre Teoria dos Números e Criptografia, no tocante à forma diferenciada de tratar alguns temas, com a perspectiva de melhorar a aprendizagem.

A princípio, apresentaremos fatos e acontecimentos históricos com participação marcante da Criptografia. Os relatos apresentados no Capítulo 1 envolvem basicamente diferentes tipos de métodos criptográficos e suas consequências, sem nos preocuparmos em detalhar tais sistemas de criptografia.

O Capítulo 3 faz referência aos Números Inteiros. Neste tratamos de forma axiomática algumas propriedades, além de conceitos e definições correlacionados a Divisibilidade, Divisão Euclidiana, Máximo Divisor Comum e Mínimo Múltiplo Comum. Na realidade, trata-se de assuntos presentes nos anos iniciais de ensino e, em particular, os tópicos abordados inicia a formação do embasamento teórico ao tema central.

Reservamos ao Capítulo 4 um tratamento preferencial aos Números Primos, pois são considerados de fundamental importância para um dos métodos criptográficos mais utilizados no mundo, em contradição com a realidade, onde a maioria dos alunos de séries iniciais questionam a carência de propósitos significativos destes.

O estudo sobre Congruências é de fundamental importância ao desenvolvimento das principais situações práticas abordadas neste trabalho. Além de aplicações diversas em métodos de Criptografia, há também variadas ocasiões relacionadas à periodicidade, já praticadas em níveis básicos de ensino, sem o conhecimento formal deste. Frequentemente, a Olimpíada Brasileira de Matemática das Escolas Públicas tem levantado algumas questões que podem ser facilmente resolvidas com o uso de congruências. Por essa razão, destinamos o Capítulo 5, com a proposta de inserir este conteúdo, mesmo de forma elementar, no ensino básico. Aprofundamos alguns conhecimentos de resultados fundamentais como, o Teorema de Euler e o Pequeno Teorema de Fermat.

Finalizando, dedicamos a Criptografia um tratamento especial, pois acreditamos que esta ciência é substancialmente necessária aos meios virtuais de comunicação da atualidade. Por esta razão, nesse capítulo abordamos alguns métodos criptográficos, em especial o RSA, com o propósito de motivar o ensino da Matemática em nível básico. Os sistemas apresentados são relativamente de fácil compreensão e com requisitos elementares, com relação à Teoria dos Números empregada. Na última seção desse capítulo, foram propostas situações com o uso de ferramentas tecnológicas acessíveis aos estudantes, para "acelerar" alguns procedimentos presentes em determinados métodos criptográficos. E ainda, buscamos aprimorar o ensino sobre funções e matrizes propondo situações relacionadas diretamente com a Criptografia.

Capítulo 2

Criptografia: Abordagem Histórica

Uma das primeiras informações sobre criptografia data de Heródoto no ano 480 a.C., o qual escreveu sobre os conflitos entre a Grécia e a Pérsia. Na época tratava-se de apenas uma escrita secreta e o termo criptografia ainda não era conhecido. Para maior aprofundamento de tais acontecimentos, sugerimos O livro dos Códigos em [20]. Este faz uma abordagem bastante detalhada a respeito.

Assim como todo conhecimento matemático, a criptografia deve o seu surgimento a situações cotidianas. Como afirma Álvaro Andrini em [1]:

> *"Além da necessidade de criar ferramentas matemáticas para resolver problemas práticos, o ser humano é curioso por natureza. Gosta de investigar, descobrir e explicar coisas que acontecem ao seu redor!"*

De fato, a criptografia que deriva do grego *kriptos* (oculto) e *graphein* (escrever), teve participação essencial em ocasiões históricas. A importância de manter em sigilo relevantes mensagens foi um fator marcante no desenvolvimento dessa ciência.

Simon Singh em [20], descreve:

> *"Durante milhares de anos, reis, rainhas e generais dependeram de comunicações eficientes de modo a governar seus países e comandar seus exércitos."*

Atualmente, o aumento exponencial de transações de dados via internet valoriza ainda mais o desenvolvimento criptográfico de modo a garantir com eficiência a proteção de informações confidenciais. Para o ensino básico, é considerável a contribuição de situações cotidianas, como a criptografia, no processo ensino - aprendizagem durante o estudo de determinado conteúdo.

Nesse sentido, apresentaremos a seguir algumas descrições de acontecimentos nos quais a criptografia participou decisivamente durante a criação, evolução e desfeche.

2.1 A morte de Maria, a rainha da Escócia

A execução de Maria Stuart, rainha da Escócia, foi consequência da confiante segurança nas suas trocas de mensagens criptografadas, que planejavam o assassinato da rainha Elizabeth. Maria foi iludida pelo seu próprio código, cuja descoberta culminou em sua trágica execução. Tal acontecido mostra a essencial presença da criptografia durante fatos históricos e seus respectivos resultados decorrentes de sua natureza sigilosa de consequências desastrosas e também vitoriosas.

2.2 A intrigante Cifra de Beale

Um segundo exemplo criptográfico intrigante é o caso da cifra de Beale. Thomas J. Beale acumulou uma fortuna, um tesouro constituído de ouro e prata, enterrado, no valor aproximado de 20 milhões de dólares em cotações atuais. Beale confiou a um dono de hotel três páginas cifradas, nas quais continham as informações de localização do seu tesouro.

As Cifras de Beale, como ficaram conhecidas as páginas cifradas, é uma enigmática história publicada em 1885 num folheto de autor desconhecido, contendo as páginas cifradas e uma nota destinada a Morris, o dono do hotel. Nessa misteriosa história apenas uma das páginas foi decifrada pelo autor do folheto, a qual não continha a localização da fortuna, apenas a indicação de seu conteúdo.

O autor do folheto, curiosos, caçadores de tesouros, especialistas em decifragem entre outros, dedicaram-se a decifrar as duas páginas restantes, mas todos fracassaram diante da cifra inquebrável do século XIX. No entanto, existem dúvidas quanto a sua veracidade e até mesmo de sua existência.

É natural a motivação ser decorrente da curiosidade. Foi dessa forma que surgiu a grande maioria dos criptógrafos, os quais extraiam da essência da curiosidade o consequente profissionalismo.

2.3 As Guerras Mundiais e seus Segredos Determinantes

Uma terceira situação é a participação crucial da criptografia na primeira e segunda guerras mundiais. Nesse contexto, os países chegaram a criar escritórios militares de cifras, os quais desenvolviam relevante trabalho na criação e decifração de mensagens militares criptografadas.

O telegrama alemão interceptado na Primeira Guerra mundial em 1917 pelos britânicos mostra como a criptografia pode alterar os resultados de uma guerra. O Telegrama de Zimmermann, como ficou conhecido, foi o grande destaque na marcante presença da criptografia durante a Primeira Guerra Mundial.

Fazendo uma comparação dessa situação com a atualidade, é possível imaginar o inconveniente uso de um telegrama para transmitir uma informação tão significativa. São nas necessidades dos fatos que surgem os grandes avanços científicos, especialmente na segurança da informação.

Em decorrência dos fracassos criptográficos durante a Primeira Guerra mundial, os criptógrafos foram motivados à desenvolver recursos tecnológicos avançados. No século XV, com a invenção do Disco de Cifras, nascia a primeira máquina criptográfica inventada pelo arquiteto italiano Leon Alberti. Esse dispositivo seria o antecessor da poderosa máquina Enigma, usada pelos alemães durante a Segunda Guerra Mundial, que frustrou as expectativas de vitória nazista, quando os mesmos tinham plena confiança de seu inexorável poder criptográfico.

Novamente, a criptografia foi fator decisivo no término de uma guerra. A quebra da Enigma modificou os caminhos da vitória na guerra, antecipando o seu fim.

2.4 Contribuições na Segurança da Informação

Com o desenvolvimento do telégrafo no século XIX, a criptografia começa a escrever sua fundamental participação na evolução dos meios de comunicação. Preservar o conteúdo de uma mensagem particular enviada pelo telégrafo era um grande obstáculo na época, assim como nos meios de comunicação atuais.

Posteriormente, o rádio possibilitou um enorme fluxo de mensagens, principalmente em guerras, e devido a sua natureza poderiam ser facilmente interceptadas. Mais uma vez, garantir a privacidade foi primordial no decorrer do progresso tecnológico. Seguindo nesse avanço, surgiu o Colossus, primeiro computador programável e antecessor do moderno computador digital, desenvolvido em 1943 com o intuito de decifrar a forte cifra alemã, Lorenz.

Na era computacional, houve várias vantagens que propiciaram o progresso da criptografia em comparação com as máquinas de cifras mecânicas. Uma das mais significativas diferenças é o uso de números *binários* no lugar de letras. Assim, com a disseminação dos computadores, transações bancárias e comerciais eram realizadas por meio computacional e asseguradas pela criptografia, pois depositavam nessa ciência a responsabilidade de suas operações.

Não necessariamente na ordem cronológica dos fatos, falaremos de importantes idealizações descobertas por Whitfield Diffie e Martin Hellman.

O criptografo Whitfield Diffie conseguiu um feito visionário, prevendo o direito à privacidade na troca de informações através de computadores conectados em rede. Essa situação seria fundamental no decorrer dos anos, principalmente com o surgimento da internet em 1982. No entanto, um fator imprescindível colocava em risco a segurança de uma cifra, a distribuição de chaves. Uma solução para esse pertinente problema seria a maior descoberta criptográfica em dois mil anos.

Vários desistiram na busca implacável de resolver o problema da distribuição de chaves, mas Martin Hellman com contribuições de Whitfield Diffie e Ralph Merkle, comparando cifragem computacional com *funções*, em especial funções de mão única, descobriram na *Aritmética Modular* uma resposta para distribuição de chaves no ano de 1976. Apesar da queda desse dogma, o sistema não era conveniente.

Diffie, em 1975, tinha criado a chave assimétrica que, diferentemente de todas as cifras de chaves simétricas já conhecidas, o processo de decifragem não era apenas o oposto da cifragem. Entretanto, Diffie não conseguiu uma função de mão única como imaginara e portanto a cifra assimétrica não se confirmou na prática.

No entanto, os pesquisadores do Laboratório de Ciências de Computação do MIT, Ron Rivest, Adir Shamir e Leonard Adleman, juntos descobriram a cifra mais revolucionária da criptografia contemporânea, o sistema RSA. Tal sistema recebera as iniciais dos sobrenomes de seus idealizadores e ficou conhecido como criptografia de chave pública. Na verdade, o RSA é fruto dos trabalhos do trio Hellman, Merkle e Diffie, com destaque para descoberta da função de mão única necessária para a cifra assimétrica de Whit Diffie, concluindo assim os problemas relacionados a distribuição de chaves.

O sistema RSA opera com *números primos* e *fatoração*, que possibilitam um enorme nível de segurança, devido às dificuldades encontradas na fatoração, principalmente, de um produto de dois números primos muito grandes.

Há uma história alternativa que antecede as grandes descobertas apresentadas anteriormente, com relação a distribuição de chaves. Trata-se de informações britânicas confidenciais do Quartel-General de Comunicações do Governo (GCHQ), que credita as conquistas referentes à criptografia de chave pública aos integrantes do GCHQ, os quais trabalhavam exclusivamente para tais propósitos e tiveram seus créditos secretamente confinados e revelados posteriormente por outros, desmerecendo assim seus resultados e criando um caso que gerou dúvidas e questionamentos.

Acredita-se que em 1975, James Ellis, Clifford Cocks e Malcolm Williamson tinham descobertos todos os fundamentos sobre a criptografia de chave pública. Nesse sentido, vale ressaltar a importante presença da *Teoria dos Números* no avanço da criptografia, pois não acreditava-se que a matemática pura teria um propósito prático para sua aplicação. Na verdade, a criptografia não alcançaria o seu auge sem a Teoria dos Números e nesse sentido percebemos a magnitude dessa área da matemática no desenvolvimento da era digital, no intuito de garantir a privacidade na troca de informações.

No pensamento que a privacidade na era da informação digital é um direito de todos, Phil Zimmermann criou o Pretty Good Privacy (uma ótima privacidade) ou PGP, um *software* que garante o sigilo das informações entre pessoas comuns, sem conhecimento criptográfico. Nenhum dos fundamentos do PGP eram ideias de seu criador, pois baseavam-se numa assinatura eletrônica confiável e mesclava cifragens simétricas e assimétricas, fatos já idealizados anteriormente. Mas, Zimmerman unificou-as num só programa, facilitando

o uso computacional no meio criptográfico. Esse *software* gerou polêmica com o governo americano, com a sua criação no final da década de 1980, mas garante com confiança a segurança na transmissão de dados com agilidade e isso acarreta ameaças, dependendo de seus maus usuários. Em 1997 o PGP foi legalizado e ainda podemos encontrar gratuitamente o programa para *download* na internet.

2.5 Computador Quântico e Criptografia Quântica

Historicamente, as cifras consideradas inquebráveis sempre pereceram no decorrer do tempo. Um forte exemplo que podemos mencionar, é a cifra de Vigenère, apontada como indecifrável, mas o genial britânico Charles Babbage a decifrou.

Os meios criptográficos atualmente usados nos computadores convencionais estão ameaçados com o desenvolvimento de computadores quânticos. Estes garantem um poder de processamento muito superior comparado aos computadores que utilizam *chips* de silício. Contudo, ainda há dificuldades na evolução dessa ferramenta criptoanalista, que intimida os sistemas criptográficos atuais. Mesmo com computadores quânticos, ainda há algoritmos criptográficos como o sistema de McEliece e a árvore de Merkle, que os superam.

Assim como toda criação de novas cifras, há os perigos relacionados ao mau uso da criptografia, o que dificultaria investigações criminosas, e deixa dúvidas na regulamentação desses fortes meios criptográficos. Entretanto, uma ascensão na criptoanálise replica uma poderosa evolução criptográfica. Assim, em paralelo, há idealizado o surgimento da criptografia quântica, que segundo Simon Singh o seu desenvolvimento cessa o fim na busca do sigilo absoluto.

No ensino básico, a criptografia necessita de diversos conteúdos programáticos que poderão ser trabalhados no intuito desse entendimento.

Sobre a história da matemática os Parâmetros Curriculares Nacionais (PCN´s) relatam:

> *"[...] conceitos abordados em conexão com a sua história constituem veículos de informação cultural, sociológica e antropológica de grande valor informativo."*

E ainda, afirmam que:

> *"Ao verificar o alto nível de abstração matemática de algumas culturas antigas, o aluno poderá compreender que o avanço tecnológico de hoje não seria possível sem a herança cultural de gerações passadas."*

Dessa forma, uma abordagem histórica enaltece a aplicação prática da Teoria dos Números, nessa ciência essencialmente necessária aos meios de comunicação atuais, que a utilizamos espontaneamente em operações sigilosas com o uso de computadores conectados em rede.

Capítulo 3

Números Inteiros

A Teoria dos Números é um dos mais antigos e belos ramos da matemática, com origem nas mais antigas das civilizações. Grandes matemáticos se destacaram por estabelecer importantes contribuições no estudo das propriedades dos números inteiros. Alguns desses, ocasionalmente, serão citados no decorrer desse trabalho, tais como:

Pitágoras (569-500 a.C.), Euclides ($\simeq$ 350 a.C.), Eratóstenes (276-196 a.C.),

Diofanto ($\simeq$ 250 d. C.), M. Mersenne (1588-1648), Fermat (1601-1665),

B. Pascal, (1623-1662), C. Goldbach (1690-1764), L. Euler (1707-1783),

C. F. Gauss (1777-1855), L. Kronecker (1823-1891), J. S. Hadamard (1865-1963),

C. de la Vallée-Poussin (1866-1962), G. H. Hardy (1877-1947).

Os resultados obtidos por eles (e outros não citados acima) nos mostram que a Teoria dos Números sempre ocupou uma posição de destaque no mundo da matemática, sendo uma das poucas teorias que têm resultados comprováveis que precede em muito a forma organizada de estudo atualmente. Dentre esses resultados, destacamos o fato de a sequência dos números primos

$$2, 3, 5, 7, 11, 13, 17, ...$$

ser infinita, que foi provado primeiro por Euclides[1]. A sua demonstração está certamente entre as mais notáveis de toda matemática.

[1] *Euclides* de Alexandria, matemático grego, que por volta de 300 a.C., escreveu um tratado que representa um grande marco na Matemática, *Os Elementos* de Euclides. Esta obra reúne 13 livros, nos quais 10 abordam sobre geometria e 3 sobre aritmética. Apesar de não ter criado muitos resultados, seu importante feito destaca-se pelo padrão de apresentação e rigor matemático empregado. Pouco se sabe da biografia deste notável matemático, no entanto, recomendamos a leitura de *Elementos de Aritmética*, de Abramo Hefez [12], este traz melhores referências sobre.

Dessa forma, os que estudam e acompanham o desenvolvimento dessa teoria podem testemunhar seu avanço, com importantes e elegantes resultados relacionados a propriedades dos números inteiros. Nesse sentido, destacamos a sua importância no avanço tecnológico, em particular, na Criptografia, ambiente no qual as propriedades dos números primos são relevantes, de modo a garantir a segurança na troca de informações na era digital.

O conjunto dos números inteiros consiste em um conteúdo essencial no ensino básico, especialmente no ensino fundamental, onde a maioria dos educandos tem dificuldades de aprendizado devido à falta de aplicações práticas que concretizem determinados conceitos. As questões abordadas no Exame Nacional do Ensino Médio (ENEM) adotam questões contextualizadas com situações práticas e próximas da realidade de muitos estudantes. Neste sentido, seria conveniente que o professor do ensino básico usasse conceitos relacionados à Teoria do Números, tais como *máximo divisor comum* e *mínimo múltiplo comum*, de modo concretizá-los. Mas, em geral, isso atualmente não é visto devido as problemáticas do ensino atual

3.1 Uma Fundamentação Axiomática dos Inteiros

As propriedades listadas nesta seção são pré-requisitos dos próximos resultados e base de fundamentação teórica do assunto central desse trabalho. Em geral, esta parte é considerada um pouco tediosa, pois apresenta algo obviamente conhecido por maioria dos estudantes nas séries iniciais.

Inicialmente, denotaremos o conjunto dos números inteiros pela seguinte representação usual:

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}.$$

As propriedades das operações de adição e multiplicação de números inteiros serão consideradas axiomas, pois não iremos prová-las aqui.

A operação de adição de números inteiros, indicada por " $+$ ", satisfaz os seguintes axiomas:

$\mathscr{A}_1$. **Fechamento:** Para quaisquer inteiros a e b,

$$a + b \in \mathbb{Z}.$$

$\mathscr{A}_2$. **Associatividade da adição:** Para quaisquer inteiros a, b e c,

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

$\mathscr{A}_3$. **Comutatividade da adição:** Para quaisquer inteiros a e b,

$$a + b = b + a.$$

$\mathscr{A}_4$. **Existência de elemento neutro para a adição:** Existe um único elemento $0 \in \mathbb{Z}$, chamado **zero**, de maneira que

$$a+0=a,\ \forall\, a \in \mathbb{Z}.$$

$\mathscr{A}_5$. **Existência de inverso aditivo:** Dado um inteiro a, existe um único inteiro $-a$, chamado **simétrico** ou **oposto** de a, tal que

$$a+(-a)=0.$$

$\mathscr{A}_6$. **Cancelativa da adição:** Dados os inteiros a, b e c,

$$a+b=a+c \Rightarrow b=c.$$

A multiplicação de números inteiros, indicada por " $\cdot$ " é essencialmente a adição repetida.

Assim como a adição, a multiplicação é associativa, comutativa e tem elemento neutro (o número 1), mais precisamente:

$\mathscr{M}_1$. **Fechamento:** Para quaisquer inteiros a e b,

$$a \cdot b \in \mathbb{Z}.$$

$\mathscr{M}_2$. **Associatividade da multiplicação:** Para quaisquer inteiros a, b e c,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

$\mathscr{M}_3$. **Comutatividade da multiplicação:** Dados os inteiros a e b,

$$a \cdot b = b \cdot a.$$

$\mathscr{M}_4$. **Existência de elemento neutro para multiplicação:** Existe um único elemento $1 \in \mathbb{Z}$, chamado **um**, tal que

$$1 \cdot a = a \cdot 1 = a, \forall\, a \in \mathbb{Z}.$$

O próximo axioma vincula as duas operações, isto é,

$\mathscr{M}_5$. **A multiplicação é distributiva em relação à adição:** Para quaisquer inteiros a, b e c,

$$a \cdot (b+c) = a \cdot b + a \cdot c.$$

Finalmente,

$\mathscr{M}_6$. **Lei do cancelamento da multiplicação:** Dados os inteiros a, b e c, com $a \neq 0$,

$$a \cdot b = a \cdot c \Rightarrow b = c.$$

Dando continuidade aos estudos feitos sobre os inteiros, na proposição que segue apresentamos algumas propriedades que são obtidas dos axiomas mencionados.

Proposição 3.1.1 *Dados a, b e c inteiros quaisquer, temos:*

(1) $a \cdot 0 = 0$.

(2) Se $a \cdot b = 0$, então $a = 0$ ou $b = 0$. **(Integridade de $\mathbb{Z}$)**

Demonstração: (1) Temos que

$$a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 = a \cdot 0 + 0,$$

ou seja, $a \cdot 0 + a \cdot 0 = a \cdot 0$. Como $a \cdot 0 \in \mathbb{Z}$, então existe $-(a \cdot 0) \in \mathbb{Z}$ tal que $-(a \cdot 0) + (a \cdot 0) = 0$. Logo, adicionando $-(a \cdot 0)$ a ambos os membros da igualdade $a \cdot 0 + a \cdot 0 = a \cdot 0$, e usando a propriedade associativa da adição, obtemos

$$(-(a \cdot 0) + a \cdot 0) + a \cdot 0 = -(a \cdot 0) + a \cdot 0,$$

isto é, $0 + a \cdot 0 = 0$, de modo que $a \cdot 0 = 0$.

(2) Pelo item (1), temos que $a \cdot 0 = 0$, e por hipótese, $a \cdot b = 0$; por isso, $a \cdot b = a \cdot 0$. Se $a = 0$, o resultado segue naturalmente. Caso contrário, usando a lei do cancelamento da multiplicação, obtemos que $b = 0$. □

A próxima proposição nos lembra algo que conhecemos desde o ensino básico sobre os inteiros quando multiplicamos números precedidos de sinais. Geralmente, alguns livros didáticos adotados no ensino fundamental trazem métodos que ajudam a decorar esse fundamento. Aqui, o trataremos de forma mais elegante.

Proposição 3.1.2 (Regra dos Sinais) *Se a e b são inteiros quaisquer, então*

(1) $-(-a) = a$.

(2) $(-a) \cdot (b) = -(a \cdot b) = a \cdot (-b)$.

(3) $(-a) \cdot (-b) = a \cdot b$.

Demonstração: (1) Notemos que por definição, se $a, b \in \mathbb{Z}$ e $a + b = 0$, então $a = -b$. Por isso, como $a + (-a) = 0$, segue imediato que $a = -(-a)$.

(2) Temos que

$$a \cdot b + (-a) \cdot (b) = (a + (-a)) \cdot b = 0 \cdot b = 0,$$

ou seja, $(-a)\cdot(b) = -(a\cdot b)$. Da mesma forma,

$$a\cdot b + a\cdot(-b) = a\cdot(b+(-b)) = a\cdot 0 = 0,$$

de modo que $a\cdot(-b) = -(a\cdot b)$. Portanto,

$$(-a)\cdot(b) = -(a\cdot b) = a\cdot(-b).$$

(3) Usando inicialmente o item (2),

$$(-a)\cdot(-b) = -(a\cdot(-b)) = -(-(a\cdot b)).$$

Agora, pelo item (1), $-(-a) = a$ para todo $a \in \mathbb{Z}$. Assim, $(-a)\cdot(-b) = a\cdot b$. □

Dado $a \in \mathbb{Z}$, o **módulo** (ou **valor absoluto**) de a, em símbolos $|a|$, é definido como:

$$|a| = \begin{cases} a & \text{se} \quad a \geq 0, \\ -a & \text{se} \quad a < 0. \end{cases}$$

Segue imediatamente da definição acima que $|a| \geq 0$ para todo $a \in \mathbb{Z}$, e ainda que $|a| = 0$ se, e somente se, $a = 0$. Por exemplo, $|-7| = 7$ e $|10| = 10$.

3.2 Divisibilidade

Nesta seção vamos considerar o conceito de divisibilidade sobre o conjunto dos números inteiros e suas principais propriedades, que são extremamente importantes na Teoria dos Números e na fundamentação teórica deste trabalho. Além do mais, consiste em um tópico bastante discutido nas séries iniciais de ensino.

A princípio, já sabemos que a adição e multiplicação usuais de inteiros são duas operações sobre $\mathbb{Z}$. Sabemos também que dados dois inteiros a e b, com $b \neq 0$, nem sempre a razão a/b é um número inteiro, ou seja, em geral, não existe um inteiro k de modo que $a = b\cdot k$. Por exemplo, $7/2$ não é um inteiro. Isso nos conduz ao conceito de divisibilidade.

Sejam a e b dois números inteiros com $b \neq 0$. Diremos que b **divide** a, e indicamos por $b \mid a$, se existir $k \in \mathbb{Z}$ tal que

$$a = bk.$$

Escrevemos $b \nmid a$ para indicar o fato que b não divide a. Assim,

$$b \mid a \;\Leftrightarrow\; a = bk \quad \text{para algum} \quad k \in \mathbb{Z}.$$

Exemplo 3.2.1 Temos que $-2 \mid 14$, pois $14 = (-2)\cdot(-7)$ e ainda que $12 \nmid -7$, pois não existe $k \in \mathbb{Z}$, tal que $-7 = 12\cdot k$.

Além disso, $1 \mid a$, $a \mid a$ e $a \mid 0$, pois $a = 1\cdot a$, $a = a\cdot 1$ e $0 = a\cdot 0$ para todo $a \in \mathbb{Z}$.

Lema 3.2.2 *Se $b \mid a$ e $a \neq 0$, então $|b| \leq |a|$.*

Demonstração: Se $b \mid a$, então existe $k \in \mathbb{Z}$ tal que $a = b \cdot k$. Logo,

$$|a| = |b \cdot k| = |b| \cdot |k| .$$

Segue $k \neq 0$, já que $a \neq 0$, então $1 \leq |k|$. Assim, multiplicando $1 \leq |k|$ por $|b|$, obtemos que $|b| \leq |b| \cdot |k| = |a|$. □

A seguir mencionaremos algumas propriedades elementares da divisibilidade, as quais são de fáceis constatações. Por conveniência, não as demonstraremos aqui.

Teorema 3.2.3 *Dados $a, b, c, d \in \mathbb{Z}$, valem as propriedades:*

(1) *Os únicos divisores de* 1 *são* 1 *e* -1.

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

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

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

(5) *Se $a \mid b$ e $a \mid c$, então $a \mid (mb + nc)$, $\forall m, n \in \mathbb{Z}$.*

3.3 Divisão Euclidiana

Um dos fundamentos de muitos resultados da Teoria dos Números, e de estimada relevância neste trabalho, é certamente a Divisão Euclidiana. O resultado é bem conhecido nas séries iniciais de ensino, mesmo que lhe tenha sido apresentado de modo informal. Entre outras, é bastante eficiente no cálculo do máximo divisor comum de dois ou mais números inteiros como veremos mais adiante.

As primeiras introduções que abordam a divisão nas etapas iniciais de ensino sempre fazem referência a situações elementares, como dividir uma quantidade x de laranjas para y pessoas e como resultado obteríamos q laranjas para cada uma e r laranjas restantes. É uma abordagem elementar e, de certo ponto eficaz. De modo formal, temos a Divisão Euclidiana (está citada em *Os Elementos* de Euclides - 300 a.C), que é uma ferramenta extremamente importante e útil em muitas demonstrações de resultados não apenas da Teoria dos Números, como também de outras áreas da Matemática.

Teorema 3.3.1 (Divisão Euclidiana) *Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$, existem únicos $q, r \in \mathbb{Z}$ tais que*

$$a = b \cdot q + r, \quad com \quad 0 \leq r < |b|$$

Os inteiros q e r são chamados, respectivamente, de **quociente** e **resto** da divisão de a por b. Consequentemente, o resto da divisão de a por b é zero se, e somente se, b divide a, isto é,

$$r = 0 \;\Leftrightarrow\; b \mid a.$$

Na Divisão Euclidiana, ressaltamos os seguintes casos particulares:

- Se $a = 0$, então $q = r = 0$.
- Se $a > 0$ e $a < b$, então $q = 0$ e $r = a$.

Vejamos alguns exemplos.

Exemplo 3.3.2 Temos que $-14 = 3 \cdot (-5) + 1$, isto é, na divisão de -14 por 3 o quociente e o resto são respectivamente -5 e 1.

Exemplo 3.3.3 Determinar o quociente e o resto da Divisão Euclidiana de 14 por 3.

Solução: Inicialmente efetuamos a divisão de 14 por 3, pelo método da chave, como é feito e ensinado naturalmente nos séries iniciais de ensino. Assim, basta manipular o resultado adequadamente e podemos escrever

$$14 = 3 \cdot 4 + 2.$$

Logo, o quociente e o resto são, respectivamente, 4 e 2. △

Note que podemos ter $a = b \cdot q + r$, porém q e r não são necessariamente quociente e resto da Divisão Euclidiana.

Exemplo 3.3.4 Temos que $20 = 2 \cdot 5 + 10$, no entanto 5 e 10 não são, respectivamente, quociente e resto da Divisão Euclidiana.

Como uma primeira aplicação da Divisão Euclidiana, notemos que se a é um inteiro qualquer, então ao efetuar sua divisão por $b = 2$, temos que os possíveis restos são $r = 0$ ou $r = 1$, ou seja,

$$a = 2q + r, \quad \text{com} \quad 0 \leq r < 2.$$

Quando $r = 0$, segue que a é da forma $a = 2q$. Um inteiro assim é chamado de **número par**. Em particular, acordamos que zero é um número par. Se $r = 1$, então $a = 2q + 1$. Qualquer inteiro desta forma é chamado de **número ímpar**.

Por exemplo, os números 4 e -14 são pares, pois

$$4 = 2 \cdot 2 \quad \text{e} \quad -14 = 2 \cdot (-7),$$

enquanto 9 e -25 são ímpares, desde que

$$9 = 2 \cdot 4 + 1 \quad \text{e} \quad -25 = 2(-13) + 1.$$

Dizemos que a e b têm a **mesma paridade** quando a e b são ambos pares ou ambos ímpares.

Se P e I denotam os conjuntos dos números pares e ímpares, respectivamente, então

$$P = \{2k : k \in \mathbb{Z}\} \quad \text{e} \quad I = \{2k+1 : k \in \mathbb{Z}\}.$$

É imediato verificar que:

(1) $P \cap I = \emptyset$.

(2) Se $x, y \in P$, então $x \pm y \in P \quad \text{e} \quad x \cdot y \in P$.

(3) Se $x, y \in I$, então $x \pm y \in P \quad \text{e} \quad x \cdot y \in I$.

(4) Se $x \in P$ e $y \in I$, então $x \pm y \in I \quad \text{e} \quad x \cdot y \in P$.

No exemplo que segue consideramos algumas aplicações elementares do Algoritmo da Divisão.

Lembremos que um inteiro a é um **quadrado perfeito** quando $a = q^2$, para algum inteiro q.

Exemplo 3.3.5 Mostrar que:

a) *Todo quadrado perfeito é da forma* $4k$ *ou* $4k+1$.

b) *Todo inteiro ímpar é da forma* $4k+1$ *ou* $4k+3$.

c) *O quadrado de todo inteiro ímpar é da forma* $8k+1$.

Solução: a) Se $a = 2q$, então $a^2 = 4q^2 = 4k$, com $k = q^2$; e se $a = 2q+1$, então $a^2 = 4(q^2+q)+1 = 4k+1$, em que $k = q^2+q$.

b) Dado um número inteiro a, temos pelo Algoritmo da Divisão que

$$a = 4q + r, \quad \text{com} \quad 0 \leq r < 4,$$

ou seja, a pode assumir as seguintes formas: $4q$, $4q+1$, $4q+2$ ou $4q+3$. Logo, se a é ímpar, então pelas considerações anteriores, concluímos que $a = 4q+1$ ou $4q+3$.

c) Sendo a ímpar, segue do item b) que $a = 4q+1$ ou $4q+3$. Se $a = 4q+1$, então

$$a^2 = 8(2q^2+q)+1 = 8k+1,$$

com $k = 2q^2+q$. Se $a = 4q+3$,

$$a^2 = 8(2q^2+3q+1)+1 = 8k+1,$$

em que $k = 2q^2+3q+1$. $\triangle$

3.4 Máximo Divisor Comum

O conceito de *Máximo Divisor Comum* (mdc) está relacionado a resultados essenciais em questões da Teoria dos Números e em particular a sistemas criptográficos considerados, especialmente, os estudados mais adiante. Neste trabalho, sua importância e utilidade estão bem além das aplicações elementares na resolução de problemas abordados no Ensino Básico.

No Ensino Fundamental, quando do estudo de mdc, é comum considerar dois números naturais relativamente pequenos, determinar seus divisores positivos, identificar os divisores comuns e verificar o maior entre eles. Há também na maioria dos livros adotados nesse nível de ensino um método prático que consiste na fatoração simultânea desses números através de divisões sucessivas por números primos, e considerando apenas os fatores primos comuns nesse processo, o resultado segue do produto destes. Por exemplo,

20, 32	2
10, 16	2
5, 8	2
5, 4	2
5, 2	2
5, 1	5
1, 1	

De modo que considerando o produto dos fatores comuns, temos que o máximo divisor comum de 20 e 32 é 4

Numa linguagem mais técnica, baseia-se no seguinte: Tomemos a e b números inteiros, não ambos nulos, e consideremos

$$D_a = \{n \in \mathbb{N} : n \mid a\} \quad \text{e} \quad D_b = \{n \in \mathbb{N} : n \mid b\},$$

em que $\mathbb{N}$ indica o conjunto dos inteiros positivos, também chamados os **números naturais**. É claro que $D_a \cap D_b \neq \emptyset$, pois $1 \mid a$ e $1 \mid b$. Além disso, $D_a \cap D_b$ é um conjunto finito e, por isso, possui maior elemento, o qual é chamado **máximo divisor comum** dos números a e b.

Notemos que se $a = b = 0$, então os conjuntos D_a e D_b são infinitos. É por isso que este caso não será considerado e convencionaremos que o máximo divisor comum entre eles é zero.

O que faremos aqui é essencialmente a mesma coisa, apenas com certo rigor e destacando propriedades relevantes relacionadas ao conteúdo que forma um dos pilares da aritmética de Euclides.

Dados $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$, o inteiro positivo d é o **máximo divisor comum** (mdc) de a e b, quando:

(a) $d \mid a$ e $d \mid b$.

(b) Se $c \in \mathbb{Z}$, é um divisor comum de a e b, então c é um divisor de d.

Em outras palavras, o máximo divisor comum de a e b é um inteiro positivo que os divide e é divisível por todo divisor comum de a e b. Indicaremos este número por

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

por familiaridade com a notação utilizada pela maioria dos livros didáticos do ensino básico, ou simplesmente $d = (a,b)$ por razão de praticidade. Notemos que:

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

Em alguns casos particulares, é imediato calcular o mdc. Por exemplo, se a é um número inteiro não nulo, temos claramente que:

(1) $mdc(a,0) = |a|$.

(2) $mdc(a,1) = 1$.

(3) $mdc(a,a) = |a|$.

Além disso, para todo $b \in \mathbb{Z}$, temos que a divide b se, e somente se, $|a|$ é o mdc entre a e b, ou seja,

$$a \mid b \;\Leftrightarrow\; mdc(a,b) = |a|.$$

Também, é imediato verificar que:

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

Assim, vamos assumir que a e b são sempre positivos.

O próximo teorema é fundamental para resoluções de muitos problemas na Teoria dos Números, em particular ao método RSA de criptografia, pois nos dá uma importante identidade que relaciona os números a e b e seu mdc. Esta identidade é conhecida como identidade de **Bachet-Bézout**.

Teorema 3.4.1 (Identidade de Bachet - Bézout) *Se $d = mdc(a,b)$, então existem inteiros x e y tais que*

$$d = ax + by.$$

□

O cálculo do $mdc(a,b)$, quando a e b são números consideravelmente grandes, é bastante tedioso e impraticável, pelo método citado no início desta seção. Por exemplo, quanto vale $mdc(3072, 4480)$?

Neste sentido, descreveremos posteriormente o Algoritmo de Euclides que consiste em um processo muito eficaz para cálculo do mdc de quaisquer que sejam os inteiros a e b, diferentemente dos métodos utilizados no ensino básico. Tal resultado fundamenta-se no seguinte lema:

Lema 3.4.2 (Euclides) *Se $a = bq + r$, então $mdc(a,b) = mdc(b,r)$.*

Demonstração: Sejam D_a e D_b o conjunto dos divisores inteiros positivos de a e b, respectivamente. É suficiente mostrar que $D_a \cap D_b = D_b \cap D_r$, pois se estes conjuntos são iguais, seus máximos também serão. Se $d \in D_a \cap D_b$, então $d \mid a$ e $d \mid b$; mas como $r = a - bq$, segue que $d \mid r$, ou seja, $d \in D_b \cap D_r$. Por outro lado, se $d \in D_b \cap D_r$, então $d \mid b$ e $d \mid r$, de modo que $d \mid bq + r = a$, isto é, $d \in D_a \cap D_b$. Logo, $D_a \cap D_b = D_b \cap D_r$ e, portanto, $mdc(a,b) = mdc(b,r)$. □

É importante destacar que o resultado do lema anterior é válido mesmo que r não seja o resto da divisão de a por b.

A aplicação repetida do lema acima consiste no *Algoritmo de Euclides (Algoritmo da Divisão)* que cessa ao chegarmos ao resto zero no processo de divisões sucessivas e, consequentemente, o último resto não nulo é o mdc de a e b.

Exemplo 3.4.3 Calcular $mdc(342,276)$.

Solução: Aplicando divisões sucessivas, temos:

$$\begin{aligned} 342 &= 276 \cdot 1 + 66, \\ 276 &= 66 \cdot 4 + 12, \\ 66 &= 12 \cdot 5 + 6, \\ 12 &= 6 \cdot 2 + 0. \end{aligned} \tag{3.1}$$

Logo,

$$mdc(342,276) = mdc(276,66) = mdc(66,12) = mdc(12,6) = 6.$$

△

Exemplo 3.4.4 Escrever o resultado do exemplo anterior na forma do Teorema 3.4.1.

Solução: Devemos encontrar x_0 e y_0 tais que $6 = 342 \cdot x_0 + 276 \cdot y_0$. Isso consistirá em isolar os restos não nulos das divisões de baixo para cima das igualdades em (3.1), substituindo-os sucessivamente. Temos,

$$\begin{aligned} 6 = 66 - 5 \cdot 12 &= 66 - 5 \cdot (276 - 4 \cdot 66) \\ &= 21 \cdot 66 - 5 \cdot 276 \\ &= 21 \cdot (342 - 276) - 5 \cdot 276 \\ &= 342 \cdot 21 + 276 \cdot (-26). \end{aligned}$$

Portanto,

$$6 = 342 \cdot 21 + 276 \cdot (-26).$$

Por conseguinte, temos que $x_0 = 21$ e $y_0 = -26$. $\triangle$

Dois inteiros a e b são ditos **primos entre si** ou **relativamente primos** quando $mdc(a,b) = 1$.

Por exemplo, 8 e 5 são primos entre si, pois $mdc(8,5) = 1$; Já 20 e 8 não são, uma vez que $mdc(20,8) = 4$.

3.4.1 Propriedades do mdc

Apresentaremos algumas propriedades sobre Máximo Divisor Comum de dois números inteiros, fundamentais em relação a situações posteriores. Na verdade, trata-se de consequências diretas de resultados de teoremas relevantes da Teoria dos Números e devido à natureza desse trabalho não foi mostrado aqui. Trataremos tais propriedades como axiomas, ressaltando que suas demonstrações são elementares e facilmente encontradas em livros sobre o conteúdo. Na ocasião, recomendamos a leitura de Martinez [13] e Vieira [22].

São válidos os seguintes:

1. Se $a,b \in \mathbb{Z}^*$, então $mdc\left(\frac{a}{d},\frac{b}{d}\right) = 1$, com $d = mdc(a,b)$.

2. Dados $a,b,k \in \mathbb{Z}$, com $k > 0$, temos $mdc(ka,kb) = k \cdot mdc(a,b)$.

3.4.2 Máximo Divisor Comum de Mais de Dois Inteiros

Consideremos três números inteiros a, b e c. Escolhamos dois entre eles, digamos a e b, e seja $d_1 = mdc(a,b)$. É claro que qualquer divisor comum k de a, b e c divide, em particular, a e b. Portanto, este, necessariamente, deve dividir d_1. Sendo k um divisor comum de d_1 e c, temos que k divide $d_2 = mdc(d_1,c)$. Logo, d_2 dividindo d_1 e c, será ele próprio um divisor comum de a, b e c. Desse modo, d_2 não apenas os divide, mas qualquer divisor comum desses três números divide d_2. Por conseguinte, d_2 é o máximo divisor comum de a, b e c, em símbolos $d_2 = mdc(a,b,c)$, de modo que,

$$d_2 = mdc(d_1,c).$$

Generalizando, temos:

Dados inteiros $a_1,a_2,...,a_n$, não todos iguais a zero e seja $n \in \mathbb{Z}$, tal que $n \geq 2$, temos que

$$mdc(a_1,a_2,...,a_n) = mdc(a_1,a_2,...,mdc(a_{n-1},a_n)).$$

Exemplo 3.4.5 Determinar $mdc(342,276,142)$.

Solução: Inicialmente, temos que $mdc(342,276) = 6$, como foi calculado no Exemplo 3.4.3. Daí, segue que

$$142 = 23 \cdot 6 + 4 \;\Rightarrow\; mdc(142,6) = mdc(6,4) = 2.$$

Dessa forma,

$$mdc(342, 276, 142) = 2.$$

$\triangle$

3.5 Mínimo Múltiplo Comum

O conceito de *Mínimo Múltiplo Comum* (mmc) é um paralelo importante do conceito de mdc, e muito familiar ao estudantes de ensino fundamental e médio. A respeito de sua aplicação neste nível de ensino é comum existirem poucos e simples exemplos de situações práticas. Sua definição se assemelha com a definição de mdc. Vejamos.

Sejam a e b dois inteiros não nulos, e tomemos os conjuntos

$$M_a = \{n \in \mathbb{N}; a \mid n\} \quad \text{e} \quad M_b = \{n \in \mathbb{N}; b \mid n\}.$$

Primeiramente, notemos que $|ab| \in M_a$ e $|ab| \in M_b$, de modo que $|ab| \in M_a \cap M_b$. Assim, o conjunto $M_a \cap M_b$ possui menor elemento, chamado de *Mínimo Múltiplo Comum* de a e b, que será indicado por $mmc(a,b)$ ou simplesmente por $[a,b]$.

Resumidamente, temos:

Dados $a, b \in \mathbb{Z}$, com $a \neq 0$ e $b \neq 0$, o inteiro positivo m é o **mínimo múltiplo comum** de a e b, quando:

(a) $a \mid m$ e $b \mid m$;

(b) Se $c \in \mathbb{Z}$ é um múltiplo comum de a e b, então m é um divisor de c.

Por exemplo,

$$mmc(2,7) = 14, \quad mmc(6,9) = 18 \quad \text{e} \quad mmc(6,-9) = 18.$$

É possível mostrar sem muitas dificuldades que, para quaisquer $a, b \in \mathbb{Z}^*$,

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

Por isso, para o cálculo do mmc, consideremos sempre $a > 0$ e $b > 0$.

O próximo teorema estabelece uma relação muito proveitosa entre o máximo divisor comum e o mínimo múltiplo comum de dois números inteiros. Além do mais é bastante prático no cálculo do mmc, diferentemente dos métodos conhecidos pela maioria dos alunos do ensino básico que por sua vez utiliza fatoração.

Teorema 3.5.1 *Para quaisquer $a, b \in \mathbb{Z}^*$, como $d = mdc(a,b)$ e $m = mmc(a,b)$, temos que*

$$m = \frac{|ab|}{d}.$$

Demonstração: Consideremos $m_1 = \frac{|ab|}{d}$ e provemos que $m = m_1$. Como $d \mid a$ e $d \mid b$, então $a = d\lambda_1$ e $b = d\lambda_2$, com $\lambda_1, \lambda_2 \in \mathbb{N}$. Assim,

$$m_1 = \frac{|ab|}{d} = \frac{\lambda_1 db}{d} = \lambda_1 b \Rightarrow b \mid m_1.$$

Da mesma forma, provamos que $a \mid m_1$. Tomemos agora m_2 outro múltiplo comum de a e b, isto é, $m_2 = a\alpha_1$ e $m_2 = b\alpha_2$, com $\alpha_1, \alpha_2 \in \mathbb{N}$. Pela identidade de Bachet-Bézout, existem inteiros x e y tais que $d = ax + by$, o que assegura o resultado. Isso mostra que $m_1 = m = mmc(a,b)$ e que $m = \frac{|ab|}{d}$. □

Com efeito do teorema anterior, o cálculo de $d = mdc(a,b)$, realizado de modo prático através do Algoritmo de Euclides, implica diretamente na determinação de $m = mmc(a,b)$. Para tanto, basta dividir o produto ab por d.

Exemplo 3.5.2 Calcular o $mmc(342,276)$.

Solução: Pelo o Algoritmo da Divisão, temos que $mdc(342,276) = 6$. Portanto,

$$mmc(342,276) = \frac{342 \cdot 276}{6} = 15732$$

△

Uma consequência óbvia do teorema anterior é o seguinte:

Corolário 3.5.3 *Dados $a, b \in \mathbb{Z}^*$, temos que*

$$mmc(a,b) = ab \Leftrightarrow mdc(a,b) = 1.$$

Exemplo 3.5.4 Calcular o $mmc(8,5)$.

Solução: Pelo o Algoritmo da Divisão, temos que $mdc(8,5) = 1$. Portanto,

$$mmc(8,5) = 8 \cdot 5 = 40$$

△

3.5.1 Mínimo Múltiplo Comum de Mais de Dois Inteiros

Igualmente como foi feito para o máximo divisor comum de mais de dois inteiros, vamos considerar algo similar para o mínimo múltiplo comum.

Consideremos a, b e c inteiros positivos e seja M_a, M_b e M_c o conjunto dos múltiplos de a, b e c, respectivamente. Analogamente, ao mdc a definição seguinte tem por base o fato de o conjunto $M_a \cap M_b \cap M_c$ possuir menor elemento, chamado *mínimo múltiplo comum* de a, b e c, denotado por $mmc(a,b,c)$, e por consequência generaliza tal fato.

Dados inteiros $a_1, a_2, ..., a_n$, todos diferentes de zero, e seja $n \in \mathbb{Z}$, tal que $n \geq 2$, temos que

$$mmc(a_1, a_2, ..., a_n) = mmc(a_1, a_2, ..., mmc(a_{n-1}, a_n))$$

Exemplo 3.5.5 Calcular $mmc(36,22,14,6)$.

Solução: Temos que:

$$\begin{aligned} mmc(6,14,22,36) &= mmc(36,22,mmc(14,6)) \\ &= mmc(36,mmc(22,42)) \\ &= mmc(36,462) \\ &= 2772 \end{aligned}$$

Portanto, $mmc(6,14,22,36) = 2772$. $\triangle$

Capítulo 4

Números Primos

A maioria dos resultados sofisticados da Teoria dos Números deve-se aos estudos realizados sobre os números primos. Por essa razão, esses números conquistaram uma posição de destaque na matemática. Além disso, trata-se de um tema geralmente desenvolvido no ensino básico sem muitos méritos e com poucas aplicabilidades práticas apresentadas.

Como observado na abordagem histórica, a dificuldade de decomposição de um número em fatores primos garantia confiabilidade na cifra RSA. Para isso, reservamos neste capítulo um tratamento especial aos números primos e a outros conceitos correlacionados de elevada importância, no sentido de considerá-los primordiais no desenvolvimento criptográfico.

4.1 Teorema Fundamental da Aritmética

O Teorema Fundamental da Aritmética (TFA) assegura que todo inteiro $a \in \mathbb{Z} - \{0, \pm 1\}$ pode ser escrito como produto finito de primos. Em outras palavras, os primos são suficientes para gerar todos os inteiros diferentes de 0 e ± 1. Isso mostra a importância desses números na Teoria dos Números e em particular na Criptografia.

Os números primos, com relação à divisibilidade, são os mais simples, conforme a seguinte:

Um número $p \in \mathbb{Z} - \{0, \pm 1\}$ é **primo** quando seus únicos divisores positivos são 1 ou $|p|$. Caso contrário, dizemos que p é **composto**.

Por exemplo, os números 2, -3, 5 e 13 são primos, enquanto $6 = 2 \cdot 3$, $15 = 3 \cdot 5$ e $18 = 2 \cdot 9$ são compostos.

Notemos que o número 2 é o único primo par. O número 1 não é primo nem composto, igualmente como convenciona os livros didáticos do ensino fundamental a exemplo de Andrini [1].

Como p é primo se, e somente se, $-p$ é primo, vamos considerar apenas primos positivos, e o conjunto desses primos indicaremos por $\mathscr{P}$, ou seja,

$$\mathscr{P} = \{2, 3, 5, 7, 11, 13, 17, ...\}$$

Observamos que um número composto $a \in \mathbb{N}$ pode ser escrito na forma

$$a = b \cdot c, \quad \text{com} \quad 1 < b, c < a.$$

Neste caso, os números b e c são chamados **divisores próprios** de a.

Se a é um número composto e a divide o produto bc, então não necessariamente $a \mid b$ ou $a \mid c$. Por exemplo, $6 \mid 3 \cdot 4$, mas $6 \nmid 3$ e $6 \nmid 4$. O mesmo não ocorre se a é um número primo. De fato,

Proposição 4.1.1 *Sejam a e b inteiros, e p um número primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração: Como p é primo, então $mdc(a,p) = 1$ ou $mdc(a,p) = p$. Assim, se $p \nmid a$, então $mdc(a,p) = 1$. Portanto, do item 5 das Propriedades do mdc (Lema de Euclides), segue que $p \mid b$. □

O resultado anterior pode ser estendido para um produto de n inteiros como veremos a seguir. Sua demonstração é facilmente desenvolvida usando indução sobre n.

Corolário 4.1.2 *Se p é primo e $p \mid a_1 a_2 ... a_n$, então $p \mid a_i$ para algum $i = 1, 2, ..., n$.* □

O próximo teorema corresponde ao resultado central dessa seção. A sua prova não será mostrada aqui, por envolver conceitos relativamente avançados com relação aos propósitos deste trabalho. Aos interessados em sua demonstração sugerimos a leitura do livro *Álgebra Abstrata para Licenciatura* [22].

Teorema 4.1.3 (Teorema Fundamental da Aritmética - TFA) *Todo inteiro $a > 1$ ou é primo ou se escreve de maneira única (a menos da ordem dos fatores) como um produto de fatores primos.* □

Observa-se que a fatoração de $a > 1$ implica diretamente na fatoração de $-a$. Além disso, como os primos que surgem na fatoração de um dado número inteiro $a > 1$ não são necessariamente distintos, podemos agrupar os primos iguais e ordená-los para obter o seguinte corolário.

Corolário 4.1.4 *Todo número inteiro $a > 1$ pode ser escrito de forma única, a menos da ordem dos fatores, na forma*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}, \tag{4.1}$$

em que $p_1 < p_2 < \cdots < p_n$ são números primos e $\alpha_i \in \mathbb{N}$ para cada $i = 1, 2, ..., n$. □

Exemplo 4.1.5 A fatoração dos números 23100 e 70560, de acordo com a definição acima, é apresentada da seguinte forma:

$$23100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11$$

e

$$70560 = 2^5 \cdot 3^2 \cdot 5 \cdot 7^2.$$

△

A representação de um número inteiro $a > 1$ dada em (4.1) é sua **fatoração** ou **decomposição canônica** em fatores primos.

4.2 Fatoração de Fermat

Sobre fatoração de um determinado inteiro em números primos, entendemos que consiste em um processo bastante árduo. Do ponto de vista computacional, a decomposição em fatores primos para inteiros relativamente grandes continua sem solução satisfatória, apesar dos grandes esforços tecnológicos empreendidos no desenvolvimento de computadores quânticos capazes de acelerar tal processo.

Nesta seção apresentaremos um método de fatoração devido a Fermat[1], que descreveremos a seguir. Mais detalhes sobre esse importante método de fatoração consulte S. C. Coutinho [4].

Se $a \in \mathbb{N}$ é um número composto, então podemos representá-lo na forma

$$a = 2^r \cdot b,$$

sendo b um número inteiro ímpar e $r \in \mathbb{N} \cup \{0\}$. Se b é um número primo, então a decomposição de a em fatores primos é $a = 2^r \cdot b$. Caso contrário, podemos proceder da seguinte maneira:

Passo 1: Seja $m = [\sqrt{b}]$ (o maior inteiro menor ou igual a $\sqrt{b}$).

Passo 2: Se $m^2 - b = n^2$, então $b = (m-n)(m+n)$.

Passo 3: Se $m^2 - b \neq n^2$, então adicione 1 a m e volte ao passo 2.

Exemplo 4.2.1 Usando o método de fatoração de Fermat, obter a decomposição em potências de primos do número $a = 6292$.

[1] *Pierre de Fermat* (1601-1665), matemático francês que contribuiu consideravelmente ao desenvolvimento da Teoria dos Números. Pela maior parte de sua vida, foi advogado e oficial do governo em Toulouse e tinha a matemática como passatempo. Dentre suas mais marcantes contribuições destaca-se o Último Teorema de Fermat, uma afirmação que demorou mais de 350 anos para ser demonstrada. Sobre Fermat recomendamos a leitura de *Elementos de Aritmética* de Abramo Hefez [12] ou ainda acesse: *www.somatematica.com.br.*

Solução: Inicialmente, notemos que o número a não é primo, pois $2 \mid a$. Além disso, $a = 2^2 \cdot 1573$, de modo que $r = 2$ e $b = 1573$. Assim, vamos encontrar apenas um fator primo de 1573, pois os outros, se existirem, são obtidos de forma similar. Considerando $m = [\sqrt{1573}] = 39$, temos

$$m^2 - b = 39^2 - 1573 = -52 \neq n^2.$$

Somando 1 a 39,

$$(m+1)^2 - b = 40^2 - 1573 = 27 \neq n^2.$$

Somando 1 a 40,

$$41^2 - b = 41^2 - 1573 = 108 \neq n^2.$$

Continuando este processo, somando 1 a 66, (pois antes de 66 não encontramos nenhum quadrado perfeito), obtemos:

$$67^2 - b = 67^2 - 1573 = 2916 = 54^2.$$

Desse modo,

$$\begin{aligned} 1573 &= 67^2 - 54^2 = (67+54)(67-54) \\ &= 11^2 \cdot 13 \end{aligned}$$

e, consequentemente,

$$a = 2^2 \cdot 11^2 \cdot 13.$$

Note que ao determinarmos o fator primo $p = 11$, este resultou diretamente na obtenção do fator primo $q = 13$. Tal fato é devido ao número 1573 ser relativamente pequeno. No entanto, caso isso não ocorra, o processo é repetido até que se obtenha todos os fatores primos de a. △

Com relação à eficiência prática da Fatoração de Fermat, podemos notar que este método perde eficácia quando a diferença (em módulo) entre os divisores iniciais de a é relativamente grande. Quando isso ocorre, necessita realizar mais alguns passos para estabelecer a fatoração completa de a. No exemplo anterior, foram necessários 27 passos para estabelecer $a = 2^2 \cdot 11^2 \cdot 13$, pois a diferença entre os divisores iniciais $c = 121$ e $d = 13$ é $c - d = 108$.

4.3 O Crivo de Eratóstenes

Sobre as várias interrogações que ainda rodeiam a Teoria dos Números, saber se um dado número inteiro é primo ou composto, é um de seus principais desafios. Nesta direção, ressaltamos um método clássico, o Teste de Primalidade dado no Teorema 4.3.1, que nos conduz a um algoritmo chamado de *Crivo de Eratóstenes*. Este algoritmo consiste em determinar números primos até uma ordem designada, elaborado pelo matemático grego

Eratóstenes[2]. Apesar de prático é inconveniente para primos relativamente grandes. Para maiores detalhes referenciamos *Números Inteiros e Criptografia RSA* de S. C. Coutinho [4].

O Teste de Primalidade e o Crivo de Eratóstenes são abordados no ensino fundamental, porém, com menos sutileza. Sobre o Teste de Primalidade, geralmente é instruído fazer divisões do número a ser verificado pela menor sequência crescente de primos positivos, isto é,

$$2,3,5,7,\ldots,$$

e caso nenhuma divisão for exata e o quociente obtido seja menor ou igual ao divisor primo, o processo cessa e garantimos que o número é primo. Caso alguma divisão for exata, o número é dito composto. Com relação ao Crivo é apresentado um exemplo para um caso particular de determinado número, não generalizando o processo para todo inteiro $n > 1$. Como podemos observar em Álvaro Andrini [1].

Teorema 4.3.1 *Se n um inteiro positivo composto, então n possui, necessariamente, um fator primo p, tal que $p \leq \sqrt{n}$. Ou seja, se n não possui divisores diferentes de 1, menores ou iguais a $\sqrt{n}$, então n é primo.*

Demonstração: Sendo n um inteiro composto, então

$$n = a \cdot b, \quad \text{com} \quad 1 < a, b < n.$$

Se $a > \sqrt{n}$ e $b > \sqrt{n}$, então

$$n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n,$$

o que é impossível. Portanto, $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$, digamos que $1 < a \leq \sqrt{n}$. Pelo Teorema 4.1.3, existe um primo p tal que $p \mid a$ ($p \leq a \leq \sqrt{n}$) e, por conseguinte, $p \mid n$. □

Dessa forma, o Teorema 4.3.1, também creditado a *Eratóstenes*, mostra que para verificar se um dado inteiro $n > 1$ é primo, é suficiente verificar sua divisibilidade pelos primos $p \leq \sqrt{n}$. No entanto, o Teste de primalidade torna-se inviável na prática, quando aumentamos os valores de n consideravelmente. Até mesmo do ponto de vista computacional, ainda não existe um algoritmo sobre primalidade que seja eficaz.

Exemplo 4.3.2 Para o número $n = 193$, temos que $\sqrt{193} \leq 13$ e os primos menores ou iguais a 10 são $2,3,5,7,11$ e 13. Como nenhum destes primos divide n, concluímos que n é primo. △

[2] *Eratóstenes* (276 a.C. - 196 a.C.) foi um matemático grego que mostrava interesse em diversos assuntos. Porém, Astronomia e Matemática eram seus prediletos. Dentre as diversas áreas as quais escreveu, destacamos sua enorme contribuição aos Números Primos. Era mal conceituado pelos seus contemporâneos, apesar de contraditório, pois consideravam que não apresentava perfeição em nenhum dos ramos de conhecimento. Mais detalhes, indicamos a leitura de *Números Inteiros e Criptografia RSA* de S. C. Coutinho [4] ou ainda acesse: *www.somatematica.com.br.*

	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~~

Tabela 4.1: Crivo de Eratóstenes - Números Primos entre 2 e 50.

Resumidamente, o método de Eratóstenes fundamenta-se em construir uma tabela e excluir todos os números compostos menores que um dado número inteiro $n > 1$, de forma sistemática. Assim, deve-se:

(1) Escrever todos os números inteiros entre 2 e n.

(2) Para todo primo $p \leq n$, risca-se todos os múltiplos de p maiores do que p.

(3) Os números restantes são todos os primos menores que n.

Observação 4.3.3 O Teorema 4.3.1 diminui o número de verificações dos múltiplos de primos no passo (2) do algoritmo descrito acima.

Vejamos, por exemplo, como determinar todos os primos menores que 50, utilizando o Crivo de Eratóstenes. Faremos tal procedimento inspirado por Bonjorno [2].

Inicialmente, escrevemos todos os números inteiros entre 2 e 50. Em seguida excluímos todos os múltiplos de 2, 3, 5 e 7 pois estes são os primos menores ou iguais a $\sqrt{50}$. Como mostra a Tabela 4.1.

Logo, os primos entre 2 e 50 são todos aqueles que não foram descartados pelo processo realizado, ou seja,

$$2,3,5,7,11,13,17,19,23,29,31,37,41,43,47.$$

4.4 Números de Fermat e de Mersenne

Nesta seção, apresentaremos dois tipos de números primos especiais. Inicialmente, veremos os famosos *Números de Fermat*, em homenagem a Pierre de Fermat. Em seguida, estudaremos os *Números de Mersenne*, que também se revelam fascinantes em razão de suas curiosidades. Para maiores detalhes sobre os dados apresentados nesta seção podemos consultar as obras: *Elementos de Aritmética* [12] e *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro* [13].

Todo número da forma $F_n = 2^{2^n} + 1$, com $n \geq 0$, é um número de Fermat. E os primos desta forma são chamados **primos de Fermat**.

Para $n = 0,1,2,3,4$, temos, respectivamente, os seguintes números primos:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257 \quad \text{e} \quad F_4 = 65537.$$

Por isso, Fermat conjecturou que todos os números da forma $2^{2^n}+1$ eram primos. Mas, em 1732, Leonhard Euler mostrou que F_5 é composto, notando que

$$F_5 = 641 \cdot 6700417,$$

contrariando a afirmação de Fermat. Até o momento não se conhece outro primo de Fermat para $n > 5$ e portanto segue como uma de tantas conjecturas envolvendo primos.

Todo número da forma $M_n = 2^n - 1$, com $n \geq 1$, é um número de Mersenne. Os números primos da forma $2^n - 1$ são chamados **primos de Mersenne**.

O GIMPS (Grande busca pelo primo de Mersenne na internet) é um concurso que ocorre desde 1996 com o objetivo de encontrar novos primos na forma $2^n - 1$, isto é, um primo de Mersenne. Recentemente, em janeiro de 2013, foi descoberto $40^{\underline{o}}$ primo de Mersenne, o primo $2^{57885161} - 1$, com mais de 17 milhões de dígitos. O sistema faz uso de uma rede compartilhada de computadores de usuários que buscam por novos primos de Mersenne. Os interessados em ser um membro GIMPS podem acessar *www.mersenne.org*. É gratuito.

Exemplo 4.4.1 Mostrar que F_n não é um quadrado perfeito.

Solução: É claro que $F_0 = 3$ não é quadrado perfeito. Consideremos $n \geq 1$ e suponhamos por absurdo que $F_n = a^2$ para algum $a \in \mathbb{N}$, isto é,

$$2^{2^n} + 1 = a^2.$$

Se a é par, digamos $a = 2k$, então

$$2^{2^n} + 1 = 4k^2,$$

o que é impossível, pois 2 não divide 1. O caso a ímpar exige um pouco mais de análise. Se $a = 2k+1$, então da igualdade $2^{2^n} + 1 = a^2$ obtemos que

$$2^{2^n} = 2^2 \cdot 2^{2^n - 2} = 4(k^2 + k),$$

ou melhor,

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

Como k ou $k+1$ é ímpar, $k(k+1)$ é divisível por um ímpar, o que não é possível, pois 2^{2^n-2} só é divisível por potências de 2. Assim, F_n não é quadrado perfeito. $\triangle$

Os primeiros 15 números de Mersenne são:

$$M_1 = 1, \quad M_2 = 3, \quad M_3 = 7, \quad M_4 = 15, \quad M_5 = 31,$$

$$M_6 = 63, \quad M_7 = 127, \quad M_8 = 255, \quad M_9 = 511, \quad M_{10} = 1023,$$

$$M_{11} = 2047, \quad M_{12} = 4095, \quad M_{13} = 8191, \quad M_{14} = 16383, \quad M_{15} = 32767.$$

O fato é que M_p só pode ser primo se p for primo. Mersenne afirmou (de forma equivocada) que M_p é primo para o seguintes valores de p:

$$2,3,5,7,13,17,19,31,67,127,257,$$

e composto para os outros primos $p < 257$. Para muitos matemáticos da época, estava claro que Mersenne não havia testado a primalidade de todos os números por ele anunciado.

A afirmação de Mersenne continha erros, desde que ele colocou em sua lista de primos os números M_{67} e M_{257} que são compostos, e excluiu dela os números M_{61}, M_{89} e M_{107} que comprovadamente são primos. Após muito tempo, no ano de 1947, a lista dos primos de Mersenne M_p, com $p \leq 252$, foi estabelecida e é composta pelos primos

$$2,3,5,7,13,17,19,31,61,89,107,127.$$

Hoje em dia, com o uso de computadores, foram descobertos mais primos de Mersenne. Mais precisamente, até o presente, foram encontrados 36 números primos além dos supracitados, para os quais M_p é primo. A lista atual se completa com os seguintes primos:

$$521,607,1279,2203,2281,3217,4253,4423,9689,9941,11213,19937,21701,$$

$$23209,44497,86243,110503,132049,216091,756839,859433,1257787$$

$$1398269,2976221,3021377,6972593,13466917,20996011,24036583,$$

$$25964951,30402457,32582657,37156667,42643801,43112609,57885161.$$

Os primos de Mersenne estão entre os maiores primos conhecidos. No site

`http://primes.utm.edu/largest.html`

o leitor pode acompanhar a lista atual dos maiores primos já descobertos.

4.5 Primos, um fascínio da matemática

Os números primos tem sido objeto de estudo há mais de 2000 anos e recebe este nome devido aos gregos, seus precursores, que os chamavam de **primeiros**, traduzindo em latim *primus*. Até os dias atuais, os primos ainda despertam grande interesse dos teóricos dos números, com seus resultados ainda obscuros, principalmente relativos ao seu comportamento, exigindo técnicas mais sofisticadas sobre o assunto.

Os fascinantes números primos desempenham um papel fundamental na vida cotidiana. A segurança nas operações bancárias e comerciais via internet dependem inteiramente do uso de números primos. Na criptografia, especialmente, os primos com números de dígitos relativamente grandes são essenciais no desenvolvimento de todo processo.

Nesse sentido, a infinidade dos números primos apresentada a seguir é claramente um resultado de suma importância. Por outro lado, ainda há barreiras de natureza tecnológica na busca de métodos eficazes de gerar primos, apesar do avanço tecnológico computacional inexoravelmente crescente. Porém, já se dispõe de *softwares* capazes de desenvolverem algoritmos que têm auxiliados em muito a busca de novos primos, por exemplo, o programa de computador *MAPLE*. Com o auxílio deste e de outros programas, já foram descobertos bilhões de números primos.Como refere o livro *Criptografia para Iniciantes* [19].

Nesta seção destacaremos apenas um resultado muito significativo sobre distribuição dos números primos, apesar da enorme quantidade existente, consideradas de encontro aos propósitos deste trabalho.

4.5.1 A Infinidade dos Primos

A prova dada por Euclides (cerca de 300 a.C.) em seu livro *Os Elementos* sobre a infinidade dos números primos é um marco em toda matemática. De acordo com relatos históricos, sua demonstração foi a primeira a ser estabelecida utilizando o método de redução ao absurdo. Assim como em algumas ocasiões anteriores, este Teorema será anunciado sem demonstração, apesar de acharmos considerável sua prova. Ao leitor interessado em sua prova sugerimos a referência *Elementos de Aritmética* [12].

Teorema 4.5.1 (Euclides) *O conjunto $\mathscr{P}$ dos números primos é infinito.*

Demonstração: Suponhamos por absurdo que $\mathscr{P}$ é um conjunto finito, e sejam $p_1, p_2, \ldots, p_n$ todos os primos. Consideremos $a \in \mathbb{N}$ dado pelo produto dos p_i's somado ao número 1, isto é,

$$a = p_1 p_2 \cdots p_n + 1.$$

Como $a > 1$, então existe um primo p que divide a. Como por hipótese $p_1, p_2, \ldots, p_n$ são os únicos primos, então $p = p_i$ para algum $i = 1, \ldots, n$, digamos que $p = p_1$. Assim, $p \mid (pp_2 \cdots p_n + 1)$, ou seja, $p \mid 1$, o que é uma contradição. Assim, $\mathscr{P}$ é infinito. □

Determinar um número primo com uma grande quantidade de dígitos é tarefa árdua mesmo com recurso computacional avançado. No entanto, saber que há uma infinidade de primos motiva brilhantes estudiosos da Teoria dos Números em suas pesquisas sobre distribuição de primos, contribuindo diretamente com o desenvolvimento criptográfico, em particular ao sistema RSA.

Capítulo 5

Congruências

O conceito de congruência está ligado a importantes resultados da Teoria dos Números. A Aritmética Modular é a ferramenta que discute sobre a Teoria das Congruências, fundamentada por meio das propriedades da divisibilidade através da aritmética dos restos.

O extraordinário Gauss, em sua admirável obra *Disquisitiones Arithmeticae* (Investigações Aritméticas) de 1801, com apenas 24 anos de idade, introduziu os conceitos e notações de congruências, utilizados até os dias atuais.

Na Aritmética Modular, os idealizadores da Criptografia de Chave Pública encontrou a função de mão única fundamental para concretizar seus ideais. Nessa direção, apresentaremos apenas tópicos essenciais de efeito direto nos métodos criptográficos que serão estudados adiante. Assim, alguns resultados não serão demonstrados, pois são muito complexos para serem discutidos, apesar de considerarmos relevantes às aplicações criptográficas.

Para maiores detalhes sobre o assunto consulte *Criptografia para Iniciantes [19], Números Inteiros e Criptografia RSA [4], Elementos de Aritmética [12] e Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro [13].*

5.1 Propriedades Básicas das Congruências

Antes de aprofundarmos sobre as congruências, esclarecemos que não se trata de um conteúdo muito distante da maioria dos estudantes em nível básico. Na verdade, existem muitos fatos apresentados em determinados conteúdos curriculares que nos interessam somente o resto euclidiano, principalmente em questões relacionadas a fatos periódicos. Além do mais, as Olimpíadas Brasileira de Matemática das Escolas Públicas (OBMEP) têm abordado várias questões relacionadas à aritmética dos restos. Como iremos constatar essa relação no desenvolvimento desta seção e das posteriores.

Sejam $m > 1$ um número inteiro e a e b inteiros quaisquer. Dizemos que a é **congruente** a b módulo m quando m divide $a - b$. O número m é chamado **módulo** da congruência.

Para representar simbolicamente que a é congruente a b módulo m, escrevemos

$$a \equiv b \pmod{m}.$$

Por exemplo,

$$7 \equiv 1 \pmod{3}, \quad 12 \equiv -3 \pmod{5}, \quad -8 \equiv 4 \pmod{2},$$

pois, $3 \mid (7-1),\ 5 \mid (12+3)$ e $2 \mid (-8-4)$.

Se $m \nmid a-b$, então dizemos que a **não é congruente** a b módulo m ou que a é **incongruente** a b módulo m. Neste caso, indicamos

$$a \not\equiv b \pmod{m}.$$

Assim, $8 \not\equiv 1 \pmod{3}$ e $15 \not\equiv 5 \pmod{7}$, pois $3 \nmid (8-1)$ e $7 \nmid (15-5)$.

O símbolo "$\equiv$ "para indicar a congruência foi estabelecido por Gauss em virtude da semelhança com a igualdade algébrica. De fato, $a \equiv b \pmod{m}$ garante que existe um inteiro k tal que

$$a = b + km.$$

O módulo $m = 1$ ou $m < 0$, também poderia ser considerado. Contudo, $a \equiv b \pmod{1}$ é verdadeiro para quaisquer inteiros a e b, de modo que $m = 1$ não desperta interesse. Por outro lado, como

$$m \mid a-b \quad \Leftrightarrow \quad -m \mid a-b,$$

então consideraremos apenas $m > 1$.

A partir daqui, em congruências módulo m, consideraremos m como sendo um inteiro maior que 1 salve menção contrária.

A noção de congruência também pode ser caracterizada de acordo com a proposição seguinte:

Proposição 5.1.1 *Dados a e b inteiros, temos que $a \equiv b \pmod{m}$ se, e somente se, a e b têm o mesmo resto euclidiano quando divididos por m.*

Demonstração: Se $a \equiv b \pmod{m}$, então $a = b + km$ para algum $k \in \mathbb{Z}$. Pela Divisão Euclidiana,

$$b = qm + r, \ \text{com} \ \ 0 \leq r < m.$$

Logo,

$$\begin{aligned} a &= b + km \\ &= qm + r + km \\ &= (q+k)m + r \end{aligned}$$

ou seja, r também é o resto da divisão de a por m. Reciprocamente, suponhamos que

$$a = q_1 m + r \ \text{ e } \ b = q_2 m + r,$$

onde $0 \leq r < m$. Daí, $a - q_1 m = b - q_2 m$, de maneira que

$$\begin{aligned} a - b &= q_1 m - q_2 m \\ &= (q_1 - q_2)m. \end{aligned}$$

Portanto, $m \mid a - b$, ou seja, $a \equiv b \pmod{m}$. □

Por exemplo, como $18 \equiv 6 \pmod{4}$, então 18 e 6 têm o mesmo resto quando divididos por 4. De fato, observa-se que

$$18 = 4 \cdot 4 + 2 \text{ e } 6 = 1 \cdot 4 + 2.$$

O conceito de congruência módulo m estabelece uma relação sobre o conjunto dos números inteiros, a *relação de congruência módulo m*, que indicaremos

$$\equiv \pmod{m} \quad \text{ou} \quad \equiv_m .$$

Essa relação tem muitas propriedades em comum com a relação de igualdade entre inteiros, conforme veremos a seguir.

Proposição 5.1.2 *Dados a, b e c inteiros quaisquer, temos que as seguintes propriedades são satisfeitas:*

(1) *($\equiv_m$ é reflexiva)* $a \equiv a \pmod{m}$ $\forall a \in \mathbb{Z}$;

(2) *($\equiv_m$ é simétrica) Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$;*

(3) *($\equiv_m$ é transitiva) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.*

Demonstração: (1) Para qualquer inteiro a, temos que $a - a = 0 = 0 \cdot m$, e consequentemente $a \equiv a \pmod{m}$.

(2) Se $a \equiv b \pmod{m}$, então $a - b = km$, com $k \in \mathbb{Z}$. Logo, $b - a = m(-k)$ e $-k \in \mathbb{Z}$, i.e., $m \mid b - a$. Portanto, $b \equiv a \pmod{m}$.

(3) Sejam $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, existem $k_1, k_2 \in \mathbb{Z}$ tais que

$$a - b = k_1 m \text{ e } b - c = k_2 m.$$

Adicionando membro a membro as igualdades acima, obtemos

$$a - c = (k_1 + k_2)m \Rightarrow a - c = k_3 m,$$

com $k_3 \in \mathbb{Z}$. Daí, $a \equiv c \pmod{m}$. □

Os resultados da proposição acima mostram que a *relação de congruência módulo m* é estreitamente familiar com a igualdade algébrica, além do mais é uma relação de equivalência sobre $\mathbb{Z}$.

O próximo teorema considera mais algumas importantes propriedades relacionadas à congruência.

Teorema 5.1.3 *Dados a, b, c e d inteiros quaisquer, temos que as propriedades seguintes são satisfeitas:*

(1) *Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então*

$$(a+c) \equiv (b+d) \pmod{m} \quad e \quad ac \equiv bd \pmod{m}.$$

(2) *Se $a \equiv b \pmod{m}$, então*

$$(a+c) \equiv (b+c) \pmod{m} \quad e \quad ac \equiv bc \pmod{m}.$$

(3) *Se $a \equiv b \pmod{m}$, então $a^k \equiv b^k \pmod{m}$ para qualquer número natural k.*

(4) *Se $(a+c) \equiv (b+c) \pmod{m}$, então $a \equiv b \pmod{m}$.*

A congruência pode ser vista como uma forma generalizada da igualdade, no sentido dos resultados do teorema anterior, com relação a soma e a multiplicação.

Veremos dois exemplos que mostra o uso das propriedades da congruência no auxílio efetivo de alguns cálculos.

Exemplo 5.1.4 Determinar o algarismo das unidades de 3^{1050}.

Solução: Devemos determinar um inteiro r tal que

$$3^{1050} \equiv r \pmod{10},$$

onde $0 \leq r < 10$. Inicialmente, observemos que é conveniente encontrar uma congruência inicial, do tipo $a \equiv 0$, $a \equiv 1$ ou $a \equiv -1$ por facilidade de calcular as potências, e possamos usar as propriedades necessárias para chegar ao resultado esperado. Um bom ponto de partida é a congruência

$$3^4 \equiv 1 \pmod{10}.$$

Elevando ambos os membros desta congruência a 262, segue do item (3) do Teorema 5.1.3 que

$$(3^4)^{262} \equiv 1^{262} \pmod{10} \quad \Rightarrow \quad 3^{1048} \equiv 1 \pmod{10}.$$

Agora, multiplicando os membros da última congruência por $c = 3^2$, então do item (2) do mesmo Teorema, obtemos

$$3^{1048} \cdot 3^2 \equiv 1 \cdot 3^2 \pmod{10} \quad \Rightarrow \quad 3^{1050} \equiv 9 \pmod{10}.$$

Logo, o algarismo das unidades é $r = 9$. △

Vale ressaltar que nem sempre é fácil ou possível encontar uma congruência inicial ideal para resolver um problema semelhante ao anterior, ou seja, uma congruência da forma

$$a^k \equiv 1 \pmod{m} \quad \text{ou} \quad a^k \equiv -1 \pmod{m},$$

onde k é um inteiro positivo. Adiante mostraremos resultados especiais tais como o Pequeno Teorema de Fermat e o Teorema de Euler, os quais facilitam obter tais congruências.

Exemplo 5.1.5 (BANCO DE QUESTÕES - OBMEP - 2010) A, B, C, D, E, F, G e H são os fios de apoio que uma aranha usa para construir sua teia, conforme mostra a figura abaixo. A aranha continua seu trabalho. Sobre qual fio de apoio estará o número 118?

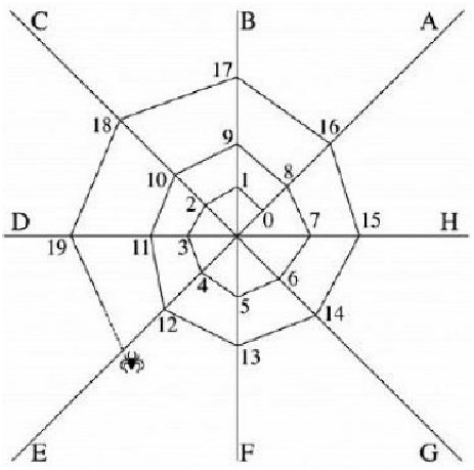

Figura 5.1: A Aranha e sua teia.

Solução: Observando a imagem, notamos que há uma periodicidade na construção da teia sobre os fios de apoio. Os fios se repetem a cada 8 números. Assim, a situação se resume em determinar o valor de r na seguinte congruência

$$118 \equiv r \pmod{8}$$

onde $0 \leq r < 8$. Como $118 = 14 \cdot 8 + 6$, segue que

$$118 \equiv 6 \pmod{8}.$$

Portanto, o fio 118 estará no fio de apoio G. $\triangle$

Definição 5.1.6 *Se k e t são inteiros e $t \equiv k \pmod{m}$, dizemos que k é um resíduo de t módulo m.*

Por exemplo, como $24 \equiv 3 \pmod{7}$, então 3 é um resíduo de 24 módulo 7. Da mesma forma, -2 é um resíduo de 18 módulo 5, pois $18 \equiv -2 \pmod{5}$.

Da Divisão Euclidiana, temos que

$$a = qm + r, \text{ com } 0 \leq r \leq m-1.$$

De modo que $r \in \{0,1,...,m-1\}$ e os elementos desse conjunto são dois a dois incongruentes módulo m. Segue que cada inteiro b é congruente módulo m a exatamente um dos valores $0,1,...,m-1$. Em particular,

$$a \equiv 0 \,(\mathrm{mod}\, m) \quad \Leftrightarrow \quad m \mid a.$$

Por essa razão, dizemos que o conjunto $\{0,1,...,m-1\}$ é um *sistema completo de resíduos módulo m*. Podemos generalizar com a seguinte:

Definição 5.1.7 *Um conjunto de inteiros $\{a_1, a_2, ..., a_r\}$ é um **sistema completo de resíduos** módulo m, quando:*

(a) $a_i \not\equiv a_j \,(\mathrm{mod}\, m)$ *para* $i \neq j$.

(b) *Para todo inteiro b, existe* a_i *tal que* $b \equiv a_i \,(\mathrm{mod}\, m)$.

Exemplo 5.1.8 O conjunto de $\{4,5,6,7\}$ é um sistema completo de resíduos módulo 4. De fato, os elementos deste conjunto são dois a dois incongruentes módulo 4, e ainda considerando a congruência módulo 4, temos

$$4 \equiv 0, \quad 5 \equiv 1, \quad 6 \equiv 2, \quad 7 \equiv 3.$$

△

Pela definição 5.1.7 é fácil ver que o conjunto $\{0,1,2,...,m-1\}$ de fato é um Sistema Completo de Resíduos módulo m que possui exatamente m elementos. Mostraremos a seguir que todo Sistema Completo de Resíduos possui m elementos.

Teorema 5.1.9 *Se $\{a_1, a_2, \ldots, a_k\}$ é um Sistema Completo de Resíduos módulo m, então $k = m$.*

Demonstração: Já sabemos que $\{0,1,\ldots,m-1\}$ é um scr módulo m. Assim, cada $a_i \in \{a_1, a_2, \ldots, a_k\}$ é congruente a exatamente um dos $r_i \in \{0,1,\ldots,m-1\}$, o que nos mostra que $k \leq m$. Por outro lado, como por hipótese $\{a_1, a_2, \ldots, a_k\}$ é um scr módulo m, cada r_i é congruente a exatamente um dos $a_i \in \{a_1, a_2, \ldots, a_k\}$ e, portanto, $m \leq k$. Desse modo, $k = m$. □

O próximo teorema é um resultado bastante útil para o decorrer desse trabalho, principalmente pelo corolário que se segue, o qual representa a Lei do Cancelamento.

Teorema 5.1.10 *Sejam a, b e c inteiros quaisquer. Temos que*

$$ac \equiv bc \;(\mathrm{mod}\, m) \;\Leftrightarrow\; a \equiv b \;(\mathrm{mod}\, m/d)\,,$$

onde $d = mdc(c,m)$. □

Como exemplo, temos que

$$14 \equiv 2 \pmod{6} \;\Rightarrow\; 7 \cdot 2 \equiv 1 \cdot 2 \pmod{6}.$$

Daí, pelo Teorema 5.1.10, segue que

$$7 \equiv 1 \pmod{3}.$$

A Lei do cancelamento segue do seguinte caso particular do teorema anterior.

Corolário 5.1.11 (Lei do Cancelamento) *Se* $ac \equiv bc \pmod{m}$ *e* $mdc(c,m) = 1$*, então* $a \equiv b \pmod{m}$.

Demonstração: Se $ac \equiv bc \pmod{m}$, com $d = mdc(c,m) = 1$, então pelo Teorema 5.1.10, segue que $a \equiv b \pmod{m/d}$. Portanto, $a \equiv b \pmod{m}$. □

Exemplo 5.1.12 Como $10 \cdot 5 \equiv 3 \cdot 5 \pmod{7}$ e $mdc(5,7) = 1$, segue da Lei do Cancelamento que $10 \equiv 3 \pmod{7}$. △

Corolário 5.1.13 *Dados a, b e c inteiros quaisquer e p primo, temos:*

(1) *Se* $m = p$*, e* $mdc(c,p) = 1$*,*

$$ac \equiv bc \pmod{p} \;\Rightarrow\; a \equiv b \pmod{p}.$$

(2) *Se* $c \equiv 0 \pmod{m}$*, então* $mdc(c,m) = m$*, de modo que*

$$ac \equiv bc \pmod{m} \;\Rightarrow\; a \equiv b \pmod{1}.$$

Curiosamente, o produto de dois inteiros que não são congruentes a zero módulo m pode ser congruente a zero. Por exemplo, $3 \not\equiv 0 \pmod{6}$ e $2 \not\equiv 0 \pmod{6}$, contudo $6 = 3 \cdot 2 \equiv 0 \pmod{6}$. Além do mais, se $ab \equiv 0 \pmod{m}$ e $mdc(a,m) = 1$, então $b \equiv 0 \pmod{m}$. Particularmente, se p é primo e $ab \equiv 0 \pmod{p}$, então $a \equiv 0 \pmod{p}$ ou $b \equiv 0 \pmod{p}$, ou seja, $p \mid a$ ou $p \mid b$.

5.2 Congruências Lineares

Nesta seção, os resultados considerados são de elevada importância ao desenvolvimento de alguns conhecimentos criptográficos, particularmente abordados adiante. Entretanto, é de fundamental relevância decidir quando uma congruência linear tem solução inteira.

Definição 5.2.1 *Sejam a e b inteiros, com $a \neq 0$. Uma congruência da forma*

$$ax \equiv b \pmod{m}$$

é chamada ***congruência linear****, onde x é uma incógnita.*

Por exemplo, $x_0 = 2$ é uma solução da congruência linear $8x \equiv 7 \pmod{3}$, pois $8 \cdot 2 = 16 \equiv 7 \pmod{3}$. Enquanto, a congruência linear $4x \equiv 3 \pmod{2}$ não tem solução inteira, pois $4x_0 - 3 = 2q$, com $q \in \mathbb{Z}$, de forma que 2 divide 3, o que é uma contradição.

Objetivamente, temos que determinar todas soluções inteiras (se existirem) de $ax \equiv b \pmod{m}$, isto é, todos os inteiros x_0 para os quais

$$ax_0 \equiv b \pmod{m}.$$

Um caso particular importante da congruência linear definida anteriormente é

$$ax \equiv 1 \pmod{m}.$$

Neste caso, se x_0 é uma solução desta congruência, então dizemos que a é **invertível** módulo m, e que x_0 é um **inverso** de a módulo m. Por exemplo, na congruência

$$19x \equiv 1 \pmod{5},$$

o número 19 é invertível, pois $x_0 = 4$ é uma solução desta congruência, de modo que este é um inverso de 19.

Vimos que nem sempre uma congruência linear tem solução inteira. Por outro lado, uma congruência linear pode ter infinitas soluções. Inicialmente, observamos que se x_0 é uma solução de $ax \equiv b \pmod{m}$ e $x_0 \equiv y_0 \pmod{m}$, então y_0 também é solução desta congruência.

Por exemplo, $x_0 = 2$ é uma solução de $8x \equiv 7 \pmod{3}$. Por outro lado, toda solução é da forma

$$x = 2 + 3k, \quad \text{com} \quad k \in \mathbb{Z},$$

como veremos adiante, de modo geral, nos passos apresentados para resolver uma congruência linear.

Os próximos resultados estabelecerão quando uma congruência linear tem solução e também o conjunto de todas as soluções.

Teorema 5.2.2 *A congruência linear $ax \equiv b \pmod{m}$ tem solução inteira se, e somente se, $d \mid b$, com $d = mdc(a,m)$.*

Demonstração: Inicialmente, tomemos $d = mdc(a,m)$ e suponhamos que x_0 seja uma solução de $ax \equiv b \pmod{m}$. Logo, existe $k \in \mathbb{Z}$, tal que, $ax_0 - b = km$, isto é, $b = ax_0 - km$. Daí, como $d \mid a$ e $d \mid m$, então $d \mid b$.

Reciprocamente, supondo que $d \mid b$ com $d = mdc(a,m)$, então pela identidade de Bachet-Bézout existem inteiros r e s tais que

$$d = a \cdot r + s \cdot m.$$

Como $b \mid d$, então existe $t \in \mathbb{Z}$, tal que $b = dt$, logo usando o valor de d, obtemos

$$b = (ar + sm)t = art + smt,$$

isto é, $a(rt) \equiv b \pmod{m}$. Portanto, $x_0 = rt$ é uma solução de $ax \equiv b \pmod{m}$. □

Por exemplo, a congruência $6x \equiv 5 \pmod{2}$ não tem solução inteira, pois $mdc(6,2) = 2$ e $2 \nmid 5$.

A solução geral de uma congruência linear fica estabelecida com o seguinte:

Teorema 5.2.3 *Se x_0 é uma solução da congruência linear $ax \equiv b \pmod{m}$, então todas as soluções desta congruência são da forma*

$$x = x_0 + (m/d)k, \quad com \quad k \in \mathbb{Z},$$

com $d = mdc(a,m)$. □

Particularmente,

Corolário 5.2.4 *Temos que $ax \equiv 1 \pmod{m}$ tem solução se, e somente se, $mdc(a,m) = 1$. Neste caso, a solução geral é dada por*

$$x = x_0 + km, \quad com \quad k \in \mathbb{Z},$$

com x_0 é uma solução inicial.

Note que um inteiro a é invertível módulo m se, e somente se, $mdc(a,m) = 1$, como pode ser observado facilmente do corolário anterior.

Quanto ao número de soluções incongruentes de uma congruência linear a proposição seguinte caracteriza esse fato.

Proposição 5.2.5 *Consideremos a congruência $ax \equiv b \pmod{m}$, em que $d = mdc(a,m)$. Se $d \mid b$, então esta congruência possui d soluções incongruentes módulo m, dadas por*

$$x_0, \quad x_0 + \frac{m}{d}, \quad x_0 + \frac{2m}{d}, \ldots, \quad x_0 + \frac{(d-1)m}{d},$$

com x_0 é uma solução particular.

Em particular, quando o $mdc(a,m) = 1$, obtemos o seguinte:

Corolário 5.2.6 *Se $mdc(a,m) = 1$, então a congruência linear $ax \equiv b \pmod{m}$ tem única solução módulo m.*

Em síntese, fazendo uso dos resultados obtidos anteriormente, podemos resolver uma congruência linear $ax \equiv b \pmod{m}$, com $d = mdc(a,m)$ e $d \mid b$, seguindo os seguintes passos:

(1) De acordo com a Identidade de Bachet-Bézout 3.4.1, obtemos inteiros r e s tais que

$$d = a \cdot r + m \cdot s.$$

(2) Se $b = dt$, então $x_0 = rt$ é uma solução de $ax \equiv b \pmod{m}$, de modo que sua solução geral é dada por

$$x = x_0 + k\frac{m}{d}, \text{ com } k \in \mathbb{Z}.$$

Além disso,

$$x_0,\ x_0 + \frac{m}{d},\ x_0 + \frac{2m}{d},\ldots,\ x_0 + \frac{(d-1)m}{d}$$

são as soluções de $ax \equiv b \pmod{m}$ duas a duas incongruentes módulo m.

Exemplo 5.2.7 Resolver as seguintes congruências lineares:

a) $6x \equiv 21 \pmod{8}$.

b) $3x \equiv 6 \pmod{12}$

Solução: a) Como $mdc(8,6) = 2$ e $2 \nmid 21$, então, pelo Teorema 5.2.2 a congruência não tem solução inteira.

b) Como $mdc(3,12) = 3$ e $3 \mid 6$, então a congruência tem solução inteira. Daí, procedendo de maneira análoga ao exemplo 3.4.4, temos pela Identidade de Bachet-Bézout 3.4.1 que

$$3 \cdot 5 + 12 \cdot (-1) = 3,$$

isto é, $r = 5$. Daí, como $b = 6 = 3 \cdot 2$, segue que $t = 2$. Logo, $x_0 = rt = 5 \cdot 2 = 10$ é uma solução particular de $3x \equiv 6 \pmod{12}$. A solução geral é dada por $x = 10 + (12/3)k$, ou seja,

$$x = 10 + 4k, \text{ com } k \in \mathbb{Z}.$$

Dessa forma, temos $d = 3$ soluções incongruentes módulo 12, que são

$$10,\ 10 + \frac{12}{3},\ 10 + 2 \cdot \frac{12}{3},$$

ou melhor, 10, 14 e 18. △

Definição 5.2.8 *Um **sistema reduzido de resíduos** módulo m é um conjunto formado a partir de um Sistema Completo de Resíduos módulo m, de modo que cada elemento é primo com m.*

Por exemplo o conjunto $\{1,3,5,7\}$ é um sistema reduzido de resíduos módulo 8.

O número de elementos de um sistema reduzido de resíduos módulo m foi calculado a primeira vez no século XVIII pelo matemático suíço Leonhard Euler (1707-1783) e denotaremos por $\varphi(m)$, também chamada *função* φ (fi) *de Euler*. Esse número é igual a

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

com p representando os divisores primos positivos de m sem repetições.

Em particular, se m é primo, então $\varphi(m) = m - 1$. A recíproca também é verdadeira.

Por exemplo, para $m = 10$, temos dois divisores primos $p_1 = 2$ e $p_2 = 5$. Logo,

$$\begin{aligned} \varphi(10) &= 10 \prod_{p|10} \left(1 - \frac{1}{p}\right) \\ &= 10 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) \\ &= 10 \cdot \frac{1}{2} \cdot \frac{4}{5} \\ &= 4. \end{aligned}$$

Como outro exemplo, consideremos $m = 7$. Nesse caso como m é primo, basta fazer

$$\begin{aligned} \varphi(7) &= 7 - 1 \\ &= 6 \end{aligned}$$

O próximo teorema tem grande aplicabilidade no cálculo da função φ, em particular no processo de decodificação do sistema RSA, como veremos adiante.

Teorema 5.2.9 *Se m e n são números naturais tais que* $mdc(m,n) = 1$*, então*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

□

Exemplo 5.2.10 Calcular $\varphi(10)$.

Solução: Como $10 = 2 \cdot 5$,

$$\begin{aligned} \varphi(10) = \varphi(2 \cdot 5) &= \varphi(2)\varphi(5) \\ &= (2-1)(5-1) \\ &= 4 \end{aligned}$$

Logo, $\varphi(10) = 4$. △

Enunciaremos a seguir dois importantes resultados já anunciados anteriormente, o Teorema de Euler e o Pequeno Teorema de Fermat. Este último, sendo uma consequência direta do primeiro. Como foi dito, eles estabelecem uma congruência inicial importante com relevantes aplicações na Criptografia. Antes de apresentá-los veremos alguns resultados necessários para sua demonstração.

Lema 5.2.11 *Dados os inteiros a, b e c, temos que*

$$mdc(a,bc) = 1 \;\Leftrightarrow\; mdc(a,b) = 1 \;\; e \;\; mdc(a,c) = 1.$$

De uma forma geral, dados inteiros $a_1, a_2, \ldots, a_n$, temos que

$$mdc(a_1, a_2a_3 \ldots a_n) = 1 \;\Leftrightarrow\; mdc(a_1, a_i) = 1 \tag{5.1}$$

para $i = 2, \ldots, n$.

Lema 5.2.12 *Seja a um inteiro tal que $mdc(a,m) = 1$. Se $a_1, a_2, \ldots, a_{\varphi(m)}$ são os inteiros positivos menores do que m e relativamente primos com m, então*

$$aa_1, aa_2, \ldots, aa_{\varphi(m)}$$

são congruentes módulo m a $a_1, a_2, \ldots, a_{\varphi(m)}$, em alguma ordem.

Demonstração: Mostremos primeiramente que os elementos $aa_1, aa_2, \ldots, aa_{\phi(m)}$ são dois a dois incongruentes módulo m. De fato, se $aa_i \equiv aa_j \pmod{m}$ para $i \neq j$, então como $mdc(a,m) = 1$, podemos cancelar o fator a desta congruência e, assim, $a_i \equiv a_j \pmod{m}$, ou seja, $m \mid a_i - a_j$, o que é uma impossibilidade, pois $1 \leq a_i, a_j \leq m-1$ e $a_i \neq a_j$. Além disso, como $mdc(a,m) = 1$ e $mdc(a_i,m) = 1$ para todo $i = 1, \ldots, \phi(m)$, então pelo Lema 5.2.11, temos que $mdc(aa_i, m) = 1$.

Desde que $\{0, 1, \ldots, m-1\}$ é um sistema completo de resíduos módulo m, então para cada aa_i, existe único inteiro b, com $0 \leq b < m$, tal que $aa_i \equiv b \pmod{m}$. Como

$$mdc(b,m) = mdc(aa_i, m) = 1,$$

então b deve necessariamente ser um dos inteiros $a_1, a_2, \ldots, a_{\phi(m)}$. Logo, $aa_i \equiv a_j \pmod{m}$ para algum $j = 1, \ldots, \phi(m)$. Isso conclui a demonstração. □

Vamos considerar um caso particular. Para $m = 10$, existem $\varphi(10) = 4$ inteiros positivos menores do que 10 e primos com 10, que são

$$a_1 = 1, \;\; a_2 = 3, \;\; a_3 = 7, \;\; a_4 = 9.$$

Considerando $a = 7$, temos

$$7 \cdot 1 \equiv 7 \pmod{10},$$

$$7 \cdot 3 \equiv 1 \pmod{10},$$

$$7 \cdot 7 \equiv 9 \pmod{10},$$

$$7 \cdot 9 \equiv 3 \pmod{10},$$

Multiplicando membro a membro estas seis congruências, obtemos que

$$7^4(1\cdot 3\cdot 7\cdot 9) \equiv (7\cdot 1\cdot 9\cdot 3) \pmod{10}.$$

Como $mdc(1\cdot 3\cdot 7\cdot 9, 10) = 1$, então $7^4 \equiv 1 \pmod{10}$, isto é,

$$7^{\varphi(10)} \equiv 1 \pmod{10}.$$

É isso que mostra o Teorema de Euler para o caso geral.

Teorema 5.2.13 (Euler) *Sejam a e m inteiros, com $m \geq 1$ e $mdc(a,m) = 1$. Então,*

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

Demonstração: O caso $m = 1$ é imediato, pois $\varphi(1) = 1$. Por isso, vamos considerar $m > 1$. Sejam $a_1, a_2, \ldots, a_{\varphi(m)}$ os inteiros positivos menores do que m que são relativamente primos com m. Desde que $mdc(a_i, m) = 1$ para cada $i = 1, \ldots, \varphi(m)$, segue do Lema (5.2.12) que $aa_1, aa_2, \ldots, aa_{\varphi(m)}$ são congruentes módulo m a $a_1, a_2, \ldots, a_{\varphi(m)}$, em alguma ordem. Desse modo,

$$\begin{aligned} a\cdot a_1 &\equiv b_1 \pmod{m},\\ a\cdot a_2 &\equiv b_2 \pmod{m},\\ &\vdots\\ a\cdot a_{\varphi(m)} &\equiv b_{\varphi(m)} \pmod{m}, \end{aligned}$$

em que $b_1, b_2, \ldots, b_{\varphi(m)}$ são os inteiros $a_1, a_2, \ldots, a_{\varphi(m)}$, não necessariamente nesta ordem. Multilicando estas congruências, segue que

$$(aa_1)(aa_2)\cdots(aa_{\varphi(m)}) \equiv b_1 b_2 \cdots b_{\varphi(m)} \pmod{m},$$

de modo que,

$$a^{\varphi(m)}(a_1 a_2 \cdots a_{\varphi(m)}) \equiv a_1 a_2 \cdots a_{\varphi(m)} \pmod{m}.$$

Como $mdc(a_i, m) = 1$ para todo $i = 1, \ldots, \varphi(m)$, segue em decorrência do Lema (5.2.11) que $mdc(a_1 a_2 \ldots a_{\varphi(m)}, m) = 1$. Por isso, podemos cancelar o fator $a_1 a_2 \ldots a_{\varphi(m)}$ da última congruência e, assim,

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

□

Na verdade o Teorema de Euler é uma generalização do Pequeno Teorema de Fermat, embora esse último tenha sido desenvolvido primeiro e provado por Fermat em 1640.

Corolário 5.2.14 (Pequeno Teorema de Fermat) *Sejam p um número primo e a um inteiro tal que $p \nmid a$. Então,*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Demonstração: Como p é primo, basta notar que $\varphi(p) = p - 1$. □

O exemplo que segue mostra a utilização dos resultados obtidos acima, ressaltando a facilidade de encontrar uma congruência inicial que facilite os cálculos com potências na resolução de determinada congruência.

Exemplo 5.2.15 Calcular o resto da divisão de:

a) 2^{194} por 17.

b) 3^{1239} por 10.

Solução: a) Como 17 é primo e $17 \nmid 2$, pelo Pequeno Teorema de Fermat, temos

$$2^{16} \equiv 1 \pmod{17}.$$

Observando que $194 = 12 \cdot 16 + 2$ e usando as propriedades vistas anteriormente, elevamos ambos os membros da congruência por 12. Daí,

$$(2^{16})^{12} \equiv 1^{12} (\mathrm{mod}\, 17).$$

Multiplicando ambos os membros por 2^2, temos que

$$2^{192} \cdot 2^2 \equiv 1 \cdot 2^2 \pmod{17}.$$

Logo,

$$2^{194} \equiv 4 \pmod{17}.$$

Portanto, o resto da divisão de 2^{194} por 17 é 4.

b) Como $mdc(3,10) = 1$ e sabendo que $\varphi(10) = 4$, pelo Teorema de Euler segue que

$$3^4 \equiv 1 \pmod{10}$$

Observando que $1239 = 309 \cdot 4 + 3$, analogamente ao item anterior temos que

$$(3^4)^{309} \equiv 1^{309} \pmod{10}.$$

Daí, segue que

$$3^{1236} \cdot 3^3 \equiv 1 \cdot 3^3 \pmod{10}.$$

Logo,

$$3^{1239} \equiv 7 \pmod{10}$$

Portanto, o resto da divisão de 3^{1239} por 10 é 7. △

Capítulo 6

Criptografia

Todo conteúdo abordado anteriormente contribui de forma direta ou indireta ao estudo sobre a essência deste trabalho, ou seja, a Criptografia como uma proposta de aplicação prática relacionada a conteúdos curriculares do ensino básico.

A necessidade de contextualização de determinados conteúdos é algo bastante questionado no ensino de matemática e inclusive descrito como um ponto inicial na abordagem de determinada atividade matemática a ser desenvolvida, conforme os Parâmetros Curriculares Nacionais (PCN's) sobre o ensino de matemática.

Nosso objetivo é propor uma situação atual importante e, de certa forma, inovadora, que estimule o educando a aprender determinados conceitos discutidos nessa faixa de ensino. Portanto, mencionaremos neste capítulo alguns métodos criptográficos, dentre eles o método RSA. Como pré-requisito, além dos tópicos relativos à Teoria dos Números especificados em capítulos anteriores, sugerimos um conhecimento elementar sobre o estudo de funções.

6.1 Conceitos preliminares

Antes de iniciarmos com os sistemas criptográficos a serem descritos a seguir, precisamos conceituar resumidamente alguns termos que serão utilizados no transcorrer desse capítulo. Como importantes referências a respeito, podemos encontrar maiores detalhes em *Criptografia para Iniciantes* [19] e *Números Inteiros e Criptografia RSA [4].*

Assim, inspirado em S. C. Coutinho [4], inicialmente façamos uma descrição dos termos *codificar*, *decodificar* e *decifrar* uma mensagem, que adotaremos como simples detalhe técnico. *Codificar* uma mensagem é transformá-la em um código secreto. O destinatário legal, usuário do código, *decodifica,* isto é, interpreta a mensagem recebida, que é um processo mais complexo do que o simples fato de codificar. Enquanto, *decifrar* uma mensagem significa "quebrar" o código secreto quando este não é um usuário lícito do código. Nesse sentido, criptografar uma mensagem baseia-se na ideia de transformar uma mensagem em um determinado código para que apenas os seus usuários legais consigam interpretá-la. Vale ressaltar, que o processo de decodificação é geralmente mais complicado, comparado com

Letra	Número	Letra	Número
A	00	N	13
B	01	O	14
C	02	P	15
D	03	Q	16
E	04	R	17
F	05	S	18
G	06	T	19
H	07	U	20
I	08	V	21
J	09	W	22
K	10	X	23
L	11	Y	24
M	12	Z	25

Tabela 6.1: Tabela de conversão.

a codificação. Enquanto decifrar consiste de um processo bem mais complexo e até mesmo impossível, em situações de condições tecnológicas atuais, para processos criptográficos específicos.

A *pré-codificação* é o nome dado ao processo de transformação de uma mensagem-texto em números. Basicamente consiste em uma relação biunívoca entre o conjunto gráfico (letras) que formam a mensagem texto e uma sequência finita apropriada de números sequenciais. Consideramos esta distinção para não confundir essa primeira etapa de processo criptográfico da codificação precisamente.

Supondo que a mensagem original é um texto sem números e constituído apenas por palavras com todas as letras maiúsculas, na etapa de pré-codificação converteremos estas letras em números, como observado na Tabela 6.1.

Por exemplo, a frase *"A MATEMATICA E BELA"* pré-codificada de acordo com a tabela acima é convertida no número

$$00120019041200190802000401041100.$$

Na codificação converteremos os números correspondentes às letras, obtidos no processo de pré-codificação conforme a Tabela 6.1, em outros números de forma a garantir o sigilo durante a transmissão da mensagem, transcritos de acordo com o método criptográfico adotado.

6.2 Criptografia de César

O imperador romano Júlio César usava um sistema criptográfico consistente de uma técnica de transposição de letras que eram substituídas por letras seguintes do alfabeto exatamente em três casas posteriores, como descrito por Suetônio em *As vidas dos Césares* do século II. Assim, codificar uma mensagem usando a Criptografia de César é transpor cada letra do alfabeto original de acordo com um determinado número natural k (chamado de **chave**), tal que $0 \leq k < 26$, considerando a mensagem já pré-codificada.

A seguir aplicaremos alguns exemplos os quais usaremos a Criptografia de César, que poderão ser facilmente aplicados em turmas do ensino básico como uma situação concreta relacionada ao ensino de conteúdos específicos.

Exemplo 6.2.1 Usando a chave original da Criptografia de César ($k = 3$) codificar a palavra

CONGRUENCIA.

Solução: Inicialmente, vamos pré-codificar a mensagem de acordo com a Tabela 6.1. Então, temos:

$$02 - 14 - 13 - 06 - 17 - 20 - 04 - 13 - 02 - 08 - 00.$$

Usando a chave $k = 3$, ou seja, adicionaremos 3 unidades a cada número da pré-codificação e teremos a seguinte codificação:

$$05 - 17 - 16 - 09 - 20 - 23 - 07 - 16 - 05 - 11 - 03.$$

△

Note que, diferentemente da mensagem original, a mensagem codificada no exemplo acima, tem a seguinte correspondência de acordo com a Tabela 6.1:

FRQJUXHQFLD.

Exemplo 6.2.2 Criptografar a mensagem "DEUS" usando a Criptografia de César e chave $k = 22$.

Solução: Inicialmente, temos a seguinte pré-codificação:

$$03 - 04 - 20 - 18.$$

Conforme a Tabela 6.1, temos 26 correspondências de letras e números pertencentes ao intervalo de 0 a 25, ou seja, todos os possíveis restos em uma divisão por 26. Isso justifica o fato de usarmos uma congruência módulo 26 nesse tipo de sistema criptográfico. Codificando, temos:

$$\begin{aligned}
03 + 22 = 25 &\equiv 25 \pmod{26},\\
04 + 22 = 26 &\equiv 00 \pmod{26},\\
20 + 22 = 42 &\equiv 16 \pmod{26},\\
18 + 22 = 40 &\equiv 14 \pmod{26}.
\end{aligned}$$

Portanto, temos a seguinte codificação:

$$25 - 00 - 16 - 14.$$

$\triangle$

Assim, de modo geral, podemos escrever a Criptografia de César para uma chave $k \in \mathbb{Z}$, tal que $0 \leq k < 26$ da seguinte forma:

$$C(t) \equiv t + k \pmod{26}, \tag{6.1}$$

em que:

- $C(t) \rightarrow$ número codificado.
- $t \rightarrow$ número pré-codificado.
- $k \rightarrow$ chave da criptografia.

Observa-se que para $k = 0$ a mensagem codificada é exatamente o texto original sem alterações. Logo, este caso não desperta interesse. Dessa forma, vamos assumir que $k \neq 3$. Além disso, quando $k \neq 3$, chamaremos (6.1) de **Criptografia de César Generalizada**.

Por outro lado, podemos decodificar uma mensagem fazendo uso da seguinte congruência:

$$D(s) \equiv s - k \pmod{26}, \tag{6.2}$$

onde:

- $D \rightarrow$ número decodificado.
- $s \rightarrow$ número codificado
- $k \rightarrow$ chave da criptografia

Exemplo 6.2.3 Codificar a mensagem "ARITMETICA"usando a chave $k = 15$.

Solução: Pré-codificando, temos:

$$00 - 17 - 08 - 19 - 12 - 04 - 19 - 08 - 02 - 00.$$

Usando (6.1) temos a seguinte codificação:

$$\begin{aligned}
C(00) &\equiv 00+15 \equiv 15 \pmod{26},\\
C(17) &\equiv 17+15 \equiv 06 \pmod{26},\\
C(08) &\equiv 08+15 \equiv 23 \pmod{26},\\
C(19) &\equiv 19+15 \equiv 08 \pmod{26},\\
C(12) &\equiv 12+15 \equiv 01 \pmod{26},\\
C(04) &\equiv 04+15 \equiv 19 \pmod{26},\\
C(19) &\equiv 19+15 \equiv 08 \pmod{26},\\
C(08) &\equiv 08+15 \equiv 23 \pmod{26},\\
C(02) &\equiv 02+15 \equiv 17 \pmod{26},\\
C(00) &\equiv 00+15 \equiv 15 \pmod{26}.
\end{aligned}$$

Portanto, a mensagem codificada é:

$$15-06-23-08-01-19-08-23-17-15.$$

$\triangle$

Usando (6.2) podemos decodificar facilmente a mensagem codificada no exemplo anterior da seguinte maneira:

$$\begin{aligned}
D(15) &\equiv 15-15 \equiv 00 \pmod{26},\\
D(06) &\equiv 06-15 \equiv 17 \pmod{26},\\
D(23) &\equiv 23-15 \equiv 08 \pmod{26},\\
D(08) &\equiv 08-15 \equiv 19 \pmod{26},\\
D(01) &\equiv 01-15 \equiv 12 \pmod{26},\\
D(19) &\equiv 19-15 \equiv 04 \pmod{26},\\
D(08) &\equiv 08-15 \equiv 19 \pmod{26},\\
D(23) &\equiv 23-15 \equiv 08 \pmod{26},\\
D(17) &\equiv 17-15 \equiv 02 \pmod{26},\\
D(15) &\equiv 15-15 \equiv 00 \pmod{26}.
\end{aligned}$$

Assim, a mensagem decodificada seguinte corresponde a pré-codificação da mensagem original. Vejamos:

$$00-17-08-19-12-04-19-08-02-00$$

Fazendo a correspondência de acordo com a tabela de conversão mostrada anteriormente, temos exatamente a mensagem original

"ARITMÉTICA".

No próximo exemplo, temos uma situação em que mesmo desconhecendo a chave k, ainda assim é possível, em alguns casos, decodificar uma mensagem cifrada pela Criptografia de César. Tal fato deve-se à frequência média que determinada letra aparece em uma frase longa de uma língua estabelecida ser relativamente constante. Conforme afirma em [4], na língua portuguesa as vogais são mais frequentes do que as consoantes e a vogal "a" é a vogal com maior frequência, além do mais as consoantes "s" e "m" são mais frequentes que as demais. É claro que numa frase curta a observação desta frequência pode ser desfavorável. Por essa razão este método criptográfico é considerado bastante frágil com relação a sua segurança.

Por exemplo, suponhamos que a mensagem codificada

$$15-01-15-08-19-01-15-08-23-17-15-19-07-03-16-19-06-15-02-15$$

tenha sido interceptada por um usuário não autorizado.

Vamos decifrar a mensagem acima sem o conhecimento da chave k.

Inicialmente, notemos que os códigos 15 e 19 apresentam as maiores frequências de valores respectivos 6 e 3. Daí, usando o processo de análise de frequências da língua portuguesa podemos supor que os respectivos códigos correspondem as vogais "A" e "E". Assim, constatamos que $k = 15$.

Portanto, usando a expressão em (6.2) e procedendo como no exemplo anterior, temos a seguinte mensagem original:

"A MATEMÁTICA É SOBERANA".

6.3 Cifra afins

Uma generalização da Criptografia de César Generalizada é a Criptografia de Cifras Afins. É notória a semelhança deste método com a função afim, componente curricular sempre presente no ensino básico. No entanto, este é abordado como uma relação de congruência módulo m. Trata-se uma situação inovadora de aplicação prática deste conteúdo à este nível de ensino. Com relação à tabela de conversão, usaremos a mesma descrita anteriormente.

Definição 6.3.1 *Sejam x e y números inteiros tais que $0 \leq x, y < 26$ e $mdc(x, 26) = 1$. A cifra representada pela expressão*

$$C(t) \equiv x \cdot t + y \pmod{26} \tag{6.3}$$

*é chamada de **Cifra Afim**.*

Os inteiros x e y são denominados de **chaves da Cifra Afim**. Além do mais, $C(t)$ e t são respectivamente o **número codificado** e o **número pré-codificado**.

Se $mdc(x,26) = 1$, então existe o inverso de x módulo 26 que denotaremos por x^{-1}, isto é, $x \cdot x^{-1} \equiv 1 \pmod{26}$. Assim, como a congruência em (6.3) também pode ser escrita sob a forma

$$x \cdot t \equiv (C(t) - y) \pmod{26},$$

podemos multiplicar ambos os membros da congruência acima por x^{-1} e obteremos

$$t \equiv x^{-1}(C(t) - y) \pmod{26}.$$

Fazendo $C(t) = s$ e $t = D(s)$, respectivamente o número codificado e o número decodificado da Cifra Afim, concluímos que

$$D(s) \equiv x^{-1}(s - y) \pmod{26}. \tag{6.4}$$

A congruência em (6.4) representa a expressão de decodificação de uma Cifra Afim.

Exemplo 6.3.2 Vamos codificar a mensagem "FERMAT" usando a criptografia de Cifras Afins.

Solução: Inicialmente vamos pré-codificar a mensagem:

$$05 - 04 - 17 - 12 - 00 - 19$$

Assim, sejam os inteiros $x = 7$ e $y = 11$ as chaves da cifra, escolhidas conforme a definição (6.3.1). Notemos que $mdc(7,26) = 1$. Usando a expressão $C(t) \equiv x \cdot t + y \pmod{26}$, vamos codificar os blocos numéricos da pré-codificação. Fazendo isto, temos:

$$\begin{aligned}
C(05) &\equiv 7 \cdot 5 + 11 \equiv 20 \pmod{26}, \\
C(04) &\equiv 7 \cdot 4 + 11 \equiv 13 \pmod{26}, \\
C(17) &\equiv 7 \cdot 17 + 11 \equiv 00 \pmod{26}, \\
C(12) &\equiv 7 \cdot 12 + 11 \equiv 17 \pmod{26}, \\
C(00) &\equiv 7 \cdot 0 + 11 \equiv 11 \pmod{26}, \\
C(19) &\equiv 7 \cdot 19 + 11 \equiv 14 \pmod{26}.
\end{aligned}$$

Portanto, temos a seguinte mensagem codificada:

$$20 - 13 - 00 - 17 - 11 - 14.$$

$\triangle$

Exemplo 6.3.3 Decodificar a mensagem

$$10-20-05-12-21-13-04$$

sendo $x=5$ e $y=13$ as chaves da Cifra Afim.

Solução: Inicialmente, usaremos o Algoritmo de Euclides para o cálculo do $mdc(5,26)$. Aplicando divisões sucessivas, temos:

$$\begin{cases} 26 &= 5\cdot 5+1, \\ 5 &= 1\cdot 5+0. \end{cases} \tag{6.5}$$

Logo, $mdc(5,26)=1$. Encontremos a e $b\in\mathbb{Z}$, tais que $1=5a+26b$. Isso consistirá em isolar os restos não nulos das divisões de baixo para cima das igualdades em (6.5), substituindo-os sucessivamente. Fazendo isso, segue que

$$\begin{aligned} 1 &= 26-5\cdot 5 \\ &= 5\cdot(-5)+26\cdot 1. \end{aligned}$$

Logo, $a=-5$ e $b=1$. Portanto $x^{-1}=-5\equiv 21 \pmod{26}$. Para decodificarmos a mensagem utilizaremos a seguinte expressão:

$$D(s)\equiv 21(s-13) \pmod{26}.$$

Assim, decodificando cada bloco da mensagem cifrada, temos:

$$\begin{aligned} D(10) &\equiv 21(10-13) \equiv 15 \pmod{26}, \\ D(20) &\equiv 21(20-13) \equiv 17 \pmod{26}, \\ D(05) &\equiv 21(5-13) \equiv 14 \pmod{26}, \\ D(12) &\equiv 21(12-13) \equiv 05 \pmod{26}, \\ D(21) &\equiv 21(21-13) \equiv 12 \pmod{26}, \\ D(13) &\equiv 21(13-13) \equiv 00 \pmod{26}, \\ D(04) &\equiv 21(4-13) \equiv 19 \pmod{26}. \end{aligned}$$

Portanto, a mensagem decodificada é:

$$15-17-14-05-12-00-19$$

que correponde a palavra

"PROFMAT".

△

É importante ressaltar que a criptografia de Cifras Afins também padecem da mesma fragilidade de segurança que a Criptografia de César, pois realizando a análise de frequências de uma determinada língua, podemos decifrar uma mensagem criptografada por uma Cifra Afim.

6.4 Criptografia RSA

Finalmente chegamos ao grande resultado relativo a sistemas criptográficos, devido a enorme contribuição da Teoria dos Números utilizada em seu funcionamento, como foi discutido no Capítulo 2. Os pré-requisitos matemáticos necessários ao entendimento do método RSA é relativamente elementar.

Para relembrar a importância e funcionamento do sistema de criptografia de chave pública, em particular o RSA, consideramos a seguinte situação: Alguns dados bancários como número da conta e número da agência são dados públicos, pois qualquer pessoa pode ter acesso a esses dados para realizar um depósito em determinada conta. Diferentemente da senha de acesso da conta. O RSA fornece a segurança necessária para que uma informação enviada a um banco, por exemplo, seja codificada por uma **chave pública**, de tal modo que nem o remetente consiga decodificá-la. Apenas o seu destinatário legal, o qual tem a **chave privada** para realizar o processo de decodificação.

Em linhas gerais, a implementação do RSA inicia-se na escolha de dois números primos distintos muito grandes que chamaremos de p e q. No processo de codificação é necessário o uso do número $n = pq$. Para decodificarmos a mensagem precisamos conhecer os primos p e q. O número n pode tornar-se público, enquanto os primos p e q devem ser mantidos em sigilo. A confiabilidade deste método é devido à dificuldade na fatoração de n. Mesmo com a existência de computadores sofisticados, a fatoração de números dessa natureza é algo ainda sem solução satisfatória, pois os números considerados são números primos com mais de 100 dígitos.

Com relação ao processo de pré-codificação iremos considerar a seguinte Tabela 6.2, que traz a conversão de símbolos (letras maiúsculas sem acentos) em números.

Note que usaremos um número de dois algarismos para cada letra para evitarmos casos de ambiguidade. Para representar o espaço entre duas palavras usaremos 99. Nesta fase, ainda devemos separar em blocos a sequência numérica obtida, ressaltando que cada bloco deve representar um número menor que n. Além disso, tomaremos alguns cuidados na escolha dos blocos. Por exemplo, devemos evitar que o bloco inicie com o algarismo zero por trazer dificuldades na decodificação. E ainda, os blocos não podem constituir nenhuma forma linguística, o que deixa a decodificação por análise de frequência praticamente impossível.

Vejamos o funcionamento completo do método durante o processo de codificação, com exemplo a seguir.

Exemplo 6.4.1 Codificar a frase

"TEORIA DOS NÚMEROS"

Solução: Primeiramente, temos a pré-codificação:

29142427181099132428992330221427242 8.

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

Tabela 6.2: Tabela de conversão - RSA.

Para dar continuidade, devemos escolher os parâmetros do método RSA, ou seja, os primos distintos p e q. Por razões de praticidade vamos escolher dois primos relativamente pequenos, digamos $p = 11$ e $q = 19$, então $n = 11 \cdot 19 = 209$. Dessa forma, finalizando a etapa de pré-codificação, podemos considerar os seguintes blocos:

$$29-142-42-71-8-109-91-32-42-89-92-3-30-22-142-72-42-8.$$

Iniciando a etapa de codificação, precisaremos da **chave pública** do sistema, ou seja, o par (n,e), tal que $mdc(e,\varphi(n)) = 1$. Como p e q são primos distintos, então

$$\begin{aligned} \varphi(n) &= \varphi(p)\varphi(q) \\ &= (p-1)(q-1). \end{aligned}$$

A chave pública é também a *chave de codificação* do método RSA. Assim, codificaremos os blocos numéricos obtidos na pré-codificação, salientando que não podemos juntar os blocos codificados para formar um extenso número, pois seria impossível decodificar a mensagem. A congruência

$$C(b) \equiv b^e \pmod{n} \tag{6.6}$$

é a expressão utilizada para codificar a mensagem, onde b representa cada bloco numérico obtido na etapa anterior.

Como $n = 209$ e $\varphi(n) = 180$, devemos escolher e de modo que $mdc(e,180) = 1$. Tomemos $e = 17$, de modo que a chave pública do sistema é formada pelo par $(209,17)$. Codificando cada bloco empregando em (6.6), temos:

$$C(29) \equiv 29^{17} \pmod{209}.$$

Como, $29^2 \equiv 5 \pmod{209}$, segue que

$$(29^2)^8 \equiv 5^8 \pmod{209},$$

ou seja,

$$29^{16} \equiv 390625 \equiv 4 \pmod{209}.$$

Assim, temos que

$$29^{16} \cdot 29 \equiv 4 \cdot 29 \pmod{209},$$

ou seja,

$$29^{17} \equiv 116 \pmod{209}.$$

Logo, $C(29) \equiv 116 \pmod{209}$. Procedendo de maneira análoga, temos:

$$\begin{aligned}
C(142) &\equiv 142^{17} \equiv 131 \pmod{209},\\
C(42) &\equiv 42^{17} \equiv 81 \pmod{209},\\
C(71) &\equiv 71^{17} \equiv 91 \pmod{209},\\
C(8) &\equiv 8^{17} \equiv 145 \pmod{209},\\
C(109) &\equiv 109^{17} \equiv 186 \pmod{209},\\
C(91) &\equiv 91^{17} \equiv 185 \pmod{209},\\
C(32) &\equiv 32^{17} \equiv 98 \pmod{209},\\
C(42) &\equiv 42^{17} \equiv 81 \pmod{209},\\
C(89) &\equiv 89^{17} \equiv 155 \pmod{209},\\
C(92) &\equiv 92^{17} \equiv 82 \pmod{209},\\
C(3) &\equiv 3^{17} \equiv 108 \pmod{209},\\
C(30) &\equiv 30^{17} \equiv 178 \pmod{209},\\
C(22) &\equiv 22^{17} \equiv 165 \pmod{209},\\
C(142) &\equiv 142^{17} \equiv 131 \pmod{209},\\
C(72) &\equiv 72^{17} \equiv 52 \pmod{209},\\
C(42) &\equiv 42^{17} \equiv 81 \pmod{209},\\
C(8) &\equiv 8^{17} \equiv 145 \pmod{209}.
\end{aligned}$$

Portanto, a mensagem codificada é:

$$116-131-81-91-145-186-185-98-81-155-82-108-178-165-131-52-81-145.$$

$\triangle$

Em todo método criptográfico deve-se estabelecer um processo de decodificação que nos leve à mensagem original, caso contrário não há utilidade para o código. Antes de iniciar um exemplo mostrando o procedimento de decodificação de uma mensagem criptografada com o RSA, devemos fazer algumas ressalvas. Primeiro, precisamos conhecer a *chave de decodificação* (**chave privada** do sistema), isto é, o par (n,d), onde d é o inverso de e módulo $\varphi(n)$, ou ainda, $ed \equiv 1 \pmod{\varphi(n)}$. Em segundo, precisamos fazer uso da expressão

$$D(a) \equiv a^d \pmod{n}, \tag{6.7}$$

onde a é um bloco codificado.

A congruência de (6.7) decodifica a mensagem codificada e por essa razão espera-se que $D(C(b)) = b$. Apesar de parecer bastante óbvio podemos encontrar uma demonstração em [4] de que a igualdade anterior sempre funciona. Vejamos um exemplo.

Exemplo 6.4.2 Decodificar a mensagem

$$80-16-102-119-81-98-7-98-116-44-16-91,$$

com $e = 11$ e $n = 133$.

Solução: Inicialmente, sabendo que $\varphi(133) = 108$ calculamos d tal que

$$11 \cdot d \equiv 1 \pmod{108}.$$

Daí, aplicando divisões sucessivas, temos:

$$\begin{cases} 108 &= 11 \cdot 9 + 9 \\ 11 &= 9 \cdot 1 + 2 \\ 9 &= 2 \cdot 4 + 1 \\ 2 &= 1 \cdot 2 + 0. \end{cases} \tag{6.8}$$

Logo, pelo Algoritmo Euclidiano, segue que $mdc(108,11) = 1$. Encontremos x e $y \in \mathbb{Z}$, tais que $1 = 108x + 11y$. Isso consistirá em isolar os restos não nulos das divisões de baixo para cima das igualdades em (6.8), substituindo-os sucessivamente. Temos,

$$\begin{aligned} 1 &= 9 - 4 \cdot 2 \\ &= 9 - 4 \cdot (11 - 9 \cdot 1) \\ &= 5 \cdot 9 - 4 \cdot 11 \\ &= 5 \cdot (108 - 9 \cdot 11) - 4 \cdot 11 \\ &= 108 \cdot 5 + 11 \cdot (-49). \end{aligned}$$

Logo, $x = 5$ e $y = -49$. Portanto, $d \equiv -49 \equiv 59 \pmod{108}$.

Usando a congruência $D(a) \equiv a^{59} \pmod{133}$, decodificaremos cada bloco da mensagem. Então,

$$\begin{aligned}
D(80) &\equiv 80^{59} \equiv 131 \pmod{133},\\
D(16) &\equiv 16^{59} \equiv 4 \pmod{133},\\
D(102) &\equiv 102^{59} \equiv 30 \pmod{133},\\
D(119) &\equiv 119^{59} \equiv 28 \pmod{133},\\
D(81) &\equiv 81^{59} \equiv 9 \pmod{133},\\
D(98) &\equiv 98^{59} \equiv 91 \pmod{133},\\
D(7) &\equiv 7^{59} \equiv 49 \pmod{133},\\
D(98) &\equiv 98^{59} \equiv 91 \pmod{133},\\
D(116) &\equiv 116^{59} \equiv 51 \pmod{133},\\
D(44) &\equiv 44^{59} \equiv 81 \pmod{133},\\
D(16) &\equiv 16^{59} \equiv 4 \pmod{133},\\
D(91) &\equiv 91^{59} \equiv 21 \pmod{133}.
\end{aligned}$$

Dessa forma, temos a seguinte mensagem decodificada:

$$131-4-30-28-9-91-49-91-51-81-4-21.$$

Fazendo a correspondência com a tabela de conversão para sequência de números, e observando que estamos lidando com números de apenas 2 algarismos, segue que

$$13-14-30-28-99-14-99-15-18-14-21,$$

corresponde a seguinte frase:

"DEUS É FIEL".

△

Observação 6.4.3 As congruências obtidas no processo de decodificação acima podem ser facilmente calculadas com o uso do Teorema de Euler e o Pequeno Teorema de Fermat.

O próximo exemplo é uma sugestão de atividade que consiste de uma sequência de etapas para trabalhar com grupos de alunos sobre o funcionamento do sistema RSA.

Exemplo 6.4.4 Considerando os números primos 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41 e 43 faça o seguinte:

(a) *Construa uma chave pública para você utilizar na codificação de mensagens RSA para seus colegas.*

(b) *Use a chave pública que você construiu no item (a) para codificar seu nome. Em seguida, escreva a chave e a mensagem em um papel. Os papéis deverão ser reunidos, embaralhados e distribuídos aleatoriamente entre os alunos para o próximo item.*

(c) *Fatore o valor de n da chave pública que você recebeu, calcule d e decodifique a mensagem para saber o seu remetente.*

Como vimos, a segurança do RSA é garantida pela dificuldade no processo de fatoração, mesmo do ponto de vista computacional. De fato, para decifrar uma mensagem criptografada pelo RSA conhecendo apenas n e e, é imprescindivelmente necessária a fatoração de n para o cálculo de $\varphi(n)$. Caso alguém possa obter $\varphi(n)$ a partir de n e e apenas, teria encontrado um algoritmo rápido para fatorar n. Isto é, quando fazemos uso de primos grandes como parâmetros para o RSA é inevitável a fatoração de n para descobrir d, sem o conhecimento de p e q. Além do mais, conhecendo d pode-se, por segurança, desfazer dos parâmetros p e q. Atualmente, o *RSA Laboratory* tem em aberto um desafio de fatorar uma chave de 617 dígitos decimais, a maior proposta, e obviamente sua fatoração está bem distante de ser realizada com os recursos atuais.

A escolha adequada dos primos é fundamental para garantir a segurança do método, pois se p e q são primos grandes, mas $|p-q|$ é pequeno, o sistema está comprometido pela Fatoração de Fermat. Também, deve-se ter atenção aos antecessores e sucessores dos primos escolhidos de modo que estes não tenham fatores primos pequenos que tornaria n facilmente fatorado por algoritmos conhecidos. Ainda vale ressaltar que para analisar se determinado número é primo, não necessariamente precisamos fatorá-lo.

6.5 Propostas de Aplicações ao Ensino Médio

Além dos exemplos criptográficos descritos anteriormente iremos propor algumas atividades que podem ser facilmente aplicadas em turmas de ensino médio envolvendo Criptografia e conceitos correlacionados. Primeiramente, é conveniente que o professor faça algumas explanações sobre Criptografia, como: conceito, métodos, história e algo mais que julgar necessário. O objetivo das propostas apresentadas a seguir é trabalhar com situações motivadoras que facilitem o processo ensino-aprendizagem de forma diferenciada aos educandos.

Proposta 1: Com o advento de novas tecnologias, temos atualmente uma grande atração dos estudantes para com a manipulação destas. No entanto, também devemos usar essas ferramentas atrativas para melhorar o aproveitamento no processo ensino-aprendizagem.

Com relação ao sistema RSA, sabemos que a garantia de segurança está relacionada com a dificuldade na fatoração do produto de dois números primos relativamente grandes. Assim, a escolha dos primos é primordial na segurança do RSA.

Vamos propor uma atividade que faz uso do *software* MAPLE, que pode ser adquirido em *www.maplesoft.com*. É uma ferramenta que pode aprofundar os conhecimentos adquiridos e acrescentar novos, conforme as diversas ferramentas matemáticas contidas neste programa. Nesta ocasião, iremos procurar números primos relativamente grandes, por exemplo, mais de 30 dígitos, com a finalidade de verificar uma chave adequada para o método RSA.

Inicialmente, podemos procurar os primos p e q, digitando um inteiro y qualquer, digamos de 30 algarismos, e efetuamos o comando

$$\text{“}isprime(y)\text{”},$$

o qual pergunta se o número y é primo. Caso a resposta seja negativa, efetuamos o comando

$$\text{“}nextprime(y)\text{”}$$

e o programa fornecerá o próximo primo.

Procedendo da maneira acima, encontraremos os primos p e q, para determinar $n = pq$. Para isto, podemos usar o MAPLE efetuando o comando de multiplicação $*$ e teremos n. Assim, para verificar se n é um número conveniente para o uso do RSA, basta usar o MAPLE com o comando

$$ifactor(n),$$

que efetua a decomposição em fatores primos do número n. Posteriormente a este comando, veremos que o MAPLE não dará uma resposta imediata, significando uma escolha bastante razoável na escolha dos primos p e q. Vale ressaltar que, quanto maior os primos escolhidos, maior será a dificuldade de fatoração e, consequentemente, um aumento na segurança do método RSA.

Proposta 2: As calculadoras são bastante eficientes no cálculo de algumas congruências, em especial nos exemplos de seções anteriores deste capítulo.

Nesta ocasião propomos o uso da *calculadora do windows 8*, acessível praticamente a maioria das escolas que possuem computadores com este sistema operacional. Com o uso desta ferramenta, podemos calcular potências com o uso da função “x^y” e ainda utilizar a função “mod” para determinar resíduos módulo m. Entre outras funções mais elementares, estas proporcionam uma grande agilidade nos cálculos de determinadas congruências.

Para cálculos ainda maiores como na solução do Exemplo 6.4.2, podemos fazer uso de *calculadoras online*, facilmente acessíveis a computadores conectados à *internet*. Como sugestão, podemos citar a calculadora disponível no endereço

`ptrow.com/perl/calculator.pl`,

que foi utilizada neste trabalho com a finalidade de simplificá-los. Essa ferramenta é de fácil manipulação e de comandos autoexplicativos.

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

Tabela 6.3: Tabela de conversão - Criptografia com funções invertíveis.

Com relação ao uso de calculadoras em sala de aula, trata-se de um tema ainda discutido que divide opiniões, mas a maioria dos livros didáticos do ensino básico geralmente traz atividades ligadas ao uso das mesmas.

Proposta 3: Esta proposta consiste no uso de funções invertíveis que serão chamadas de funções cifradoras. A mensagem original será pré-codificada e transformada em uma sequência numérica aleatória, ou seja, a mensagem é codificada através de uma função cifradora, podendo esta ser do tipo afim, exponencial ou logarítmica.

Para o processo de pré-codificação iremos adotar a Tabela 6.3 para convertermos os símbolos (letras sem sinais de acentuação gráfica) em números.

Contudo, é importante explicar que o processo de codificação, propriamente dito, é uma permutação de números através de uma regra $f : A \longrightarrow B$, em que $A = \{0, 1, ..., 25\}$ e B é um subconjunto de $\mathbb{Z}$ convenientemente escolhido.Para o processo de decodificação, o receptor deverá calcular as imagens de f^{-1}.

Como uma primeira situação, vamos utilizar a função afim $f(x) = 3x + 2$, chave de codificação, para codificar a mensagem

"JESUS E A SALVACAO".

Inicialmente, temos a seguinte pré-codificação:

$$9 - 4 - 18 - 20 - 18 - 4 - 0 - 18 - 0 - 11 - 21 - 0 - 2 - 0 - 14.$$

Codificando, de acordo a regra f, temos:

$$\begin{aligned}
f(9) &= 3\cdot 9+2 = 29,\\
f(4) &= 3\cdot 4+2 = 14,\\
f(18) &= 3\cdot 18+2 = 56,\\
f(20) &= 3\cdot 20+2 = 62,\\
f(18) &= 3\cdot 18+2 = 56,\\
f(4) &= 3\cdot 4+2 = 14,\\
f(0) &= 3\cdot 0+2 = 2,\\
f(18) &= 3\cdot 18+2 = 56,\\
f(0) &= 3\cdot 0+2 = 2,\\
f(11) &= 3\cdot 11+2 = 35,\\
f(21) &= 3\cdot 21+2 = 65,\\
f(0) &= 3\cdot 0+2 = 2,\\
f(2) &= 3\cdot 2+2 = 8,\\
f(0) &= 3\cdot 0+2 = 2,\\
f(14) &= 3\cdot 14+2 = 44.
\end{aligned}$$

Logo, temos a seguinte mensagem codificada:

$$29-14-56-62-56-14-2-56-2-35-65-2-8-2-44.$$

Para decodificar a mensagem o receptor deverá fazer uso da inversa de f, ou seja, a função $f^{-1}(x)=\dfrac{x-2}{3}$, chave de decodificação, para calcular a imagem de cada número codificado.

É importante ressaltar que, caso um usuário não autorizado intercepte uma mensagem codificada por uma função afim invertível, fica fácil decifrar a mensagem conhecendo apenas duas correspondências, que podem ser facilmente determinadas através da análise de frequências, e descobrir a lei de formação da função.

Consideremos, agora, a função exponencial $f(x)=3^x$ para codificar a mensagem

"AMO MEUS FILHOS".

Inicialmente vamos pré-codificar a mensagem. Assim, temos:

$$0-12-14-12-4-20-18-5-8-11-7-14-18.$$

Para codificar a mensagem pré-codificada acima, pode ser recomendado o uso da cal-

culadora em sala de aula, para simplificar os cálculos. Temos,

$$\begin{aligned}
f(0) &= 3^0 = 1,\\
f(12) &= 3^{12} = 531441,\\
f(14) &= 3^{14} = 4782969,\\
f(12) &= 3^{12} = 531441,\\
f(4) &= 3^4 = 81,\\
f(20) &= 3^{20} = 3486784401,\\
f(18) &= 3^{18} = 387420489,\\
f(5) &= 3^5 = 243,\\
f(8) &= 3^8 = 6561,\\
f(11) &= 3^{11} = 177147,\\
f(7) &= 3^7 = 2187,\\
f(14) &= 3^{14} = 4782969,\\
f(18) &= 3^{18} = 387420489,
\end{aligned}$$

Portanto, temos a seguinte mensagem codificada:

$$\begin{aligned}
1 &- 531441 - 4782969 - 531441 - 81\\
&- 3486784401 - 387420489 - 243 - 6561\\
&- 177147 - 2187 - 4782969 - 387420489.
\end{aligned}$$

Para decodificar a mensagem codificada acima, devemos fazer uso da inversa da função exponencial cifradora, ou seja, a função logarítmica $f^{-1}(x) = \log_3 x$.

Como exemplo de decodificação, vamos decodificar a mensagem

$$4096 - 16 - 262144 - 524288 - 131072 - 1 - 8 - 16384$$

cifrada pela a função $f(x) = 2^x$.

Primeiramente, consideremos a função inversa de f, isto é, a função logarítmica $f^{-1}(x) =$

$\log_2 x$. Em seguida, decodificaremos a mensagem calculando

$$\begin{aligned}
f^{-1}(4096) &= \log_2 4096 = 12,\\
f^{-1}(16) &= \log_2 16 = 4,\\
f^{-1}(262144) &= \log_2 262144 = 18,\\
f^{-1}(524288) &= \log_2 524288 = 19,\\
f^{-1}(131072) &= \log_2 131072 = 17,\\
f^{-1}(1) &= \log_2 1 = 0,\\
f^{-1}(8) &= \log_2 8 = 3,\\
f^{-1}(16384) &= \log_2 16384 = 14.
\end{aligned}$$

Logo, a mensagem original é

$$12-4-18-19-17-0-3-14$$

que fazendo a correspondência com a Tabela 6.3, significa

"MESTRADO"

A proposta de atividade acima pode ser aplicada em duplas ou grupos de alunos que possam interagir na troca de mensagens secretas e na tentativa de decifrá-las, reforçando o estudo sobre funções e, em especial, o conceito de função inversa.

Além do mais, podemos aplicar a ideia do uso de funções invertíveis para criptografar mensagens ao uso de matrizes invertíveis. Dessa forma, consideremos uma matriz invertível A, chave de codificação, e sua inversa B, a chave de decodificação. Para codificarmos uma matriz M efetuamos a operação de multiplicação entre as matrizes A e M. Enquanto, para realizar o processo de decodificação, basta multiplicar a matriz B pela matriz codificada N.

Observação 6.5.1 Para aplicação das situações propostas acima é necessário o conhecimento sobre funções, um conteúdo sempre presente no currículo do 1^o ano do ensino médio, assim como a função afim no 9^o ano do ensino fundamental de forma mais elementar. O estudo sobre matrizes é geralmente lecionado para alunos do 2^o ano do ensino médio.

6.6 Considerações Finais

Esperamos que este trabalho possa atingir os propósitos de fundamentação teórica e principalmente prática, no intuito de suprir as eventuais necessidades de contextualização de conteúdos curriculares nos níveis básicos de ensino, ressaltando a possibilidade de inserir

conceitos pertinentes à Teoria dos Números em níveis iniciais com aplicações básicas, sobretudo a Criptografia. Inclusive, recentes livros didáticos do ensino médio trazem seções voltadas a este tema, no estudo sobre Matrizes.

É necessária uma dedicação dos professores em buscar novos caminhos que proporcionem uma aprendizagem significativa. Com isso, a inserção dos conceitos e aplicações tratadas neste, podem auxiliar na busca de resultados mais proveitos no estudo de determinados assuntos.

Dessa forma, o trabalho pode eventualmente originar melhorias das práticas metodológicas de professores que venham colaborar com o surgimento de novas propostas aplicadas na base de ensino educacional, especificamente ao ensino de Matemática.

Referências Bibliográficas

[1] ANDRINI, A.; VASCONCELLOS, M. J. *Praticando Matemática*. 3^a ed. São Paulo, 2012.

[2] BONJORNO, J. R. et al. Matemática: Fazendo a diferença. 1^a ed. FTD, São Paulo, 2006.

[3] BRASIL. Secretaria de Educação Fundamental. *Parâmetros Curriculares Nacionais*: 3^o e 4^o ciclos do Ensino Fundamental. Matemática. Brasília, MEC/SEF, 1998.

[4] COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. 2^a ed. Rio de Janeiro, IMPA, 2014.

[5] COUTINHO, S. C. *Introdução à Criptografia I*. Apostila Profmat, 2011.

[6] DAINEZE, .A. L. *Números Primos e Criptografia: da Relação com a Educação ao Sistema RSA*. Dissertação (Mestrado Profissional em Matemática em Rede Nacional). UFRRJ, Seropédica-RJ, 2013.

[7] DICIONÁRIO ONLINE - *Dicionários Michaelis - UOL*. Disponível em: <http://michaelis.uol.com.br>. Acesso em: 05 de agosto de 2014.

[8] ENEM 2014 - Exame Nacional do Ensino Médio. INEP-Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira. Ministério da Educação. *Edital Enem 2014*. Disponível em: <http://www.enem.inep.gov.br/download.html>. Acessado em agosto de 2014.

[9] EUCLIDES. *Os elementos/Euclides*; tradução e introdução de Irineu Bicudo. UNESP, São Paulo, 2009.

[10] FINCATTI, C. A. *Criptografia como Agente Motivador na Aprendizagem da Matemática em Sala de Aula*. Monografia (Licenciatura em Matemática). UPM, São Paulo, 2010.

[11] GIMPS: *Great Internet Mersenne Prime Search*. Disponível em: <www.mersenne.org>. Acesso em: 06 de agosto de 2014.

[12] HEFEZ, A. *Elementos de Aritmética*. 2^a ed. Rio de Janeiro, SBM, 2011.

[13] MARTINEZ, F. B. et al. *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro*. 3^a ed. Rio de Janeiro, IMPA, 2013.

[14] NASCIMENTO, M. C.; FEITOSA, H. A. *Elementos da Teoria dos Números.* UNESP, São Paulo, 2013.

[15] OBMEP - *Olimpíada Brasileira de Matemática das Escolas Públicas*. Disponível em: <www.obmep.org.br>. Acessado em 06 de agosto de 2014.

[16] OLIVEIRA, M. C. *Aritmética: Criptografia e outras Aplicações de Congruências.* Dissertação (Mestrado Profissional em Matemática em Rede Nacional). UFMS, Campo Grande-MS, 2013.

[17] PEDROSA, A. C. P. et al. *GTA/UFRJ*. Disponível em: <www.gta.ufrj.br>. Acesso em: 15 de maio de 2014.

[18] PIMENTEL, F. R. *Teorida dos Números*. Apostila. UFOP, Ouro Preto-MG, 2005.

[19] SHOKRANIAN, S. *Criptografia para Iniciantes*. 2^a ed. Rio de Janeiro, Editora Ciência Moderna Ltda, 2012

[20] SINGH, S. *O Livro dos Códigos*. Rio de Janeiro, Record, 2001.

[21] SOMATEMATICA. *Só matemática*. Disponível em: <www.somatematica.com.br>. Acesso em: 05 de setembro de 2014.

[22] VIEIRA, V. L. *Álgebra Abstrata para Licenciatura.* Editora da Universidade Estadual da Paraíba (Co-edição: Livraria de Física da USP), Campina Grande/São Paulo, 2013.