UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE CIÊNCIAS NATURAIS E EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

Anderson Pinheiro Machado

TEORIA DOS NÚMEROS E CRIPTOGRAFIA RSA: UMA PROPOSTA DE ENSINO PARA ALUNOS DE MATEMÁTICA OLÍMPICA

Santa Maria, RS
2018

Anderson Pinheiro Machado

TEORIA DOS NÚMEROS E CRIPTOGRAFIA RSA: UMA PROPOSTA DE ENSINO PARA ALUNOS DE MATEMÁTICA OLÍMPICA

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional - PROFMAT, da Universidade Federal de Santa Maria (UFSM, RS) como requisito parcial para obtenção do grau de **Mestre em Matemática**.

Orientador: Prof. Dr. João Roberto Lazzarin

Santa Maria, RS
2018

Machado, Anderson Pinheiro
Teoria dos Números e Criptografia RSA: uma proposta de ensino para alunos de matemática olímpica / Anderson Pinheiro Machado.- 2018.
93 p.; 30 cm

Orientador: João Roberto Lazzarin
Dissertação (mestrado) - Universidade Federal de Santa Maria, Centro de Ciências Naturais e Exatas, Programa de Pós-Graduação em Matemática em Rede Nacional, RS, 2018

1. Criptografia RSA 2. Proposta de Ensino 3. Olimpíadas de Matemática 4. Aritmética Modular 5. Pensamento Matemático I. Lazzarin, João Roberto II. Título.

Sistema de geração automática de ficha catalográfica da UFSM. Dados fornecidos pelo autor(a). Sob supervisão da Direção da Divisão de Processos Técnicos da Biblioteca Central. Bibliotecária responsável Paula Schoenfeldt Patta CRB 10/1728.

Anderson Pinheiro Machado

TEORIA DOS NÚMEROS E CRIPTOGRAFIA RSA: UMA PROPOSTA DE ENSINO PARA ALUNOS DE MATEMÁTICA OLÍMPICA

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional - PROFMAT, da Universidade Federal de Santa Maria (UFSM, RS) como requisito parcial para obtenção do grau de **Mestre em Matemática**.

Aprovado em 24 de agosto de 2018:

João Roberto Lazzarin, Dr. (UFSM)
(Presidente/orientador)

Ana Marli Bulegon, Dra. (UFN)

Pedro Fusieger, Dr. (UFSM)

Santa Maria, RS
2018

DEDICATÓRIA

Para minha esposa, Jussânia Maciel Fortunato, incansável companheira, amiga dedicada e parte fundamental em minha vida. Com ela sempre tive o apoio, o carinho e o amor incondicional do qual sempre lembrarei. Espero ser minimamente digno em retribuir.

AGRADECIMENTOS

Agradeço a Deus que sempre iluminou minha jornada até aqui, tornando o caminho mais fácil onde muitos, de igual esforço e dedicação, falharam em seus objetivos.

A minha esposa, por sua compreensão, apoiando de todas as formas possíveis e estando ao meu lado nos momentos em que mais precisei. Ela me motiva a ser uma pessoa melhor.

Aos meus pais, José Dilson Machado e Zilca Pinheiro Machado, que sempre foram meu referencial moral, seja pelo caráter, seja pela honestidade de ambos. São fonte de amor e repouso em tempos difíceis, dos quais sempre pude contar.

Ao meu irmão, Marcio Pinheiro Machado, responsável por todo o apoio logístico em minhas viagens para Santa Maria. Eu deveria fazer mais do que simplesmente agradecer a alguém que, muitas vezes cansado, nunca negou ajuda, nem reclamou. Ele não sabe, mas nasceu para servir.

Ao Prof. Dr. João Roberto Lazzarin, pelo direcionamento e sábios conselhos, conduzindo este trabalho de maneira muito serena e tranquila, além das excelentes aulas na disciplina de Aritmética, parte da motivação que culminou em sua escolha como orientador.

A todos os professores do PROFMAT, em especial ao Prof. Dr. Denílson Gomes e à Profª. Dra. Cláudia Candida Pansonato, por ter tido o privilégio de ser novamente aluno de ambos, sendo a primeira vez na graduação.

À Sociedade Brasileira de Matemática (SBM) pela criação deste curso e à Coordenação de Matemática da UFSM, por acreditar na proposta do PROFMAT.

Ao Colégio Militar de Porto Alegre (CMPA), pelas concessões que permitiram, por meio de meus comandantes, o desenvolvimento de minha capacitação. Por muitas vezes, necessitei do amparo de colegas e chefes, dos quais nomino o Tenente Coronel Marcelo Moraes Machado, o Major Denilson Amaral Nolibos, a Profª. Dra. Josaine de Moura Pinheiro e o Prof. Ms. Alexandre Leiria Machado.

A todos os colegas da turma PROFMAT 2016, pelo companheirismo. Compartilhamos não somente estudo, mas também expectativas e anseios sobre os diversos processos de avaliação aos quais éramos submetidos.

A todos familiares, amigos e colegas de trabalho que, mesmo indiretamente, contribuíram para a realização deste trabalho.

RESUMO

TEORIA DOS NÚMEROS E CRIPTOGRAFIA RSA: UMA PROPOSTA DE ENSINO PARA ALUNOS DE MATEMÁTICA OLÍMPICA

AUTOR: Anderson Pinheiro Machado
ORIENTADOR: João Roberto Lazzarin

Este trabalho traz uma proposta de ensino de Criptografia RSA para uma turma de alunos de 8º e 9º anos do Ensino Fundamental, voluntários em um Clube de Matemática do Colégio Militar de Porto Alegre (CMPA). Grande parte dos discentes desta turma são medalhistas frequentes em Olimpíadas de Matemática, mas todos compartilham da facilidade e da curiosidade em resolver desafios. Estes alunos, mesmo sem nenhuma aversão à Matemática e, apresentando raciocínio acima da média, questionavam o uso prático de ferramentas da Teoria dos Números, bem como o estudo de números primos e da Aritmética Modular, ao contrário de outras áreas como Geometria e Álgebra. Com o objetivo de apresentar uma aplicação adequada para o nível da turma, criou-se uma sequência de treze aulas sobre o tema Criptografia RSA que incluía desde uma visão geral sobre a história e o uso de métodos criptográficos simples, até os pré-requisitos necessários para entender o funcionamento do RSA, onde a Aritmética Modular, o cálculo de inversos multiplicativos e a função de Euler são parte fundamental deste processo. Destaca-se que o RSA é um método criptográfico utilizado em compras *online* e transações bancárias que, juntamente com o caráter histórico e o desafio de decifrar mensagens, tornou-se naturalmente atraente aos alunos. Durante todas as aulas, foram utilizadas questões de Olimpíadas de Matemática e de outros concursos, agregando discussões aprofundadas, conjecturando resultados e permitindo pequenas demonstrações que auxiliavam no desenvolvimento do pensamento e do raciocínio matemático. Em momentos oportunos, também se fez uso de aplicativos para *smartphone* e *softwares* associados à Criptografia. Concluiu-se um resultado satisfatório tendo em vista o retorno dado pelos alunos (registrado em forma de questionário) e as novas possibilidades que contribuirão ainda mais com a formação deste professor.

Palavras-chave: Criptografia RSA. Proposta de Ensino. Olimpíadas de Matemática. Aritmética Modular. Pensamento Matemático.

ABSTRACT

THEORY OF NUMBERS AND RSA CRYPTOGRAPHY: A TEACHING PROPOSAL FOR STUDENTS OF OLYMPIC MATHEMATICS

AUTHOR: ANDERSON PINHEIRO MACHADO
ADVISOR: JOÃO ROBERTO LAZZARIN

This work presents a teaching proposal of RSA Cryptography for a group of 8th and 9th grade students of Elementary School, volunteers in a Mathematics Club from Colégio Militar de Porto Alegre (CMPA). Most of the students in this class are frequent medalists in Mathematical Olympiads, but they all share the ease and curiosity in solving challenges.These students, even without any aversion to Mathematics, and presenting above-average reasoning, questioned the practical use of Number Theory tools, as well as the study of prime numbers and Modular Arithmetic, unlike other areas such as Geometry and Algebra. In order to present an application suitable for the class level, was created a sequence of thirteen classes on the subject of RSA Cryptography which included an overview of history and the use of simple cryptographic methods, up to the prerequisites necessary to understand the operation of the RSA, where the Modular Arithmetic, the calculation of multiplicative inverses and the Euler function are fundamental part of this process. It should be noted that RSA is a cryptographic method used in online shopping and banking transactions which, together with the historical character and the challenge of deciphering messages, has become naturally attractive to students. During all classes, were used questions Mathematical Olympiad and other competitions, aggregating in-depth discussions, conjecturing results and allowing small demonstrations that aided in the development of thinking and mathematical reasoning. At appropriate times, it was also made use of applications for smartphones and software associated with Cryptography. A satisfactory result was obtained in view of the students' return (registered in shape of questionnaire) and the new possibilities that will contribute even more to the formation of this teacher.

Keywords: Cryptography RSA. Teaching Proposal. Mathematical Olympiads. Modular Arithmetic. Mathematical Thinking.

SUMÁRIO

1 INTRODUÇÃO

Em uma sociedade que questiona cada vez mais o papel da Educação e as formas tradicionais de aprendizagem, surge a necessidade de um ensino dinâmico e atento às expectativas e anseios de formar não somente profissionais capacitados, mas também cidadãos criativos e conscientes. Neste sentido, torna-se importante fornecer, além de uma educação global e de qualidade, ferramentas que potencializem os talentos e particularidades de cada aluno, permitindo o contato com diferentes formas de conhecimento, ao mesmo tempo que seja possível explorar e aprimorar os interesses de cada discente. Diante disto, a Escola, ciente de sua função, deve buscar constante desenvolvimento de seu projeto pedagógico, visando amplo atendimento e eficiência ao trabalhar propostas e metodologias de ensino edificantes e atraentes.

Com este objetivo, o Sistema Colégio Militar do Brasil (SCMB), do qual faço parte como professor, preocupa-se em disponibilizar atividades extracurriculares no contraturno do que é considerado ensino regular, visando desenvolver e complementar habilidades específicas que vão ao encontro dos interesses dos alunos. No caso particular do Colégio Militar de Porto Alegre (CMPA) as opções são diversas: Clube de Matemática, Clube de Astronomia, Clube de Robótica, Clube de Latim, Xadrez, Coral e música, além de muitas atividades esportivas, sendo a adesão a estas atividades sempre voluntária.

Assim, os estudantes que participam do Clube de Matemática podem ser considerados mais aptos, sendo que muitos dos alunos participantes são medalhistas frequentes em olimpíadas. Não por acaso, o principal motivo pela escolha deste clube é a preparação para Olimpíadas de Matemática, notavelmente a Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP), a Olimpíada Brasileira de Matemática (OBM) e concursos militares, como a Escola Preparatória de Cadetes do Ar (EPCAr) e o Colégio Naval. Embora estas provas possuam propostas distintas, todas são reconhecidas pelo elevado nível de exigência, sempre com questões interessantes e desafiadoras.

As aulas do Clube de Matemática são divididas em níveis que seguem o mesmo padrão estabelecido pela OBMEP e OBM: 6º e 7º anos do Ensino Fundamental formam o nível 1; 8º e 9º anos do Ensino Fundamental formam o nível

2; Ensino Médio compõe o nível 3. Destes, sou professor dos níveis 1 e 2. As aulas são divididas em "minicursos" sobre assuntos específicos, como "Geometria Olímpica" e "História da Matemática", por exemplo. Como o efetivo é menor do que o ensino regular, além de diferenciado pelas suas altas habilidades e interesse, os resultados costumam ser bem positivos.

Sendo professor de um público de alunos tão especial, as possibilidades eram diversas, assim como os desafios. Além disso, a experiência de ministrar aulas pelo terceiro ano consecutivo no Clube de Matemática, fez com que os acertos fossem mantidos, dentre eles, a criação de um bom material sobre os temas tratados, conciliando teoria e prática, complementada com exercícios que iam de básicos a desafiadores. Um bom material ajudou a manter o foco, organizando o estudo dos alunos, que deram um bom retorno ao trabalho feito.

A produção de material conciso, que atendesse as necessidades e expectativas dos alunos nas áreas de Geometria e Combinatória, por exemplo, não era problema, pois a contextualização sempre norteou questões da OBMEP e de outros concursos.

Eis que aqui surge uma inquietação: quando o tema proposto era Teoria dos Números, sempre havia o questionamento dos alunos sobre aplicações e a importância deste estudo. Eram comuns perguntas tais como: "Por que tanto interesse em estudar números primos?", "Sim, eu entendo aritmética modular, mas qual é a necessidade de encontrar restos de números tão grandes?". "Para que tanto esforço e pesquisa matemática nesta área?"

A inquietude causada por tais questionamentos não estava relacionada à alguma dificuldade de ensinar técnicas básicas de Aritmética ou no fraco desempenho por parte dos alunos no entendimento dos conceitos e ideias, muito menos de dirimir alguma aversão à Matemática, afinal tratavam-se de alunos com gosto pela disciplina e facilidade em resolver problemas. O desafio era encontrar aplicações palatáveis para o público em questão, e que dessem respostas satisfatórias a tais questionamentos.

E aqui surge uma proposta de ensino de Criptografia RSA - sigla oriunda das iniciais de seus criadores, Ron Rivest, Adi Shamir e Leonard Adleman. Este tipo de

criptografia, conforme será visto neste trabalho, é do tipo assimétrica, e utiliza resultados de Aritmética Modular em seu funcionamento. Assim, com o objetivo de construir uma proposta de ensino viável para este seleto grupo – alunos de 8º e 9º anos do Ensino Fundamental, participantes de um Clube de Matemática – necessitava-se não somente explorar conceitos e ferramentas de Teoria dos Números, mas também uma noção básica de Criptografia geral.

O tema criptografia é naturalmente atraente, seja pela ideia de decifrar ou codificar mensagens ou pela questão histórica em si. Outro ponto agregador é a possibilidade do uso de tecnologia, com *softwares* e aplicativos que permitam maior interação entre os alunos. A boa quantidade de *softwares* e aplicativos reafirma sua importância e utilidade em processos cotidianos. Mesmo para alunos que apresentam facilidade e interesse em Matemática, o estudo da Criptografia mostra-se amplo e motivador. Particularmente, o emprego da Criptografia RSA é bem atual, sendo utilizada desde transações bancárias até compras *online*, colaborando na busca por uma aplicação que chame atenção dos discentes.

No desenvolvimento desta proposta de ensino, percebeu-se uma excelente oportunidade de discussão sobre a construção do pensamento matemático e a importância da pesquisa. Parte desta possibilidade surgiu da decisão de usar questões de olimpíadas de matemática (um interesse comum dos alunos deste clube) e observar que grande parte das mesmas permitiam esta discussão, trazendo conjecturas e propondo pequenas demonstrações, adequadas ao nível.

Finalmente, a Criptografia RSA é um bom exemplo de que estudar Matemática desassociada de um problema prático pode ser crucial para o desenvolvimento de novas tecnologias, pois todas as ferramentas teóricas já tinham sido desenvolvidas antes mesmo do surgimento das primeiras criptografias assimétricas. Isso correspondia às expectativas dos alunos que, ao demonstrarem talento em Matemática, já aspiravam uma carreira acadêmica em ciências exatas como possibilidade futura.

Então, com o objetivo de aplicar uma proposta de ensino de Criptografia RSA, estruturou-se esta dissertação: o Capítulo 2 traz alguns conceitos básicos de Criptografia, além de um breve histórico; o Capítulo 3 trata da fundamentação

matemática necessária para entender o funcionamento do método RSA. Dando continuidade, o Capítulo 4 traz um exemplo de aplicação do RSA em si, além de uma discussão sobre sua segurança. Por fim, o Capítulo 5 apresenta a proposta de ensino propriamente dita, seguida de uma Conclusão. Ainda compondo a Introdução, tem-se os objetivos (geral e específicos) e uma fundamentação pedagógica.

1.1 OBJETIVOS

1.1.1 Objetivo geral

Apresentar a Criptografia RSA como uma aplicação da Teoria dos Números, desenvolvendo-a de maneira compatível com o nível dos alunos, discentes de 8º e 9º anos do Ensino Fundamental voluntários em um Clube de Matemática.

1.1.2 Objetivos específicos

Visando o entendimento do método de Criptografia RSA e de seu funcionamento, pretende-se:

a) Apresentar conceitos básicos de Criptografia, bem como métodos criptográficos simples, além de uma abordagem sobre curiosidades e fatos históricos sobre esta ciência e sua modernização, de uso indispensável na atualidade.

b) Construir a base teórica necessária para aplicação e compreensão da Criptografia RSA, com ênfase na Aritmética Modular e no cálculo de inversos multiplicativos, fixando o conhecimento a partir de questões de nível básico até desafios olímpicos.

c) Propiciar um ambiente de investigação em sala de aula, destacando a importância da pesquisa e do pensamento matemático, conjecturando e demonstrando alguns resultados ligados à Teoria dos Números.

d) Fazer uso de aplicativos e *softwares* relacionados à Criptografia e determinação de restos de potências, comparando com “técnicas manuais” de codificação e cálculo.

1.2 FUNDAMENTAÇÃO PEDAGÓGICA

Conhecer bem os alunos e o potencial dos mesmos é uma vantagem na elaboração de uma proposta de ensino. Entre os quinze alunos participantes, a maioria já possuía algum conhecimento sobre Aritmética Modular, que aparece com frequência em gabaritos oficiais de concursos militares de ensino fundamental e como alternativa na resolução de questões olímpicas destinadas aos 8º e 9º anos do Ensino Fundamental (exemplos podem ser vistos na Seção 5.8).

No entanto, é preciso nivelar este aprendizado e certificar-se de que todos tenham uma correta compreensão e domínio das ferramentas necessárias em Aritmética. Estas, são relativamente simples e perfeitamente possíveis de serem ensinadas para este nível. O desafio, então, é saber dosar teoria e prática, sem perder o foco.

De fato, esta proposta de ensino parte do princípio que a contextualização propiciada pela Criptografia, juntamente do uso de tecnologia, são os fatores motivadores; já a estrutura de sequência didática, ministrada como um “minicurso” para os alunos, permite, além do aprendizado de uma aplicação, um aprofundamento e construção do pensamento matemático.

Sem dúvida, a construção do pensamento matemático é muito importante: conjecturar resultados e dispor de ferramentas para garantir a validade dos mesmos, ou mesmo usar de raciocínio a partir de resultados básicos é um dos objetivos do ensino no país, como destacado pelos Parâmetros Curriculares Nacionais (PCN):

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

Moran, Masetto e Behrens (2000, p. 28) acrescentam que: “Avançaremos mais se soubermos adaptar os programas previstos às necessidades dos alunos, criando conexões com o cotidiano, com o inesperado, se transformamos a sala de aula em uma comunidade de investigação”.

Ainda sobre investigação matemática, Ponte, Brocardo e Oliveira (2009, p. 23) trazem que:

> O conceito de investigação matemática, como atividade de ensino-aprendizagem, ajuda a trazer para a sala de aula o espírito da atividade matemática genuína, constituindo, por isso, uma poderosa metáfora educativa. O aluno é chamado a agir como um matemático, não só na formulação de questões e conjecturas e na realização de provas e refutações, mas também na apresentação de resultados e na discussão e argumentação com os seus colegas e o professor.

Por outro lado, trazer uma aplicação para sala de aula pode consolidar definições, cálculos e todo a estrutura do conteúdo em questão. Neste sentido, contextualizar pode ser compreendido como transpor um conhecimento para outros contextos, verificando o real aprendizado (ou não) do discente.

Micotti (1999, p. 154) afirma que “a aplicação do aprendizado em contextos diferentes daqueles que foram adquiridos exige muito mais que a simples decoração ou a solução mecânica de exercícios”. Os PCN (BRASIL, 1998, p. 36) também abordam a contextualização de maneira semelhante: “mesmo no ensino fundamental, espera-se que o conhecimento aprendido não fique indissoluvelmente vinculado a um contexto concreto e único, mas que possa ser generalizado, transferido a outros contextos”. Por fim, Lorenzato (2010, p. 63) acrescenta que “ensinar matemática utilizando-se de suas aplicações torna a aprendizagem mais interessante e realista (...)”.

Sobre as vantagens do uso de recursos tecnológicos, Moran, Masetto e Behrens (2000, p. 102) discutem que:

> O apelo atrativo da tecnologia da informação pode propiciar caminhos de criação, iniciativa e autonomia, e esse fator motivador deve ser valorizado. Além do valor da informação que o aluno acessou, está o caminho que tomou para buscar na rede as informações necessárias para responder aos problemas propostos que venham desencadear a aprendizagem. O fato de poder publicar e disponibilizar a produção individual e coletiva do conhecimento dos alunos e do grupo cria um ambiente de atração e estímulo.

Porém, se é inegável que a tecnologia possui efeito magnético em nossos alunos, sendo parte constante na realidade dos mesmos, acredita-se que seu uso só tem sentido se proporcionar algum tipo de discussão, inferência ou comparação.

Quando os alunos compreendem as ideias, alguns *softwares* podem ser usados livremente, abrindo espaço para outros questionamentos. Nesta linha de raciocínio, Bettega (2010, p. 18) complementa que “a tecnologia deve servir para enriquecer o ambiente educacional, propiciando a construção de conhecimentos por meio de uma atuação ativa, crítica e criativa por parte de alunos e professores”.

Finalmente, Teixeira e Passos (2013, p. 162) definem:

> Uma sequência didática é uma série de situações que se estruturam ao longo de uma quantidade pré-fixada de aulas. Devidamente estruturadas, essas situações têm como objetivo tornar possível a aquisição de saberes bastante claros, sem esgotar o assunto trabalhado.

Assim, acredita-se que os objetivos de uma proposta de ensino só podem ser cumpridos frente à organização e construção de uma sequência didática adequada. Baseado nesta premissa, considerou-se bastante oportuna a elaboração de uma apostila que serviu de material de apoio e que fundamentou todas as etapas de um minicurso executado em treze aulas (a proposta de ensino apresentada no Capítulo 5). Nela, buscou-se conciliar a contextualização da Criptografia com a investigação matemática no intuito de compreender o funcionamento do RSA (discutido na Subseção 4.2.1).

2 CRIPTOGRAFIA: HISTÓRICO E CONCEITOS PRELIMINARES

2.1 PRIMEIROS CONCEITOS

Segundo Hefez (2014, p. 310), a palavra criptografia origina-se do grego, onde *kriptos* significa oculto e, portanto, a palavra criptografia significa "escrita oculta".

O desenvolvimento da criptografia está associado com a história da humanidade, pois desde as primeiras guerras, há milhares de anos, reis e rainhas, generais e diplomatas já entendiam que certas informações não poderiam ser de conhecimento de todos. Era preciso criar métodos seguros de comunicação, de tal maneira que apenas o emissor de uma mensagem e o receptor da mesma pudessem compreender o que queria ser dito. Uma mensagem, caso caísse nas mãos do inimigo, não deveria fazer sentido para este, que ao tentar desvendá-la, fracassaria, seja pela complexidade ou pela falta de tempo hábil.

Assim, todo processo criptográfico só faz sentido se puder ser desfeito, voltando à mensagem original. Por isso, muitos métodos de criptografia fazem uso de uma chave. Esta chave deve ser de conhecimento apenas do emissor e do receptor da mensagem; secreta aos demais. Diz-se, então, que o emissor cifra (codifica) a mensagem e que o receptor, usando a chave secreta, decifra (decodifica) o texto cifrado, obtendo a mensagem original.

Portanto, tem-se de um lado a Criptografia, a ciência que busca ocultar o verdadeiro significado de uma informação; do outro lado existe a Criptoanálise, a ciência que busca deduzir a informação original a partir de um texto cifrado (codificado), porém sem o conhecimento da chave secreta. Englobando ambas, Criptografia e Criptoanálise, define-se a Criptologia.

Aliás, muitas ideias e desenvolvimento tecnológico partiram da disputa entre criptógrafos, cujo objetivo é criar métodos seguros e eficientes de proteger uma informação, e criptoanalistas, dispostos a "quebrar" os códigos criados. Vários são os fatos históricos e curiosidades envolvendo a Criptologia, dos quais cita-se a Máquina Enigma (ver Apêndice A), o Telegrama Zimmermann (ver Apêndice B) e as Cifras de Beale (ver Apêndice C). Para uma leitura mais completa sobre o caráter histórico da Criptologia, recomenda-se Singh (2001).

2.1.1 Cifra de transposição e cifra de substituição

Carneiro (2017, p. 4) define que a criptografia tradicional pode ser dividida em dois ramos: transposição e substituição. Na transposição, as letras da mensagem são simplesmente rearranjadas (embaralhadas) criando anagramas. Por exemplo: a palavra RSA possui seis anagramas distintos: RSA, RAS, SRA, SAR, ARS e ASR. Porém, com uma noção mínima de combinatória, percebe-se que quanto maior a mensagem, maiores são as possibilidades de anagramas distintos. Uma palavra relativamente curta, como Aritmética, por exemplo, possui 453600 anagramas possíveis. Imagine um texto inteiro.

Isto cria uma boa dose de segurança, pois seriam muitas possibilidades a serem testadas pelo criptoanalista. Por outro lado, alguns destes anagramas podem ser mais sugestionáveis que outros. Além disso, como o receptor irá decodificar a mensagem? O exemplo abaixo ilustra o funcionamento de um tipo de **cifra de transposição**.

Exemplo 1. Suponha que se queira cifrar a mensagem "EU ESTUDO ARITMÉTICA". Uma maneira de fazê-la é que emissor e receptor convencionem uma chave. Escolheu-se LIVRO como chave, o que resultou na criação do Quadro 1 abaixo:

Quadro 1 - Exemplo de cifra de transposição.

ORDEM	**2**	**1**	**5**	**4**	**3**
CHAVE	**L**	**I**	**V**	**R**	**O**
MENSAGEM ORIGINAL	E	U	E	S	T
	U	D	O	A	R
	I	T	M	E	T
	I	C	A	#	#

Fonte: o autor.

No Quadro 1, o número 21543 é a ordem alfabética que as letras ocorrem dentro da palavra LIVRO: I é a primeira letra; L é a segunda, O é a terceira, R a quarta e V a quinta. A mensagem "EU ESTUDO ARITMÉTICA" é escrita linha após linha. Observa-se ainda a utilização do caractere # para completar o quadro. A cifra

é obtida lendo as colunas na ordem numérica. Assim, suprimindo os espaços e acento, EUESTUDOARITMETICA resulta em UDTCEUIITRT#SAE#EOMA.

Por outro lado, alguém que quisesse decifrar a mensagem UDTCEUIITRT#SAE#EOMA e conhecesse a palavra-chave LIVRO, poderia construir outro quadro (cujo resultado será idêntico ao Quadro 1); porém o receptor deve levar em conta quantas linhas devem ser criadas. Para isto, observa que UDTCEUIITRT#SAE#EOMA possui 20 caracteres e a palavra-chave possui 5 letras. Logo, devem ser criadas $\frac{20}{5} = 4$ linhas. Depois disto, divide a mensagem em blocos de quatro caracteres, UDTC, EUII, TRT#, SAE#, EOMA dispondo-os nas colunas da ordem 21543.

Uma alternativa para a transposição é a substituição. A **cifra de substituição** consiste em trocar uma letra ou conjunto de letras por outras letras, símbolos ou números, como no exemplo abaixo.

Exemplo 2. Coutinho (2014, p. 2) traz informações sobre o imperador romano Júlio César, que utilizava uma técnica de cifra por substituição que mais tarde ficou conhecida por seu nome: Cifra de César. Com ela, mensagens ao campo de batalha eram repassadas, distraindo o inimigo. A ideia é usar um alfabeto cifrado, deslocado um determinado número de casas em relação ao alfabeto original. No Quadro 2, tem-se um alfabeto deslocado três casas.

Quadro 2: Exemplo de alfabeto cifrado.

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

J	M	W	Z
K	N	X	A
L	O	Y	B
M	P	Z	C

Fonte: o autor.

Utilizando o alfabeto cifrado do Quadro 2, uma frase como "ATAQUE AO AMANHECER, PREPARE A TROPA" ficaria DWDTXHDRDPDQKHFHUSUHSDHDWURSD, onde foram suprimidos espaços e pontuação.

Ainda que este tipo cifra seja muito simples, foi muito eficiente na época de Júlio César. Tanto que foi adotada muitos anos depois, na Guerra Civil americana, conforme traz Singh (2001, p. 144). Eram utilizados discos concêntricos, como os da Figura 1, contendo todas as letras do alfabeto.

Figura 1 - Discos concêntricos.

Fonte: Disponível em: < https://www.amazon.com/Classic-Caesar-Cipher-Medallion Decoder/dp/B004D1L0B0>. Acesso em 21 fev. 2018.

Segundo Carneiro (2017, p. 7), aprimoramentos de cifras como a de César são conhecidas como **Cifras de Substituição Monoalfabética**. Por muitos anos, foram largamente utilizadas e consideradas praticamente inquebráveis (pelo menos em tempo hábil). Porém, conforme a humanidade foi elevando seu nível de conhecimento em diversas áreas como estatística e linguística, por exemplo, os

criptoanalistas ganharam ferramentas adequadas para "quebrar" este tipo de cifra. Surge então a análise de frequências.

Dentro de cada idioma, as letras do alfabeto utilizado podem aparecer com maior ou menor frequência. Na Língua Portuguesa, esta frequência, em porcentagem, é mostrada no Quadro 3.

Quadro 3 - Frequência das letras na Língua Portuguesa.

Letra	%	Letra	%	Letra	%	Letra	%
A	14,64	G	1,30	N	5,05	T	4,34
B	1,04	H	1,28	O	10,73	U	4,64
C	3,88	I	6,18	P	2,52	V	1,70
D	4,10	J	0,40	Q	1,20	X	0,21
E	12,57	L	2,78	R	6,53	Z	0,47
F	1,02	M	4,75	S	7,81		

Fonte: (COUTINHO, 2014, p.3).

Ou seja, no contato com um texto cifrado usando substituição monoalfabética, o símbolo que aparece com maior frequência provavelmente será a letra "A". As vogais aparecem mais que as consoantes; além disso, em nosso idioma é comum o uso de dígrafos (NH, LH, SS, RR, por exemplo) que funcionam como "dicas" aos criptoanalistas. Em resposta, os criptógrafos criaram melhorias para as cifras de substituição monoalfabética, como escrever deliberadamente uma mensagem com ortografia incorreta (porém sem perder o sentido original) ou acrescentar caracteres nulos no texto.

Os caracteres nulos não possuíam correspondente no alfabeto original, servindo de distração ao criptoanalista, mas eram de conhecimento do receptor, que sabia que deviam ser ignorados. Mesmo assim, para um criptoanalista experiente, não costumavam ser obstáculo suficiente.

Os Exemplos 1 e 2 desta seção são considerados métodos de **criptografia simétrica**, isto é, quando a chave usada para decodificar é a mesma que é usada para a codificação da mensagem original. Existem outros diversos métodos de criptografia simétrica como o Atbash, a Cerca de Ferrovia e a Cifra de Vigenère, cujo funcionamento é explicado, respectivamente, nos Apêndices D, E e F.

2.2 MODERNIZAÇÃO DA CRIPTOGRAFIA

As formas de criptografia apresentadas até agora são antigas, eficientes para a época, mas muito vulneráveis à criptoanálise de um computador. Aliás, com o desenvolvimento da tecnologia, a criptografia precisou tomar outros rumos. Não eram apenas mensagens trocadas entre governos e militares, por exemplo, que precisavam ser protegidas. Todo mundo, ao mandar *e-mails*, fazer compras na *internet* ou usar de cartão de crédito, precisa de segurança nestas ações, fazendo uso (mesmo que não saibam) de técnicas de criptografia moderna em seu dia-a-dia.

Já na década de 1960, com a popularização dos computadores, começaram a surgir problemas, tanto na padronização de qual sistema de criptografia deveria ser adotado, quanto na distribuição de chaves.

Como dito anteriormente, os exemplos descritos na Subseção 2.1.1, utilizam o conceito de criptografia simétrica. Na teoria moderna de criptografia, a ideia é justamente oposta, ao introduzir o **conceito de criptografia assimétrica**.

Na criptografia assimétrica, a chave utilizada para cifrar não é a mesma usada para decifrar. Para ilustrar melhor seu funcionamento, considere os personagens fictícios Alice, Bob e Eva. Suponha que Bob queira transmitir uma mensagem secreta à Alice sendo que mesmo que Eva intercepte a mensagem, não consiga decifrá-la. Estes personagens (Alice, Bob e Eva) e suas funções são comumente utilizados como um padrão na Criptografia.

Vamos fazer uma analogia com chaves e cadeados. Fechar um cadeado (cifrar uma mensagem) é fácil, mas somente quem possui a chave do cadeado pode abri-lo (decifrar a mensagem). Assim, suponha que Alice faça milhares de cópias de seu cadeado, distribuindo a todos que queiram comunicar-se com ela. Os cadeados estão abertos. Se Bob pretende transmitir uma informação para Alice, ele escreve sua mensagem, coloca dentro de uma caixa e a tranca usando um "cadeado de Alice", que é público, disponível a todo mundo que queira comunicar-se com ela. Quando Alice receber a caixa, somente ela pode abri-la, pois apenas ela possui a chave particular. Mesmo que Eva intercepte a caixa no caminho, ela não tem conhecimento da chave. De fato, depois de trancar a caixa, nem Bob consegue abri-la; apenas Alice.

Usando a mesma analogia com a criptografia simétrica, Alice e Bob deveriam ter cópias da mesma chave e existe apenas um cadeado fechado. Em algum

momento, Alice e Bob devem encontrar-se para fazer a troca de chaves, secretamente e evitando Eva. Caso Alice queira comunicar-se com outra pessoa, digamos Charles, ela deve criar outra chave e cópia para trocar informações secretas com este, além do contato para a troca de chaves.

É aqui que surge o problema de distribuição de chaves, citado anteriormente. Bancos ou *sites* de compra *online*, com milhares de clientes, teriam de encontrar-se secretamente com cada um destes para a distribuição de uma chave. Por outro lado, quando todos conhecem o "cadeado de Alice", mas somente a mesma tem a chave para abri-lo, é uma forma de tratar da **criptografia de chave pública** (cadeado aberto) onde também é usada uma chave particular.

Esta ideia simples revolucionou o mundo da Criptografia, resolvendo o problema de distribuição de chaves. Foi creditada a Whitfield Diffie, matemático americano formado no Instituto de Tecnologia de Massachussets (MIT) e Martin Hellman, criptógrafo e professor da Universidade de Stanford, na Califórnia. Eles demonstraram que era possível a existência de uma chave assimétrica, mas ainda não sabiam qual seria esta chave.

2.2.1 Surgimento da Criptografia RSA

Diffie e Hellman divulgaram a descoberta da chave assimétrica para o mundo, oportunizando que muitos pesquisadores pudessem buscar uma solução.

Entre estes pesquisadores, estavam Ron Rivest, Adi Shamir e Leonard Adleman. Rivest e Shamir eram cientistas da computação e Adleman, matemático. Enquanto Rivest e Shamir buscavam por um método eficiente de cifra assimétrica, Adleman apontava as falhas. Foi em abril de 1977, que Rivest fez a descoberta, após um ano de pesquisa. Apresentou a Adleman que não conseguiu encontrar erros. Das iniciais de seus sobrenomes, surgiu o RSA, um sistema de criptografia de chave pública. Foi o primeiro deste tipo a ser implementado e até hoje um dos mais populares.

O método RSA emprega em seu funcionamento resultados e ferramentas da Teoria dos Números, onde a Aritmética Modular é o centro deste processo.

Neste sentido, o próximo capítulo visa explorar a base necessária para esta compreensão.

3 FUNDAMENTAÇÃO MATEMÁTICA

Este capítulo destina-se a apresentar a teoria matemática que valida o funcionamento do RSA, onde destacam-se o entendimento da Aritmética Modular, da existência de inversos multiplicativos e do Teorema de Euler.

Neste aspecto, as seções de 3.1 a 3.5 (o conjunto dos números inteiros, princípio da boa ordem e princípio de indução finita, divisibilidades nos inteiros, máximo divisor comum e mínimo múltiplo comum, números primos e o teorema fundamental da aritmética) trazem definições, propriedades, proposições e teoremas básicos com o objetivo de construir e justificar os resultados das seções 3.7 a 3.9 (aritmética modular, classes residuais e inversos multiplicativos, função de Euler). A inclusão da Seção 3.6 (equações diofantinas) serve apenas como ferramenta e uma alternativa para o cálculo de inversos multiplicativos.

De maneira geral, foram utilizados nesta fundamentação principalmente os autores Hefez (2013) e Santos (2007), complementados por outras fontes de consulta devidamente referenciadas. Uma noção mínima de Teoria dos conjuntos - relação de pertinência ($\in$ ou $\notin$), relação de inclusão ($\subset, \subseteq$) e operações (união e intersecção) - é admitida como pré-requisito.

3.1 O CONJUNTO DOS NÚMEROS INTEIROS

O ponto de partida é o conjunto dos números inteiros, indicado por $\mathbb{Z}$, de onde tem-se: $\mathbb{Z} = \{\dots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots\}$. Notavelmente, destacam-se o conjunto dos números naturais, indicado por $\mathbb{N}$, sendo este um subconjunto dos números inteiros: $\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$. Por vezes, também será utilizado $\mathbb{Z}_+ = \mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$ para referir-se aos inteiros positivos. Em $\mathbb{Z}$, admitem-se duas operações: adição $(+)$ e multiplicação $(\cdot)$, que possuem as seguintes propriedades:

Propriedade 1. A adição e a multiplicação são bem definidas, isto é, para quaisquer $a, b, a', b' \in \mathbb{Z}$, se $a = a'$ e $b = b'$, então $a + b = a' + b'$ e $a \cdot b = a' \cdot b'$.

Propriedade 2. A adição e a multiplicação são comutativas, isto é, para quaisquer $a, b \in \mathbb{Z}$, $a + b = b + a$ e $a \cdot b = b \cdot a$.

Propriedade 3. A adição e a multiplicação são associativas, isto é, para quaisquer $a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$ e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Propriedade 4. A adição e a multiplicação possuem elementos neutros, isto é, para quaisquer $a \in \mathbb{Z}$, $a + 0 = a$ e $a \cdot 1 = a$.

Propriedade 5. A adição possui elementos simétricos, isto é, para quaisquer $a \in \mathbb{Z}$, existe $b \in \mathbb{Z}$, tal que $a + b = 0$. Tal elemento será denotado por $b = -a$.

Propriedade 6. A multiplicação é distributiva em relação à adição, isto é, para quaisquer $a, b, c \in \mathbb{Z}$, tem-se $a \cdot (b + c) = a \cdot b + a \cdot c$.

Propriedade 7. O conjunto dos números inteiros é fechado em relação às operações de adição e multiplicação, ou seja, se $a, b \in \mathbb{Z}$, então $a + b \in \mathbb{Z}$ e $a \cdot b \in \mathbb{Z}$.

Observação 1. A operação de adição e a Propriedade 5 permitem definir a operação de subtração, onde dados $a, b \in \mathbb{Z}$, temos "a menos b" como $a - b = a + (-b)$. A subtração, então, pode ser vista como uma mera simplicidade de notação.

Proposição 1. Para todo $a \in \mathbb{Z}$, $a \cdot 0 = 0$.

Demonstração. Pela Propriedade 6, tem-se: $a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, enquanto o uso da Propriedade 4 mostra que $a \cdot (0 + 0) = a \cdot 0$. Logo, $a \cdot 0 + a \cdot 0 = a \cdot 0$. Já a Propriedade 5 garante a existência do simétrico $-(a \cdot 0)$ de $a \cdot 0$. Assim, somando $-(a \cdot 0)$ em ambos os membros da equação $a \cdot 0 + a \cdot 0 = a \cdot 0$, tem-se: $a \cdot 0 + a \cdot 0 + (-a \cdot 0) = a \cdot 0 + (-a \cdot 0)$. Usando as Propriedades 3, 5 e 4, respectivamente, a demonstração é concluída, pois $a \cdot 0 + (a \cdot 0 + (-a \cdot 0)) = a \cdot 0 + (-a \cdot 0)$ implica em $a \cdot 0 + 0 = 0$ que por sua vez resulta em $a \cdot 0 = 0$. ■

Observação 2. Deste ponto em diante o uso das propriedades 1 a 7 será feito livremente, mencionadas apenas em observações importantes.

3.2 PRINCÍPIO DA BOA ORDEM E PRINCÍPIO DE INDUÇÃO MATEMÁTICA

Nesta seção, são apresentados o Princípio da Boa Ordem (PBO) e o Princípio da Indução Matemática (PIM), que são ferramentas importantes no desenvolvimento da teoria aqui apresentada. Complementando a construção dos mesmos seguem, primeiramente, as duas definições abaixo.

Definição 1. Diz-se que $a \leq b$ quando existir um $c \in \mathbb{N} \cup \{0\}$ tal que $b = a + c$. Esta relação de ordem é completa em $\mathbb{Z}$, isto é, dados a e b inteiros, somente um dos três casos pode ocorrer: $a < b$ (a menor que b), $b < a$ (b menor que a) ou $a = b$ (a igual a b). Quando $b < a$, poderá ser usada a notação $a > b$ (a maior que b). Da mesma maneira, quando $b \leq a$, poderá ser usada a notação $a \geq b$ (a maior ou igual a b).

Definição 2. Seja S um subconjunto não-vazio dos números inteiros ($S \neq \emptyset \; e \; S \subseteq \mathbb{Z}$). Diz-se que S é limitado inferiormente se existe um $c \in \mathbb{Z}$ tal que $c \leq s$ para todo $s \in S$. O número c é chamado cota inferior de S. Além disso, um elemento $s_o \in S$ é chamado mínimo de S, se para todo $s \in S$, tem-se $s_o \leq s$.

Princípio da Boa Ordem (PBO). Se S é limitado inferiormente com $S \subseteq \mathbb{Z}$ e $S \neq \emptyset$, então S possui mínimo.

Proposição 2. Não existe $n \in \mathbb{Z}$ tal que $0 < n < 1$.

Demonstração. Supõe-se, por absurdo, que exista um n inteiro com $0 < n < 1$, ou seja, admite-se que o conjunto $S = \{x \in \mathbb{Z} | 0 < x < 1\}$ seja não vazio. Da forma como foi construído, S é limitado inferiormente com $S \subseteq \mathbb{Z}$ e $S \neq \emptyset$; então, pelo PBO, S possui mínimo. Seja s_o este mínimo, ou seja, para todo $s \in S$, tem-se $s_o \leq s$ e $0 < s_o < 1$. Multiplicando esta última desigualdade por s_o obtém-se $0 < {s_o}^2 < s_o$ e, consequentemente, $0 < {s_o}^2 < s_o < 1$. Uma contradição, pois resultaria em $s_0^2 \in S$ com ${s_o}^2$ menor que o mínimo de S. ■

Observação 3. Pode-se tomar como corolário do resultado acima que, para todo $n \in \mathbb{Z}$, não existe $x \in \mathbb{Z}$ tal que $n < x < n + 1$. De fato, se existisse tal inteiro x, então $n + (-n) < x + (-n) < n + 1 + (-n)$ forneceria $0 < x + (-n) < 1$, contradizendo a Proposição 2.

Princípio de Indução Matemática (PIM). Seja $a \in \mathbb{Z}$ e $S \subseteq \mathbb{Z}$ tais que:
(i) $a \in S$;
(ii) Se para qualquer $n \geq a$, $n \in S$ implica em $n + 1 \in S$.
Então $\{x \in \mathbb{Z} | x \geq a\} \subset S$.
Demonstração. Seja $S' = \{x \in \mathbb{Z} | x \geq a\}$. Supõe-se, por absurdo, que $S' \not\subset S$, ou seja, que $S' - S \neq \emptyset$. Como este conjunto é não-vazio e, limitado inferiormente (por a), o PBO garante a existência de um mínimo $s_o \neq a$ com $a < s_o$ em $S' - S$, ou seja, $s_o \in S'$, mas $s_o \notin S$. Observa-se que $s_o - 1$ é menor que este mínimo s_o, portanto $s_o - 1$ não pertence a $S' - S$. Mas $s_o - 1$ também não pertence a S, pois se pertencesse, o item (ii), tomado como hipótese, implicaria em $s_o = (s_o - 1) + 1 \in S$. A única possibilidade é de que $s_o - 1$ também não pertença a S', o que é equivalente a dizer $s_o - 1 < a$. Por fim, tem-se $s_o - 1 < a < s_o$, que contradiz o resultado da Observação 3 e conclui a demonstração. ■

Outra maneira de enunciar o Princípio de Indução Matemática é a que se segue.

Seja $a \in \mathbb{Z}$ e $p(n)$ uma sentença aberta em $n \in \mathbb{N}$. Suponha que:
(i) $p(a)$ é verdadeira;
(ii) Se para todo $n \geq a$, $p(n)$ verdadeira implica em $p(n + 1)$ verdadeira.
Então, $p(n)$ é verdadeira para todo $n \geq a$.

Esta forma do PIM será particularmente útil em demonstrações posteriores. Uma demonstração desta forma de enunciar o PIM pode ser conferida em Hefez (2013, p.16).

3.3 DIVISIBILIDADE NO CONJUNTO DOS NÚMEROS INTEIROS

Definição 3. Sejam $a, b \in \mathbb{Z}$. Diz-se que a divide b, denotando por $a|b$, se existir um número inteiro $k \in \mathbb{Z}$ tal que $b = a \cdot k$. Se $a|b$, dizemos que "b é múltiplo de a", "b é divisível por a", ou ainda que "a é um divisor de b". Por outro lado, para indicar que a não divide b, será usada a notação $a \nmid b$.

Exemplo 1. $6|12$, pois existe um número inteiro ($k = 2$) tal que $12 = 6 \cdot 2$. Já $7 \nmid (-16)$, pois não existe nenhum número inteiro k tal que $-16 = 7 \cdot k$.

Proposição 3. Sejam $a, b, c, \in \mathbb{Z}$. Então:

(i) $a|a$ e $1|a$;

(ii) $a|0$;

(iii) Se $a|b$, com $b \neq 0$, então $|a| \leq |b|$.

(iv) Se $a|b$ e $b|c$, então $a|c$.

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

Demonstração.

(i) É consequência da Definição 3 e do fato de que para todo $a \in \mathbb{Z}$, $a = a \cdot 1 = 1 \cdot a$ (ver Seção 3.1, Propriedades 2 e 4).

(ii) Também consequência da Definição 3 e do fato de que para todo $a \in \mathbb{Z}$, $0 = a \cdot 0$. (ver Seção 3.1, Proposição 1).

(iii) Pela Definição 3, se $a|b$, existe um número inteiro k tal que $b = a \cdot k$. Usando propriedades do módulo, sabe-se que $|b| = |a| \cdot |k|$. Como $b \neq 0$, tem-se que $k \neq 0$. Assim, $1 \leq |k|$. Consequentemente, $|a| \leq |b|$.

(iv) Pela Definição 3, se $a|b$ e $b|c$, então existem k' e k'' inteiros tais que: $b = a \cdot k'$ e $c = b \cdot k''$, de onde tem-se $c = (a \cdot k') \cdot k''$, o que implica em $c = a \cdot (k' \cdot k'')$. Como a multiplicação é uma operação "fechada" em relação à multiplicação (Seção 3.1, Propriedade 7), o produto $k' \cdot k''$ resulta em um número $k \in \mathbb{Z}$ tal que $c = a \cdot k$, ou seja, $a|c$. Da Seção 3.1, também foi usada a Propriedade 3 (associativa).

(v) Novamente a Definição 3 diz que se $c|a$ e $c|b$, então existem k' e k'' inteiros tais que: $a = c \cdot k'$ e $b = c \cdot k''$. Assim, $x \cdot a + y \cdot b = x \cdot c \cdot k' + y \cdot c \cdot k'' = c \cdot (x \cdot k' + y \cdot k'')$. Desde que $x \cdot k' + y \cdot k'' = k \in \mathbb{Z}$, conclui-se que $c|(x \cdot a + y \cdot b)$.■

A seguir, um importante teorema é enunciado. Uma demonstração do mesmo pode ser encontrada em Hefez (2014, p. 53).

Teorema 1 (Algoritmo da Divisão). Sejam a e b dois números inteiros com $b \neq 0$. Existem dois únicos números inteiros, q e r, tais que: $a = b \cdot q + r$ com $0 \leq r < |b|$.

Os números q e r são chamados, respectivamente, de quociente e resto da divisão de a por b.

Este algoritmo já era encontrado na obra *Elementos*, escrita entre os séculos IV e III a.C pelo matemático grego Euclides. Aliás, não é por acaso que este resultado seja também conhecido como método de divisão euclidiana. Embora Euclides não o enuncie e demonstre explicitamente, os livros VII a IX (de um total de treze livros) que compõe sua obra e, tratam particularmente da Aritmética, têm como pon-

to central a ideia de quociente e resto. Além disso, Euclides tratava apenas de números inteiros não-negativos.

Já Hefez divide a demonstração deste teorema em duas partes: existência (onde usa o Princípio da Boa Ordem) e unicidade. Aqui, cabe ressaltar a importância destes dois pontos, pois em sua forma atual, da maneira como o teorema é apresentado, não se garante apenas a existência e unicidade do quociente q e do resto r na divisão de a por b. Ao fixar $0 \leq r < |b|$, as possibilidades ficam restritas. Por exemplo, quando se divide 81 por 5, encontra-se quociente 16 e resto 1. De fato, os restos possíveis na divisão euclidiana por 5 são 0, 1, 2, 3 ou 4. Por outro lado, poderia ser trabalhoso encontrar o quociente da divisão de 7^{8400} por 5, mas as possibilidades para o resto são as mesmas: 0, 1, 2, 3 ou 4.

Essa ideia é a base para o desenvolvimento da Aritmética Modular (ou Aritmética dos Restos) que será discutida na Seção 3.7. Com as ferramentas adequadas, será relativamente simples determinar que o resto da divisão de 7^{8400} por 5 também será 1 (ver Subseção 3.9.1, Observação 18).

3.4 MÁXIMO DIVISOR COMUM E MÍNIMO MÚLTIPLO COMUM

Segue-se apresentando mais algumas ferramentas que serão utilizadas na construção da Criptografia RSA.

Definição 4. Considere os números inteiros $a_1, a_2, \dots, a_n$. Suponha que eles não sejam todos nulos, ou seja, que pelo menos um deles seja diferente de zero. O **Máximo Divisor Comum (MDC)** dos números inteiros $a_1, a_2, \dots, a_n$ é o maior número inteiro d que divide todos esses números. Denota-se por $d = mdc(a_1, a_2, \dots, a_n)$**.** Particularmente, para dois números inteiros, a e b, diz-se que $d \geq 0$ é o máximo divisor comum de a e b, se satisfazer as seguintes condições:

1) d é um divisor comum de a e b, isto é, $d|a$ e $d|b$;
2) Se $d'|a$ e $d'|b$, então $d'|d$, isto é, d é o **maior** divisor comum de a e b.

Observação 4. Como o MDC não depende da ordem em que a e b são tomados, tem-se que: $mdc(a, b) = mdc(b, a)$. Além disso, assim como o elemento mínimo de um conjunto dado pela Definição 2, o elemento máximo de um conjunto, quando existe é único. Em se tratando de elementos inteiros em conjuntos formados por

divisores não negativos de a e b, limitados superiormente, segue-se que $d = mdc(a_1, a_2, \dots, a_n)$ existe e é único.

Observação 5. Em alguns casos particulares, é fácil verificar a existência do MDC. Por exemplo, se a é um número inteiro, então $mdc(a, 0) = |a|$ e $mdc(a, 1) = 1$.

Observação 6. Dados a e b inteiros, é válido que: $mdc(a, b) = mdc(-a, b) = mdc(a, -b) = mdc(-a, -b)$, ou seja, para fins de cálculo de MDC de dois números inteiros a e b, pode-se sempre considerá-los positivos.

Teorema 2. Se a e b são inteiros tais que $a = b \cdot q + r$, com q e r também inteiros. Então $mdc(a, b) = mdc(b, r)$.

Demonstração. Deve-se mostrar que todo divisor comum de a e b também é um divisor comum de b e r. Então, ao tomar d como um divisor de a e b, tem-se que $d|a$ e $d|b$. Como $a = b \cdot q + r$, então $d|(b \cdot q + r)$. Assim, existem $x, y \in \mathbb{Z}$ tais que: $b = d \cdot x$ e $b \cdot q + r = d \cdot y$. Estas equações implicam em $(d \cdot x)q + r = d \cdot y$ de onde segue $d \cdot (y - x \cdot q) = r$. Portanto, $d|r$. De maneira semelhante, verifica-se que todo divisor comum de b e r é um divisor comum de a e b, concluindo a demonstração. ■

A ideia do teorema acima é a base do método para encontrar o MDC entre números inteiros através de divisões sucessivas. Este método é conhecido como Algoritmo de Euclides, formalizado como Teorema abaixo. A demonstração do mesmo foi adaptada de Carneiro (2007, p. 34-35).

Teorema 3 (Algoritmo de Euclides). Dados dois números positivos a e b, aplica-se sucessivamente o algoritmo da divisão para obter a sequência de igualdades.

$$\begin{cases} b = aq_1 + r_1, & 0 \le r_1 < a \\ a = r_1 q_2 + r_2 & 0 \le r_2 < r_1 \\ r_1 = r_2 q_3 + r_3 & 0 \le r_3 < r_2 \\ \vdots & \\ r_{n-2} = r_{n-1} q_n + r_n & 0 \le r_n < r_{n-1} \\ r_{n-1} = r_n q_{n-1} & \end{cases}$$

Demonstração. A sequência de números inteiros r_k $(1 \le k \le n)$ é estritamente decrescente e está contida no conjunto $\{r \in \mathbb{Z}; 0 \le r < a\}$. Logo, o processo de divisões do teorema é finito e não contém mais do que a inteiros positivos. Examinando as igualdades e, aplicando o Teorema 2, temos que: $mdc(a, b) = mdc(a, r_1) = mdc(r_1, r_2) = \cdots = mdc(r_{1n-1}, r_n) = r_n$. Portanto, o máximo divisor comum entre a e b é o último resto não nulo da sequência de divisões sucessivas, o que encerra a demonstração. ■

Observação 7. As divisões sucessivas do Algoritmo de Euclides permitem encontrar x e y inteiros tais que $a \cdot x + b \cdot y = mdc(a,b)$. Neste caso, a existência de x e y inteiros é garantida pelo *Algoritmo de Euclides Estendido*. Esta possibilidade será particularmente útil na resolução de equações diofantinas da Seção 3.6 e na procura por inversos multiplicativos da Seção 3.8.

Definição 5. Diz-se que um número inteiro p é primo se, e somente se, $p \neq 0$, $p \neq \pm 1$ e seus únicos divisores inteiros são -1, 1, $-p$ e p. Se p não é primo, diz-se que p é composto.

Definição 6. Dois números inteiros, a e b, são ditos primos entre si (ou co-primos), se $mdc(a,b) = 1$.

Proposição 4. Dois números inteiros, a e b, são primos entre si se, e somente se, existem números inteiros x e y tais que $a \cdot x + b \cdot y = 1$.

Demonstração. Se a e b são primos entre si, então, pela Definição 6, $mdc(a,b) = 1$. O Algoritmo Estendido de Euclides garante a existência de x e y inteiros com $a \cdot x + b \cdot y = 1$. Reciprocamente, ao supor que existam x e y inteiros tais que $a \cdot x + b \cdot y = 1$, tem-se que se $d = mdc(a,b)$ então $d|a$ e $d|b$. Mas pela Seção 3.3, o item (v) da Proposição 3, diz que $d|(a \cdot x + b \cdot y)$ para quaisquer x, y inteiros. Em particular, $d|1$ e, portanto, $d = 1$ (d não pode ser -1, pois pela Definição 4, $d \geq 0$). Logo, a e b são primos entre si. ■

Observação 8. Uma consequência do Algoritmo de Euclides Estendido e da Proposição 4 é que se $d = mdc(a,b)$, com a e b não nulos, então $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Primeiramente, observa-se que $\frac{a}{d}$ *e* $\frac{b}{d}$ são números inteiros (pois $d|a$ e $d|b$) e que se a e b são ambos diferentes de zero, d também será. Tomando $a \cdot x + b \cdot y = d$ e, dividindo ambos os membros desta equação por d, obtém-se $\frac{a}{d} \cdot x + \frac{b}{d} \cdot y = 1$, o que implica naturalmente em $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

O Teorema abaixo é referenciado como Lema de Gauss em Hefez (2014, p. 96).

Teorema 4 (Lema de Gauss). Sejam a, b e c números inteiros. Se $a|b \cdot c$ e $mdc(a,b) = 1$, então $a|c$.

Demonstração. Se $a|(b \cdot c)$, então existe $k \in \mathbb{Z}$ tal que $b \cdot c = a \cdot k$. Por outro lado, como $mdc(a,b) = 1$, tem-se pela Proposição 4 que existem x e y inteiros tais que:

$a \cdot x + b \cdot y = 1$. Multiplicando ambos os membros desta equação por c, obtém-se $a \cdot x \cdot c + b \cdot y \cdot c = c$ que implica em $a \cdot (x \cdot c + y \cdot k) = c$. Portanto, $a|c$. ■

Proposição 5. Se $a, b, c \in \mathbb{Z}$, então:

(i) Se $mdc(a, b) = 1$, então $mdc(a \cdot c, b) = mdc(c, b)$;

(ii) $mdc(a \cdot c, b) = 1$ se, e somente se, $mdc(a, b) = mdc(c, b) = 1$.

Demonstração

(i) Seja $d = mdc(c, b)$. Então, $d|c$ e $d|b$. Além disso, d é um divisor comum de $a \cdot c$ e b. Resta mostrar que d é o maior divisor comum de $a \cdot c$ e b (MDC), ou seja, que todo divisor comum f, de $a \cdot c$ e b, divide d. Por outro lado, toma-se $g = mdc(a, f)$. Como $g|a$ e $f|b$, então $g|mdc(a, b)$. Por hipótese, $mdc(a, b) = 1$, logo $g = mdc(a, f) = 1$. Assim, se $f|a \cdot c$ e $mdc(a, f) = 1$, então $f|c$ (pelo Teorema 4, o Lema de Gauss). Por fim, se $f|b$ e $f|c$, então $f|d$.

(ii) Pela Proposição 4, existem x e y inteiros tais que $(a \cdot c) \cdot x + b \cdot y = 1$. Assim, tem-se $a \cdot (c \cdot x) + b \cdot y = 1$ e $c \cdot (a \cdot x) + b \cdot y = 1$, o que implica em novamente pela Proposição 4 em $mdc(a, b) = mdc(c, b) = 1$. Reciprocamente, se $mdc(a, b) = mdc(c, b) = 1$, do item (i) segue-se que $mdc(a \cdot c, b) = mdc(c, b) = 1$. ■

A seguir, a definição de Mínimo Múltiplo Comum e um resultado do mesmo com o MDC.

Definição 7. Considere os números inteiros $a_1, a_2, \dots, a_n$, não nulos, ou seja, todos diferentes de zero. O **Mínimo Múltiplo Comum (MMC)** dos números inteiros $a_1, a_2, \dots, a_n$ é o menor inteiro m não nulo que é múltiplo de todos esses números. Denota-se por $m = mmc(a_1, a_2, \dots, a_n)$. Particularmente, para dois números inteiros a e b, diz-se que $m \geq 0$ é o mínimo múltiplo comum de a e b, se satisfazer as seguintes condições:

1) m é um múltiplo comum de a e b, ou seja, $a|m$ e $b|m$;
2) Se $a|m'$ e $b|m'$, então $m|m'$, isto é, m é o menor dos múltiplos comuns.

Vale observar que o MMC tem existência e unicidade garantidas pelo PBO e pela unicidade do mínimo de um conjunto, quando existir. O próximo resultado unirá os conceitos de MDC e MMC.

Proposição 6. Dados dois números inteiros, a e b, então $mdc(a, b).mmc(a, b) = |ab|$.

Demonstração. Para efeitos de simplificação, irão ser considerados $d = mdc(a,b)$, $m = mmc(a,b)$ e tomados a, b inteiros positivos. Assim, deve-se mostrar que $md = ab$, o que resulta em $m = \frac{ab}{d}$. Observa-se que $\frac{ab}{d}$ satisfaz as condições 1) e 2) da Definição 7, pois: $\frac{ab}{d} \geq 0$ ($m \geq 0$) e:

1) Tanto a quanto b dividem $\frac{ab}{d}$.

2) Se $a|m'$ e $b|m'$ então existem x e y inteiros tais que: $m' = ax$ e $m' = by$. Igualando estas equações, obtém-se: $ax = by$. Dividindo ambos os membros desta última equação por d resulta em $\frac{a}{d}x = \frac{b}{d}y$. Usando que $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ (da Observação 8, $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si) e o Teorema 4 (Lema de Gauss), conclui-se que $\frac{a}{d}|y$ e $\frac{b}{d}|x$. Portanto, existe $k \in \mathbb{Z}$ com $x = \frac{b}{d}k$. Finalmente, substituindo esta última equação em $m' = ax$, tem-se $m' = \left(\frac{ab}{d}\right)k$. Portanto, $\frac{ab}{d}|m'$. ■

3.5 NÚMEROS PRIMOS E O TEOREMA FUNDAMENTAL DA ARITMÉTICA

Números primos ocupam papel central em Teoria dos Números. Existem diversos problemas em aberto envolvendo números primos, como a conjectura de Golbach que diz: “Qualquer número par maior que 2 pode ser escrito como a soma de dois números primos”.

Nesta seção serão discutidos resultados sobre números primos, com destaque para o Teorema Fundamental da Aritmética e testes de primalidade. Inicialmente, segue uma proposição referenciada em Hefez (2014, p.141) como Lema de Euclides.

Proposição 7 (Lema de Euclides). Seja p um número primo e a e b números inteiros positivos. Se $p|ab$, então $p|a$ ou $p|b$.

Demonstração. É consequência do Teorema 4 (Lema de Gauss), pois se $p \nmid a$, então o único divisor positivo comum de p e a é 1. Em outras palavras, $mdc(p,a) = 1$. Logo, $p|b$, o que conclui a demonstração. ■

Na demonstração do próximo teorema foi adotada abordagem semelhante ao que pode ser visto em Santos (2007, p. 9).

Teorema 5 (Teorema Fundamental da Aritmética). Todo número inteiro n maior do que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos. Em outras palavras, queremos dizer que se $n \geq 2$,

$$n = {p_1}^{a_1}.{p_2}^{a_2} \dots {p_m}^{a_m}$$

Onde $1 < p_1 < p_2 < \cdots < p_m$ são números inteiros e $a_1, a_2, \dots, a_m$ são inteiros positivos (os respectivos expoentes dos números primos; definem a multiplicidade de cada fator primo).

Demonstração. A demonstração será dividida em duas partes: Existência e Unicidade. **Existência***.* Se n é primo, a demonstração está terminada. Supõe-se então que n é composto, isto é, possua mais de dois divisores positivos. Logo, se n é composto, existe um número inteiro x, onde $1 < x < n$ tal que $x|n$. Mas isto implica que existe um inteiro y e que $n = x.y$, com $1 < y < n$ (nada impede de x e y serem iguais). Seja p_1 o menor dos divisores positivos de n ($p_1|n$). Afirma-se que p_1 é primo. De fato, se p_1 não fosse primo, seria composto e existiria um x_1, onde $1 < x_1 < p_1$. Assim, $x_1|p_1$. Consequentemente, $x_1|n$, contradizendo o fato de p_1 ser o menor divisor positivo inteiro. Escreve-se $n = p_1 \cdot k_1$. Se k_1 é primo, a prova está completa. Caso contrário, toma-se p_2 como o menor divisor positivo e inteiro de k_1. Pelo que foi visto, p_2 é primo. Continuando, escreve-se $n = p_1 \cdot p_2 \cdot k_2$.

Repetindo este procedimento, obtém-se uma sequência decrescente de números inteiros positivos $k_1, k_2, \dots, k_r$. Como todos estes números são maiores que 1, este processo é finito. Por outro lado, alguns dos primos podem se repetir, explicando a multiplicidade e a possibilidade de expoentes $a_1, a_2, \dots, a_m$ maiores que 1. **Unicidade.** Seja n o menor inteiro positivo que admite duas fatorações distintas, ou seja: $n = {p_1}^{a_1}.{p_2}^{a_2} \dots {p_m}^{a_m} = {q_1}^{b_1}.{q_2}^{b_2} \dots {q_s}^{b_s}$. Como p_1 divide n, pela Proposição 7, p_1 deve dividir alguns dos primos q_j, com $1 \leq j \leq s$. Pode-se supor, sem perda de generalidade que $p_1|q_1$. Como ambos são primos, $p_1 = q_1$. Cancelando p_1 em ambos os lados da igualdade, obtém-se um número inteiro m, tal que $m = {p_1}^{a_1-1}.{p_2}^{a_2} \dots {p_m}^{a_m} = {q_1}^{b_1-1}.{q_2}^{b_2} \dots {q_s}^{b_s}$.

Assim, m é um número inteiro positivo menor que n e que também admite duas fatorações distintas. Absurdo, pois isto contraria a minimalidade de n. ■

Observação 9. Se os números -1 e 1 não fossem excluídos da definição de primo, a unicidade no Teorema Fundamental da Aritmética não poderia ser garantida. Por

exemplo, se 1 fosse primo, 3 e $1^3 \cdot 3$ seriam duas decomposições em fatores primos distintas para o número 3. Para excluir este tipo de decomposição trivial, diz-se que -1 e 1 não são primos.

3.5.1 Testes de primalidade

Ao observar uma lista dos primeiros primos, 2, 3, 5, 7, 11, 13, 19, 23, 29 ..., percebe-se duas coisas: 2 é o único primo par (pois qualquer outro inteiro n par terá 2 como divisor, além de 1 e n) e que não parece ter uma certa regularidade nesta distribuição. Outro ponto: existem infinitos números primos (como será visto no Teorema 7 desta seção).

É atribuído ao matemático grego Eratóstenes (230 a. C) a criação de um dos mais antigos métodos de listagem de primos, posteriormente conhecido como *Crivo de Eratóstenes*. Neste método, alguém que quisesse encontrar todos os primos entre 1 e 100, por exemplo, agiria da seguinte maneira:

Passo 1. Excluir todos os múltiplos de 2 maiores que 2;

Passo 2. O próximo primo é o 3, que não será excluído. Excluir todos os múltiplos de 3 maiores que 3;

Passo 3. O próximo primo é o 5, que não será excluído. Excluir todos os múltiplos de 5 maiores que 5;

Passo 4. O próximo primo é o 7, que não será excluído. Excluir todos os múltiplos de 7 maiores que 7. Pode-se parar por aqui. Por quê? O próximo primo seria o 11, cujo quadrado é 121, maior que 100. Para verificar se um dado número n é primo ou não, basta testar sua divisibilidade por todos os primos p, onde $p \leq \sqrt{n}$ (este resultado será enunciado e demonstrado formalmente a seguir). Este procedimento pode ser resumido no quadro abaixo, com os números primos de 1 a 100 (células brancas), onde foram aplicados os Passos 1 a 4 descritos:

Quadro 4 - Números primos de 1 a 100 obtidos pelo Crivo de Eratóstenes.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Fonte: O autor.

Teorema 6. Se um número natural $n > 1$ não é divisível por nenhum primo p tal que $p^2 \leq n$, então ele é primo.

Demonstração. Supõe-se que mesmo que $n > 1$ não seja divisível por nenhum primo p tal que $p^2 \leq n$, ainda seja possível obter n composto, ou seja, que exista um menor fator primo q tal que q divide n. Escreve-se $n = q \cdot x$, onde x é inteiro e $q \leq x$. Multiplicando ambos os lados desta desigualdade por q, obtém-se $q^2 \leq q \cdot x$ o que implica em $q^2 \leq n$, uma contradição. ■

Teorema 7. Existem infinitos primos.

Demonstração. Deve-se mostrar que supor a existência de um número k finito de primos, $p_1, p_2, \dots, p_k$, resultará um absurdo matemático. De fato, considere n um número inteiro positivo tal que $n = p_1.p_2 \dots p_k + 1$. Pelo Teorema Fundamental da Aritmética, n possui um fator primo p (que deve ser um dos finitos $p_1, p_2, \dots, p_k$) que divide n e que divide $p_1.p_2 \dots p_k$. Não obstante, se $p|n$ e $p|p_1.p_2 \dots p_k$, existem inteiros x e y com: $n = p \cdot x$ e $p_1.p_2 \dots p_k = py$. Combinando estas equações com $n = p_1.p_2 \dots p_k + 1$ obteria-se $p|1$, absurdo, pois p é primo. ■

Observação 10. O Teorema 6 fornece um teste de primalidade, pois, para verificar se um dado número n é primo ou não, basta testar sua divisibilidade por todos os primos p, onde $p \leq \sqrt{n}$.

Como será visto no Capítulo 4, a procura por “números primos grandes” é um interesse da Criptografia RSA e muita pesquisa matemática tem sido feita neste sentido, visando testes de primalidade funcionais e eficientes, principalmente pela vantagem do uso de métodos computacionais para os cálculos.

Aliás, historicamente, a busca por uma fórmula de “fabricar números primos” desafiou matemáticos de várias gerações, dos quais citam-se Fermat e Mersenne. Os números de Fermat são da forma $F_n = 2^{2^n} + 1$ para $n \in \mathbb{N} \cup \{0\}$. Em 1640, Fermat acreditava que todos os números desta forma seriam primos, como $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65537$. No entanto, em 1732, Leonhard Euler mostrou que $F_5 = 4294967297$ pode ser escrito como um produto de 641 e 6700417 sendo, portanto, composto. Até hoje não se sabe se existem outros primos entre os números de Fermat.

Já Mersenne, contemporâneo de Fermat, usava números da forma $M_p = 2^p - 1$, onde p é um número primo. Nem todos os números desta forma serão primos, mas fornece a possibilidade de gerar “primos gigantescos” como $M_{77232917}$, um primo de Mersenne de 23249425 dígitos descoberto em dezembro de 2017.

3.6 EQUAÇÕES DIOFANTINAS

A resolução de vários problemas de Aritmética recai em equações do tipo: $a \cdot x + b \cdot y = c$ de soluções inteiras para x e y, com a, b e c também inteiros. Tais equações são chamadas equações diofantinas lineares em homenagem a *Diofanto de Alexandria* - matemático grego que viveu por volta de 300 d.C; considerado por muitos o “Pai da Álgebra”.

Mas nem sempre essas equações possuem solução. Por exemplo, a equação $4 \cdot x + 6 \cdot y = 3$**,** não possui nenhuma solução para x, y inteiros. De fato, o resultado seria que $4 \cdot x + 6 \cdot y = 3$ implica em $2 \cdot (2x + 3y) = 3$ e assim $2|3$ (absurdo).

Para resolver uma equação diofantina do tipo $a \cdot x + b \cdot y = c$, pode-se seguir os passos abaixo:

Passo 1. Calcule $d = mdc(a, b)$. Se $d|c$ a equação tem infinitas soluções. Em caso negativo (se d não divide c), não existe solução para x e y inteiros.

Passo 2. Encontre uma solução particular (x_0, y_0).

Passo 3. Escreva a solução geral como:

$$\begin{cases} x = x_0 - \frac{b}{d} \cdot t \\ y = y_0 + \frac{a}{d} \cdot t \end{cases} \qquad t \in \mathbb{Z}.$$

As proposições a seguir justificam estes passos.

Proposição 8. A equação diofantina $a \cdot x + b \cdot y = c$, admite soluções inteiras para x e y se, e somente se, $d|c$, onde $d = mdc(a, b)$.

Demonstração. Primeiramente, supõe-se que $d|c$, ou seja, existe k inteiro com $c = d \cdot k$. O Algoritmo Estendido de Euclides, garante a existência de m e n inteiros tais que: $a \cdot m + b \cdot n = d$. Multiplicando ambos os membros desta equação por k, obtém-se $a \cdot (k \cdot m) + b \cdot (n \cdot k) = d \cdot k$ que implica em $a \cdot (k \cdot m) + b \cdot (n \cdot k) = c$. Pode-se tomar $x = k \cdot m$ e $y = n \cdot k$. Assim, x e y são soluções inteiras para a equação diofantina. Reciprocamente, se $a \cdot x + b \cdot y = c$ admite soluções inteiras para x e y e, levando em conta o fato de que $d|a$ e $d|b$**,** fica evidente que $d|c$. ■

Proposição 9. Seja (x_0, y_0) uma solução da equação diofantina $ax + by = c$. Então, existem infinitas soluções e todas serão do tipo:

$$\begin{cases} x = x_0 - \dfrac{b}{d} \cdot t \\ y = y_0 + \dfrac{a}{d} \cdot t \end{cases}, t \in \mathbb{Z}$$

Demonstração. Se (x_0, y_0) é uma solução, tem-se $a \cdot x_0 + b \cdot y_0 = a \cdot x + b \cdot y = c$. Consequentemente, $a \cdot (x_0 - x) = b \cdot (y - y_0)$. Dividindo ambos os membros desta última equação por $d = mmc(a, b)$, resulta em $\frac{a}{d} \cdot (x_0 - x) = \frac{b}{d} \cdot (y - y_0)$. Levando em conta que $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ (conforme Seção 3.4, Observação 8, $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si), pelo Lema de Gauss (Seção 3.4, Teorema 4) tem-se que $\frac{a}{d}|(y - y_0)$. Logo, existe $t \in \mathbb{Z}$, tal que $(y - y_0) = \frac{a}{d} \cdot t$. Manipulando esta última equação chega-se em $y = y_0 + \frac{a}{d} \cdot t$. Para encontrar $x = x_0 - \frac{b}{d} \cdot t$, basta substituir $y = y_0 + \frac{a}{d} \cdot t$ em $\frac{a}{d} \cdot (x_0 - x) = \frac{b}{d} \cdot (y - y_0)$. Finalmente, $\left(x_0 - \frac{b}{d} \cdot t, y_0 + \frac{a}{d} \cdot t\right)$ é solução da equação $a \cdot x + b \cdot y = c$, pois, $a \cdot \left(x_0 - \frac{b}{d} \cdot t\right) + b \cdot \left(y_0 + \frac{a}{d} \cdot t\right) = a \cdot x_0 - \frac{a \cdot b}{d} \cdot t + by_0 + \frac{a \cdot b}{d} \cdot t = a \cdot x_0 + b \cdot y_0 = c$. ■

3.7 ARITMÉTICA MODULAR

Como destacado no início deste capítulo, a Aritmética Modular é fundamental para o entendimento da Criptografia RSA. A ideia de trabalhar com o resto da divisão

euclidiana, comentada na seção 3.3 após o Teorema 1, foi introduzida por Gauss em seu livro *Disquitiones Arithmeticae*, escrito em 1801, uma obra de grande influência na Aritmética. Segue a teoria.

Definição 8. Sejam $m \in \mathbb{N}$ e $a, b \in \mathbb{Z}$. Diz-se que a e b são congruentes módulo m, se os restos da divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se: $a \equiv b\ (mod\ m)$. Caso contrário, diz-se que a e b não são congruentes, ou que são incongruentes módulo m. Nesse caso, escreve-se $a \not\equiv b\ (mod\ m)$.

Exemplo.

- $29 \equiv 13\ (mod\ 8)$, pois 29 e 13 deixam resto 5 na divisão por 8.
- $7 \not\equiv 5\ (mod\ 3)$, pois 7 deixa resto 1 quando dividido por 3; já 5 deixa resto 2.

Observação 11. como o resto de um número inteiro por 1 é sempre zero, não faz muito sentido considerar o caso de congruência módulo 1. Por isto, deste ponto em diante, sempre será considerado $m \neq 1$.

A seguir, serão listadas uma série de proposições importantes, tanto no desenvolvimento da teoria, quanto em diversas aplicações da congruência modular.

Proposição 10. Sejam $a, b, m \in \mathbb{Z}$ com $m > 1$. Então, $a \equiv b\ (mod\ m)$ se, e somente se, $m \mid b - a$.

Demonstração. Pela Definição 8, se $a \equiv b\ (mod\ m)$, a e b deixam o mesmo resto r na divisão euclidiana por m. Escreve-se, então: $a = m \cdot q + r$, para algum $q \in \mathbb{Z}$ e $0 \leq r < m$ e $b = m \cdot k + r$, para algum $k \in \mathbb{Z}$ e $0 \leq r < m$. Subtraindo, membro a membro, a segunda equação da primeira, obtém-se $b - a = m \cdot (k - q)$. Como $k - q$ é um número inteiro, $m \mid b - a$.

Reciprocamente, seria uma contradição considerar $m \mid b - a$ e restos diferentes para a e b na divisão euclidiana por m. De fato, ao supor que a deixa resto r e b deixa resto r', com $r' \neq r$, resultaria em $a = m \cdot q + r, com\ 0 \leq r < m$ e $b = m \cdot k + r', com\ 0 \leq r' < m$. Subtraindo, membro a membro estas equações, conclui-se que $b - a = m \cdot (k - q) + (r' - r)$. Mas $m \mid (r' - r)$ somente se $r' - r = 0$, pois $m > 1$ e tanto r' quanto r são menores que m. Como r e r' são ambos positivos, $r' - r$ também será menor que m e maior que $-m$. A única saída é admitir $r' - r = 0$, ou seja, $r' = r$. Portanto, a e b deixam o mesmo resto na divisão euclidiana por m. Então, $a \equiv b\ (mod\ m)$. ■

Proposição 11. Seja $m \in \mathbb{N}, m > 1$. Para todos $a, b, c \in \mathbb{Z}$, temos, como propriedades da congruência modular:

(i) Propriedade reflexiva: $a \equiv a \ (mod\ m)$.

(ii) Propriedade simétrica: se $a \equiv b \ (mod\ m)$ então $b \equiv a \ (mod\ m)$.

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

Demonstração. A demonstração destas propriedades segue diretamente da Definição 8.

(i) Obviamente, o número a deixa o mesmo resto que si mesmo na divisão euclidiana por m.

(ii) Também óbvia. Se a e b deixam o mesmo resto da divisão por m, b e a também possuem este mesmo resto.

(iii) Se a e b deixam resto r, b e c também deixam resto r. ■

Observação 12. Quando uma relação, como a aritmética modular, satisfaz as propriedades reflexiva, simétrica e transitiva, diz-se tratar de uma *relação de equivalência*.

Proposição 12. Seja $m \in \mathbb{N}, m > 1$. Para todos $a, b, c, d \in \mathbb{Z}$, são válidas:

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

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

(iii) Para todo $n \in \mathbb{N}$, se $a \equiv b \ (mod\ m)$, então $a^n \equiv b^n \ (mod\ m)$.

Demonstração

(i) Se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, então, pela Proposição 10, tem-se que $m|b - a$ e $m|d - c$. Da Seção 3.3, Proposição 3, item (v), chega-se à $m|(b - a) + (d - c)$. Consequentemente, $m|(b + d) - (a + c)$. Portanto, $a + c \equiv b + d \ (mod\ m)$.

(ii) Da mesma maneira, $m|b - a$ e $m|d - c$. Novamente, usando o resultado da Proposição 3, item (v), conclui-se que $m|(x \cdot (b - a) + y \cdot (c - d))$, para quaisquer x e y inteiros. Particularmente, tomando $x = d$ e $y = a$, tem-se que $m|(d \cdot (b - a) + a \cdot (d - c))$, o que implica em $m|(b \cdot d - a \cdot c)$. Portanto, $ac \equiv bd \ (mod\ m)$.

(iii) Será usado o Princípio de Indução Matemática em $n \in \mathbb{N}$.

- A proposição é válida para $n = 1$. De fato, $a^1 \equiv b^1 (mod\ m)$ é garantida pela hipótese de que $a \equiv b \ (mod\ m)$.

- Toma-se a proposição verdadeira para um $k \in \mathbb{N}$ (hipótese de indução) e verifica-se que isto implica na validez de $k+1$, ou seja, se $a^k \equiv b^k (mod\, m)$ e $a \equiv b\ (mod\, m)$ ocorrem, aplica-se o item (ii) para concluir que $a^{k+1} \equiv b^{k+1} (mod\, m)$ também ocorrerá, sendo válida para todo $n \in \mathbb{N}$.

Isto conclui a demonstração. ■

Observação 13. Do item (i), é natural questionar a validade do cancelamento em relação à adição. De fato, é fácil verificar que $a + c \equiv b + c (mod\, m)$ implica em $a \equiv b\ (mod\, m)$, pois da hipótese, $m|(b + c) - (a + c)$. Deste fato, $m|(b - a)$. Segue, então, que $a \equiv b\ (mod\, m)$.

Por outro lado, o exemplo a seguir ilustra que nem sempre é válido o cancelamento em relação à multiplicação.

Exemplo: Sabe-se que $32 \equiv 24\ (mod\ 4)$, que poderia ser escrito como $4 \cdot 8 \equiv 3 \cdot 8\ (mod\ 4)$. No entanto, ao "cortarmos" o 8, obtemos $4 \equiv 3\ (mod\ 4)$, o que não é verdade. Observa-se que neste exemplo, $mdc(8,4) = 4$. De fato, o cancelamento da multiplicação em $a \cdot c \equiv b \cdot c\ (mod\, m)$ só é válido, quando $mdc(c, m) = 1$. A proposição a seguir confirma este resultado.

Proposição 13. Seja $m \in \mathbb{N}$, $m > 1$. Para todos $a, b, c, \in \mathbb{Z}$, tem-se que:

$$a \cdot c \equiv b \cdot c\ (mod\, m) \Leftrightarrow a \equiv b \left(mod\, \frac{m}{d}\right), \text{ onde } d = mdc(c, m).$$

Demonstração. Primeiramente, toma-se $d = mdc(c, m)$, assim, $d|c$ e $d|m$. Então, tudo bem fazer uso de $\frac{m}{d}$, pois este será um número inteiro. Além disto, $\frac{m}{d}$ e $\frac{c}{d}$ são primos entre si (Seção 3.4, Observação 8) ou seja, $mdc\left(\frac{m}{d}, \frac{c}{d}\right) = 1$. Então, pelo Lema de Gauss (Seção 3.4, Teorema 4),

$a \cdot c \equiv b \cdot c\ (mod\, m) \Leftrightarrow m|b \cdot c - a \cdot c \Leftrightarrow m|c \cdot (b - a) \Leftrightarrow \frac{m}{d}|\frac{c}{d} \cdot (b - a) \Leftrightarrow \frac{m}{d}|(b - a) \Leftrightarrow a \equiv b \left(mod\, \frac{m}{d}\right)$ ■

Proposição 14. Sejam $m_1, m_2, \ldots, m_r$ números naturais, todos maiores que 1 e, a e b, números inteiros quaisquer.

(i) Se $a \equiv b\ (mod\, m)$ e $n|m$, então $a \equiv b\ (mod\, n)$.

(ii) Se $a \equiv b\ (mod\, m_i)$, para $1 \leq i \leq r$ então $a \equiv b\ (mod\, M)$, onde $M = mmc(m_1, m_2, \ldots, m_r)$. A recíproca também é verdadeira.

Demonstração.

(i) Se $a \equiv b\ (mod\ m)$, então $m|(b-a)$. Se $n|m$, então $n|(b-a)$ (onde foi usado resultado da Seção 3.3, Capítulo 3, Proposição 3, item (iv)). Consequentemente, $a \equiv b\ (mod\ n)$.

(ii) Para cada $a \equiv b\ (mod\ m_i)$, $m_i|(b-a)$. Sendo $b-a$ um múltiplo comum de $m_1, m_2, \dots, m_r$, então $M|(b-a)$. Consequentemente, $M|(b-a)$ e $a \equiv b\ (mod\ M)$. A recíproca é uma conseqüência direta da parte (i), pois se $a \equiv b\ (mod\ M)$ e $m_i|M$, então $a \equiv b\ (mod\ m_i)$.

Isto conclui a demonstração. ■

3.8 CLASSES RESIDUAIS E INVERSOS MULTIPLICATIVOS

A Criptografia RSA faz uso de chave pública e chave privada. No Capítulo 4 será visto que a obtenção da chave privada passa pelo conhecimento de inversos multiplicativos, motivo que torna esta seção particularmente importante.

Considere inicialmente um número inteiro $m > 1$. Pode-se dividir o conjunto $\mathbb{Z}$ dos números inteiros em subconjuntos, onde cada um deles é formado por todos os números inteiros que possuem o mesmo resto quando divididos por m.

Definição 9. O conjunto $[a] = \{x \in \mathbb{Z}; x \equiv a\ (mod\ m)\}$ é chamado de classe residual módulo m do elemento a de $\mathbb{Z}$.

Assim, os subconjuntos que dividem $\mathbb{Z}$ em uma partição são exatamente as classes:

$$[0] = \{x \in \mathbb{Z}; x \equiv 0\ (mod\ m)\}$$
$$[1] = \{x \in \mathbb{Z}; x \equiv 1\ (mod\ m)\}$$
$$[2] = \{x \in \mathbb{Z}; x \equiv 2\ (mod\ m)\}$$
$$\vdots$$
$$[m-1] = \{x \in \mathbb{Z}; x \equiv m-1\ (mod\ m)\}$$

Definição 10. Denomina-se sistema completo de resíduos módulo m ao conjunto de todas suas classes residuais, aos quais serão representadas por $\mathbb{Z}_m$. Portanto, $\{0,1, \dots, m-1\}$ é um sistema completo de resíduos módulo m.

Exemplo: Tem-se que $\mathbb{Z}_2 = \{[0], [1]\}$ e $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$. Nada impediria, no entanto, de escrevermos $\mathbb{Z}_2 = \{[8], [5]\}$ ou $\mathbb{Z}_4 = \{[12], [13], [14], [15]\}$, afinal de contas, $[8] = [0]$, $[5] = [1]$, etc.

Proposição 15. Sejam $a, k, m \in \mathbb{Z}$, com $m > 1$ e $mdc(k, m) = 1$. Se $\{a_1, \dots, a_m\}$ é um sistema completo de resíduos módulo m, então $\{a + k \cdot a_1, \dots, a + k \cdot a_m\}$ também é um sistema completo de resíduos módulo m.

Demonstração. Da Seção 3.7, Proposição 11 sabe-se que se $mdc(c, m) = 1$, então $a \cdot c \equiv b \cdot c \ (mod\ m) \Leftrightarrow a \equiv b (mod\ m)$. Assim, considere os inteiros i e j, tais que $0 \leq i, j \leq m - 1$. Então:

$$a + k \cdot a_i \equiv a + k \cdot a_j (mod\ m) \Leftrightarrow k \cdot a_i \equiv k \cdot a_j (mod\ m) \Leftrightarrow a_i \equiv a_j (mod\ m) \Leftrightarrow i = j.$$

Isso mostra que $\{a + k \cdot a_1, \dots, a + k \cdot a_m\}$ são, dois a dois, não congruentes módulo m e, portanto, formam um sistema completo de resíduos módulo m. Na passagem acima, também foi usado o "cancelamento em relação à adição", justificado na Observação 13, o que conclui a demonstração. ■

Esta proposição, permite que cada classe residual de $\mathbb{Z}_m$ possa ser representada de infinitas maneiras. Quando $[x] \in \mathbb{Z}_m$ e temos $[x] = [a]$, diz-se que o número inteiro a é um representante de $[x]$.

Observação 14. Em $\mathbb{Z}_m$, escrever que uma classe residual $[a]$ é igual a uma classe residual $[x]$, isto é, $[a] = [x]$, é equivalente a escrever $a \equiv x \ (mod\ m)$. Com isto, podem ser definidas operações de adição e multiplicação, da seguinte maneira:

Adição: $[a] + [b] = [a + b]$.

Multiplicação: $[a] \cdot [b] = [a \cdot b]$.

Exemplo: Em $\mathbb{Z}_5$, tem-se, por exemplo: $[1] + [4] = [1 + 4] = [5] = [0]$. Na multiplicação: $[2] \cdot [3] = [2 \cdot 3] = [6] = [1]$.

Definição 11. Um elemento $[a] \in \mathbb{Z}_m$ será dito invertível quando existir $[b] \in \mathbb{Z}_m$ tal que $[a] \cdot [b] = [1]$. Nesse caso, dizemos que $[b]$ é o inverso de $[a]$.

Exemplo: no exemplo anterior, em $\mathbb{Z}_5$, verificou-se que $[2] \cdot [3] = [1]$. Neste caso, diz-se que $[2]$ é o inverso de $[3]$, assim como $[3]$ é o inverso de $[2]$. Porém, nem sempre é possível a existência de inverso em $\mathbb{Z}_m$. Considere, por exemplo, $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$. Aqui o elemento $[2]$ não possui inverso. De fato, $[2] \cdot [x] = [1]$, equivale a $6|(2x - 1)$, o que implicaria em 1 como um número par.

A próxima proposição discute a existência e as condições de um inverso em $\mathbb{Z}_m$.

Proposição 16. Um elemento $[a] \in \mathbb{Z}_m$ é invertível se, e somente se, $mdc(a,m) = 1$.

Demonstração. Se a e m são primos entre si, isto é, $mdc(a,m) = 1$, então, da Seção 3.4, Capítulo 3, Proposição 4, sabe-se que existem x e y inteiros tais que $ax + my = 1$. Consequentemente, $[a \cdot x + m \cdot y] = [1]$. Mas, $[a \cdot x + m \cdot y] = [a \cdot x] + [m \cdot y] = [a] \cdot [x] + [0] = [a] \cdot [x]$. Logo, $[a] \cdot [x] = [1]$. Portanto o inverso de $[a]$ é $[x]$ (ou qualquer representante deste).

Reciprocamente, se $[a]$ é invertível em $\mathbb{Z}_m$, existe $[x]$ tal que $[a] \cdot [x] = [1]$. Isto é o equivalente a escrever a congruência $ax \equiv 1\ (mod\ m)$. Ou seja, $m|(a \cdot x - 1)$ e isto implica que existe y inteiro onde $a \cdot x - 1 = m \cdot y$. Por fim, $a \cdot x + m \cdot (-y) = 1$. Fazendo uso, novamente, da Proposição 4, conclui-se que $mdc(a,m) = 1$. ■

Por fim, na próxima observação, um método de calcular inversos multiplicativos usando equações diofantinas.

Observação 15. Determinar o inverso multiplicativo de 7 módulo 40 é determinar um inteiro d, $0 < d \leq 40$ tal que $[7] \cdot [d] = 1$ ou, em outras palavras, $7 \cdot d \equiv 1(mod\ 40)$. Se esta congruência ocorre, então da Seção 3.7, Proposição 10, $40|(7 \cdot d - 1)$, isto é, existe $k \in \mathbb{Z}$ tal que $7 \cdot d - 1 = 40 \cdot k$ ou ainda $7 \cdot d - 40 \cdot k = 1$. No caso, apenas o valor inteiro de d é do interesse, encontrando $d = 23$ na resolução desta equação diofantina. Da mesma maneira, encontrar o inverso multiplicativo de 5 módulo 132 seria obter um inteiro d tal que $5 \cdot d \equiv 1(mod\ 132)$. Desta vez, o valor seria $d = 53$.

3.9 FUNÇÃO DE EULER

O método utilizado pelo RSA depende muito de um resultado que na Teoria dos Números é conhecido como Teorema de Euler. Tamanha é esta ligação que algumas novas reformulações deste resultado já são renomeadas como Teorema RSA. Este teorema será o objeto de estudo desta seção.

Definição 12. Denomina-se como função φ de Euler (lê-se função “fi” de Euler) aplicada a um inteiro n, ao número $\varphi(n)$ que representa a quantidade de números inteiros, entre 1 e $n - 1$ que são coprimos com n. Convenciona-se que $\varphi(1) = 1$.

Observação 16. A função φ de Euler é conhecida também como *Função Totiente*.

Exemplo: Para um número inteiro n "pequeno" é fácil calcular $\varphi(n)$. Pela Definição 12, basta contar quantos inteiros, entre 1 e $n-1$, são coprimos com n, isto é, $x \in \mathbb{Z}, 1 \leq x \leq n-1$, tal que $mdc(n,x)=1$. Assim, $\varphi(8)=4$, pois de 1 a 8 existem quatro números co-primos com 8 (1, 3, 5 e 7). Da mesma maneira, $\varphi(3)=2$, pois 3 é coprimo com 1 e 2.

A situação fica mais complexa se precisarmos calcular $\varphi(2600)$, por exemplo. Para isto, serão enunciadas algumas proposições que auxiliam nesta tarefa, generalizando o cálculo de $\varphi(n)$.

Proposição 17. O número p é primo, se e somente se, $\varphi(p)=p-1$.

Demonstração. Se p é primo, seus únicos divisores positivos são 1 e p. Analisando os inteiros entre 1 e $p-1$, p será coprimo com todos. Portanto, $\varphi(p)=p-1$.

Proposição 18. Se p é primo e se α é um inteiro positivo, então:

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

Demonstração. O objetivo é encontrar $\varphi(p^{\alpha})$, ou seja, a quantidade de números inteiros x, $1 \leq x \leq p^{\alpha}-1$, tal que $mdc(x,p^{\alpha})=1$. Desta maneira, $p \nmid x$. Então, adota-se outra estratégia, ao procurar pela quantidade de números inteiros y, $1 \leq y \leq p^{\alpha}-1$ que são divisíveis por p. Estes ocorrem em quantidade $p^{\alpha-1}$. Portanto, do total de números inteiros positivos menores que p^{α}, desconta-se a quantidade daqueles que são divisíveis por p, obtendo: $\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1}$ e concluindo a demonstração. ■

Baseado nos argumentos de Santos (2007, p.72-73) seguem as Proposições 19 e 20, enunciadas e demonstradas.

Proposição 19. Se m e n são inteiros positivos tais que $mdc(m,n)=1$, então $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Demonstração.

Vamos dispor os números de 1 até $m \cdot n$ da seguinte forma abaixo.

1	$m+1$	$2 \cdot m+1$	...	$m \cdot (n-1)+1$
2	$m+2$	$2 \cdot m+2$	...	$m \cdot (n-1)+2$
3	$m+3$	$2 \cdot m+3$	...	$m \cdot (n-1)+3$
$\vdots$	$\vdots$	$\vdots$	...	$\vdots$
r	$m+r$	$2 \cdot m+r$	...	$m \cdot (n-1)+r$
$\vdots$	$\vdots$	$\vdots$	...	$\vdots$
m	$2m$	$3m$	...	$m \cdot n$

Analisando cada uma das linhas r, $1 \leq r \leq m$, pode-se ignorar aquelas em que $mdc(r,m) \neq 1$. De fato, se $mdc(r,m) = d$ e $d > 1$, os elementos desta linha r são da forma $k \cdot m + r$, com $0 \leq r \leq n-1$. Como $d|r$ e $d|m$, todos os elementos desta linha serão divisíveis por d e nenhum deles será co-primo com $m \cdot n$.

Portanto, tem-se $\varphi(m)$ linhas onde todos os elementos são co-primos com m. Procurando, em cada uma destas $\varphi(m)$ linhas, quantos elementos são co-primos com n, observamos que $\{r, m+r, 2 \cdot m + r, \ldots, m \cdot (n-1) + r\}$ forma um sistema completo de resíduos módulo n (garantido pela Seção 3.8, Capítulo 15, Proposição 15). Logo, cada uma destas $\varphi(m)$ linhas possui $\varphi(n)$ elementos co-primos com n e, como eles são co-primos com m, são co-primos com $m.n$. Isto leva à $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Nesta demonstração, também foi usado que $mdc(r, m \cdot n) = 1$ se, e somente se, $mdc(r,m) = mdc(r,n) = 1$, que é um resultado da Seção 3.4, Proposição 5, item (ii). ■

Observação 17. Como conseqüência das Proposições 17 e 19, ao considerarmos um número inteiro $n = p \cdot q$, produto de dois primos, p e q, então $\varphi(n) = (p-1) \cdot (q-1)$. Este é um resultado fundamental na aplicação da Criptografia RSA.

Proposição 20. Considere n um número inteiro decomposto em fatores primos:

$$n = {p_1}^{a_1} \cdot {p_2}^{a_2} \cdot \ldots \cdot {p_m}^{a_m}$$

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

Demonstração. É uma consequência direta das Proposições 19 e 17, respectivamente, pois p_1, p_2, ..., p_m, são obviamente primos entre si. Assim:

$$\varphi(n) = \varphi({p_1}^{a_1}) \cdot \varphi({p_1}^{a_1}) \cdot \ldots \cdot \varphi({p_m}^{a_m})$$

$$= {p_1}^{a_1} \cdot \left(1 - \frac{1}{p_1}\right) \cdot {p_2}^{a_2} \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot {p_m}^{a_m} \cdot \left(1 - \frac{1}{p_m}\right)$$

$$= {p_1}^{a_1} \cdot {p_2}^{a_2} \cdot \ldots \cdot {p_m}^{a_m} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_m}\right)$$

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

Exemplo: Para determinar, respectivamente, $\varphi(37)$, $\varphi(55)$, $\varphi(243)$ e $\varphi(2600)$, pode-se proceder do seguinte modo:

- Como 37 é primo, pela Proposição 17, $\varphi(37) = 37 - 1 = 36$.

- Como $55 = 5 \cdot 11$ e $mdc\,(5{,}11) = 1$, pelas Proposições 17 e 19 tem-se $\varphi(55) = \varphi(5) \cdot \varphi(11) = (5-1) \cdot (11-1) = 40$.
- Como $243 = 3^5$, pela Proposição 18 encontra-se $\varphi(243) = 3^5 - 3^4 = 243 - 81 = 162$.
- Como $2600 = 2^3.5^2.13$, pode ser usada diretamente a Proposição 20; $\varphi(2600) = 2600 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{13}\right) = 960$.

3.9.1 Pequeno Teorema de Fermat e Teorema de Euler

Por fim, são trazidos dois teoremas que auxiliam nos cálculos de aritmética modular: o Teorema de Euler e o Pequeno Teorema de Fermat. A abordagem feita nas demonstrações pode ser vista em Santos (2007, p. 41 a 44). Iniciemos definindo o que é um sistema reduzido de resíduos.

Definição 13. Um sistema reduzido de resíduos módulo m é um conjunto de $\varphi(m)$ inteiros $\{r_1, r_2, \dots, r_{\varphi(m)}\}$ tais que cada elemento deste conjunto é relativamente primo com m, e se $i \neq j$, então $r_i \not\equiv r_j (mod\, m)$ - eles são, dois a dois, incongruentes módulo m.

Exemplo: O conjunto $\{0{,}1{,}2{,}3{,}4{,}5{,}6{,}7\}$ é um sistema completo de resíduos módulo 8. Já o conjunto $\{1{,}3{,}5{,}7\}$ é um sistema reduzido de resíduos módulo 8. Então, para obter um sistema reduzido de resíduos módulo m, basta retirar os elementos que não são co-primos com m de um sistema completo de resíduos módulo m.

Teorema 8. Seja a um número inteiro tal que $mdc(a, m) = 1$. Se $\{r_1, r_2, \dots, r_{\varphi(m)}\}$ é um sistema reduzido de resíduos módulo m, então $\{a \cdot r_1, a \cdot r_2, \dots, a \cdot r_{\varphi(m)}\}$ é, também, um sistema reduzido de resíduos módulo m.

Demonstração. Como $\{a \cdot r_1, a \cdot r_2, \dots, a \cdot r_{\varphi(m)}\}$ possui a mesma quantidade de $\varphi(m)$ elementos do conjunto $\{r_1, r_2, \dots, r_{\varphi(m)}\}$, deve-se mostrar que eles são, dois a dois, incongruentes módulo m, além de serem todos co-primos com m. Como $mdc(a, m) = 1$ e $mdc(r_i, m) = 1$ para i inteiro entre 1 e $\varphi(m)$, tem-se $mdc(a \cdot r_i, m) = 1$, (conforme Seção 3.4, Capítulo 3, Proposição 5, item (ii)) o que mostra que são todos co-primos com m. Para mostrar que são, dois a dois, incongruentes módulo m, percebe-se que se i e j são inteiros entre 1 e $\varphi(m)$, $a \cdot r_i \equiv a \cdot r_j (mod\, m)$ implica em $r_i \equiv r_j (mod\, m)$ (o "corte" na multiplicação é válido pois $mdc(a, m) = 1$, um resultado

da Seção 3.7, Capítulo 3, Proposição 13) e isto ocorre se, e somente se, $i = j$. Assim, $\{a \cdot r_1, a \cdot r_2, \dots, a \cdot r_{\varphi(m)}\}$ é, também, um sistema reduzido de resíduos módulo m. ■

Teorema 9 (Teorema de Euler). Sejam m e a inteiros, com $m > 1$ e $mdc(a, m) = 1$. Então,

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

Demonstração. No Teorema 8 verificou-se que se $X = \{r_1, r_2, \dots, r_{\varphi(m)}\}$, então $Y = \{a \cdot r_1, a \cdot r_2, \dots, a \cdot r_{\varphi(m)}\}$ é, também, um sistema reduzido de resíduos módulo m. Então, pode-se fazer uma correspondência entre os elementos destes conjuntos, de maneira que cada um dos elementos do conjunto X é congruente a exatamente (e apenas) um dos elementos do conjunto Y. Com isso, $a \cdot r_1 \cdot a \cdot r_2 \cdot \dots \cdot a \cdot r_{\varphi(m)} \equiv r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)} (mod\ m)$, resultando em $a^{\varphi(m)} \cdot r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)} \equiv r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)} (mod\ m)$.

O "corte" do produto $r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)}$, em ambos os lados da congruência, pode ser feito, pois todos os elementos do conjunto X são co-primos com m (assim como o produto dos mesmos). Então, tem-se $a^{\varphi(m)} \equiv 1 \ (mod\ m)$, concluindo a demonstração. ■

Teorema 10 (Pequeno Teorema de Fermat). Dado um número primo p e um número inteiro a, onde $p \nmid a$, temos que $p|(a^{p-1} - 1)$. Em termos de congruência modular, escrevemos $a^{p-1} \equiv 1 \ (mod\ p)$.

Demonstração. É uma consequência do Teorema de Euler. De fato, da Seção 3.8, Capítulo 3, Proposição 17, tem-se $\varphi(p) = p - 1$. Assim, se $p \nmid a$, $mdc(p, a) = 1$. Aplicando o Teorema de Euler, $a^{\varphi(p)} \equiv 1 \ (mod\ p)$ implica em $a^{p-1} \equiv 1 \ (mod\ p)$. ■

Corolário. Se p é primo e a é inteiro, então $p|(a^p - a)$. Em termos de congruência modular, escreve-se $a^p \equiv a \ (mod\ p)$.

Demonstração. Basta analisar dois casos: $p|a$ ou $p \nmid a$. Se $p|a$, então $p|(a \cdot (a^{p-1} - 1))$, de onde temos $a^p \equiv a \ (mod\ p)$. Se $p \nmid a$, então combina-se $a^{p-1} \equiv 1 \ (mod\ p)$ do teorema acima com $a \equiv a \ (mod\ p)$, para encontrar novamente $a^p \equiv a \ (mod\ p)$. ■

Observação 18. Na Seção 3.3, após o Teorema 1, uma das afirmações feitas foi que o resto da divisão de 7^{8400} por 5 era 1. Pode-se chegar a esta conclusão fazen-

do uso do Pequeno Teorema de Fermat. De fato, usando $a = 7$ e $p = 5$, tem-se $7^4 \equiv 1\ (mod\ 5)$. Como $7^{8400} = (7^4)^{2100}$, combina-se com resultado da Seção 3.7, Proposição 12, item (iii) para obter $7^{8400} \equiv 1\ (mod\ 5)$, ou seja, 7^{8400} deixa resto 1 na divisão por 5.

4 APLICANDO A CRIPTOGRAFIA RSA

A proposta deste capítulo é a de apresentar a metodologia da Criptografia RSA. Para facilitar a compreensão, primeiramente será feita a codificação da palavra UFSM, ilustrando a aplicação do método. Em seguida, há uma discussão sobre a fundamentação e o funcionamento do RSA.

4.1 O MÉTODO

O processo será dividido em três passos: pré-codificação, codificação e decodificação.

Exemplo: Codificação da palavra UFSM.

1º Passo: Pré-codificação.

O processo de pré-codificação consiste em converter as letras em números usando o Quadro 5, abaixo:

Quadro 5 - Convertendo caracteres em números.

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35
-	0	1	2	3	4	5	6	7	8	9		
36	37	38	39	40	41	41	43	44	45	46		

Fonte: (CARNEIRO, 2017, p.80).

Observação 19. O Quadro 5 é considerado adequado pois cada caractere (letra, número ou espaço) é representado por números com dois algarismos. Isto evita a ocorrência de ambiguidades. Um quadro onde o A fosse o 1, B fosse 2, C fosse 3, D fosse 4... traria alguns problemas. Continuando esta sequência, teríamos o N como 13; não saberíamos se 13 representa AC ou a letra N, por exemplo. Observe também que os espaços serão substituídos pelo número 36.

Continuando em nosso exemplo, a palavra UFSM fica convertida como 30152822, pois:

U	F	S	M
30	15	28	22

A seguir, são escolhidos dois primos distintos, p e q, conhecidos como parâmetros RSA. O produto dos mesmos, $n = p \cdot q$, gera o que é chamado de módulo RSA. Para fins de exemplo, escolheremos dois primos pequenos, $p = 11$ e $q = 5$, resultando em $n = 55$.

Por último, o número convertido, 30152822, é separado em blocos. A maneira como esta divisão em blocos é feita não é única, porém, cada bloco deve ser um número b menor que n. Além disso, deve ser evitado blocos que comecem pelo número zero (o que geraria problemas posteriores na decodificação). Opta-se pela divisão 30 – 1 – 52 – 8 – 22.

2º Passo: Codificação.

Na codificação usa-se o produto n (que neste exemplo é 55) e um número inteiro positivo e que seja inversível módulo $\varphi(n)$. Da Seção 3.9, Observação 17, sabe-se que se $n = p \cdot q$, então: $\varphi(n) = (p-1) \cdot (q-1)$. Já o número e deve ser escolhido tal que $mdc(\varphi(n), e) = 1$ (conforme Seção 3.8, Proposição 16). Então, calculamos: $\varphi(55) = (11-1) \cdot (5-1) = 40$. Escolhe-se $e = 7$. O par (n, e) é denominado chave pública do RSA.

Em seguida, cada um dos blocos é codificado separadamente. A codificação de um bloco b será denotada por $C(b)$, onde $C(b) \equiv b^e (mod\ n)$.

Para cada bloco, 30 – 1 – 52 – 8 – 22, tem-se:

- Bloco 30:

$$C(30) \equiv 30^7 (mod\ 55) \equiv (-25)^7 (mod\ 55) \equiv [(-25)^2]^3 \cdot (-25) (mod\ 55)$$
$$\equiv 625^3 \cdot (-25) (mod\ 55) \equiv 20^3 \cdot (-25) (mod\ 55)$$
$$\equiv 20^2 \cdot 20 \cdot (-25) (mod\ 55) \equiv 15 \cdot 20 \cdot (-25) (mod\ 55)$$
$$\equiv 300 \cdot (-25) (mod\ 55) \equiv 25 \cdot (-25) (mod\ 55) \equiv -625 \equiv 35\ (mod\ 55)$$

Portanto, $C(30) = 35$.

- Bloco 1:

$$C(1) \equiv 1^7 \equiv 1\ (mod\ 55).$$

Portanto, $C(1) = 1$.

- Bloco 52:

$$C(52) \equiv 52^7 (mod\ 55) \equiv [(-3)^2]^3 \cdot (-3) (mod\ 55) \equiv 9^3 \cdot (-3) (mod\ 55)$$
$$\equiv 729 \cdot (-3) (mod\ 55) \equiv 14 \cdot (-3) (mod\ 55) \equiv -42 \equiv 13\ (mod\ 55)$$

Portanto, $C(52) = 13$.

- Bloco 8:

$$C(8) \equiv 8^7 (mod\ 55) \equiv (8^2)^3 \cdot 8 (mod\ 55) \equiv 64^3 \cdot 8 (mod\ 55) \equiv 9^3 \cdot 8 (mod\ 55)$$
$$\equiv 729 \cdot 8 (mod\ 55) \equiv 14 \cdot 8 (mod\ 55) \equiv 112 \equiv 2\ (mod\ 55)$$

Portanto, $C(8) = 2$.

- Bloco 22:

$$C(22) \equiv 22^7 (mod\ 55) \equiv (22^2)^3 \cdot 22 (mod\ 55) \equiv 484^3 \cdot 22 (mod\ 55)$$
$$\equiv (-11)^3 \cdot 22 (mod\ 55) \equiv (-11)^2 \cdot (-11) \cdot 22 (mod\ 55)$$
$$\equiv 121 \cdot (-11) \cdot 22 (mod\ 55) \equiv 11 \cdot (-11) \cdot 22 (mod\ 55)$$
$$\equiv (-121) \cdot 22 (mod\ 55) \equiv 44 \cdot 22 (mod\ 55) \equiv 968 \equiv 33\ (mod\ 55)$$

Portanto, $C(22) = 33$.

Assim, a palavra UFSM foi codificada como 35 – 1 – 13 – 2 – 33.

3º Passo: Decodificação.

Agora, o objetivo é verificar que é possível voltar a mensagem original, ou seja, decodifica-la. Primeiramente, é preciso determinar o par (n, d), chamado de chave privada ou chave de decodificação. O número d é o inverso multiplicativo de e módulo $\varphi(n)$. Em outras palavras, temos que encontrar d tal que $e \cdot d \equiv 1 (mod\ \varphi(n))$. Em nosso exemplo, $e = 7$ e $\varphi(n) = 40$. Assim:

$$7 \cdot d \equiv 1 (mod\ 40) \Leftrightarrow 40 | (7 \cdot d - 1) \Leftrightarrow \exists\ k \in \mathbb{Z}; 7 \cdot d - 1 = 40 \cdot k \Leftrightarrow 7 \cdot d - 40 \cdot k = 1$$

Observa-se o aparecimento de uma equação diofantina, $7 \cdot d - 40 \cdot k = 1$ (onde o interesse é determinar o valor inteiro de d). Deve-se resolvê-la, acrescentando o fato que $0 < d < 40$. Por outro lado, estudando os inversos multiplicativos, não seria difícil obter $d = 23$ (conforme Seção 3.9, Observação 15).

Conhecido o par $(n, d) = (55, 23)$, usa-se como fórmula de decodificação: $D(a) \equiv a^d (mod\ n)$. Continuando, deve-se decodificar 35 – 1 – 13 – 2 – 33.

- Bloco 35:

$$D(35) \equiv 35^{23}(mod\ 55) \equiv (35^2)^{11} \cdot 35(mod\ 55) \equiv 15^{11} \cdot 35(mod\ 55)$$
$$\equiv (15^2)^5 \cdot 15 \cdot 35(mod\ 55) \equiv 225^5 \cdot 15 \cdot 35(mod\ 55)$$
$$\equiv 5^5 \cdot 15 \cdot 35(mod\ 55) \equiv 45 \cdot 15 \cdot 35(mod\ 55) \equiv 675 \cdot 35(mod\ 55)$$
$$\equiv 15 \cdot 35(mod\ 55) \equiv 525 \equiv 30\ (mod\ 55)$$

Portanto, $D(35) = 30$.

- Bloco 1:

$$D(1) \equiv 1^{23} \equiv 1\ (mod\ 55)$$

Portanto, $D(1) = 1$.

- Bloco 13:

$$D(13) \equiv 13^{23}(mod\ 55) \equiv (13^2)^{10} \cdot 13^2 \cdot 13(mod\ 55) \equiv 169^{10} \cdot 4 \cdot 13(mod\ 55)$$
$$\equiv 4^{10} \cdot 52(mod\ 55) \equiv (4^4)^2 \cdot 4^2 \cdot 52(mod\ 55)$$
$$\equiv (-19)^2 \cdot 16 \cdot 52(mod\ 55) \equiv 361 \cdot 16 \cdot 52(mod\ 55)$$
$$\equiv (-24) \cdot 16 \cdot 52(mod\ 55) \equiv 1 \cdot 52 \equiv 52\ (mod\ 55)$$

Portanto, $D(13) = 52$.

- Bloco 2:

$$D(2) \equiv 2^{23}(mod\ 55) \equiv (2^{10})^2 \cdot 2^3(mod\ 55) \equiv (-21)^2 \cdot 8(mod\ 55) \equiv 441 \cdot 8(mod\ 55)$$
$$\equiv 1 \cdot 8(mod\ 55) \equiv 8\ (mod\ 55)$$

Portanto, $D(2) = 8$.

- Bloco 33:

$D(33) \equiv 33^{23}(mod\ 55) \equiv (-22)^{23}(mod\ 55) \equiv [(-22)^2]^{11} \cdot (-22)(mod\ 55) \equiv$
$484^{11} \cdot (-22)(mod\ 55) \equiv (-11)^{11} \cdot (-22)(mod\ 55) \equiv [(-11)^3]^3 \cdot (-11)^2 \cdot$
$(-22)(mod\ 55) \equiv 2 \cdot 11^3(mod\ 55) \equiv 2 \cdot 11 \equiv 22\ (mod\ 55)$.

Portanto, $D(33) = 22$.

Por fim, verifica-se que o processo de decodificação de fato levou à mensagem original pré-codificada: 30 – 1 – 52 – 8 – 22. De acordo, com o Quadro 5, tem-se:

30	15	28	22
U	F	S	M

4.2 FUNDAMENTAÇÃO DA CRIPTOGRAFIA RSA

Na seção anterior, o método RSA foi posto em prática a partir de um exemplo. Também foram definidos o par (n, e) como a chave pública do sistema RSA e o par (n, d) como a chave privada. A chave pública, como o próprio nome sugere, pode ser conhecida por todos.

Assim, conforme Shokranian (2012, p. 48), no RSA, a comunicação entre duas fontes, A e B, está baseada no uso destas chaves. Resumindo:

1) A fonte B conhece a chave pública, (n, e), da fonte A.

2) A fonte B pré-codifica a mensagem, convertendo-a em números, usando uma tabela que também deve ser conhecida por A. A mensagem deve ser quebrada em blocos b, sendo b menor que n.

3) Usando a fórmula de codificação, $C(b) \equiv b^e \equiv a\ (mod\ n)$, para cada bloco b, temos $C(b) = a$. Estes blocos codificados são transmitidos para A.

4) Ao receber os códigos, a fonte A os decodifica usando $D(a) \equiv a^d (mod\ n)$. A chave privada (n, d) é conhecida apenas por A. Como A usa a mesma tabela de pré-codificação de B, fará o caminho inverso para encontrar a mensagem original.

4.2.1 Por que o método funciona?

Mostrar que o método funciona é mostrar que, respeitando as condições do RSA, sempre é possível retornar à mensagem original. De fato, quando se codifica um bloco b, obtém-se um bloco $C(b) = a$, resultado da fórmula de codificação: $C(b) \equiv b^e \equiv a\ (mod\ n)$. E quando se decodifica o bloco a, aplicando a fórmula de decodificação $D(a) \equiv a^d (mod\ n)$, retorna-se ao bloco b, isto é, $D(a) = b$.

Por que é possível afirmar que isto sempre ocorrerá? Em outras palavras, é preciso mostrar que:

$$D\big(C(b)\big) \equiv b (mod\ n)\ (I)$$

A congruência acima é suficiente para concluir que $D\big(C(b)\big) = b$, pois tanto para b quanto para $D\big(C(b)\big)$, tem-se $0 \leq b \leq n-1$ e $0 \leq D(C(b)) \leq n-1$. Decorre daqui a necessidade imposta de que os blocos b sejam números menores que n.

Segue-se na explicação:

$$D\big(C(b)\big) \equiv (C(b))^d \equiv (b^e)^d \equiv b^{e \cdot d}\ (mod\ n)\ (II)$$

Por outro lado, nota-se que d é inverso multiplicativo de $\varphi(n)$, ou seja:

$$e \cdot d \equiv 1 \left(mod\ \varphi(n)\right) \Leftrightarrow \varphi(n) | (ed - 1) \Leftrightarrow \exists k \in \mathbb{Z}; e \cdot d - 1 = \varphi(n) \cdot k \Leftrightarrow e \cdot d = \varphi(n) \cdot k + 1\ (III)$$

De (III) em (II), conclui-se que:

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

Agora, podem ser considerados dois casos:

1º caso: b e n são primos entre si, isto é, $mdc(b,n) = 1$. Então, aplica-se o Teorema de Euler (Subseção 3.9.1, Teorema 9), encontrando:

$$b^{\varphi(n)} \equiv 1\ (mod\ n)\ (V)$$

Sabendo que $b \equiv b\ (mod\ n)$, chega-se em:

$$b^{\varphi(n)}.b \equiv b\ (mod\ n)\ (VI)$$

Combinando os resultados de (IV) e (VI), a verificação de que $D\big(C(b)\big) \equiv b(mod\ n)$ será obtida.

2º caso: b e n não são primos entre si. Lembrando que $n = p \cdot q$ e $\varphi(n) = (p-1) \cdot (q-1)$, reescreve-se $D(C(b)) \equiv b^{e \cdot d}\ (mod\ n) \equiv b^{\varphi(n) \cdot k} \cdot b\ (mod\ n)$ como:

$$D\big(C(b)\big) \equiv b^{(p-1)\cdot(q-1)\cdot k} \cdot b\ (mod\ pq)\ (VII)$$

O resultado em (VII) pode ser analisado de duas maneiras:

$$D\big(C(b)\big) \equiv b^{(p-1)\cdot(q-1)k}.b\ (mod\ p)\ (VIII)$$

E, com raciocínio que será análogo:

$$D\big(C(b)\big) \equiv b^{(p-1)\cdot(q-1)\cdot k} \cdot b\ (mod\ q)\ (IX)$$

Para mostrar que a congruência $(VIII)$ resultará em $D\big(C(b)\big) \equiv b(mod\ p)$, percebe-se que se $p|b$, então $b \equiv 0\ (mod\ p)$. Logo, p divide qualquer potência de b, em particular, $b^{(p-1)\cdot(q-1)k} \cdot b \equiv 0\ (mod\ p)$. Consequentemente, $D\big(C(b)\big) \equiv b^{(p-1)\cdot(q-1)\cdot k} \cdot b\ \equiv b\ (mod\ p)$.

Caso $p \nmid b$, reescreve-se $(VIII)$ como:

$$D\big(C(b)\big) \equiv b^{(p-1)\cdot(q-1)\cdot k} \cdot b \equiv (b^{(p-1)})^{q-1} \cdot b\ (mod\ p)\ (X)$$

Pelo Pequeno Teorema de Fermat (Subseção 3.9.1, Teorema 10):

$$b^{p-1} \equiv 1\ (mod\ p) \text{ e } (b^{(p-1)})^{q-1} \equiv 1\ (mod\ p)\ (XI)$$

Combinando (X) e (XI) chega-se em:

$$D\big(C(b)\big) \equiv b(mod\ p)\ (XII)$$

Argumentos análogos levam (IX) à:

$$D\big(C(b)\big) \equiv b(mod\ q)\ (XIII)$$

Por fim, usando a Seção 3.7, Proposição 14, item (ii) e do fato que p e q são primos (o MMC entre eles será $n = p \cdot q$, um resultado garantido pela Seção 3.4, Proposição 6), temos que (XII) e $(XIII)$ implicam em:

$$D\big(C(b)\big) \equiv b(mod\ p \cdot q) \equiv b(mod\ n)$$ ■

4.2.2 Sobre a segurança do RSA

No exemplo da Seção 4.1 foram usados números primos pequenos. Mesmo assim, uma boa dose de cálculos é gerada, aplicando várias das propriedades da Aritmética Modular. Porém, neste exemplo o nível de segurança é extremamente baixo, visto que seria relativamente simples descobrir o valor de d. Qualquer um conheceria a chave privada (n, d).

Por isto, na implementação do método RSA, os primos p e q envolvidos são muito grandes (números com mais de 200 algarismos). Consequentemente, o número $n = p \cdot q$ é maior ainda.

Como dito anteriormente, qualquer um pode conhecer a chave privada (n, e). Com esta conhecida, alguém que estivesse determinado a quebrar o código, deveria determinar o número inteiro d, inverso multiplicativo de e módulo $\varphi(n) = (p-1) \cdot (q-1)$. Para isto, deve conhecer os primos p e q; em outras palavras, deve saber como fatorar n. É aqui que se apóia a segurança do RSA, sendo que até o momento não são conhecidos métodos realmente eficientes para a fatoração de números suficientemente grandes.

De fato, para $n = 55$ não é difícil descobrir que os primos envolvidos são 5 e 11. No entanto, como decompor em fatores primos o número 313093757? Neste exemplo, os primos envolvidos nem foram tão grandes assim: 15559 e 20123.

Diante disto, um pensamento natural é que, com a tecnologia atual, qualquer computador deve realizar esta decomposição em poucos segundos. Porém, mesmo para um computador, com os algoritmos de fatoração disponíveis, este processo poderia levar anos. A Tabela 1 a seguir traz uma ideia desta dificuldade.

Tabela 1 – Tempo estimado de fatoração.

Quantidade de dígitos do número n	Número de operações	Tempo estimado de fatoração
50	$1{,}4.10^{10}$	3,9 horas
70	$9{,}0.10^{12}$	104 anos
100	$2{,}3.10^{15}$	740 anos
200	$1{,}2.10^{23}$	$3{,}8.10^{9}$ anos
300	$1{,}5.10^{29}$	$4{,}9.10^{15}$ anos
500	$1{,}3.10^{39}$	$4{,}2.10^{25}$ anos

Fonte: (CARNEIRO, 2017, p.84).

Um exemplo disto foi o que ficou conhecido como “desmascaramento do RSA 129”. Tratava-se de um número de 129 algarismos, que os autores do sistema RSA tornaram público, lançando-o como desafio no final da década de 1970. Um grupo de 600 matemáticos, com a ajuda de 1600 voluntários recrutados na Internet conseguiram decompor o número, utilizando o processamento dos computadores destes voluntários em períodos de inatividade. O resultado foi publicado em abril de 1994, após descoberta dos primos envolvidos. Os autores do RSA continuaram propondo desafios com números bem maiores, oferecendo prêmios que chegavam a US$ 200000,000 (duzentos mil dólares americanos).

Então, quanto mais algarismos forem usados na chave, provavelmente será mais confiável, mas também traz o inconveniente de que o processo de decodificação se torne mais lento.

Assim, restam duas saídas para “quebrar” o RSA: descobrir técnicas promissoras de decomposição em fatores primos ou investir em tecnologias que possam acelerar as operações da Tabela 1. Neste sentido, existe muita pesquisa em volta de uma forma radicalmente nova de computador, o computador quântico. Acredita-se que o computador quântico será capaz de fazer cálculos com uma velocidade tão grande que fará os supercomputadores modernos literalmente coisas do passado. Enquanto estas técnicas e tecnologias não surgirem, a segurança do RSA estará garantida.

4.2.3 Sobre a escolha dos parâmetros do RSA

Para facilitar o cálculo de d, inverso multiplicativo de e módulo $\varphi(n) = (p-1)\cdot(q-1)$, pode-se delimitar que tipo de primos p e q serão escolhidos. Por exemplo, ao optar por primos da forma $6\cdot x+5$, com $x \in \mathbb{N}$ e o número $e=3$, garante-se a existência de d, além de um algoritmo para o cálculo do mesmo. Observe que se p e q são da forma $6\cdot x+5$, com $x \in \mathbb{N}$, então $p \equiv 5\ (mod\ 6)$ e $q \equiv 5\ (mod\ 6)$. Consequentemente:

$$p-1 \equiv 4\ (mod\ 6) \text{ e } q-1 \equiv 4\ (mod\ 6)\ (I)$$

Para determinar $\varphi(n) = (p-1)\cdot(q-1)$, calcula-se:

$$(p-1)\cdot(q-1) \equiv 16 \equiv 4\ (mod\ 6)\ (II)$$

Com isto, $\varphi(n) \equiv 4\ (mod\ 6)$, ou seja, $6|(\varphi(n)-4)$ e assim, existe um k inteiro tal que $\varphi(n) = 6\cdot k+4$. Por outro lado, é necessário determinar d, onde $e\cdot d \equiv 1\ (mod\ \ \varphi(n))$. Como fixamos $e=3$:

$$3\cdot d \equiv 1\ (mod\ \ (6\cdot k+4))\ (III)$$

Assim, de $\varphi(n) = 6\cdot k+4 = 3\cdot(2\cdot k+1)+1$, tem-se $3\cdot(2\cdot k+1) \equiv -1\ (mod\ (6\cdot k+4))$ que implica em:

$$3\cdot(-2\cdot k-1) \equiv 1\ (mod\ (6\cdot k+4))\ (IV)$$

Mas, $-2\cdot k-1 \equiv 4\cdot k+3\ (mod\ (6\cdot k+4))$. Portanto, concluímos que:

$$3\cdot(4\cdot k+3) \equiv 1\ (mod\ (6\cdot k+4))\ (V)$$

Desta maneira, (III) e (V) fornecem uma forma de calcular $d = 4\cdot k+3$, conhecendo os primos p e q. O k é encontrado de $(p-1)\cdot(q-1) = 6\cdot k+4$.

Assim, por exemplo, caso a escolha fosse $e=3$, $p=29$ e $q=23$ (dois primos da forma $6\cdot x+5,\ x \in \mathbb{N}$), seria fácil deduzir a chave privada. Primeiramente, encontra-se k:

$$(29-1)\cdot(23-1) = 616 = 6\cdot k+4 \Rightarrow k = 102$$

Como $d = 4\cdot k+3$, $d=411$. A chave privada será (667, 411).

5 PROPOSTA DE ENSINO

Este capítulo abordará uma proposta de ensino aplicada aos alunos do Colégio Militar de Porto Alegre (CMPA), voluntários de um Clube de Matemática. Este grupo conta com 15 alunos participantes, oriundos dos 8º e 9º ano do Ensino Fundamental.

Com o objetivo de trazer uma aplicação da Aritmética, foi criado um "minicurso" intitulado "Criptografia RSA e Teoria dos Números", dividido em treze aulas de duas horas cada. Cada aluno recebeu um material de apoio, em forma de apostila, que trazia os pré-requisitos necessários para entender o RSA. Este minicurso seguiu a seguinte distribuição:

Aula I: Introdução à Criptografia.

Aula II: Introdução à Criptografia (continuação).

Aula III: Divisibilidade nos números inteiros.

Aula IV: Máximo Divisor Comum (MDC) e Mínimo Múltiplo Comum (MMC).

Aula V: Números primos e o Teorema Fundamental da Aritmética.

Aula VI: Equações diofantinas.

Aula VII: Aritmética dos restos.

Aula VIII: Pequeno Teorema de Fermat e exercícios de Aritmética dos restos.

Aula IX: Inversos multiplicativos e o Teorema de Euler.

Aula X: Aplicando a Criptografia RSA.

Aula XI: Aplicando a Criptografia RSA (continuação).

Aula XII: Entendendo por que a Criptografia RSA funciona.

Aula XIII: Conclusão e questionamentos.

De uma maneira geral, ao elaborar esta proposta de ensino, “começou-se pelo final”: a partir do conhecimento teórico necessário para aplicar e entender o RSA, os assuntos foram escolhidos; tópicos mais elementares como divisibilidade nos inteiros, MDC e MMC puderam ganhar um tratamento mais formal, onde foram propostas pequenas demonstrações, estimulando o pensamento matemático.

O que seguirá em cada seção são os planos de aula, descrevendo a metodologia empregada, além de trazer os objetivos e um relato do que pôde ser observado.

5.1 PLANO DE AULA I

Duração: duas horas/aula de cinquenta minutos cada.

Conteúdo: Introdução à Criptografia.

Objetivos: apresentar conceitos básicos como Criptografia, Criptoanálise, Criptologia, cifra de transposição e cifra de substituição. Motivar o ensino da Aritmética, por meio de uma aplicação bastante atual, destacando aspectos históricos que ilustram sua aplicabilidade e validade. Fazer uso de métodos de criptografia simétrica simples, como a cifra de César, cifrando ou decifrando mensagens curtas.

Desenvolvimento: os conceitos, a parte histórica e os exemplos serão transmitidos por meio de apresentação *Power Point*, servindo como apoio aos textos da apostila. Entre os temas escolhidos estão o uso da Máquina Criptográfica Enigma na Segunda Guerra Mundial, o telegrama Zimmermann e as cifras de Beale – discutidas, respectivamente, nos Apêndices A, B e C. Um dos principais pontos desta aula será o estudo de análise de frequências (Subseção 2.1.1, Quadro 3) de cada letra de nosso alfabeto e como isto ajuda a quebrar cifras como a de César.

Avaliação: serão propostos alguns exercícios, presentes na apostila, com o objetivo de fixar os métodos criptográficos apresentados e estimular o raciocínio dos alunos. Seguem os exercícios da Aula I, incluídos aqui por serem de minha autoria (com exceção do Exercício 7).

Exercício 1. Usando o método de criptografia de transposição do Exemplo 1 (o mesmo da Subseção 2.1.1), decifre as mensagens abaixo:

a) UAIT#ARTCANGARCANMBITMTIOLIEON - palavra-chave ENIGMA.

b) DECRUVEFVODRDOMIICEA - palavra-chave SORTE.

Exercício 2. Decifre as mensagens abaixo sabendo que foram cifradas usando a técnica "cerca de ferrovia" (ver Apêndice E).

a) PEAAAPROIPAARPRCOAALMIDS.

b) BMUACFADBAEOEIMESMLSSIEQESIRSEELPDRASRIPEASM.

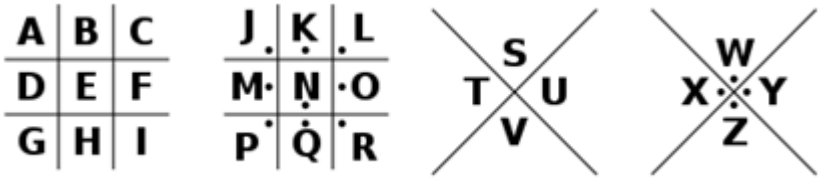
Exercício 3. Decifre as mensagens abaixo sabendo que foram escritas utilizando cifras de substituição de César (ver Subseção 2.1.1, Exemplo 2).

a) IHZAHHWSPJHYHUHSPZLKLMYLXBLUJPH.

b) ZQYEQYBDQQFDUHUMX.

c) GUMPIWYWIHMYAOCOJULUVYHM.

Exercício 4. Existem diversas formas de criptografia de substituição monoalfabética, e uma das mais famosas é a cifra do chiqueiro (*pigpen,* em inglês), conhecida também por ter sido usada entre maçons. Ela usa símbolos no lugar de letras. No entanto, como todas cifras do mesmo tipo, pode ser facilmente quebrada usando análise de frequência. A seguir, a chave e um exemplo.



C	I	F	R	A	D	O	C	H	I	Q	U	E	I	R	O
∟	⌜	⊏	⌝	⌟	⌐	⊡	∟	⊓	⌜	⌝	<	□	⌜	⌝	⊡

Devido ao seu uso simples, ficou popular entre estudantes e agora você também pode usá-la.

Exercício 5. Utilizando o quadrado de Vigenère (ver Apêndice F), cifre ou decifre as frases abaixo, de acordo com as palavras-chave propostas:

a) A PEDRA DE ROSETA E OS HIERÓGLIFOS EGÍPCIOS, palavra-chave FAROL.

b) O TELEGRAMA ZIMMERMANN E A PRIMEIRA GUERRA MUNDIAL, palavra-chave MUNDO.
c) NSWZGZRTMAUSXRVTXHIILHHJAWMTUOD, palavra-chave LETRA.

Exercício 6. A cifra ADFGVX é uma forma de criptografia em que é usada, ao mesmo tempo, transposição e substituição. Nela, uma tabela 6X6 é preenchida aleatoriamente com 26 letras e 10 dígitos. Cada linha e cada coluna é identificada por uma das seis letras: A, D, F, G, V e X. A tabela formada é a chave, ou seja, deve ser de conhecimento tanto do emissor quanto do receptor. Além disso, há uma segunda parte de cifragem, onde uma palavra-chave deve ser escolhida. Observe um exemplo:

	A	**D**	**F**	**G**	**V**	**X**
A	e	1	b	r	t	8
D	q	3	c	v	w	4
F	s	z	a	0	f	g
G	p	y	d	9	i	5
V	m	o	j	2	k	7
X	u	r	n	l	6	x

Cada letra ou número do texto original será codificada por um par de letras combinando linha e coluna. Assim, por exemplo, a letra "c" será substituída por DF, enquanto o dígito 3 será substituído por DD. Uma mensagem informando posição através da latitude (LT) e longitude (LG) poderia ser transmitida como LT30LG51:

L	T	3	0	L	G	5	1
XG	AV	DD	FG	XG	FX	GX	AD

Até aqui, usamos cifra de substituição. O que torna a criptoanálise muito mais complexa é a segunda parte, em que é aplicada cifra de transposição. Em nosso exemplo, escolhemos a palavra-chave CANO e aplicamos o processo do Exemplo 1 (Subseção 2.1.1).

2	**1**	**3**	**4**
C	**A**	**N**	**O**
X	G	A	V
D	D	F	G
X	G	F	X
G	X	A	D

Por fim, LT30LG51 ficará cifrada como GDGXXDXGAFFAVGXD. Esta mensagem cifrada será transmitida por código Morse e o receptor, conhecendo a tabela e palavras-chave, faz o processo reverso. O motivo da escolha das letras ADFGVX no lugar de ABCDEF, por exemplo, é que elas são muito diferentes quando transmitidas em código Morse, evitando erros em sua transmissão.

Sendo assim, tente decifrar a mensagem DVDDFXFXVVAVDFFADFAF utilizando a mesma tabela e palavra-chave deste exercício.

Exercício 7. (OBMEP 2007 - 2ª fase) Um antigo método para codificar palavras consiste em escolher um número de 1 a 26, chamado chave do código, e girar o disco interno do aparelho ilustrado na figura até que essa chave corresponda à letra A. Depois disso, as letras da palavra são substituídas pelos números correspondentes, separados por tracinhos. Por exemplo, na figura ao lado a chave é 5 e a palavra PAI é codificada como 20-5-13.

a) Usando a chave indicada na figura, descubra qual palavra foi codificada como 23-25-7-25-22-13.

b) Codifique OBMEP usando a chave 20.

c) Chicó codificou uma palavra de 4 letras com a chave 20, mas esqueceu-se de colocar os tracinhos e escreveu 2620138. Ajude Chicó colocando os tracinhos que ele esqueceu e depois escreva a palavra que ele codificou.

d) Em uma outra chave, a soma dos números que representam as letras A, B e C é 52. Qual é essa chave?

RESPOSTAS DOS EXERCÍCIOS DA AULA I.

01. a) Alan Turing matemático britânico. b) Duvido você me decifrar.

02. a) Preparação para olimpíadas. b) Bem que as cifras de Beale poderiam ser simples assim.

03. a) Basta aplicar análise de frequência. b) Nem sempre é trivial. c) Mas você conseguiu, parabéns.

05. a) FPVRCFDVFZXEKOPTSYWPWOXZTKOJSRNPTWZX.

b) ANROSSLNPOLCZPSDGNQBQUCUWYYVUOSORUFMGHQRUUY.

c) CÓDIGO NAVAJO E A VITÓRIA DOS ALIADOS.

06. REFORÇOS JÁ.

07. a) SUCURI. b) 8-21-6-24-9 c) 26-20-13-8; GATO. d) 25.

Análise e observações da Aula I: a recepção ao tema foi bem positiva. Os alunos ficaram motivados com o assunto, com questionamentos pertinentes durante toda aula. A máquina Enigma, por exemplo, despertou muita curiosidade, pois a maioria já sabia de sua existência, vide sua popularidade nos últimos anos, presente em documentários e filmes - como o "Jogo da Imitação", de 2014 - e pretendia entender melhor seu funcionamento. Como este não era o foco, foram indicados o vídeo "Demonstração da Máquina Enigma - Museu da UFRGS", disponível em: <https://www.youtube.com/watch?v=VMJeDLv2suw>, acesso em 04 mar. 2018 e o aplicativo para *smartphone Enigma Simulator*, disponível de forma gratuita para os interessados em um maior aprofundamento.

Por outro lado, o ápice desta aula foi na resolução de exercícios. Os alunos não demonstraram grandes dificuldades, mas pode-se perceber muito entusiasmo na execução da atividade.

5.2 PLANO DE AULA II

Duração: duas horas/aula de cinquenta minutos cada.

Conteúdo: Introdução à Criptografia (continuação).

Objetivos: dar sequência à aula anterior, acrescentando o conceito de criptografia assimétrica, criptografia de chave pública e privada, além de um histórico de

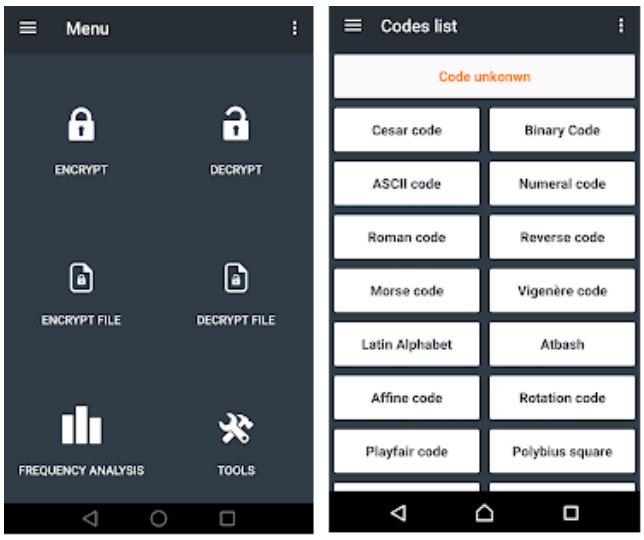
modernização que culminará no método RSA. Destacar o uso da criptografia nos dias atuais relacionando-a à tecnologia e à informação.

Desenvolvimento: uso de apresentação *Power Point* para ilustrar o texto presente na apostila. Apresentação do aplicativo para *smartphone Decrypto*, uma ferramenta gratuita que codifica e decodifica com facilidade mensagens criptografadas por diferentes métodos, inclusive alguns dos vistos na aula anterior.

Avaliação: uso do aplicativo *Decrypto* para codificar/decodificar as mensagens da aula anterior, além de propiciar que os alunos também criassem mensagens próprias com certa facilidade. O aplicativo foi apresentado apenas na segunda aula para não atrapalhar a resolução dos exercícios da primeira aula.

Análise e observações da Aula II: os alunos gostaram do uso do aplicativo *Decrypto*; ao final da aula usavam-no para transmitir mensagens codificadas uns para os outros (uma possibilidade do aplicativo). Apesar da linguagem em inglês, a interface (Figura 2) é simples e intuitiva, não sendo obstáculo para os alunos. Há diversos aplicativos semelhantes. O *Decrypto* foi apenas uma sugestão.

Figura 2 – Interface do aplicativo *Decrypto*.



Fonte: o autor.

O entusiasmo visto na aula anterior manteve-se, principalmente pelo argumento de que a tecnologia estava aliada à criptografia, visto a correspondência via *e-mail* e compras *online*. Por fim, esta aula trouxe a conclusão de que um bom

entendimento do RSA necessitava de certo domínio sobre ferramentas de Teoria dos Números que seriam aprendidas a partir da terceira aula.

5.3 PLANO DE AULA III

Duração: duas horas/aula de cinquenta minutos cada.

Conteúdo: Divisibilidade nos números inteiros.

Objetivos: definir divisibilidade para os números inteiros. Apresentar o Algoritmo da Divisão. Definir números primos.

Desenvolvimento: além de apresentar os temas em questão, serão trabalhadas questões da OBMEP e OBM. Será usado apenas quadro branco e caneta para expor teoria e exercícios que os alunos acompanharão pela apostila.

Avaliação: lista de exercícios selecionados sobre o tema de aula.

Análise e observações da Aula III: a aula transcorreu normalmente, bem mais expositiva por parte deste professor do que as anteriores. Porém os alunos têm ciência do cronograma de treze aulas; sabem do caminho a ser percorrido e já foram orientados da importância teórica de aulas como esta.

5.4 PLANO DE AULA IV

Duração: duas horas/aula de cinquenta minutos cada.

Conteúdo: Máximo Divisor Comum (MDC) e Mínimo Múltiplo Comum (MMC).

Objetivos: definir MDC e MMC. Apresentar propriedades do MDC e o Algoritmo de Euclides. Relacionar MDC e MMC.

Desenvolvimento: além de apresentação dos temas em questão, serão trabalhadas questões da OBMEP e OBM. Será usado apenas quadro branco e caneta para expor teoria e exercícios que os alunos acompanharão pela apostila.

Avaliação: lista de exercícios selecionados sobre o tema da aula.

Análise e observações da Aula IV: a ênfase da aula foi sobre o cálculo e as propriedades do MDC. A menção ao MMC foi apenas oportuna na resolução de alguns exercícios.

5.5 PLANO DE AULA V

Duração: duas horas/aula de cinquenta minutos cada.

Conteúdo: Números primos e o Teorema Fundamental da Aritmética.

Objetivos: destacar a importância do Teorema Fundamental da Aritmética e do estudo sobre números primos.

Desenvolvimento: além da resolução de alguns exercícios, esta aula trará questionamentos sobre pesquisa em Matemática, a importância do raciocínio, da formulação (e comprovação ou não) de hipóteses.

Avaliação: lista de exercícios selecionados sobre o tema da aula.

Análise e observações da Aula V: a menção aos primos de Fermat, de Mersenne e a existência de primos com milhares de casas, bem como as tentativas de encontrar métodos mais eficientes na decomposição em fatores primos e um algoritmo ou "fórmula para construir números primos" despertaram o interesse de alguns alunos, o que pode ser considerado um ponto positivo.

5.6 PLANO DE AULA VI

Duração: duas horas/aula de cinquenta minutos cada.

Conteúdo: Equações diofantinas.

Objetivos: definir e resolver equações diofantinas.

Desenvolvimento: serão listados exemplos de resolução de equações diofantinas.

Avaliação: lista de exercícios selecionados sobre o tema da aula.

Análise e observações da Aula VI: os temas das aulas III a V discutiam conceitos e propriedades familiares aos alunos. Neste sentido, a resolução de equações diofantinas fugiu um pouco do que eles estavam acostumados. Por outro lado, procurou-se não atrapalhar o raciocínio e perspicácia da turma. Assim, a construção desta aula foi interessante. Antes de discutir um método de resolução geral, foram propostas algumas equações diofantinas do tipo $a \cdot x + b \cdot y = c$ (algumas delas sem resolução para x e y inteiros), verificando que os alunos apresentavam diferentes métodos na resolução das mesmas: tentativa e erro, atribuição de valores aleatórios, estudar soluções possíveis devido aos critérios de divisibilidade dos números envolvidos, etc. Este é um tema que aparece com certa frequência em olimpíadas, porém, geralmente com restrições que permitem soluções específicas. Nesta aula, este paralelo pôde ser realizado, enriquecendo o aprendizado.

5.7 PLANO DE AULA VII

Duração: duas horas/aula de cinquenta minutos cada.

Conteúdo: Aritmética modular.

Objetivos: apresentar a definição de congruência modular e as propriedades e resultados que decorrem desta definição.

Desenvolvimento: a validade das propriedades da aritmética modular será reforçada com diversos exemplos, visando a fixação por parte dos alunos.

Avaliação: questionamentos aos alunos.

Análise e observações da Aula VII: esta é possivelmente uma das aulas mais importantes no que se refere ao entendimento dos cálculos envolvidos na aplicação do RSA. Ainda no planejamento do curso como um todo, sabia-se do destaque que esta aula deveria ter. Assim, a abordagem foi bem dinâmica, procurando a todo momento verificar o entendimento dos alunos. Alguns alunos já tinham

conhecimento; não foi um assunto totalmente novo para todos. Particularmente, dois alunos já dominavam bem as técnicas envolvidas.

5.8 PLANO DE AULA VIII

Duração: duas horas/aula de cinquenta minutos cada.

Conteúdo: Pequeno Teorema de Fermat e exercícios de Aritmética dos restos.

Objetivos: apresentar o Pequeno Teorema de Fermat como ferramenta da aritmética modular. Resolver exercícios envolvendo restos obtidos na divisão euclidiana por potências.

Desenvolvimento: a aula anterior teve como objetivo apresentar a teoria e a resolução de alguns exemplos práticos. Nesta aula, todos os exercícios serão resolvidos pelos alunos. Haverá correção e orientações no final da aula.

Avaliação: lista de exercícios selecionados sobre o tema da aula.

Análise e observações da Aula VIII: Durante os exercícios, questões como "determinar o resto da divisão de 22^5 por 161" serão frequentes, pois aparecerão nos cálculos dos exemplos das aulas X e XI. Além disso, alguns exercícios de olimpíadas e de concursos também foram aplicados e resolvidos, ilustrados pelos três exercícios abaixo (trazidos neste ponto do trabalho para uma noção geral do nível trabalhado, sendo que nem todas as questões da apostila, inclusive de outras aulas, poderiam aparecer aqui).

Exercício 1 (ORM RS 2012). Achar todos os inteiros positivos n, tais que 7 é divisor de $6^n + 8^n$.

Solução

Observa-se que $6 \equiv -1(mod\ 7)$ e $8 \equiv 1\ (mod\ 7)$. Logo:

$$6^n \equiv (-1)^n (mod\ 7) \text{ e } 8^n \equiv 1^n (mod\ 7)$$

Decorrente disto, tem-se $6^n + 8^n \equiv 0(mod\ 7)$ sempre que n for ímpar.

Portanto, sempre que n for ímpar, 7 é um divisor de $6^n + 8^n$.

Exercício 2 (OBM 2012). Para homenagear a Copa do Mundo e as Olimpíadas no Brasil, Esmeralda, a prefeita da cidade Gugulândia, decidiu que seria feriado em sua

cidade no dia x do mês de número y, onde x é o último algarismo do número 2016^{2014} e y é o resto de 2014^{2015} na divisão por 11. Assim, esse feriado será no dia:

(A) 8 de março (B) 6 de janeiro (C) 4 de janeiro (D) 6 de abril
(E) 6 de março

Observação: O mês de janeiro corresponde ao mês de número 1 e assim por diante.

Solução

O último algarismo de 2016^{2014} é 6, pois qualquer potência de 6 segue este padrão.

Analisando o resto de 2014^{2015}por 11, tem-se: $2014 \equiv 1\ (mod\ 11)$. Por fim, $2014^{2015} \equiv 1\ (mod\ 11)$.

Ou seja, 2014^{2015} deixa resto 1 na divisão por 11. O feriado será no dia 6 de janeiro. Alternativa B.

Exercício 3. (Colégio Naval 2017) Os números x e y pertencem ao conjunto $C = \{17,20,23,26,\ldots,2018\}$ e são tais que $x > y$. Sendo assim, pode-se concluir que $2017 \cdot 2^x + 8^y$, na divisão por 7, deixa resto

(A) 0 (B) 1 (C) 3 (D) 4 (E) 5

Solução

Primeiramente, nota-se que x e y são da forma $17 + 3k$, com $k \in \mathbb{N} \cup \{0\}$. Assim, analisando 2^x e 8^y módulo 7, tem-se: $2^{17+3k} = 2^{17}.2^{3k}$ onde 2^{3k} e 8^y são potências de 8. Qualquer potência de 8 deixa resto 1 na divisão por 7 (pois $8 \equiv 1\ (mod\ 7)$ obtendo $8^y \equiv 1\ (mod\ 7)$). Então, $2^{17} = (2^3)^5 \cdot 2^2$, do que se obtém: $(2^3)^5 \equiv 1\ (mod\ 7)$, $2^2 \equiv 4\ (mod\ 7)$ e $2^{17} \equiv 4\ (mod\ 7)$. Ou seja, $2^x \equiv 1\ (mod\ 7)$. Leva-se em conta também que $2017 \equiv 1(mod\ 7)$. Por fim, juntando todas estas informações: $2017 \cdot 2^x + 8^y \equiv 5\ (mod\ 7)$. ALTERNATIVA E.

5.9 PLANO DE AULA IX

Duração: duas horas/aula de cinquenta minutos cada.

Conteúdo: Inversos multiplicativos e o Teorema de Euler.

Objetivos: Compreender o que são classes residuais e inversos multiplicativos e como determiná-los. Definir a função φ de Euler e apresentar proposições que permitam o cálculo de $\varphi(n)$ para qualquer n inteiro. Apresentar o Teorema de Euler e fazer uso do mesmo como ferramenta em cálculos de aritmética modular.

Desenvolvimento: primeiramente, serão trabalhados os conceitos e teoria. Serão resolvidos alguns exercícios práticos, empregando o que foi aprendido.

Avaliação: durante os exercícios propostos, aparecerão os cálculos de $\varphi(161)$, $\varphi(55)$, do inverso multiplicativo de 5 módulo 132 (d, onde $5d \equiv 1(mod\ 132)$) e do inverso multiplicativo de 7 módulo 40 (d, onde $7d \equiv 1(mod\ 40)$), já prevendo a utilidade destes resultados na codificação/decodificação dos exemplos das aulas X e XI.

Análise e observações da Aula IX: nesta aula, procurou-se dar maior ênfase aos exercícios, pois o total entendimento da teoria exigia detalhes bem técnicos. Afinal, para aplicação do RSA, basta que os alunos saibam calcular $\varphi(n) = (p-1)\cdot(q-1)$ para $n = p \cdot q$, produto de dois primos e calcular inversos multiplicativos simples. Por outro lado, procurou-se dar uma noção da função φ de Euler aos alunos, para que a fórmula $\varphi(n) = (p-1)\cdot(q-1)$ fizesse sentido e não fosse apenas uma "fórmula pronta".

5.10 PLANO DE AULA X

Duração: duas horas/aula de cinquenta minutos cada.

Conteúdo: Aplicando a Criptografia RSA.

Objetivos: fazer uso da criptografia RSA por meio de um exemplo prático.

Desenvolvimento: a palavra UFSM será codificada e decodificada (ver exemplo da Seção 4.1). Para facilitar a compreensão, o método será dividido em 3 passos: pré-codificação, codificação e decodificação. Os alunos poderão acompanhar o exemplo pela apostila, completando com os cálculos que devem ser realizados. A aula será expositiva, com quadro branco e caneta.

Avaliação: observação e questionamentos aos alunos.

Análise e observações da Aula X: no planejamento inicial, foi previsto apenas o exercício de codificação/decodificação da palavra UFSM, pois acreditava-se que seria muito complexo e confuso (pelo menos inicialmente) para a turma. No entanto, a divisão em passos parece ter facilitado bastante. Assim, o andamento da aula foi mais rápido que o previsto. Verificou-se que alguns alunos já estavam fazendo o segundo exemplo (codificar e decodificar a palavra CMPA) presente na apostila e que seria objeto do desenvolvimento da próxima aula. Desta maneira, a Aula XI poderia ter sido eliminada. Por outro lado, decidiu-se manter o planejamento. Solicitou-se aos alunos que realizassem a resolução do segundo exemplo como "tarefa para casa".

5.11 PLANO DE AULA XI

Duração: duas horas/aula de cinquenta minutos cada.

Conteúdo: Aplicando a Criptografia RSA (continuação).

Objetivos: reforçar o entendimento da criptografia RSA por meio de mais um exemplo prático.

Desenvolvimento: a palavra CMPA será codificada e decodificada. A ênfase será maior no entendimento do método RSA do que no desenvolvimento de cálculos. Assim, será liberado o uso de *softwares* e/ou aplicativos que possam auxiliar nos cálculos de aritmética modular, particularmente, restos de potências muito grandes. Nesta tarefa, serão sugeridos o aplicativo *Módulo Calculator* e o *software Microsoft Excel*.

Avaliação: observação e questionamentos aos alunos.

Análise e observações da Aula XI: o Laboratório de Matemática, local das aulas, é equipado com computadores com acesso à *internet*, além do pacote *Office*. Portanto, o uso do *Microsoft Excel* foi uma sugestão considerada adequada. O *Excel* calcula restos por meio da função "MOD". A estrutura deste comando é

=MOD(número;divisor). Então, para calcular o resto da divisão de 123 por 4, por exemplo, escolhe-se uma célula qualquer, e digita-se =MOD(123;4). Além disso, a potenciação pode ser feita usando "^", ou seja, calcular 625^3 é equivalente a escrever =625^3 em uma célula qualquer. Verificou-se que para potências "pequenas", o comando MOD retornava o resultado esperado. Calcular o resto da divisão de 625^3 por 55, por exemplo, era possível (escrevendo =MOD(625^3;55)). A limitação ocorre quando é preciso calcular o resto de potências muito grandes. Em um dos exemplos, foi necessário obter o resto de 30^7 por 55. Desta vez, o comando =MOD(30^7;55) deu erro. Isto não foi obstáculo para os alunos que por meio de propriedades da potenciação e aritmética modular, puderam encontrar os resultados esperados. De fato, alguns alunos já tinham conseguido codificar e decodificar a palavra CMPA como "tarefa de casa", conforme sugestão da aula anterior. Estes ajudaram os demais colegas. Pode-se perceber que parte da turma enfrentava dificuldades, pois estavam muito preocupados com as contas, enquanto o foco deveria ser no método RSA. Nesta aula, estes entenderam melhor os passos de codificação/decodificação pois tinham auxílio de aplicativos e *softwares*.

Aqui, surgiu uma oportunidade de melhoria: o professor pode certificar-se, em aulas anteriores, que os alunos saibam empregar as propriedades de aritmética modular, resolvendo exercícios diversos, já prevendo que alguns destes exercícios irão aparecer na codificação/decodificação de exemplos de emprego do RSA. Assim, as aulas X e XI poderiam ser condensadas em uma só, concentrando-se no método e não nos cálculos.

Sobre a limitação do *Excel*, sabe-se que outros *softwares*, como o *Maple*[1], por exemplo, são bem mais eficientes no cálculo de restos de potências. Porém, optou-se pelo primeiro pela facilidade de já estar disponível nos computadores usados.

5.12 PLANO DE AULA XII

Duração: duas horas/aula de cinquenta minutos cada.

[1] O *Maple* é um *software* matemático que utiliza linguagem de computação algébrica e simbólica. É desenvolvido e comercializado pela *Maplesoft* (www.maplesoft.com).

Conteúdo: Entendendo por que a Criptografia RSA funciona.

Objetivos: compreender que sempre que a codificação em RSA é usada, é possível reverter o processo, ou seja, realizar a decodificação e retornar à mensagem original.

Desenvolvimento: será feita uma demonstração semelhante ao que pode ser conferido na Subseção 4.2.1.

Avaliação: observação e questionamentos aos alunos.

Análise e observações da Aula XII: esta aula foi puramente teórica e não tão bem recebida por alguns alunos que acharam demasiadamente complicado todas as justificativas realizadas. Acredita-se que a maioria não absorveu todos os detalhes envolvidos, pois geralmente gostam de desafios e de "fazer contas". Foi uma oportunidade de chamar a atenção que, muitas vezes, não só na Matemática, a compreensão de ideias é mais importante do que obter resultados, pois calculadoras e computadores poderiam realizar os cálculos; raciocínio ainda é uma exclusividade humana.

Por outro lado, já era esperado que esta parte fosse muito complexa, mesmo para o público em questão. Este fator foi levado no planejamento inicial das aulas, mas decidiu-se manter a explicação por acreditar-se que justificaria e empregaria várias das ferramentas aprendidas ao longo do curso.

Uma sugestão de melhoria é disponibilizar uma demonstração completa na apostila, para aqueles que tenham mais facilidade. A ideia da justificativa do funcionamento do RSA poderia ser dada de maneira simplificada, apresentando as linhas gerais da demonstração. Assim, não seria necessário ocupar uma aula inteira neste processo, sobrando tempo para uma ênfase maior em outros aspectos ou mesmo avaliação do entendimento dos alunos.

5.13 PLANO DE AULA XIII

Duração: duas horas/aula de cinquenta minutos cada.

Conteúdo: Conclusão e questionamentos.

Objetivos: realizar um questionário avaliando o retorno dado pelos discentes sobre o curso. Aplicar uma avaliação, feita em duplas, para verificar o nível de entendimento dos alunos. Reforçar os fatores que garantem a segurança do RSA.

Desenvolvimento: aplicação de questionário e avaliação.

Avaliação: os alunos responderam ao questionário/avaliação que segue abaixo.

01. Vocês consideram o tema relevante? Acharam interessante esta aplicação da Teoria dos Números, bem como de todos os conceitos envolvidos na Criptografia?
02. O grupo conseguiu entender os conceitos envolvidos? Conseguiram compreender a aplicação do método RSA?
03. O "Minicurso Criptografia RSA" contribuiu para a formação de vocês? Em que sentido?
04. Vamos codificar a palavra RSA, escolhendo os primos $p = 5$ e $q = 17$, com $e = 3$. Pré-codificando a mensagem, teremos 272810 que podemos quebrar em 2-72-8-10.
a) Usando os dados do exercício, codifique a mensagem através da Criptografia RSA.
b) Decodifique o resultado encontrado no item anterior, verificando se seus cálculos estão corretos (ou seja, voltando à mensagem original).
05. Quando o número n, módulo do RSA, é pequeno, é fácil descobrir os primos p e q tais que $n = p \cdot q$. Por isto a importância de escolhermos primos com centenas ou milhares de algarismos. Assim, o número n fica maior ainda e, mesmo para um computador, fica muito difícil a fatoração de n. Veja, por exemplo, que você conseguiria decifrar a mensagem 19-1-23-8 sabendo que a chave pública utilizada foi (55,3) - ou será que não?
06. Crie uma chave pública - par (n, e) - e codifique uma mensagem curta, usando o RSA. Entregue para os outros grupos esta mensagem codificada junto da chave pública. Será que eles conseguirão quebrar seu código?

Análise e observações da Aula XIII: com base nas respostas do questionário/avaliação, pôde-se perceber que os alunos consideraram o tema

relevante. A maioria dos grupos compreendeu os conceitos envolvidos, além da aplicação do método RSA em si - embora aqui, a resposta de alguns tenha sido "parcialmente". Destacaram ainda a contribuição do curso para um melhor entendimento da aritmética modular.

No item 04, a resposta esperada era criptografar a mensagem 2-72-8-10 como 8-13-2-65. No processo, como os primos $p = 5$ e $q = 17$ são conhecidos, deveriam encontrar $n = 85$ e $d = 43$, obtendo assim a chave privada (85,43). No item 05, é fácil decompor o número 55 como o produto dos primos 5 e 11. A mensagem 19-1-23-8 será decodificada como 24-1-12-2; sem traços, tem-se 241122, onde $d = 27$. Os números 24, 11 e 22 correspondem respectivamente, segundo a Seção 4.1, Quadro 5, às letras O, B e M - mensagem OBM.

Aqui, uma grata surpresa: todos alunos conseguiram encontrar respostas corretas para os itens 04 e 05. De fato, dispor os alunos em duplas foi um acerto, visto que alguns aparentavam ter maior facilidade que outros. Não foram definidos critérios para a formação das duplas, mas por iniciativa própria, alunos que estavam mais inseguros juntaram-se aos que tinham maior domínio e entendimento. Além disso, outro fator facilitador foi que os alunos puderam conferir o material da apostila, seguindo os passos indicados e trabalhados em aulas anteriores.

Porém, devido a uma questão de tempo, nenhuma dupla conseguiu completar o item 06. Uma pena, pois considerava-se esta tarefa como a mais atraente. A sugestão dada foi de que este "desafio" entre os grupos poderia ser feito posteriormente. Eles conseguiriam encontrar uma chave pública segura o suficiente? Indicou-se também o aplicativo *RSA Calculator*, disponível gratuitamente e cuja interface é mostrada pela Figura 3. Verificou-se a validade do funcionamento deste aplicativo testando os exemplos anteriores (CMPA, UFSM e RSA) confirmando a codificação/decodificação esperada. No entanto, não foram exploradas, nem encontradas as limitações do aplicativo - qual tamanho dos números primos poderiam ser utilizados, por exemplo. Por outro lado, o *RSA Calculator* auxiliava nos cálculos excessivamente longos. O desafio dos alunos era, então, decompor em fatores primos o número $n = p \cdot q$ da chave pública fornecida.

Figura 3 - Interface do aplicativo *RSA Calculator*.

Fonte: o autor.

Estabeleceu-se que, em um primeiro momento, os números primos escolhidos deveriam ser menores que 1000 - mesmo que consultassem uma lista, existem 168 primos menores que 1000.

Informalmente, conversando com os alunos alguns dias após esta aula, alguns deles descobriram "*calculadoras on-line*" de decomposição em fatores primos para números inteiros positivos menores que um milhão. A saída foi escolher números primos maiores, entre 1000 e 10000, pois com a ajuda desta ferramenta, o desafio perdia o sentido.

Como as atividades do curso continuaram instigando os alunos, considerou-se o resultado positivo e muito satisfatório. A última aula contou também com a entrega de certificados aos participantes; uma maneira singela, mas simbólica de concretizar o esforço e aprendizado da turma.

6 CONCLUSÃO

Ao apresentar uma proposta de ensino de Criptografia RSA para alunos de 8º e 9º anos de um Clube de Matemática, pode-se perceber que os objetivos iniciais foram alcançados: trazer uma aplicação de Teoria dos Números que pudesse ser adequada ao nível da turma, e que fizesse ligação com assuntos que geralmente são associados ao conhecimento matemático teórico, mas pouco prático no cotidiano, como testes de primalidade e cálculo de restos de “potências grandes”.

Além disso, a Criptografia confirmou-se como um tema que chamaria a atenção dos alunos, não somente pelo desafio em resolver problemas, a “quebra de códigos” e o uso de tecnologia, mas também por mostrar-se atual e encontrar papel fundamental na sociedade.

Outro ponto que pode ser considerado positivo é o fato de haver uma preocupação muito grande de que os alunos não soubessem apenas aplicar o método RSA, mas também entender o porquê de seu funcionamento. Isto demandou um planejamento mais complexo, visto que era preciso preparar os alunos para um tratamento mais formal da Matemática, com algumas demonstrações e generalização de ideias, indo além de meros exemplos numéricos. Provavelmente, este é o grande diferencial do trabalho aqui apresentado, que foi possível em grande parte por trabalhar com um público diferenciado - alunos medalhistas em olimpíadas de matemática e de alto interesse no estudo de ciências exatas em geral.

Tais preocupações eram cabíveis, pois algumas etapas demandavam cálculos não tão simples. Um exemplo desse tipo é o cálculo da função φ de Euler para n inteiro, quando $n = p \cdot q$, produto de dois primos, que é algo a ser determinado na aplicação do método RSA. Não se pretendia apenas fornecer uma “fórmula pronta” para os alunos (no caso, $\varphi(n) = (p-1) \cdot (q-1)$), pois isto iria contra ao que pretendíamos, que era a construção do pensamento matemático, um dos objetivos desta proposta. Provavelmente, uma “fórmula pronta” assim, seria motivo de questionamento dos alunos e, considerando o potencial da turma, seria um desperdício não aprofundar e compreender melhor o método RSA.

Nesse sentido, o paralelo feito com questões de olimpíadas de Matemática foi bem interessante. Analisando provas anteriores e bancos de questões, percebe-se

que há um ótimo número de questões ligadas à Aritmética, geralmente propondo que o aluno conjecture ou teste resultados, partindo de casos específicos para resultados mais gerais, desenvolvendo raciocínio e argumentação matemática. Agregar desafios e questões da OBMEP e OBM à apostila criada para o curso, mostrou-se uma boa decisão. Inicialmente, pensava-se que poderia desviar o foco da Criptografia, mas o observado foi justamente o contrário, visto que auxiliou no desenvolvimento da teoria. Afinal, a preparação para olimpíadas também era um dos motivos da procura pelo Clube de Matemática.

Enfim, foi muito gratificante contribuir com o aprendizado destes alunos, apresentando, além de uma aplicação da Aritmética, a importância da pesquisa, da investigação e do raciocínio em Matemática. Várias ideias brilhantes, ao longo da História, surgiram da observação, estudo e domínio teórico de conceitos matemáticos, porém, sempre aliadas com soluções elegantes e inovadoras. Estes fatores foram evidenciados quando se apresentou o histórico do RSA para a turma; o trabalho de Rivest, Shamir e Adleman é um exemplo onde o conhecimento vem antes da inovação e da criatividade, o que nos impele a acreditar que a valorização do conhecimento é um axioma importante para a construção de novos resultados.

Entre as oportunidades de melhoria, pensa-se em atualizar a apostila distribuída aos alunos, reformulando certos detalhes. Seu texto poderia ser mais direto em alguns pontos. Cremos que é possível fazer uma reformulação que traga uma proposta mais abrangente de ensino, adequada para alunos com um nível distinto, não necessariamente medalhistas em olimpíadas de matemática.

Acredita-se que, com alguma simplificação, uma nova proposta poderia se concentrar mais na aplicação do método RSA em si, do que em seu funcionamento, tornando-se viável para alunos do Ensino Médio. Neste caso, não deixariam de ser trabalhados conceitos e ferramentas de Aritmética modular, nem discussões sobre a procura por “números primos grandes” e a falta de métodos computacionais eficazes, que pudessem decompor qualquer inteiro, por maior que seja, em fatores primos, fator essencial na segurança do RSA.

Com esta proposta de ensino mais objetiva, em vez de treze encontros, poderiam ser seis: uma aula sobre noções básicas de Criptografia; uma aula sobre

tópicos como divisibilidade nos inteiros, divisão euclidiana e máximo divisor comum; duas aulas sobre Aritmética dos restos e inversos multiplicativos e duas aulas de aplicação do método RSA em si. Sendo um tema amplo, provavelmente despertaria o interesse dos alunos e um aprofundamento maior poderia ser feito posteriormente.

Acrescenta-se que não foram apenas os alunos a serem beneficiados com a proposta de ensino. Foi uma experiência enriquecedora pesquisar e preparar-se para as aulas. Aliás, toda esta preparação e pesquisa também levou ao contato com outras aplicações da Aritmética modular, como o uso de sistemas de identificação – entre eles, o código de barras, o número do cadastro de pessoas físicas (CPF) e o *International Standard Book Number* (ISBN) que identifica livros e publicações – e o funcionamento de calendários. Ou seja, mais possibilidades de ensino que futuramente podem ser exploradas. Destaca-se ainda que grande parte das noções iniciais de Criptografia incluem fatos históricos e métodos de cifragem simétrica simples, que podem ser trabalhados com alunos do 6º ano em diante, pois não necessitam de pré-requisitos como o RSA.

Assim, o ganho em minha formação como professor foi enorme. O estudo envolvido trouxe segurança em diversos assuntos de Teoria dos Números, algo muito positivo quando se ministra aulas de preparação para olimpíadas de matemática.

Diante de tudo isto, e do fato de que a proposta de ensino surgiu em uma aula de Aritmética do PROFMAT, reitero a importância deste mestrado profissionalizante, que contribui na formação dos professores ao mesmo tempo que traz qualidade e novas possibilidades para a sala de aula. A Criptografia, como um todo, é um tema fascinante, mas o RSA mostra-se particularmente genial.

Porém, propostas de ensino como esta exigem, além do conhecimento, tempo e dedicação do professor. Provavelmente, não se obteria contato com uma aplicação tão interessante, sem o embasamento que o PROFMAT fornece, pilar fundamental para a educação do país.

REFERÊNCIAS

BETTEGA, M. H. S. **Educação continuada na era digital.** 2ª ed. São Paulo: Cortez, 2010.

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

CARNEIRO, F. J. F. **Criptografia e Teoria dos Números.** Rio de Janeiro: Editora Ciência Moderna Ltda., 2017.

COUTINHO, S. C. C. **Programa de Iniciação Científica da OBMEP:** Criptografia. Rio de Janeiro: IMPA, 2014.

HEFEZ, A. **Aritmética:** Coleção PROFMAT. 1ª ed, 2ª impressão. Rio de Janeiro: SBM, 2014.

INSTITUTO DE MATEMÁTICA PURA E APLICADA (IMPA). **Maior número primo do mundo tem 23 milhões de dígitos.** Disponível em: <https://impa.br/page-noticias/largest-prime-number-in-the-world-has-23-million-digits/> Acesso em: 06 de jul. 2018.

LORENZATO, S. **Para aprender matemática:** Coleção Formação de Professores. 3ª ed. Campinas: Autores Associados, 2010.

MICOTTI, M. C. O. O ensino e as propostas pedagógicas. In: BICUDO, M. A. V. **Pesquisa em educação matemática:** concepções e perspectivas. São Paulo: Editora UNESP, 1999.

MORAN, J. M.; MASETTO, M.T.; BEHRENS, M.A. **Novas Tecnologias e mediação pedagógica.** 6ª ed. Campinas: Papirus, 2000.

PONTE, J. P. da; BROCARDO, J.; OLIVEIRA. H. **Investigações Matemáticas na Sala de Aula.** 2ª ed**.** Belo Horizonte: Autêntica Editora, 2009.

SANTOS, J. P. de O. **Introdução à Teoria dos Números.** 3ª ed, 4ª impressão. Rio de Janeiro: IMPA, 2007.

SHOKRANIAN, S. **Criptografia para Iniciantes.** 2ª ed. Rio de Janeiro: Editora Ciência Moderna Ltda., 2012.

SINGH, S. **O livro dos códigos:** a ciência do sigilo - do antigo Egito à criptografia quântica. Rio de Janeiro: Record, 2001.

TEIXEIRA, P. J. M; PASSOS, C. C. M. **Um pouco da teoria das situações didáticas (tsd) de Guy Brousseau.** Zetetiké-FE/Unicamp, 2013.

APÊNDICE A – A MÁQUINA ENIGMA

A Enigma foi uma máquina criptográfica utilizada pelo exército alemão durante a Segunda Guerra Mundial (1939-1945), com o objetivo de estabelecer segurança na comunicação entre o comando e a frota de navegação. O criador da Enigma foi o engenheiro alemão Alan Scherbius.

A grande dificuldade, na época, de decifrar a Enigma (Figura 4) explica-se pelo seu funcionamento: dentro de cada máquina existiam três discos com cifras, chamados de rotores, que poderiam ser substituídos ou retirados. Cada rotor possui um alfabeto de A a Z, ligado à diferentes sistemas internos de fiação. Quando uma letra do texto original é acionada no teclado da Enigma, os rotores são acionados de acordo com uma configuração pré-estabelecida. O resultado é que uma luz, no painel de lâmpadas, ficava acesa, indicando a letra codificada. Cada vez que uma letra era pressionada, os rotores mudavam de posição e, se esta mesma letra fosse acionada posteriormente, provavelmente seria cifrada de forma distinta.

Figura 4 – A Enigma.

Fonte: Disponível em: <https://www.theregister.co.uk/2015/10/23/enigma_machine_4_rotor_sale/> Acesso em 21 fev. 18.

Outras versões da Enigma, poderiam ter cinco ou mais rotores, aumentando a segurança. Toda a segurança dependia da chave, que neste caso era a configuração inicial dos rotores. Por isto, os alemães alteravam a chave todos os dias e os operadores de codificação recebiam um livro-código com as chaves usadas no mês. Estes livros, além de serem bem guardados, geralmente eram escritos com tinta solúvel, sendo mergulhados na água em caso de contato com o inimigo. Os alemães acreditavam que a Enigma era "inquebrável" pois seria impossível para os aliados

descobrir a chave entre bilhões de possibilidades a serem testadas dentro de um dia.

Fato é que antes mesmo da Segunda Guerra, intelectuais poloneses já estudavam maneiras de decifrar a Enigma e grandes avanços foram feitos pelo matemático Marian Rejewski. Estas descobertas foram passadas aos franceses e ingleses.

Naquela época, as mensagens eram transmitidas usando código Morse. Uma vez interceptadas pelos ingleses, eram encaminhadas para um lugar chamado Bletchley Park - onde diversos estudiosos reuniam esforços para quebrar os códigos recebidos. Entre estes, encontrava-se Alan Turing, matemático britânico que sempre demonstrou brilhantismo intelectual diferenciado.

Turing idealizou uma máquina construída especificamente para quebrar os códigos da máquina Enigma. Suas ideias foram o princípio do computador moderno. O sucesso na empreitada de decodificar estes códigos certamente alterou o rumo da guerra. Acredita-se que muitas vidas foram salvas, antecipando o fim da guerra em pelo menos três anos.

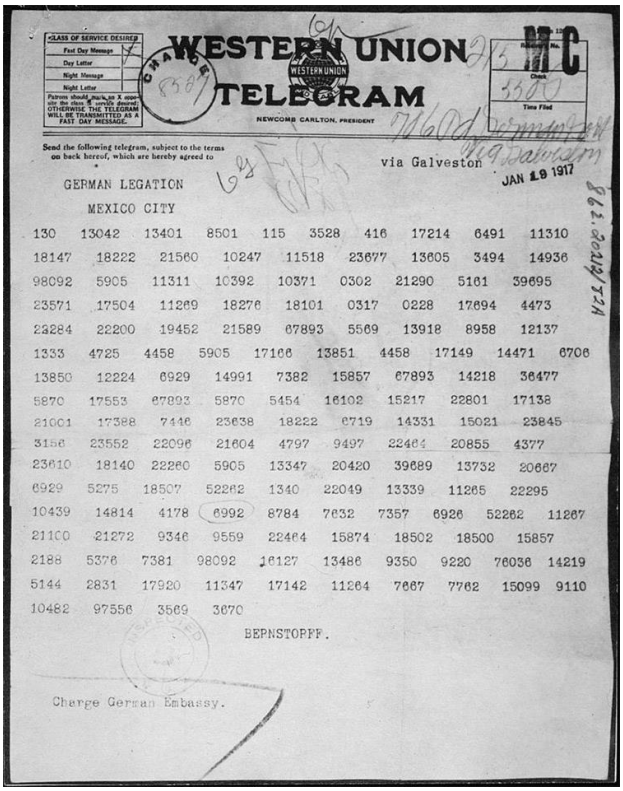
Obviamente, houve todo um esforço conjunto: pesquisadores, serviço de espionagem e militares em objetivo comum. Isto não diminui o intelecto de Turing. É também desta época que a criptografia começou a ser uma área dominante dos matemáticos (até então era creditada a linguistas e historiadores).

Infelizmente, Turing não viveu para ter o reconhecimento público que merecia. Homossexual assumido (o que era crime na época), foi obrigado a ser submetido a um tratamento hormonal. Deprimido, suicidou-se em 7 de junho de 1954, aos 42 anos. Soma-se ainda o fato de que as descobertas sobre a Enigma não puderam ser reveladas até a década de 1970.

APÊNDICE B – O TELEGRAMA ZIMMERMANN

Não raras vezes, a criptografia mudou o rumo de guerras e tramas políticas. O telegrama Zimmermann (Figura 5) é um exemplo disto.

Figura 5 – Telegrama Zimmermann



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTORFF.

Charge German Embassy.

Fonte: Disponível em: <https://www.historytoday.com/david-nicholas/lucky-break-zimmermann-telegram>. Acesso em 21 fev. 2018.

Arthur Zimmermann era o Ministro das Relações Exteriores da Alemanha em 1917. Um telegrama, codificado, foi enviado para Heinrich von Eckardt, embaixador alemão no México durante a Primeira Guerra Mundial. O telegrama propunha uma aliança com o México para atacar os Estados Unidos. Porém, a mensagem foi interceptada e decodificada pelos britânicos que alertaram os americanos. Este fato, acelerou a entrada dos EUA na Primeira Guerra Mundial, que até então mantinha posição de neutralidade.

Tudo foi feito de maneira secreta pelos britânicos. Quando o conteúdo do telegrama foi revelado, os alemães acharam que a falha foi dos mexicanos. A autenticidade do telegrama foi confirmada pelo próprio Zimmermann.

APÊNDICE C – AS CIFRAS DE BEALE

Considerado um dos grandes mistérios criptográficos do mundo, as cifras de Beale consistem em três mensagens criptografadas que levariam a um tesouro enterrado no estado de Virgínia, EUA.

Thomas J. Beale seria o homem por trás do tesouro escondido em 1822. A primeira mensagem (Figura 6) indicaria a localização do tesouro; a segunda mensagem (a única que foi decifrada) diz respeito ao conteúdo do tesouro; a terceira mensagem diz quem são os herdeiros e como o dinheiro deve ser distribuído. De acordo com a segunda mensagem, o valor do tesouro seria de vinte milhões de dólares, já na cotação atual.

Figura 6 – A primeira cifra de Beale.

71, 194, 38, 1701, 89, 76, 11, 83, 1629, 48, 94, 63, 132, 16, 111, 95, 84, 341, 975,
14, 40, 64, 27, 81, 139, 213, 63, 90, 1120, 8, 15, 3, 126, 2018, 40, 74, 758, 485,
604, 230, 436, 664, 582, 150, 251, 284, 308, 231, 124, 211, 486, 225, 401, 370,
11, 101, 305, 139, 189, 17, 33, 88, 208, 193, 145, 1, 94, 73, 416, 918, 263, 28, 500,
538, 356, 117, 136, 219, 27, 176, 130, 10, 460, 25, 485, 18, 436, 65, 84, 200, 283,
118, 320, 138, 36, 416, 280, 15, 71, 224, 961, 44, 16, 401, 39, 88, 61, 304, 12, 21,
24, 283, 134, 92, 63, 246, 486, 682, 7, 219, 184, 360, 780, 18, 64, 463, 474, 131,
160, 79, 73, 440, 95, 18, 64, 581, 34, 69, 128, 367, 460, 17, 81, 12, 103, 820, 62,
116, 97, 103, 862, 70, 60, 1317, 471, 540, 208, 121, 890, 346, 36, 150, 59, 568,
614, 13, 120, 63, 219, 812, 2160, 1780, 99, 35, 18, 21, 136, 872, 15, 28, 170, 88, 4,
30, 44, 112, 18, 147, 436, 195, 320, 37, 122, 113, 6, 140, 8, 120, 305, 42, 58, 461,
44, 106, 301, 13, 408, 680, 93, 86, 116, 530, 82, 568, 9, 102, 38, 416, 89, 71, 216,
728, 965, 818, 2, 38, 121, 195, 14, 326, 148, 234, 18, 55, 131, 234, 361, 824, 5,
81, 623, 48, 961, 19, 26, 33, 10, 1101, 365, 92, 88, 181, 275, 346, 201, 206, 86,
36, 219, 324, 829, 840, 64, 326, 19, 48, 122, 85, 216, 284, 919, 861, 326, 985,
233, 64, 68, 232, 431, 960, 50, 29, 81, 216, 321, 603, 14, 612, 81, 360, 36, 51, 62,
194, 78, 60, 200, 314, 676, 112, 4, 28, 18, 61, 136, 247, 819, 921, 1060, 464, 895,
10, 6, 66, 119, 38, 41, 49, 602, 423, 962, 302, 294, 875, 78, 14, 23, 111, 109, 62,
31, 501, 823, 216, 280, 34, 24, 150, 1000, 162, 286, 19, 21, 17, 340, 19, 242, 31,
86, 234, 140, 607, 115, 33, 191, 67, 104, 86, 52, 88, 16, 80, 121, 67, 95, 122, 216,
548, 96, 11, 201, 77, 364, 218, 65, 667, 890, 236, 154, 211, 10, 98, 34, 119, 56,
216, 119, 71, 218, 1164, 1496, 1817, 51, 39, 210, 36, 3, 19, 540, 232, 22, 141, 617,
84, 290, 80, 46, 207, 411, 150, 29, 38, 46, 172, 85, 194, 39, 261, 543, 897, 624, 18,
212, 416, 127, 931, 19, 4, 63, 96, 12, 101, 418, 16, 140, 230, 460, 538, 19, 27, 88,
612, 1431, 90, 716, 275, 74, 83, 11, 426, 89, 72, 84, 1300, 1706, 814, 221, 132,
40, 102, 34, 868, 975, 1101, 84, 16, 79, 23, 16, 81, 122, 324, 403, 912, 227, 936,
447, 55, 86, 34, 43, 212, 107, 96, 314, 264, 1065, 323, 428, 601, 203, 124, 95, 216,
814, 2906, 654, 820, 2, 301, 112, 176, 213, 71, 87, 96, 202, 35, 10, 2, 41, 17, 84,
221, 736, 820, 214, 11, 60, 760.

Fonte: Disponível em: <http://theunexplainedmysteries.com/Beale-Ciphers.html>. Acesso em 21 fev. 2018.

A história começa com a publicação de um folheto, em 1885, intitulado "*The Beale Papers*" cujo autor preferiu anonimato. O documento conta que Thomas J. Beale teria acumulado grande fortuna em ouro. Beale teria entregue a um amigo, Robert Morriss, as três mensagens dentro de uma caixa de ferro. Explicou também

que outro amigo possuía a chave para decifrá-las. A caixa de ferro deveria ser mantida em segredo até que Beale retornasse. No entanto, isto nunca ocorreu - nem o contato com o amigo possuidor da chave.

Morriss esperou por Beale por anos, abrindo a caixa somente em 1845. Sem sucesso nas tentativas de decifrar as mensagens, contou o que sabia para um amigo próximo - o autor anônimo de "*The Beale Papers*". Este amigo anônimo revelou a história de Beale ao mundo, após anos tentando desvendar o mistério. Foi ele que decifrou a segunda mensagem, baseada no texto da Declaração de Independência dos Estados Unidos da América.

Não se sabe se as cifras de Beale são verdadeiras, nem se os personagens envolvidos realmente existiram. Muitos acreditam que pode ser apenas um golpe publicitário da época. Fato é que o condado de Bedford, provável local do tesouro, até hoje recebe muitas visitas de aventureiros arriscando a sorte. Existe também quem conspire que o governo americano já teria solucionado o conteúdo das mensagens e adquirido o tesouro há anos.

APÊNDICE D – ATBASH

Conforme o que pode ser visto em Singh (2001, p. 43), na Idade Média, religiosos estudiosos da Bíblia ficavam intrigados com o fato de que o Velho Testamento continha trechos criptografados, codificados com o que ficou conhecido como *atbash*, uma forma tradicional de substituição hebraica. Neste sistema, a primeira letra do alfabeto hebreu (*aleph*) é substituída pela última (*taw*), a segunda letra (*beth*) é trocada pela penúltima (*shin*). Destas quatro letras deriva o nome da cifra: **A**leph, **T**aw, **B**eth, **Sh**in.

Aplicando a mesma ideia ao nosso alfabeto, tem-se:

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

Assim, o Atbash pode ser considerado um método de **criptografia de substituição**. Observa-se que a palavra ESCOLA seria cifrada como VHXLOZ, por exemplo.

APÊNDICE E – CERCA DE FERROVIA

A cerca de ferrovia é um método de **criptografia de transposição**. A maneira mais simples de entender seu funcionamento é por meio de um exemplo. Assim, considere a mensagem "TEORIA DOS NÚMEROS". A ideia consiste em escrever o texto a ser cifrado alternando as letras em duas linhas diferentes (variações desta técnica podem usar três ou mais linhas). O resultado pode ser conferido no Quadro 6, abaixo.

Quadro 6 - Exemplo da cifra "cerca de ferrovia".

Linha 1	T		O		I		D		S		U		E		O	
Linha 2		E		R		A		O		N		M		R		S

Fonte: o autor.

O texto cifrado fica: TOIDSUEOERAONMRS, onde foram suprimidos espaços e acentos. O receptor deve simplesmente reverter o processo para obter a mensagem original. É um tipo de cifra muito simples, porém muito vulnerável.

APÊNDICE F – CIFRA DE VIGENÈRE

Percebendo as fraquezas do sistema de substituição monoalfabética diante da análise de frequência (discutida na Seção 2.1, do Capítulo 2), muitos estudos foram feitos na tentativa de criar uma criptografia mais forte e poderosa. Segundo Carneiro (2017, p. 9), em 1586, o diplomata francês Blaise Vigenère, reúne o conhecimento de estudiosos anteriores, aprimorando-os para apresentar uma forma de **cifra do tipo polialfabética**, que mais tarde levaria seu nome. Utilizava não um, mas vinte e seis alfabetos distribuídos conforme o Quadro 7, abaixo.

Quadro 7 - Quadrado de Vigenère.

	a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

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

Fonte: (CARNEIRO, 2017, p. 7).

Na prática, é como se fossem usados os vinte e seis alfabetos possíveis da criptografia monoalfabética de César (ver Exemplo 2 da Seção 2.1, Capítulo 2). Em seguida, uma palavra-chave deve ser escolhida. Como exemplo, será cifrada a mensagem "ESTA FRASE DEVERIA SER SECRETA" utilizando a palavra-chave IMUNE - pois a cifra de Vigenère é imune à quebra por análise de frequência comum.

A palavra-chave é repetida em cima de cada letra da mensagem original e cada letra da mensagem cifrada será obtida observando a intersecção da letra da palavra-chave (linha do Quadro 7) com a letra correspondente da mensagem original (coluna do Quadro 7).

O Quadro 8 ilustra esta construção.

Quadro 8 - Exemplo de cifra utilizando o quadrado de Vigenère.

Palavra-chave	I	M	U	N	E	I	M	U	N	E	I	M	U	N	E	I
Mensagem original	E	S	T	A	F	R	A	S	E	D	E	V	E	R	I	A
Mensagem cifrada	M	E	N	N	J	Z	M	M	R	H	M	H	Y	E	M	I
Palavra-chave	M	U	N	E	I	M	U	N	E	I						
Mensagem original	S	E	R	S	E	C	R	E	T	A						
Mensagem cifrada	E	Y	E	W	M	O	L	R	X	I						

Fonte: o autor.

Por fim, a mensagem cifrada será: MENNJZMMRHMHYEMIEYEWMOLRXI. Para decifrar, conhecendo a palavra-chave, basta fazer o processo inverso. Escreve-se a palavra-chave em cima de cada letra da mensagem cifrada. Porém, desta vez, dentro de cada linha do alfabeto da letra da palavra-chave, procura-se a letra da mensagem cifrada. A letra do texto original será a da coluna correspondente.

Como visto, cifrar usando substituição polialfabética não é tão prático quando o sistema monoalfabético. Para determinados usos, mais corriqueiros, a cifra monoalfabética continuou sendo usada. Em assuntos de suma importância, envolvendo diplomacia e estratégias militares, costumava-se optar pelo emprego de cifras polialfabéticas.

Observa-se ainda que o criptoanalista que tentasse decifrar a mensagem MENNJZMMRHMHYEMIEYEWMOLRXI, usando da análise de frequência, poderia conjecturar que a letra M da mensagem cifrada é a letra A do alfabeto original. Porém, neste exemplo, o M substitui as letras E, A, S e I. E mesmo que soubesse se tratar de uma cifra polialfabética, ele não sabe nem quantas letras possui a palavra-chave. De fato, descobrir o tamanho da palavra-chave é o primeiro passo para decifrar uma cifra de Vigenère.

Um método geral para "quebrar" este tipo de cifra só foi descoberto por Charles Babbage, um pesquisador britânico, do século XIX. No entanto, de forma independente, o método também foi descoberto por Friedrich Wilhelm Kasiski, oficial da reserva do exército prussiano. A diferença é que Kasiski publicou sua descoberta, em 1863, enquanto as contribuições de Babbage só vieram a público no século XX, com o conhecimento de suas anotações. Especula-se que o serviço britânico de espionagem possa ter exigido o segredo de Babbage, obtendo vantagem em um conhecimento que ainda não era de domínio do resto do mundo.