O principal objetivo desta dissertação é apresentar a congruência modular em uma aplicação prática que é o método RSA da criptografia. Além disso, utilizá-la como uma nova ferramenta para a resolução de problemas encontrados em olimpíadas de matemática de nível básico.

Orientador: Ligia Liani Barz

Coorientador: Fernando Deeke Sasse

Joinville, 2019

ANO
2019

REJEANE DE LIMA | CONGRUÊNCIAS MODULARES: APLICAÇÕES EM PROBLEMAS DE OLIMPÍADAS DE MATEMÁTICA E CHAVE PÚBLICA RSA

UNIVERSIDADE DO ESTADO DE SANTA CATARINA – UDESC
CENTRO DE CIÊNCIAS TECNOLÓGICAS – CCT
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

DISSERTAÇÃO DE MESTRADO

CONGRUÊNCIAS MODULARES: APLICAÇÕES EM PROBLEMAS DE OLIMPÍADAS DE MATEMÁTICA E CHAVE PÚBLICA RSA

REJEANE DE LIMA

JOINVILLE, 2019

REJEANE DE LIMA

CONGRUÊNCIAS MODULARES: APLICAÇÕES EM PROBLEMAS DE OLIMPÍADAS DE MATEMÁTICA E CHAVE PÚBLICA RSA

Dissertação apresentada ao Curso de Pós-Graduação em Ensino de Ciências, Matemática e Tecnologias, da Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas–CCT, como requisito parcial para obtenção do grau de Mestre em Matemática.

Orientador: Profa. Dra. Ligia Liani Barz
Coorientador: Prof. Dr. Fernando Deeke Sasse

JOINVILLE

2019

Ficha catalográfica elaborada pelo programa de geração automática da

Biblioteca Setorial do CCT/UDESC,

com os dados fornecidos pelo(a) autor(a)

Lima, Rejeane
Congruências modulares: Aplicações em Problemas de Olimpíadas de Matemática e Chave Pública RSA / Rejeane Lima. -- 2019.
119 p.

Orientador: Ligia Liani Barz
Coorientador: Fernando Deeke Sasse
Dissertação (mestrado) -- Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação Profissional em Matemática em Rede Nacional, Joinville, 2019.

1. Congruência Modular. 2. Olimpíadas de Matemática. 3. Criptografia. 4. RSA. I. Liani Barz, Ligia . II. Deeke Sasse, Fernando . III. Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação Profissional em Matemática em Rede Nacional. IV. Titulo.

Congruências Modulares: Aplicações em Problemas de Olimpíadas de Matemática e Chave Pública RSA

por

Rejeane de Lima

Esta dissertação foi julgada adequada para obtenção do título de

MESTRA EM MATEMÁTICA

Área de concentração em "Ensino de Matemática"
e aprovada em sua forma final pelo

CURSO DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL
DO CENTRO DE CIÊNCIAS TECNOLÓGICAS DA
UNIVERSIDADE DO ESTADO DE SANTA CATARINA.

Banca Examinadora:

Profa. Dra. Lígia Liani Barz
CCT/UDESC (Orientadora/Presidente)

Prof. Dr. Felipe Delfini Caetano Fidalgo
UFSC/Blumenau

Profa. Dra. Viviane Maria Beuter
CCT/UDESC

Joinville,SC, 15 de agosto de 2019.

Dedico esta dissertação ao meu esposo Marcos Elias Nunes, ao meu avô David de Lima Junior (*in memoriam*) e ao meu filho Davi de Lima Nunes.

AGRADECIMENTOS

Agradeço primeiramente a Deus pela saúde e pelas oportunidades que me proporcionou em todas as etapas da vida.

Aos meus pais Julio Cesar de Lima e Maribel Aparecida Tavares de Lima pela educação e valores transmitidos.

A minha irmã Mayara de Lima por todo o apoio, carinho e torcida pela conclusão do curso.

Ao meu esposo e melhor amigo Marcos Elias Nunes por insistir, incentivar e acreditar. Por não me deixar desistir e por permanecer ao meu lado em todos os momentos.

Ao meu avô David de Lima Junior (*in memoriam*) por me ensinar com sua incrível história de vida que, tudo o que almejamos conseguimos alcançar com dedicação e força de vontade.

Agradeço aos familiares e amigos pela compreensão nos momentos de ausência em que precisei estudar.

Aos professores do PROFMAT por todo o conhecimento compartilhado, em especial a professora Dra Ligia Liani Barz e ao professor Dr. Fernando Deeke Sasse que acompanharam e auxiliaram em todos os passos desta dissertação.

Aos meus colegas do PROFMAT pelos momentos de angustia e descontração.

As minhas amigas Ana, Fabiane, Magnólia e Pahola por me ouvirem pacientemente, me ajudarem a manter a calma e acreditarem junto comigo que esse momento chegaria.

RESUMO

Esta dissertação aborda dois temas. O primeiro é o uso dos conceitos de congruências modulares como uma ferramenta para a resolução de problemas envolvendo teoria de números no nível básico de ensino. O segundo é a possibilidade de se fazer uma introdução pedagógica da criptografia RSA como uma aplicação da teoria de números no ensino básico. Apresentamos a fundamentação teórica com conceitos da teoria dos números como divisibilidade, números primos e congruências modulares com demonstrações de um modo acessível a professores de matemática, sem experiência prévia no assunto. A teoria desenvolvida é aplicada a problemas do bancos de questões de olimpíadas de matemática do ensino básico. As resoluções destes problemas apresentadas aqui, usando congruência modulares, são comparadas com aquelas tradicionalmente apresentadas. Os problemas foram classificados em três níveis: fácil, intermediário e difícil e comentários sobre as resoluções foram feitos baseados nessa classificação. A apresentação pedagógica da criptografia RSA foi escolhido por ser uma aplicação não trivial e relevante da teoria de congurências modulares. Nossa proposta é que este assunto, normalmente abordado somente em matemática de nível universitário, pode ser introduzido no ensino básico. Apresentamos como problemas que requerem extenso trabalho computacional podem ser resolvidos usando o sistema de computação algébrica Maxima, que é um software livre. Apresentamos também sugestões de atividades práticas em sala de aula para os professores.

Palavras-chave: Congruência Modular, Olimpíadas de Matemática, Criptografia , RSA.

ABSTRACT

This dissertation addresses two themes. The first is the use of modular congruence concepts as a problem-solving tool involving number theory at the high school level. The second is the possibility of making a pedagogical introduction to RSA cryptography as an application of number theory in basic education. We present the theoretical foundation with concepts of number theory such as divisibility, prime numbers, and modular congruences with demonstrations accessible to math teachers with no prior experience in the subject. The theory developed is applied to problems of the mathematical olympiad question banks of basic school. The solutions for these problems presented here using modular congruence are compared to the high school traditional approaches. Problems were classified into three levels: easy, intermediate, and difficult, and comments about the solutions were based on this classification. The pedagogical presentation of RSA cryptography was chosen because it is a nontrivial and relevant application of modular congruence theory. Our proposal is that this subject usually addressed only in university-level mathematics, can be introduced in high school level. We show how problems that require extensive computational work can be solved using the Maxima algebraic computing system, which is free software. We also present suggestions for practical classroom activities for teachers.

Keywords: Modular Congruence, Mathematical Olympiad, Cryptography, RSA.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

O ramo da matemática que estuda os números inteiros e suas propriedades é chamado de teoria dos números. Os gregos foram os primeiros a se dedicar ao estudo dessa teoria, embora sejam conhecidos registros de sistemas de numeração antigos na Mesopotâmia, no Egito e na China. De acordo com Contador (2008), na Grécia dessa época os sábios pensadores não eram funcionários públicos, nem prestavam contas a nenhuma autoridade, eram livres para criar e defender seus pontos de vistas o que contribuiu com o avanço dos estudos na matemática. Dos pensadores que estudaram a teoria dos números destacam-se Pitágoras, Tales, Euclides e Arquimedes. Muito do que foi escrito na época se perdeu e a obra matemática mais importante foi a de Euclides, o livro *Os Elementos*. Além de suas próprias demonstrações, Euclides reuniu o que se sabia sobre matemática até a época e escreveu este tratado de 13 capítulos. Sabe-se muito pouco sobre a vida de Euclides, nem ao menos seu local de nascimento é conhecido (Boyer (1996)). É chamado de Euclides de Alexandria porque lecionava matemática no local, e não por ter nascido lá. Em seu livro, três capítulos são dedicados à teoria dos números. Nestes capítulos é possível encontrar a definição de números pares, ímpares, primos e compostos, assim como máximo divisor comum de dois números. Além disso, são apresentados teoremas, proposições e demonstrações da teoria dos números, como por exemplo o famoso Algoritmo de Euclides, utilizado para determinar o máximo divisor comum de dois números e a prova de que há infinitos números primos. Segundo Contador (2008), Os Elementos é o segundo trabalho mais traduzido e estudado na história, tem cerca de 800 edições e é superado apenas pela Bíblia. Foi escrito por volta de 300 a.C e sua primeira versão impressa foi em 1482.

Embora a matemática tenha sido estudada por gregos, árabes, indianos e europeus, a teoria dos números caiu em esquecimento até o século XVII quando Pierre de Fermat redescobriu a teoria e passou a estudá-la (Coutinho (2005)). Fermat não tinha a matemática como profissão, se dedicava aos estudos em suas horas vagas. Morreu no ano de 1665 aos 63 anos. O sucessor de Fermat no estudo da teoria dos números foi Leonhard Euler, nascido em 1707. Euler, ao contrário de Fermat tinha sua ocupação no estudo e pesquisa da matemática. De acordo com Burton (2011), Euler foi o escritor mais versátil de toda a história. Mesmo ficando quase cego, continuou suas obras realizando os cálculos mentalmente e ditando para que alguém escrevesse. Morreu em 1783 com 76 anos. Deixou muitos trabalhos inéditos, alguns publicados 47 anos após a sua morte. Euler popularizou a teoria dos números, mas o desenvolvimento da teoria se deu no século XIX a partir da publicação de *Disquisitiones Arithmeticae*, de Carl Friedrich Gauss (Coutinho (2005)). Gauss desde criança mostrou interesse e muita facilidade na resolução de problemas matemáticos. No ano de 1801 publicou a obra *Disquisitiones Arithmeticae*

reunindo resultados obtidos por matemáticos como Fermat, Euler, Lagrange e Legendre, assim como suas próprias descobertas. Além de contribuições na área da matemática, Gauss também contribuiu para descobertas na astronomia e na física. No primeiro capítulo de *Disquisitiones Arithmeticae* Gauss introduziu o conceito de congruência modular e a notação utilizada até os dias de hoje (Burton (2011)).

A congruência modular tem diversas aplicações em nosso cotidiano atualmente. Neste trabalho direcionaremos o estudo da congruência modular para sua aplicação na criptografia. Em Coutinho (2005), encontramos a definição de que criptografia é o estudo dos métodos necessários para codificar uma mensagem e a criptoanálise consiste na arte de decifrar sistemas criptográficos. De acordo com Singh (2003), o que motivou o desenvolvimento da criptografia foi a necessidade de manter em segredo mensagens trocadas entre reis, rainhas e generais. Essa necessidade levou nações a criar departamentos específicos para elaboração de códigos, assim como a contratação de pessoas capazes de decifrar os códigos dos inimigos. A batalha entre criadores e decifradores dos códigos inspirou uma série de grandes descobertas científicas. Hoje em dia, toda movimentação que realizamos através da internet está protegida pela criptografia. Isso só é possível graças ao avanço dos estudos nessa área. Segundo Figueiredo e Costa (2010) traços de criptografia apareceram na Mesopotâmia e no Egito por volta de 2000 a.C. com a utilização de hieróglifos. Uma das primeiras e mais conhecidas técnicas da criptografia foi a cifra de substituição utilizada pelo imperador romano Júlio César para se comunicar com seu exército. A técnica consiste em substituir cada letra do alfabeto por outra que está três posições a frente. Este método foi utilizado durante muito tempo, com chaves de codificações diferentes, até que criptoanalistas desenvolveram o estudo da análise de frequências. Neste estudo, é possível identificar a frequência com que cada letra do alfabeto é utilizada, facilitando assim a decodificação de uma mensagem criptografada através desse método. Além disso, nesse método de criptografia, para que o receptor da mensagem possa decodificar o que foi enviado, é necessário que este conheça a chave de codificação. Este tipo de criptografia é chamado de criptografia de chave privada e a explicação de seu funcionamento está na Seção 4.1 deste trabalho.

Em 1918 foi criada pelo engenheiro eletricista Arthur Scherbius a primeira máquina de cifras que foi chamada de Enigma. Após o desenvolvimento de novas versões dessa máquina, o exército alemão passou a utilizá-la na Segunda Guerra Mundial para a transmissão de mensagens secretas. Utilizando-se da análise de frequência, uma equipe inglesa liderada por Alan Turing quebrou a cifra da máquina Enigma podendo ter antecipado o fim da guerra em até um ano (Singh (2003)). Com a criação dos computadores e conhecendo a análise de frequências a criptografia de substituição era facilmente quebrada. Então, surgiu a necessidade de um algoritmo mais poderoso, difícil de ser quebrado até mesmo por computadores. A ideia de uma nova cifra, chamada de assimétrica, surgiu apenas em 1976 por Whitfield Diffie e Martin Hellmann.

A dupla desenvolveu um sistema criptográfico que utiliza chaves públicas e privadas. A ideia foi inovadora e gerou muitas pesquisas pelos estudiosos da criptografia. Embora a ideia tenha sido de Diffie e Hellmann, a criptografia assimétrica foi implementada por Ronald Rivest, Adi Shamir e Leonard Adleman utilizando a teoria das congruências modulares. O método ficou conhecido como RSA, sigla proveniente das iniciais dos sobrenomes Rivest, Shamir e Adleman. Hoje em dia o método é utilizado para garantir a segurança de procedimentos bancários realizados pela internet e compras *on-line* realizadas com cartão de crédito. O detalhamento do funcionamento desse método está presente na Seção 4.4 deste trabalho.

O principal objetivo deste trabalho é apresentar a congruência modular em uma aplicação prática que é o método RSA da criptografia. Além disso, utilizá-la como uma nova ferramenta para a resolução de problemas encontrados em olimpíadas de matemática. Embora a congruência modular não seja trabalhada em sala de aula no Ensino Básico, a teoria necessária para sua compreensão é amplamente discutida nos anos finais do Ensino Fundamental.

A Base Nacional Comum Curricular (MEC (2017)) inclui como habilidades a serem desenvolvidas no sexto ano a classificação de números naturais em primos e compostos, estabelecer relações entre múltiplos, divisores e fatores, critérios de divisibilidade por 2, 3, 4, 5, 6, 8, 9, 10, 100 e 1000, além de resolver e elaborar problemas que envolvam ideia de múltiplo e divisor. Estes conceitos trabalhados no Ensino Fundamental são conhecimentos prévios necessários para iniciar o estudo das congruências modulares.

Realizamos uma revisão de literatura com a intenção de encontrar trabalhos cujos temas envolveram congruência modular e criptografia. Encontramos vários relacionados com o tema, sendo muitos deles feitos por alunos do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT). Como vários destes trabalhos são parecidos entre si, destacamos aqui quatro que chamaram mais atenção. A dissertação de Pinheiro (2018) apresenta um projeto que foi aplicado a 20 alunos que obtiveram bom rendimento escolar em matemática, matriculados do sexto ao nono ano do Ensino Fundamental de uma escola da rede privada. Com objetivo de aprofundar os conteúdos trabalhados em sala de aula e mostrar aos alunos algumas aplicações de congruências modulares, Pinheiro aplicou o projeto em 10 aulas com duração de 90 minutos cada. Tópicos como divisibilidade, números primos, divisão euclidiana, aritmética modular e criptografia foram ensinados aos alunos através de teoremas, propriedades, exemplos numéricos e resolução de exercícios. Segundo Pinheiro (2018), o resultado obtido com o projeto foi bom, visto que a maior parte dos alunos compreendeu os conceitos e resolveu as atividades sem grandes dificuldades. A dissertação de Pinheiro apresenta um projeto desenvolvido com alunos que possuem aptidão em matemática, embora não seja focado na preparação de alunos em olimpíadas de matemática. Já o trabalho de Barros (2014), relata a aplicação de um projeto desenvolvido para alunos do Curso de Nível Médio Integrado em Química do Ins-

tituto Federal de Educação, Ciência e Tecnologia de Mato Grosso. Todos os alunos da 5ª fase participaram. Podemos encontrar nesta dissertação todas as listas de exercícios elaboradas, as avaliações que foram aplicadas, assim como as notas obtidas pelos alunos. Os exercícios propostos foram retirados de provas da Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP), Exame Nacional do Ensino Médio (ENEM) e vestibulares. Temas como números complexos, progressão aritmética, progressão geométrica e matrizes foram trabalhados através de congruências modulares. De acordo com Barros, os alunos não tiveram dificuldade em assimilar a teoria de congruências modulares com conteúdos já trabalhados no Ensino Médio. Na dissertação de Domingues (2017), o tema congruências modulares é proposto como um conteúdo extracurricular para alunos do Ensino Médio. Encontramos neste trabalho, um amplo capítulo sobre aplicações de congruências modulares. Dentre estas estão os códigos de barras, dígitos do CPF, ISBN e a criptografia. Domingues apresenta ainda uma sugestão de oficina destinada a alunos que desejam realizar provas da OBMEP e uma lista de exercícios envolvendo as aplicações de congruências modulares abordadas em sua dissertação. Seu trabalho difere dos dois primeiros citados por abordar as aplicações de uma forma mais detalhada, além de apresentar uma proposta na forma de uma oficina preparatória para OBMEP focada na aritmética e destinada a alunos do Ensino Médio. A dissertação de Fiarresga (2010) difere das demais por ter o enfoque na criptografia. Ela faz um estudo histórico da criptografia, apresenta um capítulo sobre a teoria matemática utilizada antes de definir e detalhar o funcionamento dos dois sistemas de criptografia: de chaves públicas e privadas. Também apresenta um capítulo sobre as assinaturas digitais, enfatizando a grande utilização da matemática nestes procedimentos. Cabe destacar que das quatro dissertações citadas, três foram elaboradas por alunos do (PROFMAT). Propomos nesta dissertação uma abordagem que estende as demais pesquisadas. Apresentamos duas resoluções de alguns exercícios retirados de olimpíadas de matemática. Uma das resoluções é feita da forma tradicional, com conceitos ensinados no Ensino Básico, enquanto que a outra é feita através de congruências modulares. As resoluções são acompanhadas de uma breve discussão e os problemas são classificados de acordo com o nível de dificuldade, segundo critérios previamente estabelecidos. Neste trabalho, focamos em uma das aplicações de congruências modulares, o método RSA, considerado um dos mais seguros e tem toda a sua base fundamentada nessa teoria.

Neste trabalho apresentamos exercícios de olimpíadas de matemática que podem ser resolvidos através de congruências modulares. Escolhemos três olimpíadas: Olimpíada Brasileira de Matemática das Escolas Públicas e Privadas (OBMEP,), Olimpíada Brasileira de Matemática (OBM,) e a Olimpíada Regional de Matemática de Santa Catarina (ORM,). A OBMEP foi criada em 2005 com o objetivo de estimular o estudo da matemática e identificar talentos na área. Podem participar dessa olimpíada alunos do 6º ano do Ensino Fundamental ao 3º ano do

Ensino Médio de escolas públicas e privadas. A olimpíada é realizada em duas fases: a primeira consiste em uma prova objetiva composta com 20 questões e os alunos, que se classificam para a segunda fase, realizam uma prova discursiva composta de 6 questões. A OBMEP é um projeto realizado pelo Instituto de Matemática Pura e Aplicada (IMPA), tem apoio da Sociedade Brasileira de Matemática (SBM) e é promovida com recursos do Ministério da Educação. Ao longo dos anos alguns projetos foram desenvolvidos pela OBMEP com o intuito de incentivar o ensino e a aprendizagem da matemática. São eles:

- Portal do Saber
- Obmep Nível A
- Banco de Questões e provas antigas
- Portal Clubes de Matemática
- POTI - Polos Olímpicos de Treinamento Intensivo
- PICME - Programa de Iniciação Científica e Mestrado
- Programa OBMEP na Escola.

Para informações sobre os programas, o leitor pode acessar o *site* oficial da OBMEP. A ORM é realizada desde 1998 e organizada pela Universidade Federal de Santa Catarina (UFSC). Podem participar dessa olimpíada alunos do 6º ano do Ensino Fundamental ao 3º ano do Ensino Médio de escolas públicas e privadas. Assim como a OBMEP, a ORM é realizada em duas fases: a primeira é composta de questões de múltipla escolha e a segunda fase composta de 5 questões discursivas. A Olimpíada Brasileira de Matemática é organizada pela Sociedade Brasileira de Matemática e teve sua primeira edição em 1979. O objetivo é estimular o estudo da matemática, desenvolver e aperfeiçoar a capacitação de professores e identificar novos talentos. Podem participar da OBM os 300 alunos com maior pontuação na segunda fase da OBMEP, todos os medalhistas da edição anterior da OBM e uma quantidade especificada, em cada ano, de alunos com melhor desempenho nas olimpíadas regionais apoiadas pela OBM.

O presente trabalho segue estruturado da seguinte forma: no Capítulo 2 apresentamos a fundamentação teórica necessária para a compreensão da teoria de congruência modular, assim como demonstrações e exemplos relacionados ao tema. No Capítulo 3 apresentamos nove problemas obtidos dos bancos de questões de olimpíadas de matemática e suas resoluções desenvolvidas de duas maneiras distintas: utilizando o conhecimento disponível no Ensino Básico e através de congruência modular. No Capítulo 4 apresentamos um breve histórico da criptografia, o método RSA, a teoria matemática aplicada, assim como alguns exemplos com o

objetivo de tornar mais claro o funcionamento do método. No Apêndice B mostramos como o *software* Maxima pode ser usado nas resoluções que exigem muitos cálculos tanto para encriptar, quanto para decriptar mensagens. No Capítulo 5 propomos uma lista de dez exercícios retirados de olimpíadas de matemática, com resoluções usando congruências modulares, e também três atividades relacionadas a criptografia. Este capítulo foi elaborado com a intenção de que o professor possa utilizar essas atividades tanto em treinamentos para olimpíadas como em uma proposta de aula diferenciada. No Capítulo 6 estão as considerações finais sobre o trabalho realizado e possibilidades para futuros projetos. Acrescentamos, ainda, no apêndice A uma demonstração do Teorema Fundamental da Aritmética utilizando o segundo princípio de indução.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo apresentaremos conceitos, proposições, teoremas e demonstrações sobre divisibilidade, números primos, divisão euclidiana e congruência modular. Dessa forma, admitiremos como conhecimentos prévios propriedades do conjunto dos números inteiros juntamente com as operações de adição e multiplicação. O conteúdo apresentado, com exceção de congruências, abrange conceitos que fazem parte da grade curricular do Ensino Básico. Embora o tema de congruências modulares não seja estudado no Ensino Básico, envolve conhecimentos prévios que são. Neste capítulo, reunimos conceitos necessários para o entendimento da teoria de congruências modulares e apresentamos, a professores e alunos do Ensino Fundamental e médio, uma nova ferramenta para a resolução de problemas que são, frequentemente, encontrados em olimpíadas de matemática. A congruência modular trata principalmente do estudo dos restos nas divisões euclidianas. Fazendo uma breve análise em algumas provas de olimpíadas de matemática verificamos que há questões em que o conhecimento sobre restos das divisões é útil ou até necessário para concluir a resolução destes exercícios.

2.1 DIVISIBILIDADE

Os primeiros registros conhecidos com definições e propriedades da divisibilidade foram encontrados na obra "Os Elementos", escrito pelo matemático grego Euclides de Alexandria. Em sua obra, composta de 13 partes, no Capítulo VII é possível identificar definições de número primo, números pares e ímpares assim como conceito de múltiplo. As definições, proposições e teoremas abaixo seguem o livro de Abramo Hefez (2014), Aritmética. Para alcançar o objetivo que é o estudo das congruências modulares, começaremos explorando a definição de divisibilidade e as proposições que dela resultam com as respectivas demonstrações. Denotaremos o produto de um número a por outro b como $a \cdot b$ ou, simplesmente ab.

Definição 2.1. *Dados dois números inteiros a e b, diremos que a divide b, denotando $a|b$, quando existir um número inteiro c tal que $b = ac$. Nesse caso, diremos também que a é um divisor ou fator de b ou ainda, que b é um múltiplo de a ou que b é divisível por a.*

Proposição 2.1. *Sejam a, b, c números inteiros. Tem-se que:*

(i) $1|a$, $a|a$, $a|0$;

(ii) $0|a$ *se, e somente se,* $a = 0$;

(iii) Se $a|b$ *e* $b|c$, *então* $a|c$.

Demonstração. (i) De fato, $1|a$, pois $a = 1a$.

Também $a|a$, pois existe o número inteiro 1 tal que $a = 1a$.

E $a|0$ pois existe o número inteiro 0 tal que $0 = a0$.

(ii) Se $0|a$, então existe um número inteiro x tal que $a = 0x$. Pelo item (i) segue que $a = 0$. Na recíproca, se $a = 0$, então pelo item (i), $0|a$.

(iii) Se $a|b$ e $b|c$, então existem números inteiros m e n tais que

$$b = am \tag{2.1}$$

e

$$c = bn. \tag{2.2}$$

Substituindo (2.1) em (2.2) temos:

$$c = (am)n \tag{2.3}$$

e assim

$$c = a(mn). \tag{2.4}$$

Como m e n são números inteiros, o produto mn também é, portanto $a|c$.

□

Proposição 2.2. *Sejam a,b,c,d números inteiros. Se $a|b$ e $c|d$, então $ac|bd$.*

Demonstração. Se $a|b$ e $c|d$ existem números inteiros m e n tais que

$$b = am \tag{2.5}$$

e

$$d = cn. \tag{2.6}$$

Multiplicando a Equação (2.5) por d, obtemos

$$bd = amd. \tag{2.7}$$

Substituindo (2.6) em (2.7), temos que

$$bd = amcn \tag{2.8}$$

e assim

$$bd = ac(mn). \tag{2.9}$$

Como m e n são números inteiros, segue que o produto mn é um número inteiro e, portanto, $ac|bd$. □

Vejamos um exemplo de aplicação desta última proposição.

Exemplo 2.1. *Notemos que* $3|9$ *, pois* $9 = 3 \cdot 3$ *, e* $5|10$ *pois* $10 = 5 \cdot 2$*. Então, pela Proposição 2.2 podemos afirmar que* $3 \cdot 5|9 \cdot 10$*. De fato,* $15|90$*, pois* $90 = 15 \cdot 6$*.*

Proposição 2.3. *Sejam a, b, c números inteiros tais que* $a|(b \pm c)$*. Então* $a|b$ *se, e somente se,* $a|c$*.*

Demonstração. Suponhamos que $a|(b+c)$. Então existe um número inteiro k tal que

$$b + c = ak. \tag{2.10}$$

Se $a|b$, então existe um número inteiro m tal que

$$b = am. \tag{2.11}$$

Subtraindo b em ambos os membros de (2.10) obtemos,

$$c = ak - b. \tag{2.12}$$

Substituindo (2.11) em (2.12) temos que

$$c = ak - am = a(k - m). \tag{2.13}$$

Como k e m são números inteiros, segue que $(k-m)$ também é inteiro, de modo que $a|c$. Para a recíproca, se $a|c$ então existe um número inteiro n tal que

$$c = an. \tag{2.14}$$

Subtraindo c em ambos os membros de (2.10), obtemos

$$b = ak - c. \tag{2.15}$$

Substituindo (2.14) em (2.15) temos que

$$b = ak - an = a(k - n). \tag{2.16}$$

Como $(k-n)$ é um número inteiro, uma vez que k e n são inteiros, segue que $a|b$.
A demonstração para o caso $a|(b-c)$ é feita de maneira análoga. □

Exemplo 2.2. *O número 6 divide 114, pois* $114 = 6 \cdot 19$*. Podemos escrever 114 como* $102 + 12$*. Pela proposição acima, temos que 6 divide 102 se, e somente se 6 divide 12. Como de fato 6 divide 12, já que* $12 = 6 \cdot 2$ *, podemos afirmar que 6 divide 102.*

Proposição 2.4. *Se a,b,c são números inteiros tais que $a|b$ e $a|c$, então para todos x,y inteiros tem-se $a|(xb+yc)$.*

Demonstração. Como $a|b$ e $a|c$, existem números inteiros m, n tais que

$$c = am \tag{2.17}$$

e

$$b = an. \tag{2.18}$$

Multiplicando (2.17) por y e (2.18) por x, obtemos

$$yc = amy \tag{2.19}$$

e

$$xb = anx. \tag{2.20}$$

Adicionando membro a membro as Equações (2.19) e (2.20) obtemos

$$yc + xb = amy + anx = a(my + nx). \tag{2.21}$$

Como os produtos my e nx são ambos números inteiros, $(my+nx)$ também é inteiro, e portanto podemos concluir que $a|(xb+yc)$. □

2.2 DIVISÃO EUCLIDIANA

A divisão Euclidiana trata da divisão com resto e é estudada por alunos já nas séries iniciais do Ensino Fundamental. Veremos a seguir, a demonstração do teorema. Para essa demonstração, utilizaremos a técnica de redução ao absurdo (do latim *reductio ad absurdum*), ou prova por contradição. Esse tipo de prova é feita assumindo como verdade o contrário do que se quer provar, chegando então a uma contradição. Vejamos um breve exemplo de uma demonstração por contradição.

Exemplo 2.3. *Se p^2 é par, então p é par.*

Solução:

Primeiramente, observemos que, se p não for par ele terá de ser ímpar. Iniciaremos a demonstração negando a tese de que p é par. Suponha que p seja ímpar. Então ele pode ser escrito da forma $2k+1$. Assim, para p^2 temos que

$$p^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1. \tag{2.22}$$

Portanto, temos que p^2 é ímpar, o que é uma contradição com a hipótese de que ele é par. Ou seja, ele teria que ser ímpar e par ao mesmo tempo. Aí está o absurdo. Logo, p não é ímpar, isto é, p é par.

Veremos a seguir o teorema da divisão euclidiana.

Teorema 2.1 (Divisão Euclidiana)**.** *Sejam a e b dois números inteiros com $b \neq 0$. Então existe um único par de números inteiros q e r tais que*

$$a = bq + r, \qquad com \quad 0 \leq r < |b|. \tag{2.23}$$

Demonstração. Provemos a existência dos inteiros q e r e também a unicidade desses elementos.

Existência: Consideremos o conjunto

$$S = \{x = a - by \; ; \; a - by \geq 0, \; y \in \mathbb{Z}\}. \tag{2.24}$$

Devemos mostrar que esse conjunto não é vazio. O conjunto dos números inteiros é ilimitado, então existe um inteiro n tal que

$$a > nb, \tag{2.25}$$

e, sendo assim

$$a - nb > 0. \tag{2.26}$$

Portanto, o conjunto S não é vazio pois $a - nb \in S$. O conjunto S é limitado inferiormente por 0. Logo, pelo Princípio da Boa Ordem, temos que S possui um menor elemento r. Suponhamos então que

$$r = a - b. \tag{2.27}$$

Como $r \in S$, sabemos que $r \geq 0$. Mostraremos que $r < |b|$. Suponhamos por absurdo que $r \geq |b|$.Portanto, existe $k \in \mathbb{N}$ tal que

$$r = |b| + k. \tag{2.28}$$

Como $r = a - bq$, da Equação (2.28) segue que

$$a - bq = |b| + k. \tag{2.29}$$

Assim,

$$a - bq - |b| = k \tag{2.30}$$

e

$$a - b(q \pm 1) = k. \tag{2.31}$$

Da Equação (2.31), temos que $k \in S$. Da Equação (2.28), temos que $0 \leq k < r$, o que é uma contradição pois, r é o menor elemento de S. Portanto, $r < |b|$.

Unicidade: Devemos mostrar que q e r são os únicos valores que satisfazem a igualdade $a = bq + r$. Suponha que existam q' e r' inteiros, tais que

$$a = bq + r = bq' + r', \tag{2.32}$$

com $0 \leq r < |b|$ e $0 \leq r' < |b|$. Como $0 \leq r$, temos que

$$-r \leq 0. \tag{2.33}$$

Somando r' em ambos os membros de (2.33), temos

$$r' - r \leq r'. \tag{2.34}$$

Também,

$$0 \leq r', \tag{2.35}$$

então, somando $-r$ em ambos os membros da Equação (2.35) temos

$$-r \leq r' - r. \tag{2.36}$$

De (2.34) e (2.36), e do fato de $r' \leq |b|$, segue que

$$-r \leq r' - r \leq r' < |b|. \tag{2.37}$$

Como $r < |b|$, tem-se que

$$-r > -|b|. \tag{2.38}$$

Das Equações (2.37) e (2.38), temos que

$$-|b| < -r \leq r' - r \leq r' < |b|. \tag{2.39}$$

Se $-|b| < r' - r < |b|$, podemos escrever que

$$|r' - r| < |b|. \tag{2.40}$$

Temos

$$a = bq + r \tag{2.41}$$

e

$$a = bq' + r'. \tag{2.42}$$

Subtraindo (2.41) de (2.42) temos que

$$0 = b(q - q') + r - r' \tag{2.43}$$

Somando $r' - r$ em ambos os lados da igualdade, temos que

$$b(q - q') = r' - r. \tag{2.44}$$

Aplicando módulo em ambos os membros, segue que

$$|b| \cdot |q - q'| = |r' - r|. \tag{2.45}$$

Das Equações (2.45) e (2.40), temos que

$$|b| \cdot |q - q'| < |b|, \tag{2.46}$$

que só ocorre se $|q - q'| = 0$, isto é, só ocorre se $q = q'$. Consequentemente, se $q = q'$ teremos $r = r'$. Portanto, q e r são os únicos números inteiros tais que

$$a = bq + r, \qquad com \quad 0 \leq r < |b|. \tag{2.47}$$

□

Para auxiliar em demonstrações e resoluções de problemas que serão tratados mais adiante, veremos a seguir a definição de máximo divisor comum, algumas proposições que dela resultam e a definição de mínimo múltiplo comum.

Definição 2.2 (Máximo Divisor Comum)**.** *Um número inteiro $d \geq 0$ é um máximo divisor comum (mdc) dos inteiros a e b, se possuir as seguintes propriedades:*

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

O máximo divisor comum dos números inteiros a e b será denotado por (a,b). Além disso, dados a e b inteiros, se existir (a,b), então $(a,b) = (-a,b) = (a,-b) = (-a,-b)$. Dessa forma, quando for necessário calcular o máximo divisor comum de dois números, podemos sempre trabalhar com números não negativos.

Exemplo 2.4. *O máximo divisor comum de 12 e 18 é 6 pois 6 divide 12 e 18 e os demais divisores de 12 e 18 são 1, 2 e 3, os quais dividem 6.*

Proposição 2.5. *Sejam a e b inteiros e seja $(a,b) = c$. Então, existem x e y inteiros tais que*

$$c = ax + by. \tag{2.48}$$

Demonstração. Se $a = 0$ e $b = 0$, então $c = 0$ e quaisquer x, y satisfazem

$$c = 0x + 0y. \tag{2.49}$$

Se $a \neq 0$, ou $b \neq 0$ considere o conjunto S como definido a seguir:

$$S = \{ax + by;\ x,\ y \in \mathbb{Z},\ ax + by > 0\}. \tag{2.50}$$

Como $a \cdot a + b \cdot b = a^2 + b^2$ e $a^2 + b^2 \in S$ (pois $a \neq 0$, ou $b \neq 0$), então S não é vazio. Pelo Princípio da Boa Ordem, existe $d \in S$ que é o menor elemento desse conjunto. Então, podemos escrever d como:

$$d = ax' + by'. \tag{2.51}$$

Afirmamos que d divide todos os elementos de S. De fato, seja m um elemento de S, logo m pode ser escrito como

$$m = ax_0 + by_0\ , \qquad x_0\ ,\ y_0 \in \mathbb{Z}. \tag{2.52}$$

Suponha que d não divide m. Então, na divisão de m por d obteremos um resto r:

$$m = dq + r\ , \qquad 0 \leq r < d. \tag{2.53}$$

Subtraindo dq em ambos os membros da Equação (2.53), temos

$$r = m - dq. \tag{2.54}$$

Substituindo (2.51) e (2.52) em (2.53), temos que

$$r = ax_0 + by_0 - (ax' + by')q. \tag{2.55}$$

Colocando a e b em evidência, temos

$$r = a(x_0 - x'q) + b(y_0 - y'q). \tag{2.56}$$

Como $(x_0 - x'q)$ e $(y_0 + y'q)$ são ambos inteiros, segue que r é um elemento de S, ou $r = 0$. Como $r < d$ e d é o menor elemento de S, segue que $r = 0$ e portanto, a Equação (2.53) pode ser reescrita como

$$m = dq, \tag{2.57}$$

o que significa que $d|m$. Logo, d divide qualquer elemento de S.

Se d divide qualquer elemento de S, temos que $d|a$ e $d|b$, uma vez que $a = a \cdot 1 + b \cdot 0\ \in S$ e

$b = a \cdot 0 + y \cdot 1 \in S$. Se $d|a$ e $d|b$, então $d|c$ pois c é o maior divisor comum de a e b. Como $d|c$ podemos afirmar que

$$d \leq c. \tag{2.58}$$

Como $(a,b) = c$ temos que $c|a$ e $c|b$, portanto, para quaisquer x e y inteiros temos que $c|ax$ e $c|by$ o que implica que $c|ax+by$. Assim, como $d = ax' + by'$, temos que $c|d$, e portanto

$$c \leq d. \tag{2.59}$$

Comparando as Equações (2.58) e (2.59), concluímos que $d = c$. Logo, existem x e y inteiros tais que $c = ax + by$. □

Quando o máximo divisor comum de dois números é 1, dizemos que os números são coprimos ou primos entre si.

Exemplo 2.5. *O máximo divisor comum entre 5 e 7 é 1, portanto 5 e 7 são coprimos.*

Os resultados a seguir serão úteis para a demonstração de outras proposições.

Proposição 2.6. *Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros m e n tais que* $ma + nb = 1$.

Demonstração. A primeira parte da demonstração é resultado direto do Teorema 2.5.
Se $(a,b) = 1$, então existem dois inteiros m, n tais que

$$1 = ma + nb. \tag{2.60}$$

Para a recíproca, suponha que existam m e n inteiros tais que

$$1 = ma + nb. \tag{2.61}$$

Então, sendo $d = (a,b)$ temos que $d|a$, $d|b$, e consequentemente $d|ma$, $d|nb$ e $d|ma+nb$. Como $ma + nb = 1$, segue que $d|1$ e, portanto , $d = 1$. □

Teorema 2.2 (Lema de Gauss)**.** *Sejam* a,b,c *números inteiros. Se* $a|bc$ *e* $(a,b) = 1$*, então* $a|c$.

Demonstração. Se $a|bc$, então existe um número inteiro z tal que

$$ab = cz. \tag{2.62}$$

Se $(a,b) = 1$ então, pela Proposição 2.6 existem x e y inteiros tais que

$$1 = ax + by. \tag{2.63}$$

Multiplicando a Equação (2.63) por um inteiro a, obtemos

$$a = acx + aby. \tag{2.64}$$

Substituindo (2.62) em (2.64), temos que

$$a = acx + czy. \tag{2.65}$$

Podemos colocar o termo c em evidência resultando na equação

$$a = c(ax + zy). \tag{2.66}$$

Como a, x, y, z são inteiros, a soma $ax + zy$ também é. Portanto, $c|a$. □

Definição 2.3 (Mínimo Múltiplo Comum)**.** *Um número inteiro $m \geq 0$ é um mínimo múltiplo comum (mmc) de dois números inteiros a e b, se possuir as seguintes propriedades:*

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

O mínimo múltiplo comum de dois números a e b inteiros, se existe, é denotado por $[a,b]$, e, $[a,b] = [-a,b] = [a,-b] = [-a,-b]$. Além disso, dados inteiros não nulos $a_1, a_2, \cdots, a_n$ o número $[a_1, \cdots, a_n]$ existe e $[a_1, a_2, \cdots, a_{n-1}, a_n] = [a_1, \cdots, [a_{n-1}, a_n]]$.

Exemplo 2.6. *O número 20 é um múltiplo comum de 2 e 5, mas não é um mmc desses números. O número 10 é um mmc desses números pois,* $10|20$.

2.3 NÚMEROS PRIMOS

De acordo com Eves (2004), os primeiros registros que se tem conhecimento sobre números primos estão na obra "Os Elementos"de Euclides. O Capítulo VII de Os Elementos, trata dos números primos e primos entre si e, no Capítulo IX, Euclides apresenta uma prova para a infinitude dos primos, assim como a primeira versão de que se tem conhecimento do Teorema Fundamental da Aritmética.

Definição 2.4 (Número Primo)**.** *Um número natural maior do que 1 que só possui como divisores positivos 1 e ele próprio é chamado de número primo. Um número natural maior do que 1 e que não é primo será dito composto.*

Vejamos alguns exemplos de números primos e números compostos.

Exemplo 2.7. *O número 5 é primo, pois possui como divisores apenas os números 1 e 5.*

Exemplo 2.8. *O número 17 é primo, pois possui como divisores apenas os números 1 e 17.*

Exemplo 2.9. *O número 10 é composto, pois possui como divisores os números 1, 2, 5 e 10.*

Exemplo 2.10. *O número 24 é composto, pois possui como divisores os números 1, 2, 3, 4, 6, 8, 12 e 24.*

Vejamos agora proposições e demonstrações importantes que envolvem números primos.

Proposição 2.7 (Lema de Euclides)**.** *Sejam a, b, p números inteiros, com p primo. Se $p|ab$, então $p|a$ ou $p|b$.*

Observação: Se $p|a_1a_2a_3\cdots a_n$, então $p|a_i$, para algum $i \in 1, 2, \cdots, n$.

Queremos provar que uma ou outra afirmação é verdadeira, então, para desenvolver essa demonstração faremos o seguinte procedimento: vamos negar que aconteça a primeira das afirmações, chegando na conclusão de que a segunda ocorre. Em seguida negamos a segunda afirmação, e concluímos que dessa forma, a primeira ocorre. Assim, podemos garantir ser verdadeira pelo menos uma das afirmações.

Demonstração. Suponhamos que p não divida a. Então, como p é primo, temos que $(p,a) = 1$. Segue pelo Lema de Gauss, Teorema 2.2, que se $(p,a) = 1$ e $p|ab$ então $p|b$. Analogamente, se supormos que p não divide b, temos $(p,b) = 1$. Pelo Lema de Gauss, Teorema 2.2, segue que $p|a$. □

Veremos agora a demonstração do Teorema Fundamental da Aritmética. Este teorema teve sua primeira versão no livro de Euclides, mas a primeira prova detalhada foi publicada em 1798 por Carl Friedrich Gauss em seu livro *Disquisitiones Arithmeticae* (Eves (2004)). A demonstração a seguir foi baseada em Niven, Zuckerman e Montgomery (1991).

Teorema 2.3 (Teorema Fundamental da Aritmética)**.** *Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como produto de números primos.*

Demonstração. A hipótese se refere a todo número natural então, suponha por absurdo que exista pelo menos um número natural maior que 1 que não pode ser escrito como produto de números primos. Seja n o menor desses números. O número n não pode ser primo, pois nesse caso seria produto de um único fator primo. Então, suponha que $n = ab$, com a e b números naturais. Como a e b são divisores de n, ambos são menores que n. Além disso, n é o menor número natural que pode ser escrito como produto de números compostos, então a e b podem ser escritos como produto de números primos. Seja $a = p_1p_2...p_r$ e $b = q_1q_2...q_t$, com p_i

$(i = 1,2,...,r)$ primo e q_i $(i = 1,2,...,t)$ primo, as decomposições em fatores primos de a e b. Logo, podemos escrever

$$n = p_1 \cdot p_2 \cdots p_r \cdot q_1 \cdot q_2 \cdots q_t. \tag{2.67}$$

Portanto, n pode ser escrito como um produto de números primos, o que é uma contradição com a afirmação inicial. Sendo assim, podemos concluir que todo número natural pode ser escrito como produto de números primos.
Agora, devemos provar que existe uma única maneira de escrever um número como produto de primos. Suponha que existam duas formas diferentes de escrever um número k como produto de números primos. Seja

$$k = p_1 \cdot p_2 ... p_r = q_1 \cdot q_2 ... q_t. \tag{2.68}$$

Portanto $p_1 | q_1 \cdot q_2 ... q_t$, e, como p_1 é primo, $p_1 | q_j$ para algum $j = 1,2,...,t$. Como p_1 e q_j são primos, temos $p_1 = q_j$. Fazendo isso para cada fator, concluímos que para cada p_i, $i = 1,2,...,r$, existe um q_j , $j = 1,2,...,t$, de igual valor e, portanto o número k é escrito de forma única, a menos da ordem dos fatores primos. □

No Apêndice A apresentamos a demonstração do Teorema Fundamental da Aritmética utilizando o segundo princípio de indução.

2.4 CONGRUÊNCIA MODULAR

Gauss quem introduziu o conceito de congruência modular, assim como sua notação (Burton (2011)). A escolha do símbolo $\equiv$ se deu pela analogia com a igualdade algébrica.

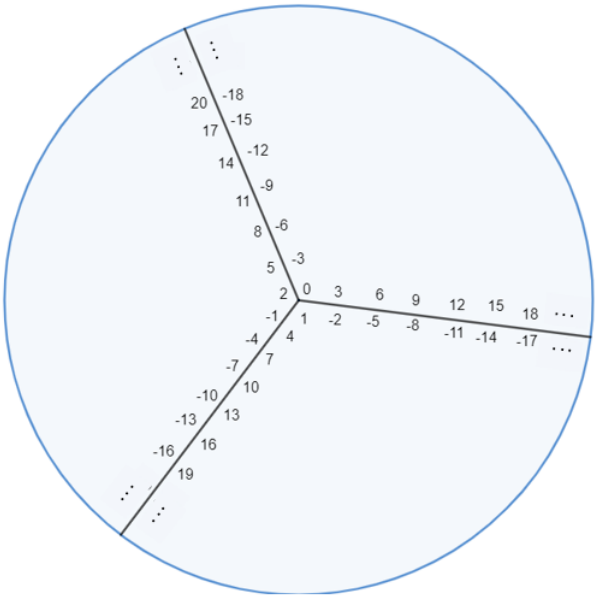
Definição 2.5. *Seja m um número natural. Diremos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se:*

$$a \equiv b \mod m. \tag{2.69}$$

Quando a relação $a \equiv b \mod m$ *for falsa, diremos que a e b não são congruentes ou que são incongruentes módulo m. Escrevemos* $a \not\equiv b \mod m$.

A Figura 2.1, baseada na referência Khan Academy (), é uma ilustração da congruência módulo 3 para os números inteiros. Neste caso, há três possíveis restos: 0, 1 ou 2. Então, representamos cada resto como uma fatia ou módulo do círculo e, em seguida, colocamos cada número inteiro no módulo que corresponde ao seu resto na divisão euclidiana.

Figura 2.1 – Congruência módulo 3



Fonte:o autor.

Observemos que os números que estão em um mesmo módulo, deixam o mesmo resto na divisão euclidiana, e portanto, dois números de uma mesma fatia são congruentes módulo 3. Por exemplo, temos que $-16 \equiv 17 \mod 3$, pois $-16 = 3 \cdot (-6) + 2$ e $17 = 3 \cdot 5 + 2$. Ou seja, -16 e 17 deixam o mesmo resto na divisão euclidiana por três. Veja mais alguns exemplos referente a outros módulos:

Exemplo 2.11. *Diremos que* $15 \equiv 11 \mod 4$*, pois os restos da divisão de 15 e 11 por 4 são ambos iguais a 3.*

Exemplo 2.12. *Temos que* $10 \not\equiv 8 \mod 5$*, pois o resto da divisão de 10 por 5 é zero, enquanto o resto da divisão de 8 por 5 é 3.*

Proposição 2.8. *Suponha que os números* a, b, m *são inteiros, com* $m > 1$*. Tem-se que* $a \equiv b \mod m$ *se, e somente se,* $m | b - a$*.*

Demonstração. Se $a \equiv b \mod m$, então os restos das divisões de a e b por m são iguais. Sejam r esse resto, x e y os quocientes na divisão de a e b por m respectivamente. Então,

$$a = mx + r, \qquad 0 \leq r < x \tag{2.70}$$

e

$$b = my + r, \qquad 0 \leq r < y. \tag{2.71}$$

Efetuando a subtração de (2.71) por (2.70) obtemos

$$b - a = (my + r) - (mx + r) \tag{2.72}$$

e assim

$$b-a = my-mx = m(y-x). \tag{2.73}$$

Como y e x são números inteiros, $(y-x)$ também é e, portanto, $m|b-a$.
Para a recíproca, se $m|b-a$, então existe um número inteiro k tal que

$$b-a = mk. \tag{2.74}$$

Sejam r_1 e r_2 os restos das divisões euclidianas de a e b por m, respectivamente e s e t os quocientes. Temos que

$$a = ms + r_1 \tag{2.75}$$

e

$$b = mt + r_2. \tag{2.76}$$

Subtraindo (2.75) de (2.76), obtemos

$$b-a = (mt+r_2) - (ms+r_1) \tag{2.77}$$

$$b-a = mt - ms + r_2 - r_1 \tag{2.78}$$

$$b-a = m(t-s) + (r_2-r_1). \tag{2.79}$$

Das Equações (2.74) e (2.79) temos $k = (t-s)$ e que $(r_2-r_1) = 0$. Sendo assim, $r_1 = r_2$ o que implica em

$$a \equiv b \mod m. \tag{2.80}$$

□

Proposição 2.9. *Seja m um número natural. Para todos os inteiros a, b, c tem-se que:*

(i) $a \equiv a \mod m$;
(ii) Se $a \equiv b \mod m$, *então* $b \equiv a \mod m$;
(iii) Se $a \equiv b \mod m$ *e* $b \equiv c \mod m$, *então* $a \equiv c \mod m$.

Demonstração. (i) De fato, $m|a-a$ pois, $a-a = 0$ e, pela Proposição 2.1, segue que $m|0$.

(ii) Por definição, se $a \equiv b \mod m$ então a e b deixam o mesmo resto na divisão por m. Se b e a deixam o mesmo resto na divisão por m então $b \equiv a \mod m$.

(iii) Se $a \equiv b \mod m$ e $b \equiv c \mod m$, então $m|b-a$ e $m|c-b$. Logo, existem x e y inteiros tais que

$$b-a = mx \tag{2.81}$$

e

$$c-b = my. \tag{2.82}$$

Somando as Equações (2.81) e (2.82) membro a membro, temos que

$$(b-a)+(c-b)=mx+my. \tag{2.83}$$

Podemos reescrever a Equação (2.83) como

$$c-a=m(x+y). \tag{2.84}$$

Como x e y são números inteiros, a soma $(x+y)$ também representa um número inteiro. Da Equação (2.84) segue que $m|c-a$ e, portanto

$$a \equiv c \mod m. \tag{2.85}$$

□

Proposição 2.10. *Sejam a,b,c,d,m números inteiros, com $m>1$. Se $a \equiv b \mod m$ e $c \equiv d \mod m$. Então :*

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

(ii) $a-c \equiv b-d \mod m$;

(iii) $ka \equiv kb \mod m$, *para todo k inteiro;*

(iv) $ac \equiv bd \mod m$;

(v) $a^k \equiv b^k \mod m$, *para todo k natural.*

Demonstração. (i) Se $a \equiv b \mod m$ e $c \equiv d \mod m$, pela Proposição 2.8 temos que $m|b-a$ e $m|d-c$. Se $m|b-a$ e $m|d-c$, então existem x e y inteiros tais que

$$b-a=mx \tag{2.86}$$

e

$$d-c=my. \tag{2.87}$$

Adicionando membro a membro as Equações (2.86) e (2.87) temos

$$(b-a)+(d-c)=mx+my \tag{2.88}$$

que pode ser reescrita como

$$(b+d)-(a+c)=m(x+y). \tag{2.89}$$

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

$$a+c \equiv b+d \mod m. \tag{2.90}$$

(ii) Se $m|b-a$ e $m|d-c$, então existem x e y inteiros tais que

$$b-a=mx \tag{2.91}$$

e

$$d-c=my. \tag{2.92}$$

Subtraindo a Equação (2.92) de (2.91) temos

$$(b-a)-(d-c)=mx-my \tag{2.93}$$

que pode ser reescrita como

$$(b-d)-(a-c)=m(x-y). \tag{2.94}$$

Logo, temos que $m|(b-d)-(a-c)$ e portanto

$$a-c\equiv b-dm. \tag{2.95}$$

(iii) Como $m|b-a$, existe um número x inteiro tal que

$$b-a=mx. \tag{2.96}$$

Sendo k um inteiro qualquer, multiplicando a Equação (2.96) por k, obtemos

$$k(b-a)=mxk. \tag{2.97}$$

Como k e x são números inteiros, o produto kx também é, logo

$$m|k(b-a)=kb-ka. \tag{2.98}$$

Portanto, $ka\equiv kb \mod m$.

(iv) Como $m|b-a$ e $m|d-c$, existem números inteiros k e q tais que

$$b-a=mk \tag{2.99}$$

e

$$d-c=mq. \tag{2.100}$$

Multiplicando (2.99) por d e (2.100) por a, obtemos

$$bd-ad=mkd \tag{2.101}$$

e

$$ad - ac = mqa. \tag{2.102}$$

Adicionando as Equações (2.101) e (2.102) membro a membro, obtemos

$$bd - ad + ad - ac = mkd + mqa. \tag{2.103}$$

Assim,

$$bd - ac = m(kd - qa). \tag{2.104}$$

Como $(kd - qa)$ é um número inteiro, segue que $m|bd - ac$ e portanto

$$ac \equiv bd \mod m. \tag{2.105}$$

(v) Se $a \equiv b \mod m$, podemos utilizar o item (iv) desta proposição uma quantidade k de vezes para obter

$$a \cdot a \cdot a \cdots a \equiv b \cdot b \cdot b \cdots b \mod m. \tag{2.106}$$

$$a^k \equiv b^k \mod m \tag{2.107}$$

□

A proposição abaixo mostra que para as congruências, vale o cancelamento com relação a adição.

Proposição 2.11. *Sejam a, b, c, m números inteiros, com $m > 1$. Tem-se que $a + c \equiv b + c \mod m$ se, e somente se, $a \equiv b \mod m$.*

Demonstração. Se $a + c \equiv b + c \mod m$, então $m|(b + c) - (a + c)$.
Como $(b + c) - (a + c) = b - a$, temos que $m|b - a$ e, portanto $a \equiv b \mod m$.
Para a recíproca, temos por hipótese que $a \equiv b \mod m$. Pelo item (i) da Proposição 2.9, temos que $c \equiv c \mod m$. Então, pelo item (i) da Proposição 2.10 segue que $a + c \equiv b + c \mod m$. □

Proposição 2.12. *Sejam a e b números inteiros, e $n, m, m_1, m_2, \ldots, m_r$ inteiros maiores que 1. Temos que*

(i) se $a \equiv b \mod m$ e $n|m$, então $a \equiv b \mod n$;
(ii) $a \equiv b \mod m_i$, para todo $i = 1, \ldots, r$ se, e somente se, $a \equiv b \mod [m_1, \ldots, m_r]$;

Demonstração. (i) $a \equiv b \mod m$ então, temos que $m|b - a$.
Como $n|m$, pelo item (iii) da Proposição 2.1, temos que se $n|m$ e $m|b - a$, então $n|b - a$, isto é $a \equiv b \mod n$.

(ii) Se $a \equiv b \mod m_i,\ i = 1,2,\ \ldots,r$, então $m_i|b-a$ para todo i. Sendo $b-a$ um múltiplo de todo m_i, então será múltiplo de $[m_1,\ \ldots,m_r]$, isto é, $[m_1,\ \ldots,m_r]|b-a$ o que significa que $a \equiv b \mod [m_1,\ \ldots,m_r]$.
Para a recíproca, se $a \equiv b \mod [m_1,\ \ldots,m_r]$, então temos que $[m_1,\ \ldots,m_r]|b-a$. Como $m_i|[m_1,\ \ldots,m_r]$ para todo i, então, pelo item (i), segue que $a \equiv b \mod m_i$.

□

As proposições e os teoremas enunciados até o momento já nos permitem resolver problemas que envolvam congruências. No entanto, em algumas situações será necessário que realizemos a resolução de sistemas lineares de congruências. E para isso, precisaremos do Teorema 2.4, conhecido como Teorema Chinês dos Restos, enunciado e demonstrado a seguir. Este teorema foi estudado simultaneamente por gregos e chineses (Prazeres (2014) e Ruivo (2016)). O primeiro registro, de que se tem conhecimento, foi feito por um matemático chinês entre os anos de 287 d.C a 473 d.C. Não se sabe ao certo quem foi este matemático, embora, alguns autores o nomeiem como Sun-Tsu. O que de fato pode-se garantir, é que o teorema foi desenvolvido durante estudos sobre astronomia e a criação de um calendário. Segundo Ing (2003), o teorema aparece no terceiro capítulo de um tratado matemático chinês chamado Sun Zi Sujanjing (O clássico matemático do mestre Sol). Para introduzir o teorema, o autor expõe o problema:

Há um número desconhecido de coisas. Se contarmos de três em três, sobram duas. Se contarmos de cinco em cinco, sobram três. E, se contarmos de sete em sete, sobram duas. Qual é essa quantidade de coisas?

O tratado apresenta apenas uma solução para o problema, fato que deixou matemáticos e pesquisadores envolvidos em seu estudo durante muitos anos. Atualmente, o Teorema Chinês dos Restos pode ser enunciado da seguinte forma.

Teorema 2.4. *(Teorema Chinês dos Restos) Sejam $m_1, m_2,\ \ldots,m_r$, inteiros positivos primos entre si, dois a dois, e sejam $a_1, a_2,\ \ldots,a_r$ inteiros quaisquer. Então, o sistema de congruências:*

$$x \equiv a_1 \mod m_1 \tag{2.108}$$

$$x \equiv a_2 \mod m_2 \tag{2.109}$$

$$\vdots \tag{2.110}$$

$$x \equiv a_r \mod m_r \tag{2.111}$$

admite uma solução única módulo $M = m_1 m_2 \cdots m_r$. As soluções são

$$x = M_1 \cdot y_1 \cdot a_1 + \cdots + M_r \cdot y_r \cdot a_r + tM, \tag{2.112}$$

onde t é um número inteiro, $M_i = \frac{M}{m_i}$ *e* y_i *é solução de* $M_iY \equiv 1 \mod m_i,\ i = 1,...,r.$

Demonstração. Vamos mostrar inicialmente que x é uma solução de todas as equações do sistema $x_i \equiv a_i \mod m_i$, para $i = 1,2,3,...,r$.
Temos $M = m_1 m_2 \cdots m_r$, $M_i = \frac{M}{m_i}$ e y_i solução de $M_iY \equiv 1 \mod m_i$.
Sabemos que $m_i|M$, já que M é o produto de todos os m_i. Além disso, tem-se que $m_i|M_j$ se $i \neq j$ pois, M_j é o produto de todos os m_i com exceção de m_j.
Considere o número x tal que

$$x = a_1M_1y_1 + a_2M_2y_2 + \cdots + a_rM_ry_r \tag{2.113}$$

Como $m_i|M_j$ para $i \neq j$, então m_i divide cada parcela de x, com exceção da parcela $a_iM_iy_i$. Então, podemos escrever

$$x \equiv a_iM_iy_i \mod m_i. \tag{2.114}$$

Como $M_iy_i \equiv 1 \mod m_i$, da Proposição 2.10 e da equação (2.114) temos que

$$x \equiv a_i \cdot 1 \mod m_i, \tag{2.115}$$

isto é,

$$x \equiv a_i \mod m_i, \tag{2.116}$$

o que mostra que x é solução de todas as equações do sistema simultaneamente.
Agora, devemos mostrar que qualquer outra solução do sistema, será congruente a x módulo M.
Suponha que x' também seja solução para o sistema. Então, como

$$x \equiv a_i \mod m_i \tag{2.117}$$

e

$$x' \equiv a_i \mod m_i. \tag{2.118}$$

Pela Proposição 2.9 segue que

$$x \equiv x' \mod m_i. \tag{2.119}$$

Como m_i e m_j são primos entre si para $i \neq j$, segue que o mínimo múltiplo comum de $m_1, m_2, \cdots, m_r$ será $m_1 \cdot m_2 \cdots m_r = M$. Logo, pela Proposição 2.12, temos que

$$x \equiv x' \mod M. \tag{2.120}$$

□

3 PROBLEMAS

Este capítulo apresenta alguns problemas retirados de olimpíadas de matemática e de programas de treinamento para olimpíadas. Para cada problema são propostas duas soluções, uma utilizando os conceitos da matemática que são aplicados no Ensino Básico (SOLUÇÃO 1) e outra utilizando os conceitos de congruência modular (SOLUÇÃO 2). Para as soluções baseadas em algum autor, citaremos a referência.

Classificamos os problemas em três níveis de dificuldade: fácil, intermediário e difícil. Para essa classificação usaremos os seguintes critérios:

- **Nível fácil:** classificamos como fácil o exercício que envolve conceitos que são de conhecimento dos alunos do Ensino Básico e que possuem poucos procedimentos a serem realizados.

- **Nível intermediário:** classificamos como nível de dificuldade intermediário o exercício que além do conhecimento teórico dos conceitos ensinados no Ensino Básico, exige do estudante um bom raciocínio lógico. Além disso, pode conter condições a serem satisfeitas, exigindo que o estudante analise com cuidado sua resposta.

- **Nível difícil:** classificamos como alto nível de dificuldade ou difícil, o exercício que envolve simultaneamente vários conceitos estudados no Ensino Básico. Sendo assim, o estudante precisará relembrar propriedades, conceitos e definições, saber o momento certo de aplicá-los, além de ter um bom raciocínio lógico e conhecimento matemático.

Após a apresentação das duas soluções serão feitos alguns comentários sobre as questões e suas respectivas soluções.

Problema 1 - (OBMEP (2010) - Nível fácil) Paula iniciou um programa de ginástica no qual os dias de treino são separados por dois dias de descanso. Se o primeiro treino foi em uma segunda-feira, em qual dia da semana cairá o centésimo treino?

a) Domingo
b) Segunda-feira
c) Terça-feira
d) Quinta-feira
e) Sexta-feira

SOLUÇÃO 1- De acordo com o enunciado, o primeiro treino foi realizado em uma segunda feira. Então, vamos listar os dias dos primeiros treinos:
o 1º treino será realizado em uma segunda feira;
o 2º treino será realizado em uma quinta feira;
o 3º treino será realizado em um domingo;
o 4º treino será realizado em uma quarta feira;
o 5º treino será realizado em um sábado;
o 6º treino será realizado em uma terça feira;
o 7º treino será realizado em uma sexta feira;
o 8º treino será realizado em uma segunda feira;
o 9º treino será realizado em uma quinta feira;

Observemos que o ciclo de dias se repete depois de 7 treinos. Como queremos saber o dia do centésimo treino, fazemos a divisão de 100 por 7. Dessa forma, descobriremos quantas vezes o ciclo de dias se repetiu por inteiro, e quantos dias ainda ela treinou. Como $100 = 7 \cdot 14 + 2$, podemos concluir que Paula treinará por 14 ciclos de dias completos e fará mais dois treinos. Isto é, o centésimo treino será realizado no mesmo dia da semana que o segundo treino, que foi em uma quinta feira.

SOLUÇÃO 2 -Podemos organizar a sequência de dias da semana em que Paula realizará seus treinos em uma tabela, como mostrado abaixo:

Segunda feira	1º treino					8º treino
Terça feira					6º treino	
Quarta feira				4º treino		
Quinta feira		2º treino				
Sexta feira					7º treino	
Sábado				5º treino		
Domingo			3º treino			

Podemos observar que depois do sétimo treino a ordem dos dias da semana para os próximos treinos se repetirá. Então, devemos encontrar o número que é o resto da divisão de 100 por 7, isto é, o número que é congruente a 100 módulo 7. Temos que

$$10 \equiv 3 \mod 7 \tag{3.1}$$

e, de acordo com a Proposição 2.10, podemos escrever

$$10^2 \equiv 3^2 \mod 7. \tag{3.2}$$

Como $3^2 = 9$ e $9 \equiv 2 \mod 7$, pela Proposição 2.9, segue que

$$100 \equiv 2 \mod 7. \tag{3.3}$$

De (3.3) podemos concluir que o centésimo treino será no mesmo dia que o segundo treino, ou seja, em uma quinta feira.

Problemas que envolvem o dia da semana em que determinado evento acontece, aparecem em várias edições da Olimpíada Brasileira de Matemática das Escolas Públicas. O problema acima possui um baixo nível de dificuldade, de acordo com os critérios estabelecidos, e mostra aos estudantes uma aplicação do estudo dos restos das divisões euclidianas. Ambas as soluções são simples e utilizam conceitos que um aluno do Ensino Básico entenderia sem grandes dificuldades. A solução com congruência se torna simples se o aluno conhecer as operações e propriedades da aritmética modular. Para concluir a resolução, é necessário que o aluno analise o resto da divisão de 100 por 7, pois é o que fundamenta cada uma das soluções apresentadas.

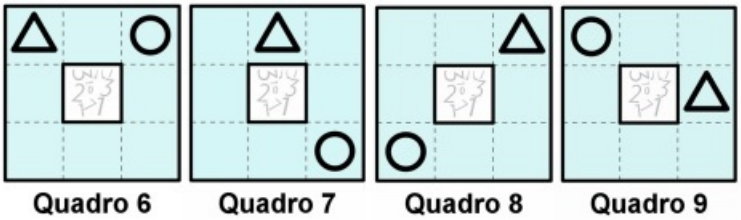
Problema 2 (OBMEP (2015) - Nível Fácil) Na sequência de quadros abaixo, uma bolinha e um triângulo caminham no sentido horário pelas casas sombreadas. De um quadro para o seguinte, o triângulo passa de uma casa para a casa vizinha, e a bolinha pula uma casa. Desenhe a bolinha e o triângulo do quadro 2015.

Figura 3.1 – Problema 4

Fonte: OBMEP (2015)

SOLUÇÃO 1 - O problema traz a imagem dos 5 primeiros quadros. Se desenharmos os quadros seguintes, teremos:

Figura 3.2 – Problema 4



Fonte: OBMEP (2015)

O quadro 9 é igual ao quadro 1. Isso significa que depois de 8 quadros o ciclo de desenhos se repete. O que precisa ser determinado é o quadro número 2015 então, vamos analisar a divisão euclidiana de 2015 por 8. Como $2015 = 8 \cdot 251 + 7$, teremos 251 ciclos completos mais 7 quadros. Logo, o quadro 2015 será igual ao quadro 7.

SOLUÇÃO 2 - Podemos perceber pela Figura 3.2 que a cada 8 quadros, a sequência de desenhos se repete. Como queremos saber o quadro 2015, temos que encontrar o resto da divisão de 2015 por 8, isto é, o número que é congruente a 2015 módulo 8. Para isso, utilizaremos a Proposição 2.10. Temos que

$$10 \equiv 2 \mod 8 \tag{3.4}$$

e, portanto

$$10^2 \equiv 2^2 \mod 8 \tag{3.5}$$

isto é,

$$100 \equiv 4 \mod 8. \tag{3.6}$$

Como

$$20 \equiv 4 \mod 8 \tag{3.7}$$

de (3.6) e (3.7) , temos que

$$100 \cdot 20 \equiv 4 \cdot 4 \mod 8 \tag{3.8}$$

ou seja,

$$2000 \equiv 16 \mod 8. \tag{3.9}$$

Como

$$16 \equiv 0 \mod 8, \tag{3.10}$$

temos que

$$2000 \equiv 0 \mod 8. \tag{3.11}$$

Além disso,

$$15 \equiv 7 \mod 8 \tag{3.12}$$

e, portanto, de (3.11) e (3.12)

$$2015 \equiv 7 \mod 8. \tag{3.13}$$

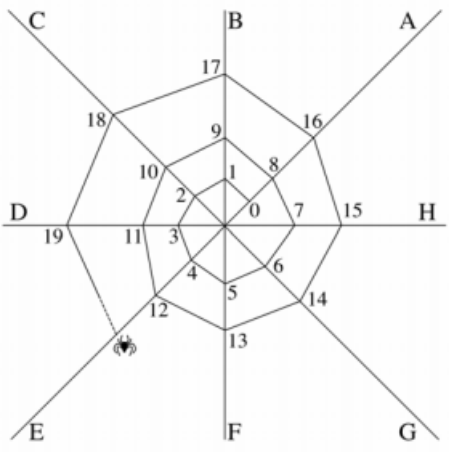
Logo, podemos concluir que o quadro 2015 será igual ao quadro 7.

Este problema fez parte da Olimpíada Brasileira de Matemática das Escolas Públicas no ano de 2015 e tem um baixo nível de dificuldade, de acordo com os critérios estabelecidos. Para

a resolução, foram utilizados os mesmos conceitos do primeiro problema. A imagem apresentada na solução 1 foi retirada da resolução apresentada no *site* da OBMEP. Ambas as soluções apresentadas para este problema são de fácil entendimento se a parte teórica for conhecida. Um professor que está apresentando aos alunos esse tipo de problema, poderia resolver o Problema 1 e deixar o Problema 2 como exercício. Possivelmente, um aluno do Ensino Básico teria preferência pela primeira solução, pois contém uma quantidade menor de cálculos a serem realizados, além do fato de que para resolver utilizando congruência modular, seria necessário conhecer bem as propriedades e proposições utilizadas. Embora os dois primeiros problemas sejam resolvidos com a mesma técnica e os mesmos conceitos, no segundo é necessário um conhecimento maior das operações com congruências já que é preciso utilizar as propriedades mais de uma vez.

Problema 3 (OBMEP (2006) - Nível fácil) A, B, C, D, E, F, G e H são os fios de apoio que uma aranha usa para construir sua teia, conforme mostra a figura. A aranha continua seu trabalho. Sobre qual fio de apoio estará o número 118?

Figura 3.3 – Problema 3



Fonte: OBMEP (2006)

SOLUÇÃO 1 - Ao todo são 8 fios de apoio. Então, para saber sobre qual fio estará o número 118, devemos fazer a divisão de 118 por 8. Essa divisão nos dirá quantas voltas completas a aranha fez e, no caso da divisão deixar resto, este representa a quantidade de fios que ela percorreu após o número inteiro de voltas. Como $118 = 8 \cdot 14 + 6$, concluímos que a aranha deu 14 voltas completas, parando novamente no fio A, e ainda realizou seu trabalho em mais 6 fios, parando portanto no fio G. Portanto, o número 118 estará sobre o fio G.

SOLUÇÃO 2 - Pela Figura 3.3, é possível observar que sobre o fio A estão os múltiplos de 8, ou seja, os números que são congruentes a zero módulo 8. Sobre o fio B, estão os números congruentes a 1 módulo 8. Sobre o fio C, estão os números congruentes a 2 módulo 8, e assim por diante, até o fio H, onde estão os números que são congruentes a 7 módulo 8. Então, para determinar o fio em que está o número 118, devemos encontrar o número que é congruente a 118 módulo 8. Utilizando a Proposição 2.10, temos que

$$10 \equiv 2 \mod 8 \tag{3.14}$$

$$10^2 \equiv 2^2 \mod 8, \tag{3.15}$$

isto é,

$$100 \equiv 4 \mod 8. \tag{3.16}$$

Além disso,

$$8 \equiv 0 \mod 8, \tag{3.17}$$

então pela Proposição 2.10 temos que

$$100 + 10 + 8 \equiv 4 + 2 + 0 \mod 8, \tag{3.18}$$

isto é,

$$118 \equiv 6 \mod 8. \tag{3.19}$$

Logo, o número 118 estará sobre o fio G.

A resolução do Problema 3 apresenta os mesmos princípios para a resolução que os dois primeiros. É preciso muita atenção por parte do aluno pois, a contagem dos fios inicia no zero. Isto é, o primeiro fio não deixa resto 1 na divisão por 8 e sim, resto zero. Este problema está disponível no banco de questões da OBMEP.

Problema 4 (ORM (2017) - Nível intermediário) Jucavo propõe o seguinte desafio: "Eu vou pensar em um número. A seguir, darei três dicas e você terá que dizer qual foi o número em que eu pensei". Você aceita o desafio? Jucavo, então, pensa em um número e fornece as seguintes dicas:

- o número que eu pensei é um múltiplo de 7;
- quando eu subtraio 17 do número que eu pensei, o resultado obtido é um múltiplo de 4;
- o número que eu pensei é um número natural entre 2000 e 2017.

Assinale a alternativa que corresponde ao número que Jucavo pensou.

a) 2005
b) 2009
c) 2002
d) 2016
e) 2003

SOLUÇÃO 1 - De acordo com a terceira condição, o número que Jucavo pensou faz parte do conjunto: 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016. A primeira condição exige que o número seja múltiplo de 7 então, eliminando do conjunto listado acima os números que não são múltiplos de 7, sobram 2002, 2009 e 2016. Agora, basta verificar qual desses três números que ao subtrair 17 é um múltiplo de 4. Temos que,
$2002-17=1985$ que não é múltiplo de 4;
$2009-17=1992$ que é múltiplo de 4, pois $1992=4\cdot 498$;
$2016-17=1999$ que não é múltiplo de 4.

Logo, o número que Jucavo pensou foi 2009.

SOLUÇÃO 2 - Seja x o número que Jucavo pensou. Dadas as três condições, buscamos um número x tal que:

$$x \equiv 0 \mod 7, \tag{3.20}$$

$$x-17 \equiv 0 \mod 4 \tag{3.21}$$

e

$$2000 < x < 2017. \tag{3.22}$$

Primeiramente, resolveremos a congruência módulo 7. Temos

$$10 \equiv 3 \mod 7 \tag{3.23}$$

Pela Proposição 2.10, temos

$$10^3 \equiv 3^3 \mod 7, \tag{3.24}$$

e como $10^3=1000$, $3^3=27$, temos que

$$1000 \equiv 27 \mod 7. \tag{3.25}$$

Como $27 \equiv 6 \mod 7$, pela Proposição 2.9 podemos escrever

$$1000 \equiv 6 \mod 7 \tag{3.26}$$

e utilizando novamente a Proposição 2.10, temos que

$$1000 \cdot 2 \equiv 6 \cdot 2 \mod 7. \tag{3.27}$$

Como $6 \cdot 2 = 12$ e $12 \equiv 5 \mod 7$, pela Propriedade 2.9, temos

$$2000 \equiv 5 \mod 7 \tag{3.28}$$

$$2000 + 2 \equiv 5 + 2 \mod 7 \tag{3.29}$$

$$2002 \equiv 7 \mod 7. \tag{3.30}$$

Da Equação (3.30), podemos concluir que $2002 \equiv 0 \mod 7$ e, portanto, $2009 \equiv 0 \mod 7$ e $2016 \equiv 0 \mod 7$. Assim sendo, os números 2002, 2009 e 2016 satisfazem a primeira e a terceira condições simultaneamente. Para satisfazer a segunda condição, queremos $x \equiv 17 \mod 4$, portanto eliminamos 2002 e 2016, uma vez que $2002 \equiv 2 \mod 4$ e $2016 \equiv 0 \mod 4$. Logo, o número x procurado é 2009, pois $2009 \equiv 17 \mod 4$.

O quarto problema fez parte da Olimpíada Regional de Matemática de Santa Catarina no ano de 2017. Possui um nível intermediário de dificuldade. Exige atenção e dedicação do aluno por conter três condições a serem satisfeitas. Ambas as soluções possuem um fácil entendimento. É claro que, os alunos do Ensino Básico que não estão habituados ao uso de congruência para resolver problemas, encontrarão certa dificuldade na segunda solução. Mas é importante salientar que a proposta deste trabalho é que o aluno conheça as técnicas de resolução de exercícios utilizando a congruência modular. A partir do momento que o aluno conhece e domina a ferramenta de congruência, a resolução dessa questão por este método se torna fácil e por muitas vezes mais rápida.

Problema 5 (OBM (2017a) - Nível intermediário) Contando-se os alunos de uma classe de 4 em 4 sobram 2, e contando-se de 5 em 5 sobra 1 . Sabendo-se que 15 alunos são meninas e que nessa classe o número de meninas é maior que o de meninos, o numero de meninos nessa classe é:

a) 7
b) 8
c) 9

d) 10

e) 11

SOLUÇÃO 1 - O problema afirma que há 15 meninas e que são a maioria comparado ao número de meninos. Com essa informação, podemos concluir que pode haver de 1 a 14 meninos e sendo assim, que a quantidade total de alunos é maior do que 15 e menor do que 30. Se contarmos a quantidade de alunos de 5 em 5 sobra um, então a quantidade total de alunos é um múltiplo de 5 somado com um, isto é , um número do tipo $5x+1$, sendo x um número natural. Podemos então afirmar que os únicos valores que satisfazem essas duas condições são 16, 21 e 26. A outra informação é que se contarmos os alunos de 4 em 4 sobram 2, então a quantidade de alunos é um múltiplo de 4 somado com dois, isto é, é um número do tipo $4y+2$, sendo y um número natural. Entre os três números listados anteriormente (16, 21 e 26), o único que satisfaz esta condição é o 26. Então, há um total de 26 alunos na classe. Agora que a quantidade total de alunos foi descoberta, vamos responder a pergunta. O problema pede para determinar a quantidade de meninos na classe. Como o total de alunos é 26 e o total de meninas é 15, então o total de meninos é 11.

SOLUÇÃO 2 - Sendo 15 o número de meninas e sendo o número de meninas maior que o de meninos, concluímos que pode haver de 1 a 14 meninos. Portanto, o total de alunos é um número compreendido entre 16 e 29. Sendo x o número total de alunos, temos que

$$x \equiv 1 \mod 5, \qquad 16 \leq x \leq 29 \tag{3.31}$$

o que nos deixa com x igual a 16, 21 ou 26. Além disso, se contarmos o número de alunos de 4 em 4 sobram 2. Então,

$$x \equiv 2 \mod 4. \tag{3.32}$$

Entre os números 16, 21 e 26 o único que satisfaz a condição da Equação (3.32) é o 26. Portanto, sendo 26 o total de alunos, o número de meninos é $26-15=11$.

Este problema fez parte da Olimpíada Brasileira de Matemática no ano de 2001. Trata-se de um problema de nível de dificuldade intermediário, segundo os critérios estabelecidos, que exige dos alunos atenção, raciocínio lógico, interpretação e domínio dos conceitos matemáticos do Ensino Básico. Para a resolução deste problema, é necessário que o aluno tenha atenção nas condições exigidas, assim como tenha um bom raciocínio lógico. O aluno pode não ter dificuldade para entender as soluções apresentadas do problema mas para ele próprio resolver a questão precisa dominar a divisão euclidiana e saber exatamente a importância do resto nessas

operações. A resolução por congruência é realizada rapidamente por um aluno que conhece a teoria. Neste exercício, a resolução por congruência além de mais simples se torna mais rápida, o que permite que o estudante tenha mais tempo para se dedicar a outras questões.

Problema 6 - (POTI (2012) - Nível difícil) Prove que p^2-1 é divisível por 24 se p é um primo maior que 3.

Vale observar que um aluno do Ensino Fundamental pode admitir a afirmação como verdadeira, se fizer o teste para alguns primos maiores do que 3. Observemos que
para $p=5$, temos $5^2-1=24$ e $24|24$;
para $p=7$, temos $7^2-1=48$ e $24|48$;
para $p=11$, temos $11^2-1=120$ e $24|120$;
para $p=13$, temos $13^2-1=168$ e $24|168$.

O fato da afirmação ser verdadeira para os números verificados não representa uma prova da afirmação. Precisamos provar que para todo número primo maior que 3 a afirmação é válida.

SOLUÇÃO 1 - Se p é primo maior que 3 podemos afirmar que p é ímpar, já que o único primo par é o número 2. Então, p é um número do tipo $2k+1$ onde k é um número inteiro e maior que 1. Sendo $p=2k+1$, teremos:
$p^2-1 \ = \ (2k+1)^2-1=4k^2+4k+1-1=4k^2+4k=4k(k+1)$.
Observação (I) - O produto $k(k+1)$ será um número par, já que é o produto entre dois números consecutivos. Ao multiplicar esse número par por 4, podemos garantir que o resultado será um múltiplo de 8. Isto é, o número $4k(k+1)=p^2-1$ é divisível por 8.
Observação (II) - Um número pode deixar resto 0, 1 ou 2 quando dividido por 3. Porém, se o número for primo, os restos na divisão por 3 serão 1 ou 2, uma vez que resto zero implica que o número é divisível por 3 e, neste caso, não seria primo. Se um número primo deixa resto 1 na divisão euclidiana por 3, podemos dizer que esse número é do tipo $3x+1$, com x um número inteiro maior que 1. Se deixa resto 2 na divisão euclidiana por 3, pode ser escrito como $3x+2$, com x um número inteiro maior do que zero. Vamos então analisar as duas opções.

Se o número p é do tipo $3x+1$, temos

$$p^2-1=(3x+1)^2-1=9x^2+6x+1-1 \tag{3.33}$$

$$p^2-1=9x^2+6x=3(3x^2+2x). \tag{3.34}$$

Se o número p é do tipo $3x+2$, temos

$$p^2-1=(3x+2)^2-1=9x^2+12x+4-1 \tag{3.35}$$

$$p^2-1=9x^2+12x+3=3(3x^2+4x+1) \tag{3.36}$$

Das equações (3.34) e (3.36), podemos concluir que p^2-1 é divisível por 3.
De acordo com as observações (I) e (II), temos que p^2-1 é divisível 8 e também é divisível por 3, portanto será divisível por 24.

SOLUÇÃO 2 - Lembrando que queremos provar que p^2-1 é divisível por 24 se p é primo maior que 3. Além disso, $24=3\cdot 8$, portanto, vamos verificar se p^2-1 é divisível por 3 e por 8 separadamente.
Primeira parte - Se p é primo maior que 3, então os restos da divisão euclidiana de p por 3 podem ser 1 ou 2, já que resto zero implicaria que p é múltiplo de 3. Então, temos que

$$p\equiv 1 \mod 3 \tag{3.37}$$

ou

$$p\equiv 2 \mod 3. \tag{3.38}$$

Se a congruência (3.37) acontece, então pela Proposição 2.10 temos que

$$p^2\equiv 1^2 \mod 3, \tag{3.39}$$

Consequentemente,

$$p^2\equiv 1 \mod 3. \tag{3.40}$$

Se a congruência (3.38) acontece, então pela Proposição 2.10 temos que

$$p^2\equiv 2^2 \mod 3. \tag{3.41}$$

E, como $4\equiv 1 \mod 3$, pela Proposição 2.9 temos que

$$p^2\equiv 1 \mod 3. \tag{3.42}$$

De (3.40) e (3.42) temos que se p é primo maior que 3, então

$$p^2\equiv 1 \mod 3. \tag{3.43}$$

Utilizando o item (ii) da Proposição 2.10 temos que

$$p^2-1\equiv 1-1 \mod 3 \tag{3.44}$$

Ou seja,

$$p^2 - 1 \equiv 0 \mod 3. \tag{3.45}$$

Segunda parte: Como p é primo e maior que 3, podemos garantir que p é ímpar e, portanto, p^2 também será ímpar. Assim sendo, na divisão euclidiana de p por 8 sempre haverá resto ímpar, já que todos os múltiplo de 8 são pares. Portanto, os restos da divisão de p por 8 podem ser 1, 3, 5 ou 7, isto é, podemos ter p congruente a 1, 3, 5 ou 7 módulo 8. Vamos analisar cada caso.
Caso I: se $p \equiv 1 \mod 8$, pelo item (v) da Proposição 2.10 temos que

$$p^2 \equiv 1^2 \mod 8, \tag{3.46}$$

e consequentemente,

$$p^2 \equiv 1 \mod 8. \tag{3.47}$$

Caso II: se $p \equiv 3 \mod 8$, pela Proposição 2.10 temos que

$$p^2 \equiv 3^2 \mod 8 \tag{3.48}$$

e, como $9 \equiv 1 \mod 8$, pela Proposição 2.9 temos

$$p^2 \equiv 1 \mod 8. \tag{3.49}$$

Caso III: se $p \equiv 5 \mod 8$, pela Proposição 2.10 temos que

$$p^2 \equiv 5^2 \mod 8 \tag{3.50}$$

e, como $25 \equiv 1 \mod 8$, pela Proposição 2.9 temos

$$p^2 \equiv 1 \mod 8. \tag{3.51}$$

Caso IV: se $p \equiv 7 \mod 8$, pela Proposição 2.10 temos que

$$p^2 \equiv 7^2 \mod 8 \tag{3.52}$$

e, como $49 \equiv 1 \mod 8$, pela Proposição 2.9 temos

$$p^2 \equiv 1 \mod 8. \tag{3.53}$$

Nos quatro casos analisados, chegamos a conclusão de que

$$p^2 \equiv 1 \mod 8. \tag{3.54}$$

Utilizando o item (ii) da Proposição 2.10, temos que

$$p^2 - 1 \equiv 1 - 1 \mod 8. \tag{3.55}$$

Ou seja,

$$p^2 - 1 \equiv 0 \mod 8 \tag{3.56}$$

De (3.45) e (3.56) podemos concluir que $p^2 - 1$ é divisível por 3 e também por 8. Logo, segue que $p^2 - 1$ será divisível por $3 \cdot 8 = 24$.

Este problema é muito interessante, pois trata de conceitos diversificados, que alunos do Ensino Fundamental já conhecem, embora não dominem. Foi retirado do POTI (Polos Olímpicos de Treinamento Intensivo). O POTI é programa de treinamento para alunos de oitavo e nono anos interessados em participar de competições matemáticas. O programa é financiado pelo IMPA, oferecido em 79 polos espalhados pelo Brasil. O problema tem um nível de dificuldade alto, de acordo com os critérios estabelecidos. Exige conhecimentos prévios sobre divisibilidade, números primos e divisão euclidiana. Além disso, o problema pede uma demonstração, técnica que alunos do Ensino Básico não estão habituados a trabalhar. Ambas as soluções apresentadas possuem conceitos que devem ser conhecidos dos alunos para que compreendam o passo a passo do que está sendo realizado. Na primeira solução, é necessário que o aluno saiba porque um número ímpar pode ser escrito como $2k + 1$ e porque a escolha foi em analisar a divisibilidade por 3 e por 8. Além disso, é preciso ficar claro ao aluno que o fato de um número ser divisível por 3 e por 8, só implica em que é divisível por 24 por que 3 e 8 são primos entre si. Na segunda solução, embora pareça mais prática, por se tratar de pequenos cálculos, é preciso que o aluno saiba os conceitos citados acima e também domine a resolução de exercícios através de congruências. Para que um aluno do Ensino Básico resolva sozinho uma questão como essa, seria necessário revisar alguns conceitos da divisibilidade e até mesmo de máximo divisor comum.

Problema 7 (OBMEP (2017b) - Nível difícil) Somando 1 a um certo número natural, obtemos um múltiplo de 11. Subtraindo 1 desse mesmo número, obtemos um múltiplo de 8. Qual é o resto da divisão do quadrado desse número por 88?

SOLUÇÃO 1 - Essa solução é apresentada por meio de um vídeo disponível no site da OBMEP. Quem participa do vídeo é a medalhista da olimpíada, Alessandra Portela.

Seja x o número em questão. Somando 1 a esse número, obtemos um múltiplo de 11, então, podemos escrever

$$x+1 = 11k, \tag{3.57}$$

para algum k inteiro.
Se subtrairmos 1 do número x, obtemos um múltiplo de 8. Então,

$$x-1 = 8n, \tag{3.58}$$

para algum n inteiro.
Multiplicando as Equações (3.57) e (3.58), temos

$$(x+1)(x-1) = 11k \cdot 8n \tag{3.59}$$

$$x^2 - 1 = 88kn \tag{3.60}$$

$$x^2 = 88kn + 1. \tag{3.61}$$

Como k e n são números inteiros, o produto kn também será e, portanto, pela Equação (3.61) temos que o resto da divisão de x^2 por 88 será 1.

SOLUÇÃO 2 - Seja x o número em questão. De acordo com o enunciado, temos que

$$x+1 \equiv 0 \mod 11 \tag{3.62}$$

e

$$x-1 \equiv 0 \mod 8. \tag{3.63}$$

Usando a Proposição 2.9 na Equação (3.62) temos que

$$x+1-1 \equiv 0-1 \mod 11 \tag{3.64}$$

portanto,

$$x \equiv -1 \mod 11. \tag{3.65}$$

Da Proposição 2.10 temos

$$x^2 \equiv (-1)^2 \mod 11, \tag{3.66}$$

isto é,

$$x^2 \equiv 1 \mod 11 \tag{3.67}$$

e, na Equação (3.63), utilizando novamente a Proposição 2.10, temos que

$$x-1+1 \equiv 0+1 \mod 8 \tag{3.68}$$

e, portanto,

$$x \equiv 1 \mod 8. \tag{3.69}$$

Também

$$x^2 \equiv 1^2 \mod 8, \tag{3.70}$$

ou seja,

$$x^2 \equiv 1 \mod 8. \tag{3.71}$$

Das Equações (3.67) e (3.71) e da Proposição (2.12) temos que

$$x^2 \equiv 1 \mod 88. \tag{3.72}$$

Portanto, o resto da divisão de x^2 por 88 será 1.

O Problema 7 fez parte da OBMEP em 2017, na prova de nível 3, destinada ao Ensino Médio. Tem um nível de dificuldade alto, de acordo com os critérios estabelecidos, pois envolve conhecimentos sobre divisão euclidiana e técnicas de resolução que os estudantes desse nível escolar não estão habituados a utilizar. Na primeira solução é necessário que o aluno conheça a técnica de multiplicar equações membro a membro, tenha a percepção de que isso é necessário e conheça a divisão euclidiana, ou ao menos compreenda a importância do resto nessa divisão. Já na segunda solução, além de dominar as propriedades de congruência modular, é necessário que conheça a Proposição (2.12) para chegar a conclusão do problema.

Problema 8 (OBMEP (2017a) - Nível difícil) Quantos divisores de 88^{10} deixam resto 4 quando divididos por 6?

SOLUÇÃO 1 - Primeiramente, vamos escrever o número 88^{10} em sua decomposição em números primos:

$$88^{10} = (8 \cdot 11)^{10} = (2^3 \cdot 11)^{10} = 2^{30} \cdot 11^{10}. \tag{3.73}$$

Observemos que se um número inteiro x deixa resto 4 quando dividido por 6, então $x+2$ será um múltiplo de 6 e, consequentemente, será um número par. Como $x+2$ é um número par, x também será par pois é o resultado da subtração entre dois números pares. Se x deixa resto 4 na divisão euclidiana por 6, podemos afirmar que existe um número inteiro q tal que

$$x = 6q + 4. \tag{3.74}$$

Como $6 = 3 \cdot 2$, em (3.74) temos

$$x = 3 \cdot 2q + (3+1) = 3(2q+1) + 1 \tag{3.75}$$

e o número x deixa resto 1 quando dividido por 3.
Buscamos então, os divisores de 88^{10} que são pares e que deixam resto 1 quando divididos por 3 pois, se satisfizer estas condições, significa que o número x deixará resto 4 quando dividido por 6. Para dar continuidade, mais alguns pontos devem ser destacados:

(i) Os divisores primos de 88^{10} são 2 e 11. Ambos deixam resto 2 na divisão por 3.

(ii) O produto entre uma quantidade par de divisores primos de 88^{10} sempre deixará resto 1 na divisão por 3. Por exemplo, se efetuarmos a multiplicação de $2 \cdot 11 \cdot 11 \cdot 11$ obtemos como resultado o número 2662 e, na divisão euclidiana, temos que $2662 = 3 \cdot 887 + 1$.

(iii) O produto entre uma quantidade ímpar de divisores primos sempre deixará resto 2 na divisão por 3. Por exemplo, se efetuarmos a multiplicação de $2 \cdot 2 \cdot 11$ obteremos como resultado o número 44 e, na divisão euclidiana, temos que $44 = 3 \cdot 14 + 2$.

Assim, buscamos os números pares com uma quantidade par de fatores primos em sua decomposição. Esses números são do tipo $2^m \cdot 11^n$, com $m \geq 1$ e $m+n$ par.

Vamos separar a contagem em duas partes:

- Para m ímpar, devemos ter n ímpar. Nesse caso há 15 possibilidades de valores para m : 1, 3, 5, 7, 9, . . . , 27, 29 e 5 possibilidades para n :1, 3, 5, 7 e 9. Então para satisfazer essa condição, temos $15 \cdot 5 = 75$ possibilidades.

- Para m par, devemos ter n par. Há 15 possibilidades para m: 2, 4, 6, 8, . . . , 30 e 6 possibilidades para n : 2, 4, 6, 8, 10. Então se m e n são ambos pares, temos ao todo $15 \cdot 6 = 90$ números que satisfazem a condição.

Portanto, ao todo teremos $75 + 90 = 165$ possibilidades, isto é, 165 divisores de 88^{10} que deixam resto 4 quando dividido por 6.

SOLUÇÃO 2 - Decompondo 88^{10} em fatores primos, temos $88^{10} = (2^3 \cdot 11)^{10} = 2^{30} \cdot 11^{10}$. Sendo assim, os divisores positivos de 88^{10} são da forma $2^n \cdot 11^m$ com $0 \leq n \leq 30$ e $0 \leq m \leq 10$. Como queremos conhecer os divisores que deixam resto 4 quanto divididos por 6, isto é, os números que são congruentes a 4 módulo 6, vamos analisar a congruência das potências de 2 e de 11 módulo 6. Utilizaremos as Proposições (2.9) e (2.10).

$$2 \equiv 2 \mod 6, \tag{3.76}$$

$$2^2 \equiv 4 \mod 6, \tag{3.77}$$

$$(2^2)^k \equiv 4^k \mod 6. \tag{3.78}$$

Precisamos agora, analisar a congruência das potências de 4 módulo 6. Observemos que

$$4 \equiv 4 \mod 6, \tag{3.79}$$

$$4^2 \equiv 16 \mod 6, \tag{3.80}$$

e, como $16 \equiv 4 \mod 6$, segue que

$$4^2 \equiv 4 \mod 6, \tag{3.81}$$

$$4^2 \cdot 4 \equiv 4 \cdot 4 \mod 6, \tag{3.82}$$

isto é,

$$4^3 \equiv 4 \mod 6. \tag{3.83}$$

As congruências acima nos levam a acreditar que toda potência de 4 será congruente a 4 módulo 6. Vamos provar esse fato. Queremos, portanto, provar que $4^k \equiv 4 \mod 6$ para todo k natural, $k > 1$. Observemos que se isso for verdade, teremos que

$$6|4^k - 4 = 4^{k-1}(4-1) = 4^{k-1} \cdot 3. \tag{3.84}$$

A divisibilidade (3.84) de fato é verdadeira, pois 4^{k-1} é um número par e, um número par multiplicado por três sempre será divisível por 6. Portanto, podemos afirmar que $4^k \equiv 4 \mod 6$ para todo k natural e maior que 1.

Voltamos agora a congruência (3.78). Como mostramos que $4^k \equiv 4 \mod 6$, temos que

$$2^{2k} \equiv 4 \mod 6, \tag{3.85}$$

e,

$$2^{2k} \cdot 2 \equiv 4 \cdot 2 \mod 6. \tag{3.86}$$

Como $8 \equiv 2 \mod 6$, temos que

$$2^{2k+1} \equiv 2 \mod 6. \tag{3.87}$$

Das congruências (3.85) e (3.87) podemos concluir que se o expoente do número 2 for par, esse número será congruente a 4 módulo 6. Se o expoente do 2 for ímpar, esse número será congruente a 2 módulo 6.

Pela definição de congruência, podemos escrever que $2 \equiv -4 \mod 6$ pois $2 = 6 \cdot 1 - 4$, então, podemos concluir que se n for par, teremos $2^n \equiv 4 \mod 6$ e se n for ímpar, teremos $2^n \equiv -4 \mod 6$.

Agora, analisando a congruência módulo 6 das potências de 11, temos que

$$11 \equiv 5 \mod 6 \tag{3.88}$$

e

$$5 \equiv -1 \mod 6, \tag{3.89}$$

então

$$11 \equiv -1 \mod 6. \tag{3.90}$$

Portanto, pela Proposição 2.10, temos

$$11^m \equiv (-1)^m \mod 6. \tag{3.91}$$

Podemos observar que, se m for par teremos $11^m \equiv 1 \mod 6$ e se m for ímpar, teremos $11^m \equiv (-1) \mod 6$.

Queremos conhecer os números positivos que são congruentes a $2^n \cdot 11^m$ módulo 6. Sendo assim, devemos ter ambos os expoentes, m e n, pares ou, ambos ímpares. Observemos que no caso de um expoente ser par e, outro ímpar teremos $m+n$ ímpar, o que no momento não nos interessa, conforme análise em (iii).

Vamos agora, fazer a análise em dois casos separados.

- **Caso 1 :** n e m são ambos pares e, portanto, $2^n \cdot 11^m \equiv 4 \mod 6$ se n for diferente de zero, pois para deixar resto 4 na divisão por 6, é necessário que o número seja par. Então, temos para n quinze valores possíveis (2, 4, 6, . . . , 28, 30), e para m seis valores (0, 2, 4, 6, 8, 10). Portanto, se m e n forem ambos pares, teremos $15 \cdot 6 = 90$ divisores de 88^{10} que deixam resto 4 na divisão por 6.

- **Caso 2:** n e m são ambos ímpares e, portanto, $2^n \cdot 11^m \equiv 4 \mod 6$. Sendo assim, para n ímpar temos 15 possibilidades (1, 3, 5, . . . , 27, 29) e para m ímpar temos 5 opções (1, 3, 5, 7, 9). Portanto, se n e m forem ímpares teremos $15 \cdot 5 = 75$ divisores de 88^{10} que deixam resto 4 na divisão por 6.

Dessa forma, analisando os dois casos, podemos concluir, que para $2^n \cdot 11^m \equiv 4 \mod 6$, isto é, para que os divisores de 88^{10} deixem resto 4 na divisão por 6 teremos $90 + 75 = 165$ possibilidades de números.

O Problema 8 tem um alto nível de dificuldade, segundo os critérios estabelecidos. Envolve conhecimentos sobre divisibilidade, restos das divisões, além de pedir como resposta a quantidade de divisores de um número muito grande, não sendo possível listá-los de forma simples. Para a solução é necessário que o aluno saiba decompor um número em fatores primos, que domine técnicas de resolução para, por exemplo, reescrever a Equação (3.74) e chegar a

conclusão de que os números procurados deixam resto 1 na divisão por 3. Pode ser ainda mais difícil o aluno chegar a conclusão de que o produto de uma quantidade par de divisores primos deixará resto 1 na divisão por 3 e o produto entre uma quantidade ímpar de primos deixará resto 2 na divisão por 3. A solução 2, aparentemente, é mais simples, pois o aluno precisa conhecer congruência modular, a decomposição de um número em fatores primos e conseguir realizar a contagem dos divisores.

O problema abaixo se diferencia dos demais por ter a opção de ser resolvido através de um sistema de congruências. Sendo assim, para a segunda solução utilizaremos o Teorema Chinês dos Restos.

PROBLEMA 9 - (Hefez (2014)[p. 262] - Nível intermediário) Quando um macaco sobe uma escada de dois em dois degraus, sobra um degrau; quando sobe de três em três degraus, sobram dois degraus e quando sobe se cinco em cinco degraus, sobram três degraus. Quantos degraus possui a escada, sabendo que o número de degraus está entre 150 e 200?

SOLUÇÃO 1 - Vamos fazer a análise de cada informação fornecida pelo problema. Se subindo as escadas de dois em dois degraus sobra um, então podemos afirmar que a quantidade de degraus é um número ímpar.

Subindo as escadas de 5 em 5 degraus, sobram 3. Então, a quantidade de degraus é um múltiplo de 5 somado com 3. Podemos escrever esse número como $5x+3$, sendo x um número inteiro. Além disso, a quantidade de degraus está entre 150 e 200. Logo, os números que satisfazem essas duas condições e são ímpares, são : 153, 163, 173, 183 e 193.

Agora, vamos analisar a última informação. Quando o macaco sobe as escadas de três em três degraus, sobram dois. Então a quantidade de degraus é um número que é múltiplo de 3 somado com 2. Podemos escrever esse número como $3k+2$, para k inteiro. Vamos descobrir qual dos 5 números listados acima é um múltiplo de 3 somado com 2:

$153 = 3 \cdot 51 + 0$

$163 = 3 \cdot 54 + 1$

$173 = 3 \cdot 57 + 2$

$183 = 3 \cdot 61 + 0$

$193 = 3 \cdot 64 + 1$

Logo, podemos concluir que a quantidade de degraus era 173.

SOLUÇÃO 2 - Sendo x a quantidade de degraus na escada, buscamos o número x que na divisão por 2 deixa resto 1, na divisão por 3 deixa resto 2 e na divisão por 5 deixa resto 3. Logo, devemos resolver o sistema :

$$x \equiv 1 \mod 2 \tag{3.92}$$

$$x \equiv 2 \mod 3 \tag{3.93}$$

$$x \equiv 3 \mod 5 \tag{3.94}$$

Com $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, $m_1 = 2$, $m_2 = 3$, $m_3 = 5$, como descrito no Teorema 2.4. Assim, $M = m_1 m_2 m_3 = 2 \cdot 3 \cdot 5 = 30$. Além disso,

$$M_1 = \frac{M}{m_1} = \frac{30}{2} = 15, \quad M_2 = \frac{M}{m_2} = \frac{30}{3} = 10 \text{ e } M_3 = \frac{M}{m_3} = \frac{30}{5} = 6. \tag{3.95}$$

Para determinar y_1, y_2 e y_3, temos que encontrar as soluções de cada uma das congruências abaixo:

$$15y_1 \equiv 1 \mod 2, \tag{3.96}$$

$$10y_2 \equiv 1 \mod 3 \tag{3.97}$$

e

$$6y_3 \equiv 1 \mod 5. \tag{3.98}$$

- Em (3.96), se $y_1 = 1$, temos que $15 \cdot 1 \equiv 1 \mod 2$ pois, 2 divide $15 - 1 = 14$.
- Em (3.97), se $y_2 = 1$, temos que $10 \cdot 1 \equiv 1 \mod 3$ pois, 3 divide $10 - 1 = 9$.
- Em (3.98), se $y_3 = 1$, temos que $6 \cdot 1 \equiv 1 \mod 5$ pois, 5 divide $6 - 1 = 5$.

Logo, temos $y_1 = 1$, $y_2 = 1$, e $y_3 = 1$. De acordo com o Teorema 2.4 uma solução do sistema é dado por

$$x_0 = M_1 a_1 y_1 + M_2 a_2 y_2 + M_3 a_3 y_3. \tag{3.99}$$

Sendo assim, temos

$$x_0 = 15 \cdot 1 \cdot 1 + 10 \cdot 2 \cdot 1 + 6 \cdot 3 \cdot 1 = 15 + 20 + 18 = 53. \tag{3.100}$$

Como a solução geral do sistema é dada por

$$x(t) = x_0 + Mt, \tag{3.101}$$

temos

$$x(t) = 53 + 30t \qquad t \in \mathbb{Z}. \tag{3.102}$$

Como o número de degraus está entre 150 e 200, atribuiremos valores para t, até encontrar o valor procurado.
Para $t = 1$, temos $x = 53 + 30 \cdot 1 = 83$.
Para $t = 2$, temos $x = 53 + 30 \cdot 2 = 113$.
Para $t = 3$, temos $x = 53 + 30 \cdot 3 = 143$.
Para $t = 4$, temos $x = 53 + 30 \cdot 4 = 173$.
Para $t = 5$, temos $x = 53 + 30 \cdot 5 = 203$.

Logo, o número de degraus da escada é 173.

Este problema apresenta um nível intermediário de dificuldade pois, embora os conceitos utilizados na primeira solução sejam de conhecimento de um aluno do Ensino Básico, o fato de precisar escrever o número de degraus através de equações pode não ser uma tarefa simples. Com a teoria de congruências e o Teorema Chinês dos Restos a segunda solução pode ser facilmente obtida. A maior dificuldade nessa resolução pode ser encontrar os valores de y_1, y_2 e y_3, o que foi feito através de uma análise (tentativa erro) das Equações (3.96), (3.97) e (3.98).

4 CRIPTOGRAFIA E O MÉTODO RSA

Neste capítulo trataremos de uma aplicação prática da congruência modular, a criptografia. Nos dias atuais, onde muita informação é trocada pela internet a criptografia está presente garantindo a segurança do envio e recebimento de informações sigilosas. Informações enviadas através de compras realizadas *on-line* e *internet banking*, por exemplo, utilizam a criptografia para garantir que dados pessoais sejam acessados apenas por pessoas autorizadas. Podemos encontrar a criptografia em alguns serviços de *e-mail* e até mesmo em um dos aplicativos mais utilizados no mundo, o WhatsApp.

Figura 4.1 – Imagem de uma conversa do WhatsApp

Fonte: o autor.

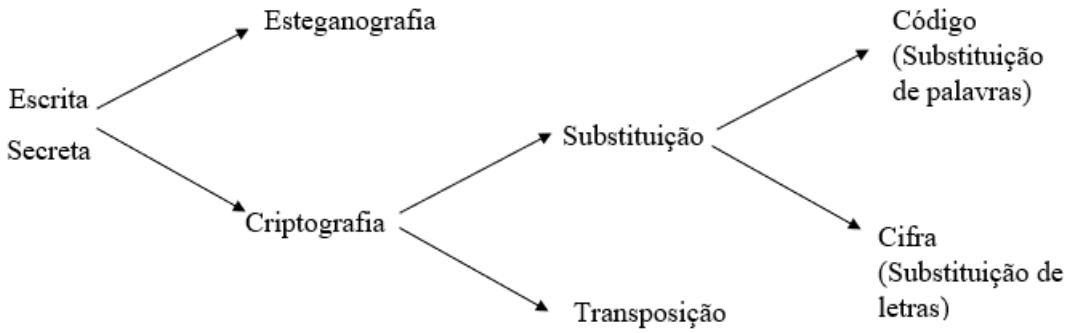
De acordo com a referência WhatsApp Inc (), o aplicativo é utilizado por mais de 1 bilhão de pessoas e é protegido por criptografia. A criptografia do WhatsApp permite que apenas emissor e destinatário tenham acesso a mensagens e arquivos compartilhados.

A palavra criptografia tem origem grega onde, *kryptós* significa "escondido"e *gráphein* significa "escrita". Portanto, criptografia pode ser traduzida como escrita escondida ou escrita oculta. De acordo com Coutinho (2005), a criptografia é o estudo dos métodos necessários para codificar uma mensagem de modo que apenas seu destinatário legítimo consiga interpretá-la. A codificação de uma mensagem também pode ser chamada de encriptação. Para cifrar uma mensagem, é necessário um algoritmo que é especificado por meio de uma chave de codificação. Aplicando o algoritmo a uma mensagem, obtemos o texto codificado. Para decodificar o texto, o receptor deve conhecer a chave e o algoritmo utilizados e os aplica no texto cifrado convertendo-o para o texto original. Conforme os estudos sobre criptografia foram evoluindo,

houve necessidade de que pesquisadores desenvolvessem um método para decodificar as mensagens. Assim, surgiu a criptoanálise que é o estudo da decodificação, ou decriptação, de mensagens criptografadas.

A necessidade de enviar mensagens secretas de forma que somente uma pessoa ou grupo tivesse acesso deu início a utilização da esteganografia. A esteganografia consiste em esconder a mensagem, sem alterar sua escrita ou seu significado. Para enviar mensagens secretas, os antigos chineses as escreviam em seda fina, que era amassada até formar uma bola bem pequena, coberta com cera e então engolida pelo mensageiro (Singh (2003)). Há ainda relatos de que no século XVI um cientista desenvolveu uma tinta que era utilizada para escrever a mensagem na casca de um ovo cozido, a mesma só ficava visível ao descascar o ovo. Também foram utilizados outros métodos como o uso de tintas invisíveis que apareciam ao aquecer o papel ou raspar o cabelo do mensageiro, escrever a mensagem em sua cabeça e esperar o cabelo crescer para enviar a mensagem. O fato é que se o mensageiro fosse descoberto, a mensagem secreta poderia facilmente ser decifrada pelo interceptador. É o caso da utilização de micropontos durante a Segunda Guerra Mundial. Agentes alemães reduziam fotograficamente uma página de texto até transformá-la em um ponto que era oculto sobre o ponto final de uma mensagem. O primeiro microponto foi descoberto em 1941 pelo *Federal Bureau of Investigation* (FBI). Assim, para tornar o envio de mensagens mais seguro houve a necessidade de estudos de métodos mais elaborados para o compartilhamento de informações. A Figura 4.2 foi baseada no livro de Singh (2003, p.47), O Livro dos Códigos, e apresenta um esquema das ramificações da escrita secreta.

Figura 4.2 – Ramificações da escrita secreta



Fonte: O autor.

A criptografia pode ser separada em dois ramos (Figueiredo e Costa (2010)): transposição e substituição. A criptografia de transposição se resume em alterar a ordem das letras na mensagem, isto é, trata-se de uma permutação entre as letras. Por exemplo, a palavra SOL pode ser escrita em 5 anagramas distintos: SLO, LOS, LSO, OLS, OSL. Podemos observar que quanto

maior for a mensagem, mais difícil se torna para um interceptador decifrar essa mensagem. Uma das formas de transposição mais conhecida é o *Scytale*. O *Scytale* espartano, também conhecido como "Bastão de Licurgo"ou Cítala (Figura 4.3) foi utilizado por volta do século V a.C. quando Esparta e Atenas estavam em guerra. A técnica foi descrita por Plutarco em 90 d.C.

Figura 4.3 – Bastão de Licurgo

Fonte: Wikipedia (a)

Para enviar a mensagem, uma tira de couro era enrolada em um bastão e nesta tira a mensagem era escrita no sentido do comprimento. A tira era retirada, enrolada com as letras para dentro e um mensageiro entregava ao destinatário da mensagem. Este por sua vez, possuía um bastão de igual espessura ao utilizado pelo emissor da mensagem. Assim, ao enrolar a tira no bastão, a mensagem ficava visível (Fiarresga (2010)).

A criptografia de substituição consiste em substituir uma palavra por um símbolo ou uma letra da mensagem original por outra seguindo um certo padrão. Segundo Figueiredo e Costa (2010), o início da criptografia foi por volta de 2000 a.C quando egípcios e mesopotâmicos utilizaram hieróglifos na escrita de mensagens. Um dos métodos mais conhecidos da criptografia de substituição é a substituição monoalfabética. Foi utilizada pela primeira vez por Júlio Cesar, na Roma Antiga, para enviar mensagens secretas aos seus generais. O padrão utilizado por Júlio César foi trocar cada letra do alfabeto por outra que estivesse três letras a frente. Podemos dizer que a chave de codificação utilizada por Júlio César é 3, pois utilizava sempre três letras a frente da original. Veja o exemplo na Tabela 4.1 abaixo:

Tabela 4.1 – Cifra de César

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
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

Dessa forma, por exemplo, ao encriptar a mensagem UNIVERSIDADE DO ESTADO DE SANTA CATARINA obtemos: XQLYHUVLGDGH GR HVWDGR GH VDQWD FDWDULQD.

Uma das principais vantagens da Cifra de César é que tanto a codificação quanto a decodificação podem ser feitas de forma fácil. E, uma das principais desvantagens é que existem apenas 26 possibilidades de padrão para substituição, isto é, 26 chaves de codificação. A cifra de César foi muito utilizada em um período onde poucos sabiam ler e ainda não existia a criptoanálise (Figueiredo e Costa (2010)). O surgimento da criptoanálise, por volta dos anos 800 e 1200, se deu através da análise de frequências. Essa análise busca fornecer informações sobre a frequência relativa de vezes que cada letra aparece em diversos tipos de textos. Na língua portuguesa, por exemplo, segundo Fiarresga (2010), a letra que mais aparece nos textos é a letra A, seguida das letras E, O, S, R e I, respectivamente. Sabendo destas informações, ao ter um texto encriptado, basta analisar o símbolo que aparece em maior frequência e substituir pelo A, o de segunda maior frequência substituir pelo E e assim sucessivamente. Para aqueles símbolos que possuem frequência parecida, é feita a análise do sentido das palavras. Dessa forma, a decodificação de uma mensagem se torna muito mais rápida. Além desses métodos existiram vários outros, como por exemplo, a substituição polialfabética inventada por Leon Battista Alberti por volta de 1465 e a invenção da cifra de Vigenère, por volta de 1580, buscando enganar a análise de frequências. Segundo Figueiredo e Costa (2010) esse método passou a ser utilizado 200 anos depois de sua invenção e, no ano de 1854, foi quebrado por Charles Babbage.

Em 1918, o engenheiro alemão Arthur Scherbius patenteou a primeira máquina de cifras chamada de Enigma. Anos depois, após aperfeiçoamentos a máquina (Figura 4.4) foi utilizada durante a segunda guerra mundial pelo exército alemão. A cifra começou a ser quebrada pelo polonês Marian Rejewski e o trabalho foi concluído por uma equipe liderada por Alan Turing e Gordon Welchman.

Figura 4.4 – Máquina Enigma

Fonte: Wikipedia (b)

A criptografia se desenvolveu em três grandes fases (Figueiredo e Costa (2010)): artesanal, mecânica e digital. A fase artesanal trata do início dos estudos e aparições da criptografia. No inicio da Idade Moderna começa a fase mecânica, com destaques para as invenções do telégrafo, do rádio e da máquina Enigma. A fase digital inicia com o surgimento do computador.

Durante as fases artesanal e mecânica a criptografia utilizava chaves privadas de codificação. O que significa que tanto emissor quanto receptor deveriam ter conhecimento sobre essa chave. Além disso, qualquer pessoa que descobrisse essa chave poderia quebrar o sigilo da mensagem. Somente em 1976 pesquisadores idealizaram um sistema de chaves públicas, onde mesmo tendo acesso a chave de codificação, a decodificação da mensagem não é realizada facilmente. Para maior compreensão da fase digital da criptografia, veremos uma breve explicação sobre chaves públicas e privadas.

4.1 CRIPTOGRAFIA DE CHAVE PRIVADA

Também conhecida como criptografia simétrica, é o tipo de criptografia em que a chave de codificação e decodificação é a mesma. Dessa forma, tanto o emissor da mensagem quanto o receptor devem possuir a chave. Esse tipo de criptografia não é considerada segura pois, assim que uma terceira pessoa descobre a chave de encriptação, esta terá total acesso a mensagem secreta. Além disso, emissor e receptor necessitam de um meio seguro para trocar informações sobre a chave de encriptação. Durante as três fases da criptografia foram utilizadas chaves privadas. Com o avanço da computação, surgiram métodos criptográficos cada vez mais difíceis de serem quebrados, uma vez que computadores podem realizar algoritmos complexos em tempo reduzido. Porém, o avanço no ramo da criptoanálise também ocorreu de forma acelerada. Apesar da codificação e decodificação acontecerem de forma mais rápida com o apoio da computação, o problema ainda era o fato da chave para isso ser privada. Ainda era necessário uma forma segura de emissor e receptor previamente combinarem uma chave. Em 1976 uma dupla de pesquisadores tiveram uma ideia para resolver essa situação.

4.2 CRIPTOGRAFIA DE CHAVE PÚBLICA

Também conhecida como criptografia assimétrica, consiste de um método que utiliza dois pares de chaves. Cada par consiste em uma chave pública e uma privada que estão relacionadas entre si. O emissor da mensagem possui um dos pares de chave e o receptor da mensagem o outro par. Para enviar uma mensagem, o emissor utiliza a chave pública do receptor e, dessa forma, apenas o receptor poderá decriptar a mensagem, uma vez que só ele possui a chave privada relacionada. Por exemplo, se Ana quer enviar uma mensagem secreta a Bia, Ana busca

a chave pública de Bia e com esta, aplica o algoritmo de encriptação. Bia recebe a mensagem encriptada e utilizando sua chave privada consegue decriptar a mensagem. A ideia de criptografia assimétrica é a mesma de uma função de mão única. Uma função de mão única é aquela fácil de fazer, mais difícil de desfazer (Singh (2003)). No ano de 1976 a dupla Whitfield Diffie e Martin Hellman publicou um artigo entitulado *"New Directions in Cryptography"* onde expuseram a ideia de criar um sistema de criptografia assimétrica, embora não tivessem conseguido implantar. O primeiro método de criptografia assimétrica foi implementado em 1977 por Ronald Rivest, Adi Shamir e Leonard Adleman, pesquisadores do *Massachusetts Institute of Technology* (MIT), baseados na ideia de Diffie e Hellman. Rivest e Shamir são cientistas da computação e Adleman é matemático. O sistema ficou conhecido como RSA, em homenagem ao trio de pesquisadores. O funcionamento do RSA baseia-se na teoria dos números, mais especificamente na congruência modular e no estudo de números primos. A criptografia assimétrica permite que, além do envio e recebimento de informações sejam realizados de forma segura, o receptor tenha a certeza de que foi realmente determinada pessoa quem enviou a mensagem. Além do RSA outros métodos são utilizados como o Diffie-Hellman, o DSA, ElGamal e o algoritmo de curvas elípticas.

De acordo com Rousseau e Saint-Aubin (2015), o método RSA é utilizado para transmitir dados como informações de cartões de crédito ou dados bancários. No caso de mensagens muito longas o algoritmo requer cálculos extremamente longos e complexos, mesmo que sejam realizados por computadores. Sendo assim, se uma mensagem não necessita de segurança por muito tempo, pode ser criptografada através de outro método. Entre outros sistemas de criptografia utilizados para o envio de e-mails, por exemplo, estão o DES (*Data Encryption Standard*, ou Padrão de Encriptação de Dados) e o AES (*Advanced Encryption Standard*, ou padrão de Encriptação avançado). Estes dois sistemas de criptografia utilizam a chave privada, o que significa que emissor e receptor devem possuir a chave de encriptação. Para garantir maior velocidade e segurança, a troca de informação sobre a chave é feita através do algoritmo RSA.

Devido a sua base matemática e a importância de sua aplicabilidade, escolhemos o método RSA para explicar o funcionamento e apresentar exemplos. Este método utiliza a teoria de congruências modulares e as propriedades de números primos. Assim sendo, além do conteúdo exposto no primeiro capítulo deste trabalho, precisaremos de mais algumas proposições e demonstrações que serão anunciadas a seguir.

4.3 O MÉTODO RSA

O método desenvolvido por Rivest, Shamir e Adleman é utilizado em operações via *internet*, como compras *on-line*, envio de *e-mails* e a garantia da assinatura digital. Basicamente o método consiste na escolha de dois números primos p e q e o cálculo do produto n entre eles. A segurança do método está em escolher p e q tendo muitos dígitos pois, para decodificar a mensagem, é necessário fatorar o número n. Atualmente há programas de computador que encontram números primos com muitos dígitos, porém, não há programa que fatore o número n em um período curto de tempo se o número for extremamente grande. É importante ressaltar que a base matemática envolvida na criptografia é aprendida no Ensino Básico. Atualmente está presente em praticamente tudo o que fazemos na internet. Além da fundamentação teórica, apresentamos exemplos de aplicação do método na encriptação e decriptação de mensagens. As proposições e demonstrações desta seção foram baseados em Rousseau e Saint-Aubin (2015).

Proposição 4.1. *Considere a,b,c,d,x,y números inteiros e n natural, com $n > 1$. Segue que se $a \equiv c \mod n$ e $b \equiv d \mod n$ então $ax+by \equiv cx+dy \mod n$.*

Demonstração. Se $a \equiv c \mod n$ então $n|c-a$. Assim, existe x inteiro tal que

$$n|x(c-a). \tag{4.1}$$

Se $b \equiv d \mod n$ então $n|b-d$. Assim, existe y inteiro tal que

$$n|y(b-d). \tag{4.2}$$

Das equações (4.1) e (4.2) segue que

$$n|x(c-a)+y(b-d) \;=\; cx-ax+by-dy \;=\; (cx+dy)-(ax+by). \tag{4.3}$$

Logo, temos que $ax+by \equiv cx+dy \mod n$. □

Proposição 4.2. *Sejam a,b,c,m números inteiros, com $m > 1$ e $(c,m) = 1$. Temos que $ac \equiv bc \mod m$ se, e somente se, $a \equiv b \mod m$.*

Demonstração. Se $ac \equiv bc \mod m$, então

$$m|bc-ac = c(a-b). \tag{4.4}$$

Como $(c,m) = 1$, pela Equação (4.4) e Proposição 2.2, segue que $m|a-b$. Logo,

$$a \equiv b \mod m. \tag{4.5}$$

Para a recíproca, se $a \equiv b \mod m$ então $m|b-a$. Logo, existe um inteiro x tal que

$$b-a = mx. \tag{4.6}$$

Multiplicando a Equação (4.6) por um inteiro c, obtemos

$$bc-ac = mxc. \tag{4.7}$$

Como c e x são ambos números inteiros, o produto xc também é, portanto, $m|ac-bc$. Isto é

$$ac \equiv bc \mod m. \tag{4.8}$$

□

Lema 4.1. *Sejam a e b números inteiros e positivos. Suponhamos que existam inteiros k e n tais que $a = bk+n$. Então $(a,b) = (b,n)$.*

Demonstração. Suponha que $(a,b) = d_1$ e $(b,n) = d_2$.
Como $(a,b) = d_1$ segue que $d_1|a$ e $d_1|b$. Então, existem s e t inteiros tais que

$$a = d_1 s, \tag{4.9}$$

e

$$b = d_1 t. \tag{4.10}$$

Substituindo (4.9) e (4.10) na equação $a = bk+n$, temos que

$$d_1 s = d_1 tk + n \tag{4.11}$$

que pode ser escrita como

$$d_1 s - d_1 tk = d_1(s-tk) = n. \tag{4.12}$$

Logo, $d_1|n$.
Observemos que d_1 é um divisor comum de n e de b (pois $(a,b) = d_1$). Como d_2 é o maior divisor comum de n e b, segue que

$$d_1 \leq d_2. \tag{4.13}$$

Como $d_2 = (b,n)$, temos que $d_2|b$ e $d_2|n$. Logo, existem x e y inteiros tais que

$$b = d_2 x \tag{4.14}$$

e

$$n = d_2 y. \tag{4.15}$$

Como

$$a = bk + n, \tag{4.16}$$

substituindo (4.14) e (4.15) na Equação (4.16), temos

$$a = d_2xk + d_2y = d_2(xk + y). \tag{4.17}$$

Logo, $d_2|a$, isto é, d_2 é um divisor comum de a e b. Como d_1 é o maior divisor comum de a e b, segue que

$$d_2 \leq d_1. \tag{4.18}$$

As desigualdades (4.13) e (4.18) não podem acontecer simultaneamente, logo, podemos concluir que $d_2 = d_1$. Portanto, se $a = bk + n$ então $(a,b) = (b,n)$. □

O algoritmo abaixo garante a existência do máximo divisor comum entre dois ou mais números, além de determinar quem é o máximo divisor comum. Foi elaborado por Euclides e publicado pela primeira vez em seu livro Os Elementos.

Proposição 4.3 (Algoritmo de Euclides)**.** *Sejam a e b dois inteiros positivos com $a \geq b$ e seja $\{r_i\}$ a sequência dos inteiros construídos da seguinte maneira. Divida a por b; chamamos q_1 o quociente dessa divisão e r_1 seu resto, de forma que*

$$a = bq_1 + r_1, \qquad 0 \leq r_1 < b. \tag{4.19}$$

Dessa maneira, dividimos b por r_1, levando-nos a

$$b = r_1q_2 + r_2, \qquad 0 \leq r_2 < r_1. \tag{4.20}$$

$$r_1 = r_2q_3 + r_3, \qquad 0 \leq r_3 < r_2. \tag{4.21}$$

$$r_2 = r_3q_4 + r_4, \qquad 0 \leq r_4 < r_3. \tag{4.22}$$

Iteramos de forma que

$$r_{i-1} = r_iq_{i+1} + r_{i+1} \qquad 0 \leq r_{i+1} < r_i \tag{4.23}$$

A sequência $\{r_i\}$ é estritamente decrescente. Portanto, deve haver um inteiro n tal que $r_{n+1} = 0$. Segue que $r_n = (a,b)$.

Demonstração. Devemos mostrar que $(a,b) = r_n$. Realizando a sequência de divisões como descrito acima, temos

$$a = bq_1 + r_1, \qquad 0 \leq r_1 < b \tag{4.24}$$

$$b = r_1q_2 + r_2, \qquad 0 \leq r_2 < r_1 \tag{4.25}$$

$$r_1 = r_2q_3 + r_3, \qquad 0 \leq r_3 < r_2 \tag{4.26}$$

$$r_2 = r_3 q_4 + r_4, \qquad 0 \leq r_4 < r_3 \tag{4.27}$$

$$\vdots \tag{4.28}$$

$$r_{n-2} = r_{n-1} q_n + r_n, \qquad 0 \leq r_n < r_{n-1} \tag{4.29}$$

$$r_{n-1} = r_n q_{n+1} + 0. \tag{4.30}$$

Observemos que na Equação (4.30), temos resto zero. Podemos garantir a existência desse resto zero pelo Princípio da Boa Ordem. Portanto $r_n | r_{n-1}$. Sendo assim, temos que $(r_{n-1}, r_n) = r_n$. Pelo Lema 4.1 , temos que

$$r_n = (r_n, r_{n-1}) = (r_{n-1}, r_{n-2}) = \ldots = (b, r_1) = (a, b). \tag{4.31}$$

Logo, $(a,b) = r_n$. □

Proposição 4.4. *Considere a, b, c números naturais. Temos que $(ma, mb) = m(a,b)$.*

Demonstração. Considere o conjunto

$$S = \{ax + by;\ x, y \in \mathbb{Z},\ \ ax + by \geq 0\}. \tag{4.32}$$

Na demonstração da Proposição 2.5 vimos que $c = (a,b)$ é o menor elemento, diferente de zero, do conjunto S, ou seja,

$$c = min\{ax + by; x, y \in \mathbb{Z},\ \ ax + by > 0\}. \tag{4.33}$$

Assim, para $d = (ma, mb)$ teremos que

$$d = min\{max + mby; x, y \in \mathbb{Z},\ \ max + mby > 0\}, \tag{4.34}$$

$$d = m \cdot min\{ax + by; x, y \in \mathbb{Z},\ \ ax + by > 0\ \} \tag{4.35}$$

isto é,

$$d = m \cdot c. \tag{4.36}$$

Portanto, $(ma, mb) = m(a,b)$. □

Lema 4.2. *Sejam a, b, e k números inteiros. Temos que $(k, ab) = 1$ se, e somente se, $(k,a) = (k,b) = 1$.*

Demonstração. Se $(k, ab) = 1$, então pela Proposição 2.6 existem m e n inteiros tais que

$$1 = mk + nab. \tag{4.37}$$

Como n, a e b são inteiros, temos que na e nb também são inteiros. Seja $na = p$ e $nb = p'$. Então, substituindo $na = p$ e $nb = p'$ na Equação (4.37), temos

$$1 = mk + pb \tag{4.38}$$

e

$$1 = mk + p'a. \tag{4.39}$$

Pela Proposição 2.6 segue que $(k,a) = (k,b) = 1$.
Para a recíproca, temos que se $(k,a) = (k,b) = 1$, então pela Proposição 2.6 existem m, n, p e q inteiros tais que

$$1 = mk + na, \tag{4.40}$$

e

$$1 = pk + bq. \tag{4.41}$$

Multiplicando as Equações (4.10) e (4.14) membro a membro, temos

$$1 = (mk + na)(pk + bq) = mpk^2 + mkbq + napk + nabq. \tag{4.42}$$

Colocando em evidência os termos semelhantes da Equação (4.42) temos

$$1 = (mpk + bqm + nap)k + (nq)ab. \tag{4.43}$$

Como os números a, b, m, p, n, q são todos inteiros, segue que $(mpk + bqm + nap)$ e nq também são, e portanto, pela Proposição 2.6, concluímos que $(k, ab) = 1$.

□

Corolário 4.1. *Sejam a e n dois inteiros com $a < n$. Se $(a,n) = 1$, então existe um único $x \in \{1,2,3,\cdots,n-1\}$ tal que $ax \equiv 1 \mod n$.*

Demonstração. Devemos mostrar a existência do número x e também sua unicidade.

(i) Existência:
Se $(a,n) = 1$, pela Proposição 2.6 existem x e y inteiros tais que

$$1 = ax + ny. \tag{4.44}$$

Subtraindo ax em ambos os membros da Equação (4.44) temos que

$$1 - ax = ny, \tag{4.45}$$

o que significa que $n|1 - ax$, isto é, $ax \equiv 1 \mod n$. Caso x não faça parte do conjunto $\{1,2,\cdots,n-1\}$, podemos alterar o múltiplo de n a fim de que x esteja nesse intervalo.

(ii) Unicidade:

Suponha que exista $x_0 \in \{1,2,\cdots,n-1\}$ tal que

$$ax_0 \equiv 1 \mod n. \tag{4.46}$$

Como temos também que $ax \equiv 1 \mod n$, pelo item (ii) da Proposição 2.10, temos que

$$ax - ax_0 \equiv 1-1 \mod n, \tag{4.47}$$

isto é,

$$a(x-x_0) \equiv 0 \mod n. \tag{4.48}$$

Logo, $n|a(x-x_0)$. Temos $(a,n)=1$ então, pela Proposição 2.2, segue que $n|x-x_0$. Como $x,x_0 \in 1,2,\cdots,n-1$, então $(x-x_0) \in -(n-1),-(n-2),\cdots,-1,0,1,2,\cdots,n-1$. Como neste conjunto não há múltiplos de n (já que os positivos são todos menores que n, e o restante são os simétricos), com exceção do zero, segue que $x-x_0=0$ e, portanto, $x=x_0$.

□

Definição 4.1. *A função phi (lê-se fi) de Euler, denotada por $\varphi(n)$ determina a quantidade de números naturais menores que n e relativamente primos com n. Define-se $\varphi(1)=1$.*

Definição 4.2. *Um sistema completo de resíduos módulo m é todo conjunto de números inteiros cujos restos pela divisão por m são os números $0,1,2,...,m-1$, sem repetições e numa ordem qualquer.*

Exemplo 4.1. *O conjunto dos números 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 forma um sistema completo de resíduos módulo 10.*

Definição 4.3. *Um sistema reduzido de resíduos módulo m é um conjunto de números inteiros $r_1,r_2,\cdots,r_s$ tais que:*

a) $(r_i,m)=1$ *para todo* $i=1,2,3,\cdots,s$;
b) $r_i \not\equiv r_j \mod m$ *se* $i \neq j$;
c) Para cada n inteiro tal que $(n,m)=1$, *existe i tal que* $n \equiv r_i \mod m$.

Exemplo 4.2. *O conjunto 1, 3, 7, 9 forma um sistema reduzido de resíduos módulo 10 pois, cada elemento deste conjunto atende a cada uma das três exigências da Definição 4.3.*

Proposição 4.5. *Seja $r_1,r_2,\cdots,r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m e seja a um número inteiro tal que $(a,m)=1$. Então, $ar_1,ar_2,\cdots,ar_{\varphi(m)}$ é um sistema reduzido de resíduos módulo m.*

Demonstração. Devemos mostrar que $ar_1, ar_2, \cdots, ar_{\varphi(m)}$ satisfaz os três itens da Definição 4.3. Seja $a_1, a_2, \cdots, a_m$ um sistema completo de resíduos módulo m do qual foi retirado o sistema reduzido $r_1, r_2, \cdots, r_{\varphi(m)}$. Como $(a,m) = 1$, pelo lema 4.2, temos que $(a_i, m) = 1$ se, e somente se, $(aa_i, m) = 1$. Então, como $(r_i, m) = 1$ e $(a,m) = 1$, segue que $(ar_i, m) = 1$. Logo, $ar_1, ar_2, \cdots, ar_{\varphi(m)}$ satisfaz o primeiro item da Definição 4.3.
Como $r_1, r_2, \cdots, r_{\varphi(m)}$ é um sistema reduzido de resíduos módulo m, segue que $r_i \not\equiv r_j \mod m$ se $i \neq j$. Logo, $ar_i \not\equiv ar_j \mod m$ se $i \neq j$, satisfazendo o item (b) da Definição 4.3.
Também, para cada n inteiro tal que $(n,m) = 1$, existe i tal que $n \equiv r_i \mod m$. Como $(a,m) = 1$, pelo Lema 4.2 segue que para an inteiro tal que $(an,m) = 1$, existe i tal que $an \equiv ar_i \mod m$, satisfazendo o item (c) da Definição 4.3.

□

Proposição 4.6. *Sejam a e b dois números inteiros tais que* $(a,b) = 1$. *Tem-se que* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Demonstração. Para $a = 1$ ou $b = 1$ o resultado é trivial. Então suponha $a > 1$ e $b > 1$. Considere a tabela abaixo formada pelos números naturais de 1 até $a \cdot b$:

Tabela 4.2 – Números de 1 a $a \cdot b$

1	2	$\cdots$	k	$\cdots$	a
$1+a$	$2+a$	$\cdots$	$k+a$	$\cdots$	$2a$
$1+2a$	$2+2a$	$\cdots$	$k+2a$	$\cdots$	$3a$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$1+(b-1)a$	$2+(b-1)a$	$\cdots$	$k+(b-1)a$	$\cdots$	ab

Queremos determinar a quantidade de números inteiros desta tabela que são relativamente primos com $a \cdot b$. Pelo Lema 4.2, basta que encontremos os números que são relativamente primos com a e b simultaneamente.

Para encontrar os números que são primos com a, podemos observar o primeiro elemento de cada coluna. Se o primeiro elemento de cada coluna for relativamente primo com a, então todos os elementos da coluna serão. Assim, como são a colunas, a quantidade se colunas onde podemos encontrar números relativamente primos com a é $\varphi(a)$. Para encontrar os números relativamente primos com b, observemos que cada coluna da tabela acima forma um sistema completo de resíduos módulo b, portanto, em cada coluna temos $\varphi(b)$ elementos que são primos com b. Sendo assim a quantidade de elementos que é relativamente primo com a e b simultaneamente é $\varphi(a) \cdot \varphi)(b)$. Logo, $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

□

Proposição 4.7. *Seja n um número inteiro. Se* $n \geq 2$*, então* $\varphi(n) = n-1$ *se, e somente se, n é primo.*

Demonstração. Se $\varphi(n) = n-1$ então há $n-1$ valores inteiros que são menores e relativamente primos com n. Isto é, os números $1, 2, 3, \cdots, n-1$ são todos relativamente primos com n o que significa que n é primo.
Para a recíproca, temos que $\varphi(n)$ é um número entre 1 e $n-1$, já que há $n-1$ números menores que n. Seja a um desses valores então, temos que

$$1 \leq a \leq n-1. \tag{4.49}$$

Como n é primo, para qualquer a neste intervalo, teremos $(a,n) = 1$. Logo, todos os $n-1$ números desse intervalo são coprimos com n. Portanto, $\varphi(n) = n-1$. □

Teorema 4.1 (Teorema de Euler)**.** *Se* $a < m$ *é relativamente primo com m, então,* $a^{\varphi(m)} \equiv 1 \mod m$.

Demonstração. Seja $r_1,\ r_2,\ \cdots, r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m. Pela Proposição 4.5 segue que $ar_1,\ ar_2,\ \cdots, ar_{\varphi(m)}$ também é um sistema reduzido de resíduos módulo m. Sendo assim, temos que

$$ar_1 \cdot ar_2 \cdot \cdots\ ar_{\varphi(m)} \equiv r_1 \cdot r_2 \cdot \cdots\ r_{\varphi(m)} \mod m. \tag{4.50}$$

No primeiro membro há uma quantidade $\varphi(m)$ de fatores a. Então, podemos escrever a congruência (4.50) como

$$a^{\varphi(m)} \cdot r_1 \cdot r_2\ \cdots\ r_{\varphi(m)} \equiv r_1 \cdot r_2 \cdot \cdots\ r_{\varphi(m)} \mod m. \tag{4.51}$$

Como $r_1,\ r_2,\ \cdots, r_{\varphi(m)}$ é um sistema reduzido de resíduos módulo m, temos que
$(r_1 \cdot r_2\ \cdots\ r_{\varphi(m)}, m) = 1$. Então, pela proposição 4.2 segue que

$$a^{\varphi(m)} \equiv 1 \mod m. \tag{4.52}$$

□

4.4 COMO FUNCIONA O MÉTODO RSA

Para explicar o funcionamento do método RSA, faremos uma apresentação dividida em passos. Em seguida apresentaremos alguns exemplos detalhando cada passo. Digamos que um emissor queira enviar uma mensagem "M", criptografada, para um certo receptor. Cada usuário possui um par de chaves matematicamente relacionados onde uma é pública e outra é privada. O emissor da mensagem busca a chave pública definida pelo receptor e com esta faz a codificação

da mensagem M. A decodificação só pode ser realizada com a chave privada que está de posse do receptor. Observemos o passo a passo abaixo:

Primeiro passo:
O receptor escolhe dois números primos grandes p e q.

Segundo passo:
O receptor calcula o produto $n = p \cdot q$. O valor n será a chave pública. Observemos que determinar n não é problema mesmo tendo p e q relativamente grandes. Porém, quanto maior for o número n, mais difícil é fatorar esse número para determinar quem são p e q.

Terceiro passo:
O receptor calcula $\varphi(n)$.

Quarto passo: determinar a chave de encriptação.
O receptor escolhe e, tal que $(e, \varphi(n)) = 1$ e $1 < e < \varphi(n)$. Esse número e será a chave de encriptação. O número e é público, e será utilizado pelo emissor da mensagem para poder codificar a mensagem.

Quinto passo: determinar a chave de decriptação.
O receptor calcula um número d tal que $d \cdot e \equiv 1 \mod \varphi(n)$. Esse número d será a chave privada, conhecida apenas pelo receptor. Também podemos chamar d de chave de decriptação.

Sexto passo: encriptar a mensagem.
Para enviar a mensagem M codificada, sendo $M \in \{1, 2, \cdots, n-1\}$, o emissor calcula o número C tal que $M^e \equiv C \mod n$. Como n e e são chaves públicas, o cálculo pode ser realizado. Observemos que a dificuldade de calcular C aumenta conforme n e e também aumentam.

Sétimo passo: decriptando a mensagem. Ao receber a mensagem encriptada "C", para decriptá-la basta calcular o número M (que será a mensagem original), tal que $M \equiv C^d \mod n$. Como d é a chave privada do receptor, os cálculos serão possíveis e, apenas o próprio receptor tem acesso. Vamos ver um exemplo simples com números pequenos.

Exemplo 4.3. *Suponha que Ana quer enviar a mensagem $M = 19$ para Bia. Bia, que é a receptora da mensagem escolhe os primos $p = 7$ e $q = 13$ e calcula o produto $n = 7 \cdot 13 = 91$. Em seguida, Bia calcula $\varphi(91) = 6 \cdot 12 = 72$ e escolhe $e = 17$. A escolha de e é válida uma vez que $(e, \varphi(91)) = (17, 91) = 1$ e $1 < e < \varphi(n)$. Para enviar a mensagem M para Bia, Ana deve*

realizar a encriptação utilizando e que é a chave pública de Bia. Assim, Ana deve calcular C de tal forma que $C \equiv M^e \mod 91$. *Isto é, buscamos o resto da divisão de* 19^{17} *por* 91. *O valor C será a mensagem encriptada por Ana. Observemos que o cálculo de C é possível, uma vez que é conhecido de Ana os valores M, n e a chave pública e. Utilizando as propriedades de congruências modulares, enunciadas e demonstradas nas Proposições 2.9 e 2.10, temos:*

$$19 \equiv 19 \mod 91, \tag{4.53}$$

$$19^2 \equiv 19^2 = 88 \mod 91, \tag{4.54}$$

$$19^2 \cdot 19^2 \equiv 88 \cdot 88 \mod 91. \tag{4.55}$$

Como $88^2 = 7744$ *e* $7744 = 85 \cdot 91 + 9$, *segue que* $19^4 \equiv 9 \mod 91$, *portanto*

$$(19^4)^4 \equiv 9^4 \mod 91. \tag{4.56}$$

Como $9^4 = 6561$ *e* $6561 = 91 \cdot 72 + 9$, *segue que* $19^{16} \equiv 9 \mod 91$. *Assim,*

$$19^{16} \cdot 19 \equiv 9 \cdot 19 \mod 91. \tag{4.57}$$

Também, $9 \cdot 91 = 171$ *e* $171 = 91 \cdot 91 + 80$ *então, segue que*

$$19^{17} \equiv 80 \mod 91. \tag{4.58}$$

Logo, $C = 80$ *é a mensagem codificada.*

Ana envia C para Bia, que por sua vez, a fim de decodificar a mensagem, calcula $M \equiv C^d \mod n$. *Para calcular d, devemos ter* $d \cdot e \equiv 1 \mod \varphi(n)$. *Como o valor* $\varphi(n)$ *é calculado por Bia, assim como o valor da chave e, resta encontrar d.*

$$d \cdot 17 \equiv 1 \mod 72. \tag{4.59}$$

Usando o algoritmo de Euclides, temos $72 = 17 \cdot 4 + 4$, *o que significa que*

$$72 - 17 \cdot 4 = 4. \tag{4.60}$$

E, $17 = 4 \cdot 4 + 1$ *o que significa que*

$$17 - 4 \cdot 4 = 1. \tag{4.61}$$

Para determinar d, vamos substituir (4.60) na Equação (4.61)

$$1 = 17 - 4(72 - 17 \cdot 4) = 17 - 4 \cdot 72 + 16 \cdot 16 = 17 \cdot 17 - 4 \cdot 72. \tag{4.62}$$

Ou seja,

$$1 = 17 \cdot 17 - 4 \cdot 72. \tag{4.63}$$

O segundo termo do lado direito é divisível por 72, então $17 \cdot 17 \equiv 1 \mod 72$. *Logo,* $d = 17$.

Uma vez que Bia tem o valor d, para decodificar a mensagem $C = 80$ *precisa calcular o resto da divisão de* 80^{17} *por* 91. *Utilizando novamente as Proposições 2.9 e 2.10, tem-se*

$$80 \equiv 80 \mod 91, \tag{4.64}$$

como $80^2 = 6400$ *e* $6400 = 91 \cdot 70 + 30$ *temos que*

$$80^2 \equiv 30 \mod 91, \tag{4.65}$$

$$(80^2)^3 \equiv 30^3 \mod 91. \tag{4.66}$$

Como $30^3 = 27000$ *e* $27000 = 296 \cdot 91 + 64$ *temos que*

$$80^6 \equiv 64 \mod 91, \tag{4.67}$$

$$(80^6)^2 \equiv 64^2 \mod 91. \tag{4.68}$$

Como $64^2 = 4096$ *e* $4096 = 91 \cdot 45 + 1$, *segue que*

$$80^{12} \equiv 1 \mod 91. \tag{4.69}$$

Logo,

$$80^{12} \cdot 80^2 \cdot 80^2 \cdot 80 \equiv 1 \cdot 30 \cdot 30 \cdot 80 \mod 91. \tag{4.70}$$

Como $1 \cdot 30 \cdot 30 \cdot 80 = 72000$ *e* $72000 = 91 \cdot 791 + 19$, *temos que*

$$80^{17} \equiv 19 \mod 91. \tag{4.71}$$

Logo, $M = 19$ *é a mensagem original enviada por Ana.*

Usamos o exemplo de duas pessoas, Ana e Bia, para facilitar o entendimento do procedimento. Todos estes cálculos são realizados por computadores. Para determinar p e q a máquina receptora da mensagem seleciona dois números com aproximadamente o mesmo tamanho (mais de cem dígitos) e os testa para saber se são primos. O teste é realizado através de um algoritmo para teste de primalidade. Caso um deles ou ambos não sejam primos, a máquina repete o procedimento até encontrar dois que sejam. Após encontrar p e q, ela determina $n = p \cdot q$ e calcula $\varphi(n)$. A máquina então seleciona um número aleatório e entre 1 e n e verifica se é relativamente

primo com $\varphi(n)$. Caso não seja, o algoritmo repete o procedimento até encontrar um que seja. Em seguida este mesmo computador calcula d, que será a chave de decriptação. Para enviar uma mensagem criptografada para o dono dessa máquina, o computador comandado pelo emissor da mensagem busca nos arquivos públicos da máquina receptora a sua chave pública para então poder fazer a encriptação da mensagem. Como o valor d é calculado pela máquina receptora e, apenas essa máquina conhece p e q para poder calcular $\varphi(n)$, apenas esta conseguirá decriptar a mensagem.

Para enviar a mensagem criptografada, o algoritmo de encriptação quebra a mensagem em blocos de tamanho menores que n e faz a encriptação de cada bloco. Se a mensagem em questão for um texto, é necessário realizar um procedimento chamado de pré codificação que consiste em transformar a mensagem de texto em caracteres numéricos. Isso pode ser feito com uma tabela de substituição, como na cifra de César. Para realizar a decriptação, o algoritmo é aplicado para cada bloco da mensagem que foi encriptada e, em seguida, a mensagem numérica é convertida para texto. Assim, é necessário que emissor e receptor conheçam o parâmetro utilizado para converter o texto em números.
Vamos agora demonstrar que o algoritmo utilizado para decriptar a mensagem é válido.

Proposição 4.8. *Encriptação e decriptação RSA são inversas uma da outra. Se encriptamos uma mensagem M como C, onde $M^e \equiv C \mod n$, a decriptação sempre levará a mensagem original M. A decriptação é feita através do cálculo de $C^d \equiv M \mod n$.*

Demonstração. Primeiramente, vamos listar todos os valores obtidos até chegar na decriptação da mensagem. Temos:

- p e q primos e $n = p \cdot q$;
- $\varphi(n) = (p-1)(q-1)$;
- $e \in \{1, 2, \cdots, n-1\}$;
- $(e, \varphi(n)) = 1$;
- $e \cdot d \equiv 1 \mod \varphi(n)$;
- $M^e \equiv C \mod n$.

Queremos mostrar que $C^d \equiv M \mod n$.
Se $M^e \equiv C \mod n$, pela Proposição 2.10 temos que

$$(M^e)^d \equiv C^d \mod n, \tag{4.72}$$

isto é,

$$M^{ed} \equiv C^d \mod n. \tag{4.73}$$

Como $n = p \cdot q$, temos que p divide n . Então, pelo item (i) da Proposição 2.12 temos que

$$M^{ed} \equiv C^d \mod p. \tag{4.74}$$

Como $ed \equiv 1 \mod \varphi(n)$, então $\varphi(n)$ divide $(ed-1)$, o que significa que existe um número inteiro k tal que

$$ed - 1 = k \cdot \varphi(n) = k(p-1)(q-1). \tag{4.75}$$

Logo, temos que

$$ed = k(p-1)(q-1) + 1. \tag{4.76}$$

Substituindo a Equação (4.76) em M^{ed}, obtemos a expressão

$$M^{ed} = M^{k(p-1)(q-1)+1} = (M^{p-1})^{k(q-1)} \cdot M. \tag{4.77}$$

Substituindo 4.77 na Equação (4.74), obtemos

$$C^d \equiv (M^{p-1})^{k(q-1)} \cdot M \mod p. \tag{4.78}$$

Temos duas situações para analisar: $(M,p) = 1$ e $(M,p) \neq 1$.
Se $(M,p) = 1$, pelo Teorema 4.1 temos que $M^{\varphi(p)} \equiv 1 \mod p$. Como p é primo temos que $\varphi(p) = p-1$, portanto

$$M^{p-1} \equiv 1 \mod p. \tag{4.79}$$

Então, podemos reescrever a congruência (4.78) como

$$C^d \equiv 1^{k(q-1)} \cdot M \mod p. \tag{4.80}$$

E, portanto,

$$C^d \equiv M \mod p. \tag{4.81}$$

Por outro lado, se $(M,p) \neq 1$, como p é primo temos que p divide M, isto é, $M \equiv 0 \mod p$.
Pela Proposição 2.10 segue que $M^{ed} \equiv 0 \mod p$. Como da Equação (4.74), temos que $M^{ed} \equiv C^d \mod p$, pela Proposição 2.9 segue que $C^d \equiv 0 \mod p$, e portanto,

$$M \equiv C^d \mod p. \tag{4.82}$$

Das Congruências (4.81) e (4.82), concluímos que $M \equiv C^d \mod p$.
Com cálculos análogos, podemos concluir que $M \equiv C^d \mod q$. Como p e q são ambos primos, temos que $[p,q] = n = p \cdot q$. Então, pelo item (ii) da Proposição 2.12 segue que

$$C^d \equiv M \mod n. \tag{4.83}$$

□

No Exemplo 4.3, escolhemos números primos pequenos e uma mensagem numérica para mostrar o funcionamento do algoritmo. Em Rousseau e Saint-Aubin (2015)[p,234] é possível ver um exemplo de aplicação do RSA para criptografar o número de um cartão de crédito utilizado para realizar uma compra *on-line*. Os primos utilizados nesse exemplo contém 25 e 26 dígitos e o número n contém 51 dígitos.

Agora, faremos a codificação de um texto. Como já foi explicado, faremos inicialmente a pré-codificação da mensagem substituindo cada letra do alfabeto por um número de dois dígitos colocados em ordem crescente. São escolhidos números de dois dígitos para evitar dúvidas na decodificação. Além disso, cada bloco a ser criptografado deve ter tamanho menor que n e nenhum bloco pode iniciar com 0. Serão apresentados dois exemplos e para ambos utilizaremos a Tabela 4.3 de conversão de caracteres. O espaço entre as palavras será substituído pelo número 99.

Tabela 4.3 – Tabela para conversão de caracteres

Letra do alfabeto	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Codificação correspondente	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
Letra do alfabeto	T	U	V	W	X	Y	Z	.	,	:	Á	Í	É	Ó	Õ	Ã	Ç	Ê	
Codificação correspondente	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	

Exemplo 4.4. *Realizar a codificação e decodificação da palavra JOINVILLE através do método RSA.*

Primeiramente, devemos realizar a pré codificação:

Tabela 4.4 – Pré codificação - Exemplo 4.4

Letra do alfabeto latino	J	O	I	N	V	I	L	L	E
Codificação numérica correspondente	20	25	19	24	32	19	22	22	15

Agora, vamos estabelecer os parâmetros.

- **Primeiro passo -**Determinar p e q: Seja $p = 17$ e $q = 13$.
- **Segundo passo -** Calcular n: $n = 13 \cdot 17 = 221$.

- **Terceiro passo -** Calcular $\varphi(n)$: $\varphi(n) = (17-1)(13-1) = 192$.

- **Quarto passo -** Determinar a chave de encriptação: a chave de encriptação e será 91 pois, $(91, 192) = 1$.

- **Quinto passo -** Determinar a chave de decriptação: precisamos determinar d, tal que $d \cdot 91 \equiv 1 \mod 192$. Isto é, determinar um número d tal que 192 divide $91d - 1$, o que significa existe um número inteiro k tal que $91d - 1 = 192k$. Ou seja,

$$91d - 192k = 1. \tag{4.84}$$

Utilizando o algoritmo de Euclides, temos que $192 = 91 \cdot 2 + 10$, isto é

$$192 - 91 \cdot 2 = 10. \tag{4.85}$$

Também, $91 = 10 \cdot 9 + 1$, isto é,

$$91 - 9 \cdot 10 = 1. \tag{4.86}$$

Substituindo (4.85) na Equação (4.86), temos:

$$1 = 91 - 9(192 - 91 \cdot 2) \tag{4.87}$$

$$1 = 91 - 9 \cdot 192 + 18 \cdot 91 = 19 \cdot 91 - 9 \cdot 192. \tag{4.88}$$

Ou seja,

$$1 = 19 \cdot 91 - 9 \cdot 192. \tag{4.89}$$

Como o segundo termo do lado direito é divisível por 192, temos que $19 \cdot 91 \equiv 1 \mod 192$. Portanto, $d = 19$ é a chave de decriptação.

- **Sexto passo -** Encriptar a mensagem.
Precisamos codificar a mensagem numérica 2025192432192222 15. Para isso vamos quebrar a mensagem em blocos de valor menor que $n = 221$:

Tabela 4.5 – Separação de blocos: Codificação - Exemplo 4.4

Valor do bloco	202	51	92	43	219	22	22	15
Bloco correspondente	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8

Agora, faremos a codificação de cada bloco separadamente, calculando $M_i^e \equiv C_i \mod n$. Observemos que os blocos podem possuir tamanhos diferentes. A única restrição é que sejam todos menores que n. Utilizaremos as Proposições 2.9 e 2.10.

Para $M_1 = 202$, temos

$$202 \equiv 202 \mod 221, \tag{4.90}$$

$$202^3 \equiv 202^3 = 8.242.408 \mod 221. \tag{4.91}$$

Como $8.242.408 = 3.7295 \cdot 221 + 213$, temos que $202^3 \equiv 213 \mod 221$.
Assim, $(202^3)^2 \equiv 213^2 \mod 221$ e como $213^2 = 45.369 = 221 \cdot 205 + 64$, segue que

$$202^6 \equiv 64 \mod 221, \tag{4.92}$$

$$(202^6)^3 \equiv 64^3 \mod 221. \tag{4.93}$$

Como $64^3 = 262.144$ e $262.144 = 221 \cdot 1.186 + 38$, segue que

$$202^{18} \equiv 38 \mod 221, \tag{4.94}$$

$$(202^{18})^5 \equiv 38^5 \mod 221. \tag{4.95}$$

Como $38^5 = 79.235.168$ e $79.235.168 = 221 \cdot 358.530 + 38$, segue que

$$202^{90} \equiv 38 \mod 221. \tag{4.96}$$

Logo, $202^{90} \cdot 202 \equiv 38 \cdot 202 \mod 221$. Como $38 \cdot 202 = 7.676$ e $7.676 = 221 \cdot 34 + 162$, segue que

$$202^{91} \equiv 162 \mod 221. \tag{4.97}$$

Portanto, a encriptação do bloco M_1 é $C_1 = 162$.

Para a encriptação dos blocos M_2 a M_8, podemos realiza o mesmo procedimento. Utilizaremos o *software* Maxima para a realização dos cálculos. O algoritmo utilizado está no Apêndice B.

Para $M_2 = 51$, $51^{91} \equiv 51 \mod 221$. Logo, $C_2 = 51$.
Para $M_3 = 92$, $92^{91} \equiv 14 \mod 221$. Logo, $C_3 = 14$.
Para $M_4 = 43$, $43^{91} \equiv 134 \mod 221$. Logo, $C_4 = 134$.
Para $M_5 = 219$, $219^{91} \equiv 145 \mod 221$. Logo, $C_5 = 145$.
Para $M_6 = 22$, $22^{91} \equiv 113 \mod 221$. Logo, $C_6 = 113$.
Para $M_7 = 22$, $22^{91} \equiv 113 \mod 221$. Logo, $C_7 = 113$.
Para $M_8 = 15$, $15^{91} \equiv 128 \mod 221$. Logo, $C_8 = 128$.

Assim, a mensagem encriptada é 162 51 14 134 145 113 113 128. Ao enviá-la é preciso deixar claro qual é cada bloco. Geralmente, a separação é feita por espaço como no exemplo, mas pode ser usada a vírgula ou hífen. Há necessidade da separação dos blocos pois a decodificação é realizada bloco a bloco.

- **Sétimo passo -** Decriptar a mensagem.
  Para decriptar a mensagem 162 51 14 134 145 113 1131 28 usamos a chave de decodificação, $d = 19$, calculada no quinto passo e efetuamos o cálculo $C_i^d \equiv M_i \mod n$ em cada bloco.

Tabela 4.6 – Separação de blocos: Decodificação - Exemplo 4.4

Valor do bloco	162	51	14	134	145	113	113	128
Bloco correspondente	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8

Para cada bloco devemos efetuar o cálculo $C_i^{19} \equiv M_i \mod 221$ Para o bloco C_1 temos que

$$162 \equiv 162 \mod 221, \tag{4.98}$$

$$162^3 \equiv 162^3 = 4.251.528 \mod 221. \tag{4.99}$$

Como $4.251.528 = 221 \cdot 19.237 + 151$, temos que $162^3 \equiv 151 \mod 221$.
Assim, $(162^3)^2 \equiv 151^2 \mod 221$ e como $151^2 = 22.801 = 221 \cdot 103 + 38$, segue que

$$162^6 \equiv 38 \mod 221, \tag{4.100}$$

$$(162^6)^5 \equiv 38^5 \mod 221. \tag{4.101}$$

Como $38^5 = 79.235.168$ e $79.235.168 = 221 \cdot 358.530 + 38$, segue que

$$162^{30} \equiv 38 \mod 221. \tag{4.102}$$

Assim, $(162^{30})^3 \equiv 38^3 \mod 221$ e como $38^3 = 54.872 = 221 \cdot 248 + 64$ segue que

$$162^{90} \equiv 64 \mod 221. \tag{4.103}$$

Logo,

$$162^{90} \cdot 162 \equiv 64 \cdot 162 \mod n, \tag{4.104}$$

$$162^{91} \equiv 10.368 \mod n. \tag{4.105}$$

Como $10.368 = 221 \cdot 46 + 202$, segue que $162^{91} \equiv 202 \mod 221$. Portanto, $M_1 = 202$.

Fazendo cálculos análogos para os demais blocos, temos:

Para $C_2 = 51$, $51^{19} \equiv 51 \mod 221$. Logo, $M_2 = 51$.

Para $C_3 = 14$, $14^{19} \equiv 94 \mod 221$. Logo, $M_3 = 94$.

Para $C_4 = 134$, $134^{19} \equiv 43 \mod 221$. Logo, $M_4 = 43$.

Para $C_5 = 145$, $145^{19} \equiv 219 \mod 221$. Logo, $M_5 = 219$.

Para $C_6 = 113$, $113^{19} \equiv 22 \mod 221$. Logo, $M_6 = 22$.

Para $C_7 = 113$, $113^{19} \equiv 22 \mod 221$. Logo, $M_7 = 22$.

Para $C_8 = 128$, $128^{19} \equiv 15 \mod 221$. Logo, $M_8 = 15$.

Estes cálculos foram realizados com auxílio do *software* Máxima e o algoritmo utilizado está no Apêndice B.

Assim, a mensagem decodificada será 202 51 94 43 219 22 22 15. Usando Tabela 4.3 e reagrupando os números, obtemos para a sequência 202519443219222215 a mensagem original JOINVILLE.

No exemplo seguinte faremos a codificação e decodificação de uma frase maior. A intenção é mostrar ao leitor que a complexidade dos cálculos que envolvem a criptografia RSA aumenta conforme o tamanho do texto e os valores de p e q. Mesmo que os cálculos sejam realizados por computadores, demandam tempo e capacidade de processamento das máquinas. Para este exemplo escolhemos números primos de 3 dígitos e o cálculo das congruências modulares de cada bloco foi realizado com auxílio do *software* livre Maxima. O algoritmo utilizado para obter os resultados está no Apêndice B.

Exemplo 4.5. *Queremos codificar a mensagem : CONGRUÊNCIAS MODULARES: APLICAÇÕES EM PROBLEMAS DE OLIMPÍADAS DE MATEMÁTICA. Para transformar essa mensagem de texto em números, utilizaremos a Tabela 4.3.*

Assim, a pré codificação da frase CONGRUÊNCIAS MODULARES: APLICAÇÕES EM PROBLEMAS DE OLIMPÍADAS DE MATEMÁTICA, resulta na sequência numérica:
1325241728311524131911299923251431221128152939991126221913114644152999152399
628251222152311299914159925221923264111141129991415992311301523403019131137.
Os parâmetros utilizados foram:

- $p = 101$, $q = 397$;
- $n = 40.097$;
- $\varphi(n) = 39600$;
- $e = 23$;
- $d = 6887$, pois $6887 \cdot 23 = 158.401$ e $158.401 \equiv 1 \mod 39600$.

Para encriptar a mensagem, precisamos primeiramente separa-lá em blocos de tamanho menor que n, isto é, cada bloco deve ter valor numérico menor que n.

Tabela 4.7 – Separação de blocos - Exemplo 4.5

Bloco	**Valor do Bloco**	**Bloco**	**Valor do Bloco**
M_1	13252	M_{18}	8251
M_2	4172	M_{19}	22215
M_3	831	M_{20}	23112
M_4	15241	M_{21}	9991
M_5	31911	M_{22}	4159
M_6	29992	M_{23}	9252
M_7	32514	M_{24}	21923
M_8	31221	M_{25}	26441
M_9	12815	M_{26}	11411
M_{10}	29399	M_{27}	29991
M_{11}	9112	M_{28}	4159
M_{12}	6221	M_{29}	9231
M_{13}	9131	M_{30}	13015
M_{14}	14644	M_{31}	2340
M_{15}	15299	M_{32}	30191
M_{16}	9152	M_{33}	31137
M_{17}	39962		

Vamos agora fazer a encriptação de cada bloco. Para isso, precisamos efetuar o cálculo

$$M_i^{23} \equiv C_i \mod 40.097, \tag{4.106}$$

onde C_i será a encriptação do bloco i. Utilizando o *software* Maxima, encontramos facilmente os valores C_i. Vamos organizar estes valores na Tabela 4.8.

Tabela 4.8 – Blocos encriptados - Exemplo 4.5

i	M_i	C_i	i	M_i	C_i
1	13252	25381	18	8251	7709
2	4172	270	19	22215	33132
3	831	35068	20	23112	39931
4	15241	15160	21	9991	9693
5	31911	3943	22	4159	23975
6	29992	36061	23	9252	7183
7	32514	7370	24	21923	1832
8	31221	4176	25	26441	31987
9	12815	14610	26	11411	6310
10	29399	8588	27	29991	36144
11	9112	35023	28	4159	23975
12	6221	9657	29	9231	38469
13	9131	32157	30	13015	22001
14	14644	22017	31	2340	19558
15	15299	25999	32	30191	35246
16	9152	10573	33	31137	3146
17	39962	9786			

Assim, a mensagem encriptada é: 25381 270 35068 15160 3943 36061 7370 4176 14610 8588 35023 9657 32157 22017 25999 10573 9786 7709 33132 39931 9693 23975 7183 1832 31987 6310 36144 23975 38469 22001 19558 35246 3146.

Para decriptar a mensagem, é necessário que seja realizado, para cada bloco, o cálculo

$$C_i^{6887} \equiv M_i \mod 40097. \tag{4.107}$$

Conforme foi demonstrado na Proposição 4.8, ao realizar o cálculo descrito na congruência (4.107), obteremos a mensagem original 13252 4172 831 15241 31911 29992 32514 31221 12815 29399 9112 6221 9131 14644 15299 9152 39962 8251 22215 23112 9991 4159 9252 21923 26411 11411 29991 4159 9231 13015 2340 30191 31137.

Reagrupando os números e usando a Tabela 4.3, obtemos a mensagem original: CONGRUÊNCIAS MODULARES: APLICAÇÕES EM PROBLEMAS DE OLIMPÍADAS DE MATEMÁTICA.

Podemos perceber que, quanto maior for a mensagem, mais complexos serão os cálculos realizados. Por conta disso, quando a mensagem não requer segurança por um longo período

de tempo utiliza-se a criptografia de chave privada. Para aumentar a segurança da mensagem, a chave de codificação é transmitida através do método RSA.

O método RSA garante a segurança no envio de mensagens, mas como podemos ter a garantia de que quem enviou a mensagem foi realmente aquele remetente? Por exemplo, se Ana envia uma mensagem para Bia pedindo que realize uma transferência bancária, como Bia pode ter certeza de que foi Ana quem enviou? A assinatura digital garante a autenticidade do remetente e seu funcionamento é através do método RSA. A criptografia de chaves públicas utiliza uma chave pública e uma privada, sendo que ambas estão relacionadas matematicamente. Para enviar uma mensagem codificada, o emissor busca no diretório do receptor da mensagem a chave pública e com esta faz a encriptação da mensagem. A assinatura digital funciona da seguinte maneira: imagine que Ana quer enviar um documento para Bia e Bia quer ter a certeza de que realmente foi enviado por Ana. Ana então criptografa o documento utilizando a sua chave privada e envia para Bia. Bia então utiliza a chave pública de Ana e faz a decriptação da mensagem. Se Bia conseguir realizar a decriptação é sinal de que a mensagem foi realmente enviada por Ana.

4.5 SEGURANÇA DO MÉTODO RSA

O RSA é considerado, atualmente, um dos mais seguros métodos de criptografia. A dificuldade encontrada pelos criptoanalistas em quebrar a cifra está na dificuldade em fatorar o número n, se este for extremamente grande. Existem atualmente algoritmos de computadores que buscam números primos grandes ou testam a primalidade de um número rapidamente. Porém, realizar a fatoração de um número que é resultado de dois primos extremamente grandes com computadores comuns, atualmente, é um processo que pode levar anos. Outras possibilidades para quebrar a segurança do RSA seriam determinar $\varphi(n)$ sem fatorar n ou determinar d sem fatorar n e sem calcular $\varphi(n)$. De acordo com Terada (2000), qualquer uma das duas últimas opções são tão difíceis ou mais do que fatorar n.

Não se pode garantir por quanto tempo a criptografia RSA pode ser considerada segura, uma vez que com os avanços tecnológicos é possível que a qualquer momento alguém encontre uma forma de fatorar n, mesmo este contendo muitos dígitos. Segundo Stallings (2008), em 1977, Rivest, Shamir e Adleman desafiaram os leitores da revista *Scientific American* a decodificar uma mensagem criptografada com o RSA usando uma chave pública com 129 dígitos. Os pesquisadores previam que isso não poderia ser realizado por cerca de 40 quadrilhões de anos. Em 1994, um grupo conseguiu a façanha depois de oito meses de trabalho. Outros desafios foram lançados e um dos mais recentes utilizava uma chave de 200 dígitos. Foi quebrada em maio de 2005. Atualmente, especialistas recomendam o uso de uma chave de 309 dígitos para

operações comerciais que não necessitam de proteção por um longo período de tempo e, para as que precisam, uma chave de 617 dígitos.

A partir do ano de 1990 pesquisadores da área da computação iniciaram os trabalhos de pesquisa para a construção de computadores quânticos (Figueiredo e Costa (2010)). Estas máquinas realizariam cálculos bilhões de vezes mais rápido e baseiam-se na teoria da mecânica quântica. Segundo Singh (2003) um dos pioneiros no estudo da computação quântica foi David Deutsch, físico que começou a trabalhar com esse conceito em 1984. Publicou um trabalho em 1985 relatando sua visão de como seria um computador trabalhando de acordo com as leis da física quântica. Basicamente, a diferença de um computador quântico para um comum é que, no comum se computarmos por exemplo duas perguntas, ele processa uma de cada vez. O computador quântico processaria e apresentaria a resposta das duas perguntas ao mesmo tempo. Em um computador comum o processamento de qualquer informação é feita através de dígitos binários, os *bits*, que podem ser representados por zeros ou uns. Basicamente, qualquer informação processada pelo computador comum é transformada em uma sequência de zeros e uns, em milésimos de segundos. Na computação quântica, o processamento das informações é feito através de bits quânticos, chamados de *qubits*, que ao invés de alternarem entre os valores 0 e 1, podem ser 0 e 1 ao mesmo tempo. Assim, é possível realizar muito mais cálculos de uma única vez. Em Singh (2003)[p.355] é possível encontrar um exemplo da comparação do poder de computadores quânticos e tradicionais. A comparação é feita através da resolução do problema de encontrar um número cujo quadrado e o cubo juntos usem todos os dígitos de 0 a 9 uma vez e somente uma vez. Um computador tradicional testaria todos os números a partir do 1 até chegar na resposta adequada que é 69 pois, $69^2 = 4761$ e $69^3 = 328509$. O processo leva tempo e, digamos que seja realizado um teste a cada segundo, para resolver esse problema o computador tradicional levaria 69 segundos. Já o computador quântico poderia encontrar a resposta em apenas um segundo, pois realiza todos os cálculos ao mesmo tempo.

Fabricantes como Google, Intel e IBM trabalham na produção de processadores e computadores quântico há muitos anos. Vários protótipos foram lançados e o primeiro a ser desenvolvido para uso comercial conta com um processamento de 20 qubits, foi produzido pela IBM e lançado em janeiro de 2019. Segundo a IBM, a máquina pode ser utilizada por empresas e pesquisadores. Ainda não desenvolve cálculos complexos como era de se esperar mas, a partir deste primeiro computador, novas pesquisas podem surgir.

Em 1994 o matemático Peter Shor desenvolveu um algoritmo, conhecido como Algoritmo de Shor, para computadores quânticos (Singh (2003)). Este algoritmo define uma série de passos para fatorar números extremamente grandes. A descoberta de Shor influenciou empresas e pesquisadores a desenvolver computadores quânticos. Em 2001 cientistas do centro de pesqui-

sas IBM desenvolveram um computador quântico de 7 *qubits* e implementaram o algoritmo de Shor para fatorar o número 15 (Navaux (2004)).

Sem sombra de dúvida a computação quântica é um avanço na tecnologia, porém é um problema para a criptografia. Assim que computadores quânticos forem utilizados para a fatoração de números muito grandes, a segurança do método RSA estará comprometida. Dessa forma, redes bancárias e comércio *on-line* não serão mais seguros, deixando para os criptologistas a função de criar um novo método ainda mais seguro, pelo menos por alguns anos.

5 PROPOSTA DE ATIVIDADE

Neste capítulo propomos atividades que podem ser desenvolvidas com alunos do Ensino Básico. Propomos a aplicação dessa atividade para estudantes que estão se preparando para olimpíadas de matemática. O professor pode ainda utilizar essas atividades em suas aulas para instigar a curiosidade dos alunos, promovendo uma aula diferenciada.

5.1 QUESTÕES DE OLIMPÍADAS DE MATEMÁTICA

Nesta seção apresentamos uma sequência didática de exercícios, retirados do banco de questões da OBMEP e da OBM, para que o professor possa trabalhar com seus alunos. Os enunciados foram transcritos como aparecem nos bancos de questões, por este motivo as tabelas e figuras não foram numeradas. Na seção 5.3, apresentamos a resolução destes problemas usando a teoria de congruências modulares.

Questão 1 (OBM (2003a)) - Seja $n = 9867$. Se você calculasse $n^3 - n^2$ você encontraria um número cujo algarismo das unidades é:

a) 0
b) 2
c) 4
d) 6
e) 8

Questão 2 (OBM (2003b)) - Considere a sequência oscilante: 1, 2, 3, 4, 5, 4, 3, 2, 1, 2, 3, 4, 5, 4, 3, 2, 1, 2, 3, 4, ... O $2003^{\underline{o}}$ termo desta sequência é:

a) 1
b) 2
c) 3
d) 4
e) 5

Questão 3 (OBM (2000)) - Se os números naturais são colocados em colunas, como se mostra abaixo, debaixo de que letra aparecerá o número 2000?

a) F
b) B
c) C

A	B	C	D	E	F	G	H	I
1		2		3		4		5
	9		8		7		6	
10		11		12		13		14
	18		17		16		15	
19		20		21		...		...

d) D

e) I

Questão 4 (OBM (2017b)) - Sejam m e n dois inteiros positivos primos entre si. O *Teorema Chinês dos Restos* afirma que, dados inteiros i e j com $0 \leq i < m$ e $0 \leq j < n$, existe exatamente um inteiro a, com $0 \leq a < m \cdot n$, tal que o resto da divisão de a por m é igual a i e o resto da divisão de a por n é igual a j. Por exemplo, para $m = 3$ e $n = 7$, temos que 19 é o único número que deixa restos 1 e 5 quando divididos por 3 e 7, respectivamente. Assim, na tabela a seguir, cada número de 0 a 20 aparecerá exatamente uma vez.

	0	**1**	**2**	**3**	**4**	**5**	**6**
0							
1						19	
2							

Qual a soma dos números das casas destacadas?

Questão 5 (OBMEP (2009)) - João mora em Salvador e seus pais em Recife. Para matar a saudade, ele telefona para seus pais a cada três dias. O primeiro telefonema foi feito no domingo, o segundo telefonema na quarta feira, o terceiro telefonema no sábado, e assim por diante. Em qual dia da semana João telefonou para seus pais pela centésima vez?

Questão 6 (OBMEP (2005)) - Distribuímos os números inteiros positivos em uma tabela com cinco colunas, conforme o seguinte padrão.

A	B	C	D	E
1				
2	3			
4	5	6		
7	8	9	10	
11	12	13	14	15
16				
17	18			
19	20	21		
22	23	24	25	
26	27	28	29	30
31				
32	33			
⋮				

Continuando a preencher a tabela desta manteira, qual será a coluna ocupada pelo número 2005?

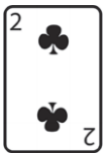
a) coluna A
b) coluna B
c) coluna C
d) coluna D
e) coluna E

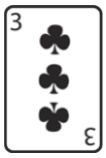
Questão 7 (OBMEP (2012a)) - Cinco cartas, inicialmente dispostas como na figura, serão embaralhadas. Em cada embaralhamento, a primeira carta passa a ser a segunda, a segunda passa a ser a quarta, a terceira passa a ser a primeira, a quarta passa a ser a quinta e a quinta passa a ser a terceira.

Qual será a primeira carta após 2012 embaralhamentos?

100

a) 

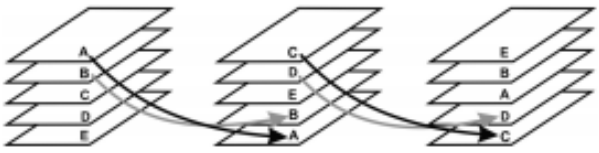
b) 

c) 

d) 

e) 

Questão 8 (OBMEP (2012b)) - Estefânia tem cinco cartas marcadas com as letras A, B, C, D e E, empilhadas nessa ordem de cima para baixo. Ela embaralha as cartas pegando as duas de cima e colocando-as, com a ordem trocada, embaixo da pilha. A figura mostra o que acontece nas duas primeiras vezes em que ela embaralha as cartas.



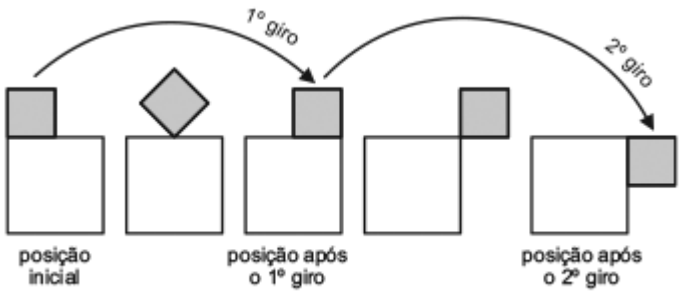
Se Estefânia embaralhar as cartas 74 vezes, qual carta estará no topo da pilha?

a) A
b) B
c) C

d) D

e) E

Questão 9 (OBMEP (2012c)) - Um quadrado de lado 1 cm roda em torno de um quadrado de lado 2 cm, como na figura, partindo da posição inicial e completando um giro cada vez que um de seus lados fica apoiado em um lado do quadrado maior.



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

a) 

b) 

c) 

d) 

e) 

Questão 10 (OBMEP (2016)) - Juca possui menos do que 800 bolinhas de gude. Ele gosta de separar as bolinhas em grupinhos com a mesma quantidade de bolinhas. Ele percebeu que se formar grupinhos com 3 bolinhas cada, sobram exatamente 2 bolinhas. Se ele formar grupinhos de 4 bolinhas, sobram 3 bolinhas. Se ele formar grupinhos de 5 bolinhas, sobram 4 bolinhas. E, finalmente, se ele formar grupinhos com 7 bolinhas cada, sobram 6 bolinhas.

a) Se Juca formasse grupinhos com 20 bolinhas cada, quantas bolinhas sobrariam?

b) Juca possui quantas bolinhas de gude?

5.2 ATIVIDADES DE CRIPTOGRAFIA

Nesta seção apresentamos uma proposta de atividades para o professor trabalhar a criptografia com os alunos. Iniciaremos com uma dinâmica proposta afim de que os estudantes compreendam que o objetivo da criptografia é proteger o conteúdo de uma mensagem.

Atividade 1 (dinâmica) - Essa dinâmica deve ser apresentada aos alunos antes de introduzir o conceito de criptografia. O professor pode iniciar a aula contando algumas formas em que as mensagens secretas eram enviadas antigamente. Pode falar por exemplo das técnicas de esteganografia, citadas no Capítulo 4, explicar o funcionamento e apresentar exemplos da cifra de César. O material a ser utilizado para a dinâmica é um cadeado com duas chaves, uma caixa que possa ser trancada e uma mensagem escrita por um dos alunos.
Dois alunos podem ajudar na realização da dinâmica. Com esse material, o professor deve pedir para que expliquem como a mensagem pode ser enviada de um aluno para outro, sendo que apenas o emissor da mensagem e o receptor podem saber do seu conteúdo. Facilmente os estudantes dirão que basta trancar a mensagem dentro da caixa e enviar para a outra pessoa que tenha a chave do cadeado. A atividade é simples, mas o professor pode explorar o conceito de chave de encriptação, explicando aos alunos que a segurança do envio da mensagem consiste em que apenas o emissor e o receptor possuam a chave de acesso para decriptar a mensagem. Além disso, a troca dessa chave deve ser combinada antes do envio. O professor pode comentar sobre a segurança no envio da mensagem e incentivá-los a discutir o que acontece se alguém for capaz de construir uma cópia dessa chave.

Atividade 2 - Utilizando os conhecimentos sobre a congruência modular o professor pode explicar o funcionamento da criptografia RSA, explicado no capítulo 4, e pedir para que cada um codifique uma mensagem curta. Sugerir para que cada aluno escolha dois números primos, p e q, de um dígito cada e deixem anotado em um papel sobre a sua carteira os valores de $n = p \cdot q$ e da chave e, onde $(e, \varphi(n)) = 1$ e $1 < e < \varphi(n)$. Em duplas, cada um deve utilizar a chave pública do colega e codificar uma mensagem de no máximo quatro letras, para facilitar os cálculos. Em seguida, cada aluno deve pedir para que o colega realize a decriptação de sua mensagem. Para a explicação da atividade, o professor pode utilizar os Exemplos 4.3 e 4.4 do Capítulo 4.

É importante que os alunos compreendam que, mesmo que a chave pública esteja disponível ao acesso de todos, apenas o receptor da mensagem vai ter a chave privada relacionada que é capaz de decodificar a mensagem. Alguns alunos podem questionar que dado n, nessas condições (n terá dois dígitos) será fácil determinar p e q. O professor deverá deixar claro que o objetivo da atividade é fazê-los compreender o funcionamento do algoritmo. Após a aplica-

ção dessa atividade, o professor pode apresentar aos alunos o *software* livre Maxima e sugerir que refaçam a atividade com números primos maiores. Assim, os cálculos não ocuparão muito tempo e o professor poderá deixar claro aos alunos que utilizando números primos maiores, a complexidade dos cálculos aumenta e a segurança no envio das mensagens também.

Atividade 3 - Para entender a complexidade da fatoração de números com muitos dígitos, o professor pode pedir para que em duplas, ou pequenos grupos, os alunos acessem o *site* <https://www.alpertron.com.ar/ECM.HTM> e realizem fatorações de alguns números com grande quantidade de dígitos. Os alunos devem digitar o número que desejam fatorar e acionar no comando *factor*. O professor pode pedir para que organizem uma tabela com a quantidade de dígitos desse número e o tempo que o *site* leva para fatorar. O *site* tem acesso gratuito e registra automaticamente o tempo, assim como a quantidade de dígitos do número.

5.3 RESOLUÇÃO DOS PROBLEMAS PROPOSTOS

Questão 1 - Para determinarmos o dígito das unidades de um número, podemos fazer a análise da congruência desse número em módulo 10. Assim, para $n = 9867$, temos:

$$9867 \equiv 7 \mod 10, \tag{5.1}$$

$$9867^2 \equiv 7^2 mod 10 \tag{5.2}$$

e como $7^2 = 49$ e $49 \equiv 9 \mod 10$, segue que

$$9867^2 \equiv 9 \mod 10. \tag{5.3}$$

Das Congruências (5.1) e (5.3), temos que

$$9867^2 \cdot 9867 \equiv 9 \cdot 7 \mod 10. \tag{5.4}$$

De $9 \cdot 7 = 63$ e $63 \equiv 3 \mod 10$, segue que

$$9867^3 \equiv 3 \mod 10. \tag{5.5}$$

Das congruências (5.3) e (5.5), temos que

$$9867^3 - 9867^2 \equiv 3 - 9 \mod 10. \tag{5.6}$$

Como $-6 \equiv 4 \mod 10$, obtemos

$$9867^3 - 9867^2 \equiv 4 \mod 10. \tag{5.7}$$

O algarismo das unidades é o 4, portanto a resposta correta é o item "c".

Questão 2 - Podemos observar que a sequência é infinita e podemos identificar que o bloco 1, 2, 3, 4, 5, 4, 3, 2, formado por 8 termos, se repete. Para determinar o termo que está na 2003^{o} posição devemos encontrar o resto da divisão de 2003 por 8, isto é, o número que é congruente a 2003 módulo 8. Temos que

$$10 \equiv 2 \mod 8, \tag{5.8}$$

$$10^2 \equiv 2^2 = 4 \mod 8, \tag{5.9}$$

$$10^2 \cdot 10 \equiv 4 \cdot 2 \mod 8. \tag{5.10}$$

Como $8 \equiv 0 \mod 8$, temos que

$$10^3 \equiv 0 \mod 8, \tag{5.11}$$

$$2 \cdot 10^3 \equiv 2 \cdot 0 \mod 8, \tag{5.12}$$

$$2000 \equiv 0 \mod 8. \tag{5.13}$$

Como $3 \equiv 3 \mod 8$, da congruência (5.13) segue que

$$2000 + 3 \equiv 0 + 3 \mod 8, \tag{5.14}$$

ou seja, $2003 \equiv 3 \mod 8$. Assim, o 2003^{o} termo da sequência será igual ao terceiro termo, ou seja, o número 3. Portanto, a resposta correta é o item "c".

Questão 3 - Escrevendo a sequência, temos : A, C, E, G, I, H, F, D, B. Já que a sequência se repete a cada 9 termos, para determinar a coluna em que estará o número 2000, devemos encontrar o resto da divisão de 2000 por 9, isto é, o número que é congruente a 2000 módulo 9. Temos que

$$10 \equiv 1 \mod 9, \tag{5.15}$$

$$10^3 \equiv 1^3 \mod 9, \tag{5.16}$$

$$2 \cdot 10^3 \equiv 2 \cdot 1 \mod 9, \tag{5.17}$$

isto é, $2000 \equiv 2 \mod 9$. Portanto, o número 2000 estará na mesma coluna que o número 2, ou seja, na coluna C. Portanto, a resposta correta é o item "c".

Questão 4 - Para encontrar a soma das casas destacadas, precisamos descobrir qual número que ocupa cada casa. Considere a Tabela (5.1)

Tabela 5.1 – Resolução problema 4

	0	**1**	**2**	**3**	**4**	**5**	**6**
0		A				B	
1				C		19	D
2		E			F		

Para determinar A, temos que

$$A \equiv 0 \mod 3 \tag{5.18}$$

e

$$A \equiv 1 \mod 7 \tag{5.19}$$

Pelo Teorema Chinês dos Restos, temos $a_1 = 0, a_2 = 1, m_1 = 3$ e $m_2 = 7$. Assim, $M = 21, M_1 = \frac{21}{3} = 7$ e M_2
Precisamos agora determinar y_1 e y_2 tais que

$$7y_1 \equiv 1 \mod 3 \tag{5.20}$$

e

$$3y_2 \equiv 1 \mod 7. \tag{5.21}$$

Analisando as congruências (5.20) e (5.21), por inspeção, obtemos $y_1 = 1$ e $y_2 = 5$. Assim, uma solução do sistema é dada por

$$A = 7 \cdot 0 \cdot 1 + 3 \cdot 1 \cdot 5 = 15 \tag{5.22}$$

Portanto, já que A é um número entre 0 e 20, temos que $A = 15$.

Podemos observar que, uma vez que a questão trata de números pequenos, o aluno pode chegar ao resultado simplesmente por inspeção das congruências (5.20) e (5.21), não havendo necessidade da aplicação rigorosa do Teorema Chinês dos Restos. Porém, isso mostra aplicação deste teorema em problemas de olimpíadas de matemática de nível básico.

De forma análoga ao cálculo anterior, obtemos os resultados de B, C, D e F.
Para determinar B, temos que $B \equiv 0 \mod 3$ e $B \equiv 5 \mod 7$ então, $B = 12$.
Para determinar C, temos que $C \equiv 1 \mod 3$ e $C \equiv 3 \mod 7$ então, $C = 10$.
Para determinar D, temos que $D \equiv 1 \mod 3$ e $D \equiv 6 \mod 7$ então, $D = 13$.
Para determinar E, temos que $E \equiv 2 \mod 3$ e $E \equiv 1 \mod 7$ então, $E = 8$.
Para determinar F, temos que $F \equiv 2 \mod 3$ e $F \equiv 4 \mod 7$ então, $F = 11$.

Portanto, a soma das casas destacadas é $A+B+C+D+E+F = 15+12+10+13+8+11 = 69$.

Questão 5 - Vamos listar os dias em que aconteceram as primeiras chamadas:

Primeira chamada: domingo
Segunda chamada: quarta feira
Terceira chamada: sábado
Quarta chamada: terça feira
Quinta chamada: sexta feira
Sexta chamada: segunda feira
Sétima chamada: quinta feira
Oitava chamada: domingo
Nona chamada: quarta feira

Como os telefonemas são realizados a cada três dias, a sequência de dias da semana se repete a cada 7 telefonemas então, para determinar o dia da centésima ligação, devemos encontrar o resto da divisão de 100 por 7. Isto é, devemos encontrar o número que é congruente a 100 módulo 7. Temos que

$$10 \equiv 3 \mod 7, \tag{5.23}$$

$$10^2 \equiv 3^2 \mod 7. \tag{5.24}$$

De $9 \equiv 2 \mod 7$, segue que

$$100 \equiv 2 \mod 7. \tag{5.25}$$

Assim, o centésimo telefonema será realizado no mesmo dia da semana que o segundo telefonema, isto é, em uma quarta feira.

Questão 6 - A cada 15 termos a sequência se repete. A sequência é formada pelos termos A, A, B, A, B, C, A, B, C, D, A, B, C, D, E. Para determinar a coluna que será ocupada pelo número 2005, devemos calcular o número que é congruente a 2005 módulo 15. Temos que

$$10 \equiv 10 \mod 15 \tag{5.26}$$

e

$$200 \equiv 5 \mod 15. \tag{5.27}$$

Então,

$$10 \cdot 200 \equiv 10 \cdot 5 \mod 15, \tag{5.28}$$

isto é, $2000 \equiv 50 \mod 15$. Como $50 \equiv 5 \mod 15$, segue que

$$2000 \equiv 5 \mod 15. \tag{5.29}$$

Também,

$$5 \equiv 5 \mod 15. \tag{5.30}$$

Das congruências (5.29) e (5.30), concluímos que

$$2005 \equiv 5 + 5 = 10 \mod 15. \tag{5.31}$$

Logo, a coluna ocupada pelo número 2005 será a mesma ocupada pelo número 10, isto é, a coluna D. Portanto, a resposta correta é o item "c".

Questão 7 - Após o primeiro embaralhamento, a sequência de cartas será: 3, A, 5, 2, 4.
Após o segundo embaralhamento, a sequência de cartas será: 5, 3, 4, A, 2.
Após o terceiro embaralhamento, a sequência de cartas será: 4, 5, 2, 3, A.
Após o quarto embaralhamento, a sequência de cartas será: 2, 4, A, 5, 3.
Após o quinto embaralhamento, a sequência de cartas será: A, 2, 3, 4, 5.
Podemos perceber que a cada cinco embaralhamentos a sequência de cartas se repete. Então, para determinar a primeira carta da sequência após 2012 embaralhamentos, devemos determinar o número que é congruente a 2012 módulo 5.

Temos que

$$2012 \equiv 2 \mod 5. \tag{5.32}$$

Portanto, após 2012 embaralhamentos a sequência de cartas será a mesma que depois de 2 embaralhamentos. Sendo assim, a primeira carta da sequência será o 5. Então o item que apresenta a resposta correta é o "e".

Questão 8 - Após o primeiro embaralhamento, a sequência de cartas será: C, D, E, B, A.
Após o segundo embaralhamento, a sequência de cartas será: E, B, A, D, C.
Após o terceiro embaralhamento, a sequência de cartas será: A, D, C, B, E.
Após o quarto embaralhamento, a sequência de cartas será: C, B, E, D, A.
Após o quinto embaralhamento, a sequência de cartas será: E, D, A, B, C.
Após o sexto embaralhamento, a sequência de cartas será: A, B,C, D, E.

Podemos perceber que após 6 embaralhadas a sequência se repete. Então, para determinar a carta que estará no topo da pilha após 74 embaralhadas, devemos encontrar o número que é congruente a 74 módulo 6. Temos que

$$74 \equiv 2 \mod 6. \tag{5.33}$$

Logo, após 74 embaralhadas, a sequência de cartas será a mesma que depois a segunda embaralhada. Logo, a carta que estará no topo, será a de letra E, que se encontra no item "e".

Questão 9 - Girando o quadrado menor em volta do maior, podemos perceber que após o oitavo giro, o quadrado menor volta a sua posição inicial e, então, a sequência de imagens se repete. Portanto, para determinar a posição do quadrado menor no $2012^{\underline{o}}$ giro, devemos encontrar o número que é congruente a 2012 módulo 8. Temos que

$$10 \equiv 2 \mod 8, \tag{5.34}$$

$$10^3 \equiv 2^3 \mod 8. \tag{5.35}$$

De $2^3 = 8$, e $8 \equiv 0 \mod 8$, segue que $1000 \equiv 0 \mod 8$. Então,

$$2 \cdot 1000 \equiv 2 \cdot 0 \mod 8. \tag{5.36}$$

Como $12 \equiv 4 \mod 8$, segue que

$$2012 \equiv 4 \mod 8. \tag{5.37}$$

Portanto, após o $2012^{\underline{o}}$ giro, a posição do quadrado menor será a mesma do quarto giro, ou seja, a resposta correta é o item "a".

Questão 10 - Para resolver esta questão é mais interessante iniciarmos pelo item "b", uma vez que podemos usar a resposta desse item para concluir a resolução do item "a".

b) Queremos determinar o número x tal que satisfaça o sistema

$$x \equiv 2 \mod 3 \tag{5.38}$$

$$x \equiv 3 \mod 4 \tag{5.39}$$

$$x \equiv 4 \mod 5 \tag{5.40}$$

$$x \equiv 6 \mod 7. \tag{5.41}$$

Podemos resolver esse problema utilizando o Teorema Chinês dos Restos. Assim, temos que $a_1 = 2$, $a_2 = 3$, $a_3 = 4$, $a_4 = 6$, $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$. Como $M = m_1 \cdot m_2 \cdot m_3 \cdot m_4$,

segue que $M = 3 \cdot 4 \cdot 5 \cdot 7 = 240$. Além disso, $M_i = \frac{M}{m_i}$ então, $M_1 = 140$, $M_2 = 105$, $M_3 = 84$ e $M_4 = 60$. Para determinar y_1, y_2, y_3 e y_4, temos que encontrar as soluções de cada uma das congruências abaixo:

$$140y_1 \equiv 1 \mod 3 \tag{5.42}$$

$$105y_2 \equiv 1 \mod 4 \tag{5.43}$$

$$84y_3 \equiv 1 \mod 5 \tag{5.44}$$

$$60y_4 \equiv 1 \mod 7. \tag{5.45}$$

Assim, por inspeção, temos que $y_1 = 2$, $y_2 = 1$, $y_3 = 4$ e $y_4 = 2$. De acordo com o Teorema Chinês dos Restos, uma solução do sistema é dado por

$$x_0 = M_1 a_1 y_1 + M_2 a_2 y_2 + M_3 a_3 y_3 + M_4 a_4 y_4. \tag{5.46}$$

Sendo assim, temos

$$x_0 = 140 \cdot 2 \cdot 2 + 105 \cdot 5 \cdot 3 + 84 \cdot 4 \cdot 4 + 60 \cdot 2 \cdot 6 = 560 + 315 + 1344 + 720 = 2939. \tag{5.47}$$

A solução geral do sistema é dada por

$$x(t) = x_0 + Mt, \tag{5.48}$$

então, temos

$$x(t) = 2939 + 420t, \qquad t \in \mathbb{Z}. \tag{5.49}$$

Como o número procurado é menor que 800, devemos resolver a inequação $2939 + 420t < 800$, obtendo o resultado $t < -5$. Portanto, para $t = -6$, obtemos

$$x = 2939 + (-6) \cdot 420 = 419 \tag{5.50}$$

Isto é, Juca possui 419 bolinhas de gude.

a) Como o total de bolinhas é 419 e $419 = 20 \cdot 20 + 19$, temos que ao formar grupinhos com 20 bolinhas cada, sobrariam 19 bolinhas.

6 CONSIDERAÇÕES FINAIS

A motivação desse trabalho se deu através da minha experiência como professora. Desde o início de minha carreira percebi em grande parte dos meus alunos a falta de interesse em aprender matemática e a dificuldade na compreensão da disciplina, acarretando no baixo desempenho dos mesmos em olimpíadas de matemática. Assim, surgiu a ideia de desenvolver na escola um projeto para treinamento de olimpíadas, assim como oficinas de matemática direcionadas a alunos interessados em aprender além do que é ensinado em sala de aula. O projeto ainda não foi implementado na escola, mas motivou a escrita desta dissertação.

O conteúdo de congruências modulares não faz parte do currículo do Ensino Básico, embora a fundamentação teórica necessária para sua aprendizagem seja abordada já no Ensino Fundamental. Acreditamos que o conhecimento das propriedades de congruências modulares seria de grande valia para os estudantes, uma vez que trata-se de uma valiosa ferramenta na resolução de exercícios. Neste sentido, apresentamos no Capítulo 2 a fundamentação teórica necessária para a compreensão da congruência modular. Um dos objetivos iniciais desta dissertação era mostrar a importância das congruências modulares atuando como facilitadora na resolução de problemas de olimpíadas de matemática do ensino básico. Com esta finalidade, realizamos uma pesquisa em bancos de questões de livre acesso e trabalhamos com nove desses problemas no Capítulo 3. Optamos por mostrar duas resoluções de cada um destes problemas. A primeira com a teoria como é ensinada nas escolas e a segunda resolução utilizando a congruência modular. Os problemas estão acompanhados de uma discussão acerca das resoluções e verificamos que alguns problemas apresentam uma resolução mais simples utilizando os conceitos tradicionalmente ensinados no nível básico de ensino (Problemas 8 e 9 do Capítulo 3) outros, utilizando congruências modulares (Problemas 4, 5 e 6 do Capítulo 3) e ainda há aqueles em que ambas as soluções apresentam o mesmo nível de dificuldade (Problemas 1, 2, 3 e 7 do Capítulo 3). A resolução através de congruências modulares pode se tornar rápida e fácil se o aluno conhecer o conteúdo e dominar as propriedades utilizadas para a resolução dos cálculos. Observamos que, dos nove problemas selecionados, sete podem ser resolvidos facilmente através de congruências. Na realização de uma olimpíada de matemática como a OBMEP, o fator tempo é muito importante e, sendo assim, entendemos que seria de grande valia se o aluno pudesse escolher a forma de resolução que permite chegar mais rápido ao resultado esperado. É claro que auxiliar na resolução de problemas é apenas uma motivação para estudar congruências modulares. O tema tem aplicações em diversas situações do cotidiano como, por exemplo, a determinação dos dígitos do CPF, ISBN, códigos de barras e a criptografia. Dentre as aplicações escolhemos o método RSA da criptografia para um estudo mais aprofundado. Assim, no

Capítulo 4 fizemos uma breve revisão histórica da criptografia e explicamos o funcionamento do método RSA. Este método baseia-se na teoria dos números, mais especificamente, em congruências modulares e tem importante aplicação no cotidiano sendo responsável por manter a segurança de grande parte das operações bancárias realizadas via *internet*. Embora a sua aplicação seja de fácil entendimento, os cálculos, em geral, são bastante complexos e demorados, como pode ser visto nos Exemplos 4.4 e 4.5. Nestes, consideramos números primos de dois e três dígitos, respectivamente, e usamos o *software* Maxima para a realização de alguns cálculos o que reduziu consideravelmente o tempo gasto na encriptação e decriptação da mensagem. Lembramos que para manter segura uma mensagem seria necessário a utilização de números primos com pelo menos 300 dígitos.

O método RSA é considerado um dos métodos mais seguros de criptografia porém, vale salientar que não é um método inquebrável. A questão é que ainda não existe um computador que realize a fatoração de um número extremamente grande em um período curto de tempo. Empresas já trabalham no desenvolvimento de computadores quânticos, que juntamente com algoritmos já existentes, serão capazes de efetuar essa fatoração rapidamente. Explicamos brevemente no Capítulo 4 o funcionamento de computadores quânticos assim como a existência de um algoritmo de fatoração chamado de Algoritmo de Shor. Não nos aprofundamos no estudo destes tópicos, mas deixamos como sugestão para um trabalho futuro. Também propomos como um trabalho futuro, a utilização do material disponível nesta dissertação para a criação de um um produto educacional desenvolvido a fim de treinar alunos interessados em participar de olimpíadas de matemática.

Acreditamos que a realização de atividades focadas em problemas de olimpíadas possa contribuir para um melhor desempenho dos alunos participantes. Por esse motivo, propomos uma lista com dez exercícios (Capítulo 5) retirados de bancos de questões de olimpíadas de matemática, assim como a resolução de cada um destes através de congruências modulares. Além disso, reunimos três atividades relacionadas com a criptografia com o intuito de facilitar a compreensão do conteúdo.

Esperamos que, com este trabalho, professores do Ensino Básico sintam-se motivados e preparados a ensinar a teoria de congruências modulares, seja em sala de aula ou em treinamentos para olimpíadas. Concluímos que conhecer mais a fundo a teoria de congruências modulares e uma importante aplicação desse conteúdo, fortalece ainda mais a percepção de que a matemática está mais presente em nosso cotidiano do que podemos imaginar.

APÊNDICE A – Demonstração do Teorema Fundamental da Aritmética

Apresentamos a seguir a demonstração do Teorema Fundamental da Aritmética utilizando o segundo princípio da indução. A demonstração está disponível em Hefez (2014, p.141). Para informações sobre o segundo princípio de indução, o leitor pode ver a referência Domingues (1991).

Teorema A.1. *Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração. Se $n = 2$, o resultado é obviamente verificado.
Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos, então, que n seja um número composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1 n_2$, com $1 < n_2 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, \ldots, p_r$ e $q_1, \ldots, q_s$ tais que $n_1 = p_1 \cdots p_r = q_1 \cdots q_s$, onde os p_i e os q_j são números primos.

Como $p_1 | q_1 \cdots q_s$, pelo Lema de Euclides, Proposição 2.7, temos que $p_1 = q_j$ para algum j, que, após reordenamento de $q_1, \ldots, q_s$, podemos supor que seja q_1. Portanto,

$$p_2 \cdots p_r = q_2 \cdots q_s. \tag{A.1}$$

Como $p_2 \cdots p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares. □

APÊNDICE B – Algoritmos

Os comandos abaixo foram realizados no *software* Maxima, que é livre e pode ser obtido através do *link* <http://maxima.sourceforge.net/pt/index.html>. Para determinar o resto da divisão do número a pelo número b devemos digitar o comando $\mod(a,b)$; e em seguida pressionar as teclas *shift* e *enter*. Assim, o aplicativo determina o número x, tal que $a \equiv x \mod b$.

B.1 ALGORITMO PARA O EXEMPLO 4.4

Apresentamos abaixo os algoritmos utilizados para a encriptação e decriptação da mensagem do Exemplo 4.4.

Algoritmo para encriptação:

```
(%i1) mod(202^(91),221);
(%o1) 162
(%i2) mod(51^(91),221);
(%o2) 51
(%i3) mod(92^(91),221);
(%o3) 14
(%i4) mod(43^(91),221);
(%o4) 134
(%i5) mod(219^(91),221);
(%o5) 145
(%i6) mod(22^(91),221);
(%o6) 113
(%i7) mod(15^(91),221);
(%o7) 128
```

Algoritmo para decriptação:

```
(%i1) mod(162^(19), 221 );
(%o1) 202
(%i2) mod(51^(19),221);
(%o2) 51
(%i3) mod(14^19,221);
(%o3) 92
(%i4) mod(134^(19),221);
(%o4) 43
(%i5) mod(145^(19),221);
(%o5) 219
(%i6) mod(113^(19),221);
(%o6) 22
(%i7) mod(128^(19),221);
(%o7) 15
```

B.2 ALGORITMO PARA O EXEMPLO 4.5

Utilizamos o algoritmo abaixo para a resolução dos cálculos na encriptação da mensagem do Exemplo 4.5. Os resultados obtidos foram apresentados na Tabela 4.8.

```
(%i1) mod(13252^(23),40097);
(%o1) 25381
(%i2) mod(4172^(23),40097);
(%o2) 270
(%i3) mod(831^(23),40097);
(%o3) 35068
(%i4) mod(15241^(23),40097);
(%o4) 15160
(%i5) mod(31911^(23),40097);
(%o5) 3943
(%i6) mod(29992^(23),40097);
(%o6) 36061
(%i7) mod(32514^(23),40097);
(%o7) 7370
(%i8) mod(31221^(23),40097);
(%o8) 4176
(%i9) mod(12815^(23),40097);
(%o9) 14610
(%i10) mod(29399^(23),40097);
(%o10) 8588
(%i11) mod(9112^(23),40097);
(%o11) 35023
(%i12) mod(6221^(23),40097);
(%o12) 9657
(%i13) mod(9131^(23),40097);
(%o13) 32157
(%i14) mod(14644^(23),40097);
(%o14) 22017
(%i15) mod(15299^(23),40097);
(%o15) 25999
(%i16) mod(9152^(23),40097);
(%o16) 10573
(%i17) mod(39962^(23),40097);
(%o17) 9786
(%i18) mod(8251^(23),40097);
(%o18) 7709
(%i19) mod(22215^(23),40097);
(%o19) 33132
(%i20) mod(23112^(23),40097);
(%o20) 39931
(%i21) mod(9991^(23),40097);
(%o21) 9693
(%i22) mod(4159^(23),40097);
(%o22) 23975
(%i23) mod(9252^(23),40097);
(%o23) 7183
(%i24) mod(21923^(23),40097);
(%o24) 1832
(%i25) mod(26441^(23),40097);
(%o25) 31987
(%i26) mod(11411^(23),40097);
(%o26) 6310
(%i27) mod(29991^(23),40097);
(%o27) 36144
(%i28) mod(4159^(23),40097);
(%o28) 23975
(%i29) mod(9231^(23),40097);
(%o29) 38469
(%i30) mod(13015^(23),40097);
(%o30) 22001
(%i31) mod(2340^(23),40097);
(%o31) 19558
(%i32) mod(30191^(23),40097);
(%o32) 35246
(%i33) mod(31137^(23),40097);
(%o33) 3146
```

A decriptação da mensagem também foi feita através do Maxima. Devido ao grande número de cálculos, apresentaremos o algoritmo utilizado nos dois primeiros blocos. Para o restante dos blocos, utilizamos o mesmo algoritmo.

```
(%i1) mod(25381^(6887),40097);
(%o1) 13252
(%i2) mod(270^(6887), 40097);
(%o2) 4172
```

REFERÊNCIAS BIBLIOGRÁFICAS

BARROS, M. A. O. de. **Aritmética Modular: Aplicações no Ensino Médio**. Dissertação (Mestrado) — Universidade Federal do Mato Grosso, 2014.

BOYER, C. B. **História da Matemática**. São Paulo: Editora Edgard Blucher, 1996.

BURTON, D. M. **The History of Mathematics**: an introduction. New York: McGraw-Hill, 2011.

CONTADOR, P. R. M. **Matemática, uma breve história**. São Paulo: Editora Livraria da Física, 2008.

COUTINHO, S. C. **Números inteiros e criptografia RSA**. Rio de Janeiro: IMPA, 2005.

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

DOMINGUES, R. F. **A aritmética como conteúdo extracurricular no ensino médio**. Dissertação (Mestrado) — Universidade Federal do Mato Grosso, 2017.

EVES, H. **Introdução à história da matemática**. Campinas, SP: UNICAMP, 2004. Tradução de Hygino H. Domingues.

FIARRESGA, V. M. C. **Criptografia e matemática**. Dissertação (Mestrado) — Universidade de Lisboa, 2010.

FIGUEIREDO, L. M.; COSTA, C. **Introdução à Criptografia**. [S.l.]: V, 2010.

HEFEZ, A. **Aritmética**. Rio de Janeiro: SBM, 2014. (Coleção PROFMAT).

ING, L. H. The history of the chinese reminder theorem. **Singapore Mathematical Society**, 2003. 2003.

KHAN ACADEMY. **Módulo de congruência**. Disponível em: <https://pt.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/congruence-modulo>. Acesso em: 03 jun. 2019.

MEC. **Base Nacional Comum Curricular**. 2017. Disponível em: <http://basenacionalcomum.mec.gov.br/abase>. Acesso em: 05 jul. 2019.

NAVAUX, P. Computação quântica. 2004. 2004. Disponível em: <http://prof.facom.ufms.br/~marco/cquantica/cquantica.pdf>.

NIVEN, I.; ZUCKERMAN, H. S.; MONTGOMERY, H. L. **An Introduction to the Theory of Numbers**. United States of America: Courier Companies, 1991.

OBM. **Olimpíada Brasileira de Matemática**. Disponível em: <https://www.obm.org.br/>. Acesso em: 05 jul. 2019.

OBM. **OBM 2000**. 2000. Disponível em: <https://www.obm.org.br/content/uploads/2017/02/obm2000_1fase-1-N1.pdf>. Acesso em: 17 out. 2018.

OBM. **OBM 2003**. 2003. Disponível em: <https://www.obm.org.br/content/uploads/2017/02/1faseOBM_2003-N2.pdf>. Acesso em: 16 out. 2018.

OBM. **OBM 2003**. 2003. Disponível em: <https://www.obm.org.br/content/uploads/2017/02/1faseOBM_2003-N2.pdf>. Acesso em: 17 out. 2018.

OBM. **OBM 2017**. 2017. Disponível em: <https://www.obm.org.br/content/uploads/2017/02/obm20011fase-N1.pdf>. Acesso em: 20 out. 2018.

OBM. **OBM 2017**. 2017. Disponível em: <https://www.obm.org.br/content/uploads/2017/01/2Fase_Nivel3_2009.pdf>. Acesso em: 17 out. 2018.

OBMEP. **Olimpíada Brasileira de Matemática das Escolas Públicas**. Disponível em: <http://www.orm.mtm.ufsc.br/index.php>. Acesso em: 05 jul. 2019.

OBMEP. **OBMEP 2005**. 2005. Disponível em: <http://www.obmep.org.br/provas_static/pf1n2-2005.pdf>. Acesso em: 15 out. 2018.

OBMEP. **OBMEP 2006**. 2006. Disponível em: <http://www.obmep.org.br/bq/bq2006.pdf>. Acesso em: 20 out. 2018.

OBMEP. **OBMEP 2009**. 2009. Disponível em: <http://www.obmep.org.br/bq/bq2009.pdf>. Acesso em: 15 out. 2018.

OBMEP. **OBMEP**. 2010. Disponível em: <https://www.obmep.org.br/banco.html>. Acesso em: 20 out. 2018.

OBMEP. **OBMEP 2012**. 2012. Disponível em: <http://www.obmep.org.br/provas_static/pf1n2-2012.pdf>. Acesso em: 15 out. 2018.

OBMEP. **OBMEP 2012**. 2012. Disponível em: <http://www.obmep.org.br/bq/bq2012.pdf>. Acesso em: 17 out. 2018.

OBMEP. **OBMEP 2012**. 2012. Disponível em: <http://www.obmep.org.br/provas_static/pf1n2-2012.pdf>. Acesso em: 16 out. 2018.

OBMEP. **OBMEP 2015**. 2015. Disponível em: <http://www.obmep.org.br/provas_static/pf2n1-2015.pdf>. Acesso em: 20 out. 2018.

OBMEP. **OBMEP 2016**. 2016. Disponível em: <http://www.obmep.org.br/bq/bq2016.pdf>. Acesso em: 16 out. 2018.

OBMEP. **Banco de questões OBMEP 2017**. 2017. Disponível em: <http://www.obmep.org.br/bq/bq2017.pdf>. Acesso em: 16 out. 2018.

OBMEP. **OBMEP 2017**. 2017. Disponível em: <http://www.obmep.org.br/provas_static/pf1n3-2017.pdf>. Acesso em: 20 out. 2018.

ORM. **Olimpíada Regional de Matemática de Santa Catarina**. Disponível em: <http://basenacionalcomum.mec.gov.br/abase>. Acesso em: 05 jul. 2019.

ORM. **ORM 2017**. 2017. Disponível em: <http://orm.mtm.ufsc.br/arquivos/provas/2017/Prova_2017_N1.pdf>. Acesso em: 20 out. 2018.

PINHEIRO, R. C. **Aritmética modular: Uma Aplicação no Ensino Fundamental**. Dissertação (Mestrado) — Universidade Federal de Goiás, 2018.

POTI. **POTI 2012**. 2012. Disponível em: <http://poti.impa.br/uploads/material_teorico/a1170g5pyrs4w.pdf>. Acesso em: 20 out. 2018.

PRAZERES, S. B. dos. **O Teorema Chinês dos Restos e a Partilha de Senhas**. Dissertação (Mestrado) — Universidade Federal Rural de Pernambuco, 2014.

ROUSSEAU, C.; SAINT-AUBIN, Y. **Matemática e Atualidade**. Rio de Janeiro: SBM, 2015.

RUIVO, A. C. A. P. C. S. J. Teorema chinês dos restos. 2016. 2016.

SINGH, S. **O livro dos códigos**. Rio de Janeiro: Editora Record, 2003.

STALLINGS, W. **Criptografia e segurança de redes**: Princípios e práticas. São Paulo: Pearson Prentice Hall, 2008.

TERADA, R. **Segurança de dados**: Criptografia em redes de computador. São Paulo: Editora Edgard Blucher Ltda., 2000.

WHATSAPP INC. **WhatsApp**. Disponível em: <https://www.whatsapp.com>. Acesso em: 22 jun. 2019.

WIKIPEDIA. **citala**. Disponível em: <https://pt.wikipedia.org/wiki/Citala>. Acesso em: 15 jul. 2019.

WIKIPEDIA. **Máquina Enigma**. Disponível em: <https://pt.wikipedia.org/wiki/Enigma_(mÃąquina)>. Acesso em: 15 jul. 2019.