UNIVERSIDADE FEDERAL DE CAMPINA GRANDE

CENTRO DE EDUCAÇÃO E SAÚDE

UNIDADE ACADÊMICA DE EDUCAÇÃO

Curso de Graduação em Licenciatura em Matemática

Maria Ioneris Oliveira Silva

CRIPTOGRAFIA:

Aplicações de Teoria dos Números e Álgebra.

Cuité - PB

2015

Maria Ioneris Oliveira Silva

CRIPTOGRAFIA:

Aplicações de Teoria dos Números e Álgebra.

TCC apresentado ao curso Graduação em Licenciatura em Matemática do Centro de Educação e Saúde da Universidade Federal de Campina Grande em cumprimento às exigências do Componente Curricular Trabalho Acadêmico Orientado, para obtenção do grau de Graduada em Licenciatura em Matemática.

Orientadora: Maria de Jesus R. da Silva
Coorientador: Aluizio Freire da Silva Júnior

Cuité - PB
2015

Biblioteca Setorial do CES.

Julho de 2021.

Cuité - PB

FICHA CATALOGRÁFICA ELABORADA NA FONTE
Responsabilidade Jesiel Ferreira Gomes – CRB 15 – 256

S586c Silva, Maria Ioneris Oliveira.

Criptografia: aplicações de teoria dos números e álgebra. / Maria Ioneris Oliveira Silva – Cuité: CES, 2015.

89 fl.

Monografia (Curso de Licenciatura em Matemática) – Centro de Educação e Saúde / UFCG, 2015.

Orientadora: Maria de Jesus Rodrigues da Silva.
Coorientador: Aluizio Freire da Silva Júnior.

1. Criptografia. 2. Criptografia RSA. 3. Curvas elípticas. I. Título.

CDU 003.26

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE – UFCG
CENTRO DE EDUCAÇÃO E SAÚDE - CES
UNIDADE ACADÊMICA DE EDUCAÇÃO – UAE

Maria Ioneris Oliveira Silva

Criptografia: aplicações de teoria dos números e álgebra

Monografia de Trabalho de Conclusão de Curso submetida à banca examinadora como parte dos requisitos necessários a obtenção do grau de Graduação em Licenciatura em Matemática.

Trabalho de Conclusão de Curso (TCC) aprovado em 12 de fevereiro de 2015.

Banca Examinadora

Maria de Jesus Rodrigues da Silva
Profª. Maria de Jesus Rodrigues da Silva
(Orientadora)

Aluizio Freire da S. Júnior
Prof. Aluizio Freire da Silva Júnior
(Coorientador)

Vladimir Soares Catão
Prof. Vladimir Soares Catão

Aos meus pais,
José Lins de Oliveira (in memorian) e
Irene Costa Lima Oliveira e ao meu esposo,
Renato Oliveira Silva.

Agradecimentos

Primeiramente a Deus. por ter renovado as minhas forças a cada dia, fazendo com que os meus objetivos fossem alcançados. Sem Ele nada disso teria sido possível.

Ao meu esposo Renato, que de forma atenciosa e carinhosa me deu coragem e força em todos os momentos de dificuldade.

À toda minha família e, em especial, aos meus pais José Lins e Irene Costa. meu irmão Jerfison, meu avô Lourival e aos meus tios Severina Helena e Antônio. Pessoas estas que estiveram sempre ao meu lado nessa jornada, me dando todo o apoio possível.

À todos os meus amigos e, em particular, a Dayana Flávia, Elenilda Viana, Macielly Buriti, Tiago Queiroz, Aparecida Lima e Paula Francinete.

À professora Maria de Jesus, pela orientação, paciência e incentivo. Ter trabalhado com ela foi uma honra.

Ao professor Aluizio, pelas sugestões, críticas e conselhos. Eles foram de grande importância para o desenvolvimento deste trabalho.

Ao professor Vladimir Catão, pelas sugestões, apoio e por ter aceito o convite de participar da banca examinadora deste trabalho.

Ao professor supervisor do estágio Fernando Múcio, pelas sugestões e pela confiança em minha pessoa.

À professora Karina de Oliveira, pela ajuda prestada.

À todos os professores e, em especial, a professora Márcia Cristina, pelo grande incentivo, a professora Maria Gisélia pelas palavras de apoio e ao professor Jorge Alves de Sousa, por todos os elogios e criticas enriquecedoras.

Obrigada à todos!

"Nossa maior fraqueza está em desistir. O caminho mais certo de vencer é tentar mais uma vez."

Thomas Edison

Resumo

Neste trabalho discutiremos sobre dois tipos de sistemas criptográficos assimétricos: a criptografia RSA e a criptografia baseada em curvas elípticas. Inicialmente iremos apresentar alguns aspectos históricos que marcaram profundamente o desenvolvimento da criptografia, abordaremos as principais características dos tipos de criptografia existentes (simétrica e assimétrica) e em seguida, apresentaremos as principais ferramentas matemáticas, indispensáveis ao desenvolvimento e entendimento dos sistemas criptográficos supracitados. Além disso, iremos descrever os detalhes do funcionamento destes criptossistemas e entender porque eles são considerados seguros. Finalmente, faremos uma breve comparação entre eles.

Palavras-chave: Criptografia. Criptografia RSA. Curvas Elípticas.

Abstract

In this paper will discuss two types of asymmetric cryptosystems: RSA encryption and cryptography based on elliptic curves. Initially we will present some historical aspects that deeply marked the development of encryption, we discuss the main characteristics of the types of encryption (symmetric and asymmetric) and then present the main mathematical tools, indispensable for the development and understanding of the above cryptographic systems. In addition, we will describe the details of the operation of these cryptosystems and understand because they are considered safe. Finally, we will make a brief comparison between them.

Keywords: Encryption. RSA Encryption. Elliptic Curves.

Sumário

Introdução **10**

1 Contexto Histórico **12**

1.1 Conceitos 12

1.2 Tipos de Criptografia 13

1.2.1 Criptografia Simétrica 13

1.2.2 Criptografia Assimétrica 24

2 Conceitos Básicos **27**

2.1 Noções Básicas de Teoria dos Números 27

2.1.1 Indução 27

2.1.2 Divisibilidade 28

2.1.3 Teorema da Divisão 30

2.1.4 Máximo Divisor Comum 31

2.1.5 Mínimo Múltiplo Comum 36

2.1.6 Números Primos 37

2.1.7 Equações Diofantinas Lineares 40

2.1.8 Congruências 42

2.1.9 A Função φ de Euler 47

2.1.10 Congruência Linear 51

2.1.11 Aritmética das Classes Residuais 54

2.2 Testes de Primalidade 57

2.2.1 O Crivo de Eratóstenes 57

2.2.2 Testes de Lucas 59

2.3 Noções Básicas de Álgebra 61

2.3.1 Anel 61
2.3.2 Grupos 63

3 Criptografia **65**

3.1 Criptografia RSA 65
3.1.1 Pré-codificação 65
3.1.2 Codificação 67
3.1.3 Decodificação 68
3.1.4 Segurança do Método RSA 72
3.1.5 Assinaturas Digitais 72
3.2 Criptografia Baseada em Curvas Elípticas 74
3.2.1 Curvas Elípticas 74
3.2.2 Ponto no Infinito 75
3.2.3 Grupo de Pontos Sobre uma Curva Elíptica 76
3.2.4 Escolha do Corpo Finito 79
3.2.5 O Algoritmo 80
3.2.6 Criptografia RSA X Criptografia Baseada em Curvas Elípticas . 81
3.3 O Futuro da Segurança dos Sistemas Criptográficos Assimétricos 83

Conclusão **84**

Referências Bibliográficas **85**

Introdução

Desde a antiguidade nota-se a necessidade de se guardar e de se descobrir segredos, esse fato é perceptível em toda a história da humanidade. Durante milhares de anos, imperadores, líderes e militares necessitaram de comunicações eficientes para impedir possíveis ataques de invasores contra os seus povos. Devido ao medo de suas informações e segredos serem descobertos através da interceptação dessas mensagens pelos inimigos, viu-se a necessidade e a motivação de desenvolver técnicas que tornassem as mensagens enviadas incompreensíveis, de forma que apenas o destinatário pudesse ler e saber do que se tratava o seu conteúdo. O estudo dessas técnicas que podem fazer com que uma mensagem escrita com clareza torne-se incompreensível é denominado criptografia. De acordo com Marins e Pimentel (2011), este nome surgiu através da junção das palavras gregas kryptos (secreto) e graphen (escrita), significando escrita secreta.

De acordo com Marins e Pimentel (2011), o uso da criptografia inicialmente visava apenas a ocultação dos conteúdos de mensagens que deveriam ser enviadas com segurança, e necessitavam apenas de pequenos princípios de matemática. Com o passar do tempo, percebeu-se que a sua aplicação crescia demasiadamente, exigindo cada vez mais a criação de algoritmos e códigos bem elaborados e sofisticados, que pudessem garantir a segurança e a integridade de mensagens cada vez maiores. Em contrapartida, os decifradores de códigos inimigos tentavam analisar e compreender os algoritmos na tentativa de quebrar os códigos, para desvendar seus segredos e informações. Esta disputa entre criadores e decifradores de códigos enriqueceu e continua enriquecendo vários ramos da ciência.

O uso da criptografia consiste em enviar uma mensagem de forma que só o destinatário autorizado possa ter acesso às informações contidas na mesma, ou seja, ape-

nas o destinatário autorizado pode ler e compreender estas informações, e para isso é necessário que sejam cumpridos quatro requisitos básicos: confidencialidade, integridade, autenticação e não-recusa. De acordo com Cavalcante (2005), a confidencialidade garante que apenas os receptores autorizados poderão ter acesso aos conteúdos da mensagem, a integridade assegura que não haverá alterações na informação durante o seu processo de transporte, com a autenticação o remetente e o destinatário podem confirmar as identidades uns dos outros, a origem e o destino da informação e na não-recusa (obtida por meio das assinaturas digitais e certificados) o remetente pode assinar a mensagem de forma digital, definindo legalmente a responsabilidade. Cavalcante (2005) destaca ainda que, " [...] para tornar incompreensível a mensagem enviada define-se um protocolo aprovado pelo remetente e pelo destinatário, geralmente chamado de chave". Além disso, ele afirma que o nível de dificuldade para se conseguir decodificar uma mensagem pode ser identificado através da chave.

O tipo de chave que deve ser utilizado no processo de codificação e decodificação de mensagens depende exclusivamente do tipo de criptografia utilizada; existem dois tipos, a criptografia simétrica e a assimétrica. Neste trabalho, daremos enfoque a dois tipos de criptografia assimétrica: a criptografia RSA e a criptografia baseada em curvas elípticas.

No primeiro capítulo, abordaremos algumas características dos tipos de criptografia existentes (simétrica e assimétrica), bem como alguns de seus aspectos históricos e descreveremos de forma breve alguns métodos criptográficos utilizados na antiguidade.

No segundo capítulo, listaremos os conceitos básicos de Teoria dos Números e de Álgebra, necessários aos nossos estudos sobre os sistemas criptográficos RSA e baseados em curvas elípticas.

Finalmente, no terceiro capítulo, apresentaremos os sistemas criptográficos de que trata o nosso trabalho: a criptografia RSA e a criptografia baseada em curvas elípticas.

Capítulo 1

Contexto Histórico

Neste capítulo, apresentaremos inicialmente alguns conceitos relevantes acerca da Criptografia. Em seguida destacaremos as principais características dos tipos de criptografia existentes (simétrica e assimétrica), enfatizando alguns aspectos da história da criptografia e destacando os seus principais precursores.

1.1 Conceitos

Os seguintes conceitos são de fundamental importância para o desenvolver deste trabalho.

Criptografia: de acordo com Coutinho (2009), a criptografia é a área do conhecimento que estuda os métodos para codificar uma mensagem de forma que apenas o seu destinatário legítimo consiga interpretá-la.

Criptografar: para Mello (2006), criptografar significa transformar um texto claro em um texto cifrado.

Decriptografar: segundo Bergamaschi e Yonezawa (2014), decriptografar significa recuperar o conteúdo de uma mensagem criptografada.

Criptoanálise: Mello (2006), destaca que a criptoanálise é a análise da criptografia utilizada, que tem por objetivo detectar fragilidades e realizar o processo de decriptografia do texto cifrado sem o conhecimento da chave.

Criptologia: de acordo com Mello (2006), a criptologia é a ciência que estuda a criptografia e a criptoanálise.

Algoritmo: de acordo com Koliver e Tonet (2014), um algoritmo é uma sequência

finita de instruções, que é ordenada de forma lógica para resolver um determinado problema ou tarefa, isto é, é um caminho para a solução.

Sistema Criptográfico: segundo Mello (2006), um sistema criptográfico é um conjunto constituido por um algoritmo, a coleção de textos em claro, textos cifrados e chaves.

1.2 Tipos de Criptografia

1.2.1 Criptografia Simétrica

A criptografia simétrica consiste em transformar um texto claro em uma mensagem cifrada e incompreensível, através da definição de uma chave secreta, a qual será usada novamente para decifrar a mesma mensagem, tornando-a novamente simples e compreensível. A principal característica da criptografia simétrica é a utilização de apenas uma chave, tanto para codificar quanto para decodificar uma mensagem. Uma das principais vantagens de utilizar a criptografia simétrica é a sua rapidez, contudo vale ressaltar a sua principal desvantagem, a de que tanto o transmissor quanto o receptor da mensagem devem conhecer a chave, isso faz com que a criptografia simétrica seja menos eficiente no quesito segurança.

Os métodos de criptografia simétrica são divididos em dois ramos: as cifras de transposição e as de substituição.

Cifra de Transposição

Na transposição é utilizado o princípio de mudança de ordem, isto é, as letras da mensagem são rearranjadas no intuito de mudar o sentido da mesma, gerando um anagrama. Quando a mensagem é muito curta este método é considerado inseguro, devido ao fato de o número de rearranjos ser limitado. Em contrapartida, a cada vez que a mensagem vai se tornando mais extensa este método torna-se bastante seguro, pois à medida que o número de letras aumenta, o número de rearranjos também aumenta de forma demasiada. Para que a transposição seja eficaz é necessário que o rearranjo das letras seja feito de forma direta, e inicialmente escolhido e concordado tanto pelo emissor quanto pelo receptor da mensagem, de forma que continue indecifrável para o

inimigo. Conforme Singh (2007), o primeiro aparelho criptográfico militar, conhecido como citale espartano, criado no século V (a.C.) era baseado no método da transposição. O citale é formado por um bastão de madeira enrolado por uma tira de couro, como pode ser visto na figura 1.1. O emissor escreve a mensagem no citale de acordo com o seu comprimento e após ter feito isso desenrola a tira, verificando que nele contém uma porção de letras sem sentido, após esta verificação o emissor tem certeza que a mensagem foi misturada. Para decriptografar a mensagem, o receptor basta enrolar a tira de couro em um citale de mesmo diâmetro do qual a mesma mensagem foi originada.

Figura 1.1: Citale

Fonte: https://repple.ru/science/kak-sformirovalas-kriptografiya/

Cifra de Substituição

A cifra de substituição consiste em substituir cada letra em um determinado texto por letras diferentes. Este método é considerado de fácil implementação, pois a chave é facilmente definida pelo emissor. Uma das principais vantagens de utilizar esse método, é que de certa forma é fácil memorizar a chave, isso faz com que, caso a mensagem enviada seja interceptada pelo inimigo, o risco de se descobrir a chave seja diminuido. De acordo com Singh (2007), o primeiro documento que utilizou a cifra de substituição foi elaborado por Júlio César (100 a.C. - 44 a.C.) para fins militares nas Guerras da Gália. A cifra de substituição utilizada por Júlio César era considerada monoalfabética, este tipo de cifragem utiliza apenas um alfabeto para cifrar um texto claro.

Os estudiosos demoraram vários séculos até conseguirem quebrar a cifra de substituição monoalfabética, sendo os árabes os responsáveis por realizarem esta quebra. Eles foram os responsáveis pela invenção da criptoanálise, conhecida como a ciência que permite revelar os segredos de uma mensagem sem ter conhecimento da sua chave.

A invenção da criptoanálise aconteceu devido a vários fatores contribuintes, e um dos principais foi o crescimento dos estudos religiosos. Particularmente, os estudos religiosos revelaram uma das principais descobertas da criptoanálise, a análise de frequência. A análise de frequência foi responsável pelo processo de quebra da cifra de substituição monoalfabética, este método consiste em analisar a frequência com que determinadas letras e símbolos apareciam em um texto, à fim de relacionar estes padrões com algumas ocorrências frequentes do alfabeto cifrado. O tratado mais antigo sobre esta técnica foi escrito por um cientista do século IX, conhecido como al-Kindi "o filósofo dos árabes", este tratado revela de forma detalhada como utilizar a análise de frequência na leitura de textos que eram encriptados através da cifra de substituição monoalfabética (SINGH, 2007, p. 33).

De acordo com Singh (2007), entre os anos 800 e 1200, enquanto os árabes avançavam com os seus estudos e descobertas sobre a criptografia e a criptoanálise, os europeus ainda buscavam entender princípios básicos da criptografia. As únicas pessoas que estudavam e pesquisavam sobre a arte da escrita secreta na Europa eram os monges, devido influências religiosas, na busca de desvendar mistérios e significados encontrados na bíblia. Os monges através das suas descobertas desempenharam um papel fundamental para o avanço da criptografia ocidental, inclusive o primeiro livro que tratava do assunto veio a ser escrito no século XIII por um monge inglês conhecido como Roger Bacon (1214 - 1284).

Por volta do século XV a criptografia tornou-se cada vez mais estudada e utilizada no ocidente, sendo motivada pelo crescimento cultural, social, científico e político da época. Com isso, alguns personagens europeus tiveram destaque no estudo da criptografia e criptoanálise, como Giovani Soro considerado o primeiro grande criptoanalista europeu, nomeado secretário das cifras de Veneza em 1506; também destacou-se Philibert Barbou que era o criptoanalista do rei Francisco I da França e no século XVI a França deixou evidente a sua capacidade de quebrar códigos com a chegada de François Viète (1540 - 1603), experiente em quebrar códigos espanhóis.

Os criptógrafos dessa época ainda dependiam muito das cifras de substituição monoalfabéticas. Alguns países percebendo a fraqueza da cifra de substiuição monoalfabética, que vinha sendo frequentemente quebrada através da análise de frequência, começaram a pensar em novas formas de aprimorar e desenvolver cifras ainda melhores,

algo que pudesse ser imune ao poder da criptoanálise.

Com a ideia de desenvolver uma nova cifra, o italiano Leon Battista Alberti (1404 - 1472) teve destaque ao começar desenvolver a cifra de substituição polialfabética. Alberti propôs utilizar dois ou mais alfabetos cifrados, usados de forma alternada e desordenada de maneira que pudesse confundir os criptoanalistas caso utilizassem a análise de frequência. De acordo com Singh (2007), esta foi a primeira proposta de substituição polialfabética de que se tem notícia. Alberti também foi responsável por projetar e utilizar um dispositivo baseado na cifra de substituição polialfabética que facilitava bastante o processo criptográfico, este dispositivo ficou conhecido como Disco de Alberti. O Disco de Alberti é composto por dois discos concêntricos, um externo (fixo) e um interno (móvel). Ambos os discos eram divididos em 24 partes, sendo que eram dispostas letras e números em cada parte, como pode ser visto na figura 1.2. Para encriptar uma mensagem através do Disco de Alberti, é necessário determinar uma das letras do disco móvel como sendo a chave. Dessa forma, cada letra da mensagem irá representar a letra fixa acima dela, para decriptá-la basta fazer o processo inverso (MARINS; PIMENTEL, 2011, p. 3).

Figura 1.2: Disco de Alberti

Fonte: http://www.mateureka.it/notizie/grafometro-incertezza-dimensionale-disco-cifrante-le-nuove-acquisizione-del-mateureka.html

Singh (2007) destaca que, embora Alberti tenha descoberto uma cifra extraordinária, ele não conseguiu desenvolver as suas ideias e teorias. Assim, coube a um grupo de intelectuais desenvolver e aprimorar as ideias de Alberti. Nessa perspectiva, surgiu um abade alemão conhecido como Johannes Trithemius (1462 - 1516), o italiano Giovanni Porta (1535 - 1615) e por último o francês Blaise de Vigenère (1523 - 1596). Com base

nas idéias desenvolvidas por Alberti, Trithemius e Porta, Vigenère formou uma nova cifra, que ficou conhecida como a cifra de Vigenère e consiste em utilizar 26 alfabetos cifrados distintos para cifrar a mensagem. Dessa forma, esta cifra pode ser considerada imune a análise de frequência. O trabalho realizado por Vigenére contribuiu para que ele publicasse um tratado sobre a escrita secreta em 1586, intitulado *Traicté des Chiffres*. A cifra de Vigenère foi pouco utilizada devido ao trabalho árduo necessário que precisaria ser depositado na sua utilização.

No século XVII a cifra de substituição monoalfabética ainda era muito utilizada, a sua utilização dependia basicamente do nível de seriedade dos assuntos que viriam a ser tratados de forma sigilosa. Um exemplo disso, é que para fins militares este método é considerado frágil, devido a facilidade que os criptoanalistas tinham em quebrá-lo. Com isso, a busca incansável dos criptógrafos por uma melhoria no método continuava, e eles se negavam à utilizar a cifra de substituição polialfabética, pois consideravam esta complicada. Uma das possíveis soluções seria a *cifra de substituição homofônica* considerada também uma cifra de substituição monoalfabética. Essa cifra consiste em converter cada letra do texto a ser cifrado em um caractere qualquer de um conjunto de caracteres determinados, utilizando sempre o mesmo número de símbolos para a substituição.

Um dos exemplos mais ilustres de cifra monoalfabética melhorada foi a grande Cifra de Luís XIV, que foi inventada por Antoine e Bonaventure Rossignal, os quais eram muito habilidosos em quebrar cifras. De acordo com Singh (2007), após a morte dos Rossignal a grande cifra deixou de ser utilizada e seus detalhes exatos foram se perdendo ao longo dos tempos, sendo decifrada apenas no século XIX pelo comandante Étienne Bazeries (1846 - 1931), especialista do Departamento Criptográfico do Exército francês.

Por volta do século XVIII a criptoanálise estava começando a se industrializar, esse fato tornou-se evidente com os criptoanalistas governamentais trabalhando juntos nas conhecidas Câmaras Negras. Estas equipes de criptoanalistas tinham o intuito de decifrar várias cifras monoalfabéticas, das mais simples até as mais complexas. Cada potência européia tinha uma Câmara Negra, sendo que a mais famosa e eficiente delas encontrava-se em Viena.

Segundo Singh (2007), as Câmaras Negras conseguiram tornar todas as cifras

de substituição monoalfabéticas inseguras, com isso os criptógrafos da época se viram na obrigação de utilizar a cifra de Vigenère, que era mais complexa, mas oferecia um nível bem mais elevado de segurança. Além da evolução da criptoanálise, outros fatores como o desenvolvimento do telégrafo e a necessidade de proteger detalhes de telegramas enviados, encorajavam a mudança para cifragens ainda mais seguras. De acordo com Singh (2007), os telégrafos junto com o avanço das telecomunicações surgiram no século XIX, mas suas origens estão presentes desde 1753.

Com a criação do telégrafo eletromagnético na inglaterra, por Charles Wheatstone (1802 - 1875) e William Fothergill (1806 - 1879), da primeira linha telegráfica e do código Morse, na América, criados por Samuel Morse (1791 - 1872), percebeu-se a necessidade de criptografar as mensagens que seriam enviadas por telégrafo a fim de preservar a segurança dos conteúdos da mesma. Uma das formas indicadas para satisfazer esses requesitos foi utilizar a cifra polialfabética de Vigenère, pois esta era considerada indecifrável, por este motivo esta cifra ficou conhecida como "*le chiffre indéchiffrable*". Porém, por volta de 1854, o matemático inglês Charles Babbage (1791 - 1871), conseguiu quebrar a cifra de Vigenère. Embora esta descoberta fosse considerada tão importante para a criptoanálise, ainda permaneceu desconhecida porque não foi publicada. De acordo com Singh (2007), ela só veio a ser revelada no século XX, quando as anotações de Babagge foram estudadas e analisadas por alguns pesquisadores. Entretanto, a técnica da quebra da cifra de Vigenère foi descoberta de forma independente por Friedrich Wilhelm Kasiski (1805 - 1881), um oficial reformado do exército prussiano. A descoberta de Kasiski foi exposta em sua obra, de 1863, intitulada "Die geheimschriften und die Dechiffrir-kunst" (A escrita secreta e a arte de decifrá-la), desde então a técnica ficou conhecida como Teste de Kasiski e geralmente a contribuição de Babagge não recebe nenhum mérito.

No final do século XIX a criptografia encontrava-se em crise. Desde que a insegurança da cifra de Vigenère tinha tornado-se evidente com as descobertas de Babagge e Kasiski, os criptógrafos da época se dedicavam a buscar uma nova cifra que pudesse garantir a segurança do uso dos telégrafos por parte dos homens de negócios e dos militares.

Entre o final do século XIX e início do século XX, o físico italiano Guglielmo Marconi (1874 - 1937) inventou o rádio, uma evolução nas telecomunicações. Uma das

principais vantagens na utilização do rádio era que as mensagens poderiam ser enviadas entre dois pontos distintos sem a necessidade de utilizar um fio e isso fascinou os militares. Embora esta fosse uma das principais vantagens, nela existia uma fraqueza para utilizações militares, através das ondas do rádio as mensagens iriam alcançar também o inimigo além do destinatário. Com isso, e com o início da Primeira Guerra Mundial, via-se cada vez mais a necessidade de cifrar mensagens com segurança. Entretanto, durante a Primeira Guerra Mundial não foi obtido nenhum avanço criptográfico, pelo contrário os criptógrafos só obtiveram derrotas, pois cada cifra nova inventada, era imediatamente decifrada.

Segundo Singh (2007), uma das cifras mais famosas que teve destaque no final da primeira guerra mundial foi a cifra *ADFGVX*, utilizada pelos alemães. Esta cifra era considerada segura devido a sua complexidade, por ser uma mistura de cifra de transposição e substituição. No entanto, a mesma foi quebrada alguns meses após a sua criação pelo criptoanalista francês Georges Painvin (1886 - 1980), confirmando assim a eficiência dos criptoanalistas franceses da época. Essa eficiência foi estimulada pelo tratado *Cryptographie militaire*, escrito em 1883 pelo holandês Auguste Kerckhoffs, neste tratado eram fornecidos alguns príncipios da criptoanálise.

Próximo ao final da Primeira Guerra Mundial, os cientistas americanos descobriram que poderiam utilizar a Cifra de Vigenère (polialfabética) para servir como base para a elaboração de uma nova cifra mais eficiente e segura. Eles perceberam que mesmo se aumentassem o tamanho da chave ao utilizar a cifra de Vigenère, o texto cifrado era facilmente decifrável, isso se a chave fosse composta através de palavras que faziam sentido. Mas, se utilizassem uma chave que fosse construída através de palavras sem sentido, poderiam obter uma cifra inquebrável.

De acordo com Singh (2007), o conceito de chave aleatória (uma chave que era constituída de letras distribuídas ao acaso) foi introduzido pelo major Joseph Mauborgne (1881 - 1971), diretor da pesquisa criptográfica do exército dos Estados Unidos. A chave aleatória deveria ser utilizada uma única vez, junto com a cifra de Vigenère, no intuito de produzir um nível de segurança significante. Um sistema criptográfico deste tipo, ficou conhecido como *bloco de cifras de uma única vez*. A garantia da segurança do bloco de cifras de uma única vez deve-se ao fato da chave ser aleatória. A chave aleatória faz com que não exista padrões no texto cifrado, dificultando e tor-

nando impossível o trabalho dos criptoanalistas. Embora este sistema criptográfico fosse considerado eficiente e seguro, apresentava algumas limitações, como a enorme quantidade de tempo que necessitaria para poder fazer grandes quantidades de chaves aleatórias e a distribuição e gerenciamento dessas chaves. Isso fez com que este tipo de cifra não fosse muito utilizada.

Após a Primeira Guerra Mundial os criptógrafos foram obrigados a aliarem-se e a explorar a tecnologia que mais tinha evoluido, à fim de tentar construir um sistema criptográfico eficiente e prático que pudesse ser utilizado em conflitos e guerras futuras. No ano de 1918, o inventor alemão Arthur Scherbius (1878 - 1929) desenvolveu uma máquina criptográfica, baseada em cifradores rotativos e era como se fosse uma versão aprimorada do disco de Alberti (já descrito anteriormente), esta máquina ficou conhecida como *Enigma*, que pode ser vista na figura 1.3. A máquina enigma forneceu aos alemães uma enorme segurança quanto à criptografia no início da Segunda Guerra Mundial.

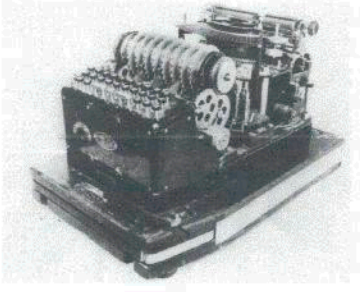

Figura 1.3: Enigma
Fonte: http://brasildelonge.com/tag/segunda-guerra/

Singh (2007), destaca que, alguns anos após o fim da Primeira Guerra Mundial, os criptoanalistas britânicos, americanos, franceses e poloneses continuaram a interceptar e analisar as comunicações alemãs. Mas, em 1926 eles começaram a ficar confusos com as novas mensagens que interceptavam, foi quando os alemães começaram a utilizar a poderosa *Enigma*. Desde então, os criptoanalistas começaram uma busca incansável por falhas e fraquezas na máquina Enigma que pudesse auxiliá-los a encontrar um meio de derrotá-la. Os criptoanalistas poloneses eram os mais persistentes, pois, queriam manter a independência que havia sido conquistada após a Primeira Guerra Mundial. Com isso, eles fundaram um departamento de cifras conhecido como *Biuro Szyfrów*,

comandado pelo capitão Maksymilian Ciezki (1898 - 1951). Ciezki tinha conhecimento da versão comercial da Enigma, mas ele não retirou bons proveitos disso, pois a versão comercial era diferente da versão militar. Contudo, o alemão Hans-Thilo Schmidt (1888 - 1943), contribuiu de forma significativa para a quebra da cifra Enigma. Schimdt havia ficado descontente com sua nação, devido à alguns fatos que ocorreram após a Primeira Guerra Mundial, e aproveitou a primeira oportunidade que teve para descarregar os seus ressentimentos. Ele vendeu e repassou várias informações secretas sobre a Enigma para países estrangeiros.

Segundo Singh (2007), no ano de 1931, Schimidt encontrou-se com um agente secreto francês, conhecido como Rex, e por uma quantia notória deixou que Rex fotografasse várias informações sobre o funcionamento da máquina Enigma. Com essas informações, os franceses poderiam criar uma réplica perfeita da máquina utilizada pelos alemães. Entretanto, devido ao excesso de confiança e a falta de motivação adquiridos após a Primeira Guerra Mundial , os franceses não estavam prontos para prosseguir com as pesquisas, e entregaram as fotografias para seus aliados poloneses prosseguirem com os trabalhos. Como a Enigma era uma cifra mecânica, o Biuro Szyfrów recrutou alguns matemáticos poloneses, com a ideia de que eles poderiam ter uma maior chance de quebrá-la. Dentre estes matemáticos, destacou-se Marian Rejewski (1905 - 1980), que encontrou dentro do Biuro Szyfrów a sua verdadeira vocação (a quebra de cifras). Rejewski iniciou seu trabalho dentro do Biuro szyfrów quebrando uma série de cifras tradicionais, e logo após começou a enfrentar o desafio de quebrar a cifra Enigma. Com algumas informações sobre a Enigma em mãos (que foram transmitidas por Schimdt aos franceses) Rejewski trabalhou incansavelmente e conseguiu montar uma tabela de relações para a chave diária analisando a ocorrência de padrões, isto era feito tendo como base a disposição do quadro de tomadas, da disposição dos misturadores e de suas orientações. Algum tempo depois Rejewski aprimorou as suas tabelas de relacionamento; projetando uma versão mecanizada das mesmas, esta versão mecanizada foi projetada com base na máquina Enigma.

Singh (2007), ainda destaca que, as habilidades de Rejewski foram suficientes até 1938, quando os criptógrafos alemães intensificaram o nível de segurança da Enigma. Os poloneses quando perceberam que não dispunham de recursos suficientes para ultrapassar os novos limites de segurança da enigma, repassaram as ideias e projetos de

Rejewski para os britânicos e para os franceses, para eles tentarem dar continuidade. De certa forma, a descoberta de Rejewski incentivou seus aliados a continuarem com o seu trabalho, pois ele conseguiu mostrar que, diferente do que se pensava, a Enigma não era perfeita. Com isso, vários estudiosos foram recrutados para Bletchley Park, em Buckinghamshire onde era localizada a sede da Escola de Cifras e Códigos do governo (GC & CS), uma organização para a quebra de códigos que contava com uma equipe maior do que a do Biuro Szyfrów.

Em 1939, os estudiosos de Bletchley aprenderam as particularidades da cifra Enigma, o que colaborou para que eles dominassem as técnicas polonesas e dessem um grande avanço em suas pesquisas, inventando suas próprias teorias para encontrar as chaves diárias da cifra Enigma. Vários criptoanalistas de Bletchley conseguiram provocar avanços significativos para o desenvolvimento de sua ciência. Entretanto, o britânico Alan Turing (1912 - 1954) merece destaque especial, pois foi ele quem identificou a principal falha da Enigma e a explorou. Turing também foi responsável por projetar uma máquina prática de decifrar mensagens encriptadas através da Enigma, esta máquina recebeu o nome de *Bomba*. O projeto de Turing foi finalizado em 1940, e foi muito útil para agilizar o processo de quebra da cifra Enigma.

Os estudiosos de Bletchley Park não foram responsáveis apenas por decifrar a Enigma alemã, mas também coube a eles decifrar mensagens italianas e japonesas. De acordo com Singh (2007), as informações obtidas dessas fontes receberam o nome de Ultra. Os arquivos de dados da Ultra fizeram com que os aliados recebessem vantagens enormes no decorrer da Segunda Guerra Mundial. A Ultra também foi considerada uma das principais responsáveis em antecipar o fim da Segunda Guerra Mundial de 1948 para 1945.

Após o fim da Segunda Guerra Mundial, a Escola de Códigos de Bletchley Park foi fechada, os estudiosos que contribuiram para a criação da Ultra foram dispersos e as descobertas realizadas por eles permaneceram em sigilo até o início da década de 1970.

Segundo Singh (2007), além da cifra Enigma fazer parte das comunicações alemães durante a Segunda Guerra Mundial, outra cifra também teve destaque neste período, a cifra Lorenz. Esta era utilizada para codificar as mensagens trocadas entre Hitler e os seus generais. A codificação das mensagens era feita pela máquina Lorenz SZ40, a

cifra Lorenz era considerada muito forte e mais poderosa do que a cifra Enigma.

Baseado nas ideias de Turing, um matemático de Bletchley, conhecido como Max Newman (1897 - 1984), conseguiu projetar uma máquina capaz de quebrar a cifra Lorenz, esta máquina ficou conhecida como *Colossus*. A Colossus tinha a característica de ser rápida e programável e esta última característica fez com que fosse considerada a precursora do computador digital.

Após o fim da Segunda Guerra Mundial, a tecnologia dos computadores continuou sendo utilizada, tanto pelos criptoanalistas quanto pelos criptógrafos. Durante o pós-guerra o computador teve fundamental importância na disputa entre codificadores e decodificadores. Mesmo utilizando a tecnologia computacional, a cifragem ainda permaneceu por muito tempo utilizando as técnicas de substituição e de transposição na sua estrutura, ou seja, príncipios já conhecidos da criptografia simétrica.

De início, os computadores eram utilizados apenas pelo governo e pelos militares. Entretanto, as várias descobertas científicas e os avanços tecnológicos fizeram com que os computadores e a cifragem por computador se tornassem cada vez mais acessíveis. Essa acessibilidade tornou-se mais ampla durante a década de 1960, pois, os computadores tornaram-se cada vez mais poderosos e, em contrapartida mais baratos. Com isso, os criptógrafos viam-se diante de um problema, a questão da padronização.

Em 1973, o National Bureau of Standards americano solicitou uma forma padrão de cifragens. Um dos candidatos a padrão, era um algoritmo de cifragem muito utilizado, desenvolvido pelo alemão Harst Feistel (1915 - 1990) que se mudara para os Estados Unidos no ano de 1934, este algoritmo era conhecido como Lucifer. Singh (2007) afirma que, o trabalho de Feistel foi reprimido algumas vezes pela Agência de Segurança Nacional (*NSA*), porém ele conseguiu desenvolvê-lo mais tarde (precisamente no início da década de 70), no laboratório Thomas J. Watson da IBM (próximo à Nova York). O sistema de cifragem Lucifer era considerado muito poderoso e foi adotado por várias organizações. No entanto, a NSA resistia a aceitá-lo como padrão americano, pois ele era um sistema de cifragem que era superior ao seu processo da quebra de códigos. Visto que, mais cedo ou mais tarde o sistema Lucifer viria a se tornar um padrão de cifragens, a NSA propôs uma alteração no mesmo, de modo que o seu número de chaves fosse limitado. Dessa forma, a decifração do Lucifer estaria ao alcance da NSA. A cifra Lucifer com a alteração descrita anteriormente, foi oficialmente

adotada em 23 de novembro de 1976 e designada como *DES - Data Encryption Standad*. Com isso, as empresas foram encorajadas a utilizarem a criptografia para garantir e manter a sua segurança e o problema da padronização foi resolvido. Contudo, um novo e grande problema surgia, a questão da *distribuição de chaves*.

Os estudiosos Martin Hellman, Whitfield Diffie e Ralph Merkle se uniram no intutito de solucionar o problema da distribuição de chaves, e no ano de 1976 abordaram publicamente e teoricamente uma forma de solucionar tal problema. De acordo com Marins e Pimentel (2011), a possível solução consistia em um modelo criptográfico, onde seria possível trocar mensagens secretas sem que fosse necessário compartilhar as chaves. Para Singh (2007) além de ter contribuido com as ideias e trabalhos de Hellman e Merkle, Diffie descobre em 1975 um novo tipo de cifra, que incluia a chamada chave assimétrica ou chave pública (vale ressaltar que todas as técnicas de encriptação citadas até agora foram simétricas).

1.2.2 Criptografia Assimétrica

Segundo Cavalcante (2005), a criptografia de chave pública, também conhecida como criptografia assimétrica consiste em utilizar um par de chaves, sendo que uma é pública (todos conhecem) e a outra privada (apenas o detentor conhece). A chave pública serve para criptografar o texto ou mensagem e a chave privada serve para decriptografar.

A criptografia assimétrica é considerada mais segura do que a criptografia simétrica, pois na criptografia simétrica a mensagem é criptografada com uma chave que tem que ser repassada para o receptor da mesma, enquanto que na criptografia assimétrica é necessário apenas fornecer a chave pública que é responsável por criptografar a mensagem que só poderá ser lida por quem possuir a chave privada.

De acordo com Marins e Pimentel (2011), a ideia de Martin Hellman, Whitfield Diffie e Ralph Merkle citada anteriormente, foi concretizada por Ronald Rivest, Adi Shamir e Leonard Adleman, no ano de 1977, eles inventaram um sistema de criptografia de chave pública ou assimétrica, que ficou conhecido como *RSA*. O sistema RSA consiste em utilizar duas chaves, uma pública e uma privada. Qualquer pessoa que deseja enviar uma mensagem para outra, pode procurar a chave pública desta pessoa

em uma lista e criptografar essa mensagem. Quando a mensagem criptografada chegar ao destinatário, será decriptografada com a chave privada (que só ele conhece).

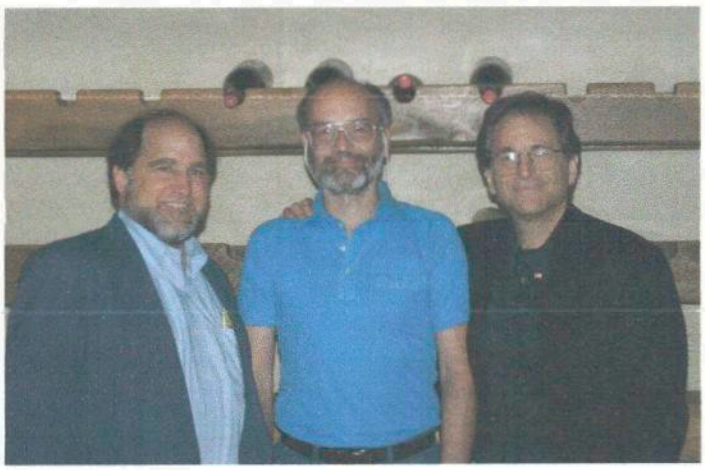

Figura 1.4: Os criadores do sistema RSA.
Fonte: http://www.usc.edu/dept/molecular-science/RSA-2003.htm

Este sistema criptográfico é fortemente utilizado em comércios eletrônicos na internet. A dificuldade de se quebrar o RSA está atrelada ao fato de que não existem algoritmos computacionais eficientes para a decomposição de números inteiros (grandes) em fatores primos. Hoje, sabe-se que a fatoração de números inteiros (muito extensos), necessitaria de uma capacidade computacional ainda não existente. Um exemplo disso, é que uma empresa (conhecida como RSA Laboratories) realiza alguns desafios acerca da fatoração de inteiros semiprimos (produtos de dois primos distintos), sendo que estes inteiros são numerados de acordo com o seu tamanho. Segundo Figueiredo (2010), o primeiro desafio proposto pela RSA Laboratories foi o RSA-100 (inteiro com 100 dígitos decimais), o qual foi fatorado em poucos dias. Por outro lado, o último inteiro fatorado foi o RSA-200 (com 200 dígitos decimais), em maio de 2005. Figueiredo (2010) destaca ainda que, o maior inteiro na lista de desafios realizados é um inteiro com 617 dígitos decimais (oferece-se um prêmio de 200 mil dólares para quem conseguir fatorá-lo). Este exemplo ilustra a confiança existente acerca do problema da fatoração de inteiros. No entanto, o avanço da tecnologia faz com que cada vez mais o poder computacional cresça, e junto com este crescimento vem a preocupação em relação à segurança do sistema criptográfico RSA. Com isso, outros tipos de sistemas criptográficos vem sendo estudados, dentre estes podemos destacar os criptossistemas

baseados em curvas elípticas.

A utilização de criptossistemas de chave-pública baseados em curvas elípticas foi proposta inicialmente no ano de 1985, por Neal Koblitz e Victor Miller, de forma independente. A ideia base desse sistema, é construir um grupo de pontos de uma curva elíptica de forma que seja inviável e praticamente impossível solucionar o problema do logaritmo discreto sobre esses pontos. Este problema é considerado a base dos sistemas criptográficos baseados nestas curvas.

Para descrevermos melhor os sistemas criptográfico baseados em curvas elípticas e o RSA, precisaremos de alguns conceitos da Teoria dos Números e da Álgebra, que serão abordados no capítulo seguinte.

Capítulo 2

Conceitos Básicos

Neste capítulo, apresentaremos os conceitos básicos necessários para a compreensão dos sistemas de *criptografia RSA* e de *criptografia baseada em curvas elípticas*, que são o foco de nosso trabalho.

2.1 Noções Básicas de Teoria dos Números

Para os tópicos apresentados nesta seção, consideraremos os seguintes conjuntos:

1. Conjunto dos *números naturais* ($\mathbb{N}$):

$$\mathbb{N} = \{1, 2, 3, \ldots\}.$$

2. Conjunto dos *números inteiros* ($\mathbb{Z}$):

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

3. Conjunto dos *números inteiros positivos ou negativos* ($\mathbb{Z}^*$):

$$\mathbb{Z}^* = \{\ldots, -2, -1, 1, 2, \ldots\}.$$

2.1.1 Indução

O Princípio de Indução Finita e o Princípio da Boa Ordem são importantes ferramentas matemáticas utilizadas para demonstrar propriedades referentes a números inteiros. Apresentemos esses resultados.

1. ***Primeira Forma do Princípio de Indução Finita***

   Seja A um conjunto de números inteiros positivos tal que:

   $i)$ $1 \in A$;

   $ii)$ $k \in A \Longrightarrow k+1 \in A$.

   Então A contém todos os números inteiros positivos.

2. ***Segunda Forma do Princípio de Indução Finita***

   Seja A um conjunto de números inteiros positivos tal que:

   $i)$ $1 \in A$;

   $ii)$ $1, 2, \ldots, k \in A \Longrightarrow k+1 \in A$.

   Então A contém todos os números inteiros positivos.

3. ***Princípio da Boa Ordem***

   Todo conjunto não vazio de números inteiros positivos contém um elemento mínimo.

   Para mais detalhes sobre esses princípios, consultar [32].

2.1.2 Divisibilidade

Definição 2.1 *Dados a, $b \in \mathbb{Z}$, com $a \neq 0$, dizemos que a divide b, e denotamos $a|b$, se existir $c \in \mathbb{Z}$ tal que $b = ac$. Caso a não divida b, denotamos $a \nmid b$.*

Da definição acima, temos que $a|a$, $1|a$ e $a|0$, para todo $a \in \mathbb{Z}$, pois $a = 1 \cdot a$ e $0 = 0 \cdot a$. Em particular, $0|0$. Por outro lado, se a é um inteiro não nulo, então $0 \nmid a$, pois não existe $c \in \mathbb{Z}$ tal que $a = 0 \cdot c$.

A principais propriedades de divisibilidade encontram-se nas proposições seguintes.

Proposição 2.1 *Sejam $a, b, c \in \mathbb{Z}$. Tem-se que:*

a) $b|c \Rightarrow ab|ac$;

b) $a|b$ *e* $c|d \Rightarrow ac|bd$;

c) $ab|ac$ *e* $a \neq 0 \Rightarrow b|c$;

d) $a|b$ *e* $b \neq 0 \Rightarrow |a| \leqslant |b|$;

e) $a|b$ *e* $b|a \Rightarrow |a| = |b|$;

f) $a|b$ *e* $a \neq 0 \Rightarrow (b/a)\,|b$.

Demonstração: *a*) Como $b|c$, existe $k \in \mathbb{Z}$ tal que $c = bk$. Daí, temos que $ac = (ab)k$ e, portanto, $ab|ac$.

b) Como $a|b$ e $c|d$, existem $k_1, k_2 \in \mathbb{Z}$ tais que $b = ak_1$ e $d = ck_2$. Logo, $bd = (ac)k_1k_2$. Fazendo $k = k_1k_2 \in \mathbb{Z}$, obtemos $bd = (ac)k$, com $k \in \mathbb{Z}$. Donde, $ac|bd$.

c) Se $ab|ac$, temos $ac = (ab)k = a(bk)$. Daí, como $a \neq 0$, obtemos $c = bk$, ou seja, $b|c$.

d) Sendo $b \neq 0$, devemos ter necessariamente $a \neq 0$. Como $a|b$, existe $c \in \mathbb{Z}$ tal que $b = ac$, com $c \neq 0$. Note que $|c| \geqslant 1$. Com isso, temos $|b| = |ac| = |a| \cdot |c| \geqslant |a| \cdot 1$. Logo, $|a| \leqslant |b|$.

e) Se $b = 0$, devemos ter necessariamente $a = 0$ e neste caso, $|a| = |b|$. Por outro lado, se $a|b$ e $b|a$, com $b \neq 0$, então $a \neq 0$ e pelo item (d) obtemos $|a| \leqslant |b|$ e $|b| \leqslant |a|$. Portanto, $|a| = |b|$.

f) Como $a|b$, temos $b = ak$, para algum $k \in \mathbb{Z}$. Logo, $k|b$ e, como $a \neq 0$, temos $k = b/a$. Donde, $(b/a)\,|b$. □

Proposição 2.2 *Se $a, b, c \in \mathbb{Z}$ são tais que $a|(b \pm c)$, então $a|b$ se, e somente se, $a|c$.*

Demonstração: Suponha que $a|(b+c)$ e $a|b$. Neste caso, existem $k_1, k_2 \in \mathbb{Z}$ tais que $b + c = ak_1$ e $b = ak_2$. Logo,

$$ak_2 + c = ak_1 \Longrightarrow c = a(k_1 - k_2),$$

de onde segue que $a|c$. Agora, suponha que $a|(b-c)$ e $a|b$. Pelo caso anterior, temos que $a| - c$. Logo, existe $k_3 \in \mathbb{Z}$ tal que $-c = ak_3$ e, daí, $c = a(-k_3)$, ou seja, $a|c$. A recíproca é análoga. □

Proposição 2.3 *Se a, b e c são inteiros tais que $a|b$ e $b|c$, então $a|c$.*

Demonstração: Como $a|b$ e $b|c$, existem $k_1, k_2 \in \mathbb{Z}$ tais que $b = ak_1$ e $c = bk_2$. Logo,

$$c = bk_2 = a(k_1k_2),$$

ou seja, $a|c$. □

Proposição 2.4 *Se a, b e c são inteiros tais que $c|a$ e $c|b$, então $c|(ma+nb)$, quaisquer que sejam $m, n \in \mathbb{Z}$.*

Demonstração: Como $c|a$ e $c|b$, existem $k_1, k_2 \in \mathbb{Z}$ tais que $a = ck_1$ e $b = ck_2$. Com isto, temos que

$$ma + nb = mck_1 + nck_2 = (mk_1 + nk_2)c,$$

ou seja, $c|(ma + nb)$. □

2.1.3 Teorema da Divisão

Teorema 2.1 (Divisão Euclidiana) *Dados $a, b \in \mathbb{Z}$, com $b > 0$, existe um único par de inteiros q e r tais que*

$$a = bq + r,$$

onde $0 \leqslant r < b$.

Demonstração: Defina o seguinte conjunto

$$S = \{n \in \mathbb{N} | \, nb > a, a \in \mathbb{Z} \text{ e } b \in \mathbb{N}\}.$$

Note que $S \neq \emptyset$. De fato, sejam $a, b \in \mathbb{Z}$, com $b > 0$, e n um inteiro tal que $n = |a| + 1$. Como $b \geqslant 1$, temos

$$nb \geqslant n = |a| + 1 > a.$$

Logo, $a \in S$. Sendo $S \subset \mathbb{N}$ não vazio, segue-se pelo *Princípio da Boa Ordem* que S possui um menor elemento p, de modo que $p \geqslant 1$. Daí, existe $q \in \mathbb{N} \cup \{0\}$ tal que, $p = q + 1$. Observe que $q \notin S$. Assim,

$$qb \leqslant a < pb = (q + 1)b = bq + b \Longrightarrow 0 \leqslant a - bq < b.$$

Fazendo $r = a - bq$, obtemos

$$a = bq + r \quad \text{e} \quad 0 \leqslant r < b.$$

Agora, sejam $q_1, r_1 \in \mathbb{Z}$ tais que

$$a = bq_1 + r_1,$$

onde $0 \leqslant r_1 < b$. Daí, temos

$$bq + r = bq_1 + r_1 \Longrightarrow b(q - q_1) = r_1 - r.$$

Suponha $r > r_1$. Neste caso, $r_1 - r < 0$ e, como $b > 0$, temos $q - q_1 < 0$. Logo, $q_1 - q > 0$, ou seja, $q_1 - q \geqslant 1$. Com isto, temos que

$$r = r_1 - b(q - q_1) = r_1 + b(q_1 - q) \geqslant b.$$

Donde, $r \geqslant b$, o que é uma contradição. Analogamente, prova-se que $r_1 > r$ também não pode ocorrer. Portanto, $r = r_1$ e, consequentemente, $q = q_1$. □

Exemplo 2.1 *Se o resto da divisão euclidiana de um inteiro m por 8 é 5, qual é o resto da divisão de m por 4?*
Note que $m = 8q + 5$, para algum $q \in \mathbb{Z}$. Logo,

$$m = 4(2q + 1) + 1$$

e, portanto, $r = 1$ é o resto da divisão de m por 4.

2.1.4 Máximo Divisor Comum

Dados dois inteiros a e b, não simultaneamente nulos, dizemos que $d \in \mathbb{Z}$ é um *divisor comum* de a e b se $d|a$ e $d|b$. Sendo assim, como 1 divide qualquer número inteiro, segue-se que 1 é divisor comum de quaisquer dois inteiros a e b.

Definição 2.2 (mdc) *Sejam $a, b \in \mathbb{Z}$, não simultaneamente nulos. Um máximo divisor comum de a e b, denotado por $mdc(a, b)$, é um inteiro d tal que:*
i) $d|a$ e $d|b$;
ii) $c|a$ e $c|b \Rightarrow c|d$.

A primeira condição diz que d é divisor comum de a e b, enquanto que a segunda condição assegura que d é o maior de todos os divisores de a e b. Além disso, o máximo divisor comum, quando existe, é único. Com efeito, se $d = \text{mdc}(a, b)$ e $d' = \text{mdc}(a, b)$, então $d|d'$ e $d'|d$. Logo, $d \leqslant |d| \leqslant d'$ e $d' \leqslant |d'| \leqslant d$. Portanto, $d = d'$.

A existência do máximo divisor comum de dois inteiros não simultaneamente nulos é garantida pelo *Algoritmo de Euclides*, que apresentaremos mais adiante. Por hora, assumiremos esta existência.

Observação 2.1 *Note que, se a e b são inteiros, não simultaneamente nulos, então*

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

Sendo assim, para calcular o máximo divisor comum de dois números inteiros, podemos considerá-los não negativos.

A seguir apresentaremos alguns resultados importantes sobre máximo divisor comum.

Proposição 2.5 *Dados $a, b \in \mathbb{Z}$, não simultaneamente nulos, tem-se que*

$$a|b \Longleftrightarrow mdc(a,b) = |a|.$$

Demonstração: De fato, se $a|b$, então, $|a||b$, isto é, $|a|$ é um divisor comum de a e b. Além disso, se c é um divisor comum de a e b, então $c \leqslant |c| \leqslant |a|$. Donde, $\text{mdc}\,(a,b) = |a|$. Reciprocamente, se $\text{mdc}\,(a,b) = |a|$, então, $|a||b$. Como $a||a|$, segue da proposição (2.3) que $a|b$. □

Proposição 2.6 *Sejam $a, b \in \mathbb{Z}$, com $b > 0$. Se $a = bq + r$, onde $0 \leqslant r < b$, então*

$$d = mdc(a,b) \Longleftrightarrow d = mdc(b,r).$$

Demonstração: ($\Rightarrow$) Se $d = mdc(a,b)$, então $d|a$ e $d|b$ e usando a proposição (2.4) segue que $d|(a - bq)$, assim $d|b$ e $d|r$. Além disso, se $c|b$ e $c|r$, então $c|(bq + r)$. Logo, $c|a$ e $c|b$ e, consequentemente, $c|d$. Portanto, $d = \text{mdc}\,(b,r)$.
($\Leftarrow$) Se $d = \text{mdc}\,(b,r)$, então, como $d|b$ e $d|r$, segue-se que $d|b$ e $d|bq + r$, ou seja, $d|b$ e $d|a$. Por fim, se $c|a$ e $c|b$, então $c|b$ e $c|(a - bq)$, ou seja, $c|b$ e $c|r$. Logo, $c|d$ e, portanto, $d = \text{mdc}\,(a,b)$. □

Teorema 2.2 *Se a e b são números inteiros, não simultaneamente nulos, então existem $x_0, y_0 \in \mathbb{Z}$ tais que, $mdc\,(a,b) = ax_0 + by_0$.*

Demonstração: Defina o seguinte conjunto

$$A = \{ax + by;\ x, y \in \mathbb{Z}\}.$$

Note que $A \neq \emptyset$, pois $a^2 + b^2 = a \cdot a + b \cdot b \in A$. Além disso, como $a^2 + b^2 > 0$, segue-se que A possui elementos positivos, dentre os quais existe um menor elemento, digamos d, em vista do *Princípio da Boa Ordem*. Como $d \in A$, existem $x_0, y_0 \in \mathbb{Z}$ tais que,

$$d = ax_0 + by_0.$$

Sendo $d > 0$, então pelo teorema (2.1) existem únicos $q, r \in \mathbb{Z}$ tais que,

$$a = dq + r,$$

com $0 \leqslant r < d$. Com isto, temos

$$a = (ax_0 + by_0)q + r = ax_0q + by_0q + r \Longrightarrow r = a(1 - x_0q) + b(-y_0q) \in A.$$

Observe que $r = 0$, pois, se fosse $r > 0$ teríamos um elemento positivo de A menor do que d, um absurdo. Sendo assim, $a = dq$, e, portanto, $d|a$. De forma análoga, obtém-se que $d|b$. Logo, d é um divisor comum de a e b.

Agora, considere $c \in \mathbb{Z}$ tal que, $c|a$ e $c|b$. Neste caso, existem x_1 e $x_2 \in \mathbb{Z}$ tais que, $a = cx_1$ e $b = cx_2$. Logo,

$$d = (cx_1)x_0 + (cx_2)y_0 = c(x_1x_0 + x_2y_0) \Longrightarrow c|d.$$

Assim, $d = \text{mdc}\,(a, b)$. Portanto,

$$\text{mdc}\,(a, b) = ax_0 + by_0.$$

□

Observe que na demonstração do teorema acima, provamos que o máximo divisor comum de a e b é o menor inteiro positivo que é combinação linear de a e b, ou seja,

$$\text{mdc}\,(a, b) = \min\{ax_0 + by_0;\ x_0, y_0 \in \mathbb{Z}\} \cap \mathbb{N}.$$

Proposição 2.7 *Para todo inteiro positivo n tem-se que $mdc\,(na, nb) = n\,mdc\,(a, b)$*

Demonstração: De fato, pelo teorema (2.2), temos que

$$\begin{aligned} \text{mdc}\,(na, nb) &= \min\{nax_0 + nby_0;\ x_0, y_0 \in \mathbb{Z}\} \cap \mathbb{N} \\ &= n \min\{ax_0 + by_0;\ x_0, y_0 \in \mathbb{Z}\} \cap \mathbb{N} \\ &= n\text{mdc}\,(a, b)\,. \end{aligned}$$

Logo, $\text{mdc}\,(na, nb) = n\text{mdc}\,(a, b)$. □

Corolário 2.1 *Sejam $a, b \in \mathbb{Z}$, não simultaneamente nulos. Se $d = mdc\,(a, b)$, então*

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

Quando $\text{mdc}(a,b) = 1$, dizemos que a e b são *primos entre si* ou *coprimos*. Em outras palavras, dizer que a e b são coprimos significa dizer que 1 é o único divisor comum de a e b.

A proposição seguinte é de grande utilidade e será empregada na demonstração de vários resultados aqui apresentados.

Proposição 2.8 *Se $a|bc$ e $mdc(a,b) = 1$, então $a|c$.*

Demonstração: De fato, pelo teorema (2.2) existem $x_0, y_0 \in \mathbb{Z}$ tais que, $x_0a + y_0b = 1$. Daí,

$$x_0ac + y_0bc = c.$$

Como $a|bc$ e $a|ac$, segue-se da igualdade acima que $a|c$. □

Finalmente, o resultado que garante a existência do máximo divisor comum.

Teorema 2.3 (Algoritmo de Euclides) *Sejam $r_0 = a$ e $r_1 = b$ inteiros não negativos, com $b \neq 0$. Se aplicarmos o teorema da Divisão Euclidiana sucessivas vezes para obter*

$$r_i = q_{i+1}r_{i+1} + r_{i+2},\ 0 \leqslant r_{i+2} < r_{i+1},$$

para $i = 1, \ldots, n-1$ e $r_{n+1} = 0$, então $mdc(a,b) = r_n$, onde r_n denota o último resto não nulo.

Demonstração: Pela *divisão euclidiana* de r_0 por r_1, temos que $r_0 = q_1r_1 + r_2$, onde $q_1, r_2 \in \mathbb{Z}$ e $0 \leqslant r_2 < r_1$. Podemos ter $r_2 = 0$ ou $0 < r_2 < r_1$. No primeiro caso, $r_1|r_0$ e, portanto,

$$r_1 = \text{mdc}(r_0, r_1) = \text{mdc}(a,b).$$

Por outro lado, se $0 < r_2 < r_1$, então, pela *divisão euclidiana*, obtemos $r_1 = q_2r_2 + r_3$, onde $q_2, r_3 \in \mathbb{Z}$ e $0 \leqslant r_3 < r_2$. Se $r_3 = 0$, então $r_2|r_1$. Logo, da proposição (2.6), segue-se que

$$r_2 = \text{mdc}(r_1, r_2) = \text{mdc}(r_0, r_1) = \text{mdc}(a,b).$$

Caso contrário, se $0 < r_3 < r_2$, realizamos o procedimento anterior. Note que este procedimento não pode continuar indefinidamente, pois, caso contrário, teríamos um conjunto de naturais $\{r_1 = b, r_2, r_3, \ldots\} \neq \emptyset$ que não possui elemento mínimo, o que

é uma contradição, em vista do *Princípio da Boa Ordem*. Sendo assim, deve existir algum $n \in \mathbb{N}$ tal que $r_n | r_{n-1}$ e, consequentemente, $r_{n+1} = 0$. Com isto temos

$$\begin{aligned} r_0 &= q_1 r_1 + r_2,\ 0 < r_2 < r_1 \\ r_1 &= q_2 r_2 + r_3,\ 0 < r_3 < r_2 \\ &\vdots \\ r_{n-1} &= q_n r_n 1 + r_{n+1},\ r_{n+1} = 0 \end{aligned}$$

Daí, aplicando a proposição (2.6), obtemos

$$r_n = \text{mdc}\,(r_{n-1}, r_n) = \text{mdc}\,(r_{n-2}, r_{n-1}) = \cdots = \text{mdc}\,(r_2, r_1) = \text{mdc}\,(r_1, r_0) = \text{mdc}\,(a, b)\,.$$

Portanto, $\text{mdc}\,(a, b) = r_n$, onde r_n é o último resto não nulo da sequência de divisões enunciadas. □

Observe que, além de assegurar a existência, o *Algoritmo de Euclides* mostra como obter o máximo divisor comum de dois inteiros, não simultaneamente nulos.

Exemplo 2.2 *Vamos obter o máximo divisor comum de* 30 *e* 144.

Solução: Note que

$$\begin{aligned} 144 &= 30 \cdot 4 + 24; \\ 30 &= 24 \cdot 1 + 6; \\ 24 &= 6 \cdot 4. \end{aligned}$$

Logo, pelo *Algoritmo de Euclides*, segue-se que

$$\text{mdc}\,(30, 144) = 6.$$

Para calcular o máximo divisor comum de uma quantidade finita $n \geqslant 2$ de inteiros, pode-se utilizar a proposição abaixo.

Proposição 2.9 *Sejam $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, não simultameamente nulos. Tem-se que*

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

A demonstração dessa proposição é feita por indução sobre n e pode ser vista em [16].

2.1.5 Mínimo Múltiplo Comum

Sejam a e b dois inteiros dados. Se $m \in \mathbb{Z}$ é simultaneamente múltiplo de a e b, dizemos que m é um *múltiplo comum* desses números. Assim, como quaisquer dois inteiros a e b dividem 0 e ab, segue-se que 0 e ab são múltiplos comuns de a e b.

Definição 2.3 (mmc) *Sejam $a, b \in \mathbb{Z}^*$. Um mínimo múltiplo comum de a e b, denotado por $mmc(a,b)$, é um natural m tal que*
i) $a|m$ e $b|m$;
ii) $a|c$ e $b|c \Rightarrow m|c$.

Note que a condição (i) significa que m é um múltiplo comum de a e b. Por sua vez, a condição (ii) garante que m é o menor dentre todos os múltiplos comuns de a e b. Da definição (2.3), segue-se que o mínimo múltiplo comum de dois inteiros, quando existe, é único.

Observação 2.2 *Note que, se a e b são inteiros não nulos, então*

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

Assim, para calcular o mínimo múltiplo comum de dois inteiros não nulos a e b, podemos considerá-los sempre positivos.

Os resultados seguintes apresentam as principais propriedades de mínimo múltiplo comum.

Proposição 2.10 *Se a e b são inteiros positivos, então*

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

Demonstração: Considere um inteiro $m = \dfrac{ab}{\text{mdc}\,(a,b)}$. Mostremos que $m = \text{mmc}\,(a,b)$. De fato, note que

$$m = a\frac{b}{\text{mdc}\,(a,b)} = b\frac{a}{\text{mdc}\,(a,b)}.$$

Logo, $a|m$ e $b|m$. Seja $c \in \mathbb{Z}$ um múltiplo comum de a e b. Existem $k_1, k_2 \in \mathbb{Z}$ tais que $c = ak_1 = bk_2$. Daí, temos que

$$k_1\frac{a}{\text{mdc}\,(a,b)} = k_2\frac{b}{\text{mdc}\,(a,b)}$$

Como $\frac{a}{\text{mdc}\,(a,b)}$ e $\frac{b}{\text{mdc}\,(a,b)}$ são coprimos, segue-se que

$$\frac{a}{\text{mdc}\,(a,b)}\Big|k_2 \Longrightarrow \frac{ab}{\text{mdc}\,(a,b)}\Big|bk_2 \Longrightarrow m|c.$$

Assim, $m = \text{mmc}\,(a,b)$ e, portanto,

$$\text{mmc}\,(a,b)\cdot\text{mdc}\,(a,b) = ab.$$

□

Corolário 2.2 *Sejam $a, b \in \mathbb{N}$. Se a e b são coprimos, então $mmc\,(a,b) = ab$.*

Proposição 2.11 *Se $a_1, a_2, \ldots, a_n$ são inteiros, não simultanemente nulos, então*

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

Para ver a demonstração desse resultado, consultar [16].

2.1.6 Números Primos

O estudo dos números primos é de grande importância para o desenvolvimento deste trabalho. A seguir, apresentaremos alguns resultados sobre essa teoria, dando ênfase em especial ao *Teorema Fundamental da Aritmética.*

Definição 2.4 *Um número inteiro $p > 1$ é primo se seus únicos divisores positivos forem 1 e p.*

Observe que 2 é o único primo par. Com efeito, os únicos divisores de 2 são 1 e 2. Logo, 2 é primo. Por outro lado, se $n > 2$ é um inteiro par, então n é divisível por 2 e, portanto, não é primo.

Observação 2.3 *Um número inteiro $n > 1$ que não é primo, é dito composto.*

Proposição 2.12 *Sejam $a, p \in \mathbb{Z}$, com p primo. Se $p \nmid a$, então $mdc\,(p,a) = 1$.*

Demonstração: Seja $d = \text{mdc}\,(p,a)$. Como $p \nmid a$ e $d|p$, segue-se que $d \neq p$ e daí, $d = 1$. Portanto, $\text{mdc}\,(p,a) = 1$. □

Proposição 2.13 *Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p|ab$, então $p|a$ ou $p|b$.*

Demonstração: Se $p \nmid a$, então pela proposição (2.12) temos que $\text{mdc}(p, a) = 1$. Logo, existem $x_0, y_0 \in \mathbb{Z}$ tais que,

$$px_0 + ay_0 = 1 \Longrightarrow p(bx_0) + (ab)y_0 = b.$$

Daí, como $p|ab$, segue da proposição (2.4) que $p|b$. De forma análoga, se $p \nmid b$ obtemos que $p|a$. Portanto, $p|a$ ou $p|b$. □

Da proposição acima, temos o seguinte corolário.

Corolário 2.3 *Sejam $p_1, p_2, \ldots, p_k$ números primos. Se $p \in \mathbb{Z}$ é primo e $p|p_1p_2 \cdots p_k$, então $p = p_i$ para algum $i = 1, \ldots, k$.*

O teorema a seguir é, de certa forma, um dos resultados mais importantes da Teoria dos Números e já constava nos *Elementos*[1] de Euclides.

Teorema 2.4 (Teorema Fundamental da Aritmética) *Todo número inteiro maior do que 1 ou é primo ou pode ser representado de maneira única (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração: Usaremos a *segunda forma do Princípio de Indução Finita.* Seja $n > 1$ um número inteiro. Note que, para $n = 2$, a afirmação é verdadeira, pois 2 é primo. Suponhamos que a afirmação seja válida para todo inteiro n' tal que, $1 < n' < n$. Se n é primo, não há o que demonstrar. Por outro lado, se n é composto, então existem $n_1, n_2 \in \mathbb{Z}$, com $1 < n_1 < n$ e $1 < n_2 < n$, tais que $n = n_1n_2$. Como $n_1 < n$ e $n_2 < n$, da hipótese de indução, segue-se que existem primos $p_1, p_2, \ldots, p_i$ e $q_1, q_2, \ldots, q_j$ tais que $n_1 = p_1p_2 \cdots p_i$ e $n_2 = q_1q_2 \cdots q_j$. Portanto,

$$n = p_1 \cdots p_iq_1 \cdots q_j.$$

Para provar a unicidade da representação, suponhamos que

$$n = p_1p_2 \cdots p_i = q_1q_2 \cdots q_j.$$

Observe que $p_1|q_1q_2 \cdots q_j$. Logo, pelo corolário (2.3), segue-se que $p_1 = q_{j_0}$, para algum $j_0 = 1, \ldots, j$. Sem perda de generalidade, suponhamos que $p_1 = q_1$. Com isto, temos

[1] Obra matemática contendo 13 livros que foram escritos por volta de 300 a.C pelo matemático grego Euclides.

que $1 < p_2 \cdots p_i = q_2 \cdots q_j < n$. Pela hipótese de indução, segue-se que $i = j$ e os primos p_r e p_s, com $1 \leqslant r \leqslant i$ e $1 \leqslant s \leqslant j$, são iguais aos pares. □

Um outro resultado apresentado e demonstrado por Euclides diz respeito à infinitude dos números primos, como veremos a seguir.

Teorema 2.5 *O conjunto dos números primos é infinito.*

Demonstração: Suponha que exista apenas um número finito de primos

$$p_1, p_2, \ldots, p_k.$$

Logo, o inteiro

$$n = p_1 p_2 \cdots p_k + 1$$

é composto. Pelo *Teorema Fundamental da Aritmética*, n possui um fator primo p, o qual deve ser um dos primos $p_1, p_2, \ldots, p_k$. Assim, temos que $p|n$ e $p|p_1 p_2 \cdots p_k$. Portanto, $p|1$, o que é um absurdo. □

Teorema 2.6 *Seja $m \in \mathbb{Z}$, com $m \neq 0, -1, 1$. Existem primos $p_1 < p_2 < \ldots < p_k$ e $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$, univocamente determinados, tais que*

$$m = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Demonstração: Consideremos $m > 1$. Usando o *Teorema Fundamental da Aritmética*, podemos escrever m de forma única como produto de fatores primos. Agrupando os fatores repetidos e dispondo os primos distintos em ordem crescente, obtemos

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Se $m < -1$, então $-m > 1$ e o resultado segue do caso anterior. □

Proposição 2.14 *Seja $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ um número natural, tal como no teorema acima. Se $m \in \mathbb{N}$ é um divisor de n, então*

$$m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

onde $0 \leqslant \beta_i \leqslant \alpha_i$, para $i = 1, 2, \ldots, k$.

Demonstração: Seja $m \in \mathbb{N}$ um divisor de n. Suponha que p^β é a potência de um primo p que aparece na decomposição de m em fatores primos. Note que $p^\beta | n$ e, portanto, p^β divide algum $p_i^{\alpha_i}$, já que p^β é primo com os demais $p_j^{\alpha_j}$. Daí, segue-se que $p = p_i$ e $\beta \leqslant \alpha_i$. □

A fatoração de números inteiros, permite dentre muitas coisas, determinar o máximo divisor comum e o mínimo múltiplo comum.

Teorema 2.7 *Sejam* $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *e* $b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, *onde* $p_1 < p_2 < \cdots < p_k$ *são primos e* $\alpha_i, \beta_i \in \mathbb{N} \cup \{0\}$, *para todo* $i = 1, 2, \ldots, k$. *Tem-se que*

$$mdc(a,b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k} \quad e \quad mmc(a,b) = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k},$$

onde $\gamma_i = \min\{\alpha_i, \beta_i\}$ *e* $\delta_i = \max\{\alpha_i, \beta_i\}$.

Demonstração: Pela proposição anterior, temos que $p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$ é um divisor comum de a e b. Seja c um divisor comum de a e b. Logo, $c = \pm p_1^{\theta_1} p_2^{\theta_2} \cdots p_k^{\theta_k}$, onde $\theta_i \leqslant \alpha_i$ e $\theta \leqslant \beta_i$. Assim, temos $\theta_i \leqslant \gamma_i$ e, portanto, $c | p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$.

Para o mínimo múltiplo comum, note que $p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}$ é divisível por a e b, em vista da proposição anterior. Seja m um múltiplo comum de a e b. Temos que $m = \pm p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_k^{\varepsilon_k}$, onde $\varepsilon_i \geqslant \alpha_i$ e $\varepsilon_i \geqslant \beta_i$. Daí, segue-se que $\varepsilon_i \geqslant \delta_i$ e, portanto, $p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k} | m$. □

2.1.7 Equações Diofantinas Lineares

Este tópico é dedicado ao estudo das equações diofantinas lineares de duas incógnitas, que são equações da forma

$$ax + by = c \tag{2.1}$$

onde $a, b, c \in \mathbb{Z}$, $a \neq 0$ e $b \neq 0$. Uma solução para uma equação do tipo (2.1) é um par $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$, de modo que se tenha

$$ax_0 + bx_0 = c.$$

Nem toda equação diofantina possui solução inteira. Por exemplo, não existem inteiros x e y que satisfaçam a igualdade $2x + 2y = 3$. De fato, como $2x + 2y$ é um número par, para quaisquer $x, y \in \mathbb{Z}$, segue-se que a igualdade $2x + 2y = 3$ não pode

ocorrer. Necessitamos, portanto, de condições que garantam a existência de soluções para uma equação diofantina do tipo (2.1).

Proposição 2.15 *Sejam $a, b, c \in \mathbb{Z}$ e $d = mdc(a, b)$. A equação diofantina $ax+by = c$ admite solução se, e somente se, $d|c$.*

Demonstração:($\Rightarrow$) Suponha que existam $x_0, y_0 \in \mathbb{Z}$ tais que, $ax_0 + by_0 = c$. Daí, como $d|a$ e $d|b$, segue-se que $d|c$.
($\Leftarrow$) Se $d|c$, então existe $k \in \mathbb{Z}$ tal que, $c = dk$. Além disso, como $d = \text{mdc}(a, b)$, existem $x_0, y_0 \in \mathbb{Z}$ tais que, $ax_0 + by_0 = d$. Com isto, obtemos

$$c = (ax_0 + by_0)k = ax_0k + by_0k = a(x_0k) + b(x_0k).$$

Portanto, a equação $ax + by = c$ possui solução. □

Teorema 2.8 *Seja (x_0, y_0) uma solução particular da equação diofantina $ax + by = c$, onde a e b são ambos não nulos. Então, essa equação admite infinitas soluções e o conjunto dessas soluções é*

$$S = \left\{ \left(x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k \right) ; k \in \mathbb{Z} \right\}$$

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

Demonstração: Seja (x_1, y_1) uma solução qualquer da equação $ax + by = c$. Temos que

$$ax_1 + by_1 = c = ax_0 + by_0 \Longrightarrow a(x_1 - x_0) = b(y_0 - y_1).$$

Além disso, como $d|a$ e $d|b$, existem $k_1, k_2 \in \mathbb{Z}$ tais que, $a = dk_1$ e $b = dk_2$. Logo,

$$dk_1(x_1 - x_0) = dk_2(y_0 - y_1) \Longrightarrow k_1(x_1 - x_0) = k_2(y_0 - y_1), \tag{2.2}$$

ou seja, $k_1|k_2(y_0 - y_1)$. Note que

$$\text{mdc}(k_1, k_2) = \text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Daí, como $k_1|k_2(y_0 - y_1)$, segue-se que $k_1|(y_0 - y_1)$. Assim, existe $k \in \mathbb{Z}$ tal que,

$$y_0 - y_1 = k_1k = \frac{a}{d}k \Longrightarrow y_1 = y_0 - \frac{a}{d}k.$$

Da igualdade (2.2), obtemos que

$$k_1(x_1 - x_0) = k_2\left(\frac{a}{d}\right)k \Longrightarrow x_1 - x_0 = k_2 k,$$

ou seja,

$$x_1 = x_0 + \frac{b}{d}k.$$

Portanto, se (x_0, y_0) é uma solução particular da equação $ax + by = c$, então o conjunto de todas as soluções dessa equação é

$$S = \left\{\left(x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k\right); k \in \mathbb{Z}\right\}.$$

□

2.1.8 Congruências

Neste tópico apresentaremos a noção de congruência, uma das mais importantes relações existentes na Teoria dos Números. Foi introduzida por Gauss (1777 - 1855) em seu livro *Disquisitiones Arithmeticae*[2].

Definição 2.5 *Sejam $a, b, m \in \mathbb{Z}$, com $m > 1$. Dizemos que a é congruente a b módulo m, e denotamos $a \equiv b\,(mod\,m)$ se $m|(a - b)$.*

De acordo com esta definição, temos $a \equiv -a \pmod 2$, pois $2|[a - (-a)]$. No caso de a não ser congruente a b módulo m, escrevemos $a \not\equiv b \pmod m$ e dizemos que a e b são incongruentes, ou não congruentes, módulo m.

Note que na definição (2.5), excluímos o caso $m = 1$, pois $a \equiv b \pmod 1$, para quaisquer $a, b \in \mathbb{Z}$, uma vez que $1|(a - b)$.

Proposição 2.16 *Sejam $a, m \in \mathbb{Z}$, com $m > 1$.*

a) Se a deixa resto r na divisão por m, então $a \equiv r\,(mod\,m)$. Em particular, todo inteiro é congruente, módulo m, a exatamente um dos números $0, 1, \ldots, m - 1$.

b) $a \equiv b\,(mod\,m)$ se, e somente se, a e b deixam um mesmo resto na divisão por m.

[2]Livro sobre Teoria dos Números escrito por Carl Friedrich Gauss em 1798 e publicado em 1801. Nesta obra, Gauss reuniu trabalhos de outros importantes matemáticos, além de apresentar resultados de sua autoria.

Demonstração: *a*) Seja $a = mq + r$, com $0 \leqslant r < m$, para algum inteiro q. Daí, $a - r = qm$, isto é, $m|(a - r)$. Portanto, $a \equiv r \,(\mathrm{mod}\, m)$. Como $r \in \{0, 1, \ldots, m-1\}$, dessa última congruência segue-se que a é congruente a um dos números: $0, 1, \ldots, m-1$.
b) Se $a \equiv b \,(\mathrm{mod}\, m)$, então $m|(a - b)$ e daí, a e b deixam um mesmo resto na divisão por m. Reciprocamente, se $a = mq_1 + r$ e $b = mq_2 + r$, com $0 \leqslant r < m$ e $q_1, q_2 \in \mathbb{Z}$, então $a - b = m(q_1 - q_2)$, ou seja, $m|(a - b)$. Portanto, $a \equiv b \,(\mathrm{mod}\, m)$. □

Podemos utilizar a relação de congruência para solucionar vários problemas de Teoria dos Números. Para tanto, é necessário conhecer suas principais propriedades, as quais encontram-se descritas nas proposições seguintes.

Proposição 2.17 *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Tem-se que:*

a) $a \equiv a \,(mod m)$.

b) $a \equiv b \,(mod m) \Rightarrow b \equiv a \,(mod m)$.

c) $a \equiv b \,(mod m)$ *e* $b \equiv c \,(mod m) \Rightarrow a \equiv c \,(mod m)$.

Demonstração: *a*) e *b*) Basta notar que $m|(a - a)$ e que $m|(a - b) \Rightarrow m|(-1)(b - a)$, isto é, $m|b - a$.
c) Como $m|(a-b)$ e $m|(b-c)$, existem k_1, $k_2 \in \mathbb{Z}$ tais que, $a = b + k_1 m$ e $b = c + k_2 m$, de onde obtemos $a = c + (k_1 + k_2)m$. Ou seja, $m|(a - c)$, o que implica em $a \equiv c \,(\mathrm{mod}\, m)$.

Proposição 2.18 *Sejam $a, b, c, d, m, n \in \mathbb{Z}$, com $m > 1$ e $n > 1$.*

a) *Se* $a \equiv b \,(mod m)$ *e* $c \equiv d \,(mod m)$, *então* $a + c \equiv b + d \,(mod m)$ *e* $ac \equiv bd \,(mod m)$. *Em particular,* $ac \equiv bc \,(mod m)$.

b) *Se* $a \equiv b \,(mod m)$, *então* $a^k \equiv b^k \,(mod m)$, *para todo* $k \in \mathbb{N}$.

c) *Se* $a \equiv b \,(mod m)$, *então* $mdc\,(a, m) = mdc\,(b, m)$.

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

e) *Se* $a \equiv b \,(mod mn)$, *então* $a \equiv b \,(mod m)$ *e* $a \equiv b \,(mod n)$.

f) *Se* $a \equiv b \,(mod m)$ *e* $a \equiv b \,(mod n)$, *com* $mdc\,(m, n) = 1$, *então* $a \equiv b \,(mod mn)$.

Demonstração: *a*) Note que $(a + c) - (b + d) = (a - b) + (c - d)$ e $ac - bd = a(c - d) + d(a - b)$. Como $m|(a - b)$ e $m|(c - d)$, segue que $m|[(a + c) - (b + d)]$ e $m|(ac - bd)$. Daí, $a + c \equiv b + d \,(\mathrm{mod}\, m)$ e $ac \equiv bd \,(\mathrm{mod}\, m)$. Além disso, como $c \equiv c \,(\mathrm{mod}\, m)$, segue-se que $ac \equiv bc \,(\mathrm{mod}\, m)$.

b) Note que $a^k \equiv b^k \,(\mathrm{mod}\, m)$, para $k = 1$. Suponhamos que para um certo $k_0 \in \mathbb{N}$ tenhamos $a^{k_0} \equiv b^{k_0} \,(\mathrm{mod}\, m)$. Daí,

$$a^{k_0+1} - b^{k_0+1} = aa^{k_0} - bb^{k_0} \equiv bb^{k_0} - bb^{k_0} \equiv 0(\mathrm{mod}\, m) \Longrightarrow a^{k_0+1} \equiv b^{k_0+1} \,(\mathrm{mod}\, m)\,.$$

Portanto, pelo *Princípio de Indução Finita*, segue-se que $a^k \equiv b^k \,(\mathrm{mod}\, m)$, para todo $k \in \mathbb{N}$.

c) Sejam $d' = \mathrm{mdc}\,(a, m)$ e $d'' = \mathrm{mdc}\,(b, m)$. Como $m|(a-b)$, existe $k \in \mathbb{Z}$ tal que, $a = mk + b$. Daí, como $d'|a$ e $d'|m$, segue-se que $d'|b$ e, consequentemente, $d'|d''$. Analogamante, como $d''|b$ e $d''|m$, segue-se que $d''|a$. Logo, $d''|d'$. Sendo $d', d'' \in \mathbb{N}$, temos $d' = d''$. Portanto, $\mathrm{mdc}\,(a, m) = \mathrm{mdc}\,(b, m)$.

d) Note que $(a + c) - (b + c) = a - b$. Assim, como $m|[(a + c) - (b + c)]$, segue-se que $m|(a - b)$ e, portanto, $a \equiv b \,(\mathrm{mod}\, m)$.

e) Suponha que $mn|(a-b)$. Daí, como $m|mn$ e $n|mn$, segue-se que $m|(a-b)$ e $n|(a-b)$, isto é, $a \equiv b \,(\mathrm{mod}\, m)$ e $a \equiv b \,(\mathrm{mod}\, n)$.

f) Como $m|(a - b)$ e $n|(a - b)$, existem $k_1, k_2 \in \mathbb{Z}$ tais que, $a - b = k_1 m = k_2 n$. Daí, $m|k_2$, pois $\mathrm{mdc}\,(m, n) = 1$, de onde segue-se que $mn|k_2 n$, ou seja, $mn|(a-b)$. Portanto, $a \equiv b \,(\mathrm{mod}\, mn)$. □

Vejamos um exemplo.

Exemplo 2.3 *Vamos obter o resto da divisão de* 13^{2014} *por* 3.

Solução: Note que $13 \equiv 1 \,(\mathrm{mod}\, 3)$. Logo, pelo item (b) da proposição anterior, temos

$$13^{2014} \equiv 1^{2014} \equiv 1(\mathrm{mod}\, 3).$$

Portanto, o resto da divisão de 13^{2014} por 3 é igual a 1.

Proposição 2.19 *Sejam* $a, b, c \in \mathbb{Z}$, *com* $c \neq 0$ *e* $m > 1$. *Tem-se que*

$$ac \equiv bc\,(mod m) \Longleftrightarrow a \equiv b\left(mod\left[\frac{m}{mdc\,(c, m)}\right]\right).$$

Demonstração: Seja $d' = \mathrm{mdc}\,(c, m)$. Se $m|(ac - bc)$, então existe $k \in \mathbb{Z}$ tal que, $(a - b)c = km$. Daí,

$$(a-b)\frac{c}{d'} = k\frac{m}{d'} \Longrightarrow \frac{m}{d'}\Big|(a-b)\frac{c}{d'}.$$

Logo, como $\text{mdc}\left(\frac{m}{d'}, \frac{c}{d'}\right) = 1$, obtemos que

$$\frac{m}{d'}|(a-b) \Longrightarrow a \equiv b \left(\text{mod } \left[\frac{m}{\text{mdc}\,(c,m)}\right]\right).$$

Reciprocamente, se $a \equiv b \left(\text{mod } \frac{m}{d'}\right)$, com $d' = \text{mdc}\,(c,m)$, então

$$\frac{m}{d'}|(a-b) \Longrightarrow m|(a-b)d' \Longrightarrow m|\text{mdc}\,((a-b)c,(a-b)m) \Longrightarrow m|(a-b)c.$$

Portanto, $ac \equiv bc\,(\text{mod}\,m)$. □

Desta proposição, temos uma importante propriedade de congruências, a qual encontra-se na forma do seguinte corolário e será muito utilizada por nós, nas demonstrações de alguns teoremas relevantes.

Corolário 2.4 *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$ e $mdc\,(c,m) = 1$. Tem-se que*

$$ac \equiv bc\,(mod\,m) \Longleftrightarrow a \equiv b\,(mod\,m)\,.$$

Outro importante resultado sobre congruências, encontra-se na seguinte proposição.

Proposição 2.20 *Sejam $a, b \in \mathbb{Z}$. Se $m_1, m_2, \ldots, m_k$ são inteiros maiores do que 1, então*

$$a \equiv b\,(mod\,m_i)\,,\ \forall i = 1, 2, \ldots, k \Longleftrightarrow a \equiv b\,(mod\,mmc\,(m_1, \ldots, m_k))\,.$$

Demonstração: Suponha que $a \equiv b\,(\text{mod}\,m_i)$, para cada $i = 1, \ldots, k$. Note que, para cada $i = 1, 2, \ldots, k$, temos que $m_i|(a-b)$. Logo, $b - a$ é um múltiplo comum de $m_1, m_2, \ldots, m_k$ e portanto, $\text{mmc}\,(m_1, \ldots, m_k)\,|(a-b)$, ou seja,

$$a \equiv b\,(\text{mod}\,\text{mmc}\,(m_1, \ldots, m_k))\,.$$

Reciprocamente, se $a \equiv b\,(\text{mod}\,\text{mmc}\,(m_1, \ldots, m_k))$, então $\text{mmc}\,(m_1, \ldots, m_k)\,|(a-b)$. Como $m_i|\text{mmc}\,(m_1, \ldots, m_k)$, para cada $i = 1, \ldots, k$, segue-se que $m_i|(a-b)$. Logo,

$$a \equiv b\,(\text{mod}\,m_i)\,,\ \forall i = 1, \ldots, k.$$

□

Exemplo 2.4 *Vamos obter o menor natural múltiplo de 13 que deixa resto igual a 1, quando dividido por 3, 4, 5 e 6.*

Solução: Seja $13n$ o número desejado. Temos que

$$\begin{cases} 13n \equiv 1\,(\mathrm{mod}\,3) \\ 13n \equiv 1\,(\mathrm{mod}\,4) \\ 13n \equiv 1\,(\mathrm{mod}\,5) \\ 13n \equiv 1\,(\mathrm{mod}\,6) \end{cases} \iff 13n \equiv 1\,(\mathrm{mod}\,\mathrm{mmc}\,(3,4,5,6))\,.$$

Daí, como $\mathrm{mmc}\,(3,4,5,6) = 60$, temos

$$13n \equiv 1\,(\mathrm{mod}\,60)\,.$$

Logo, devemos ter $13n - 60k_1 = 1$, para algum $k_1 \in \mathbb{Z}$. Como $\mathrm{mdc}\,(13,60) = 1$, essa equação possui solução inteira. Pelo Algoritmo de Euclides, temos que

$$\begin{cases} 60 = 13 \cdot 4 + 8 \\ 13 = 8 \cdot 1 + 5 \\ 8 = 5 \cdot 1 + 3 \\ 5 = 3 \cdot 1 + 2 \\ 3 = 2 \cdot 1 + 1 \end{cases} \Longrightarrow 1 = 60 \cdot 5 - 13 \cdot 23.$$

Assim, $(-23,-5)$ é uma solução particular de $13n - 60k_1 = 1$. Pelo teorema (2.8), segue-se que $n = -23 - 60k$, com $k \in \mathbb{Z}$, e daí, $n = 37$ é o menor valor que $n \in \mathbb{N}$ pode assumir. Portanto, o número procurado é $13 \cdot 37 = 481$.

Definição 2.6 *Se $a \equiv b\,(mod\,m)$, dizemos que b é um resíduo de a módulo m.*

Definição 2.7 *Um sistema completo de resíduos módulo m é um conjunto de m inteiros $\{a_1, a_2, \ldots, a_m\}$ tal que:*
i) $a_i \not\equiv a_j (mod\,m)$, para todo $i \neq j$;
ii) dado $n \in \mathbb{Z}$, existe um a_i tal que $n \equiv a_i\,(mod\,m)$.

Note que de acordo com a definição (2.7), os números $0, 1, \ldots, m-1$ formam um sistema completo de resíduos módulo m. Observe ainda que um sistema completo de resíduo módulo m possui exatamente m elementos.

Além disso, se $a_1, a_2, \ldots, a_m$ são m números inteiros, dois a dois não congruentes módulo m, então eles formam um sistema completo de resíduos módulo m. De fato, basta notar que os restos das divisões dos números $a_1, a_2, \ldots, a_m$ por m são dois a dois distintos e, portanto, iguais a $0, 1, \ldots, m-1$, numa ordem qualquer.

Proposição 2.21 *Sejam $a, k, m \in \mathbb{Z}$, com $m > 1$ e $mdc(k, m) = 1$. Se $a_1, a_2, \ldots, a_m$ é um sistema completo de resíduos módulo m, então*

$$a + ka_1, a + ka_2, \ldots, a + ka_m$$

também é um sistema completo de resíduos módulo m.

Demonstração: Sendo mdc $(k, m) = 1$, pela proposição (2.19), temos

$$a + ka_i \equiv a + ka_j \,(\text{mod}\, m) \Longleftrightarrow ka_i \equiv ka_j \,(\text{mod}\, m) \Longleftrightarrow a_i \equiv a_j \,(\text{mod}\, m) \Longleftrightarrow i = j,$$

uma vez que $a_1, a_2, \ldots, a_m$ é um sistema completo de resíduos módulo m. Assim, $a + ka_1, a + ka_2, \ldots, a + ka_m$ são dois a dois não congruentes módulo m e, portanto, formam um sistema completo de resíduos módulo m. □

2.1.9 A Função φ de Euler

A função φ de Euler[3] desempenha papel importante na *Criptografia RSA*, como veremos no próximo capítulo. Por hora, nos limitaremos à sua definição e algumas de suas propriedades e, especialmente, aos famosos *Teorema de Euler* e *Pequeno Teorema de Fermat.*

Definição 2.8 (Função φ de Euler) *A função $\varphi : \mathbb{N} \mapsto \mathbb{N}$ que associa a cada $n \in \mathbb{N}$ o número*

$$\varphi(n) = \#\{1 \leqslant k \leqslant n;\ mdc(k, n) = 1\}$$

é chamada função φ de Euler.

Assim, pela definição acima, a função $\varphi(n)$ indica quantos números do conjunto $\{1, 2, \ldots, n\}$ são primos com n. Por exemplo, $\varphi(10) = 4$, pois, dentre os números de 1 até 10, os únicos que são primos com 10 são: $1, 3, 7$ e 9.

Observe que, se p é primo, então $\varphi(p) = p - 1$. Com efeito, sendo p primo, o único elemento do conjunto $\{1, 2, \ldots, p\}$ que não é primo com p é ele mesmo. Logo, $\varphi(p) = p - 1$.

[3]Leonhard Euler (1707 - 1783) publicou importantes resultados em várias áreas da Matemática, sendo considerado um dos maiores matemáticos de todos os tempos.

Na prática, para valores grandes de n, não é muito viável contar um por um os elementos de 1 até n que são primos com n. Os teoremas que seguem, apresentam duas importantes propriedades da função φ, as quais podem ser combinadas juntamente com o *Teorema Fundamental da Aritmética* para se obter o valor de $\varphi(n)$.

Teorema 2.9 *Sejam $a, p \in \mathbb{N}$, com p primo. Tem-se que*

$$\varphi(p^a) = p^a - p^{a-1}.$$

Demonstração: Pela definição (2.8), temos que

$$\varphi(p^a) = \#\{1 \leqslant k \leqslant p^a;\ \text{mdc}\,(k, p^a) = 1\}.$$

Note que $\#\{1, 2, \ldots, p^a\} = p^a$. Além disso, os únicos valores que k não pode assumir são precisamente os múltiplos de p, ou seja, p, $2p$,..., $p^{a-1}p$. Sendo p^{a-1} a quantidade desses múltiplos, obtemos

$$\varphi(p^a) = p^a - p^{a-1}.$$

□

Teorema 2.10 *Sejam $m, n \in \mathbb{N}$ tais que $mdc\,(m, n) = 1$. Tem-se que*

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

Demonstração: Note que o resultado é válido se $m = 1$ ou $n = 1$. Considere $m > 1$ e $n > 1$ e disponha os números de 1 até mn da forma abaixo.

$$\begin{array}{ccccc}
1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\
\vdots & \vdots & \vdots & & \vdots \\
k & m+k & 2m+k & \cdots & (n-1)m+k \\
\vdots & \vdots & \vdots & & \vdots \\
m & 2m & 3m & \cdots & nm
\end{array}$$

Observe que $\text{mdc}\,(i, mn) = 1$ se, e somente se, $\text{mdc}\,(i, m) = \text{mdc}\,(i, n) = 1$. Sendo assim, para obter $\varphi(mn)$ devemos determinar na disposição acima, os inteiros que são primos com m e n, simultaneamente.

Se na linha k, cujos termos são $k, m+k, \ldots, (n-1)m+k$, tivermos $\text{mdc}\,(m,k) = d > 1$, então nenhum termo dessa linha será primo com mn, pois todos os termos da forma $qm+k$, com $0 \leqslant q \leqslant n-1$, são divisíveis por d. Assim, na disposição acima, os elementos que são primos com mn são os que formam a linha k, onde $\text{mdc}\,(m,k) = 1$. Logo, há um total de $\varphi(m)$ linhas onde todos os elementos são primos com mn. Agora, devemos obter nessas $\varphi(m)$ linhas o número de elementos que são primos com n. Para tanto, note que os termos

$$k, m+k, \ldots, (n-1)m+k$$

formam um sistema completo de restos módulo n, uma vez que $\text{mdc}\,(m,n) = 1$. Daí, cada uma dessas linhas possui $\varphi(n)$ elementos primos com n. Portanto, o número de elementos na disposição acima que são primos com mn é $\varphi(m)\varphi(n)$, ou seja,

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

□

Dos teoremas acima, segue-se a expressão geral de $\varphi(n)$, para todo $n \in \mathbb{N}$.

Teorema 2.11 *Seja $m > 1$ um inteiro. Se $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ é a decomposição de m em fatores primos, então*

$$\varphi(m) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Demonstração: Pelo teorema (2.9), temos

$$\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1} = p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right).$$

Como $p_1, p_2, \ldots, p_k$ são dois a dois coprimos, o mesmo vale para $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$, de sorte que podemos aplicar o teorema (2.10), obtendo

$$\begin{aligned} \varphi(m) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k}) \\ &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \end{aligned}$$

□

Definição 2.9 *Um sistema reduzido de resíduos módulo m é um conjunto de $\varphi(m)$ inteiros $r_1, r_2, \ldots, r_{\varphi(m)}$ tais que:*

i) $mdc\,(r_i, m) = 1$, para todo $i = 1, 2, \ldots, \varphi(m)$;

ii) $r_i \not\equiv r_j (mod\, m)$, para todo $i \neq j$.

Teorema 2.12 *Seja a um inteiro positivo tal que $mdc(a,m)=1$. Se $r_1, r_2, \ldots, r_{\varphi(m)}$ é um sistema reduzido de restos módulo m, então $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ também é um sistema reduzido de resíduos módulo m.*

Demonstração: Sendo $\text{mdc}(a,m)=1$ e $\text{mdc}(r_i,m)=1$, temos que $\text{mdc}(ar_i,m)=1$. Além disso, como $\text{mdc}(a,m)=1$, segue-se que

$$ar_i \equiv ar_j \,(\text{mod}\, m) \Longleftrightarrow r_i \equiv r_j \,(\text{mod}\, m) \Longleftrightarrow i=j,$$

uma vez que $r_1, r_2, \ldots, r_{\varphi(m)}$ é um sistema reduzido de resíduos módulo m. Portanto, $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ é um sistema reduzido de resíduos módulo m. □

A seguir, apresentaremos dois importantes teoremas da *Teoria dos Números*.

Teorema 2.13 (Teorema de Euler) *Sejam $m, a \in \mathbb{Z}$, com $m>1$ e $mdc(a,m)=1$. Então,*

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

Demonstração: Seja $r_1, r_2, \ldots, r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m. Como $\text{mdc}(a,m)=1$, então, pelo teorema (2.12), $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ formam um sistema reduzido de resíduos módulo m. Logo, para cada i, $1 \leqslant i \leqslant \varphi(m)$, existe um único j, $1 \leqslant j \leqslant \varphi(m)$ tal que $ar_i \equiv r_j \,(\text{mod}\, m)$. Com isto, temos

$$a_1r_1 \cdot a_2r_2 \cdots ar_{\varphi(m)} \equiv r_1 \cdot r_2 \cdots r_{\varphi(m)} \,(\text{mod}\, m),$$

ou seja,

$$a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \,(\text{mod}\, m).$$

Como $\text{mdc}\left(r_1 r_2 \cdots r_{\varphi(m)}, m\right)=1$, pela proposição (2.19), segue-se que

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

□

O *Teorema de Euler* é uma generalização de um famoso resultado, conhecido como *Pequeno Teorema de Fermat*[4].

Teorema 2.14 (Pequeno Teorema de Fermat) *Sejam $a \in \mathbb{Z}$ e p um número primo. Se $p \nmid a$, então*

$$a^{p-1} \equiv 1 \,(mod p).$$

[4]Resultado que se deve ao matemático francês Pierre de Fermat (1601 - 1665).

Demonstração: Sendo p um número primo, temos $\varphi(p) = p - 1$. Além disso, como $p \nmid a$, segue-se que $\text{mdc}(a, p) = 1$. Daí, pelo *Teorema de Euler*, obtemos

$$a^{p-1} \equiv 1 \,(\text{mod}\, p)\,.$$

□

Uma versão mais geral deste teorema, também conhecida como *Pequeno Teorema de Fermat*, é a seguinte.

Teorema 2.15 (Pequeno Teorema de Fermat) *Se p é um número primo, então*

$$a^p \equiv a \,(mod p)\,,$$

para todo $a \in \mathbb{Z}$.

Demonstração: Suponha $\text{mdc}(a, p) = 1$. Neste caso, pelo teorema anterior, temos

$$a^{p-1} \equiv 1 \,(\text{mod}\, p) \Longrightarrow a^p = a^{p-1} \cdot a \equiv a \,(\text{mod}\, p)\,.$$

Por outro lado, se $\text{mdc}(a, p) \neq 1$, então $p|a$. Logo,

$$a \equiv 0 \,(\text{mod}\, p) \Longrightarrow a^p \equiv 0 \equiv a \,(\text{mod}\, p)\,.$$

Portanto, $a^p \equiv a \,(\text{mod}\, p)$, para todo $a \in \mathbb{Z}$. □

2.1.10 Congruência Linear

Muitos problemas de Aritmética se reduzem à resolução de uma conguência linear, tema este, que passaremos a discutir a partir de agora.

Definição 2.10 *Sejam $a, b, m \in \mathbb{Z}$, com $a \neq 0$ e $m > 1$. Uma congruência linear em uma variável é uma congruência da forma $ax \equiv b \,(mod m)$ onde x é uma incógnita.*

Dizemos que um inteiro x_0 é uma solução de $ax \equiv b \,(\text{mod}\, m)$ se $ax_0 \equiv b \,(\text{mod}\, m)$. Quando tal solução existir, diremos que a congruência é solúvel; caso contrário ela será insolúvel.

Nem sempre um congruência linear possui solução inteira. Por exemplo, a congruência $2x \equiv 1 \,(\text{mod}\, 2)$ é insolúvel. De fato, basta observar que $2 \nmid (2x - 1)$, qualquer que seja $x \in \mathbb{Z}$.

Note que, se x_0 é solução de $ax \equiv b \,(\mathrm{mod}\, m)$ e $x_1 \equiv x_0 \,(\mathrm{mod}\, m)$, então x_1 também é solução de $ax \equiv b \,(\mathrm{mod}\, m)$. Com efeito, se $ax_0 \equiv b \,(\mathrm{mod}\, m)$ e $x_1 \equiv x_0 \,(\mathrm{mod}\, m)$, então $ax_1 \equiv ax_0 \equiv b \,(\mathrm{mod}\, m)$ e, portanto, x_1 também é solução de $ax \equiv b \,(\mathrm{mod}\, m)$.

O resultado que segue, fornece condições necessária e suficiente para que uma dada congruência linear admita solução.

Teorema 2.16 *Uma congruência linear $ax \equiv b \,(mod\, m)$, onde $a \neq 0$, admite solução em $\mathbb{Z}$ se, e somente se, b é divisível por $d = mdc\,(a, m)$. E, neste caso, se x_0 é uma solução particular, então o conjunto de todas as soluções tem d elementos, a saber:*

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

Demonstração: Se x_0 é uma solução de $ax \equiv b \,(\mathrm{mod}\, m)$, então $ax_0 \equiv b \,(\mathrm{mod}\, m)$. Logo, existe $y_0 \in \mathbb{Z}$ tal que, $ax_0 - my_0 = b$. Isto significa que a equação diofantina $ax - my = b$ tem solução e, portanto, $d|b$. Reciprocamente, se $d|b$, então a equação diofantina $ax - my = b$ admite solução. Daí, existem $x_0, y_0 \in \mathbb{Z}$ tais que, $ax_0 - my_0 = b$, ou seja, $ax_0 - b = my_0$. Assim $ax_0 \equiv b \,(\mathrm{mod}\, m)$, isto é, x_0 é solução da congruência $ax \equiv b \,(\mathrm{mod}\, m)$.

Agora, considere (x_0, y_0) uma solução particular de $ax \equiv b \,(\mathrm{mod}\, m)$. Isto significa que (x_0, y_0) é uma solução particular de $ax - my = b$. Logo, pelo teorema (2.8), temos

$$x = x_0 - \frac{m}{d}k;\ k \in \mathbb{Z}.$$

Pela *divisão euclidiana*, temos $k = dq + r$, com $0 \leqslant r < d$. Daí,

$$x = x_0 - \frac{m}{d}k = x_0 - \frac{m}{d}(dq + r) = x_0 - mq - \frac{m}{d}r \equiv x_0 - \frac{m}{d}r \,(\mathrm{mod}\, m).$$

Fazendo r variar de 0 a $d-1$, obtemos as soluções de $ax \equiv b \,(\mathrm{mod}\, m)$, a saber:

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

Suponha que

$$x_0 - \frac{m}{d}k_1 \equiv x_0 - \frac{m}{d}k_2 \,(\mathrm{mod}\, m)\,,$$

onde $0 \leq k_1 < k_2 < d$. Daí, como $\mathrm{mdc}\left(m, \frac{m}{d}\right) = \frac{m}{d}$, temos que

$$\frac{m}{d}k_1 \equiv \frac{m}{d}k_2 \,(\mathrm{mod}\, m) \Longrightarrow k_1 \equiv k_2 \,(\mathrm{mod}\, d)\,, \tag{2.3}$$

de onde obtemos $k_1 = k_2$, o que é uma contradição, tendo em vista que k_1 e k_2 pertencem a um sitema completo de resíduos módulo m.

Portanto, as soluções apresentadas em (2.3) são duas a duas incongruentes módulo m e representam todas as soluções de $ax \equiv b \,(\mathrm{mod}\, m)$. □

Observação 2.4 *Dizemos que uma solução x_0 de $ax \equiv b\,(mod\, m)$ é única módulo m, quando qualquer outra solução x_1 for congruente a x_0 módulo m.*

De acordo com o teorema (2.16), a congruência $ax \equiv b \,(\mathrm{mod}\, m)$ admite solução única módulo m se, e somente se, $\mathrm{mdc}\,(a, m) = 1$.

Definição 2.11 *Se x_0 é uma solução de $ax \equiv 1\,(mod\, m)$, dizemos que x_0 é o inverso de a módulo m.*

O teorema (2.16) assegura a existência de um único inverso de a módulo m, desde que $\mathrm{mdc}\,(a, m) = 1$.

Proposição 2.22 *Seja p um número primo. Um inteiro a é seu próprio inverso módulo p se, e somente se, $a \equiv 1\,(mod\, p)$ ou $a \equiv -1\,(mod\, p)$.*

Demonstração:($\Rightarrow$) Suponha que a seja seu próprio inverso módulo p, isto é, $a \cdot a \equiv 1 \,(\mathrm{mod}\, p)$. Logo, $a^2 \equiv 1 \,(\mathrm{mod}\, p)$, de onde segue-se que

$$p|(a^2 - 1) \Longrightarrow p|(a+1)(a-1).$$

Como p é primo, temos que $p|(a+1)$ ou $p|(a-1)$ e, portanto, $a \equiv 1 \,(\mathrm{mod}\, p)$ ou $a \equiv -1 \,(\mathrm{mod}\, p)$.
($\Leftarrow$) Agora, suponha que $a \equiv 1 \,(\mathrm{mod}\, p)$ ou $a \equiv -1 \,(\mathrm{mod}\, p)$. Neste caso, $p|(a-1)$ ou $p|(a+1)$ e, consequentemente,

$$p|(a-1)(a+1) \Longrightarrow p|(a^2 - 1),$$

ou seja, $a \cdot a \equiv 1 \,(\mathrm{mod}\, p)$. □

Em muitos problemas de *Aritmética*, lidamos com a resolução simultânea de várias congruências lineares. Daí a necessidade de um resultado que nos dê alguma informação sobre a existência de tais soluções. Nesse sentido, o *Teorema Chinês dos Restos* é de fundamental importância e será tratado a partir de agora.

Teorema 2.17 (O Teorema Chinês dos Restos) *Se* $mdc(m_i, m_j) = 1$, *para todo* $i \neq j$, *então o sistema de congruências*

$$\begin{cases} x \equiv a_1 \,(mod\, m_1) \\ x \equiv a_2 \,(mod\, m_2) \\ \qquad \vdots \\ x \equiv a_k \,(mod\, m_k) \end{cases} \tag{2.4}$$

possui uma única solução módulo $m = m_1 \cdot m_2 \cdots m_k$ *e, além disso, tem-se que*

$$x = n_1 y_1 a_1 + \cdots + n_k y_k a_k,$$

onde $n_i = \dfrac{m}{m_i}$ *e* $n_i y_i \equiv 1 \,(mod\, m_i)$, $i = 1, 2, \ldots, k$.

Demonstração: Mostremos que x é solução de (2.4). De fato, se $m_i | n_j$, para todo $i \neq j$, e $n_i y_i \equiv 1 \,(\mathrm{mod}\, m_i)$, temos que

$$x = n_1 y_1 a_1 + \cdots + n_k y_k a_k \equiv n_i y_i a_i \,(\mathrm{mod}\, m_i).$$

Logo, x é uma solução do sistema (2.4). Agora, seja x' uma outra solução de (2.4). Neste caso, temos $x' \equiv a_i \,(\mathrm{mod}\, m_i)$ e, consequentemente,

$$x \equiv x' \,(\mathrm{mod}\, m_i)\,, \forall i = 1, 2, \ldots, k.$$

Sendo $\mathrm{mdc}\,(m_i, m_j) = 1$, para todo $i \neq j$, então $\mathrm{mmc}\,(m_1, m_2, m_k) = m_1 m_2 \cdots m_k = m$ e da proposição (2.20) segue-se que

$$x \equiv x' \,(\mathrm{mod}\, m)\,.$$

Portanto, x é a única solução módulo m para o sistema (2.4). □

2.1.11 Aritmética das Classes Residuais

Podemos definir novas aritméticas a partir das congruências módulo um número natural $m > 1$, as quais encontram muitas aplicações em outros ramos da Matemática. Estas novas aritméticas desempenham um papel fundamental nos procedimentos de cálculo dos computadores e possuem muitas aplicações na tecnologia. Definiremos agora as classes residuais módulo m.

Consideremos um inteiro $m > 1$. Repartiremos o conjunto dos números inteiros ($\mathbb{Z}$) em subconjuntos, onde cada um destes subconjuntos é constituído por todos os números inteiros que nos fornecem o mesmo resto na divisão por m. Com isto, obtemos a seguinte partição de $\mathbb{Z}$:

$$\begin{aligned}
\overline{0} &= \{x \in \mathbb{Z};\ x \equiv 0 \,(\mathrm{mod}\, m)\},\\
\overline{1} &= \{x \in \mathbb{Z};\ x \equiv 1 \,(\mathrm{mod}\, m)\},\\
&\vdots\\
\overline{m-1} &= \{x \in \mathbb{Z};\ x \equiv m-1 \,(\mathrm{mod}\, m)\}.
\end{aligned}$$

Note que, $\overline{m} = \overline{0}$, pois $\overline{m} = \{x \in \mathbb{Z};\ x \equiv m \equiv 0 \,(\mathrm{mod}\, m)\} = \overline{0}$. Da mesma forma, tem-se $\overline{m+1} = \overline{1}$ e de forma geral $\overline{m+r} = \overline{r}$, com $r \geq 0$.

Chamamos o conjunto

$$\overline{a} = \{x \in \mathbb{Z};\ x \equiv a \,(\mathrm{mod}\, m)\}.$$

de **classe residual módulo m** do elemento $a \in \mathbb{Z}$. Representaremos o conjunto de todas as classes residuais módulo m por $\mathbb{Z}_m$. Deste modo, temos

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}.$$

Seja $x \in \mathbb{Z}_m$. Dizemos que um número inteiro a é o representante de x se $x = \overline{a}$.

Além disso, note que $\mathbb{Z}_m$ possui exatamente m elementos, a saber, $\overline{0}, \overline{1}, \ldots, \overline{m-1}$.

Definimos em $\mathbb{Z}_m$ as seguintes operações:

$$\begin{aligned}
+ : \mathbb{Z}_m \times \mathbb{Z}_m &\to \mathbb{Z}_m\\
(\overline{a}, \overline{b}) &\mapsto \overline{a} + \overline{b} = \overline{a+b}
\end{aligned}
\qquad \text{e} \qquad
\begin{aligned}
\cdot : \mathbb{Z}_m \times \mathbb{Z}_m &\to \mathbb{Z}_m\\
(\overline{a}, \overline{b}) &\mapsto \overline{a} \cdot \overline{b} = \overline{a \cdot b}
\end{aligned}$$

Estas operações gozam das seguintes propriedades:

i) $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$ (associatividade da soma);

ii) $\overline{a} + \overline{b} = \overline{b} + \overline{a}$ (comutatividade da soma);

iii) $\exists\ \overline{0} \in \mathbb{Z}_m$ tal que $\overline{a} + \overline{0} = \overline{a}$ (existência do elemento neutro da soma);

iv) $\exists\ \overline{-a} \in \mathbb{Z}_m$ tal que $\overline{a} + \overline{-a} = \overline{0}$ (existência do elemento simétrico);

v) $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$ (associatividade do produto);

vi) $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$ (comutatividade do produto);

vii) $\exists\ \overline{1} \in \mathbb{Z}_m$ tal que $\overline{a} \cdot \overline{1} = \overline{a}$ (existência do elemento neutro do produto);

viii) $(\overline{a} + \overline{b}) \cdot \overline{c} = \overline{a} \cdot \overline{b} + \overline{b} \cdot \overline{c}$ (distributividade).

Estas propriedades são de verificação imediata.

A definição e o teorema que apresentaremos a seguir é de grande importância quando estamos trabalhando com as operações de $\mathbb{Z}_m$.

Definição 2.12 *Seja $\overline{a} \in \mathbb{Z}_m$. Dizemos que $\overline{a}$ é invertível se existe $\overline{b} \in \mathbb{Z}_m$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$. Neste caso, dizemos que $\overline{b}$ é o inverso de $\overline{a}$.*

Teorema 2.18 *$\overline{a} \in \mathbb{Z}_m$ é invertível se, e somente se, $mdc(a, m) = 1$.*

Demonstração: ($\Rightarrow$) Inicialmente suponha que $\overline{a}$ é invertível, então existe $\overline{b} \in \mathbb{Z}_m$ tal que $\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{1}$. Logo, $a \cdot b \equiv 1 \pmod{m}$, ou seja, existe $k \in \mathbb{Z}$ tal que $a \cdot b + (-k)m = 1$. Daí, segue-se que $\text{mdc}\,(a, m) = 1$.
($\Leftarrow$) Agora, suponha que $\text{mdc}\,(a, m) = 1$. Assim, existem inteiros b e k tais que $a \cdot b + (k)m = 1$, donde segue-se que, $a \cdot b \equiv 1 \pmod{m}$. Logo, $\overline{a \cdot b} = \overline{a} \cdot \overline{b} = \overline{1}$.
Portanto, $\overline{a}$ é invertível.

Apresentaremos agora um exemplo envolvendo as operações de $\mathbb{Z}_m$.

Exemplo 2.5 *As tabelas da adição e da multiplicação em $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ são*

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Para finalizar esta seção, apresentaremos agora um famoso teorema da *Teoria dos Números*, conhecido como *Teorema de Wilson* (1741-1793).

Teorema 2.19 (Teorema de Wilson) *Um número inteiro $p \geqslant 2$ é primo se, e somente se,*

$$(p-1)! \equiv -1 \,(mod\, p)\,.$$

Demonstração: ($\Rightarrow$) Seja p um número primo. Pelo teorema (2.16), a congruência $ax \equiv 1 \pmod{p}$ tem uma única solução para cada $a \in \{1, 2, \ldots, p-1\}$. Logo, para cada $a \in \{1, 2, \ldots, p-1\}$, existe um único $b \in \{1, 2, \ldots, p-1\}$ tal que $ab \equiv 1 \pmod{p}$. Além disso, se $a \cdot a \equiv 1 \pmod{p}$, pela proposição (2.22), temos que $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$, o que só é possível se $a = 1$ ou $a = p - 1$. Assim, os únicos

elementos desse conjunto que são seus próprios inversos módulo p são 1 e $p-1$. Com isso, podemos agrupar os números $\{2, 3, \ldots, p-2\}$ em $\frac{p-3}{2}$ pares, de modo que o produto dos elementos de cada um desses pares seja congruente a 1 módulo p. Se multiplicarmos estas congruências, membro a membro, obtemos

$$2 \cdot 3 \cdots (p-2) \equiv 1 \,(\mathrm{mod}\, p) \Longrightarrow 1 \cdot 2 \cdots (p-2)(p-1) \equiv p-1 \equiv -1 (\mathrm{mod}\, p).$$

Portanto, $(p-1)! \equiv -1 \,(\mathrm{mod}\, p)$.

($\Leftarrow$) Suponha que $(p-1)! \equiv -1 \,(\mathrm{mod}\, p)$ e que p não seja primo. Logo, $p|[(p-1)!+1]$ e $p = q_1 q_2$, onde $q_1, q_2 \in \mathbb{Z}$, $1 < q_1 < p$ e $1 < q_2 < p$. Como $q_1|p$ e $q_1 \leqslant p-1$, temos que $q_1|[(p-1)!+1]$ e $q_1|(p-1)!$. Daí, $q_1|[(p-1)!+1-(p-1)!]$, ou seja, $q_1|1$, o que é um absurdo, uma vez que $q_1 > 1$. Portanto, se $(p-1)! \equiv -1 \,(\mathrm{mod}\, p)$, então p é primo. □

Observe que o *Teorema de Wilson* fornece um teste de primalidade, pouco eficiente, pois, para verificar se um inteiro $n \geqslant 2$ é primo, deve-se calcular $(n-1)!+1$, o que é inviável para valores altos de n, e depois verificar se n divide este valor. Mais adiante, apresentaremos alguns testes de primalidade, bem mais eficientes do que este.

2.2 Testes de Primalidade

Nesta seção apresentaremos alguns testes de primalidade, a saber, o *Crivo de Eratostenes* e os *testes de Lucas*.

2.2.1 O Crivo de Eratóstenes

O *Crivo de Eratóstenes* é o mais antigo método de se encontrar números primos. Desenvolvido pelo matemático grego Eratóstenes, no século III a.C, este método não requer a utilização de nenhuma expressão matemática. Muito embora, não seja tão eficiente, como veremos a seguir, pode ser utilizado para determinar todos os números primos e, também, os fatores primos dos números compostos, inferiores a um número $n \in \mathbb{N}$, dado arbitrariamente.

Para se obter todos os números primos menores do que um dado $n \in \mathbb{N}$, dispõem-se numa tabela todos os números naturais de 2 até n e riscam-se de modo sistemático, todos os números compostos dessa tabela, da seguinte forma:

1. O primeiro número não riscado é 2, que é primo. Risque todos os múltiplos de 2 maiores do que 2, pois nenhum destes é primo;

2. O segundo número não riscado é 3, que é primo. Risque todos os múltiplos de 3 maiores do que 3, pois estes não são primos;

3. O terceiro número não riscado é 5, que é primo. Risque todos os múltiplos de 5 maiores do que 5, pois estes não são primos; e assim por diante, até obter um primo p tal que $p^2 > n$.

Assim, em cada nova etapa, devemos riscar todos os múltiplos do menor natural p (primo) que ainda não foram riscados e que são maiores do que p. O processo termina quando obtémos um primo p tal que $p^2 > n$. A demonstração deste fato, segue imediatamente da proposição abaixo, devida ao própio Eratóstenes.

Proposição 2.23 *Se um número natural $n > 1$ não é divisível por nenhum número primo p tal que $p^2 \leqslant n$, então n é primo.*

Demonstração: Suponha que n são seja divisível por nenhum primo p, com $p^2 \leqslant n$, e que n não seja primo. Neste caso, se p_1 é o menor primo que divide n, temos $n = p_1 k$, com $p_1 \leqslant k$. Daí, $p_1^2 \leqslant p_1 k = n$. Assim, n é divisível por um primo p_1 tal que $p_1^2 \leqslant n$, o que é um absurdo. □

Exemplo 2.6 *Usando o Crivo de Eratóstenes, vamos obter todos os número primos menores do que* 100.

Solução: Dispondo os números de 2 até 100 na tabela, devemos ir até o número 7, já

que o próximo primo que é 11, tem quadrado maior do que 100.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Os números que não foram eliminados (riscados) na tabela acima, são precisamente, os primos menores do que 100.

Note que a proposição (2.23) também fornece um teste de primalidade. De fato, para saber se um número n é primo, basta verificar se n não é divisível por nenhum primo p tal que $p^2 \leqslant n$.

2.2.2 Testes de Lucas

Para os testes que apresentaremos a seguir, necessitamos de mais alguns conceitos de Teoria dos Números.

Definição 2.13 *Sejam $a, m \in \mathbb{Z}$, com $m > 1$ e $mdc(a, m) = 1$. A ordem de a módulo m, denotada por $ord_m a$, é o menor $k \in \mathbb{N}$ tal que*

$$a^k \equiv 1 \, (mod m) \, .$$

Note que a $\text{ord}_m a$ está bem definida, pois, pelo *Teorma de Euler*, temos

$$\{i \in \mathbb{N}; a^i \equiv 1 \, (\text{mod}\, m)\} \neq \emptyset.$$

Um resultado importante sobre $\text{ord}_m a$ é o seguinte teorema.

Teorema 2.20 *Sejam $a, m \in \mathbb{Z}$, com $m > 1$ e $mdc(a, m) = 1$. Tem-se que*

$$a^n \equiv 1 \, (mod m) \Longleftrightarrow ord_m a | n.$$

Demonstração: Se $\mathrm{ord}_m a | n$, então $n = q \cdot \mathrm{ord}_m a$, para algum $q \in \mathbb{Z}$. Daí,

$$a^n = a^{q \cdot \mathrm{ord}_m a} = \left(a^{\mathrm{ord}_m a}\right)^q \equiv 1^q \equiv 1 (\mathrm{mod}\, m).$$

Reciprocamente, suponha que $a^n \equiv 1 \,(\mathrm{mod}\, m)$. Pela *divisão euclidiana*, podemos escrever $n = q \cdot \mathrm{ord}_m a + r$, onde $0 \leqslant r < \mathrm{ord}_m a$. Se fosse $r \neq 0$, teríamos

$$1 \equiv a^n = a^{q \cdot \mathrm{ord}_m a + r} = \left(a^{\mathrm{ord}_m a}\right)^q \cdot a^r \equiv a^r (\mathrm{mod}\, m),$$

o que é um absurdo, pois $0 < r < \mathrm{ord}_m a$ e $\mathrm{ord}_m a$ é o menor expoente natural k tal que $a^k \equiv 1 \,(\mathrm{mod}\, m)$. Logo, $r = 0$ e, portanto, $\mathrm{ord}_m a | n$. □

Do teorema acima, temos o seguinte corolário.

Corolário 2.5 *Sejam $a, m \in \mathbb{Z}$, com $m > 1$ e $mdc(a, m) = 1$. Temos que $ord_m a | \varphi(m)$, onde φ é a função de Euler.*

Por fim, apresentaremos nas proposições seguintes mais três testes de primalidade, os chamados *testes de Lucas.*

Proposição 2.24 (Teste 1 de Lucas) *Seja $n > 1$ um número natural. Se existe um inteiro $a > 1$ tal que:*

i) $a^{n-1} \equiv 1 \,(mod\, n)$;

ii) $a^m \not\equiv 1 (mod\, n)$, *para* $m = 1, 2, \ldots, n-2$.

Então n é primo.

Demonstração: Devemos mostrar que todo inteiro m, com $1 \leqslant m < n$ é primo com n ou, equivalentemente, que $\varphi(n) = n - 1$. Para tanto, é suficiente mostrar que existe a, com $1 \leqslant a < n$ e $\mathrm{mdc}\,(a, n) = 1$, tal que $\mathrm{ord}_n a = n - 1$, o que segue diretamente da hipótese. □

O teste 1 exige um número muito elevado de operações, pois, é preciso fazer $n-2$ multiplicações sucessivas por a e, além disso, verificar que 1 não é resíduo módulo n de uma potência de a, menor do que $n - 1$.

Proposição 2.25 (Teste 2 de Lucas) *Seja $n > 1$ um número natural. Se existe um inteiro $a > 1$ tal que:*

i) $a^{n-1} \equiv 1 \,(mod\, n)$;

ii) $a^m \not\equiv 1 (mod\, n)$, *para todo divisor m de $n - 1$.*

Então n é primo.

A demonstração dessa proposição é análoga à da proposição anterior. Para usar o teste 2, devemos conhecer todos os fatores de $n-1$ e, além disso, o teste se mostra mais eficiente quando $n = 2^n + 1$ ou $n = 3 \cdot 2^n + 1$.

O próximo teste de primalidade é um aprimoramento dos dois testes anteriores, o teste 1 e o teste 2.

Proposição 2.26 (Teste 3 de Lucas) *Seja $n > 1$ um número naturral. Se, para todo fator primo p de $n-1$, existe um inteiro $a = a(p)$ tal que:*
i) $a^{n-1} \equiv 1\,(mod n)$;
ii) $a^{\frac{n-1}{p}} \not\equiv 1 (mod n)$.
Então n é primo.

Uma demonstração para este resultado pode ser vista em [28]. Esse teste apresenta-se mais eficiente do que os dois anteriores, uma vez que o número de congruências a serem examinadas é menor, embora ainda devemos conhecer os fatores primos de $n-1$.

2.3 Noções Básicas de Álgebra

Nesta seção, apresentaremos alguns conceitos de Álgebra, os quais constituem a base dos sistemas criptográficos baseados em curvas elípticas.

2.3.1 Anel

Definição 2.14 *Seja $A \neq \emptyset$ um conjunto munido de duas operações, as quais chamaremos de soma e produto em A e denotaremos por $+$ e $\cdot$, tais que*

$$\begin{array}{ccc} +: A \times A \to A & & \cdot: A \times A \to A \\ (a,b) \mapsto a+b & e & (a,b) \mapsto a \cdot b \end{array}$$

Dizemos que A é um ***anel*** *e denotamos $(A, +, \cdot)$ se para quaisquer $a, b, c \in A$, as seguintes propriedades são verificadas:*
i) $(a+b)+c = a+(b+c)$ *(associatividade da soma);*
ii) $\exists\ 0 \in A$ *tal que* $0 + a = a + 0 = a$ *(elemento neutro da soma);*
iii) para todo $x \in A$ existe $y \in A$, denotado por $-x$, tal que $x + y = y + x = 0$ (inverso aditivo ou simétrico);

iv) $a+b=b+a$ *(comutatividade da soma);*

v) $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ *(associatividade do produto);*

vi) $a\cdot(b+c)=a\cdot b+a\cdot c$ *e* $(a+b)\cdot c=a\cdot c+b\cdot c$ *(distribuividade à esquerda e à direita).*

Exemplo 2.7 *Os conjuntos* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ *e* $\mathbb{Z}_m$, *munidos das operações usuais de soma e produto são exemplos de anéis.*

No caso de existir um elemento não nulo $1 \in A$ tal que

$$1\cdot x = x\cdot 1 = x,\ \forall\, x \in A,$$

dizemos que $(A, +, \cdot)$ é um **anel com unidade**. Além disso, se

$$x\cdot y = y\cdot x,\ \forall x, y \in A,$$

dizemos ainda que este anel é **comutativo**.

Exemplo 2.8 *O anel* $(M_{(2\times 2)}, +, \cdot)$ *das matrizes quadradas de ordem* 2, *com as operações usuais de adição e multiplicação de matrizes, possui unidade, mas não é comutativo. De fato, a matriz identidade*

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

é a unidade de $(M_{(2\times 2)}, +, \cdot)$. *Por outro lado, temos que*

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 2 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}.$$

Ou seja, $(M_{(2\times 2)}, +, \cdot)$ *não é comutativo.*

Por sua vez, o anel dos números reais $(\mathbb{R}, +, \cdot)$ é comutativo e com unidade. Alguns anéis que apresentam essas características são conhecidos como corpos e são importantes na definição de curvas elípticas. Em particular, trabalharemos sobre os chamados corpos finitos, como veremos mais tarde.

Definição 2.15 *Um* ***corpo*** *é um anel comutativo e com unidade* $F = (A, +, \cdot)$ *em que*

$$\forall\, x \in A,\ x \neq 0,\ \exists\, y \in A \text{ tal que } xy = 1.$$

Denotaremos y *por* x^{-1}.

Exemplo 2.9 *O conjunto dos números racionais $\mathbb{Q}$ e o conjunto dos números reais $\mathbb{R}$ com as operações usuais de adição e multiplicação são exemplos de corpos.*

Exemplo 2.10 *O conjunto $\mathbb{Z}_p$, com p primo, munido das operações de adição e multiplicação é um corpo.*

Definição 2.16 *Seja F um corpo. Para um número natural n definimos*

$$n \cdot 1 = \underbrace{(1+1+1+...+1)}_{n \text{ parcelas}}.$$

A característica de F é, por definição, o menor número natural n tal que

$$n \cdot 1 = 0.$$

Se tal número não existir, dizemos que o corpo tem característica zero.

Assim, de acordo com a definição (2.16), o corpo do reais $\mathbb{R}$ tem característica zero. De fato, dado qualquer $n \in \mathbb{N}$ temos sempre $n \cdot 1 = n > 0$. Por outro lado, o corpo $\mathbb{Z}_3$ tem característica três, pois $n = 3$ é o menor número natural para o qual $n \cdot \overline{1} = \overline{0}$ em $\mathbb{Z}_3$.

Definição 2.17 *Um corpo F é dito finito se possui uma quantidade finita de elementos. Neste caso, dizemos que a ordem de F é o seu número de elementos.*

Um fato importante de se destacar é que para todo p primo e um inteiro positivo n, existe exatamente um corpo finito de $q = p^n$ elementos; este corpo é denotado por F_q ou $GF(q)$ e é conhecido como *corpo de Galois*. Para mais detalhes sobre corpos de Galois, indicamos [13].

Para finalizar esta seção, apresentaremos a seguir algumas informações básicas a respeito de grupos.

2.3.2 Grupos

Definição 2.18 *Seja $G \neq \emptyset$ um conjunto munido de uma operação $*$ dada por*

$$\begin{aligned} * : G \times G &\to G \\ (x, y) &\mapsto x * y. \end{aligned}$$

Dizemos que o conjunto G é um ***grupo*** *e denotamos $(G, *)$ se a operação $*$ tiver as seguintes propriedades:*

i) $a * (b * c) = (a * b) * c, \ \forall a, b, c \in G$ *(associatividade);*

ii) existe um elemento $e \in G$ *tal que* $a * e = e * a = a, \ \forall a \in G$ *(elemento neutro);*

iii) para todo $a \in G$*, existe um elemento* $a' \in G$ *tal que* $a * b = b * a = e$ *(elemento inverso ou simétrico).*

Observação 2.5 *No intuito de tornar as notações mais simples usaremos G ao invés de $(G, *)$. A operação de G será sempre explicitada no seu contexto.*

Quando a operação $*$ é comutativa, dizemos que G é um grupo abeliano. Neste caso, temos

$$a * b = b * a, \ \forall a, b \in G.$$

Definição 2.19 *Um grupo G é dito* ***finito*** *se o seu número de elementos é finito.*

A ordem de um grupo finito G, denotada por $o(G)$ é, por definição, o número de elementos de G.

Definição 2.20 *Um grupo G é chamado de* ***grupo cíclico****, se existe $g \in G$ tal que para todo $a \in G$*

$$a = \underbrace{g \cdot g \cdot g \cdot \cdots \cdot g}_{k \text{ vezes}}$$

para algum inteiro k. Neste caso, dizemos que g gera o grupo G (g é chamado de ***gerador****).*

Capítulo 3

Criptografia

Neste capítulo abordaremos o sistema criptográfico RSA e o sistema criptográfico baseado em curvas elípticas. Iremos descrever os detalhes do funcionamento destes criptossistemas e entender porque eles são considerados seguros. Finalmente, faremos uma breve comparação entre eles.

3.1 Criptografia RSA

3.1.1 Pré-codificação

Se desejamos utilizar o método RSA, devemos inicialmente converter a mensagem dada em uma sequência de números. Neste trabalho, para tornarmos mais simples o entendimento deste método, iremos supor que a mensagem original é um texto que não apresenta números (apenas palavras). Desta forma, podemos afirmar que a mensagem é formada pelas letras que constituem as palavras e pelos espaços entre as palavras. Esta etapa que acabamos de descrever será chamada pré-codificação.

No processo de pré-codificação as letras são convertidas em números tendo como base a seguinte tabela de conversão:

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

No momento em que a conversão for realizada, o espaço entre as palavras será substituído pelo número 99.

Exemplo 3.1 *Consideremos a frase* ***Amor Eterno****. Esta frase é convertida no número*

$$102224279914291427324. \tag{3.1}$$

Devemos notar que, quando fazemos cada letra da mensagem corresponder a um número de dois algarismos estamos evitando ambiguidades, o que é muito importante. Em outras palavras, se fizéssemos a letra **A** corresponder ao número 1, a letra **B** corresponder ao número 2, e assim continuamente, não saberiamos decidir se o número 12 representaria a junção **AB** ou a letra **L** (décima segunda letra do alfabeto).

Para darmos continuidade ao entendimento do método RSA, precisamos determinar os parâmetros deste sistema que serão utilizados. Estes parâmetros são dois números primos distintos, os quais denotaremos por p e q. Façamos $n = pq$. Para que o processo de pré-codificação seja finalizado precisamos quebrar em blocos o grande número produzido no processo de conversão realizado no exemplo (3.1). Estes blocos devem ser menores do que n.

Exemplo 3.2 *Suponhamos que* $p = 17$ *e* $q = 19$*. Com isso, teremos*

$$n = 17 \cdot 19 = 323.$$

Assim, a mensagem que foi convertida em números no exemplo (3.1), pode ser quebrada nos seguintes blocos:

$$102 - 224 - 279 - 91 - 42 - 9 - 142 - 72 - 32 - 4. \tag{3.2}$$

É importante destacar que a escolha dos blocos não é única, porém devemos tomar determinados cuidados nesta escolha. Um exemplo disso é que deve-se evitar que o bloco seja começado pelo número 0, pois isto poderia causar problemas no momento da decodificação. Destacamos ainda que a decodificação por análise de frequência torna-se praticamente impossível nesta última etapa, uma vez que não é estabelecido um padrão entre os blocos da mensagem.

3.1.2 Codificação

Terminado o processo de pré-codificação, podemos dar continuidade aos nossos estudos com o processo de codificação. Para realizarmos a codificação da mensagem precisamos inicialmente de dois inteiros: o inteiro n (produto de dois primos) e de outro inteiro positivo e que seja inversível módulo $\varphi(n)$. Ou seja, $\text{mdc}(e, \varphi(n)) = 1$. Observe que se os primos p e q forem conhecidos, podemos calcular $\varphi(n)$ facilmente, pois pelo teorema (2.10), a função $\varphi(n) = \varphi(p \cdot q)$ é multiplicativa para p e q primos entre si. Em outras palavras,

$$\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1).$$

Iremos chamar o par (n, e) de chave de codificação do sistema RSA que estamos utilizando. Quando o processo de pré-codificação na mensagem é realizado, obtemos uma sequência de números ou blocos. Os blocos serão codificados separadamente e devem permanecer separados, pois caso contrário será impossível decodificar a mensagem.

Agora, veremos como codificar determinado bloco, digamos b. Pelo que vimos anteriormente, sabemos que b deve ser um inteiro positivo menor do que n. Denotaremos o bloco b já codificado por $C(b)$. A forma de calcular $C(b)$ é a seguinte:

$$C(b) = \text{resto da divisão de } b^e \text{ por } n.$$

Note que, em termos de aritmética modular, temos

$$C(b) \equiv b^e \,(\text{mod}\, n).$$

Voltemos agora ao exemplo (3.2), onde $p = 17$ e $q = 19$, donde obtemos $n = 323$ e $\varphi(n) = \varphi(17 \cdot 19) = 16 \cdot 18 = 288$. Para codificarmos um bloco da mensagem, precisamos ainda encontrar o inteiro positivo e. Note que, neste exemplo o menor valor possível para e é 5, pois este é o menor primo que não divide 288. Em outras palavras temos, $\text{mdc}(5, 288) = 1$. Com isso, a codificação de cada bloco da nossa mensagem pode ser realizada como segue

$C(102) = 68$, pois $102^5 \equiv 68 \,(\text{mod}\, 323)$;

$C(224) = 192$, pois $224^5 \equiv 192 \,(\text{mod}\, 323)$;

$C(279) = 147$, pois $279^5 \equiv 147 \,(\text{mod}\, 323)$;

$C(91) = 211$, pois $91^5 \equiv 211 \pmod{323}$;

$C(42) = 264$, pois $42^5 \equiv 264 \pmod{323}$;

$C(9) = 263$, pois $9^5 \equiv 263 \pmod{323}$;

$C(142) = 92$, pois $142^5 \equiv 92 \pmod{323}$;

$C(72) = 21$, pois $72^5 \equiv 21 \pmod{323}$;

$C(32) = 223$, pois $32^5 \equiv 223 \pmod{323}$;

$C(4) = 55$, pois $4^5 \equiv 55 \pmod{323}$.

Deste modo, podemos codificar toda a mensagem, obtendo a seguinte sequência de blocos:

$$68 - 192 - 147 - 211 - 264 - 263 - 92 - 21 - 223 - 55. \tag{3.3}$$

3.1.3 Decodificação

Tendo conhecimento de como se dá o processo de codificação de mensagens através do método RSA, podemos dar continuidade aos nossos estudos. Agora estudaremos o processo de decodificação de mensagens.

Para decodificarmos uma mensagem codificada precisamos de dois números: n e o inverso de e em $\varphi(n)$, que será denotado por d. O par (n, d) será chamado de *chave de decodificação do sistema*. Supondo que a é um bloco da mensagem codificada, então $D(a)$ será o resultado do processo de decodificação. $D(a)$ será calculado da seguinte forma:

$$D(a) = \text{resto da divisão de } a^d \text{ por } n.$$

Note que, em termos de aritmética modular, isto significa que

$$D(a) \equiv a^d \pmod{n}.$$

Observe que, se e e $\varphi(n)$ forem conhecidos, então podemos encontrar d facilmente, pois neste caso basta-nos aplicar o algorítmo euclidiano estendido. Além disso, se b é um bloco da mensagem original, devemos esperar que $D(C(b)) = b$. Isto é, ao decodificarmos um bloco da mensagem codificada esperamos encontrar o bloco que corresponde a mensagem original. É através disso que podemos saber se determinado código é útil.

Teorema 3.1 *Seja b um bloco ainda não-codificado de determinada mensagem. Utilizando o sistema RSA mostre que $D(C(b)) = b$.*

Demonstração: Consideremos inicialmente um sistema RSA de parâmetros p e q. Com isso, teremos $n = pq$. Dessa forma, os dados de codificação serão n e e, e os de decodificação serão n e d. O que estamos querendo mostrar é que se b é um inteiro e $1 \leq b \leq n-1$, então $D(C(b)) = b$. Contudo, vamos provar apenas que $D(C(b)) \equiv b \pmod{n}$. Isto é suficiente, pois tanto b quanto $D(C(b))$ estão no intervalo $[1, n-1]$, o que implica que só podem ser congruentes módulo n se são iguais (por este motivo devemos escolher b menor do que n, e também é por este motivo que temos de manter os blocos separados, mesmo após a codificação).

Note que, por definição de D e de C temos

$$D(C(b)) \equiv [C(b)]^d \equiv (b^e)^d \equiv b^{ed} \pmod{n}. \tag{3.4}$$

Devemos lembrar que $n = pq$, onde p e q são primos distintos. Iremos calcular a forma reduzida de b^{ed} módulo p e módulo q. Encontraremos inicialmente a forma reduzida de b^{ed} módulo p. Daí, como d é o inverso de e módulo $\varphi(n)$, temos $ed = 1 + k\varphi(n)$, para algum inteiro k. Além disso, como e e d são inteiros maiores que 2 e $\varphi(n) = (p-1)(q-1) > 0$, temos $k > 0$. Logo,

$$b^{ed} \equiv b^{1+k\varphi(n)} \equiv b \cdot b^{k\varphi(n)} \equiv b(b^{\varphi(n)})^k \equiv b(b^{(p-1)})^{(q-1)k} \pmod{p}. \tag{3.5}$$

Observe que, se $p \nmid b$ podemos utilizar o Teorema (2.14). Assim, supondo que $p \nmid b$, temos que $b^{(p-1)} \equiv 1 \pmod{p}$, donde de (3.5) segue-se que $b^{ed} \equiv b \pmod{p}$.

Agora, suponha que $p|b$. Como p é primo temos que $b \equiv 0 \pmod{p}$, o que implica $b^{ed} \equiv b \pmod{p}$. Com isso, temos que a congruência $b^{ed} \equiv b \pmod{p}$ é válida para quaisquer valor de b. E, analogamente podemos mostrar que $b^{ed} \equiv b \pmod{q}$. Isto significa que, $b^{ed} - b$ é divisível por p e por q. Como p e q são primos distintos, temos que $\text{mdc}(p, q) = 1$, donde segue-se que pq divide $b^{ed} - b$. Portanto, como $n = pq$, temos que $b^{ed} \equiv b \pmod{n}$, o que implica $D(C(b)) \equiv b \pmod{n}$, para qualquer número inteiro b. Logo, $D(C(b)) = b$. □

Com base no que apresentamos até aqui, vimos que a codificação é realizada utilizando n e a decodificação utilizando p e q; vem daí a necessidade de fatorar n no processo de decodificação.

Para exemplificarmos o processo de decodificação voltaremos ao exemplo (3.2).

Exemplo 3.3 *No exemplo* (3.2) *temos* $n = 323$, $e = 5$ *e* $\varphi(n) = 288$. *Dessa forma, utilize estas informações para decodificar o bloco* (192) *da mensagem codificada em* (3.3).

Solução: Nosso intuito é calcular d apartir da congruência

$$ed \equiv 1 \,(\mathrm{mod}\, \varphi(n)) \Longrightarrow 5d \equiv 1 \,(\mathrm{mod}\, 288).$$

Donde, obtemos

$$5d - 1 = 288k \Rightarrow 5d - 288k = 1;\ k \in \mathbb{Z}.$$

Assim, nosso trabalho será encontrar uma solução particular da equação diofantina

$$5d - 288k = 1;\ k \in \mathbb{Z}. \tag{3.6}$$

Note que $\mathrm{mdc}\,(288, 5) = 1$ e que $1|1$. Daí, segue que a equação (3.6) possui solução inteira. Pelo Algoritmo de Euclides, temos

$$\begin{cases} 288 = 57 \cdot 5 + 3 \\ 5 = 1 \cdot 3 + 2 \\ 3 = 1 \cdot 2 + 1. \end{cases} \Longrightarrow 1 = 5 \cdot (-115) - (-2) \cdot 288.$$

Com isso, temos que $k = -2$ e $d = -115$ é uma solução particular da equação (3.6). Como vamos usar d como expoente de potências, precisamos que d seja positivo. Logo, $d = 288 - 115 = 173$, este é o menor inteiro positivo que é côngruo a 115 módulo 288. Então, para decodificarmos o bloco 192 da mensagem codificada devemos calcular a forma reduzida de $(192)^{173}$ módulo 323. Isto é, devemos encontrar $D(192)$ tal que

$$D(192) \equiv (192)^{173} \,(\mathrm{mod}\, 323).$$

Neste caso, não é possível realizarmos este cálculo se estivermos limitados ao uso de lápis e papel. Com o auxílio do programa computacional Geogebra (software livre), podemos verificar que $(192)^{173} \equiv 224 \,(\mathrm{mod}\, 323)$, o que implica $D(192) = 224$. Este era exatamente o resultado que esperávamos encontrar.

Vejamos outro exemplo de decodificação de mensagens utilizando o método RSA.

Exemplo 3.4 *A chave pública utilizada pelo Banco de Toulouse para codificar suas mensagens é a seguinte:* $n = 10403$ *e* $e = 8743$. *Recentemente os computadores do banco receberam, de local indeterminado, a seguinte mensagem:*

$$4746 - 8214 - 9372 - 9009 - 4453 - 8198.$$

O que diz a mensagem mandada ao Banco de Toulouse?

Solução: Queremos decodificar a mensagem dada. Assim, precisamos dos valores de n e de d. Temos que $n = 10403$ e, para encontrarmos o valor de d precisamos conhecer os valores de e e $\varphi(n)$. Pelo enunciado da questão temos que $e = 8743$. O valor de $\varphi(n)$ pode ser obtido através da fatoração de n. Utilizando o programa computacional Geogebra (software livre) obtemos

$$n = (101)(103).$$

Considerando $p = 101$ e $q = 103$, temos

$$\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1) = 10200.$$

Com isso, iremos calcular d a partir da congruência

$$ed \equiv 1 \,(\mathrm{mod}\, \varphi(n)) \Longrightarrow 8743d \equiv 1 \,(\mathrm{mod}\, 10200). \tag{3.7}$$

Note que, da congruência (3.7) obtemos

$$8743d - 1 = 10200k \Rightarrow 8743d - 10200k = 1;\ k \in \mathbb{Z}.$$

Daí, nosso trabalho será encontrar uma solução particular da equação diofantina

$$8743d - 10200k = 1;\ k \in \mathbb{Z}. \tag{3.8}$$

Como mdc $(10200, 8743) = 1$ e, claramente $1|1$, segue que a equação (3.8) possui solução inteira. Pelo Algoritmo de Euclides, temos que

$$\begin{cases} 10200 = 1 \cdot 8743 + 1457 \\ 8743 = 6 \cdot 1457 + 1. \end{cases} \Longrightarrow 1 = 7 \cdot 8743 - 6 \cdot 10200.$$

Assim, temos que $k = 6$ e $d = 7$ é uma solução particular de (3.8). Com isso, já podemos decodificar os blocos da mensagem codificada, como segue:

$D(4746) = 1514$, pois $(4746)^7 \equiv 1514 \pmod{10403}$;

$D(8214) = 2722$, pois $(8214)^7 \equiv 2722 \pmod{10403}$;

$D(9372) = 1029$, pois $(9372)^7 \equiv 1029 \pmod{10403}$;

$D(9009) = 9931$, pois $(9009)^7 \equiv 9931 \pmod{10403}$;

$D(4453) = 1831$, pois $(4453)^7 \equiv 1831 \pmod{10403}$;

$D(8198) = 14$, pois $(8198)^7 \equiv 14 \pmod{10403}$.

Assim, obtemos a seguinte mensagem original

$$1514272210299931183114,$$

que corresponde a frase: "Fermat Vive".

3.1.4 Segurança do Método RSA

Como sabemos, o RSA é um método de chave pública. Considerando p e q os parâmetros do sistema que estamos utilizando e $n = pq$. Qualquer usuário poderá ter conhecimento do par (n, e), pois este par corresponde a chave de codificação do sistema (chave pública). De acordo com Coutinho (2011), o sistema criptográfico RSA será considerado seguro se for difícil calcular d quando apenas n e e forem conhecidos. Na verdade, só conseguimos calcular d se aplicarmos o algoritmo euclidiano estendido a $\varphi(n)$ e a e. Em contrapartida, só conseguimos calcular $\varphi(n)$ se soubermos fatorar n para obtermos p e q. Deste modo, só podemos quebrar o código se conseguirmos fatorar n. Porém, sabemos que, se n for um número grande, este é um problema muito difícil, pois não dispomos de algoritmos rápidos de fatoração.

Finalmente, a possibilidade de encontrar b a partir da forma reduzida de b^e módulo n, sem tentar encontrar d é praticamente impossível se n for grande. Na verdade, acredita-se que quebrar o código RSA e fatorar n são problemas equivalentes. Além disso, devemos ter muito cuidado no momento da escolha dos primos p e q, pois se estes forem pequenos, o sistema torna-se vulnerável.

3.1.5 Assinaturas Digitais

Apresentaremos aqui uma aplicação da Criptografia RSA, estamos falando das assinaturas digitais.

Imaginemos que uma empresa realiza suas transações bancárias por computador, através de rede telefônica. Por motivo de segurança, espera-se que tanto a empresa quanto o banco exijam que as informações sejam codificadas antes de serem enviadas pelo sistema telefônico. Porém, isto não é suficiente, pois se o método RSA é utilizado, os dados de codificação do banco são públicos. Dessa forma, qualquer pessoa pode enviar uma mensagem codificada ao banco referente ao movimento financeiro da empresa. Um exemplo disso, é que alguém poderia mandar uma mensagem ao banco pedindo que o saldo bancário da empresa fosse transferido para uma outra conta. Por esse motivo o banco precisa de uma confirmação de que a mensagem foi enviada por um usuário autorizado da empresa. Isto é, a mensagem tem que ser "assinada" por meio de uma assinatura eletrônica.

Podemos mandar uma mensagem assinada utilizando o RSA, ou qualquer outro sistema de chave pública. Para isso, iremos chamar de C_e e D_e as funções codificação e decodificação da empresa, respectivamente. Do mesmo modo, chamaremos C_b e de D_b as funções codificação e decodificação do banco. Assim, consideremos a um bloco da mensagem que a empresa deseja enviar ao banco. Pelo que vimos anteriormente, a empresa teria que codificar o bloco a como $C_b(a)$ e em seguida, enviá-lo por linha telefônica. Para que a mensagem seja enviada assinada, ao invés de $C_b(a)$ enviamos $C_b(D_e(a))$. Isto significa que primeiramente aplicamos a função decodificação da empresa ao bloco a, e somente depois aplicamos a função codificação do banco para codificarmos o bloco $D_e(a)$.

Ao receber a mensagem assinada da empresa, ou seja, tendo recebido a mensagem $C_b(D_e(a))$, o banco aplica primeiramente a sua função de decodificação, obtendo o bloco $D_e(a)$. E, finalmente, para que o bloco original a seja obtido, o banco aplica a função de codificação da empresa (C_e) ao bloco $D_e(a)$ (devemos lembrar que a função C_e é conhecida publicamente).

Devemos nos perguntar: por que o que foi feito aqui é suficiente para garantir ao banco que a mensagem foi enviada por algum usuário autorizado? Para obtermos uma resposta para tal pergunta, devemos observar que, o banco aplica a sequência de funções C_eD_b aos blocos da mensagem recebida. Se a mensagem obtida fizer sentido, então significa que a mensagem enviada foi codificada aplicando a sequência de funções C_bD_e aos blocos da mensagem original. Devemos ressaltar que a função D_e é apenas

conhecida pela empresa. Deste modo, se a mensagem obtida fizer algum sentido, tem que ter sido originada na empresa. Se uma mensagem for produzida sem utilizar a função D_e, então a possibilidade do banco decodificar esta mensagem utilizando a sequência de funções $C_e D_b$ produzindo uma mensagem com sentido é praticamente nula. Portanto, o banco pode estar seguro de que a mensagem é legítima.

3.2 Criptografia Baseada em Curvas Elípticas

Nesta seção, K poderá representar qualquer um dos seguintes corpos: o corpo dos números reais ($\mathbb{R}$), o corpo dos números racionais ($\mathbb{Q}$), o corpo dos números complexos ($\mathbb{C}$) ou o corpo finito F_q de $q = p^r$ elementos.

3.2.1 Curvas Elípticas

Definição 3.1 *Sejam K um corpo de característica diferente de 2 e de 3 e $x^3 + ax + b$ um polinômio cúbico sem raízes múltiplas, com $a, b \in K$. Definimos uma curva elíptica E sobre K, como o conjunto dos pontos (x, y) tal que*

$$y^2 = x^3 + ax + b, \tag{3.9}$$

juntamente com um único elemento chamado de ponto no infinito e denotado por $\mathcal{O}$ (o qual descreveremos mais adiante).

Se K é um corpo de característica 2, então a curva elíptica E sobre K é definida como o conjunto de pontos (x, y) que satisfazem uma das seguintes igualdades

$$y^2 + cy = x^3 + ax + b \quad \text{ou} \quad y^2 + xy = x^3 + ax + b \tag{3.10}$$

juntamente com o chamado ponto no infinito $\mathcal{O}$.

No caso de K ser um corpo de característica 3, definimos uma curva elíptica E sobre K como o conjunto de pontos (x, y) que satisfaz a equação

$$y^2 = x^3 + ax^2 + bx + c, \tag{3.11}$$

(onde o polinômio $x^3 + ax^2 + bx + c$ não possui raízes múltiplas) juntamente com o ponto no infinito $\mathcal{O}$.

Observação 3.1 *Existe uma forma geral de uma equação que é utilizada para definir uma curva elíptica sobre um corpo K de característica qualquer. Esta equação é conhecida como* ***equação de Weierstrass*** *e é dada por*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

com a_1, a_2, a_3, a_4, $a_6 \in K$.

Observação 3.2 *Seja* $F(x, y) = 0$ *uma equação implicíta que define uma curva elíptica e que possui* x *e* y *como variáveis dessa função em* (3.9), (3.10) *ou* (3.11), *ou seja,*

$$F(x, y) = y^2 - x^3 - ax - b,$$
$$F(x, y) = y^2 + cy - x^3 - ax - b,$$
$$F(x, y) = y^2 + xy - x^3 - ax - b,$$
$$F(x, y) = y^2 - x^3 - ax^2 - bx - c.$$

Um ponto (x, y) sobre uma curva elíptica E é dito não-singular (ou suave) se as derivadas parciais $\frac{\partial F}{\partial x}$ e $\frac{\partial F}{\partial y}$ não são simultaneamente nulas. Segundo Koblitz (1994), a condição para que os polinômios à direita em (3.9) e (3.11) não possuam raízes múltiplas é equivalente a afirmar que os pontos na curva são não-singulares.

3.2.2 Ponto no Infinito

Desde o início da definição de curvas elípticas estamos falando de um determinado ponto, conhecido como ponto no infinito ($\mathcal{O}$). Para definirmos a operação de soma existente entre pontos de uma curva elíptica precisaremos definir este ponto. Para isso utilizaremos um argumento de geometria algébrica, a saber:

Um plano projetivo é o conjunto de classes de equivalência das triplas (X, Y, Z), com elementos não simultaneamente nulos.

Dizemos que duas triplas (X, Y, Z) e (X_0, Y_0, Z_0) são equivalentes, se existir λ tal que $\lambda(X, Y, Z) = (X_0, Y_0, Z_0)$. Tal classe de equivalência é conhecida como *ponto projetivo*. Se um ponto projetivo tem coordenada Z diferente de 0, então existe uma e somente uma tripla em sua classe de equivalência da forma $(x, y, 1)$. Neste caso, basta-nos definir $x = \frac{X}{Z}$ e $y = \frac{Y}{Z}$.

Dessa forma, o plano projetivo pode ser identificado como todos os pontos (x, y) do plano cartesiano mais os pontos para os quais $Z = 0$. Esses últimos pontos formam a chamada reta no infinito.

Qualquer equação $F(x, y) = 0$, de uma curva no plano cartesiano corresponde a uma equação $\widetilde{F}(X, Y, Z) = 0$ satisfeita pelos pontos projetivos correspondentes. Para isto, basta substituir x por $\frac{X}{Z}$ e y por $\frac{Y}{Z}$ e multiplicá-los por uma potência adequada de Z para eliminar os denominadores. Por exemplo, dada a equação cartesiana de uma curva elíptica $y^2 = x^3 + ax + b$, aplicamos o procedimento descrito anteriormente e obtemos a equação projetiva

$$Y^2Z = X^3 + aXZ^2 + bZ^3. \tag{3.12}$$

Esta última equação é satisfeita por todos os pontos projetivos (X, Y, Z) com $Z \neq 0$ para os quais o ponto cartesiano correspondente (x, y), com $x = \frac{X}{Z}$ e $y = \frac{Y}{Z}$, satisfaz a equação $y^2 = x^3 + ax + b$. Além disso, qual é o ponto projetivo (X, Y, Z) sobre a reta no infinito que satisfaz a equação $\widetilde{F} = 0$? Para obtermos uma resposta para tal pergunta, devemos observar que fazendo $Z = 0$ na equação (3.12), obtemos $X^3 = 0$, o que implica $X = 0$. Mas a única classe de equivalência de triplas (X, Y, Z) com X e Z simultaneamente nulos é a classe de $(0, 1, 0)$. Este ponto é o que chamamos de *ponto no infinito* $\mathcal{O}$, que é o ponto de intersecção do eixo y com a reta no infinito.

3.2.3 Grupo de Pontos Sobre uma Curva Elíptica

Dados dois pontos quaisquer sobre uma curva elíptica, podemos definir uma operação de soma entre estes pontos. Esta operação é conhecida como **soma elíptica** e simbolizada por $+$. Através desta operação e de algumas de suas propriedades podemos estabelecer uma estrutura de grupo abeliano sobre o conjunto de pontos de uma curva.

Apresentaremos aqui uma abordagem geométrica e algébrica da chamada soma elíptica. Inicialmente iremos considerar o caso particular em que $K = \mathbb{R}$, pois poderemos visualizar a lógica geométrica que define a operação de pontos sobre uma curva elíptica. Tal lógica é conhecida como **lei da corda e tangente**.

Operação de adição entre pontos de uma curva elíptica

A definição que apresentaremos aqui será baseada na definição apresentada por Koblitz (1994).

Definição 3.2 *Seja E uma curva elíptica definida sobre $\mathbb{R}$, e sejam P e Q dois pontos em E. Definimos o oposto de P e a soma de P e Q a partir das seguintes regras:*
i) Se P é o ponto no infinito $\mathcal{O}$, definimos $-P$ como $\mathcal{O}$ e $P+Q$ como Q. Em outras palavras, $\mathcal{O}$ é tido como elemento neutro do grupo de pontos.
ii) Considere $P=(x, y)$. Assim, o seu oposto $-P$ é formado pela sua coordenada x e pela sua coordenada oposta y; isto é, $-P=(x, -y)$. Pela equação (3.9) pode-se notar que P e $-P$ pertencem, simultaneamente, à curva.
iii) Se P e Q possuem coordenadas diferentes x, então facilmente nota-se que a reta $l=\overline{PQ}$ intercepta a curva E em exatamente mais um ponto R (exceto quando a reta l é tangente a curva E em P ou em Q, onde deve-se tomar $R=P$ ou $R=Q$, respectivamente). Então define-se a soma $P+Q=-R$, onde $-R$ é a reflexão do ponto R em torno do eixo x (veja a figura (3.1)).

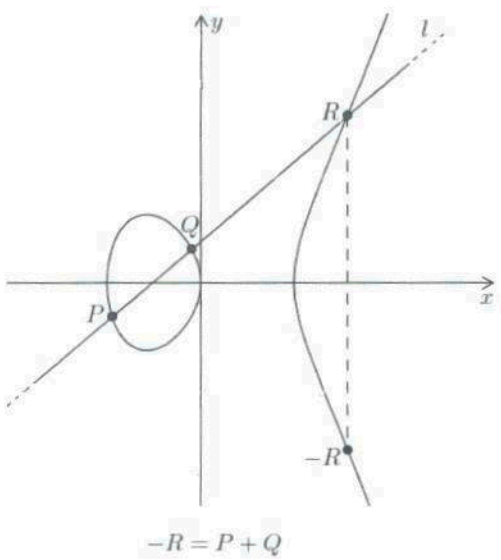

Figura 3.1: Soma de pontos distintos de uma curva elíptica.

iv) Se $P=-Q$, então definimos $P+Q=\mathcal{O}$ (isto segue imediatamente de (ii)).
v) Finalmente, consideraremos o caso em que $P=Q$. Neste caso, sejam l a reta tangente a curva E em P e R o único ponto de intersecção da reta l com a curva E,

definimos $P + Q = -R$, onde $-R$ é a reflexão do ponto R em torno do eixo x (R é considerado como sendo P, se P é um ponto de inflexão de E) (veja a figura (3.2)).

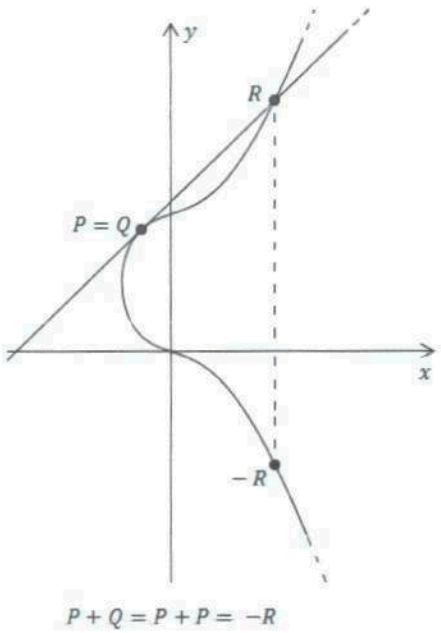

Figura 3.2: Soma de pontos iguais de uma curva elíptica.

Observação 3.3 *Para as regras apresentadas em (ii), (iii), (iv) e (v), considerou-se que nem P e nem Q são pontos no infinito.*

De modo geral, a soma elíptica possui as seguintes propriedades:

(P_1) Se $P, Q \in E$, então $(P + Q) \in E$ *(fechamento)*;

(P_2) $(P + Q) + S = P + (Q + S)$, $\forall\ P, Q, S \in E$ *(associatividade)*;

(P_3) Para todo $P \in E$ existe um $Q \in E$ tal que $P + Q = \mathcal{O}$. O ponto Q pode ser representado por $-P$ *(existência do inverso)*;

(P_4) Para todo $P \in E$, $P + \mathcal{O} = \mathcal{O} + P = P$ *(elemento neutro)*;

(P_5) $(P + Q) = (Q + P)$, $\forall\ P, Q \in E$ *(comutatividade)*.

Dessa forma, pelas propriedades $(P_1) - (P_4)$ o conjunto de pontos sobre E munido da operação soma (soma elíptica) é um grupo. Além disso, a propriedade (P_5) garante que este grupo é abeliano.

Embora tenhamos apresentado um caso particular da soma elíptica (sobre o corpo dos números reais), enfatizamos que os resultados obtidos com este caso particular pode ser generalizado para qualquer corpo K, onde a curva possa está definida sobre ele.

Com base na soma elíptica, podemos obter a multiplicação de pontos de uma curva elíptica, por um número inteiro (isto se dá de forma análoga à multiplicação de números inteiros). Neste caso, considerando P um ponto sobre uma curva elíptica E definida sobre um corpo K e um inteiro n, calculando a soma de n pontos P obtemos nP. Esta operação é conhecida como *multiplicação escalar*.

A multiplicação escalar nP pode ser realizada em um tempo curto. No entanto, não se conhece nenhum algoritmo eficiente que seja capaz de encontrar o valor de n, sendo conhecidos apenas nP e P. Este problema é conhecido como *problema do logaritmo discreto sobre curvas elípticas* e é a base dos sistemas criptográficos baseados nestas curvas. Apresentaremos abaixo uma definição formal deste problema.

Definição 3.3 *(problema do logaritmo discreto sobre curvas elípticas) Sejam K um corpo, E uma curva elíptica sobre K e P e Q pontos de E. O problema do logaritmo discreto sobre E (para a base P) consiste em encontrar um inteiro n, se existir, tal que $nP = Q$.*

Embora tenhamos um contato maior com o uso de curvas elípticas sobre o corpo dos números reais, sua utilização em sistemas criptográficos não seria prática e nem precisa. Isto está relacionado principalmente com os problemas de arredondamento ou "truncamento" apresentados neste conjunto. As aplicações criptográficas requerem uma aritmética que seja rápida e precisa, que pode ser obtida com a utilização dos corpos inteiros finitos. Por este motivo, iremos considerar a partir de agora apenas curvas elípticas definidas sobre corpos finitos.

3.2.4 Escolha do Corpo Finito

Segundo Miranda (2002), quando trabalhamos com curvas elípticas, devemos sempre levar em conta que existem dois tipos de aritméticas envolvidas. A primeira delas é comumente chamada chamada de aritmética de baixo nível, que compreende o corpo finito sobre o qual a curva está definida, este corpo é responsável por determinar o tamanho dos blocos de ciframento e também está relacionado de forma intrínseca ao tamanho das chaves do sistema criptográfico trabalhado. O segundo tipo de Aritmética envolvida está atrelado ao grupo de pontos da curva elíptica, este grupo possui como

operação básica a soma elíptica "+", de onde decorre a multiplicação escalar. Miranda (2002), destaca ainda que uma das escolhas mais importante a ser realizada é a do corpo finito F que será utilizado, pois a soma elíptica, e consequentemente a multiplicação escalar, consiste de um conjunto de operações de baixo nível.

Tendo em vista a importância da escolha do corpo finito para a implementação de um sistema baseado em curvas elípticas, a literatura recomenda (sem restrição) três tipos de corpos finitos para este fim. O primeiro destes compreende os corpos $GF(p)$, onde p é um número primo grande; o segundo corpo corresponde aos Corpos de Extensão Ótima e o terceiro compreende os corpos de Galois de característica 2, conhecidos como corpos binários.

Neste trabalho não iremos descrever a estrutura destes corpos. Aos interessados indicamos [23].

3.2.5 O Algoritmo

Segundo Miranda (2002), como o problema do logaritmo discreto sobre o grupo de pontos de uma curva elíptica é análogo ao problema do logaritmo discreto sobre o grupo multiplicativo dos corpos finitos, é possível adaptar alguns algoritmos criptográficos que são originalmente apresentados sobre corpos finitos ao grupo elíptico. Algumas vezes, não é necessário passar pelo processo de adaptação do algoritmo, ou seja, a aplicação do mesmo pode ser realizada de forma imediata. Deste modo, pode-se perceber que o algoritmo criptográfico sobre curvas elípticas não é único.

A seguir, apresentaremos um algoritmo criptográfico de ciframento e deciframento baseado em curvas elípticas, faremos isto a partir do algoritmo criptográfico do sistema ElGamal [1].

Neste trabalho não apresentaremos os detalhes do problema do logaritmo discreto sobre o grupo multiplicativo dos corpos finitos. Algumas considerações sobre este problema podem ser vistas em [17].

[1] O ElGamal é um sistema criptográfico assimétrico, que foi desenvolvido entre os anos de 1984 e 1985 pelo criptógrafo egípcio Taher Elgamal. Este sistema criptográfico baseia-se na dificuldade de solucionar o problema do logaritmo discreto para determinados grupos cíclicos.

Geração de Chaves

Inicialmente deve-se escolher o corpo finito (F_q) sobre o qual será definida a curva elíptica E, ambos conhecidos publicamente. Em seguida, escolhe-se um ponto base $T \in E$. Com isso, cada usuário seleciona um inteiro aleatório a e mantém em segredo. O número inteiro a escolhido pelos usuários será a chave privada destes, que em seguida geram as suas chaves públicas dadas por aT.

Algoritmos de Ciframento e Deciframento

Ciframento: Seja M uma mensagem mapeada em um ponto $P_m \in E$. Para que um usuário **A** envie a mensagem M à um usuário **B**, ele deve escolher um número inteiro k e enviar o par de pontos $(kT,\ P_m + k(a_BT))$, onde a_BT é a chave pública de B.

Deciframento: Para ler a mensagem, B multiplica o primeiro ponto do par pela sua chave privada a_B e subtrai o resultado do segundo ponto:

$$P_m + k(a_BT) - a_B(kT) = P_m.$$

Assim, A disfarçou a mensagem P_m somando $k(a_BT)$. Neste caso, mesmo a_BT sendo conhecida publicamente, somente quem possuir a chave privada a_B poderá decodificar a mensagem cifrada. Um intruso **C** que tiver acesso a mensagem P_m enviada de **A** para **B** não poderá decifrá-la, a menos que consiga solucionar o *problema do logaritmo discreto* sobre E, o que atualmente é praticamente impossível.

3.2.6 Criptografia RSA X Criptografia Baseada em Curvas Elípticas

Como já foi destacado anteriormente, a segurança dos sistemas criptográficos baseados em curvas elípticas está relacionada a dificuldade de solucionar o problema do logaritmo discreto sobre estas curvas. De acordo com Miranda (2002), este problema é atualmente considerado de dificuldade superior ao problema da fatoração de inteiros (que garante a segurança do sistema criptográfico RSA). Por esse motivo, os sistemas criptográficos baseados nestas curvas podem ser utilizados com parâmetros bem menores do que os do sistema RSA, tal como a chave criptográfica, o que leva a

uma diminuição do consumo de recursos computacionais, isto acarreta em um maior desempenho do sistema, sendo que é fornecido o mesmo nível de segurança do sistema RSA. Esta característica dos sistemas criptográficos baseados em curvas elípticas faz com que estes sejam fortes candidatos para aplicações em dispositivos limitados, como os telefones celulares, tablets, iPhones, entre outros. Devido ao surgimento e desenvolvimento de tais aplicações, o interesse por curvas elípticas como a base de sistemas criptográficos vem aumentando cada vez mais.

Um problema que poderíamos encontrar na adoção de criptossistemas baseados em curvas elípticas seria a questão de se definir alguns parâmetros antes de executar o algoritmo de cifragem/decifragem. Pois, antes disso devemos escolher um corpo finito sobre o qual iremos definir a curva elíptica, e com isso encontraremos o grupo de pontos sobre esta curva sobre o qual as operações aritméticas serão definidas. Se estes parâmetros não forem bem escolhidos, podemos obter um sistema criptográfico inseguro. Com isso, percebemos que este é um processo bem complicado comparado com o processo para encontrar os parâmetros do sistema RSA. No entanto, com a preocupação em relação à segurança dos sistemas baseados nestas curvas, algumas empresas oferecem listas de curvas e de parâmetros que garantem a segurança destes sistemas criptográficos.

Como já vimos nas subseções (3.1.2) e (3.1.3), para gerar chaves no RSA temos as seguintes exigências: obter números aleatórios para candidatos a primos, testar se estes candidatos são realmente primos e solucionar uma congruência para determinar o expoente d. Este processo deve ser realizado exclusivamente pelo proprietário do par de chaves, de forma segura e sem erros. Já no sistema baseado em curvas elípticas, se conhecermos os parâmetros do sistema, precisamos apenas escolher um número inteiro a, que será a chave privada e em seguida gerar a chave pública, que será dada por $Q = aP$, onde P e Q são dois pontos da curva. Em outras palavras, a geração do par de chaves no sistema baseado em curvas elípticas requer apenas a capacidade de obter números aleatórios e calcular multiplicações escalares, o que é considerado uma operação normal neste sistema. Dessa forma, se os parâmetros do sistema baseado em curvas elípticas já forem conhecidos, então encontrar as chaves deste sistema é mais simples e rápido do que encontrá-las no RSA.

3.3 O Futuro da Segurança dos Sistemas Criptográficos Assimétricos

Em nosso trabalho evidenciamos que a criptografia assimétrica consiste na utilização de duas chaves criptográficas, a chave pública que serve para criptografar a mensagem e a chave privada que serve para decriptografar.

De acordo com Oliveira (2004), para que a segurança de um sistema criptográfico assimétrico seja garantida é necessário que sejam definidas funções e chaves criptográficas de forma que, mesmo que um intruso possua a chave pública do sistema ele não conseguirá decriptografar a mensagem sem ter o conhecimento da chave privada. Esta ideia é reforçada por Rieznik e Rigolin (2005), que afirmam que a segurança destes sistemas é garantida pelo grau de complexidade dos conceitos matemáticos inerentes ao algoritmo de decodificação, algoritmo este que serviria para recuperar o conteúdo de uma mensagem criptografada sem o conhecimento da chave privada.

Como destacamos, a segurança do sistema criptográfico RSA está baseada no problema da fatoração de inteiros e a segurança do sistema criptográfico baseado em curvas elípticas está apoiada no problema do logaritmo discreto sobre estas curvas. Esta segurança se dá devido ao fato de que, esses problemas não podem ser solucionados através dos algoritmos computacionais clássicos existentes. No entanto, Barros e Schechter (2013) destacam que problemas como estes seriam solucionados com o surgimento do computador quântico.

Não iremos descrever o funcionamento de um computador quântico. Contudo, tendo como base as ideias de Barros e Schechter (2013), salientamos que devido alguns fenômenos utilizados da Mecânica Quântica, os computadores quânticos podem ser capazes de realizar tarefas muito mais rápido (bilhões de vezes mais rápido) do que um computador clássico.

Conclusão

Neste trabalho apresentamos alguns aspectos históricos da criptografia, evidenciando a importância da "luta" entre os criadores e decifradores de códigos para o desenvolvimento da Matemática e da Tecnologia. Apresentamos também o embasamento teórico necessário para a compreensão da Criptografia RSA e da Criptografia baseada em curvas elípticas e finalmente, fizemos uma breve comparação entre estes sistemas criptográficos.

Desse modo, foi possível perceber que o sistema RSA tem como principal fator de segurança o problema da fatoração de inteiros. Sabemos que a decomposição de números inteiros (muito grandes) em fatores primos, precisaria de um poder computacional ainda não existente. No entanto, a capacidade computacional vem crescendo continuamente, gerando uma preocupação acerca da segurança do sistema criptográfico RSA. Com isso, há a necessidade de que os parâmetros deste sistema sejam aumentados. Por outro lado, os sistemas criptográficos baseados em curvas elípticas são capazes de garantir o mesmo nível de segurança do sistema RSA utilizando parâmetros bem menores. Isso faz com que os sistemas criptográficos baseados nessas curvas sejam considerados ideais para aplicações criptográficas em dispositivos limitados.

Referências Bibliográficas

[1] BARBOSA, Júlio César da. *Criptografia de chave pública baseada em curvas elípticas.*
Disponível em: http://www.lockabit.coppe.ufrj.br/sites/lockabit.coppe.ufrj.br/files/publicacoes/lockabit/eccmono.pdf.
Acessado em: 09/12/2014.

[2] BARROS, Charles F. de; L. Menasché Schechter. *Uma análise do sistema de criptografia GGH-YK.*
Disponível em: http://www.sbmac.org.br/cmacs/cmac-se/2013/trabalhos/PDF/4-257.pdf.
Acessado em: 21/02/2015.

[3] BERGAMASCHI, Sidnei; Wilson M. Yonezawa. *Internet e Comércio Eletrônico: uma visão geral.*
Disponível em: http://www.ead.fea.usp.br/Semead/3semead/pdf/MQI/ART122.-PDF.
Acessado em: 23/12/2014.

[4] CAVALCANTE, André L. B. *Teoria dos números e criptografia.*
Disponível em: http://www.ebah.com.br/content/ABAAAAayYAA/teoria-dos-numeros-criptografia.
Acessado em: 01/02/2014.

[5] COUTINHO, S. Collier. *Criptografia.*
Disponível em: http://www.obmep.org.br/docs/Apostila7-Criptografia.pdf.
Acessado em: 10/12/2014.

[6] COUTINHO, S. Collier. *Números inteiros e criptografia RSA*. 2ª ed. Rio de Janeiro: IMPA, 2011.

[7] CECHINEL, Cristian; Fabricio Ferrari. *Introdução a algoritmos e programação*. Disponível em: http://www.ferrari.pro.br/home/documents/FFerrari-CCechinel-Introducao-a-algoritmos.pdf.
Acessado em: 19/12/2014.

[8] CRUZ, Edilson Fernandes da. *A criptografia e seu papel na segurança da informação e das comunicações (SIC) - retrospectiva, atualidade e perspectiva*. 2009. 84f. Monografia (Especialização em Gestão de Segurança da Informação e Comunicações) - Departamento de Ciência da Computação. Universidade de Brasilia, Brasilia.

[9] DAHAB, Ricardo; HÉRNANDEZ, Júlio C. Lopez. *Técnicas criptográficas modernas: algoritmos e protocolos*. 2007. 73f. Dissertação (Mestrado em Ciência da Computação) - Instituto de Computação. Universidade Estadual de Campinas, Campinas.

[10] DOMINGUES, Hygino H. *Fundamentos de aritmética*. São Paulo: Atual, 1991.

[11] FIGUEIREDO, Luiz Manoel. *Introdução à Criptografia*. Rio de Janeiro: UFF/CEP-EB, 2010.

[12] FLOSE, Vania Batista Schunck. *Criptografia e curvas elipticas*. 2011. 57f. Dissertação (Mestrado Profissional em Matemática) - Instituto de Geociências e Ciências Exatas. Universidade Estadual Paulista, São Paulo.

[13] FRALEIGH, John B. *A first course in abstract algebra*. 6° ed. Boston: Addisson-Wesley Publishing Company, 1998.

[14] GONÇALVES, Adilson. *Introdução à Álgebra*. 5ª ed. Rio de Janeiro: IMPA, 2007.

[15] *Grafometro, incertezza dimensionale, disco cifrante: le nuove acquisizione del mateureka*.

Disponível em: http://www.mateureka.it/notizie/grafometro-incertezza-dimensionale-disco-cifrante-le-nuove-acquisizione-del-mateureka.html.
Acessado em: 02/01/2015.

[16] HEFEZ, Abramo. *Elementos de Aritmética.* 2ª ed. Rio de Janeiro: SBM, 2005.

[17] KOBLITZ, Neal. *A course in number theory and cryptography.* 2ª ed. Siatle: Graduate texts in mathematics, 1948.

[18] KOLIVER, Cristian; Bruno Tonet. *Introdução aos algoritmos.*
Disponível em: http://www.cefetsp.br/edu/adolfo/disciplinas/lpro/materiais/Linguagem_Visualg2.0.pdf.
Acessado em: 19/12/2014.

[19] MANZANO, José Horta. *O Segredo é a alma do negócio.*
Disponível em: http://brasildelonge.com/tag/segunda-guerra/.
Acessado em: 03/01/2015.

[20] MARQUES, Leonardo Garcia. *Curvas Elipticas: aplicações criptográficas* 2007. 109f. Monografia (Graduação em Ciência da Computação) - Departamento de Ciências da Computação. Universidade Federal de Goiás, Catalão.

[21] MARINS, Marina Tebet A; Solimá Gomes Pimentel. *A evolução da criptografia a partir dos números primos.* [S.l.], 2011.

[22] MELLO, Cláudio Gomes de. *Codificação livre de prefixo para cripto-compressão.*
Disponível em: http://www.maxwell.vrac.puc-rio.br/9932/9932_4.PDF.
Acessado em: 19/12/2014.

[23] MIRANDA, Rogério Albertoni. *Criptossistemas baseados em curvas elipticas.* 2002. 98f. Dissertação (Mestrado em Ciência da Computação) - Instituto de Computação. Universidade Estadual de Campinas, Campinas.

[24] MUNIZ NETO, Antonio Caminha. *Tópicos de matemática elementar: teoria dos números.* Vol.5, 2ª ed. Rio de Janeiro: SBM, 2012.

[25] OLIVEIRA, Anderson Gomes de. *Criptografia usando protocolos quânticos* 2004. 110f. Monografia (Especiaização em Administração de Redes Linux) - Departamento de Ciências da Computação. Universidade Federal de Lavras, Minas Gerais.

[26] *Repple.*
Disponível em: https://repple.ru/science/kak-sformirovalas-kriptografiya/.
Acessado em: 03/01/2015.

[27] *RSA-2003.*
Disponível em: http://www.usc.edu/dept/molecular-science/RSA-2003.htm.
Acessado em: 05/02/2015.

[28] RIBENBOIM, Paulo. *Velhos mistérios e novos recordes.* 1ª ed. Rio de Janeiro: IMPA, 2012.

[29] RIEZNIK, Andrés Anibal; Gustavo Rigolin. *Introdução à criptografia quântica.*
Disponível em: http://www.scielo.br/pdf/rbef/v27n4/a04v27n4.pdf.
Acessado em: 21/02/2015.

[30] ROCHA, Roldão da. *Álgebra linear.*
Disponível em: http://posmat.ufabc.edu.br/attachments/043_livro%20algebra%20linear%20roldao.pdf.
Acessado em: 10/12/2014.

[31] SANGALLI, Leandro Aparecido; Marco Aurélio Amaral Henriques. *Criptossistemas baseados em curvas elípticas e seus desafios.*
Disponível em: http://www.dca.fee.unicamp.br/portugues/pesquisa/seminarios/2012/artigos/217.pdf.
Acessado em: 08/12/2014.

[32] SANTOS, José Plínio de Oliveira. *Introdução à Teoria dos Números.* 3ª ed. Rio de Janeiro: IMPA, 2007.

[33] SINGH, Simon. *O livro dos códigos.* Trad. Jorge Calife. 6ª ed. Rio de Janeiro: Record, 2007.

[34] STALLINGS, William. *Criptografia e segurança de redes*. 4ª ed. São Paulo: Pearson Prentice Hall, 2008.