Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Câmpus de Rio Claro

O uso de elementos da Criptografia como estímulo matemático na sala de aula.

Leandro Rodrigues de Carvalho

Dissertação apresentada ao Programa de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional como requisito parcial para a obtenção do grau de Mestre

Orientadora
Profa. Dra. Erika Capelato

2016

512.7 Carvalho, Leandro Rodrigues de
C331u O uso de elementos da criptografia como estímulo matemático na sala de aula / Leandro Rodrigues de Carvalho. - Rio Claro, 2016
78 f. : il., figs., tabs., fots.

Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas
Orientador: Erika Capelato

1. Teoria dos números. 2. Números primos. 3. Cifra de César. 4. Atividade para sala de aula. I. Título.

Ficha Catalográfica elaborada pela STATI - Biblioteca da UNESP
Campus de Rio Claro/SP

TERMO DE APROVAÇÃO

Leandro Rodrigues de Carvalho

O uso de elementos da Criptografia como estímulo matemático na sala de aula.

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Profa. Dra. Erika Capelato
Orientadora

Profa. Dra. Renata Zotin Gomes de Oliveira
Departamento de Matemática IGCE - UNESP

Profa. Dra. Camila Fernanda Bassetto
Faculdade de Ciências e Letras - UNESP

Rio Claro, 28 de Abril de 2016

Dedico este trabalho a minha querida esposa e companheira Cris...

Agradecimentos

Primeiramente agradeço a DEUS, grande criador do universo, sem ele nem mesmo estaríamos aqui. Aos meus pais por terem me concebido e criado com todo amor e carinho. Agradeço imensamente a minha companheira e esposa Cristiane pelo apoio e motivação e aos nossos gatos que sempre me acompanharam nas madrugadas de estudo.

Em especial a minha orientadora Érika Capelato, pelas orientações e correções, sempre solícita e educada.

A todos os professores do curso, pela dedicação e paciência, o meu aprendizado foi além dos conteúdos. Em especial agradeço a professora Renata Zotin Gomes de Oliveira, pelas orientações referentes ao capítulo sobre a Teoria dos Números e a professora Suzinei Marconato, coordenadora deste programa durante minha trajetória, que sempre nos auxiliou de maneira prestimosa.

Não poderia me esquecer dos amigos e amigas de turma, no começo parecia uma competição (saudável) e ao longo do curso se transformou em companheirismo e dedicação, percebemos que dividir conhecimento só nos engrandece. Foram tantas as amizades que seria injusto esquecer alguns nomes, por isso achei melhor omiti-los, mas todos estão no meu coração.

Para finalizar, agradeço a todos os funcionários da UNESP/Rio Claro: portaria, biblioteca, segurança e limpeza, que propiciam um ambiente salutar e agradável ao meu aprendizado.

A matemática é o alfabeto com o qual DEUS escreveu o universo.

Pitágoras

Resumo

O grande desafio no ensino da matemática, pelo menos no meu ponto de vista como professor nos últimos dez anos, é fazer com que os alunos percebam a importância e a praticidade da matemática em suas vidas. Isso vai além das teorias da Aritmética, Álgebra ou Geometria ensinadas na educação básica. Os alunos precisam perceber que os conceitos matemáticos são ferramentas que os ajudam a compreender o mundo a sua volta. Diante disto, esta dissertação busca apresentar conceitos matemáticos que levam à compreensão da Criptografia: conceitos da Teoria dos Números e da Álgebra. Fazemos ainda, um breve histórico sobre a Criptografia descrevendo a cifra de César e as cifras afins, o Sistema RSA e alguns métodos de troca de chaves. Relatamos alguns trabalhos desenvolvidos pelos estudantes do PROFMAT neste tema e apresentamos uma proposta de atividade para os estudantes do ensino básico. Esta atividade consiste na construção de um kit de encriptação e decriptação utilizando copos descartáveis. Com dinâmicas unindo elementos da Criptografia e o aplicativo Whatsapp, como meio de troca das mensagens criptografadas, motivamos a sala de aula para o aprendizado da Divisão Euclidiana e da Permutação. Além disso, pretendemos despertar nos alunos o interesse em aprofundar-se nos estudos da Matemática, principalmente na Teoria dos Números, já que esta é uma das ferramentas fundamentais no contexto da Criptografia, uma ciência com grande aplicabilidade na atualidade.

Palavras-chave: Teoria dos Números, Números Primos, Cifra de César, Criptografia, Atividade para sala de aula.

Abstract

The great challenge in teaching mathematics, at least in my point of view as a teacher in the past ten years is to make students understand the importance and practicality of mathematics in their lives. This goes beyond the theories of arithmetic, algebra or geometry taught in basic education. Students need to realize that mathematical concepts are tools that help them understand the world around them. In view of this, this dissertation aims to present mathematical concepts that lead to understanding of cryptography: concepts of number theory and algebra. We also a brief history on the Encryption describing the Caesar cipher and related figures, the RSA system and some methods of key exchange. We report some work done by students PROFMAT this theme and present a proposal activity for students of basic education. This activity consists in building a kit of encryption and decryption using disposable cups. With dynamic linking elements Encryption and Whatsapp application as a means of exchange of encrypted messages, we motivate the classroom for learning Euclidean division and permutation. In addition, we intend to arouse students' interest in deepening the study of mathematics, especially in Number Theory, as this is one of the fundamental tools in the context of cryptography, a science with great applicability today.

Keywords: Number Theory, Primes Number, Caesar Cipher, Cryptography, activity to classroom.

Lista de Figuras

Lista de Tabelas

Sumário

1 Introdução

A iniciativa para o tema do presente trabalho surgiu da necessidade em motivarmos os estudantes do ensino básico nas aulas de matemática. Durante dez anos lecionando matemática nas escolas estaduais e particulares da região de Americana-SP para estudantes do quinto ao nono ano do ensino fundamental e do primeiro ao terceiro ano do ensino médio, sempre me deparei com um grande número de alunos que faziam as mesmas perguntas: "...para que serve esse conteúdo?"ou "...onde usarei isso?" Encontrar razões para se aprender matemática parecem óbvias para quem, pela própria natureza e beleza da matemática, se interessa por esta ciência. Porém, para um grande número de alunos que tem fobia ou aversão ao seu estudo, isto não é uma tarefa fácil. Atualmente, as facilidades do cotidiano de um estudante, onde quase tudo já vem "calculado", causa a falsa ilusão de que não há necessidade de se aprender matemática além das operações fundamentais. Nesse sentido associar um conceito matemático, que vai além das situações comuns do dia a dia, a algo concreto ou que faça parte da realidade dos estudantes pode melhorar o seu interesse pela matemática.

Com base na premissa acima, surgiu a ideia de utilizarmos a criptografia, ou seus conceitos mais elementares, para auxiliar o desenvolvimento do aprendizado matemático com a utilização do smartphone através do uso de um software de mensagem instantânea.

Pesquisando sobre trabalhos relacionados à criptografia na plataforma do PROFMAT encontramos onze dissertações sobre este tema defendidas no ano de 2013, treze no ano de 2014 e dez no ano de 2015. A seguir fazemos uma síntese sobre alguns dos trabalhos que nos chamaram mais a atenção.

O autor em [18], faz um levantamento histórico da criptografia, abordando como a matemática auxilia a criptografia, fazendo uso dos conceitos da teoria dos números. Apresenta as perspectivas para o futuro da criptografia, através da criptografia quântica e pós-quântica e suas implicações para o futuro, porém não apresenta proposta de atividades para sala de aula.

Em [19] o autor tem como foco principal o sistema criptográfico RSA. Iniciando com uma síntese da teoria dos números, o autor também aborda os aspectos históricos da criptografia, suas origens e motivações. Finaliza o trabalho com a implementação de um algorítimo criptográfico baseado em RSA, utilizando exemplos para auxiliar a

compreensão.

Uma reflexão sobre a educação matemática e suas implicações no uso da teoria dos números no ensino fundamental é feita em [3]. Além disso, a autora apresenta a história da criptografia com ênfase no algoritmo RSA, em seguida apresenta um estudo da situação do ensino da matemática no Brasil entre os anos de 1995 e 2005, incluindo as dificuldades e desafios ao aprendizado matemático. Para finalizar, apresenta uma proposta de trabalho com foco na criptografia intuitiva, através da escrita em Braille e a utilização da cifra de César para auxílio do ensino da matemática na sala de aula.

Em [9] o autor começa com a história da criptografia, origens e métodos antigos de ocultação de mensagens até a criptografia utilizada atualmente nos computadores. Aborda conceitos da Álgebra e aritmética necessários para compreensão do sistema criptográfico baseado no protocolo Diffie-Hellman. Este trabalho apresenta três propostas de atividades para uso da criptografia em sala de aula. Na primeira proposta, apresenta o uso de funções para criação de um sistema de criptação e decriptação de mensagens com os alunos. A segunda proposta utiliza matrizes como elemento central do sistema criptográfico. Por último apresenta uma forma de se criar um sistema criptográfico baseado no protocolo Diffie-Hellman para troca de mensagens secretas entre grupos de alunos. Em todas as propostas o autor especifica cada parte como trabalhar com os alunos.

O trabalho [11] tem como objetivo a utilização das equações diofantinas e a criptografia. Na parte das equações diofantinas o autor utiliza uma situação problema envolvendo compras de mercadorias. Em seguida apresenta os sistemas criptográficos baseados na cifra de César e RSA com o auxílio do Excel para realização dos cálculos, porém não apresenta proposta para utilização em sala de aula.

No trabalho [7] o autor faz uma introdução à criptografia e depois apresenta um resumo da teoria dos números necessária para o entendimento do sistema RSA. Por fim, utiliza o *software Maxima* para o desenvolvimento dos cálculos necessários para implementação do sistema criptográfico RSA. Este trabalho também não apresenta proposta para se trabalhar com alunos em sala de aula.

É possível observarmos ainda que a literatura apresenta uma grande diversidade de trabalhos que aplicam a criptografia no ensino de conteúdos matemáticos. Assim, a motivação principal desta dissertação é contribuir para a discussão que vem sendo feita pelos estudantes do PROFMAT e de outros pesquisadores, que veem neste tema, elementos motivadores dentro da sala de aula da disciplina de Matemática.

No primeiro capítulo, discorremos sobre as motivações do presente trabalho e em seguida há uma síntese de algumas dissertações de mestrado profissional realizadas sobre o tema, criptografia. No segundo capítulo abordamos alguns conceitos básicos da Teoria dos Números, pois atualmente esta teoria é umas das principais ferramentas da criptografia moderna, tais como, números primos, classes de congruência e testes de primalidade. No terceiro capítulo abordamos, dentre outros elementos da álgebra,

o tema curvas elípticas, necessário para o entendimento do conceito de criptografia baseado em tais curvas. No quarto capítulo há uma síntese dos principais elementos da criptografia, sua história e motivações. No quinto capítulo, há uma proposta de atividade baseada em um vídeo do youtube referente a uma aula de introdução a criptografia do MIT (Massachusetts Institute of Technology), na qual fazem a construção de um kit de encriptação e decriptação utilizando copos descartáveis. Nossa proposta tem como público alvo alunos dos anos finais da educação básica e utiliza-se, além do kit de copos, dinâmicas com os elementos da criptografia e o aplicativo de mensagens Whatsapp como meio de troca de mensagens criptografadas entre os grupos de alunos. Nosso objetivo é motivar os alunos para o aprendizado de alguns conceitos da Matemática, bem como despertar o seu interesse em aprofundar os seus estudos na Matemática.

2 Teoria dos Números - conceitos básicos

A teoria dos números é um ramo da Matemática que teve sua origem na antiga Grécia e hoje, inspira, dentre outras aplicações, o processo de criptografia em transações financeiras. Alguns problemas em teoria dos números demoraram séculos para serem resolvidos, como por exemplo o *último teorema de Fermat* que instigou muitos pesquisadores durante mais de 300 anos e foi finalmente demonstrado por Andrew Wiles em 1995. Este capítulo está dedicado ao estudo de propriedades básicas dos números inteiros e os resultados foram retirados de [10] e [12].

2.1 Conjunto dos números inteiros $\mathbb{Z}$

O conjunto dos números inteiros, denotado por $\mathbb{Z}$, cujo símbolo vem da palavra *Zahlen* (que significa número em alemão) é a união do conjunto dos números naturais $\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6...\}$, já incluindo o zero, e o conjunto dos números naturais "negativos"$\{-1, -2, -3, -4, -5, -6, \cdots\}$ ou seja,

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

Assumiremos axiomaticamente que existem duas operações no conjunto dos números inteiros, a adição e a multiplicação, denotadas respectivamente como $a + b$ e $a \cdot b$ (ou simplesmente ab), para quaisquer inteiros $a, b \in \mathbb{Z}$, satisfazendo as seguintes propriedades:

Propriedade 2.1. Fechamento: $a+b$ e $a \cdot b$ são inteiros sempre que a e b forem inteiros.

Propriedade 2.2. Comutativa: $a + b = b + a$ e $a \cdot b = b \cdot a$, para quaisquer inteiros a e b.

Propriedade 2.3. Associativa: $(a + b) + c = a + (b + c)$ e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. para quaisquer inteiros a, b e c.

Propriedade 2.4. Distributiva: $(a+b) \cdot c = a \cdot c+b \cdot c$, para quaisquer a, b e c inteiros.

Propriedade 2.5. Existência de elemento neutro: $a + 0 = 0 + a$ e $a \cdot 1 = 1 \cdot a$, para todo inteiro a, sendo 0 e 1 elementos neutros das operações de adição e multiplicação, respectivamente.

Propriedade 2.6. Existência de inverso aditivo: Para todo inteiro a , com $a \neq 0$, existe um inteiro x tal que $a + x = 0$. Esse inteiro x é denominado inverso aditivo ou simétrico de a, denotado por $-a$. Dessa forma a subtração é definida como como $a + (-b) = a - b$ para quaisquer inteiros a e b.

2.2 Módulo de um número inteiro

O módulo, ou valor absoluto, de um número inteiro a é denotado como $|a|$ que, geometricamente, é interpretado como a distância entre o número inteiro a e a origem da reta numérica.

Definição 2.1. *Seja a um inteiro qualquer. Definimos:*

$$|a| = a \text{ se } a \geq 0.$$
$$|a| = -a \text{ se } a < 0.$$

O módulo de um número inteiro a também pode ser definido como $|a| = \sqrt{a^2}$ e possui a seguinte propriedade:

Propriedade 2.7. Sejam a e b quaisquer números reais. Então

1. $|a| \geq 0$
2. $|a| = 0 \iff a = 0$
3. $|a| = |-a|$.
4. $|ab| = |a||b|$.
5. $|a + b| \leq |a| + |b|$ (desigualdade triangular).

2.3 Conceitos fundamentais de Divisibilidade

Dados dois inteiros a e b, com $a \neq 0$, dizemos que a divide b, denotado por $a \mid b$, se existir um inteiro c tal que $b = ac$. Se a não divide b denotamos por $a \nmid b$. Além disso, b/a indica o quociente: b dividido por a. A seguir enumeramos uma série de propriedades da divisão:

Propriedade 2.8. Sejam a, b, c, m e n inteiros quaisquer. Então seguem as seguintes propriedades:

1. $1 \mid a$.
2. $a \mid a$.
3. $a \mid 0$.
4. $a \mid b$ e $b \neq 0 \Rightarrow |a| \leq |b|$.
5. $a \mid b$ e $b \mid a \Rightarrow |a| = |b|$.
6. $a \mid b$ e $b \mid c \Rightarrow a \mid c$.
7. $c \mid a$ e $c \mid b \Rightarrow c \mid (ma + nb)$, quaisquer que sejam $m, n \in \mathbb{Z}$.
8. $a \mid b$ e $a \neq 0 \Rightarrow (b/a) \mid b$.

Demonstração. A demostração de 1 e 2 está garantida pela Proposição 2.5 e a demonstração de 3 sai do inverso aditivo na Proposição 2.6.

Para a demonstração de 4: se $a|b$ então existe um inteiro c tal que $b = ac$, mas $|a| \leq |a||c| = |ac| = |b|$, da mesma forma, demonstramos 5.

Para demonstrarmos 6: se $a|b$ e $b|c$, por definição existem m e n inteiros tais que $b = ma$ e $c = nb \Rightarrow c = n(ma)$ ou $c = (nm)a$, portanto $a \mid c$.

Na demonstração de 7: existem $p, q \in \mathbb{Z}$, tais que $a = pc$ e $b = qc$. Multiplicando estas igualdades por m e n, respectivamente, teremos $ma = mpc$ e $nb = nqc$. Somando os membros $ma + nb = mpc + nqc$ ou $ma + nb = c(mp + nq) \Rightarrow c \mid (ma + bn)$.

Na demonstração de 8 temos, por hipóteses que $b = ma$, para algum inteiro m, então b/a é um inteiro. Como $a \neq 0$ temos $(b/a) \cdot a = b$ que implica $(b/a) \mid b$. □

Exemplo 2.1. Os próximos exemplos ilustram alguns itens do resultado acima:

i) $3 \mid 6$ e $6 \mid 24$ então $3 \mid 24$ (item 6).

ii) $3 \mid 6$ e $3 \mid 9$ então $3 \mid (5 \cdot 6 + 7 \cdot 9)$ o que nos dá $3 \mid 93$ (item 7).

iii) $3 \mid 6$ e $6/3 = 2$ implica $2 \mid 6$ (item 8).

2.4 Algoritmo Euclidiano da divisão

Dados dois números inteiros não negativos a e b, com $b \neq 0$, na divisão de a por b, sempre existem números inteiros q (quociente) e r (resto) que satisfazem a seguinte relação:

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

Essa relação é chamada de algoritmo Euclidiano da divisão (esse algoritmo apareceu no livro VII dos "Elementos"de Euclides, por volta do ano 300 a.C) e também se aplica a números inteiros negativos. Quando $r = 0$, ou seja, o resto é zero, dizemos que a divisão é exata. Se $b \nmid a$ então r satisfaz a desigualdade estrita $0 < r < a$.

Exemplo 2.2. A divisão de 21 por 4, tem como resultado o inteiro 5 e o resto 1, assim $21 = 5.4 + 1$.

O próximo resultado será usado para demonstrar o principal Teorema desta seção.

Teorema 2.1. *(Teorema de Eudoxius) Dados os inteiros a e b, com $b \neq 0$, então a é múltiplo de b ou encontra-se entre dois múltiplos consecutivos de b. Isto é, existe um inteiro k tal que $kb \leq a < (k+1)b$.*

Teorema 2.2. *(Algoritmo Euclidiano) Sejam a e b inteiros, $b \neq 0$. Existe um único par de inteiros q e r, chamados, respectivamente, de quociente e resto da divisão euclidiana de a por b, tais que $a = bq + r$ com $0 \leq r < |b|$.*

Demonstração. Supondo $b > 0$, o caso $b < 0$ é análogo.

Se $a = 0$, basta tomar $q = r = 0$.

Se $a \neq 0$, pelo Teorema Eudoxius, existe q satisfazendo $qb \leq a < (q+1)b$, que implica $0 \leq a - qb$ e $a - qb < b$. Para demonstrar a unicidade, supomos que a existência de outro par q_1 e r_1:

$$a = q_1 b + r_1, \text{ com } 0 \leq r_1 < b.$$

Assim temos $a - a = 0$ então $(qb + r) - (q_1 b + r_1) = 0$ que implica em $b(q - q_1) = r_1 - r$, concluímos que $b \mid (r_1 - r)$. Mas como $r_1 < b$ e $r < b$, temos $\mid r_1 - r \mid < b$, se $b \mid (r_1 - r)$ devemos ter $r_1 - r = 0$ o que implica em $r = r_1$. Como $b \neq 0$ temos $q - q_1 = 0$ que implica $q = q_1$. □

Podemos encontrar outra demonstração para o Algoritmo Euclidiano usando o Princípio da Boa Ordenação[1] em [12].

2.5 Números Primos

Um número inteiro n com $(n > 1)$ que possua apenas dois divisores positivos: o 1 e o próprio n, é chamando de número primo. Como por exemplo, a seguinte sequência: $2, 3, 5, 7, 11, 13, 17, 19, 23...$

Apesar da aparente simplicidade, a sequência dos números primos representa um desafio supremo, que atravessa gerações de grandes matemáticos, devido ao seu caráter caótico e aleatório. Segundo [15] esses números são os próprios átomos da natureza, devido a sua capacidade de gerar os demais números.

Teorema 2.3. *(Teorema Fundamental da Aritmética) Todo inteiro maior que 1 pode ser representado de maneira única, a menos da ordem, como o produto de fatores primos.*

[1] Todo subconjunto não vazio $A \subseteq \mathbb{N}$ possui um elemento menor que todos os outros elementos deste.

Demonstração. Se n é primo não há o que se provar. Seja n composto, então $n = p_1.n_1$ onde $1 < p_1$ é um número primo e representa o menor dos divisores de n e n_1 um inteiro satisfazendo $1 < n_1 < n$. Se n_1 for primo a prova está completa, caso contrário, tomemos p_2, um número primo, como o menor fator de n_1 e $n_1 = p_2.n_2$. Então $n = p_1.p_2.n_2$.

Repetindo este processo, obtemos uma sequência decrescente de inteiros positivos $n_1, n_2, n_3, n_4, n_5, .., n_r$. Como todos os n_i são inteiros maiores do que 1, este processo deve terminar. Como os primos na sequência $p_1, p_2, p_3, ..., p_k$ não são necessariamente distintos, n terá a seguinte forma geral:

$$n = p_1^{a_1}.p_2^{a_2}.p_3^{a_3}...p_k^{a_k}$$

Para demonstrarmos a unicidade, usaremos indução em n. Para $n = 2$ a afirmação é verdadeira, para $n > 2$ temos que n pode ser primo (não há nada a provar) ou composto. Vamos supor que n seja composto e que tenha duas fatorações:

$$n = p_1.p_2.p_3...p_s = q_1.q_2.q_3...q_r$$

Para provarmos que $s = r$ e que cada p_i é igual a q_j temos: como p_1 divide o produto $q_1.q_1.q_3...q_r$ ele divide pelo menos um dos fatores q_j. Sem perda da generalidade podemos supor que $p_1 \mid q_1$, mas ambos são primos, logo $p_1 = q_1$. Temos então que $\dfrac{n}{p_1} = p_2.p_3...p_s = q_2.q_3...q_r$ e $1 < \dfrac{n}{p_1} < n$. Assim a hipótese de indução nos diz que as duas fatorações são idênticas, a menos da ordem. Concluímos, que $p_1p_2.p_3...p_s$ e $q_1.q_1.q_3...q_r$ são iguais. □

O próximo resultado é um dos mais clássicos da Matemática. De acordo com [12] até onde se conhece, a demonstração a seguir foi a primeira demonstração escrita utilizando o método de redução ao absurdo e é devida a Euclides cerca de 300 A.C.

Teorema 2.4. *(Teorema de Euclides) A quantidade de números primos é infinita.*

Demonstração. Faremos a prova por redução ao absurdo. Vamos supor que a sequência dos números primos seja finita. Consideremos $p_1, p_2, p_3, .., p_n$ a lista de todos os primos. Consideremos também o número $R = p_1+p_2+p_3+...+p_n+1$. É evidente que R é maior que todos os primos p_i, $i = 1, \cdots, n$ da lista, além de não ser divisível por nenhum dos p_i. Pelo Teorema 2.3, R é primo ou possui algum fator primo, o que implica na existência de um primo que não pertence à lista considerada. Portanto, a sequência de números primos não pode ser finita. □

2.6 Máximo divisor comum

O máximo divisor comum entre dois inteiros a e b, ambos diferentes de zero, denotado por $\text{mdc}(a, b)$ ou simplesmente (a, b), é o maior inteiro que divide a e b simultaneamente. Se $(a, b) = 1$, temos que a e b são primos entre si.

Exemplo 2.3. Temos mdc(8,12)=4, pois os divisores de 8 são $\{1, 2, 4, 8\}$ e os divisores de 12 são $\{1, 2, 3, 4, 6, 12\}$.

A seguir vamos descrever as propriedades do máximo divisor comum entre dois números inteiros.

Propriedade 2.9. Podemos demonstrar que:

1. Se $a \neq 0$ então $\text{mdc}(a, 0) = |a|$.
2. Se $a \neq 0$ então $\text{mdc}(a, a) = |a|$.
3. Temos $\text{mdc}(a, b) = \text{mdc}(b, a)$.
4. Se $a \mid b$ então $\text{mdc}(a, b) = a$.
5. Se $t \in \mathbb{Z}$, então $\text{mdc}(t \cdot a, t \cdot b) = t \cdot \text{mdc}(b, a)$.
6. Sejam $a_1, a_2, a_3, a_4, ..., a_{n-1}, a_n$ uma coleção finita de inteiros, não todos nulos. Então $\text{mdc}(a_1, a_2, a_3, a_4, ..., a_{n-1}, a_n) = \text{mdc}(a_1, a_2, a_3, a_4, ..., \text{mdc}(a_{n-1}, a_n))$.

Demonstração. As demonstrações das propriedades acima podem ser encontradas em [10]. □

Lema 2.1. *(Lema de Bézout[2]) Dados inteiros a e b, não ambos nulos, existem inteiros m e n, tais que $am + bn = mdc(a, b)$.*

Demonstração. Se a, b e c são números inteiros e se $c \mid a$ e $c \mid b$ então pela Propriedade 2.8 item 7, $c \mid am' + bn'$ quaisquer que sejam m', n' inteiros ou seja, $am' + bn' = r \cdot c$, para algum r inteiro. □

2.7 Aritmética Modular

Em [10] os autores descrevem que 1801, o proeminente jovem matemático Carl Friedrich Gauss (1777-1855) publicou seu livro intitulado *Disquisitiones Arithmeticae*, considerado o marco para o nascimento da teoria dos números como disciplina propriamente dita. Uma das contribuições desse trabalho, foi a criação da *calculadora relógio*.

Se em um relógio convencional de 12 horas que está marcando 10 horas nós adicionarmos 5 horas, o ponteiro das horas avança até as 3 horas. Assim a calculadora relógio de Gauss daria como resposta 3 e não 15. Assim, o conceito básico desta calculadora relógio consiste em fornecer o resto da divisão de um resultado por 12. Dessa forma a calculadora de Gauss tornou-se uma ferramenta muito útil para se trabalhar com números grandes. Por exemplo, mesmo sem saber o valor de 7^{99}, a calculadora relógio diz que esse número deixa resto 7 quando dividido por 12.

[2]Matemático francês Étienne Bézout (1730 – 1783).

Gauss logo percebeu que o relógio podia conter valores diferentes de 12 horas, assim desenvolveu a ideia de se realizar a *aritmética relógio* ou *aritmética modular*, também conhecida como *congruência módulo m*.

Definição 2.2. *Sejam a e b inteiros. Dizemos que a é congruente a b módulo m,* $(m > 0)$ *e denotamos por* $a \equiv b (mod\, m)$*, se* $m \mid (a - b)$*. Se* $m \nmid (a - b)$*, dizemos que a é incongruente a b módulo m e denotamos por* $a \not\equiv b (mod\, m)$*.*

Podemos ilustrar a definição acima com o seguinte exemplo:

Exemplo 2.4. $15 \equiv 3 (\text{mod } 4)$, pois $4 \mid (15 - 3)$.

Proposição 2.1. *Se a e b são inteiros, temos* $a \equiv b (mod\, m)$ *se, e somente se, existir um inteiro k tal que* $a = b + km$*.*

Demonstração. Se $a \equiv b$ (mod m), então $m \mid (a - b)$ o que implica a existência de um número inteiro k tal que $a - b = km$, isto é, $a = b + km$, a recíproca é trivial. □

O próximo resultado fornece propriedades da congruência entre dois números.

Proposição 2.2. *Se* a, b, c, m *e d são inteiros,* $m > 0$ *e* $a \equiv b (mod\, m)$*, as seguintes propriedades são verdadeiras:*

1. $a \equiv a\ (mod\ m)$*.*
2. $b \equiv a\ (mod\ m)$*.*
3. *Se* $a \equiv b\ (mod\ m)$ *e* $b \equiv d\ (mod\ m)$*, então* $a \equiv d\ (mod\ m)$*.*
4. $a + c \equiv b + c\ (mod\ m)$*, onde c é um inteiro qualquer.*
5. $a - c \equiv b - c\ (mod\ m)$*, onde c é um inteiro qualquer.*
6. $ac \equiv bc\ (mod\ m)$*, onde c é um inteiro qualquer.*

Demonstração. (1) Como $m \mid 0$ então $m \mid (a - a)$, o que implica $a \equiv a$ (mod m).

(2) Se $a \equiv b$ (mod m), então $a = b + k_1 m$, para algum inteiro k_1 logo, $b = a - k_1 m$. Se $k_2 = -k_1$ obtemos $b = a + k_2 m$, o que implica em $b \equiv a$ (mod m).

(3) Por definição, existem k_1 e k_2 tais que, $a - b = k_1 m$ e $b - d = k_2 m$, somando membro a membro obtemos $a - d = (k_1 + k_2)m$. Logo, $a \equiv d$ (mod m).

(4) Se $a \equiv b$ (mod m), existe k inteiro tal que, $a - b = km$. Temos, para qualquer c inteiro, que $a - b = (a + c) - (b + c)$, o que implica em $a + c \equiv b + c$ (mod m) .

(5) De maneira análoga à propriedade anterior, se $a \equiv b$ (mod m), existe k inteiro tal que, $a - b = km$. Para qualquer c inteiro $a - b = (a - c) - (b - c)$, o que implica em $a - c \equiv b - c$ (mod m).

(6) Se $a \equiv b$ (mod m), existe k inteiro tal que, $a - b = km$. multiplicando esta igualdade por um inteiro c obtemos $ac - bc = ckm$. Logo, $ac \equiv bc$ (mod m) . □

Além destas, outras propriedades podem ser demonstradas:

Proposição 2.3. *Se a, b, c, d e m são inteiros tais que $a \equiv b$ (mod m)e $c \equiv d$ (mod m), então valem as seguintes resultados:*

1. $a + c \equiv b + d$ (mod m).
2. $a - c \equiv b - d$ (mod m).
3. $ac \equiv bd$ (mod m).
4. $ac \equiv bc$ (mod m), então $a \equiv b$(mod m/d) onde $d = mdc(c, m)$.
5. Para qualquer inteiro $k > 0$ e $a \equiv b$(mod m), então $a^k \equiv b^k$(mod m).

Demonstração. (1) Se $a \equiv b(\text{mod } m)$e $c \equiv d(\text{mod } m)$ existem inteiros k_1 e k_2, tais que $a-b = k_1m$ e $c-d = k_2m$. Somando as igualdades obtemos, $(a+c)-(b+d) = (k_1+k_2)m$. Logo, $a + c \equiv b + d(\text{mod } m)$.

(2) Se $a \equiv b(\text{mod } m)$ e $c \equiv d(\text{mod } m)$, existem inteiros k_1 e k_2 tais que $a - b = k_1m$ e $c - d = k_2m$. Subtraindo as igualdades obtemos $(a - c) - (b - d) = (k_1 - k_2)m$. Logo, $a - c \equiv b - d(\text{mod } m)$.

(3) Se $a \equiv b(\text{mod } m)$ e $c \equiv d(\text{mod } m)$ existem inteiros k_1 e k_2, tais que $a - b = k_1m$ e $c - d = k_2m$. Multiplicando a primeira igualdade por c e a segunda por b obtemos $ac - bc = ck_1m$ e $bc - bd = bk_2m$. Somando as últimas igualdades, obtemos $ac - bd = (ck_1 + bk_2)m$. Logo, $ac \equiv bd(\text{mod } m)$.

(4) Como $ac \equiv bc(\text{mod } m)$, existe um inteiro k tal que $ac - bc = c(a - b) = km$. Se dividirmos os dois membros por d, teremos $(c/d)(a - b) = k(m/d)$. Assim, $(m/d)|(c/d)(a-b)$ e como $\text{mdc}(m/d, c/d) = 1$, usando o fato que $a|bc$ e $(a, b) = 1$ temos $a|c$. Assim, $a \equiv b(\text{mod } m/d)$.

(5) Temos $a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + ... + ab^{k-2} + b^{k-1})$ e $m|(a - b)$ então $m|a^k - b^k$. Logo, $a^k \equiv b^k(\text{mod } m)$. □

Definição 2.3. *Se h e k são dois inteiros com $h \equiv k$(mod m), dizemos que k é um resíduo de h módulo m.*

Definição 2.4. *O conjunto dos inteiros $\{r_1, r_2, ..., r_s\}$ é um sistema completo de resíduos módulo m se:*
(1) $r_i \not\equiv r_j$(mod m) para $i \neq j$.
(2) para todo inteiro n existe um r_i tal que $n \equiv r_i$ (mod m).

Exemplo 2.5. Seja $h = 25$ e k um inteiro tal que $25 \equiv k(\text{mod } 7)$ e k pertence ao conjunto $\{0, 1, 2, 3, 4, 5, 6\}$ que é sistema completo de resíduos módulo 7, neste caso $k = 4$.

2.8 Equações Diofantinas lineares

Equações Diofantinas[3] lineares, são equações na forma $ax + by = c$, com a, b e c inteiros não simultaneamente nulos. A solução deste tipo de equação é dada pelo par de inteiros (x_0, y_0), tal que $ax_0 + by_0 = c$ seja verdadeira. Ou seja, as soluções da Equação Diofantina linear são os pontos de coordenadas inteiras do plano cartesiano, que estão dispostos sobre a reta que esta representa.

Apresentaremos a seguir alguns resultados retirados de [14] para tais equações.

Proposição 2.4. *Uma equação diofantina linear da forma $ax + by = c$, em que $a \neq 0$ ou $b \neq 0$, admite solução se, e somente se, $d = mdc(a, b)$ divide c.*

Demonstração. ($\Rightarrow$)Suponhamos que (x_0, y_0) é um par de inteiros satisfazendo $ax_0 + by_0 = c$. Sendo $d = \text{mdc}(a, b)$, temos que $d \mid a$ e $d \mid b$, logo pela Propriedade 2.8 item (7), $d \mid (ax_0 + by_0)$, ou seja, $d \mid c$.
($\Leftarrow$) Seja $d = \text{mdc}(a, b)$ supondo que $d \mid c$, temos $c = pd$, para algum p inteiro. Se $d = mdc(a, b)$ temos $d \mid a$ e $d \mid b$, da Proposição 2.8 item 7, $d \mid (ar + bs)$, com r e s inteiros. Assumindo que $ar + bs = 1 \cdot d$ e multiplicando ambos os membros pelo inteiro p temos $arp + bsp = pd$, ou seja, $a(rp) + b(sp) = c$. Assim $(x_0, y_0) = (rp, sp)$ é solução de $ax + by = c$. □

Teorema 2.5. *Sejam a e b inteiros e $d = mdc(a, b)$. Se $d \mid c$ então a equação diofantina linear $ax + by = c$ possui infinitas soluções. Se (x_0, y_0) é uma solução particular da equação, então existe um inteiro t tal que todas as soluções (x, y) são dadas por:*

$$x = x_0 + (b/d)t$$

$$y = y_0 - (a/d)t$$

Demonstração. Se $d = \text{mdc}(a, b)$ então $d \mid a$ e $d \mid b$. Pelo lema de Bézout existem inteiros n e m, tais que $an + bm = d$. Como $d \mid c$, existe um inteiro t tal que $c = td$. Se multiplicarmos a equação anterior por t temos $ant + bmt = td = c$. Isto nos diz que o par $(x_0, y_0) = (nt, mt)$ é uma solução de $ax + by = c$.
Vamos supor que (x, y) seja uma solução. Como $ax_0 + by_0 = c$ obtemos $ax + by = ax_0 + by_0$, o que implica $a(x - x_0) = b(y_0 - y)$. Dividindo os dois membros por d teremos $(a/d)(x - x_0) = (b/d)(y_0 - y)$. Logo $(b/d) \mid (x - x_0)$ e portanto existe um inteiro t satisfazendo $x - x_0 = t(b/d)$, ou seja, $x = x_0 + (b/d)t$. De maneira análoga, como $(a/d) \mid (y_0 - y)$, existe um inteiro t tal que $y_0 - y = (a/d)t$ e assim obtemos $y = y_0 - (a/d)t$. □

Corolário 2.1. *Se $d = mdc(a, b) = 1$ e (x_0, y_0) é uma solução particular da equação diofantina linear $ax + by = c$, então todas as outras soluções serão dadas por:*

[3]Diofanto de Alexandria foi um matemático grego, cuja data de nascimento se estima entre o anos 201 e 214 e a data de falecimento entre os anos 284 e 298.

$$S = \{(x_0 + bt, y_0 - at); t \in \mathbb{Z}\}$$

Exemplo 2.6. De quantas maneiras podemos comprar selos de cinco reais e selos de três reais com apenas cinquenta reais?

Podemos modelar esse problema com a equação diofantina $5x + 3y = 50$, onde x e y são respectivamente a quantidade de selos de 5 e 3 reais, respectivamente.

De acordo com a Proposição 2.4 esta equação possui solução, pois mdc$(5, 3) = 1$ e 1 divide 50. No problema acima as soluções tem que ser positivas para ter sentido, então:

Comprando apenas selos de 5 reais teremos a solução $(10, 0)$. Pelo Corolário 2.1 as soluções desta equação são do tipo $(x_0 - bt, y_0 + at)$, ou seja, $(10 - 3t, 0 + 5t)$, $t \in \mathbb{Z}$. Como as soluções são positivas, $t \in \{0, 1, 2, 3\}$ e assim, $(10, 0), (7, 5), (4, 10)$ e $(1, 15)$ são as soluções para o problema.

2.9 Congruência Linear

Em [16] o autor define como congruência linear em uma variável toda congruência da forma $ax \equiv b(\text{mod } m)$ onde a e b são números inteiros dados chamados de coeficientes e x é a incógnita. Essa equação também é conhecida como equação de congruência de grau 1 ou equação afim.

Reorganizando a equação temos $ax - b \equiv 0(\text{mod } m)$. Logo, existe um inteiro y, tal que $ax - b = ym$ ou $ax + (-m)y = b$, que representa uma equação diofantina linear. Pela Proposição 2.4 a equação $ax + (-m)y = b$, tem solução se, e somente se o $mdc(a, m)$ divide b.

2.10 Classes de congruência

Os resultados desta Seção podem ser encontrados em [6]. A classe módulo n ou classe de congruência módulo n é o conjunto de elementos que apresentam o mesmo resto quando dividido por n. Cada classe é denotada por $\overline{a}_n$ e o conjunto das classes é denotado por $\mathbb{Z}_n$, ou também por $\mathbb{Z}/n\mathbb{Z}$.

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

Dessa forma teremos a classe dos elementos que geram resto zero quando divididos por n, resto 1 e assim sucessivamente.

Exemplo 2.7. $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$,

$\overline{0} = \{0, 5, 10, 15, ...\}$

$\overline{1} = \{0, 1, 6, 11, ...\}$

$\overline{2} = \{0, 2, 7, 12, ...\}$

$\overline{3} = \{0, 3, 8, 13, ...\}$

$\overline{4} = \{0, 4, 9, 14, ...\}$

Antes de prosseguirmos, definiremos quando uma classe módulo m é inversível.

Definição 2.5. *Seja $b(mod\ m)$ uma classe módulo m, se existir uma classe m com $d(mod\ m)$ tal que:*

$$b(mod\ m).d(mod\ m) = 1(mod\ m)$$

então $b(mod\ m)$ possui inversa.

O próximo resultado nos da uma condição necessária e suficiente para obtermos a inversa:

Proposição 2.5. *Seja $b \neq 0$ um número inteiro, então a classe $b(mod\ m)$ tem inversa (é inversível) se, e somente se, $mdc(b, m) = 1$.*

Demonstração. ($\Rightarrow$) Suponhamos que a classe $b(\text{mod } m)$ tenha inversa e que sua inversa seja $d(\text{mod } m)$. Assim, $bd(\text{mod } m) \equiv 1(mod\ m)$ ou $bd - 1 \equiv 0(mod\ m)$. Logo, podemos escrever como $db - 1 = ym$ ou $bd + (-y)m = 1$ que só terá solução se $mdc(b, m) = 1$. ($\Leftarrow$) Por hipótese $mdc(b, m) = 1$ implica que a equação $bx + my = 1$ tem solução, (x_0, y_0), que são números inteiros tais que $bx_0 + my_0 = 1$. Podemos reescrever a última equação como $bx_0 - 1 \equiv 0(\text{mod } m)$ ou $bx_0 \equiv 1(\text{mod } m)$. Concluímos assim, que a classe $x_0(\text{mod } m)$ é inversa da classe $b(\text{mod } m)$. □

2.11 Números de Mersenne

Números de Mersenne[4] são números na forma $M_n = 2^n - 1$, onde n é um número natural. Definindo M_n como número de Mersenne para um n natural, temos:

$n = 0 \Rightarrow M_0 = 0$

$n = 1 \Rightarrow M_1 = 1$

$n = 2 \Rightarrow M_2 = 3$

$n = 3 \Rightarrow M_3 = 7$

...

Nem todos os números de Mersenne são números primos, como por exemplo $M_4 = 2^4 - 1 = 15$.

Propriedade 2.10. Se M_n é primo, então n é primo.

Demonstração. Provar essa proposição equivale a mostrar que a sua forma contrarrecíproca vale. Ou seja, que se n é composto, digamos $n = ab$ com $a \geq b > 1$, então M_n também é composto. De fato,

$$2^{ab} - 1 = (2^a - 1).(2^{a(b-1)} + 2^{a(b-2)} + 2^{a(b-3)} + ... + 2^a + 1)$$

□

[4]Marin Mersenne, matemático e monge Francês que viveu entre os anos de 1588 e 1648.

A recíproca da afirmação acima não é verdadeira. Por exemplo, em [12] encontramos um contraexemplo dado por Hudalricus Regius em 1536: $M_{11} = 2^{11} - 1 = 2047$ não é primo, já que $2047 = 23 \cdot 89$.

Podemos finalizar esta seção com um critério interessante, obtido pela matemática francesa Sophie Germain (1776-1831), que nos permite saber quando um número não é primo.

Propriedade 2.11. (Identidade de Sophie Germain) Dados $a, b \in \mathbb{R}$, vale a igualdade

$$a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$$

.

Demonstração. A prova segue das seguintes igualdades: $a^4 + 4b^4 = a^4 + 4a^2b^2 + 4b^4 - 4a^2b^2 = (a^2 + 2b^2)^2 - 4a^2b^2 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$. □

Exemplo 2.8. O número $5^{20} + 2^{30}$ é composto. De fato, $5^{20} + 2^{30} = 5^{5 \cdot 4} + 2^{2 \cdot 28} = (5^5)^4 + 4(2^7)^4$, de onde podemos usar a Identidade de Sophie Germain.

2.12 Números de Fermat

Números de Fermat [5] são números da forma $F_n = 2^{2^n} + 1$. Fermat acreditava que para todo n inteiro maior que zero a sua fórmula gerava um número primo. Como por exemplo para $n = 1$ temos $2^{2^1} + 1 = 5$, para n=2 temos $2^{2^2} + 1 = 17$. Porém, em 1732 Euler[6] mostra que 641 divide o número de Fermat para $n = 5$. Sabe-se que F_n é composto para $n \in \{5, 6, ..., 32\}$. Atualmente, mesmo com todo aparato computacional, é uma tarefa árdua encontrar um divisor próprio de um número de Fermat muito grande.

O Pequeno Teorema de Fermat é utilizado para realizar testes para determinar se certo número é primo.

Teorema 2.6. *(Pequeno teorema de Fermat) Sejam p e a inteiros com p primo, se $p \nmid a$ então $a^{p-1} \equiv 1 (mod\ p)$.*

Demonstração. O conjunto $X = \{0, 1, 2, 3, ..., p-1\}$ constitui um sistema completo de resíduos módulo p. Esse fato determina que qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado em correspondência biunívoca com um subconjunto de X. Considere os números $a, 2a, 3a, ..., (p-1)a$. Como por hipótese o $mdc(a, p) = 1$, nenhum destes elementos é divisível por p, ou seja, nenhum é congruente a zero módulo p. Logo, cada um deles é congruente a exatamente um dentre os elementos de X. Se multiplicarmos estas congruências membro a membro, teremos:

[5] Pierre de Fermat, matemático francês, que viveu entre 1601 e 1665.

[6] Leonhard Paul Euler, matemático suíço, que viveu entre os anos de 1707 e 1783.

$$a.2a.3a...(p-1).a \equiv 1.2.3...(p-1)(\text{mod } p)$$

Então $a^{p-1}(p-1)! \equiv (p-1)!(\text{mod } p)$. Como $mdc((p-1)!, p) = 1$, podemos cancelar o fator $(p-1)!$ obtendo:

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

□

Corolário 2.2. *Se p é um primo e a um inteiro positivo, então $a^p \equiv a(mod\ p)$.*

Demonstração. Se $p \mid a$, então $p \mid a(a^{p-1} - 1)$ ou $p \mid (a^p - a)$, assim $a^p - a \equiv 0(\text{mod } p)$ que é equivalente a $a^p \equiv a(\text{mod } p)$. □

2.13 Função ϕ de Euler

A demonstração dos resultados desta seção podem ser encontradas em [4].

Definição 2.6. *Dado um número natural n, a função $\phi(n)$ de Euler representa a quantidade de números naturais k, $1 \leq k < n$, tais que o $mdc(k, n) = 1$.*

Exemplos:

$$\phi(2) = 1$$
$$\phi(3) = 2$$
$$\phi(10) = 4$$
$$\phi(12) = 4$$
$$\phi(15) = 8.$$

Proposição 2.6. *Se p é um número primo, então $\phi(p) = p - 1$.*

Exemplos:

$$\phi(5) = 4$$
$$\phi(11) = 10$$
$$\phi(13) = 12$$
$$\phi(17) = 16$$
$$\phi(23) = 22.$$

Proposição 2.7. *Se p é um número primo, então $\phi(p^n) = p^n - p^{n-1}$.*

Exemplos:

$$\phi(9) = \phi(3^2) = 3^2 - 3^1 = 6$$
$$\phi(16) = \phi(2^4) = 2^4 - 2^3 = 8$$
$$\phi(25) = \phi(5^2) = 5^2 - 5^1 = 20$$
$$\phi(49) = \phi(7^2) = 7^2 - 7^1 = 42$$
$$\phi(64) = \phi(2^6) = 2^6 - 2^5 = 32.$$

Proposição 2.8. *Sejam a e b números inteiros positivos primos entre si, ou seja, $mdc(a,b) = 1$, então $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.*

Exemplos:

$$\phi(15) = \phi(3 \cdot 5) = \phi(3) \cdot \phi(5) = 2 \cdot 4 = 8 \ ,$$
$$\phi(1001) = \phi(7 \cdot 11 \cdot 13) = \phi(7) \cdot \phi(11) \cdot \phi(13) = 6 \cdot 10 \cdot 12 = 720 \ .$$

Com base nas proposições anteriores e usando o Teorema Fundamental da Aritmética 2.3, podemos deduzir a função $\phi(n)$:

Se n é um inteiro positivo, então ele possui a seguinte fatoração $n = p_1^{a_1}.p_2^{a_2}.p_3^{a_3}...p_k^{a_k}$, independente da ordem dos fatores, logo:

$$\phi(n) = \phi(p_1^{a_1}.p_2^{a_2}.p_3^{a_3}...p_k^{a_k})$$

$$\phi(n) = \phi(p_1^{a_1}).\phi(p_2^{a_2}).\phi(p_3^{a_3})...\phi(p_k^{a_k})$$

$$\phi(n) = (p_1^{a_1} - p_1^{a_1-1}).(p_2^{a_2} - p_2^{a_2-1}).(p_3^{a_3} - p_3^{a_3-1})...(p_k^{a_k} - p_k^{a_k-1})$$

$$\phi(n) = p_1^{a_1}(1 - \tfrac{1}{p_1}).p_2^{a_2}(1 - \tfrac{1}{p_2}).p_1^{a_3}(1 - \tfrac{1}{p_3})...p_k^{a_k}(1 - \tfrac{1}{p_k})$$

Assim, obtemos a função $\phi(n)$ de Euler:

$$\phi(n) = n.(1 - \tfrac{1}{p_1}).(1 - \tfrac{1}{p_2}).(1 - \tfrac{1}{p_3})...(1 - \tfrac{1}{p_k})$$

Exemplo 2.9. $\phi(30) = ?$

$$30 = 2 \cdot 3 \cdot 5$$
$$\phi(30) = 30 \cdot (1 - \tfrac{1}{2}).(1 - \tfrac{1}{3}).(1 - \tfrac{1}{5})$$
$$\phi(30) = 30 \cdot (\tfrac{1}{2}) \cdot (\tfrac{2}{3}) \cdot (\tfrac{4}{5})$$
$$\phi(30) = 30 \cdot (\tfrac{8}{30})$$
$$\phi(30) = 8$$

2.14 Teorema de Euler

O Teorema de Euler, conhecido também como Teorema Fermat-Euler, é uma generalização do pequeno Teorema de Fermat 2.6, que diz:

Teorema 2.7. *(Teorema de Euler) Se a e n são números positivos e $mdc(a,n) = 1$, então:*

$$a^{\phi(n)} \equiv 1 (mod\ n)$$

Antes de demonstrarmos o teorema de Euler, se faz necessário a utilização dos seguintes resultados:

Definição 2.7. *Um sistema reduzido de resíduos módulo m é o conjunto dos inteiros $\{r_1, r_2, r_3, ..., r_{\phi(m)}\}$, tais que cada elemento do conjunto é relativamente primo com m, se $i \neq j$ então $r_i \neq r_j (mod\ m)$.*

Exemplo 2.10. O conjunto {0,1,2,3,4,5,6,7,8,9} é um sistema completo de resíduos módulo 10, já o conjunto {1,3,7,9} é um sistema reduzido de resíduos módulo 10.

Teorema 2.8. *Sejam a e m números inteiros positivos tal que $mdc(a, m) = 1$. Se $\{r_1, r_2, r_3, ..., r_{\phi(m)}\}$ é um sistema reduzido de resíduos módulo m, então $\{ar_1, ar_2, ar_3, \cdots, ar_{\phi(m)}\}$ também é um sistema reduzido de resíduos módulo m.*

Demonstração. Como $mdc(a, m) = 1$ e $mdc(r_i, m) = 1$, para todo $1 \leq i \leq \phi(m)$, temos $mdc(ar_i, m) = 1$, para todo $1 \leq i \leq \phi(m)$. Assim, se $ar_i \equiv ar_j \pmod m$ temos $r_i \equiv r_j \pmod m$ o que implica $i = j$. A negação também é verdadeira pois $ar_i \neq ar_j \pmod m$ implica em $i \neq j$. □

Demonstração. (Teorema de Euler 2.7): Se n for um número primo, então $\phi(n) = n-1$ e pelo pequeno teorema de Fermat $a^{\phi(n)} = a^{n-1} \equiv 1 (\text{mod } n)$.
Caso contrário, se n é composto, $n = p_1^{a_1}.p_2^{a_2}.p_3^{a_3}...p_k^{a_k}$. Por hipótese mdc($a$,$m$)=1 e pelo Teorema 2.8 os elementos de $\{ar_1, ar_2, ar_3, ..., ar_{\phi(m)}\}$ constituem um sistema reduzido módulo m assim, $\{r_1, r_2, r_3, ..., r_{\phi(m)}\}$ também é um sistema reduzido de resíduos módulo m. Isso implica que cada elemento ar_i é congruente a exatamente um dos elementos r_j, para todo $1 \leq j \leq \phi(m)$. Portanto o produto dos ar_i deve ser congruente ao produto dos rj módulo m:

$$ar_1 \cdot ar_2 \cdot ar_3 \cdots ar_{\phi(m)} \equiv r_1 \cdot r_2 \cdot r_3 \cdots r_{\phi(m)} \pmod m$$
$$a^{\phi(m)} \cdot r_1 \cdot r_2 \cdot r_3 \cdots r_{\phi(m)} \equiv r_1 \cdot r_2 \cdot r_3 \cdots r_{\phi(m)} \pmod m.$$

Considere $k = r_1 \cdot r_2 \cdot r_3 \cdots r_{\phi(m)}$ então $a^{\phi(m)} \cdot k \equiv 1 \cdot k \pmod m$. Cancelando k de ambos os lados temos

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

□

2.15 Testes de primalidade

Nesta Seção descrevemos alguns testes de primalidade retirados de [13]. Estes testes visam determinar se um número é primo ou composto, sem a necessidade de fatorá-lo. Existem muitos algoritmos de primalidade utilizados principalmente na matemática computacional, cada um com sua base teórica, com suas vantagens e desvantagens. A seguir será apresentado alguns destes testes a fim de exemplos.

2.15.1 Teste de força bruta

O teste de força bruta é o mais antigo e mais simples teste para determinar a primalidade de um número natural n. O teste consiste em verificar todos os possíveis divisores de n no intervalo de 2 a $n/2$, em busca de um divisor diferente dele próprio.

Podemos utilizar também os números primos menores que $\sqrt{n}$ para dividir o próprio n. Se nenhum dos números pesquisado é fator de n então n é um número primo. Apesar deste método ser muito simples é ineficiente para números grandes, mesmo para um computador.

2.15.2 Aplicação do Pequeno Teorema de Fermat

O Pequeno Teorema de Fermat dá origem a um teste de primalidade chamado Teste de Fermat que consiste em:

Dados dois inteiros $b > 1$, $n > 1$, escolhemos $1 < b < n - 1$ e calculamos $b^{n-1} \equiv 1 (\text{mod } n)$. Se o resultado encontrado for verdadeiro, então n **pode** ser um número primo e recebe o nome de primo provável na base b.

Exemplo 2.11. $2^{341-1} \equiv 1 (\text{mod } 341)$, porém $341 = 11 \cdot 31$, ou seja, um número composto.

Os números, como no exemplo acima, que passam no teste de Fermat e não são primos, são chamados de pseudoprimos ou primos falsos. O teste de Fermat é um teste probabilístico, para cada valor de b existe uma infinidade de não primos para os quais $b^{n-1} - 1$ é divisível por n. Quanto maior for o número de testes maior a confiança que se pode ter no resultado, mas nunca será certeza.

2.15.3 Números de Carmichael

Dados a e n números inteiros positivos, dizemos que n é um número de Carmichael[7] se $n > 0$ é composto ímpar e $a^{n-1} \equiv 1 (\text{mod } n)$ para todo $1 < a < n - 1$. Portanto, números de Carmichael são pseudoprimos de Fermat para todas as bases menores que ele.

Exemplo 2.12. O menor número de Carmichael é o 561. Para provarmos esta afirmação usando a definição, precisaríamos verificar que $a^{561} \equiv a (\text{mod } 561)$, para $a \in \{2, 3, \ldots, 559\}$, num total de 558 bases a serem testadas.

Em 1899 uma caracterização para os números de Carmichael foi dada no Teorema de Korselt.

[7] Robert Daniel Carmichael, nasceu em 1 de março de 1879 em Goodwater e morreu em 2 de maio de 1967 em Merriam EUA.

Teorema 2.9. *(Teorema de Korselt) Um inteiro positivo ímpar n é um número de Carmichael se, e somente se, cada fator primo p de n satisfaz as duas condições seguintes:*

$$p^2 \text{ não divide } n \text{ e } p-1 \text{ divide } n-1.$$

Exemplo 2.13. Temos que $561 = 3 \cdot 11 \cdot 17$. Note que 3^2 não divide 561, 11^2 não divide 561 e 17^2 não divide 561. Porém, $3-1=2$ e 2 divide 560, $11-1=10$ e 10 divide 560, 17-1 = 16 e 16 divide 560. Portanto, 561 é um número de Carmichael e é o menor deles.

Em 1994, os matemáticos Willian Alford, Andrew Granville e Carl Pomerance provaram que há infinitos números de Carmichael.

2.15.4 Algoritmo de Lucas

De acordo com o pequeno teorema de Fermat, se p é primo, então para qualquer número inteiro a tem-se:

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

O primeiro Algoritmo de Lucas[8] foi criado em 1872, e resumidamente pode ser definido da seguinte forma:

Se $a^{p-1} \equiv 1(\text{mod } p)$ e $a^m \neq 1(\text{mod } n)$, onde a, n, m são inteiros $a > 1$, $n > 1$ e $m = 1, 2, 3, 4, 5, ..., n-2$, então n é um número primo.

A desvantagem desse método se refere ao longo tempo gasto para efetuar os cálculos com números compostos grandes, pois temos que testar $(n-2)$ multiplicações sucessivas por a mais a verificação que 1 não é resíduo módulo n de uma potência de a inferior a $(n-1)$.

O segundo Algoritmo de Lucas foi desenvolvido em 1891, onde diz que n é primo se satisfizer as seguintes condições:

$$a^{n-1} \equiv 1(\text{mod } n) \qquad \text{e} \qquad a^m \neq 1(\text{mod } n)$$

para cada $m < n$, tal que $m \mid (n-1)$, ou seja, m é divisor de $n-1$.

Devido ao fato desse algoritmo requerer o conhecimento prévio de todos os fatores de $n-1$, isso se torna computacionalmente custoso para números muito grandes.

2.15.5 Método de Lucas Lehmer

Este teste de primalidade em relação aos números de Mersenne foi desenvolvido por Lucas em 1876 e aperfeiçoado em 1930 por Lehmer [9].

[8] François Édouard Anatole Lucas, nasceu na cidade francesa de Amiens em 4 de Abril de 1842 e morreu em Paris 3 de outubro de 1891.

[9] Normando Lehmer do Derrick, nasceu em 1867 em Somerset e faleceu em 1938 em Berkeley,EUA.

O algoritmo de Lucas-Lehmer diz que o número de Mersenne $M_n = 2^n - 1$ será primo se $M_n \mid L_n$ onde L_n é o número de Lucas-Lehmer dado por:

$$L_n = L_{n-1}^2 - 2$$

Os números L_n são formados pela sequência $L_0 = 4$, $L_1 = 14$, $L_2 = 194$, ..., obter esses números é uma tarefa computacional simples, em seguida verifica-se:

$$L_n \equiv 0 (\text{mod } M_n)$$

Com esse método Lehmer provou que Mersenne errou ao afirmar que o número $2^{257} - 1$ era primo.

2.15.6 Teste de primalidade AKS

Na tentativa de se encontrar testes de primalidades mais rápidos e eficientes e testes probabilísticos com chances de acertos cada vez maiores surgiu, em 2002 o algoritmo AKS, cujo o nome é formado pelas iniciais dos sobrenomes de seus criadores, os indianos: Agrawal[10] , Kayal[11] e Saxena[12].

O teste de primalidade AKS esta baseado em um algoritmo que é ao mesmo tempo polinomial, determinístico e incondicional. Ou seja, o tempo máximo de processamento do algoritmo pode ser expresso como um polinômio em relação ao número de dígitos do número a ser testado e assim é possível classificar o número informado como primo ou composto.

O AKS é baseado na generalização do Pequeno teorema de Fermat 2.6: Seja a um número inteiro e n um número natural maior que 1, tal que mdc(a, n)=1, n é um número primo se, e somente se,

$$(x - a)^n \equiv (x^n - a) \ (\text{mod } n)$$

Ou de modo equivalente:

$$(x + a)^n \equiv x^n + a \ (\text{mod } n)$$

Exemplo 2.14. Considere $a = -1$ e $n = 2$ (para efeito de facilidade nos cálculos), temos:

$$\begin{gathered}(x + 1)^2 \equiv x^2 + 1 \ (\text{mod } 2) \\ (x^2 + 2x + 1) \equiv x^2 + 1 \ (\text{mod } 2) \\ (x^2 + 1) + 2x \equiv x^2 + 1 \ (\text{mod } 2) \\ 2x \equiv 0 \ (\text{mod } 2)\end{gathered}$$

A equação acima possui infinitas soluções e, para qualquer inteiro x a equivalência é verdadeira, logo $n = 2$ é primo.

[10]Manindra Agrawal nasceu em 1966 em Allahabad, Índia.
[11]Neeraj Kayal nasceu em 1979 em Guwahati, Índia.
[12]Nitin Saxena nasceu em 1981 em Allahabad, Índia.

2.16 Raízes primitivas

O definição de raiz primitiva engloba vários conceitos vistos anteriormente e alguns novos que serão enunciados nesta seção.

Definição 2.8. *Seja k um inteiro positivo que satisfaz a equivalência $a^k \equiv 1 (mod\ m)$, onde $mdc(a, m) = 1$. O menor valor de k é chamado de ordem de a módulo m e a notação é $ord_m a = k$.*

Exemplo 2.15. Seja k um inteiro positivo $3^k \equiv 9(mod\ 13)$, sendo que $\text{mdc}(3, 13) = 1$, temos :

$$3^1 \equiv 3(mod\ 13),$$
$$3^2 \equiv 9(mod\ 13),$$
$$3^3 \equiv 1(mod\ 13),$$
$$3^4 \equiv 3(mod\ 13),$$
$$3^5 \equiv 9(mod\ 13),$$
$$3^6 \equiv 1(mod\ 13),$$
$$...$$

Logo a ordem de 3 módulo 13 é igual a 3, ou seja , $\text{ord}_{13}3 = 3$.

Teorema 2.10. *Sejam k, m, a, h inteiros positivos tal que $k = ord_m a$ e $a^h \equiv 1(mod\ m)$, então $k \mid h$.*

Demonstração. Pelo algoritmo da divisão de Euclides, dados h e k inteiros diferentes de zero, existe um único par de inteiros q e r, $0 \leq r < k$ tal que $h = q \cdot k + r$. Logo:

$$a^h = a^{q \cdot k + r} = (a^k)^q \cdot a^r$$

Como $a^h \equiv 1(mod\ m)$, temos:

$$(a^k)^q \cdot a^r \equiv 1(\text{mod } m)$$

Por hipótese $a^k \equiv 1(mod\ m)$, pois $k = \text{ord}_m a$, então obtemos:

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

Sendo $r < k$, r deve ser zero pois k é o menor elemento positivo no qual $a^k \equiv 1(mod\ m)$. Portanto , $r = 0$ e $h = q \cdot k$, ou seja, $k \mid h$. □

Corolário 2.3. *Sejam m e a inteiros positivos, então $ord_m a \mid \phi(m)$.*

Demonstração. Pelo o Teorema de Euler 2.7, $a^{\phi(m)} \equiv 1(mod\, m)$, para todo $\text{mdc}(a, m) = 1$. De Teorema 2.10 temos $ord_m a \mid \phi(m)$. □

Definição 2.9. *Sejam a e m inteiros positivos e $ord_m a = \phi(m)$, dizemos que a é raiz primitiva módulo m.*

Exemplo 2.16. Temos que $ord_{10}3 = 4$, pois $3^4 \equiv 1(mod\ 10)$.

3 Elementos da Álgebra

O objetivo deste capítulo é fornecer algumas definições e resultados básicos da Álgebra para tratarmos do assunto referente a curvas elípticas, um conceito novo que vêm sem sendo aplicado à Criptografia.

3.1 Grupo

Os resultados desta seção foram retirados de [8].

Definição 3.1. *Seja G um conjunto não vazio e uma operação $\otimes$ definida. O par $(G, \otimes)$ será um grupo se satisfazer as seguintes propriedades:*

Propriedade 3.1. Fechamento: Para quaisquer elementos $a, b \in G$ temos $a \otimes b \in G$.

Propriedade 3.2. Associativa: Para quaisquer elementos $a, b, c \in G$ temos $(a \otimes b) \otimes c = a \otimes (b \otimes c)$.

Propriedade 3.3. Elemento neutro: Existe um único elemento $e \in G$, tal que $a \otimes e = e \otimes a = a$.

Propriedade 3.4. Elemento inverso: Para cada $a \in G$ existe um único elemento $i \in G$, tal que $a \otimes i = i \otimes a = e$, onde e é o elemento neutro de G.

3.1.1 Grupo abeliano

Um grupo é dito abeliano [1] se além das propriedades de grupo contém a propriedade comutativa para operação $\otimes$ definida.

Definição 3.2. *Seja $(G, \otimes)$ um grupo. Este será chamado de grupo abeliano se a operação $\otimes$ for comutativa em G, ou seja, para quaisquer elementos $a, b \in G$ temos $a \otimes b = b \otimes a$.*

[1] Em homenagem ao matemático norueguês Niels Henrik Abel, que nasceu em Nedstrand em dia 5 de agosto de 1802 e faleceu em Froland em 6 de abril de 1829.

3.2 Corpo

Um corpo é uma estrutura algébrica que consiste num conjunto R munido de duas operações binárias, geralmente chamada de adição $\oplus$ e multiplicação $\otimes$ e denotado por $(R, \oplus, \otimes)$. Para ser considerado um corpo o conjunto R tem que satisfazer as seguintes propriedades em relação as operações de $\oplus$ e $\otimes$ para a, b e c elementos de R:

Propriedade 3.5. Fechamento: $a \oplus b \in R$ e $a \otimes b \in R$.

Propriedade 3.6. Comutativa: $a \oplus b = b \oplus a$ e $a \otimes b = b \otimes a$.

Propriedade 3.7. Associativa: $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ e $(a \otimes b) \otimes c = a \otimes (b \otimes c)$.

Propriedade 3.8. Distributiva: $(a \oplus b) \otimes c = a \otimes c + b \otimes c$.

Propriedade 3.9. Existência de elemento neutro: $a \oplus 0 = a$ e $a \otimes 1 = a$.

Propriedade 3.10. Existência de inverso aditivo: $a \neq 0$, exite um $(-a)$ tal que $a \oplus (-a) = 0$.

Propriedade 3.11. Existência de inverso multiplicativo: $a \neq 0$, exite um (a^{-1}) tal que $a \otimes (a^{-1}) = 1$.

Exemplo 3.1. O conjunto[2] $\mathbb{Z}_n$ será um corpo se n for primo, caso contrário teremos divisores de zero[3].
$\mathbb{Z}_3 = \{0, 1, 2\}$, é um corpo.
$\mathbb{Z}_4 = \{0, 1, 2, 3\}$, não é um corpo pois $2 \cdot 2 = 0$.

3.3 Curvas Elípticas

O tema Curvas Elípticas é muito complexo e atualmente tem grande impacto na Cripografia e Teoria dos números. Como o objetivo deste trabalho é a Criptografia e seu uso em sala de aula, o assunto sobre curvas elípticas será apresentado de forma elementar e voltado à Criptografia.

3.3.1 Definição

Antes de definirmos uma curva elíptica, temos que compreender o que é uma curva algébrica. Uma curva algébrica plana é um lugar geométrico[4] no plano que são soluções de uma equação f polinomial de duas variáveis, ou seja, é o conjunto de pontos (x, y)

[2] O conjunto $\mathbb{Z}_n$ é finito constituído dos seguintes elementos {0 , 1 , 2 , 3 , 4 ,..., n-2 , n-1}

[3] Um divisor de zero são números, diferentes de zero que, quando multiplicados o resultado é zero

[4] Lugar geométrico é o conjunto de infinitos pontos que possuem uma propriedade em comum, como a circunferência, reta bissetriz, etc.

que satisfazem $f(x, y) = 0$. A seguir apresentamos uma definição de curva elíptica geral.

Seja um corpo F, uma *curva elíptica* sobre F é uma curva algébrica definida pela seguinte equação geral:

$$y^2 + Axy + By = Cx^3 + Dx^2 + Ex + F \tag{3.1}$$

onde A, B, C, D, E, F, são coeficientes pertencentes ao corpo F.

Na criptografia se utiliza uma versão reduzida ou simplificada da curva elíptica definida em (3.1), a qual vamos definir abaixo:

Seja $\mathbb{Z}_p$ um corpo de característica[5] diferente de 2 e de 3, ou seja, para um corpo $\mathbb{Z}_p$, p primo maior que 2, a curva elíptica, denotada por E, sobre o corpo $\mathbb{Z}_p$ é definida pela equação:

$$y^2 = x^3 + ax + b \tag{3.2}$$

de modo que a e $b \in \mathbb{Z}_p$ e satisfaça a relação $4a^3 + 27b^2 (\text{mod } p) \neq 0$. Esta curva é mostrada pela Figura 3.1.

O conjunto dos pontos $P(x, y)$, onde $x, y \in \mathbb{Z}_p$, que satisfaz a equação (3.2) mais o elemento neutro O, também chamado ponto no infinito, é denotado por $E(\mathbb{Z}_p)$.

O número de pontos que satisfaz a curva elíptica (3.2) em $\mathbb{Z}_{11}$, pode ser calculado pelo Teorema de Hasse [6], que diz que o número N de pontos de uma curva elíptica sobre F_q satisfaz: $1 + q - 2\sqrt{q} \leq N \leq 1 + q + 2\sqrt{q}$, onde q é uma potência de um número primo.

Conhecer o número de pontos que satisfaz uma curva elíptica é fundamental para se calcular a segurança do sistema criptográfico nela baseado.

Exemplo 3.2. Considerando a curva elíptica $y^2 = x^3 + 1x + 1$ definida sobre o corpo $\mathbb{Z}_{11}$, podemos calcular o número de pontos da curva elíptica pelo teorema de Hasse:

$$\begin{gathered} 1 + 11 - 2\sqrt{11} \leq N \leq 1 + 11 + 2\sqrt{11} \\ 12 - 2\sqrt{11} \leq N \leq 12 + 2\sqrt{11} \\ 5,36... \leq N \leq 18,63... \end{gathered}$$

De acordo com este teorema teremos no máximo 18 pontos que satisfazem esta curva elíptica. A Figura 3.2 mostra apenas 13 pontos, mas os pontos (2,11), (11,10), (11,12), (13,0), (13,11) também pertencem a curva elíptica. De fato:

$$\begin{gathered} 11^2 \equiv 2^3 + 2 + 1 \ (mod\ 11) \\ 10^2 \equiv 11^3 + 11 + 1 \ (mod\ 11) \\ 12^2 \equiv 11^3 + 11 + 1 \ (mod\ 11) \\ 0^2 \equiv 13^3 + 13 + 1 \ (mod\ 11) \\ 11^2 \equiv 13^3 + 13 + 1 \ (mod\ 11) \end{gathered}$$

[5] Característica de um corpo é o menor inteiro positivo n tal que $n \cdot 1 = 0$, caso não exista, o corpo tem característica zero.

[6] Helmut Hasse, matemático alemão (1898-1979).

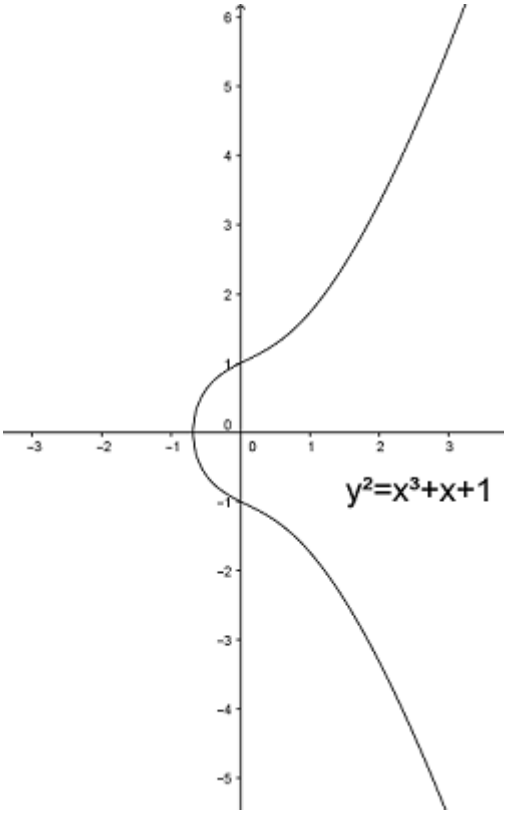

Figura 3.1: Exemplo de curva elíptica $y^2 = x^3 + 1x + 1$, imagem elaborada pelo próprio autor.

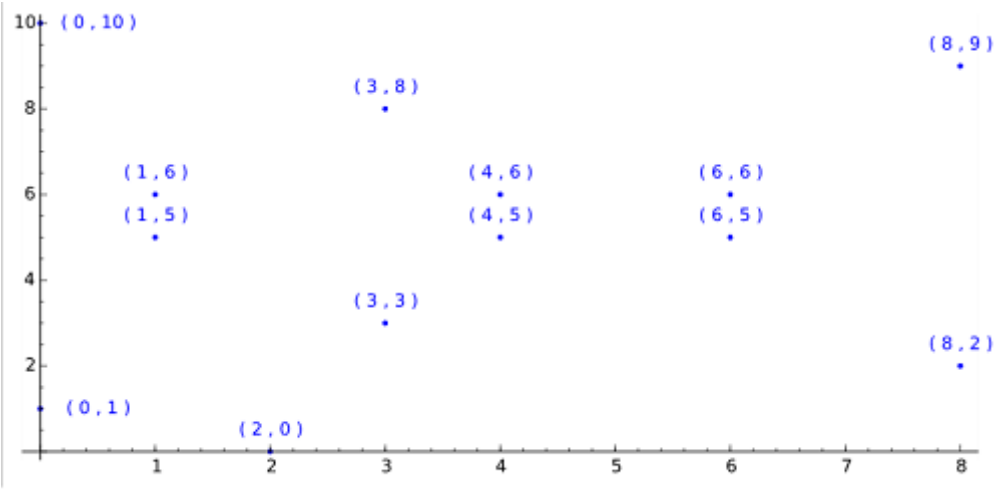

Figura 3.2: Exemplo da curva elíptica $y^2 = x^3 + 1x + 1$ utilizando $\mathbb{Z}_{11}$. Fonte: www.criptored.upm.es/crypt4you/temas/ECC/leccion1/leccion1.html. Acesso em 01/02/2016

3.3.2 Propriedades

As propriedades a seguir são fundamentais para as operações entre pontos que pertencem a curva elíptica $E(\mathbb{Z}_p)$:

Propriedade 3.12. $P+O = O+P = P$, para todo $P \in E(\mathbb{Z}_p)$, o ponto O é chamado de ponto no infinito.

Propriedade 3.13. Se $P = (x, y)$, então $-P = (x, -y)$.

Propriedade 3.14. Sejam P e $Q \in E(\mathbb{Z}_p)$, com $P \neq Q$, $P+Q = R$, onde $R = (x_R, y_R)$, é da forma:

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}$$
$$x_R = \lambda^2 - x_P - x_Q \pmod{p}$$
$$y_R = -y_P + \lambda(x_P - x_R) \pmod{p}$$

Propriedade 3.15. Seja $P = (x_p, y_P) \in E(\mathbb{Z}_p)$, com $y_P \neq 0$. A soma $P + P = 2P = R = (x_R, y_R)$, onde:

$$\lambda = \frac{3(x_P)^2 + a}{2y_P}$$
$$x_R = \lambda^2 - 2x_P \pmod{p}$$
$$y_R = \lambda(x_P - x_R) - y_P \pmod{p}$$

Com a proposição acima podemos generalizar a soma de pontos iguais:

$$3P = P + (P + P)$$
$$4P = P + (P + (P + P))$$
$$\ldots$$

Dessa forma fica definida a operação $k \cdot P$ para qualquer k inteiro positivo, a operação mais utilizada na criptografia baseada em curvas elípticas, que faz de $E(\mathbb{Z}_p)$, juntamente com a operação de soma, um grupo abeliano, onde o ponto no infinito é o elemento neutro.

As curvas elípticas num sistema de criptografia mostram um nível de segurança melhor comparado ao RSA, que é o sistema de criptografia assimétrica mais utilizada, porém sua complexidade e grau de sofisticação é devidamente maior e por isso não detalharemos mais neste trabalho. Em [20] os leitores interessados podem encontrar mais sobre o assunto.

4 Criptografia

4.1 Um breve histórico sobre criptografia

A criptografia pode ser resumida de modo simples como um conjunto de técnicas que permite tornar incompreensível uma mensagem, de modo que somente o destinatário consegue decifrá-la. Há registros[1] mostrando que a ocultação de informações era utilizada desde o Egito antigo, cerca de 1900 a.c. Os escribas dos faraós substituíam alguns trechos e palavras de documentos importantes por símbolos estranhos, dificultando assim a ação de ladrões.

Alguns séculos mais tarde apareceram outros métodos de transmitir mensagens de modo secreto na Mesopotâmia e na Ásia de modo geral. Métodos simples como mensagem tatuada na cabeça de escravos, mensagens escondidas dentro de caças, dentre outras. Estas formas de ocultação de mensagens, recebem o nome de esteganografia e diferentemente da criptografia, não altera a mensagem original como ocorre na criptografia, onde a mensagem original é completamente alterada. Atualmente, ainda se utiliza a esteganografia na ocultação de mensagem em imagens digitais, como por exemplo, no código de barras bidimensional, chamados de QR[2] (Quick Response).

Figura 4.1: Exemplo da esteganografia aplicada no QR.

[1]Esta seção está baseada em [1].

[2]Imagem retirada de fttps://pt.wikipedia.org/wiki/Codigo-QR, acessado em 12/02/2016.

Cerca de 600 a.c. os hebreus criaram alguns sistemas criptográficos que consistiam de uma troca simples entre as letras do hebraico por ordem inversa. O primeiro sistema criptográfico de uso militar que se tem notícia ocorreu por volta de 475 a.c., chamado de bastão de Licurgo, e foi utilizado pelo general espartano Pasanius. Esse sistema criptográfico consistia em enrolar uma tira de couro em volta de um bastão específico, no qual escrevia-se a mensagem e enviava a tira contendo a mensagem. O receptor deveria ter um bastão idêntico para que a mensagem pudesse ser lida.

Figura 4.2: Bastão de Licurgo. Fonte:https://siriarah.wordpress.com/2013/05/13/criptografia-bastao-de-licurgo-scytale-em-python/. Acesso em 12/02/2016.

O imperador romano Júlio César utilizava uma forma de criptografia que consistia em substituir cada letra da mensagem por outra letra que se encontrava três posições a frente no alfabeto.

Em 1466, Leon Batista Alberti escreveu um ensaio no qual mencionava um método de criptografia baseado em disco, fornecendo as bases para a cifra poli alfabéticas. Giovan Batista Belaso inventou, em 1553, um sistema baseado no conceito de cifra poli alfabética chamado atualmente de cifra de Vigeniere (atribuído falsamente a Blaise de Vigeniere durante o século XIX). Vigeniere, no entanto, criou o conceito de auto-chave, processo ainda hoje utilizado.

Durante e após a segunda guerra mundial houve grande proliferação de sistemas criptográficos, tanto para uso militar quanto comercial. Em 1923, Arthur Scherbius desenvolveu o Enigma, uma máquina criptográfica utilizada pelos alemães durante a guerra. Alan Turing e sua equipe, na Inglaterra, conseguiram decifrar o Enigma, permitindo aos aliados decifrar as mensagens dos alemães.

Figura 4.3: Máquina enigma. Fonte: http://www.eldiario.es/turing/criptografia/alan-turing-enigma-codigo-0-226078042.html, acessado em 12/02/2016.

Atualmente a criptografia se divide em dois tipos: a de chave simétrica e a de chave assimétrica. Uma chave criptográfica pode ser um número ou um conjunto de caracteres utilizado no processo de encriptação ou descriptação de uma mensagem.

No sistema de criptografia de chave simétrica, a mesma chave que se utiliza para encriptar uma mensagem é a mesma utilizada para decriptar a mensagem. No final do século XIX foi descoberto um método para quebrar esse tipo de codificação e, com o avanço da computação, esse tipo de criptografia se tornou totalmente frágil.

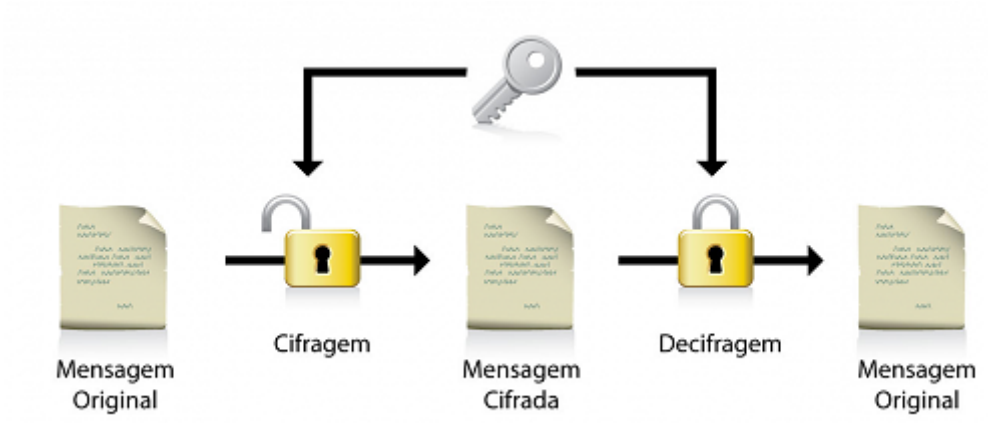

Figura 4.4: Criptografia de chave simétrica. Fonte: http://biblioo.info/certificacao-digital/. Acesso em 12/02/2016.

A criptografia assimétrica (ou de chave pública) surgiu na década de 70 e utiliza

duas chaves, uma pública e outra privada. Nessa criptografia, o remetente possui a chave pública e com ela realiza a encriptação da mensagem, que só poderá ser descriptografada com a chave privada do destinatário.

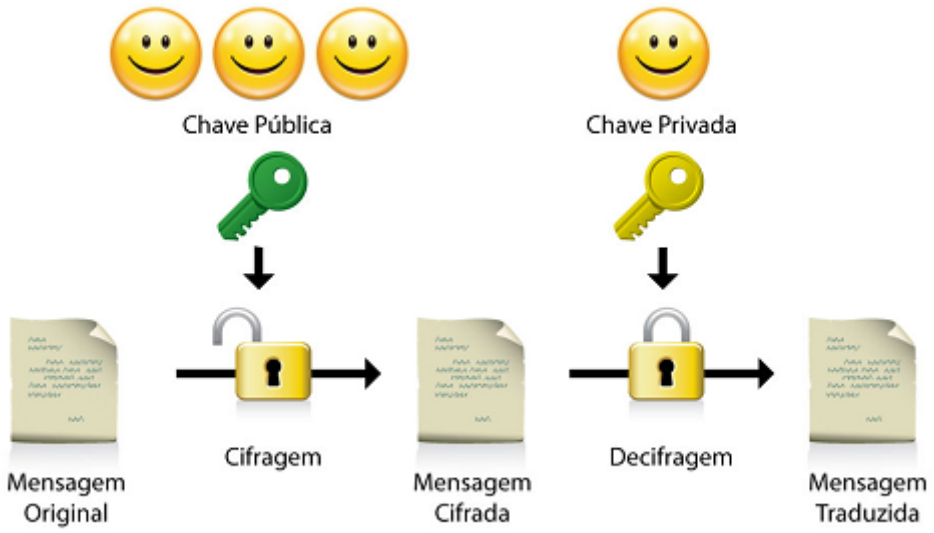

Figura 4.5: Criptografia de chave assimétrica.Fonte: http://biblioo.info/certificacao-digital/. Acesso em 12/02/2016.

Nesse sistema as chaves são relacionadas matematicamente, o sistema de criptografia assimétrica mais utilizado é o RSA, criado em 1978 por Rivest, Shamir e Adleman. Segundo Lemos(2010) seu funcionamento está baseado em dois princípios, sendo que o segundo é empírico:

- É fácil encontrar dois números primos grandes.
- Atualmente, é praticamente impossível fatorar o seu produto.

A criptografia permeia o mundo digital de tal forma que, sem ela não seria possível a comunicação sigilosa. Compras online, e-mails, transações financeiras, proteção de informações em bancos de dados, etc. De acordo com [6] para transações utilizando a rede mundial de computadores o alfabeto utilizado possui todos os símbolos de um teclado de computador, o padrão Unicode por exemplo, utiliza atualmente mais de 107 mil caracteres. Não é exagero dizer que nossas vidas dependem da criptografia, pois nossas informações pessoais estão espalhadas em diversos bancos de dados, pela internet, seja por instituições governamentais ou privadas. A seguir discutiremos procedimentos para ocultar informação contida em uma mensagem e como recuperá-la. Para isso necessitamos fixar um alfabeto para escrever esta mensagem. Assumiremos que este alfabeto contém 26 letras:

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

4.2 Cifras de César

Esta seção está baseada em [16]. A Cifra de César, em homenagem ao imperador Romano Júlio César que usava essa técnica para se comunicar com os seus generais, também conhecida como cifra de troca, é uma das formas mais simples e mais antigas de criptografar. Consiste em substituir cada letra do texto por outra que está um número fixo de vezes a frente. Por exemplo, com uma troca de cada letra, cinco posições a frente: desta forma "A"seria substituído por "F", "B"se tornaria "G", e assim sucessivamente, ficando da seguinte forma:

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

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

Chamaremos a associação de letras acima de *Cifra 1*.

Exemplo 4.1. Se uma fonte $\mathscr{A}$ quisesse enviar a mensagem

CRIPTOGRAFIA PROFMAT

para uma fonte $\mathscr{B}$, utilizando a cifra 1, o resultado da encriptação seria:

HWNUYTLWFKNF UWTKRFY

A fonte $\mathscr{B}$, por sua vez, deveria possuir a mesma *Cifra 1* para decriptar a mensagem.

Considerando a posição das letras do alfabeto da *Cifra 1*, podemos escrever a relação entre os textos da seguinte forma:

Seja D a posição das letras do alfabeto e seja E a posição das letras do alfabeto deslocado cinco posições, então teremos a seguinte fórmula de congruência:

$$E \equiv (D + 5)(mod\ 26)$$

Dessa forma para determinarmos D (o texto original), utilizamos a seguinte fórmula:

$$D \equiv (E - 5)(mod\ 26)$$

Para uma melhor visualização dessa técnica utilizaremos o alfabeto digital, onde cada letra do alfabeto será associado a um número, que nesse caso representa a sua posição, de acordo com a Tabela 4.1.

Realizando a congruência descrita acima: $E \equiv (D+5)(mod\ 26)$, onde substituímos D pelo número da posição de cada letra do alfabeto, conforme a Tabela 4.1, obtemos o alfabeto deslocado, de acordo com a Tabela 4.2.

Exemplo 4.2. Utilizando o mesmo exemplo anterior a mensagem CRIPTOGRAFIA PROFMAT teria como resultado da encriptação: 072213202419112205 20221910170524

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

Tabela 4.1: Alfabeto digital.

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

Tabela 4.2: Exemplo da Cifra de César com alfabeto digital.

A utilização dessa técnica de encriptação de mensagens oferece pouca segurança, pois para decifrar mensagens longas basta verificar a frequência de repetição de determinadas letras ou mesmo testar as possibilidades da Cifra de César. No caso do exemplo anterior teríamos que testar 26 posições. A cifra de César é um caso particular das cifras afins.

Observamos que na Cifra de César o espaço não tem um caractere que o representa, utilizando assim os espaços originais da mensagem.

4.3 Cifras Afins

A Cifra Afim é definida considerando dois números a, b de modo que $0 \leq a, b \leq 25$ e $\text{mdc}(a, 26) = 1$, de acordo com a seguinte congruência:

$$E \equiv (aD + b)(mod\ 26),$$

onde D é o número que corresponde a posição de uma letra do alfabeto e E sua posição no alfabeto deslocado. Os números a, b são chamados de chave da Cifra Afim. No caso particular da Cifra de César temos $a = 1$. A decriptação ocorre calculado:

$$aD \equiv (E - b)(mod\ 26)$$

Utilizando o fato de $\text{mdc}(a, 26) = 1$, a possui um inverso multiplicativo a^{-1}. Então:

$$D \equiv a^{-1}(E - b)(mod\ 26)$$

Se fixamos o valor de a obtemos 26 possibilidades para b, já que $0 \leq b \leq 25$, como ocorre na cifra de César. Levando em conta que a tem que ser escolhido de tal forma que satisfaça a condição $\text{mdc}(a, 26) = 1$, com $0 \leq a \leq 25$ e ϕ (26)=12 então há 12 possibilidades para a escolha de a. Assim, teremos $12 \cdot 26 = 312$ maneiras de escolher a e b para cifras afins de um alfabeto de 26 letras.

Exemplo 4.3. Vamos encriptar a mensagem "Estou estudando criptografia", utilizando a Cifra Afim: $E \equiv (5D + 8)(mod\ 26)$.

A mensagem criptografada será "CUZAE CUEXIVXA SPWFZAMPIHWI"ou em números "0220250004 0220042308212300 18152205001215080722 08".

A tabela abaixo foi construída utilizando a Cifra Afim: $E \equiv (5D + 8)(mod\ 26)$.

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

Tabela 4.3: Exemplo da Cifra afim com chaves 5 e 8:

Para descriptografar a mensagem do exemplo teremos que utilizar a seguinte equivalência:

$$D \equiv 5^{-1}(E - 8)(mod\ 26)$$

Utilizando o fato de que $5^{-1} = 21$, pois $5 \cdot 21$ tem resto 1 quando dividido por 26, temos:

$$D \equiv 21E - 168(mod\ 26) \Rightarrow D \equiv 21E - 12(mod\ 26)$$
$$D \equiv 21E + 14(mod\ 26).$$

4.4 Sistema RSA

Esta seção está baseada em [5]. O sistema de criptografia RSA é resultado do trabalho de três matemáticos do MIT[3], Ronald Rivest, Adi Shamire e Leonard Adleman, em 1978. Boa parte das transações efetuadas na internet são realizadas com o uso da RSA, sendo considerado um dos sistemas criptográficos mais seguros da atualidade.

No sistema RSA as chaves são geradas utilizando dois números primos, geralmente primos muito grandes que chamaremos de p e q. Em seguida encontra-se o produto n desses primos :

$$n = p \cdot q$$

Depois calcula-se $\phi(n)$ e como p e q são primos temos:

$$\phi(n) = (p - 1) \cdot (q - 1)$$

. De posse do valor de $\phi(n)$, devemos escolher um inteiro D, de modo que $1 < D < \phi(n)$ e mdc$(\phi(n), D)$=1. O par de valores n e D será a chave pública do sistema RSA.

Para determinar a chave privada desse sistema, temos que calcular o valor de E da seguinte congruência:

[3]MIT-Massachusetts Institute of Technology.

$$ED \equiv 1 \pmod{\phi(n)}$$

Exemplo 4.4. Vamos determinar as chaves pública e privada de um sistema RSA utilizando os números primos $p = 7$ e $q = 19$:

$$n = 7 \cdot 19 = 133$$
$$\phi(133) = (7-1) \cdot (19-1) = 108$$

Seja $D = 13$, já que $1 < 13 < 108$, iremos calcular E.

$$E \cdot 13 \equiv 1 \pmod{108}$$

Logo, E pode ser calculado de acordo com a seguinte equação:

$$13 \cdot E - 1 = K \cdot 108$$

$$E = \frac{1+108K}{13}$$

Como E tem que ser um número inteiro, temos que $K = 3$, obtendo $E = 25$. Na verdade há infinitas possibilidades para escolhermos K (por exemplo $K = 16$) mas somente $K = 3$ é aceitável. Concluindo que a chave pública é $(133, 13)$ e a chave privada é $(133, 25)$.

Para cifrarmos uma mensagem M utilizando o sistema RSA, primeiramente fazemos a transformação das letras em sequências de números, onde $0 < M < n$, obtendo o texto cifrado C com a chave pública $(n,\ D)$:

$$C \equiv M^D \pmod{n}$$

A recuperação da mensagem cifrada C da mensagem M se dá pelo uso da chave privada $(n\ ,\ E)$:

$$M \equiv C^E \pmod{n}.$$

A segurança do sistema RSA se baseia no fato de não haver um algorítmo eficiente que fatore um número como produto de dois primos, geralmente números grandes, em tempo computacionalmente viável, mesmo utilizando super computadores.

Uma desvantagem no uso do sistema de criptografia de chave assimétrica, como o RSA, reside no fato de ser computacionalmente custoso, tornando inviável para sistemas com pouca capacidade computacional, como por exemplo smartphones. Para contornar essa dificuldade, em muitos casos, utilizamos um sistema de criptografia de chave simétrica e somente a chave secreta é enviada utilizando o sistema de criptografia de chave assimétrica.

4.5 Método para troca de chaves

Em todos os métodos criptográficos baseados em chaves, seja pública ou privada, possui um grande desafio que consiste em compartilhá-las em segredo. Os métodos a seguir tem sua segurança baseado na Matemática, mais especificamento na dificuldade em se encontrar o logaritmo discreto de um número específico em tempo plausível. Antes de apresentar os métodos mais conhecidos, se faz necessário uma pequena explanação sobre o logaritmo discreto. Os resultados das próximas subseções podem ser encontrados em [1].

4.5.1 Problema do logaritmo discreto

O logaritmo discreto é análogo ao logaritmo natural, sendo $\log_a b$ a solução de uma equação $a^x = b$, com $a, b, x \in \mathbb{R}_+$, com $a \neq 1$.

Definição 4.1. *Seja $(G, \otimes)$ um grupo cíclico e finito com n elementos e a e $b \in G$, tal que b é uma potência de a. O logaritmo discreto de b na base a é o menor inteiro x tal que $a^x = b$, denotado por $\log_a b = x$.*

O problema do logaritmo discreto consiste no alto custo computacional em determinar o valor de x, em tempo plausível, para números a e b meticulosamente escolhidos. Abaixo damos um exemplo de como calcular um logaritmo discreto.

Exemplo 4.5. Encontre x tal que $\log_7 9 = x$ em $\mathbb{Z}_{13}$.

Para resolvermos, utilizaremos o método iterativo:

$$7^0 \bmod 13 = 1$$
$$7^1 \bmod 13 = 7$$
$$7^2 \bmod 13 = 10$$
$$7^3 \bmod 13 = 5$$
$$7^4 \bmod 13 = 9$$
$$7^5 \bmod 13 = 11$$
$$7^6 \bmod 13 = 12$$
$$7^7 \bmod 13 = 6$$
$$7^8 \bmod 13 = 3$$
$$7^9 \bmod 13 = 8$$
$$7^{10} \bmod 13 = 4$$
$$7^{11} \bmod 13 = 2$$
$$7^{12} \bmod 13 = 1$$
$$7^{13} \bmod 13 = 7$$
$$7^{14} \bmod 13 = 10$$
$$7^{15} \bmod 13 = 5$$
$$7^{16} \bmod 13 = 9$$

e assim repetidamente...

Como $7^4 = 9mod(13)$ e $7^{16} = 9mod(13)$, a solução é $x = 4$.

Note que esse processo iterativo se torna inviável para números grandes.

4.5.2 Método de Diffie-Hellman

O principal problema com a criptografia simétrica é a troca de chaves entre os envolvidos, pois se a chave for enviada junto com a mensagem de nada adiantará.

O método de Diffie-Hellman é um método criptográfico específico para troca de chaves desenvolvido por Whitfield Diffie [4] e Martin Hellman [5] e publicado em 1976. Foi um dos pioneiros métodos de troca de chaves implementado na criptografia. O método da troca de chaves de Diffie-Hellman permite que duas partes compartilhem uma chave secreta sob um canal de comunicação inseguro. A chave secreta é usada para encriptar mensagens posteriores usando a criptografia de chave simétrica.

Seja k uma chave secreta que deve ser compartihada por A e B o método de Diffie-Hellman consiste em :

1. A e B pré determinam um número primo p e um $\alpha \in \mathbb{Z}_p$, tal que mdc(α , p)=1.
2. A escolhe um número a , tal que $1 < a \leq p-2$, e envia o número $m = \alpha^a \bmod p$ para B.
3. B escolhe um número b , tal que $1 < b \leq p-2$, e envia o número $n = \alpha^b \bmod p$ para A.
4. A calcula $K = n^a = (\alpha^b)^a \bmod p$ e B calcula $K = m^b = (\alpha^a)^b \bmod p$.

Exemplo 4.6. A e B precisam trocar informações utilizando cifra simétrica:
A e B pré determinan um número primo $p = 51$ e um $\alpha = 11$.
A escolhe o número 3 e calcula $m = 11^3 \bmod 51$, $m = 5$, e envia para B.
B escolhe o número 7 e calcula $n = 11^7 \bmod 51$, $n = 20$, e envia para A.
A calcula $K = 20^3 = 44 \bmod 51$ e B calcula $K = 5^7 = 44 \bmod 51$.
Logo a chave secreta entre A e B é 44.

4.5.3 Método de ElGamal

Taher ElGamal [6] desenvolveu em 1985 um método de troca de informações secretas, que hoje é muito utilizado em assinaturas digitais, baseado na dificuldade computacional dos logaritmos discretos.

O método consiste em escolher um grupo $\mathbb{Z}_p$, com p primo grande, previamente conhecido pelas partes envolvidas na comunicação.

[4] Bailey Whitfield Diffie, matemático estadunidense nascido em 5 de junho de 1944.
[5] Martin Edward Hellman, criptógrafo estadunidense nascido em 2 de outubro de 1945.
[6] Taher ElGamal, criptógrafo egício nascido em 18 de agosto de 1955.

O emissor escolhe um inteiro a, tal que $1 < a \leq p-2$ e um gerador inteiro g e calcula $A = g^a$, em seguida envia a chave (A, g) para o receptor.

O receptor escolhe um inteiro b, tal que $1 < b \leq p-2$ e calcula $B = g^b$, para cifrar a mensagem m ele calcula $c = A^b m \bmod p$ e envia para o emissor o par (B, c).

O emissor em seguida calcula $c\dot{B}^{-a} \bmod p$, substituindo c e B temos $m(A^b)(g^b)^{-a} \bmod p$, que por sua vez é equivalente a $m(g^{ab})(g^{-ab}) \bmod p$, encontrando assim a mensagem m.

Exemplo 4.7. B deseja enviar a mensagem $m = 10$ para A , para criar um meio seguro para troca da informação combinam o grupo $\mathbb{Z}_{13}$. A escolhe $a = 3$ e o gerador $g = 2$ e calcula $A = 2^3 = 8$, em seguida envia a chave $(8, 2)$ para B .

B escolhe $b = 5$ e calcula $B = 2^5 = 32$ então encripta a mensagem $m = 10$ com $c = 8^5 \cdot 10 \bmod 13 = 2$ e envia $(32, 2)$ para A.

A calcula $2(32)^{-3} \bmod 13$, que é equivalente à $2(32768)^{-1} \bmod 13 \rightarrow 2(8)^{-1} \bmod 13 \rightarrow 2 \cdot 5 \bmod 13$, chegando à mensagem $m = 10$.

4.6 Criptografia baseada em curvas elípticas

A criptografia baseada em curvas elípticas, tem como um de seus objetivos reduzir o tamanho da chave criptográfica, de modo a tornar viável o uso da criptografia assimétrica em dispositivos com pouca capacidade computacional, como os smartphones.

Praticamente qualquer sistema de chave pública pode ser adaptado para o uso de curvas elípticas, necessitando substituir a operação de exponenciação módulo p pela soma de pontos em um grupo cíclico. As subseções abaixo está baseada em [17].

4.6.1 Método de Diffie-Hellman com curvas elípticas

A construção do algoritmo criptográfico de troca de chaves de Diffie-Hellman, baseado em curvas elípticas, se justifica pela utilização de chaves menores do que as tradicionalmente utilizadas em RSA e sua segurança está baseada na dificuldade do problema do logaritmo discreto.

Supomos que dois indivíduos, o remetente e o destinatário, desejam trocar secretamente suas chaves criptográficas utilizando o sistema de Diffie-Hellman baseado em curvas elípticas. Seguirão os seguintes procedimentos:

- Previamente, tanto o remetente quanto o destinatário, combinam a utilização de uma curva elíptica $E(\mathbb{Z}_p)$, ou da curva elíptica $E(F_q)$ [7] e de um ponto P pertencente a curva.

[7] O corpo F_q é construído a partir de $q = p^n$, com p primo e n inteiro.

- Em seguida o remetente escolhe um inteiro α e calcula αP, através de adição repetida, e o envia para o destinatário sem revelar α, pois α é a chave secreta e αP é a chave pública.
- O destinatário escolhe um inteiro β e calcula βP, também através de adição repetida, e o envia para o remetente sem revelar β.
- Agora ambos podem calcular a chave secreta $\alpha\beta P$.

4.6.2 Algoritmo criptográfico Menezes-Vanstone

Outra aplicação do uso das curvas elípticas na criptografia é através do criptossistema denominado Menezes-Vanstone [8]. Nesse sistema a mensagem m é um par ordenado (x_1, x_2), com x_1 e x_2 pertencentes a um grupo $\mathbb{Z}_p$, mas que não pertencem a curva elíptica $E(\mathbb{Z}_p)$.

A mensagem encriptada r é representada pela tripla ordenada (y_0, y_1, y_2) onde y_0 é um ponto da curva elíptica $E(\mathbb{Z}_p)$ e y_1, y_2 são gerados a partir da mensagem m e também são pertencentes a $\mathbb{Z}_p$.

O algoritmo criptgráfico Menezes-Vanstone consiste em:

1- Um emissor B deseja enviar uma mensagem m para o receptor A , representada pelo par ordenando $m = (x_1, x_2)$, ambos conhecem a curva elíptica $E(\mathbb{Z}_p)$ e um ponto P pertencente a essa curva, sendo esse ponto P a chave "pública"do sistema.

2- Em seguida A escolhe um inteiro s, com $s \in \mathbb{Z}_p$, e calcula $Q = sP$ e o envia para B.

3- O emissor B recebe o ponto Q e escolhe um inteiro k , com $k \in \mathbb{Z}_p$, em seguida encripta a mensagem $m = (x_1, x_2)$:

$$\begin{aligned} kQ &= (c_1, c_2), \\ y_0 &= kP, \\ y_1 &= c_1 \cdot x_1 \bmod p, \\ y_2 &= c_2 \cdot x_2 \bmod p, \end{aligned}$$

E envia $r = (y_0, y_1, y_2)$ para A.

4- Após receber a mensagem r A efetua a decriptação:

$$\begin{aligned} sy_0 = kQ &= (c_1, c_2), \\ x_1 &= y_1(c_1)^{-1} \bmod p, \\ x_2 &= y_2(c_2)^{-1} \bmod p, \end{aligned}$$

[8] Alfred Menezes(1965) e Scott Alexander Vanstone (1947-2014) são co-autores do livro "Handbook of Applied Cryptography".

Assim A recupera a mensagem $m = (x_1, x_2)$ enviada por B.

Exemplo 4.8. Bob irá enviar a mensagem "mct"para Alice, a mensagem legível será $m = (x_1, x_2) = (7767, 84)$, justamente "mc"e "t"codificada na tabela ASCII [9].

Alice e Bob combinam utilizar a curva elíptica $y^2 = x^3 + 67100x + 262147$ sobre o corpo $\mathbb{Z}_{2097421}$ e os pontos P e Q ambos pertencentes a curva elíptica escolhida. Sendo $P(1355793, 621792)$, Alice então escolhe o inteiro $s = 78771$, e calcula o ponto Q como $Q = s \cdot P$.

[9] ASCII (American Standard Code for Information Interchange),desenvolvida a partir de 1960, é uma tabela de códigos usada para representar textos em computadores, entre outros dispositivos que trabalham com texto.

5 Proposta de Atividade para o Ensino Médio

A proposta a seguir tem como objetivo estimular os alunos no estudo da Matemática, mostrando a sua importância, que vai além da aritmética utilizada em situações diárias. Após pesquisar sobre recursos que poderiam ser utilizados na aplicação dos conceitos da criptografia, encontrei um vídeo[1] que ensina a criar um dispositivo para encriptação e decriptação de mensagens, baseado em copos descartáveis, para se trabalhar com sistemas criptográficos baseados na cifra de Cesar e cifras afim. A diferença desta proposta em relação ao vídeo, consiste na utilização de um meio eletrônico para troca de mensagens criptografadas, de modo que todos possam interceptar estes textos, bem como a indicação dos conteúdos matemáticos que podem ser abordados. Com o intuito de maior interação dos alunos, utilizaremos o aplicativo Whatsapp [2], muito comum no dia a dia dos alunos. A escolha do aplicativo se deu pelo grande número de usuários, sendo possível a substituição por outro aplicativo similar.

O público alvo são os alunos do 1º ao 3º ano do Ensino Médio, mas nada impede de ser utilizada nos anos finais do Ensino Fundamental, adaptando conforme necessário.

Inicialmente, o professor terá que dividir os alunos em grupos, de preferência não mais que 8 pessoas, em que pelo menos dois deles tenham o aplicativo Whatsapp e acesso a internet. A quantidade de grupos variará de acordo com a turma. Será preciso também uma forma de identificação dos grupo, que pode ser por cores, números, países, etc. Em seguida, o professor criará um grupo no Whatsapp com os alunos da sala e irá propor o seguinte:

Desafio: Como dois indivíduos podem trocar uma informação sigilosa, de modo que todos possam ler a mensagem, mas que somente o emissor e o destinatário consigam interpretá-la?

Este desafio visa simular um ambiente de comunicação que não seja seguro, ou seja, a informação pode ser capturada ou vista por terceiros, assim como ocorre na internet,

[1] Introdução a criptografia - Aula do MIT, disponível no YouTube em https://youtu.be/wtwlVqEoyyw, 20/10/2015.

[2] Aplicativo de mensagens que permite a criação de grupos para compartilhamento de textos, imagens, vídeos, disponível em diversas plataformas de smartphones.

onde o tráfego de dados pode ser monitorado ou espionado por outras pessoas além do emissor e o destinatário. Para sistematizar a organização dessa proposta dividiremos em partes, sendo apenas uma sugestão, podendo o professor alterá-la conforme necessário.

5.1 Parte 1

O objetivo desta parte consiste em deixar que os grupos criem seus próprios métodos de ocultação da mensagem. O professor será apenas o responsável pela divisão da sala em grupos (pode ser feita por sorteio), a criação do grupo no Whatsapp e construção das mensagens que os grupos trocarão entre si. Além disso, esta parte tem como objetivo, motivá-los ao tema da Criptografia, sua importância para a vida cotidiana e o uso da Matemática para ocultar e descriptografar uma mensagem.

Para começar o professor pedirá que os grupos se reúnam para que possam definir a estratégia/código para a troca das mensagens, de modo que estas não fiquem evidentes para os demais grupos.

Após todos os grupos decidirem a forma de ocultação da mensagem o professor designará um texto diferente para cada um dos grupos, de preferência uma frase pequena, de forma que os demais grupos não tenham acesso. O primeiro grupo, após codificar a mensagem, irá transmiti-la usando o aplicativo para os grupos. Começa então, a tarefa de descobrir qual é a mensagem escolhida pelo professor e transmitida pelo primeiro grupo. Este processo se repetirá até que todos os grupos enviem a sua mensagem codificada.

Após todos os grupos participarem, o professor conduzirá uma discussão geral sobre os casos de sucesso no envio da mensagem, e quais métodos falharam. A intenção não é definir ganhadores ou perdedores e sim, mostrar que há uma grande variedade de métodos de ocultação de mensagens, uns mais eficientes e outros menos.

Em seguida o professor trabalhará os seguintes tópicos:

- Origem e a história da criptografia;
- Algumas técnicas de ocultação de mensagens;
- A importância dos números primos;

5.2 Parte 2

O objetivo desta parte é trabalhar a Cifra de César. Para isto o professor irá trabalhar o algorítimo da Divisão Euclidiana e a congruência. Além disso, nesta parte os grupos irão construir seus dispositivos de encriptação e decriptação, constituído de um

Kit[3] que será feito de acordo com os seguintes materiais:

- Dois copos grandes de plástico descartável;
- Três tiras de papel, o comprimento das tiras deve ser igual ao diâmetro da boca do copo, conforme a Figura 5.1.

Figura 5.1: Material dos Kits.

Em duas das tiras vamos escrever o alfabeto com as 26 letras, como na Figura 5.2. Em seguida, estas tiras deverão ser colada nos copos, conforme a Figura 5.3.

[3]As imagens deste Capítulo são fotos que o próprio autor fez do material que construiu.

Figura 5.2: Alfabeto

Após o Kit construído por cada grupo de alunos, o professor explicará sobre a Cifra de César, enfatizando que esta consiste em deslocar as letras do alfabeto um determinado número de "casas", sendo que essa quantidade de "casas deslocadas"é a

Figura 5.3: Copos e alfabetos.

chave deste método.

O professor convidará os grupos para que possam transmitir uma mensagem utilizando a Cifra de César. Para isso, cada grupo deverá escolher a sua chave e transmitir, via Whatsapp para os demais grupos, uma mensagem que o professor entregará para cada grupo (diferente das utilizadas na Parte 1). Para facilitar a encriptação e decriptação das mensagens, o professor explicará que será utilizado o Kit com os copos colocados um dentro do outro, e ajustando a chave combinada pelo grupo, conforme a Figura 5.4. Dessa forma, podemos efetuar o deslocamento do alfabeto de maneira fácil e rápida, utilizando qualquer chave. É conveniente que o professor apresente um exemplo de como encriptar e decriptar uma mensagem pela Cifra de César utilizando o Kit, antes que os grupos comecem a dinâmica de transmitir as suas mensagens.

Exemplo 5.1. Imaginem que devemos transmitir a seguinte mensagem secreta:

"MATEMÁTICA"

A chave secreta será a letra L. O copo da esquerda será nosso alfabeto original e devemos rotacionar o copo da direita de modo a alinhar a letra L com a letra A. Cada letra do copo da esquerda representará as letras da mensagem original e terá sua correspondente de encriptação no copo da direita e assim a mensagem encriptada será:

"XLEPXLETNL"

Figura 5.4: Cifra de César com a chave criptográfica L.

Para a decriptação da mensagem, basta realizar a operação inversa, alinhar os copos de acordo com a chave e cada letra da mensagem estará no copo da direita. Assim, basta reescrever a mensagem com as letras do copo da esquerda.

Após os alunos realizarem a dinâmica, os grupos perceberão que descobrir a mensagem secreta não é tão difícil, pois notarão que para cada letra há apenas 26 combinações possíveis. Sabendo qual é a letra que mais se repete, em determinado idioma, fica relativamente fácil de descobrir a chave de encriptação, e por isso este método apresenta fragilidade.

5.3 Parte 3

O objetivo desta parte será obter um sistema criptográfico mais eficiente. O conceito matemático trabalhado com os alunos será a Permutação.

Para isso, vamos propor a seguinte modificação no Kit construído na Parte 2: Se em vez de apenas deslocarmos o alfabeto, como na Cifra de César, construirmos uma tira de papel contendo as letras do alfabeto de modo aleatório, por exemplo o da Figura 5.5, aumentaremos a segurança em relação a Cifra de César?

Nesta etapa sugerimos que os copos de cada grupo sejam identificados, como sugerido na Figura 5.6, pois se houver trocas acidentais não será possível decriptar a mensagem.

O professor convidará os grupos para que possam transmitir uma mensagem utilizando o novo Kit de copos. Para isso, cada grupo deverá escolher a sua chave e transmitir, via Whatsapp para os demais grupos, uma mensagem que o professor entregará para cada grupo (diferente das utilizadas nas partes anteriores). Para facilitar a encriptação e decriptação das mensagens, o professor explicará que será utilizado, como anteriormente, o novo Kit com os copos colocados um dentro do outro, e ajustando a chave combinada pelo grupo, conforme a Figura 5.7. Dessa forma, podemos efetuar o deslocamento do alfabeto de maneira fácil e rápida, utilizando qualquer chave. É conveniente que o professor apresente um exemplo de como encriptar e decriptar uma mensagem com este novo Kit, antes que os grupos comecem a dinâmica de transmitir as suas mensagens.

Exemplo 5.2. Utilizando a mesma mensagem secreta:

"MATEMÁTICA"

Manteremos a chave secreta com a letra L. O copo da esquerda será nosso alfabeto original e devemos rotacionar o copo da direita de modo a alinhar a letra L com a letra A. Cada letra do copo da esquerda, representará as letras da mensagem original e terá sua correspondente de encriptação no copo da direita. Assim, a mensagem encriptada será:

"KLWMKLWPRL"

Para decriptação basta realizar a operação inversa, alinhar os copos de acordo com a chave e a cada letra da mensagem estará no copo da direita. Assim, é só reescrever com as letras do copo da esquerda.

O objetivo será alcançado se os alunos perceberem que para descobrir a mensagem secreta haverá mais dificuldade, pois agora teremos 26! possibilidades diferentes de combinação entre as letras, o que torna inviável a tentativa de descobrir a mensagem.

Figura 5.5: Alfabeto e alfabeto posicionado aleatoriamente.

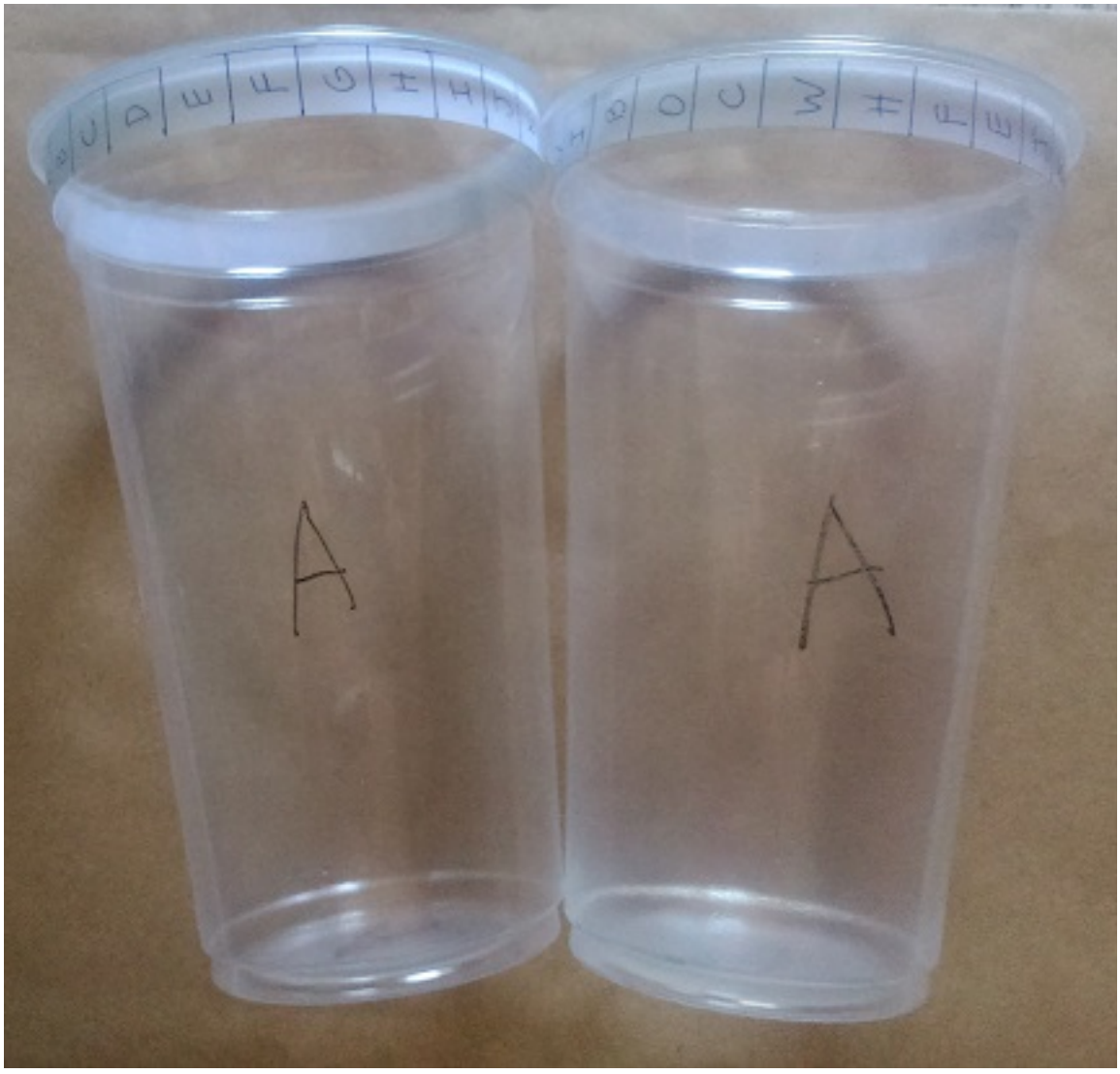

Figura 5.6: Identificando os copos por grupos.

Figura 5.7: Cifra de letras aleatórias com a chave criptográfica L.

6 Considerações Finais

Segundo os Parâmetros Curriculares Nacionais da Matemática [2], o conhecimento matemático é um importante componente na construção da cidadania, que auxilia a apropriação dos conhecimentos científicos e tecnológicos pelos cidadãos. Porém, o ensino da matemática, principalmente na educação básica, apresenta muitos desafios dentre eles, o interesse e a motivação dos estudantes pelos conhecimentos matemáticos.

Sabemos que é necessária uma dedicação dos professores em buscar novos caminhos que tornem a aprendizagem mais significativa e é neste sentido que a Criptografia pode ser uma grande aliada na árdua tarefa do ensino-aprendizagem da Matemática.

Em um mundo cada vez mais tecnológico e interconectado, onde a segurança na transmissão de dados se faz necessária, notamos uma enorme atenção de governos e empresas de segurança da informação a cada nova descoberta na Teoria dos Números, a base da Criptografia.

Assim, este trabalho procurou alinhar a fundamentação teórica para o ensino de alguns conceitos da Matemática com a prática, no que se refere a contextualização destes conceitos com a Criptografia, uma área com infinitas possibilidades e que, além de permitir aplicações da matemática básica até a avançada como mostram os trabalhos da literatura, é importantíssima para o cotidiano em que vivemos.

Referências

[1] ALMEIDA, P. J. *Criptografia e Segurança*. Julho 2012. Departamento de Matemática da Universidade de Aveiro.

[2] BRASIL, S. da E. F. *Parâmentros curriculares nacionais: Matemática*. Brasília: MEC/SEF, 1997.

[3] DAINEZE, K. C. S. A. L. *Números primos e criptografia: Da Relação com a Educação ao sistema RSA*. 2013. Universidade Federal Rural do Rio de Janeiro, Departamento de Matemática - PROFMAT.

[4] DOMINGUES, H. H. *Fundamentos de Aritmética*. 1. ed. São Paulo: Atual, 1991.

[5] FIGUEIREDO, L. M. *Introdução à Criptografia*. v2. Rio de Janeiro: UFF/CEP-EB, 2010.

[6] LEMOS, M. *Criptografia, Números Primos e Algoritmos*. 4. ed. Pernambuco: impa, 2010.

[7] LUZ, W. B. *Introdução à Matemática do Criptossistema RSA*. 2013. Universidade Federal do Sergipe, Pró-Reitoria de Pós-Graduação e Pesquisa - PROFMAT.

[8] MAIER, R. R. *Álgebra I*. 2005. Departamento de Matemática da Universidade de Brasília.

[9] MARQUES, T. V. *Criptografia: abordagem histórica, protocolo Diffie-Hellman e aplicações em sala de aula.* 2013. Universidade Federal da Paraíba, Departamento de Matemática - PROFMAT.

[10] OLIVEIRA, J. P. de. *Introduçao à teoria dos números*. 1. ed. Rio de Janeiro: IMPA, 2007.

[11] OLIVEIRA, M. C. de. *Aritmética: Criptografia e outras aplicações de Congruências*. 2013. Universidade Federal de Mato Grosso do Sul, Centro de Ciências Exatas e Tecnologia - PROFMAT.

[12] OLIVEIRA, K. I. M.; FERNANDEZ, A. J. C. *Iniciação à Matemática: um curso com problemas e soluções*. 1. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2010.

[13] PERUZZO, J. *O facínio dos números Primos*. 1. ed. Santa Catarina: Irani, 2012.

[14] SAMPAIO, J. C.; CAETANO, P. A. S. *Introdução à teoria dos números:Um curso breve*. 1. ed. São Carlos: EdUSCar, 2008.

[15] SAUTOY, M. du. *A música dos números primos: a história de um problema não resolvido na matemática*. 1. ed. Rio de Janeiro: Jorge Zahar, 2007. Traduçao , Diego Alfaro.

[16] SHOKRANIAN, S. *Criptografia para iniciantes*. 2. ed. Rio de Janeiro: Ciência Moderna, 2012.

[17] SILVA, F. B. d. O. Pedro Carlos da. *Curvas Elípticas: Aplicações em Criptografia Assimétrica*. LNCC Laboratório Nacional de Computação Científica-RJ.

[18] SOUZA, C. C. L. *Um Estudo Sobre Criptografia*. 2013. Universidade Estadual Júlio de Mesquita Filho (UNESP - Rio Claro), Instituto de Geociência Exatas.

[19] SOUZA, A. N. L. *Criptografia de Chave Pública, Criptografia RSA*. 2013. Universidade Estadual Júlio de Mesquita Filho (UNESP - Rio Claro), Instituto de Geociência Exatas.

[20] WASHINGTON, L. C. *Elliptic curves: number theory and cryptography*. [S.l.: s.n.], 2008. CRC press.