Universidade Federal do Recôncavo da Bahia - UFRB
Centro de Ciências Exatas e Tecnológicas - CETEC
Programa de Pós Graduação em Matemática em Rede Nacional - PROFMAT
Dissertação de Mestrado

CRIPTOGRAFIA VIA CURVAS ELÍPTICAS: APLICAÇÕES NA EDUCAÇÃO BÁSICA

Patricia Santos Pereira Argolo

Cruz das Almas - Bahia
Fevereiro de 2022

CRIPTOGRAFIA VIA CURVAS ELÍPTICAS: APLICAÇÕES NA EDUCAÇÃO BÁSICA

Patricia Santos Pereira Argolo

Dissertação de Mestrado apresentada ao curso de Mestrado Profissional em Matemática em Rede Nacional do Centro de Ciências Exatas e Tecnológicas da Universidade Federal do Recôncavo da Bahia e Sociedade Brasileira de Matemática como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Anderson Reis da Cruz.

Cruz das Almas - Bahia
Fevereiro de 2022

FICHA CATALOGRÁFICA

A693c

Argolo, Patricia Santos Pereira.

Criptografia via curvas elípticas: aplicações na educação básica / Patricia Santos Pereira Argolo._ Cruz das Almas, BA, 2022.

78f.; il.

Dissertação (Mestrado) – Universidade Federal do Recôncavo da Bahia, Centro de Ciências Agrárias, Ambientais e Biológicas, Mestrado Profissional em Matemática – PROFMAT.

Orientador: Prof. Dr. Anderson Reis da Cruz.

1.Matemática – Curvas elípticas – Criptografia. 2.Matemática – Estudo e ensino – Análise. I.Universidade Federal do Recôncavo da Bahia, Centro de Ciências Agrárias, Ambientais e Biológicas. II.Título.

CDD: 512.742

Ficha elaborada pela Biblioteca Universitária de Cruz das Almas - UFRB.
Responsável pela Elaboração –Antonio Marcos Sarmento das Chagas (Bibliotecário - CRB5 / 1615).
Os dados para Catalogação foram enviados pela usuária via formulário eletrônico.

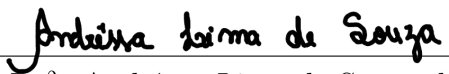
CRIPTOGRAFIA VIA CURVAS ELÍPTICAS: APLICAÇÕES NA EDUCAÇÃO BÁSICA

Patricia Santos Pereira Argolo

Dissertação de Mestrado apresentada ao curso de Mestrado Profissional em Matemática em Rede Nacional do Centro de Ciências Exatas e Tecnológicas da Universidade Federal do Recôncavo da Bahia e Sociedade Brasileira de Matemática como requisito parcial para obtenção do título de Mestre em Matemática, recomendada para aprovação em 18/02/2022.

Banca examinadora:

Prof. Dr. Anderson Reis da Cruz (Orientador)
UFRB



Profª. Drª. Andrêssa Lima de Souza da Cruz
UFRB

Prof. Dr. Edward Landi Tonucci
UEFS

Dedico esse trabalho a minha mãe Lourdes, meu exemplo de força, fé e coragem.

Agradecimentos

Nessa jornada do PROFMAT meu agradecimento especial:

A Deus e a Nossa Senhora Aparecida pela proteção e sabedoria dada em todo percurso.

A minha mãe Lourdes pelo incentivo e amor.

Ao meu amor Neto pela compreensão e apoio de sempre.

As minhas irmãs de sangue e de coração pelo carinho e torcida de sempre.

A minha amiga Delane por me incentivar entrar nessa viagem.

Aos meus amigos Erica Nery e Genildo Nery pelos socorros de sempre.

A minha família e amigos pelo incentivo e torcida.

A todos os meus colegas do PROFMAT pelo amparo durante todo o caminho, fazendo a caminhada mais agradável, leve e divertida.

Ao meu orientador professor Anderson Cruz por ser a minha bússola nesse trajeto final, tornando a chegada mais fácil e suave.

A todos os professores do PROFMAT pelo incentivo e contribuições para a minha formação profissional.

Aos professores Edward Tonucci e Andrêssa Cruz pelo interesse e disponibilidade em participar da banca examinadora e pelas contribuições no trabalho.

"Ninguém é digno do oásis se não aprender a atravessar seus desertos."

Augusto Cury.

Resumo

Visto a importância da criptografia no convívio social, neste trabalho elencamos diferentes esquemas criptográficos utilizados no decorrer da história com o propósito de compreendermos a evolução da criptografia e a sua importância social ao longo dos anos. Em seguida, apresentamos as contribuições de Diffie-Helman para a criptografia de chave pública e o esquema criptográfico RSA. Posteriormente, descrevemos como a criptografia se desenvolve por intermédio das curvas elípticas e abordo algoritmos no ponto de vista da organização e estruturação do pensamento para solucionar problemas e sua afinidade com a criptografia. Por fim, apresentamos algumas sugestões de atividades para serem aplicadas na Educação Básica.

Palavras-chave: Criptografia; Curvas elípticas; Educação Básica.

Abstract

In this work, we presente several examples of cryptographic schemes used at different times in hystory to illustrate the evolution of technology applied to encript messages. We then briefly describe Diffie and Hellman's contributions to public key cryptography and give the description of the RSA scheme. Afterwards, we explain what is an elliptic curve and how it is applied to encript informations. In addition, we present some ideas of algorithms and their importance to solve problems. In particular, the concept of algorithm is closely related to the process of decrypting message by intruders. At the end, we give some suggestions of activities for teaching these topics in basic education.

Keywords: Cryptography; Elliptic curves; Basic education

Sumário

Lista de Figuras

Lista de Tabelas

Introdução

Chegamos ao século XXI e os avanços tecnológicos continuam a todo vapor e é evidente o seu crescimento em todas as áreas, seja na medicina, indústria, comércio, agricultura, no esporte e na educação não é diferente. Se a tecnologia já era necessária no meio educacional, com o desencadear da pandemia em 2019 causada pelo vírus Sars-CoV-2 tornou primordial a sua inserção, pois a pandemia direcionou muitos serviços públicos e privados para o atendimento online e na educação foi necessário adotar o Ensino Remoto. Assim, mais do que nunca precisamos ensinar os nossos alunos a compreender o mundo tecnológico e as suas performances.

Diariamente, fazemos transações bancárias, trocamos mensagem via whatsapp, instagram, facebook, e-mail entre outras redes sociais, e como compreender a confidencialidade das comunicações? Quando acessamos algumas redes sociais e também sites de empresas financeiras, eles comunicam que suas informações estão protegidas por meio da criptografia de ponta a ponta, mas o que significa isso?

A criptografia está presente no nosso dia a dia em diversas situações desempenhado sua função de modo imperceptível na proteção das informações privadas. As mensagens eletrônicas que enviamos diariamente estão protegidas de intrusos em decorrências das evoluções da criptografia ao longo do tempo.

Desse modo, ensinar o aluno a compreender a criptografia e como se desenvolve, é proporcionar ao aluno compreender os meios de comunicações e ampliar a sua visão sobre as tecnologias digitais e sobre os acontecimentos sociais.

O nosso objetivo é apresentar a criptografia por meio das curvas elípticas e propor atividades para serem desenvolvidas na Educação Básica.

Nessa perspectiva, este trabalho esta estruturado da seguinte maneira:

No Capítulo 1, apresentamos noções gerais sobre a criptografia e alguns sistemas criptográficos utilizados ao longo do tempo, posteriormente expandimos a nosso estudo a criptografia de chave pública sugerido por Diffie e Hellman e para a criptografia RSA proposto pelos norte americanos Ronald Rivest, Adi Shamir e Leonard Adleman.

No Capítulo 2, definimos curvas elípticas e estabelecemos a operação de soma entre pontos de uma curva elíptica através de retas tangentes e secantes. Na segunda

seção do capítulo descrevemos os criptossistemas: Diffie- Hellman, Elgamal e de Menezes-Vanstone.

No Capítulo 3, abordamos algoritmo e sua correlação com os sistemas criptográficos e as diferentes maneiras de representar um algoritmo: a linguagem pseudocódigo e a linguagem fluxografica. No final do capítulo, trazemos os algoritmos de Skanks e o método ρ de Pollard que resolve o problema do logaritmo discreto.

Por fim, no capítulo 4, apresentamos sugestões de atividades para serem aplicadas na Educação Básica que abordam curvas elípticas e criptografia sobre curvas elípticas.

Capítulo 1

Noções gerais sobre criptografia

A palavra criptografia é derivada de duas palavras gregas: kryptós que significa oculto e gráphein que significa escrita, essas palavras gregas nos dão pistas de como a criptografia funciona. A criptografia repousa no estudo de técnicas para transformar mensagens de modo que apenas o emissor e o receptor saibam o real significado, ou seja, no estudo das técnicas de codificação e decodificação de textos.

> Na linguagem da criptografia, os códigos são denominados cifras, as mensagens não codificadas são textos comuns e as mensagens codificadas são textos cifrados ou criptogramas. O processo de converter um texto comum em cifrado é chamado cifrar ou criptografar e o processo inverso de converter um texto cifrado em comum é chamado decifrar. ([RORRES 2001] apud [PAIXÃO 2020, p.28]).

Na criptografia podemos citar o método de substituição e o método por transposição que são empregados para a cifração de textos. No método por substituição, as letras conservam a identidade, porém no texto a sua posição é reordenada, já no método por transposição as letras são substituídas por símbolos, mas a sua posição dentro do texto permanece.

O processo de codificar mensagens é realizada com o intuito de manter o teor na mensagem em sigilo, para que intrusos não consigam identificar a real informação contida no texto. Conforme [FIARRESGA 2010, p. 4] a criptografia apresenta quatro objetivos:

- Confidencialidade – mantém o conteúdo da informação secreto para todos excepto para as pessoas que tenham acesso à mesma.
- Integridade da informação – assegura que não há alteração, intencional ou não, da informação por pessoas não autorizadas.
- Autenticação de informação – serve para identificar pessoas ou processos com quem se estabelece comunicação.

• Não repudiação – evita que qualquer das partes envolvidas na comunicação negue o envio ou a recepção de uma informação.

Ao longo do tempo a criptografia vem esboçando sua trajetória com desafios, evolução e magnitude na sociedade. Segundo [LUIZ 2021], os primeiros indícios indica que a criptografia começou a ser usada desde a antiguidade nas regiões do Egito e da Mesopotâmia por volta de 2000 a.C.

Durante séculos a criptografia vem sendo utilizada por governantes e militares em comunicação secretas, até mesmo por pessoas desprovidas de cargos públicos. Assim, vamos elencar alguns sistemas criptográficos utilizados por diferentes governantes na tentativa de tornar suas comunicações confidenciais.

Para iniciar a listagem de alguns sistemas criptográficos, vamos começar pelo Oriente Médio, a região da Palestina para conhecermos algumas cifras utilizadas pelos povos hebreus. Depois, iremos abranger outros continentes para dar continuidade as descrições de algumas cifras que foram importantes no decorrer dos séculos.

De acordo com [FERREIRA 2019], na antiguidade os povos hebreus mantiveram uso três cifras: a cifra ATBASH, cifra ALBAM e a cifra ATBAH. Todas as cifras utilizavam o método de substituição.

A cifra ATBASH considerava o alfabeto de 26 letras, na cifragem da mensagem a primeira letra era trocada pela última letra, a segunda letra era trocada pela penúltima letra, a terceira pela antepenúltima e assim seguia essa lógica até a vigésima sexta letra do alfabeto.

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

Tabela 1.0.1: Cifra ATBASH

Na cifra ALBAM a substituição das letras no texto comum para o texto cifrado, a primeira letra do alfabeto trocava pela décima quarta do alfabeto, a segunda letra do alfabeto era substituída pela décima quinta, a terceira trocava pela décima sexta, seguia essa lógica até a décima terceira letra do alfabeto, a partir da décima quarta letra trocava pelas primeiras letras do alfabeto em ordem decrescente, conforme tabela 1.2:

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

Tabela 1.0.2: Cifra ALBAM

Já na cifra ATBAH, as substituições das letras são organizadas da seguinte maneira: as quatros primeiras letras do alfabeto são substituídas pelas quatro letras subsequentes a sexta posição das letras no alfabeto em ordem decrescente, a quinta letra pela décima terceira, as quatro letras após a nono posição são substituídas, respectivamente, pelas quatro letras que subsequentes a décima quarta posição em ordem decrescente. Por fim, as letras de posições décima oitava até a vigésima primeira, são substituídas pelas quatro últimas letras do alfabeto em ordem decrescente. Para as demais letras basta fazer o processo inverso.

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

Tabela 1.0.3: Cifra de ATBAH

Exemplo 1.0.1. A codificação da palavra PANDEMIA pelas cifras ATBASH, ALBAM e ATBAH pode ser visto na tabela abaixo.

Texto comum	P	A	N	D	E	M	I	A
Texto cifrado/ Cifra ATBASH	K	Z	M	W	V	N	R	Z
Texto cifrado/ Cifra ALBAM	K	N	M	Q	R	Z	V	N
Texto cifrado/ Cifra ATBAH	L	I	E	F	N	O	A	I

A sigla ATBASH deriva do próprio esquema criptográfico. A primeira letra do alfabeto hebraico (aleph), seguida última (taw), seguida pela segunda letra (beth), seguida por shin, penultima letra. Analogamente, ATBAH deriva de aleph teth beth heth e nesse esquema aleph é trocada por teth e beth por heth e ALBAM deriva de aleph lamed beth mem. Veja por exemplo [PRIETO 2020] e [FERREIRA 2019].

No Século V a.C. na cidade de Esparta o Bastão de Licurgo era utilizado da seguinte maneira para codificar a mensagem. Primeiramente, estabelecia bastões de madeira de medidas iguais, ou seja, com as mesmas dimensões para o emissor e o receptor das mensagens. O emissor utilizava um tira de couro ou pergaminho, enrolava no bastão e escrevia o texto, em seguida desenrola a tira e transportava como um cinto até o receptor

da mensagem. O texto escrito na tira de couro ou pergaminho deixava virado para o lado de dentro da cintura. O receptor, ao receber a tira com o texto, enrolava no bastão novamente e identificava a mensagem.

Figura 1.0.1: Bastão de Licurgo. Fonte: [FIARRESGA 2010]

O processo de escrever o texto na tira enrolada no bastão, ao desenrolar a tira, as letras na tira ficam desordenadas e ao enrolar novamente elas mantêm a ordem que foram escritas, isso ocorre pois os bastões possuem as mesmas dimensões. Dessa forma, essa cifra é considerada de transposição.

A cifra de Políbio ou código de Políbio surge por volta de 200 a.C. Essa cifra considera o alfabeto de 23 letras (exclui as letras k, w e y) e baseia-se em uma tabela 6x6. A primeira casa da primeira coluna fica vazia e as demais casas da primeira coluna são preenchidas com as letras A, B, C, D e E, a partir da segunda casa da primeira linha também são preenchidas com as letras A, B, C, D e E. As demais casas são preenchidas com todas as letras do alfabeto, sendo uma letra em cada casa, exceto a casa 3x5 que é preenchida com as letras I e J. A ordem de preenchimento segue a ordem das linhas. É importante ressaltar que a localização das letras para cifrar o texto comum é baseada linhasXcolunas, dessa maneira cada letra do texto comum é localizada na tabela e é substituida, respctivamente pelo par de letras localizadas na primeira coluna e a primeira linha na qual a letra do texto comum esta situada.

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

Tabela 1.0.4: Cifra de Políbio

Exemplo 1.0.2. A codificação da palavra PANDEMIA pela cifra de Políbio pode ser visto na tabela abaixo.

Texto comum	P	A	N	D	E	M	I	A
Texto cifrado	CE	AA	CC	AD	AE	CB	BD	AA

O código de Políbio possui uma outra versão, que é a troca das letras das casas da primeira linha e das casas da primeira coluna por números de 0 até 4. Com isso o texto cifrado deixa de ser representado por letras e passa a ser representado por números.

	0	1	2	3	4
0	A	B	C	D	E
1	F	G	H	I/J	K
2	L	M	N	O	P
3	Q	R	S	T	U
4	V	W	X	Y	Z

Tabela 1.0.5: Cifra numérica de Políbio

Exemplo 1.0.3. A codificação da palavra PANDEMIA pela cifra numérica de Políbio pode ser visto na tabela abaixo.

Texto comum	P	A	N	D	E	M	I	A
Texto cifrado	24	00	22	03	04	21	13	00

A cifra de César ou código César foi método utilizado pelo imperador Júlio César para o envio de mensagem confidenciais para os seus generais. Devido ao seu nome a cifra ficou conhecida como "cifra de César". O imperador Júlio César apostou sua comunicação secreta na troca das letras do alfabeto pela letra que está a 3 posições adiante da letra a ser cifrada, porém as letras de posições $23^{\underline{a}}$, $24^{\underline{a}}$ e $25^{\underline{a}}$ eram substituídas, respectivamente, pelas três primeiras letras do alfabeto. Na cifração das mensagens não considerava os acentos e espaços entre as palavras.

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

Tabela 1.0.6: Cifra de César

Exemplo 1.0.4. A codificação do texto AULAS REMOTAS pela cifra de César pode ser visto na tabela abaixo.

Texto comum	A	U	L	A	S	R	E	M	O	T	A	S
Texto cifrado	D	X	O	D	V	U	H	P	R	W	D	V

A cifra de Alberti ou disco de Alberti conhecido em homenagem ao criador italiano Leon Battista Alberti, foi construída por ele sobrepondo dois discos com diferentes medidas, o menor sobre o maior e dividiu cada circunferência em 24 setores, com ângulos de cada setor com a mesma medida. No disco maior, inseriu em cada setor os números

de 1 até 4 e as letras do alfabeto em ordem crescente, exceto as letras H, J, K, U, W e Y. No disco menor, inseriu apenas as letras do alfabeto de maneira aleatória, mas excluiu as letras J, U e W, por fim sobrou um setor que incluiu o & (et). Em ambos os discos inseriu apenas um símbolo em cada setor.

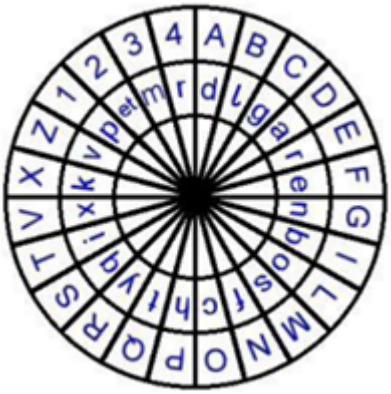


Figura 1.0.2: Disco de Alberti. Fonte: [FIARRESGA 2010]

O processo de cifragem de uma mensagem é realizada da seguinte maneira: Escolhe uma letra-chave e uma palavra-chave. A letra-chave é empregue no disco menor e as letras da palavra-chave observadas no disco maior. Assim para cifrar um texto, alinha a letra-chave com cada letra da palavra-chave na ordem das letras da palavra-chave, em cada alinhamento é cifrada uma letra do texto simples. Finalizada todas as letras da palavra-chave, retorna ao início até que todo o texto seja cifrado. O texto simples é observado no disco maior e a texto cifrado no disco menor.

Exemplo 1.0.5. A codificação do texto VACINAS SALVAM pelo disco de Alberti usando a palavra-chave PANDEMIA pode ser visto na tabela abaixo.

Palavra-chave	PANDEMIA												
Letra-chave	P												
Texto comum	V	A	C	I	N	A	S	S	A	L	V	A	M
Texto cifrado	N	P	A	X	V	G	Y	G	N	Y	I	H	N

A cifra de Vigenére ou a cifra indecifrável como também ficou conhecido pela sua variedade de alfabeto cifrado em uma única cifra e pela crença na impossibilidade de alguém decifrar sem o acesso a palavra-chave. Contudo, segundo [PAIXÃO 2020, p.39] em 1863, Friedrich Kasiski publicou um livro que revelava a decodificação dessa cifra, porém acredita-se que 1854 o cientista Charles Babbage tenha quebrado a cifra de Vigenére, mas que no período da descoberta não a publicou.

A cifra de Vigenére baseava-se em uma tabela 26X26. Nas linhas, a partir da segunda coluna, escrevia o alfabeto com 26 letras, da seguinte forma: na primeira linha,

o alfabeto inicia com a letra A, na segunda linha com a letra B, na terceira linha com C e assim sucessivamente. Observa-se que temos um total de 26 alfabetos cifrados na tabela.

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

Tabela 1.0.7: Tabela de Vigenére

A cifra de Vigenére além de trabalhar com 26 alfabetos cifrados, ainda incluía uma palavra-chave para cifrar e não considerava os acentos e espaços entre as palavras. A palavra-chave era necessário para cifrar e para decifrar a mensagem. Dessa maneira, o receptor da mensagem também deveria conhecer a palavra-chave.

Para cifrar a mensagem deve-se trocar a letra do texto simples pela letra de posição referente a linha relativa a letra do texto simples e coluna relativa a letra da palavra-chave. Como segue no exemplo abaixo:

Exemplo 1.0.6. A codificação do texto AULAS REMOTAS pela cifra de Vigenére usando a palavra-chave PANDEMIA pode ser visto na tabela abaixo.

Palavra-chave	PANDEMIA											
Texto comum	A	U	L	A	S	R	E	M	O	T	A	S
Texto cifrado	P	U	Y	D	W	D	M	M	D	T	N	V

O Enigma foi criado em 1918 pelo engenheiro alemão Arthur Scherbius, no entanto, ficou conhecido na Segunda Guerra Mundial. A máquina Enigma funcionava tanto para encriptar como para decifrar as mensagens, para isso era necessário que o emissor e o receptor estivesse acesso ao instrumento. As principais partes da máquina Enigma era teclado, os modificadores, painel de plugs e o painel luminoso. O teclado, na qual

o operador digitava o texto simples, os modificadores eram responsáveis por alterar os sistemas e determinar a letra cifrada, o painel de plugs que permitiam alterar as letras e o painel luminoso sinalizava a letra cifrada. Cada modificador compreendia um alfabeto de 26 letras.

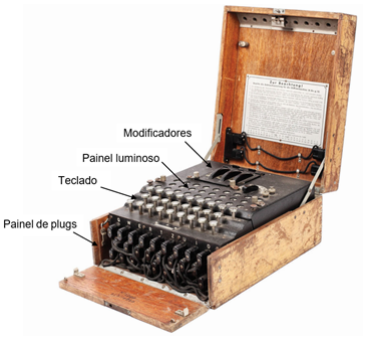


Figura 1.0.3: Máquina Enigma.

Para cifrar a mensagem o emisor posiciona os modificadores e os plugs de acordo com a chave do dia, digita o texto comum no teclado e o texto cifrado é sinalizado no painel luminoso. O processo para decifrar a mensagem é semelhante, o receptor posiciona os modificadores e os plugs de acordo com a chave do dia, digita o texto cifrado no teclado e o texto comum é sinalizado no painel luminoso.

Um fator relevante ao enigma que diferenciava das demais método de cifrar era a grande variedade de chaves que possuía. Essas chaves eram inseridas em um livro e distribuídos para os agentes envolvidos nas comunicações. Assim, acreditava-se que era impossível decifrar as mensagens criptografadas pelo enigma, mas em 1939, uma equipe de matemáticos, composta por Marian Rejewski, Jerzy Różycki e Henryk Zygalski, mostrou o contrário.

Inicialmente, a máquina era composta de três modificadores, com o tempo viram a necessidade de tornar o processo de ciframento mais seguro, desse modo implantado mais dois modificadores e posteriormente mais três. Mesmo com a evolução da máquina Enigma, tempos depois o matemático Alan Turing teve a façanha de quebrar o Enigma.

Com o surgimento e evolução dos computadores veio a necessidades de cifras que pudessem ser agregados a esses novos meios de comunicação.

> Depois da Segunda Guerra Mundial, com a invenção do computador, a área realmente floresceu incorporando complexos algoritmos matemáticos. Durante a guerra, os ingleses ficaram conhecidos por seus esforços para decifração de mensagens. Na verdade, esse trabalho criptográfico formou a base para a ciência da computação moderna (SILVA. 2008. p.137 apud [LUIZ 2021, p.6]).

Assim três décadas após a Segunda Guerra Mundial a álgebra e o trabalho com a teorias dos números entra em cena para impulsionar a criptografia de forma segura.

1.1 Criptografia de chave pública e o RSA.

Todos os esquemas criptográficos mencionados anteriormente utilizam-se do sistema de chave privada, ou seja, esse sistema requer que todos os usuários do esquema criptográfico conheçam a chave que fornece o método de encriptação e decriptação. Deste modo, a cifra é considerada simétrica, já que a chave é única para todos os usuários.

Assim, dois usuários que desejam trocar mensagens cifradas empregando esse sistema de chave privada, ambos devem ter conhecimento da chave para decifrá-las. Considere a seguinte situação hipotética:

Sejam Alice e Duda, dois usuários que desejam trocar informações confidenciais. Alice escolhe um meio para enviar uma mensagem para Duda, no entanto Raul é um intruso que pode interceptar a mensagem enviada por Alice. Assim para que a mensagem chegue até Duda em segurança, sem que Raul entenda o real significado da mensagem enviada, Alice utiliza uma cifra e manda a mensagem encriptada para Duda. Duda por sua vez, utiliza a chave e desencripta a mensagem recebida.

Na situação hipotética descrita, Alice e Duda devem dispor da mesma chave para o processo de encriptação e decriptação. Dessa forma, a fragilidade desse sistema está na troca das chaves, pois qualquer pessoa de posse da chave consegui decifrar a mensagem cifrada.

Até a década de 70 do século passado, a chave privada dominava a criptografia. A partir 1976, um novo esquema criptográfico é prosposto por Whitfield Diffie e Martin E. Hellman e, com isso, o rumo da criptografia é redirecionado. Esse novo esquema criptográfico ficou conhecido como sistema assimétrico ou criptografia de chave pública. A ideia desse novo modelo de sistema consiste na utilização de duas chaves: uma chave pública e uma chave privada. Assim como o significado da própria palavra, a chave pública é de conhecimento de todas e todos podem ter acesso. Em contrapartida a chave privada, apenas o receptor da mensagem a conhece.

Dessa forma, o conceito introduzido de chave pública por Whitfield Diffie e Martin E. Hellman, (a chave pública para cifrar e privada para decifrar) permite que os usuários tenham uma chave que é pública, mas a decriptação da mensagem só é possível pelos indivíduos designados a saberem o teor das mensagens.

Na construção do sistema de chave pública, Diffie e Hellman implementaram a aritmética modular na criptografia. Assim a criptografia mergulhou no universo da álgebra e na teoria dos números para formar sua base e investiu em funções de mão única.funções

de mão única são funções que apresentam dificuldades em retornar ao ponto inicial quando alguma informação é ocultada.

A aritmética modular é uma importante ferramenta para criação de funções de mão única. Lembramos que:

Definição 1.1.1. Sejam a e b dois números inteiros e m um número natural. Se o resto da divisão euclidiana de a e b por m forem iguais, diremos que a e b são congruentes módulo m e denotamos $a \equiv b \, mod \, m$.

Um esquema de criptografia de chave pública é discutido a seguir:

Alice e Duda vão trocar informações confidenciais, para tal usarão meios de comunicação, na qual outras pessoas também têm acesso. Alice e Duda devem gerar as chaves para encriptar e desencriptar a mensagem, de maneira que a chave não seja enviada, para tanto elas seguirão as seguintes etapas.

Alice e Duda combinam dois números Y e p, tal que p seja primo e $Y < p$. Em seguida divulga tais números.

1. Alice escolhe um número d, tal que $d < p$ e guarda.
2. Duda também escolhe um número t, tal que $t < p$ e guarda.
3. Alice calcula $A \equiv Y^d \, mod \, p$ e envia A para Duda.
4. Duda calcula $B \equiv Y^{\,t} mod \, p$ e envia B para Alice.
5. Alice calcula $B^d \equiv (Y^t)^d \equiv \alpha \, mod \, p$.
6. Duda calcula $A^t \equiv (Y^d)^t \equiv \alpha \, mod \, p$.

Observe que Y, A, B e p é de conhecimento de todos e d, t e α são as informações sigilosas e α é a chave para decodificar, ou seja, a chave privada.

Assim, ainda que Raul saiba das informações $Y, A, B, p, A \equiv Y^d \, mod \, p$ e $B \equiv Y^t \, mod \, p$, ele precisa da chave secreta para decodificar as mensagens de Alice e Duda, contudo é necessário que Raul calcule o logaritmo discreto $d \equiv log_Y A \, (mod \, p)$ ou $t \equiv log_Y B \, (mod \, p)$ que é algo inviável, se p possuir centenas de dígitos decimais.

O logaritmo discreto consiste em encontrar x em $\mathbb{Z}_p$ tal que $a^x \equiv b \, (mod \, p)$, chamamos o número x de logaritmo discreto de b na base a e denotamos $x \equiv log_a b \, (mod \, p)$.

Exemplo 1.1.2. Alice e Duda combinam dois números 15 e 19 e tornam públicos. Esses números serão a base e divisor no cálculo da congruência, ou seja, as usuárias deverão calcular $15^x (mod \, 19)$. Individualmente, Alice e Duda escolhe um número e guarda, que são respectivamente 4 e 7. Determinados os números 15, 19, 4 e 7, Alice e Duda seguirão as seguintes etapas:

1. Alice calcula $15^4 \equiv 9 \, mod \, 19$ e envia para Duda.

2. Duda Calcula $15^7 \equiv 13 \, mod \, 19$ e envia para Alice.

3. Alice Calcula $13^4 \equiv 4 \, mod \, 19$.

4. Duda Calcula $9^7 \equiv 4 \, mod \, 19$.

Dessa forma, os números 15 e 19 são as chaves pública e o número 4 é a chave privada. Observe que ambos os usuários obtiveram a chave privada sem necessidade de trocar as chaves.

A partir da proposta de Diffie e Hellman, surgiram outras ideias para a solução do problema da chave pública e a mais conhecida e eficiente até o momento é o algoritmo de ciframento desenvolvido pelos nortes americanos Ronald Rivest, Adi Shamir e Leonard Adleman, conhecido como RSA, em homenagem aos seus nomes.

Um fato importante é que os algoritmos que tentam descobrir o logaritmo discreto fazem testes, ou seja, trabalham utilizando a força bruta. Se o número primo for muito grande o computador irá gastar muito tempo para calcular o logaritmo discreto, pois esse problema é computacionalmente muito difícil ([MARQUES, p. 50]).

Antes de descrevermos como funciona a criptografia RSA, vamos rever algumas propriedades importantes da aritmética modular e da teoria dos números, na qual esse criptossistema apodera-se.

Proposição 1.1.3. *Suponha que $a, b, m \in \mathbb{Z}, m > 1$. Tem-se que $a \equiv b \, mod \, m$ se, e somente se, m divide $b - a$.*

Demonstração. Sejam $a = mq + r$, com $0 \leq r < m$ e $b = mq' + r'$ com $0 \leq r' < m$ respectivamente as divisões euclidianas dos números a e b por m. Observe que $b - a = (mq^{'} + r^{'}) - (mq + r) = m(q^{'} - q) + (r^{'} - r)$, daí que $m \mid b - a$ se $r^{'} - r = 0$, ou seja, $r^{'} = r$. Portanto $a \equiv b \, mod \, m$ se, e somente se, m divide $b - a$. □

Observação 1.1.4. Representamos m divide b por $m|b$.

A seguinte proposição nos dirá que a congruência $mod \, m$ é uma relação de equivalência em $\mathbb{Z}$. Consequentemente podemos particionar $\mathbb{Z}$ nas classes de equivalência por esta relação.

Proposição 1.1.5. *Seja $m \in \mathbb{N}$. Para quaisquer $a, b, c \in \mathbb{Z}$, tem-se que*

1. $a \equiv a \, mod \, m$,

2. se $a \equiv b \, mod \, m$, então $b \equiv a \, mod \, m$,

3. se $a \equiv b \, mod \, m$ e $b \equiv c \, mod \, m$, então $a \equiv c \, mod \, m$.

Demonstração.

1. Observe que $a - a = 0$ e 0 é divisível por m, portanto $a \equiv b \, mod \, m$.

2. Se $a \equiv b \, mod \, m$, então $m|(b - a)$, o que implica que $b - a = mq$ para algum q. Por outro lado, $a - b = m(-q)$, daí $m|(a - b)$ e consequentemente $b \equiv a \, mod \, m$.

3. Como $a \equiv b \, mod \, m$ e $b \equiv c \, mod \, m$, temos que $m|(b - a)$ e $m|(c - b)$, daí que $m|[(b - a) + (c - b)]$, segue que $m|(c - a)$ e, portanto, $a \equiv c \, mod \, m$.

□

O próximo resultado nos mostra como a congruência se relaciona com a soma e o produto.

Proposição 1.1.6. *Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$.*

1. Se $a \equiv b \, mod \, m$ e $c \equiv d \, mod \, m$, então $a + c \equiv b + d \, mod \, m$.

2. Se $a \equiv b \, mod \, m$ e $c \equiv d \, mod \, m$, então $ac \equiv bd \, mod \, m$.

Demonstração.

1. Se $a \equiv b \, mod \, m$ e $c \equiv d \, mod \, m$, então $m|(b - a)$ e $m|(d - c)$, logo temos que $m|(b-a)+(d-c)$, consequentemente $m|(b+d)-(a+c)$. Portanto $a+c \equiv b+d \, mod \, m$.

2. Se $a \equiv b \, mod \, m$ e $c \equiv d \, mod \, m$, então $m|(b - a)$ e $m|(d - c)$. Além disso, $m|d(b - a)$ e $m|a(d - c)$, logo $m|d(b - a) + a(d - c)$. Note que $d(b - a) + a(d - c) = bd - ac$, daí $m|bd - ac$. Portanto $ac \equiv bd \, mod \, m$.

□

Como consequência imediata temos o seguinte.

Corolário 1.1.7. . *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$ e $(c, m) = 1$. Temos que $ac \equiv bc \, mod \, m$ se, e somente se, $a \equiv b \, mod \, m$.*

Se $ac \equiv bc \, mod \, m$ então $m \mid bc - ac$. Como $(c, m) = 1$, se $m \mid (b - a)c$ então m deve dividir $(b - a)$. Reciprocamente, se $a \equiv b \, mod \, m$ a proposição 1.1.6 garante que $ac \equiv bc \, mod \, m$.

Dados a, $b \in \mathbb{Z}$, lembramos que o máximo divisor comum entre a e b é um $d \geqslant 0$ tal que:
i) $d \mid a$ e $d \mid b$.
ii) Se $c \mid a$ e $c \mid b$ então $c \mid d$.

Definimos ainda o mínimo múltiplo comum entre a e b como um $m \geqslant 0$ tal que:
i) $a \mid m$ e $b \mid m$.
ii) Se $a \mid n$ e $b \mid n$ então $m \mid n$.

Denotamos o máximo divisor comum de a e b por (a, b)e o mínimo múltiplo comum de a e b por $[a, b]$.

Estendemos a definição de máximo divisor comum para um número finito de qualquer de inteiros $a_1, ..., a_n$ por $d \geq 0$ tal que:
i) $d \mid a_1$, $d \mid a_2$, ..., $d \mid a_n$.
ii) Se $c \mid a_1$, $c \mid a_2$, ..., $c \mid a_n$ então $c \mid d$.

Analogamente o mínimo múltiplo comum de $a_1, ..., a_n$ é um $m \geq 0$ tal que:
i) $a_1 \mid m$, $a_2 \mid m, ..., a_n \mid m$.
ii) Se $a_1 \mid k$, $a_2 \mid k, ..., a_n \mid k$. então $m \mid k$.

A existência do máximo divisor comum e do mínimo múltiplo comum é garantida pelos seguintes lemas.

Lema 1.1.8. *Sejam a, b, $n \in Z$. Se $(a, b - na)$ existe então (a, b) existe e $(a, b) = (a, b - na)$.*

Lema 1.1.9. *Dados a, $b \in Z$ temos que $[a, b] \cdot (a, b) =\mid ab \mid$.*

As provas destes lemas podem ser consultadas em [[HEFEZ 2016], lema 5.2 e proposição 5.15].

Proposição 1.1.10. *Sejam $a, b \in \mathbb{Z}$ e $m, n, m_1, \ldots, m_r$ inteiros maiores que 1. Temos que*

1. se $a \equiv b \, mod \, m$ e $n \mid m$, então $a \equiv b \, mod \, n$;
2. $a \equiv b \, mod \, m_i$, $\forall i = 1, \ldots, r$ se e somente se $a \equiv b \, mod \, [m_1, \ldots, m_r]$;
3. se $a \equiv b \, mod \, m$, então $(a, m) = (b, m)$.

Demonstração.

1. Se $a \equiv b \, mod \, m$ então $m|(b - a)$, mas $n \mid m$, logo temos que $n|(b - a)$ e, portanto $a \equiv b \, mod \, n$.
2. Se $a \equiv b \, mod \, m_i$, $i = 1, \ldots, r$ então $m_i|(b - a)$, para todo i. Note que $b - a$ é múltiplo de cada m_i, daí que $[m_1, \ldots, m_r]|b - a$. Portanto $a \equiv b \, mod \, [m_1, \ldots, m_r]$. A recíproca decorre do item (i).
3. Se $a \equiv b \, mod \, m$, então $m|(b - a)$, logo $b - a = mt$, com $t \in \mathbb{Z}$. Daí que $b = a + mt$. Pelo 1.1.8 temos que $(a, m) = (a + tm, m)$ e, portanto $(a, m) = (b, m)$.

□

O seguinte teorema estabelece um ponto central na teoria dos números, permitindo o estudo de qualquer inteiro a partir das propriedades de números primos.

Teorema 1.1.11. *(Teorema fundamental da aritmética) Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como produto de números primos.*

Demonstração. Provaremos usando o segundo princípio por indução.

Para $n = 2$ é verdadeira, pois 2 é primo.

Suponhamos que o resultado é válido para todo número natural menor que n, com $n > 2$.

Agora vamos provar que é válido para n.

Se n é um número primo, já é valido. Suponhamos que n seja composto. Logo, existem números n_1 e n_2, tais que $n = n_1 n_2$, com números naturais $1 < n_1 < n$ e $1 < n_2 < n$.

Pela hipótese de indução, temos que existem números primos $p_1, \ldots, p_r$ e $q_1, \ldots, q_s$, tais que $n_1 = p_1 \cdot \ldots \cdot p_r$ e $n_2 = q_1 \cdot \ldots \cdot q_s$. Logo $n = n_1 n_2 = p_1 \cdot \ldots \cdot p . q_1 \cdot \ldots \cdot q_s$.

Portanto $n = p_1 \cdot \ldots \cdot p_r \cdot q_1 \cdot \ldots \cdot q_s$. □

Definição 1.1.12. Seja r um número inteiro positivo. A função de Euler φ é uma função que associa r a um número n inteiro positivo, tal que n é a quantidade de números naturais menores que r e que são coprimos com r.

Exemplo 1.1.13. $\varphi(8) = 4$, visto que os números naturais menores que 8 e que são coprimos com 8 são os números 1, 3, 5 e 7.

Definição 1.1.14. Seja m um número natural. O conjunto $\{r_1, \ldots, r_s\}$ de números inteiros é um sistema de resíduos módulo m se:

1. $(r_i, m) = 1$, para todo $i = 1, \ldots, k$.
2. Se $i \neq j$ então $r_i \neq r_j \, mod \, m$.
3. Para todo a tal que $(a, m) = 1$, existe r_i tal que $r_i \equiv a \, mod \, m$.

Definição 1.1.15. Um sistema de reduzido de resíduos módulo m é um conjunto de $\varphi(m)$ inteiros $r_1, r_2, \ldots, r_{\varphi(m)}$, tais que cada elemento do conjunto é relativamente primo com m, e $i \neq j$, então $r_i \neq r_j (mod \, m)$.

Proposição 1.1.16. *Seja* $r_1, r_2, \ldots, r_{\varphi(m)}$um sistema reduzido de resíduos módulo m e seja $a \in \mathbb{Z}$ tal que $(a, m) = 1$. *Então,* $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ é um sistema de resíduos módulo m.

A demonstração dessa proposição pode ser encontrada no livro [HEFEZ 2016].

Teorema 1.1.17. *(Teorema de Euler) Sejam $m, a \in \mathbb{Z}$ com $m > 1$ e $(a, m) = 1$. Então, $a^{\varphi(m)} \equiv 1 \, mod \, m$.*

Demonstração. Seja $\{r_1, \ldots, r_{\varphi(m)}\}$ um conjunto de resíduo módulo m. Pela Proposição 1.1.16, temos que $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ também forma um sistema de resíduo módulo m, daí que $ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\varphi(m)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} \, mod \, m$.

Note que $ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\varphi(m)} = a^{\varphi(m)} r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)}$ e $(r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)}, m) = 1$ e por meio do Corolário 1.1.7, temos que $a^{\varphi(m)} \equiv 1 \, mod \, m$. □

Teorema 1.1.18. *(Pequeno Teorema de Fermat) Sejam $a \in \mathbb{Z}$ e p um número primo, tais que $(a, p) = 1$. Tem-se que $a^{p-1} = 1 \, mod \, p$.*

Demonstração. Como p um primo, então $\varphi(p) = p - 1$. Pelo Teorema 1.1.17, temos que $a^{p-1} \equiv 1 \, mod \, m$. □

Agora que já relembramos algumas propriedades fundamentais, vamos prosseguir com funcionamento da criptografia RSA.

A criptografia RSA inicia com o usuário que deseja receber a mensagem codificada.

Nessa perspectiva vamos considerar a seguinte situação. Suponhamos que Alice é uma usuária que deseja receber mensagens cifradas, para tanto é necessário que ela divulgue a chave pública para que os usuários que desejam encaminhar mensagens codificadas. Considere o seguinte contexto: Você quer receber cartas de amigos pelos correios, no entanto, você precisa informar o seu endereço para que a correspondência seja entregue na sua casa, caso você não informe corretamente ou deixe de informar, a correspondência não será entregue ou outra pessoa a receberá. No sistema RSA, cada usuário possui uma chave pública que utiliza para codificar as suas mensagens. Assim é necessário que Alice crie a suas chaves e faça a publicação da chave que codifica.

Desse modo, Alice seguirá os seguintes passos:

1. Escolhe dois números primos, p e q.
2. Calcula $r = pq$. Calcula $\varphi(r) = (p - 1)(q - 1)$.
3. Escolhe s, tal que $1 < s < \varphi(r)$ e $mdc(s, \varphi(r)) = 1$.
4. Encontre t que satisfaça $1 < t < \varphi(r)$ e $s \cdot t \equiv 1 \, mod \, \varphi(r)$.
5. Torna público s e r.

Portanto (s, r) são as chaves públicas de Alice. Assim, qualquer usuário que desejar enviar uma mensagem para Alice utilizará a chave (r, s) para codificar. E (s, t) é a chave privada, ou seja, a chave que Alice utilizará para decodificar as mensagens recebidas.

Entretanto para um usuário que deseja encaminhar uma mensagem representada pelo inteiro $M \in [0, r-1]$, deve encaminhar $E = M^s mod\, r$.

Exemplo 1.1.19. Na geração das chaves pública e privada, Alice escolhe os números 17 e 23, segue da seguinte maneira.

1. Calcula $r = 17 \cdot 23 = 391$.
2. Calcula $\varphi(391) = 16 \cdot 22 = 352$.
3. Escolhe $s = 7$, tal que $1 < s < \varphi(391)$ e $mdc\,(s, \varphi(391)) = 1$.
4. Encontre $t = 151$ que satisfaça $1 < t < \varphi(391)$ e $s \cdot t \equiv 1 mod\, 352$.

No final Alice pública os números 391 e 7 que são as suas chaves públicas.

Se r for um número muito grande, com centenas de algarismos, torna difícil calcular $\varphi(r)$. Porém de posse dos valores p e q esse trabalho se torna simples pelo fato de $\varphi(r) = (p-1)(q-1)$.

Exemplo 1.1.20. Duda deseja enviar a mensagem "ENSINO REMOTO" cifrada para Alice. Inicialmente, ela deverá criar uma tabela que relacione cada letra do alfabeto com um número inteiro. Consideremos a tabela abaixo.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Tabela 1.1.1: Correspondência letras e números

Utilizando a tabela Duda converterá as letras em números, assim a mensagem representada por meios de números inteiros será:

5 14 19 9 14 15 18 5 13 15 20 15

De posse da mensagem representada por meio dos inteiros, Duda emprega as chaves públicas de Alice para codificar a mensagem e calcula.

$$316 \equiv 5^7 mod\, 391$$

$$295 \equiv 14^7 mod\, 391$$

$$383 \equiv 19^7 mod\, 391$$

$$257 \equiv 9^7 mod\, 391$$

$$295 \equiv 14^7 mod\, 391$$

$$195 \equiv 15^7 mod\, 391$$

$$52 \equiv 18^7 mod\, 391$$

$$316 \equiv 5^7 mod\, 391$$

$$55 \equiv 13^7 mod\, 391$$

$$195 \equiv 15^7 mod\, 391$$

$$113 \equiv 20^7 mod\, 391$$

$$195 \equiv 15^7 mod\, 391.$$

Assim Duda enviará a mensagem "ENSINO REMOTO" para Alice codificada como:

316 295 383 257 295 195 52 316 55 195 113 195

A decriptação consiste em elevar t ao expoente da unidade de texto cifrado e calcular modulo r, ou seja, calcular $E^t \equiv (M^s)^t mod\, r$, que resulta na recuperação do inteiro M.

Esse processo é justificado pelo seguinte fato:

Escolhidos s, tal que o $(s, \varphi(r)) = 1$, temos pelo Teorema 1.1.17 que:

$$s^{\varphi(\varphi(r))} \equiv 1 mod\, \varphi(r).$$

Observe que $s \cdot t \equiv 1\, mod\, \varphi(r)$ então $s \cdot t \equiv s^{\varphi(\varphi(r))}\, mod\, \varphi(r)$. Portanto, pela Proposição 1.1.6 temos:

$$t \equiv s^{\varphi(\varphi(r))-1} mod\, \varphi(r).$$

A mensagem encriptada é representada por E, quando elevo ao expoente t, temos que

$$E^t \equiv (M^s)^t mod\, r \Rightarrow E^t \equiv M^{st}\, mod\, r. \tag{1.1.1}$$

Por escolha de t, tal que $s \cdot t \equiv 1\, mod\, 352$, daí que $\varphi(r) | st - 1$, desse modo, existe algum inteiro $K > 0$, tal que $s \cdot t - 1 = k\varphi(r) \Rightarrow st = k\varphi(r) + 1$.

Substituindo $s \cdot t$ em (1.1.1), temos que

$$E^t \equiv M^{k\varphi(r)+1} mod\, r \Rightarrow E^t \equiv M^{k\varphi(r)} M mod\, r. \tag{1.1.2}$$

Vamos desdobrar a análise em dois casos:

Caso 1. Se $(M, r) = 1$.

Como o $(M, r) = 1$, temos pelo teorema de Euler que $M^{\varphi(r)} \equiv 1 mod\, r$.

Logo, $E^t \equiv M^{k\varphi(r)} M mod\, r \Rightarrow E^t \equiv M mod\, r$.

Caso 2. Se $(M, r) \neq 1$.

Observe que $\varphi(r) = (p-1)(q-1)$, daí $s \cdot t = k(p-1)(q-1)+1$. Substituindo $s \cdot t = k(p-1)(q-1)+1$ em (1.1.1) temos que:

$$E^t \equiv M^{k(p-1)(q-1)+1} mod\, r.$$

Por outro lado, $r = pq$, então

$$E^t \equiv M^{k(p-1)(q-1)+1} mod\, pq.$$

Aplicando a Proposição 1.1.10 item 1, implica que

$$E^t \equiv M^{k(p-1)(q-1)+1} mod\, p$$

e

$$E^t \equiv M^{k(p-1)(q-1)+1} mod\, q.$$

Note que $M < pq$, então $p|M$ e $q \nmid M$ou $p \nmid M$ e $q|M$. Assim, basta analisar a circunstância na qual $E^t \equiv M^{k(p-1)(q-1)+1} mod\, p$ para as situações que $p|M$ e $p \nmid M$. Desse modo, vamos subdividir em dois casos.

Caso i. Se p divide M.

Note que se $p|M$, então $p|M^{st}$ e $p|M^{st} - M$. Pela Proposição 1.1.6 $M^{st} \equiv M mod\, p$.

Logo, $E^t \equiv M mod\, p$.

Caso ii. Se p não divide M.

Pelo Teorema 1.1.18 temos que $M^{p-1} \equiv 1 mod\, p$. Além do mais $E^t \equiv M^{k(p-1)(q-1)+1} mod\, p \Rightarrow E^t \equiv [M^{(p-1)}]^{k(q-1)} M mod\, p$.

Daí,

$$E^t \equiv [M^{(p-1)}]^{k(p-1)} M mod\, p \Rightarrow E^t \equiv M mod\, p.$$

Logo, $E^t \equiv M mod\, p$.

Colocando q no lugar de p no argumento acima, concluímos que $E^t \equiv M\, mod\, q$. Portanto,

$$E^t \equiv M\, mod\, (p \cdot q)$$

ou seja

$$E^t \equiv M mod\, r.$$

Dessa forma, recuperamos o inteiro M a partir de E.

Agora vamos entender o processo pela qual Alice vai decifrar as mensagens recebida de Duda.

Exemplo 1.1.21. Consideremos novamente o exemplo 1.1.20, Alice deverá elevar as unidades do texto ao expoente 151 em correspondência com os números inteiros enviado por Duda e calcular módulo 391. Assim, o texto codificado é 316 295 383 257 295 195 52 316 55 195 110 195. Alice calcula:

$316^{151} mod\, 391 = 5$
$295^{151} mod\, 391 = 14$
$383^{151} mod\, 391 = 19$
$257^{151} mod\, 391 = 9$
$295^{151} mod\, 391 = 14$
$195^{151} mod\, 391 = 15$
$52^{151} mod\, 391 = 18$
$316^{151} mod\, 391 = 5$
$55^{151} mod\, 391 = 13$
$195^{151} mod\, 391 = 15$
$113^{151} mod\, 391 = 20$
$195^{151} mod\, 391 = 15$

Por fim, Alice encontra a sequência 5 14 19 9 14 15 18 5 13 15 20 15.

Capítulo 2

Curvas Elípticas e Criptossistemas

Inicialmente nesse capítulo, vamos apresentar algumas definições sobre grupos, anéis e corpos, tendo como livro base [DOMINGUES e IEZZI 2003].

2.1 Grupos, anéis e corpos.

Definição 2.1.1. Um par formado por um conjunto não vazio G e uma operação $(x, y) \mapsto x * y$ sobre G é chamada grupo se essa operação satisfaz às seguintes propriedades:

1. Associatividade: $(a * b) * c = a * (b * c)$, quaisquer que sejam $a, b, c \in G$;
2. Existência de elemento neutro: existe um elemento $e \in G$, tal que $a * e = e * a = a$, qualquer que seja $a \in G$ (e é o elemento neutro ou elemento identidade);
3. Existência de simétricos: para todo $a \in G$ existe um elemento $a' \in G$ tal que $a * a' = a' * a = e$.

Neste caso representamos o grupo por $(G, *)$, na qual o símbolo $*$ indica a operação sobre G. Quando a operação já está subtendida podemos apenas expressar "G um grupo", ou ainda " G tem uma estrutura de grupo em relação à operação $*$ ".

Definição 2.1.2. Quando um grupo G satisfaz a propriedade da comutatividade ($a * b = b * a$, quaisquer que sejam $a, b \in G$), dizemos que G é grupo comutativo ou abeliano.

Algumas propriedades de um grupo $(G, *)$:

1. unicidade do elemento neutro;
2. unicidade do simétrico de cada elemento de G;
3. se e é o elemento neutro, então $e' = e$;

4. $(a')' = a$, qualquer que seja $a \in G$.

O leitor pode consultar as propriedades descritas acima, bem como outras propriedades de grupos no livro [DOMINGUES e IEZZI 2003].

Definição 2.1.3. Seja um grupo $(G, *)$ em que G é um conjunto finito, dizemos que G é um grupo finito. Definimos o número de elementos do G como ordem do grupo e representamos com a notação $\#(G)$.

Definição 2.1.4. Seja A um conjunto não vazio, munido de duas operações $(x, y) \mapsto x+y$ e $(x, y) \mapsto x \cdot y$. $(A, +, \cdot)$ é em anel se satisfaz as seguintes condições:

1. $(A, +)$ é um grupo abeliano.

2. A multiplicação goza da propriedade associativa, ou seja, se $a, b, c \in A$, então $a(bc) = (ab)c$.

3. A multiplicação é distributiva em relação à adição, ou seja, se $a, b, c \in A$, então a$(b + c) = ab + ac$ e $(a + b)c = ac + bc$.

4. Quando a multiplicação é comutativa, dizemos que o anel é comutativo.

Comumente chamamos as operações de + por adição e $\cdot$ por multiplicação.

Definição 2.1.5. Um anel $(A, +, \cdot)$ é chamado de corpo se todo elemento não nulo de A admitr um inverso multiplicativo. Isto é, se $x \neq 0$ então existe $x^{-1} \in A$ tal que $xx^{-1} = 1$.

Exemplo 2.1.6. Veja alguns exmplos de corpo.
a)$\mathbb{R}$ com as operações usuais é um corpo.
b) $\mathbb{Q}$com as operações usuais é um corpo.
c) Vimos que anteriormente que a relação de congruência módulo m é uma relação de equivalência. Podemos considerar $\mathbb{Z}_p = \{classes\, de\, equivalência\, mod\, m\}$.

Denotando $[x]_m = \{y \in \mathbb{Z};\, y \equiv x\, mod\, m\}$, ou seja, $[x]_m$ é uma classe de equivalência módulo m de x. Definimos

- $[x]_m + [y]_m \coloneqq [x + y]_m$, para todo $[x]_m, [y]_m \in \mathbb{Z}_m$.
- $[x]_m \cdot [y]_m \coloneqq [x \cdot y]_m$, para todo $[x]_m, [y]_m \in \mathbb{Z}_m$.

Temos que $\mathbb{Z}_m$ é um anel e que se p é um primo então $\mathbb{Z}_p$ é um corpo.
Decorre da definição da congruência que $\mathbb{Z}_m = \{[0]_m, [1]_m, ..., [m-1]_m\}$.
Por abuso de notação escrevemos $0 = [0]_m$, $1 = [1]_m, ..., m-1 = [m-1]_m$.

2.2 Curvas Elípticas.

Definição 2.2.1. Uma curva elíptica C sobre $\mathbb{R}$, é o conjunto dos pontos $(x, y) \in \mathbb{R}^2$ que satisfazem a equação $y^2 = x^3 + ax + b$, em que $4a^3 + 27b^2 \neq 0$ (com $a, b \in \mathbb{R}$), unido a um ponto que chamamos de ponto do infinito, que representaremos pelo símbolo ∞, ou seja, $C = \{(x, y) \in \mathbb{R}^2 : y^2 = x^3 + ax + b\} \cup \{\infty\}$.

A restrição $4a^3 + 27b^2 \neq 0$ garante a existência de retas tangentes à curva elíptica para todo $(x, y) \in C \cap \mathbb{R}^2$. De fato, $C \cap \mathbb{R}^2$ é a curva de nível 0 da função de duas variáveis $f(x, y) = y^2 - x^3 - ax - b$. A existência da reta tangente à essa curva de nível ocorre se e somente se o vetor gradiente no respectivo ponto é não nulo. Mas o gradiente ser não nulo no ponto $(x_0, y_0) \in \mathbb{R}^2$ é o mesmo que dizer que $y_0 \neq 0$ ou $3x_0^2 + a \neq 0$. Ou seja, $y_0^2 = x_0^3 + ax + b \neq 0$ ou $3x_0^2 + a \neq 0$. Isto é equivalente a dizer que x_0 não é uma raiz múltipla de $x^3 + ax + b$. Tal polinômio não admite raiz múltipla se, e somente se $4a^3 + 27b^2 \neq 0$.

Observação 2.2.2. Vamos representar a curva elíptica C sobre o corpo $\mathbb{R}$ da seguinte forma $C(\mathbb{R})$.

Exemplo 2.2.3. Curva elíptica $C : y^2 = x^3 - 3x + 1$.

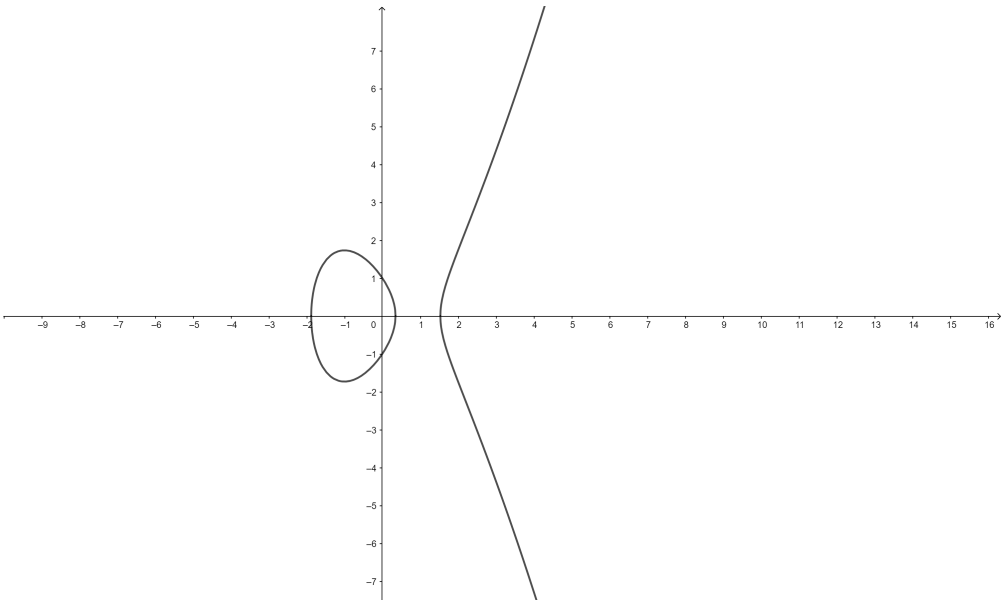


Figura 2.2.1: Gráfico da curva elíptica $y^2 = x^3 - 3x + 1$ definida sobre $\mathbb{R}$.

Um fato importante é que podemos dotar uma curva elíptica de estrutura de grupo. Vamos definir a operação de soma entre pontos de uma curva elíptica, a partir de retas tangentes e secantes, de forma que $(C, +)$ seja um grupo abeliano.

Sejam C uma curva elíptica, pontos $P,\ Q,\ R \in C \cap \mathbb{R}^2$, um ponto do infinito ∞ e uma função de simetria, em relação ao eixo horizontal, $S : \mathbb{R}^2 \longrightarrow \mathbb{R}^2,\ S(x, y) = (x, -y)$.

Representamos $S(R)$ e $S(P)$ os pontos simétricos aos pontos R e P, respectivamente.

Vamos considerar o ponto do infinito ∞ o elemento neutro na operação. Daí que

$$P + \infty := P =: \infty + P,$$

para todo $P \in C$.

- Se $P \neq Q$ e $Q \neq S(P)$ a reta r que passa por P e Q caso exista, $R \in C \cap \mathbb{R}^2$ tal que $R \in r$. Assim, definimos

$$P + Q := S(R).$$

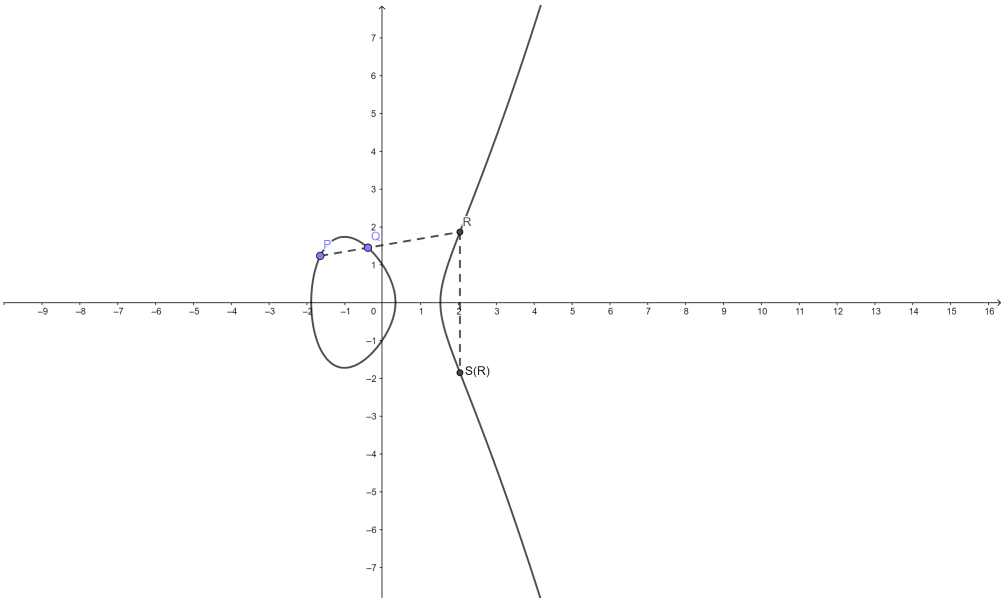


Figura 2.2.2: Gráfico da curva elíptica $y^2 = x^3 - 3x + 1$ definida sobre $\mathbb{R}$: Soma de pontos $P + Q = S(R)$

Agora vamos analisar algebricamente a soma $P + Q = S(R)$ na curva elíptica. Considerando as coordenadas dos pontos $P = (x_p, y_p)$, $Q = (x_q, y_q)$, $R = (x_r, y_r)$, $S(R) = (x_{S(R)}, y_{S(R)})$ e $S(P) = (x_{S(P)}, y_{S(P)})$.

Como a reta r passa pelos pontos P e Q, temos que a equação da reta é dada por

$$y - y_p = m\,(x - x_p) \tag{2.2.1}$$

e o coeficiente angular $m = \frac{(y_q - y_p)}{(x_q - x_p)}$, com $x_q \neq x_p$.

Para obter a interseção da reta r com a curva $C(\mathbb{R})$, basta substituir a equação $y = m\,(x - x_p) + y_p$ na equação da curva $C(\mathbb{R})$. Assim,

$$(m(x - x_p) + y_p)^2 = x^3 + ax + b.$$

Desenvolvendo a expressão, temos que

$$x^3 - m^2x^2 + (a + 2m^2x_p - 2my_p)x + (b - m^2{x_p}^2 + 2mx_py_p - {y_p}^2) = 0. \tag{2.2.2}$$

Considerando $A = -m^2$, $B = a + 2m^2x_p - 2my_p$ e $C = b - m^2{x_p}^2 + 2mx_py_p - {y_p}^2$ e substituindo na equação (2.2.2), temos que

$$x^3 + Ax^2 + Bx + C = 0. \tag{2.2.3}$$

Observe que x_p e x_q são raízes do polinômio 2.2.3. O Teorema Fundamental da Álgebra garante que existe uma terceira raiz x_r, que corresponderá à coordenada do ponto R procurado. Isto somente a existência do ponto de interseção da reta secante com a curva $C \cap \mathbb{R}^2$.

Observe que x_p, x_q e x_r são as raízes da equação da curva $C(\mathbb{R})$, pois P, Q e R são pontos da interseção da reta r com a curva elíptica $C(\mathbb{R})$. Vamos usar o seguinte resultado:

Teorema 2.2.4. *Considere o polinômio $x^3 + Ax^2 + Bx + C$. Sejam r_1, r_2, r_3 raízes reais, possivelmente repetidas, deste polinômio. Então valem*

$$\begin{cases} r_1 + r_2 + r_3 = -A \\ r_1 \cdot r_2 + r_1 \cdot r_3 + r_2 \cdot r_3 = B \\ r_1, \cdot r_2 \cdot r_3 = -C \end{cases}$$

Demonstração. Podemos escrever $x^3 + Ax^2 + Bx + C = (x - r_1)(x - r_2)(x - r_3) = x^3 - (r_1 + r_2 + r_3)x^2 + (r_1 \cdot r_2 + r_1 \cdot r_3 + r_2 \cdot r_3)x - (r_1, \cdot r_2 \cdot r_3)$.

Comparando os polinômios devemos ter que $r_1 + r_2 + r_3 = -A$, $r_1 \cdot r_2 + r_1 \cdot r_3 + r_2 \cdot r_3 = B$ e que $r_1, \cdot r_2 \cdot r_3 = -C$, como queríamos mostrar. □

Este resultado estende-se para qualquer polinômio e é conhecido como Relações de Girard. Vamos aplicá-lo às raízes x_p, x_q e x_r.

Entretanto consideramos $A = -m^2$, daí

$$m^2 = x_p + x_q + x_r.$$

e

$$x_r = m^2 - x_p - x_q. \tag{2.2.4}$$

Para obtermos o y_r, basta substituir as coordenadas do ponto R na equação (2.2.1), já que R $\in C(\mathbb{R})$, daí

$$y_r - y_p = m(x_r - x_p) \Longrightarrow y_r = m(x_r - x_p) + y_p. \tag{2.2.5}$$

Como $P + Q = S(R)$, de acordo com a função de simetria S, temos que

$$S(R) = (x_{S(R)}, y_{S(R)}) = (x_r, -y_r).$$

Substituindo as coordenadas de $S(R)$ nas equações (2.2.4) e (2.2.5), temos que

$$x_{S(R)} = m^2 - x_p - x_q \Longrightarrow x_{S(R)} = \left(\frac{y_q - y_p}{x_q - x_p}\right)^2 - x_p - x_q$$

$$y_{S(R)} = m(x_p - x_r) - y_p \Longrightarrow y_{S(R)} = \left(\frac{y_q - y_p}{x_q - x_p}\right)(x_p - x_{S(R)}) - y_p.$$

- Se $P \neq S(P)$, a reta tangente à curva elíptica no ponto P, intersecta a curva em um ponto $R.$, como veremos adiante.

$$P + P \coloneqq S(R).$$

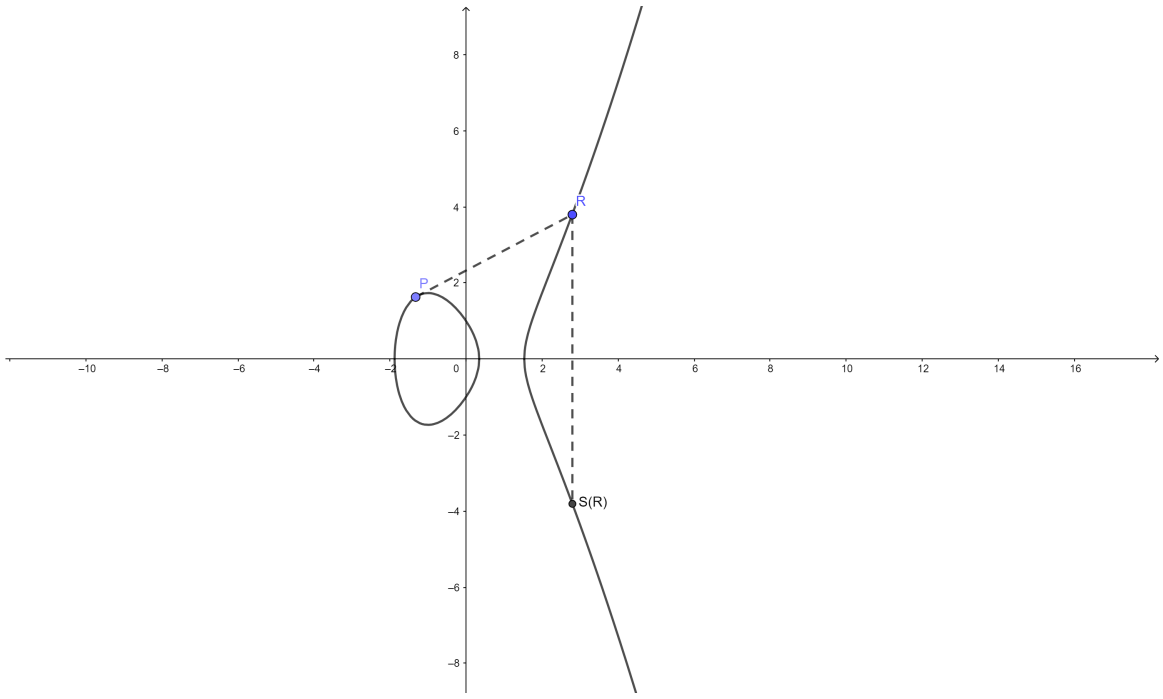


Figura 2.2.3: $y^2 = x^3 - 3x + 1$

Analisando algebricamente, temos que a reta é tangente à curva elíptica no ponto P. Daí utilizando derivação implícita sobre $y^2 - x^3 - ax - b = 0$, temos que o coeficiente angular dessa reta que é tangente à curva elíptica no ponto P é dada por

$$m = \frac{3x_p^2 + a}{2y_p}.$$

Nessa formula y_p é diferente de 0, pois $P \neq S(P)$.

Como mencionamos anteriormente que, a equação fundamental da reta é dada por

$$y - y_p = m(x - x_p). \tag{2.2.6}$$

Seguindo o mesmo procedimento realizado anteriormente, temos que a interseção da reta com a curva elíptica é representada pela equação $x^3+ax+bx+c = 0$. Temos que x_p é raiz de $[y_p + m(x - x_p)]^2-(x^3 + ax + b^2)$. Mas também é raiz de $2\,[y_p + m(x - x_p)] \cdot m-(3x^2 + a)$. Portanto, x_p é raiz de $[y_p + m(x - x_p)]^2 - (x^3 + ax + b^2)$, com multiplicidade maior ou igual a 2. Novamente utilizando as relações de Girard, temos que $-a = x_p + x_p + x_r$.

Entretanto consideramos

$$a = -m^2,$$

daí

$$m^2 = 2x_p + x_r \text{ e } x_r = m^2 - 2x_p. \tag{2.2.7}$$

Para determinar o y_r, basta substituir as coordenadas do ponto R na equação (2.2.6),

$$y_r - y_p = m(x_x - x_p) \Longrightarrow y_r = m(x_r - x_p) + y_p. \tag{2.2.8}$$

Como $P + P = S(R)$, temos que

$$S(R) = (x_{S(R)}, y_{S(R)}) = (x_r, -y_r).$$

Substituindo as coordenadas de $S(R)$ nas equações (2.2.7) e (2.2.8), temos que

$$x_{S(R)} = m^2 - 2x_p \Longrightarrow x_{S(R)} = \left(\frac{3x^2 + a}{2y_p}\right)^2 - 2x_p$$

$$y_{S(R)} = m(x_p - x_r) - y_p \Longrightarrow y_{S(R)} = \left(\frac{3x^2 + a}{2y_p}\right)(x_p - x_{S(R)}) - y_p$$

- No caso em que $P \neq S(P)$ e desejamos calcular $P + S(P)$ usando os procedimentos anteriores não será possível encontrar o ponto $R \in C \cap \mathbb{R}^2$ interseção da reta tangente/secante com a curva elíptica. Nesta situação definimos:

$$P + S(P) \coloneqq \infty$$

- Para $P = S(P)$ e desejamos calcular $P + P$, analogamente ao caso anterior definimos:

$$P + P \coloneqq \infty$$

Como a $P = S(P)$ a reta tangente a curva no ponto P é paralela ao eixo das ordenadas.

Resumimos os procedimentos acima na seguinte definição.

Definição 2.2.5. Seja C uma curva elíptica sobre $\mathbb{R}$ e os pontos $P, Q \in C$, temos que

- $\infty + P = P$ e $P + \infty = P$, para todo $P \in C$.
- $P + S(P) = \infty$.
- Se $P \neq S(P)$, então $P + P = S(R)$, em que R é o ponto de interseção da reta tangente à curva elíptica no ponto P com a curva elíptica C.
- Se $P \neq Q$ e $Q \neq S(P)$, então $P + Q = S(R)$, em que R é o ponto de interseção da reta secante a P e Q que passo pelos pontos P e Q com a curva elíptica C.

Observe que uma curva elíptica sobre $\mathbb{R}$ consiste de um conjunto não enumerável de pontos. Com vistas a um tratamento computacional é interessante que consideremos conjuntos finitos/discretos. Uma forma de realizarmos isto é procurarmos por soluções em $\mathbb{Z}_p$, com p primo, para a equação $y^2 = x^3 + ax + b$. Vimos que nesta situação $\mathbb{Z}_p$ é um corpo, o que permitirá o aproveitamento da estrutura definida para a curva elíptica sobre $\mathbb{R}$.

Agora vamos partir para uma importante etapa na criptografia em curvas elípticas que é o trabalho dessas curvas sobre corpos finitos $\mathbb{Z}_p$, com p um número primo, tal que $\mathbb{Z}_p = \{0,\ 1,\ ...,\ p-1\}$ um conjunto finito de pontos.

Curvas elípticas sobre corpos finitos $\mathbb{Z}_p$ é o conjunto dos pontos $(x, y) \in \mathbb{Z}_p^2$ que satisfazem a equação $C : y^2 = x^3 + ax + b$, com $a,\ b\ \in \mathbb{Z}_p$ e $4a^3 + 27b^2 \not\equiv 0\ mod\ Z_p$ unido o ponto do infinito.

Exemplo 2.2.6. Considerando a curva elíptica $C :\ y^2 = x^3 + 2x + 6$ sobre o corpo finito $\mathbb{Z}_7$. Vamos calcular os pontos $\mathbb{Z}_7$ que satisfazem a equação da curva C, para isso vamos fazer todos os cálculos em função do resto da divisão por 7.

Dessa forma, vamos substituindo os pontos de $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ na equação da curva C e analisar quais deles satisfaz $y^2 = x^2 + 2x + 6\, mod\ 7$. Representaremos tal situação na tabela abaixo.

y	$y^2 (mod\ 7)$	x	$x^3 + 2x + 6\ (mod\ 7)$
0	0	0	6
1	1	1	2
2	4	2	4
3	2	3	4
4	2	4	1
5	4	5	1
6	1	6	3

Tabela 2.2.1: Pontos da curva elíptica $C : y^2 = x^3 + 2x + 6$ sobre $\mathbb{Z}_7$.

Comparando as tabelas de $y^2 mod\ 7$ e $x^3 + 2x + 6\, mod\ 7$ acima, concluímos que $C(\mathbb{Z}_7) = \{\infty, (1,3), (1,4), (2,2), (2,5), (3,2), (3,5), (4,1), (4,6), (5,1), (5,6)\}$.

Observe que apenas 10 pares $(x, y) \in \mathbb{Z}_7^2$ que satisfazem a curva $C : \ y^2 = x^3 + 2x + 6$. Representamos esses pontos da curva $C(\mathbb{Z}_7)$ no plano cartesiano abaixo.

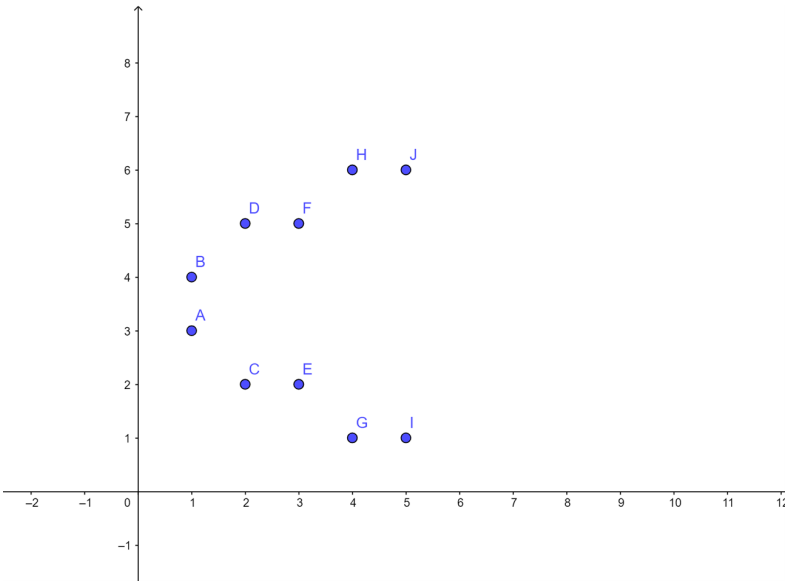


Figura 2.2.4: Gráfico da curva elíptica $C : y^2 = x^3 + 2x + 6$ sobre $\mathbb{Z}_7$.

Generalizando para qualquer p primo, note que conjunto $\mathbb{Z}_p$ é finito, assim temos apenas p valores que x podem assumir e consequentemente, para cada valor de x podemos obter até duas possibilidades para y, pois se (x, y) é solução, $(x, -y)$ também é solução da equação da curva. Sendo assim, até $2p$ possibilidades de pares que satisfazem a curvas elípticas sobre corpos finitos $\mathbb{Z}_p$, além disso temos o ponto no infinito, totalizando $2p + 1$ elementos que uma curvas elípticas sobre corpos finitos $\mathbb{Z}_p$ pode conter no máximo.

Podemos estimar a quantidade de elementos do conjunto dos pontos de $\mathbb{Z}_p$ que satisfazem a curva elíptica C através do Teorema de Hasse.

Teorema 2.2.7. *(Teorema de Hasse) Se $C(\mathbb{Z}_p)$ é uma curva elíptica sobre $\mathbb{Z}_p$ então* $|| \ C(\mathbb{Z}_p) \ | - 1 - (p + 1)| \leq \ 2\sqrt{p}$.

Veja por exemplo [KOBLITZ 1998].

No que refere-se as operações em $C(\mathbb{R})$, as mesmas propriedades podem ser consideradas nas expressões algébricas em $\mathbb{Z}_p$.

Exemplo 2.2.8. Consideremos a curva elíptica $C : \ y^2 = x^3 + 2x + 6$ sobre $\mathbb{Z}_7$ e os pontos (1,3), (1,4),(2,5), (4,6). Vamos calcular a soma entre $(1, 3)$ e $(1, 4)$:

Note que os valores das abcissas são iguais, logo esses pontos são simétricos e pelo definição, temos que $(1, 3) + (1, 4) = \infty$.

Para a soma de $(2,5)$ e $(2,5)$ temos que $(2,5)$ é diferente do seu simétrico $(2,2)$. Sendo assim

$$x_{S(R)} \equiv \left(\frac{3\cdot 2^2+2}{2\cdot 5}\right)^2 - 2\cdot 2 \equiv 0^2 - 4 \equiv -4 \equiv 3 \; mod \; 7$$

e

$$y_{S(R)} \equiv \left(\frac{3\cdot 2^2+2}{2\cdot 5}\right)(2-3) - 2 \equiv -5 \equiv 2 \; mod \; 7.$$

Portando temos que $(2,5)+(2,5)=(3,2)$.

Já a soma de $(2,5)$ e $(4,6)$, note que $(2,5) \neq (4,6)$ e $(4,6) \neq (2,2)$, ou seja o ponto $(4,6)$ é diferente do simétrico do ponto $(2,5)$. Assim, temos que

$$x_{S(R)} \equiv \left(\frac{6-5}{4-2}\right)^2 - 2 - \; 4 \equiv 4^2 \; - 2 - 4 \equiv 10 \equiv 3 \; mod \; 7$$

e

$$y_{S(R)} \equiv 4\,(2-3) - 5 \equiv -4 - 5 \equiv -9 \equiv 5 \; mod \; 7.$$

Portanto $(2,5)+(4,6)=(3,5)$.

Na tabela abaixo, estão representadas as somas dos pontos de $C(\mathbb{Z}_7)$.

+	∞	(1,3)	(1,4)	(2,2)	(2,5)	(3,2)	(3,5)	(4,1)	(4,6)	(5,1)	(5,6)
∞	∞	(1,3)	(1,4)	(2,2)	(2,5)	(3,2)	(3,5)	(4,1)	(4,6)	(5,1)	(5,6)
(1,3)	(1,3)	(2,2)	∞	(5,1)	(1,4)	(5,6)	(4,1)	(4,6)	(3,2)	(3,5)	(2,5)
(1,4)	(1,4)	∞	(2,5)	(1,3)	(5,6)	(4,6)	(5,1)	(3,5)	(4,1)	(2,)	(3,2)
(2,2)	(2,2)	(5,1)	(1,3)	(3,5)	∞	(2,5)	(4,6)	(3,2)	(5,6)	(4,1)	(1,4)
(2,5)	(2,5)	(1,4)	(5,6)	∞	(3,2)	(4,1)	(2,2)	(5,1)	(3,5)	(1,3)	(4,6)
(3,2)	(3,2)	(5,6)	(4,6)	(2,5)	(4,1)	(5,1)	∞	(1,3)	(2,2)	(1,4)	(3,5)
(3,5)	(3,5)	(4,1)	(5,1)	(4,6)	(2,2)	∞	(5,6)	(2,5)	(1,4)	(3,2)	(1,3)
(4,1)	(4,1)	(4,6)	(3,5)	(3,2)	(5,1)	(1,3)	(2,5)	(1,4)	∞	(5,6)	(2,2)
(4,6)	(4,6)	(3,2)	(4,1)	(5,6)	(3,5)	(2,2)	(1,4)	∞	(1,3)	(2,5)	(5,1)
(5,1)	(5,1)	(3,5)	(2,2)	(4,1)	(1,3)	(1,4)	(3,2)	(5,6)	(2,5)	(4,1)	∞
(5,6)	(5,6)	(2,5)	(3,2)	(1,4)	(4,6)	(3,5)	(1,3)	(2,2)	(5,1)	∞	(4,1)

Tabela 2.2.2: Soma dos pontos da curva elíptica $C : y^2 = x^3 + 2x + 6$ sobre $\mathbb{Z}_7$.

As operações assim definidas em $\mathbb{Z}_p$, introduzem uma estrutura de grupo em $C(\mathbb{Z}_p)$, veja [SILVERMAN 1986].

A multiplicação de um ponto P por $n \in \mathbb{N}$ em $C(\mathbb{Z}_p)$ é o mesmo que somar este ponto n vezes. E a multiplicação por $n \in \mathbb{Z}$,com $n < 0$ é o mesmo que considerar o inverso aditivo de $(-n)\,P$.

Exemplo 2.2.9. Na tabela abaixo, representamos a multiplicação de n pelos pontos de $C(\mathbb{Z}_p)$.

n	$n(1,3)$	$n(1,4)$	$n(4,6)$
1	(1,3)	(1,4)	(4,6)
2	(2,2)	(2,5)	(1,3)
3	(5,1)	(5,6)	(3,2)
4	(3,5)	(3,2)	(2,2)
5	(4,1)	(4,6)	(5,6)
6	(4,6)	(4,1)	(5,1)

Tabela 2.2.3: Multiplicação de alguns pontos da curva elíptica $C : y^2 = x^3 + 2x + 6$ sobre $\mathbb{Z}_7$.

Seja P um ponto da curva elíptica $C : \ y^2 = x^3 + ax + b$ sobre o corpo finito $\mathbb{Z}_p$ e $n \in \mathbb{N}$, dizemos que P é gerador do grupo $C(\mathbb{Z}_p)$ se calculamos nP com $n \in \mathbb{Z}$ obtemos todos os pontos da curva $C(\mathbb{Z}_p)$, com $n = 1, ..., k$.

Exemplo 2.2.10. O ponto $(1, 3)$ é gerador da curva $C : y^2 = x^3 + 2x + 6$ sobre $\mathbb{Z}_7$, conforme a tabela abaixo.

n	Soma de n vezes (1,3)	$=$
1	(1,3)	(1,3)
2	(1,3)+1·(1,3)	(2,2)
3	(1,3)+2·(1,3)=(1,3)+(2,2)	(5,1)
4	(1,3)+3·(1,3)=(1,3)+(5,1)	(3,5)
5	(1,3)+4·(1,3)=(1,3)+(3,5)	(4,1)
6	(1,3)+5·(1,3)=(1,3)+(4,1)	(4,6)
7	(1,3)+6·(1,3)=(1,3)+(4,6)	(3,2)
8	(1,3)+7·(1,3)=(1,3)+(3,2)	(5,6)
9	(1,3)+8·(1,3)=(1,3)+(5,6)	(2,5)
10	(1,3)+9·(1,3)=(1,3)+(2,5)	(1,4)
11	(1,3)+10·(1,3)=(1,3)+(1,5)	∞

Tabela 2.2.4: Gerador da curva elíptica $C : y^2 = x^3 + 2x + 6$ sobre $\mathbb{Z}_7$.

Note que todos os pontos de $C(\mathbb{Z}_7)$ geram os demais pontos da curva.

2.3 Criptografia via Curvas Elípticas.

Agora vamos apresentar os criptossistemas por meio de curvas elípticas, na qual também se fundamenta o Problema do Logaritmo Discreto, semelhante ao criptossistema RSA. No sistema RSA, tem-se que dado um grupo multiplicativo e fixado um B, o Problema do Logaritmo Discreto concentra-se na dificuldade de encontrar um x tal que $A^x = B$, ou seja, calcular o $\log_A B = x$, já no caso das curvas elípticas, temos que dado uma curva C e fixado um $B \in C(\mathbb{Z}_p)$ a dificuldade está em encontrar um $x \in \mathbb{Z}$, tal que $Ax = B$, com $A \in C(\mathbb{Z}_p)$.

Trazendo para este capítulo as personagens Alice e Duda, e suas comunicações para essa seção, vamos apresentar os criptossistemas de Diffie Hellman, Elgamal e Menezes -Vanstone, com respectivas exemplificações.

2.3.1 Sistema de troca de chaves de Diffie Hellman.

Vamos supor que Alice e Duda desejam trocar mensagens confidenciais por vias não seguras de comunicação. No entanto, decidem criptografar as mensagens utilizando curvas elípticas sobre corpos finitos $\mathbb{Z}_p$.

Inicialmente, elas geram as chaves para encriptar e desencriptar as mensagens. Utilizando as seguintes estratégias. Escolhem uma curva Elíptica $C : y^2 = x^3 + ax + b$, com $a,\ b\ \in \mathbb{Z}_p$, tal que $4a^3 + 27b^2 \not\equiv 0 \, mod \, p$ e um $B \in C(\mathbb{Z}_p)$. Essas informações são combinadas publicamente. Depois as etapas seguintes serão realizadas:

1. Alice escolhe um inteiro n e guarda.
2. Duda escolhe um inteiro m e guarda.
3. Alice calcula $n \cdot B = A$ e envia para Duda.
4. Duda calcula $m \cdot B = D$ e envia para Alice.
5. Alice calcula $n \cdot D = n \cdot m \cdot B = P$.
6. Duda calcula $m \cdot A = m \cdot n \cdot B = n \cdot m \cdot B = P$.

Dessa forma, a curva elíptica C e B são as chaves públicas e P é a chave privada. Observe que Alice e Duda estão de posse dos números inteiros n e m, respectivamente, daí é fácil para ambas calcular P, mas para outro qualquer que deseje calcular P de posse apenas dos resultados $n \cdot B$ e $m \cdot B$ é um trabalho difícil para um primo p muito grande.

Para melhor entendimento desse método de criptografar utilizando curvas elípticas sobre corpos finitos $\mathbb{Z}_p$, vamos trazer um exemplo, porém com números pequenos.

Exemplo 2.3.1. Alice e Duda escolhem a curva elíptica $C:\ y^2 = x^3 + 2x + 6$ sobre o corpo finito $\mathbb{Z}_7$ e $B = (1, 3)$.

1. Alice escolhe um inteiro 2 e guarda.
2. Duda escolhe um inteiro 3 e guarda.
3. Alice calcula $2\cdot (1, 3) = (2, 2) =$ e envia para Duda.
4. Duda calcula $3\cdot (1, 3) = (5, 1)$ e envia para Alice.
5. Alice calcula $2\cdot (5, 1) = 2\cdot 3\cdot (1, 3) = (4, 6)$.
6. Duda calcula $3\cdot (2, 2) = 3\cdot 2\cdot (1, 3) = (4, 6)$.

Observe que a curva elíptica $C:\ y^2 = x^3 + 2x + 6$ sobre o corpo finito $\mathbb{Z}_7$ e $B = (1, 3)$ são as chaves públicas e $(4, 6)$ é a chave privada.

2.3.2 Criptossistema de Elgamal.

Nesse criptossistema vamos considerar que Alice deseja enviar uma mensagem numérica M para Duda. Assim como no criptossistema de Diffie Hellman, no criptossistema de Elgamal a primeira etapa é a escolha da curva Elíptica $C : y^2 = x^3 + ax + b$, com $a,\ b\ \in \mathbb{Z}_p$, tal que $4a^3 + 27b^2 \not\equiv 0\, mod\, \mathbb{Z}_p$ e um $B \in C(\mathbb{Z}_p)$, informações públicas. Em seguida as etapas seguintes serão desencadeadas:

1. Duda escolhe um inteiro $d\ \in \mathbb{Z}_p$ e guarda.
2. Duda calcula $D = d\cdot B$ e publica.

Cifrar a mensagem numérica M, sendo M um ponto da curva elíptica:

1. Alice escolhe um inteiro k e calcula $M_1 = kB$ e $M_2 = M + kD$ envia o par (M_1, M_2).

Para Duda decodificar a mensagem numérica M:

1. Duda multiplica d pelo primeiro ponto M_1 e subtrai no segundo ponto

$$M_1\cdot d = kB\cdot d$$

$$M_2 - kBd = M + kD - kBd = M + kdB - kdB = M.$$

Exemplo 2.3.2. Alice e Duda escolhem a curva elíptica $C:\ y^2 = x^3 + 2x + 6$ sobre o corpo finito $\mathbb{Z}_7$ e $B = (1, 4)$.

1. Duda escolhe um inteiro 3 e guarda.

2. Duda calcula $3\cdot(1,4) = (5,6)$ e publica.

Cifrar a mensagem numérica $M = (2,2)$.

1. Alice escolhe um inteiro 4 e calcula $4\cdot(1,4) = (3,2)$ e $(2,2) + 4\cdot(5,6) = (1,3)$ envia o par $((3,2),(1,3))$.

Para Duda decodificar a mensagem numérica M.

1. Duda multiplica 3 pelo primeiro ponto $(3,2)$e subtrai no segundo ponto (1,3), ou seja soma com o inverso aditivo.

$$(3,2)\cdot 3 = 4\cdot 3\cdot(1,4) = (1,4)$$

$$(1,3) - (1,4) = (2,2) + 4\cdot(5,6) - (1,4) = (2,2) + (1,4) - (1,4) = (2,2)$$

2.3.3 Criptossistema de Menezes -Vanstone.

No sistema criptográfico de Menezes-Vanstone a mensagem é representada por um par ordenado $M = (m_1, m_2) \in \mathbb{Z}_p^2$, é convertida em uma tripla ordenada (y_0, y_1, y_1), subsequentemente o receptor a transforma a trinca no par ordenada original para identificar a mensagem.

Dando continuidade a comunicação entre Alice e Duda, consideremos que Alice deseja enviar uma mensagem para Duda utilizando este novo sistema. Como nos demais criptossistemas vias curvas elípticas apresentadas anteriormente, previamente são definidas a curva Elíptica $C : y^2 = x^3 + ax + b$, com $a,\ b\ \in \mathbb{Z}_p$, tal que $4a^3 + 27b^2 \not\equiv 0\ mod\ \mathbb{Z}_p$ e um $B \in C(\mathbb{Z}_p)$.

Geração das chaves:

1. Duda escolhe $d \in\ \mathbb{Z}$.

2. Duda Calcula $d\cdot B = D$ e publica.

Codificando a mensagem:

1. Alice escolhe um inteiro k.

2. Alice Calcula

$$y_0 = k\cdot B,$$

$$S = k\cdot D = (x_s, y_s),$$

$$y_1 \equiv x_s\cdot m_1 mod p$$

e

$$y_2 \equiv y_s\cdot m_2 mod\ p.$$

3. Alice converte a mensagem numericamente em $M = (m_1, m_2)$, com $m_1, m_2 \in \mathbb{Z}_p$ e $M \notin C(\mathbb{Z}_p)$.

4. Alice envia $(y_0,\ y_1, y_2)$.

Decifrando a mensagem:

1. Duda calcula

$$d\cdot y_0 = d\cdot k\cdot B = k\cdot D = S = (x_s, y_s),$$

$$x_s^{-1}\cdot y_1 \equiv m_1 mod p$$

e

$$y_s^{-1}\cdot y_2 \equiv m_2 mod p.$$

2. Duda obtém $M = (m_1, m_2)$.

Exemplo 2.3.3. Alice e Duda escolhem a curva elíptica $C:\ y^2 = x^3 + 2x + 6$ sobre o corpo finito $\mathbb{Z}_7$ e $B = (2, 2)$.

Geração das chaves:

1. Duda escolhe $3 \in\ \mathbb{Z}$.

2. Duda Calcula $3\cdot (2, 2) = (4, 6)$ e publica.

Codificando a mensagem numérica $M = (2, 4)$:

1. Alice escolhe um inteiro 5.

2. Alice Calcula

$$y_0 = 5\cdot (2, 2) = (1, 4)$$

$$S = 5\cdot (4, 6) = (5, 6),$$

$$y_1 \equiv 5\cdot 2\ \equiv 3\, mod\, 7$$

e

$$y_2 \equiv 6\cdot 4 \equiv 24 \equiv 3\, mod\ 7.$$

3. Alice converte a mensagem $M = (2, 4)$ na tripla ordenada $((1, 4), 3, 3)$.

4. Alice envia $((1, 4), 3, 3)$.

Decifrando a mensagem:

1. Duda calcula

$$3 \cdot (1, 4) = 3 \cdot 5 \cdot (2, 2) = 5 \cdot (4, 6) = (5, 6)$$

$$\frac{1}{5} \cdot 3 \equiv 2 \, mod \, 7$$

e

$$\frac{1}{6} \cdot 3 \equiv 4 \, mod \, 7.$$

2. Duda obtém $M = (2, 4)$.

Capítulo 3

Algoritmos

No decorrer dos capítulos anteriores, apresentamos alguns sistemas criptográficos. Observando todos esses esquemas de criptografia, podemos observar uma característica comum, todos esses sistemas adotam uma sistematização de ações para encriptação e decriptação das mensagens. Por exemplos temos:

- Na cifra de Cesar, o autor da mensagem trocava cada letra do texto original pela terceira letra que segue, respectivamente, no alfabeto. O receptor da mensagem agia de modo inverso a ação do autor da mensagem.
- No esquema RSA, o receptor cria as chaves e divulga a chave de encriptação. O emissor da mensagem utiliza a chave de encriptação para codificar o texto. E posteriormente, receptor utiliza a chave privada e decodifica a mensagem.

Um conjunto finito de ações sistematizadas e definidas com a finalidade de solucionar um determinado problema, chamamos de algoritmo. Em outras palavras,

> Algoritmo é uma sequência de instruções finitas, que não podem ser ambíguas, com a finalidade de resolver algum problema. Cada instrução deve ser executada de maneira manual, mecânica ou eletrônica obedecendo um intervalo de tempo e uma quantidade de esforço ou processamento finito ([SANTOS 2020, p. 3]).

Segundo [CASTRO 2020, p. 16] o algoritmo é uma fórmula lógica utilizada para resolvermos situações da maneira mais automática possível, ou seja, com menos esforço, a partir de uma sequência de passos pré-estabelecidos.

Diariamente, empregamos algoritmos para resolvemos problemas em situações adversas, porém fazemos isso de maneira tão corriqueira que não percebemos. Como exemplos do uso de algoritmos no nosso dia a dia, temos: Receita de bolo, pilotar um carro, enviar uma mensagem por meios digitais, abrir uma porta, entre outras.

Na matemática não é diferente, constantemente empregamos os algoritmos para resolver diversas situações. Os algoritmos têm a propriedade de promover o desenvolvimento do raciocínio lógico e auxiliar na nossa capacidade de resolver problemas ([SANTOS 2020, p. 17]).

Conforme [CASTRO 2020],

> Para se ter noção, etimologicamente falando, o termo algoritmo por si só tem bastante ligação com a matemática. Tanto a palavra "algoritmo" quanto a palavra "algarismo" são palavras derivadas do mesmo radical algoritmi, que são heranças relacionadas ao nome do célebre matemático, astrônomo e geógrafo muçulmano Abu-Abdullah Muhammad Ibn Musa al-Khwarizmi (738-850 d.C) (algoritmi seria a forma latina do nome al-Khwarizmi), sendo esse considerado um dos pais do algoritmo (p.12).

Com a advento dos computadores e as máquinas digitais o uso de algoritmos tornou-se mais apreciável, pois um algoritmo bem projetado aliado um computador torna-se uma ferramenta potente.

De acordo com [CASTRO 2020] para a computação um algoritmo é

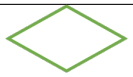
> qualquer procedimento computacional bem definido que toma algum valor ou conjunto de valores como entrada e produz algum valor ou conjunto de valores como saída. Portanto, um algoritmo é uma sequência de passos computacionais que transformam a entrada na saída. Também podemos visualizar um algoritmo como uma ferramenta para resolver um problema computacional bem especificado. O enunciado do problema especifica em termos gerais o relacionamento entre a entrada e a saída desejada. O algoritmo descreve um procedimento computacional específico para se alcançar esse relacionamento da entrada com a saída ([Cormen et al. 2002]).

Um algoritmo pode ser representado por meio de várias tipos linguagens, por exemplo temos a linguagem de programação Java, Python, C++, porém nesse trabalho vamos tratar apenas as linguagens: Fluxograma, Narrativa descritiva e o Pseudocódigo.

3.1 Fluxograma

O fluxograma é uma linguagem algorítmica que utiliza figuras geométricas para representar os comandos, definindo assim uma estrutura. Na linguagem fluxográfica, cada figura geométrica possui um significado.

Exemplo 3.1.1. Temos uma padronização de figuras geométricas na linguagem fluxográfica que representamos na tabela abaixo.

FIGURA GEOMÉTRICA	COMANDO
	Início e fim do algoritmo.
	Indica os dados de entrada.
	Processo a ser executado.
	Decisão.
	Declara os dados de saída.
	Indica a direção do próximo comando.

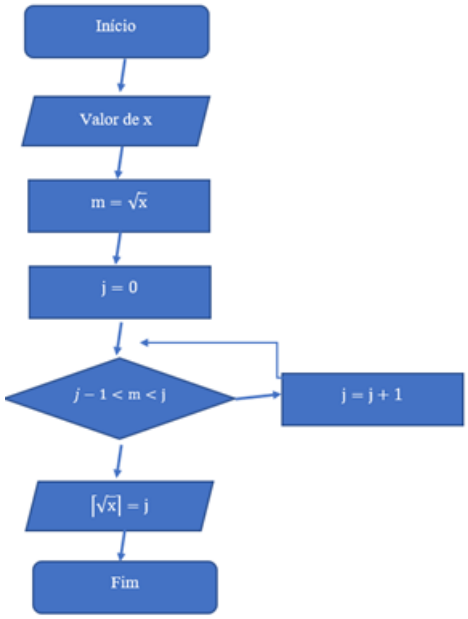
A padronização das formas geométricas utilizadas na construção do fluxograma para representar um algoritmo facilita a compreensão do mesmo de forma mais rápida do que outras linguagens algorítmicas. Para [WESLEY, GONDIM e AMBROSIO],

> O uso de fluxogramas se deve a três razões principais. Primeiro: fluxogramas possuem uma sintaxe mínima. Quando se reduz o foco em sintaxe, pode-se aumentar o esforço em análise. Segundo: fluxogramas é uma representação universal. Nenhum outro sistema visual alcançou a aceitação dos fluxogramas. Terceiro: fluxograma são mais fáceis para estudantes iniciantes em computação do que estrutura de código (p . 110).

Por outro lado, a representação por meio do fluxograma também possui desvantagens, como menciona [CASTRO 2020],

> Alguns problemas relacionados ao uso do fluxograma é a falta de detalhamento em quais variáveis são analisadas, além do que dependendo do tamanho ou complexidade do algoritmo o fluxograma crescer bastante, dificultando tanto a aplicação como até mesmo a construção (p. 17).

Exemplo 3.1.2. Vamos representar por meio do fluxograma a função Teto de $\sqrt{x}$. A função Teto, denotado por $\lceil x \rceil$, transforma o número real em um número inteiro maior ou igual que seja o mais próximo do número real dado.



No exemplo acima, o algoritmo funciona da seguinte maneira:

1. Declarar o número real x.
2. Calcular $\sqrt{x}$.
3. Considerar um número j igual a zero.
4. Analisar se $j - 1 < \sqrt{x} \leq j$.

- Se desigualdade for verdadeira, o resultado é número j.
- Caso contrário, soma uma unidade ao número j e analisar se $j < \sqrt{x} \leq j + 1$.
- Se $\sqrt{x}$ for maior que j e menor que $j + 1$, o resultado é o número $j + 1$.
- Caso contrário soma uma unidade ao número j, n vezes até que a desigualdade $j + (n - 1) < \sqrt{x} \leq j + n$ torne verdadeira,. Sendo assim o resultado em questão é $j + n$.

3.2 Narrativa Descritiva

A Narrativa descritiva é uma linguagem algoritma que utiliza da linguagem usual para descrever os comandos para desenvolver uma tarefa. Nessa linguagem não utiliza símbolos, figuras ou códigos para representar os comandos.

Exemplo 3.2.1. Vamos representar a função Teto de $\sqrt{x}$ por meio da narrativa descritiva.

Algoritmo: Algoritmo função Teto de $\sqrt{x}$.

1: Declarar o número real x.

2: Calcular o valor de $\sqrt{x}$.

3: Se o resultado de $\sqrt{x}$ for um número inteiro a resposta será o próprio valor.

4: Caso contrário, a resposta será o número inteiro maior mais próximo do valor de $\sqrt{x}$.

A representação do algoritmo com esse tipo de linguagem é construída com base na linguagem natural de cada indivíduo. Assim alguns autores alertam sobre possibilidades de más interpretações do algoritmo quando utlizadas por outros indivíduos.

3.3 Pseudocódigo

O pseudocódigo é uma linguagem algorítmica que mais aproxima da linguagem de programação, diferentemente do fluxograma que utiliza figuras geométricas para representar os comandos, o pseudocódigo é representado com base em normas de estrutura que fornece comandos para o desenvolvimento do algoritmo. A estrutura do pseudocódigo possibilita que os passos para o desdobramento do algoritmo sejam mais detalhados.

Podemos representar uma estrutura do pseudocódigo da seguinte forma:

Estrutura	Comando
Algoritmo:	Nome do algoritmo.
Entrada	Indica os dados de entrada do algoritmo.
Saída	Solução processado pelo algoritmo.
Início	Indica início do algoritmo.
Fim	Indica o término do algoritmo.
Corpo do algoritmo	São os passos para o desdobramento do algoritmo que são descritos entre os comandos "início" e "fim".

Exemplo 3.3.1. Vamos representar por meio do pseudocódigo a função Teto de $\sqrt{x}$.

Algoritmo: Algoritmo função Teto de $\sqrt{x}$.

Entrada: Número x.

Saída: $\lceil\sqrt{x}\rceil$

1: início

2: calcule $\sqrt{x}$

3: para $j \in \mathbb{Z}$

4: encontre $j-1 < \sqrt{x} \leq j$

5: retorne j

6: fim

3.4 Algoritmos para Solução do Problema do Logaritmo Discreto.

Nessa seção vamos citar alguns algoritmos para solução do logaritmo discreto. Segundo [MARQUES] uma abordagem intuitiva para a resolução deste problema é a busca exaustiva, que consiste em percorrer todo o conjunto G a procura do elemento x que satisfaça a relação $x = \log_b a$ (2007, p. 48).

Dado um grupo finito G, se adotamos a notação multiplicativa temos que $a^n = \underbrace{a \cdot a \cdot a \cdot ... \cdot a}_{n\, vezes}$, $n \in \mathbb{N}$,segue que $a^{-n} = \underbrace{(a^{-1}) \cdot (a^{-1}) \cdot ... \cdot (a^{-1})}_{n\, vezes}$. O problema do logaritmo discreto consiste em tenta resolver a equação $a^n = b$, com $a, b \in G$. Neste caso $n = log_a b$. Na notação aditiva temos $n \cdot a = \underbrace{a + a + a + ... + a}_{n\, vezes}$, segue que $na = b$, $n = log_a b$.

Os métodos criptográficos apresentados a seguir, são baseados na dificuldade de encontrar a solução do problema do logaritmo discreto tomando como referência o grupo $C(\mathbb{Z}_p)$ dos pontos de uma curva elíptica sobre $\mathbb{Z}_p$, com p primo. Vamos apresentar aqui alguns algoritimos que debruçam sobre a situação deste problema . Não nos ateremos a execução computacional de tais algoritmos.

O algoritmo de Shanks e o Método ρ de Pollard são os algoritmos que abordaremos para solucionar o problema do logaritmo discreto e como base teórica adotaremos [MARQUES].

3.4.1 Algoritmo de Shanks

O algoritmo de Shanks considera dois números inteiros i e j, tal que $i \in [0,\ m-1]$ e $j \in [0,\ m]$ com $m = \lceil\sqrt{n}\rceil$. Esse método busca construir dois conjuntos $S = \{(i, ab^{-i})\}$ e $T = \{(j, b^{mj})\}$, em seguida analisar os casos que $ab^{-i} = b^{mj}$ e obter i e j,

tal que $x = mj + i$. Podemos verificar a validez dessa solução uma vez que $x = \log_b a$, ou seja, $a = b^x = b^{mj+i} = b^{mj}b^i$. Portanto a solução do logaritmo é $a = b^x = b^{mj+i} = b^{mj}b^i$.

Algoritmo 1: Algoritmo de Shanks

Entrada: O elemento $a \in \langle b \rangle$, com $\#(\langle b \rangle) = n$ e $m = \lceil \sqrt{n} \rceil$

Saída: $x = \log_b a$, com $x \in [0,\ n-1]$

1: para i de 0 até $m-1$ faça

2: calcule ab^{-i}

3: fim para

4: Construa o conjunto S formado pelos pares ordenados (i, ab^{-i})

5: para j de 0 até $m-1$ faça

6: Calcule b^{mj}

7: fim para

8: Construa o conjunto T, formado pelos pares ordenados (j, b^{mj})

9: Encontre $(i, ab^{-i}) \in S$ e $(j, b^{mj}) \in T$, tais que $ab^{-i} = b^{mj}$ e destaque os inteiros i e j

10: retorne $mj + i$

Exemplo 3.4.1. Para a solução de $x = \log_3 47$ no grupo $\mathbb{Z}_{97}$, temos que $a = 47$, $b = 3$, $n = 97$ e $m = \lceil \sqrt{97} \rceil = 10$.

Calcule $47 \cdot 3$ para i de 0 até 9.

Observe que $3^{-1} \equiv 65\, mod\, 97$, logo basta calcular $47 \cdot 65^i$.

$S = \{(i,\ 47 \cdot 65^i)\}$

$S = \{(0,\ 47),\ (1,\ 48),\ (2,\ 16),\ (3,\ 70),\ (4,\ 88),\ (5,\ 94),\ (6,\ 96),\ (7,\ 32),\ (8,\ 43),\ (9,\ 79)\}$

Calcule 3^{10j} para j de 0 até 9.

Observe que $3^{10} \equiv 73\ mod\ 97$, logo basta calcular 73^j.

$T = \{j,\ 73^j)\}$

$T = \{(0,1),\ (1,\ 73),\ (2,91),\ (3,\ 47),\ (4,36),\ (5,9),\ (6,\ 75),(7,43),\ (8,35),\ (9,33)\}$

Temos que $(0, 47) \in S$ e $(3,\ 47) \in T$, logo $i = 0$ e $j = 3$.

Portanto, $\log_3 47\ mod\ 97 = (10 \cdot 3 + 0)\ mod\ 97 = 30$.

3.4.2 Método ρ de Pollard

O algoritmo ρ de Pollard foi proposto em 1974 pelo Matemático John M. Pollard. Segundo [DULLIUS 2001] a vantagem desde algoritmo sobre o Shanks, está no espaço que ocupa para o armazenamento dos dados durante o processamento.

O método de Pollard é aplicado a um grupo cíclico qualquer de ordem n. De modo que, dado G um grupo cíclico de ordem n, $b \in G$ um gerador de G e $a \in G$ é possível calcular o logaritmo discreto $x = \log_b a$ através da repartição de G em três partes: S_1, S_2 e S_3, tal que essas partes tenham aproximadamente os mesmos tamanhos e $1 \notin S_2$.

Para gerar os três conjuntos, vamos definir uma sequência x_i, com $x_0 = 1$ e $i \geq 0$, tal que

$$x_{i+1} = \begin{cases} ax_i, & para\ x_i \in S_1, \\ x_i^2, & para\ x_i \in S_2, \\ bx_i, & para\ x_i \in S_3. \end{cases} \tag{3.4.1}$$

A sequência x_i nada mais é do que uma representação de outras duas sequências $a_0,\ a_1,\ a_2, ...,$ e $b_0,\ b_1,\ b_2, ...,$ pois podemos desdobrar todos os x_i em termos de a_i e b_i obedecendo a relação $x_i = a^{a_i} b^{b_i}$ com $a_0 = b_0 = 0$.

Observe que:

Para $x_i \in S_1$ implica que $x_{i+1} = ax_i$, de acordo com a relação $x_i = a^{a_i} b^{b_i}$, temos que $a^{a_{i+1}} b^{b_{i+1}} = a\ a^{a_i} b^{b_i} = \ a^{a_i+1} b^{b_i}$. Daí que $a_{i+1} \equiv a_i + 1 mod\ n$ e $b_{i+1} \equiv b_i\ mod\ n$.

Para $x_i \in S_2$ implica que $x_{i+1} = x_i^2$, de acordo com a relação $x_i = a^{a_i} b^{b_i}$, temos que $a^{a_{i+1}} b^{b_{i+1}} = \left(a^{a_i} b^{b_i} \right)^2 = \ a^{2a_i} b^{2b_i}$. Daí que $a_{i+1} \equiv 2a_i mod\ n$ e $b_{i+1} \equiv 2b_i\ mod\ n$.

Para $x_i \in S_3$ implica que $x_{i+1} = bx_i$, de acordo com a relação $x_i = b^{a_i} b^{b_i}$, temos que $a^{a_{i+1}} b^{b_{i+1}} = b\ a^{a_i} b^{b_i} = \ a^{a_i} b^{b_i+1}$. Daí que $a_{i+1} \equiv a_i mod\ n$ e $b_{i+1} \equiv b_i + 1\ mod\ n$.

A partir dessas observações obtemos as sequências

$$a_{i+1} = \begin{cases} a_i + 1\ mod\, n, & para\ x_i \in S_1, \\ 2a_i\ mod\, n, & para\ x_i \in S_2, \\ a_i & para\ x_i \in S_3, \end{cases} \tag{3.4.2}$$

$$b_{i+1} = \begin{cases} b_i, & para\ x_i \in S_1, \\ 2b_i\ mod\, n, & para\ x_i \in S_2, \\ b_i + 1\ mod\, n, & para\ x_i \in S_3. \end{cases} \tag{3.4.3}$$

Para a sequência x_i definida acima, existe um inteiro $i \leq 3\sqrt{n}$ para a qual $x_i = x_{2i}$ ([DULLIUS 2001]). Dessa maneira, obtemos que

$$a^{a_i} b^{b_i} = \ a^{a_{2i}} b^{b_{2i}} \Rightarrow a^{a_i - a_{2i}} = b^{b_{2i} - b_i}$$

Daí

$$\log_b a^{a_i - a_{2i}} = \log_b b^{b_{2i} - b_i}$$

$$(a_i - a_{2i}) \log_b a = b_{2i} - b_i$$

$$\log_b a = \frac{b_{2i} - b_i}{a_i - a_{2i}}$$

Algoritmo 2: Algoritmo ρ de Pollard para o cálculo do logaritmo discreto.

Entrada: Um gerador b de um grupo cíclico de um grupo G de ordem prima n e um elemento $a \in G$.

Saída: O logaritmo discreto $x = \log_b a$

1: início

2: $x_0 \to 1$,$a_0 \to 0$, $b_0 \to 0$

3: para $i = 1, 2, ...$ faça

4: calcule x_i, a_i, b_i e x_{2i}, a_{2i}, b_{2i} utilizando as equações 3.4.1, 3.4.2 e 3.4.3, respectivamente

5: se $x_i = x_{2i}$ então

6: $r \leftarrow (a_i - a_{2i})\ mod\ n$

7: se $r = 0$ então

8: retorne "falha"

9: retorne $x = r^{-1}(b_{2i} - b_i)\ mod\, n$

10: fim se

11: fim para

12: fim

Exemplo 3.4.2. Seja G um grupo cíclico de ordem $n = 83$, e $b = 2$ um gerador de G e $a = 54$. Vamos calcular o logaritmo discreto $x = \log_2 54$.

Inicialmente iremos dividir o conjunto G em três partes: S_1, S_2 e S_3, tal que para todo $x \in G$ então $x \in S_1$ se $x \equiv 1\ mod\ 3$, $x \in S_2$ se $x \equiv 0\ mod\ 3$ e $x \in S_3$ se $x \equiv 2\ mod\ 3$ para todo $x \in G$.

Calculado x_i, a_i, b_i e x_{2i}, a_{2i} e b_{2i} com $x_0 = 1$,$a_0 = 0$, $b_0 = 0$, temos a tabela abaixo:

i	x_i	$x_i \in S_{j\in\{1,2,3\}}$	a_i	b_i	i	x_i	$x_i \in S_{j\in\{1,2,3\}}$	a_i	b_i
0	1	S_1	0	0	26	101	S_3	29	33
1	54	S_2	1	0	27	5	S_3	29	34
2	158	S_3	2	0	28	10	S_1	29	35
3	119	S_3	2	1	29	146	S_3	30	36
4	41	S_3	2	2	30	95	S_3	30	37
5	82	S_1	2	3	31	190	S_1	30	38
6	94	S_1	3	3	32	16	S_1	31	38
7	151	S_1	4	3	33	76	S_1	32	38
8	77	S_3	5	3	34	164	S_3	33	38
9	154	S_1	5	4	35	131	S_3	33	39
10	42	S_2	6	4	36	65	S_3	33	40
11	188	S_3	12	8	37	130	S_1	33	41
12	179	S_3	12	9	38	125	S_3	34	41
13	161	S_3	12	10	39	53	S_3	34	42
14	125	S_3	12	11	40	106	S_1	34	43
15	53	S_3	12	12	41	11	S_3	35	43
16	106	S_1	12	12	42	22	S_1	35	44
17	11	S_3	13	12	43	6	S_2	36	44
18	2	S_1	13	14	44	36	S_2	72	5
19	6	S_2	14	14	45	114	S_2	61	10
20	36	S_2	28	28	46	191	S_3	39	20
21	114	S_2	56	56	47	185	S_3	39	21
22	191	S_3	29	29	48	173	S_3	39	22
23	185	S_3	29	30	49	149	S_3	39	23
24	173	S_3	29	31	50	101	S_3	39	24
25	149	S_3	29	32	51	5	S_3	39	25

i	x_{2i}	a_{2i}	b_{2i}
0	1	0	0
1	158	2	0
2	41	2	2
3	94	3	3
4	77	5	3
5	42	6	4
6	179	12	9
7	125	12	11
8	106	12	13
9	22	13	14
10	36	28	28
11	191	29	29
12	173	29	3

i	x_{2i}	a_{2i}	b_{2i}
13	101	29	3
14	10	29	35
15	95	30	37
16	16	31	38
17	164	33	38
18	65	33	40
19	125	34	41
20	106	34	43
21	22	35	44
22	36	72	5
23	191	39	20
24	173	39	22
25	101	39	24

Observe nas tabelas acima que $x_{24} = x_{48} = 173$.

Calculando

$$r \equiv (29 - 39)\ mod\ 83$$

$$r \equiv 73\ mod\ 83$$

.

Temos que

$$x \equiv 58 \cdot (22 - 31)\ mod\ 83$$

$$x \equiv 59\ mod\ 83$$

Portanto, o logaritmo discreto $x = \log_2 54 = 59$.

Observe que na tabela a sequência $(x_i)_{i \in N}$ é periódica a partir de $i = 48$ com os valores repetindo, respectivamente para $i > 24$. Segundo [DULLIUS 2001], esse comportamento da sequência x_i fez com esse algoritmo ficasse conhecido como método ρ de Pollard, pois a parte não periódica da sequência aparenta uma cauda e a parte periódica um formato de um laço e daí que assemelha a letra do alfabeto grego ρ (Rho).

Capítulo 4

Aplicações do Tema no Ensino Básico

Nesse capítulo, vamos apresentar algumas atividades com curvas elípticas que podem ser aplicadas no Ensino Básico. As sugestões de atividades podem ser aplicadas em qualquer turma de Ensino Fundamental anos finais como no Ensino Médio, já que aborda habilidades que devem ser desenvolvidas nessas etapas. Contudo a nossa sugestão é para que essas atividades sejam aplicadas em turmas de 7º ano, já que as atividades contemplam mais habilidades a serem trabalhadas segundo a BNCC (Base Nacional Curricular Comum). As propostas de atividades podem ser trabalhadas separadamente ou de forma sequencial. Como recurso tecnológico para desenvolver as atividades escolhemos o software Geogebra por ser gratuito e pelas grandes contribuições no ensino-aprendizado da Matemática.

O Geogebra tem a característica de ser um software dinâmico e de fácil manuseio que contribui para que os alunos manipulem os objetos e construa conjecturas sobre determinados conteúdos matemáticos, possibilitando a produção de conhecimento de forma mais interativa e significativa. O software na sua interface possui a janela algébrica e a planilha gráfica que possibilita aos alunos visualizarem os objetos de diferentes maneiras facilitando a verificação de conceitos matemáticos. Para maiores informações sobre o software Geogebra indicamos o leitor acessar o site: www.geogebra.org. No site do software encontra-se disponível o aplicativo para download, manual e materiais didáticos de apoio, entre outros.

4.1 Atividade I

Série: 7º ano.

Área: Geometria

Conteúdos relacionados: Retas perpendiculares, ponto médio e simetria.

Habilidades de acordo com a BNCC: (EF07MA20) Reconhecer e representar, no plano cartesiano, o simétrico de figuras em relação aos eixos e à origem.

(EF07MA21) Reconhecer e construir figuras obtidas por simetrias de translação, rotação e reflexão, usando instrumentos de desenho ou softwares de geometria dinâmica e vincular esse estudo a representações planas de obras de arte, elementos arquitetônicos, entre outros.

Objetivo: Estudar a propriedade de simetria da curva elíptica.

Recursos necessários: Computador e software Geogebra.

Inicialmente, o professor deverá fazer uma breve apresentação da curva elíptica. Definição 2.5. Curvas elípticas sobre $\mathbb{R}$, é um conjunto dos pontos $(x, y) \in \mathbb{R}^2$ que satisfazem a equação $C: \ y^2 = x^3 + ax + b$, tal que $4a^3 + 27b^2 \neq 0$, com $a, \ b \ \in \mathbb{R}$ e unido a um ponto que chamamos de ponto do infinito, que representaremos pelo símbolo ∞. Em seguida, o professor dividirá os alunos em grupos (sugestão no máximo em trio), em seguida solicitará que acesse o geogebra e utilizando o software desenvolvam os seguintes passos.

Passo 1. Digite no campo de entrada do software a equação da curva elíptica $y^2 = x^3 - 2x + 1$.

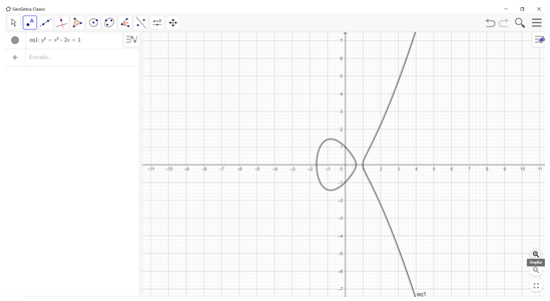


Figura 4.1.1: Atividade I: passo 1.

Passo 2. Na barra de ferramentas, utilize opção "ponto" e crie um ponto sobre a curva elíptica $y^2 = x^3 - 2x + 1$.

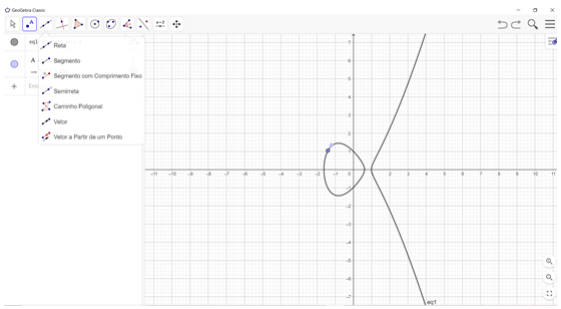


Figura 4.1.2: Atividade I: passo 2.

Passo 3. Na barra de ferramentas, utilize opção “reta perpendicular” e clique no eixo das abscissas e no ponto criado no passo anterior.

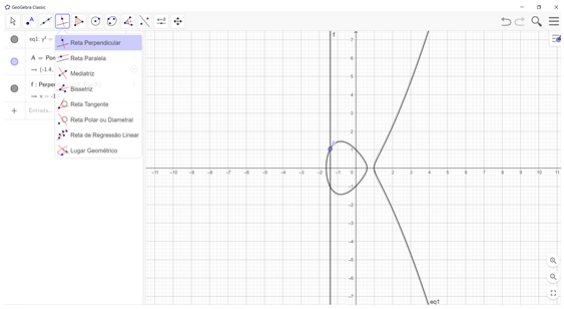


Figura 4.1.3: Atividade I: passo 3.

Passo 4. Na barra de ferramentas, utilize opção “interseção de dois objetos” e clique na curva $y^2 = x^3 - 2x + 1$ e na reta perpendicular.

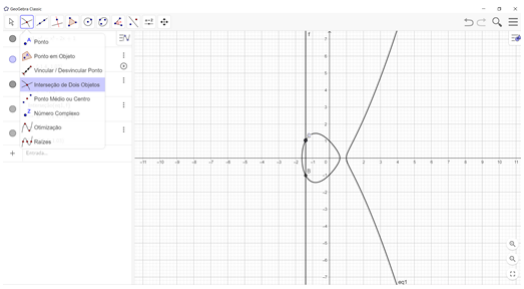


Figura 4.1.4: Atividade I: passo 4.

Passo 5. Na barra de ferramentas, utilize opção “interseção de dois objetos” e clique no eixo das abcissas e na reta perpendicular.

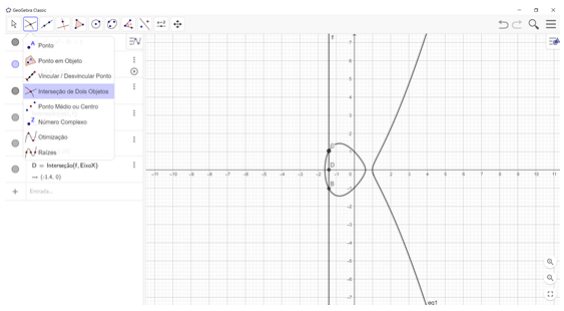


Figura 4.1.5: Atividade I: passo 5.

Passo 6. Na barra de ferramentas, utilize opção “distância” e clique em um dos pontos da curva e no ponto de interseção da reta perpendicular com o eixo das abcissas, em seguida realize o mesmo procedimento com o outro ponto da curva.

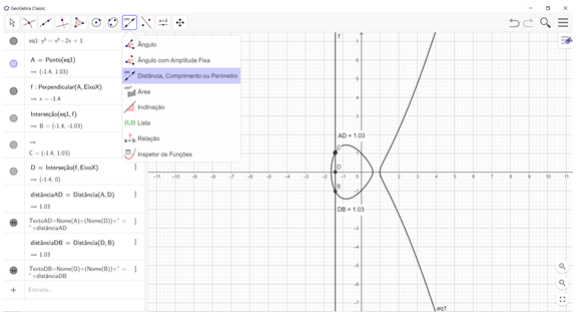


Figura 4.1.6: Atividade I: passo 6.

Passo 7. Na barra de ferramentas, utilize opção “mover” e clique em um dos pontos da interseção da reta perpendicular com a curva elíptica e mova o ponto.

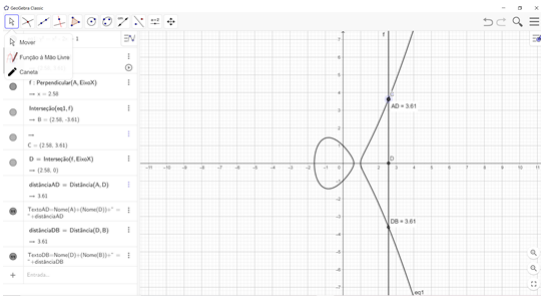


Figura 4.1.7: Atividade I: passo 7.

Após os alunos realizar os todos os passos, o professor deve orientar os alunos a continuar movendo um dos pontos de interseção da reta perpendicular com a curva elíptica e observarem as coordenadas dos pontos da interseção da curva e reta perpendicular e a distância desses pontos da curva e o ponto de interseção da reta perpendicular com o eixo das abcissas.

O professor deverá instigar os alunos a deduzir que a curva elíptica é simétrica em relação ao eixo das abcissas. O professor pode relacionar a simetria ao formato da equação e fazer alguns questionamentos: Se a equação fosse $y^2 + ay = x^3 + bx + c$ o gráfico seria simétrica? Qual é o eixo de simetria? o professor pode apresentar outros tipos de equação e solicitar aos alunos que plotem no geogebra os gráficos das equações apresentadas para que os mesmos visualizem.

4.2 Atividade II

Série: 7º ano.

Área: Geometria

Conteúdos relacionados: Usar a simetria, retas tangentes e secantes para definir operações entre os pontos de uma curva elíptica.

Habilidades: (EF07MA20) Reconhecer e representar, no plano cartesiano, o simétrico de figuras em relação aos eixos e à origem.

(EF07MA21) Reconhecer e construir figuras obtidas por simetrias de translação, rotação e reflexão, usando instrumentos de desenho ou softwares de geometria dinâmica e vincular esse estudo a representações planas de obras de arte, elementos arquitetônicos, entre outros.

Objetivos: Estudar a soma entre dois pontos na curva elíptica.

Recursos necessários: Computador e software Geogebra.

Desenvolvimento: Inicialmente, o professor dividirá os alunos em grupos, em seguida solicitará que os alunos acessem o Geogebra. Contudo, antes de iniciar a construção, o professor deve explicar que uma das propriedades das curvas elípticas é que podemos definir uma soma entre dois pontos quaisquer da curva que resulta em outro ponto que também está contido na mesma curva. Assim, podemos definir a operação de soma entre pontos de uma curva elíptica, por meio de retas tangentes e secantes. Desse modo, para determinar a soma de dois pontos A e B da curva elíptica, devemos traçar uma reta que passe por estes dois pontos. Esta reta que contém os pontos A e B interceptará a curva em um terceiro ponto E. A reflexão do ponto E em relação ao eixo das abcissas é ponto que representa a soma dos pontos A e B. É importante que o professor ressalte que o ponto do infinito ∞ é o elemento neutro na operação, ou seja, $A + \infty = A = \infty + A$ e este representa o terceiro ponto de interseção quando este não é visível.

Finalizada a explicação, os alunos deverão começar a construção sob orientação do professor.

Passo 1. Digite a equação $y^2 = x^3 - 2x + 1$ no campo de entrada.

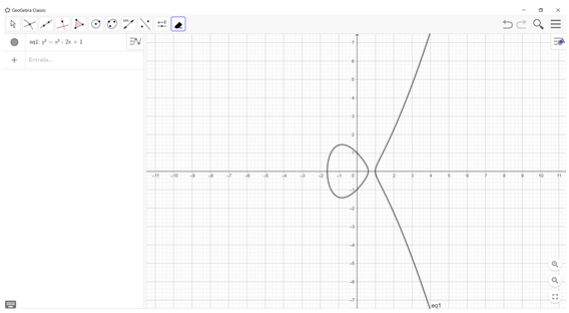


Figura 4.2.1: Atividade II: passo 1.

Passo 2. Na barra de ferramentas, utilize opção “ponto” e crie dois pontos sobre a curva elíptica $y^2 = x^3 - 2x + 1$.

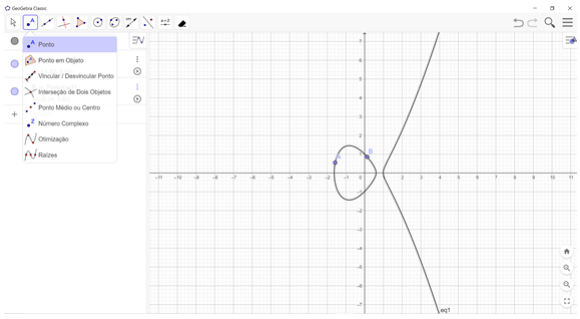


Figura 4.2.2: Atividade II: passo 2.

Passo 3. Na barra de ferramentas, utilize opção "Reta" e clique no ponto A e no ponto B.

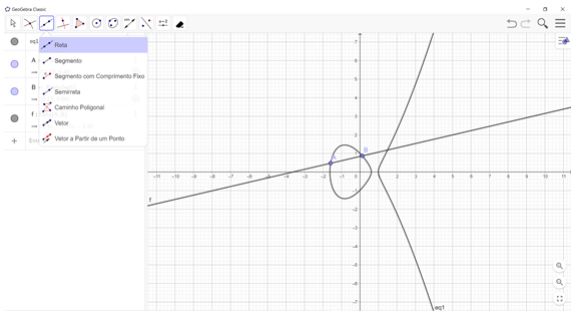


Figura 4.2.3: Atividade II: passo 3.

Passo 4. Na barra de ferramentas, utilize opção "interseção de dois objetos" e clique na curva $y^2 = x^3 - 2x + 1$ e na reta.

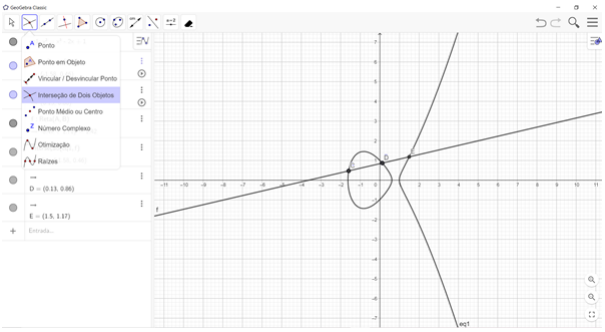


Figura 4.2.4: Atividade II: passo 4.

Passo 5. Na área algébrica, clique nos pontos C e D para ocultar os pontos.

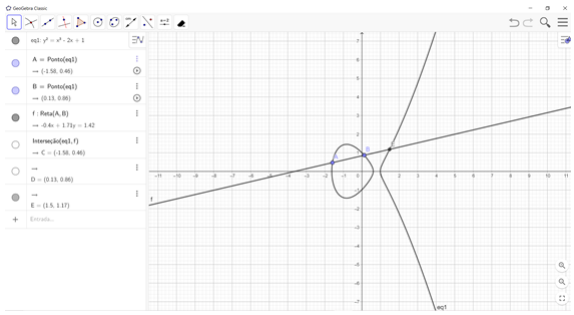


Figura 4.2.5: Atividade II: passo 5.

Passo 6. Na barra de ferramentas, utilize opção “reflexão em relação a uma reta” e clique no ponto E e no eixo das abcissas.

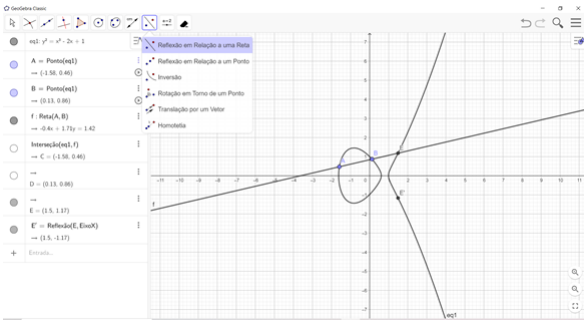


Figura 4.2.6: Atividade II: passo 6.

Passo 7. Na barra de ferramentas, utilize opção “mover” e clique em um dos pontos A ou B e mova o ponto.

Nesse momento, o professor pode solicitar aos alunos que posicione os pontos A e B, tal que $A \neq B$ e o ponto B não seja reflexão do ponto A e conduzir os alunos a perceberem que o ponto E' representa a soma dos pontos A e B, ou seja, $A + B = E'$.

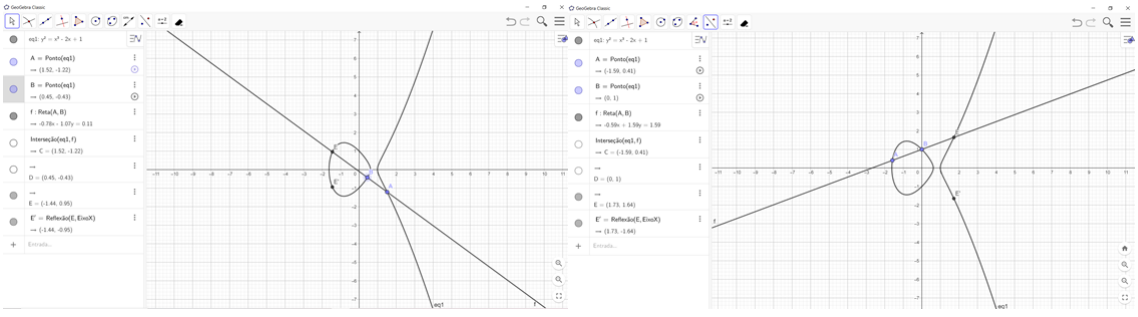


Figura 4.2.7: Atividade II: passo 7.1.

Em seguida, o professor pode pedir para os alunos posicionem o ponto A sobre o ponto B. Assim, os pontos A e B são iguais e E' representa a soma de pontos iguais, ou seja $A + A = E'$.

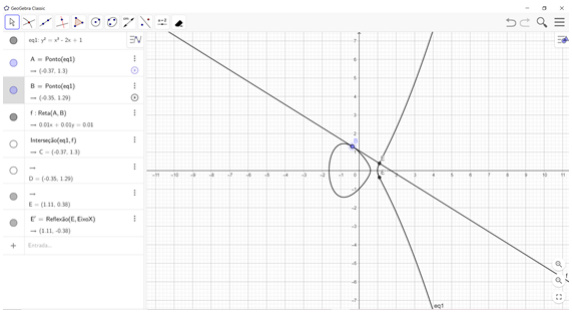


Figura 4.2.8: Atividade II: passo 7.2.

Agora o professor deverá pedir aos alunos que posicione o ponto A sobre o eixo das abcissas e mova o ponto B em direção ao ponto A e observem as coordenadas do ponto E'.

O professor deve instigar os alunos a concluir que a medida que o ponto B se aproxima do ponto A as coordenadas y do ponto E' tornam cada vez maiores, isto é, os valores das coordenadas y tendem para o infinito e quando os pontos A e B estão sobrepostos o software representa as coordenadas y do ponto E' na forma $(?, ?)$. Posteriormente, o professor deve explicar que denominamos esse ponto como o ponto do infinito ∞ e representamos o mesmo como a soma dos pontos A e B, sendo $A = B$ e B igual o simétrico de A em relação ao eixo das abcissas, ou seja, a soma do ponto A e do simétrico de A é representado pelo ponto do infinito ∞.

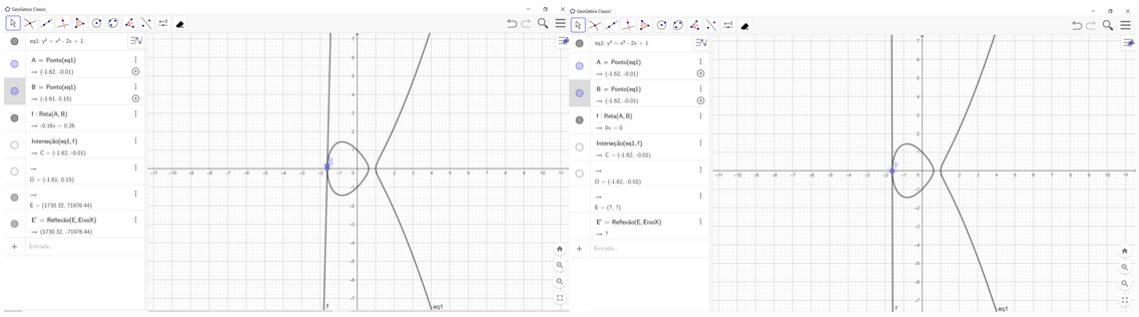


Figura 4.2.9: Atividade II: passo 7.3.

Nesse momento, o professor orientará os alunos mover o ponto B em direção ao simétrico do ponto A, sendo o ponto A diferente do seu simétrico e observem as coordenadas do ponto E' à medida que o ponto B se próxima do simétrico de A. Como observado anteriormente, as coordenadas do ponto E' torna imenso. Da mesma forma, representamos o ponto do infinito ∞ como a soma do ponto A com o seu simétrico em relação ao eixo das abcissas.

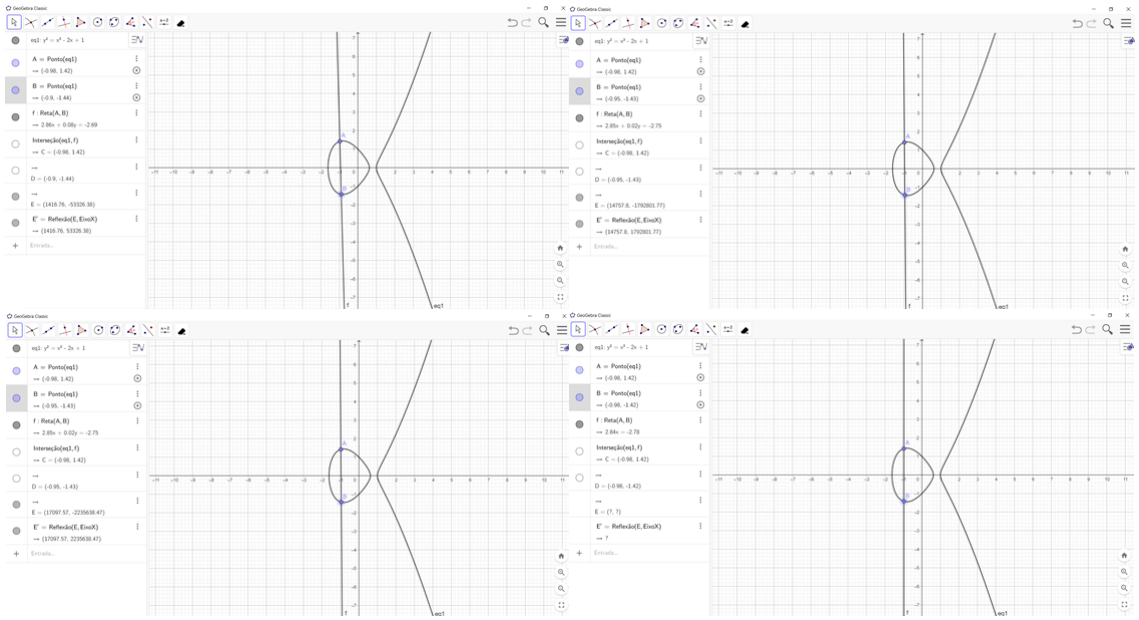


Figura 4.2.10: Atividade II: passo 7.4.

4.3 Atividade III

Série: 7º ano.

Área: Geometria

Conteúdo relacionado: Simetria por reflexão.

Habilidades: (EF07MA20) Reconhecer e representar, no plano cartesiano, o simétrico de figuras em relação aos eixos e à origem.

(EF07MA21) Reconhecer e construir figuras obtidas por simetrias de translação, rotação e reflexão, usando instrumentos de desenho ou softwares de geometria dinâmica e vincular esse estudo a representações planas de obras de arte, elementos arquitetônicos, entre outros.

(EF07MA05) Resolver um mesmo problema utilizando diferentes algoritmos.

Objetivos: Estudar a soma entre pontos na curva elíptica.

Recursos necessários: Computador e software Geogebra.

Desenvolvimento: Inicialmente, o professor dividirá os alunos em grupos, em seguida solicitará que os alunos acessem o geogebra e com o uso do software desenvolvam os seguintes passos.

Passo 1. Digite a equação $y^2 = x^3 - 2x + 1$ no campo de entrada.

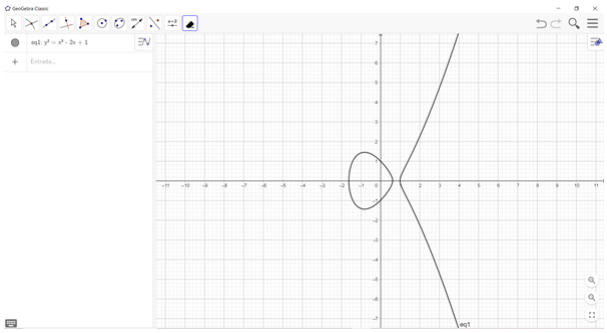


Figura 4.3.1: Atividade III: passo 1.

Passo 2. Na barra de ferramentas, utilize a opção "ponto" e crie um ponto sobre a curva elíptica $y^2 = x^3 - 2x + 1$. Depois, renomeie o ponto de E.

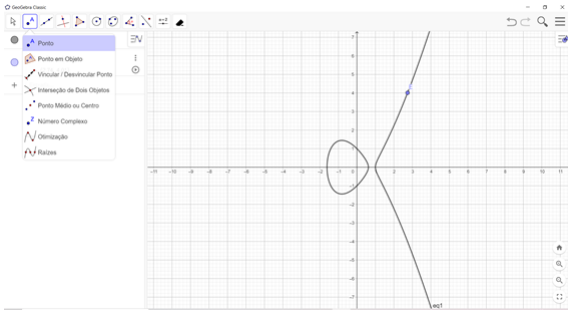


Figura 4.3.2: Atividade III: passo 2.

Passo 3. Na barra de ferramentas, utilize opção "reflexão em relação a uma reta" e clique no ponto E e no eixo das abcissas.

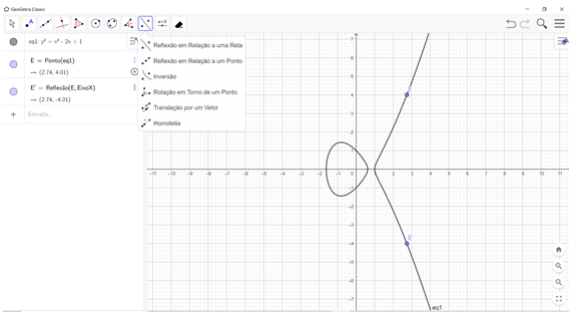


Figura 4.3.3: Atividade III: passo 3.

Passo 4. Na barra de ferramentas, utilize opção "reta" e clique no ponto E e na curva $y^2 = x^3 - 2x + 1$.

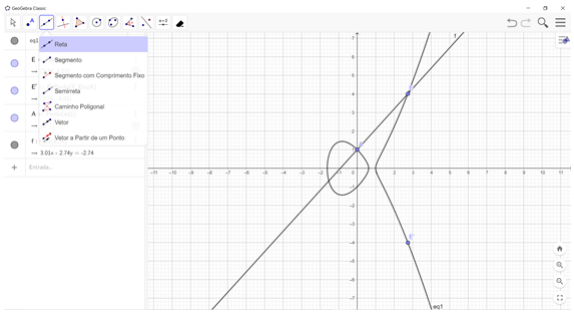


Figura 4.3.4: Atividade III: passo 4.

Passo 5. Na barra de ferramentas, utilize opção "interseção de dois objetos" e clique na reta e na curva $y^2 = x^3 - 2x + 1$. Em seguida, renomeie o ponto D de B e oculte os pontos C e B_1.

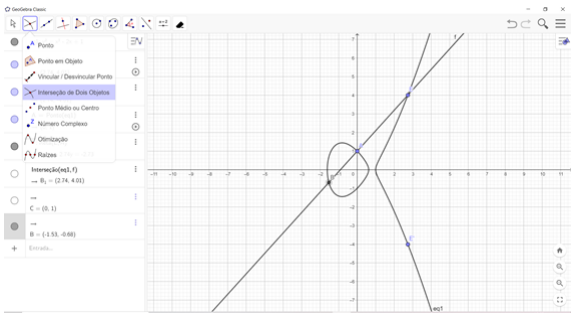


Figura 4.3.5: Atividade III: passo 5.

Passo 6. Na barra de ferramentas, utilize opção "mover" e clique no ponto A e mova o ponto.

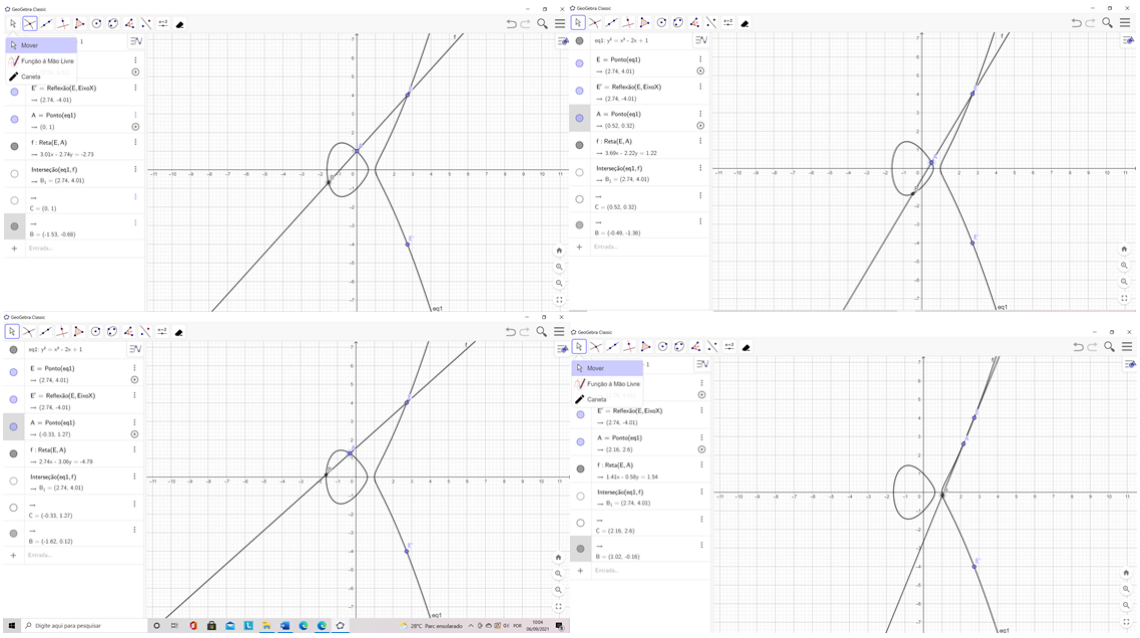


Figura 4.3.6: Atividade III: passo 6.

O professor solicitará aos alunos que observem as coordenadas dos pontos A e B à medida que o ponto A desloca. O professor deve questionar aos alunos o que acontece com as coordenadas dos pontos A e B e qual a relação com o ponto E'. Dessa forma, o mesmo deve instigar os alunos a concluir que existe diversos pares de pontos da curva elíptica que a soma é o ponto E'. Além disso, o professor pode complementar que a criptografia sobre curvas elípticas baseia na dificuldade de encontrar os pontos A e B dado um ponto E'.

O professor pode ressaltar que essa dificuldade aumenta quando trabalhamos com curvas elípticas sobre corpos finitos $\mathbb{Z}_p$ e quando escolhemos p um número primo com dezenas de algarismos.

4.4 Atividade IV

Série: 7º ano.

Área: Geometria.

Conteúdos relacionados: Operações com números inteiros.

Habilidades: (EF07MA05) Resolver um mesmo problema utilizando diferentes algoritmos.

(EF07MA04) Resolver e elaborar problemas que envolvam operações com números inteiros.

(EF07MA07) Representar por meio de um fluxograma os passos utilizados para resolver um grupo de problemas.

Objetivos: Estudar criptografia via curvas elípticas.

Recursos necessários: Material contendo as curvas elípticas e as tabelas com as somas dos pontos das curvas elípticas.

Desenvolvimento: Inicialmente, o professor dividirá os alunos em dupla e distribuirá o material contendo algumas curvas elípticas e suas tabelas operatórias.

Em seguida, solicitará as duplas que:

1. Cada dupla escolha uma curva elíptica C e um ponto $P \in C$ e divulgue aos demais colegas.

2. O aluno 1 de cada dupla deve escolher $a \in \mathbb{Z}$ e manter em segredo.

3. O aluno 2 de cada dupla deve escolher $b \in \mathbb{Z}$ e manter em segredo.

4. A partir da tabela o aluno 1 calcula aP e torna público.

5. A partir da tabela o aluno 2 calcula bP e torna público.

6. O aluno 1 multiplica bP por a e encontra $K = abP$.

7. O aluno 2 multiplica aP por b e encontra $K = abP$.

Após as duplas encerrarem os passos solicitados, o professor deverá instigar os alunos a reconhecer que a curva elíptica e o ponto P são as chaves públicas e ponto K encontrado por cada aluno é a chave privada.

Depois o professor solicitará que cada dupla escolha as informações públicas de outra dupla e tentem desvendar sua chave privada compartilhada.

Para finalizar, o professor deve solicitar aos alunos que esquematizem os passos desta tentativa de descobrir a chave privada dos colegas.

O professor deverá ressaltar que quanto mais pontos mais difícil é essa descoberta. Na prática o primo escolhido é muito grande.

Observação. Segue abaixo, algumas sugestões de tabelas operatórias.

$\oplus$	∞	(0,0)	(2,3)	(2,4)	(3,2)	(3,5)	(6,3)	(6,4)
∞	∞	(0,0)	(2,3)	(2,4)	(3,2)	(3,5)	(6,3)	(6,4)
(0,0)	(0,0)	∞	(2,4)	(2,3)	(6,3)	(6,4)	(3,2)	(3,5)
(2,3)	(2,3)	(2,4)	(0,0)	∞	(3,5)	(6,3)	(6,4)	∞
(2,4)	(2,4)	(2,3)	∞	(0,0)	(6,4)	(3,2)	(3,5)	(6,3)
(3,2)	(3,2)	(6,3)	(3,5)	(6,4)	(2,4)	∞	(2,3)	(0,0)
(3,5)	(3,5)	(6,4)	(6,3)	(3,2)	∞	(2,3)	(0,0)	(2,4)
(6,3)	(6,3)	(3,2)	(6,4)	(3,5)	(2,3)	(0,0)	(2,4)	∞
(6,4)	(6,4)	(3,5)	(3,2)	(6,3)	(0,0)	(2,4)	∞	(2,3)

Tabela 4.4.1: Soma dos pontos da curva elíptica $\mathcal{C}(\mathbb{Z}_7) : y^2 = x^3 - 3x$

$\oplus$	∞	(2,0)	(3,2)	(3,3)	(4,1)	(4,4)
∞	∞	(2,0)	(3,2)	(3,3)	(4,1)	(4,4)
(2,0)	(2,0)	∞	(4,1)	(4,4)	(3,2)	(3,3)
(3,2)	(3,2)	(4,1)	(3,3)	∞	(4,4)	(2,0)
(3,3)	(3,3)	(4,4)	∞	(3,2)	(2,0)	(4,1)
(4,1)	(4,1)	(3,2)	(4,4)	(2,0)	(3,3)	∞
(4,4)	(4,4)	(3,3)	(2,0)	(4,1)	∞	(3,2)

Tabela 4.4.2: Soma dos pontos da curva elíptica $\mathcal{C}(\mathbb{Z}_5) : y^2 = x^3 - 5x + 2$

$\oplus$	∞	(1,1)	(1,4)	(2,1)	(2,4)
∞	∞	(1,1)	(1,4)	(2,1)	(2,4)
(1,1)	(1,1)	(2,1)	∞	(2,4)	(1,4)
(1,4)	(1,4)	∞	(2,4)	(1,1)	(2,1)
(2,1)	(2,1)	(2,4)	(1,1)	(1,4)	∞
(2,4)	(2,4)	(1,4)	(2,1)	∞	(1,1)

Tabela 4.4.3: Soma dos pontos da curva elíptica $\mathcal{C}(\mathbb{Z}_5) : y^2 = x^3 - 2x + 2$

Capítulo 5

Considerações finais

A importância da criptografia é notável na sociedade, porém é um tema que ainda não faz parte da grade curricular na Educação Básica, apesar disso alguns livros didáticos do Ensino Médio abordam sucintamente esse tema em projetos.

Trabalhar com a criptografia em sala de aula é estimular os educandos a investigação e a desenvolver o pensamento algébrico, aritmético e o raciocínio lógico, ao mesmo tempo em que estamos apresentando aplicações que fazem parte da realidade dos mesmos. Nessa perspectiva, esse tema está diretamente interligado as competências propostas pela BNCC, uma vez que esse documento normativo ressalta que o ensino da matemática deve desenvolver potencialidades e orienta que esse componente curricular deve ser trabalhado como uma ciência humana que surgiu a partir das necessidades humanas ao longo da história em diferentes culturas.

Visto que a criptografia está atrelada com as relações comerciais e também comunicações sociais garantindo a integridade da informação, ao sigilo das operações comerciais e plataformas digitais de interatividade, estudar esse tema pode proporcionar aos nossos alunos compreender melhor os avanços tecnológicos no mundo contemporâneo, o que pode contribuir para um maior conhecimento envolvendo as tecnologias digitais além de uma melhor formação humana e cidadã.

Referências Bibliográficas

[CASTRO 2020]CASTRO, S. A. D. *Algoritmo e Pensamento Computacional como Ferramenta no Processo de Ensino-Aprendizagem*. Dissertação (Mestrado), 2020.

[Cormen et al. 2002]CORMEN, T. H. et al. Algoritmos: teoria e prática. *Editora Campus*, v. 2, p. 296, 2002.

[DOMINGUES e IEZZI 2003]DOMINGUES, H. H.; IEZZI, G. *Álgebra Moderna*. [S.l.]: Atual, 2003.

[DULLIUS 2001]DULLIUS, M. M. O problema do logaritmo discreto. 2001.

[FERREIRA 2019]FERREIRA, A. C. S. *Criptografia de chave pública-privada: RSA e curvas elípticas*. Tese (Doutorado), 2019.

[FIARRESGA 2010]FIARRESGA, V. M. C. *Criptografia e Matemática*. Tese (Doutorado), 2010.

[HEFEZ 2016]HEFEZ, A. *Aritmética*. [S.l.]: SBM, 2016.

[KOBLITZ 1998]KOBLITZ, N. *Algebraic Aspects of Cryptography*. [S.l.]: Springer-Verlag, 1998.

[LUIZ 2021]LUIZ, B. S. N. Um estudo exploratório envolvendo criptografia e noções de computação quântica. Universidade Federal de São Carlos, 2021.

[MARQUES]MARQUES, L. G. Curvas elıpticas: Aplicaç oes criptograficas.

[PAIXÃO 2020]PAIXÃO, J. S. d. *Criptografia: história, atividades e divulgação*. Dissertação (Mestrado), 2020.

[PRIETO 2020]PRIETO, M. J. *Historia de la criptografia*: Cifras, códigos y secretos, de la antigua grecia a la guerra fría. [S.l.]: La Esfera de los Libros, 2020.

[RORRES 2001]RORRES, A. *Álgebra Linear com aplicações*. [S.l.]: Porto Alegre, Rio Grande do Sul: Bookman, 2001.

[SANTOS 2015]SANTOS, D. T. *O Uso de Algoritmos e Programação no Ensino de Matemática*. Dissertação (Mestrado), 2015.

[SANTOS 2020]SANTOS, N. S. *Alguns Algoritmos em Java para Matemática Basica*. Dissertação (Mestrado), 2020.

[SILVERMAN 1986]SILVERMAN, J. H. *The Arithmetic of Elliptic Curves*. [S.l.]: New York, EUA, 1986.

[WESLEY, GONDIM e AMBROSIO]WESLEY, H.; GONDIM, A.; AMBROSIO, A. Esboços de fluxogramas no ensino de algoritmos. In: *Workshop sobre Educação em Computação–WEI. Anais do XXVIII Congresso da Sociedade Brasileira de Computação. Belém do Pará, PA, Brasil*. [S.l.: s.n.]. v. 12.

Universidade Federal do Recôncavo da Bahia - UFRB
Centro de Ciências Exatas e Tecnológicas / Mestrado Profissional em Matemática em Rede Nacional

Rua Rui Barbosa, s/n, Campus Universitário de Cruz das Almas - BA
CEP: 44380 -000
<http://www.ufrb.edu.br/profmat>
<http://www.profmat-sbm.org.br>