Universidade Federal de Juiz de Fora

Instituto de Ciências Exatas

PROFMAT - Mestrado Profissional em Matemática em Rede Nacional

Maria Cristina Antunes Lana

Curvas Elípticas e Criptografia

Juiz de Fora

2016

Maria Cristina Antunes Lana

Curvas Elípticas e Criptografia

Dissertação apresentada ao PROFMAT (Mestrado Profissional em Matemática em Rede Nacional) na Universidade Federal de Juiz de Fora, na área de concentração em Ensino de Matemática, como requisito para obtenção do título de Mestre em Matemática

Orientador: Sérgio Guilherme de Assis Vasconcelos

Juiz de Fora

2016

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF
com os dados fornecidos pelo(a) autor(a)

Lana, Maria Cristina Antunes.
Curvas Elípticas e Criptografia / Maria Cristina Antunes Lana. – 2016.
43 f. : il.

Orientador: Sérgio Guilherme de Assis Vasconcelos
Dissertação (Mestrado Profissional) – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. PROFMAT - Mestrado Profissional em Matemática em Rede Nacional, 2016.

1. Ensino Médio. 2. Criptografia. 3. Curvas Elípticas. I. Vasconcelos, Sérgio Guilherme de Assis, orient. II Título.

Maria Cristina Antunes Lana

Curvas Elípticas e Criptografia

Dissertação apresentada ao PROFMAT (Mestrado Profissional em Matemática em Rede Nacional) na Universidade Federal de Juiz de Fora, na área de concentração em Ensino de Matemática, como requisito para obtenção do título de Mestre em Matemática

Aprovada em: 25 de agosto de 2016

BANCA EXAMINADORA

Prof. Dr. Sérgio Guilherme de Assis Vasconcelos
Orientador Universidade Federal de Juiz de Fora

Professor Dr. Luís Fernando Crocco Afonso
Universidade Federal de Juiz de Fora

Professor Dr. Rônei Sandro Vieira
Centro Federal de Educação Tecnológica de Minas Gerais

Dedico este trabalho aos meus alunos estudantes de escola pública, merecedores de uma educação de melhor qualidade.

AGRADECIMENTOS

A Deus, acima de tudo, por ter permitido a realização desse grande sonho.

Aos professores do curso, em particular ao professor Sérgio Guilherme de Assis Vasconcelos meu orientador, pela paciência e dedicação em me auxiliar nesse trabalho.

Agradeço aos colegas de curso, em especial ao amigo Santi Singulani, companheiro de viagem, por tornar meus sábados mais felizes, (rimos muito e por vezes choramos também nesses dois anos), e à amiga Juliana Athouguia que sempre se esforçou em ajudar a todos de nossa turma.

Agradeço à CAPES pela grande ajuda, com o incentivo financeiro dado durante todo o curso.

A minha família, pelo apoio; e aos meus sogros Antônio e Francisca, por cuidarem da minha pequena Elisa, meu maior bem, me deixando tranquila, sabendo que ela estava em boas mãos.

Por fim, agradeço ao meu marido e companheiro de todas as horas, Marconi, pelo apoio e paciência nas diversas vezes em que não pudemos estar juntos em função das muitas horas dedicadas ao estudo.

Por que nos torna tão pouco felizes esta maravilhosa ciência aplicada, que economiza trabalho e torna a vida mais fácil? A resposta é simples: porque ainda não aprendemos a nos servir dela com bom senso.

Einstein (1879-1955)

RESUMO

Este trabalho tem como objetivo apresentar aos alunos do 3º ano do ensino médio, uma aplicação da matemática à criptografia através de curvas elípticas, com o intuito de reforçar alguns conteúdos já estudados tais como: funções, construção de gráficos, polinômios e equações algébricas, geometria analítica. Criptografia é um tema atual e de grande relevância, visto que é amplamente utilizada na web para: segurança ao autenticar os usuários ao lhes fornecer acesso, na proteção de transações financeiras e em redes de comunicação. Acreditamos que, ao introduzir o conceito de criptografia através de curvas elípticas de maneira simples e intuitiva, os alunos se sentirão entusiasmados ao perceber que a matemática estudada por eles é de grande importância para a aplicação em fenômenos próximos a eles no dia a dia.

Palavras-chave: Ensino Médio. Criptografia. Curvas Elípticas.

ABSTRACT

This paper aims to introduce students to the 3rd year of high school, a math application to encryption using elliptic curves, for the purpose of increasing some studies such as: functions, graphics constructions, polynomials and algebraic equations, analytical geometry. Encryption is a current topic of great importance, since it is widely used on the web for: security by identifying users by providing them access, financial transactions protection and network communication. We believe that through introducing the concept of encryption using elliptic curves in a simple and intuitive way, the students feel excited to realize that mathematics studied by them is a great importance to the application in situations near them on a daily basis.

Keywords: High School. Encryption. Elliptic Curves.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Este trabalho tem como objetivo apresentar a alunos que cursam o ano final do ensino médio, como motivação para revisar temas do ensino médio, um assunto raras vezes trabalhado na educação básica: criptografia via curvas elípticas. Apresentaremos noções básicas sobre criptografia através de curvas elípticas, de forma simples e intuitiva, mostrando a esses alunos mais uma área em que são aplicados os conhecimentos em matemática. A partir disso, cada aluno tem a possibilidade de aprofundar seus conhecimentos, de acordo com o seu interesse.

No capítulo 2, apresentaremos um breve histórico e as motivações para os estudos da criptografia.

No capítulo 3, exemplificamos a construção de gráficos de curvas elípticas utilizando conhecimentos prévios sobre funções tais como, intersecção com os eixos x e y, estudo do sinal e domínio. Trataremos também da soma dos pontos em uma curva elíptica e suas propriedades.

No capítulo 4, apresentaremos noções básicas de congruência, e suas propriedades, visto que a criptografia através de curvas elípticas é aplicada sobre corpos finitos. Por fim veremos a soma de pontos em curvas elípticas sobre Z_p.

Finalmente no capítulo 5, apresentaremos um exemplo de criptografia. Primeiramente, esboçando a ideia geral de como é feita a codificação e decodificação de uma mensagem e, em seguida, a apresentação de um exemplo resolvido.

2 CRIPTOGRAFIA

2.1 UMA POUCO DE HISTÓRIA

A criptografia, ao contrário do que muitos pensam, não é um recurso que passou a ser usado recentemente mas, segundo a história, vem se aprimorando desde épocas clássicas, como no uso de hieróglifos, onde era necessário uma interpretação para entender a mensagem, até os dias de hoje. A criptografia é a arte de cifrar/codificar uma mensagem como mecanismo de segurança. A história da criptografia começa há milhares de anos, com os Hebreus a 600 a.C., por meio de cifras de substituição monoalfabéticas (onde um símbolo do alfabeto é substituído por outro símbolo no alfabeto cifrado). Até o início da primeira guerra mundial nada de inovador havia sido desenvolvido no campo de criptografia, até que Alexander's Weekly escreveu um ensaio sobre métodos de criptografia, que se tornou útil como uma introdução para os criptoanalistas britânicos na quebra dos códigos e cifras alemães durante a I Guerra Mundial.

Figura 1 – Militares criptografando/descriptografando mensagens.

Fonte: História da computação. Disponível em:<http://www.dsc.ufcg.edu.br>

Durante a segunda guerra mundial, os alemães usaram uma máquina eletromecânica para criptografar e descriptografar, denominada de Enigma. Logo após o estopim da segunda guerra mundial, um grupo de criptógrafos britânicos (alguns matemáticos e mestres em xadrez) conseguiu quebrar as cifras da Enigma e decifrar mensagens secretas dos nazistas. Os militares alemães implantaram máquinas usando one-time pad (cifra de

chave única), um algoritmo de criptografia, em que o texto é combinado com uma chave aleatória; enquanto isso, os ingleses criaram o primeiro computador digital programável, o Colossus. Durante a chamada "Guerra Fria", entre Estados Unidos e União Soviética, foram criados e utilizados diversos métodos para esconder mensagens com estratégias e operações. Desses esforços, surgiram outros tipos de criptografia, tais como: por chave simétrica, onde existe uma chave com um segredo e essa chave é compartilhada pelos interlocutores; por chave assimétrica, onde existem 2 chaves, uma pública e uma privada. Essas chaves são geradas simultaneamente e são relacionadas entre si, o que possibilita que a operação executada por uma seja revertida pela outra. A chave privada deve ser mantida em sigilo e protegida por quem gerou as chaves. A chave pública é disponibilizada e tornada acessível a qualquer indivíduo que deseje se comunicar com o proprietário da chave privada correspondente, permitindo garantir tanto a confidencialidade quanto a autenticidade das informações por eles protegidas.

Figura 2 – Criptografia por chave assimétrica.

Fonte: História da computação. Disponível em:<http://www.dsc.ufcg.edu.br>

Atualmente, a criptografia é comumente usada na internet, principalmente na proteção de transações financeiras, em segurança e acesso em comunicação, havendo diversos sistemas criptográficos. Dentre eles destacamos a criptografia via curvas elípticas, tema de nossos estudos.

3 CURVAS ELÍPTICAS

Uma *curva elíptica* $\mathbb{E}$ é o conjunto de soluções para uma equação da forma

$$y^2 = x^3 + Ax + B \tag{3.1}$$

que são chamadas de *equações de Weierstrass*, em homenagem ao matemático alemão Karl Weierstrass (1815 - 1897).

3.1 CONSTRUÇÃO DO GRÁFICO

Exemplo 1. $y^2 = x^3 - 4x$.

- Raízes: encontremos as interseções com o eixo x determinando, na equação, os valores de x para os quais $y = 0$. Então, devemos ter:

$$0^2 = (x^3 - 4x) \iff 0 = x(x^2 - 4) \iff x = 0 \text{ ou } x^2 - 4 = 0$$

$$\iff x = 0,\ x = -2 \text{ ou } x = 2.$$

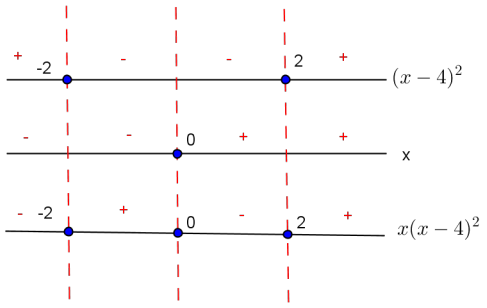
  Portanto, a curva encontra o eixo x nos pontos: $(-2, 0), (0, 0)$ e $(2, 0)$.

- Interseção com o eixo y: pontos da curva com abscissa igual a 0. Fazendo $x = 0$ na equação, obtemos:

$$y^2 = 0^3 - 4 \cdot 0 \Rightarrow y = 0.$$

  Portanto, essa curva intersecta o eixo y somente na origem $(0, 0)$.

Figura 3 – Estudo dos sinais $\mathbb{E}$: $y^2 = x(x^2 - 4)$



Fonte: própria autora

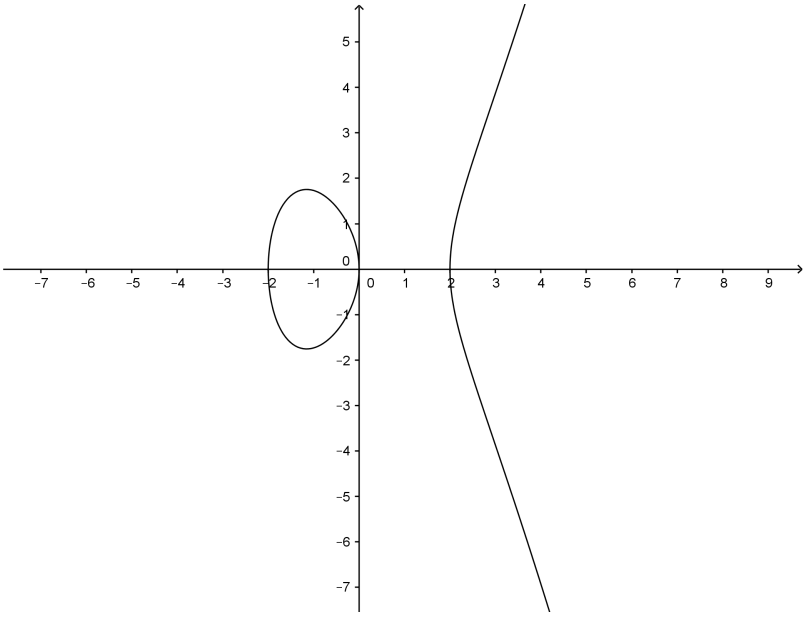
- Simetria: Como $(-y)^2 = y^2$ podemos verificar que (x, y) satisfaz a equação 3.1 se, e somente se, $(x, -y)$ também a satisfaz. Logo, o gráfico de uma curva elíptica qualquer, é sempre simétrico em relação ao eixo x.

- Estudo dos sinais: como $y^2 \geq 0$, então, existe y tal que (x, y) satisfaz 3.1 se, e somente se, $x^3 + Ax + B \geq 0$. Assim, para encontrarmos o domínio da equação, isto é, o conjunto de valores de x para os quais a equação tem solução, fazemos o estudo do sinal do termo $x^3 + Ax + B$.

  Na figura 3, fazemos o estudo do sinal do termo $x^3 - 4x = x(x^2 - 4)$ da equação deste exemplo. Analisemos: para valores de x menores que -2 e para valores de x maiores que zero e menores que 2, temos $x^3 - 4x$ negativo. Logo, teríamos valores negativos para y^2 o que é impossível. Portanto a curva não existe para esses valores de x. Para x maior ou igual a -2 e menor ou igual a 0 e para x maior ou igual a 2 temos $x^3 - 4x \geq 0$. Assim, para estes valores de x, existe y tal que $y^2 = x^3 - 4x$ e, portanto, temos o gráfico definido. Assim, o domínio desta equação é:

$$D = \{x \in \mathbb{R} \,|\, -2 \leq x \leq 0 \text{ ou } x \geq 2\}.$$

Figura 4 – Gráfico $\mathbb{E}$: $y^2 = x^3 - 4x$



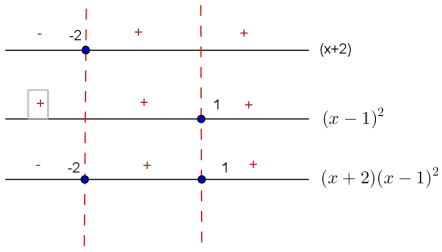
Fonte: própria autora

Vejamos mais alguns exemplos de curvas elípticas:

Exemplo 2. $y^2 = x^3 - 3x + 2$.

- Raízes: pelo Teorema das Raízes Racionais de um polinômio, os valores racionais de x candidatos a zeros da expressão $x^3 - 3x + 2$ são os inteiros divisores de 2. Testando

Figura 5 – Estudo dos sinais $\mathbb{E}: y^2 = x^3 - 3x + 2$



Fonte: própria autora

esses valores na equação, obtemos:

$$(-2)^3 - 3(-2) + 2 = -8 + 6 + 2 = 0,$$

$$(-1)^3 - 3(-1) + 2 = -1 + 3 + 2 = 4 \neq 0,$$

$$1^3 - 3 \cdot 1 + 2 = 1 - 3 + 2 = 0,$$

$$2^3 - 3 \cdot 2 + 2 = 8 - 6 + 2 = 4 \neq 0.$$

Logo $x = -2$ e $x = 1$ são as raízes racionais. Se dividirmos a expressão por $(x + 2)(x - 1)$ obtemos $x - 1$ como quociente. Logo, a expressão se fatora em $x^3 - 3x + 2 = (x + 2)(x - 1)^2$ e vemos que -2 e 1 são as únicas raízes. Portanto, a curva encontra o eixo x nos pontos $(-2, 0)$ e $(1, 0)$.

- Intersecção com o eixo y. Fazendo $x = 0$ na equação, obtemos:

$$y^2 = 0^3 - 3 \cdot 0 + 2 \iff y = \pm\sqrt{2}.$$

Portanto, a curva encontra o eixo y nos pontos $(0, -\sqrt{2})$ e $(0, \sqrt{2})$.

- Estudo dos sinais: na figura 5, fazemos o estudo do sinal do termo $x^3 - 3x + 2 = (x + 2)(x - 1)^2$. O domínio encontrado é:

$$D = \{x \in \mathbb{R} \,|x \geq -2\}.$$

Exemplo 3. $y^2 = x^3 - 2x + 4$.

- Raízes: pelo Teorema das Raízes Racionais de um polinômio, os valores racionais de x candidatos a zeros da expressão $x^3 - 3x + 2$ são os inteiros divisores de 4. Como no exemplo anterior, substituindo na expressão os valores de x pertencentes ao conjunto $\{-4, -2, -1, 1, 2, 4\}$, podemos verificar que a expressão se anula somente para $x = -2$. Se dividirmos a expressão por $(x + 2)$ obtemos $x^2 - 2x + 2$ como quociente. Logo, a expressão se fatora em $x^3 - 2x + 4 = (x + 2)(x^2 - 2x + 2)$. O discriminante do termo quadrático $x^2 - 2x + 2$ é:

$$\Delta = (-2)^2 - 4 \cdot 1 \cdot 2 = 4 - 8 = -4 < 0.$$

  Logo, este termo não tem raízes reais e, então, $x = -2$ é o único zero da expressão $x^3 - 2x + 4$. Portanto, a curva encontra o eixo x no ponto $(-2, 0)$.

- Intersecção com o eixo y. Fazendo $x = 0$ na equação, obtemos:

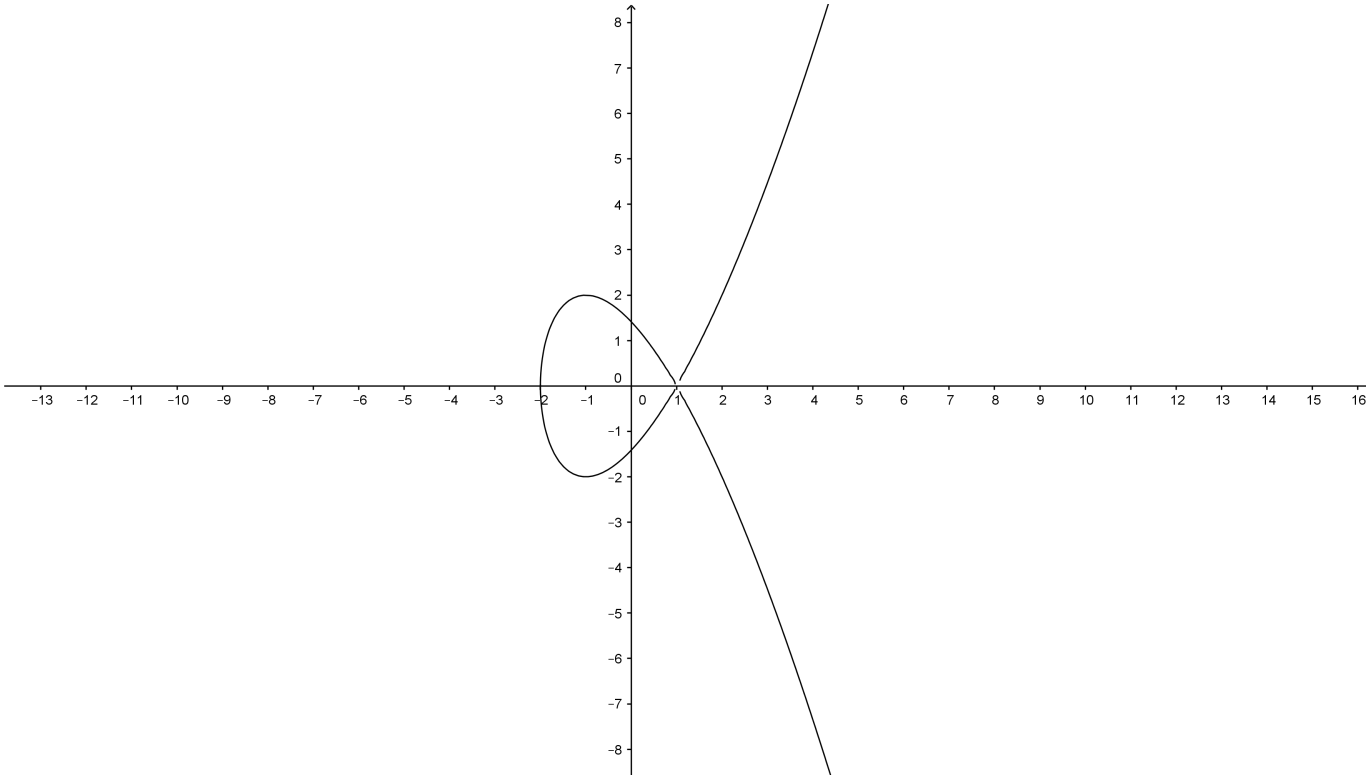
$$y^2 = 0^3 - 2 \cdot 0 + 4 \iff y = \pm 2.$$

  Portanto, a curva encontra o eixo y nos pontos $(0, -2)$ e $(0, 2)$.

- Estudo dos sinais: na figura 7, fazemos o estudo do sinal do termo $x^3 - 2x + 4 = (x + 2)(x^2 - 2x + 2)$. O domínio encontrado é:

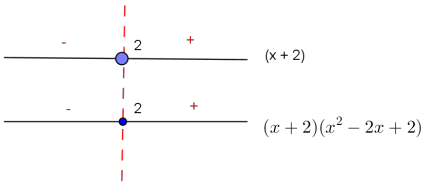
$$D = \{x \in \mathbb{R} \,|\, x \geq -2\}.$$

Figura 6 – Gráfico $\mathbb{E}: y^2 = x^3 - 3x + 2$



Fonte: própria autora

Figura 7 – Estudo dos sinais $\mathbb{E}: y^2 = x^3 - 2x + 4$

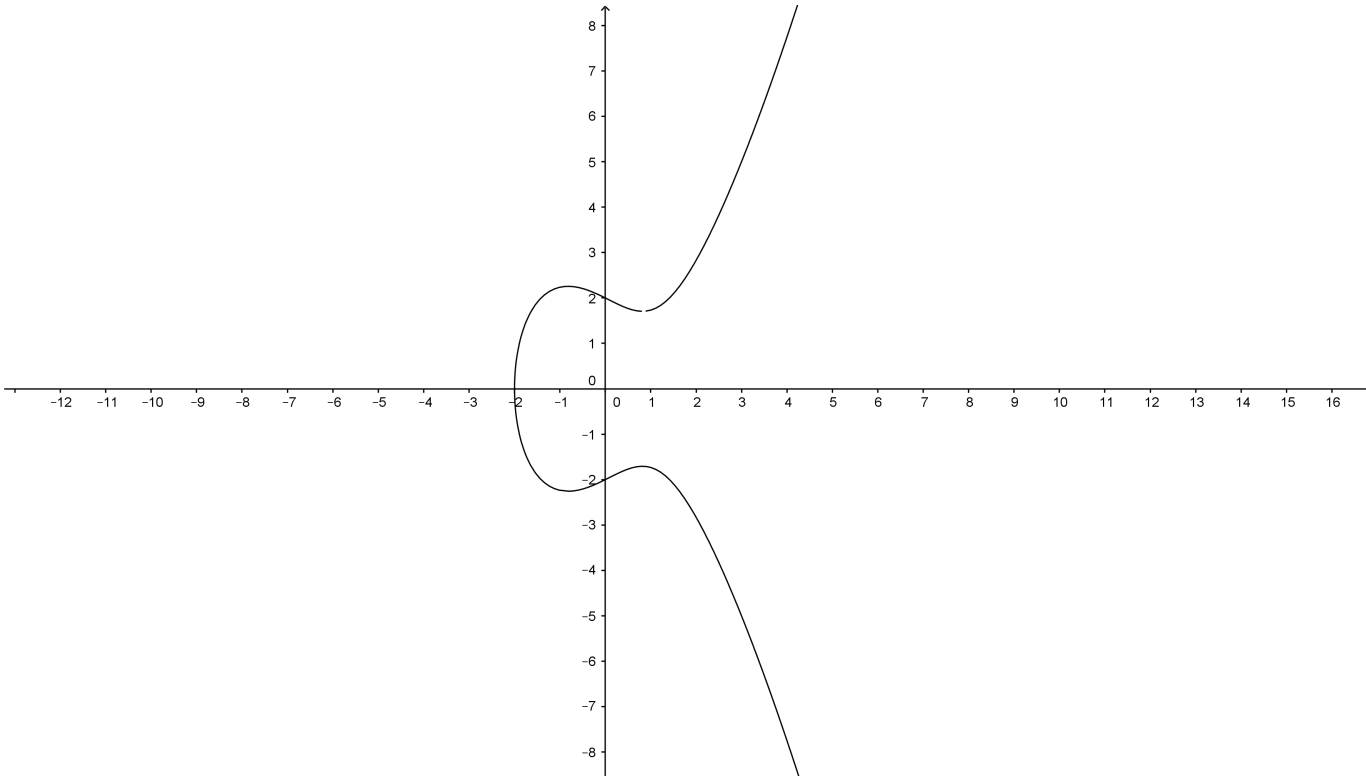


Fonte: própria autora

3.2 ÁLGEBRA DOS PONTOS

Uma característica surpreendente de curvas elípticas, é o fato de que podemos definir uma operação de soma que torna toda curva elíptica um grupo *abeliano*. Isso quer dizer que podemos "SOMAR" de um modo diferente dois pontos P e Q de uma curva elíptica $\mathbb{E}$ obtendo um terceiro ponto R de $\mathbb{E}$. Esta operação goza das propriedades: comutatividade, existência de elemento neutro, existência do elemento inverso e associatividade. Usando o símbolo $\oplus$ para denotar este novo jeito de somar, podemos escrever $R = P \oplus Q$. A maneira mais natural para descrever esta soma de dois pontos em curvas elípticas é a utilização da geometria. Sejam P e Q dois pontos sobre uma curva elíptica $\mathbb{E}$, tal como ilustrado na figura 9.

Figura 8 – Gráfico $\mathbb{E}$: $y^2 = x^3 - 2x + 4$



Fonte: própria autora

Começamos por desenhar a reta l, que intersecta $\mathbb{E}$ em três pontos, ou seja, P, Q e um outro R'. Tomamos nesse ponto R' a reflexão através do eixo x (ou seja, multiplicamos a sua coordenada y por -1) para obter um novo ponto R. O ponto R é chamado de "soma de P e Q" embora, como você pode observar, este processo não se assemelha em nada com uma adição comum.

Exemplo 4. $\mathbb{E}: y^2 = x^3 - 3x + 7$.

Sejam $P = (2, 3)$ e $Q = (3, 5)$ dois pontos de $\mathbb{E}$. A reta passando por P e Q tem equação

$$y - 3 = \frac{5-3}{3-2}(x - 2)$$
$$y = 2x - 1.$$

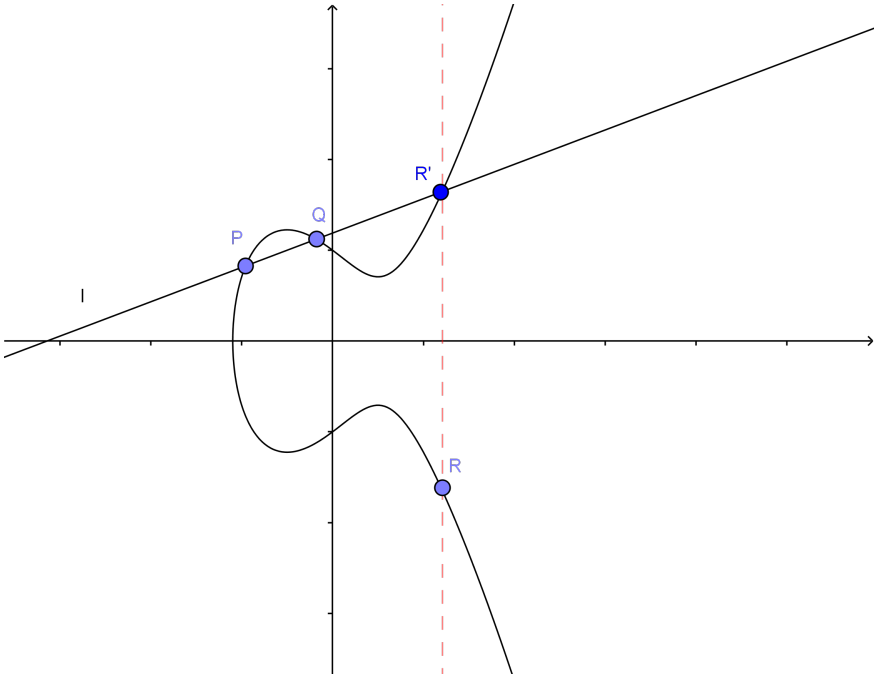
Para encontrar a interseção entre a reta e a curva, fazemos:

$$(2x - 1)^2 = x^3 - 3x + 7$$

$$4x^2 - 4x + 1 = x^3 - 3x + 7$$

$$x^3 - 4x^2 + x + 6 = 0.$$

Figura 9 – Soma de pontos $R = P \oplus Q$



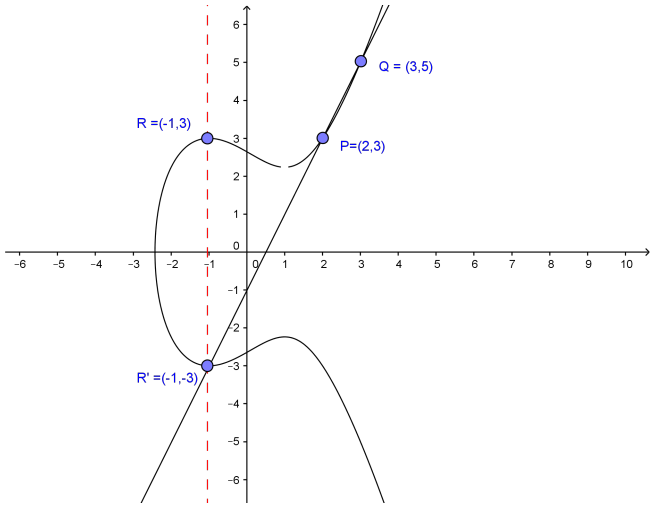
Fonte: própria autora

Como P e Q são dois pontos desta interseção, sabemos que $x = 2$ e $x = 3$ são raízes dessa equação. Dividindo o polinômio $x^3 - 4x^2 + x + 6$ por $(x - 2)(x - 3)$, obtemos a forma fatorada da equação:

$$(x + 1)(x - 2)(x - 3) = 0.$$

Logo $x = -1$ é a terceira raiz da equação.

Figura 10 – Soma de pontos: $R = P \oplus Q = (-1, 3) = (2, 3) \oplus (3, 5)$



Fonte: própria autora

Substituindo na equação da reta $y = 2x - 1$, obtemos

$$y = -3 \Rightarrow R' = (-1, -3).$$

Refletindo ao longo do eixo horizontal, obtemos:

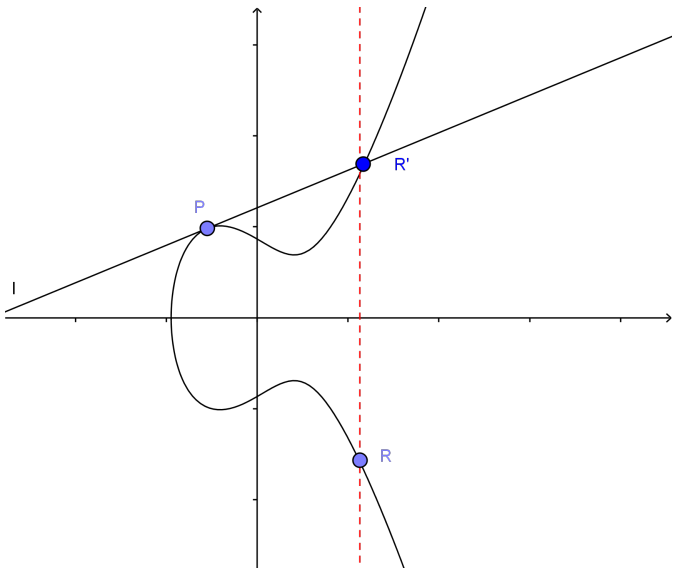
$$R = (-1, 3);$$

logo:

$$P \oplus Q = (-1, 3). \text{ (figura 10)}$$

Outro caso que também devemos analisar é a soma de um ponto com ele mesmo $P \oplus P$. Geometricamente, analise o que acontece com a reta l e com os pontos P e Q, se P e Q ficarem cada vez mais próximos: a reta l torna-se a reta tangente à curva $\mathbb{E}$ no ponto P. Assim, quando adicionamos P consigo mesmo, consideramos que l cruza $\mathbb{E}$ em P e em um outro ponto R', para que possamos proceder como antes. Em certo sentido, l ainda cruza $\mathbb{E}$ em três pontos, mas P conta como dois deles.(figura 11)

Figura 11 – Soma de um ponto com ele mesmo $R = P \oplus P = 2P$



Fonte: própria autora

Para encontrarmos $R = P \oplus P$ precisamos encontrar a equação da reta tangente l à curva $\mathbb{E}$ que, por sua vez, depende do cálculo da inclinação dessa reta. Mas como encontrar a inclinação da reta se dispomos de apenas um ponto?

Vejamos como resolver esse problema. Seja $l : y = mx + n$ a reta tangente a $\mathbb{E}$ no ponto $P = (x_0, y_0)$ e $R' = (x_1, y_1)$ o outro ponto de intersecção da curva $\mathbb{E}$ com a reta tangente l. Substituindo $y = mx + n$, em $y^2 = x^3 + Ax + B$, obtemos:

$$(mx + n)^2 = x^3 + Ax + B \Rightarrow x^3 - m^2x^2 + x(A - 2mn) + B - n^2 = 0.$$

Como a reta $r : y = mx + n$ é tangente à curva $\mathbb{E}$ no ponto $P = (x_0, y_0)$, a raiz x_0 possui multiplicidade maior ou igual a 2.

Assim, podemos representar as raízes da equação $x^3 - m^2x^2 + x(A - 2mn) + B - n^2 = 0$ por x_0, x_0 e x_1. Segue das **Relações de Girard**, que:

$$m^2 = x_0 + x_0 + x_1 \Rightarrow x_1 = m^2 - 2x_0$$

$$A - 2mn = x_0x_1 + x_0x_1 + x_0x_0$$

$$A - 2mn = 2x_0(m^2 - 2x_0^2) + x_0^2.$$

Como $P = (x_0, y_0)$, pertence à reta l, podemos escrever $n = y_0 - mx_0$, obtendo:

$$A - 2m(y_0 - mx_0) = 2x_0(m^2 - 2x_0) + x_0^2$$

$$A - 2my_0 = -3x_0^2$$

$$m = \frac{3x_0^2 + A}{2y_0}. \tag{3.2}$$

Observação: Esta fórmula pode ser obtida através da derivada da curva elíptica

$$y^2 = x^3 + Ax + B \Rightarrow 2yy' = 3x^2 + A \Rightarrow y' = \frac{3x^2 + A}{2y}.$$

Exemplo 5. Seja $\mathbb{E} : \ y^2 = x^3 - 3x + 7$ e o ponto $P = (-1, 3)$. Usando a fórmula 3.2 obtida acima, calculamos a inclinação m da reta l tangente a $\mathbb{E}$ em P por:

$$m = \frac{3x_0^2 + A}{2y_0} = \frac{3 \cdot (-1)^2 + (-3)}{2 \cdot 3}$$

$$m = \frac{0}{6}$$

$$m = 0.$$

Portanto, a reta tangente l é dada por:

$$l : \ y - 3 = 0$$

$$l : \ y = 3.$$

Para encontrar a intersecção entre a reta tangente e a curva fazemos:

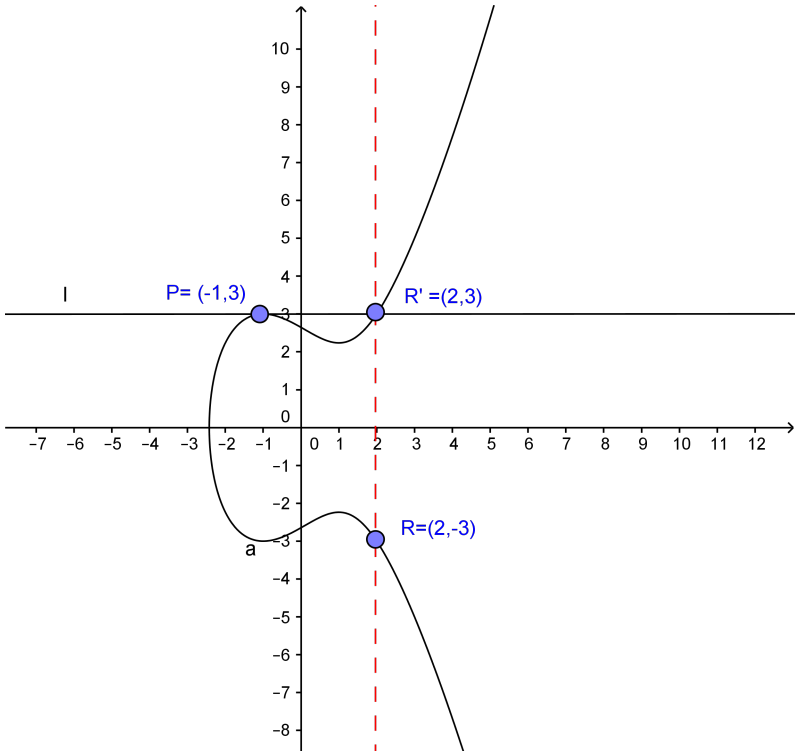
$$(3)^2 = x^3 - 3x + 7$$

$$x^3 - 3x - 2 = 0$$

$$(x + 1)^2(x - 2) = 0.$$

Note que $x = -1$ é uma raíz deste polinômio com multiplicidade 2. Logo a solução $x = 2$ é a abscissa do ponto que queremos determinar. Como a reta tangente tem equação $l : y = 3$,o valor de y é constante, logo $R' = (2, 3)$; refletindo, obtemos $R = P \oplus P = (2, -3)$.(figura 12)

Figura 12 – $R = P \oplus P = (2, -3) = (-1, 3) \oplus (-1, 3)$



Fonte: própria autora

O próximo problema que iremos abordar é quando queremos somar um ponto $P = (a, b)$ com a sua reflexão, em torno do eixo x, $P' = (a, -b)$. A reta l que passa por P e P' é a reta vertical $x = a$, e esta reta cruza $\mathbb{E}$ em apenas dois pontos P e P' (ver Figura 13). Não há um terceiro ponto; assim, parece que temos um impasse, mas a solução é criar um ponto O extra que vive "no infinito". Mais precisamente, o ponto O não existe no Plano XY, mas supomos que encontra-se em cada reta vertical. Em seguida, definimos

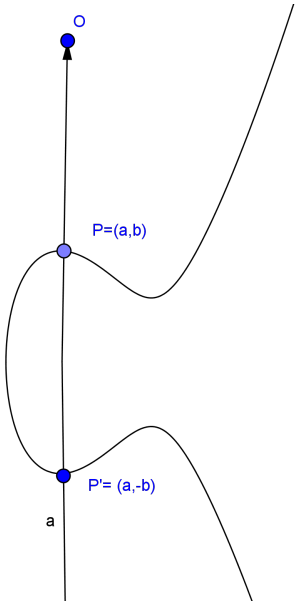
$$P \oplus P' = O.$$

Note que, a partir dessa ideia, também podemos definir $P \oplus O = P$, pois a reta que passa pelos pontos P e O encontra o ponto P' da curva elíptica E cuja reflexão é o ponto P, portanto O é o elemento neutro para esta definição de soma e, consequentemente, $O \oplus O = O$. Observe também que P', o simétrico de P em relação ao eixo horizontal, é o único ponto que somado com P é igual a 0. Então, o inverso de P é o ponto P' isto é $P' = -P$.

A **adição dos pontos** de uma curva elíptica que nós introduzimos goza de algumas propriedades dos números reais.

- Se $P \neq Q$ são pontos de $\mathbb{E}$ então existe uma reta secante à curva, definida pelos pontos P e Q. Esta reta sempre intercepta a curva num terceiro ponto R. Assim,

Figura 13 – Soma de um ponto com seu simétrico



Fonte: própria autora

temos: $P \oplus Q = R$.

- Se $P = Q$, então existe uma reta tangente à curva no ponto P. Esta reta sempre intersecta a curva em um segundo ponto R, assim: $P \oplus Q = P \oplus P = 2P = R$.
- Para quaisquer pontos P e Q duma curva elíptica verifica-se a identidade $P \oplus Q = Q \oplus P$;
- Existência de um **elemento nulo**, $P \oplus O = O \oplus P = P$, para qualquer ponto P.
- Existência do **ponto simétrico**: para qualquer ponto P existe $-P$ tal que $P \oplus (-P) = O$; assim podemos definir a subtração de pontos em $\mathbb{E}$: $Q \ominus P = Q \oplus (-P)$.

Nosso próximo objetivo é encontrar fórmulas explícitas para sermos capazes de somarmos pontos em uma curva elíptica. Para obtermos estas fórmulas, utilizaremos simplesmente geometria analítica elementar e pequenas manipulações algébricas conforme resultado abaixo.

Algoritmo de Soma de Pontos na Curva Elíptica: Seja $\mathbb{E} : y^2 = X^3 + AX + B$ uma curva elíptica e sejam P_1 e P_2 em $\mathbb{E}$. Então:

(1) Se $P_1 = O$, então $P_1 \oplus P_2 = P_2$;

(2) Se $P_2 = O$, então $P_1 \oplus P_2 = P_1$;

(3) Se nenhum destes casos ocorrem, escrevemos $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$ então:

(4) Se $x_1 = x_2$ e $y_1 = -y_2$, então $P_1 \oplus P_2 = O$;

(5) Caso contrário, defina λ por:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ se } P_1 \neq P_2$$

ou

$$\lambda = \frac{3x_1^2 + A}{2y_1} \text{ se } P_1 = P_2$$

Então $P_3 = P_1 \oplus P_2 = (x_3, y_3)$, onde

$$x_3 = \lambda^2 - x_1 - x_2 \text{ e } y_3 = \lambda(x_1 - x_3) - y_1.$$

Vejamos porque calculamos

$$P_3 = P_1 \oplus P_2 = (x_3, y_3)$$

fazendo

$$x_3 = \lambda^2 - x_1 - x_2$$

e

$$y_3 = \lambda(x_1 - x_3) - y_1.$$

Se $y = \lambda x + \mu$ é a reta que passa por P_1 e P_2 (com $P_1 \neq P_2$ ou $P_1 = P_2$) e $P_3' = (x_3', y_3')$ é o outro ponto de interseção entre a reta e a curva E então, intersectando com a curva, obtemos:

$$(\lambda x + \mu)^2 = x^3 + Ax + B \Rightarrow x^3 - \lambda^2 x^2 + (A - 2\lambda\mu)x + B - \mu^2 = 0.$$

Como x_1, x_2, x_3' são raízes dessa equação, devemos ter:

$$x_1 + x_2 + x_3' = \lambda^2 \Rightarrow x_3' = \lambda^2 - x_2 - x_1.$$

Para encontrarmos o valor de y_3', basta substituir $x_3' = x_3$ na equação da reta. Mas antes, notemos que $P_1 = (x_1, y_1)$ também pertence à reta $y_1 = \lambda x + \mu$, de modo que:

$$y_1 = \lambda x_1 + \mu \Rightarrow \mu = y_1 - \lambda x_1.$$

$$y_3' = \lambda x_3 + \mu = \lambda x_3 + (y_1 - \lambda x_1) = \lambda(x_3 - x_1) + y_1.$$

Consequentemente

$$y_3 = -y_3' = \lambda(x_1 - x_3) - y_1.$$

4 CURVAS ELÍPTICAS SOBRE CORPOS FINITOS

Apesar de conhecermos bem a álgebra e a geometria das curvas elípticas sobre o conjunto dos números reais, para o estudo de criptografia com curvas elípticas as truncagens e arredondamentos que ocorrem quando lidamos na prática com esses números não são adequadas. Esses estudos necessitam de uma aritmética rápida e precisa que pode ser obtida através do uso de corpos inteiros finitos. Para isto, precisamos introduzir o conceito de congruência. O livro de Coutinho [2] traz uma boa introdução desse tema para os alunos do ensino médio. O livro de Hefez [6], escrito para formação de professores, faz uma abordagem mais completa e com aplicações.

4.1 CONGRUÊNCIA

Usamos congruência quando lidamos com fenômenos periódicos, aqueles que tem a propriedade de se repetirem com regularidade. Por exemplo, a Terra leva 24 horas para dar uma volta em torno de si mesma, de forma que seu período de rotação é de 24 horas. Já o período de revolução da Terra é de 365 dias e um quarto e corresponde ao menor tempo que ela leva para dar uma volta em torno do Sol.

Ao tratarmos de congruências, estaremos lidando com a grande ideia de Gauss de desenvolver uma aritmética dos restos da divisão por um certo número fixado. Vejamos um exemplo.

Exemplo 6. Se hoje é domingo, que dia da semana será daqui a 1000 dias? E daqui a 7881 dias? Usemos o fato dos dias da semana se repetirem de 7 em 7 dias, ou seja, é um fenômeno periódico com período 7. Como $1000 = 142 \cdot 7 + 6$ então, em 1000 dias passarão 142 semanas e mais 6 dias. Ao se passarem 142 semanas estaremos novamente no domingo e, em mais 6 dias, estaremos em um sábado. Como $7881 = 1125 \cdot 7 + 6$, após 7881 dias terão se passado 1125 semanas mais 6 dias. Também estaremos em um sábado. Assim, apesar de serem números inteiros distintos, para efeito do dia alcançado na semana eles são iguais pois deixam o mesmo resto na divisão por 7.

Definição. Seja dado um número inteiro n maior do que 1. Diremos que dois números inteiros a e b são *congruentes módulo* n quando a e b possuírem mesmo resto quando divididos por n. Neste caso, simbolizaremos esta situação como segue:

$$a \equiv b \pmod{n}.$$

Mais precisamente, usando a divisão euclidiana, se escrevemos $a = n \cdot q_1 + r_1$ e $b = n \cdot q_2 + r_2$ com $0 \leq r_1, r_2 < n$ então:

$$a \equiv b \pmod{n} \iff r_1 = r_2.$$

Observe que, explicitando os restos nas expressões euclidianas obtemos $r_1 = a - n \cdot q_1$ e $r_2 = b - n \cdot q_2$ e podemos concluir que:

$$r_1 = r_2 \iff a - n \cdot q_1 = b - n \cdot q_2 \iff a - b = n(q_1 - q_2).$$

Logo, fazendo $q_1 - q_2 = k$, obtemos o critério:

$$a \equiv b \pmod{n} \iff a - b = n \cdot k. \tag{4.1}$$

Ou seja, dois inteiros são congruentes módulo n se, e somente se, a diferença entre eles for um múltiplo de n.

Quando a e b **não** são congruentes módulo n, escreve-se:

$$a \not\equiv b \pmod{n}.$$

Exemplo 7.

- $22 \equiv 8 \pmod{7}$ pois, como $22 = 3 \cdot 7 + 1$ e $8 = 1 \cdot 7 + 1$, os restos das divisões de 22 e de 8 por 7 são os mesmos (iguais a 1). De outra forma, note que $22 - 8 = 14 = 2 \cdot 7$ e a diferença é um múltiplo de 7.
- $27 \equiv 32 \pmod{5}$ pois, como $27 = 5 \cdot 5 + 2$ e $32 = 6 \cdot 5 + 2$, os restos das divisões de 27 e 32 por 5 são os mesmos (iguais a 2). Também, $27 - 32 = -5 = -1 \cdot 5$ e a diferença é um múltiplo de 5.
- $31 \not\equiv 29 \pmod{3}$ pois, como $31 = 3 \cdot 10 + 1$ e $29 = 9 \cdot 3 + 2$, o resto da divisão de 31 por 3 é 1 enquanto o resto da divisão de 29 por 3 é 2. Neste caso, $31 - 29 = 2$ que não é um múltiplo de 3.
- $-45 \equiv 3 \pmod{8}$ pois, como $-45 = -6 \cdot 8 + 3$ e $3 = 0 \cdot 8 + 3$, os restos das divisões de -45 e 3 por 8 são os mesmos (iguais a 3). Também, $-45 - 3 = -48 = -6 \cdot 8$ e a diferença é um múltiplo de 8.

Propriedades da Congruência Modular

A congruência modular satisfaz algumas propriedades que a tornam muito semelhante à igualdade usual. As propriedades mais elementares da igualdade são as seguintes:

reflexiva Todo número é igual a si próprio;

simétrica Se $a = b$ então $b = a$;

transitiva Se $a = b$ e $b = c$, então $a = c$.

No caso da congruência modular, temos propriedades análogas às enunciadas acima para igualdade. Precisamos dessas propriedades para podermos utilizar de forma correta a congruência modular nos cálculos que faremos mais adiante, incluindo a codificação de uma mensagem através de curvas elípticas. Mais precisamente, estas propriedades são:

reflexiva Todo número é congruente módulo n a si próprio;

simétrica Se $a \equiv b \pmod{n}$ então $b \equiv a \pmod{n}$;

transitiva Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$ então $a \equiv c \pmod{n}$.

As duas primeiras propriedades seguem imediatamente da definição de congruência. Para a terceira, usando o critério 4.1, se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$ então devem existir inteiros k_1 e k_2 tais que $a - b = n \cdot k_1$ e $b - c = n \cdot k_2$. Logo:

$$(a - b) + (b - c) = n \cdot k_1 + n \cdot k_2 \iff a - c = n(k_1 + k_2).$$

Portanto, $a - c$ é múltiplo de n e daí $a \equiv c \pmod{n}$.

Há dois fatos importantes que sabemos sobre a congruência módulo n. O primeiro é que a congruência funciona de maneira muito semelhante à igualdade de inteiros. O segundo é consequência da própria definição e afirma que números inteiros diferentes podem ser congruentes módulo n.

Exemplo 8. Os números 31, 1 e 51 são diferentes, mas se olhamos para eles através da congruência módulo 5, não conseguimos distingui-los entre si: eles são todos congruentes módulo 5.

Em verdade, as 3 propriedades enunciadas logo acima garantem que a congruência módulo n é uma relação de equivalência sobre os inteiros. Isto induz uma repartição de $\mathbb{Z}$ em classes de elementos equivalentes chamadas, neste caso, de *classes residuais*. A classe residual do 0 são todos os inteiros congruentes a 0 módulo n (ou seja, todos os múltiplos de n); a classe residual do 1 são todos os inteiros congruentes a 1, e assim por diante. Para um n fixado, quantas classes residuais teremos para a congruência módulo n?

Para responder, precisamos estudar em mais detalhes a relação entre a congruência módulo n e a divisibilidade de inteiros. Seja a um inteiro. Dividindo a por n temos

$$a = n \cdot q + r \text{ e } 0 \leq r < n.$$

Assim,

$$a - r = n \cdot q$$

o que equivale a dizer que

$$a \equiv r \pmod{n}.$$

Verificamos com isto que todo inteiro positivo é congruente módulo n ao resto de sua divisão por n, que é um número inteiro de 0 a $n - 1$. Em geral, se $a \equiv r \pmod{n}$ e $0 \leq r < n$, dizemos que r é o *resíduo* de a módulo n. O conjunto dos resíduos módulo n é o conjunto:

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n - 1\}.$$

Exemplo 9. $\mathbb{Z}_2 = \{0, 1\}$, $\mathbb{Z}_3 = \{0, 1, 2\}$, $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $\mathbb{Z}_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.

Uma pergunta parece natural: como a congruência módulo n se comporta em relação à soma de inteiros? Vejamos um exemplo.

Exemplo 10. $51 \equiv 31 \pmod 5$ e $43 \equiv 103 \pmod 5$, ao passo que $51 + 43 = 94$ e $31 + 103 = 134$; além disso, $94 - 134 = -40 = 5 \cdot -8$ donde $94 \equiv 134 \pmod 5$. Ou seja, $51 + 43 \equiv 31 + 143 \pmod 5$.

Agora com base no exemplo, podemos pensar: se $a_1 \equiv b_1 \pmod n$ e $a_2 \equiv b_2 \pmod n$ será que $a_1 + a_2 \equiv b_1 + b_2 \pmod n$ sempre? Suponha que $a_1 \equiv b_1 \pmod n$ e $a_2 \equiv b_2 \pmod n$. Então, existem inteiros k_1 e k_2 tais que $a_1 - b_1 = k_1 \cdot n$ e $a_2 - b_2 = k_2 \cdot n$. Logo:

$$(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) = k_1 \cdot n + k_2 \cdot n = (k_1 + k_2)n$$

$$\Rightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod n.$$

O mesmo pode ser feito trocando a soma pela diferença. Assim, provamos a proposição seguinte.

Proposição 1. *Sejam a_1, a_2, b_1, b_2 inteiros quaisquer e seja n um inteiro maior do que 1. Se $a_1 \equiv b_1 \pmod n$ e $a_2 \equiv b_2 \pmod n$, então $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod n$.*

Passemos, agora, à pergunta análoga para a multiplicação: se $a_1 \equiv b_1 \pmod n$ e $a_2 \equiv b_2 \pmod n$, o que podemos afirmar sobre a relação entre $a_1 \cdot a_2$ e $b_1 \cdot b_2$? Novamente, devem existir inteiros k_1 e k_2 tais que $a_1 - b_1 = k_1 \cdot n$ e $a_2 - b_2 = k_2 \cdot n$. Logo:

$$a_1 \cdot a_2 - b_1 \cdot b_2 = a_1 \cdot a_2 - b_1 \cdot a_2 + b_1 \cdot a_2 - b_1 \cdot b_2 = (a_1 - b_1)a_2 + (a_2 - b_2)b_1$$

$$= k_1 \cdot n \cdot a_2 + k_2 \cdot n \cdot b_1 = (k_1 \cdot a_2 + k_2 \cdot b_1)n$$

$$\Rightarrow a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod n.$$

Assim, temos a proposição análoga para o produto.

Proposição 2. *Sejam a_1, a_2, b_1, b_2 inteiros quaisquer e seja n um inteiro maior do que 1. Se $a_1 \equiv b_1 \pmod n$ e $a_2 \equiv b_2 \pmod n$, então $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod n$.*

Testemos nossa conclusão no mesmo exemplo usado no caso da adição.

Exemplo 11. $51 \equiv 31 \pmod 5$ e $43 \equiv 103 \pmod 5$, enquanto que $51 \cdot 43 = 2193$ e $31 \cdot 103 = 3193$ cuja diferença é -1000 e, portanto, um múltiplo de 5; assim $51 \cdot 43 \equiv 31 \cdot 103 \pmod 5$.

Usando as proposições acima, ao operar com inteiros módulo n, podemos primeiro achar os resíduos de cada termo para depois fazermos as operações. Isto simplifica bastante as operações, como pode ser notado no exemplo seguinte.

Exemplo 12.
- $33 + 67 \equiv 3 + 2 = 5 \equiv 0 \pmod 5$;
- $79 \cdot 104 \equiv 1 \cdot 2 = 2 \pmod 3$;
- $(477 + 1035)(908 - 334) \equiv (7 + 5)(8 - 4) = 12 \cdot 4 \equiv 2 \cdot 4 = 8 \pmod{10}$.

O exemplo acima mostra que para operarmos com os inteiros módulo n basta conhecermos o resultado das operações para os resíduos módulo n. Ou seja, basta conhecermos as tábuas de soma e produto em $\mathbb{Z}_n$. As tabelas 1, 2 e 3 a seguir mostram as tábuas de operações módulo 8 e módulo 13.

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	8
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

·	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Tabela 1 – Tábuas da soma e do produto em $\mathbb{Z}_8$

+	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12	1
2	2	3	4	5	6	7	8	9	10	11	12	1	2
3	3	4	5	6	7	8	9	10	11	12	1	2	3
4	4	5	6	7	8	9	10	11	12	1	2	3	4
5	5	6	7	8	9	10	11	12	1	2	3	4	5
6	6	7	8	9	10	11	12	1	2	3	4	5	6
7	7	8	9	10	11	12	1	2	3	4	5	6	7
8	8	9	10	11	12	1	2	3	4	5	6	7	8
9	9	10	11	12	1	2	3	4	5	6	7	8	9
10	10	11	12	1	2	3	4	5	6	7	8	9	10
11	11	12	1	2	3	4	5	6	7	8	9	10	11
12	12	1	2	3	4	5	6	7	8	9	10	11	12

Tabela 2 – Tábua da soma em $\mathbb{Z}_{13}$

Sabendo fazer as operações em $\mathbb{Z}_n$, a próxima pergunta natural a fazer é: como resolver uma equação em $\mathbb{Z}_n$? Se as operações envolvidas forem somente soma e subtração, resolvemos similar ao que fazemos em $\mathbb{Z}$. Isto funciona pois o 0 e o $-a$ funcionam em $\mathbb{Z}_n$ como elemento neutro e elemento simétrico de a, respectivamente, com relação à soma. De fato:

$$0 + a \equiv a \pmod n \text{ e } -a + a \equiv 0 \pmod n.$$

Vejamos o exemplo seguinte.

·	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12
2	0	2	4	6	8	10	12	1	3	5	7	9	11
3	0	3	6	9	12	2	5	8	11	1	4	7	10
4	0	4	8	12	3	7	11	2	6	10	1	5	9
5	0	5	10	2	7	12	4	9	1	6	11	3	8
6	0	6	12	5	11	4	10	3	9	2	8	1	7
7	0	7	1	8	2	9	3	10	4	11	5	12	6
8	0	8	3	11	6	1	9	4	12	7	2	10	5
9	0	9	5	1	10	6	2	11	7	3	12	8	4
10	0	10	7	4	1	11	8	5	2	12	9	6	3
11	0	11	9	7	5	3	1	12	10	8	6	4	2
12	0	12	11	10	9	8	7	6	5	4	3	2	1

Tabela 3 – Tábua do produto em $\mathbb{Z}_{13}$

Exemplo 13. Vamos determinar $x \in \mathbb{Z}_8$ tal que:

$$37 + x \equiv 26 \pmod 8.$$

Trocando os inteiros pelos seus resíduos módulo 8 e depois somando o simétrico obtemos:

$$37 + x \equiv 26 \pmod 8$$

$$5 + x \equiv 2 \pmod 8$$

$$-5 + 5 + x \equiv -5 + 2 \pmod 8$$

$$0 + x \equiv -3 \pmod 8$$

$$x \equiv 5 \pmod 8$$

Note que, na prática, a operação de somar simétrico equivale a passar para o outro lado da equação com o sinal trocado, como já estamos habituados em $\mathbb{Z}$.

Mas, e quando a equação envolver um produto? Como determinar $x \in \mathbb{Z}_n$ tal que: $ax \equiv b \pmod n$? É fácil ver que o 1 funciona como elemento neutro também para o produto em $\mathbb{Z}_n$ pois $1 \cdot x \equiv x \pmod n$ para todo $x \in \mathbb{Z}_n$. Então, seguindo o modelo da soma, se existir $a' \in \mathbb{Z}_n$ tal que $a'a \equiv 1 \pmod n$ podemos resolver a equação fazendo:

$$ax \equiv b \,(\text{mod } n) \iff a'ax \equiv a'b \,(\text{mod } n) \iff 1x \equiv a'b \,(\text{mod } n) \iff x \equiv a'b \,(\text{mod } n).$$

Vejamos dois exemplos.

Exemplo 14. Vamos tentar determinar $x \in \mathbb{Z}_8$ tal que:

$$54x \equiv 19 \pmod 8.$$

Trocando os inteiros pelos seus resíduos módulo 8 obtemos:

$$54x \equiv 19 \pmod 8 \iff 6x \equiv 3 \pmod 8.$$

Ora, se consultarmos a tabela 1 veremos que não existe $x \in \mathbb{Z}_8$ que multiplicado por 6 seja congruente a 3. A equação não tem solução em $\mathbb{Z}_8$. Note que não podemos resolver usando o procedimento descrito antes do exemplo pois não existe elemento em $\mathbb{Z}_8$ que multiplicado por 6 seja congruente a 1.

Exemplo 15. Vamos tentar determinar $x \in \mathbb{Z}_8$ tal que:

$$53x \equiv 19 \pmod 8.$$

Trocando os inteiros pelos seus resíduos módulo 8 obtemos:

$$53x \equiv 19 \pmod 8 \iff 5x \equiv 3 \pmod 8.$$

Agora, ao consultarmos a tabela 1 vemos que o valor de $x \in \mathbb{Z}_8$ que multiplicado por 5 é congruente a 3 é 7. Assim, $x = 7$ é a solução da equação. Também podemos encontrar a solução usando o procedimento descrito antes do exemplo anterior. De fato, vemos na tabela que $5 \cdot 5 \equiv 1 \pmod 8$. Então:

$$5x \equiv 3 \pmod 8 \iff 5 \cdot 5x \equiv 5 \cdot 3 \pmod 8 \iff 1x \equiv 15 \pmod 8 \iff x \equiv 7 \pmod 8.$$

Quando utilizamos a linguagem de números racionais, dizemos que dois números são inversos quando o produto entre eles é igual a 1. Quando falamos de congruência dois números são inversos quando o produto entre eles é congruente a 1 $\pmod n$. Sistematizando, diremos que a e a' são *inversos módulo* n se

$$a \cdot a' \equiv 1 \pmod n.$$

Note que 0 não pode ter inverso módulo n para qualquer $n > 1$, pois:

$$0 \cdot b = 0 \not\equiv 1 \pmod n, \text{ qualquer que seja } b \in \mathbb{Z}.$$

Consultando a tabela 1, podemos montar uma tabela de inversos dos resíduos módulo 8.

Resíduo	1	2	3	4	5	6	7
Inverso	1	$*$	3	$*$	5	$*$	7

Tabela 4 – Tabela de inversos módulo 8

O asterisco que aparece na linha dos inversos indica que o elemento correspondente não tem inverso. Neste caso, 2, 4 e 6 não admitem inverso módulo 8. Se observarmos com cuidado veremos que na tabela de inversos módulo 8, os números que não possuem inverso são aqueles que tem divisores comuns com 8 enquanto que os números que possuem inverso são aqueles primos com 8. Será que isto é sempre verdade para quaisquer a e n?

De fato, a e n são primos entre si quando o máximo divisor comum entre eles é igual a 1. Do algoritmo de Euclides para cálculo do máximo divisor comum sabemos que isto ocorre se, e somente se, existem números inteiros, digamos s e t, tais que

$$1 = s \cdot a + t \cdot n \iff 1 - s \cdot a = t \cdot n \iff 1 \equiv s \cdot a \pmod{n}$$

que ocorre se, e somente se, s for inverso de a módulo n. Assim, provamos a proposição seguinte.

Proposição 3. *O elemento $a \in \mathbb{Z}_n$ possui inverso módulo n se, e somente se, a e n são primos entre si.*

Quando n é um número primo, sabemos que os números inteiros $1, 2, \ldots, n-1$ são todos primos com n. Portanto, todos os resíduos diferentes de 0 em $\mathbb{Z}_n$ tem inverso módulo n. Por exemplo, vejamos na tabela 3 de multiplicação módulo 13 quais os produtos são congruentes a 1 módulo 13:

$$1 \cdot 1 \equiv 1 \pmod{13};$$

$$2 \cdot 7 \equiv 1 \pmod{13};$$

$$3 \cdot 9 \equiv 1 \pmod{13};$$

$$4 \cdot 10 \equiv 1 \pmod{13};$$

$$5 \cdot 8 \equiv 1 \pmod{13};$$

$$6 \cdot 11 \equiv 1 \pmod{13};$$

$$12 \cdot 12 \equiv 1 \pmod{13}.$$

Em geral, dado um primo p, o conjunto $\mathbb{Z}_p$ dos resíduos módulo p é um corpo com exatamente p elementos. Isto significa que a soma e o produto em $\mathbb{Z}_p$ possuem todas as propriedades algébricas dos inteiros (comutatividade, associatividade, elemento neutro, simétrico da soma, distributiva) e, além disso, todos os elementos não nulos de $\mathbb{Z}_p$ possuem inverso multiplicativo.

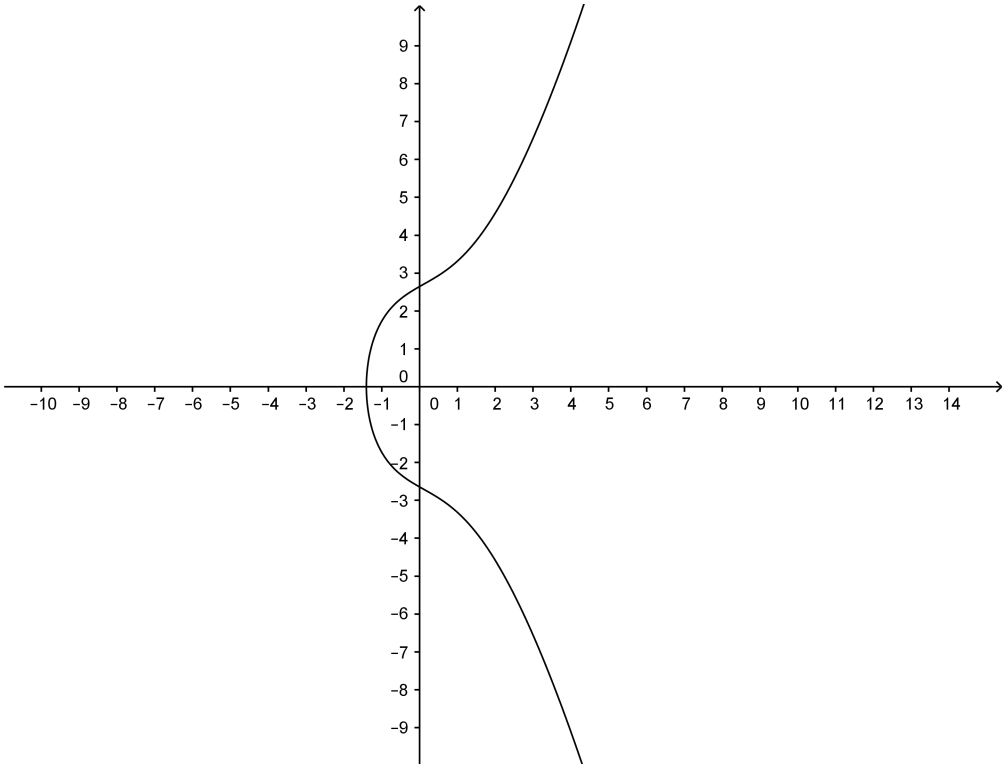
4.2 CURVAS ELÍPTICAS SOBRE $\mathbb{Z}_p$

Chegamos a uma etapa importante para a aplicação de curvas elípticas na criptografia. Agora, vamos aplicar a definição que vimos para a soma de pontos de uma curva elíptica sobre o corpo finito $\mathbb{Z}_p$, em que p é um número primo. Para isso, definimos uma curva elíptica $\mathbb{E}(\mathbb{Z}_p)$ sobre $\mathbb{Z}_p$ como uma equação do tipo

$$y^2 \equiv x^3 + Ax + B \pmod{p},$$

em que $A, B \in \mathbb{Z}_p$. A curva elíptica inclui todos os pontos $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ que satisfazem a equação, mais o ponto O. Lembremos que o conjunto $\mathbb{Z}_p$ é composto por valores de 0

Figura 14 – Gráfico $\mathbb{E}$: $Y^2 = X^3 + 3X + 7$ em $\mathbb{R}^2$



Fonte: própria autora

a $p-1$ ($Z_p = \{0, 1, ...p-1\}$) e todas as operações devem ser finalizadas calculando-se o resto da divisão por p. Dessa forma, sempre alcançamos resultados dentro de $\mathbb{Z}_p$.

Como exemplo, consideremos a curva elíptica

$$\mathbb{E} : Y^2 = X^3 + 3X + 7 \text{ sobre o corpo } \mathbb{Z}_{13}.$$

Podemos encontrar os pontos de $\mathbb{E}(\mathbb{Z}_{13})$ substituindo todos os valores possíveis de $x = 0, 1, 2, 3, ..., 12$ no polinômio $x^3 + 3x + 7$ e checando se este valor é um quadrado módulo 13 ou não. Na tabela 5 listamos os quadrados módulo 13. Na tabela 6 listamos os valores de $x^3 + 3x + 7 \pmod{13}$ para $x \in \mathbb{Z}_p$.

y	0	1	2	3	4	5	6	7	8	9	10	11	12
y^2	0	1	4	9	3	12	10	10	12	3	9	4	1

Tabela 5 – Tabela de resíduos quadráticos: y^2 em $\mathbb{Z}_{13}$

Por exemplo para $x = 0$, temos como resultado 7, que não é um quadrado módulo 13. Para $x = 1$, obtemos 11, que também não é um quadrado módulo 13. Para $x = 2$, obtemos 21 que é congruente a 8 módulo 13 e também não é um quadrado módulo 13. Contudo, para $x = 3$ obtemos 43 que é congruente a 4 módulo 13 e é um quadrado em

x	0	1	2	3	4	5	6	7	8	9	10	11	12
x^3+3x+7	7	11	8	4	5	4	7	7	10	9	10	6	3

Tabela 6 – Tabela de resíduos: x^3+3x+7 em $\mathbb{Z}_{13}$

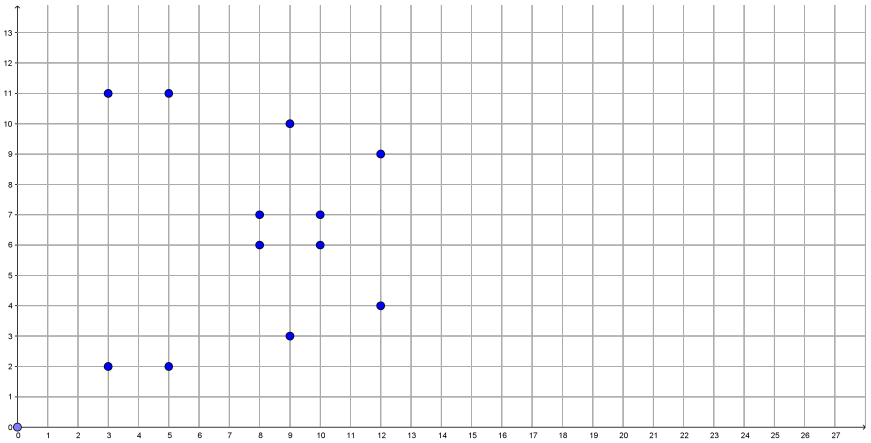
$\mathbb{Z}_{13}$. De fato, pois $y^2 = 2^2 = 4$ e também $y^2 = 11^2 = 121 \equiv 4 \pmod{13}$. Então obtemos dois pontos $(3,2)$ e $(3,11)$ em $\mathbb{E}(\mathbb{Z}_{13})$.

Continuando desta maneira, teremos uma lista completa com todos os pontos $\mathbb{E}(\mathbb{Z}_{13}) =$

$$\{O,(3,2),(3,11),(5,2),(5,11),(8,6),(8,7),(9,3),(9,10),(10,6),(10,7),(12,4),(12,9)\}.$$

Temos assim que $\mathbb{E}(\mathbb{Z}_{13})$ é composto por 13 pontos.

Figura 15 – Pontos da Curva elíptica $Y^2 = X^3+3X+7$ em $\mathbb{Z}_{13}$



Fonte: própria autora

Vamos agora, usando o Algoritmo de Soma de Pontos na Curva Elíptica, calcular alguns pontos da curva:

$$\mathbb{E} : Y^2 = X^3+3X+7 \text{ sobre o corpo } \mathbb{Z}_{13}.$$

- Se $P_1 = (3,2)$ e $P_2 = O$ então $P_1 \oplus P_2 = (3,2)$.
- Se $P_1 = (3,2)$ e $P_2 = (3,11)$ então $P_1 \oplus P_2 = O$. De fato $(3,2)$ e $(3,11)$ são simétricos em relação ao eixo horizontal, pois $11 \equiv -2 \pmod{13}$.
- Se $P_1 = (3,2)$ e $P_2 = (5,11)$, fazemos:

$$\lambda \equiv \frac{y_2 - y_1}{x_2 - x_1} \pmod{p} \iff \lambda(x_2 - x_1) \equiv (y_2 - y_1) \pmod{p};$$

substituindo P_1 e P_2, temos:

$$\lambda \cdot (5-3) \equiv (11-2) \pmod{p}$$

$$2\lambda \equiv 9 \pmod{p}.$$

Como $2 \cdot 7 \equiv 1 \pmod{13}$, encontramos λ fazendo:

$$7 \cdot 2\lambda \equiv 7 \cdot 9 \pmod{13} \iff \lambda \equiv 11 \pmod{13}.$$

Agora, podemos calcular as coordenadas de $P_3 = (x_3, y_3)$ fazendo:

- $x_3 = \lambda^2 - x_2 - x_1 \equiv 11^2 - 5 - 3 = 113 \equiv 9 \pmod{13}$;
- $y_3 = \lambda(x_1 - x_3) - y_1 \equiv 11(3 - 9) - 2 = -68 \equiv 10 \pmod{13}$. Assim:

$$P_3 = (9, 10).$$

- Se $P_1 = P_2 = (3, 11)$, fazemos:

$$\lambda \equiv \frac{3x_1^2 + A}{2y_1} \pmod{13} \iff \lambda \cdot 2y_1 \equiv 3x_1^2 + A \pmod{13} \iff 2 \cdot 11 \cdot \lambda \equiv 3 \cdot 3^2 + 3 \pmod{13} \iff$$

Como $9 \cdot 3 \equiv 1 \pmod{13}$, encontramos λ fazendo:

$$3 \cdot 9\lambda \equiv 4 \cdot 3 \pmod{13} \iff \lambda \equiv 12 \pmod{13}.$$

Agora, fazendo:

- $x_3 = \lambda^2 - x_2 - x_1 \equiv 12^2 - 3 - 3 = 144 - 6 \equiv 8 \pmod{13}$;
- $y_3 = \lambda(x_1 - x_3) - y_1 \equiv 12(3 - 8) - 11 = 12(-5) - 11 = -71 \equiv 7 \pmod{13}$. Assim:

$$P_3 = (8, 7).$$

Repetindo este procedimento para todos os pares de pontos de $\mathbb{E}(\mathbb{Z}_{13})$ obtemos a tábua de soma de pontos desta curva elíptica que consta na tabela 7.

$\oplus$	O	(3,2)	(3,11)	(5,2)	(5,11)	(8,6)	(8, 7)	(9,3)	(9,10)	(10,6)	(10,7)	(12, 4)	(12, 9)
O	O	(3,2)	(3,11)	(5,2)	(5,11)	(8,6)	(8, 7)	(9,3)	(9,10)	(10,6)	(10,7)	(12, 4)	(12, 9)
(3,2)	(3,2)	(8,6)	O	(5,11)	(9,10)	(12,9)	(3,11)	(5,2)	(10,6)	(12,4)	(9,3)	(8,7)	(10,7)
(3,11)	(3,11)	O	(8,7)	(9,3)	(5,2)	(3,2)	(12,4)	(10,7)	(5,11)	(9,10)	(12,9)	(10,6)	(8,6)
(5,2)	(5,2)	(5,11)	(9,3)	(3,11)	O	(9,10)	(10,7)	(8,7)	(3,2)	(8,6)	(12,4)	(12,9)	(10,6)
(5,11)	(5,11)	(9,10)	(5,2)	O	(3,2)	(10,6)	(9,3)	(3,11)	(8,6)	(12,9)	(8,7)	(10,7)	(12,4)
(8,6)	(8,6)	(12,9)	(3,2)	(9,10)	(10,6)	(10,7)	O	(5,11)	(12,4)	(8,7)	(5,2)	(3,11)	(9,3)
(8,7)	(8,7)	(3,11)	(12,4)	(10,7)	(9,3)	O	(10,6)	(12,9)	(5,2)	(5,11)	(8,6)	(9,10)	(3,2)
(9,3)	(9,3)	(5,2)	(10,7)	(8,7)	(3,11)	(5,11)	(12,9)	(12,4)	O	(3,2)	(10,6)	(8,6)	(9,10)
(9, 10)	(9,10)	(10,6)	(5,11)	(3,2)	(8,6)	(12,4)	(5,2)	O	(12,9)	(10,7)	(3,11)	(9,3)	(8,7)
(10,6)	(10,6)	(12,4)	(9,10)	(8,6)	(12,9)	(8,7)	(5,11)	(3,2)	(10,7)	(9,3)	O	(5,2)	(3,11)
(10,7)	(10,7)	(9,3)	(12,9)	(12,4)	(8,7)	(5,2)	(8,6)	(10,6)	(3,11)	O	(9,10)	(3,2)	(5,11)
(12, 4)	(12,4)	(8,7)	(10,6)	(12,9)	(10,7)	(3,11)	(9,10)	(8,6)	(9,3)	(5,2)	(3,2)	(5,11)	O
(12, 9)	(12,9)	(10,7)	(8,6)	(10,6)	(12,4)	(9,3)	(3,2)	(9,10)	(8,7)	(3,11)	(5,11)	O	(5,2)

Tabela 7 – Tábua de somas dos pontos $\mathbb{E} : y^2 = x^3 + 3X + 7$ sobre $\mathbb{Z}_{13}$

5 CRIPTOGRAFIA UTILIZANDO CURVAS ELÍPTICAS

Dois agentes em uma comunicação, digamos o Emissor ou codificador e o Receptor ou decodificador (por exemplo, um cliente e seu banco), vão usar uma curva elíptica $\mathbb{E}$ sobre um corpo $\mathbb{Z}_p$, p primo, dada por uma equação de Weierstrass:

$$y^2 \equiv x^3 + ax + b, \qquad a, b \in \mathbb{Z}_p.$$

Escolhem um ponto chave $P \in \mathbb{E}(\mathbb{Z}_p)$. Nesse sistema criptográfico, a curva $\mathbb{E}$, o primo p e o ponto P são chaves públicas.

Cada agente escolhe uma chave secreta que é um número inteiro: o Emissor escolhe n e o Receptor escolhe m.

O Emissor calcula $A = nP \in \mathbb{E}(\mathbb{Z}_p)$ e envia ao Receptor. O Receptor calcula $B = mP \in \mathbb{E}(\mathbb{Z}_p)$ e envia ao Emissor. Como o meio de comunicação pode ser inseguro, essas chaves são públicas.

O Emissor calcula $S = nB$ enquanto o Receptor calcula mA. Como:

$$nB = n(mP) = m(nP) = mA$$

então os dois agentes encontram o mesmo ponto $S \in \mathbb{E}(\mathbb{Z}_p)$. Esta é a chave secreta que eles agora dividem e vão usar para codificar e decodificar uma mensagem.

Nesse sistema, a mensagem deve ser um conjunto de pontos de $\mathbb{E}(\mathbb{Z}_p)$. Seja M um ponto de uma mensagem. O Emissor codifica a mensagem fazendo:

$$C(M) = M \oplus S$$

e envia $N = C(M)$ ao Receptor. O Receptor decodifica a mensagem fazendo a operação contrária:

$$D(N) = N \ominus S$$

A decodificação claramente funciona pois:

$$D(N) = N \ominus S = C(M) \ominus S = M \oplus S \ominus S = M \oplus S \oplus (-S) = M \oplus O = M.$$

Vamos dar um exemplo para ilustrar esse sistema. Um cliente, o Emissor, vai enviar uma mensagem numérica para um banco, o Receptor. O sistema usado será dado pela curva elíptica $\mathbb{E} : y^2 = x^3 + 3x + 7$ sobre $\mathbb{Z}_{13}$ cujo conjunto $\mathbb{E}(\mathbb{Z}_{13})$ e a sua tabela de somas foram dados na seção anterior. Além disso, escolhe-se o ponto chave $P = (12, 9) \in \mathbb{E}(Z_{13})$.

Como a mensagem é numérica e o sistema funciona para pontos de $\mathbb{E}(\mathbb{Z}_{13})$, vamos usar a tabela 8 que atribui a cada algarismo um ponto.

Algarismo	0	1	2	3	4	5	6	7	8	9
Ponto	(3,2)	(3,11)	(5,2)	(5,11)	(8,6)	(8,7)	(9,3)	(9,10)	(10,6)	(10,7)

Tabela 8 – Algarismos por pontos de $\mathbb{E}(\mathbb{Z}_{13})$

O Emissor escolhe a chave secreta $n = 5$. Usando a tabela 7 de somas, calcula $5P$ fazendo:

$$2P = P \oplus P = (12, 9) \oplus (12, 9) = (5, 2)$$

$$3P = 2P \oplus P = (5, 2) \oplus (12, 9) = (10, 6)$$

$$5P = 2P \oplus 3P = (5, 2) \oplus (10, 6) = (8, 6).$$

Ele então envia $A = nP = (8, 6)$ para o Receptor.

O Receptor escolhe a chave secreta $m = 7$ e calcula $7P$:

$$2P = P \oplus P = (12, 9) \oplus (12, 9) = (5, 2)$$

$$4P = 2P \oplus 2P = (5, 2) \oplus (5, 2) = (3, 11)$$

$$6P = 4P \oplus 2P = (3, 11) \oplus (5, 2) = (9, 3)$$

$$7P = 6P \oplus P = (9, 3) \oplus (12, 9) = (9, 10).$$

Ele então envia $B = mP = (9, 10)$ para o Emissor.

O Emissor, com a sua chave secreta $n = 5$ calcula nB, fazendo:

$$2B = B \oplus B = (9, 10) \oplus (9, 10) = (12, 9)$$

$$3B = 2B \oplus B = (12, 9) \oplus (9, 10) = (8, 7)$$

$$5B = 2B \oplus 3B = (12, 9) \oplus (8, 7) = (3, 2).$$

Assim ele obtém a chave $S = (3, 2)$.

O Receptor, com a sua chave secreta $m = 7$ calcula mA, fazendo:

$$2A = A \oplus A = (8, 6) \oplus (8, 6) = (10, 7)$$

$$4A = 2A \oplus 2A = (10, 7) \oplus (10, 7) = (9, 10)$$

$$6A = 4A \oplus 2A = (9, 10) \oplus (10, 7) = (3, 11).$$

$$7A = 6A \oplus A = (3, 11) \oplus (8, 6) = (3, 2).$$

Assim ele também obtém a chave $S = (3, 2)$.

Suponha que a mensagem seja o número do CPF do cliente que é igual a 5378916044. Ele então usa a tabela 8 para converter cada algarismo em um ponto de $\mathbb{E}(\mathbb{Z}_{13})$ e a mensagem se transforma na sequência de pontos $M_1 M_2 \dots M_{10}$ onde:

$$M_1 = (8, 7), M_2 = (5, 11), M_3 = (9, 10), M_4 = (10, 6), M_5 = (10, 7), M_6 = (3, 11),$$

$$M_7 = (9,3), M_8 = (3,2), M_9 = (8,6), M_{10} = (8,6).$$

O Emissor converte cada ponto da mensagem fazendo:

$$N_1 = C(M_1) = M_1 \oplus S = (8,7) \oplus (3,2) = (3,11),$$

$$N_2 = C(M_2) = M_2 \oplus S = (5,11) \oplus (3,2) = (9,10),$$

$$N_3 = C(M_3) = M_3 \oplus S = (9,10) \oplus (3,2) = (10,6),$$

$$N_4 = C(M_4) = M_4 \oplus S = (10,6) \oplus (3,2) = (12,4),$$

$$N_5 = C(M_5) = M_5 \oplus S = (10,7) \oplus (3,2) = (9,3),$$

$$N_6 = C(M_6) = M_6 \oplus S = (3,11) \oplus (3,2) = O,$$

$$N_7 = C(M_7) = M_7 \oplus S = (9,3) \oplus (3,2) = (5,2),$$

$$N_8 = C(M_8) = M_8 \oplus S = (3,2) \oplus (3,2) = (8,6),$$

$$N_9 = C(M_9) = M_9 \oplus S = (8,6) \oplus (3,2) = (12,9),$$

$$N_{10} = C(M_{10}) = M_{10} \oplus S = (8,6) \oplus (3,2) = (12,9).$$

Assim ele envia a mensagem codificada $N_1N_2 \ldots N_{10}$ para o Receptor.

O Receptor decodifica a mensagem aplicando $D(N_i) = N_i \ominus S = N_i \oplus (-S)$ para cada $i = 1, 2, \ldots 10$. Observe que, em $\mathbb{E}(\mathbb{Z}_{13})$, $-S = (3,11)$. Assim:

$$D(N_1) = N_1 \oplus (-S) = (3,11) \oplus (3,11) = (8,7) = M_1,$$

$$D(N_2) = N_2 \oplus (-S) = (9,10) \oplus (3,11) = (5,11) = M_2,$$

$$D(N_3) = N_3 \oplus (-S) = (10,6) \oplus (3,11) = (9,10) = M_3,$$

$$D(N_4) = N_4 \oplus (-S) = (12,4) \oplus (3,11) = (10,6) = M_4,$$

$$D(N_5) = N_5 \oplus (-S) = (9,3) \oplus (3,11) = (10,7) = M_5,$$

$$D(N_6) = N_6 \oplus (-S) = O \oplus (3,11) = (3,11) = M_6,$$

$$D(N_7) = N_7 \oplus (-S) = (5,2) \oplus (3,11) = (9,3) = M_7,$$

$$D(N_8) = N_8 \oplus (-S) = (8,6) \oplus (3,11) = (3,2) = M_8,$$

$$D(N_9) = N_9 \oplus (-S) = (12,9) \oplus (3,11) = (8,6) = M_9,$$

$$D(N_{10}) = N_{10} \oplus (-S) = (12,9) \oplus (3,11) = (8,6) = M_{10}.$$

Finalmente, usando a tabela 8, o Receptor converte a mensagem $M_1M_2 \ldots M_{10}$ para o número 5378916044, recuperando a mensagem original.

Como vimos, $\mathbb{E}$, p e P são chaves públicas enquanto as chaves secretas são n e m. Como $A = nP$ e $B = mP$ podem ser interceptados, a segurança desse sistema criptográfico depende da incapacidade do interceptador de encontrar n e m conhecendo A, B e P.

No nosso exemplo, com o objetivo de ilustrar o mecanismo da criptografia usando a álgebra de curvas elípticas, trabalhamos com uma versão simplificada e números pequenos. O leitor deve ter percebido que, conhecida toda a tabela 7 de somas, é possível encontrar n e m. Basta somar P com P repetidamente, determinando a sequência P, $2P$, $3P, \ldots$, até obter $5P = A = (8, 6)$ e $7P = B = (9, 10)$. Então, $n = 5$ e $m = 7$. Porém, nas implementações comerciais, trabalha-se com valores muito grandes para o primo p, sendo impraticável conhecer a tabela de soma em $\mathbb{E}(\mathbb{Z}_p)$. Coutinho, em [2], cita alguns desses primos usados em sistemas comerciais de criptografia sendo um deles:

$$p = 1900871281664822113126851573935413975471896789968515493666638539$$

$$088027103802104498957191261465571.$$

Nessas implementações, usa-se essencialmente todo o poder de simplificação de cálculos da álgebra da congruência módulo p como também o poder da tecnologia da computação.

6 CONCLUSÃO E CONSIDERAÇÕES FINAIS

Esse trabalho apresenta noções de criptografia via curvas elípticas, tendo como proposta o aprofundamento de conteúdos do ensino médio. A criptografia possui o atrativo, de ser um tema atual de grande importância na segurança da informação. Hoje, ela é uma ferramenta de segurança amplamente utilizada nos meios de comunicação e consiste basicamente na transformação de determinado dado ou informação a fim de ocultar seu real significado. Esperamos que o tema trabalhado seja um incentivador ao estudo dos conteúdos comuns ao ensino médio, assim como a introdução de novos conteúdos tornando assim uma ferramenta a mais para o professor de matemática. Quando mostramos aos alunos outras áreas em que são aplicados os conhecimentos em matemática, automaticamente renovamos o interesse desses alunos. Enfim, esperamos dessa forma estar contribuindo para a melhoria da qualidade da educação.

REFERÊNCIAS

[1] BARBOSA, Júlio Cesar. **Criptografia de Chave Pública Baseada em Curvas Elípticas**. Rio de Janeiro: 2003.

[2] COUTINHO, Severino. **Criptografia**. Rio de Janeiro: Impa, 2015 MEC/SEF, 1997.

[3] CORREIA JÚNIOR, Sergio dos Santos, **Criptografia via curvas elípticas.** Rio de Janeiro: UNIRIO, 2013.

[4] CYLK, **Criptografia você deveria conhecer**. Disponível em: <http://cylk.com.br> (Acesso em: 29/07/2016).

[5] HEFEZ, Abramo. **Iniciação à Aritmética**. Rio de Janeiro: Impa, 2015.

[6] HEFEZ, Abramo. **Aritmética**. SBM (Coleção PROFMAT), 2014.

[7] HOFFSTEIN, Jeffrey; PIPHER, Jill; SILVERMAN, Joseph H. **An Introduction to Mathematical Cryptography**. New York: Springer, 2008.

[8] **História da computação**. Disponível em: <http://www.dsc.ufcg.edu.br> (Acesso em: 29/07/2016).

[9] SALOMÃO, Rodrigo, **Um passeio pelo mundo secreto das curvas elípticas - Aula 3**. UFF, 2011.