2016: DISSERTAÇÃO DE MESTRADO
Mestrado Profissional em Matemática - PROFMAT, Universidade Federal de São João Del-Rei - UFSJ
Sociedade Brasileira de Matemática - SBM

# MÉTODO ELGAMAL DE CRIPTOGRAFIA E AS CURVAS ELÍPTICAS

José Helvésio Rosa Júnior [1]
Fábio Alexandre de Matos[2]

**Resumo:** Apresentamos neste trabalho a Função de Euler, o Teorema de Euler, o Método Elgamal de Codificação e um breve estudo sobre Curvas Elípticas e suas aplicações em Criptografia. Tais teoremas, definições e métodos possibilitaram uma elevação substancial no nível de proteção de dados, tão necessária em nosso cotidiano.

**Palavras-chave:** Criptografia, Curvas Elípticas, Método Elgamal, Função de Euler.

## 1 Introdução

O aperfeiçoamento e a necessidade de utilização da criptografia foram ampliados com o início da Era da Informação (ou Era Digital - cujo início pode ser estabelecido como o fim do século XX). Os diversos sistemas e produtos que surgem com início deste novo período na história humana estão propiciando uma diversidade de possibilidades baseadas na troca rápida de informações. Inerente às trocas está a necessidade de proteger os componentes da informação. Dentro deste contexto, a criptografia, que figura como uma aliada na proteção das inúmeras informações que circulam pelos diversos meios, tem se tornado objeto de compreensão de poucos e a beleza dos conceitos matemáticos envolvidos atua como desconhecida, apesar de extremamente necessária.

O advento dos métodos de criptografia utilizados atualmente só foi possível a partir de conceitos elementares da Teoria dos Números - ramo da Matemática que estuda propriedades dos números em geral, e em particular dos números inteiros. A Função Totiente (ou Função de Euler) (Definição 6) e o Teorema de Euler (Teorema 3), dentre outros, são frutos deste Ramo desenvolvidos a mais de dois séculos. Reunidos, alicerçam processos brilhantes de codificação, como exemplo está o Método Elgamal, apresentado em 1985 pelo Criptógrafo Egípcio Taher Elgamal. Este método, quando aplicado sobre curvas elípticas, apresenta uma enorme eficiência já que aumenta a proteção quando da transmissão eletrônica de dados.

[1]Aluno de Mestrado do PROFMAT, Turma 2014, Universidade Federal de São João Del-Rei - UFSJ, helvesiomat@yahoo.com.br
[2]Professor orientador, Departamento de Matemática e Estatística - DEMAT, UFSJ, matos@ufsj.edu.br

O aumento desta proteção é atingido quando é utilizada a definição da adição sobre Curvas Elípticas. Somar, então, passa a ser um 'caminhar aleatório' - Koblitz (1994) - sobre um conjunto finito de pares ordenados com coordenadas inteiras que satisfazem certas expressões. Como convite ao leitor, sugerimos comparar como o método de criptografia citado é desenvolvido em cada uma das duas maneiras apresentadas - aritmética modular e sobre curvas elípticas - enfatizando as peculiaridades sobre a segunda.

Apresentar uma base teórica completa foge ao objetivo deste texto, mas é algo que pode ser satisfeito na bibliografia referenciada. Entretanto, por intermédio de uma linguagem simples e com exemplos numéricos, acreditamos que esta obra possa servir como uma apresentação do tema e consequentemente possa instigar o interesse pela aritmética modular e demais assuntos decorrentes além de tentar provocar uma reflexão sobre os questionamentos e eventuais respostas que podem ser construídas por professores, em sala de aula, sobre o amadurecimento e a aplicabilidade da Matemática no dia a dia.

Quando o assunto é cotidiano, é impossível não perceber como diversas tarefas, essenciais ou não, são efetuadas por intermédio de dispositivos eletrônicos que trocam os mais variados tipos de informação. Dentro desta realidade surge a necessidade de um tráfego rápido de mensagens, mas com privacidade e segurança. Inseridos neste contexto estão alunos dos mais diversos níveis de ensino, seus *smartphones*, computadores, milhares de aplicativos e uma pergunta - como proteger dados? A resposta almejada foi alcançada e tem sido constantemente aprimorada graças à Matemática.

# 2 Método Elgamal de Criptografia

## 2.1 O Método

O Método Elgamal de criptografia foi apresentado pela primeira vez em um artigo [1] em 1985 pelo Criptógrafo Egípcio Taher Elgamal. O processo utiliza chaves públicas e privadas cujas definições apresentamos a seguir:

**Definição 1** *Uma Chave Pública é uma parte do protocolo de criptografia composta por itens que podem ser divulgados sem qualquer tipo de restrição.*

**Definição 2** *Uma Chave Privada é uma parte do protocolo de criptografia composta por itens que só podem ser do conhecimento do(s) transmissor(es) e do(s) receptor(es) da informação codificada.*

Uma, dentre outras características do método, está a transformação de cada parte de uma mensagem em um par de dados codificados. Sua segurança está baseada no Problema do Logaritmo Discreto, ou seja, está estruturada sobre a enorme dificuldade de encontrar o expoente $a$ sabendo apenas o resto da divisão de $b^a$ por um número primo quando os cálculos são realizados utilizando números formados por mais de 200 algarismos.

## 2.2 Embasamento Teórico

Diversos processos de criptografia tem se baseado na Aritmética Modular - uma ferramenta importantíssima da Teoria dos Números. Devido a riqueza deste conteúdo, assumiremos a familiaridade do leitor quanto às definições elementares e a simbologia. Indicamos [4] - Apostila 7 do Programa de Iniciação Científica da Olimpíada Brasileira de Matemática das Escolas Públicas - e [5] como fontes iniciais de consulta. Ressaltaremos abaixo algumas definições, teoremas e demonstrações que propiciam a funcionalidade da codificação e posteriormente decodificação abordados na subseção [2.3]:

**Definição 3** *Um Sistema Completo de Resíduos é um conjunto formado por todos os m elementos representantes de uma classe de equivalência módulo m.*

**Definição 4** *Uma Função aritmética é uma função que está definida para todos os inteiros positivos.*

**Definição 5** *Uma função aritmética é dita multiplicativa quando* $f(\mathbf{a} \cdot \mathbf{b}) = f(\mathbf{a}) \cdot f(\mathbf{b})$ *para qualquer par de inteiros positivos* $\boldsymbol{a}$ *e* $\boldsymbol{b}$*, tais que mdc (*$\mathbf{a}$*,* $\mathbf{b}$*) = 1.*

**Definição 6** *A Função Totiente, ou Função de Euler (denotada por* $\phi$*) é uma função aritmética que informa a quantidade de números inteiros positivos relativamente primos a* $n \in \mathbb{N}$*, ou seja*

$$\phi(n) = \#\{a \in \mathbb{Z} | 1 \leq a < n, mdc(a, n) = 1\}.$$

**Exemplo 1** $\phi(10) = 4$*, pois* $\{1, 3, 7 \text{ e } 9\}$ *são os quatro números relativamente primos a 10.*
**Observação:** $\phi(1) = 1$ *pois mdc(1,1)=1.*

**Teorema 1** *A Função de Euler é uma função aritmética multiplicativa.*

Sejam $\boldsymbol{a}$ e $\boldsymbol{b} \in \mathbb{Z}$, positivos de maneira que mdc($\boldsymbol{a}$,$\boldsymbol{b}$)=1. É necessário mostrar que $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.

Se $\boldsymbol{a}$=$\boldsymbol{b}$=1 é verdadeiro pois $\phi(1) = 1$ então $\phi(a \cdot b) = \phi(a) \cdot \phi(b) = 1 \cdot 1 = 1$.

Se $\mathbf{a} > 1$ e $\mathbf{b} > 1$, podemos escrever $\mathbf{a} \cdot \mathbf{b}$ em $\boldsymbol{a}$ colunas, da seguinte maneira:

| | | | | | |
|---|---|---|---|---|---|
| 1 | 2 | ... | n | ... | $\boldsymbol{a}$ |
| $\boldsymbol{a}$ + 1 | $\boldsymbol{a}$ + 2 | ... | $\boldsymbol{a}$ + n | ... | 2·$\boldsymbol{a}$ |
| 2·$\boldsymbol{a}$ + 1 | 2·$\boldsymbol{a}$ + 2 | ... | 2·$\boldsymbol{a}$ + n | ... | 3·$\boldsymbol{a}$ |
| ... | ... | ... | ... | ... | ... |
| ($\boldsymbol{b}$ - 1)·$\boldsymbol{a}$ + 1 | ($\boldsymbol{b}$ - 1)·$\boldsymbol{a}$ + 2 | ... | ($\boldsymbol{b}$ - 1)·$\boldsymbol{a}$ + n | ... | $\boldsymbol{b}$·$\boldsymbol{a}$ |

Todos os inteiros da $n$-ésima coluna serão primos com $\boldsymbol{a}$ se, e somente se, mdc($\boldsymbol{a}$, $n$)=1.

Como mdc(x·$\boldsymbol{a}$+$n$, $\boldsymbol{a}$)=mdc($n$, $\boldsymbol{a}$), evidentemente, a quantidade de inteiros primos com $\boldsymbol{a}$ é definida por $\phi(\mathbf{a})$, então há $\phi(\mathbf{a})$ colunas cujos inteiros que as compõe são todos primos com $\boldsymbol{a}$.

Analisando cada uma destas $\phi(\mathbf{a})$ colunas, verifica-se um sistema completo de resíduos, pois são compostas por **b** elementos todos incongruentes 2 a 2. Assim, há $\phi(\mathbf{b})$ elementos relativamente primos com **b**, logo há $\phi(\mathbf{a}) \cdot \phi(\mathbf{b})$ primos com $a \cdot b$, então $\phi(\mathbf{a} \cdot \mathbf{b}) = \phi(\mathbf{a}) \cdot \phi(\mathbf{b})$.

**Teorema 2** *Se $p > 1$ é um número primo, então $\phi(\mathbf{p}) = \mathbf{p} - 1$.*

*Como $\boldsymbol{p}$ é primo, todos os inteiros positivos menores que $\boldsymbol{p}$ é primo com $\boldsymbol{p}$, logo $\phi(\mathbf{p}) = \mathbf{p} - 1$. A recíproca é verdadeira pois, se $\boldsymbol{p}$ fosse composto, ele possuiria um divisor $1 < n < p$ tal que $p = n \cdot a$, o que implicaria em $\phi(\mathbf{p}) < \mathbf{p} - 1$.*

**Teorema 3** *(Teorema de Euler) Sejam os números a e n, com n inteiro positivo, tais que mdc(a,n)=1, a seguinte relação de congruência é válida:*

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

Para a prova, é necessário estabelecer o Lema 2.2:
lemaLema
Sejam $a$ e $n$> 1 inteiros tais que mdc($a$, $n$)=1. Se $a_1, a_2, ..., a_{\phi(n)}$ são inteiros positivos menores que $n$ e que são relativamente primos com $n$, então cada um dos inteiros $a \cdot a_1, a \cdot a_2, ..., a \cdot a_{\phi(n)}$ é congruente módulo $n$ a um dos inteiros $a_1, a_2, ..., a_{\phi(n)}$ (não necessariamente nesta ordem em que aparecem).

Os inteiros $a \cdot a_1, a \cdot a_2, ..., a \cdot a_{\phi(n)}$ são mutuamente incongruentes módulo $n$, pois, se $a \cdot a_i \equiv a \cdot a_j \pmod{n}$, com $1 \leq i \leq j \leq \phi(n)$.

Como mdc($a$, $n$)=1, podemos utilizar o inverso multiplicativo do fator comum $a$ o que resulta em $a_i \equiv a_j \pmod{n} \Leftrightarrow n|(a_i - a_j)$, o que é impossível visto que $(a_i - a_j) < n$.

Por outro lado, como o mdc($a_i$, n)=1, $i = 1, 2, ..., \phi(n)$ e o mdc($a$, $n$)=1, então

$$\text{mdc}(a \cdot a_i,\ n)=1.$$

Mas, pelo algoritmo da divisão, $a \cdot a_i = n \cdot q_i + r_i, 0 \leq r_i \leq n$, que implica em

$$a \cdot a_i \equiv r_i \pmod{n}, \text{ com } 0 \leq r_i \leq n$$

portanto, mdc($r_i$, n)= mdc($a \cdot a_i$, n)=1 de modo que $r_i$ é um dos inteiros $a_1, a_2, ..., a_{\phi(n)}$, isto é, cada um dos inteiros $a_1, a_2, ..., a_{\phi(n)}$ é congruente módulo $n$ a um único dos inteiros $a_1, a_2, ..., a_{\phi(n)}$, em uma certa ordem.
Reunidas as condições, segue agora a prova do Teorema de Euler:
A verificação para $n = 1$ é trivial, pois $a^{\phi(1)} \equiv 1 \pmod{1}$. Supondo, pois $n > 1$, e sejam

$a_1, a_2, ..., a_{\phi(n)}$ os inteiros positivos menores que $n$ e relativamente primos a $n$. Como mdc $(a, n)$=1, então, pelo Lema 2.2, os inteiros $a \cdot a_1, a \cdot a_2, ..., a \cdot a_{\phi(n)}$ são congruentes módulo $n$ aos inteiros $a_1, a_2, ..., a_{\phi(n)}$ em uma certa ordem

$$a \cdot a_1 \equiv {a_1}^*, a \cdot a_2 \equiv {a_2}^*, ..., a \cdot a_{\phi(n)} \equiv {a_{\phi(n)}}^*$$

onde ${a_1}^*, {a_2}^*, ..., {a_{\phi(n)}}^*$ denotam os inteiros $a_1, a_2, ..., a_{\phi(n)}$ em uma certa ordem. Multiplicando ordenadamente todas essas $\phi(n)$congruências, obtemos $(a \cdot a_1) \cdot (a \cdot a_2) \cdot ... \cdot (a \cdot a_{\phi(n)})$ (mod $n$) ou seja, $a^{\phi(n)} \cdot (a_1 \cdot a_2 \cdot ... \cdot a_{\phi(n)}) \equiv a_1 \cdot a_2 \cdot ... \cdot a_{\phi(n)}$ (mod $n$). Cada um dos inteiros $a_1, a_2, ..., a_{\phi(n)}$ é relativamente primo a $n$, e quando multiplicados por seus respectivos inversos geram, então, a congruência em questão, $a^{\phi(n)} \equiv 1$ (mod $n$).

## 2.3 As Etapas do Método

Sintetizando o processo de criptografia em três etapas, temos:

[I - ]Determinação das Chaves:
Para gerar as chaves é necessário:

1. (a) Definir um número primo $p$;
   (b) Definir um gerador $g \in \mathbb{Z}_p$;
   (c) Escolher aleatoriamente um inteiro $a$, tal que $1 \leq a \leq p-2$ e determinar $g^a$ (mod $p$);

   Satisfeitos I-(a), I-(b), I-(c), a Chave Pública fica definida como o trio $(p, g, g^a)$ e a Chave Privada como sendo o inteiro $a$.

2. Codificação:
   De posse da chave pública, a codificação deve respeitar os seguintes passos, atentando para a definição abaixo:

   **Definição 7** *Uma Pré-codificação é a maneira pela qual transforma-se uma letra, ou qualquer outro componente de uma informação, em um número que será utilizado num processo de criptografia.*

   **Exemplo 2** *A letra 'A' pode se pré-codificada como o número 65, de acordo com a tabela ASCII* [3]*.*

   (a) Pré-codificar a mensagem $m$ para números inteiros de modo que $0 \leq m \leq (p-1)$;
   (b) Selecionar aleatoriamente um inteiro $k$ tal que $1 \leq k \leq (p-2)$; e

[3]Do inglês American Standard Code for Information Interchange; "Código Padrão Americano para o Intercâmbio de Informação". É um código binário (cadeias de bits: 0s e 1s) que codifica um conjunto de 128 sinais: 95 sinais gráficos (letras do alfabeto latino, sinais de pontuação e sinais matemáticos) e 33 sinais de controle, utilizando portanto apenas 7 bits para representar todos os seus símbolos.

(c) Determinar $\gamma = g^k \pmod{p}$ e $\delta = m \cdot (g^a)^k$.

Concluídos os passos II-(a), II-(b), II-(c), a mensagem $m$ passa a ser o par $(\gamma, \delta)$.

3. Decodificação:
Para decodificar a mensagem, após receber o par codificado $(\gamma, \delta)$ e de posse da chave privada $a$, o receptor deverá:

(a) Determinar $\gamma^{p-1-a} \pmod{p}$; e

(b) Recuperar a mensagem $m$ por intermédio de $(\gamma^{-a}) \cdot \delta \pmod{p}$.

A expressão abaixo apresenta uma equação modular que resume o processo de codificação e decodificação:

$$\mathrm{m} \equiv m \cdot (g^a)^k \cdot (g^k)^{p-1-a} \equiv m \pmod{p}. \quad (1)$$

Um leitor mais atento pode se perguntar como calcular o passo III-(a). A resposta para esta pergunta é facilmente respondida pela utilização conjunta dos Teoremas 2 e 3:

- Pelo Teorema 2, $\phi(\mathbf{p}) = \mathbf{p} - 1$ logo temos $\gamma^{p-1-a} = \gamma^{\phi(\mathbf{p})-a} = \gamma^{\phi(\mathbf{p})} \cdot \gamma^{-a}$; e
- Pelo Teorema de Euler temos $\gamma^{\phi(\mathbf{p})} = 1$, então $\gamma^{\phi(\mathbf{p})} \cdot \gamma^{-a} = 1 \cdot \gamma^{-a}$.

## 2.4 Um Exemplo

Supondo que o João pretende enviar, de maneira codificada, a letra 'A' para Maria. Utilizando o método em questão, ele escolhe $p = 17$, $g = 6$, $a = 5$(chave privada). Calcula então

$$g^a = 6^5 \pmod{17}$$
$$6^5 \equiv 7 \pmod{17}.$$

Assim, a chave pública (17,6,7) é determinada.

Pre-codificando a letra 'A' como o inteiro 10 (obtido pela numeração das letras em ordem alfabética começando por 10), João ainda escolhe aleatoriamente um inteiro $k = 11$ e determina

$$\gamma = g^k = 6^{11} \pmod{17}, \text{ então } \gamma = 5.$$

Determina também o $\delta = 10 \cdot (g^a)^k = 10 \cdot 7^{11} \equiv 4 \pmod{17}$. A mensagem a ser enviada, então, será o par $(5, 4)$.

Para decodificar a mensagem, Maria, ao receber o par $(5, 4)$, de posse da chave pública e da chave privada calcula $\gamma^{-a} \cdot \delta \pmod{17}$, ou seja:

$$5^{-5} \cdot 4 \pmod{17}.$$

Como $5^{-5} \equiv 7^5 \pmod{17}$ (pois $5^{-1}$=7, definição de inverso multiplicativo), Maria calcula:

$$5^{-5} \equiv 7^5 \cdot 4 \equiv 11 \cdot 4 \equiv 44 \equiv 10 \pmod{17},$$

encontrando a letra "A", conforme a pré-codificação.

# 3 Curvas Elípticas

Curvas Elípticas tem sido objeto de intenso estudo nos últimos dois séculos e gerando uma estrutura algébrica riquíssima quando o assunto é criptografia. O nome remete erroneamente à ideia de trabalhos com elipses. Na verdade trata-se de conceitos muitos mais profundos e densos, começando nas definições de Geometria Projetiva e Equações de Weierstrass. Recentemente (maio de 2016) o *WhatsApp Messenger*, aplicativo de mensagens mundialmente conhecido, foi atualizado e passou a oferecer conversas criptografadas baseando-se em um tipo específico de Curva Elíptica cuja implementação é explanada em [9]. Tal atualização é um excelente exemplo de contextualidade e aplicabilidade do tema.

Abaixo apresentamos a definição de curvas elípticas omitindo o embasamento teórico precedente por ser extremamente complexo e profundo mas que pode ser encontrado principalmente em [7] e [3].

**Definição 8** *Seja $K$ um corpo, com característica diferente de 2 e 3. E seja o polinômio cúbico $x^3 + ax + b$, com $a$ e $b$ pertencentes a este corpo, sem multiplicidade de raízes. Uma curva elíptica $E$ sobre $K$ é o conjunto de pares ordenados $(x, y)$ que satisfazem a expressão*

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

*além de um elemento denotado por $O$, chamado de ponto no infinito.*

A partir desta definição, uma aritmética muito específica é construída e, quando são utilizados pontos originados de um corpo finito, uma excelente condição é criada para codificações - uma quantidade finita de elementos e um 'caminhar aleatório" sobre eles. Neste caminhar, o ponto $O$ desempenhará o papel de elemento neutro por ocasião da adição de pontos conforme a definição 9.

Como exemplo, a Curva Elíptica $y^2 = x^3 - 36x$ sobre o conjunto dos números reais pode ser representada geometricamente pela figura (1) a seguir:

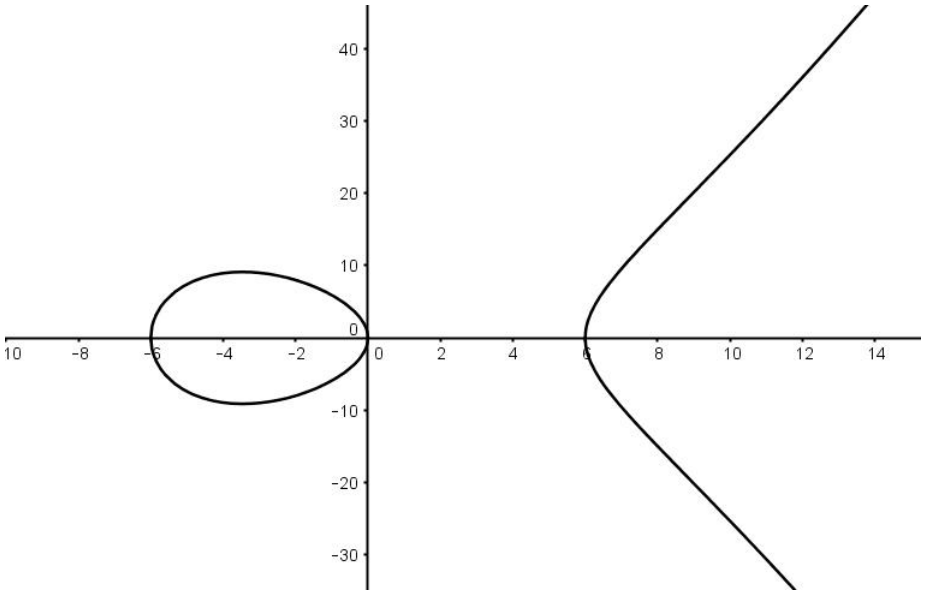


Figura 1: **Curva Elíptica $y^2 = x^3 - 36x$ sobre $\mathbb{R}$.**

## 3.1 Aritmética sobre Curvas Elípticas

**Definição 9** *Seja $E$ uma curva elíptica sobre $\mathbb{R}$ e sejam $P$ e $Q$ dois pontos pertencentes a $E$. O negativo de $P$ e a soma $P + Q$ são definidas conforme as seguintes regras:*

*[(i)]*

1. *Se o ponto $P$ é o ponto no infinito $O$, então o ponto $-P$ será o ponto $O$ e $P + Q$ será o ponto $Q$, ou seja, o ponto $O$ será o elemento neutro da adição. Para as próximas regras os pontos $P$ e $Q$ não serão considerados pontos no infinito.*

2. *O ponto negativo $-P$ é um ponto com a mesma abcissa porém com a ordenada simétrica ao ponto $P$, ou seja $-(x, y) = (x, -y)$. Obviamente, os pontos (x,y) e (x,-y) pertencerão à equação (2).*

   *A regra (3) se ampara na seguinte proposição:*

   ***Proposição 1:*** *Se $P$ e $Q$ tem coordenadas diferentes, então a reta $l = \overline{PQ}$ intersectará a curva em um único ponto $R$.*

   *Sejam $(x_1, y_1)$, $(x_2, y_2)$ e $(x_3, y_3)$ as coordenadas de $P$, $Q$ e $P + Q$, respectivamente. Seja ainda $y = \alpha x + \beta$ a equação da reta $l$ determinada pelos pontos $P$ e $Q$. Então $\alpha = \frac{(y_2 - y_1)}{(x_2 - x_1)}$ e $\beta = y_1 - \alpha x_1$.*
   *Um ponto $(x, \alpha x + \beta)$ pertencente a $l$ estará sobre a curva elíptica se, e somente se, $(\alpha x + \beta)^2 = x^3 + ax + b$. Assim, pelas Relações de Girard [4] , é necessário que o discriminante $\Delta = 4a^3 - 27b^2 \neq 0$ para que hajam 3 raízes reais e distintas e,*

[4]Relações entre os coeficientes e as raízes de um polinômio, determinadas pelo Matemático francês Albert Girard (1595-1632).

*consequentemente, haverá um único ponto de interseção para cada raiz da equação cúbica* $x^3 - (\alpha x + \beta)^2 + ax + b = 0$. *Duas raízes* $x_1$ *e* $x_2$ *já são conhecidas pois* $(x_1, \alpha x_1 + \beta)$ *e* $(x_2, \alpha x_2 + \beta)$ *são os pontos conhecidos* $P$ *e* $Q$ *sobre a curva. Como a soma das raízes é igual ao coeficiente* $\alpha^2$ *da segunda maior potência de* $x$*, determina-se, então, a terceira raiz como* $x_3 = \alpha^2 - x_1 - x_2$.

3. *Se* $P$ *e* $Q$ *tem coordenadas diferentes, então a reta* $l = \overline{PQ}$ *intersectará a curva em um único ponto* $R$*, assim a soma* $P + Q = -R$ *fica definida, ou seja, a adição de dois pontos será o ponto simétrico, em relação ao eixo das abcissas, da interseção da reta* $l$ *com a curva elíptica, conforme ilustrado na figura (2).*
   *Satisfeitas as devidas manipulações, as coordenadas do resultado de* $P+Q$ *são dadas por:*

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \quad (3)$$

$$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3). \quad (4)$$

*Se* $P = Q$*, o coeficiente angular da reta* $l$ *é obtido por intermédio da derivação implícita da equação (2), obtendo para as coordenadas do ponto* $P + P = 2P = (x_3, y_3)$*:*

$$x_3 = \left(\frac{3{x_1}^2 + a}{2y_1}\right)^2 - 2x_1 \quad (5)$$

$$y_3 = -y_1 + \left(\frac{3{x_1}^2 + a}{2y_1}\right)(x_1 - x_3) \quad (6)$$

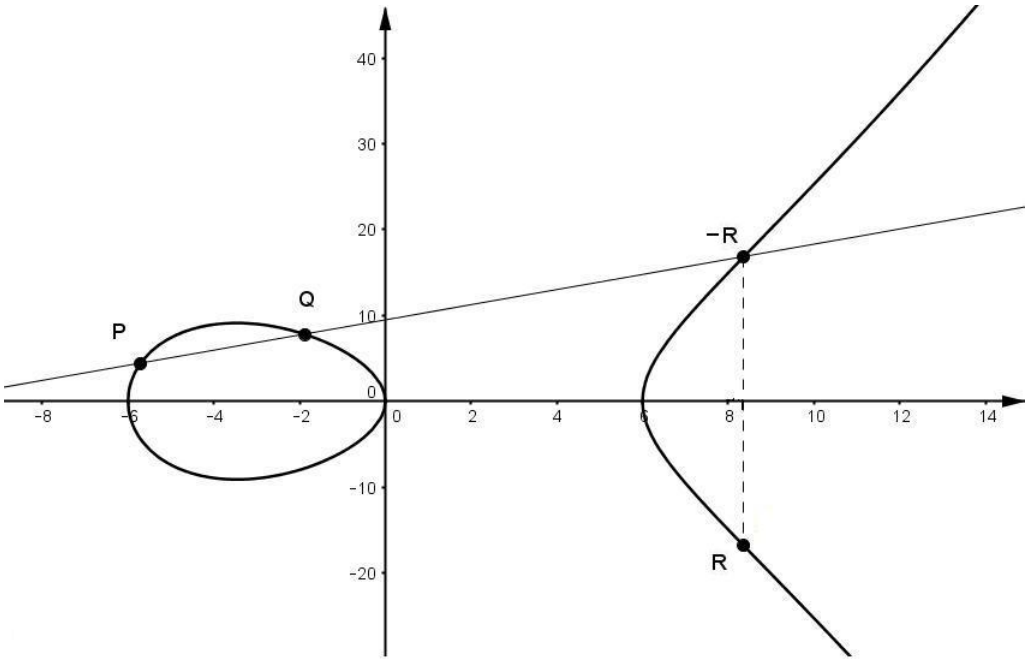


Figura 2: **Interpretação geométrica da adição sobre Curvas Elípticas.**

4. *Se $Q = -P$ (ou seja, se $Q$ e $P$ tem a mesma abcissa e ordenadas opostas) então é definido $P + Q = O$ (o ponto no infinito).*

5. *A última possibilidade para os valores das coordenadas ocorre se $P = Q$. Quando isto ocorre, a reta $l$ será tangente à curva em $P$ e intersectará a curva no ponto $R$ definido como $P + P = 2P = -R$ ou seja, o dobro de $P$ é o ponto simétrico a $R$ em relação ao eixo das abcissas, conforme ilustrado na figura (3).*

Uma observação importante é que a aritmética definida anteriormente, apesar de ter sido exemplificada sobre o conjunto dos números reais, é aplicada a qualquer corpo, não sendo diferente para $F_p$.

Para exemplificar as definições, serão encontrados os pontos $P + Q$ e $2P$, com $P = (-3, 9)$ e $Q = (-2, 8)$ sobre a curva elíptica $y^2 = x^3 - 36x$:

- Para $P + Q$:
  Substituindo os valores $x_1 = -3$, $y_1 = 9$, $x_2 = -2$ e $y_2 = 8$ nas equações (3) e (4) obtendo $x_3 = 6$ e $y_3 = 0$. A figura (4) ilustra o resultado da operação:

- Para $P + P = 2P$:
  Analogamente, substituindo os valores das coordenadas de $P$ nas equações (5) e (6) os valores $x_{2P} = \frac{25}{4}$ e $y_{2P} = \frac{-35}{8}$ são obtidos e ilustrados na figura (5).

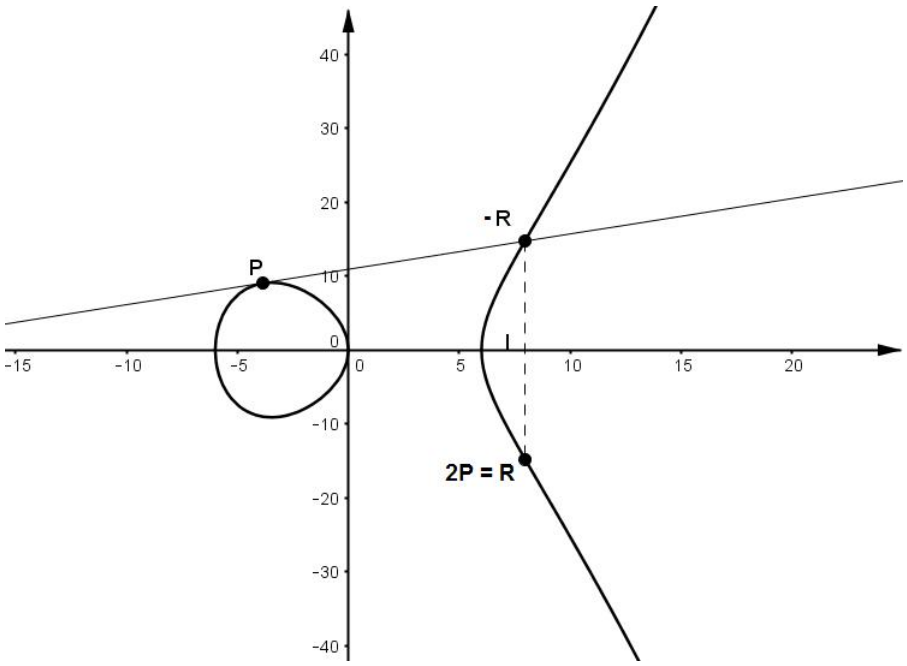


Figura 3: **Interpretação geométrica do dobro de P.**

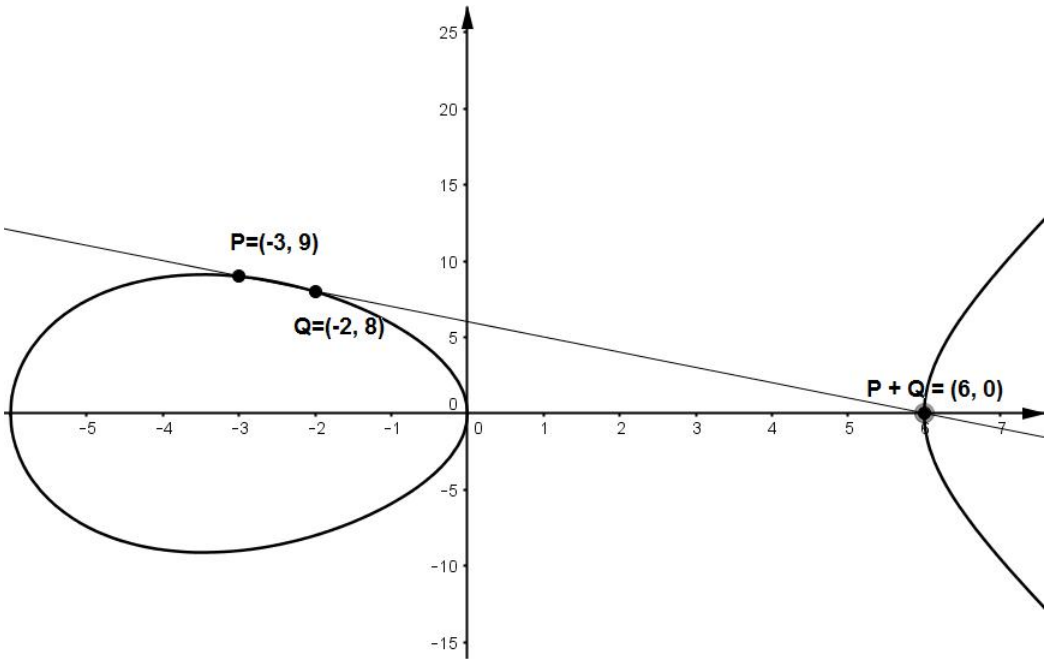


Figura 4: **Exemplo numérico da soma de P + Q sobre a curva elíptica** $y^2 = x^3 - 36x$**.**

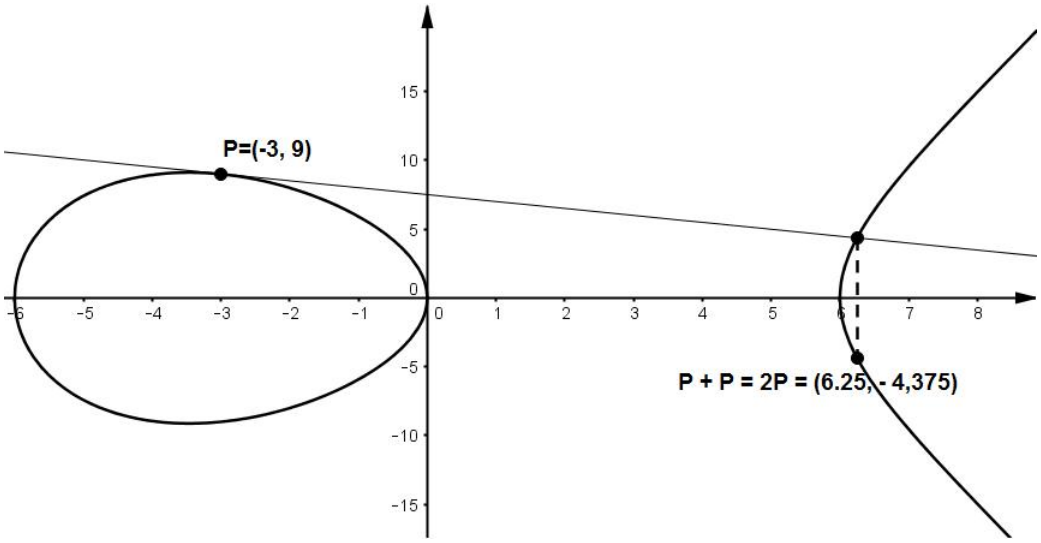


Figura 5: **Exemplo numérico da soma de $P + P = 2P$ sobre a curva elíptica $y^2 = x^3 - 36x$.**

## 3.2 Curvas Elípticas sobre Corpos Finitos

Curvas Elípticas sobre Corpos Finitos compõe uma estrutura muito rica para a criptografia pois surge daí um conjunto finitos de pontos sobre os quais a codificação e consequentemente a decodificação tornam-se possíveis. Por intermédio de algoritmos eficientes e protegidos pelas definições elencadas na subseção 3.1, os métodos criptográficos têm seu nível de segurança aumentado pois o Problema do Logaritmo Discreto torna-se muito mais difícil de ser resolvido.

Conforme a definição 8, uma Curva Elíptica sobre um Corpo Finito $F_p$, com $p$ um número primo é o conjunto de pontos $(x, y)$ que satisfazem a equação (2) módulo $p$, ou seja:

$$\mathrm{y}^2 \pmod p = x^3 + ax + b \pmod p \quad (7)$$

A quantidade de pontos encontrados satisfaz a inequação apresentada no Teorema de Hasse[5], $|N - (q + 1)| \leq 2\sqrt{q}$, onde $N$ é a quantidade de pontos e $q$ é a quantidade de elementos do Corpo Finito. Este fato consolida uma característica essencial para a criptografia - a quantidade finita de elementos.

Exemplificando, utilizaremos o corpo finito $F_5$ (cujos elementos são os números inteiros de 0 a 4). Sabemos que qualquer operação resultará em um número inteiro entre 0 e 4 se $p = 5$. Fazendo $a = 1$ e $b = 1$ em (7), os cálculos necessários para encontrar os pares $(x, y)$ que satisfazem a Curva Elíptica $y^2 = x^3 + x + 1$ sobre $F_5$ são os seguintes:

[5]Para mais detalhes sobre o Teorema de Hasse e sua demonstração, consulte [2].

| $x$ | $x^3+x+1$ | $x^3+x+1 \pmod 5$ |
|---|---|---|
| 0 | 1 | 1 |
| 1 | 3 | 2 |
| 2 | 11 | 1 |
| 3 | 31 | 1 |
| 4 | 69 | 4 |

**Cálculos das abcissas.**

| $y$ | $y^2$ | $y^2 \pmod 5$ |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 1 | 1 |
| 2 | 4 | 4 |
| 3 | 9 | 4 |
| 4 | 16 | 1 |

**Cálculos das ordenadas.**

E assim os pontos procurados são (0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,2) e (4,3). Apesar de não ser o caso exemplificar geometricamente as operações devido ao corpo utilizado, representando os pontos num plano cartesiano é possível perceber uma certa simetria na figura (6).

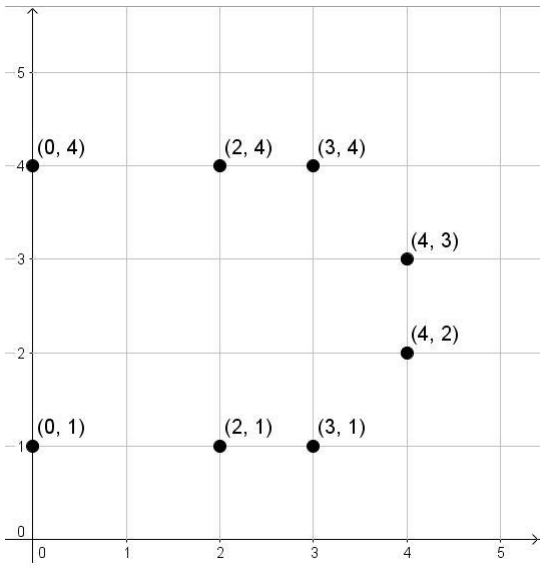


Figura 6: **Representação cartesiana da Curva Elíptica $y^2 = x^3 + x + 1$ sobre $F_5$.**

Cabe ressaltar como se dá a adição elencada na definição 9:

- Seja P(0,1), como obter P+P=2P? Conforme a regra (3) da subseção 3.1 temos P=P, então a abcissa será obtida por intermédio da regra (3)(4) da mesma subseção, com a atenção para o detalhe do inverso multiplicativo:

  $x_{2P} = \left(\frac{3\cdot 0^2+1}{2\cdot 1}\right)^2 - 2\cdot 0 = (1\cdot 2^{-1})^2 \pmod 5$, onde $2^{-1}$ é o inverso de 2 (mod 5).
  Portanto $x_{2P} = 3^2 \equiv 4 \pmod 5$.

  Para ober $y_{2P}$, utiliza-se a regra (3)(5) da subseção 3.1, ou seja:

  $y_{2P} = -1 + \left(\frac{3\cdot 0^2+1}{2\cdot 1}\right)(0-4) \pmod 5$.

$y_{2P} = -1 + 1 \cdot 2^{-1} \cdot (-4) \pmod 5$,
substituindo $2^{-1}$ por 3 e $-4$ por 1
$y_{2P} = -1 + 3 \cdot 1 \equiv 2 \pmod 5$.

Logo temos 2P=(4,2).

- Sejam P(0,1) e Q(4,2). Para obter abcissa e a ordenada do ponto P+Q basta utilizar as regras (3)(2) e (3)(3), ambos da subseção 3.1, respectivamente:

  $x_{P+Q} = \left(\frac{2-1}{4-0}\right)^2 - 0 - 4 \pmod 5$
  $x_{P+Q} = (1 \cdot 4^{-1})^2 - 4 \pmod 5$, substituindo $4^{-1}$ por 4,
  $x_{P+Q} = 4^2 - 4 = 12 \equiv 2 \pmod 5$
  e
  $y_{P+Q} = -1 + \left(\frac{2-1}{4-0}\right)(0 - 2) \pmod 5$
  $y_{P+Q} = -1 + 4(-2) \pmod 5$,
  substituindo $-2$ por 3,
  $y_{P+Q} = -1 + 4 \cdot 3 = 11 \equiv 1 \pmod 5$.

  Logo temos P+Q=(2, 1).

# 4 O Método Elgamal sobre Curvas Elípticas

O método, agora, possuirá uma diferença quando da *adição de pontos* ou da *multiplicação de um ponto por um escalar*, pois serão utilizadas as regras aritméticas apresentada na definição 9.

De maneira análoga à subseção (2.3), as etapas serão:

[I - ]Determinação das Chaves:
Para gerar as chaves é necessário:

1. (a) Escolher um número primo $p$ para um corpo $F_p$ e uma Curva Elíptica $E$;
   (b) Escolher um ponto $P$ que pertença ao conjunto de pontos de $E$ sobre $F_p$;
   (c) Escolher aleatoriamente um inteiro $a$, tal que $1 \leq a \leq p - 2$ e determinar um novo ponto $A = a \cdot P$ respeitando a multiplicação por escalar sobre curvas elípticas;

   Satisfeitos I-(a), I-(b), I-(c), a Chave Pública será composta por $(E, F_p, P, A)$ e a Chave Privada será apenas inteiro $a$.

2. Codificação:
   De posse da chave pública, a codificação deve respeitar os seguintes passos:

   (a) Pré-codificar a mensagem $m$ de modo a associá-la a um ponto $M$ pertencente à curva $E$ sobre $F_p$;

(b) Escolher um inteiro $k$ e computar $M_1 = k \cdot P$ atentando para a definição de multiplicação por escalar sobre curvas elípticas; e

(c) Somar $M_2 = M + k \cdot A$, atentando para a definição da soma de dois pontos em curvas elípticas.

Concluídos os passos II-(a), II-(b), II-(c), a mensagem $m$ passa a ser o par $(M_1, M_2)$.

3. Decodificação:
Para decodificar a mensagem, após receber o par codificado $(M_1, M_2)$ e de posse da chave privada $a$, o receptor deverá:

(a) Computar o ponto $M$ utilizando a equação $M = M_2 - a \cdot M_1$; e

(b) Obter a mensagem $m$ conforme a associação ao ponto $M$.

Assim, todo o processo pode ser resumido pelos passos abaixo:

$$M = M_2 - a \cdot M_1, \text{ como } M_2 = M + k \cdot A \text{ e } M_1 = k \cdot P$$
$$M = M + k \cdot A - a \cdot k \cdot P, \text{ fazendo } A = a \cdot P, \text{ temos}$$
$$M = M + k \cdot a \cdot P - a \cdot k \cdot P, \text{ então } M = M.$$

Exemplificando o método em questão, será utilizada a Curva Elíptica $E : y^2 = x^3+x+1$ sobre $F_{11}$ cujos pontos tem sua representação na figura 7 onde, mais uma vez, percebe-se uma simetria:

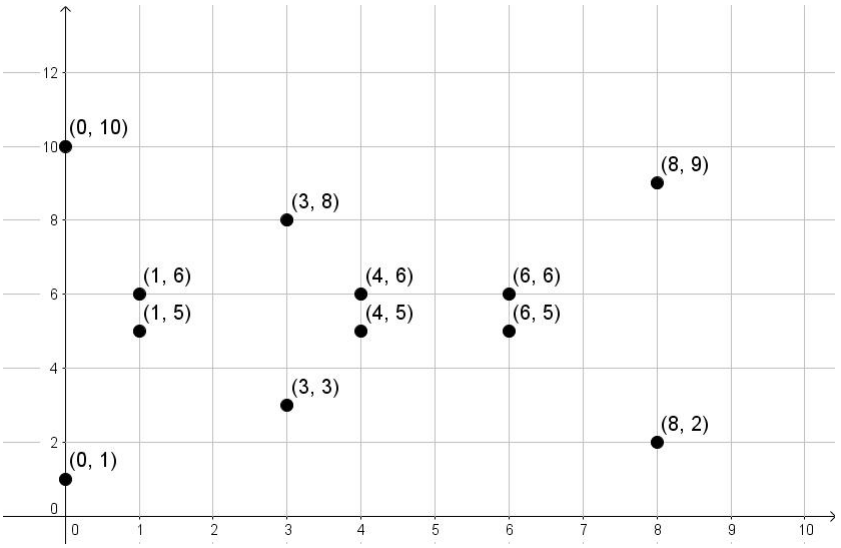


Figura 7: **Representação cartesiana da Curva Elíptica** $E : y^2 = x^3 + x + 1$ **sobre** $F_{11}$**.**

- Estabelecendo o ponto inicial $P = (1, 5)$.

- Escolhendo $a = 2$, calculamos $A = 2 \cdot P$:

$$x_A = \left(\frac{3 \cdot 1^2 + 1}{2 \cdot 5}\right)^2 - 2 \cdot 1 \equiv 3 \pmod{11}$$

$$y_A = -5 + \left(\frac{3 \cdot 1^2 + 1}{2 \cdot 5}\right)(1 - 3) \equiv 3 \pmod{11}$$

  Assim obtemos $A = (3, 3)$ e a chave pública será $[E, F_{11}, (1, 5), (3, 3)]$.

- Supondo que o transmissor desejasse transmitir a palavra 'FÉ', pré-codificada como 65 (conforme a numeração das letras do alfabeto - F=6, E=5) associada, então ao ponto $M = (6, 5)$. De posse da chave pública, determina $M_1 = k \cdot P$ e $M_2 = M + k \cdot A$. Escolhendo aleatoriamente $k = 3$ temos:
  Para o cálculo de $M_1$:
  Como $M_1 = 3 \cdot P = P + 2 \cdot P$, basta fazer $M_1 = (1, 5) + (3, 3)$:

$$x_{M1} = \left(\frac{3-5}{3-1}\right)^2 - 1 - 3 \pmod{11}$$
$$x_{M1} = \left(\frac{4}{4}\right) - 4 = 1 - 4 = -3 \equiv 8 \pmod{11}.$$

$$y_{M1} = -5\left(\frac{-2}{2}\right) \cdot (1 - 8) \pmod{11}$$
$$y_{M1} = -5(-1) \cdot (-7) \equiv 2 \pmod{11}.$$

Obtemos, então, o ponto $M_1 = (8, 2)$.

Para o cálculo de $M_2 = M + 3 \cdot A$, primeiro calcularemos $3 \cdot A$ sabendo que $3 \cdot A = A + 2 \cdot A$:
Para $2 \cdot A$:

$$x_{2A} = \left(\frac{3 \cdot 3^2 + 1}{2 \cdot 3}\right)^2 - 2 \cdot 3 \pmod{11}$$
$$x_{2A} = \left(\frac{28}{6}\right)^2 - 6$$
$$x_{2A} = (1)^2 - 6 = -5 \equiv 6 \pmod{11}$$

$$y_{2A} = -3 + (1) \cdot (3 - 6) \pmod{11}$$
$$y_{2A} = -3 - 3 = -6 \equiv 5 \pmod{11}$$

Portanto, $2A = (6, 5)$.

Para $3 \cdot A$:

$$3 \cdot (3, 3) = (3, 3) + (6, 5)$$

Para $x_{3A}$, calculamos:

$$x_{3A} = \left(\frac{5-3}{6-3}\right)^2 - 3 - 6 \pmod{11}$$
$$x_{3A} = \left(\frac{2}{3}\right)^2 - 9$$
$$x_{3A} = \left(\frac{4}{9}\right)^2 - 9 = 4 \cdot 9^{-1} - 9, \text{ onde } 9^{-1} = 5 \pmod{11}, \text{ então}$$
$$x_{3A} = 20 - 9 = 11 \equiv 0 \pmod{11}.$$

Para $y_{3A}$, calculamos:

$$y_{3A} = -3 + \left(\frac{2}{3}\right) \cdot (3 - 0) \pmod{11}$$
$$y_{3A} = -3 + 2 \cdot 3^{-1} \cdot 3 = -3 + 2 \cdot 4 \cdot 3 = 21 \equiv 10 \pmod{11}.$$

Agora, obtendo $M_2 = M + 3 \cdot A$:
Para $x_{M_2}$, calculamos:

$$x_{M_2} = \left(\frac{10-5}{0-6}\right)^2 - 6 - 0 \pmod{11}$$
$$x_{M_2} = \left(\frac{-5}{-6}\right)^2 - 6$$
$$x_{M_2} = \left(\frac{25}{36}\right) - 6$$
$$x_{M_2} = \left(\frac{3}{3}\right) - 6$$
$$x_{M_2} = (1) - 6 = -5 \equiv 6 (\text{mod } 11).$$

Para $y_{M_2}$, calculamos:

$$y_{M_2} = -10 + \left(\frac{6}{5}\right) \cdot (6) \pmod{11}$$
$$y_{M_2} = -10 + (6 \cdot 5^{-1}) \cdot (6), \text{ onde } 5^{-1} = 20 \pmod{11}$$
$$y_{M_2} = -10 + (6 \cdot 20) \cdot (6)$$
$$y_{M_2} = -10 + 60$$
$$y_{M_2} = 50 \equiv 6 \pmod{11}.$$

Desta forma, fica determinado $M_2 = (6, 6)$ e a mensagem a ser transmitida passa a ser a dupla de pontos [(8,2),(6,6)], descaracterizando completamente a palavra 'FÉ'.

- Para a decodificação, o receptor, de posse da mensagem codificada, calcula $M = M_2 - a \cdot M_1$. Os detalhes dos cálculos apresentados durante a codificação serão omitidos, mas podem ser confirmados na síntese abaixo:

$$M = M_2 - a \cdot M_1$$
$$M = (6, 6) - 2 \cdot (8, 2), \text{ onde podemos usar a definição e calcularmos}$$
$$M = (6, 6) + 2 \cdot (8, 9), \text{ fazendo } -(8, 2) = (8, -2) = (8, 9)$$
$$M = (6, 6) + (0, 1)$$
$$M = (6, 5), \text{ restaurando o ponto associado à mensagem original.}$$

Com esta estrutura matemática, este método consegue um nível de segurança utilizando chaves públicas e privadas muito menores que outros sistemas criptográficos.

> "Em 2003, a principal empresa ligada a ECC (CERTICOM) promoveu um teste para verificação de segurança do criptossistema baseado em curvas elípticas, que foi atacado por 10.000 computadores do tipo Pentium durante 540 dias seguidos. Nesse episódio foi quebrado um sistema com chave de 109 bits..." (Sangalli, 2012)

Entretanto, devido a presença de cálculos sofisticados, sua utilização é restrita a situações em que a complexidade de sua implementação não comprometa a rapidez do processo onde a criptografia está inserida.

# 5 Conclusão

A matemática, em alguns momentos durante a vida estudantil, pode ser uma linguagem muito densa e distante do que se aplica no cotidiano. Esta situação aliada à rapidez, volume e modo cujo o qual as informações e diversas opções de entretenimento se apresentam à sociedade têm dificultado o ensino de conceitos mais abstratos.

Dentro desta realidade, o Mestrado Profissional em Matemática (PROFMAT) desenvolvido na Universidade Federal de São João del Rei (UFSJ), por intermédio de seus professores e material didático, conduz o aluno participante a um mergulho sobre diversos temas, permitindo a percepção da complexidade, profundidade e beleza de vários ramos desta Ciência e, simultaneamente, incentiva o aprofundamento em temas que dificilmente seriam conhecidos fora de um ambiente universitário.

Ao escolher estudar, de maneira sutilmente mais atenciosa, como a Matemática está inserida em alguns ramos da Criptografia, percebe-se como é frutífero o estudo das diversas abstrações algébricas. Um Professor de Ensino Básico, ao tomar conhecimento destas teorias, é revestido de um amadurecimento que permite responder questionamentos em sala de aula e exemplificar aplicações de conceitos, mostrando que a densidade e complexidade de certos temas não diminuem sua beleza e importância para humanidade e ainda, ao eventualmente convidar seus alunos para uma análise histórica sobre como as técnicas de codificação evoluíram ao longo dos séculos, pode evidenciar a genialidade presente na dedicação de diversas personalidades e simultaneamente provocar uma nova percepção de heroísmo.

# Referências


[1] EL GAMAL, Taher . **A public key cryptosystem and a signature scheme based on discrete logarithms**. In Proceedings of CRYPTO 84 on Advances in cryptology, pages 10-18. Springer-Verlag, New York, Inc., 1985.

[2] SILVERMAN, J. **The Arithmetic of Elliptic Curves**, Springer-Verlag, New York, 1986.

[3] KOBLITZ, Neal. **A Course in Number Theory and Cryptography**, 2ªEd., Springer-Verlag, New York, 1994.

[4] COUTINHO, Severino. **Criptografia**, IMPA, Rio de Janeiro, 2015.

[5] VIDIGAL, Angela et al. **Fundamentos de Álgebra**, Belo Horizonte, UFMG, 2005.

[6] LIMA, Elon Lages **Curso de Análise, Volume 1**, 11ª Ed., IMPA, Rio de Janeiro, 2006.

[7] COHEN, Henri et al. **Handbook of Elliptic and Hyperelliptic Curve Cryptography**. Chapman  Hall/CRC, Florida, 2006.

[8] <https://www.certicom.com/-30-elliptic-curve-groups-over-fp>. Acesso em 20/03/2016.

[9] <https://www.whatsapp.com/security/>. Acesso em 05/06/2016.