

**CENTRO FEDERAL DE EDUCAÇÃO
TECNOLÓGICA DE MINAS GERAIS - CEFETMG**

Departamento de Matemática

Uma Pequena Introdução à Criptografia com Curvas elípticas

Belo Horizonte, 2026

Conteúdo

1	Introdução	2
2	Introdução as Curvas Algébricas e Suas Aplicações	3
2.1	Curvas afins	7
2.2	Aplicações do Teorema de Bézout - caso afim	12
2.3	Plano projetivo	12
3	Curvas Elípticas	16
3.1	A Regra Geométrica da Soma	18
3.2	Estrutura de Grupo	19
3.3	Regra Algébrica da Soma	20
3.3.1	Lei de Grupo para $E/K : y^2 = x^3 + ax + b, \text{char}(K) \neq 2, 3$	20
3.3.2	Lei de grupo para $E/\mathbb{F}_{2^m}$ não-supersingular : $y^2 + xy = x^3 + ax^2 + b$	23
3.3.3	Lei de grupo para $E/\mathbb{F}_{2^m}$ supersingular : $y^2 + cy = x^3 + ax + b$	24
3.4	Ordem do Grupo	24
3.5	Estrutura do Grupo	25
3.6	Representação por Coordenadas Homogêneas	26
4	Criptografia com Curvas elípticas	27
4.1	Troca de Chave Diffie-Hellman	27
4.2	Massey-Omura	28
4.3	O Problema do Logaritmo Discreto	31
4.4	O Criptossistema Menezes-Vanstone	37
4.5	Ataques	39

1 Introdução

Estas notas têm como objetivo apresentar uma introdução às curvas elípticas e à criptografia baseada nessas curvas, reunindo os principais conceitos necessários para compreender seus fundamentos matemáticos e suas aplicações. Inicialmente, são revisados tópicos de curvas algébricas, como curvas afins, o plano projetivo e resultados básicos da geometria algébrica. Em seguida, são estudadas as curvas elípticas, destacando sua estrutura de grupo, a lei de composição e diferentes representações. Na parte final, são introduzidos os principais protocolos criptográficos baseados em curvas elípticas, bem como o problema do logaritmo discreto e alguns algoritmos de ataque. Ao longo do texto, são apresentados exemplos resolvidos que ilustram os conceitos e algoritmos discutidos, tornando o conteúdo mais acessível ao leitor.

Embora o material tenha caráter introdutório, recomenda-se que o leitor possua conhecimentos prévios de Álgebra, especialmente de estruturas algébricas, como grupos, anéis e corpos. Familiaridade com teoria dos números e álgebra linear também é desejável, pois esses tópicos constituem a base matemática necessária para o estudo das curvas elípticas e de suas aplicações em criptografia.

2 Introdução as Curvas Algébricas e Suas Aplicações

Definição 1. Uma curva algébrica plana é o lugar dos pontos cujas coordenadas satisfazem uma equação do tipo $f(x, y) = 0$, onde f é um polinômio não constante.

As curvas algébricas planas começaram a serem estudadas há mais de dois mil anos, muito antes de usar o sistema de coordenadas em geometria. Elas eram estudadas de uma maneira mais primitiva, como lugares geométricos.

Por exemplo,

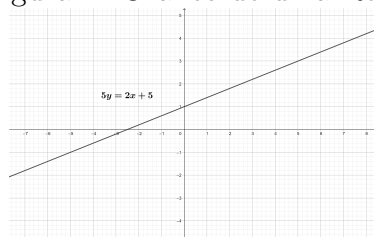
1. A parábola é o lugar geométrico dos pontos do plano equidistantes de um ponto fixo, denominado foco, e de uma reta fixa, denominada diretriz.
2. A elipse é o lugar geométrico dos pontos de um plano cuja soma das distâncias a dois pontos fixos, denominados focos, é constante.

No final do século 17, o método de Fermat e Descartes para descrever um lugar geométrico no plano por meio de equações de duas variáveis já era bastante conhecido. Usando métodos de cálculo diferencial as curvas algébricas reais apareceram para reformular vários problemas

O estudo das curvas algébricas planas envolve relações muito interessantes entre várias áreas da matemática, entre elas a Álgebra e a Geometria. Além disso, pode-se encontrar curvas em diversas áreas. Segue alguns exemplos de curvas que certamente são conhecidas.

Exemplo 1. A reta é um exemplo de uma curva.

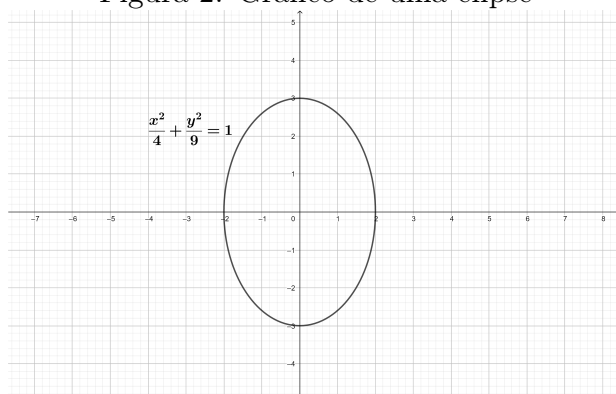
Figura 1: Gráfico de uma Reta



Fonte: próprio autor.

Exemplo 2. A Elipse também é uma curva.

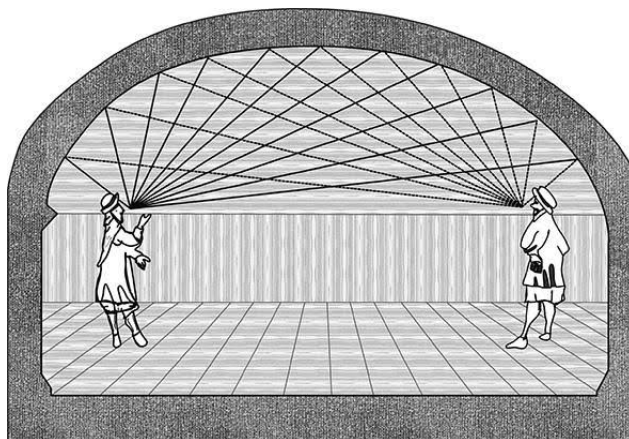
Figura 2: Gráfico de uma elipse



Fonte: próprio autor.

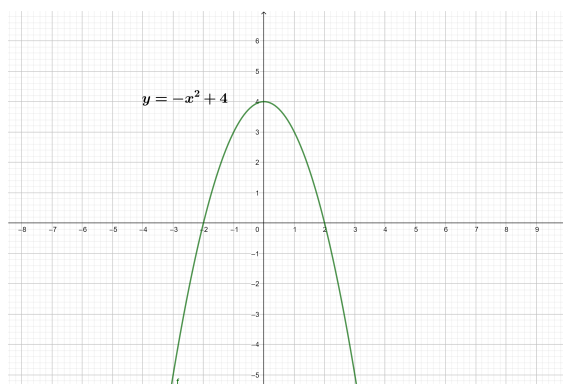
Podemos usar as propriedades da elipse para construir a sala do sussurro.

Figura 3: Sala do Sussurro



Exemplo 3. A Parábola é uma curva.

Figura 4: Parábola



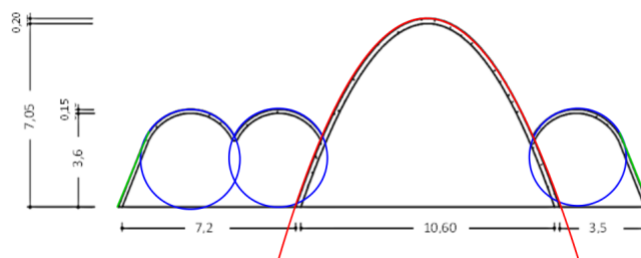
Fonte: próprio autor.

Podemos ver a aplicação da parábola Igreja da Pampulha.

Figura 5: Igreja da São Francisco na Pampulha



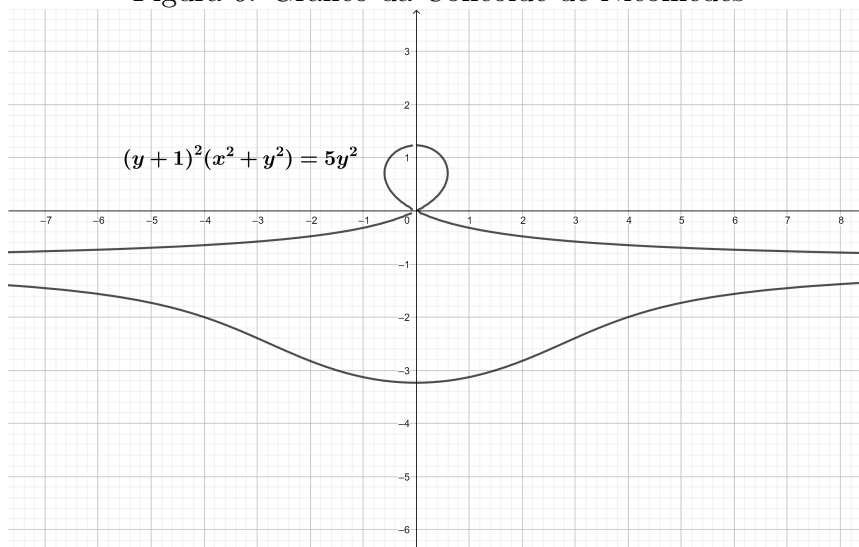
Fonte: <https://www.rotasale.com.br/blog/detalhe/89>



Fonte: Oliveira. T. C

Exemplo 4. Concoide de Nicomedes usada para resolver problema de cálculo de médias proporcionais.

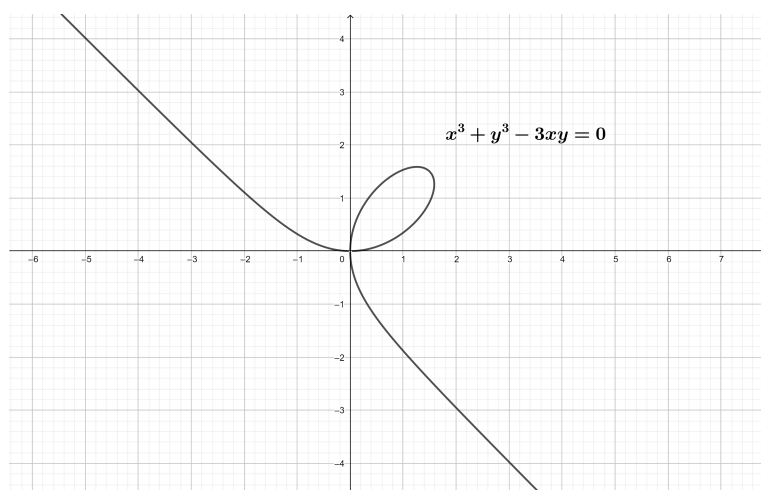
Figura 6: Gráfico da Concoide de Nicomedes



Fonte: próprio autor.

Exemplo 5. A Folium de Descartes é usada principalmente em estudos de Geometria Algébrica e Geometria Analítica, sendo utilizada na análise de curvas algébricas, singularidades e parametrizações.

Figura 7: Gráfico da Folium de Descartes



Fonte: próprio autor.

2.1 Curvas afins

Seja k um corpo e $\mathbb{A}^n = k \times \dots \times k = \{(a_1, \dots, a_n) / a_i \in k, \forall i\}$. $\mathbb{A}^n(k)$ ou simplesmente $\mathbb{A}^n$ é chamado de espaço afim, ou n -espaço afim.

Para $n = 1$ temos a reta afim, para $n = 2$ temos o plano afim.

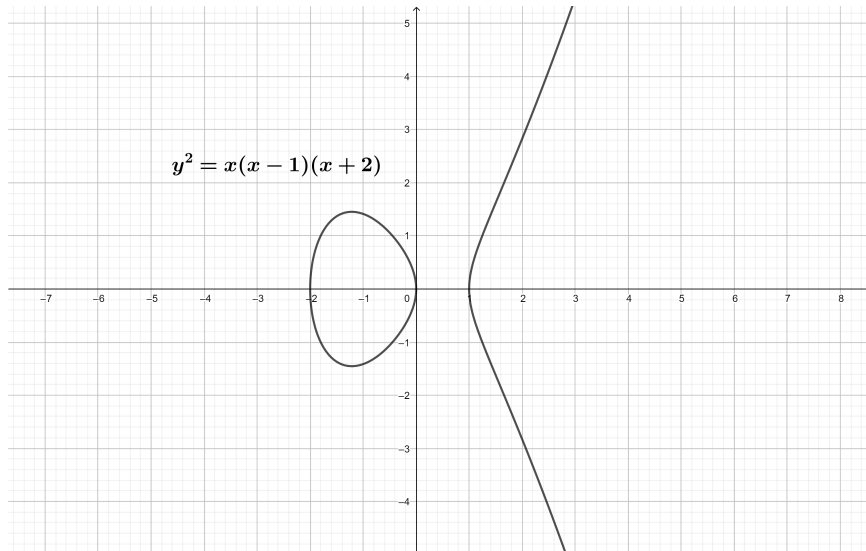
Seja k um corpo algebricamente fechado e $f(x, y)$ um polinômio não nulo em $k[x, y]$. Denotamos por $V_k(f)$ o conjunto dos pontos em k^2 da curva algébrica plana afim, ou simplesmente, curva algébrica, determinada por $f(x, y)$, isto é,

$$C = V_k(f) = \{(x, y) \in k^2 / f(x, y) = 0\}$$

O grau da curva C é igual ao grau do polinômio que a define.

Exemplo 6. As Curvas Elípticas são curvas afins e usadas em criptografia.

Figura 8: Gráfico de uma Curva elíptica



Fonte: próprio autor.

Um polinômio é dito homogêneo quando todos os seus termos tem o mesmo grau.

Exemplo 7. O polinômio $P(x, y, z) = 3x^8 - 2x^3y^5 + x^7z - 5x^2y^6$ é um exemplo de polinômio homogêneo.

Seja C é uma curva definida por $f \in k[x, y]$. Observe que f admite uma fatoração, pois todo anel de polinômios sobre um corpo é domínio de fatoração única. Assim, podemos escrever f da seguinte forma:

$$f = f_1^{n_1} \cdots f_k^{n_k},$$

onde f_i 's São polinômios irredutíveis não-associados. Cada curva definida por f_i é chamada de uma componente de f .

Exemplo 8. Seja C definida por $f(x, y) = x^2 - y^2 = (x - y)(x + y)$. As componentes aqui são $f_1 = x - y$ e $f_2 = x + y$.

Definição 2. Uma curva algébrica C é chamada redutível se existem curvas algébricas distintas irredutíveis C_1 e C_2 tais que $C = C_1 \cup C_2$. Se C não puder ser escrita como a união de duas ou mais curvas redutíveis, dizemos que C é irredutível.

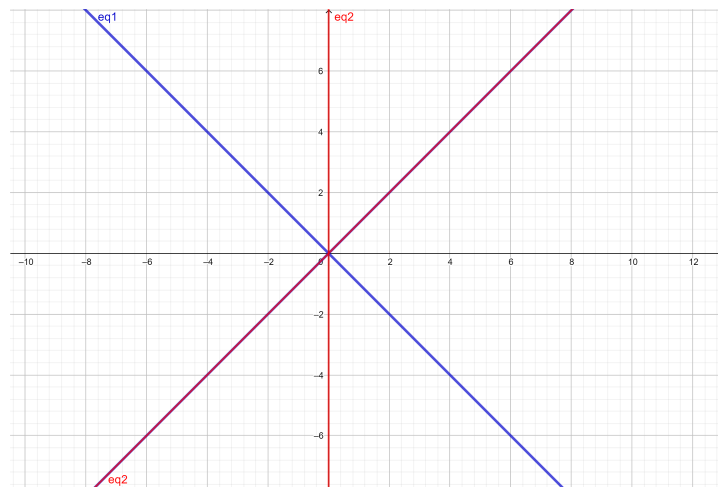
Exemplo 9. a) A reta é uma curva irredutível, por exemplo $f(x, y) = x + y$.

b) A curva C definida por $p(x, y) = xy$ é uma curva redutível, pois se p se decompõe em $p_1(x, y) = x$ e $p_2(x, y) = y$ que definem duas curvas irredutíveis.

Proposição 2.1. A interseção de duas curvas algébricas planas sem componentes em comum é finita.

Exemplo 10. Seja C_1 uma curva plana definida por $f(x, y) = x^2 - y^2$ e C_2 uma curva plana definida por $g(x, y) = (x - y)x$. A interseção de C_1 e C_2 é finita? A resposta é não. Observe que a interseção das curvas f e g é a reta $x = y$, ou seja, possui infinitos pontos de interseção.

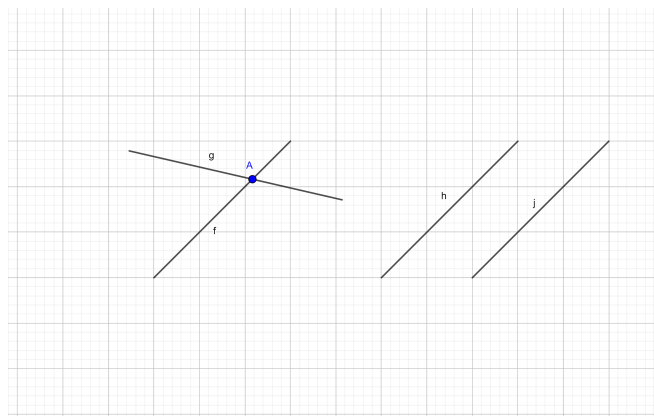
Figura 9: Inteseção de f e g



Fonte: próprio autor.

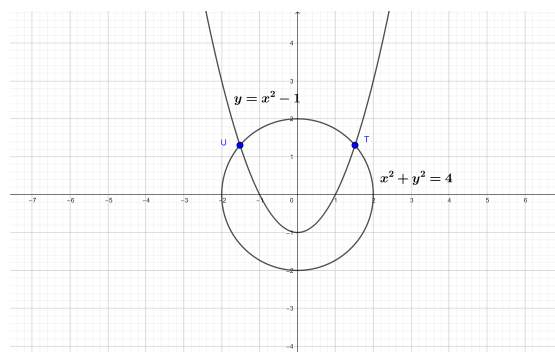
Exemplo 11. Podemos ver abaixo exemplos de curvas que se intersectam em uma quantidade infinita de pontos, finita e caso que não se intersectam.

Figura 10: Interseção de duas retas



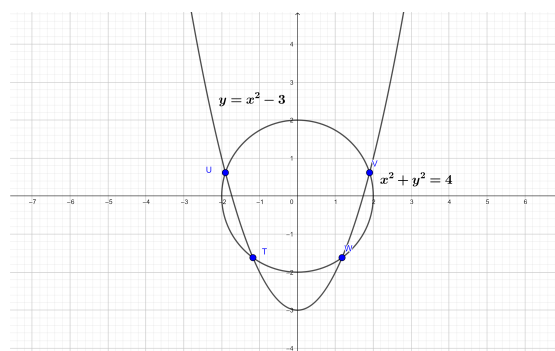
Fonte: próprio autor.

Figura 11: Interseção de uma parábola e uma circunferência



Fonte: próprio autor.

Figura 12: Interseção de uma parábola e uma circunferência



Fonte: próprio autor.

Como encontrar a interseção de duas curvas C_1 e C_2 definidas por f e g respectivamente, com $f, g \in k[x, y]$?

Sejam $f, g \in k[x, y]$. Selecione uma das variáveis, digamos x , e escreva f e g como

polinômios em y com coeficientes em $k[x]$:

$$f(x, y) = a_0 y^m + \dots + a_m, \quad m \geq 1 \text{ e } g(x, y) = b_0 y^n + \dots + b_n, \quad n \geq 1.$$

Definimos a resultante de f e g por

$$R = R_{f,g} = \begin{vmatrix} a_0 & \dots & a_m & 0 & \dots & 0 & 0 \\ 0 & a_0 & \dots & a_m & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & a_0 & \dots & a_m \\ b_0 & \dots & b_n & 0 & \dots & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & b_0 & \dots & b_n \end{vmatrix}$$

determinante da matriz $(m+n) \times (m+n)$ com n linhas $a's$ e m linhas $b's$, [1]

Exemplo 12. Sejam $f(x, y) = y^2 + x^2 - 4$ e $g(x, y) = xy - 1$, Calcule a resultante de f e g

Solução 1. Escrevendo os polinômios em função da variável y , obtemos

$$f(x, y) = y^2 + 0 \cdot y + (x^2 - 4)$$

e

$$g(x, y) = xy - 1 = (x)y - 1.$$

Assim,

$$a_0 = 1, \quad a_1 = 0, \quad a_2 = x^2 - 4,$$

e

$$b_0 = x, \quad b_1 = -1.$$

Como $m = 2$ e $n = 1$, a matriz é

$$\begin{pmatrix} 1 & 0 & x^2 - 4 \\ x & -1 & 0 \\ 0 & x & -1 \end{pmatrix},$$

cujo determinante é a resultante de f e g .

Calculando o determinante pela primeira linha,

$$\begin{aligned}
 R_{f,g}(x) &= \begin{vmatrix} 1 & 0 & x^2 - 4 \\ x & -1 & 0 \\ 0 & x & -1 \end{vmatrix} \\
 &= 1 \begin{vmatrix} -1 & 0 \\ x & -1 \end{vmatrix} + (x^2 - 4) \begin{vmatrix} x & -1 \\ 0 & x \end{vmatrix} \\
 &= 1((-1)(-1) - 0 \cdot x) + (x^2 - 4)(x^2) \\
 &= 1 + x^2(x^2 - 4) \\
 &= x^4 - 4x^2 + 1.
 \end{aligned}$$

Portanto,

$$R_{f,g}(x) = x^4 - 4x^2 + 1.$$

Como verificação, da equação $g(x, y) = 0$, temos:

$$xy - 1 = 0$$

segue que

$$y = \frac{1}{x}, \quad x \neq 0.$$

Substituindo em $f(x, y) = 0$, obtemos

$$\frac{1}{x^2} + x^2 - 4 = 0.$$

Multiplicando ambos os membros por x^2 , resulta

$$x^4 - 4x^2 + 1 = 0,$$

que coincide exatamente com a resultante calculada.

Definição 3. Seja $f \in k[x, y] - \{k\}$ e escreva $f = f_0 + \dots + f_d$, onde cada f_i é homogêneo de grau i e $f_d \neq 0$. Cada componente $ax + by$ de f_d é chamada de uma direção assintótica de f .

Exemplo 13. 1) $f(x, y) = 1 - xy$ tem direções assintóticas x e y .

2) $f(x, y) = y^2 - x$ tem apenas a direção assintótica y

Proposição 2.2. O grau da resultante de duas curvas sem direção assintótica em comum é

$$\deg(R_{f,g}) = \deg(f) \cdot \deg(g).$$

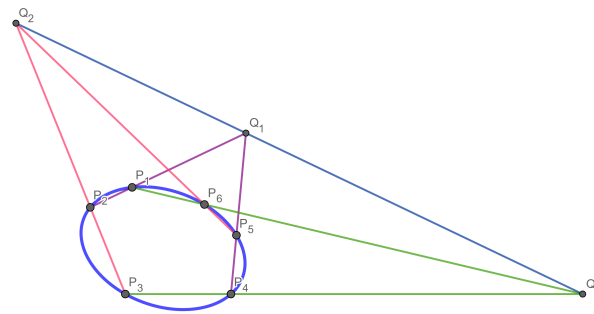
Teorema 2.3. (Teorema de Bézout- Caso afim) Sejam C e D duas curvas algébricas definidas por f e g de graus m e n respectivamente. Supondo que C e D não tem componentes em comum, ou seja, f e g não possuem fatores em comum. Então C e D têm no máximo mn pontos de interseção, isto é, $\#C \cap D \leq \deg(C) \cdot \deg(D)$.

2.2 Aplicações do Teorema de Bézout - caso afim

Proposição 2.4. Sejam $P_1, \dots, P_5$ cinco pontos distintos em posição geral em um plano. Então existe no máximo uma cônica passando por eles.

Teorema 2.5. (Teorema do hexágono de Pascal) Sejam $P_1, \dots, P_6$ seis pontos distintos sobre uma cônica irreduzível C . Se as retas P_1P_2 e P_4P_5 se intersectam em Q_1 , se as retas P_2P_3 e P_5P_6 se intersectam em Q_2 e se as retas P_3P_4 e P_6P_1 se intersectam em Q_3 , então os pontos Q_1, Q_2, Q_3 são colineares.

Figura 13: Ilustração geométrica do Teorema



Fonte: Próprio autor

Definição 4. Seja C uma curva definida por f . Um ponto $P \in C$ é chamado ponto singular de C se

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

O conjunto de pontos singulares de C é denotado por $Sing(C)$.

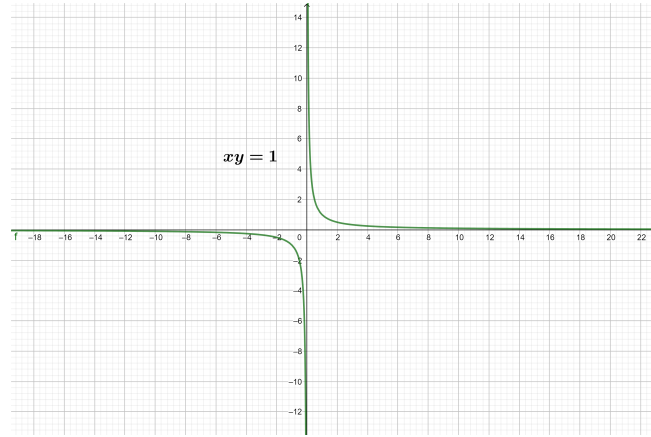
Proposição 2.6. Seja C uma curva algébrica. Então $Sing(C)$ é finito.

2.3 Plano projetivo

Considere a curva $xy = 1$ e suas assíntotas (eixo x e eixo y). Observe que as assíntotas nunca encosta na curva em $\mathbb{R}^2$, mas no plano que chamados de projetivo, elas se

intersectam no infinito.

Figura 14: A hipérbole e suas assíntotas



Fonte: Próprio autor

Seja k um corpo $\mathbb{A}^3 = \{(x, y, z) \mid x, y, z \in k\}$. Considere a seguinte relação em $\mathbb{A}^3 - \{(0, 0, 0)\}$

$$(x_1, y_1, z_1) \sim (x_2, y_2, z_2) \Leftrightarrow \exists \lambda \in k \text{ com } \lambda \neq 0 \text{ tal que } (x_1, y_1, z_1) = \lambda(x_2, y_2, z_2).$$

A relação acima é uma relação de equivalência em $\mathbb{A}^3 - \{(0, 0, 0)\}$.

A classe de $(x, y, z) \neq (0, 0, 0)$ denotada por $(x : y : z)$, ou seja, todo ponto da forma $(a : b : c)$ é visto como $(a : b : c) = \{(x, y, z) \in \mathbb{A}^3 \mid (x, y, z) = \lambda(a, b, c) \text{ com } \lambda \neq 0\}$. Definimos $\mathbb{P}^2 = \mathbb{A}^3 - \{(0, 0, 0)\} / \sim$ como o plano projetivo. Os pontos $(x : y : z)$ são chamados de coordenadas homogêneas de $\mathbb{P}^2$.

Considere

$$\varphi : \mathbb{A}^2 \longrightarrow \mathbb{P}^2, \quad \varphi(x, y) = (x : y : 1).$$

Observe que φ é injetiva. De fato, suponha que

$$\varphi(x, y) = \varphi(x', y').$$

Então,

$$(x : y : 1) = (x' : y' : 1)$$

como pontos de $\mathbb{P}^2$. Pela definição de coordenadas homogêneas, existe um escalar λ não nulo, tal que

$$(x, y, 1) = \lambda(x', y', 1).$$

Comparando a terceira coordenada, obtemos

$$1 = \lambda \cdot 1,$$

logo $\lambda = 1$. Consequentemente,

$$x = x' \quad \text{e} \quad y = y'.$$

Assim,

$$(x, y) = (x', y'),$$

o que prova que φ é injetiva.

Podemos também interpretar o plano projetivo $\mathbb{P}^2$, como $\mathbb{P}^2 = \mathbb{A}^2 \cup L_\infty$, onde $L_\infty = \{(x : y : 0) \mid x \neq 0 \text{ ou } y \neq 0\}$. Cada ponto da forma $(x : y : 0)$ com $x \neq 0$ ou $y \neq 0$ é dito um ponto no infinito.

Definição 5. Uma curva projetiva C em $\mathbb{P}^2$ é um subconjunto de $\mathbb{P}^2$ que satisfaz

$$C = \{(x, y, z) \in \mathbb{P}^2 \mid F(x, y, z) = 0, F \in k[x, y, z]\}$$

e F é um polinômio homogêneo.

Ou ainda, uma curva plana projetiva C é uma classe de equivalência de polinômios homogêneos não constantes, $F \in k[x, y, z]$, módulo uma relação que identifica dois tais polinômios, F, G , se um for múltiplo constante um do outro.

O grau da curva projetiva C definida por $F(x, y, z)$ é o grau de $F(x, y, z)$.

Exemplo 14. Vemos aqui dois exemplos de curvas projetivas

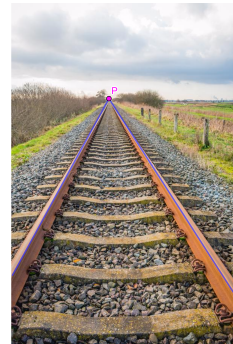
1. A equação da reta em $\mathbb{P}^2$ é dada por $ax + by + cz = 0$;
2. $F(x, y, z) = z^3 + xyz$

Exemplo 15. Duas curvas sempre se intersectam em $\mathbb{P}^2$, inclusive duas retas paralelas.

Figura 15: Trilhos paralelos



Figura 16: Trilhos intersectando no infinito



Podemos ver os pontos no infinito nas pinturas artísticas e na construção, como mostram as figuras 17, 18 e 19. O ponto no infinito nesses casos é chamado de fuga.

Figura 17: Santa ceia com ponto de fuga no olho esquerdo de Cristo

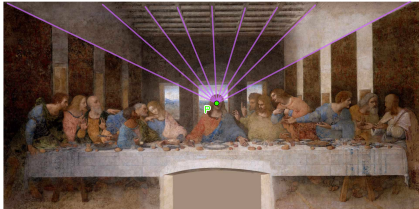


Figura 18: Santíssima Trindade com ponto de fuga nos pés da cruz



Figura 19: Palácio Planalto com dois pontos de fuga



Fonte: Gonçalves. T. S

Proposição 2.7. Sejam F e G curvas planas projetivas. Então $F \cap G$ é finita, se e somente se, F e G não admitem componentes em comum.

Teorema 2.8. Teorema de Bézout Se F e G são curvas planas projetivas sem componentes em comum, então o número de pontos na interseção $F \cap G$, contados com multiplicidade, é igual a $\deg(G) \cdot \deg(F)$. Isto é

$$\#F \cap G = \deg(G) \cdot \deg(F).$$

3 Curvas Elípticas

Essa seção é baseada no livro [7] e tem como objetivo introduzir o estudo das curvas elípticas, destacando a estrutura de grupo que elas apresentam.

Definição 6. Uma curva elíptica E sobre um corpo K é definida por uma equação

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

onde $a_1, a_2, a_3, a_4, a_6 \in K$ e $\Delta \neq 0$, onde Δ é o *discriminante* de E e é definido como segue:

$$\left. \begin{aligned} \Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \\ d_2 &= a_1^2 + 4a_2 \\ d_4 &= 2a_4 + a_1a_3 \\ d_6 &= a_3^2 + 4a_6 \\ d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned} \right\} \quad (2)$$

Se L é qualquer corpo de extensão de K , então o conjunto de *pontos L -racionais* sobre E é

$$E(L) = \{(x, y) \in L \times L : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\infty\}$$

em que ∞ é um ponto no infinito.

Exemplo 16. (Curvas elípticas sobre $\mathbb{R}$) Considere as curvas elípticas

$$\begin{aligned} E_1 : y^2 &= x^3 - x \\ E_2 : y^2 &= x^3 + \frac{1}{4}x + \frac{5}{4} \end{aligned}$$

definidas sobre o corpo $\mathbb{R}$ dos números reais. Os pontos $E_1(\mathbb{R}) \setminus \{\infty\}$ e $E_2(\mathbb{R}) \setminus \{\infty\}$ estão representados na Figura a seguir.

Definição 7. Duas curvas elípticas E_1 e E_2 definidas sobre K e dadas pelas equações de Weierstrass

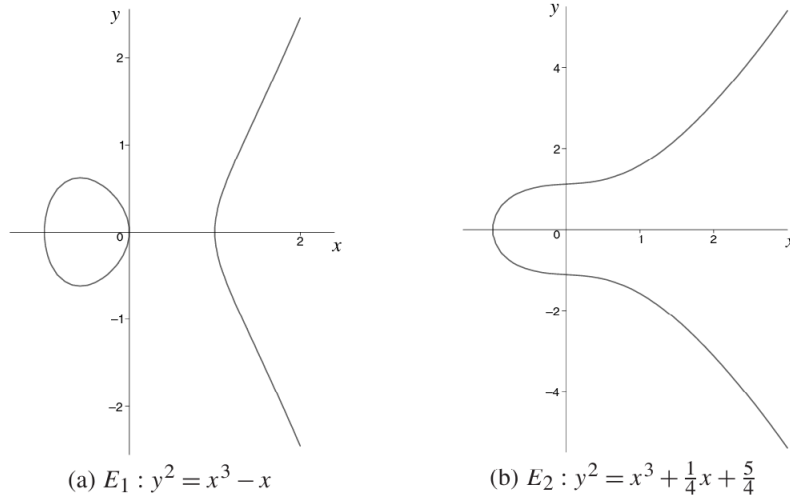
$$\begin{aligned} E_1 : y^2 + a_1xy + a_3y &= x^3 + a_2x^2 + a_4x + a_6 \\ E_2 : y^2 + \bar{a}_1xy + \bar{a}_3y &= x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6 \end{aligned}$$

são ditas isomórficas sobre K se existirem $u, r, s, t \in K, u \neq 0$, tais que a mudança de variáveis

$$(x, y) \rightarrow (u^2x + r, u^3y + u^2sx + t) \quad (3)$$

transforma a equação E_1 na equação E_2 . A transformação (3) é chamada de mudança de variáveis admissível.

Figura 20: Exemplo de gráfico de Curvas Elípticas



Fonte: Extraído de [7]

Considere uma equação de Weierstrass dada por

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (4)$$

definida sobre K pode ser simplificada consideravelmente através da aplicação de mudanças de variáveis admissíveis. Consideramos separadamente os casos em que o corpo K possui característica diferente de 2 e 3, ou possui característica igual a 2 ou 3.

1. Se a característica de K não for igual a 2 ou 3, então a mudança admissível de variáveis

$$(x, y) \rightarrow \left(\frac{x - 3a_1^2 - 12a_2}{36}, \frac{y - 3a_1x}{216} - \frac{a_1^3 + 4a_1a_2 - 12a_3}{24} \right)$$

transforma E na curva

$$y^2 = x^3 + ax + b \quad (5)$$

onde $a, b \in K$. O discriminante desta curva é $\Delta = -16(4a^3 + 27b^2)$.

2. Se a característica de K for 2, então há dois casos a considerar.

Caso 1: $a_1 \neq 0$

A mudança de variáveis admissível

$$(x, y) \rightarrow \left(a_1^2x + \frac{a_3}{a_1}, a_1^3y + \frac{a_1^2a_4 + a_3^2}{a_1^3} \right)$$

transforma E na curva

$$y^2 + xy = x^3 + ax^2 + b \quad (6)$$

onde $a, b \in K$. Tal curva é dita *não-supersingular* e possui discriminante $\Delta = b$.

Caso 2: $a_1 = 0$

A mudança de variáveis admissível

$$(x, y) \rightarrow (x + a_2, y)$$

transforma E na curva

$$y^2 + cy = x^3 + ax + b \quad (7)$$

onde $a, b, c \in K$. Tal curva é dita *supersingular* e possui discriminante $\Delta = c^4$.

Se a característica de K é 3, então há dois casos a considerar.

Caso 1: $a_1^2 \neq -a_2$

A mudança admissível de variáveis

$$(x, y) \rightarrow \left(x + \frac{d_4}{d_2}, y + a_1x + a_1\frac{d_4}{d_2} + a_3 \right),$$

onde $d_2 = a_1^2 + a_2$ e $d_4 = a_4 - a_1a_3$, transforma E na curva

$$y^2 = x^3 + ax^2 + b \quad (8)$$

onde $a, b \in K$. Tal curva é dita *não-supersingular* e possui discriminante $\Delta = -a^3b$.

Caso 2: $a_1^2 = -a_2$

A mudança admissível de variáveis

$$(x, y) \rightarrow (x, y + a_1x + a_3)$$

transforma E na curva

$$y^2 = x^3 + ax + b \quad (9)$$

onde $a, b \in K$. Tal curva é dita *supersingular* e possui discriminante $\Delta = -a^3$.

3.1 A Regra Geométrica da Soma

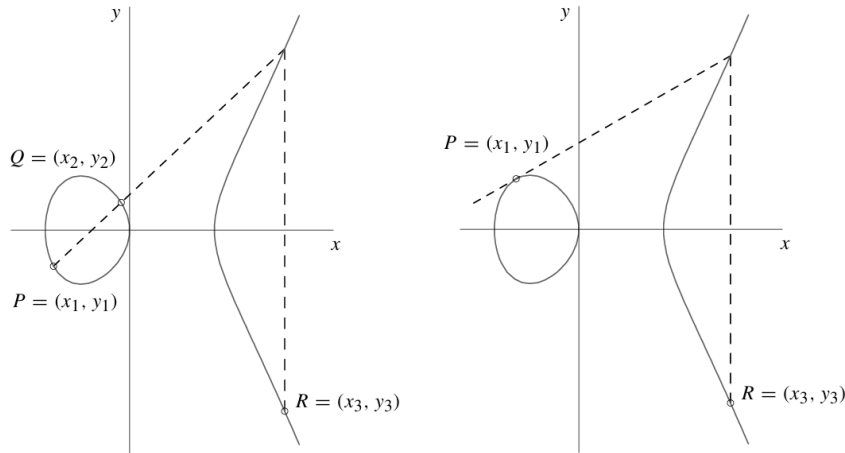
A operação de soma em uma curva elíptica E é realizada através do método secante-tangente, uma construção geométrica que permite obter um terceiro ponto R a partir de dois pontos dados, P e Q .

- **Soma de pontos distintos** ($P \neq Q$): Traça-se uma reta s que passa pelos pontos P e Q . Como a equação da curva possui grau 3, essa reta intersecta a curva em um terceiro ponto T (onde $T \in s \cap E$). Define-se a soma $P + Q = R$, sendo R o ponto obtido pela reflexão de T em relação ao eixo x .
- **Soma de pontos idênticos** ($P = Q$): Neste caso, a reta s é a reta tangente à

curva no ponto P . A reta tangente intersecta a curva em um ponto T . O resultado $2P$ é a reflexão de T em relação ao eixo x .

- **Caso vertical:** Se a reta s for perpendicular ao eixo x , não existe uma terceira interseção finita com a curva. Convenciona-se, então, que $P + Q = \infty$, onde ∞ é chamado de *ponto no infinito*.

Figura 21: Soma de Pontos da curva



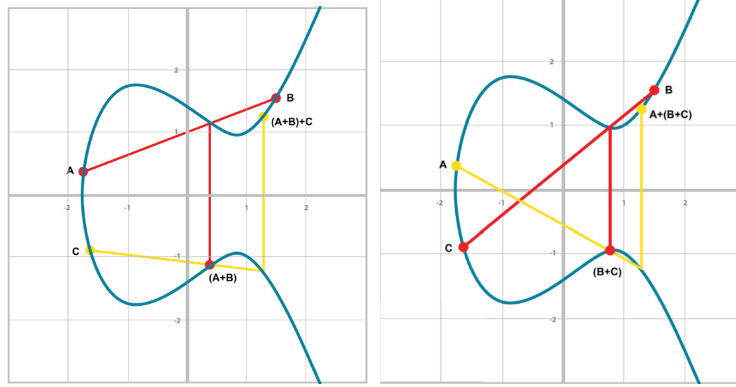
Fonte: Extraído de [7]

3.2 Estrutura de Grupo

O conjunto de pontos $E(K)$, munido da operação de soma elíptica, satisfaz os axiomas de um grupo abeliano:

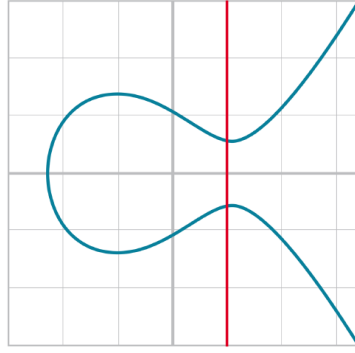
1. **Fechamento:** Se $P, Q \in E$, então $(P + Q) \in E$.
2. **Associatividade:** Para quaisquer pontos $P, Q, S \in E$, tem-se $(P + Q) + S = P + (Q + S)$.
3. **Existência de elemento neutro:** Existe um ponto θ tal que $P + \theta = P$ para todo $P \in E$.
4. **Existência de elemento inverso:** Para todo $P \in E$, existe um ponto $Q \in E$ (simbolizado por $-P$) tal que $P + Q = \infty$.
5. **Comutatividade:** Para quaisquer pontos $P, Q \in E$, tem-se $P + Q = Q + P$.

Figura 22: Associativa



Fonte: Extraído de [6]

Figura 23: Elemento Inverso



Fonte: Extraído de [6]

3.3 Regra Algébrica da Soma

3.3.1 Lei de Grupo para $E/K : y^2 = x^3 + ax + b, \text{char}(K) \neq 2, 3$

1) **Identidade.** $P + \infty = \infty + P = P$ para todo $P \in E(K)$.

2) **Elementos inversos.** Se $P = (x, y) \in E(K)$, então $(x, y) + (x, -y) = \infty$. O ponto $(x, -y)$ é denotado por $-P$ e é chamado de negativo de P ; note que $-P$ é, de fato, um ponto em $E(K)$. Além disso, $-\infty = \infty$.

3) **Adição de pontos.** Sejam $P = (x_1, y_1) \in E(K)$ e $Q = (x_2, y_2) \in E(K)$, onde $P \neq \pm Q$. Então $P + Q = (x_3, y_3)$, onde:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 \quad \text{e} \quad y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right) (x_1 - x_3) - y_1.$$

4) **Duplicação de ponto.** Seja $P = (x_1, y_1) \in E(K)$, onde $P \neq -P$. Então

$2P = (x_3, y_3)$, onde:

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

Exemplo 17. Curva elíptica sobre o corpo primo $\mathbb{F}_{29}$

Seja $p = 29$, $a = 4$ e $b = 20$, e considere a curva elíptica

$$E : y^2 = x^3 + 4x + 20$$

definida sobre $\mathbb{F}_{29}$. Note que

$$\Delta = -16(4a^3 + 27b^2) = -176896 \not\equiv 0 \pmod{29},$$

logo E é de fato uma curva elíptica.

Exemplo 18. Os pontos em $E(\mathbb{F}_{29})$ são os seguintes:

$$\begin{aligned} &\infty, (2, 6), (4, 19), (8, 10), (13, 23), (16, 2), (19, 16), (27, 2), \\ &(0, 7), (2, 23), (5, 7), (8, 19), (14, 6), (16, 27), (20, 3), (27, 27), \\ &(0, 22), (3, 1), (5, 22), (10, 4), (14, 23), (17, 10), (20, 26), \\ &(1, 5), (3, 28), (6, 12), (10, 25), (15, 2), (17, 19), (24, 7), \\ &(1, 24), (4, 10), (6, 17), (13, 6), (15, 27), (19, 13), (24, 22). \end{aligned}$$

Exemplos de adição na curva elíptica são:

$$(5, 22) + (16, 27) = (13, 6),$$

e

$$2(5, 22) = (14, 6).$$

Exemplo 19 (Corpo Binário). $\mathbb{F}_{2^m}$ são corpos finitos binários de característica 2. Uma maneira de construir $\mathbb{F}_{2^m}$ é com base polinomial. para essa construção, vamos considerar os coeficientes em $\mathbb{F}_2 = \{0, 1\}$ e o grau máximo $m - 1$.

$$\mathbb{F}_{2^m} = \{a_{m-1}z^{m-1} + a_{m-2}z^{m-2} + \cdots + a_2z^2 + a_1z + a_0 : a_i \in \{0, 1\}\}.$$

O Número de elementos de $\mathbb{F}_{2^m}$ é 2^m .

Aritmética em $\mathbb{F}_{2^m}$

1. Adição e Subtração São operações idênticas e extremamente eficientes:

(a)

I) Realizadas através da soma dos coeficientes **módulo 2**.

2. Multiplicação e Inverso Para garantir que o resultado permaneça no corpo:

- (a) Escolhe-se um **polinômio irredutível** $f(z)$ de grau m .
- (b) O produto é calculado como: $r(z) = [a(z) \cdot b(z)] \pmod{f(z)}$.
- (c) $f(z)$ atua como um "número primo" para polinômios.

Exemplo 20. (Corpo binário $\mathbb{F}_{2^4}$).

Considere o corpo finito $\mathbb{F}_{2^4}$ construído a partir do polinômio irredutível

$$f(z) = z^4 + z + 1.$$

Os elementos de $\mathbb{F}_{2^4}$ podem ser representados pelos polinômios binários de grau inferior a 4, isto é,

0	z^2	z^3	$z^3 + z^2$
1	$z^2 + 1$	$z^3 + 1$	$z^3 + z^2 + 1$
z	$z^2 + z$	$z^3 + z$	$z^3 + z^2 + z$
$z + 1$	$z^2 + z + 1$	$z^3 + z + 1$	$z^3 + z^2 + z + 1$.

A seguir, apresentam-se alguns exemplos de operações em $\mathbb{F}_{2^4}$.

1. Soma:

$$(z^3 + z^2 + 1) + (z^2 + z + 1) = z^3 + z.$$

2. Subtração:

$$(z^3 + z^2 + 1) - (z^2 + z + 1) = z^3 + z.$$

Como o corpo possui característica 2, vale $-a = a$ para todo $a \in \mathbb{F}_{2^4}$.

3. Multiplicação:

$$(z^3 + z^2 + 1)(z^2 + z + 1) = z^5 + z + 1.$$

Reduzindo o resultado módulo $f(z) = z^4 + z + 1$, obtém-se

$$z^5 + z + 1 \equiv z^2 + 1 \pmod{z^4 + z + 1}.$$

Portanto,

$$(z^3 + z^2 + 1)(z^2 + z + 1) = z^2 + 1 \quad \text{em } \mathbb{F}_{2^4}.$$

4. Inverso multiplicativo:

$$(z^3 + z^2 + 1)^{-1} = z^2,$$

pois

$$(z^3 + z^2 + 1) z^2 \equiv 1 \pmod{z^4 + z + 1}.$$

3.3.2 Lei de grupo para $E/\mathbb{F}_{2^m}$ não-supersingular: $y^2 + xy = x^3 + ax^2 + b$

1. *Identidade.* $P + \infty = \infty + P = P$ para todo $P \in E(\mathbb{F}_{2^m})$.

2. *Negativos.* Se $P = (x, y) \in E(\mathbb{F}_{2^m})$, então $(x, y) + (x, x + y) = \infty$. O ponto $(x, x + y)$ é denotado por $-P$ e é chamado de *negativo* de P ; note que $-P$ é de fato um ponto em $E(\mathbb{F}_{2^m})$. Além disso, $-\infty = \infty$.

1. *Adição de pontos.* Sejam $P = (x_1, y_1) \in E(\mathbb{F}_{2^m})$ e $Q = (x_2, y_2) \in E(\mathbb{F}_{2^m})$, onde $P \neq \pm Q$. Então $P + Q = (x_3, y_3)$, onde

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a \quad \text{e} \quad y_3 = \lambda(x_1 + x_3) + x_3 + y_1$$

com $\lambda = (y_1 + y_2)/(x_1 + x_2)$.

2. *Dobramento de ponto.* Seja $P = (x_1, y_1) \in E(\mathbb{F}_{2^m})$, onde $P \neq -P$. Então $2P = (x_3, y_3)$, onde

$$x_3 = \lambda^2 + \lambda + a = x_1^2 + \frac{b}{x_1^2} \quad \text{e} \quad y_3 = x_1^2 + \lambda x_3 + x_3$$

com $\lambda = x_1 + y_1/x_1$.

Exemplo 21. (*curva elíptica não-supersingular sobre $\mathbb{F}_{2^4}$*) Considere o corpo finito $\mathbb{F}_{2^4}$ representado pelo polinômio de redução $f(z) = z^4 + z + 1$. Sejam $a = z^3$, $b = z^3 + 1$, e considere a curva elíptica não-supersingular

$$E : y^2 + xy = x^3 + z^3 x^2 + (z^3 + 1)$$

definida sobre $\mathbb{F}_{2^4}$. Os pontos em $E(\mathbb{F}_{2^4})$ são os seguintes:

∞	(0011, 1100)	(1000, 0001)	(1100, 0000)
(0000, 1011)	(0011, 1111)	(1000, 1001)	(1100, 1100)
(0001, 0000)	(0101, 0000)	(1001, 0110)	(1111, 0100)
(0001, 0001)	(0101, 0101)	(1001, 1111)	(1111, 1011)
(0010, 1101)	(0111, 1011)	(1011, 0010)	
(0010, 1111)	(0111, 1100)	(1011, 1001)	

Exemplos de adição em curvas elípticas são $(0010, 1111) + (1100, 1100) = (0001, 0001)$, e $2(0010, 1111) = (1011, 0010)$.

3.3.3 Lei de grupo para $E/\mathbb{F}_{2^m}$ supersingular: $y^2 + cy = x^3 + ax + b$

1. *Identidade.* $P + \infty = \infty + P = P$ para todo $P \in E(\mathbb{F}_{2^m})$.
2. *Negativos.* Se $P = (x, y) \in E(\mathbb{F}_{2^m})$, então $(x, y) + (x, y + c) = \infty$. O ponto $(x, y + c)$ é denotado por $-P$ e é chamado de *negativo* de P ; note que $-P$ é de fato um ponto em $E(\mathbb{F}_{2^m})$. Além disso, $-\infty = \infty$.
1. *Adição de pontos.* Sejam $P = (x_1, y_1) \in E(\mathbb{F}_{2^m})$ e $Q = (x_2, y_2) \in E(\mathbb{F}_{2^m})$, onde $P \neq \pm Q$. Então $P + Q = (x_3, y_3)$, onde

$$x_3 = \left(\frac{y_1 + y_2}{x_1 + x_2} \right)^2 + x_1 + x_2 \quad \text{e} \quad y_3 = \left(\frac{y_1 + y_2}{x_1 + x_2} \right) (x_1 + x_3) + y_1 + c.$$

2. *Dobramento de ponto.* Seja $P = (x_1, y_1) \in E(\mathbb{F}_{2^m})$, onde $P \neq -P$. Então $2P = (x_3, y_3)$, onde

$$x_3 = \left(\frac{x_1^2 + a}{c} \right)^2 \quad \text{e} \quad y_3 = \left(\frac{x_1^2 + a}{c} \right) (x_1 + x_3) + y_1 + c.$$

3.4 Ordem do Grupo

Seja E uma curva elíptica definida sobre $\mathbb{F}_q$. O número de pontos em $E(\mathbb{F}_q)$, denotado por $\#E(\mathbb{F}_q)$, é chamado de **ordem** de E sobre $\mathbb{F}_q$.

Teorema 3.1 ((Hasse)). Seja E uma curva elíptica definida sobre $\mathbb{F}_q$. Então:

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$$

O intervalo $[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$ é conhecido como o **intervalo de Hasse**.

Exemplo 22 (Ordens de curvas elípticas sobre $\mathbb{F}_{37}$). Seja $p = 37$. A Tabela lista, para cada número inteiro n no intervalo de Hasse $[37 + 1 - 2\sqrt{37}, 37 + 1 + 2\sqrt{37}]$, os coeficientes (a, b) de uma curva elíptica $E : y^2 = x^3 + ax + b$ definida sobre $\mathbb{F}_{37}$ com $\#E(\mathbb{F}_{37}) = n$.

n	(a, b)	n	(a, b)	n	(a, b)	n	(a, b)	n	(a, b)
26	(5, 0)	31	(2, 8)	36	(1, 0)	41	(1, 16)	46	(1, 11)
27	(0, 9)	32	(3, 6)	37	(0, 5)	42	(1, 9)	47	(3, 15)
28	(0, 6)	33	(1, 13)	38	(1, 5)	43	(2, 9)	48	(0, 1)
29	(1, 12)	34	(1, 18)	39	(0, 3)	44	(1, 7)	49	(0, 2)
30	(2, 2)	35	(1, 8)	40	(1, 2)	45	(2, 14)	50	(2, 0)

Tabela 1: Ordens de curvas elípticas sobre $\mathbb{F}_{37}$

3.5 Estrutura do Grupo

Teorema 3.2. Seja E uma curva elíptica definida sobre $\mathbb{F}_q$. Então $E(\mathbb{F}_q)$ é isomorfo a $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ onde n_1 e n_2 são inteiros positivos unicamente determinados tais que n_2 divide tanto n_1 quanto $q - 1$.

Observe que $\#E(\mathbb{F}_q) = n_1 n_2$.

1. Se $n_2 = 1$, então $E(\mathbb{F}_q)$ é um grupo cíclico.
2. Se $n_2 > 1$, então diz-se que $E(\mathbb{F}_q)$ tem posto 2.
3. Se n_2 for um inteiro pequeno, dizemos que $E(\mathbb{F}_q)$ é *quase cíclico*.

Como n_2 divide tanto n_1 quanto $q - 1$, espera-se que $E(\mathbb{F}_q)$ seja cíclico ou quase cíclico para a maioria das curvas elípticas E sobre $\mathbb{F}_q$.

Exemplo 23. A curva elíptica $E : y^2 = x^3 + 4x + 20$ definida sobre $\mathbb{F}_{29}$ tem $\#E(\mathbb{F}_{29}) = 37$. Como 37 é primo, $E(\mathbb{F}_{29})$ é um grupo cíclico e qualquer ponto em $E(\mathbb{F}_{29})$, exceto por ∞ , é um gerador de $E(\mathbb{F}_{29})$. O que se segue mostra que os múltiplos do ponto $P = (1, 5)$ geram todos os pontos em $E(\mathbb{F}_{29})$.

$0P = \infty$	$8P = (8, 10)$	$16P = (0, 22)$	$24P = (16, 2)$	$32P = (6, 17)$
$1P = (1, 5)$	$9P = (14, 23)$	$17P = (27, 2)$	$25P = (19, 16)$	$33P = (15, 2)$
$2P = (4, 19)$	$10P = (13, 23)$	$18P = (2, 23)$	$26P = (10, 4)$	$34P = (20, 26)$
$3P = (20, 3)$	$11P = (10, 25)$	$19P = (2, 6)$	$27P = (13, 6)$	$35P = (4, 10)$
$4P = (15, 27)$	$12P = (19, 13)$	$20P = (27, 27)$	$28P = (14, 6)$	$36P = (1, 24)$
$5P = (6, 12)$	$13P = (16, 27)$	$21P = (0, 7)$	$29P = (8, 19)$	
$6P = (17, 19)$	$14P = (5, 22)$	$22P = (3, 28)$	$30P = (24, 7)$	
$7P = (24, 22)$	$15P = (3, 1)$	$23P = (5, 7)$	$31P = (17, 10)$	

Exemplo 24. Considere $\mathbb{F}_{24}$ como representado pelo polinômio de redução $f(z) = z^4 + z + 1$. A curva elíptica $E : y^2 + xy = x^3 + z^3 x^2 + (z^3 + 1)$ definida sobre $\mathbb{F}_{24}$ tem $\#E(\mathbb{F}_{24}) = 22$. Como 22 não possui fatores repetidos, $E(\mathbb{F}_{24})$ é cíclico. O ponto $P = (z^3, 1) = (1000, 0001)$ tem ordem 11; seus múltiplos são mostrados abaixo.

$$\begin{array}{lll}
0P = \infty & 1P = (1000, 0001) & 2P = (1001, 1111) \\
3P = (1100, 0000) & 4P = (1111, 1011) & 5P = (1011, 0010) \\
6P = (1011, 1001) & 7P = (1111, 0100) & 8P = (1100, 1100) \\
9P = (1001, 0110) & 10P = (1000, 1001) &
\end{array}$$

3.6 Representação por Coordenadas Homogêneas

- Um ponto no plano projetivo é representado por uma tripla $(X : Y : Z)$, onde ao menos uma coordenada deve ser não nula.
- **Relação de Equivalência:** $(X : Y : Z)$ é o mesmo ponto que $(\lambda X : \lambda Y : \lambda Z)$ para qualquer $\lambda \neq 0$.
- Isso significa que um ponto projetivo representa, na verdade, uma reta que passa pela origem no espaço tridimensional.

2. A Transição Afim $\rightarrow$ Projetiva

- **Mergulho Afim:** Pontos comuns (x, y) são mapeados para o plano projetivo como $(x : y : 1)$ (onde $Z = 1$).
- **Recuperação de Coordenadas:** Para retornar ao plano afim a partir de um ponto onde $Z \neq 0$, calculamos $x = X/Z$ e $y = Y/Z$.

Exemplo 25. A forma projetiva da equação de Weierstrass

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

definida sobre K é

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

O único ponto na linha no infinito que também reside em E é $(0 : 1 : 0)$. Este ponto projetivo corresponde ao ponto ∞ .

4 Criptografia com Curvas elípticas

A criptografia de curvas elípticas (*Elliptic Curve Cryptography* – ECC) foi proposta de forma independente, em 1985, pelos matemáticos Neal Koblitz, da Universidade de Washington, e Victor Miller, da IBM. A principal contribuição desses pesquisadores foi a utilização dos grupos de pontos de curvas elípticas definidas sobre corpos finitos como alternativa aos grupos multiplicativos tradicionalmente empregados em sistemas de criptografia de chave pública.

A segurança da ECC fundamenta-se no Problema do Logaritmo Discreto em Curvas Elípticas (*Elliptic Curve Discrete Logarithm Problem* – ECDLP). As curvas elípticas utilizadas são, em geral, descritas por equações da forma

$$y^2 = x^3 + ax + b,$$

definidas sobre um corpo apropriado e sujeitas a condições que garantem sua não singularidade.

Uma das principais vantagens da ECC em relação a sistemas criptográficos clássicos, como o RSA, é que ela proporciona o mesmo nível de segurança utilizando chaves significativamente menores. Por exemplo, uma chave ECC de 256 bits oferece um nível de segurança comparável ao de uma chave RSA de 3072 bits. Essa característica reduz o consumo de memória, o custo computacional e o tempo de processamento, tornando a ECC especialmente adequada para dispositivos com recursos limitados, como smartphones, cartões inteligentes e dispositivos da Internet das Coisas (IoT).

Problema do Logaritmo Discreto

Esse problema consiste em encontrar o x na equação $g^x = h$ dentro de um grupo finito.

No contexto de curvas elípticas, tentamos encontrar o x tal que $Q = xP$.

É computacionalmente difícil.

4.1 Troca de Chave Diffie-Hellman

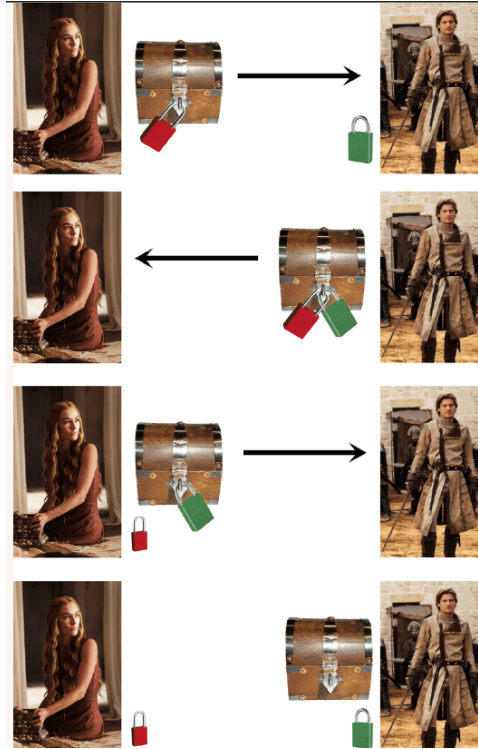
- 1) Alice e Bob concordam com uma curva elíptica E sobre um corpo finito $\mathbb{F}_q$ tal que o problema do logaritmo discreto é difícil em $E(\mathbb{F}_q)$. Eles também concordam com um ponto $P \in E(\mathbb{F}_q)$, tal que, o subgrupo gerado por P tem uma ordem grande (geralmente, a curva e o ponto são escolhidos de tal forma que a ordem é um primo grande).
- 2) Alice escolhe um inteiro secreto a , computa $P_a = aP$, e envia P_a para Bob.

- 3) Bob escolhe um inteiro secreto b , computa $P_b = bP$, e envia P_b para Alice.
- 4) Alice computa $aP_b = abP$.
- 5) Bob computa $bP_a = baP$.
- 6) Alice e Bob usa algum método aceito publicamente para extrair uma chave de abP .

4.2 Massey-Omura

A apresentação do método Massey-Omura e o exemplo desenvolvido nesta seção têm como referência o trabalho de [8].

Suponhamos que Alice queira enviar uma mensagem para Bob. A mensagem é colocada em um baú. Alice o fecha com seu cadeado e o envia para Bob. Como Bob não pode remover o cadeado de Alice, ele apenas acrescenta o seu próprio cadeado e devolve o baú. Alice então remove apenas o seu cadeado, deixando o cadeado de Bob, e envia novamente o baú. Por fim, Bob remove seu cadeado e abre o baú. Assim, a mensagem permanece protegida durante todo o processo, sem que Alice e Bob precisem compartilhar suas chaves.



- 1) Alice e Bob escolhem uma curva elíptica E sobre um corpo finito $\mathbb{F}_q$, tal que o problema do logaritmo discreto é difícil em $E(\mathbb{F}_q)$. Defina $N = \#E(\mathbb{F}_q)$.

- 2) Alice representa sua mensagem como um ponto $M \in E(\mathbb{F}_q)$.
- 3) Alice escolhe um inteiro secreto m_A com $\text{mdc}(m_A, N) = 1$, computa $M_1 = m_A M$, e envia M_1 à Bob.
- 4) Bob escolhe um inteiro secreto m_B com $\text{mdc}(m_B, N) = 1$, computa $M_2 = m_B M_1$, e envia M_2 à Alice.
- 5) Alice computa $m_A^{-1} \in \mathbb{Z}_N$. Ela computa $M_3 = m_A^{-1} M_2$ e envia M_3 à Bob.
- 6) Bob computa $m_B^{-1} \in \mathbb{Z}_N$. Ele computa $M_4 = m_B^{-1} M_3$. Então, $M_4 = M$ é a mensagem.

Escolha do ponto

Definição de Parâmetros:

- A mensagem m é um número natural no intervalo $0 \leq m \leq R$.
- Fixamos um número natural t (fator de precisão).
- Escolhemos um corpo finito $\mathbb{F}_q$ tal que $q > Rt$.

Mapeamento para a Curva:

- Para uma mensagem m , testamos valores de $x = mt + j$, onde $j = 1, \dots, t - 1$.
- Calculamos $f(x) = x^3 + Ax + B$ em $\mathbb{F}_q$.
- Se $f(x)$ for um quadrado em $\mathbb{F}_q$, definimos o ponto $P_m = (x, \sqrt{f(x)})$.
- Caso contrário, incrementamos j e repetimos o processo até encontrar um quadrado.

Recuperação da Mensagem:

- Para extrair m a partir do ponto $P_m = (x, y)$, aplica-se a função piso: $m = \lfloor x/t \rfloor$.

Análise de Falha:

- A probabilidade de o algoritmo não encontrar um ponto após t tentativas é de aproximadamente $1/2^t$.

Exemplo 26 (Exemplo retirado da referência 8). **Definição da Curva:** Consideramos a curva elíptica $E(\mathbb{F}_{751})$ definida por $y^2 = x^3 - 7x + 2$.

Mapeamento do Alfabeto: Identificamos as letras do alfabeto com o conjunto $\{10, 11, \dots, 35\}$, respectivamente.

Mensagem Original: O usuário **A** deseja enviar a mensagem $\mathbf{m} = \text{APROVADO-NOTCC}$ para o usuário **B**.

Parâmetros de Codificação:

- Como $0 \leq m \leq 35 = R$, escolhemos $t = 20$.
- Assim, $q = 751 \geq Rt = 700$.

Codificação da Letra A:

- Temos $A = 10$, logo, $10 \cdot 20 = 200 = x$.
- Calculamos $f(x) = 200^3 - 7(200) + 2 \equiv 452 \pmod{751}$.
- Como a equação $y^2 \equiv 452 \pmod{751}$ não tem solução, tomamos $x + 1 = 201$, onde $f(201) \equiv 135 \pmod{751}$ (também sem solução).
- Tomamos $x + 2 = 202$, resultando em $f(202) \equiv 273 \pmod{751}$.
- A equação $y^2 \equiv 273 \pmod{751}$ tem soluções $y = 32$ ou $y = 719$. Escolhemos $y = 32$, portanto, $P_A = (202, 32)$.

Pontos das Demais Letras:

- $P_P = (501, 53)$, $P_R = (541, 104)$, $P_O = (485, 263)$, $P_V = (621, 324)$, $P_D = (261, 110)$,
 $P_N = (460, 247)$, $P_T = (581, 283)$, $P_C = (241, 372)$.

Criptografia pelo Usuário A:

- O usuário **A** escolhe o inteiro secreto $m_A = 5$, com $\text{mdc}(5, \#E(\mathbb{F}_{751}) = 764) = 1$.
- Computa os pontos: $m_AP_A = 5(202, 32) = (553, 147)$, $m_AP_P = (535, 214)$, $m_AP_R = (232, 634)$, $m_AP_O = (49, 553)$, $m_AP_V = (98, 16)$, $m_AP_D = (627, 163)$, $m_AP_N = (529, 475)$, $m_AP_T = (128, 233)$, $m_AP_C = (398, 743)$.
- A envia a Mensagem Criptografada (M.C.) para **B**:

$$M.C. = \{(553, 147), (535, 214), (232, 634), (49, 553), (98, 16), \\ (553, 147), (627, 163), (49, 553), (529, 475), (49, 553), \\ (128, 233), (398, 743), (398, 743)\}$$

Ação do Usuário B:

- O usuário **B** multiplica cada ponto de (M.C.) por seu inteiro secreto $m_B = 3$ ($\text{mdc}(3, 764) = 1$) e envia para **A**:

$$\{(263, 658), (627, 163), (50, 509), (111, 745), (691, 589), \\ (263, 658), (569, 88), (111, 745), (238, 456), (111, 745), \\ (331, 64), (55, 696), (55, 696)\}$$

Finalização pelo Usuário A:

- O usuário **A** multiplica cada ponto por $m_A^{-1} = 153$ e envia para **B**:

$$\{(324, 143), (261, 110), (10, 593), (237, 187), (140, 362), \\ (324, 143), (714, 725), (237, 187), (471, 374), (237, 187), \\ (173, 109), (353, 428), (353, 428)\}$$

Recuperação pelo Usuário B:

- O usuário **B** recupera a mensagem original multiplicando os pontos por $m_B^{-1} = 255$.
- A decodificação final é feita calculando a parte inteira de x/t . Exemplo: para $P_A = (202, 32)$, temos $[202/20] = 10 = A$.

4.3 O Problema do Logaritmo Discreto

A apresentação do método e o exemplo desenvolvido nesta seção têm como referência o trabalho de [9].

A segurança do esquema ElGamal e de outros protocolos apresentados reside na dificuldade do **Problema do Logaritmo Discreto em Curvas Elípticas (ECDLP)**.

Esse problema consiste em encontrar o x na equação $g^x = h$ dentro de um grupo finito. No contexto de curvas elípticas, tentamos encontrar o x tal que $Q = xP$. É computacionalmente difícil.

Passo 1: Preparação de Bob no ECDLP Alice deseja enviar uma mensagem m para Bob.

Algoritmo.

1. Bob escolhe, e mantém em segredo, um inteiro $b \in \mathbb{N}^*$.
2. Ele envia à Alice o valor $Q = bP$.
3. P é um ponto da curva elíptica conhecido publicamente.

Passo 2: Criptografia por Alice

2. Alice escolhe um inteiro $a \in \mathbb{N}^*$ (também o guarda para si).
3. Ela computa os valores do criptograma:

- $M_1 = aP$
- $M_2 = m + aQ$

Passo 3: Decifração por Bob

3. Para decifrar a mensagem m , Bob utiliza sua chave privada b .
4. Ele realiza o seguinte cálculo:

$$M_2 - bM_1 = m + abP - baP = m$$

Resumo das Notações Para a correta execução, as partes devem garantir:

- **Segredos (Privados):** Inteiros a (Alice) e b (Bob) pertencentes a $\mathbb{N}^*$.
- **Público:** Ponto P e Chave Pública $Q = bP$.
- **Criptograma:** O par (M_1, M_2) enviado via canal inseguro.

Passo 1: Mapeamento Numérico do Alfabeto Para iniciar a cifragem, cada letra do alfabeto é associada a um valor numérico entre 01 e 26.

- $A = 01, B = 02, C = 03 \dots Z = 26$.
- Este mapeamento permite que o texto seja tratado como dado matemático para as operações na curva.

Exemplo 27. Para a palavra **LNCC**, primeiro identificamos os números de cada letra antes de agrupá-las em blocos.

Passo 2: Agrupamento e Concatenação A mensagem é dividida em blocos de duas letras (neste exemplo, LN e CC).

- Os números associados às letras de cada bloco são concatenados para formar um único valor escalar.

- **Exemplo com o bloco AB:**

- $A = 01$ e $B = 02$.
- Valor concatenado: 0102 (ou 102).

Passo 3: Mapeamento em Pontos da Curva O valor concatenado é multiplicado por um ponto público P da curva elíptica.

- **Configuração:** Curva $y^2 = x^3 + 373x + 402$ sobre $\mathbb{F}_{3697}$.
- **Ponto Base:** $P = (551, 1946)$.
- **Cálculo para AB:**

$$102 \cdot P = 102(551, 1946) = (3108, 1065)$$

Resultado Final O par de letras **AB** é mapeado para o ponto $(3108, 1065)$ na curva elíptica.

Passo 1: Configuração e Chave Pública de Bob Bob inicia o processo definindo sua chave privada e os parâmetros da curva $y^2 = x^3 + 373x + 402$ sobre $\mathbb{F}_{3697}$:

- **Chave Privada:** Bob escolhe $b = 919$.
- **Ponto Base:** $P = (551, 1946)$.
- **Chave Pública (Q):** Bob calcula $Q = bP = 919(551, 1946) = (301, 3454)$.

Segurança É computacionalmente inviável descobrir b a partir de Q e P (Problema do Logaritmo Discreto).

Passo 2: Alice Criptografa o Bloco “LN” Alice deseja enviar a string **LN**, previamente mapeada no ponto $m = (2309, 2502)$:

1. Alice escolhe um inteiro aleatório $a = 815$.

2. Calcula a primeira parte do criptograma (M_1):

$$M_1 = 815P = 815(551, 1946) = (958, 14)$$

3. Calcula o segredo compartilhado para mascarar a mensagem:

$$aQ = 815(301, 3454) = (837, 2461)$$

Passo 2: Finalizando o Criptograma de “LN” Para ocultar o ponto m , Alice o soma ao ponto aQ :

- **Segunda parte (M_2):**

$$M_2 = m + aQ = (2309, 2502) + (837, 2461) = (1518, 14)$$

- **Transmissão:** Alice envia a Bob o par cifrado:

$$(M_1, M_2) = ((958, 14), (1518, 14))$$

Passo 3: Bob Recupera a Mensagem “LN” Bob recebe (M_1, M_2) e usa sua chave privada $b = 919$ para calcular $m = M_2 - bM_1$:

1. Bob primeiro calcula bM_1 :

$$919(958, 14) = (837, 2461)$$

2. Subtrai este valor de M_2 :

$$m = (1518, 14) - (837, 2461) = (2309, 2502)$$

Resultado O ponto $(2309, 2502)$ corresponde exatamente à string **LN**.

Passo 4: Processamento do Bloco “CC” Para as letras **CC**, o procedimento é análogo. O bloco é mapeado no ponto $m = (3023, 762)$:

- Alice utiliza o mesmo segredo compartilhado $aQ = (837, 2461)$.
- Alice calcula o novo M_2 :

$$M_2 = (3023, 762) + (837, 2461) = (3084, 2426)$$

- Alice envia $M_2 = (3084, 2426)$ para Bob.

Passo 5: Conclusão do Processo Bob recupera a string final repetindo a subtração:

- Cálculo de descriptografia:

$$m = M_2 - bM_1 = (3084, 2426) - (837, 2461)$$

$$m = (3084, 2426) + (837, -2461) = (3023, 762)$$

Encerramento Bob recupera a string **CC** e a mensagem completa **LNCC** é finalizada com sucesso.

Exemplo 28. Este exemplo foi extraído da referência [10].

Consideramos a curva elíptica definida sobre o corpo finito $\mathbb{F}_{29}$:

$$E : y^2 = x^3 + 4x + 20$$

A curva possui ordem 37 e utilizamos como ponto gerador:

$$G = (24, 7)$$

No algoritmo ElGamal, o destinatário escolhe inicialmente uma chave privada b . Em nossa execução foi escolhido:

$$b = 28$$

A chave pública é obtida multiplicando a chave privada pelo ponto gerador:

$$Q = bG$$

Logo,

$$Q = 28(24, 7) = (10, 4)$$

Portanto:

- **Chave privada:** $b = 28$
- **Chave pública:** $Q = (10, 4)$

Letra	Número	Ponto
A	22	(17, 10)
B	34	(0, 7)
C	24	(27, 2)
D	4	(14, 23)
E	23	(16, 2)
F	1	(24, 7)
G	15	(17, 19)
H	14	(16, 27)
I	20	(8, 10)
J	18	(3, 28)
K	17	(8, 19)
L	29	(2, 6)
M	12	(13, 6)

Letra	Número	Ponto
N	25	(13, 23)
O	30	(19, 13)
P	33	(14, 6)
Q	27	(15, 2)
R	21	(1, 5)
S	37	Neutro
T	11	(20, 26)
U	35	(5, 22)
V	8	(2, 23)
W	26	(20, 3)
X	6	(6, 17)
Y	28	(10, 4)
Z	7	(19, 16)

Pré-codificação da Mensagem

Antes da criptografia, cada letra da mensagem é associada a um ponto da curva elíptica por meio de uma tabela de pré-codificação.

A mensagem utilizada foi:

CODIGO

Cada letra é substituída pelo ponto correspondente da tabela:

Letra	Ponto da Curva
C	(27, 2)
O	(19, 13)
D	(14, 23)
I	(8, 10)
G	(17, 19)
O	(19, 13)

Assim, a mensagem passa a ser representada por uma lista de pontos da curva elíptica.

Criptografia no ElGamal

Para criptografar a mensagem, escolhe-se um valor aleatório a e calcula-se:

$$M_1 = aG$$

nesse exemplo, obteve-se:

$$M_1 = (1, 5)$$

Para cada ponto P da mensagem pré-codificada, calcula-se:

$$M_2 = P + aQ$$

onde:

- P é o ponto correspondente à letra;

- Q é a chave pública;
- a é o valor aleatório escolhido.

O texto criptografado é enviado como o par: (M_1, M_2) **Descriptografia no ElGamal**

Tabela M_2

C	(8, 10)
O	(20, 3)
D	Elemento neutro
I	(1, 24)
G	(20, 26)
O	(20, 3)

O destinatário utiliza sua chave privada b para recuperar cada ponto original da mensagem.

A recuperação é feita por meio da operação:

$$P = M_2 - bM_1$$

onde:

- M_1 e M_2 são os valores recebidos;
- b é a chave privada.

Após recuperar os pontos da curva, utiliza-se novamente a tabela de pré-codificação para transformar cada ponto em letra. Dessa forma, obtemos novamente a mensagem original:

CODIGO

4.4 O Criptossistema Menezes-Vanstone

A apresentação do método e o exemplo desenvolvido nesta seção têm como referência o trabalho de [9].

Diferente de outros sistemas, no Menezes-Vanstone a mensagem não precisa ser um ponto da curva.

- **Texto Legível (m):** Um par ordenado $m = (x_1, x_2)$, onde $x_1, x_2 \in \mathbb{F}_p^*$.
- **Texto Ilegível (r):** Uma tripla ordenada $r = (y_0, y_1, y_2)$.
 - y_0 é um ponto da curva elíptica.
 - $y_1, y_2 \in \mathbb{F}_p^*$ são componentes numéricos calculados.

Algoritmo: Criptografando a Mensagem Para cifrar $m = (x_1, x_2)$, Bob realiza os seguintes passos:

1. Escolhe um inteiro secreto $k \in \mathbb{F}_p^*$ e calcula o ponto $y_0 = kP$.
2. Computa o segredo compartilhado: $(c_1, c_2) = kQ$.
3. Mascara a mensagem através de multiplicações modulares:
 - $y_1 = c_1x_1 \pmod{p}$.
 - $y_2 = c_2x_2 \pmod{p}$.
4. Envia a tripla $r = (y_0, y_1, y_2)$ para Alice.

Algoritmo: Descriptografando a Mensagem Ao receber $r = (y_0, y_1, y_2)$, Alice usa sua chave privada s para recuperar m :

1. Alice recupera o segredo compartilhado calculando:

$$sy_0 = s(kP) = k(sP) = kQ = (c_1, c_2)$$

2. Utiliza o inverso modular dos componentes para isolar x_1 e x_2 :
 - $x_1 = y_1(c_1)^{-1} \pmod{p}$.
 - $x_2 = y_2(c_2)^{-1} \pmod{p}$.
3. A mensagem original $m = (x_1, x_2)$ é recuperada.

Exemplo 29. Exemplo Prático: Mensagem “MCT” Bob deseja enviar “MCT” para Alice usando a curva $\Omega : y^2 = x^3 + 67110x + 262147$ sobre $\mathbb{F}_{2097421}$.

- **Codificação ASCII:** M=77, C=67, T=84.
- **Formação do Par:** Separamos em dois blocos, resultando em $m = (7767, 84)$.
- **Parâmetros Públicos:**
 - $P = (1355793, 621792)$.
 - $Q = sP = (949594, 812871)$, com chave privada $s = 78771$.

Exemplo Prático: Cifragem de Bob

1. Bob escolhe $k = 23358$ e computa y_0 :

$$y_0 = 23358 \cdot P = (1390038, 1344654)$$

2. Calcula o segredo compartilhado kQ :

$$kQ = (647014, 449701) = (c_1, c_2)$$

3. Calcula os componentes cifrados:

- $y_1 = 647014 \cdot 7767 \equiv 2034443 \pmod{p}$.
- $y_2 = 449701 \cdot 84 \equiv 21306 \pmod{p}$.

4. Bob envia $r = (y_0, 2034443, 21306)$ para Alice.

Exemplo Prático: Decifração de Alice

1. Alice calcula $s \cdot y_0$:

$$78771 \cdot (1390038, 1344654) = (647014, 449701) = (c_1, c_2)$$

2. Recupera os valores originais usando inversos modulares:

- $x_1 = 2034443(647014)^{-1} \equiv 7767 \pmod{p}$.
- $x_2 = 21306(449701)^{-1} \equiv 84 \pmod{p}$.

Conclusão Ao final, Alice obtém $m = (7767, 84)$, que convertido de volta para ASCII resulta na mensagem original **MCT**.

4.5 Ataques

Nesta seção serão apresentados os principais tipos de ataques aplicáveis à Criptografia de Curvas Elípticas (ECC). Serão discutidos os ataques matemáticos, descrevendo apenas a ideia geral de seu funcionamento, incluindo força bruta, Baby-Step Giant-Step, Rho de Pollard e Pohlig–Hellman e tem como referência o livro [7].

Força Bruta

A abordagem de força bruta consiste em testar exaustivamente todas as possíveis chaves privadas até encontrar a correta. Sua complexidade é $O(n)$, em que n é a ordem do corpo $\mathbf{F}_q$. Isso significa que seu custo cresce linearmente com a ordem da curva e a chave privada. Embora ineficiente para curvas grandes, serve como referência para avaliar métodos mais avançados.

Big-Step Giant-Step

O método Big-Step Giant-Step otimiza a busca ao dividir o espaço de soluções em duas fases: uma pré-computação de valores (passos pequenos) armazenados em uma tabela e uma busca com saltos maiores (passos grandes). Sua complexidade é proporcional à raiz quadrada da ordem do grupo dos pontos da curva. Apesar de reduzir significativamente as operações em comparação à força bruta (reduz operações para $O(\sqrt{n})$), exige mais memória para armazenar os valores pré-calculados.

Rho de Pollard

O método ρ de Pollard é um algoritmo probabilístico usado para atacar o problema do logaritmo discreto em curvas elípticas (ECDLP). Ele gera sequências pseudoaleatórias de pontos da curva até ocorrer uma colisão, isto é, a repetição de um ponto. Como o grupo é finito, essas colisões permitem determinar o logaritmo discreto. O número médio de iterações necessárias é aproximadamente $1,2533\sqrt{n}$, o que dá ao método complexidade $O(\sqrt{n})$. O nome do algoritmo vem do formato do percurso gerado, semelhante à letra grega ρ .

Pohlig-Hellman

Já o algoritmo de Pohlig-Hellman utiliza a fatoração da ordem do grupo da curva para dividir o problema em subproblemas menores, resolvendo cada um separadamente e combinando as soluções com o Teorema Chinês do Resto. Sua complexidade depende do somatório dos fatores primos da ordem do grupo, sendo especialmente eficiente quando esses fatores são pequenos. O desempenho varia pouco com a chave, pois depende principalmente da estrutura do grupo.

Teorema 4.1 (Teorema Chinês do Resto). Se, para todo $i \in \{1, 2, \dots, k\}$,

$$\text{mdc}(a_i, m_i) = 1,$$

então, para quaisquer $b_1, \dots, b_k$, o sistema

$$\begin{cases} a_1x \equiv b_1 \pmod{m_1} \\ a_2x \equiv b_2 \pmod{m_2} \\ \vdots \\ a_kx \equiv b_k \pmod{m_k} \end{cases}$$

admite solução

$$x_0 = c_1n_1\ell_1 + c_2n_2\ell_2 + \dots + c_kn_k\ell_k,$$

onde c_i é solução de $a_i x \equiv b_i \pmod{m_i}$, e $n_i x \equiv 1 \pmod{m_i}$. tem solução l_i .

Além disso, se y for outra solução, então $y \equiv x_0 \pmod{M}$. E reciprocamente, se $y \equiv x_0 \pmod{M}$, então y também é solução do sistema. $M = m_1.m_2.\dots.m_k$.

Introdução ao Algoritmo de Pohlig-Hellman

- **Objetivo:** Resolver $Q = lP$ onde a ordem n de P é composta.
- **Estratégia:** Reduzir um ECDLP grande em vários ECDLPs menores em subgrupos.
- **Fatoração da Ordem:** Seja a fatoração de n :

$$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$$

- O algoritmo calcula $l_i \equiv l \pmod{p_i^{e_i}}$ para cada i e reconstrói l usando o **Teorema Chinês dos Restos (CRT)**.

Cálculo de $l_i \pmod{p^e}$ Para cada fator p^e , escrevemos l_i na base p :

$$l_i = z_0 + z_1 p + z_2 p^2 + \dots + z_{e-1} p^{e-1}$$

Passo a Passo para os dígitos z_j :

1. **Dígito z_0 :** Define-se $P_0 = \frac{n}{p}P$ e $Q_0 = \frac{n}{p}Q$. Resolve-se $Q_0 = z_0 P_0$ no subgrupo de ordem p .
2. **Dígito z_1 :** Define-se $Q_1 = \frac{n}{p^2}(Q - z_0 P)$. Resolve-se $Q_1 = z_1 P_0$.
3. **Generalização (z_t):**

$$Q_t = \frac{n}{p^{t+1}} \left(Q - \sum_{j=0}^{t-1} z_j p^j P \right) = z_t P_0$$

Exemplo 30 (Algoritmo de Pohlig–Hellman para resolver o ECDLP). Considere a curva elíptica E definida sobre $\mathbb{F}_{7919}$ pela equação

$$E : y^2 = x^3 + 1001x + 75.$$

Seja

$$P = (4023, 6036) \in E(\mathbb{F}_{7919}).$$

A ordem de P é

$$n = 7889 = 7^3 \cdot 23.$$

Seja

$$Q = (4135, 3169) \in \langle P \rangle.$$

Desejamos determinar

$$l = \log_P Q.$$

1. Primeiro determinamos

$$l_1 \equiv l \pmod{7^3}.$$

Escrevemos

$$l_1 = z_0 + z_1 \cdot 7 + z_2 \cdot 7^2$$

e calculamos

$$P_0 = 7^2 \cdot 23 P = (7801, 2071),$$

$$Q_0 = 7^2 \cdot 23 Q = (7801, 2071).$$

Como $Q_0 = P_0$, concluimos que

$$z_0 = 1.$$

Em seguida, calculamos

$$Q_1 = 7 \cdot 23 (Q - P) = (7285, 14)$$

e verificamos que

$$Q_1 = 3P_0.$$

Logo,

$$z_1 = 3.$$

Finalmente, calculamos

$$Q_2 = 23 (Q - P - 3 \cdot 7P) = (7285, 7905)$$

e verificamos que

$$Q_2 = 4P_0.$$

Assim,

$$z_2 = 4.$$

Portanto,

$$l_1 = 1 + 3 \cdot 7 + 4 \cdot 7^2 = 218.$$

2. Em seguida, determinamos

$$l_2 \equiv l \pmod{23}.$$

Calculamos

$$P_0 = 7^3 P = (7190, 7003),$$

$$Q_0 = 7^3 Q = (2599, 759),$$

e verificamos que

$$Q_0 = 10P_0.$$

Logo,

$$l_2 = 10.$$

3. Por fim, resolvemos o sistema de congruências

$$l \equiv 218 \pmod{7^3},$$

$$l \equiv 10 \pmod{23}.$$

Aplicando o Teorema Chinês do Resto, obtemos

$$l = 4334.$$

Portanto,

$$\boxed{\log_P Q = 4334.}$$

Os próximos exemplos ilustra uma comparação entre os algoritmos de ataque ao ECC e tem como referência [11].

Exemplo 31. Foram utilizados a curva elíptica

$$E : y^2 = x^3 + 1001x + 75,$$

definida sobre o corpo finito $\mathbb{F}_{7919}$, juntamente com o ponto gerador

$$P = (4023, 6036).$$

Os valores são a quantidade de somas de pontos realizadas.

CHAVE	Força Bruta	Pohlig-Hellman	BSGS
1000	999	1055	189
2000	1999	1037	200
3000	2999	996	211
4000	3999	978	222
5000	4999	937	234
6000	5999	919	245
7000	6999	878	256

Exemplo 32. Foram utilizados a curva elíptica

$$E : y^2 = x^3 + 5x - 3,$$

definida sobre o corpo finito $\mathbb{F}_{839}$, juntamente com o ponto gerador

$$P = (154, 5).$$

Os valores são a quantidade de somas de pontos realizadas.

CHAVE	Força Bruta	Pohlig-Hellman	BSGS
100	99	560	63
200	199	588	66
300	299	788	70
400	399	643	73
500	499	843	76
600	599	698	80
700	699	553	63
800	799	753	86

Referências

- [1] VAINSENCER, I. *Introdução às Curvas Algébricas Planas*. Coleção Matemática Universitária. 2. ed. Rio de Janeiro: IMPA, 2005.
- [2] GARCIA, A.; LEQUAIN, Y. *Elementos de Álgebra*. 5. ed. Rio de Janeiro: IMPA, 2008.
- [3] SALEHYAN, P. *Curvas Algébricas: uma breve introdução*. Minicurso da VII Semana da Matemática da FEIS–UNESP, Ilha Solteira, 2008.
- [4] OLIVEIRA, T. C. *Área da superfície e volume da Igreja de São Francisco de Assis*. Monografia (Graduação) – Universidade Federal de Minas Gerais, Belo Horizonte, 2017.
- [5] GONÇALVES, T. S. *Uma Introdução à Geometria Projetiva para o Ensino Fundamental*. Dissertação (Mestrado) – Universidade Federal do Rio Grande, Rio Grande, 2013.
- [6] SONG, Jimmy. *Programming Bitcoin: Learn How to Program Bitcoin from Scratch*. Sebastopol: O'Reilly Media, 2019.
- [7] HANKERSON, Darrel; MENEZES, Alfred J.; VANSTONE, Scott. *Guide to Elliptic Curve Cryptography*. New York: Springer, 2004.
- [8] MEIRELES, Tiago Aprigio Bezerra. *Curvas Elípticas e Criptografia*. 2023. Trabalho de Conclusão de Curso (Bacharelado em Matemática) – Faculdade de Matemática, Universidade Federal de Uberlândia, Uberlândia, 2023.
- [9] LARA, P. C. S.; OLIVEIRA, F. B. *Curvas Elípticas: Aplicação em Criptografia Assimétrica*. Petrópolis, RJ: LNCC, [s.d.].
- [10] ANDRADE, H. D. A. *Implementação do Algoritmo ElGamal utilizando Curvas Elípticas e Curvas Hiperelípticas no SageMath*. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – PUC Minas, Belo Horizonte, MG, Brasil, 2025.
- [11] ANDRADE, H. D. A.; OLIVEIRA, N. M. G.; DANTAS, D. A. M. **Um Estudo Sobre Algoritmos de Ataque ao ECC**. *Proceeding Series of the Brazilian Society of Computational and Applied Mathematics*, v. 12, n. 1, 2026. DOI: 10.5540/03.2026.012.01.05094.