GET Criptografia 2 - Material Complementar

Guilherme Cappelli

1 Introdução

Nesse segundo material abordaremos um pouco sobre Teoria dos Grupos de maneira extremamente superficial e simplificada e sua aplicação em Criptografia de Curvas Elípticas. Recomendo fortemente a leitura da seção 4 do material anterior para a compreensão dessa GET.

2 Teoria dos Grupos

Para introduzir esse conceito, surigo uma alusão: Suponha que exista um grupo de 5 amigos que são próximos e outro grupo de 5 colegas de trabalho que não interagem muito, respectivamente G_1 e G_2. Entre eles, podem interagir de formas distintas como um aperto de mãos ou abraço.

Não é um salto muito grande afirmar que os amigos do grupo G_1 se abraçam, já que são próximos, mas para os colegas de trabalho do grupo G_2 talvez não seja tão apropriado, sendo mais provável se cumprimentarem com um aperto de mãos.

Para os dois grupos distintos, são estabelecidas formas de comunicação diferentes, seja o aperto de mão ou o abraço, e na Matemática não é tão diferente.

Definição 2.1

Um conjunto $G \neq \emptyset$ munido com uma operação binária $\circ$, que pode ser $+$ ou $\times$, é chamado de grupo se os seguintes axiomas forem satisfeitos:
(i) Fechado: $a \circ b = c \in G, \forall a, b, c \in G$.
(ii) Associatividade: $(a \circ b) \circ c = a \circ (b \circ c), \forall a, b, c \in G$.
(iii) Elemento Neutro: $\exists\ e \in G : a \circ e = a = e \circ a$.
(iv) Elemento Inverso: $\forall a \in G, \exists\ b \in G : a \circ b = e = b \circ a$.

Contudo, para a criptografia de curva elítpicas vamos usar um grupo específico que será essencial para o Diffie-Hellman, o Grupo Abeliano, que tem uma mais propriedade.

Definição 2.2

Um grupo $(G, \circ)$ é *abeliano* se $\forall a, b \in G : a \circ b = b \circ a \in G$, isto é, vale a propriedade de *comutatividade*.

Considere o conjunto finito $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, perceba que ele contém 9 elementos, em outras palavras, sua cardinalidade $|\mathbb{Z}_9| = 9$. Nesse sentido, se G for um conjunto finito, então $(G, \circ)$ é um *grupo finito*.

Definição 2.3

A *ordem* de um elemento $a \in (G, \circ)$ é o menor inteiro positivo k que satisfaz $a^k = \underbrace{a \circ a \circ \cdots \circ a}_{k \text{ vezes}} = e$, para $e \in G$ o elemento neutro do grupo. Se não existir tal inteiro, então a ordem de a é definida como ∞.

Com efeito, determinemos a ordem de $3 \in (\mathbb{Z}_5^*, \times)$ efetuando a operação binária $\times : \mathbb{Z}_5^* \longrightarrow \mathbb{Z}_5^*$ sucessivamente.

$$3^1 \equiv 3 \mod 5$$
$$3^2 \equiv 4 \mod 5$$
$$3^3 \equiv 2 \mod 5$$
$$3^4 \equiv 1 \mod 5$$

Seja $\text{ord} : G \longrightarrow G$ a função que determina a ordem de um elemento do grupo. Temos que $\text{ord}(3) = 4$, em particular $\text{ord}(3) = |\mathbb{Z}_5^*|$. Se continuarmos realizando essas operações binárias, percebemos um comportamento interessante:

$$3^5 \equiv 3 \mod 5$$
$$3^6 \equiv 4 \mod 5$$
$$3^7 \equiv 2 \mod 5$$
$$3^8 \equiv 1 \mod 5$$

Percebe-se que a sequência $(3, 4, 2, 1)$, que é uma permutação do conjunto do grupo que se repete, mais adiante vamos provar que esse comportamento cíclico é mantido para sempre.

Proposição 2.4

Se $\text{ord}(a) = n$, então existem n potências de a distintas e são elas: $a^0, a^1, a^2, \ldots, a^{n-1}$.

Demonstração: Seja $S := \{a^0, a^1, \ldots, a^{n-1}\}$ e considere a^m, onde $m \in \mathbb{Z}$. Pelo algoritmo da divisão, temos que $m = n \cdot q + r$, para $0 \leq r < n$, isto é, $r \in \{0, 1, \ldots, n-1\}$. Logo, $a^m = a^{nq+r} = (a^n)^q \cdot a^r = e^q a^r = a^r$, ou seja, $a^m \in S$. Suponha, por absurdo, que $a^r = a^s$, para $r \neq s$ e $0 \leq r, s \leq n-1$, temos pela tricotomia da ordem que $r < s$ ou $s < r$, tome sem perda de generalidade $r < s$. Portanto, $0 < s - r < n$ e $a^{s-r} \neq e$, porque $s - r \neq 0$ e $\text{ord}(a) = n$. Contudo, $a^{s-r} = a^s \cdot (a^r)^{-1} = a^r (a^r)^{-1} = e$, absurdo. Segue disso, que para todos $x, y \in S$, temos que $x \neq y$. □

Proposição 2.5

Seja $a \in G$, tal que $\text{ord}(a) = n$, então $a^t = e \iff t$ é múltiplo de n.

Demonstração: ($\Longleftarrow$) Se $t = nq$, então $a^t = a^{nq} = (a^n)^q = e^q = e$. ($\Longrightarrow$) Suponha que $a^t = e$, temos pelo algoritmo da divisão que $t = nq + r$, onde $0 \leq r < n$. Então $e = a^t = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r$. Logo, $a^r = e$, com $0 \leq r < n$, mas como $\text{ord}(a) = n$, então $a^r \neq e$ para $0 < r < n$, então $r = 0$, daí $t = nq$. □

Definição 1.6

Se $G = \{a^n : n \in \mathbb{Z}\}$, então G é um grupo cíclico e a é um de seus *geradores*. Podemos escrever $G = \langle a \rangle$ e dizemos que G é um grupo cíclico gerado por a.

Note que já nos deparamos com um gerador para o grupo $(\mathbb{Z}_5^*, \times)$. Vimos que $\langle 3 \rangle = \{3^n : n \in \mathbb{Z}\} = \{3, 4, 2, 1\}$ que é apenas uma permutação do conjunto $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$.

Definição 2.7

Seja $(G, \circ)$ um grupo. Dado $\emptyset \neq H \subset G$, dizemos que H é um subgrupo de G se atende:
(i) Para todo $a, b \in H$, temos que $a \circ b \in H$
(ii) O elemento neutro de G, $e_G \in H$
(iii) Para todo $h \in H$, existe $h^{-1} \in H$

Definição 2.8

Seja G um grupo e $H \subset G$ um subgrupo de G. Para qualquer $x \in G$, definimos $xH := \{xh : h \in H\}$ como o 'coset' (ou coclasse em pt-BR) à esquerda de H em G. De maneira análoga, temos $Hx := \{hx : h \in H\}$ o 'coset' à direita de H em G.

Perceba que qualquer coset em G é um subconjunto de G. Tome o grupo aditivo $(\mathbb{Z}_4, +)$ e o subgrupo $H \subset \mathbb{Z}_4 = \{0, 2\}$. Temos $H + 1 = \{1, 3\}$ e $H + 3 = \{3, 1\}$, porque $H + 1 = \{0 + 1 \mod 4, 2 + 1 \mod 4\}$ e $H + 3 = \{0 + 3 \mod 4, 2 + 3 \mod 4\}$. Agora, se temos os cosets $H + 0 = \{0, 2\}$ e $H + 2 = \{2, 0\}$, percebemos um comportamento que será demonstrado na proposição abaixo: se eu pego um elemento de um coset e uso-o para criar outro coset, eles serão iguais.

Proposição 2.9

Se $a \in Hb$, então $Ha = Hb$.

k=1 i = 2 j = 3 *Demonstração:* Por hipótese, $a \in Hb \implies a = h_1 b$. Tome $x \in Ha$, por definição, temos $x = h_2 a = (h_2 h_1) b \in Hb \implies Ha \subseteq Hb$. Considere $y \in Hb$, que por definição é $y = h_3 b$. Como $a = h_1 b$, obtemos $h_1^{-1} a = b$, então $y = (h_3 h_1^{-1}) a \in Ha \implies Hb \subset Ha$. Daí, por dupla inclusão, $Ha = Hb$.

Lema 2.10

Seja G um grupo e $H \lhd G$. A *família* de todos os cosets de $Ha, \forall a \in G$ é uma partição de G, isto é, $\bigcup_{i=1}^{n} Ha_i = G$.

Demonstração: Suponha que $Ha \cap Hb \neq \emptyset$ e tome $x \in Ha \cap Hb$.Logo $x = h_1 a$ e $x = h_2 b$ e tomando o inverso de h_1, temos $a = h_1^{-1} x = h_1^{-1} h_2 b$, que implica em $a \in Hb$, pois $h_1^{-1} h_2 \in H$ pela **Definição 2.7**. Pela **Proposição 2.9**, conclui-se que $Ha = Hb$. Além disso, $e_G \in H$, porque H é subgrupo de G, então $e \cdot c \in Hc$, para todo $c \in G$, que implica em $c \in Hc$. Portanto, os cosets formam uma partição de G. □

Lema 2.11

Seja H um subgrupo de G. A ordem de qualquer coset de H é igual a ordem de H.

Demonstração: Seja $f : H \to Ha$ uma função definida por $f(h) = ha$. Como $a^{-1} \in G$, se $f(h_1) = f(h_2)$, temos $h_1 a = h_2 a \implies h_1 = h_2$, portanto f é injetiva. Considere $ha \in Ha$, é fácil ver que $h \in H$, então $f(h) = ha$. Daí, qualquer elemento do contradomínio é imagem de algum elemento do dóminio de f, portanto é sobrejetora. Segue que f é bijetora. □

Teorema de Lagrange

Em um grupo finito, a ordem de qualquer subgrupo divide a ordem do grupo.

Demonstração: Pelo **Lema 2.10**, sabemos que $|G| = |Ha_1| + |Ha_2| + \cdots + |Ha_n|$ e pelo **Lema 2.11**, temos que $|Ha_i| = |H|$, então $|G| = \underbrace{|H| + |H| + \cdots + |H|}_{\text{n vezes}} = n|H|$. Assim, a ordem de G é múltiplo da ordem de qualquer subgrupo H, ou seja, um grupo G só pode ter subgrupos cuja ordem divide $|G|$. □

Proposição 2.13

Se $|G| = n$, para n primo, então G é um grupo cíclico e todo elemento $a \neq e_G$ é gerador.

Demonstração: Considere $a \in G$, se $a \neq e_G$, então $\text{ord}(a) = m \neq 1$. Daí, vale para o subgrupo cíclico $|\langle a \rangle| = m \neq 1$ e pelo **Teorema de Lagrange**, temos que $m|n$. Como $m \neq 1$ e n é primo, então $m = n \Longrightarrow \langle a \rangle = G$. Perceba que esse argumento vale para seja qual for $a \in G \setminus \{e_G\}$, logo o subgrupo cíclico $\langle a \rangle$ tem $m = n$ elementos, então todos elementos de $G \setminus \{e_G\}$ são geradores. □

3 Problema do Logaritmo Discreto

Grupos cíclicos são fundamentais para problemas de logaritmo discreto, pois a partir de um gerador α, conseguimos reconstruir todos os elementos do grupo nas potências do gerador. Dito isso, considere $(\mathbb{Z}_{47}^*, \times)$, cuja cardinalidade é um número primo, e portanto, pelo **Teorema de Lagrange** sabemos que esse grupo é *cíclico*. Com efeito, tome o gerador $\alpha = 5$ do grupo multiplicativo e encontre

$$5^x \equiv 41 \mod 47$$

Talvez você tenha percebido que essa conta é um tanto complicada, pois exige o cálculo de

$$x \equiv \log_5 41 \mod 47$$

Como esse é um problema que envolve números pequenos, com um simples brute-force obtemos o resultado x, mas para números arbitrariamente grandes, temos que recorrer à alguns outros métodos para tentar solucionar o *PLD*.

Problema do Logaritmo Discreto

Dados $\beta \in \mathbb{Z}_n$ para n primo e um gerador α do grupo, encontre x que satisfaça a condição abaixo:

$$\alpha^x \equiv \beta \mod n$$

que é resolvido por $x \equiv \log_\alpha \beta \mod p$.

Vale observar que, esse problema não é efetivo em alguns grupos, são eles: $(\mathbb{Z}/m\mathbb{Z}, +)$, que é resolvido pelo Algoritmo de Euclides; $(\mathbb{R}^*, \times)$ e $(\mathbb{C}^*, \times)$ que são resolvidos pelo próprio logaritmo analítico, etc.

4 Curvas Elípticas

Uma curva elíptica nada tem a ver com elipses, então esqueça imediatamente as elipses e cônicas do querido (e temido) Cálculo 2. Na verdade, as curvas elípticas são curvas algébricas, o que significa que se eu traçar uma reta qualquer nessa curva, ela intersectará uma quantidade finita de pontos da curva.

A lei de grupo das curvas elípticas são construídas geometricamente. Com efeito, mostramos que Curvas Elípticas, em particular para ECC, cujos pontos estão sob um corpo finito $\mathbb{Z}_n$ formam um Grupo Finito Abeliano com uma operação fundamentada no fato de serem curvas algébricas.

Definição 4.1

Uma curva elíptica em $\mathbb{Z}_n$, $n > 3$ é o conjunto de todos os pares coordenados $(x, y) \in \mathbb{Z}_n$ que satisfazem

$$y^2 \equiv x^3 + ax + b \mod n$$

onde $a, b \in \mathbb{Z}_n$.

Para que a curva seja regular, ou seja, não possua cúspide exigimos que o discriminante $\Delta = 4a^3 + 27b^3 \neq 0$. Para formarmos um grupo, denote $\mathcal{O}$ como o elemento neutro no 'infinito' e defina o conjunto de pontos $E := \{(x, y) : y^2 \equiv x^3 + ax + b \mod n\} \cup \{\mathcal{O}\}$.

Caso queiramos verificar a pertinência de um ponto P na curva, basta computarmos $y^2 - x^3 - ax - b \mod n$. Se for congruente a zero, temos $P \in E$, caso contrário $P \notin E$.

Exemplo

Seja $E_1 := \{(x, y) \in \mathbb{R}^2 : y^2 = x^3 - 2x + 2\}$ e $E_2 := \{(x, y) : y^2 = x^3 - 2x + 2 \mod n\} \cup \{\mathcal{O}\}$. Quando estamos em E_1 podemos elevar ambos os lados da equação da curva por $1/2$ e obtemos $y = \pm\sqrt{x^3 - 2x + 2}$. Note que a curva é simétrica em relação ao eixo x.

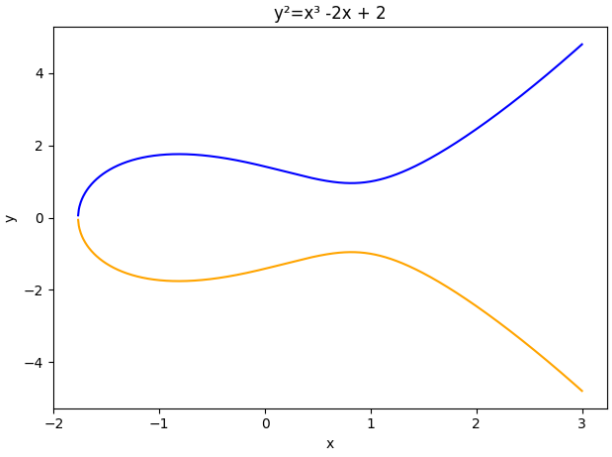

Figure 1: Curva Elíptica em $\mathbb{R}$

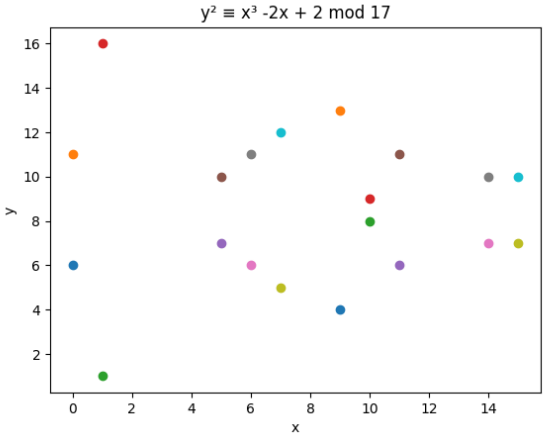

Figure 2: Curva Elíptica em $\mathbb{Z}_p$

Figure 3: Comparação entre curvas elípticas em $\mathbb{R}$ e no corpo finito $\mathbb{Z}_p$.

5 Grupos e Curvas Elípticas

Para definirmos o nosso grupo, precisamos de um conjunto finito de pontos e um operador de grupo, são eles:

- O conjunto $\{(x, y) \in \mathbb{Z}_n \equiv y^2 \equiv x^3 + ax + b \mod n\} \cup \{\mathcal{O}\}$.
- Operador de Adição $(+)$.

A curva elíptica sob um corpo finito munida com a operação de adição é um Grupo Finito Aditivo. Entretanto, essa operação será definida geometricamente para atender a condição do grupo ser fechado.

$$P + Q = R$$

onde $P = (x_P, y_P), Q = (x_Q, y_Q)$ e $R = (x_R, y_R)$.

5.1 Adição de Pontos ($P \neq Q$)

Nesse cenário, o ponto R é obtido ao traçar uma reta entre os pontos P e Q que, por definição, intersecta a curva em outro ponto, digamos R'. Por fim, esse ponto é espelhado em relação ao eixo x da seguinte maneira:

$$R' = (x_{R'}, y_{R'}) \Longrightarrow R = (x_R, -y_{R'}) \qquad \text{OBS: } R = -R'$$

Sejam a curva elíptica $E := \{(x, y) \in \mathbb{Z}_n : y^2 \equiv x^3 + ax + b \mod n\} \cup \{\mathcal{O}\}$ e os pontos $P = (x_P, y_P), Q = \{x_Q, y_Q\} \in E$. A reta r que passa por P e Q tem equação $y = sx + m$, onde s é o coeficiente angular dessa reta, que é dado por

$$s = \frac{y_Q - y_P}{x_Q - x_P} \equiv (y_Q - y_P) \cdot (x_Q - x_P)^{-1} \mod n$$

Para encontrar as interseções da reta com a curva, basta substituirmos y em E

$$\begin{aligned}
(sx + m)^2 &= x^3 + ax + b \\
s^2x^2 + 2smx + m^2 &= x^3 + ax + b \\
x^3 - s^2x^2 - 2smx - m^2 + ax + b &= 0 \\
x^3 - s^2x^2 + (a - 2sm)x + (b - m^2) &= 0 \qquad (1)
\end{aligned}$$

Como uma equação cúbica tem três raízes, que nesse caso seriam as coordenadas parciais x_P, x_Q e x_R, podemos reescrever a equação característica como

$$x^3 + ax^2 + bx + c = (x - x_P)(x - x_Q)(x - x_R)$$

onde $a \neq 0$. Expandindo o lado direito dessa equação obtemos

$$\begin{aligned}
&(x - x_P)(x - x_Q)(x - x_R) = \\
&= (x^2 - (x_P + x_Q)x + x_Px_Q)(x - x_R) = \\
&= x^3 - (x_P + x_Q + x + R)x^2 + (x_Px_Q + x_Px_R + x_Qx_R)x - x_Px_Qx_R \qquad (2)
\end{aligned}$$

Igualando os coeficientes das equações **(1)** e **(2)** pelo grau de x conseguimos encontrar o valor desejado de x_R.

$$\begin{cases}
-sx^2 = -(x_P + x_Q + x_R)x^2 \\
(a - 2sm)x = (x_Px_Q + x_Px_R + x_Qx_R)x \\
(b - m^2) = -x_Px_Qx_R
\end{cases}$$

Pela primeira linha do sistema, temos

$$-s^2 = -(x_P + x_Q + x_R) \Longrightarrow s^2 = (x_P + x_Q + x_R)$$

Se colocarmos esses valores em função de x_R,

$$x_R = s^2 - x_P - x_Q$$

Como agora temos x_R, é possível determinar o valor de y_R partindo da equação da reta entre P e R'

$$s = \frac{y'_R - y_P}{x_R - x_P}$$

Com uma simples manipulação algébrica é encontrado y'_R

$$s(x_R - x_P) = y'_R - y_P \Longrightarrow y'_R = s(x_R - x_P) + y_P$$

Como $y_R = -y'_R$, temos

$$y_R = s(x_P - x_R) - y_P$$

5.2 Point Doubling (P=Q)

Quando os pontos P e Q são iguais, o ponto R é resultado de

$$R = P + Q = P + P = 2P$$

Suponha que existam dois pontos $P \neq Q \in E$ arbitrariamente próximos e que é traçada uma reta secante que passa por P e Q. Imagine que o ponto Q vai se aproximando cada vez mais de P, e que isso acontece de tal maneira que a distância final entre eles seja infinitesimal. Assim, os pontos P, Q vão coincidir e a reta tocará o ponto $P = Q$.

Isso que descrevemos é a Reta Tangente, que também tem equação $y = sx + m$. Dessa vez, o coeficiente angular é dado pela derivada de $y^2 = x^3 + ax + b$. Para isso vamos derivar primeiro para $y > 0$

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

$$\frac{dy}{dx} = \frac{d}{dx}(\sqrt{x^3 + ax + b}) = \frac{d}{dx}(x^3 + ax + b)^{1/2}$$

Pela Regra da Cadeia,

$$\frac{dy}{dx} = \frac{1}{2}(x^3 + ax + b)^{-1/2} \cdot (3x^2 + a)$$

$$\frac{dy}{dx} = \frac{3x^2 + a}{2\sqrt{x^3 + ax + b}}$$

Como $y = \sqrt{x^3 + ax + b}$, substituimos

$$\frac{dy}{dx} = \frac{3x^2 + a}{2y}$$

Entretanto, $2y$ já leva em consideração o sinal de y, portanto, não é necessário derivar para $y < 0$ para concluirmos que

$$s = \frac{3x^2 + a}{2y}$$

Já calculamos previamente os valores de x_R e y_R, basta substituir o valor de s e $P = Q$

$$x_R = s^2 - 2x_P \qquad\qquad y_R = s(x_P - x_R) - y_P$$

5.3 Elemento Neutro do Grupo ($\mathcal{O}$)

O questionamento do que acontece quando a reta que passa por P e Q for vertical ao eixo x é mais do que razoável. Em termos mais precisos, esse cenário ocorre quando $P = (x, y)$ e $Q = (x, -y)$. Para isso, definimos um ponto no 'infinito', denotado por $\mathcal{O}$, por onde toda reta vertical passa.

Tal definição vem da Geometria Projetiva, mas como são duas horas pra GET e ficaria muito conteúdo, prefiro apenas mostrar uma intuição para explicar porquê das retas verticais se encontrarem no infinito.

Lembremos que, na Geometria Afim, uma curva elíptica é descrita pela equação $y^2 = x^3 + ax + b$, onde os pontos estão no plano usual (x, y). Entretanto, se considerarmos coordenadas projetivas, que

tem forma $(X : Y : Z)$, nós adicionamos um 'horizonte' ao espaço que nos permite dizer que pontos no infinito existem.

Nesse contexto a equação da curva elíptica terá o seguinte formato $Y^2Z = x^3 + aXZ^2 + bZ^3$. Para encontrar os pontos no infinito, considere $Z = 0$ e substitua na equação:

$$Y^2 \cdot 0 = X^3 + aX \cdot 0^2 + b \cdot 0^3 \Longrightarrow X^3 = 0$$

que nos resulta um único ponto projetivo no infinito: $\mathcal{O} := (0 : 1 : 0)$.

Perceba que todas as retas verticais $x = c$, para c constante, convergem para o mesmo ponto $(0 : 1 : 0)$ no infinito. Usaremos $\mathcal{O}$ como elemento neutro do grupo, para que a operação $P - P$ sempre tenha solução no grupo, e que tal solução seja o elemento neutro $\mathcal{O}$.

Vale ressaltar, que, por definição, $-P = (x_P, -y_P)$, mas como estamos sob um corpo finito, queremos que $y_P + (-y_P) \equiv 0 \mod n$. É fácil ver, que $y_P + (n - y_P) = n \equiv 0 \mod n$. Portanto,

$$-P = (x_P, n - y_P) \mod n$$

5.4 Lei de Grupo

Sejam $E : y^2 \equiv x^3 + ax + b \mod n$ uma curva elíptica sob o corpo finito $\mathbb{Z}_n$, $P = (x_P, y_P), Q = (x_Q, y_Q) \in E$ onde $P, Q \neq \mathcal{O}$. Defina $P + Q = R = (x_R, y_R)$ como:

$$x_R \equiv s^2 - x_P - x_Q \mod n$$
$$y_R \equiv s(x_P - x_R) - y_P \mod n$$

$$s = \begin{cases} (y_Q - y_P) \cdot (x_Q - x_P)^{-1} \mod n, & \text{se} \quad P \neq Q \\ (3x_P^2 + a) \cdot (2y_P)^{-1} \mod n, & \text{se } P = Q \end{cases}$$

Se $x_P = x_Q$, mas $y_P \neq y_Q$, então $P + Q = \mathcal{O}$; e se $P = Q$ e $y_P = 0$, então $P + Q = \mathcal{O}$. Além disso, tome $P + \mathcal{O} = P$, para todos pontos P em E.

Lema 5.1

A soma de pontos sobre uma curva elíptica E satisfaz as seguintes propriedades:
(i) Fechado em relação a adição.
(ii) $P + Q = Q + P$, para todos $P, Q \in E$.
(iii) $P + \mathcal{O} = P$, para todos pontos P em E.
(iv) Dado $P \in E$, existe $P' \in E$ tal que $P + P' = \mathcal{O}$, que será denotado por $-P$.
(v) $(P + Q) + R = P + (Q + R)$, para todos $P, Q, R \in E$.
em outras palavras esse é um grupo abeliano.

Demonstração: (i) Perceba que pela própria construção geométrica da operação, conferimos ao grupo a propriedade de E ser fechado em relação a operação de adição. (ii) Como a reta que passa por P e Q é a mesma reta que passa por Q e P, vale a comutatividade. (iii) Por definição, existe $\mathcal{O}$. (iv) Como a curva elíptica é simétrica em relação ao eixo x, existe $-P = (x_P, -y_P)$. (v) A prova da associatividade do grupo é estupidamente complicada e não será demonstrada. Portanto, $(E, +)$ é um grupo abeliano. □

Teorema 5.2

O grupo aditivo em Curvas Elíptica sobre um corpo finito $\mathbb{Z}_n$ é *cíclico*.

Demonstração: Como pelo **Lema 5.1**, temos que $E := \{(x, y) : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$ constitui um grupo abeliano aditivo, então $E := \{(x, y) : y^2 \equiv x^3 + ax + b \mod n\} \cup \{\mathcal{O}\}$ é um grupo finito aditivo abeliano. Nesse sentido, se $|E|$ for primo, pela **Proposição 2.13**, temos um grupo *cíclico*. □

Exemplo Prático

Seja $E := \{(x, y) : y^2 \equiv x^3 + 2x + 2 \mod 17\}$ de $|E| = 19$. Tome o ponto $P = (5, 1)$, podemos verificar sua pertinência a curva com $y^2 - x^3 - 2x - 2 \equiv 0 \mod 17$. Se $P \in E$, então como $|E| = 19$ temos que P é gerador.

$$1^2 - 5^2 - 2(5) - 2 = 136$$

$$136 = 8 \cdot 17 + 0 \Longrightarrow 136 \equiv 0 \mod 17$$

Vamos computar adições consecutivas de P e vejamos se eventualmente teremos $nP = \mathcal{O}$. A fim de fixar o conteúdo visto, farei a soma $2P$ manualmente:

$$s \equiv (3x_P^2 + a) \cdot (2y_P)^{-1} \mod n$$

$$s \equiv (3(5)^2 + 2) \cdot (2)^{-1} \mod 17$$

$$s \equiv (3 \cdot 25 + 2) \cdot 9 \equiv 13 \mod 17$$

Assim,

$$\begin{aligned} x_R &\equiv s^2 - 2x_P \mod n \\ &\equiv (13)^2 - 2 \cdot 5 \mod 17 \\ &= 6 \mod 17 \end{aligned} \qquad \begin{aligned} y_R &\equiv s(x_P - x_R) - y_P \mod n \\ &\equiv 13(5 - 6) - 1 \mod 17 \\ &\equiv 3 \mod 17 \end{aligned}$$

$$2P = (6, 3)$$

E assim segue,

$$\begin{aligned} 2P &\equiv (6, 3) \\ 3P &\equiv 2P + P = (10, 6) \\ 4P &\equiv 3P + P = (3, 1) \\ 5P &\equiv (9, 16) \\ 6P &\equiv (16, 13) \\ 7P &\equiv (0, 6) \\ 8P &\equiv (13, 7) \\ 9P &\equiv (7, 6) \\ 10P &\equiv (7, 11) \end{aligned} \qquad \begin{aligned} 11P &\equiv (13, 10) \\ 12P &\equiv (0, 11) \\ 13P &\equiv (16, 4) \\ 14P &\equiv (9, 1) \\ 15P &\equiv (3, 16) \\ 16P &\equiv (10, 11) \\ 17P &\equiv (6, 14) \\ 18P &\equiv (5, 16) \\ 19P &\equiv 18P + P \end{aligned}$$

Perceba que $17 \equiv 0 \mod 17 \Longrightarrow 16 \equiv -1 \mod 17$, e por definição $-P = (x_P, -y_P)$. Logo, $P = (5, 1) \Longrightarrow -P = (5, -1) = 18P$ e então $19P = P + (-P) = \mathcal{O}$.

6 Variante de Menezes e Vanstone para o ElGamal

Em 1985, o Criptógrafo Taher Elgamal criou um sistema de criptografia baseado no **Problema do Logaritmo Discreto** em Curvas Elípticas, que usa um mecanismo público de acordo de chaves, o **Diffie-Hellman**.

Dez anos depois, os matemáticos Alfred Menezes e Scott Vanstone elaboraram uma versão alternativa para o ElGamal em que não é necessário pré-codificar a mensagem como um ponto na curva. Esse sistema não altera a segurança da criptografia e, por isso, vou usar como exemplo de Criptografia de Curvas Elípticas nesse material.

A chave pública desse sistema é: $pub\_key = (n, E, P)$. Já a chave privada vem do problema do logaritmo discreto, onde

$$T = \underbrace{P + P + \cdots + P}_{k \text{ vezes}} = kP$$

A dificuldade de decriptar uma mensagem se dá em encontrar k, logo $priv\_key = k$.

6.1 Diffie-Hellman (Troca de Chaves)

Suponha que dois amigos Alice e Bob queiram testar essa criptografia em um canal público. Para isso, eles precisam entrar em um consenso sobre quais serão as chaves pública e privada, e nesse sentido, Alice e Bob escolhem inteiros k_A e k_B como suas chaves privadas, respectivamente.

Alice e Bob encontram os pontos A e B e trocam essa informação no canal público.

$$A = k_A P \qquad\qquad B = k_B P$$

Com esses segredos compartilhados em mãos, cada um obtém um novo ponto $T = (x_T, y_T)$ da curva que será usado para encriptar a mensagem

$$T = k_A B \qquad\qquad T = k_B A$$

$$T = k_A k_B P \xrightarrow[\text{Abeliano}]{} T = k_B k_A P$$

Nesse teste, Alice vai enviar a mensagem m para Bob, mas como já sabemos, não é possível encriptar uma mensagem sem codificá-la previamente. Adotando os métodos *bytes_to_long* e *long_to_bytes*, obtemos

$$m' = 65692885099055597532957417782617275609506 49$$

Entretanto, ainda precisamos transformar essa mensagem em um ponto no plano cartesiano, que será feito ao quebrar em dois essa mensagem codificada. Deve-se ter bastante cautela para que os valores não se iniciem em zero, porque na hora de converter de volta, os zeros que eram essenciais na codificação desaparecem e não conseguimos obter a mensagem original.

$$m = (m_1, m_2)$$

$$m = (6569288509905559753295741778261727560950649)$$

6.2 Encriptando e Decriptando a Mensagem

Como Alice e Bob já trocaram suas chaves na etapa do Diffie-Hellman e ambos já possuem T, então Alice encripta a mensagem m em uma simples passo:

$$x_S \equiv x_T \cdot m_1 \mod n$$

$$y_S \equiv y_T \cdot m_2 \mod n$$

Em seguida, ela envia a mensagem encriptada (x_S, y_S) para Bob, que por sua vez, pode decriptar a mensagem ao encontrar o inverso multiplicativo de sua chave $T = (x_T, y_T)$ em $\mathbb{Z}_n$.

$$x_T^{-1} \cdot x_S \equiv x_T^{-1} \cdot x_T \cdot m_1 \equiv m_1 \mod n$$

$$y_T^{-1} \cdot y_S \equiv y_T^{-1} \cdot y_T \cdot m_2 \equiv m_2 \mod n$$

Perceba que para isso precisamos $\text{mdc}(x_T, n) = \text{mdc}(y_T, n) = 1$, para existirem x_T^{-1} e $y_T^{-1} \in \mathbb{Z}_n$. Quando n é primo e $x_T, y_T < n$ garantimos essa condição.

Exemplo Prático

Sejam

$$n = 68468698583326932648793823668667977345 69$$
$$E : \{(x, y) : y^2 \equiv x^3 + x + 1 \mod n\} \cup \{\mathcal{O}\}$$
$$P = (0, 1)$$

Alice e Bob geram dois números inteiros 'aleatórios' para suas chaves privadas na etapa de Diffie-Hellman e calculam $A = k_A P$ e $B = k_B P$, respectivamente.

$$k_A = 394756376$$
$$A = k_A P$$

$$k_B = 4857628576$$
$$B = k_B P$$

Assim, os pontos A e B são trocados pelo canal de comunicação

$$A = (132155833514596227411159749086721101325 5, 465112924000968106419957886949913791803 3)$$

$$B = (422061900257492441516394928629041653952 3, 179076010304836427257727577914388125458 0)$$

Para Alice enviar a mensagem $m = (656928850990555975329, 5741778261727560950649)$, ela deve primeiro calcular $T = k_A B$ e Bob, $T = k_B A$.

$$T = (338859256239172459526871882992404398021 3, 129495594649667554566611905764330384728)$$

Basta Alice encontrar o ponto $S = (x_S, y_S)$, que é a mensagem encriptada na curva e enviá-la para Bob.

$$x_S \equiv x_T \cdot m_1 \mod n$$
$$y_S \equiv y_T \cdot m_2 \mod n$$

$$x_S \equiv 45290498516610770328017806827982556170 77 \mod n$$
$$y_S \equiv 16426341661398620329906137533798810675 58 \mod n$$

Bob recebe o ponto S e decripta o ciphertext com sua chave privada T.

$$x_T \cdot x_S \equiv x_T^{-1} \cdot x_T \cdot m_1 \equiv m_1 \mod n$$

$$y_T^{-1} \cdot y_S \equiv y_T^{-1} \cdot y_T \cdot m_2 \equiv m_2 \mod n$$

Para transformar de volta em texto, Bob junta as coordenadas m_1 e m_2 em uma única string e converte via *long_to_bytes*. Fica de exercício de fixação achar a mensagem original.

7 Assinatura Digital (ECDSA)

Uma assinatura digital tem como propósito identificar o Autor de uma mensagem de forma única, ou seja, somente o autor pode ser capaz de gerar sua assinatura digital. Assim, ele não pode negar a autoria da mensagem.

Existem alguns algoritmos de assinatura digital, mas atualmente Criptografias de Curvas Elípticas

são amplamente utilizadas com esse propósito, principalmente porque elas usam chaves de menor tamanho e são mais ágeis.

ECDSA ("Algoritmo de Assinatura Digital em Curvas Elípticas" em pt-BR) é implementado desde a infraestrutura do certificado de segurança SSL e TLS, até endereços de Bitcoins.

7.1 Algoritmo

Suponha que Alice e Bob agora queiram testar o ECDSA. Para isso, eles devem concordar nos parâmetros da curva (n, E, P), com $|E|$ primo.

Alice vai mandar a mesma mensagem m, só que dessa vez ela vai assinar usando ECDSA. Primeiro, ela gear um inteiro $d_A \in \{1, \ldots, n-1\}$ como sua chave privada e calcula o ponto da curva $Q_A = d_A \times P$ como chave pública. Com isso em mãos, ela vai seguir o algoritmo abaixo

1. Calcule a hash dessa mensagem: $e = \text{HASH}(m)$
2. Defina z como os $L_{|E|}$ bits mais à esquerda de e, onde $L_{|E|}$ é o comprimento em bits da ordem do gerador.
3. Escolha $k \in \{1, \ldots, n-1\}$
4. Calcule $(x_1, y_1) = kP$
5. Calcule $r \equiv x_1 \mod |E|$ e se $r = 0$, volte para a etapa 3
6. Calcule $s \equiv k^{-1}(z + r \cdot d_A) \mod |E|$ e se $s = 0$, volte para a etapa 3

No final desse processo, Alice obtém o par (r, s) que é sua assinatura digital em ECDSA.

7.2 Verificação de Assinatura

Após Bob receber a mensagem com a assinatura de Alice, ele pode autenticar a mesma utilizando a chave pública previamente acordada.

Antes de tudo, ele verifica se $Q_A \in E$ ao calcular $|E| \cdot Q_A$, se $|E|Q_A = \mathcal{O}$, a assinatura é autêntica. Entretanto, Bob ainda tem que descobrir se essa assinatura pertence a Alice.

1. Verifique se $r, s \in \{1, n-1\}$
2. Calcule $e = \text{HASH}(m)$
3. Considere z como os $L_{|E|}$ bits mais à esquerda de e.
4. Encontre o inverso multiplicativo de s em $\mathbb{Z}_{|E|} : w \equiv s^{-1} \mod |E|$
5. Calcule $u_1 \equiv zw \mod |E|$ e $u_2 \equiv rw \mod |E|$
6. Calcule o ponto da curva $(x_1, y_1) = u_1 \cdot P + u_2 \cdot Q_a$, se $(x_1, y_1) = \mathcal{O}$ a assinatura é inválida.
7. Se $r \equiv x_1 \mod |E|$, a assinatura é válida.

7.3 Ataque à ECDSA

Se um mesmo k for usado para assinar duas mensagens distintas, é possível recuperar a chave privada do autor através de algumas simples operações.

Lembrando que, k igual para duas assinaturas implica em r ser o mesmo também, visto que

$$r \equiv (k \cdot P)_x \mod |E|$$

Contudo, k igual não implica em s iguais para as duas assinaturas. Na verdade, esse fato apenas dá a brecha para o ataque.

Suponha que temos duas mensagens diferentes cujas hashes são z_1 e z_2, respectivamente. O inverso multiplicativo de k continua sendo o mesmo, tanto para s_1 quanto para s_2 e o valor de rd_A também se mantém.

$$s_1 \equiv ((z_1 + rd_A) \cdot k^{-1}) \mod |E|$$

$$s_2 \equiv ((z_2 + rd_A) \cdot k^{-1}) \mod |E|$$

Com uma simples manipulação algébrica,

$$s_1 - s_2 \equiv ((z_1 + rd_A) \cdot k^{-1}) - ((z_2 + rd_A) \cdot k^{-1}) \mod |E|$$

$$(z_1 + rd_A - z_2 - rd_A) \cdot k^{-1} \equiv (z_1 - z_2) \cdot k^{-1} \mod |E|$$

Mas isso tudo é congruente a diferença entre s_1 e s_2

$$(s_1 - s_2) \equiv (z_1 - z_2) \cdot k^{-1} \mod |E|$$

Multiplicando k de ambos os lados,

$$(s_1 - s_2) \cdot k \equiv (z_1 - z_2) \mod |E|$$

Dessa forma, k pode ser facilmente obtido com o cálculo abaixo

$$k \equiv (z_1 - z_2) \cdot (s_1 - s_2)^{-1} \mod |E|$$

Com k em mãos, é possível colocar tudo em função de d_A a partir da congruência

$$s_1 \equiv ((z_1 + rd_A) \cdot k^{-1}) \mod |E|$$

Novamente, multiplicamos k de ambos os lados

$$(z_1 + rd_A) \equiv s_1 \cdot k \mod |E|$$

$$rd_A \equiv (s_1 \cdot k - z_1) \mod |E|$$

Portanto, a chave privada é a solução de

$$d_A \equiv (s_1 \cdot k - z_1) \cdot r^{-1} \mod |E|$$