BREVE INTRODUÇÃO À CRIPTOGRAFIA COM CURVAS ELÍPTICAS

Rodrigo Salomão

JOGA 2011

Programa do Minicurso

Programa do Minicurso

1. Notações e Definições Básicas;

Programa do Minicurso

1. Notações e Definições Básicas;
   - Anel dos inteiros módulo “m”;

Programa do Minicurso

1. Notações e Definições Básicas;
   - Anel dos inteiros módulo “m”;
   - Corpos finitos;

Programa do Minicurso

1. Notações e Definições Básicas;
   - Anel dos inteiros módulo “m”;
   - Corpos finitos;
   - Estrutura de grupo;

Programa do Minicurso

1. Notações e Definições Básicas;
   - Anel dos inteiros módulo “m”;
   - Corpos finitos;
   - Estrutura de grupo;
2. Sistemas de Criptografia;

Programa do Minicurso

1. Notações e Definições Básicas;
   - Anel dos inteiros módulo “m”;
   - Corpos finitos;
   - Estrutura de grupo;
2. Sistemas de Criptografia;
   - Sistema de chave privada;

Programa do Minicurso

1. Notações e Definições Básicas;
   - Anel dos inteiros módulo “m”;
   - Corpos finitos;
   - Estrutura de grupo;
2. Sistemas de Criptografia;
   - Sistema de chave privada;
   - O problema do logaritmo discreto;

Programa do Minicurso

1. Notações e Definições Básicas;
   - Anel dos inteiros módulo “m”;
   - Corpos finitos;
   - Estrutura de grupo;
2. Sistemas de Criptografia;
   - Sistema de chave privada;
   - O problema do logaritmo discreto;
   - Sistema de chave pública;

Programa do Minicurso

1. Notações e Definições Básicas;
   - Anel dos inteiros módulo “m”;
   - Corpos finitos;
   - Estrutura de grupo;
2. Sistemas de Criptografia;
   - Sistema de chave privada;
   - O problema do logaritmo discreto;
   - Sistema de chave pública;
3. Curvas Elípticas;

Programa do Minicurso

1. Notações e Definições Básicas;
   - Anel dos inteiros módulo “m”;
   - Corpos finitos;
   - Estrutura de grupo;
2. Sistemas de Criptografia;
   - Sistema de chave privada;
   - O problema do logaritmo discreto;
   - Sistema de chave pública;
3. Curvas Elípticas;
   - Forma de Weierstrass;

Programa do Minicurso

1. Notações e Definições Básicas;
   - Anel dos inteiros módulo “m”;
   - Corpos finitos;
   - Estrutura de grupo;
2. Sistemas de Criptografia;
   - Sistema de chave privada;
   - O problema do logaritmo discreto;
   - Sistema de chave pública;
3. Curvas Elípticas;
   - Forma de Weierstrass;
   - A estrutura de grupo;

Programa do Minicurso

1. Notações e Definições Básicas;
   - Anel dos inteiros módulo “m”;
   - Corpos finitos;
   - Estrutura de grupo;
2. Sistemas de Criptografia;
   - Sistema de chave privada;
   - O problema do logaritmo discreto;
   - Sistema de chave pública;
3. Curvas Elípticas;
   - Forma de Weierstrass;
   - A estrutura de grupo;
   - Curvas elípticas sobre corpos finitos;

Programa do Minicurso

1. Notações e Definições Básicas;
   - Anel dos inteiros módulo “m”;
   - Corpos finitos;
   - Estrutura de grupo;
2. Sistemas de Criptografia;
   - Sistema de chave privada;
   - O problema do logaritmo discreto;
   - Sistema de chave pública;
3. Curvas Elípticas;
   - Forma de Weierstrass;
   - A estrutura de grupo;
   - Curvas elípticas sobre corpos finitos;
   - O problema do logaritmo discreto para curvas elípticas;

Programa do Minicurso

1. Notações e Definições Básicas;
   - Anel dos inteiros módulo “m”;
   - Corpos finitos;
   - Estrutura de grupo;
2. Sistemas de Criptografia;
   - Sistema de chave privada;
   - O problema do logaritmo discreto;
   - Sistema de chave pública;
3. Curvas Elípticas;
   - Forma de Weierstrass;
   - A estrutura de grupo;
   - Curvas elípticas sobre corpos finitos;
   - O problema do logaritmo discreto para curvas elípticas;
   - Um sistema de criptografia sobre curvas elípticas;

Notações e Definições Básicas

Sejam $m > 1$ e a e b dois inteiros.

Notações e Definições Básicas

Sejam $m > 1$ e a e b dois inteiros. Dizemos que a e b são *congruentes módulo* m, quando m divide $a - b$.

Notações e Definições Básicas

Sejam $m > 1$ e a e b dois inteiros. Dizemos que a e b são *congruentes módulo* m, quando m divide $a - b$. Notação: $a \equiv b \bmod m$.

Notações e Definições Básicas

Sejam $m > 1$ e a e b dois inteiros. Dizemos que a e b são *congruentes módulo* m, quando m divide $a - b$. Notação: $a \equiv b \bmod m$. Temos as seguintes classes deste relação de equivalência:

Notações e Definições Básicas

Sejam $m > 1$ e a e b dois inteiros. Dizemos que a e b são *congruentes módulo* m, quando m divide $a - b$. Notação: $a \equiv b \bmod m$. Temos as seguintes classes deste relação de equivalência:

$$\begin{aligned}
\overline{0} &:= \{n \in \mathbb{Z} \mid n \equiv 0 \bmod m\} = \{n \in \mathbb{Z} \mid n = q \cdot m \text{ para algum } q \in \mathbb{Z}\};\\
\overline{1} &:= \{n \in \mathbb{Z} \mid n \equiv 1 \bmod m\} = \{n \in \mathbb{Z} \mid n = q \cdot m + 1 \text{ para algum } q \in \mathbb{Z}\};\\
\overline{2} &:= \{n \in \mathbb{Z} \mid n \equiv 2 \bmod m\} = \{n \in \mathbb{Z} \mid n = q \cdot m + 2 \text{ para algum } q \in \mathbb{Z}\};\\
\overline{3} &:= \{n \in \mathbb{Z} \mid n \equiv 3 \bmod m\} = \{n \in \mathbb{Z} \mid n = q \cdot m + 3 \text{ para algum } q \in \mathbb{Z}\};\\
&\vdots\\
\overline{m-1} &:= \{n \in \mathbb{Z} \mid n \equiv m - 1 \bmod m\}\\
&= \{n \in \mathbb{Z} \mid n = q \cdot m + (m-1) \text{ para algum } q \in \mathbb{Z}\};
\end{aligned}$$

Notações e Definições Básicas

Sejam $m > 1$ e a e b dois inteiros. Dizemos que a e b são *congruentes módulo* m, quando m divide $a - b$. Notação: $a \equiv b \bmod m$. Temos as seguintes classes deste relação de equivalência:

$$\begin{aligned}
\overline{0} &:= \{n \in \mathbb{Z} \mid n \equiv 0 \bmod m\} = \{n \in \mathbb{Z} \mid n = q \cdot m \text{ para algum } q \in \mathbb{Z}\};\\
\overline{1} &:= \{n \in \mathbb{Z} \mid n \equiv 1 \bmod m\} = \{n \in \mathbb{Z} \mid n = q \cdot m + 1 \text{ para algum } q \in \mathbb{Z}\};\\
\overline{2} &:= \{n \in \mathbb{Z} \mid n \equiv 2 \bmod m\} = \{n \in \mathbb{Z} \mid n = q \cdot m + 2 \text{ para algum } q \in \mathbb{Z}\};\\
\overline{3} &:= \{n \in \mathbb{Z} \mid n \equiv 3 \bmod m\} = \{n \in \mathbb{Z} \mid n = q \cdot m + 3 \text{ para algum } q \in \mathbb{Z}\};\\
&\vdots\\
\overline{m-1} &:= \{n \in \mathbb{Z} \mid n \equiv m - 1 \bmod m\}\\
&= \{n \in \mathbb{Z} \mid n = q \cdot m + (m-1) \text{ para algum } q \in \mathbb{Z}\};
\end{aligned}$$

O conjunto destas classes

$$\mathbb{Z}_m := \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$$

será chamado de *anel dos inteiros módulo* m.

Notações e Definições Básicas

A palavra anel se dá pelo fato das operações

$$\begin{array}{rcll} \overline{a} + \overline{b} & := & \text{classe no qual } a+b \text{ pertence} & = \overline{a+b} \\ \overline{a} \cdot \overline{b} & := & \text{classe no qual } a \cdot b \text{ pertence} & = \overline{a \cdot b} \end{array}$$

definirem uma estrutura de anel em $\mathbb{Z}_m$, com $\overline{0}$ como elemento neutro da soma e $\overline{1}$ como elemento neutro do produto.

Notações e Definições Básicas

A palavra anel se dá pelo fato das operações

$$\begin{array}{rcccl} \overline{a}+\overline{b} & := & \text{classe no qual } a+b \text{ pertence} & = & \overline{a+b} \\ \overline{a}\cdot\overline{b} & := & \text{classe no qual } a\cdot b \text{ pertence} & = & \overline{a\cdot b} \end{array}$$

definirem uma estrutura de anel em $\mathbb{Z}_m$, com $\overline{0}$ como elemento neutro da soma e $\overline{1}$ como elemento neutro do produto.
Além disso, no caso em que p é primo temos as seguintes propriedades nos anéis dos inteiros módulo p:

1. Se $\overline{a}\cdot\overline{b}=\overline{0}$, então $\overline{a}=\overline{0}$ ou $\overline{b}=\overline{0}$;
2. Para cada $\overline{a}\neq\overline{0}$, existe $\overline{a}^{-1}\in\mathbb{Z}_p$ tal que $\overline{a}\cdot\overline{a}^{-1}=\overline{1}$

Notações e Definições Básicas

A palavra anel se dá pelo fato das operações

$$\begin{array}{rcccl} \overline{a}+\overline{b} & := & \text{classe no qual } a+b \text{ pertence} & = & \overline{a+b} \\ \overline{a}\cdot\overline{b} & := & \text{classe no qual } a\cdot b \text{ pertence} & = & \overline{a\cdot b} \end{array}$$

definirem uma estrutura de anel em $\mathbb{Z}_m$, com $\overline{0}$ como elemento neutro da soma e $\overline{1}$ como elemento neutro do produto.
Além disso, no caso em que p é primo temos as seguintes propriedades nos anéis dos inteiros módulo p:

1. Se $\overline{a}\cdot\overline{b}=\overline{0}$, então $\overline{a}=\overline{0}$ ou $\overline{b}=\overline{0}$;
2. Para cada $\overline{a}\neq\overline{0}$, existe $\overline{a}^{-1}\in\mathbb{Z}_p$ tal que $\overline{a}\cdot\overline{a}^{-1}=\overline{1}$

Por isso, temos que $\mathbb{Z}_p$ é dito um corpo.

Notações e Definições Básicas

Estas propriedades que $\mathbb{Z}_p$ satisfaz vêm dos seguintes fatos:

1. $\overline{a \cdot b} = \overline{0} \Rightarrow p|(a \cdot b) \Rightarrow p|a$ ou $\Rightarrow p|b$

Notações e Definições Básicas

Estas propriedades que $\mathbb{Z}_p$ satisfaz vêm dos seguintes fatos:

1. $\overline{a \cdot b} = \overline{0} \Rightarrow p|(a \cdot b) \Rightarrow p|a$ ou $\Rightarrow p|b$
2. (Algoritmo Euclidiano Estendido)
   Sejam a e b inteiros positivos. Então a equação nas variáveis X e Y

$$aX + bY = \text{mdc}(a, b)$$

   possui solução inteira, digamos $X = u_0$ e $Y = v_0$. Além disso, todas as suas soluções são da forma

$$X = u_0 + \frac{bk}{\text{mdc}(a, b)} \quad \text{e} \quad Y = v_0 - \frac{ak}{\text{mdc}(a, b)}$$

   com $k \in \mathbb{Z}$.

Notações e Definições Básicas

Um conjunto G munido com uma operação

$$\begin{array}{rccc} * : & G \times G & \longrightarrow & G \\ & (a, b) & \longmapsto & a * b \end{array}$$

é dito um *grupo* quando a operação $*$ satisfaz:

Notações e Definições Básicas

Um conjunto G munido com uma operação

$$\begin{array}{rccc} * : & G \times G & \longrightarrow & G \\ & (a, b) & \longmapsto & a * b \end{array}$$

é dito um *grupo* quando a operação $*$ satisfaz:

- Existe um elemento $e \in G$, chamado de *elemento neutro* de G, tal que $a * e = e * a = a$ para todo $a \in G$;

Notações e Definições Básicas

Um conjunto G munido com uma operação

$$\begin{array}{rccc} * : & G \times G & \longrightarrow & G \\ & (a, b) & \longmapsto & a * b \end{array}$$

é dito um *grupo* quando a operação $*$ satisfaz:

- Existe um elemento $e \in G$, chamado de *elemento neutro* de G, tal que $a * e = e * a = a$ para todo $a \in G$;
- Para cada $a \in G$ existe um único $a^{-1} \in G$, chamado de *inverso* de a, tal que $a * a^{-1} = a^{-1} * a = e$;

Notações e Definições Básicas

Um conjunto G munido com uma operação

$$\begin{array}{rccc} * : & G \times G & \longrightarrow & G \\ & (a, b) & \longmapsto & a * b \end{array}$$

é dito um *grupo* quando a operação $*$ satisfaz:

- Existe um elemento $e \in G$, chamado de *elemento neutro* de G, tal que $a * e = e * a = a$ para todo $a \in G$;
- Para cada $a \in G$ existe um único $a^{-1} \in G$, chamado de *inverso* de a, tal que $a * a^{-1} = a^{-1} * a = e$;
- $a * (b * c) = (a * b) * c$ para todo $a, b, c \in G$.

Notações e Definições Básicas

Um conjunto G munido com uma operação

$$\begin{array}{rccc} * : & G \times G & \longrightarrow & G \\ & (a, b) & \longmapsto & a * b \end{array}$$

é dito um *grupo* quando a operação $*$ satisfaz:

- Existe um elemento $e \in G$, chamado de *elemento neutro* de G, tal que $a * e = e * a = a$ para todo $a \in G$;
- Para cada $a \in G$ existe um único $a^{-1} \in G$, chamado de *inverso* de a, tal que $a * a^{-1} = a^{-1} * a = e$;
- $a * (b * c) = (a * b) * c$ para todo $a, b, c \in G$.

Além disso, o grupo G é dito *comutativo* ou *abeliano* quando $a * b = b * a$ para todo $a, b \in G$.

Notações e Definições Básicas

Um conjunto G munido com uma operação

$$\begin{array}{rccc} * : & G \times G & \longrightarrow & G \\ & (a, b) & \longmapsto & a * b \end{array}$$

é dito um *grupo* quando a operação $*$ satisfaz:

- Existe um elemento $e \in G$, chamado de *elemento neutro* de G, tal que $a * e = e * a = a$ para todo $a \in G$;
- Para cada $a \in G$ existe um único $a^{-1} \in G$, chamado de *inverso* de a, tal que $a * a^{-1} = a^{-1} * a = e$;
- $a * (b * c) = (a * b) * c$ para todo $a, b, c \in G$.

Além disso, o grupo G é dito *comutativo* ou *abeliano* quando $a * b = b * a$ para todo $a, b \in G$.
Um grupo é dito *finito* quando o conjunto G é finito. Neste caso, a quantidade de elementos de G é chamada de *ordem* de G e denotada por $|G|$.

Exemplo

1. O conjunto $\mathbb{Z}_m$ dos inteiros módulo m, com a operação de adição, é um grupo de ordem m, cujo elemento neutro é a classe $\overline{0}$.

Exemplo

1. O conjunto $\mathbb{Z}_m$ dos inteiros módulo m, com a operação de adição, é um grupo de ordem m, cujo elemento neutro é a classe $\overline{0}$.
2. Seja $p > 0$ um número primo.

Exemplo

1. O conjunto $\mathbb{Z}_m$ dos inteiros módulo m, com a operação de adição, é um grupo de ordem m, cujo elemento neutro é a classe $\overline{0}$.
2. Seja $p > 0$ um número primo. O conjunto

$$\mathbb{Z}_p^* := \{\overline{a} \in \mathbb{Z}_p \mid \overline{a} \neq \overline{0}\}$$

com a operação do produto, é um grupo de ordem $p - 1$, cujo elemento neutro é a classe $\overline{1}$.

Notações e Definições Básicas

Seja g um elemento do grupo G. Se existe um inteiro positivo n tal que $g^n = e$,

Notações e Definições Básicas

Seja g um elemento do grupo G. Se existe um inteiro positivo n tal que $g^n = e$,onde

$$g^n := \begin{cases} \underbrace{g * g * \cdots * g}_{\text{n vezes}} & \text{se } n > 0; \\ e & \text{se } n = 0; \\ \underbrace{g^{-1} * g^{-1} * \cdots * g^{-1}}_{\text{-n vezes}} & \text{se } n < 0; \end{cases}$$

então definimos a *ordem* de g pelo menor inteiro positivo satisfazendo esta propriedade.

Notações e Definições Básicas

Seja g um elemento do grupo G. Se existe um inteiro positivo n tal que $g^n = e$,onde

$$g^n := \begin{cases} \underbrace{g * g * \cdots * g}_{\text{n vezes}} & \text{se } n > 0; \\ e & \text{se } n = 0; \\ \underbrace{g^{-1} * g^{-1} * \cdots * g^{-1}}_{\text{-n vezes}} & \text{se } n < 0; \end{cases}$$

então definimos a *ordem* de g pelo menor inteiro positivo satisfazendo esta propriedade. Lembramos que se n é a ordem de g e $g^x = e$, então n divide x.

Sistema de criptografia de chave privada

Um *sistemas de criptografia de chave privada* requer que ambas as partes, envolvidas na troca da mensagem, combinem previamente uma chave secreta que serve tanto para codificar quanto para decodificar a mensagem.

Sistema de criptografia de chave privada

Um *sistemas de criptografia de chave privada* requer que ambas as partes, envolvidas na troca da mensagem, combinem previamente uma chave secreta que serve tanto para codificar quanto para decodificar a mensagem. O primeiro exemplo que vamos apresentar foi utilizado por Júlio César na época do império Romano para transmitir informações sobre estratégias nas batalhas.

Sistema de criptografia de chave privada

Um *sistemas de criptografia de chave privada* requer que ambas as partes, envolvidas na troca da mensagem, combinem previamente uma chave secreta que serve tanto para codificar quanto para decodificar a mensagem. O primeiro exemplo que vamos apresentar foi utilizado por Júlio César na época do império Romano para transmitir informações sobre estratégias nas batalhas. A tabela abaixo identifica em cada coluna a letra da primeira linha com a letra da segunda linha.

a	b	c	d	e	f	g	h	i	j	k	l	m
f	g	h	i	j	k	l	m	n	o	p	q	r

n	o	p	q	r	s	t	u	v	x	y	w	z
s	t	u	v	x	y	w	z	a	b	c	d	e

Sistema de criptografia de chave privada

Sistema de criptografia de chave privada

Portanto se a mensagem "nsnrnltxjhzfsit" chega para Júlio César, então ele utiliza o quadro acima para decodificar a mensagem, como podemos ver na tabela abaixo:

Sistema de criptografia de chave privada

Portanto se a mensagem "nsnrnltxjhzfsit" chega para Júlio César, então ele utiliza o quadro acima para decodificar a mensagem, como podemos ver na tabela abaixo:

n	s	n	r	n	l	t	x	j	h	z	f	s	i	t
i	n	i	m	i	g	o	r	e	c	u	a	n	d	o

Sistema de criptografia de chave privada

Portanto se a mensagem "nsnrnltxjhzfsit" chega para Júlio César, então ele utiliza o quadro acima para decodificar a mensagem, como podemos ver na tabela abaixo:

n	s	n	r	n	l	t	x	j	h	z	f	s	i	t
i	n	i	m	i	g	o	r	e	c	u	a	n	d	o

Com isso ele entenderia a mensagem: "inimigo recuando".

Sistema de criptografia de chave privada

O próximo exemplo (na folha entregue) tem como objetivo estabelecer um código padrão para associar uma numeração e um número binário (de 8 dígitos) a cada símbolo e cada letra que utilizamos (no alfabeto inglês).

Sistema de criptografia de chave privada

O próximo exemplo (na folha entregue) tem como objetivo estabelecer um código padrão para associar uma numeração e um número binário (de 8 dígitos) a cada símbolo e cada letra que utilizamos (no alfabeto inglês). Ele se chama de código padrão americano para intercâmbio de informação.

Sistema de criptografia de chave privada

O próximo exemplo (na folha entregue) tem como objetivo estabelecer um código padrão para associar uma numeração e um número binário (de 8 dígitos) a cada símbolo e cada letra que utilizamos (no alfabeto inglês). Ele se chama de código padrão americano para intercâmbio de informação. Seu principal objetivo não é criptografar mensagens, mas sim de associar uma mensagem a um número.

Sistema de criptografia de chave privada

Com esta codificação entregue, a mensagem abaixo:

01100011011101010111001001110110011000010111001100100000
01100101011011000110100101110000011101000110100101100011011000010111001100

Sistema de criptografia de chave privada

Com esta codificação entregue, a mensagem abaixo:

01100011011101010111001001110110011000010111001100100000011001010110110001101001011100000111010001101001011000110110000101110011

significa:

01100011	01110101	01110010	01110110	01100001	01110011
99	117	114	118	97	115
c	*u*	*r*	*v*	*a*	*s*
00100000					
32					

01100101	01101100	01101001	01110000	01110100	01101001
101	108	105	112	116	105
e	*l*	*i*	*p*	*t*	*i*
01100011	01100001	01110011			
99	97	115			
c	*a*	*s*			

O problema do logaritmo discreto

Em 1976, Whitfield Diffie e Martin Hellman publicaram um trabalho chamado "New directions in cryptography", cujo objetivo era definir o conceito de sistema de criptografia de chave pública

O problema do logaritmo discreto

Em 1976, Whitfield Diffie e Martin Hellman publicaram um trabalho chamado "New directions in cryptography", cujo objetivo era definir o conceito de sistema de criptografia de chave pública, isto é, um sistema de criptografia que não necessita de um encontro prévio para combinar uma chave de codificação.

O problema do logaritmo discreto

Em 1976, Whitfield Diffie e Martin Hellman publicaram um trabalho chamado "New directions in cryptography", cujo objetivo era definir o conceito de sistema de criptografia de chave pública, isto é, um sistema de criptografia que não necessita de um encontro prévio para combinar uma chave de codificação.
Basicamente, este sistema é definido sobre problemas que são difíceis de serem resolvidos, mas que sob hipóteses adicionais, se tornam viáveis.

O problema do logaritmo discreto

Em 1976, Whitfield Diffie e Martin Hellman publicaram um trabalho chamado "New directions in cryptography", cujo objetivo era definir o conceito de sistema de criptografia de chave pública, isto é, um sistema de criptografia que não necessita de um encontro prévio para combinar uma chave de codificação.
Basicamente, este sistema é definido sobre problemas que são difíceis de serem resolvidos, mas que sob hipóteses adicionais, se tornam viáveis.
Neste sentido, foi proposto o "problema do logaritmo discreto", que apresentaremos agora.

O problema do logaritmo discreto

Seja G um grupo, cuja operação será denotada por "$*$". O *problema do logaritmo discreto* em G é de determinar, para dois elementos $g, h \in G$ fixados, um inteiro x satisfazendo:

$$g^x = h.$$

O problema do logaritmo discreto

Seja G um grupo, cuja operação será denotada por "$*$". O *problema do logaritmo discreto* em G é de determinar, para dois elementos $g, h \in G$ fixados, um inteiro x satisfazendo:

$$g^x = h.$$

O problema do logaritmo discreto

É claro, que em alguns grupos este problema pode não ter solução.

O problema do logaritmo discreto

É claro, que em alguns grupos este problema pode não ter solução.

Exemplo

Se consideramos o grupo $\mathbb{Z}_4$, com a operação de adição, e fixarmos $g = \overline{2}$ e $h = \overline{3}$, então não existe x inteiro tal que $x \cdot \overline{2} = \overline{3}$, já que,

$$x \cdot \overline{2} = \begin{cases} \overline{0} & \text{se} \quad x \text{ é par;} \\ \overline{2} & \text{se} \quad x \text{ é ímpar.} \end{cases}$$

O problema do logaritmo discreto

Quando existe solução para o problema do logaritmo discreto $g^x = h$, então denominamos x por logaritmo discreto de h na base g e utilizamos a notação $x := \log_g(h)$.

O problema do logaritmo discreto

Quando existe solução para o problema do logaritmo discreto $g^x = h$, então denominamos x por logaritmo discreto de h na base g e utilizamos a notação $x := \log_g(h)$.
Note que este símbolo não está bem definido como um número inteiro

O problema do logaritmo discreto

Quando existe solução para o problema do logaritmo discreto $g^x = h$, então denominamos x por logaritmo discreto de h na base g e utilizamos a notação $x := \log_g(h)$.
Note que este símbolo não está bem definido como um número inteiro, já que, se n é a ordem de g, então $x + n$ também é uma solução para o problema do logaritmo discreto $g^x = h$.

O problema do logaritmo discreto

Quando existe solução para o problema do logaritmo discreto $g^x = h$, então denominamos x por logaritmo discreto de h na base g e utilizamos a notação $x := \log_g(h)$.
Note que este símbolo não está bem definido como um número inteiro, já que, se n é a ordem de g, então $x + n$ também é uma solução para o problema do logaritmo discreto $g^x = h$. De fato,

$$g^{x+n} = g^x * g^n = h * e = h.$$

Por outro lado, se x_1 e x_2 são soluções do problema $g^x = h$

O problema do logaritmo discreto

Quando existe solução para o problema do logaritmo discreto $g^x = h$, então denominamos x por logaritmo discreto de h na base g e utilizamos a notação $x := \log_g(h)$.
Note que este símbolo não está bem definido como um número inteiro, já que, se n é a ordem de g, então $x + n$ também é uma solução para o problema do logaritmo discreto $g^x = h$. De fato,

$$g^{x+n} = g^x * g^n = h * e = h.$$

Por outro lado, se x_1 e x_2 são soluções do problema $g^x = h$, então n divide $x_1 - x_2$

O problema do logaritmo discreto

Quando existe solução para o problema do logaritmo discreto $g^x = h$, então denominamos x por logaritmo discreto de h na base g e utilizamos a notação $x := \log_g(h)$.
Note que este símbolo não está bem definido como um número inteiro, já que, se n é a ordem de g, então $x + n$ também é uma solução para o problema do logaritmo discreto $g^x = h$. De fato,

$$g^{x+n} = g^x * g^n = h * e = h.$$

Por outro lado, se x_1 e x_2 são soluções do problema $g^x = h$, então n divide $x_1 - x_2$, já que, $g^{x_1 - x_2} = g^{x_1} * (g^{x_2})^{-1} = h * h^{-1} = e$.

O problema do logaritmo discreto

Quando existe solução para o problema do logaritmo discreto $g^x = h$, então denominamos x por logaritmo discreto de h na base g e utilizamos a notação $x := \log_g(h)$.
Note que este símbolo não está bem definido como um número inteiro, já que, se n é a ordem de g, então $x + n$ também é uma solução para o problema do logaritmo discreto $g^x = h$. De fato,

$$g^{x+n} = g^x * g^n = h * e = h.$$

Por outro lado, se x_1 e x_2 são soluções do problema $g^x = h$, então n divide $x_1 - x_2$, já que, $g^{x_1 - x_2} = g^{x_1} * (g^{x_2})^{-1} = h * h^{-1} = e$. Portanto,

$$\overline{x_1} = \overline{x_2}$$

em $\mathbb{Z}_n$, ou equivalentemente,

$$x_1 \equiv x_2 \bmod n.$$

O problema do logaritmo discreto

Quando existe solução para o problema do logaritmo discreto $g^x = h$, então denominamos x por logaritmo discreto de h na base g e utilizamos a notação $x := \log_g(h)$.
Note que este símbolo não está bem definido como um número inteiro, já que, se n é a ordem de g, então $x + n$ também é uma solução para o problema do logaritmo discreto $g^x = h$. De fato,

$$g^{x+n} = g^x * g^n = h * e = h.$$

Por outro lado, se x_1 e x_2 são soluções do problema $g^x = h$, então n divide $x_1 - x_2$, já que, $g^{x_1 - x_2} = g^{x_1} * (g^{x_2})^{-1} = h * h^{-1} = e$. Portanto,

$$\overline{x_1} = \overline{x_2}$$

em $\mathbb{Z}_n$, ou equivalentemente,

$$x_1 \equiv x_2 \bmod n.$$

Consequentemente, o símbolo $\log_g(h)$ está bem definido como elemento de $\mathbb{Z}_n$

O problema do logaritmo discreto

Quando existe solução para o problema do logaritmo discreto $g^x = h$, então denominamos x por logaritmo discreto de h na base g e utilizamos a notação $x := \log_g(h)$.
Note que este símbolo não está bem definido como um número inteiro, já que, se n é a ordem de g, então $x + n$ também é uma solução para o problema do logaritmo discreto $g^x = h$. De fato,

$$g^{x+n} = g^x * g^n = h * e = h.$$

Por outro lado, se x_1 e x_2 são soluções do problema $g^x = h$, então n divide $x_1 - x_2$, já que, $g^{x_1 - x_2} = g^{x_1} * (g^{x_2})^{-1} = h * h^{-1} = e$. Portanto,

$$\overline{x_1} = \overline{x_2}$$

em $\mathbb{Z}_n$, ou equivalentemente,

$$x_1 \equiv x_2 \bmod n.$$

Consequentemente, o símbolo $\log_g(h)$ está bem definido como elemento de $\mathbb{Z}_n$ ou como um número inteiro entre 0 e $n - 1$.

O problema do logaritmo discreto

Vamos considerar o grupo multiplicativo $\mathbb{Z}_{13}^*$ e $g = \overline{2}$.

O problema do logaritmo discreto

Vamos considerar o grupo multiplicativo $\mathbb{Z}_{13}^*$ e $g = \overline{2}$. Temos a seguinte tabela com todas as potências de g:

n	g^n
1	$\overline{2}$
2	$\overline{4}$
3	$\overline{8}$
4	$\overline{3}$
5	$\overline{6}$
6	$\overline{12}$
7	$\overline{11}$
8	$\overline{9}$
9	$\overline{5}$
10	$\overline{10}$
11	$\overline{7}$
12	$\overline{1}$

h	$\log_g(h)$
$\overline{1}$	0
$\overline{2}$	1
$\overline{3}$	4
$\overline{4}$	2
$\overline{5}$	9
$\overline{6}$	5
$\overline{7}$	11
$\overline{8}$	3
$\overline{9}$	8
$\overline{10}$	10
$\overline{11}$	7
$\overline{12}$	6

Sistema de criptografia de chave pública

O primeiro sistema de criptografia de chave pública foi o RSA, inventado por Rivest, Shamir e Adleman em 1978.

Sistema de criptografia de chave pública

O primeiro sistema de criptografia de chave pública foi o RSA, inventado por Rivest, Shamir e Adleman em 1978. Este sistema foi naturalmente patenteado, o que levou a busca de outros sistemas de criptografia de chave pública, tão eficientes quanto ele.

Sistema de criptografia de chave pública

O primeiro sistema de criptografia de chave pública foi o RSA, inventado por Rivest, Shamir e Adleman em 1978. Este sistema foi naturalmente patenteado, o que levou a busca de outros sistemas de criptografia de chave pública, tão eficientes quanto ele. Neste sentido, foi proposto a utilização de curvas elípticas, de modo independente por Neal Koblitz e Victor Miller em 1986.

Sistema de criptografia de chave pública

O primeiro sistema de criptografia de chave pública foi o RSA, inventado por Rivest, Shamir e Adleman em 1978. Este sistema foi naturalmente patenteado, o que levou a busca de outros sistemas de criptografia de chave pública, tão eficientes quanto ele. Neste sentido, foi proposto a utilização de curvas elípticas, de modo independente por Neal Koblitz e Victor Miller em 1986.
Para introduzir este sistema, vamos descrever o sistema de criptografia de chave pública ElGamal, que foi elaborado por Taher ElGamal em 1985.

Sistema ElGamal de criptografia de chave pública

Suponhamos que Bob queira enviar uma mensagem a Alice.

Sistema ElGamal de criptografia de chave pública

Suponhamos que Bob queira enviar uma mensagem a Alice. Esta mensagem é codificada em um número m, como já vimos que é possível.

Sistema ElGamal de criptografia de chave pública

1. Bob e Alice combinam inteiros $p > m$ (primo grande) e g (com $\text{mdc}(g, p) = 1$) e compartilham por um canal não seguro de comunicação.

Sistema ElGamal de criptografia de chave pública

1. Bob e Alice combinam inteiros $p > m$ (primo grande) e g (com $\text{mdc}(g, p) = 1$) e compartilham por um canal não seguro de comunicação. Além disso, Bob escolhe um inteiro k somente para codificar a mensagem m e que será descartado após isto.

Sistema ElGamal de criptografia de chave pública

1. Bob e Alice combinam inteiros $p > m$ (primo grande) e g (com $\text{mdc}(g, p) = 1$) e compartilham por um canal não seguro de comunicação. Além disso, Bob escolhe um inteiro k somente para codificar a mensagem m e que será descartado após isto. Por este motivo, denominamos k por *chave efêmera*;

Sistema ElGamal de criptografia de chave pública

1. Bob e Alice combinam inteiros $p > m$ (primo grande) e g (com $\text{mdc}(g, p) = 1$) e compartilham por um canal não seguro de comunicação. Além disso, Bob escolhe um inteiro k somente para codificar a mensagem m e que será descartado após isto. Por este motivo, denominamos k por *chave efêmera*;
2. Alice escolhe um inteiro secreto a e envia para Bob o inteiro $A \equiv g^a \bmod p$;

Sistema ElGamal de criptografia de chave pública

1. Bob e Alice combinam inteiros $p > m$ (primo grande) e g (com $\text{mdc}(g, p) = 1$) e compartilham por um canal não seguro de comunicação. Além disso, Bob escolhe um inteiro k somente para codificar a mensagem m e que será descartado após isto. Por este motivo, denominamos k por *chave efêmera*;
2. Alice escolhe um inteiro secreto a e envia para Bob o inteiro $A \equiv g^a \bmod p$;
3. Então, Bob calcula os dois inteiros:

$$c_1 \equiv g^k \quad \text{e} \quad c_2 \equiv mA^k \mod p$$

Sistema ElGamal de criptografia de chave pública

1. Bob e Alice combinam inteiros $p > m$ (primo grande) e g (com $\text{mdc}(g, p) = 1$) e compartilham por um canal não seguro de comunicação. Além disso, Bob escolhe um inteiro k somente para codificar a mensagem m e que será descartado após isto. Por este motivo, denominamos k por *chave efêmera*;
2. Alice escolhe um inteiro secreto a e envia para Bob o inteiro $A \equiv g^a \bmod p$;
3. Então, Bob calcula os dois inteiros:

$$c_1 \equiv g^k \quad \text{e} \quad c_2 \equiv mA^k \mod p$$

e a *mensagem codificada* será o par (c_1, c_2), que é enviado para Alice;

Sistema ElGamal de criptografia de chave pública

1. Bob e Alice combinam inteiros $p > m$ (primo grande) e g (com $\text{mdc}(g, p) = 1$) e compartilham por um canal não seguro de comunicação. Além disso, Bob escolhe um inteiro k somente para codificar a mensagem m e que será descartado após isto. Por este motivo, denominamos k por *chave efêmera*;
2. Alice escolhe um inteiro secreto a e envia para Bob o inteiro $A \equiv g^a \bmod p$;
3. Então, Bob calcula os dois inteiros:

$$c_1 \equiv g^k \quad \text{e} \quad c_2 \equiv mA^k \mod p$$

   e a *mensagem codificada* será o par (c_1, c_2), que é enviado para Alice;
4. Para decifrar a mensagem de Bob, primeiro Alice calcula

$$x \equiv c_1^a \quad \text{e} \quad x^{-1} \bmod p.$$

Sistema ElGamal de criptografia de chave pública

1. Bob e Alice combinam inteiros $p > m$ (primo grande) e g (com $\text{mdc}(g, p) = 1$) e compartilham por um canal não seguro de comunicação. Além disso, Bob escolhe um inteiro k somente para codificar a mensagem m e que será descartado após isto. Por este motivo, denominamos k por *chave efêmera*;
2. Alice escolhe um inteiro secreto a e envia para Bob o inteiro $A \equiv g^a \bmod p$;
3. Então, Bob calcula os dois inteiros:

$$c_1 \equiv g^k \quad \text{e} \quad c_2 \equiv mA^k \mod p$$

   e a *mensagem codificada* será o par (c_1, c_2), que é enviado para Alice;
4. Para decifrar a mensagem de Bob, primeiro Alice calcula

$$x \equiv c_1^a \quad \text{e} \quad x^{-1} \bmod p.$$

   Note que só Alice pode calcular x, já que, só ela conhece o inteiro a ;

Sistema ElGamal de criptografia de chave pública

1. Bob e Alice combinam inteiros $p > m$ (primo grande) e g (com $\text{mdc}(g, p) = 1$) e compartilham por um canal não seguro de comunicação. Além disso, Bob escolhe um inteiro k somente para codificar a mensagem m e que será descartado após isto. Por este motivo, denominamos k por *chave efêmera*;
2. Alice escolhe um inteiro secreto a e envia para Bob o inteiro $A \equiv g^a \bmod p$;
3. Então, Bob calcula os dois inteiros:

$$c_1 \equiv g^k \quad \text{e} \quad c_2 \equiv mA^k \mod p$$

   e a *mensagem codificada* será o par (c_1, c_2), que é enviado para Alice;
4. Para decifrar a mensagem de Bob, primeiro Alice calcula

$$x \equiv c_1^a \quad \text{e} \quad x^{-1} \bmod p.$$

   Note que só Alice pode calcular x, já que, só ela conhece o inteiro a ;
5. Por último, observamos que basta Alice calcular

$$c_2 \cdot x^{-1} \equiv m \mod p.$$

Sistema ElGamal de criptografia de chave pública

Agora, podemos ver o quão importante, para esta construção, é o problema do logaritmo discreto.

Sistema ElGamal de criptografia de chave pública

Agora, podemos ver o quão importante, para esta construção, é o problema do logaritmo discreto. De fato, se um intruso tiver acesso aos dados enviados entre Alice e Bob, isto é, p, g, $A = g^a$, c_1 e c_2,

Sistema ElGamal de criptografia de chave pública

Agora, podemos ver o quão importante, para esta construção, é o problema do logaritmo discreto. De fato, se um intruso tiver acesso aos dados enviados entre Alice e Bob, isto é, p, g, $A = g^a$, c_1 e c_2, e, se além disso, ele ainda souber resolver o problema do logaritmo discreto $g^x = A$ em $\mathbb{Z}_p$,

Sistema ElGamal de criptografia de chave pública

Agora, podemos ver o quão importante, para esta construção, é o problema do logaritmo discreto. De fato, se um intruso tiver acesso aos dados enviados entre Alice e Bob, isto é, p, g, $A = g^a$, c_1 e c_2, e, se além disso, ele ainda souber resolver o problema do logaritmo discreto $g^x = A$ em $\mathbb{Z}_p$, então ele poderá descobrir a.

Sistema ElGamal de criptografia de chave pública

Agora, podemos ver o quão importante, para esta construção, é o problema do logaritmo discreto. De fato, se um intruso tiver acesso aos dados enviados entre Alice e Bob, isto é, p, g, $A = g^a$, c_1 e c_2, e, se além disso, ele ainda souber resolver o problema do logaritmo discreto $g^x = A$ em $\mathbb{Z}_p$, então ele poderá descobrir a. Consequentemente ele poderá descobrir m, seguindo os passos listados acima.

Sistema ElGamal de criptografia de chave pública

Desta forma, para haver uma segurança real no problema do logaritmo discreto

Sistema ElGamal de criptografia de chave pública

Desta forma, para haver uma segurança real no problema do logaritmo discreto é recomendado que o primo escolhido seja aproximadamente 2^{1000}

Sistema ElGamal de criptografia de chave pública

Desta forma, para haver uma segurança real no problema do logaritmo discreto é recomendado que o primo escolhido seja aproximadamente 2^{1000} e que a ordem de g deva ser prima e deva ser aproximadamente $p/2$.

Sistema ElGamal de criptografia de chave pública

Desta forma, para haver uma segurança real no problema do logaritmo discreto é recomendado que o primo escolhido seja aproximadamente 2^{1000} e que a ordem de g deva ser prima e deva ser aproximadamente $p/2$. Neste sentido, algumas questões são relevantes:

Sistema ElGamal de criptografia de chave pública

Desta forma, para haver uma segurança real no problema do logaritmo discreto é recomendado que o primo escolhido seja aproximadamente 2^{1000} e que a ordem de g deva ser prima e deva ser aproximadamente $p/2$. Neste sentido, algumas questões são relevantes:

Sistema ElGamal de criptografia de chave pública

Desta forma, para haver uma segurança real no problema do logaritmo discreto é recomendado que o primo escolhido seja aproximadamente 2^{1000} e que a ordem de g deva ser prima e deva ser aproximadamente $p/2$. Neste sentido, algumas questões são relevantes:

- Como construir primos grandes?

Sistema ElGamal de criptografia de chave pública

Desta forma, para haver uma segurança real no problema do logaritmo discreto é recomendado que o primo escolhido seja aproximadamente 2^{1000} e que a ordem de g deva ser prima e deva ser aproximadamente $p/2$. Neste sentido, algumas questões são relevantes:

- Como construir primos grandes?
- Este método de criptografia não carrega junto uma forma fácil de ser decifrado?

Sistema ElGamal de criptografia de chave pública

Desta forma, para haver uma segurança real no problema do logaritmo discreto é recomendado que o primo escolhido seja aproximadamente 2^{1000} e que a ordem de g deva ser prima e deva ser aproximadamente $p/2$. Neste sentido, algumas questões são relevantes:

- Como construir primos grandes?
- Este método de criptografia não carrega junto uma forma fácil de ser decifrado?
- Qual é o tempo necessário para que um ataque possa quebrar este sistema?

Sistema ElGamal de criptografia de chave pública

Desta forma, para haver uma segurança real no problema do logaritmo discreto é recomendado que o primo escolhido seja aproximadamente 2^{1000} e que a ordem de g deva ser prima e deva ser aproximadamente $p/2$. Neste sentido, algumas questões são relevantes:

- Como construir primos grandes?
- Este método de criptografia não carrega junto uma forma fácil de ser decifrado?
- Qual é o tempo necessário para que um ataque possa quebrar este sistema?
- Seria possível construir algum grupo de modo que o problema do logaritmo discreto fosse mais difícil de ser quebrado?

Sistema ElGamal de criptografia de chave pública

Desta forma, para haver uma segurança real no problema do logaritmo discreto é recomendado que o primo escolhido seja aproximadamente 2^{1000} e que a ordem de g deva ser prima e deva ser aproximadamente $p/2$. Neste sentido, algumas questões são relevantes:

- Como construir primos grandes?
- Este método de criptografia não carrega junto uma forma fácil de ser decifrado?
- Qual é o tempo necessário para que um ataque possa quebrar este sistema?
- Seria possível construir algum grupo de modo que o problema do logaritmo discreto fosse mais difícil de ser quebrado? Acredita-se que o problema do logaritmo discreto no grupo associado a curvas elípticas possui uma dificuldade maior de ser resolvido que o problema em $\mathbb{Z}_p^*$.

A forma de Weierstrass

Uma *curva elíptica* E é o conjunto de soluções em $\mathbb{C}^2$ para uma equação da forma

$$Y^2 = X^3 + AX + B \quad (\text{com } A, B \in \mathbb{C})$$

que será chamada de equação de Weierstrass.

A forma de Weierstrass

Figura: $Y^2 = X^3 - X + 1$

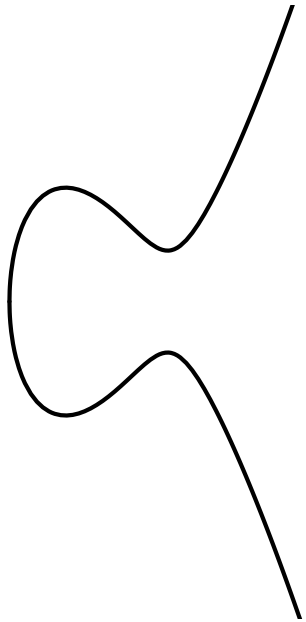


Figura: $Y^2 = X^3 - 3X$

A forma de Weierstrass

Figura: $Y^2 = X^3 - 3X + 2$

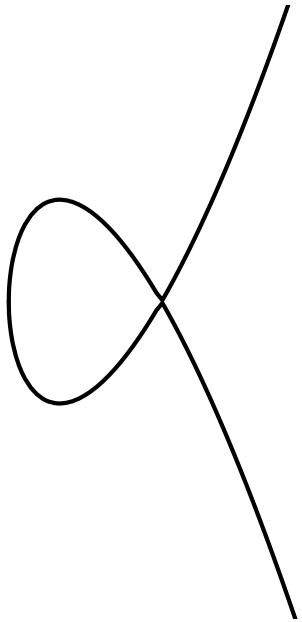
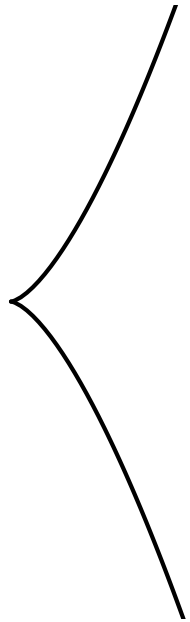


Figura: $Y^2 = X^3$



A estrutura de grupo

Agora vamos construir a estrutura de grupo de uma curva elíptica.

A estrutura de grupo

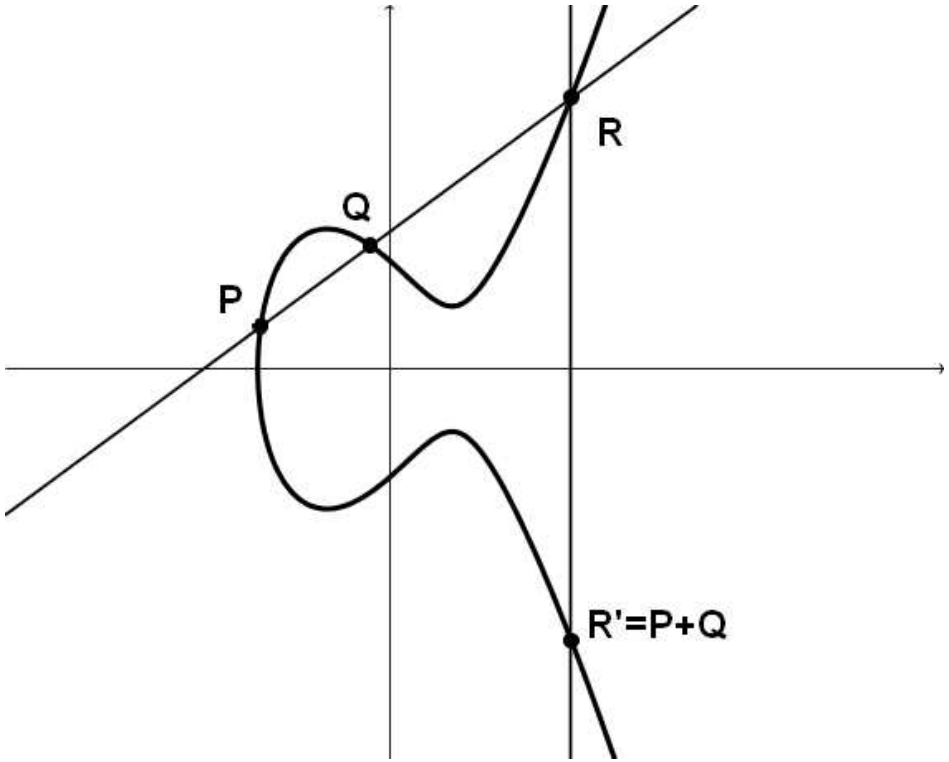
Agora vamos construir a estrutura de grupo de uma curva elíptica. Para isso, vamos construir a soma de dois pontos.

A estrutura de grupo

Agora vamos construir a estrutura de grupo de uma curva elíptica. Para isso, vamos construir a soma de dois pontos.
Sejam P e Q na curva elíptica e L a reta passando por P e Q, como na figura abaixo.

A estrutura de grupo

Agora vamos construir a estrutura de grupo de uma curva elíptica. Para isso, vamos construir a soma de dois pontos.
Sejam P e Q na curva elíptica e L a reta passando por P e Q, como na figura abaixo.



A estrutura de grupo

A reta L ainda vai cortar a curva em um terceiro ponto, digamos R.

A estrutura de grupo

A reta L ainda vai cortar a curva em um terceiro ponto, digamos R.
De fato, suponhamos que a reta L não seja vertical,

A estrutura de grupo

A reta L ainda vai cortar a curva em um terceiro ponto, digamos R.
De fato, suponhamos que a reta L não seja vertical,isto é, L é dada por uma das seguintes equações: $Y = aX + b$ ou $X = cY + d$ com $c \neq 0$.

A estrutura de grupo

A reta L ainda vai cortar a curva em um terceiro ponto, digamos R.
De fato, suponhamos que a reta L não seja vertical,isto é, L é dada por uma das seguintes equações: $Y = aX + b$ ou $X = cY + d$ com $c \neq 0$.
Substituindo estas equações na equação da curva temos que as interseções da reta com a curva são determinadas pelas raízes de um dos seguintes polinômios:

$$X^3 - a^2X^2 + (A - 2ab)X + (B - b^2)$$

ou

$$c^3Y^3 + (3c^2d - 1)Y^2 + (Ac + 3cd^2)Y + (B + d^3 + d).$$

A estrutura de grupo

A reta L ainda vai cortar a curva em um terceiro ponto, digamos R.
De fato, suponhamos que a reta L não seja vertical,isto é, L é dada por uma das seguintes equações: $Y = aX + b$ ou $X = cY + d$ com $c \neq 0$.
Substituindo estas equações na equação da curva temos que as interseções da reta com a curva são determinadas pelas raízes de um dos seguintes polinômios:

$$X^3 - a^2X^2 + (A - 2ab)X + (B - b^2)$$

ou

$$c^3Y^3 + (3c^2d - 1)Y^2 + (Ac + 3cd^2)Y + (B + d^3 + d).$$

Por outro lado sabemos que se $P = (x_1, y_1)$ e $Q = (x_2, y_2)$, então

$$X^3 - a^2X^2 + (A - 2ab)X + (B - b^2) = (X - x_1)(X - x_2)(X - x_3)$$

ou

$$c^3Y^3 + (3c^2d - 1)Y^2 + (Ac + 3cd^2)Y + (B + d^3 + d) = c^3(Y - y_1)(Y - y_2)(Y - y_3).$$

A estrutura de grupo

A reta L ainda vai cortar a curva em um terceiro ponto, digamos R.
De fato, suponhamos que a reta L não seja vertical,isto é, L é dada por uma das seguintes equações: $Y = aX + b$ ou $X = cY + d$ com $c \neq 0$.
Substituindo estas equações na equação da curva temos que as interseções da reta com a curva são determinadas pelas raízes de um dos seguintes polinômios:

$$X^3 - a^2X^2 + (A - 2ab)X + (B - b^2)$$

ou

$$c^3Y^3 + (3c^2d - 1)Y^2 + (Ac + 3cd^2)Y + (B + d^3 + d).$$

Por outro lado sabemos que se $P = (x_1, y_1)$ e $Q = (x_2, y_2)$, então

$$X^3 - a^2X^2 + (A - 2ab)X + (B - b^2) = (X - x_1)(X - x_2)(X - x_3)$$

ou

$$c^3Y^3 + (3c^2d - 1)Y^2 + (Ac + 3cd^2)Y + (B + d^3 + d) = c^3(Y - y_1)(Y - y_2)(Y - y_3).$$

Assim, só nos resta encontrar a terceira raiz e substituir na equação da reta para achar a outra coordenada do terceiro ponto de interseção da curva com a reta.

A estrutura de grupo

Por este ponto R passa uma reta perpendicular ao eixo horizontal.

A estrutura de grupo

Por este ponto R passa uma reta perpendicular ao eixo horizontal. Esta reta vai cortar a curva em mais um ponto, digamos R'.

A estrutura de grupo

Por este ponto R passa uma reta perpendicular ao eixo horizontal. Esta reta vai cortar a curva em mais um ponto, digamos R'. De fato, se $r = (x, y)$, então $R' = (x, -y)$.

A estrutura de grupo

Por este ponto R passa uma reta perpendicular ao eixo horizontal. Esta reta vai cortar a curva em mais um ponto, digamos R'. De fato, se $r = (x, y)$, então $R' = (x, -y)$.
O ponto R' será chamado de *a soma de P e Q* e será denotado por

$$P + Q.$$

A estrutura de grupo

Consideremos a curva elíptica

$$E: \quad Y^2 = X^3 - 15X + 18.$$

A estrutura de grupo

Consideremos a curva elíptica

$$E: \quad Y^2 = X^3 - 15X + 18.$$

Sejam $P = (7, 16)$ e $Q = (1, 2)$ dois pontos de E. A reta passando por P e Q tem equação

$$Y = \frac{7}{3}X - \frac{1}{3}.$$

A estrutura de grupo

Consideremos a curva elíptica

$$E: \quad Y^2 = X^3 - 15X + 18.$$

Sejam $P = (7, 16)$ e $Q = (1, 2)$ dois pontos de E. A reta passando por P e Q tem equação

$$Y = \frac{7}{3}X - \frac{1}{3}.$$

Para encontrar o ponto em comum entre E e L resolvemos a equação abaixo:

$$\begin{aligned}
\left(\tfrac{7}{3}x - \tfrac{1}{3}\right)^2 &= x^3 - 15x + 18 \\
\tfrac{49}{9}x^2 - \tfrac{14}{9}x - \tfrac{1}{9} &= x^3 - 15x + 18 \\
0 &= x^3 - \tfrac{49}{9}x^2 - \tfrac{121}{9}x - \tfrac{161}{9}
\end{aligned}$$

A estrutura de grupo

Note que, já sabemos que $x = 7$ e $x = 1$ são duas raízes desta equação polinomial.

A estrutura de grupo

Note que, já sabemos que $x = 7$ e $x = 1$ são duas raízes desta equação polinomial. Desta forma, é mais fácil encontrar a terceira, já que, podemos dividir o polinômio $x^3 - \frac{49}{9}x^2 - \frac{121}{9}x - \frac{161}{9}$ por $(x - 7)(x - 1)$.

A estrutura de grupo

Note que, já sabemos que $x = 7$ e $x = 1$ são duas raízes desta equação polinomial. Desta forma, é mais fácil encontrar a terceira, já que, podemos dividir o polinômio $x^3 - \frac{49}{9}x^2 - \frac{121}{9}x - \frac{161}{9}$ por $(x-7)(x-1)$. Fazendo esta conta temos:

$$x^3 - \frac{49}{9}x^2 - \frac{121}{9}x - \frac{161}{9} = (x-7)(x-1)(x+\frac{23}{9}).$$

A estrutura de grupo

Note que, já sabemos que $x = 7$ e $x = 1$ são duas raízes desta equação polinomial. Desta forma, é mais fácil encontrar a terceira, já que, podemos dividir o polinômio $x^3 - \frac{49}{9}x^2 - \frac{121}{9}x - \frac{161}{9}$ por $(x-7)(x-1)$. Fazendo esta conta temos:

$$x^3 - \frac{49}{9}x^2 - \frac{121}{9}x - \frac{161}{9} = (x-7)(x-1)(x+\frac{23}{9}).$$

Assim, $R = (-\frac{23}{9}, ?)$.

A estrutura de grupo

Note que, já sabemos que $x = 7$ e $x = 1$ são duas raízes desta equação polinomial. Desta forma, é mais fácil encontrar a terceira, já que, podemos dividir o polinômio $x^3 - \frac{49}{9}x^2 - \frac{121}{9}x - \frac{161}{9}$ por $(x-7)(x-1)$. Fazendo esta conta temos:

$$x^3 - \frac{49}{9}x^2 - \frac{121}{9}x - \frac{161}{9} = (x-7)(x-1)(x+\frac{23}{9}).$$

Assim, $R = (-\frac{23}{9}, ?)$. Para encontrar a coordenada y basta substituir na equação da reta e obter $y = \frac{170}{27}$.

A estrutura de grupo

Note que, já sabemos que $x = 7$ e $x = 1$ são duas raízes desta equação polinomial. Desta forma, é mais fácil encontrar a terceira, já que, podemos dividir o polinômio $x^3 - \frac{49}{9}x^2 - \frac{121}{9}x - \frac{161}{9}$ por $(x-7)(x-1)$. Fazendo esta conta temos:

$$x^3 - \frac{49}{9}x^2 - \frac{121}{9}x - \frac{161}{9} = (x-7)(x-1)(x+\frac{23}{9}).$$

Assim, $R = (-\frac{23}{9}, ?)$. Para encontrar a coordenada y basta substituir na equação da reta e obter $y = \frac{170}{27}$. Refletindo ao longo do eixo horizontal, obtemos

$$P + Q = (-\frac{23}{9}, -\frac{170}{27}).$$

A estrutura de grupo

Por outro lado, existem algumas sutilezas quando variamos a escolha dos pontos à somar e variamos as possíveis curvas elípticas.

A estrutura de grupo

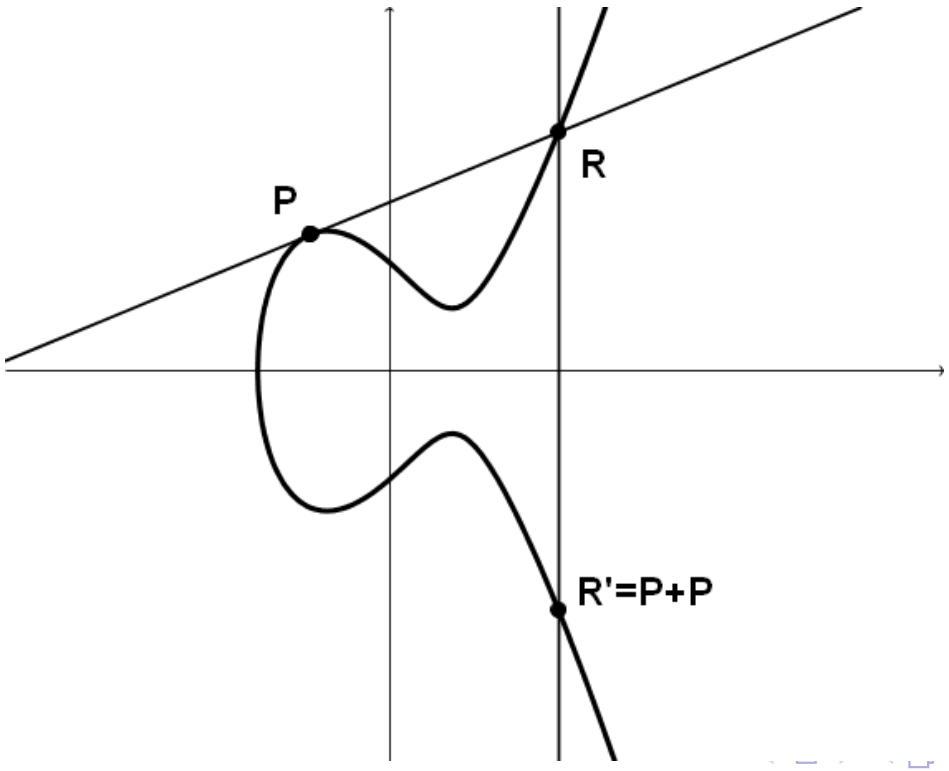
Por outro lado, existem algumas sutilezas quando variamos a escolha dos pontos à somar e variamos as possíveis curvas elípticas. Além disso, se queremos que esta soma forneça uma estrutura de grupo, então ainda temos que definir o elemento neutro e o inverso.

A estrutura de grupo

Por outro lado, existem algumas sutilezas quando variamos a escolha dos pontos à somar e variamos as possíveis curvas elípticas. Além disso, se queremos que esta soma forneça uma estrutura de grupo, então ainda temos que definir o elemento neutro e o inverso.
Primeiro vamos definir a adição de um ponto com ele mesmo.

A estrutura de grupo

Por outro lado, existem algumas sutilezas quando variamos a escolha dos pontos à somar e variamos as possíveis curvas elípticas. Além disso, se queremos que esta soma forneça uma estrutura de grupo, então ainda temos que definir o elemento neutro e o inverso.
Primeiro vamos definir a adição de um ponto com ele mesmo.



A estrutura de grupo

Como intuímos, seja E uma curva elíptica e $P \in E$.

A estrutura de grupo

Como intuímos, seja E uma curva elíptica e $P \in E$. Consideremos a reta tangente L a E em P.

A estrutura de grupo

Como intuímos, seja E uma curva elíptica e $P \in E$. Consideremos a reta tangente L a E em P. Esta reta ainda corta E em um outro ponto, digamos R.

A estrutura de grupo

Como intuímos, seja E uma curva elíptica e $P \in E$. Consideremos a reta tangente L a E em P. Esta reta ainda corta E em um outro ponto, digamos R.
De fato, suponhamos que a reta L não seja vertical,

A estrutura de grupo

Como intuímos, seja E uma curva elíptica e $P \in E$. Consideremos a reta tangente L a E em P. Esta reta ainda corta E em um outro ponto, digamos R.
De fato, suponhamos que a reta L não seja vertical,isto é, L é dada por uma das seguintes equações: $Y = aX + b$ ou $X = cY + d$ com $c \neq 0$.

A estrutura de grupo

Como intuímos, seja E uma curva elíptica e $P \in E$. Consideremos a reta tangente L a E em P. Esta reta ainda corta E em um outro ponto, digamos R.
De fato, suponhamos que a reta L não seja vertical,isto é, L é dada por uma das seguintes equações: $Y = aX + b$ ou $X = cY + d$ com $c \neq 0$.
Substituindo estas equações na equação da curva temos que as interseções da reta com a curva são determinadas pelas raízes de um dos seguintes polinômios:

$$X^3 - a^2X^2 + (A - 2ab)X + (B - b^2) = (X - x)^2(X - x')$$

ou

$$c^3Y^3 + (3c^2d - 1)Y^2 + (Ac + 3cd^2)Y + (B + d^3 + d) = c^3(Y - y)^2(Y - y').$$

onde $P = (x, y)$.

A estrutura de grupo

Como intuímos, seja E uma curva elíptica e $P \in E$. Consideremos a reta tangente L a E em P. Esta reta ainda corta E em um outro ponto, digamos R.
De fato, suponhamos que a reta L não seja vertical,isto é, L é dada por uma das seguintes equações: $Y = aX + b$ ou $X = cY + d$ com $c \neq 0$.
Substituindo estas equações na equação da curva temos que as interseções da reta com a curva são determinadas pelas raízes de um dos seguintes polinômios:

$$X^3 - a^2X^2 + (A - 2ab)X + (B - b^2) = (X - x)^2(X - x')$$

ou

$$c^3Y^3 + (3c^2d - 1)Y^2 + (Ac + 3cd^2)Y + (B + d^3 + d) = c^3(Y - y)^2(Y - y').$$

onde $P = (x, y)$.
Considerando a reta vertical que passa por R,

A estrutura de grupo

Como intuímos, seja E uma curva elíptica e $P \in E$. Consideremos a reta tangente L a E em P. Esta reta ainda corta E em um outro ponto, digamos R.
De fato, suponhamos que a reta L não seja vertical,isto é, L é dada por uma das seguintes equações: $Y = aX + b$ ou $X = cY + d$ com $c \neq 0$.
Substituindo estas equações na equação da curva temos que as interseções da reta com a curva são determinadas pelas raízes de um dos seguintes polinômios:

$$X^3 - a^2X^2 + (A - 2ab)X + (B - b^2) = (X - x)^2(X - x')$$

ou

$$c^3Y^3 + (3c^2d - 1)Y^2 + (Ac + 3cd^2)Y + (B + d^3 + d) = c^3(Y - y)^2(Y - y').$$

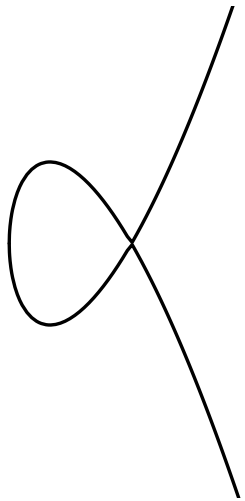
onde $P = (x, y)$.
Considerando a reta vertical que passa por R, então a soma de P com ele mesmo será definido pelo ponto de encontro desta reta com E.

A estrutura de grupo

Antes de fazer um exemplo, vamos fazer uma observação. Note que, na seguinte curva, temos problemas para falar da tangente em todos os pontos de E.

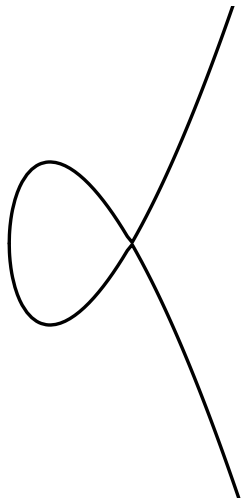
A estrutura de grupo

Antes de fazer um exemplo, vamos fazer uma observação. Note que, na seguinte curva, temos problemas para falar da tangente em todos os pontos de E.



A estrutura de grupo

Antes de fazer um exemplo, vamos fazer uma observação. Note que, na seguinte curva, temos problemas para falar da tangente em todos os pontos de E.



Para acabar com este problema vamos colocar uma condição na definição de curva elíptica.

A estrutura de grupo

Uma *curva elíptica* E é o conjunto de soluções para uma equação da forma

$$Y^2 = X^3 + AX + B$$

A estrutura de grupo

Uma *curva elíptica* E é o conjunto de soluções para uma equação da forma

$$Y^2 = X^3 + AX + B$$

com A e B satisfazendo

$$4A^3 + 27B^2 \neq 0.$$

A estrutura de grupo

Uma *curva elíptica* E é o conjunto de soluções para uma equação da forma

$$Y^2 = X^3 + AX + B$$

com A e B satisfazendo

$$4A^3 + 27B^2 \neq 0.$$

Esta desigualdade é uma forma de impor, nos coeficientes da curva, que ela não tenha "singularidades".

A estrutura de grupo

Uma *curva elíptica* E é o conjunto de soluções para uma equação da forma

$$Y^2 = X^3 + AX + B$$

com A e B satisfazendo

$$4A^3 + 27B^2 \neq 0.$$

Esta desigualdade é uma forma de impor, nos coeficientes da curva, que ela não tenha "singularidades". Isto, por sua vez, vai implicar na possibilidade de encontrar a reta tangente em todos os pontos. Mas não entraremos muito nos detalhes desta questão.

A estrutura de grupo

Vamos fazer um exemplo utilizando, novamente a curva do exemplo anterior. Consideremos a curva elíptica $E: \quad Y^2 = X^3 - 15X + 18$ e o ponto $P = (7, 16)$.

A estrutura de grupo

Vamos fazer um exemplo utilizando, novamente a curva do exemplo anterior. Consideremos a curva elíptica $E: \quad Y^2 = X^3 - 15X + 18$ e o ponto $P = (7, 16)$. Utilizamos as técnicas de derivação implícita do curso de cálculo para determinar a reta tangente a E em P.

A estrutura de grupo

Vamos fazer um exemplo utilizando, novamente a curva do exemplo anterior. Consideremos a curva elíptica $E: \quad Y^2 = X^3 - 15X + 18$ e o ponto $P = (7, 16)$. Utilizamos as técnicas de derivação implícita do curso de cálculo para determinar a reta tangente a E em P. Para isso, veremos Y como função de X na igualdade que define E e derivamos esta igualdade em X para obter:

A estrutura de grupo

Vamos fazer um exemplo utilizando, novamente a curva do exemplo anterior. Consideremos a curva elíptica $E: \quad Y^2 = X^3 - 15X + 18$ e o ponto $P = (7, 16)$. Utilizamos as técnicas de derivação implícita do curso de cálculo para determinar a reta tangente a E em P. Para isso, veremos Y como função de X na igualdade que define E e derivamos esta igualdade em X para obter:

$$\frac{dY}{dX} = \frac{3X^2 - 15}{2Y}.$$

A estrutura de grupo

Vamos fazer um exemplo utilizando, novamente a curva do exemplo anterior. Consideremos a curva elíptica $E: \quad Y^2 = X^3 - 15X + 18$ e o ponto $P = (7, 16)$. Utilizamos as técnicas de derivação implícita do curso de cálculo para determinar a reta tangente a E em P. Para isso, veremos Y como função de X na igualdade que define E e derivamos esta igualdade em X para obter:

$$\frac{dY}{dX} = \frac{3X^2 - 15}{2Y}.$$

Avaliando isto no ponto P, podemos deduzir que a inclinação da reta tangente em P é $\frac{33}{8}$.

A estrutura de grupo

Vamos fazer um exemplo utilizando, novamente a curva do exemplo anterior. Consideremos a curva elíptica $E: \quad Y^2 = X^3 - 15X + 18$ e o ponto $P = (7, 16)$. Utilizamos as técnicas de derivação implícita do curso de cálculo para determinar a reta tangente a E em P. Para isso, veremos Y como função de X na igualdade que define E e derivamos esta igualdade em X para obter:

$$\frac{dY}{dX} = \frac{3X^2 - 15}{2Y}.$$

Avaliando isto no ponto P, podemos deduzir que a inclinação da reta tangente em P é $\frac{33}{8}$. Portanto a equação da reta tangente é dada por $Y - 16 = \frac{33}{8}(X - 7)$,

A estrutura de grupo

Vamos fazer um exemplo utilizando, novamente a curva do exemplo anterior. Consideremos a curva elíptica $E: \quad Y^2 = X^3 - 15X + 18$ e o ponto $P = (7, 16)$. Utilizamos as técnicas de derivação implícita do curso de cálculo para determinar a reta tangente a E em P. Para isso, veremos Y como função de X na igualdade que define E e derivamos esta igualdade em X para obter:

$$\frac{dY}{dX} = \frac{3X^2 - 15}{2Y}.$$

Avaliando isto no ponto P, podemos deduzir que a inclinação da reta tangente em P é $\frac{33}{8}$. Portanto a equação da reta tangente é dada por $Y - 16 = \frac{33}{8}(X - 7)$, isto é,

$$Y = \frac{33}{8}X - \frac{103}{8}.$$

A estrutura de grupo

Para descobrir o outro ponto de encontro entre a reta tangente e E calculamos:

$$\begin{aligned} \left(\tfrac{33}{8}X - \tfrac{103}{8}\right)^2 &= x^3 - 15x + 18 \\ 0 &= x^3 - \tfrac{1089}{64}x^2 - \tfrac{2919}{32}x - \tfrac{9457}{64} \\ 0 &= (x-7)^2(x - \tfrac{193}{64}). \end{aligned}$$

A estrutura de grupo

Para descobrir o outro ponto de encontro entre a reta tangente e E calculamos:

$$\begin{aligned} \left(\tfrac{33}{8}X - \tfrac{103}{8}\right)^2 &= x^3 - 15x + 18 \\ 0 &= x^3 - \tfrac{1089}{64}x^2 - \tfrac{2919}{32}x - \tfrac{9457}{64} \\ 0 &= (x-7)^2(x - \tfrac{193}{64}). \end{aligned}$$

Note que $x = 7$ é uma raíz deste polinômio com multiplicidade 2. Logo a solução $x = \frac{193}{64}$ nos dá exatamente a abscissa do ponto que queremos determinar.

A estrutura de grupo

Para descobrir o outro ponto de encontro entre a reta tangente e E calculamos:

$$\begin{aligned} \left(\tfrac{33}{8}X - \tfrac{103}{8}\right)^2 &= x^3 - 15x + 18 \\ 0 &= x^3 - \tfrac{1089}{64}x^2 - \tfrac{2919}{32}x - \tfrac{9457}{64} \\ 0 &= (x-7)^2(x - \tfrac{193}{64}). \end{aligned}$$

Note que $x = 7$ é uma raíz deste polinômio com multiplicidade 2. Logo a solução $x = \frac{193}{64}$ nos dá exatamente a abscissa do ponto que queremos determinar.
Substituindo $x = \frac{193}{64}$ na equação da reta, obtemos $y = -\frac{223}{512}$.

A estrutura de grupo

Para descobrir o outro ponto de encontro entre a reta tangente e E calculamos:

$$\begin{aligned} (\tfrac{33}{8}X - \tfrac{103}{8})^2 &= x^3 - 15x + 18 \\ 0 &= x^3 - \tfrac{1089}{64}x^2 - \tfrac{2919}{32}x - \tfrac{9457}{64} \\ 0 &= (x-7)^2(x - \tfrac{193}{64}). \end{aligned}$$

Note que $x = 7$ é uma raíz deste polinômio com multiplicidade 2. Logo a solução $x = \frac{193}{64}$ nos dá exatamente a abscissa do ponto que queremos determinar.
Substituindo $x = \frac{193}{64}$ na equação da reta, obtemos $y = -\frac{223}{512}$. refletindo em torno do eixo $y = 0$ obtemos:

$$P + P = (\frac{193}{64}, \frac{223}{512}).$$

A estrutura de grupo

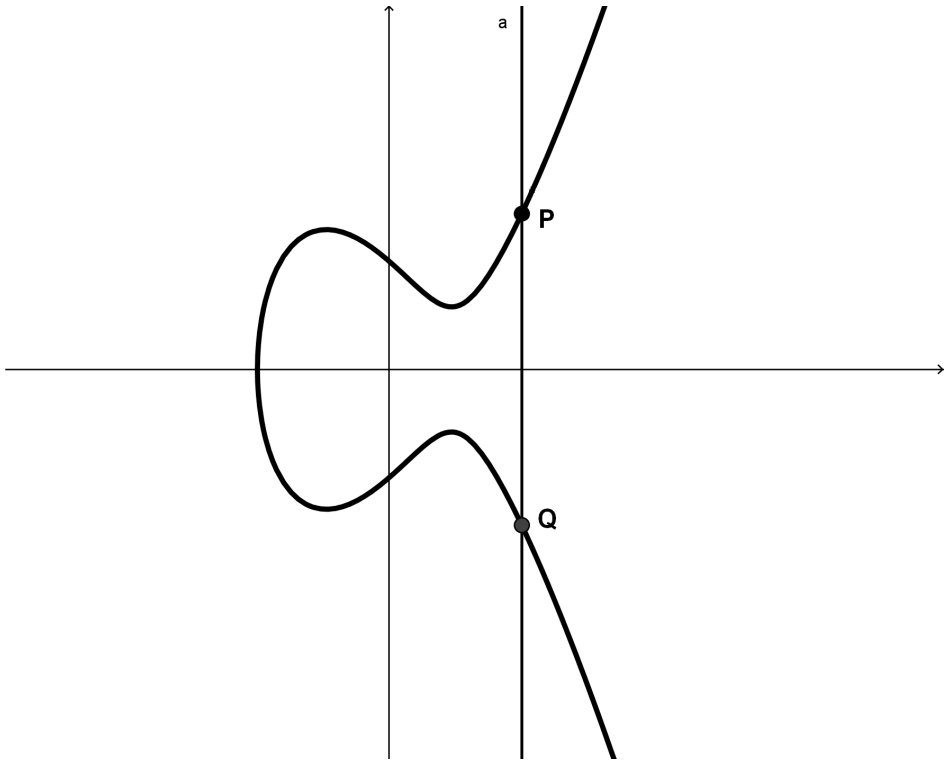
O próximo problema que iremos abordar é quando queremos somar um ponto $P = (a, b)$ com a sua reflexão, em torno do eixo $y = 0$, digamos $Q = (a, -b)$.

A estrutura de grupo

O próximo problema que iremos abordar é quando queremos somar um ponto $P = (a, b)$ com a sua reflexão, em torno do eixo $y = 0$, digamos $Q = (a, -b)$.

A estrutura de grupo

O próximo problema que iremos abordar é quando queremos somar um ponto $P = (a, b)$ com a sua reflexão, em torno do eixo $y = 0$, digamos $Q = (a, -b)$.



A estrutura de grupo

A solução para este impasse é criar um ponto $\mathcal{O}$ que "mora" no infinito!

A estrutura de grupo

A solução para este impasse é criar um ponto $\mathcal{O}$ que "mora" no infinito! Isto é, ele não está no plano cartesiano XY e

A estrutura de grupo

A solução para este impasse é criar um ponto $\mathcal{O}$ que "mora" no infinito! Isto é, ele não está no plano cartesiano XY e, além disso, queremos que ele esteja na interseção entre toda reta vertical e E.

A estrutura de grupo

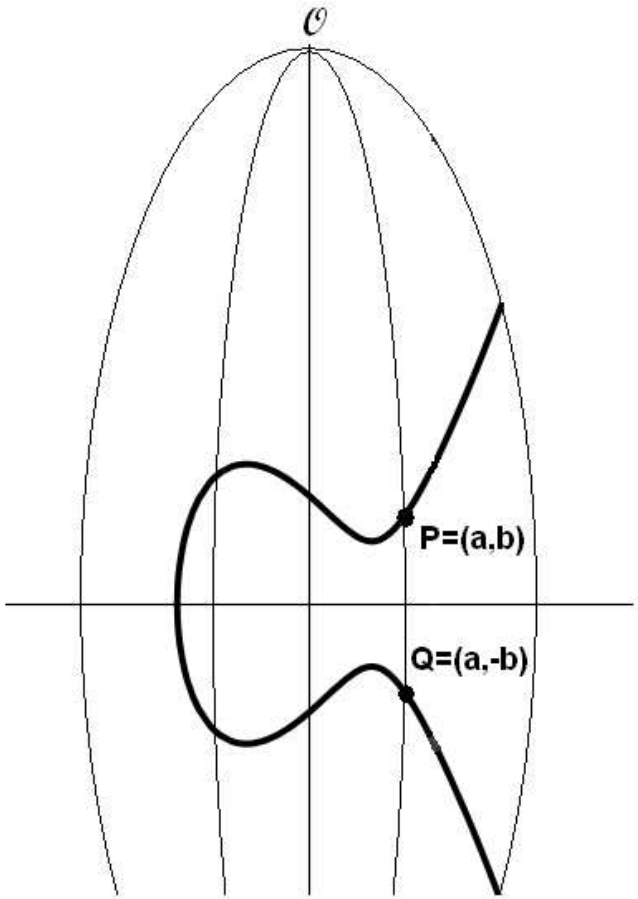
A solução para este impasse é criar um ponto $\mathcal{O}$ que "mora" no infinito! Isto é, ele não está no plano cartesiano XY e, além disso, queremos que ele esteja na interseção entre toda reta vertical e E. Esta propriedade desejada se torna natural quando pensamos que estamos em uma estrada que vai até o "infinito".

A estrutura de grupo

A solução para este impasse é criar um ponto $\mathcal{O}$ que "mora" no infinito! Isto é, ele não está no plano cartesiano XY e, além disso, queremos que ele esteja na interseção entre toda reta vertical e E. Esta propriedade desejada se torna natural quando pensamos que estamos em uma estrada que vai até o "infinito". Neste caso, definimos

$$P + Q = \mathcal{O}.$$

A estrutura de grupo



A estrutura de grupo

Pela figura anterior, ainda podemos deduzir que, para todo $P \in E$, vale:

$$P + \mathcal{O} = P$$

A estrutura de grupo

Pela figura anterior, ainda podemos deduzir que, para todo $P \in E$, vale:

$$P + \mathcal{O} = P$$

Portanto, $\mathcal{O}$ é o elemento neutro que estamos procurando para esta soma definida.

A estrutura de grupo

Pela figura anterior, ainda podemos deduzir que, para todo $P \in E$, vale:

$$P + \mathcal{O} = P$$

Portanto, $\mathcal{O}$ é o elemento neutro que estamos procurando para esta soma definida.
Observa ainda que se $P = (a, b)$, então o único ponto Q de E tal que $P + Q = \mathcal{O}$ é $Q = (a, -b)$.

A estrutura de grupo

Pela figura anterior, ainda podemos deduzir que, para todo $P \in E$, vale:

$$P + \mathcal{O} = P$$

Portanto, $\mathcal{O}$ é o elemento neutro que estamos procurando para esta soma definida.
Observa ainda que se $P = (a, b)$, então o único ponto Q de E tal que $P + Q = \mathcal{O}$ é $Q = (a, -b)$. Portanto, Q é o inverso de P pela adição que definimos.

A estrutura de grupo

Pela figura anterior, ainda podemos deduzir que, para todo $P \in E$, vale:

$$P + \mathcal{O} = P$$

Portanto, $\mathcal{O}$ é o elemento neutro que estamos procurando para esta soma definida.
Observa ainda que se $P = (a, b)$, então o único ponto Q de E tal que $P + Q = \mathcal{O}$ é $Q = (a, -b)$. Portanto, Q é o inverso de P pela adição que definimos. Usamos a seguinte notação

$$-P := Q.$$

A estrutura de grupo

Pela definição que demos, não é difícil de ver que a soma que definimos satisfaz:

$$P + Q = Q + P$$

para cada P e Q em E.

A estrutura de grupo

Pela definição que demos, não é difícil de ver que a soma que definimos satisfaz:

$$P + Q = Q + P$$

para cada P e Q em E. A propriedade que necessita ser verificada, e que não é nada simples, é a associatividade:

$$(P + Q) + R = Q + (P + R)$$

para cada P, Q e R em E.

A estrutura de grupo

Pela definição que demos, não é difícil de ver que a soma que definimos satisfaz:

$$P + Q = Q + P$$

para cada P e Q em E. A propriedade que necessita ser verificada, e que não é nada simples, é a associatividade:

$$(P + Q) + R = Q + (P + R)$$

para cada P, Q e R em E.
Com estas propriedades, temos que a adição que definimos fornece uma estrutura de grupo em E.

A estrutura de grupo

Pela definição que demos, não é difícil de ver que a soma que definimos satisfaz:

$$P + Q = Q + P$$

para cada P e Q em E. A propriedade que necessita ser verificada, e que não é nada simples, é a associatividade:

$$(P + Q) + R = Q + (P + R)$$

para cada P, Q e R em E.
Com estas propriedades, temos que a adição que definimos fornece uma estrutura de grupo em E.
É interessante observar que esta adição pode ser obtida por formulas explicitas, nas coordenadas dos pontos de E, como vamos enunciar a seguir.

A estrutura de grupo

Teorema

Seja $E : Y^2 = X^3 + AX + B$ uma curva elíptica e sejam P_1 e P_2 em E. Então:

- Se $P_1 = \mathcal{O}$, então $P_1 + P_2 = P_2$;
- Se $P_2 = \mathcal{O}$, então $P_1 + P_2 = P_1$;

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

- Se $x_1 = x_2$ e $y_1 = -y_2$, então $P_1 + P_2 = \mathcal{O}$;
- Caso contrário, $P_1 + P_2 = (x_3, y_3)$ onde

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

e

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{se } P_1 \neq P_2 \text{ (inclinação da reta ligando } P_1 \text{ e } P_2) \\ \frac{3x_1^2 + A}{2y_1} & \text{se } P_1 = P_2. \text{ (inclinação da reta tangente em } P_1) \end{cases}$$

Curvas elípticas sobre corpos finitos

Seja $p > 0$ primo.

Curvas elípticas sobre corpos finitos

Seja $p > 0$ primo. Uma *curva elíptica sobre* $\mathbb{Z}_p$ é uma equação da forma

$$Y^2 = X^3 + AX + B \quad \text{com} \quad A, B \in \mathbb{Z}_p \quad \text{e} \quad 4A^3 + 27B^2 \neq 0.$$

Curvas elípticas sobre corpos finitos

Seja $p > 0$ primo. Uma *curva elíptica sobre* $\mathbb{Z}_p$ é uma equação da forma

$$Y^2 = X^3 + AX + B \text{ com } A, B \in \mathbb{Z}_p \text{ e } 4A^3 + 27B^2 \neq 0.$$

Já o conjunto dos pontos que satisfazem a equação de E e que tem coordenadas em $\mathbb{Z}_p$ será denotado por

$$E(\mathbb{Z}_p) = \{(x, y) \mid x, y \in \mathbb{Z}_p \text{ e } y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$$

Curvas elípticas sobre corpos finitos

Considere a curva elíptica $E : Y^2 = X^3 + 3X + 8$ sobre $\mathbb{Z}_{13}$.

Curvas elípticas sobre corpos finitos

Considere a curva elíptica $E : Y^2 = X^3 + 3X + 8$ sobre $\mathbb{Z}_{13}$. Podemos encontrar os pontos de $E(\mathbb{Z}_{13})$ substituindo cada $x \in \mathbb{Z}_{13}$ no polinômio $X^3 + 3X + 8$ e decidindo se este valor é um quadrado ou não.

Curvas elípticas sobre corpos finitos

Considere a curva elíptica $E : Y^2 = X^3 + 3X + 8$ sobre $\mathbb{Z}_{13}$. Podemos encontrar os pontos de $E(\mathbb{Z}_{13})$ substituindo cada $x \in \mathbb{Z}_{13}$ no polinômio $X^3 + 3X + 8$ e decidindo se este valor é um quadrado ou não.

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

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

Curvas elípticas sobre corpos finitos

Considere a curva elíptica $E : Y^2 = X^3 + 3X + 8$ sobre $\mathbb{Z}_{13}$. Podemos encontrar os pontos de $E(\mathbb{Z}_{13})$ substituindo cada $x \in \mathbb{Z}_{13}$ no polinômio $X^3 + 3X + 8$ e decidindo se este valor é um quadrado ou não.

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

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

Pela tabela que montamos, temos que
$E(\mathbb{Z}_p) = \{\mathcal{O}, (1,5), (1,8), (2,3), (2,10), (9,6), (9,7), (12,2), (12,11)\}$.

Curvas elípticas sobre corpos finitos

Podemos construir uma estrutura de grupo para o conjunto $E(\mathbb{Z}_p)$ de duas formas.

Curvas elípticas sobre corpos finitos

Podemos construir uma estrutura de grupo para o conjunto $E(\mathbb{Z}_p)$ de duas formas.

1. Definir geometria sobre corpos quaisquer, o que é o propósito da Geometria Algébrica;

Curvas elípticas sobre corpos finitos

Podemos construir uma estrutura de grupo para o conjunto $E(\mathbb{Z}_p)$ de duas formas.

1. Definir geometria sobre corpos quaisquer, o que é o propósito da Geometria Algébrica;
2. Utilizar as fórmulas que observamos no teorema anterior.

Curvas elípticas sobre corpos finitos

Podemos construir uma estrutura de grupo para o conjunto $E(\mathbb{Z}_p)$ de duas formas.

1. Definir geometria sobre corpos quaisquer, o que é o propósito da Geometria Algébrica;
2. Utilizar as fórmulas que observamos no teorema anterior. Como as formulas envolviam apenas as operações de soma, subtração, produto e divisão nas coordenadas, então temos que a soma de dois pontos de $E(\mathbb{Z}_p)$ é um ponto em $E(\mathbb{Z}_p)$, já que, $\mathbb{Z}_p$ é um corpo.

Curvas elípticas sobre corpos finitos

Portanto, $E(\mathbb{Z}_p)$ com as operações definidas no teorema anterior é um grupo finito.

Curvas elípticas sobre corpos finitos

Portanto, $E(\mathbb{Z}_p)$ com as operações definidas no teorema anterior é um grupo finito. Com relação a ordem deste grupo, podemos enunciar o seguinte resultado.

Curvas elípticas sobre corpos finitos

Portanto, $E(\mathbb{Z}_p)$ com as operações definidas no teorema anterior é um grupo finito. Com relação a ordem deste grupo, podemos enunciar o seguinte resultado.

Teorema (Hasse)

Seja E uma curva elíptica sobre $\mathbb{Z}_p$. Então $|E(\mathbb{Z}_p)| = p + 1 - t_p$, onde $|t_p| \leq 2\sqrt{p}$.

Curvas elípticas sobre corpos finitos

Portanto, $E(\mathbb{Z}_p)$ com as operações definidas no teorema anterior é um grupo finito. Com relação a ordem deste grupo, podemos enunciar o seguinte resultado.

Teorema (Hasse)

Seja E uma curva elíptica sobre $\mathbb{Z}_p$. Então $|E(\mathbb{Z}_p)| = p + 1 - t_p$, onde $|t_p| \leq 2\sqrt{p}$.

Este valor t_p é chamado de *traço de Frobenius* de E e é obtido como o traço de uma matriz.

ElGamal sobre curvas elípticas

É fácil construir um análogo ao ElGamal para o grupo das curvas elípticas sobra corpos finitos.

ElGamal sobre curvas elípticas

É fácil construir um análogo ao ElGamal para o grupo das curvas elípticas sobra corpos finitos. Porém, teremos que supor que a mensagem Bob deseja enviar para Alice é um ponto $M \in E(\mathbb{Z}_p)$ da curva elíptica,

ElGamal sobre curvas elípticas

É fácil construir um análogo ao ElGamal para o grupo das curvas elípticas sobra corpos finitos. Porém, teremos que supor que a mensagem Bob deseja enviar para Alice é um ponto $M \in E(\mathbb{Z}_p)$ da curva elíptica, onde o primo p e a curva elíptica E, sobre $\mathbb{Z}_p$, são previamente fixados por um canal não seguro de comunicação.

ElGamal sobre curvas elípticas

É fácil construir um análogo ao ElGamal para o grupo das curvas elípticas sobra corpos finitos. Porém, teremos que supor que a mensagem Bob deseja enviar para Alice é um ponto $M \in E(\mathbb{Z}_p)$ da curva elíptica, onde o primo p e a curva elíptica E, sobre $\mathbb{Z}_p$, são previamente fixados por um canal não seguro de comunicação. Além disso eles ainda compartilham um ponto $P \in E(\mathbb{Z}_p)$.

ElGamal sobre curvas elípticas

É fácil construir um análogo ao ElGamal para o grupo das curvas elípticas sobra corpos finitos. Porém, teremos que supor que a mensagem Bob deseja enviar para Alice é um ponto $M \in E(\mathbb{Z}_p)$ da curva elíptica, onde o primo p e a curva elíptica E, sobre $\mathbb{Z}_p$, são previamente fixados por um canal não seguro de comunicação. Além disso eles ainda compartilham um ponto $P \in E(\mathbb{Z}_p)$. Vamos descrever o resto do sistema.

ElGamal sobre curvas elípticas

É fácil construir um análogo ao ElGamal para o grupo das curvas elípticas sobra corpos finitos. Porém, teremos que supor que a mensagem Bob deseja enviar para Alice é um ponto $M \in E(\mathbb{Z}_p)$ da curva elíptica, onde o primo p e a curva elíptica E, sobre $\mathbb{Z}_p$, são previamente fixados por um canal não seguro de comunicação. Além disso eles ainda compartilham um ponto $P \in E(\mathbb{Z}_p)$. Vamos descrever o resto do sistema.

1. Alice escolhe um inteiro secreto n_A e envia para Bob o ponto $Q_A = n_A P$;

ElGamal sobre curvas elípticas

É fácil construir um análogo ao ElGamal para o grupo das curvas elípticas sobra corpos finitos. Porém, teremos que supor que a mensagem Bob deseja enviar para Alice é um ponto $M \in E(\mathbb{Z}_p)$ da curva elíptica, onde o primo p e a curva elíptica E, sobre $\mathbb{Z}_p$, são previamente fixados por um canal não seguro de comunicação. Além disso eles ainda compartilham um ponto $P \in E(\mathbb{Z}_p)$. Vamos descrever o resto do sistema.

1. Alice escolhe um inteiro secreto n_A e envia para Bob o ponto $Q_A = n_A P$;
2. Bob escolhe um inteiro k somente para codificar a mensagem e que será descartado após isto. Ele calcula os pontos

$$C_1 = kP \quad \text{e} \quad C_2 = M + kQ_A$$

ElGamal sobre curvas elípticas

É fácil construir um análogo ao ElGamal para o grupo das curvas elípticas sobra corpos finitos. Porém, teremos que supor que a mensagem Bob deseja enviar para Alice é um ponto $M \in E(\mathbb{Z}_p)$ da curva elíptica, onde o primo p e a curva elíptica E, sobre $\mathbb{Z}_p$, são previamente fixados por um canal não seguro de comunicação. Além disso eles ainda compartilham um ponto $P \in E(\mathbb{Z}_p)$. Vamos descrever o resto do sistema.

1. Alice escolhe um inteiro secreto n_A e envia para Bob o ponto $Q_A = n_A P$;
2. Bob escolhe um inteiro k somente para codificar a mensagem e que será descartado após isto. Ele calcula os pontos

$$C_1 = kP \quad \text{e} \quad C_2 = M + kQ_A$$

e a *mensagem codificada* será o par (C_1, C_2), que é enviado para Alice;

ElGamal sobre curvas elípticas

É fácil construir um análogo ao ElGamal para o grupo das curvas elípticas sobra corpos finitos. Porém, teremos que supor que a mensagem Bob deseja enviar para Alice é um ponto $M \in E(\mathbb{Z}_p)$ da curva elíptica, onde o primo p e a curva elíptica E, sobre $\mathbb{Z}_p$, são previamente fixados por um canal não seguro de comunicação. Além disso eles ainda compartilham um ponto $P \in E(\mathbb{Z}_p)$. Vamos descrever o resto do sistema.

1. Alice escolhe um inteiro secreto n_A e envia para Bob o ponto $Q_A = n_A P$;
2. Bob escolhe um inteiro k somente para codificar a mensagem e que será descartado após isto. Ele calcula os pontos

$$C_1 = kP \quad \text{e} \quad C_2 = M + kQ_A$$

e a *mensagem codificada* será o par (C_1, C_2), que é enviado para Alice;
3. Para decifrar a mensagem de Bob, Alice calcula

$$C_2 - n_A C_1 = (M + kQ_A) - n_A kP = M + k(n_A P) - n_A kP = M.$$

ElGamal sobre curvas elípticas

É claro que a pergunta natural é:

ElGamal sobre curvas elípticas

É claro que a pergunta natural é: como podemos associar mensagens de texto a pontos da curva elíptica?

ElGamal sobre curvas elípticas

É claro que a pergunta natural é: como podemos associar mensagens de texto a pontos da curva elíptica?
Uma resposta para isso, pode ser de associar aleatoriamente caracteres a pontos.

ElGamal sobre curvas elípticas

É claro que a pergunta natural é: como podemos associar mensagens de texto a pontos da curva elíptica?
Uma resposta para isso, pode ser de associar aleatoriamente caracteres a pontos. Mas existe outra forma de fazer um análogo do ElGamal sem que surja este problema.

ElGamal sobre curvas elípticas

É claro que a pergunta natural é: como podemos associar mensagens de texto a pontos da curva elíptica?
Uma resposta para isso, pode ser de associar aleatoriamente caracteres a pontos. Mas existe outra forma de fazer um análogo do ElGamal sem que surja este problema. Isto foi sugerido por Menezes e Vanstone em um trabalho que reduzia o problema do logaritmo discreto em curvas elípticas para o problema em corpos finitos.

ElGamal sobre curvas elípticas

É claro que a pergunta natural é: como podemos associar mensagens de texto a pontos da curva elíptica?
Uma resposta para isso, pode ser de associar aleatoriamente caracteres a pontos. Mas existe outra forma de fazer um análogo do ElGamal sem que surja este problema. Isto foi sugerido por Menezes e Vanstone em um trabalho que reduzia o problema do logaritmo discreto em curvas elípticas para o problema em corpos finitos. Vamos dar a descrição deste método, para finalizar.

Variante de Menezes e Vanstone para ElGamal sobre curvas elípticas

Começamos com um primo p grande, uma curva elíptica E, sobre $\mathbb{Z}_p$, e um ponto $P \in E(\mathbb{Z}_p)$ previamente fixados por um canal não seguro de comunicação.

Variante de Menezes e Vanstone para ElGamal sobre curvas elípticas

Começamos com um primo p grande, uma curva elíptica E, sobre $\mathbb{Z}_p$, e um ponto $P \in E(\mathbb{Z}_p)$ previamente fixados por um canal não seguro de comunicação. Neste caso, a mensagem que Bob enviará para Alice será quebrada em dois números

$$m_1 \text{ e } m_2 \bmod p.$$

Variante de Menezes e Vanstone para ElGamal sobre curvas elípticas

Começamos com um primo p grande, uma curva elíptica E, sobre $\mathbb{Z}_p$, e um ponto $P \in E(\mathbb{Z}_p)$ previamente fixados por um canal não seguro de comunicação. Neste caso, a mensagem que Bob enviará para Alice será quebrada em dois números

$$m_1 \text{ e } m_2 \bmod p.$$

1. Alice escolhe um inteiro secreto n_A e envia para Bob o ponto $Q_A = n_A P$;

Variante de Menezes e Vanstone para ElGamal sobre curvas elípticas

Começamos com um primo p grande, uma curva elíptica E, sobre $\mathbb{Z}_p$, e um ponto $P \in E(\mathbb{Z}_p)$ previamente fixados por um canal não seguro de comunicação. Neste caso, a mensagem que Bob enviará para Alice será quebrada em dois números

$$m_1 \text{ e } m_2 \bmod p.$$

1. Alice escolhe um inteiro secreto n_A e envia para Bob o ponto $Q_A = n_A P$;
2. Bob escolhe um inteiro k somente para codificar a mensagem e que será descartado após isto. Ele calcula os pontos $R = kP$ e $S = kQ_A$ e escreve $S = (x_S, y_S)$.

Variante de Menezes e Vanstone para ElGamal sobre curvas elípticas

Começamos com um primo p grande, uma curva elíptica E, sobre $\mathbb{Z}_p$, e um ponto $P \in E(\mathbb{Z}_p)$ previamente fixados por um canal não seguro de comunicação. Neste caso, a mensagem que Bob enviará para Alice será quebrada em dois números

$$m_1 \text{ e } m_2 \bmod p.$$

1. Alice escolhe um inteiro secreto n_A e envia para Bob o ponto $Q_A = n_A P$;
2. Bob escolhe um inteiro k somente para codificar a mensagem e que será descartado após isto. Ele calcula os pontos $R = kP$ e $S = kQ_A$ e escreve $S = (x_S, y_S)$. Além disso, Bob ainda calcula

$$c_1 \equiv x_S m_1 \text{ e } c_2 \equiv y_S m_2 \bmod p.$$

Variante de Menezes e Vanstone para ElGamal sobre curvas elípticas

Começamos com um primo p grande, uma curva elíptica E, sobre $\mathbb{Z}_p$, e um ponto $P \in E(\mathbb{Z}_p)$ previamente fixados por um canal não seguro de comunicação. Neste caso, a mensagem que Bob enviará para Alice será quebrada em dois números

$$m_1 \text{ e } m_2 \bmod p.$$

1. Alice escolhe um inteiro secreto n_A e envia para Bob o ponto $Q_A = n_A P$;
2. Bob escolhe um inteiro k somente para codificar a mensagem e que será descartado após isto. Ele calcula os pontos $R = kP$ e $S = kQ_A$ e escreve $S = (x_S, y_S)$. Além disso, Bob ainda calcula

$$c_1 \equiv x_S m_1 \text{ e } c_2 \equiv y_S m_2 \bmod p.$$

e a *mensagem codificada* será o trio (R, c_1, c_2), que é enviado para Alice;

Variante de Menezes e Vanstone para ElGamal sobre curvas elípticas

Começamos com um primo p grande, uma curva elíptica E, sobre $\mathbb{Z}_p$, e um ponto $P \in E(\mathbb{Z}_p)$ previamente fixados por um canal não seguro de comunicação. Neste caso, a mensagem que Bob enviará para Alice será quebrada em dois números

$$m_1 \text{ e } m_2 \bmod p.$$

1. Alice escolhe um inteiro secreto n_A e envia para Bob o ponto $Q_A = n_A P$;
2. Bob escolhe um inteiro k somente para codificar a mensagem e que será descartado após isto. Ele calcula os pontos $R = kP$ e $S = kQ_A$ e escreve $S = (x_S, y_S)$. Além disso, Bob ainda calcula

   $$c_1 \equiv x_S m_1 \text{ e } c_2 \equiv y_S m_2 \bmod p.$$

   e a *mensagem codificada* será o trio (R, c_1, c_2), que é enviado para Alice;
3. Para decifrar a mensagem de Bob, Alice calcula $T = n_A R$ e escreve $T = (x_T, y_T)$.

Variante de Menezes e Vanstone para ElGamal sobre curvas elípticas

Começamos com um primo p grande, uma curva elíptica E, sobre $\mathbb{Z}_p$, e um ponto $P \in E(\mathbb{Z}_p)$ previamente fixados por um canal não seguro de comunicação. Neste caso, a mensagem que Bob enviará para Alice será quebrada em dois números

$$m_1 \text{ e } m_2 \bmod p.$$

1. Alice escolhe um inteiro secreto n_A e envia para Bob o ponto $Q_A = n_A P$;
2. Bob escolhe um inteiro k somente para codificar a mensagem e que será descartado após isto. Ele calcula os pontos $R = kP$ e $S = kQ_A$ e escreve $S = (x_S, y_S)$. Além disso, Bob ainda calcula

   $$c_1 \equiv x_S m_1 \text{ e } c_2 \equiv y_S m_2 \bmod p.$$

   e a *mensagem codificada* será o trio (R, c_1, c_2), que é enviado para Alice;
3. Para decifrar a mensagem de Bob, Alice calcula $T = n_A R$ e escreve $T = (x_T, y_T)$. Daí ela calcula

   $$x_T^{-1} c_1 \equiv m_1 \text{ e } y_T^{-1} c_2 \equiv m_2 \bmod p,$$

   já que $T = S$.