Curvas Elípticas en Criptografía

Trabajo Fin de Grado

Adrián H. Ranea Robles

13 de julio de 2016

Universidad de Granada

Tabla de contenidos

Teoría de curvas elípticas

Definición de curva elíptica

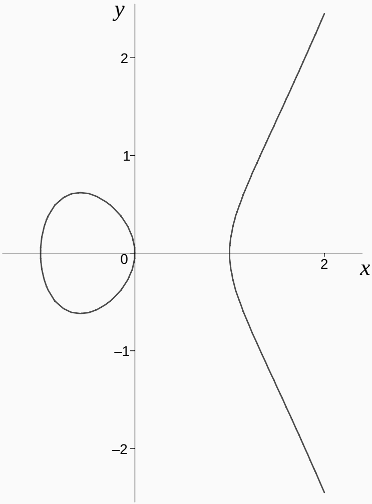
Sea K un cuerpo. Una curva elíptica E se define por una ecuación de la forma

$$E : y^2 = x^3 + ax^2 + b \tag{1}$$

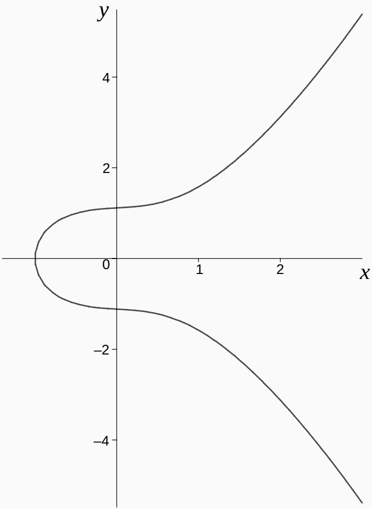
donde $a, b \in K$ y $-16(4a^3 + 27b^2) \neq 0$.

Denotamos por $E(K)$ al conjunto de pares $(x, y) \in K \times K$ que verifican (1) más un punto adicional ∞.

Ejemplos de curvas elípticas sobre $\mathbb{R}$

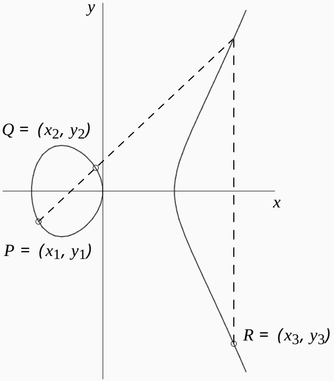


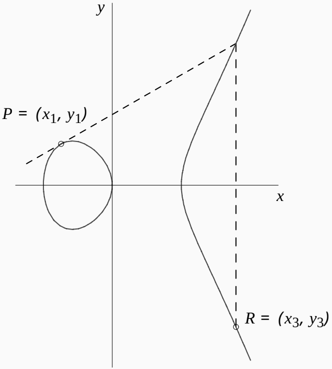
$y^2 = x^3 - x$



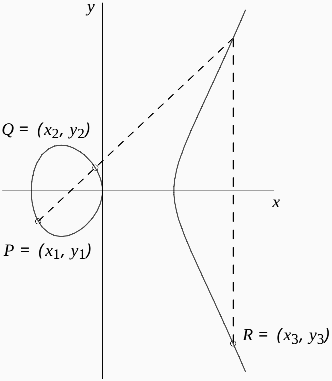
$y^2 = x^3 + x$

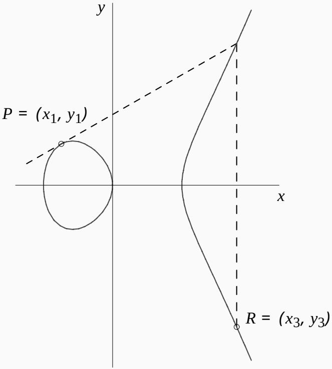
Versión geométrica del método de la cuerda y la tangente





Versión geométrica del método de la cuerda y la tangente





Teorema

$(E(K), +, \infty)$ es un grupo abeliano.

Endomorfismos

Un endomorfismo de E es un homomorfismo $\alpha : E(\overline{K}) \to E(\overline{K})$ dado por funciones racionales r_1, r_2

$$\alpha(x, y) = (r_1(x), r_2(x)y).$$

El grado de un endomorfismo α es el grado de r_1.

α es separable si la derivada $r_1(x)'$ no es idénticamente cero.

Un ejemplo es el *endomorfismo multiplicación por n*

$$n(P) = nP, \; \forall P \in E(\overline{K}).$$

Endomorfismos

Proposición

α es separable $\implies$ $\deg(\alpha) = |\ker(\alpha)|$.

α no es separable $\implies$ $\deg(\alpha) > |\ker(\alpha)|$.

Proposición

$\alpha \neq 0 \implies \alpha$ es sobreyectiva.

Proposición

$n(P)$ es separable $\iff$ $car(K) \nmid n$.

Subgrupos de torsión

Un elemento de $E(\overline{K})$ cuyo orden es finito se llama punto de torsión.

El subgrupo de n-torsión es el subgrupo de $E(\overline{K})$ dado por

$$E[n] = \{P \in E(\overline{K}) \mid nP = \infty\}.$$

Subgrupos de torsión

Un elemento de $E(\overline{K})$ cuyo orden es finito se llama punto de torsión.

El subgrupo de n-torsión es el subgrupo de $E(\overline{K})$ dado por

$$E[n] = \{P \in E(\overline{K}) \mid nP = \infty\}.$$

Teorema

Si $car(K) \nmid n$, entonces

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

Si $car(K) = p > 0$, y $p|n$, entonces

$$E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \text{ o } \simeq \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$$

donde $n = p^r n'$ con $p \nmid n'$.

Curvas elípticas sobre cuerpos finitos

Sea $\mathbb{F}_q$ el cuerpo finito de q elementos.

$E(\mathbb{F}_q)$ es un grupo abeliano *finito*.

Un ejemplo importante de endomorfismo sobre $E(\overline{\mathbb{F}_q})$ es el *endormofirsmo de Frobenius*

$$\phi_q(x, y) = (x^q, y^q), \quad \phi_q(\infty) = \infty$$

Curvas elípticas sobre cuerpos finitos

Sea $\mathbb{F}_q$ el cuerpo finito de q elementos.

$E(\mathbb{F}_q)$ es un grupo abeliano *finito*.

Un ejemplo importante de endomorfismo sobre $E(\overline{\mathbb{F}_q})$ es el *endormofirsmo de Frobenius*

$$\phi_q(x, y) = (x^q, y^q), \quad \phi_q(\infty) = \infty$$

Proposición

Sea E una curva elíptica definida sobre un cuerpo finito $\mathbb{F}_q$ y consideremos el endomorfismo $\phi_q^n - 1$ con $n \geq 1$. Entonces

1. $\ker(\phi_q^n - 1) = E(\mathbb{F}_{q^n})$.
2. $\phi_q^n - 1$ es separable, por lo que $|E(\mathbb{F}_{q^n})| = \deg(\phi_q^n - 1)$.

Teorema de Hasse

Teorema de Hasse

Sea E una curva elíptica definida sobre un cuerpo finito $\mathbb{F}_q$. Entonces el orden de $E(\mathbb{F}_q)$ verifica

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

Criptografía con curvas elípticas

RSA vs ECC

El problema del logaritmo discreto sobre curvas elípticas

Parámetros de dominio y pareja de llaves

ECDH

ccepy

Criptografía con Curvas Elípticas con Python

ccepy es una biblioteca escrita en python 3 para operar con el grupo de puntos de una curva elíptica y trabajar con protocolos criptográficos basados en curvas elípticas.

Herramientas

- Sphinx
- Hypothesis
- Google Style Guide
- Git

Módulos

El software ccepy consta de cuatro módulos principales:

- Aritmética elemental
- Cuerpos finitos
- Curvas elípticas
- Esquemas criptográficos

y uno secundario:

- Listado de curvas elípticas.

Curvas elípticas

Aritmética con curvas elípticas.

Este módulo permite operar con el grupo de puntos de una curva elíptica.

Para utilizar las funciones y las clases de este módulo, debe importarlo previamente:

```
# reemplace ... por la función/clase que desea utilizar
from ccepy.curvas_elipticas import ...
```

Para operar con puntos de una curva elíptica, use las funciones de la forma `curva_eliptica_sobre_*` y los operadores aritméticos habituales.

```
>>> E = curva_eliptica_sobre_Fq(a=2, b=3, p=97)  # y^2 = x^3 + 2x + 3 sobre F97
>>> E.coeficientes
Coeficientes(a=2, b=3)
>>> P = E(0, 10)
>>> P
(0,10)
>>> Q = E(3, 6)
>>> Q
(3,6)
>>> P + Q
(85,71)
>>> -P
(0,87)
>>> 3 * P
(23,24)
```

Usando ccepy

Para instalar la última versión de ccepy:

```
pip install ccepy
```

Un ejemplo de aritmética de curvas elípticas:

```
>>> E = curva_eliptica_sobre_Fq(a=2, b=3, p=97)
>>> E(0, 10) + E(3, 6)
(85,71)
```

Cifrado de las páginas de la UGR

Introducción a HTTPS

Páginas web de la UGR vulnerables