Curvas Elípticas

Emanuel Nicolás Herrador

Facultad de Matemática, Astronomía, Física y Computación
Universidad Nacional de Córdoba

21 de Octubre 2025

Índice

Definición y modelos

Definición (Forma general)

Una curva elíptica (EC) es definida en un cuerpo $\mathbb{K}$ con la ecuación:

$$E/\mathbb{K}: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

donde $a_i \in \mathbb{K}$ $(i = 1, 2, 3, 4, 6)$ y tal que $\Delta \neq 0$ (discriminante).

Definición y modelos

Definición (Forma general)

Una curva elíptica (EC) es definida en un cuerpo $\mathbb{K}$ con la ecuación:

$$E/\mathbb{K}: \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

donde $a_i \in \mathbb{K}$ $(i = 1, 2, 3, 4, 6)$ y tal que $\Delta \neq 0$ (discriminante).

Hay muchos modelos para representar ECs con funciones más sencillas.

Definición y modelos

Hay muchos modelos para representar ECs con funciones más sencillas. Algunos de ellos son:

Definición y modelos

Hay muchos modelos para representar ECs con funciones más sencillas. Algunos de ellos son:

- Weierstrass: $y^2 = x^3 + ax + b \rightarrow$ Modelo más general

Definición y modelos

Hay muchos modelos para representar ECs con funciones más sencillas. Algunos de ellos son:

- Weierstrass: $y^2 = x^3 + ax + b \rightarrow$ Modelo más general
- Montgomery: $by^2 = x^3 + ax^2 + x \rightarrow$ Puntos de orden 2

Definición y modelos

Hay muchos modelos para representar ECs con funciones más sencillas. Algunos de ellos son:

- Weierstrass: $y^2 = x^3 + ax + b \rightarrow$ Modelo más general
- Montgomery: $by^2 = x^3 + ax^2 + x \rightarrow$ Puntos de orden 2
- Twisted Edwards: $ax^2 + y^2 = 1 + dx^2y^2 \rightarrow$ Puntos de orden 4

Definición y modelos

Hay muchos modelos para representar ECs con funciones más sencillas. Algunos de ellos son:

- Weierstrass: $y^2 = x^3 + ax + b \rightarrow$ Modelo más general
- Montgomery: $by^2 = x^3 + ax^2 + x \rightarrow$ Puntos de orden 2
- Twisted Edwards: $ax^2 + y^2 = 1 + dx^2y^2 \rightarrow$ Puntos de orden 4
- Twisted Hessian
- Jacobi intersections

Definición y modelos

Hay muchos modelos para representar ECs con funciones más sencillas. Algunos de ellos son:

- Weierstrass: $y^2 = x^3 + ax + b \rightarrow$ Modelo más general
- Montgomery: $by^2 = x^3 + ax^2 + x \rightarrow$ Puntos de orden 2
- Twisted Edwards: $ax^2 + y^2 = 1 + dx^2y^2 \rightarrow$ Puntos de orden 4
- Twisted Hessian
- Jacobi intersections

Nota

Montgomery $\leftrightarrow$ Weierstrass con cambio de variable $u := bx - \frac{a}{3}$ y $v := by$.

Puntos en EC

Definición (Punto en la curva)

Sea $E/\mathbb{F}_p$ EC y $e \geq 1$, decimos que (x_1, y_1) con $x_1, y_1 \in \mathbb{F}_{p^e}$ es un punto en la curva E si (x_1, y_1) satisface la ecuación de E.

Puntos en EC

Definición (Punto en la curva)

Sea $E/\mathbb{F}_p$ EC y $e \geq 1$, decimos que (x_1, y_1) con $x_1, y_1 \in \mathbb{F}_{p^e}$ es un punto en la curva E si (x_1, y_1) satisface la ecuación de E.

- Se incluye un punto especial $\mathcal{O}$ llamado *punto al infinito*.

Puntos en EC

Definición (Punto en la curva)

Sea $E/\mathbb{F}_p$ EC y $e \geq 1$, decimos que (x_1, y_1) con $x_1, y_1 \in \mathbb{F}_{p^e}$ es un punto en la curva E si (x_1, y_1) satisface la ecuación de E.

- Se incluye un punto especial $\mathcal{O}$ llamado *punto al infinito*.
- $E(\mathbb{F}_{p^e})$ denota el conjunto de puntos de E sobre $\mathbb{F}_{p^e}$ incluyendo $\mathcal{O}$.

Puntos en EC

Definición (Punto en la curva)

Sea $E/\mathbb{F}_p$ EC y $e \geq 1$, decimos que (x_1, y_1) con $x_1, y_1 \in \mathbb{F}_{p^e}$ es un punto en la curva E si (x_1, y_1) satisface la ecuación de E.

- Se incluye un punto especial $\mathcal{O}$ llamado *punto al infinito*.
- $E(\mathbb{F}_{p^e})$ denota el conjunto de puntos de E sobre $\mathbb{F}_{p^e}$ incluyendo $\mathcal{O}$.
- El número de puntos de una EC es cercano a $p^e + 1$:

Teorema (Hasse)

$|E(\mathbb{F}_{p^e})| = p^e + 1 - t$ *para algún entero* t *tal que* $|t| \leq 2\sqrt{p^e}$.

Operaciones: Suma

Supongamos $P, Q, R \in E(\mathbb{F}_{p^e})$.

- Denotamos la suma como $\boxplus$

Operaciones: Suma

Supongamos $P, Q, R \in E(\mathbb{F}_{p^e})$.

- Denotamos la suma como $\boxplus$
- La identidad es $\mathcal{O} \rightarrow \forall P, P \boxplus \mathcal{O} = \mathcal{O} \boxplus P = P$.

Operaciones: Suma

Supongamos $P, Q, R \in E(\mathbb{F}_{p^e})$.

- Denotamos la suma como $\boxplus$
- La identidad es $\mathcal{O} \rightarrow \forall P, P \boxplus \mathcal{O} = \mathcal{O} \boxplus P = P$.
- Supongamos $P \neq Q$ y queremos $P + Q = R$. Gráficamente la idea es:
  1. Dibujar la línea que cruza P y Q.
  2. Denotar $-R$ al tercer punto intersecado en la curva por la línea.
  3. Trazar la recta vertical en $-R$, de tal modo que el punto intersecado en la curva es R.

Operaciones: Suma

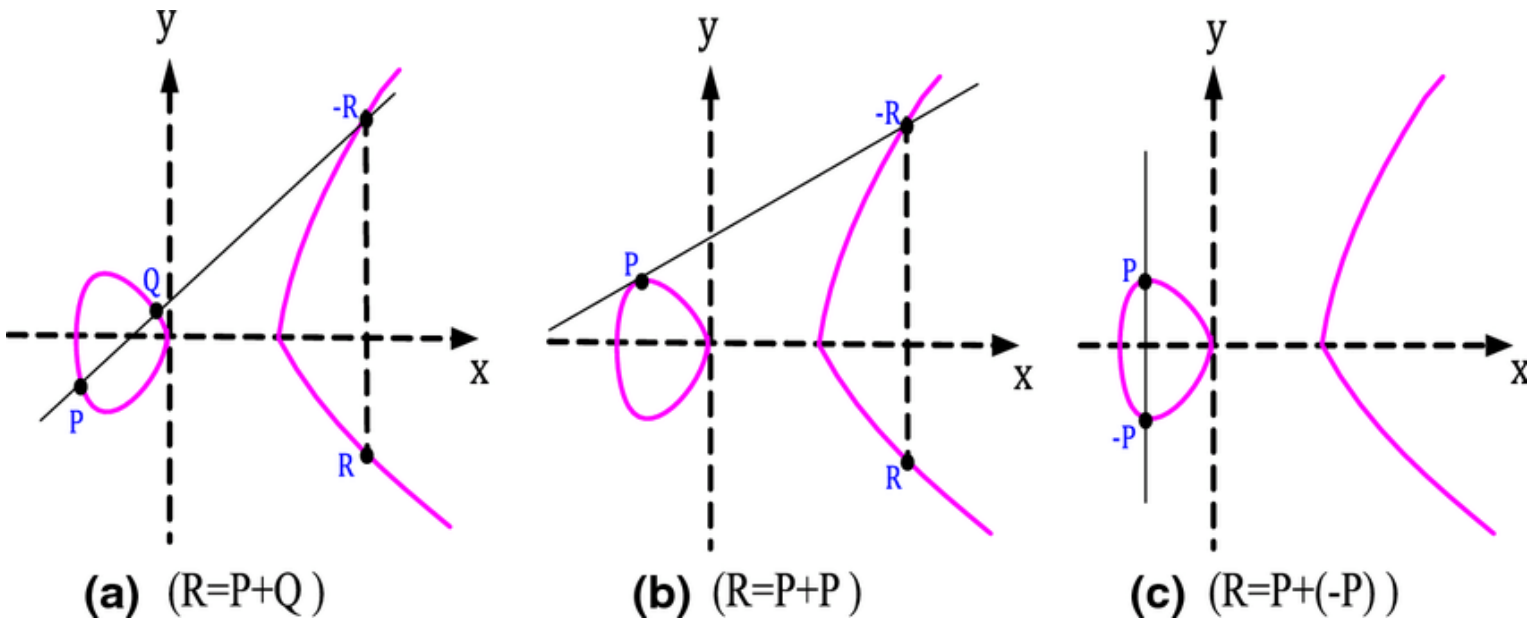
Supongamos $P, Q, R \in E(\mathbb{F}_{p^e})$.

- Denotamos la suma como $\boxplus$
- La identidad es $\mathcal{O} \rightarrow \forall P, P \boxplus \mathcal{O} = \mathcal{O} \boxplus P = P$.
- Supongamos $P \neq Q$ y queremos $P + Q = R$. Gráficamente la idea es:
  1. Dibujar la línea que cruza P y Q.
  2. Denotar $-R$ al tercer punto intersecado en la curva por la línea.
  3. Trazar la recta vertical en $-R$, de tal modo que el punto intersecado en la curva es R.
- Si $P = Q$, el *doblado de puntos* es el mismo proceso pero trazando la tangente a P.

Operaciones: Suma

Supongamos $P, Q, R \in E(\mathbb{F}_{p^e})$.

- Denotamos la suma como $\boxplus$
- La identidad es $\mathcal{O} \rightarrow \forall P, P \boxplus \mathcal{O} = \mathcal{O} \boxplus P = P$.



Operaciones: Suma

Supongamos $P, Q, R \in E(\mathbb{F}_{p^e})$.

- Denotamos la suma como $\boxplus$
- La identidad es $\mathcal{O} \to \forall P, P \boxplus \mathcal{O} = \mathcal{O} \boxplus P = P$.

Nota

Es un grupo abeliano porque cada punto tiene un inverso aditivo, la suma es asociativa y también conmutativa.

Operaciones: Multiplicación por escalar

Supongamos $P \in E(\mathbb{F}_{p^e})$

- Denotamos $kP := \overbrace{P \boxplus \cdots \boxplus P}^{k \text{ veces}}$

Operaciones: Multiplicación por escalar

Supongamos $P \in E(\mathbb{F}_{p^e})$

- Denotamos $kP := \overbrace{P \boxplus \cdots \boxplus P}^{k \text{ veces}}$
- Se puede computar en $O(2 \log_2 k)$ operaciones de grupo usando los algoritmos de Montgomery o de Joye.

Operaciones: Multiplicación por escalar

Supongamos $P \in E(\mathbb{F}_{p^e})$

- Denotamos $kP := \overbrace{P \boxplus \cdots \boxplus P}^{k \text{ veces}}$
- Se puede computar en $O(2\log_2 k)$ operaciones de grupo usando los algoritmos de Montgomery o de Joye.

Algoritmo 1: Idea similar a *binexp*

Input: $P \in E(\mathbb{F}_{p^e}),\ k \in \mathbb{Z}^+$
Output: $kP \in E(\mathbb{F}_{p^e})$
$kP = \mathcal{O},\ b = P$
while $k > 0$ **do**
  if $k\&1$ **then**
    $kP \leftarrow kP \boxplus b$
  $b \leftarrow 2b$
  $k \leftarrow (k \gg 1)$
return kP

Índice

EC en criptografía

Sea $E/\mathbb{F}_p$ una EC, consideraremos:

- $E(\mathbb{F}_p)$ cícliclo, i.e., generado por algún punto $P \in E(\mathbb{F}_p)$.

EC en criptografía

Sea $E/\mathbb{F}_p$ una EC, consideraremos:

- $E(\mathbb{F}_p)$ cícliclo, i.e., generado por algún punto $P \in E(\mathbb{F}_p)$.
- Asunción de que los siguientes problemas son *difíciles* en el grupo:
  - Logaritmo discreto (DL)
  - Computational Diffie-Hellman (CDH)
  - Decision Diffie-Hellman (DDH)

EC en criptografía

Sea $E/\mathbb{F}_p$ una EC, consideraremos:

- $E(\mathbb{F}_p)$ cícliclo, i.e., generado por algún punto $P \in E(\mathbb{F}_p)$.
- Asunción de que los siguientes problemas son *difíciles* en el grupo:
  - Logaritmo discreto (DL)
  - Computational Diffie-Hellman (CDH)
  - Decision Diffie-Hellman (DDH)
- Además de otros usos en esquemas de pairings o isogenies, pueden aplicarse en los criptosistemas vistos anteriormente con grupos finitos.

Análisis de DL y curvas inseguras

Definición (Problema DL)

Sea $P \in E(\mathbb{F}_p)$ de orden q (i.e., tal que $qP = \mathcal{O}$). Son dados (P, q, Q) donde $Q := \alpha P$ para algún $\alpha \in \mathbb{Z}_q$ y se pretende computar α, el logaritmo discreto de Q base P en $E(\mathbb{F}_q)$.

Análisis de DL y curvas inseguras

- El algoritmo para romper DL en un grupo cíclico de orden q usa al menos $O(\sqrt{q})$ operaciones de grupo. En el caso de ECC, tenemos $q := |E(\mathbb{F}_p)|$.

Análisis de DL y curvas inseguras

- El algoritmo para romper DL en un grupo cíclico de orden q usa al menos $O(\sqrt{q})$ operaciones de grupo. En el caso de ECC, tenemos $q := |E(\mathbb{F}_p)|$.
- No todas las curvas son seguras:
  - Si $|E(\mathbb{F}_p)| = q_1 \cdot \cdots \cdot q_n$ con q_i primos tal que $q_i \leq q_{\text{máx}}$, entonces existe un algoritmo que resuelve DL en $\tilde{O}(\sqrt{q_{\text{máx}}})$.
  - Si $|E(\mathbb{F}_p)| = p$ entonces DL es resoluble en tiempo polinomial.

Análisis de DL y curvas inseguras

- El algoritmo para romper DL en un grupo cíclico de orden q usa al menos $O(\sqrt{q})$ operaciones de grupo. En el caso de ECC, tenemos $q := |E(\mathbb{F}_p)|$.
- No todas las curvas son seguras:
  - Si $|E(\mathbb{F}_p)| = q_1 \cdot \cdots \cdot q_n$ con q_i primos tal que $q_i \leq q_{\text{máx}}$, entonces existe un algoritmo que resuelve DL en $\tilde{O}(\sqrt{q_{\text{máx}}})$.
  - Si $|E(\mathbb{F}_p)| = p$ entonces DL es resoluble en tiempo polinomial.
- En particular para $E/\mathbb{F}_{p^e}$, existe un algoritmo que lo resuelve en un tiempo conjeturado de $\tilde{O}\left(p^{2-\frac{2}{e}}\right)$. Por ello, se suele tomar p suficientemente grande para hacerlo impráctico ($p \geq 2^{256}$ es suficiente).

secp256r1

- Conocida como Curva P256 en el estándar de NIST
- Primo $p_r := 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$
- Forma de Weierstrass $y^2 = x^3 - 3x + b$ con b de 255-bits dado por

$$b := \texttt{5ac635d8 aa3a93e7 b3ebbd55 769886bc}$$
$$\texttt{651d06b0 cc53b0f6 3bce3c3e 27d2604b}$$

  elegido de un algoritmo determinístico público con una constante S (seed) dada.
- $|E(\mathbb{F}_{p_r})|$ es primo cercano a p_r
- Se especifica un punto G_r que genera el grupo $E(\mathbb{F}_{p_r})$

secp256r1

- Conocida como Curva P256 en el estándar de NIST
- Primo $p_r := 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$
- Forma de Weierstrass $y^2 = x^3 - 3x + b$ con b de 255-bits dado por

$$b := \texttt{5ac635d8 aa3a93e7 b3ebbd55 769886bc}$$
$$\texttt{651d06b0 cc53b0f6 3bce3c3e 27d2604b}$$

  elegido de un algoritmo determinístico público con una constante S (seed) dada.
- $|E(\mathbb{F}_{p_r})|$ es primo cercano a p_r
- Se especifica un punto G_r que genera el grupo $E(\mathbb{F}_{p_r})$

Nota

Si una organización elige/setea el S, estamos confiando de que no lo haga de modo tal que sea fácil para ellos romper DL el los grupos generados.

secp256k1

- Primo $p_k := 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$
- Forma de Weierstrass $y^2 = x^3 + 7$
- $|E(\mathbb{F}_{p_k})|$ primo cercano a p_k
- Se especifica un punto G_k que genera a $E(\mathbb{F}_{p_k})$

secp256k1

- Es una curva de Koblitz, por lo que $\exists \omega \neq 1 \in \mathbb{F}_p : \omega^3 = 1$.
- Sea el mapeo $\phi : \mathbb{F}_p^2 \to \mathbb{F}_p^2$ dado por $\phi(x, y) := (\omega x, y)$, entonces:
  - Es un mapeo de $E(\mathbb{F}_p)$ en $E(\mathbb{F}_p)$, i.e., homomorfismo de grupo.
  - Luego, $\exists \lambda \in \mathbb{Z}_q : \forall P \in E(\mathbb{F}_p), \phi(P) = \lambda \cdot P$. Este es la raíz no trival en $1 + \lambda + \lambda^2 = 0$.
- Dado $\alpha \in \mathbb{Z}_q$, podemos encontrar $|\tau_i| \leq 2q^{\frac{1}{3}}$ tal que

$$\alpha = \tau_0 + \tau_1 \lambda + \tau_2 \lambda^2$$

- Luego, αP se computa como $\tau_0 \cdot P + \tau_1 \cdot \phi(P) + \tau_2 \cdot \phi^2(P)$, reduciendo su complejidad.

Curve25519

Definición (Twist)

Sean $E/\mathbb{F}_p$ una EC y $c \in \mathbb{F}_p$ no residuo cuadrático. Entonces si la curva E es $y^2 = x^3 + ax + b$, luego su twist/torcedura $\tilde{E}$ es $cy^2 = x^3 + ax + b$.

Curve25519

Definición (Twist)

Sean $E/\mathbb{F}_p$ una EC y $c \in \mathbb{F}_p$ no residuo cuadrático. Entonces si la curva E es $y^2 = x^3 + ax + b$, luego su twist/torcedura $\tilde{E}$ es $cy^2 = x^3 + ax + b$.

Definición (Security twist)

Una curva $E/\mathbb{F}_p$ es *twist secure* si DL es difícil en $E(\mathbb{F}_q)$ y en $\tilde{E}(\mathbb{F}_q)$.

Curve25519

Definición (Twist)

Sean $E/\mathbb{F}_p$ una EC y $c \in \mathbb{F}_p$ no residuo cuadrático. Entonces si la curva E es $y^2 = x^3 + ax + b$, luego su twist/torcedura $\tilde{E}$ es $cy^2 = x^3 + ax + b$.

Definición (Security twist)

Una curva $E/\mathbb{F}_p$ es *twist secure* si DL es difícil en $E(\mathbb{F}_q)$ y en $\tilde{E}(\mathbb{F}_q)$.

Ejemplo de importancia: Supongamos oblivious PRF donde Bob tiene SK $\alpha \in \mathbb{Z}_q$ y dado $P \in E(\mathbb{F}_p)$ retorna αP. Por optimización, a veces solo se pide P_x por lo que no se corrobora pertenencia. Luego, podemos considerar $P \in \tilde{E}(\mathbb{F}_q)$ y como DL es fácil en el twist, obtenemos α.

Demo: Twist and shout (RCSC 2023 - Noruega)

Curve25519

- Diseñada para soportar operaciones de grupo optimizadas y ser twist secure
- Primo $p := 2^{255} - 19$
- Forma de Montgomery: $y^2 = x^3 + 486662 \cdot x^2 + x$
- El cofactor de la curva es 8 (i.e., $|E(\mathbb{F}_p)| = 8k$ con k primo)
- Generada por $P = (x_1, y_1)$ con $x_1 = 9$

Ejemplos de uso

Algunos esquemas de ejemplo donde se usan las EC son:

- ECDH: variante de Diffie-Hellman
- ECDSA: variante de DSA (firma)

La ventaja de EC por sobre esquemas basados en RSA o factorización es que obtiene la misma seguridad con claves más cortas.