

## ARITMÉTICA DE LAS CURVAS ELÍPTICA

En el apartado 1.1 se introducen las curvas elípticas. Se explican las operaciones de grupo adición y duplicación para los puntos de una curva elíptica, junto con su estructura fundamental y otras propiedades.

Las principales referencias usadas en este capítulo han sido [4] y [1].

### 1.1 INTRODUCCIÓN A LAS CURVAS ELÍPTICAS

**Definición 1.1.1.** Una *curva elíptica*  $E$  se define por una ecuación de la forma

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

donde  $a_1, a_2, a_3, a_4, a_6 \in K$  y  $\Delta \neq 0$ , donde  $\Delta$  es el *discriminante* de  $E$  y se define como:

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

Si  $L$  es una extensión del cuerpo  $K$ , entonces el conjunto de puntos  $L$ -*racionales* de  $E$  es:

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

**Nota 1.1.1** (comentarios de la definición 1.1.1).

- La ecuación (1) se conoce como la *ecuación de Weierstrass*.
- Diremos que  $E$  *está definida sobre*  $K$  y lo notaremos  $E/K$ . A  $K$  lo llamaremos *cuerpo base*.
- La condición  $\Delta \neq 0$  asegura que la curva elíptica es «suave», esto es, no hay puntos en los que la curva tenga dos o mas rectas tangentes.
- El punto  $\infty$  es el único punto en la línea del infinito que satisface la forma proyectiva de la ecuación de Weierstrass (véase ??).

**Ejemplo 1.1.1** (curvas elípticas sobre  $\mathbb{R}$ ). Consideramos las curvas elípticas:

$$E_1 : y^2 = x^3 - x$$

$$E_2 : y^2 = x^3 + x$$

definidas sobre el cuerpo  $\mathbb{R}$  de los números reales. Los puntos  $E_1(\mathbb{R})$  y  $E_2(\mathbb{R})$  se han representado en la Figura 1.

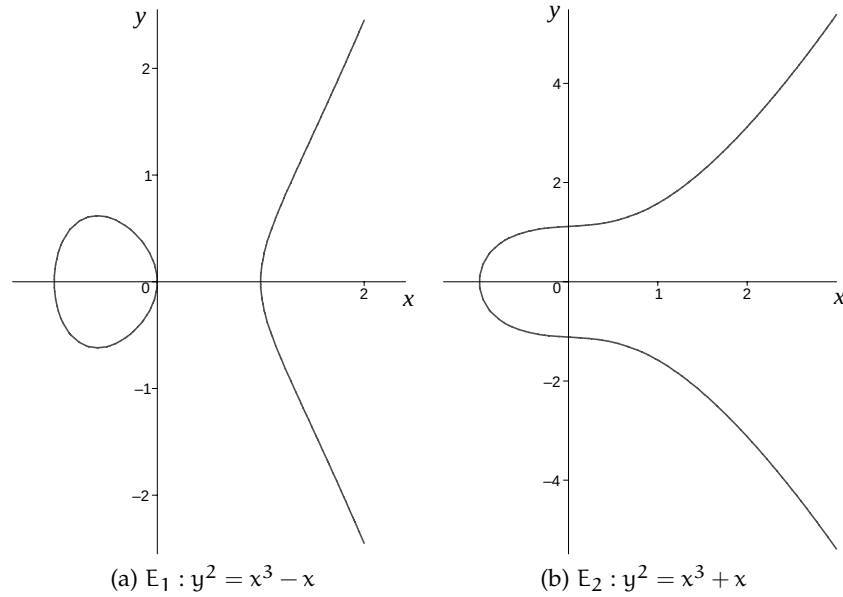


Figura 1: Curvas elípticas sobre  $\mathbb{R}$

### 1.1.1 Ecuaciones de Weierstrass simplificadas

**Definición 1.1.2.** Dos curvas elípticas  $E_1$  y  $E_2$  definidas sobre  $K$  y dadas por las ecuaciones de Weierstrass:

$$E_1 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

$$E_2 : y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6$$

se dicen que son *isomorfas sobre  $K$*  si existen  $u, r, s, t \in K$ ,  $u \neq 0$ , tal que el cambio de variables lineal

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

transforma la ecuación  $E_1$  en la ecuación  $E_2$ . La transformación (3) se llama un cambio de variables admisible.

El cambio de variables (3) es el único que deja «fijo» el punto del infinito y preserva la forma de la ecuación de Weierstrass. No vamos a entrar en más detalle, pero puede consultar [3, prop. III.3.1b] para más información.

Una ecuación de Weierstrass

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

puede simplificarse considerablemente aplicando cambios de variables admisibles. Usaremos las ecuaciones simplificadas en vez de la general en el resto del trabajo. Vamos a considerar por separado los casos en los que el cuerpo base tenga característica distinta de 2 y 3 o tenga característica 2 o 3.

1. Si la característica de  $K$  es distinta de 2 y 3, entonces el cambio de variables admisible

$$(x, y) \mapsto \left( \frac{x - 3a_1^2 - 12a_2}{36}, \frac{y - 3a_1x}{216} - \frac{a_1^3 + 4a_1a_2 - 12a_3}{240} \right)$$

transforma  $E$  en la curva

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

donde  $a, b \in K$ . El discriminante de esta curva es  $\Delta = -16(4a^3 + 27b^2)$ .

2. Si la característica de  $K$  es 2, hay dos casos que considerar. Si  $a_1 \neq 0$ , entonces el cambio de variables admisible

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

transforma  $E$  en la curva

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

donde  $a, b \in K$ . Tales curvas se llaman *no supersingulares* (véase ??) y tiene discriminante  $\Delta = b$ . Si  $a_1 = 0$ , entonces el cambio de variables admisible

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

transforma  $E$  en la curva

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

donde  $a, b, c \in K$ . Tales curvas se llaman *supersingulares* (véase ??) y tiene discriminante  $\Delta = c^4$ .

3. Si la característica de  $K$  es 4, entonces hay dos casos que considerar. Si  $a_1^2 \neq -a_2$ , entonces el cambio de variables admisible

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

donde  $d_2 = a_1^2 + a_2$  y  $d_4 = a_4 - a_1 a_3$ , transforma E en la curva

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

donde  $a, b \in K$ . Tales curvas se llaman *no supersingulares* (véase ??) y tiene discriminante  $\Delta = -a^3b$ . Si  $a_1^2 = -a_2$ , entonces el cambio de variables admisible

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

transforma E en la curva

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

donde  $a, b \in K$ . Tales curvas se llaman *supersingulares* (véase ??) y tiene discriminante  $\Delta = -a^3$ .

*Demostración.* La demostración completa puede encontrarse en [3, sec. III.1]. Se trata simplemente de completar cuadrados y realizar sustituciones, por ello aquí solo mostraremos la demostración de la primera simplificación.

En primer lugar, sumando en la ecuación de Weierstrass (1) en ambos lados por  $(a_1 a_3 x)/2 + a_3^2/4 + (a_1^2 x^2)/4$ , completamos el cuadrado:

$$\left(y + \frac{a_1 x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1 a_3}{2}\right)x + \left(a_6 + \frac{a_3^2}{4}\right)$$

Haciendo  $y_1 = y + (a_1 x)/2 + a_3/2$ , obtenemos

$$y_1^2 = x^3 + a'_2 x^2 + a'_4 x + a'_6$$

para algunas constantes  $a'_2, a'_4, a'_6 \in K$ . Finalmente, sustituyendo  $x_1 = x + a'_2/3$  resulta

$$y_1^2 = x_1^3 + ax_1 + b$$

para algunas constante  $a, b \in K$ . Para obtener el discriminante  $\Delta$  basta sustituir el valor de las constantes  $a_4 = a$ ,  $a_6 = b$  y  $a_1 = a_3 = a_2 = 0$  en (2).  $\square$

### 1.1.2 Ley de grupo

Sea E una curva elíptica definida sobre un cuerpo K. Hay un *método de la cuerda y la tangente* para sumar dos puntos en  $E(K)$  y obtener un tercer punto en  $E(K)$ . Junto con esta operación aditiva, el conjunto de puntos  $E(K)$  forma un grupo abeliano con  $\infty$  como elemento neutro.

La regla aditiva se explica fácilmente geométricamente. Sea P y Q dos puntos distintos de una curva elíptica E. Entonces la *suma* R, de P y Q esta definido como sigue. Se dibuja una recta L de P a Q. Esta recta intersecta la curva elíptica en un tercer punto. Entonces R es la

reflexión de este punto sobre el eje- $x$ . Esto se puede apreciar en la Figura 2a.

El *doble*  $R$ , de  $P$ , se define como sigue. Se dibuja la línea tangente  $L$  a la curva elíptica en  $P$ . Esta línea intersecta la curva elíptica en un segundo punto. Entonces  $R$  es la reflexión de este punto sobre el eje- $x$ . Esto se puede apreciar en la Figura 2b.

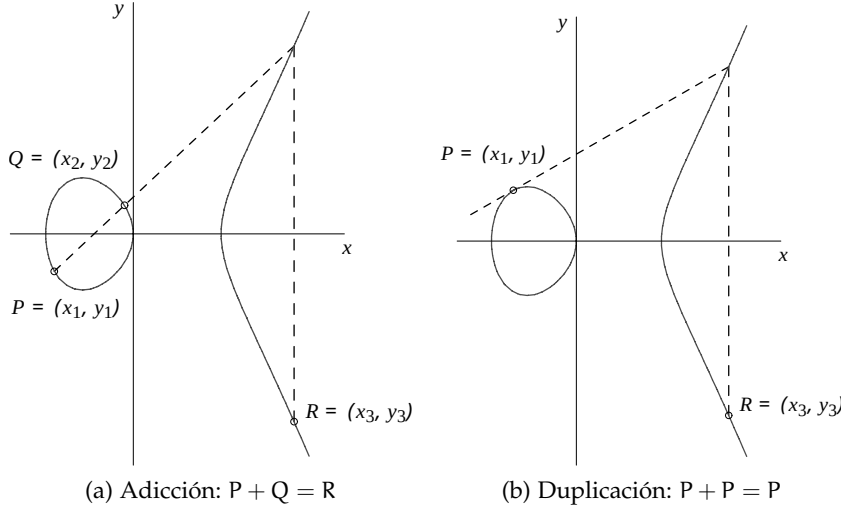


Figura 2: Adición y duplicación geométrica de puntos de una curva elíptica

El hecho de que  $L \cap E$ , contando multiplicidades, consiste en exactamente tres puntos (no necesariamente distintos) es un caso especial del teorema de Bézout [2, sec. I.7.8]. Sin embargo, como vamos a dar fórmulas explícitas posteriormente en esta sección, no hay necesidad de usar un teorema general.

**Definición 1.1.3** (ley de grupo). Sea  $E$  una curva elíptica definida por la ecuación  $y^2 = x^3 + ax + b$  sobre un cuerpo  $K$  de característica distinta de 2 y 3. Definimos la operación binaria  $+$  :  $E(K) \times E(K) \rightarrow E(K)$  como sigue:

- a)  $P + \infty = \infty + P = P$ , para todo  $P \in E(K)$
- b) Si  $P = (x, y) \in E(K)$ , entonces  $(x, y) + (x, -y) = \infty$ . El punto  $(x, -y)$  se denotará por  $-P$  y se llamará el *negativo* de  $P$ . Además,  $-\infty = \infty$ .
- c) Sea  $P = (x_1, y_1) \in E(K)$  y  $Q = (x_2, y_2) \in E(K)$ , donde  $P \neq \pm Q$ . Entonces  $P + Q = (x_3, y_3)$ , donde

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

- d) Sea  $P = (x_1, y_1) \in E(K)$ , donde  $P \neq \pm P$ . Entonces  $2P = (x_3, y_3)$  donde:

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

*Demostración.* Tenemos que comprobar que  $+$  es una operación binaria válida, esto es, que a cada par de elementos de  $E(K) \times E(K)$  le corresponde un único elemento de  $E(K)$ . Como la casuística anterior es total y exclusiva, basta ver que  $+$  es una operación cerrada. Los casos a) y b) son triviales. Veamos los otros dos casos con detalle.

CASO c) Supongamos  $P = (x_1, y_1)$ ,  $Q = (x_2, y_2)$ ,  $P, Q \in E(K)$  con  $P \neq \pm Q$ . Consideramos la recta siguiente

$$L : y = m(x - x_1) + y_1, \text{ donde } m = \frac{y_2 - y_1}{x_2 - x_1}$$

Nótese que  $x_2 \neq x_1$  ya que  $P \neq \pm Q$ . Para hallar la intersección de  $L$  con  $E$  sustituimos  $y$ :

$$(m(x - x_1) + y_1)^2 = x^3 + ax + b$$

Podemos reescribir esto de la forma

$$0 = x^3 - m^2x^2 + b'x + c' \quad (4)$$

para algunas constantes  $b', c' \in K$ . Así, las raíces de esta cúbica es justamente  $L \cup E$ .

Sabemos que las raíces de un polinomio están relacionadas con sus coeficientes. De hecho, para un polinomio cúbico mónico  $x^3 + c_2x^2 + c_1x + c_0$  con raíces  $r, s, t$  se tiene:

$$\begin{aligned} x^3 + c_2x^2 + c_1x + c_0 &= (x - r)(x - s)(x - t) \\ &= x^3 - (r + s + t)x^2 + (rs + rt + st)x - rst, \end{aligned}$$

En particular,  $r + s + t = -c_2$ . Como  $P$  y  $Q$  están en la intersección,  $x_1$  y  $x_2$  son dos raíces de (4), luego la tercera raíz  $\alpha$  es  $m^2 - x_1 - x_2$ . Sustituyendo  $\alpha$  en  $L$  resulta  $\beta = m(x_3 - x_1) + y_1$ , luego  $(\alpha, \beta) \in E(K)$ . Entonces  $(\alpha, -\beta) = (x_3, y_3) \in E(K)$ .

CASO d) Sea  $P = (x_1, y_1)$ , donde  $P \neq -P$ . Consideramos la recta siguiente

$$L : y = m(x - x_1) + y_1, \text{ donde } m = \frac{3x_1^2 + a}{2y_1}$$

Nótese que  $y_1 \neq 0$  ya que si no estaríamos en el caso b). Hallamos la intersección con  $E$  de forma análoga al caso c) y obtenemos la cúbica:

$$0 = x^3 - m^2x^2 + b'x + c'$$

para algunas constantes  $b', c' \in K$ . Análogamente al caso c), como  $x_1$  es una raíz doble de la cúbica (derívese y evalúe en  $x_1$ ) tenemos que la tercera raíz  $\alpha$  es  $m^2 - 2x_1$ . Sustituyendo  $\alpha$  en  $L$  resulta  $\beta = m(x_3 - x_1) + y_1$ , luego  $(\alpha, \beta) \in E(K)$ . Entonces  $(\alpha, -\beta) = (x_3, y_3) \in E(K)$ .  $\square$

**Teorema 1.1.1.** La suma de puntos en una curva elíptica  $E$  sobre un cuerpo  $K$  de característica distinta de 2 y 3 satisface las siguientes propiedades:

- *Conmutatividad.*  $P_1 + P_2 = P_2 + P_1, \forall P_1, P_2 \in E(K).$
- *Existencia de elemento neutro.*  $P + \infty = P, \forall P \in E(K).$
- *Existencia de elemento opuesto.*  $P + -P = \infty, \forall P \in E(K).$
- *Asociatividad.*  $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3), \forall P_1, P_2, P_3 \in E(K).$

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

*Demostración.* ...

□





Parte I

APÉNDICE



## BIBLIOGRAFÍA

---

- [1] Darrel Hankerson, Alfred J. Menezes y Scott Vanstone. *Guide to Elliptic Curve Cryptography*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2003. ISBN: 038795273X.
- [2] R. Hartshorne. *Algebraic Geometry*. Encyclopaedia of mathematical sciences. Springer, 1977. ISBN: 9780387902449.
- [3] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009. ISBN: 9780387094946.
- [4] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition*. 2.<sup>a</sup> ed. Chapman & Hall/CRC, 2008. ISBN: 9781420071467.