# Curvas elípticas

**Alexey Beshenov (cadadr@gmail.com)**

**Universidad de El Salvador. Abril de 2018**

Estos son mis apuntes para una serie de charlas sobre las curvas elípticas dadas en el seminario de pregrado ALGA (= álgebra, geometría, aritmética) en la universidad de San Salvador. El lector interesado debe consultar las partes relevantes de la biblia de las curvas elípticas [Sil2009].

## 1 Ecuaciones de Weierstrass

charla 19.04.18

Sea $k$ un cuerpo. Recordemos brevemente que el **plano proyectivo** sobre $k$ es el conjunto

$$\mathbb{P}^2(k) := (\mathbb{A}^3(k) \setminus \{0\}) / \sim,$$

donde $\mathbb{A}^3(k) = k^3$ es el espacio afín tridimensional sobre $k$ y $\sim$ es la relación de equivalencia definida por

$$(X, Y, Z) \sim (X', Y', Z') \iff (X', Y', Z') = (\lambda X, \lambda Y, \lambda Z) \text{ para algún } \lambda \in k^\times.$$

Entonces, los puntos de $\mathbb{P}^2(k)$ son las clases de equivalencia

$$[X : Y : Z] := \{(\lambda X, \lambda Y, \lambda Z) \mid \lambda \in k^\times\}.$$

Se dice que un polinomio

$$F = \sum_{i,j,k} a_{i,j,k} X^i Y^i Z^k \in k[X, Y, Z]$$

es **homogéneo** si todos sus términos tienen el mismo grado; es decir, si $a_{i,j,k} \neq 0$ solamente cuando $i + j + k = d$, donde $d$ es algún número fijo, llamado el **grado** de $F$.

En este caso a $F$ se asocia una **función homogénea** de grado $d$ sobre el espacio afín $\mathbb{A}^3(k)$: para cualesquiera $X, Y, Z, \lambda \in k$

$$F(\lambda X, \lambda Y, \lambda Z) = \lambda^d F(X, Y, Z).$$

Para cualesquiera $X, Y, Z$ y $\lambda \in k^\times$ se cumple

$$F(\lambda X, \lambda Y, \lambda Z) = 0 \iff F(X, Y, Z) = 0.$$

Esto significa que está bien definido el conjunto de los ceros de $F$ sobre el plano proyectivo $\mathbb{P}^2(k)$:

$$C := \{[X : Y : Z] \in \mathbb{P}^2(k) \mid F(X, Y, Z) = 0\}.$$

Este conjunto es la **curva algebraica (plana, proyectiva)** asociada al polinomio homogéneo $F$.

Nos van a interesar las curvas definidas por un polinomio cúbico de la forma

$$F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3,$$

donde $a_1, a_2, a_3, a_4, a_6 \in k$ son algunos parámetros fijos (aunque al principio su numeración parece rara, detrás de esta hay una buena razón).

En otras palabras, nos interesan las soluciones de las ecuaciones de la forma

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

Estas se llaman las **ecuaciones de Weierstrass**.

Si $Z = 0$, se ve que también $X = 0$ y el único punto que nos queda es $[0 : 1 : 0]$. Este se llama **el punto al infinito** de la curva. Si asumimos que $Z \neq 0$, podemos reescribir la ecuación en términos de las coordenadas inhomogéneas $x := X/Z$ e $y := Y/Z$:

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

Los ceros $(x, y)$ de esta ecuación en el plano afín $\mathbb{A}^2(k)$ corresponden precisamente a los puntos de la curva proyectiva, salvo el punto $O := [0 : 1 : 0]$.

Si $\operatorname{char} k \neq 2$, entonces podemos simplificar la parte izquierda de la ecuación reemplazando $y$ por $\frac{1}{2}(y - a_1x - a_3)$ (note que esta es una aplicación lineal invertible). Se obtiene

$$\frac{1}{4}y^2 - \frac{a_1^2}{4}x^2 - \frac{a_1\,a_3}{2}x - \frac{a_3^2}{4} = x^3 + a_2x^2 + a_4x + a_6.$$

Multiplicando ambas partes por 4 y reordenando los términos, la ecuación se vuelve

$$y^2 = 4\,x^3 + (a_1^2 + 4\,a_2)\,x^2 + (4\,a_4 + 2\,a_1\,a_3)\,x + (a_3^2 + 4\,a_6).$$

Pongamos

$$b_2 := a_1^2 + 4\,a_2, \quad b_4 := 2\,a_4 + a_1\,a_3, \quad b_6 := a_3^2 + 4\,a_6.$$

Entonces, nuestra ecuación es

$$y^2 = 4\,x^3 + b_2\,x^2 + 2\,b_4\,x + b_6.$$

Ahora si $\operatorname{char} k \neq 2, 3$ podemos hacer otra sustitución más:

$$x \mapsto \frac{x - 2\,b_2}{36}, \quad y \mapsto \frac{y}{108}$$

(nota: $36 = 2^2 \cdot 3^2$, $108 = 2^2 \cdot 3^3$, y de nuevo se trata de una aplicación lineal invertible). La ecuación se vuelve

$$y^2 = x^3 + 27\,(24\,b_4 - b_2^2)\,x + 54\,(b_2^3 - 36\,b_2\,b_4 + 216\,b_6).$$

Poniendo

$$c_4 := b_2^2 - 24\,b_4, \quad c_6 := -b_2^3 + 36\,b_2\,b_4 - 216\,b_6,$$

podemos escribir la ecuación como

$$y^2 = x^3 - 27\,c_4\,x - 54\,c_6.$$

Esto quiere decir que para $\operatorname{char} k \neq 2, 3$ se puede considerar las curvas definidas por las ecuaciones

$$y^2 = x^3 + A\,x + B,$$

donde

$$A = -27\,c_4, \quad B = -54\,c_6.$$

Volviendo a las ecuaciones homogéneas proyectivas, tenemos

$$Y^2Z = X^3 + A\,XZ^2 + B\,Z^3.$$

A partir de ahora vamos a trabajar solamente con estas curvas, bajo la hipótesis que $\operatorname{char} k \neq 2, 3$.

## 2 Discriminante

Un punto $P$ de una curva algebraica definida por un polinomio homogéneo $F \in k[X, Y, Z]$ es **singular** si todas las derivadas parciales de $F$ se anulan en $P$:

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0.$$

Las ecuaciones de arriba automáticamente implican que $F(P) = 0$; es decir, para encontrar los puntos singulares, hay que encontrar las soluciones del sistema de ecuaciones de arriba. Para una curva afín definida por un polinomio $f \in k[x, y]$, hay que considerar el sistema de ecuaciones

$$f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

En nuestro caso de interés se trabaja con

$$F(X, Y, Z) = Y^2 Z - X^3 - A\, XZ^2 - B\, Z^3.$$

Notamos que el punto $O := [0 : 1 : 0]$ nunca es singular: tenemos

$$\frac{\partial F}{\partial Z} = Y^2 - A\, X^2 - 3\, B\, Z^2,$$

y luego

$$\frac{\partial F}{\partial Z}(O) = 1 \neq 0.$$

Entonces, podemos pasar a la ecuación afín

$$f(x, y) = y^2 - x^3 - A\, x - B = 0.$$

Examinemos cuándo $(x, y) \in \mathbb{A}^2(k)$ es un punto singular de la curva. Se obtiene un sistema de ecuaciones

$$\begin{aligned} f(x, y) = y^2 - x^3 - A\, x - B &= 0, \\ \frac{\partial f}{\partial x} = -3\, x^2 - A &= 0, \\ \frac{\partial f}{\partial y} = 2\, y &= 0. \end{aligned}$$

De la última ecuación se obtiene $y = 0$, así que todo punto singular necesariamente pertenece al eje $x$. Luego, nos queda el sistema de ecuaciones

$$\begin{aligned} x^3 + A\, x + B &= 0, \\ 3\, x^2 + A &= 0. \end{aligned}$$

Notamos primero que estas dos ecuaciones tienen a lo sumo una raíz en común (sin contar las multiplicidades). He aquí un modo elemental de verlo. Si hubiera dos raíces en común, el polinomio $x^2 + A/3$ tendría que dividir a $x^3 + A\, x + B$; es decir, tendríamos para algún $c \in k$

$$x^3 + A\, x + B = \left(x^2 + \frac{A}{3}\right)\, (x - c).$$

Sin embargo,

$$\left(x^2+\frac{A}{3}\right)(x-c)=x^3-c\,x^2+\frac{A}{3}\,x-\frac{Ac}{3},$$

y se ve que este polinomio será igual a $x^3+A\,x+B$ solamente cuando $A=B=0$ (como siempre, $\operatorname{char} k\neq 2,3$) y se trata de la curva $y^2=x^3$ que tiene solamente un punto singular $(0,0)$.

Sería instructivo recordar un método general que nos permita detectar existencia de una raíz común de dos polinomios con coeficientes en $k$

$$f=a_m\,x^m+a_{m-1}\,x^{m-1}+\cdots+a_1\,x+a_0\quad\text{y}\quad g=b_n\,x^n+b_{n-1}\,x^{n-1}+\cdots+b_1\,x+b_0.$$

Los polinomios $f$ y $g$ tienen una raíz común en $k$ si y solamente si su **resultante** $\operatorname{Res}(f,g)$ es nulo.

Por la definición, $\operatorname{Res}(f,g)$ es el determinante de la **matriz de Sylvester** que es la matriz de $(m+n)\times(m+n)$ donde en la primera fila está el vector

$$(a_m,a_{m-1},\ldots,a_1,a_0,0,\ldots,0)$$

en la segunda fila está

$$(0,a_m,a_{m-1},\ldots,a_1,a_0,0,\ldots,0),$$

en la tercera fila

$$(0,0,a_m,a_{m-1},\ldots,a_1,a_0,0,\ldots,0),$$

etcétera, hasta que se llegue al vector

$$(0,\ldots,0,a_m,a_{m-1},\ldots,a_1,a_0).$$

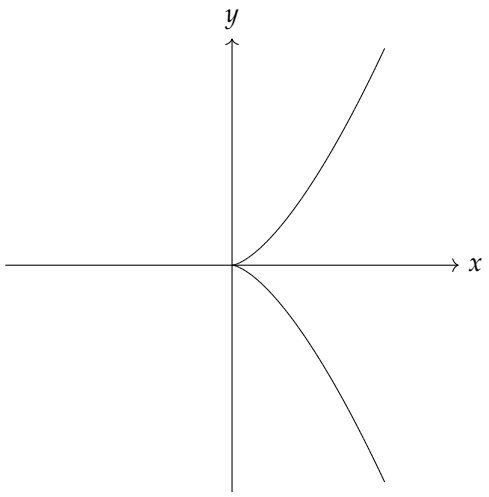
Luego siguen los vectores

$$\begin{gathered}(b_n,b_{n-1},\ldots,b_1,b_0,0,\ldots,0),\\(0,b_n,b_{n-1},\ldots,b_1,b_0,0,\ldots,0),\\(0,0,b_n,b_{n-1},\ldots,b_1,b_0,0,\ldots,0),\\\ldots\\(0,\ldots,0,a_n,a_{n-1},\ldots,a_1,a_0).\end{gathered}$$

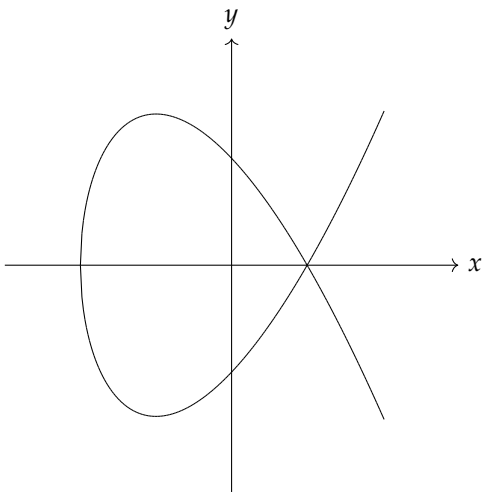
En nuestro caso tenemos

$$\operatorname{Res}(x^3+A\,x+B,\ 3\,x^2+A)=\det\begin{pmatrix}1&0&A&B&0\\0&1&0&A&B\\3&0&A&0&0\\0&3&0&A&0\\0&0&3&0&A\end{pmatrix}=4\,A^3+27\,B^2.$$

Podemos concluir que la curva definida por $Y^2Z=X^3+A\,XZ^2+B\,Z^3$ tiene un punto singular si y solamente si $4\,A^3+27\,B^2=0$.




cúbica singular $y^2 = x^3$




cúbica singular $y^2 = x^3 - 3x + 2$

El número

$$\Delta := -16\,(4\,A^3 + 27\,B^2)$$

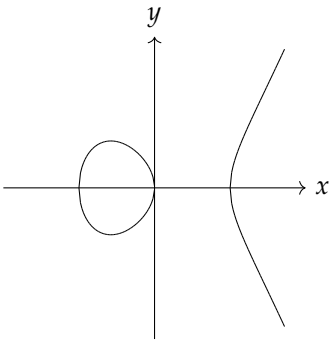
se llama el **discriminante** de la curva. El múltiplo "$-16$" tiene cierto significado, pero no nos va a servir por el momento.

**Definición.** Para $\operatorname{char} k \neq 2, 3$ una **curva elíptica** sobre $k$ es una curva proyectiva definida por una ecuación cúbica

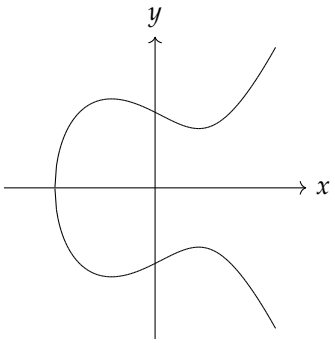
$$Y^2Z = X^3 + A\,XZ^2 + B\,Z^3,$$

donde $A, B \in k$ y el discriminante $\Delta$ no es nulo.

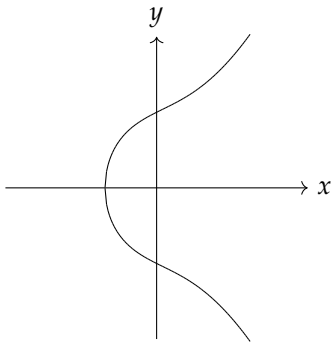
Esta definición *ad hoc* será suficiente para nuestros objetivos. La verdadera definición es más bonita, pero al final se reduce a estas ecuaciones. He aquí las gráficas de los puntos reales de algunas curvas de la forma $y^2 = x^3 + A\,x + B$.




curva elíptica $y^2 = x^3 - x$




curva elíptica $y^2 = x^3 - x + 1$




curva elíptica $y^2 = x^3 + x + 1$

## 3 El caso general ($a_1, a_2, a_3, a_4, a_6$)

Para simplificar la exposición vamos a trabajar principalmente con las curvas elípticas de la forma

añadido después

$$Y^2Z = X^3 + AXZ^2 + BZ^3,$$

pero más adelante nos servirán las curvas definidas por

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0.$$

De nuevo, tenemos

$$\frac{\partial F}{\partial Z} = Y^2 + a_1XY + 2\,a_3YZ - a_2X^2 - 2\,a_4XZ - 3\,a_6Z^2.$$

Luego, se ve que $\frac{\partial F}{\partial Z}(O) = 1 \neq 0$, así que podemos pasar al polinomio inhomogéneo correspondiente

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6.$$

Calculamos

$$\begin{aligned}\frac{\partial f}{\partial x} &= a_1y - 3\,x^2 - 2\,a_2x - a_4,\\ \frac{\partial f}{\partial y} &= 2\,y + a_1x + a_3.\end{aligned}$$

Así que un punto singular corresponde a una solución del sistema de ecuaciones

$$\begin{aligned}y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 &= 0,\\ a_1y - 3\,x^2 - 2\,a_2x - a_4 &= 0,\\ 2\,y + a_1x + a_3 &= 0.\end{aligned}$$

Si $\operatorname{char} k \neq 2$, de la última ecuación podemos expresar $y = -(a_1x + a_3)/2$, sustituirlo en las primeras dos ecuaciones y obtener

$$\begin{aligned}4\,x^3 + b_2\,x^2 + 2\,b_4\,x + b_6 &= 0,\\ 6\,x^2 + b_2\,x + b_4 &= 0,\end{aligned}$$

donde

$$b_2 := a_1^2 + 4\,a_2, \quad b_4 := 2\,a_4 + a_1\,a_3, \quad b_6 := a_3^2 + 4\,a_6.$$

Luego, se puede calcular que

$$\operatorname{Res}(4\,x^3 + b_2\,x^2 + 2\,b_4\,x + b_6, 6\,x^2 + b_2\,x + b_4) = -8\,\Delta,$$

donde

$$\Delta := -b_2^2\,b_8 - 8\,b_4^3 - 27\,b_6^2 + 9\,b_2\,b_4\,b_6, \quad b_8 := a_1^2\,a_6 + 4\,a_2\,a_6 - a_1\,a_3\,a_4 + a_2\,a_3^2 - a_4^2.$$

En particular, para $a_1 = a_2 = a_3 = 0$ y $a_4 = A$, $a_6 = B$, se tiene $b_2 = 0$, $b_4 = 2\,A$, $b_6 = 4\,B$, $b_8 = -A^2$, $\Delta = -16(4\,A^3 + 27\,B^2)$.

# 4 La ley de grupo

charla 26.04.18

**Definición.** Consideremos una curva elíptica $E$ sobre un cuerpo $k$ definida por la ecuación

$$Y^2Z = X^3 + A\,XZ^2 + B\,Z^3.$$

Consideremos la siguiente operación sobre los puntos $E(k) \subset \mathbb{P}^2(k)$, o en general $E(K) \subset \mathbb{P}^2(K)$ para cualquier extensión de cuerpos $K/k$. Para dos puntos $P, Q \in E(K)$, sea $\ell$ la recta que pasa por $P$ y $Q$ (si $P = Q$, se considera la tangente que pasa por $P$) y sea $R$ el tercer punto de intersección de $\ell$ con $E$. Sea $\ell'$ la recta que pasa por $R$ y $O := [0:1:0]$. Entonces, el punto $P \oplus Q$ es el tercer punto de intersección de $E$ con $\ell'$.

Todas las intersecciones se cuentan con multiplicidades.

Para entender todo esto, no estaría mal revisar un poco de la "geometría analítica" proyectiva. Hagamos una serie de observaciones.

1. La definición es simétrica en $P$ y $Q$, así que $P \oplus Q = Q \oplus P$ para cualesquiera $P, Q \in E(K)$.

2. Una recta proyectiva que pasa por dos puntos $P = [X_P : Y_P : Z_P]$ y $Q = [X_P : Y_P : Z_P]$ corresponde al plano en el espacio afín $\mathbb{A}^3(k)$ que pasa por las rectas que corresponden a $P$ y $Q$. Entonces, los puntos de esta recta proyectiva están dados por la ecuación

$$\begin{aligned}\det \begin{pmatrix} X & Y & Z \\ X_P & Y_P & Z_P \\ X_Q & Y_Q & Z_Q \end{pmatrix} &= X \det \begin{pmatrix} Y_P & Z_P \\ Y_Q & Z_Q \end{pmatrix} - Y \det \begin{pmatrix} X_P & Z_P \\ X_Q & Z_Q \end{pmatrix} + Z \det \begin{pmatrix} X_P & Y_P \\ X_Q & Y_Q \end{pmatrix} \\ &= X\,(Y_P\,Z_Q - Z_P\,Y_Q) - Y\,(X_P\,Z_Q - Z_P\,X_Q) + Z\,(X_P\,Y_Q - Y_P\,X_Q) = 0.\end{aligned}$$

   Si nos interesa la parte afín donde $Z \neq 0$ y si $Z_P, Z_Q \neq 0$, podemos dividir todo por $Z, Z_P, Z_Q$ y obtener la ecuación de la recta afín en las coordenadas inhomogéneas $x := X/Z$, $y := Y/Z$:

$$\frac{1}{Z}\frac{1}{Z_P}\frac{1}{Z_Q} \det \begin{pmatrix} X & Y & Z \\ X_P & Y_P & Z_P \\ X_Q & Y_Q & Z_Q \end{pmatrix} = \det \begin{pmatrix} X/Z & Y/Z & 1 \\ X_P/Z_P & Y_P/Z_P & 1 \\ X_Q/Z_Q & Y_Q/Z_Q & 1 \end{pmatrix} = \det \begin{pmatrix} x & y & 1 \\ x_P & y_P & 1 \\ x_Q & y_Q & 1 \end{pmatrix} = 0.$$

   Es la ecuación habitual para la recta en $\mathbb{A}^2(k)$ que pasa por $(x_P, y_P)$ y $(x_q, y_q)$. Recordemos que cuando $x_P \neq x_Q$, de aquí se puede pasar a la ecuación

$$\frac{1}{x_P - x_Q} \det \begin{pmatrix} x & y & 1 \\ x_P & y_P & 1 \\ x_Q & y_Q & 1 \end{pmatrix} = x\,\frac{y_P - y_Q}{x_P - x_Q} - y + \frac{x_P\,y_Q - y_P\,x_Q}{x_P - x_Q} = 0$$

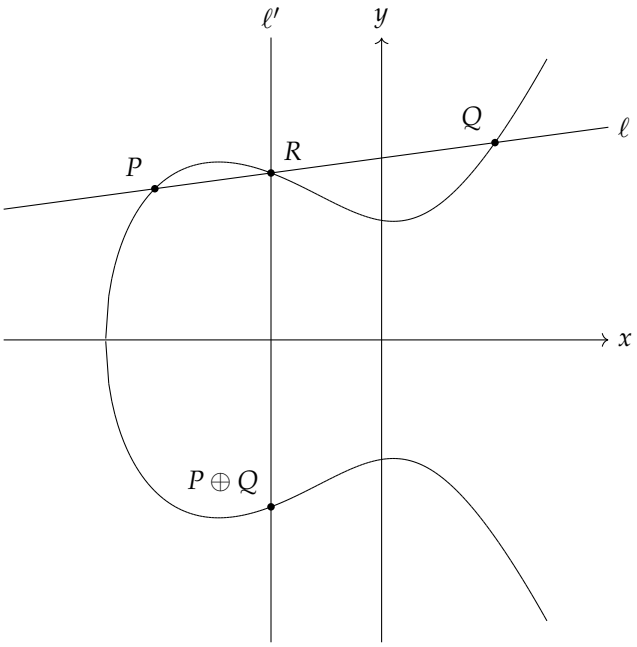
   que puede ser escrita como

$$y = \frac{y_P - y_Q}{x_P - x_Q}\,(x - x_Q) + y_Q.$$

3. Para $O = [0 : 1 : 0]$ y $P = [X_P : Y_P : Z_P] \neq 0$ se ve que la recta que pasa por $P$ y $O$ viene dada por

$$\det \begin{pmatrix} X & Y & Z \\ X_P & Y_P & Z_P \\ 0 & 1 & 0 \end{pmatrix} = \det \begin{pmatrix} X & Z \\ X_P & Z_P \end{pmatrix} = X\,Z_P - Z\,X_P = 0.$$

   El punto $O$ es el único punto de la curva que satisface $Z = 0$, así que podemos suponer que $Z_P, Z \neq 0$ y escribir la ecuación como $x = x_P$ en las coordenadas inhomogéneas. Esto significa que en el plano afín la recta misteriosa que pasa por $R$ y $O$ es nada más la recta vertical que pasa por $R$:




Entonces, si $R = (x_R, y_R)$, tenemos $P \oplus Q = (x_R, -y_R)$.

4. Se ve que $P \oplus O = P$ para todo punto de la curva elíptica $P \neq O$.

5. En general, si $C$ es una curva proyectiva definida por una ecuación homogénea $F(X, Y, Z) = 0$, entonces la recta tangente en un punto *no singular* $P = [X_P : Y_P : Z_P]$ está definida por la ecuación

$$X \frac{\partial F}{\partial X}(P) + Y \frac{\partial F}{\partial Y}(P) + Z \frac{\partial F}{\partial Z}(P) = 0.$$

Calculemos la recta tangente a la curva elíptica $F(X, Y, Z) = Y^2 Z - X^3 - A\,X\,Z^2 - B\,Z^3$ en el punto al infinito $O = [0 : 1 : 0]$. Tenemos

$$\begin{aligned}
\frac{\partial F}{\partial X}(O) &= -3\,X^2 - A\,Z^2\Big|_{X=Z=0} = 0, \\
\frac{\partial F}{\partial Y}(O) &= 2\,YZ|_{Y=1,Z=0} = 0, \\
\frac{\partial F}{\partial Z}(O) &= Y^2 - 2\,A\,X\,Z - 3\,B\,Z^2\Big|_{X=0,Y=1,Z=0} = 1.
\end{aligned}$$

Entonces, la recta tangente consiste en los puntos $[X : Y : 0]$. Es la "recta al infinito". Su intersección con la curva consiste en un punto $O$, pero es una intersección de multiplicidad 3, así que tenemos

$$O \oplus O = O.$$

6. Ahora si tenemos dos puntos diferentes de la curva $P \neq Q$, $P, Q \neq O$, podemos calcular las coordenadas de $P \oplus Q$. Ya que $P, Q \neq O$, podemos pasar a las coordenadas inhomogéneas.

Si $x_P = x_Q$, entonces $y_P = -y_Q$, la recta que pasa por $P$ y $Q$ es la recta vertical $x = x_P = x_Q$ y su tercer punto de intersección es el punto al infinito $O$ (que ya no se ve que pasamos al plano afín). En este caso $P \oplus Q = O$.

Ahora si $x_P \neq x_Q$, la ecuación de la recta que pasa por $P$ y $Q$ es

$$y = \frac{y_P - y_Q}{x_P - x_Q}\,(x - x_Q) + y_Q.$$

Para encontrar las intersecciones de esta recta con la curva $y^2 = x^3 + A\,x + B$, consideremos la ecuación

$$\left(\frac{y_P - y_Q}{x_P - x_Q}\,(x - x_Q) + y_Q\right)^2 = x^3 + A\,x + B.$$

Es una ecuación cúbica de la forma

$$x^3 + C\,x^2 + D\,x + E = 0,$$

donde

$$C = -\left(\frac{y_P - y_Q}{x_P - x_Q}\right)^2.$$

Si sus raíces son $x_P, x_Q, x_R$, tenemos

$$\begin{aligned} x^3 + C\,x^2 + D\,x + E &= (x - x_P)\,(x - x_Q)\,(x - x_R) \\ &= x^3 - (x_P + x_Q + x_R)\,x^2 + (x_P x_Q + x_P x_R + x_Q x_R)\,x - x_P\,x_Q\,x_R. \end{aligned}$$

En particular, igualando los coeficientes de $x^2$, se obtiene

$$\left(\frac{y_P - y_Q}{x_P - x_Q}\right)^2 = x_P + x_Q + x_R,$$

así que las coordenadas del tercer punto de intersección con la recta son

$$x_R = \left(\frac{y_P - y_Q}{x_P - x_Q}\right)^2 - x_P - x_Q, \quad y_R = \frac{y_P - y_Q}{x_P - x_Q}\,(x_R - x_Q) + y_Q.$$

Note que puede suceder que $(x_R, y_R) = (x_P, y_P)$ o $(x_R, y_R) = (x_Q, y_Q)$. Esto significa que la recta es tangente a la curva en el punto $R$.

Las coordenadas de $P \oplus Q$ vienen dadas por $(x_R, -y_R)$.

7. Si $Q = P$, entonces $P \oplus P$ se calcula a partir de la tangente que pasa por $P$. Ya hemos analizado el caso de $O \oplus O$ y ahora supongamos que $P \neq O$. Podemos pasar a las coordenadas inhomogéneas y la ecuación $f(x, y) = y^2 - x^3 - A\,x - B$. En este caso la ecuación de la tangente en $(x_P, y_P)$ es

$$\frac{\partial f}{\partial x}(P)\,(x - x_P) + \frac{\partial f}{\partial y}(P)\,(y - y_P) = 0.$$

Tenemos

$$\frac{\partial f}{\partial x}(P) = -3\,x_P^2 - A, \quad \frac{\partial f}{\partial y}(P)\,(y - y_P) = 2\,y_P.$$

Entonces, la tangente viene dada por

$$(-3\,x_P^2 - A)\,(x - x_P) + 2\,y_P\,(y - y_P) = 0.$$

Si $y_P = 0$, entonces $\partial f/\partial y(P) = 0$. Sin embargo, esto implica que $\partial f/\partial x(P) \neq 0$, puesto que el punto $P$ no es singular. Así que la tangente es la recta vertical $x = x_P$ que interseca la curva... en el punto $O$ que hemos olvidado. En este caso $P \oplus P = O$.

Supongamos ahora que $y_P \neq 0$. En este caso la ecuación de la tangente puede ser escrita como

$$y = \frac{3\,x_P^2 + A}{2\,y_P}\,(x - x_P) + y_P.$$

Otra vez podemos sustituir $y$ en $y^2 = x^3 + A\,x + B$ y considerar

$$\left(\frac{3\,x_P^2 + A}{2\,y_P}\,(x - x_P) + y_P\right)^2 = x^3 + A\,x + B.$$

Esto es una ecuación cúbica de la forma

$$x^3 + C\,x^2 + D\,x + E = 0,$$

donde

$$C = -\frac{(3\,x_P^2 + A)^2}{4\,y_P^2}.$$

Luego, sabemos que el polinomio cúbico de arriba tiene como su raíz $x = x_P$ de multiplicidad 2 y alguna otra raíz $x = x_R$. Entonces, analizando la ecuación

$$x^3 + C\,x^2 + D\,x + E = (x - x_P)^2\,(x - x_R),$$

vemos que el coeficiente de $x^2$ en la parte izquierda es $-2\,x_P - x_R$, así que

$$2\,x_P + x_R = \frac{(3\,x_P^2 + A)^2}{4\,y_P^2},$$

de donde

$$x_R = \frac{(3\,x_P^2 + A)^2}{4\,y_P^2} - 2\,x_P, \quad y_R = \frac{3\,x_P^2 + A}{2\,y_P}\,(x_R - x_P) + y_P$$

(como siempre en esta serie de exposiciones, se supone que $\operatorname{char} k \neq 2$). Puede suceder que $(x_R, y_R) = (x_P, y_P)$, y en este caso la recta tangente tiene multiplicidad 3 con la curva, así que $P$ es un **punto de inflexión**. En general, un punto de inflexión es un punto donde esta multiplicidad es $\geq 3$, y para una curva afín $f(x, y) = 0$ un punto de la curva $P$ será un punto de inflexión si y solamente si

$$\det \begin{pmatrix} \dfrac{\partial^2 f}{\partial x \partial x} & \dfrac{\partial^2 f}{\partial x \partial y} & \dfrac{\partial f}{\partial x} \\ \dfrac{\partial^2 f}{\partial x \partial y} & \dfrac{\partial^2 f}{\partial y \partial y} & \dfrac{\partial f}{\partial y} \\ \dfrac{\partial f}{\partial x} & \dfrac{\partial f}{\partial y} & 0 \end{pmatrix} (P) = 0.$$

Por ejemplo, el punto al infinito $O$ es un punto de flexión de cualquier curva elíptica

$$Y^2 Z = X^3 + AXZ^2 + BZ^3;$$

lo vimos demostrando que $O \oplus O = O$.

Las coordenadas de $P \oplus P$ vienen dadas por $(x_R, -y_R)$.

¡Uf! Esto cubre todos los casos posibles y nos da ciertas fórmulas explícitas.

**Teorema.** *$E(K)$ es un grupo abeliano respecto a la operación $\oplus$.*

*Demostración.* Si $P, Q \in E(K)$, entonces $P \oplus Q \in E(K)$. Por ejemplo, esto puede ser comprobado por las fórmulas explícitas que obtuvimos arriba (las coordenadas de $P \oplus Q$ se expresan mediante las operaciones básicas $+, -, \times, /$ aplicadas a $x_P, y_P, x_Q, y_Q$).

Hemos visto que $P \oplus O = O$ para todo $P \in E(K)$, así que $O$ es el elemento neutro. Luego, para todo punto $P$ existe su inverso: si $P = [X : Y : Z]$, entonces $-P = [X : -Y : Z]$. Está claro que $P \oplus Q = Q \oplus P$.

La única propiedad que no está clara es la asociatividad:

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R) \quad \text{para cualesquiera } P, Q, R \in E(K).$$

En teoría, podríamos hacer cálculos explícitos con las fórmulas de arriba, pero esto no sería muy instructivo. Existe una prueba más inteligente basada en el teorema de Riemann–Roch; véase [Sil2009, Proposition III.3.4]. ■

# 5 Ejemplos y cálculos en PARI/GP

Ciertos cálculos con curvas elípticas se pueden hacer en el programa PARI/GP que el lector puede descargar de la página http://pari.math.u-bordeaux.fr/. Para definir una curva elíptica

$$y^2 = x^3 + A\,x + B,$$

podemos escribir

```
E = ellinit ([A,B]);
```

En general, para definir una curva elíptica en la forma

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

hay que escribir

```
E = ellinit ([a1,a2,a3,a4,a6]);
```

- La función `elladd (E,[xP,yP],[xQ,yQ])` calcula la suma $(x_P, y_P) \oplus (x_Q, y_Q)$.
- La función `ellmul (E,[x,y],n)` calcula $\underbrace{P \oplus \cdots \oplus P}_{n}$ para el punto de la curva $P = (x, y)$.

**Ejemplo.** Consideremos la curva

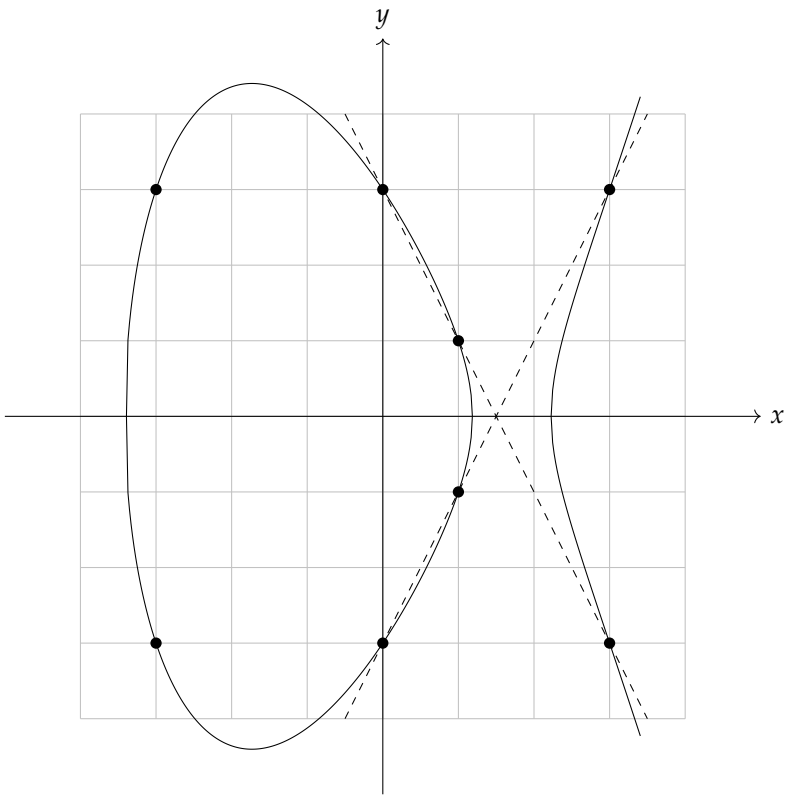
$$y^2 = x^3 - 9x + 9.$$

Tenemos $(0, -3) \oplus (3, 3) = (1, 1)$.

```
? E = ellinit([-9,9]);
? elladd(E,[0,-3],[3,3])
% = [1, 1]
```

El punto $P = (3, 3)$ es de orden 3.

```
? P = [3,3];
? ellmul (E,P,2)
% = [3, -3]
? ellmul (E,P,3)
% = [0]
```




curva elíptica $y^2 = x^3 - 9\,x + 9$

De hecho, $(3, \pm 3)$ es un punto de inflexión. Tenemos otro punto entero parecido $Q = (-3, 3)$. Primero se ve que $Q \oplus Q$ nos da otro punto entero menos evidente $(15, -57)$.

```
? Q = [-3,3];
? ellmul (E,Q,2)
% = [15, -57]
```

Si seguimos calculando los múltiplos $n\,P$, se ve que este punto tiene orden infinito.

```
? ellmul (E,Q,3)
% = [-8/9, 109/27]
? ellmul (E,Q,4)
```

```
% = [1491/361, -44601/6859]
? ellmul (E,Q,5)
% = [13209/20449, 5436183/2924207]
? ellmul (E,Q,6)
% = [1048753/427716, -361921823/279726264]
? ellmul (E,Q,7)
% = [310669305/265918249, 1226474628261/4336328886443]
```

▲

**Ejemplo.** Consideremos la curva

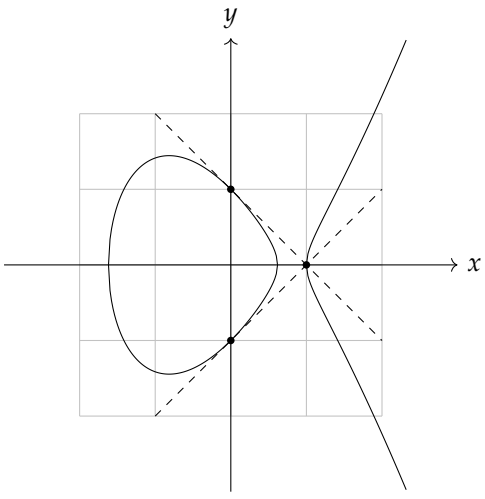
$$y^2 = x^3 - 2x + 1$$

y su punto $P = (0,1)$. Calculemos los múltiplos de $P$.

```
? E = ellinit ([-2,1]);
? P = [0,1];
? ellmul (E,P,2)
% = [1, 0]
? ellmul (E,P,3)
% = [0, -1]
? ellmul (E,P,4)
% = [0]
```

Entonces,

$$P \oplus P = (1,0), \quad P \oplus P \oplus P = (0,-1), \quad P \oplus P \oplus P \oplus P = O.$$




curva elíptica $y^2 = x^3 - 2x + 1$

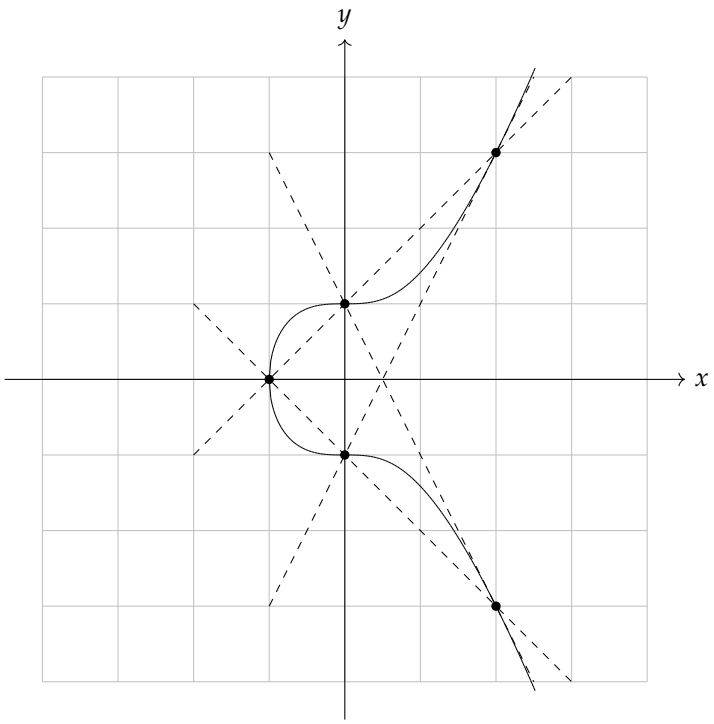
▲

**Ejemplo.** Para la curva $y^2 = x^3 + 1$ podemos calcular que el punto $(2,3)$ es de orden 6:

$$2 \cdot (2,3) = (0,1), \quad 3 \cdot (2,3) = (-1,0), \quad 4 \cdot (2,3) = (0,-1), \quad 5 \cdot (2,3) = (2,-3), \quad 6 \cdot (2,3) = 0.$$

```
? E = ellinit ([0,1]);
? ellmul(E,[2,3],2)
% = [0, 1]
? ellmul(E,[2,3],3)
% = [-1, 0]
? ellmul(E,[2,3],4)
% = [0, -1]
? ellmul(E,[2,3],5)
% = [2, -3]
? ellmul(E,[2,3],6)
% = [0]
```

Todo esto se ve del dibujo de abajo. Note que $(0, \pm 1)$ son puntos de inflexión: en estos puntos la tangente tiene intersección de multiplicidad 3 con la curva.




curva elíptica $y^2 = x^3 + 1$

▲

*Continuará...*

## Referencias

[Sil2009] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094
https://doi.org/10.1007/978-0-387-09494-6