Álgebra Aplicada y Computacional

Juan Rojo Carulli, Alfonso Zamora Saiz

ETSI Informáticos
Universidad Politécnica de Madrid

Optativa del octavo semestre
GMI Curso 2022-23

Variedades.

Sea $\mathbb{K}$ un cuerpo, que puede ser $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, o un cuerpo finito $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$.

Los conjuntos de soluciones en el espacio afín $\mathbb{K}^n$ de sistemas de ecuaciones polinomiales del tipo

$$\begin{cases} f_1(x_1, \ldots, x_n) &= 0 \\ \vdots & \vdots \\ f_m(x_1, \ldots, x_n) &= 0 \end{cases}$$

se llaman **variedades afines**. Tienen un análogo en el espacio proyectivo $\mathbb{P}(\mathbb{K}^{n+1}) = \mathbb{P}^n_{\mathbb{K}}$, llamadas **variedades proyectivas**.

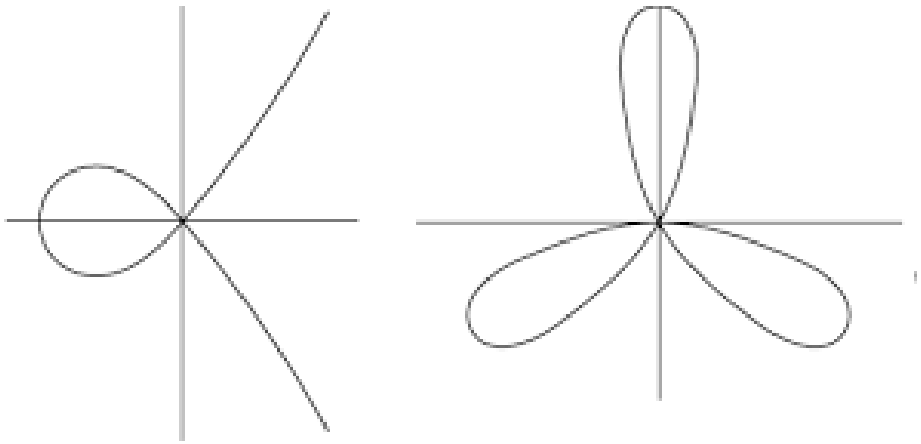
Las propiedades álgebro-geométricas de las variedades constituyen uno de los temas centrales de las matemáticas, de cuyo estudio se encarga la **Geometría Algebraica**.

Variedades de dimensión uno: curvas.

Una curva (algebraica) afín en $\mathbb{K}^2$ es el conjunto de soluciones $(x, y) \in \mathbb{K}^2$ de una ecuación polinomial de dos variables $f(X, Y) = 0$.

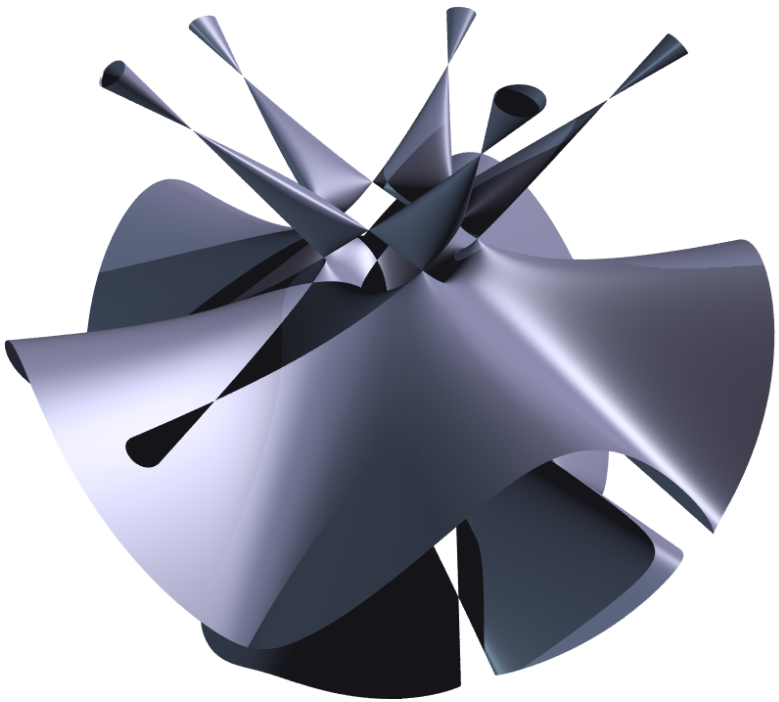
Una curva algebraica proyectiva es el conjunto de soluciones $[x_0 : x_1 : x_2] \in \mathbb{P}^2_{\mathbb{K}}$ de una ecuación polinomial *homogénea* $F(X_0, X_1, X_2) = 0$.

Las curvas algebraicas son un ejemplo paradigmático a la par que abarcable dentro del área de la geometría algebraica.

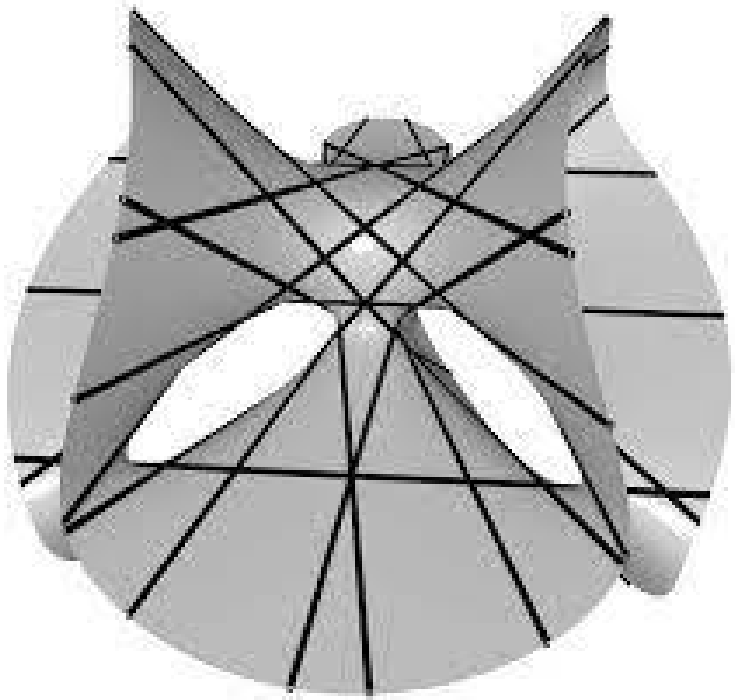


$D = Y^2 - X^3 - X^2$ $E = (X^2 + Y^2)^2 + 3X^2Y - Y^3$

Si el cuerpo es $\mathbb{K} = \mathbb{C}$, las curvas algebraicas de $\mathbb{C}^2$ definen superficies reales, que se pueden proyectar a $\mathbb{R}^3$ y representar gráficamente:



(A) Quíntica.



(B) Cúbica.

FIGURA: Curvas complejas de grado 5 y 3.

Sistemas de ecuaciones polinomiales.

Algunas aplicaciones:

Sabemos resolver sistemas de ecuaciones lineales:

$$\begin{cases} a_{11}x_1 & + & \cdots & + & a_{1n}x_n & + & b_1 & = & 0 \\ \vdots & & & & & & \vdots & \vdots & = & \vdots \\ a_{m1}x_1 & + & \cdots & + & a_{mn}x_n & + & b_m & = & 0 \end{cases}$$

mediante el método de Gauss. Sin embargo, ¿cómo resolvemos **sistemas de ecuaciones polinomiales**?

$$\begin{cases} f_1(x_1,\ldots,x_n) & = & 0 \\ \vdots & & \vdots \\ f_m(x_1,\ldots,x_n) & = & 0 \end{cases}$$

Sistemas de ecuaciones polinomiales

Por ejemplo, ¿cómo resolver el siguiente sistema?

$$\begin{cases} 0 = f_1(x,y,z) = x^2 + 2xy - y^3 + 4zy \\ 0 = f_2(x,y,z) = x + 3x^2 - 5yx^2 - z \\ 0 = f_3(x,y,z) = x^3 + 6xz - 3yz^3 \end{cases}$$

¿Podemos encontrar una parametrización de la variedad afín dada por su conjunto de soluciones?

Idea: Podemos identificar la variedad afín con el ideal $\langle f_1, f_2, f_3 \rangle$, e intentar hallar otra base del ideal que sea más sencilla.

Esto nos llevará al concepto de **base de Gröbner** de un ideal $\langle f_1, \ldots f_m \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$, que será otro conjunto de generadores $g_1, \ldots, g_l$ del ideal con el que sí podremos parametrizar la variedad y resolver el sistema.

Usaremos el **algoritmo de Buchberger** para calcular estas bases.

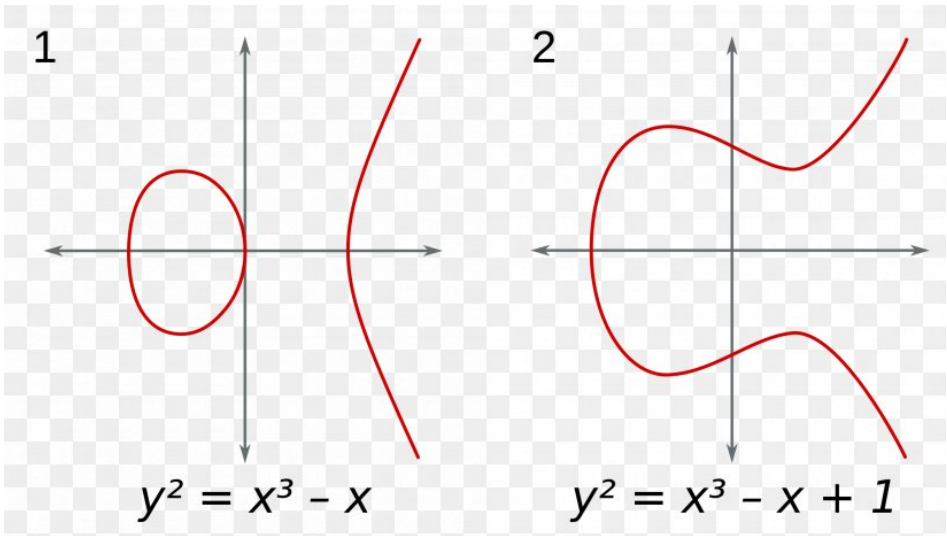
Curvas Elípticas

Una **curva elíptica** sobre un cuerpo $\mathbb{K}$ viene dada por el conjunto de soluciones $(x, y) \in \mathbb{K}^2$ de una ecuación del tipo

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

con $A, B \in \mathbb{K}$ los coeficientes de la curva.

Las curvas elípticas son un caso particular de curvas algebraicas. En concreto, son curvas algebraicas de grado 3 sin puntos singulares, también llamadas *cúbicas lisas*.



Curvas Elípticas

Lo que hace especiales a las curvas elípticas es el hecho de que el conjunto de sus soluciones (junto con el punto de infinito) tiene una estructura natural de **grupo conmutativo**. Es decir, se puede definir una *suma* en dicho conjunto de soluciones.

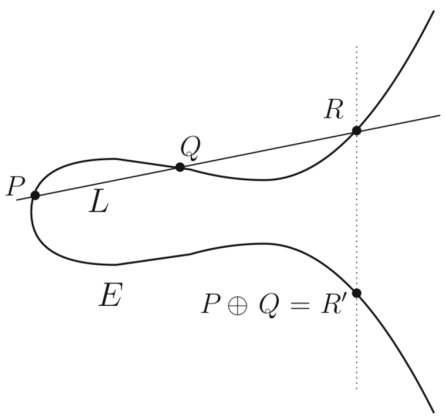
Esta estructura de grupo es especialmente interesante desde el punto de vista de la computación, y tiene numerosas aplicaciones en teoría de números y en criptografía. A partir de ella se obtienen:

- Algoritmos de factorización de enteros.
- Tests de primalidad.
- Métodos de encriptación (Elliptic Curve Cryptography).

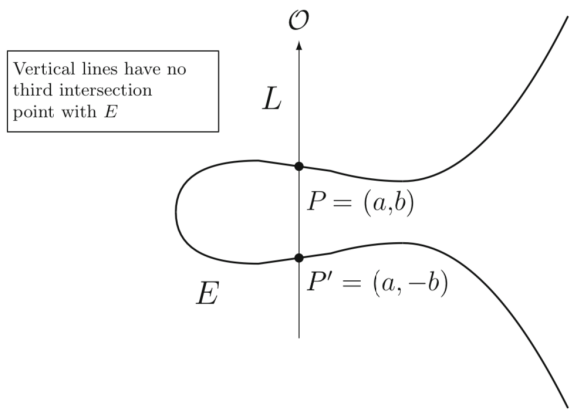
Podemos visualizar geométricamente la operación de grupo en una curva elíptica como sigue.

Dados P, Q dos puntos en la curva elíptica E, su suma $P \oplus Q = R'$ se obtiene como el punto simétrico de R, el tercer punto de intersección de la recta $L = PQ$ con la curva.

Si los puntos P, P' están en una vertical, su suma es el punto del infinito de la curva. Esto muestra que es necesario trabajar en el plano proyectivo $\mathbb{P}^2_{\mathbb{K}}$.



(A) Suma de puntos, caso general.



(B) Suma de puntos en una vertical.

Los algoritmos de encriptación que usan curvas elípticas siguen una estructura sencilla. Por ejemplo, siguiente esquema lo pueden usar Alice y Bob para construir una clave secreta (que sólo conozcan ellos):

Public parameter creation	
A trusted party chooses and publishes a (large) prime p, an elliptic curve E over $\mathbb{F}_p$, and a point P in $E(\mathbb{F}_p)$.	
Private computations	
Alice	**Bob**
Chooses a secret integer n_A. Computes the point $Q_A = n_A P$.	Chooses a secret integer n_B. Computes the point $Q_B = n_B P$.
Public exchange of values	
Alice sends Q_A to Bob $\longrightarrow$	Q_A
Q_B $\longleftarrow$	Bob sends Q_B to Alice
Further private computations	
Alice	**Bob**
Computes the point $n_A Q_B$.	Computes the point $n_B Q_A$.
The shared secret value is $n_A Q_B = n_A(n_B P) = n_B(n_A P) = n_B Q_A$.	

El siguiente esquema lo pueden usar Alice y Bob para intercambiar un mensaje privado:

Public parameter creation	
A trusted party chooses and publishes a (large) prime p, an elliptic curve E over $\mathbb{F}_p$, and a point P in $E(\mathbb{F}_p)$.	
Alice	**Bob**
Key creation	
Choose a private key n_A. Compute $Q_A = n_A P$ in $E(\mathbb{F}_p)$. Publish the public key Q_A.	
Encryption	
	Choose plaintext $M \in E(\mathbb{F}_p)$. Choose a random element k. Use Alice's public key Q_A to compute $C_1 = kP \in E(\mathbb{F}_p)$. and $C_2 = M + kQ_A \in E(\mathbb{F}_p)$. Send ciphertext (C_1, C_2) to Alice.
Decryption	
Compute $C_2 - n_A C_1 \in E(\mathbb{F}_p)$. This quantity is equal to M.	

Lo que hace que la criptografía con curvas elípticas funcione es la alta complejidad computacional de la operación *suma de puntos* en dichas curvas.

Esto da lugar al llamado **problema del logaritmo discreto** (PLD) en una curva elíptica:

Si conocemos los puntos $Q = nP$ y P de la curva elíptica $E(\mathbb{F}_p)$, ¿podemos recuperar el número n?

A este número n se le llama *logaritmo (discreto) de Q en base P*.

Como veremos, los mejores algoritmos conocidos para resolver el PLD en una curva elíptica son equivalentes al algoritmo de *fuerza bruta* y requieren $O(\sqrt{p})$ pasos, por lo que son muy ineficientes.

Por ejemplo, la empresa *Certicom* ha propuesto varios desafíos para descifrar la clave privada de un sistema de encriptación con curvas elípticas.

La mayoría siguen abiertos a día de hoy. Consúltese *The Certicom ECC Challenge*.

Contenidos de la asignatura:

Tema 1: Variedades afines y proyectivas

- Anillos de polinomios e ideales. Homogeneización de polinomios.
- Completada proyectiva de una variedad afín.
- Correspondencia entre variedades e ideales.
- Bases de Gröbner y teorema de la base de Hilbert.

Tema 2: Propiedades y aplicaciones de las bases de Gröbner.

- Algoritmo de Buchberger para la construcción de bases de Gröbner.
- Algoritmo de división asociado a una base de Gröbner.
- El problema de pertenencia a un ideal.
- Eliminación de variables.
- Resolución de sistemas de ecuaciones polinomiales.

Tema 3. Curvas algebraicas afines y proyectivas.

- Parametrizaciones de curvas.
- Puntos singulares y regulares.
- Intersección de curvas y Teorema de Bézout.
- El género de una curva.

Tema 4. Curvas elípticas.

- Ecuación de Weirstrass de una curva elíptica.
- Estructura de grupo conmutativo.
- Algoritmos para la suma de puntos.
- El género de una curva.

Tema 5. Curvas elípticas sobre cuerpos finitos.

- Acotación del número de puntos. Teorema de Hasse.
- Cálculo del número de puntos. Algoritmo de Schoof.
- Algoritmo de Lenstra para la factorización de números enteros.
- Tests de primalidad basados en curvas elípticas. Algoritmo de Atkin-Morain.
- El problema del logaritmo discreto.
- Aplicaciones criptográficas.

Evaluación:

Sistema de evaluación continua: entrega de prácticas (8/10) y presentación oral de prácticas (2/10).

Sistema de evaluación por prueba final: realización de prueba escrita (10/10). Sólo para quien solicite no participar en la evaluación continua.

Bibliografía:

- *Ideals, Varieties and Algorithms*, David A. Cox, John Little, Donal O'Shea. Springer, 2015.
- *An Introduction to Gröbner Bases*, William W. Adams, Philippe Loustaunau. AMS, 1994.
- *Algebraic Curves*, William Fulton, W.A. Benjamin, Inc, 1969.
- *The Arithmetic of Elliptic Curves*, Joseph H. Silverman. Springer, 2nd edition 2008.
- *An introduction to Mathematical Cryptography*, Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. Springer, 2010.