Capítulo 1

Aritmética en curvas elípticas

Dado un cuerpo $\mathbb{K}$ consideramos una ecuación

$$y^2 + uxy + vy = x^3 + ax^2 + bx + c$$

(llamada ecuación de Weirestrass), donde u, v, a, b, c son coeficientes dados en $\mathbb{K}$.

El conjunto de los puntos $(x, y) \in \mathbb{K}^2$ que verifican esta ecuación junto con un elemento extra, que denotaremos por Ø y al que llamaremos *punto del infinito*, forman una **curva elíptica** sobre $\mathbb{K}$.

En lo que sigue consideraremos que $\mathbb{K}$ es un cuerpo finito de la forma $\mathbb{Z}_p$ con p primo y $p \neq 2, 3$.

En esta situación la ecuación general anterior puede transformarse para que adopte una forma simplificada:

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

Una curva eliptica estará entonces determinada conociendo el primo p y los coeficientes de la curva $a, b \in \mathbb{Z}_p$ (deben cumplir $\Delta = 4a^3 + 27b^2 \neq 0$).

Ejemplo:

Consideremos $\mathbb{K} = \mathbb{Z}_5$ *y la ecuación* $y^2 = x^3 + 2x + 1$. *Para comprobar que el punto* $(1, 3)$ *está en la curva calculamos*

$$\begin{aligned} y^2 &= 3^2 = 4 \\ x^3 + 2x + 1 &= 1^3 + 2 \cdot 1 + 1 = 4 \end{aligned}$$

y como ambos miembros de la ecuación resultan ser iguales al sustituir $x = 1, y = 3$*, entonces el punto está en la curva.*

Por el contrario, el punto $(2, 2)$ *no pertenece a la curva:*

$$\begin{aligned} x^3 + 2x + 3 &= 2^3 + 4 + 1 = 3 \\ y^2 &= 4 \end{aligned}$$

puesto que la igualdad no se cumple.

En este ejemplo es fácil calcular qué puntos están en la curva, además del punto del infinito. Para ello podemos hacer dos tablas (que escribimos juntas por economía de espacio) en la que calculamos cada uno de los miembros de la ecuación para todos los elementos del cuerpo:

y	y^2		x^3+2x+1	x
0	0		1	0
1	1		4	1
2	4		3	2
3	4		4	3
4	1		3	4

Ahora comparamos los resultados de calcular el primer miembro de la ecuación y el del segundo y obtenemos que están en la curva los puntos:

$$(0,1),(0,4),(1,2),(1,3),(3,2),(3,3)$$

con lo que en total nuestra curva elíptica tiene 7 puntos (incluyendo al punto del infinito).

En general el problema de determinar el número de puntos de una curva elíptica está fuera de nuestras pretensiones, pero puede consultarse el algoritmo de Schoof (por ejemplo en la wikipedia, en inglés).

Existe un resultado, llamado Teorema de Hasse, que da una cota en función del número de elementos del cuerpo finito:

Sea N el número de puntos de una curva elíptica sobre el cuerpo finito con q elementos. Entonces

$$|N-(q+1)| \leq 2\sqrt{q}$$

1.1. Geometría de una curva elíptica

El aspecto de una curva elíptica sobre los reales podría ser el del siguiente dibujo:

El punto del infinito puede interpretarse como el punto en que se cortan todas las rectas verticales. Entonces una recta contiene al punto del infinito exactamente cuando es una recta vertical.

La propiedad geométrica que nos va a permitir definir una operación suma entre los puntos de una curva elíptica es la siguiente:

Dada una recta que corta a la curva en dos puntos (o es tangente a la curva en un punto), entonces existe otro punto en común de la recta y la curva.

En un dibujo podemos ver la primera posibilidad:

Si ahora consideramos una recta vertical entonces corta a la curva elíptica en el punto del infinito. Esta recta puede cortar a la curva en otro punto más, en cuyo caso o es tangente a la curva en ese punto (y entonces se considera un punto de corte doble), o bien la corta en un tercer punto, siguiendo el resultado general.

1.2. Aritmética en una curva elíptica

Para definir la suma de dos puntos distintos de la curva P y Q observemos el dibujo:

El procedimiento geométrico consiste en:

› Trazar la recta que pasa por P y Q.

› Determinar el tercer punto de corte $-R$.

› Trazar la recta vertical que pasa por $-R$.

› Tomar el otro punto donde la recta vertical corta a la curva y entonces $R = P + Q$.

Si P es un punto de la curva también podemos calcular $P + P = 2P$, trazando la recta tangente a la curva en P y siguiendo el mismo procedimiento anterior:

No olvidemos que el punto del infinito Ø también es un punto de la curva, por tanto también es necesario definir la suma con Ø de cualquier punto de la curva. El punto del infinito representa al punto donde se cortan todas las rectas verticales, por tanto toda recta vertical que corte a la curva en un cierto punto $P = (x, y)$, como también la corta en el punto del infinito Ø, contiene un tercer punto. Pero es inmediato comprobar que ese tercer punto debe ser el de coordenadas $(x, -y)$. El procedimiento geométrico anterior nos lleva entonces a obtener:

$$Ø + P = P$$

con lo que el punto del infinito es un neutro para la suma. Además si $P = (x, y)$ es un punto de la curva, su opuesto respecto de esta suma es $-P = (x, -y)$.

Veamos ahora cómo efectuar la suma de dos puntos usando sus coordenadas.
La ecuación de la curva elíptica es

$$y^2 = x^3 + ax + b \tag{1.1}$$

Si $P = (x_1, y_1)$**,** $Q = (x_2, y_2)$ **son distintos pero** $x_1 = x_2$ entonces están sobre la misma recta vertical y su suma es el punto del infinito Ø, es decir $Q = -P$.

Si $x_1 \neq x_2$ entonces la recta que contiene a P y Q tiene ecuación

$$y - y_1 = \lambda(x - x_1) \tag{1.2}$$

donde λ es la pendiente de la recta, es decir

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \tag{1.3}$$

El punto que buscamos $P + Q = (x_3, y_3)$ tiene opuesto $(x_3, -y_3)$, que está en la curva elíptica y también en la recta anterior, así que si podemos calcular x_3 podemos despejar en la ecuación 1.2 y obtendremos

$$-y_3 = \lambda(x_3 - x_1) + y_1 \tag{1.4}$$

Ahora nos queda determinar x_3. Para ello calculamos la intersección entre la curva 1.1 y la recta 1.2 sustituyendo el valor de y en la ecuación de la curva

$$(\lambda(x - x_1) + y_1)^2 - x^3 - ax - b = 0$$

Ahora, sabemos que x_1, x_2, x_3 son tres soluciones de la ecuación anterior, es decir, la ecuación anterior puede escribirse también como

$$(x - x_1)(x - x_2)(x - x_3) = 0$$

y como los coeficientes de grado 2 en x deben coincidir, desarrollando e igualando los coeficientes obtenemos

$$-\lambda^2 = -x_1 - x_2 - x_3$$

que nos permite despejar el valor de x_3:

$$x_3 = \lambda^2 - x_1 - x_2 \tag{1.5}$$

Recopilamos entonces las ecuaciones 1.5, 1.4:

$$\boxed{\begin{array}{l} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \\ \lambda = \frac{y_2 - y_1}{x_2 - x_1} \end{array}}$$

Si $P = Q$ **y** $y_1 \neq 0$ entonces debemos calcular la recta tangente a la curva en P. La pendiente de la curva es la derivada de y en el punto P. Podemos calcularla a partir de la ecuación 1.1

$$2y\dot{y}' = 3x^2 + a$$

y tenemos que en el punto $P = (x_1, y_1)$ es $\lambda = \frac{3x_1^2 + a}{2y_1}$

Las fórmulas del caso anterior pueden usarse sustituyendo el nuevo valor de λ y que $x_2 = x_1$:

$$\boxed{\begin{array}{l} x_3 = \lambda^2 - 2x_1 \\ y_3 = \lambda(x_1 - x_3) - y_1 \\ \lambda = \frac{3x_1^2 + a}{2y_1} \end{array}}$$

Si $P = Q = (x_1, 0)$ entonces la tangente a la curva en el punto P es una recta vertical, puesto que la curva es simétrica respecto del eje horizontal, así que el otro punto donde la recta corta a la curva es el punto del infinito y por tanto $P + P = \emptyset$.

Ejemplo

Calculemos en la curva del ejemplo $y^2 = x^3 + 2x + 1$ en $\mathbb{Z}_5$ la suma en cada uno de los casos anteriores:

$P = (1, 2); Q = (1, 3)$ entonces P y Q están sobre la misma recta vertical y por tanto $P + Q = \emptyset$.

$P = (0, 1); Q = (1, 2)$ Usamos las fórmulas del caso correspondiente y realizamos las operaciones en $\mathbb{Z}_5$:

$$\begin{array}{l} \lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{2-1}{1-0} = 1 \\ x_3 = \lambda^2 - x_1 - x_2 = 1^2 - 0 - 1 = 1 - 0 - 1 = 0 \\ y_3 = \lambda(x_1 - x_3) - y_1 = 1(0 - 0) - 1 = 0 - 1 = 4 \end{array}$$

luego $P + Q = (0, 4)$

$P = (0, 1) = Q$ Calculamos 2P usando las fórmulas del caso y sustituyendo

$$\begin{array}{l} \lambda = \frac{3x_1^2 + a}{2y_1} = \frac{3 \cdot (0)^2 + 2}{2 \cdot 1} = 1 \\ x_3 = \lambda^2 - 2x_1 = 1^2 - 2 \cdot 0 = 1 \\ y_3 = \lambda(x_1 - x_3) - y_1 = 1(0 - 1) - 1 = 3 \end{array}$$

luego $2P = (1, 3)$.

Cuadro 1.1: Tabla de sumar en la curva elíptica $y^2 = x^3 + 2x + 1$ en $\mathbb{Z}_5$

$+$	$\emptyset$	$(0,1)$	$(0,4)$	$(1,2)$	$(1,3)$	$(3,2)$	$(3,3)$
$\emptyset$	$\emptyset$	$(0,1)$	$(0,4)$	$(1,2)$	$(1,3)$	$(3,2)$	$(3,3)$
$(0,1)$	$(0,1)$	$(1,3)$	$\emptyset$	$(0,4)$	$(3,3)$	$(1,2)$	$(3,2)$
$(0,4)$	$(0,4)$	$\emptyset$	$(1,2)$	$(3,2)$	$(0,1)$	$(3,3)$	$(1,3)$
$(1,2)$	$(1,2)$	$(0,4)$	$(3,2)$	$(3,3)$	$\emptyset$	$(1,3)$	$(0,1)$
$(1,3)$	$(1,3)$	$(3,3)$	$(0,1)$	$\emptyset$	$(3,2)$	$(0,4)$	$(1,2)$
$(3,2)$	$(3,2)$	$(1,2)$	$(3,3)$	$(1,3)$	$(0,4)$	$(0,1)$	$\emptyset$
$(3,3)$	$(3,3)$	$(3,2)$	$(1,3)$	$(0,1)$	$(1,2)$	$\emptyset$	$(0,4)$