El Teorema de Hasse para curvas elípticas

Nicolás Vilches

Viernes 03 de Mayo, 2019

1. Curvas elípticas

Uno de los objetos más estudiados y divertidos son las *curvas elípticas*. Hay muchos enfoques para estudiarlos, y por ello muchas maneras de entenderlos; a priori, no es obvio que los objetos $\mathbb{C}/\mathbb{Z}^2$ y $\left\{(x,y) \in \mathbb{C}^2 \,\middle|\, y^2 = x^3 - x\right\} \cup \{\infty\}$ representen a "algo similar", o que tengan algún tipo de relación.

Informalmente, para nosotros una *curva elíptica* sobre un cuerpo k (con $\mathrm{char}(k) \neq 2, 3$) será una curva en k^2 descrito por una ecuación $y^2 = x^3 + ax + b$, donde $a, b \in k$ y $x^3 + ax + b$ sin raíces repetidas. Escribiremos, si K/k es una extensión,

$$E(K) = \left\{(x,y) \in K^2 \,\middle|\, y^2 = x^3 + ax + b\right\} \cup \{\infty\};$$

o, de otra manera, $E(K)$ son los puntos K-racionales de la curva. Observemos además que a la componente *afín* de la curva estamos adicionando un punto extra al infinito.

Observación. Estamos obviando el caso $\mathrm{char}(k) = 2, 3$ a propósito. La definición precisa de curva elíptica es algo así como "curva algebraica proyectiva de género 1", que a priori no prohibe tener característica 2 o 3. No obstante, para poder escribir la curva con una ecuación así de compacta (un tipo de *forma de Weierstrass* para la curva) necesitamos característica distinta de 2 y 3.

Las curvas elípticas vienen dotadas de una *operación de grupo*. Desde nuestro punto de vista, tiene una descripción muy geométrica: si queremos sumar P y Q en la curva, los unimos con una recta, que debe cortar a la curva en un tercer punto, que llamaremos R. Reflejamos R con respecto al eje y, obteniendo otro punto sobre la curva, $P + Q$.

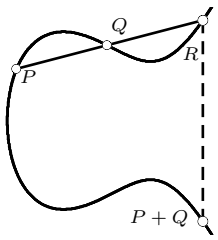

Figura 1: Sumando P y Q

Esto en el caso general funciona perfecto. Hay algunos casos que requieren más detalle (por ejemplo, ¿qué significa sumar un punto consigo mismo?), pero esta es la idea general. En otras representaciones de una curva elíptica ésta puede verse de manera más explícita (por ejemplo, la suma en $\mathbb{C}/\mathbb{Z}^2$ no es más que la operación de grupo cociente). No ahondaremos en más detalles con respecto a los detalles formales de ser curva elíptica, salvo mencionar que la suma puede escribirse de manera explícita en general (como una *función racional* sobre la curva).

2. Curvas elípticas en cuerpos finitos

El día de hoy nos focalizaremos en estudiar curvas elípticas sobre cuerpos finitos. Fijaremos $a, b \in \mathbb{F}_p$, de modo que $4a^3 - 27b^2 \neq 0$, y estudiaremos

$$E = \{y^2 = x^3 + ax + b\} \cup \{\infty\};$$

donde, a priori, los puntos de E viven en la clausura algebraica de $\mathbb{F}_p$. Podemos ser un poco menos ambiciosos y considerar sólo los puntos $\mathbb{F}_q$-racionales (con $q = p^r$). Por ejemplo, si consideramos

$$E = \{y^2 = x^3 - x + 1\} \cup \{\infty\}$$

sobre $\mathbb{F}_5$, podemos evaluar en todos los puntos para ver cuáles pertenecen. Haciendo las cuentas,

$$E(\mathbb{F}_5) = \{(0,1), (0,4), (1,1), (1,4), (3,0), (4,1), (4,4), \infty\}.$$

Esto nos da una idea divertida que no podemos hacer en curvas elípticas en otros cuerpos: contar la cantidad de puntos (y siempre obtener un número finito). Acá, $\#E(\mathbb{F}_5) = 8$; en extensiones superiores ya no es tan factible hacer los cálculos a mano. Por medio de un computador esto es fácil; los valores de abajo fueron obtenidos utilizando Sage.

n	$\#E(\mathbb{F}_{5^n})$
1	8
2	32
3	104
4	640
5	3208
6	15392
7	78184
8	391608
9	1950728

Cuadro 1: Puntos $\mathbb{F}_{5^n}$-racionales

A simple vista observamos que los valores de puntos están sospechosamente cercanos a 5^n. No es complicado ver que estos valores deberían ser cercanos a 5^n, con la siguiente cota

Proposición 1. Se tiene la cota $\#E(\mathbb{F}_q) \leq 2q + 1$.

Demostración. Tenemos siempre el punto al infinito. Para el resto de puntos, si fijamos un $x_0 \in \mathbb{F}_q$, buscamos resolver $y^2 = x_0^3 + ax_0 + b$, a lo más con dos soluciones. Así, hay a lo más $2q + 1$ puntos en total. □

El argumento de arriba es correcto, pero estamos exagerando al estimar. Intuitivamente, como la mitad de los valores de $\mathbb{F}_q$ tienen raíz cuadrada en $\mathbb{F}_q$, uno espera que el número de puntos $\mathbb{F}_q$ racionales sea algo así como $q + 1$. Eso calza con las observaciones de arriba, y fue una conjetura de Emil Artin en su tesis doctoral. Este resultado fue probado por Hasse en los años 30, en la siguiente forma

Teorema 2 (Hasse)**.** Con la notación de arriba, se tiene que $|\#E(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q}$.

Al parecer no estábamos tan mal con nuestra estimación. Veamos qué tan cercanos son estos valores a la realidad; al menos, para la curva $y^2 = x^3 - x + 1$.

n	$E(\mathbb{F}_{5^n})$	5^n+1	Diferencia	$\lfloor 2\sqrt{5^r} \rfloor$
1	8	6	2	4
2	32	26	6	10
3	104	126	22	22
4	640	626	14	50
5	3208	3126	82	111
6	15392	15626	234	250
7	78184	78126	58	559
8	391608	390626	1054	1250
9	1950728	1953126	2398	2795

Cuadro 2: Cantidad de puntos versus el Teorema de Hasse

Nuestra primera meta es dar una demostración de este hecho. Esto requerirá trabajar con isogenias, junto con un resultado pequeño de formas bilineales.

3. Formas cuadráticas

Definición. Sea A un grupo abeliano. Una función $d : A \to \mathbb{R}$ es una *forma cuadrática* si cumple

(i) $d(\alpha) = d(-\alpha)$ para todo $\alpha \in A$.

(ii) El emparejamiento
$$A \times A \to \mathbb{R}, \qquad (\alpha, \beta) \mapsto d(\alpha+\beta) - d(\alpha) - d(\beta)$$
es bilineal.

Si además cumple

(iii) $d(\alpha) \geq 0$ para todo $\alpha \in A$.

(iv) $d(\alpha) = 0$ si y sólo si $\alpha = 0$,

decimos que d es una forma *positiva definida*.

Ejemplo. Si $A = \mathbb{R}^n$, tenemos un ejemplo clásico de forma cuadrática positiva definida, $d(v) = \|v\|^2$. Acá, las identidades de polarización garantizan que

$$d(v+w) - d(v) - d(w) = 2\langle v, w\rangle,$$

que es claramente bilineal.

Lo único que necesitaremos de formas bilineales es el siguiente resultado, esencialmente equivalente a la desigualdad de Cauchy-Schwarz

Lema 1. Sea A grupo abeliano, $d : A \to \mathbb{Z}$ forma cuadrática positiva definida. Se tiene entonces

$$|d(x-y) - d(x) - d(y)| \leq 2\sqrt{d(x)d(y)}, \qquad \forall x, y \in A.$$

No probaremos esto; su demostración se parece mucho a la de Cauchy-Schwarz. De hecho, tenemos la siguiente observación

Observación. Si hacemos oídos sordos al hecho que el lema exige $d(A) \subseteq \mathbb{Z}$, tenemos, para $d(v) = \|v\|^2$,

$$|d(x-y) - d(x) - d(y)| = 2\,|\langle x, y\rangle|\,.$$

Así, el lema equivale a $|\langle x, y\rangle| \leq \|x\|\,\|y\|$, la desigualdad de Cauchy-Schwarz.

4. Isogenias

Como siempre, al estudiar algún tipo de objeto estudiamos funciones que los relacionen (como homomorfismos en grupos y anillos, funciones continuas en espacios topológicos y así). En el caso de curvas elípticas se llaman isogenias.

Definición. Sean E_1, E_2 dos curvas elípticas. Una *isogenia* de E_1 a E_2 es un morfismo $\phi : E_1 \to E_2$ (como variedades algebraicas) que además es un homomorfismo de grupo.

Observación. Si $\phi : E_1 \to E_2$ es un morfismo que manda el neutro en el neutro, es un teorema que ϕ es un homomorfismo de grupos y, así, sería una isogenia según nuestra definición. De hecho, otras definiciones piden solamente esto, y ahí ser homomorfismo de grupos es un teorema más que una definición.

Ejemplo. Si E/k es una curva elíptica, el mapeo $P \mapsto 2P$ (denotado típicamente [2]) es una isogenia. Formalmente deberíamos dar una fórmula explícita para esto, pero es medio feo de escribir. Por ejemplo, si $P = (x, y)$, la coordenada x de $2P$ es

$$\frac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}.$$

Lo único importante (para nosotros) de esta fórmula explícita es que es un morfismo de variedades. En $\mathbb{C}/\mathbb{Z}^2$ es un poco más claro geométricamente

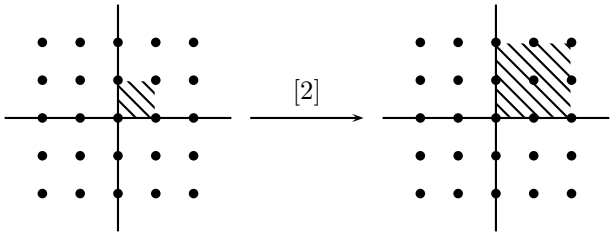

Figura 2: Isogenia [2] en $\mathbb{C}/\mathbb{Z}^2$

Ejemplo. Sea $E/\mathbb{F}_q$ curva elíptica ($q = p^r$). Definimos

$$\phi_q : E \to E, \qquad (x, y) \mapsto (x^q, y^q).$$

Eso manda E en E: si $y^2 = x^3 + ax + b$, elevando todo a q (y recordando que estamos en característica p),

$$(y^q)^2 = (x^q)^3 + ax^q + b,$$

gracias a que $a, b \in \mathbb{F}_q$. Este es un endomorfismo llamado *endomorfismo de Frobenius.*

Observación. Con el ejemplo anterior, si $(x, y) \in E$ es un punto cualquiera, tenemos que $\phi_q(x, y) = (x, y)$ si y sólo si $x^q = x, y^q = y$; esto es, $x, y \in \mathbb{F}_q$. De esta manera,

$$\{P \in E \mid \phi_q(P) = P\} = E(\mathbb{F}_q).$$

Esto será útil en la demostración del Teorema de Hasse.

Definición. Sea $\phi : E_1/K \to E_2/K$ una isogenia. Tenemos que ϕ induce un morfismo de cuerpos de funciones,

$$\phi^* : \overline{K}(E_2) \to \overline{K}(E_1)$$

de la manera obvia: si $f : E_2 \to \overline{K}$ es una función racional, $\phi^*(f) := f \circ \phi$. Definimos el *grado* de ϕ como

$$\deg(\phi) = \left[\overline{K}(E_1) : \phi^*(\overline{K}(E_2))\right].$$

Por ejemplo, $\deg(1) = 1$, y no es tan difícil ver que $\deg \phi_q = q$, donde ϕ_q es el endomorfismo de Frobenius antes descrito.

Observación. El conjunto $\hom(E_1, E_2) = \{\phi : E_1 to E_2 \text{ isogenia}\}$ es un grupo abeliano, con la suma componente a componente. Acá, el grado $\deg : \hom(E_1, E_2) \to \mathbb{Z}$ es una forma cuadrática positiva definida.

Observación. Como estamos trabajando en característica positiva, hay un riesgo al estudiar la extensión $\overline{K}(E_1)/\phi^*(\overline{K}(E_2))$, que es la aparición de extensiones inseparables. Esto produce problemas técnicos en las demostraciones. Por lo mismo, separamos el grado de la extensión en *separable* e *inseparable*, llamando a una isogenia separable si el grado inseparable es 1. Para el día de hoy, lo único importante es que la isogenia $1 - \phi_q$ es separable.

El siguiente resultado muestra por qué nos preocupamos de trabajar con isogenias separables. Esto tiene análogos con isogenias no-separables, colocando el grado separable en vez del grado usual.

Teorema 3. Sea ϕ una isogenia separable. Se tiene entonces que $\# \ker \phi = \deg \phi$.

5. Probando el Teorema de Hasse

Recordemos qué queremos demostrar.

Teorema 4 (Hasse, $\sim$1930)**.** Sea $E/\mathbb{F}_q$ una curva elíptica. Se tiene la siguente cota

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Demostración. Consideremos $\phi_q : (x, y) \mapsto (x^q, y^q)$ el endomorfismo de Frobenius. Vimos antes que $P \in E(\mathbb{F}_q)$ si y sólo si $\phi_q(P) = P$. Así,

$$E(\mathbb{F}_q) = \ker(1 - \phi_q).$$

Ahora bien, como $1 - \phi_q$ es separable,

$$\#E(\mathbb{F}_q) = \# \ker(1 - \phi_q) = \deg(1 - \phi_q).$$

Por último, como deg es una forma cuadrática positiva definida,

$$|\deg(1 - \phi_q) - \deg(1) - \deg(\phi_q)| \leq 2\sqrt{\deg(1)\deg(\phi_q)} = 2\sqrt{q},$$

o, equivalentemente,

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q},$$

probando lo pedido. □