Seminario de modularidad de representaciones de Galois (2020-1)

Héctor Pastén

Pontificia Universidad Católica de Chile

2020/04/07

Contenido de hoy:

Curvas elípticas.

- Recuerdo de conceptos básicos
- Sobre $\mathbb{C}$
- Sobre $\mathbb{Q}_p$
- Sobre $\mathbb{Q}$
- Tipos de reducción

“Recuerdo”: Curvas elípticas de varios tipos

K un campo. Una curva elíptica E sobre K es una curva suave, proyectiva definida sobre K, de género 1 y con un punto K-racional distinguido $0_E \in E(K)$. Automáticamente tiene una estructura de grupo algebraico abeliano. Algunos ejemplos:

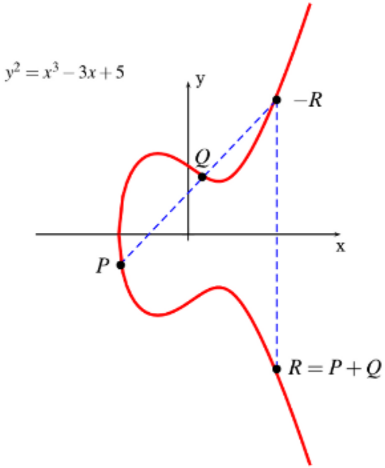
- Dada por una ecuación de Weierstrass suave $y^2 = x^3 + ax^2 + bx + c$ sobre un campo K. Hay que proyectivizar:

  $$y^2 z = x^3 + ax^2 z + bxz^2 + cz^3, \quad [x : y : z] \in \mathbb{P}^2_K$$

  y el punto distinguido es $[0 : 1 : 0]$. Ley de grupo: cuerda-tangente.
- $E = \mathbb{C}/\Lambda$ donde $\Lambda \subseteq \mathbb{C}$ es un retículo ($\Lambda \simeq \mathbb{Z}^2$ y es discreto). Esto es un toro complejo. El punto distinguido es $[\Lambda] \in \mathbb{C}/\Lambda$. Estructura de grupo: la suma de $\mathbb{C}$.
- (Teoría de análisis rígido de J. Tate) $E = \mathbb{Q}_p^\times / \langle q \rangle$ para cierto $q \in \mathbb{Q}_p$ con $|q| < 1$. Estructura de grupo: multiplicación de $\mathbb{Q}_p^\times$.

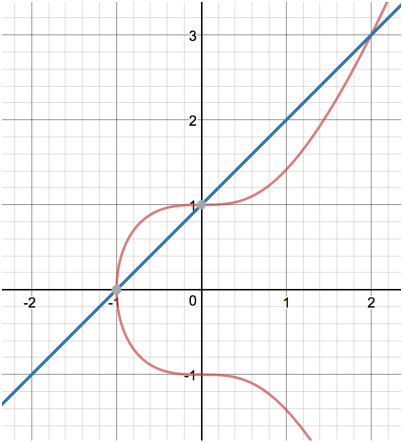
Cuerda-tangente

Sea E curva elíptica dada por una ecuación de Weierstrass sobre un campo K. Por ejemplo $y^2 = x^3 - 3x + 5$ sobre $\mathbb{R}$. La ley de grupo cuerda-tangente es:



Cuerda-tangente

En $y^2 = x^3 + 1$. Calculando $(-1, 0) + (0, 1) = (2, -3)$:



Curvas elípticas sobre $\mathbb{C}$

Sea $E/\mathbb{C}$ curva elíptica. $E(\mathbb{C})$ es una superficie de Riemann compacta de género 1 así que es un toro. Su cubrimiento universal es $\mathbb{C}$ y su uniformización es

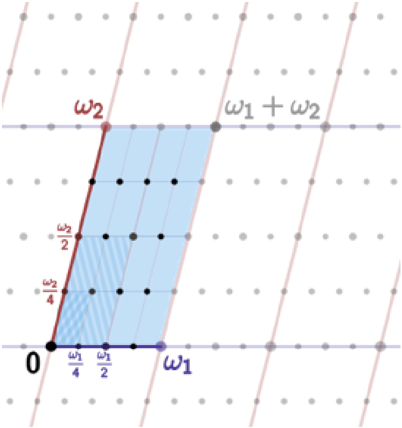
$$\pi : \mathbb{C} \to \mathbb{C}/\Lambda \simeq E, \quad \Lambda \subseteq \mathbb{C} \text{ un retículo.}$$

Λ no es único porque no estamos fijando el isomorfismo; después volveremos a este problema.
Para conectar con ecuaciones de Weierstrass uno define cierta función meromorfa $\wp_\Lambda : \mathbb{C} \to \mathbb{C}_\infty$ que cumple:

- Λ-periodica: $\wp_\Lambda(z + \lambda) = \wp_\Lambda(z)\ \forall \lambda \in \Lambda$
- polos exactamente en Λ, y son de orden 2.
- Ec. Dif.: $(\wp'_\Lambda(z))^2 = 4\wp_\Lambda(z)^3 - g_{2,\Lambda} \cdot \wp_\Lambda(z) - g_{3,\Lambda}$ para ciertos $g_{2,\Lambda}, g_{3,\Lambda} \in \mathbb{C}$ (vienen de series de Eisenstein —ojo con ellos).

Curvas elípticas sobre $\mathbb{C}$: torsión

Resultado importante: Si E es curva elíptica sobre $\mathbb{C}$ entonces $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
Demostración: Reflexionar sobre este dibujo con $n = 4$:



Curvas elípticas sobre $\mathbb{C}$: ambigüedad de Λ

Eligiendo otro Λ para la misma clase de isomorfismo de E, cambia $\wp_\Lambda$ y los $g_{2,\Lambda}, g_{3,\Lambda} \in \mathbb{C}$. PERO la cantidad siguiente no cambia:

$$j(E) = 1728 \frac{g_{2,\Lambda}^3}{g_{2,\Lambda}^3 - 27 g_{3,\Lambda}^2}.$$

Es el *invariante* j y *clasifica las curvas elípticas sobre* $\mathbb{C}$ *salvo isomorfismo*.

Curvas elípticas sobre $\mathbb{C}$: ambigüedad de Λ

Dado $\Lambda \subseteq \mathbb{C}$ podemos multiplicar por un $\alpha \in \mathbb{C}^\times$ (da isomorfismo en curvas elípticas) de modo que el retículo es de la forma

$$\Lambda_\tau = \mathbb{Z} + \mathbb{Z} \cdot \tau, \quad \tau \in \mathfrak{h} = \mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\}.$$

No hay unicidad debido al cambio de base en el retículo. Así que muchos $\tau \in \mathfrak{h}$ corresponden a la misma clase de isomorfismo de curva elíptica. No hay problema; ¡cuocuientamos por la acción del cambio de base!

$$SL_2(\mathbb{Z}) \times \mathfrak{h} \to \mathfrak{h}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}.$$

Entonces $Y(1) := SL_2(\mathbb{Z}) \backslash \mathfrak{h}$ es el espacio correcto para parametrizar clases de isomorfismo de curvas elípticas complejas. Obtenemos $j : Y(1) \to \mathbb{C}$ biyección holomorfa inducida por el invariante j.

Curva de Tate sobre $\mathbb{C}$

$\pi : \mathbb{C} \to \mathbb{C}/\Lambda_\tau$ se puede escribir en dos tramos:

$$\mathbb{C} \to \mathbb{C}/\mathbb{Z} \to \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau).$$

Salvo isomorfismos, esto es

$$\mathbb{C} \to \mathbb{C}^\times \to \mathbb{C}^\times/\langle q_\tau \rangle$$

donde la primera flecha es $z \mapsto e^{2\pi i z}$ y las segunda es usando $q_\tau = e^{2\pi i \tau}$. Notar que $|q_\tau| = e^{-2\pi \mathrm{Im}\,(\tau)} < 1$ porque $\tau \in \mathfrak{h}$. La presentación $\mathbb{C}^\times/\langle q_\tau \rangle$ para E es la *curva de Tate*.

Curva de Tate sobre $\mathbb{Q}_p$

En $\mathbb{Q}_p$ no existe una función exponencial que converja en todas partes. Pero el segundo tramo de $\mathbb{C} \to \mathbb{C}^\times \to \mathbb{C}^\times/\langle q_\tau \rangle$ tiene sentido:

Teorema (John Tate)

Dado $q \in \mathbb{Q}_p$ con $|q| < 1$ hay una curva elíptica E sobre $\mathbb{Q}_p$ tal que $E(\mathbb{Q}_p)$ es analíticamente isomorfo al grupo p-ádico $\mathbb{Q}_p^\times/\langle q \rangle$.

- Se puede trabajar con extensiones algebraicas de $\mathbb{Q}_p$, con sus completaciones (e.g $\mathbb{C}_p$), etc.
- Las curvas de Tate p-ádicas *siempre tienen reducción multiplicativa*: reducidas módulo p dan un nodo (en particular, mala reducción).
- Tate demostró el recíproco: si una curva E sobre $\mathbb{Q}_p$ tiene reducción multiplicativa, entonces es analíticamente isomorfa a una curva de Tate (salvo, quizá, reemplazar $\mathbb{Q}_p$ por una extensión cuadrática en caso de reducción multiplicativa non-split).

Sobre $\mathbb{Q}$

Sea $E/\mathbb{Q}$ curva elíptica. Dos teoremas fundamentales

Teorema (Mordell-Weil)

El grupo de puntos con coordenadas racionales $E(\mathbb{Q})$ es finitamente generado. En particular, es de la forma $E(\mathbb{Q}) \simeq \mathbb{Z}^r \times (\text{finito})$.

$r = \operatorname{rk} E(\mathbb{Q})$ es el *rango*.

Teorema (Lutz-Nagell)

Si E es dada en la forma $y^2 = x^3 + Ax^2 + Bx + C$ con $A, B, C \in \mathbb{Z}$, entonces los puntos de torsión de $E(\mathbb{Q})$ tienen coordenadas enteras. Además son calculables.

Sobre $\mathbb{Q}$

Un resultado mucho más difícil:

Teorema (Mazur)

Dada $E/\mathbb{Q}$, las únicas posibilidades para $E(\mathbb{Q})_{tor}$ son

$$\mathbb{Z}/n\mathbb{Z}, \quad n = 1, 2...., 9, 10, 12$$

o bien

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, \quad n = 1, 2, 3, 4.$$

Todos ocurren.

La función $L(E,s)$ para $E/\mathbb{Q}$

Si $E/\mathbb{Q}$ tiene buena reducción mod p entonces

$$N_p := \#E(\mathbb{F}_p) = p + 1 - a_p$$

para cierto $|a_p| < 2\sqrt{p}$ (la *cota de Hasse*). Se define:

$$L_p(E,s) = \begin{cases} (1 - a_p p^{-s} + p \cdot p^{-2s})^{-1} & \text{buena reducción} \\ 1 \quad \text{reducción aditiva (cúspide: se ve como un "3")} \\ (1 - p^{-s})^{-1} & \text{reducción multiplicativa split: como un "}\alpha\text{"} \\ (1 + p^{-s})^{-1} & \text{reducción multiplicativa non-split} \end{cases}$$

con esto la *función L* es

$$L(E,s) = \prod_p L_p(E,s) = (*) \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

La función $L(E,s)$ para $E/\mathbb{Q}$

Notar el parecido de

$$L(E,s)=\prod_p L_p(E,s)=(*)\prod_p \frac{1}{1-a_p p^{-s}+p^{1-2s}}.$$

con

$$\zeta(s)=\prod_p \frac{1}{1-p^{-s}} \quad \text{(Euler; Riemann).}$$

Uno quisiera continuación analítica y ecuación funcional para $L(E,s)$ tal y como se sabe sobre $\zeta(s)$, pero lo único claro es que $L(E,s)$ converge para $\Re(s)>3/2$ gracias a la cota de Hasse.
La modularidad nos dirá muchas cosas más.

Conjetura [BSD]: $\mathrm{ord}_{s=1}L(E,s)=\mathrm{rk}\, E(\mathbb{Q})$.