Curvas y formas modulares

Matías Alvarado, con apuntes y un apéndice de José Cuevas Barrientos

1. El problema de moduli

Considere[1] $\mathscr{A}_1(\mathbb{C})$ el cual va a ser, momentaneamente, un conjunto cuyos puntos corresponden a clases de isomorfismo de curvas elípticas complejas. El invariante j determina entonces una función $j\colon \mathscr{A}_1(\mathbb{C}) \to \mathbb{C} = \mathbb{A}^1(\mathbb{C})$ que es de hecho una biyección (cfr. Silverman [**6,** pág. 45], Prop. III.1.4). Así, podríamos decir que $\mathscr{A}_{1,\mathbb{C}} \cong \mathbb{A}^1_{\mathbb{C}}$ es una curva algebraica compleja que también funciona de espacio de moduli para las curvas elípticas.

Ahora bien, si definiesemos $\mathscr{A}_{1,K}$ «=» $\mathbb{A}^1_K$ para un cuerpo cualquiera mediante el invariante j nos toparíamos con el problema de que dos curvas elípticas E_1, E_2 sobre K tienen $j(E_1) = j(E_2)$ si son isomorfas sobre K^{alg}, de modo que esta noción no es adecuada para cuerpos arbitrarios (ni mucho menos, para un esquema base S general). Así, nuestra misión será poder definir una familia de esquemas algebraicos $\mathscr{A}_{1,d,N}$ sobre $\mathbb{Q}$ que sí puedan, en conjunto, clasificar curvas elípticas sobre $\mathbb{Q}$.

2. Uniformización

El primer paso será revisar, con otros ojos, la teoría de curvas elípticas complejas (vid. Silverman [**6,** págs. 157 ss.], Ch. VI). Un ***reticulado*** $\Lambda \subseteq \mathbb{C}$ es un subgrupo aditivo discreto tal que es un $\mathbb{Z}$-módulo libre de rango 2; en otras palabras, existen $\omega_1, \omega_2 \in \Lambda$ no nulos tales que $\omega_2/\omega_1 \notin \mathbb{R}$ y tales que $\Lambda = \langle \omega_1, \omega_2 \rangle = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$. Dado un reticulado $\Lambda \leq \mathbb{C}$, podemos construir un espacio complejo analítico $E_\Lambda := \mathbb{C}/\Lambda$, donde una función holomorfa $E_\Lambda \to X$ es la identificación de una función holomorfa $\mathbb{C} \to X$ tal que dados $z \in \mathbb{C}$ y $\tau \in \Lambda$ se cumpla que $f(z+\tau) = f(z)$. Topológicamente, es fácil comprobar que E_Λ es un toro, es decir, $E_\Lambda \approx \mathbb{S}^1 \times \mathbb{S}^1$, de modo que es conexo, compacto, de género (topológico) 1 y de dimensión (compleja) 1; es decir, es analíticamente una curva elíptica.

Bajo esta perspectiva, un morfismo entre curvas elípticas complejas

$$f\colon \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2$$

es necesariamente de la forma $f(z) = \lambda z$ para un $\lambda \in \mathbb{C}$, donde se exige que $\lambda\Lambda_1 \subseteq \Lambda_2$. Se sigue que dos reticulados Λ_1 y Λ_2 inducen la misma curva elíptica compleja si y solo si son ***homotéticos*** (i.e. si existe $\alpha \in \mathbb{C}$ tal que

Fecha: 14 de junio de 2024.

[1] En general, $\mathscr{A}_g(\mathbb{C})$ denota el *espacio de moduli* de variedades abelianas complejas de dimensión g.

$\alpha\Lambda_1 = \Lambda_2$). Más aún, es claro que todo reticulado Λ es homotético a uno de la forma $\langle 1, \tau\rangle$, donde $\tau \in \mathbb{C}$ tiene $\operatorname{Im}\tau > 0$, es decir, pertenece al semiplano superior[2]

$$\mathfrak{h} := \{\tau \in \mathbb{C} : \operatorname{Im}\tau > 0\}.$$

Así, tenemos una función $j\colon \mathfrak{h} \to \mathbb{C}$ que a cada $\tau \in \mathfrak{h}$ le asocia el invariante j de la curva elíptica compleja $\mathbb{C}/\langle 1, \tau\rangle$. Lo primero que hay que saber es que:

Teorema 2.1 (de uniformización): La función $j\colon \mathfrak{h} \to \mathbb{C}$ tiene las siguientes propiedades:

1. j es sobreyectiva.
2. j es holomorfa, en particular, no posee polos.
3. j es invariante bajo la acción de $\mathrm{SL}_2\mathbb{Z}$.

Demostración: La analiticidad se sigue de la teoría misma de las curvas elípticas complejas. El que sea invariante bajo la acción de $\mathrm{SL}_2\mathbb{Z}$ viene de que $\tau_1, \tau_2 \in \mathfrak{h}$ están en la misma órbita de la acción syss determinan reticulados homotéticos. La sobreyectividad es más complicada, pero está hecha, por ejemplo, en Apostol [**1,** págs. 34-39], Thm. 2.5. □

En particular, el inciso 1, dice que cada curva elíptica compleja es isomorfa al cociente de algún reticulado. En consecuencia, el *espacio de moduli* de curvas elípticas complejas es el de los reticulados complejos salvo homotecia.

Procedemos a detallar la acción de $\mathrm{SL}_2(\mathbb{Z}) \curvearrowright \mathfrak{h}$: como $\mathbb{C}$ es, como $\mathbb{R}$-espacio vectorial, isomorfo a $\mathbb{R}^2$, existe una acción natural $\mathrm{GL}_2\mathbb{R} \curvearrowright \mathbb{C}$. Si ahora queremos «preservar orientación», vale decir, queremos que $\mathfrak{h}$ sea estable bajo esta acción, debemos restringirnos a matrices de determinante positivo; en particular, $\mathrm{SL}_2\mathbb{R} \curvearrowright \mathbb{C}$ respetando a $\mathfrak{h}$ (como conjunto, no punto a punto). Como $\mathrm{SL}_2\mathbb{Z} \leq \mathrm{SL}_2\mathbb{R}$ es subgrupo, tenemos una acción $\mathrm{SL}_2\mathbb{Z} \curvearrowright \mathfrak{h}$ canónica dada por

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot z := \frac{az+b}{cz+d}.$$

Uno puede verificar que esta acción manda τ_1 en τ_2 de modo que $\langle 1, \tau_1\rangle$ y $\langle 1, \tau_2\rangle$ son homotéticos. Así, uno puede construir el espacio de órbitas $\mathrm{SL}_2\mathbb{Z} \setminus \mathfrak{h}$, que admite una estructura analítica y el teorema de uniformización se traduce en que:

Corolario 2.1.1: La función $j\colon \mathrm{SL}_2\mathbb{Z} \setminus \mathfrak{h} =: Y(1) \to \mathbb{C} = \mathbb{A}^1(\mathbb{C})$ es un isomorfismo analítico.

Este $Y(1)$ ahora admite estructura de curva afín sobre $\mathbb{C}$, por lo que nos gustaría dar una expresión similar de su *compactificación* (i.e., de $\mathbb{P}^1(\mathbb{C})$).

[2]Nótese que esto último es una mera convención, también podríamos haber exigido que estuviera en el semiplano inferior y virtualmente nada cambiaría.

Si ahora consideramos el semiplano extendido

$$\mathfrak{h}^* := \mathfrak{h} \cup \mathbb{Q} \cup \{\infty\},$$

se puede probar que sigue siendo estable bajo la acción de $\mathrm{SL}_2\,\mathbb{Z}$ y que el cociente analítico $X(1) := \mathrm{SL}_2\,\mathbb{Z} \setminus \mathfrak{h}^*$ posee la siguiente propiedad:

Teorema 2.2 (de uniformización): La función j se extiende a una función biholomorfa $X(1) \to \mathbb{C} \cup \{\infty\} = \mathbb{P}^1(\mathbb{C})$.

Más generalmente, podemos considerar varios subgrupos de $\mathrm{SL}_2\,\mathbb{Z}$ que, en el problema de moduli, agarran más información:

Definición 2.3: Dado un entero $N \in \mathbb{Z}$, el cociente $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/N\mathbb{Z}$ induce un homomorfismo de grupos $\mathrm{SL}_2\,\mathbb{Z} \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ cuyo núcleo definimos como $\Gamma(1)$, llamado el ***subgrupo principal modular de nivel*** N. Más explícitamente:

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2\,\mathbb{Z} : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}.$$

Un subgrupo intermedio $\Gamma(N) \subseteq \Gamma \subseteq \mathrm{SL}_2\,\mathbb{Z}$ se dice un ***subgrupo de congruencia***.

Así, construimos a $\Gamma(N)$ como la preimagen del grupo trivial de $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ mediante el homomorfismo de reducción. En un anillo general, hay otros grupos de matrices de importancia general como el *grupo de matrices triangulares superiores* o el *grupo especial unipotente*, cuyas preimagenes son los siguientes subgrupos de congruencia:

$$\Gamma_0(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2\,\mathbb{Z} : c \equiv 0 \pmod{N} \right\},$$

$$\Gamma_1(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2\,\mathbb{Z} : c \equiv 0,\ b \equiv d \equiv 1 \pmod{N} \right\}.$$

Las relaciones entre estos grupos es la siguiente:

$$\begin{array}{l|ccccc} G = & \Gamma(N) & \leq & \Gamma_1(N) & \leq & \Gamma_0(N) \\ G \setminus \mathfrak{h} & Y(N) & & Y_1(N) & & Y_0(N) \\ G \setminus \mathfrak{h}^* & X(N) & & X_1(N) & & X_0(N) \end{array}$$

Asociado a ellos hay dos números de suma importancia:

- El género (topológico) de $\Gamma \setminus \mathfrak{h}^*$.
- La cantidad de puntos de $(\Gamma \setminus \mathfrak{h}^*) \smallsetminus (\Gamma \setminus \mathfrak{h})$.

Por ejemplo, cuando $\Gamma = \mathrm{SL}_2\,\mathbb{Z}$ vimos que el género es 0 y la cantidad de puntos es 1.

Finalmente, a los espacios de la forma $\Gamma \setminus \mathfrak{h}^*$ les llamaremos ***curvas modulares***.

Apéndice A. Las curvas modulares sobre $\mathbb{Q}$

Hasta ahora solo hemos tocado el aspecto analítico de las curvas modulares, pero también tienen una descripción algebraica (cfr. Rohrlich [**5**]). Sea $t \in \mathbb{Q}(t)$ trascendente sobre $\mathbb{Q}$, sea E una curva elíptica sobre $\mathbb{Q}(t)$ con $j(E) = t$, sea $P \in E(\mathbb{Q}(t)^{\text{alg}})$ un punto de orden N y sea $C \subseteq E(\mathbb{Q}(t)^{\text{alg}})$ el subgrupo cíclico generado por P. Definiremos el subcuerpo fijado

$$K := \text{Fix}(\{\sigma \in \text{Gal}(\mathbb{Q}(t)^{\text{alg}}/\mathbb{Q}(t)) : \sigma[C] = C\}) \supseteq \mathbb{Q}(t).$$

Entonces, se puede probar que $\mathbb{Q}$ es algebraicamente cerrado en K, es decir, que $K \cap \mathbb{Q}^{\text{alg}} = \mathbb{Q}$. Por tanto, K es una extensión *puramente trascendente* y de grado de trascendencia 1 sobre $\mathbb{Q}$, luego podemos asociarle un *modelo regular propio* (i.e., la única curva regular proyectiva $C_{\mathbb{Q}}$ sobre $\mathbb{Q}$ tal que $K(C_{\mathbb{Q}}) = K$). Éste modelo se denotará $X_0(N)_{\mathbb{Q}}$.

Procedemos a detallar exactamente qué clase de problema de moduli ataca $X_0(N)$.

Fijemos un cuerpo algebraicamente cerrado k. Considere a los pares $(\mathcal{E}, C)$, donde $\mathcal{E}$ es una curva elíptica sobre k y donde $C \subseteq \mathcal{E}[N](k)$ es un subgrupo cíclico de orden N. Podemos tomar la relación de equivalencia $(\mathcal{E}_1, C_1) \sim (\mathcal{E}_2, C_2)$ dada por la existencia de un k-isomorfismo $f\colon \mathcal{E}_1 \to \mathcal{E}_1$ tal que $f[C_1] = C_2$. Denotaremos por $\text{Ell}_0(N)(k)_S$ al conjunto de pares $[\mathcal{E}, C]$ salvo equivalencia, tales que $j(\mathcal{E}) \notin S$ donde $S \subseteq \mathbb{P}^1(k)$ es un conjunto fijo de puntos.

Considere $\mathbb{P}^1_{\mathbb{Q}}$, el cual es un esquema de Dedekind (conexo) que, el lector no acostumbrado a la idea de esquemas, puede pensar como órbitas de Galois de $\mathbb{Q}^{\text{alg}}$ junto a un punto al infinito. Dentro de S tenemos un único punto genérico cuyo cuerpo de restos es $\mathbb{Q}(t)$. Si E es una curva elíptica sobre $\mathbb{Q}(t)$, podemos construir un modelo de Néron $\mathcal{E} \to \mathbb{P}^1_{\mathbb{Q}}$ (cfr. Bosch *et al.* [**2**]). Si $x \in \mathbb{P}^1_{\mathbb{Q}}$ es un punto cerrado, entonces podemos considerar la fibra $\mathcal{E}_x$ que es una curva sobre un cuerpo numérico $\Bbbk(x)$; si x es de «buena reducción», entonces $\mathcal{E}_x$ es una curva elíptica que, por comodidad, pensaremos sobre $\mathbb{Q}^{\text{alg}}$ (o $\mathbb{C}$) mediante un cambio de base. Esto, por la propiedad de extensión de Néron, induce una función de reducción (¡que no viene de un morfismo!) $E[N] \to \mathcal{E}_x[N]$ en puntos de N-torsión, la cual es inyectiva; por lo que $P \in C \subseteq E[N]$ se mandan a $P_x \in C_x \subseteq \mathcal{E}_x[N]$ mediante esta función. Si $S \subseteq \mathbb{P}^1_{\mathbb{Q}}$ es un conjunto finito de puntos cerrados, denotaremos por $X_0(N)_S$ a la preimagen de $\mathbb{P}^1_{\mathbb{Q}} \smallsetminus S$ mediante j. Por ejemplo, si $S = \{\infty\}$, entonces $X_0(N)(\mathbb{C})_S = Y_0(N)(\mathbb{C})$.

Proposición A.1: Sea E una curva elíptica sobre $\mathbb{Q}(t)$ con $j(E) = t$ y sea $S \subseteq \mathbb{P}^1_{\mathbb{Q}}$ los puntos de mala reducción de E. Sea $P \in E[N]$ un punto de orden N y sea $C := \langle P \rangle \leq E[N]$. Entonces, la función $x \mapsto [\mathcal{E}_{j(x)}, C_{j(x)}]$ determina una biyección entre $X_0(N)(\mathbb{C})_S$ y $\text{Ell}_0(N)(\mathbb{C})_S$.

Demostración: Cfr. Rohrlich [**5,** págs. 47 s.]. □

Ahora queremos poder asociarle a $X_0(N)$ un esquema sobre $\mathbb{Z}$ o, más generalmente, sobre algún dominio de Dedekind. El problema es que $X_0(N)$ no admite estructuras adicionales (como la de un grupo algebraico sobre $\mathbb{C}$) que permitan emplear técnicas como las de los modelos de Néron. En su lugar, uno puede construir el modelo minimal $\overline{\mathcal{X}_0(N)}$ sobre $\operatorname{Spec}\mathbb{Z}$ (esto es por la resolución de singularidades de superficies fibradas excelentes, vid. Liu [**4,** págs. 361 ss.], §8.3.4), el cual no es, por lo general, suave sobre $\mathbb{Z}$ (i.e., tiene fibras singulares). Podemos así, definir $\mathcal{X}_0(N)$ removiendo las fibras singulares, el cual ahora es suave sobre $\mathbb{Z}$, pero no es propio, sino que es propio sobre $\mathbb{Z}[1/N]$.

Referencias

1. Apostol, T. M. *Modular Functions and Dirichlet Series in Number Theory Graduate Texts in Mathematics* **41** (Springer-Verlag, 1976).
2. Bosch, S., Lütkebohmert, W. y Raynaud, M. *Néron models Grundlehren der mathematischen Wissenschaften* **21** (Springer-Verlag, 1990).
3. Chai, C.-L. *Siegel Moduli Schemes and Their Compactifications over* $\mathbb{C}$ en *Arithmetic Geometry* (eds. Cornell, G. y Silverman, J. H.) (Springer-Verlag, 1986), 231-252.
4. Liu, Q. *Algebraic Geometry and Arithmetic Curves* (Oxford University Press, 2002).
5. Rohrlich, D. E. *Modular Curves, Hecke Correspondences, and L-functions* en *Modular Forms and Fermat's Last Theorem* (eds. Cornell, G., Silverman, J. H. y Stevens, G.) (Springer-Verlag, 2000), 41-100.
6. Silverman, J. H. *The arithmetic of elliptic curves* 2.ª ed. (Springer-Verlag, 2009).

Correo electrónico: mnalvarado1@mat.uc.cl

Departamento de Matemáticas, Pontificia Universidad Católica de Chile. Facultad de Matemáticas, 4860 Av. Vicuña Mackenna, Macul, RM, Chile

Correo electrónico: josecuevasbtos@uc.cl