Cómo reconocer curvas elípticas isógenas

José Cuevas Barrientos, con aportes de Rocío Sepúlveda-Manzo

Resumen. Este fue originalmente una terna de informes para un curso acerca de formas modulares dictado por Héctor Pastén. En ellos se presentaron aplicaciones de la teoría de formas modulares, mediante el teorema de modularidad de Wiles y un teorema de Serre-Faltings, a la clasificación de curvas elípticas salvo isogenia. Se incluyeron ejemplos con cálculos explícitos hechos en `Sage`.

Índice

Introducción

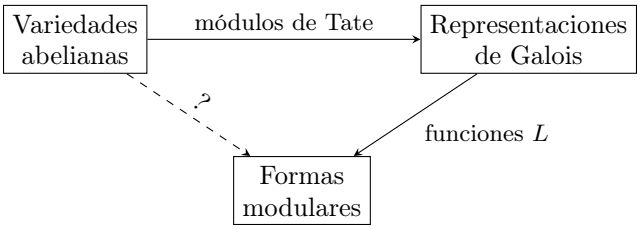
En teoría de números encontramos dos objetos de gran interés: las curvas elípticas y las formas modulares. Históricamente se sabe que estos objetos poseen cierta relación, por ejemplificar, el invariante j determina una función holomorfa $j\colon X(1) \to \mathbb{P}^1(\mathbb{C})$ que induce un biholomorfismo entre $Y(1) = X(1) \smallsetminus \{[\mathrm{i}\infty]\}$ y $\mathbb{A}^1(\mathbb{C}) = \mathbb{P}^1(\mathbb{C}) \smallsetminus \{\infty\}$. Similarmente, las curvas modulares $X(N)$ son compactificaciones de espacios de *moduli* de curvas elípticas dotadas con cierta información adicional (como un punto de torsión de periodo n, o una polarización). No obstante, una de las cuestiones centrales para la teoría de números era obtener alguna otra clase de objeto que fuese capaz de parametrizar curvas elípticas sobre $\mathbb{Q}$ o al menos con cierta información aritmética.

La relación de «ser isógenas» es un buen sustituto de «isomorfas» (vea la primera sección), por lo cual, teoremas que den criterios de ser isógenas son bien recibidos.

Fecha: 11 de diciembre de 2024. Actualizado: 24 de febrero de 2025.

Uno de los primeros vino de parte de Tate, quién probó en 1966 que, sobre *cuerpos finitos* k, basta ver los módulos de Tate $T_\ell(E)$ asociados a una curva elíptica (dotados de una acción del grupo de Galois absoluto $\mathrm{Gal}(k^{\mathrm{alg}}/k)$) para clasificarlos salvo isogenia. Esto se sigue de aplicar las llamadas *hipótesis de finitud de Tate* que él verificó para cuerpos finitos, pero que, para cuerpos numéricos, estaban abiertas. Serre probó incondicionalmente que el criterio de Tate aplica cuando las curvas tienen invariante j *entero* y finalmente Faltings probó que las hipótesis de Tate se satisfacen, extendiendo el teorema de isogenias de Tate a cuerpos numéricos.

Ahora bien, verificar a mano que dos curvas poseen los mismos módulos de Tate parece una reducción no demasiado significativa ni calculable. El remate sucede en que, a través de los módulos de Tate, a una curva elíptica se le asocia una función L específica, así que, en principio, podríamos solo comparar las funciones L, lo que reduce las verificaciones de infinitos primos a un conjunto de densidad no nula (mediante el teorema de Čebotarev). Si, además, tomamos los coeficientes y, con ellos, construimos la expansión de Fourier de una función f_E, esta aparentaría ser una forma modular. Así, el panorama es más o menos el siguiente:



La conjetura de Shimura-Taniyama-Weil, formulada en las décadas de los 1950's y 60's, afirmaba precisamente que f_E es modular. Fue probada para curvas elípticas sobre $\mathbb{Q}$ *semiestables* (principalmente) gracias a Wiles en 1995, lo que bastó para demostrar el último teorema de Fermat; un par de años más tarde, en 2001 fue probada en completa generalidad. El punto de este trabajo es aplicar este teorema para calcular curvas elípticas salvo isogenia.

En la primera sección juntamos ciertos preliminares para lo que sigue (definición de isogenia y criterios para los tipos de reducción módulo p). En §2 explicamos el teorema de modularidad de Wiles y en §4 explicamos la relación con la relación de ser isógenas entre curvas elípticas. En §3 explicamos cómo calcular el género de ciertas curvas modulares, lo que nos da aplicaciones inmediatas; no obstante, si el espacio de *newforms* fuese demasiado grande, conocer el género no provee una solución eficiente.

Así, nos topamos con el problema de reconocer eficientemente formas modulares. Como la dimensión del espacio de formas modulares es finita, es intuitivo que debería haber alguna cota y, en 1987, Jacob Sturm **[12]** encontró cotas para el grupo $\mathrm{SL}_2(\mathbb{Z})$ y, mejor aún, para el grupo $\Gamma_0(N)$. Explicamos su demostración y cómo emplear sus cotas en §5.

En §6 explicamos por encima algunas distintas versiones del teorema de modularidad, lo que nos ofrece un nuevo invariante: el *grado modular*. En la última §7 esbozamos cómo dar una expresión explícita para dicho invariante.

1. Resumen sobre curvas elípticas

Vamos a hacer un breve recuento de la teoría de curvas elípticas, el lector puede consultar a Silverman **[11].** Dado un cuerpo K, una ***curva elíptica*** E sobre K es una curva proyectiva y suave, que es también un *grupo algebraico*. En particular, satisface que para toda extensión de cuerpos L/K se cumple que el conjunto de puntos racionales $E(L)$ posee estructura de grupo definida funtorialmente.

1.1. Isogenias. Un ***homomorfismo de grupos algebraicos*** $f\colon G \to H$ es un morfismo entre variedades algebraicas (definidas sobre K) tal que para toda extensión L/K la función $f(L)\colon G(L) \to H(L)$ es un homomorfismo de grupos. Una ***isogenia*** entre curvas elípticas será un homomorfismo de grupos algebraicos tal que el núcleo $\ker f$ es un esquema finito sobre K.

Proposición 1.1: Toda isogenia entre curvas elípticas es (geométricamente) sobreyectiva.

Daremos dos pruebas de ello, la primera es sobre $\mathbb{C}$ para dar intuición topológica:

Demostración: Vamos a probarlo en nuestro caso de interés, es decir, para curvas sobre un cuerpo de números K. Haciendo cambio de base podemos ver que $(\ker f)(\mathbb{C}) = \ker(f_{\mathbb{C}})(\mathbb{C})$ el cual sigue siendo finito, es decir, sigue siendo isogenia. Ahora bien, $E(\mathbb{C})$ posee estructura de variedad analítica compacta (ya que E es proyectiva), de modo que $F := f(\mathbb{C})\colon E(\mathbb{C}) \to E'(\mathbb{C})$ tiene imagen compacta (en particular, cerrada). No obstante, como las fibras de F son finitas y tienen misma cardinalidad, entonces se verifica que F es un homeomorfismo local, por lo que F es abierta. Finalmente, como $E'(\mathbb{C})$ es conexo e infinito, se concluye que F es sobreyectiva. □

La segunda es general:

Demostración: Queremos emplear la misma técnica de que la imagen de $f\colon E \to E'$ es abierta y cerrada. Que la imagen sea cerrada, se sigue del hecho de que E es proyectiva, luego el morfismo $E \to \operatorname{Spec} k$ es universalmente cerrado. Por otro lado, para ver que f es abierto, basta probar que sea plano. Esto se sigue del hecho de que E' es regular (pues es suave), de que E sea propia (pues es proyectiva) y regular, y de que las fibras tengan todas dimensión $0 = \dim E - \dim E'$; por lo que aplica el criterio de Görtz y Wedhorn **[6,** pág. 481], Cor. 14.130. (Este criterio viene del caso afín, cfr. **[Stacks],** `Tag 00R4`.) □

El siguiente resultado es clásico:

Teorema 1.2 (Mordell-Weil): Sea E una curva elíptica definida sobre un cuerpo numérico K. Para toda extensión finita L/K el grupo $E(L)$ es finitamente generado y, por lo tanto, posee una parte libre de torsión $\mathbb{Z}^r$, donde $r := \operatorname{rang} E(L)$.

Corolario 1.2.1: Si E y E' son curvas elípticas definidas sobre un cuerpo numérico K y son isógenas, entonces para toda extensión finita L/K se cumple que $\operatorname{rang} E(L) = \operatorname{rang} E'(L)$.

El corolario anterior motiva el hecho de que «ser isógenas» es una relación de interés.

Definición 1.3: Sea E una curva elíptica sobre un cuerpo k de $\operatorname{car} k =: p$. Dado un entero $n > 0$ se define el esquema $E[n]$ de n-torsión de E como el núcleo de la multiplicación $[n]_E \colon E \to E$; si $p \nmid n$, entonces $E[n]$ posee exactamente n^2 puntos en la clausura algebraica y son todos separables. Dado un primo ℓ se define el ***módulo de Tate*** como

$$T_\ell(E) := \varprojlim_m E[\ell^m](k^{\mathrm{alg}}),$$

donde el diagrama implícito consta de flechas $[\ell] \colon E[\ell^{m+1}] \to E[\ell^m]$. Cada objeto en el diagrama es un $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-módulo, vale decir, es un grupo abeliano (con la suma de $E(k^{\mathrm{sep}})$) dotado de una acción de $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ que es compatible. Dicha acción corresponde a un cambio de base.

Observación 1.3.1: Cuando $\ell = p = \operatorname{car} k > 0$, lo que sucede es que el módulo de Tate es 0 o $\mathbb{Z}_\ell$ con la acción trivial. Esto se sigue de resultados conocidos en teoría de variedades abelianas (cfr. **[Stacks],** `Tag 03RP`), aunque por alguna extraña razón no suele ser mencionado.

Una proposición más acorde a nuestros propósitos es la siguiente:

Proposición 1.4: Sean E y E' un par de curvas elípticas sobre un mismo cuerpo K. Si E y E' son isógenas, entonces sus módulos de Tate $T_\ell(E)$ y $T_\ell(E')$ son isomorfos para cada primo ℓ de buena reducción a ambos.

Demostración: Esto se sigue de la funtorialidad del módulo de Tate, recordando que para toda isogenia $f \colon E \to E'$ existe otra $g \colon E' \to E$ tal que la composición $f \circ g = [n]_E$ es una multiplicación. □

1.2. Tipos de reducción módulo p. Sea A un dominio de Dedekind (e.g., el anillo de enteros algebraicos $\mathcal{O}_K$ para un cuerpo numérico K), sea $K := \operatorname{Frac} A$ y sea E una curva elíptica sobre K.

Elijamos $\mathfrak{p} \in \operatorname{Spec} A$ un primo no nulo. Diremos que una ecuación de Weierstrass

$$E \colon \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

es ***minimal en*** $\mathfrak{p}$ si cada $a_j \in A_{\mathfrak{p}}$ (equivalentemente, $\nu_{\mathfrak{p}}(a_j) \geq 0$) y $\nu_{\mathfrak{p}}(\Delta) \geq 0$ es minimal sujeto a la condición anterior. Denotaremos por $\Bbbk(\mathfrak{p}) := A/\mathfrak{p}$, el cual es un cuerpo.

Uno puede probar lo siguiente:

Proposición 1.5: Sea A un dominio de Dedekind y sea E una curva elíptica sobre $K := \operatorname{Frac} A$. Elijamos una ecuación de Weierstrass $E \colon y^2 = x^3 + a_4x + a_6$ con $a_4, a_6 \in A$, y un primo $\mathfrak{p} \in \operatorname{Spec} A$ no nulo.

1. Si
$$\nu_{\mathfrak{p}}(\Delta) < 12, \qquad \nu_{\mathfrak{p}}(a_4) < 4 \quad \text{o} \quad \nu_{\mathfrak{p}}(a_6) < 6 \tag{1}$$
entonces la ecuación es minimal en $\mathfrak{p}$.
2. Si $\operatorname{car} \Bbbk(\mathfrak{p}) \nmid 6$ y la ecuación es minimal en $\mathfrak{p}$, entonces (1).

No es cierto que $\nu_{\mathfrak{p}}(\Delta) < 12$ siempre, ni siquiera cuando $\operatorname{car}\Bbbk(\mathfrak{p}) \nmid 6$. Esto implicaría que la conjetura de Szpiro (o equivalentemente, la conjectura *abc*) sería trivial.

Teorema 1.6: Sea A un dominio de Dedekind y sea E una curva elíptica sobre $K := \operatorname{Frac} A$. Dado $\mathfrak{p} \in \operatorname{Spec} A$ no nulo, escojamos una ecuación de Weierstrass minimal en $\mathfrak{p}$ y considere la reducción módulo $\mathfrak{p}$ para obtener una variedad $\mathcal{W}_{\mathfrak{p}}$ sobre $\Bbbk(\mathfrak{p})$. Sea $\mathcal{E}^{\circ}_{\mathfrak{p}} := \mathcal{W}_{\mathfrak{p},\mathrm{sm}}$ el lugar suave, entonces es un grupo algebraico conmutativo suave y conexo, por lo que es uno de los siguientes:

(a) Una curva elíptica sobre $\Bbbk(\mathfrak{p})$.
En cuyo caso, diremos que E tiene ***buena reducción*** en $\mathfrak{p}$.
(b) El grupo aditivo $\mathbb{G}_{a,\mathfrak{p}}$.
En cuyo caso, diremos que E tiene ***reducción aditiva*** en $\mathfrak{p}$.
(c) Un toro lineal; es decir, $\mathcal{E}^{\circ}_{\mathfrak{p}} \times_{\Bbbk(\mathfrak{p})} \operatorname{Spec}(\Bbbk(\mathfrak{p})^{\mathrm{alg}}) \cong \mathbb{G}_{m,\Bbbk(\mathfrak{p})^{\mathrm{alg}}}$.
En cuyo caso, diremos que E tiene ***reducción multiplicativa*** en $\mathfrak{p}$. Además, diremos que dicha reducción es ***escindida*** o no, según si $\mathcal{E}^{\circ}_{\mathfrak{p}} \cong \mathbb{G}_{m,\mathfrak{p}}$ o no.

Aquí habrían dos maneras de proceder. O bien empleamos teoremas duros de comparación y diríamos que $\mathcal{E}^{\circ}_{\mathfrak{p}}$ es la componente conexa de la fibra del modelo de Néron, el cuál será un grupo algebraico conmutativo y suave, y concluímos mediante un teorema de clasificación. O bien notamos que esta tricotomía se explica así en $\operatorname{car}\Bbbk(\mathfrak{p}) \neq 2$, dada una ecuación de Weierstrass $y^2 = f(x)$, los tres casos se corresponden a si $f(x) \mod \mathfrak{p}$ tiene 3, 1 o 2 raíces distintas en $\Bbbk(\mathfrak{p})^{\mathrm{alg}}$, resp.

De esto se desprende el siguiente criterio:

Proposición 1.7: Una curva nodal singular en forma de Weierstrass tiene una única singularidad de orden 2 y esta corresponde a un nodo k-racional cuyas coordenadas son

$$(x_0, y_0) = \left(\frac{18b_6 - b_2b_4}{c_4}, \frac{b_2b_5 + 3b_7}{c_4} \right)$$

donde los coeficientes b_j y c_j son los estándar salvo por

$$b_5 = a_1a_4 - 2a_2a_3, \qquad b_7 = a_1(a_3^2 - 12a_6) + 8a_3a_4.$$

Las dos tangentes están dadas en términos del parámetro t por $x = x_0+t$, $y = y_0+\mu t$ para las dos raíces distintas del polinomio separable $\mu^2+a_1\mu-3x_0-a_2 = 0$. Cuando $\operatorname{car} K \neq 2$, se tiene que

$$\mu = \frac{-a_1c_4 \pm \sqrt{-c_4c_6}}{2c_4}.$$

Demostración: Cfr. Connell **[3],** Prop. 1.5.4. □

Teorema 1.8: Sea $S\colon y^2 + a_1xy = x^3 + a_2x^2$ una curva singular en forma de Weierstrass sobre k, que se factoriza $(y - \alpha x)(y - \beta x) = x^3$ en $K := k(\alpha, \beta)$ con $\alpha \neq \beta$. El K-morfismo

$$S_{\mathrm{sm}} \longrightarrow \mathbb{G}_m, \qquad (x, y) \longmapsto \frac{y - \beta x}{y - \alpha x}.$$

determina o bien un k-isomorfismo $S_{\mathrm{sm}}(k) \cong \mathbb{G}_m(k) = k^\times$ cuando $\alpha, \beta \in k$; o bien un K-isomorfismo $S_{\mathrm{sm}}(k) = \ker(\mathrm{Nm}_{K/k})$ cuando $K \neq k$.

Demostración: Cfr. Husemöller **[7],** Thm. III.7.2. □

Para el caso de $p = 2$, aplicamos el teorema 1.8 para obtener el siguiente criterio:

Proposición 1.9: Una curva nodal (proyectiva) singular de Weierstrass $S\colon y^2 + a_1xy = x^3 + a_2x^2$ sobre $k = \mathbb{F}_2$ se escinde syss S tiene 2 puntos (y no se escinde syss tiene 4 puntos).

2. Cómo asociarle una forma modular a una curva elíptica

Definición 2.1: Sea E una curva elíptica sobre $\mathbb{Q}$. Si p es un primo de buena reducción para E, denotaremos por $\mathcal{W}_p$ a su reducción módulo p y definiremos

$$a_p(E) := p + 1 - |\mathcal{W}_p(\mathbb{F}_p)|.$$

Si p es de mala reducción, definimos:

$$a_p(E) = \begin{cases} 1, & p \text{ es de reducción multiplicativa escindida,} \\ -1, & p \text{ es de reducción multiplicativa no escindida,} \\ 0, & p \text{ es de reducción aditiva.} \end{cases}$$

En particular, $a_p \in \{0, \pm 1\}$ en primos de mala reducción.

La función L de E está dada por el producto de Euler

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

donde $\chi(p)$ es 0 si E tiene mala reducción en p, y 1 en el otro caso.

Considere $L(E, s) = \sum_{n=1}^{\infty} a_n n^{-s}$, y defina

$$f_E(z) = \sum_{n=1}^{\infty} a_n q^n, \qquad q := \exp(2\pi i z), \tag{3}$$

el enunciado del teorema de modularidad afirma que f_E es una forma modular.

Sea $N > 1$ entero, definiremos

$$\Gamma_0(N) := \left\{ \gamma \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod{N} : \gamma \in \mathrm{SL}_2(\mathbb{Z}) \right\}$$

Considere el espacio de formas cuspidales $\mathcal{S}_k(\Gamma_0(N))$. Note que para cualquier $M \mid N$ el espacio $\mathcal{S}_k(\Gamma_0(M))$ es un subespacio de $\mathcal{S}_k(\Gamma_0(N))$ (ya que la invariancia bajo $\Gamma_0(M)$ implica invariancia bajo $\Gamma_0(N)$ para $M \mid N$). Más aún, si $Md = N$, entonces la siguiente es una transformación $\mathbb{C}$-lineal

$$\mathcal{S}_k(\Gamma_0(M)) \longrightarrow \mathcal{S}_k(\Gamma_0(N)), \qquad f(z) \longmapsto f(d \cdot z).$$

Diremos que una forma cuspidal $f \in \mathcal{S}_k(\Gamma_0(N))$ es *vieja* si pertenece al subespacio $\mathcal{S}_k^{\mathrm{old}}(\Gamma_0(N))$ generado por las imágenes de las transformaciones anteriores. Definimos $\mathcal{S}_k^{\mathrm{new}}(\Gamma_0(N))$ como un complemento de $\mathcal{S}_k^{\mathrm{old}}(\Gamma_0(N))$ (de hecho, es el complemento ortogonal respecto al producto interno de Petersson). Es decir,

$$\mathcal{S}_k(\Gamma_0(N)) = \mathcal{S}_k^{\mathrm{old}}(\Gamma_0(N)) \oplus \mathcal{S}_k^{\mathrm{new}}(\Gamma_0(N)).$$

Empleando la teoría de operadores de Hecke, podemos encontrar una base para $\mathcal{S}_k^{\text{new}}(\Gamma_0(N))$, para ser más específicos:

Definición 2.2: Una *newform* $f \in \mathcal{S}_2(\Gamma_0(N))$ es una función propia respecto a los operadores de Hecke, normalizada (i.e., cuyo $a_1 = 1$) y que no es *vieja*, es decir, tal que no existen $ab = N$ con $a \neq N$ y $g \in \mathcal{S}_2(\Gamma_0(d))$ tales que $f(z) = g(b \cdot z)$.

Definición 2.3: La función L de una forma cuspidal $f(z) = \sum_{n=1}^{\infty} a_n q^n$, con $q = \exp(2\pi i z)$ de peso k es la función compleja definida por la serie de Dirichlet

$$L(f, s) := \sum_{n=1}^{\infty} a_n n^{-s},$$

la cual converge uniformemente sobre compactos a una función holomorfa para $\text{Re}(s) > 1 + k/2$.

Teorema 2.4: Sea $f \in \mathcal{S}_k^{\text{new}}(\Gamma_0(N))$. La función L se puede escribir como el producto de Euler

$$L(f, s) = \prod_p (1 - a_p p^{-s} + \chi(p) p^{k-1} p^{-2s})^{-1}, \tag{4}$$

donde $\chi(p) = 0$ para $p \mid N$ y $\chi(p) = 1$ de otro modo.

Si reemplazamos $k = 2$ en las ecuaciones (2) y (4), ambos nos dan el producto de Euler

$$\prod_p (1 - a_p p^{-s} + \chi(p) p^{1-2s})^{-1}.$$

Se puede ver que $\chi(p)$ en ambos casos es el mismo: para *newforms* $f \in \mathcal{S}_k^{\text{new}}(\Gamma_0(N))$ se tiene que $\chi(p) = 0$ para cada $p \mid N$, mientras que para curvas elípticas $E/\mathbb{Q}$ se tiene $\chi(p) = 0$ para $p \mid \Delta_{\text{mín}}(E)$.

Esto conlleva a conjeturar lo siguiente:

Teorema 2.5 (de modularidad): Para toda curva elíptica $E/\mathbb{Q}$, la función f_E definida en (3) es una *newform* de peso 2 y de nivel $\Gamma_0(N)$.

DEMOSTRACIÓN: El teorema fue probado por WILES **[13]** para curvas semiestables y completada en general en el artículo de BREUIL *et al.* **[2].** □

De hecho, un teorema de Carayol-Eichler-Shimura da una especie de recíproco, a decir, toda *newform* viene de una curva elíptica.

3. El género de algunas curvas modulares

Al igual que en el caso de $\text{SL}_2(\mathbb{Z})$, podemos dotar a $Y_0(N) := Y(\Gamma_0(N)) = \Gamma_0(N) \setminus \mathfrak{H}$ de estructura de superficie de Riemann y compactificarla a la *curva modular* $X_0(N) := \Gamma_0(N) \setminus \mathfrak{H}^*$. La $\dim_{\mathbb{C}} \mathcal{S}_2(\Gamma) = g(X(\Gamma))$ por Cor. 2.17 de SHIMURA **[10,** pág. 39], así que calcularemos el género. Primero un poco de terminología:

Definición 3.1: Sea $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ un subgrupo de índice finito. Un punto $x \in \mathfrak{H}^*$ tal que $\Gamma_x \supset Z(\Gamma) := \{\pm 1\} \cap \Gamma$ se dice ***elíptico*** si $x \in \mathfrak{H}$ y una ***cúspide*** si $x \in \mathbb{P}^1(\mathbb{Q})$; de lo contrario, x se dice ***ordinario***. La misma terminología aplica para su imagen en $X(\Gamma)$.

Se dice que un punto $[x] \in X(\Gamma)$ es elíptico ***de periodo*** h si $\Gamma_x / Z(\Gamma)$ es un grupo (finito) de orden h.

Ejemplo 3.2: Para el grupo $\Gamma(1) := \mathrm{SL}_2(\mathbb{Z})$ los únicos puntos elípticos son [i] y $[\zeta_3]$ de periodos 2 y 3 resp., mientras que la única cúspide es [i∞]. En particular, todos salvo finitos puntos de $X(\Gamma)$ son ordinarios. ⌟

Para calcular el género de las curvas modulares recurriremos a la teoría de superficies de Riemann (referencias en Miranda [**8**]), donde $f\colon X \to Y$ es una función holomorfa entre superficies compactas:

Definición 3.3: Sea $f\colon X \to Y$ una función holomorfa entre superficies de Riemann compactas. Se le llama su ***grado*** $\deg f$ a la máxima cantidad de preimágenes de un punto $y \in Y$ (que es finita).

Lema 3.4 (Prop. II.4.1): Sea $f\colon X \to Y$ una función holomorfa entre superficies de Riemann compactas. Dado $x \in X$, existe un único $m := \mathrm{mult}_x(f)$ tal que existen cartas (φ, U, U') en torno a x y (ψ, V, V') en torno a $f(x)$ tal que $\psi(f(\varphi^{-1}(z))) = z^m$.

Lema 3.5 (Prop. II.4.8): Sea $f\colon X \to Y$ una función holomorfa entre superficies de Riemann compactas. Para todo $y \in Y$ se cumple que

$$\deg f = \sum_{f(x)=y} \mathrm{mult}_x(f).$$

Teorema 3.6 (fórmula de Riemann-Hurwitz, Thm. II.4.16): Sea $f\colon X \to Y$ una función holomorfa entre superficies de Riemann compactas. Entonces:

$$2(g(X) - 1) = 2(\deg f)(g(Y) - 1) + \sum_{x \in X} (\mathrm{mult}_x(f) - 1).$$

En particular, todos salvo finitos $y \in Y$ tienen exactamente $\deg f$ preimágenes.

Sea $x \in \mathfrak{H}^*$, y denotemos por Γx a su órbita por el grupo $\Gamma \leq \mathrm{SL}_2 \mathbb{Z} =: \Gamma(1)$, entonces tenemos una función

$$X(\Gamma) \longrightarrow X(1), \qquad \Gamma x \longmapsto \Gamma(1)x$$

y afirmamos que es holomorfa. Procedemos a calcular las preimágenes de un punto:

1. Si $[x] \in X(1)$ es ordinario, afirmamos que las preimágenes son todas distintas.
   En efecto si $\Gamma\gamma_{j_1} x = \Gamma\gamma_{j_2} x$ para $j_1 \neq j_2$, existen $\delta_1, \delta_2 \in \Gamma$ tales que $\delta_1\gamma_{j_1} x = \delta_2\gamma_{j_2} x$, esto implica que $\gamma_{j_2}^{-1}\delta_2^{-1}\delta_1\gamma_{j_1} \in \Gamma(1)_x$ y, como $[x]$ es ordinario entonces $\Gamma_x \subseteq \{\pm 1\}$ y, por lo tanto, $\delta_1\gamma_{j_1} = \pm\delta_2\gamma_{j_2}$, de modo que $\gamma_{j_1} \equiv \gamma_{j_2}$ (mód Γ). Por lo tanto, $\deg f = [\Gamma(1) : \{\pm 1\}\Gamma]$.
2. Si $[y] \in X(1)$ es elíptico de periodo h_1, para una preimagen $[x] \in X(\Gamma)$ de periodo h_Γ podemos calcular la multiplicidad de la siguiente forma: mediante

el diagrama

$$\begin{array}{ccc} \mathfrak{H} & = & \mathfrak{H} \\ {\scriptstyle \pi_\Gamma}\downarrow & & \downarrow{\scriptstyle \pi_1} \\ Y(\Gamma) & \xrightarrow{f} & Y(1) \end{array}$$

se verifica que $\mathrm{mult}_x(\pi_1) = \mathrm{mult}_x(\pi_\Gamma)\ \mathrm{mult}_{[x]}(f)$, de modo que $\mathrm{mult}_{[x]}(f) = h_1/h_\Gamma$. Si ahora denotamos $y_2 := i, y_3 := \zeta_3$, vemos que

$$d = h_\tau(|f^{-1}(y_\tau)| - \varepsilon_\tau) + \varepsilon_\tau, \qquad \sum_{f(x)=y_\tau} \mathrm{mult}_x(f) - 1 = \frac{h_\tau - 1}{h_\tau}(d - \varepsilon_\tau).$$

Finalmente, empleando que $\sum_{f(x)=[\infty]} \mathrm{mult}_x(f) - 1 = d - \varepsilon_\infty$, concluimos que:

Proposición 3.7: Sea $\Gamma \leq \Gamma(1)$ un subgrupo de índice finito con $\varepsilon_2, \varepsilon_3$ puntos elípticos de periodo 2 (resp. 3) y ε_∞ cúspides. Sea $d := [\Gamma(1) : \{\pm I\}\Gamma]$, entonces

$$g(X(\Gamma)) = 1 + \frac{d}{12} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{3} - \frac{\varepsilon_\infty}{2}.$$

Así que procedemos a calcular estos números cuando $\Gamma = \Gamma_0(N)$.

Lema 3.8: $d = \mu_N := [\Gamma(1) : \Gamma_0(N)] = N \prod_{p|N} \left(1 + \frac{1}{p}\right)$.

DEMOSTRACIÓN: Esto es un mero ejercicio de teoría de grupos guiado en DIAMOND y SHURMAN [**5,** págs. 106 s.]. □

Quedan por calcular $\varepsilon_2, \varepsilon_3$ y ε_∞. Comenzaremos por las cúspides:

Proposición 3.9: Para $N > 0$ entero, la cantidad de cúspides ε_∞ de $\Gamma_0(N)$ es

$$\varepsilon_\infty\big(\Gamma_0(N)\big) = \sum_{d|N} \phi(\mathrm{mcd}(d, N/d)).$$

DEMOSTRACIÓN: Esto se deduce de que, un punto $[a : c] \in \mathbb{P}^1(\mathbb{Q})$ escrito como vector columna $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]$ está en la misma órbita que $\left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right]$ si y sólo si existe $\gamma \in \Gamma_0(N)$ tal que

$$\begin{bmatrix} a \\ c \end{bmatrix} = \pm\gamma \cdot \begin{bmatrix} a' \\ c' \end{bmatrix},$$

y, para que dicha condición se cumpla, se reduce a que exista $u \in (\mathbb{Z}/N\mathbb{Z})^\times$ y $j \in \mathbb{Z}/N\mathbb{Z}$ tales que

$$\begin{bmatrix} ua' \\ c' \end{bmatrix} \equiv \begin{bmatrix} a + jc \\ uc \end{bmatrix} \quad (\text{mód } N).$$

Estas equivalencias están probadas en los lemas 3.8.1 y 3.8.3 de **[5].** La sección §3.8 llena los detalles faltantes. □

Lema 3.10: Sea $\Gamma \leq \Gamma(1)$ un subgrupo de índice finito. Mediante la función $X(\Gamma) \to X(1)$, puntos elípticos de periodo h van a puntos elípticos de periodo h.

DEMOSTRACIÓN: Basta notar que $\Gamma(1)_x \supseteq \Gamma_x$ y que, salvo signo, $\overline{\Gamma(1)}_x$ es o bien el cíclico C_2 o bien C_3, y ambos no tienen subgrupos propios no nulos. □

Empleando el hecho de que $\Gamma_{\gamma x} = \gamma\Gamma(1)_x\gamma^{-1} \cap \Gamma$ y que $\Gamma(1)_i = \{\pm I, \pm S\}$ y $\Gamma(1)_{\zeta_3} = \{\pm I, \pm ST, \pm(ST)^2\}$, podemos deducir que un $[\gamma i] \in X(\Gamma)$ es elíptico de periodo 2 si y sólo si $\gamma S\gamma^{-1} \in \Gamma$ (y similar con $[\gamma\zeta_3]$). Así son calculables con el siguiente código:

```
from sage.all import *
S = matrix([[0, -1], [1, 0]])
TS = matrix([[1, 1], [0, 1]])*S

def inGamma(N: int, matr) -> bool:
    return (matr[1][0] % N == 0)

def epsilon2(cosets: list, N: int) -> int:
    total = 0
    for gamma in cosets:
        if inGamma(N, gamma * S * gamma.inverse()):
            total += 1
    return total
def epsilon3(cosets: list, N: int) -> int:
    total = 0
    for gamma in cosets:
        if inGamma(N, gamma * TS * gamma.inverse()):
            total += 1
    return total

def epsilonInf(N: int) -> int:
    s = 0
    for d in Integer(N).divisors():
        s += euler_phi(gcd(d, N // d))
    return s

def deg(N: int) -> int:
    d = N
    for p in factor(-Integer(N)):
        d *= 1 + 1/p[0]
    return int(d)
def genus(N: int) -> int:
    cosets = list(Gamma0(N).coset_reps())
    return 1 + (deg(N) - 3*epsilon2(cosets, N) - 4*epsilon3(cosets, N) -
                6*epsilonInf(N))//12
```

4. CURVAS ISÓGENAS

Tenemos el siguiente criterio de «ser isógenas»:

Teorema 4.1 (de la isogenía de Serre-Faltings): Dos curvas elípticas sobre $\mathbb{Q}$ son isógenas si y sólo si $a_p(E) = a_p(E')$ para todo primo p de buena reducción a ambos. En consecuencia, son isógenas si tienen la misma forma modular.

DEMOSTRACIÓN: Esto es consecuencia del Cor. 1.3 de SCHAPPACHER **[9].** □

No obstante, como las *newforms* de conductor fijo son finitas, se sigue como consecuencia del teorema de modularidad, el siguiente resultado profundo:

Teorema 4.2 (Faltings-Tate): Sean E y E' curvas elípticas sobre $\mathbb{Q}$. Si $a_p(E) = a_p(E')$ para una cantidad *suficientemente grande* de primos p de buena reducción para E y E', entonces E y E' son isógenas.

Acá, la *cantidad suficientemente grande* es finita, pero depende del conductor de E (y de E'); el lector verá una versión explícita en §5.

Veámoslo en práctica. En la sección anterior dimos una manera de calcular el género de $X_0(N)$ con lo que podemos obtener la siguiente tabla:

N	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$g(X_0(N))$	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0

Así, por ejemplo, concluimos que:

Corolario 4.2.1: No hay curvas elípticas sobre $\mathbb{Q}$ con conductor ≤ 10.

También, del cálculo del género podemos ver que las curvas elípticas `11.a1` y `11.a3`:

$$E_1 \colon y^2 + y = x^3 - x^2 - 7820x - 263580, \qquad E_2 \colon y^2 + y = x^3 - x$$

son isógenas, ya que tienen conductor 11 y solo hay una *newform* de nivel $\Gamma_0(11)$. Esto es interesante, ya que las curvas *no* son isomorfas, puesto que la primera solo tiene un punto racional y la segunda tiene cinco.

Empleando el mismo código, vemos que $g(X_0(26)) = 2$, por lo que hay a lo más dos curvas elípticas salvo isogenia. En particular, las curvas elípticas `26.a3` y `26.b2`:

$$E_1 \colon y^2 + xy + y = x^3, \qquad E_2 \colon y^2 + xy + y = x^3 - 3x + 3,$$

no son isógenas, ya que $a_3(E_1) = 3$ y $a_3(E_2) = 7$, pero la curva elíptica $E_3 \colon y^2 + xy + y = x^3 - 5x - 8$ (`26.a2`) ha de ser isógena a E_1, puesto que, $a_3(E_3) = 3$.

5. COTAS DE STURM

En esta sección daremos un recuento de los trabajos de Sturm **[12].** Recuerde que $(f|_k\gamma)(z) := (cz + d)^{-k} f(\gamma \cdot z)$ para $\gamma := \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbb{R})$.

Lema 5.1: Sean $f, g \in \mathcal{M}_k(\mathrm{SL}_2\,\mathbb{Z})$ y supongamos que $\mathrm{ord}(f - g) > k/12$. Entonces $f = g$.

DEMOSTRACIÓN: Basta notar que existe $\Delta \in \mathcal{S}_{12}(\mathrm{SL}_2\,\mathbb{Z})$, la forma discriminante, la cual no se anula en $\mathfrak{H}$ y tal que $\mathrm{ord}_q \Delta = 1 > 0$. Luego, $(f - g)^{12}/\Delta^k$ es una forma automorfa de peso 0, tiene

$$\mathrm{ord}_q((f - g)^{12}/\Delta^k) = 12\,\mathrm{ord}(f - g) - k > 0,$$

y no tiene polos en $\mathfrak{H}$, así que, de hecho, es modular (i.e., es holomorfa en $X(1)$). Luego esta forma es constante, pero como se anula en q, ha de ser la forma nula. □

Teorema 5.2 (Sturm, 1987): Sean $f, g \in \mathcal{M}_k(\Gamma_0(N))$ y supongamos que $\mathrm{ord}(f-g) > k\mu_N/12$. Entonces $f = g$.

DEMOSTRACIÓN: Escribamos $\mathrm{SL}_2(\mathbb{Z})$ como unión disjunta de clases laterales

$$\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{j=1}^{\mu_N} \Gamma_0(N)\gamma_j, \qquad \gamma_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

y definamos $\psi := \varphi \cdot \prod_{j=2}^{\mu_N} (\varphi|_k \gamma_i)$, entonces $\psi \in \mathcal{M}_{k\mu_N}(\mathrm{SL}_2(\mathbb{Z}))$ y satisface

$$\mathrm{ord}(\psi) \geq \mathrm{ord}(\varphi) = \mathrm{ord}(f-g) > \frac{k\mu_N}{12}.$$

Aplicamos el lema anterior para ψ y obtenemos que necesariamente $\psi = 0$, por lo que $\varphi = 0$ y, en consecuente, $f = g$. □

Corolario 5.2.1: Si $f, g \in \mathcal{S}_k(\Gamma_0(N))$ son *newforms* y $a_p(f) = a_p(g)$ para todo primo $p \leq k\mu_N/12$, entonces $f = g$.

DEMOSTRACIÓN: La razón es que simple y llanamente los coeficientes $a_n(f)$ coinciden con $a_1(T(n)(f))$, donde $T(n)$ denota el n-ésimo operador de Hecke. Como el álgebra de Hecke está generada (como álgebra) por los $T(p)$, vemos que $T(n)$ es un polinomio en los $T(p)$ con $p \leq n$, de modo que $a_n(f)$ es un polinomio en términos de los $a_p(f)$ con $p \leq n$ y aplicamos la cota de Sturm. □

Esta cota, sin embargo, se puede mejorar sustancialmente, para lo cual requerimos el siguiente resultado:

Teorema 5.3 (Asai): Sea $N \geq 1$ un entero libre de cuadrados, sea $N = ab$ y sean u, v tales que $ua + vb = 1$. Denotemos

$$\omega_b := \begin{bmatrix} 1 & 0 \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} vb & u \\ -a & 1 \end{bmatrix}.$$

Sea $f \in \mathcal{S}_k(\Gamma(N))$ una *newform*, entonces $f|_k\omega = \lambda f$, donde

$$\lambda = \prod_{q|b} (-q^{1-k/2}) \overline{a}_q(f) \in \mathbb{C}^\times. \tag{5}$$

DEMOSTRACIÓN: Cfr. Thm. 1 de ASAI **[1]**. □

Teorema 5.4: Sea N libre de cuadrados. Sean $f, g \in \mathcal{S}_k(\Gamma_0(N))$ un par de *newforms*, sea $I := \{p_1, \ldots, p_r\}$ un conjunto de factores primos de N. Supongamos que:

1. $a_p(f) = a_p(g)$ para todo primo $p \leq k\mu_N/(12 \cdot 2^r)$.
2. $a_{p_j}(f) = a_{p_j}(g)$ para todo $1 \leq j \leq r$.

Entonces $f = g$.

DEMOSTRACIÓN: Sean $1 = b_1 < b_2 < \cdots < b_d = N$ todos los divisores positivos de N y sean $\omega_j := \omega_{b_j}$, al igual que en el enunciado anterior. Para b_j fijo y $0 \leq t \leq b_j$,

definamos

$$\gamma_j^{(t)} := \omega_j^{-1} \cdot \begin{bmatrix} 1 & t \\ 0 & b_j \end{bmatrix},$$

de modo que tenemos la descomposición

$$\Gamma(1) = \bigcup_{j=1}^{d} \bigcup_{t=0}^{b_j-1} \Gamma_0(N)\gamma_j^{(t)}$$

en clases laterales disjuntas. Definamos $\tilde{f}_j := f|_k\omega_j$ y $\tilde{g}_j := g|_k\omega_j$. Consideramos entonces

$$\varphi := \prod_{j=1}^{d} \prod_{t=0}^{b_j-1} (\tilde{f}_j - \tilde{g}_j)|_k\gamma_j^{(t)}.$$

Por el teorema de Asai, cada $\tilde{f}_j(z) = \lambda_j(f)f(z)$, donde $\lambda_j(f) = \lambda_j(g)$ cuando $b_j \mid p_1 \cdots p_r$ (por la fórmula (5)), de modo que $\operatorname{ord}(\tilde{f}_j - \tilde{g}_j) = \operatorname{ord}(f_j - g_j)$ para estos índices. Nótese que hay 2^r divisores de $p_1 \cdots p_r$, de modo que

$$\operatorname{ord}(\varphi) = 2^r \operatorname{ord}(f - g) > \frac{k\mu_N}{12},$$

y concluimos por la cota de Sturm. □

Observación 5.4.1: En el trabajo original de Sturm, él tuvo que trabajar bastantes detalles adicionales. La razón es que su teorema no involucra igualdad, sino *congruencia*, para lo cual debe exigir que los coeficientes de f y g sean enteros algebraicos sobre un cuerpo numérico $K(\zeta_N)$ y elegir adecuadamente ideales primos $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_K)$, además de invocar teoremas sobre la teoría de Galois de las *newforms* expuestas en §6.1 de **[10].**

Además de ello, otra complicación es que el teorema anterior y el de Asai traen consigo modificaciones de un caracter de Dirichlet; nosotros limpiamos los enunciados con el caracter principal.

Un ejemplo. Ya con esto podemos escribir un programa en `Sage` que, dada una curva elíptica E con conductor N libre de cuadrados (para poder emplear la cota de Sturm 5.4) calcule los coeficientes a_p para todos los primos de mala reducción:

```
from sage.all import *
from sage.modular.dims import dimension_cusp_forms

def countpoint(a1, a2, a3, a4, a6, p): # contar puntos de curva en 𝔽_p
  total = 1 # Comienza por el punto al infinito
  for (x, y) in [ (x,y) for x in range(0, p) for y in range(0, p) ]:
    if (x**3 + a2*x**2 + a4*x + a6 - (y**2 + a1*x*y + a3*y)) % p == 0:
      total += 1
  return total

def Fourier(a1, a2, a3, a4, a6):
    E = EllipticCurve([a1,a2,a3,a4,a6])
    N = E.conductor()
    primos_malos = [ f[0] for f in factor(N) ]
    sturm_cota = N/6 * prod([ 1/2*(1 + 1/p) for p in primos_malos])
    coeficientes = []
```

```
    for p in primos_malos:
        if p == 2:
            ap = 1 if countpoint(a1,a2,a3,a4,a5,a6,p) == 2 else -1
            coeficientes.append((2, ap))
        else:
            b2 = a1**2 + 4*a2
            b4 = a1*a3 + 2*a4
            b6 = a3**2 + 4*a6
            c4 = b2**2 - 24*b4
            c6 = -b2**3 + 36*b2*b4 - 216*b6
            ap = kronecker(-c4*c6, p) # Símbolo de Legendre
            coeficientes.append((p, ap))
    for p in [ q for q in range(2, int(sturm_cota)+1) if q in Primes() ]:
        if p in primos_malos:
            continue
        ap = 1 + p - countpoint(a1,a2,a3,a4,a6,p)
        coeficientes.append((p, ap))
    return coeficientes
```

Considere las curvas

$$E_1: \quad y^2+y=x^3+x \qquad (\texttt{91.a1}),$$
$$E_2: \quad y^2+y=x^3+x^2-7x+5 \qquad (\texttt{91.b2}),$$
$$E_3: \quad y^2+y=x^3+x^2+13x+42 \qquad (\texttt{91.b3}),$$

las cuales tienen todas conductor $N=7\cdot 13=91$. Se calcula que $g(X_0(91))=7$ y se verifica que $\mathcal{S}_2^{\text{old}}(\Gamma_0(91))=0$ (¿por qué?). Así que hay 7 clases de isogenia de curvas elípticas de conductor 91, por lo que el método anterior no aplica; no obstante, el código calcula:

E	a_7	a_{13}	a_2	a_3
91.a1	-1	-1	-2	0
91.b2	1	1	0	-2
91.b3	1	1	0	-2

Así, concluimos que E_2 y E_3 son isógenas entre sí, pero no son isógenas a E_1.

6. Modularidad, otra vez

Si el lector investiga acerca del «teorema de modularidad» rápidamente encontrará una variedad de enunciados que pueden no estar relacionados de manera aparente. Aquí explicaremos un poco la relación entre ellos.

Formalmente, para nosotros, el resultado es el siguiente:

Teorema 6.1 (Wiles [13]): Para toda curva elíptica E sobre $\mathbb{Q}$ existe un morfismo no constante $\phi\colon X_0(N)\to E$ definido sobre $\mathbb{Q}$.

A estos morfismos se les llaman ***parametrizaciones modulares*** y siempre podemos elegir una con grado minimal, al que denotaremos (con cierto abuso de notación) por $\deg(\phi_E)$, llamado el ***grado modular***. A una parametrización que alcance dicho grado le llamaremos ***minimal***.

Daremos una breve indicación de cómo este resultado se relaciona con el anterior: considere una parametrización modular $\phi\colon X_0(N) \to E$, donde en principio éste N puede ser distinto del conductor de E (*a posteriori,* probaremos que N debe ser un múltiplo del conductor y hay igualdad si la parametrización es minimal). En E podemos tomar un diferencial no nulo ω_E, más explícitamente, si

$$E\colon \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{6}$$

podemos tomar

$$\omega_E := \frac{\mathrm{d}x}{2y + a_1x + a_3}. \tag{7}$$

Entonces su pullback $\phi^*\omega_E$ es un diferencial holomorfo en $X_0(N)$, en consecuencia, es de la forma $f(\tau)\,\mathrm{d}\tau$ para una forma cuspidal $f \in \mathcal{S}_2(\Gamma_0(N))$ de peso 2. Uno puede probar entonces que existe $c_\phi \in \mathbb{Q}^\times$ tal que $a_p(f) = c_\phi a_p(E)$ para todo $p \nmid N_E N$ y, por un argumento de Carayol, de hecho la igualdad se da para todos los primos p.

Como f_E se definía de modo que

$$L(s, f_E) = \sum_{n=1}^{\infty} a_n q^n = \prod_p \frac{1}{1 - a_p p^{-s} + \chi(p)p^{1-2s}},$$

entonces $f = f_E$ ha de ser una *newform* de nivel N_E por **[10],** Thm. 3.43. Esto prueba que ϕ se factoriza $X_0(N) \to X_0(N_E) \to E$. En consecuencia, una parametrización minimal tiene por dominio a la curva modular de nivel N_E. Los detalles están rellenos en **[5],** §8.8 y las referencias allí contenidas.

Definición 6.2: Sea E una curva elíptica sobre $\mathbb{Q}$ dada por una ecuación de Weierstrass minimal (6). Su ***diferencial de Néron*** es, entonces, (7). Este es único salvo signo.

Lema 6.3: Sea ω_E el diferencial de Néron de una curva elíptica E sobre $\mathbb{Q}$ y sea $\phi_E\colon X_0(N) \to E$ una parametrización minimal. El pullback $\phi_E^*\omega_E$ es de la forma $c_E f_E(\tau)d\tau$, donde $c_E \in \mathbb{Q}^\times$ y f_E es la *newform* asociada a la curva elíptica E.

Desde ahora en adelante, E denotará una curva elíptica sobre $\mathbb{Q}$ con parametrización modular minimal $\phi\colon X_0(N) \to E$. La relación entre formas modulares y el grado modular está dada por la siguiente fórmula:

Proposición 6.4: $|c_E|^2 \, \|f_E\|^2 = \deg\phi \,\mathrm{Vol}(E_f)$.

Demostración: Como $\mathrm{d}x \wedge \mathrm{d}y = \frac{1}{2\mathrm{i}}(\mathrm{d}\tau \wedge \overline{\mathrm{d}\tau})$, basta calcular

$$\begin{aligned}
|c_E|^2\|f\|^2 &= -\frac{1}{2\mathrm{i}} \int_{X_0(N)} c_E f(\tau)\,\mathrm{d}\tau \wedge \overline{c_E f(\tau)\,\mathrm{d}\tau} \\
&= \frac{\mathrm{i}}{8\pi^2} \int_{X_0(N)} (2\pi\mathrm{i} c_E f(\tau)\,\mathrm{d}\tau) \wedge \overline{(2\pi\mathrm{i} c_E f(\tau)\,\mathrm{d}\tau)} \\
&= \frac{\mathrm{i}}{8\pi^2} \int_{X_0(N)} \phi^*(\mathrm{d}z) \wedge \overline{\phi^*(\mathrm{d}z)} \\
&= \frac{\mathrm{i}}{8\pi^2} \deg(\phi) \int_E \mathrm{d}z \wedge \overline{\mathrm{d}z} = \frac{\mathrm{i}}{4\pi^2} \deg(\phi)\,\mathrm{Vol}(E).
\end{aligned}$$

□

Donde aquí $\mathrm{Vol}(E)$ denota el área fundamental del reticulado Λ tal que $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ (bianalíticamente).

7. Cómo calcular el grado modular

En la siguiente sección, nos daremos un método, de Zagier [**14**] (mediante la exposición de Cremona [**4**]).

Definición 7.1: Sea $f \in \mathcal{S}_2(\Gamma)$ una forma cuspidal para un grupo modular Γ. Definimos

$$\varphi_1(z) := 2\pi\mathrm{i} \int_\infty^z f(\zeta)\,\mathrm{d}\zeta,$$

lo que determina $\varphi_1 \colon \mathfrak{H} \to \mathbb{C}$.

Sea $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma_0(N)$ y $z \in \mathfrak{H}^*$, entonces

$$\begin{aligned} \frac{\mathrm{d}}{\mathrm{d}z}\left(2\pi\mathrm{i}\int_z^{\gamma\cdot z} f(\zeta)\mathrm{d}\zeta\right) &= 2\pi\mathrm{i}\left(f(\gamma\cdot z)\frac{\mathrm{d}(\gamma\cdot z)}{\mathrm{d}z} - f(z)\right) \\ &= 2\pi\mathrm{i}\left((cz+d)^2 f(z)(cz+d)^{-2} - f(z)\right) = 0, \end{aligned}$$

de modo que la diferencia $\varphi_1(\gamma\cdot z) - \varphi_1(z)$ no depende del punto base z. Con ello damos la siguiente...

Definición 7.2: Para cada $\gamma \in \Gamma_0(N)$ definimos la función

$$\omega(\gamma) := \varphi_1(\gamma\cdot z) - \varphi_1(z) = 2\pi\mathrm{i}\int_z^{\gamma\cdot z} f(\zeta)\,\mathrm{d}\zeta, \qquad z \in \mathfrak{H}^*.$$

Además ω es un homomorfismo de grupos de $\Gamma_0(N)$ a $\mathbb{C}$.

Desde ahora en adelante, supondremos que $\Gamma_0(N)$ no contiene conjugados de S, TS ni $(TS)^2$.

Fijemos un conjunto $\mathcal{R} \subseteq \Gamma(1)$ de representantes para $\Gamma_0(N) \setminus \Gamma(1)$ tal que si $\gamma \in \mathcal{R}$, entonces también $\gamma TS \in \mathcal{R}$. Para cada $\gamma \in \mathcal{R}$, descompongamos (de forma única) $\gamma S = s(\gamma)\sigma(\gamma)$ donde $s(\gamma) \in \Gamma_0(N)$ y $\sigma(\gamma) \in \mathcal{R}$, de modo que $\sigma \colon \mathcal{R} \to \mathcal{R}$ determina una permutación.

Similarmente hacemos lo mismo para $\gamma T = t(\gamma)\tau(\gamma)$, donde $t(\gamma) \in \Gamma_0(N)$ y $\tau(\gamma) \in \mathcal{R}$. En cada órbita de τ de largo k, elijamos un punto base $\gamma_1 \in \mathcal{R}$ y sea $\gamma_{j+1} := \tau^j(\gamma_1)$. Denotamos $\alpha \prec \beta$ si están en la misma τ-órbita y $\alpha = \gamma_i, \beta = \gamma_j$ con $1 \le i < j < k$. Necesitaremos los siguientes cálculos chicos:

Lema 7.3: Para $\gamma \in \mathcal{R}$, se tiene:

1. $s(\sigma(\gamma)) = s(\gamma)^{-1}$.
2. $s(\gamma TS) = t(\gamma)$.

Demostración:

1. Esto es debido a que
$$\gamma = \gamma S \cdot S = s(\gamma)\sigma(\gamma)S = s(\gamma)s(\sigma(\gamma))\sigma^2(\gamma),$$
y como la descomposición es única, vemos que $\sigma^2(\gamma) = \gamma \in \mathcal{R}$ y $s(\gamma)s(\sigma(\gamma)) = 1 \in \Gamma_0(N)$.

2. Tenemos que $t(\gamma)\tau(\gamma) = \gamma T = (\gamma TS)S = s(\gamma TS)\sigma(\gamma TS)$, pues $\gamma TS \in \mathcal{R}$. Por tanto, por unicidad, $t(\gamma) = s(\gamma TS)$. □

También denotaremos por $\gamma_0 \in \mathcal{R}$ al (único) representante de la clase trivial $\Gamma_0(N)$.

Lema 7.4: $\omega(\gamma_0) = 0$.

Demostración: El elemento $\gamma_0 \in \Gamma_0(N)$ fija a algún punto $z \in \mathfrak{H}^*$. Si ese punto fuese *elíptico* (i.e., estuviese en $\mathfrak{H}$), entonces $z = \sigma \cdot \mathrm{i}$ o $z = \sigma \cdot \zeta_3$ para algún $\sigma \in \Gamma(1)$. Note que $\gamma_0\sigma z_0 = \sigma z_0$ (con $z_0 \in \{\mathrm{i}, \zeta_3\}$) implica entonces $\sigma^{-1}\gamma_0\sigma$ está en el estabilizador de i o ζ_3, es decir, es $\pm S, \pm TS$ ó $\pm(TS)^2$. Pero dijimos que $\Gamma_0(N)$ no contiene tales conjugaciones, así que γ_0 fija a una cúspide z y

$$\omega(\gamma_0) = \varphi_1(\gamma_0 \cdot z) - \varphi_1(z) = 0. \qquad \square$$

Lema 7.5: Se tiene $\sum_{j=1}^{k} \omega(t(\gamma_j)) = 0$. donde la suma es sobre la órbita completa de γ_1.

Demostración: Basta notar que

$$\gamma_1 T^k = t(\gamma_1)t(\tau(\gamma_1)) \cdots t(\tau^{k-1}(\gamma_1))\tau^k(\gamma_1) = \gamma_0\gamma_1$$

donde $\gamma_0 = t(\gamma_1)t(\tau(\gamma_1)) \cdots t(\tau^{k-1}(\gamma_1)) \in \Gamma_0$ y $\tau^k(\gamma_1) = \gamma_1$. Así concluimos por el lema anterior. □

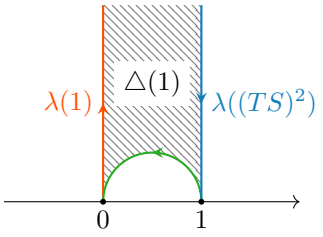
Teorema 7.6: Sea $f \in \mathcal{S}_2(\Gamma_0(N))$ con función de periodos $\omega\colon \Gamma_0(N) \to \mathbb{C}$, entonces

$$\|f\|^2 = \frac{1}{8\pi^2} \sum_{\alpha \prec \beta} \mathrm{Im}\big(\omega(t(\alpha))\overline{\omega(t(\beta))}\big),$$

donde la suma recorre todos los pares $(\alpha, \beta) \in \mathcal{R} \times \mathcal{R}$ que pertenecen a la misma τ-órbita.

Demostración: Considere, como dominio fundamental de $\Gamma(1) \curvearrowright \mathfrak{H}$ el triángulo (geodésico) Δ con vértices en 0, $\xi := \zeta_3$ e $\mathrm{i}\infty$. Si $\mathcal{R}' \subseteq \mathcal{R}$ denota un conjunto que contenga a exactamente un elemento de la terna $\{\gamma, \gamma TS, \gamma(TS)^2\}$ para cada γ, entonces un dominio fundamental para $\Gamma_0(N)$ es

$$\mathfrak{F}_N := \bigcup_{\gamma \in \mathcal{R}'} \triangle(\gamma),$$



donde $\triangle(\gamma)$ tiene por vértices a $\gamma(0)$, $\gamma(\infty)$ y $\gamma(1)$.
También denotaremos por $\partial\triangle(\gamma)$ a las aristas orientadas según el orden anterior. Note que como $\partial\triangle(TS) = [\infty, 1, 0]$, entonces definiendo $\lambda(\gamma) := [\gamma(0), \gamma(\infty)]$ como el camino en $\mathfrak{H}^*$, entonces

$$\partial\triangle(\gamma) = \lambda(\gamma) + \lambda(\gamma TS) + \lambda(\gamma(TS)^2).$$

Ahora calculamos

$$\begin{aligned}\|f\|^2 &= \frac{\mathrm{i}}{2}\int_{\mathfrak{F}_N} f(z)\overline{f(z)}\,\mathrm{d}z\wedge\overline{\mathrm{d}z} = \frac{1}{4\pi}\int_{\mathfrak{F}_N}\mathrm{d}\big(\varphi_1(z)\overline{f(z)\,\mathrm{d}z}\big)\\ &= \frac{1}{4\pi}\int_{\partial\mathfrak{F}_N}\varphi_1(z)\overline{f(z)\,\mathrm{d}z} = \frac{1}{4\pi}\sum_{\gamma\in\mathcal{R}'}\int_{\partial\triangle(\gamma)}\varphi_1(z)\overline{f(z)\,\mathrm{d}z}\\ &= \frac{1}{8\pi}\sum_{\gamma\in\mathcal{R}}\left(\int_{\lambda(\gamma)}\varphi_1(z)\overline{f(z)\,\mathrm{d}z}+\int_{\lambda(\sigma(\gamma))}\varphi_1(z)\overline{f(z)\,\mathrm{d}z}\right).\end{aligned}$$

Trabajaremos el término de la derecha, para ello note que, como f tiene peso 2, el diferencial $f(z)\,\mathrm{d}z$ es invariante bajo $\Gamma_0(N)$, de modo que

$$\begin{aligned}\int_{\lambda(\sigma(\gamma))}\varphi_1(z)\overline{f(z)\,\mathrm{d}z} &= \int_{\lambda(s(\gamma)^{-1}\gamma S)}\varphi_1(z)\overline{f(z)\,\mathrm{d}z}\\ &= \int_{\lambda(\gamma S)}\varphi_1(s(\gamma)z)\overline{f(z)\,\mathrm{d}z},\end{aligned}$$

y empleamos que $\lambda(S)=[\infty,0]=-\lambda(1)$ es el camino
con orientación inversa para ver que

$$= -\int_{\lambda(\gamma)}\varphi_1(s(\gamma)z)\overline{f(z)\,\mathrm{d}z}.$$

Así

$$\|f\|^2 = \frac{1}{8\pi}\sum_{\gamma\in\mathcal{R}}\int_{\lambda(\gamma)}\big(\varphi_1(z)-\varphi_1(s(\gamma)z)\big)\overline{f(z)\,\mathrm{d}z} = \frac{1}{8\pi}\sum_{\gamma\in\mathcal{R}}\omega(s(\gamma))\int_{\lambda(\gamma)}\overline{f(z)\,\mathrm{d}z}.$$

La última integral viene dada por

$$\int_{\lambda(\gamma)}f(z)\,\mathrm{d}z = \int_{\gamma(0)}^{\gamma(\infty)}f(z)\,\mathrm{d}z = \frac{1}{2\pi\mathrm{i}}\big(\varphi_1(\gamma(\infty))-\varphi_1(\gamma(0))\big),$$

como está conjugado, vemos que

$$\|f\|^2 = \frac{-\mathrm{i}}{16\pi^2}\sum_{\gamma\in\mathcal{R}}\omega(s(\gamma))\overline{\big(\varphi_1(\gamma(\infty))-\varphi_1(\gamma(0))\big)}.$$

Esta suma es finita y, para calcularla, aplicamos σ:

$$\begin{aligned}\sum_{\gamma\in\mathcal{R}}\omega(s(\gamma))\overline{\varphi_1(\gamma(\infty))} &= \sum_{\gamma\in\mathcal{R}}\omega(s(\sigma(\gamma)))\overline{\varphi_1(\sigma(\gamma)(\infty))}\\ &= -\sum_{\gamma\in\mathcal{R}}\omega(s(\gamma))\overline{\varphi_1(\sigma(\gamma)(\infty))}\\ &= -\sum_{\gamma\in\mathcal{R}}\omega(s(\gamma))\overline{\varphi_1(s(\gamma)^{-1}\gamma(0))}\\ &= -\sum_{\gamma\in\mathcal{R}}\omega(s(\gamma))\overline{\big(\varphi_1(\gamma(0))-\omega(s(\gamma))\big)}\\ &= -\sum_{\gamma\in\mathcal{R}}\omega(s(\gamma))\overline{\varphi_1(\gamma(0))}+\sum_{\gamma\in\mathcal{R}}|\omega(s(\gamma))|^2;\end{aligned}$$

donde la segunda igualdad viene del lema 7.3 y la tercera de que $\sigma(\gamma)=s(\gamma)^{-1}\gamma S$.

Como $\|f\|^2 \in \mathbb{R}$ es real, vemos que $\|f\|^2 = \operatorname{Re}\|f\|^2$ y

$$\|f\|^2 = \frac{-1}{8\pi^2}\operatorname{Im}\left(\sum_{\gamma\in\mathcal{R}} \omega(s(\gamma))\overline{\varphi_1(\gamma(0))}\right).$$

Finalmente, como $\gamma TS \in \mathcal{R}$ para todo $\gamma \in \mathcal{R}$, vemos que multiplicar por TS es una permutación y

$$\|f\|^2 = \frac{-1}{8\pi^2}\operatorname{Im}\left(\sum_{\gamma\in\mathcal{R}} \omega(s(\gamma TS))\overline{\varphi_1(\gamma(\infty))}\right) = \frac{-1}{8\pi^2}\operatorname{Im}\left(\sum_{\gamma\in\mathcal{R}} \omega(t(\gamma))\overline{\varphi_1(\gamma(\infty))}\right).$$

Si ahora particionamos por τ-órbitas de largo k, podemos desarrollar la sumatoria empleando el lema 7.5:

$$\begin{aligned}\sum_{j=1}^{k} \omega(t(\gamma_j))\overline{\varphi_1(\gamma_j(\infty))} &= \sum_{j=1}^{k} \omega(t(\gamma_j))\overline{\big(\varphi_1(\gamma_j(\infty)) - \varphi_1(\gamma_1(\infty))\big)} \\ &= \sum_{j=1}^{k}\sum_{i=1}^{j-1} \omega(t(\gamma_j))\overline{\big(\varphi_1(\gamma_{i+1}(\infty)) - \varphi_1(\gamma_i(\infty))\big)}\end{aligned}$$

empleando que $T\cdot\infty = \infty$ y que $\gamma_i T = t(\gamma_i)\gamma_{i+1}$ tenemos

$$\begin{aligned}&= \sum_{j=1}^{k} \omega(t(\gamma_j)) \sum_{i=1}^{j-1} \overline{\big(\varphi_1(\gamma_{i+1}(\infty)) - \varphi_1(t(\gamma_i)\gamma_{i+1}(\infty))\big)} \\ &= -\sum_{1\le j<i\le k} \omega(t(\gamma_j))\omega(t(\gamma_i)).\end{aligned}$$

Esto corresponde a una sumatoria con índice $\gamma_j \prec \gamma_i$ de la misma τ-órbita. Sumando sobre todas ellas, se sigue el enunciado. □

Aplicando el teorema anterior con la proposición 6.4 se concluye lo siguiente:

Corolario 7.6.1: Para una curva elíptica E sobre $\mathbb{Q}$ se tiene

$$\deg\phi_E = \frac{1}{2\operatorname{Vol}(E)}\sum_{\alpha\prec\beta} \operatorname{Im}\left(\omega(t(\alpha))\overline{\omega(t(\beta))}\right),$$

donde la función ω es aquella asociada a $c_E f_E$.

Gracias a éste trabajo, se tiene que el grado modular se define a través de elementos calculables. Específicamente, las integrales y el volúmen pueden aproximarse: la primera mediante sumas de Riemann y la segunda mediante el método de las tangentes para encontrar la preimagen mediante la función j analítica.

Agradecimientos

Agradezco a Rocío Sepúlveda-Manzo y a Daniel Rodríguez con quiénes escribimos en conjunto los informes. Este trabajo estuvo arduamente inspirado en ellos, aunque especialmente agradezco a Rocío ya que toda la sección 2 fue de su pluma, por mostrarme también el teorema de Faltings-Tate mencionado en §4, por el código en `Sage` para el ejemplo en §5, y por enseñarme el artículo [**4**] y co-escribir §7.

Los autores agradecen al profesor Héctor Pastén por la sugerencia de la proposición 1.9 para identificar el tipo de reducción en característica 2.

Referencias

1. Asai, T. On the Fourier coefficients of automorphic forms at various cusps and some applications to Rankin's convolution. *J. Math. Soc. Japan* **28,** 48-61. doi:10.2969/jmsj/02810048 (1976).
2. Breuil, C., Conrad, B., Diamond, F. y Taylor, R. On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises. *J. Amer. Math. Soc.* **14,** 843-939. doi:10.1090/S0894-0347-01-00370-8 (2001).
3. Connell, I. *Elliptic Curve Handbook* (1999).
4. Cremona, J. E. Computing the Degree of the Modular Parametrization of a Modular Elliptic Curve. *Math. Comput.* **64,** 1235-1250. doi:10.2307/2153493 (1995).

Stacks. De Jong, A. J. *et al. Stacks project* https://stacks.math.columbia.edu/.

5. Diamond, F. y Shurman, J. *A First Course in Modular Forms Graduate Texts in Mathematics* **228** (Springer-Verlag, 2010).
6. Görtz, U. y Wedhorn, T. *Schemes. With Examples and Exercises* 2.ª ed. (Springer Spektrum Wiesbaden, 2010).
7. Husemöller, D. *Elliptic Curves Graduate Texts in Mathematics* **111** (Springer-Verlag, 2004).
8. Miranda, R. *Algebraic curves and Riemann surfaces* (Amer. Math. Soc., 1995).
9. Schappacher, N. *Tate's conjecture on the endomorphisms of abelian varieties* en *Rational Points. Seminar Bonn-Wuppertal 1983/84* (eds. Faltings, G. y Wüstholz, G.) **E6** (Springer Fachmedien Wiesbaden, Bonn, 1984), 114-153.
10. Shimura, G. *Introduction to Arithmetic Theory of Automorphic Functions* (Princeton Univ. Press, 1971).
11. Silverman, J. H. *The arithmetic of elliptic curves* 2.ª ed. (Springer-Verlag, 2009).
12. Sturm, J. *On the congruence of modular forms* en *Number Theory* (eds. Chudnovsky, D., Chudnovsky, G., Cohn, H. y Nathanson, M.) (Springer-Verlag, 1987), 275-280.
13. Wiles, A. Modular Elliptic Curves and Fermat's Last Theorem. *Ann. Math.* **141,** 443-551. doi:10.2307/2118559 (1995).
14. Zagier, D. Modular parametrizations of elliptic curves. *Canad. Math. Bull.* **28,** 372-384. doi:10.4153/CMB-1985-044-8. https://doi.org/10.4153/CMB-1985-044-8 (1985).

Departamento de Matemáticas, Pontificia Universidad Católica de Chile. Facultad de Matemáticas, 4860 Av. Vicuña Mackenna, Macul, RM, Chile
Correo electrónico, J. C.B.: josecuevasbtos@uc.cl
URL, J. C.B.: josecuevas.xyz

Departamento de Matemáticas, Pontificia Universidad Católica de Chile. Facultad de Matemáticas, 4860 Av. Vicuña Mackenna, Macul, RM, Chile
Correo electrónico, R. S.-M.: rseplveda@uc.cl
URL, R. S.-M.: rseplveda.xyz