Cómo reconocer curvas elípticas isógenas

José Cuevas Barrientos, con aportes de Rocío Sepúlveda-Manzo

Resumen. Este fue originalmente un informe para un curso acerca de formas modulares dictado por Héctor Pastén. En él se presentan aplicaciones de la teoría de formas modulares, mediante el teorema de modularidad de Taylor-Wiles y un teorema de Serre-Faltings, a la clasificación de curvas elípticas salvo isogenia.

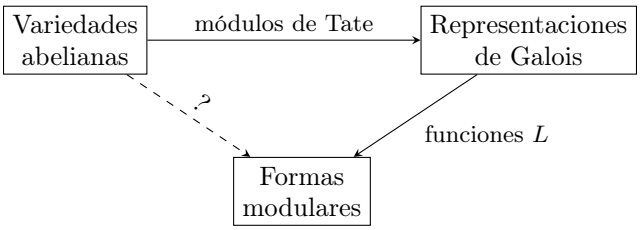
Introducción

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. 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:

Fecha: 26 de septiembre de 2024.



La conjetura de Shimura-Taniyama-Weil afirmaba precisamente que f_E es modular. Fue probada para curvas elípticas sobre $\mathbb{Q}$ *semiestables* por Taylor, Wiles y otros; lo que bastó para demostrar el último teorema de Fermat, pero un par de años más tarde fue probada en completa generalidad. El punto de este trabajo es probar que este teorema ofrece la posibilidad de calcular curvas elípticas salvo isogenia.

1. Isogenias

Vamos a hacer un breve recuento de la teoría de curvas elípticas, el lector puede consultar a Silverman **[6].** 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.

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.

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 $\ell = p = \mathrm{car}\, k > 0$, 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. □

2. Cómo asociarle una forma modular a una curva elíptica

Sea E una curva elíptica sobre un cuerpo numérico K. Recordemos que se dice que E tiene buena reducción en un primo $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ si existe una ecuación de Weierstrass para E/K que tiene coeficientes enteros y, al hacer reducción módulo $\mathfrak{p}$, determina una curva elíptica sobre $\Bbbk(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$. Los distintos tipos de reducción en un primo están detallados en **[6].**

Definición 2.1: La función L de una curva elíptica $E/\mathbb{Q}$ está dada por el producto de Euler

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

donde $\chi(p)$ es 0 si E tiene mala reducción en p, y 1 de otra forma. Para primos de buena reducción en E (los cuales son todos salvo finitos), se tiene que $a_p := p + 1 - |E_p(\mathbb{F}_p)|$, donde E_p se refiere a la reducción de E módulo p. Para primos de mala reducción en E, se tiene

$$L_p(p^{-s}) = \begin{cases} 1 & \text{si } E \text{ tiene reducción aditiva en } p, \\ 1 - p^{-s} & \text{si } E \text{ tiene reducción multiplicativa escindida en } p, \\ 1 + p^{-s} & \text{si } E \text{ tiene reducción multiplicativa no escindida en } p. \end{cases}$$

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

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

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

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 $M \mid N$) Diremos que una forma cuspidal $f \in \mathcal{S}_k(\Gamma_0(N))$ es *vieja* si pertenece al subespacio $\mathcal{S}_k(\Gamma_0(M))$ para algún $M < N$ que divida a N. Las formas viejas en $\mathcal{S}_k(\Gamma_0(N))$ generan un subespacio $\mathcal{S}_k^{\mathrm{old}}(\Gamma_0(N))$, y 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 $\mathcal{S}_k^{\mathrm{new}}(\Gamma_0(N))$ cuyos elementos se llaman *newforms*.

Definición 2.2: 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 $\mathrm{Re}(s) > 1 + k/2$.

Teorema 2.3: Sea $f \in \mathcal{S}_k^{\mathrm{new}}(\Gamma_0(N))$. La función L se puede escribir como el producto de Euler

$$L(f,s) = \prod_p (1 - a_p p^{-s} + \chi(p) p^{k-1} p^{-2s})^{-1}, \tag{3}$$

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

Si reemplazamos $k = 2$ en las ecuaciones (1) y (3), 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* $f \in \mathcal{S}_k^{\mathrm{new}}(\Gamma_0(N))$ 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 $p \mid \Delta_{\mathrm{mín}}(E)$.

Esto conlleva a conjeturar lo siguiente:

Teorema 2.4 (de modularidad): Para toda curva elíptica $E/\mathbb{Q}$, la función f_E definida en (2) es una *newform* de peso 2 y de nivel $\Gamma_0(N)$.

DEMOSTRACIÓN: La demostración completa está en el artículo de BREUIL *et al.* **[1]** que se construye sobre ideas de Frey, Serre, Ribet y Wiles. □

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 $\mathrm{SL}_2(\mathbb{Z})$, 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 **[5,** 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 **[3]**), 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 $\gamma_{j_1} \equiv \gamma_{j_2} \pmod{\Gamma}$. 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: $d = [\Gamma(1) : \Gamma_0(N)] = N \prod_{p|N} \left(1 + \frac{1}{p}\right)$.

Demostración: Esto es un mero ejercicio de teoría de grupos guiado en Diamond y Shurman [**2,** 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

$$\begin{bmatrix} ua' \\ c' \end{bmatrix} \equiv \begin{bmatrix} a + jc \\ uc \end{bmatrix} \pmod{N}.$$

Estas equivalencias están probadas en los lemas 3.8.1 y 3.8.3 de **[2]**. 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 [4]. □

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').

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, $a_3(E_3) = 3$.

Agradecimientos

Agradezco a Rocío Sepúlveda-Manzo y a Daniel Rodriguez con quiénes escribimos en conjunto el informe. Este trabajo estuvo arduamente inspirado en tal, aunque especialmente agradezco a Rocío ya que toda la sección 2 fue de su pluma, y por mostrarme también el teorema de Faltings-Tate mencionado en la última sección.

Referencias

1. 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).

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

2. Diamond, F. y Shurman, J. *A First Course in Modular Forms Graduate Texts in Mathematics* **228** (Springer-Verlag, 2010).
3. Miranda, R. *Algebraic curves and Riemann surfaces* (Amer. Math. Soc., 1995).
4. 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.
5. Shimura, G. *Introduction to Arithmetic Theory of Automorphic Functions* (Princeton Univ. Press, 1971).
6. Silverman, J. H. *The arithmetic of elliptic curves* 2.ª ed. (Springer-Verlag, 2009).

Correo electrónico, J. C.B.: josecuevasbtos@uc.cl

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

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