0.1 La irreducibilidad de $\bar{\rho}_{E,3}$ y $\bar{\rho}_{E,5}$

El popósito de esta sección es probar el siguiente teorema:

Teorema 1. *Sea $E/\mathbb{Q}$ una curva elíptica semiestable. Entonces*

$$\bar{\rho}_{E,3} \text{ es reducible} \quad \Longrightarrow \quad \bar{\rho}_{E,5} \text{ es irreducible.}$$

Este teorema permite reducir STW a dos casos: podemos asumir que $\bar{\rho}_{E,3}$ es irreducible o que es $\bar{\rho}_{E,5}$ irreducible. Para hacer esto necesitamos calcular propiedades específicas de dos curvas modulares: $X_0(15)$ y $X_0(50)$. Afortunadamente Birch tiene un informe extenso de los cálculos necesarios para estudiar $X_0(50)$. Entonces seremos explítos con la curva $X_0(15)$.

En esta sección fijamos la notación $\Gamma = \Gamma_0(15)$ y $X = X_0(15)$. Primero enunciamos algunas propiedades básicas de Γ y de la curva modular asociada:

Proposición 2. *Γ tiene 4 cúspides: $0, \frac{1}{3}, \frac{1}{5}, \frac{1}{15}$ (donde $\frac{1}{15}$ es la cúspide ∞). No tiene puntos elípticos y el género de X es 1.*

Proof. Todas las afirmaciones las probamos en el ejemplo **??** salvo la descripción explícitas de las cúspides. Sea $x/y \in \mathbb{Q}$ expresado como fracción irreducible, definimos $\delta = (15, y)$. Observe que $(\frac{15}{\delta}, \frac{y}{\delta}) = 1$ y que $(x, \frac{y}{\delta}) = 1$ por hipótesis, entonces

$$\exists c, d \in \mathbb{Z} \quad \text{tales que} \quad c\tfrac{15}{\delta}x + d\tfrac{y}{\delta} = 1.$$

En particular $(c, d) = 1$.

Por el teorema de Dirichlet sobre primos en progresiones aritméticas*, podemos tomar d un primo suficientemente gande y así $(15, d) = 1$. Por lo tanto $(15c, d) = 1$ y así:

$$\exists a, b \in \mathbb{Z} \quad \text{tales que} \quad ad - 15bc = 1.$$

Por lo tanto obtenemos una matriz en Γ y así:

$$\frac{x}{y} \equiv \begin{pmatrix} a & b \\ 15c & d \end{pmatrix} \frac{x}{y} = \frac{ax + by}{15cx + dy} = \frac{ax + by}{\delta(c\frac{15}{\delta}x + d\frac{y}{\delta})} = \frac{ax + by}{\delta} \pmod{\Gamma},$$

$$\therefore \quad \frac{x}{y} \equiv \frac{x'}{\delta} \pmod{\Gamma} \quad \text{donde } \delta = (y, 15) \text{ y para alguna } x' \in \mathbb{Z}.$$

Podemos reducir el problema aun más. Como Γ contiene las matrices asociadas a las traslaciones $z \mapsto z + t$ por un entero t, tenemos que:

$$\frac{x'}{\delta} \equiv \begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix} \frac{x'}{\delta} = \frac{x' - \delta t}{\delta} \pmod{\Gamma},$$

$$\therefore \quad \frac{x'}{\delta} \equiv \frac{r}{\delta} \pmod{\Gamma} \quad \text{donde } 0 \leq r < \delta.$$

*El teorema de Dirichlet dice que para cualesquiera q y n primos relativos, existen una infinidad de números primos p que satisfacen la congruencia $p \equiv q \pmod{n}$. Seguramente hay un argumento más elemental para el caso particular de $\Gamma_0(15)$, pero el teorema de Dirichlet se puede generalizar fácilmente a cualquier $\Gamma_0(N)$.

Por lo tanto cada racional x/y es congruente módulo Γa un racional en el siguiente conjunto

$$\left\{\frac{0}{1}, \frac{1}{3}, \frac{2}{3}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}, \frac{1}{15}, \frac{2}{15}, \frac{4}{15}, \frac{7}{15}, \frac{8}{15}, \frac{11}{15}, \frac{13}{15}, \frac{14}{15}\right\}.$$

Observa que si el denominador es 15, entonces una fracción irreducible $x/15$ induce una combinación lineal $ax + 15b = 1$ para algunas $a, b \in \mathbb{Z}$. Por lo tanto

$$\frac{x}{15} \equiv \begin{pmatrix} a & b \\ -15 & x \end{pmatrix} \frac{x}{15} = \frac{ax - 15b}{-15x + 15x} = \infty \pmod{\Gamma}.$$

Por lo tanto podemos reducir el conjunto de representantes: cada racional x/y es congruente módulo Γa un racional en el siguiente conjunto

$$\left\{0, \infty, \frac{1}{3}, \frac{2}{3}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}\right\}.$$

Observe que:

$$\frac{1}{3} \equiv \begin{pmatrix} 11 & -3 \\ 15 & 4 \end{pmatrix} \frac{1}{3} = \frac{2}{3} \pmod{\Gamma} \quad \text{y} \quad \frac{1}{5} \equiv \begin{cases} \begin{pmatrix} 7 & -1 \\ 15 & -2 \end{pmatrix} \frac{1}{5} = \frac{2}{5} \\ \begin{pmatrix} -17 & 4 \\ -30 & 7 \end{pmatrix} \frac{1}{5} = \frac{3}{5} \\ \begin{pmatrix} 11 & -3 \\ 15 & -4 \end{pmatrix} \frac{1}{5} = \frac{4}{5} \end{cases} \pmod{\Gamma}$$

Por lo tanto cada racional x/y es congruente módulo Γ a un racional en el siguiente conjunto

$$\left\{0, \infty, \frac{1}{3}, \frac{1}{5}\right\}.$$

Afirmamos que este conjunto es el conjunto de cúspides de Γ. Debemos verificar que esos racionales son incongruentes dos a dos, peo aquí solamente hacemos explícitos dos relaciones porque las demás son muy similares:

$$\begin{aligned} 0 \equiv \frac{1}{3} &\implies \exists \gamma = \begin{pmatrix} a & b \\ 15c & d \end{pmatrix} \in \Gamma \text{ tal que } \tfrac{1}{3} = \gamma \tfrac{0}{1} = \tfrac{b}{d} \implies d = 3b \implies 3 \mid \det \gamma. \\ \frac{1}{3} \equiv \frac{1}{5} &\implies \exists \gamma = \begin{pmatrix} a & b \\ 15c & d \end{pmatrix} \in \Gamma \text{ tal que } \tfrac{1}{5} = \gamma \tfrac{1}{3} = \tfrac{a+3b}{15c+3d} \implies 3d = 5a - 15c + 15d \\ &\implies 5 \mid d \implies 5 \mid \det \gamma. \end{aligned}$$

Con esto terminamos la prueba. □

La figura 1 ilustra el dominio fundamental de Γ y muestra sus cuatro cúspides. Cada sección del dominio fundamental es la traslación del dominio fundamental de $\mathrm{SL}_2(\mathbb{Z})$ por un representante de los elementos de $\mathrm{SL}_2(\mathbb{Z})/\Gamma$ En el apéndice viene otra imagen del dominio fundamental donde cada sección viene etiquetada con la matriz q

Como X es una cuva elíptica, el siguiente paso es calcular una ecuación de Weierstrass. Este tema ha sido estudiado extensamente por Fricke [**?**], Newmann [**?**] y resuelto por Ligozat [**?**], alumno de Nerón, en su tesis doctoral publicada por la *Société mathématique de France*. Tenemos:

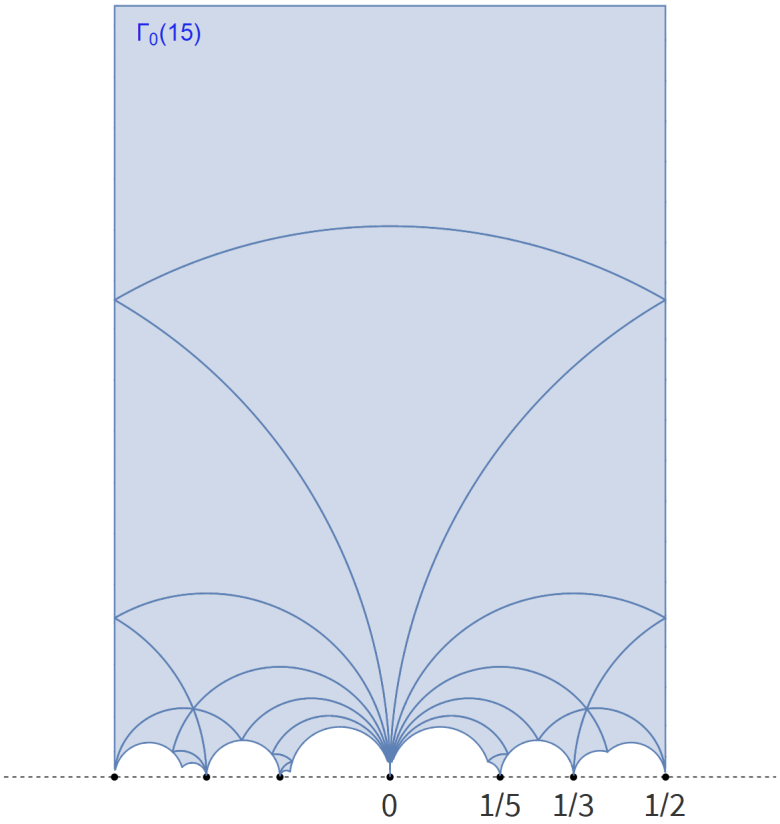

Figure 1: El dominio fundamental del subgrupo de congruencia $\Gamma_0(15)$

Proposición 3. *La curva modular elíptica $X = X_0(15)$ es tiene la ecuación de Weierstrass*

$$X: \quad y^2 + xy + y = x^3 + x^2 - 10x - 10$$

Proof. Más precisamente probamos que X es isomorfo sobre $\mathbb{Q}$ a la subvariedad proyectiva W definida por la ecuación homogenizada:

$$y^2z + xyz + yz^2 = x^3 + x^2z - 10xz^2 - 10z^3.$$

□

. Los puntos racionales no-cuspidales de la curva $X_0(15)$ corresponden a curvas elípticas E definidos sobre $\mathbb{Q}$ tales que $E(\overline{\mathbb{Q}})$ contiene un subgrupo de orden 15 estable bajo la acción natural $G_{\mathbb{Q}} \curvearrowright E(\overline{\mathbb{Q}})$. Los j-invariantes de esas curvas se pueden calcular y deducimos que todas las curvas elípticas asociadas a los puntos racionales no-cuspidales de $X_0(15)$ deben ser modulares. En particular tendríamos:

Teorema 4. *Si una curva elíptica E sobre $\mathbb{Q}$ es tal que $E(\overline{\mathbb{Q}})$ contiene un subgrupo de orden 15 estable bajo la acción de $G_{\mathbb{Q}}$, entonces E es modular.*

Antes de probar este teorema, revisamos un corolario importante:

Corolario 5. *Si E es una curva elíptica sobre $\mathbb{Q}$ tal que $\bar{\rho}_{E,3}$ y $\bar{\rho}_{E,5}$ son reducibles, entonces E es modular.*

Proof. Supongamos que $\bar{\rho}_{E,3}$ y $\bar{\rho}_{E,5}$ son reducibles. Por definición existen subespacios no triviales $V_3 \subset E[3]$ y $V_5 \subset E[5]$ que son invariantes bajo la acción de $G_{\mathbb{Q}}$. Recuerda que $\#E[N] = N^2$, entonces el orden de cualquier subgrupo divide a N^2, pero en este caso $N = 3, 5$. Por lo tanto cualquier subgrupo no-trivial de $E[3]$ (respectivamente $E[5]$) necesariamente es de orden 3 (respectivamente 5). En particular $V_i \cong \mathbb{Z}/i\mathbb{Z}$ para $i = 3, 5$ y sean P_3 un generador de V_3 y P_5 un generador de V_5. Por último, como subgrupos de $E(\overline{\mathbb{Q}})$, V_3 y V_5 tienen intersección trivial (porque los elementos distintos del neutro de V_3 tienen orden 3 y los de V_5 tienen orden 5).

Ahora definimos $V = V_3 + V_5 = \{P + P' \in E(\overline{\mathbb{Q}}) \mid P \in E[3],\ P' \in E[5]\}$. Claramente el orden de cada punto de V divide a 15 pues $15(P + P') = 5(3P) + 3(5P') = 3O + 5O = O$, es decir $V \subset E[15]$. Por otro lado el punto $P_3 + P_5$ es de orden exactamente 15 porque

$$3(P_3 + P_5) = 3P_5 \neq O \quad \text{y} \quad 5(P_3 + P_5) = 5P_3 = 2P_3 \neq O.$$

Por lo tanto V es un subgrupo de $E(\overline{\mathbb{Q}})$ de orden 15.

Por último, V es invariante bajo la acción de $G_{\mathbb{Q}}$. En efecto, sea $\sigma \in G_{\mathbb{Q}}$ arbitrario, entonces

$$(P + P')^{\sigma} = P^{\sigma} + P'^{\sigma} \in V_3 + V_5 = V$$

ya que la $G_{\mathbb{Q}}$-estabilidad de V_3 (respectivamente de V_5) implica que $P^{\sigma} \in V_3$ (respectivamente $P'^{\sigma} \in V_5$).

Por lo tanto $E(\overline{\mathbb{Q}})$ contiene un subgrupo de orden 15 estable bajo la acción de $G_{\mathbb{Q}}$. Aplicamos el teorema 3 para concluir que E es modular. □

Ahora nos enfocamos en probar el teorema 3. Para esto necesitamos estudiar las propiedades geométricas de $X_0(15)$.

En general, el grupo de congruencia $\Gamma_0(N)$ actúa sobre $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ mediante transformaciones de Möbius y el espacio cociente $\mathbb{H}^*/\Gamma_0(N)$ es una superficie de Riemann compacta que denotamos por $X_0(N)$. Esta variedad también se puede obtener compactificando el espacio $\mathbb{H}/\Gamma_0(N)$, agregándole las cúspides de la acción.

Para pobar el teorema 3 necesitamos las siguientes propiedades de $X_0(15)$ (cf. [**?**, capítulo XVI, §2, Lema 9]):

Proposición 6. *La curva modular $X_0(15)$ cumple las siguientes propiedades:*

i) *$X_0(15)$ es una curva de género 1 con cuatro cúspides racionales.*

ii) *$X_0(15)$ tiene 8 puntos racionales, ie. $\#X_0(15)(\mathbb{Q}) = 8$.*

iii) *Los cuatro puntos racionales no-cuspidales de $X_0(15)(\mathbb{Q})$ corresponden a cuatro clases de isomorfismos de parejas (E_i, C_i) donde $C_i \subset E_i(\overline{\mathbb{Q}})$ es un subgrupo de orden 15 y cuyos j-invariantes son:*

$$j(E_i) \in \left\{ -\frac{5^2}{2}, -\frac{5^2 241^3}{2^3}, -\frac{5 \cdot 29^3}{2^5}, \frac{5 \cdot 211^3}{2^{15}} \right\}$$

Proof. El género g de $X_0(N)$ se calcula con la siguiente fórmula [**?**, §1.6, proposición 1.40]:

$$g = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}$$

donde $\mu = [\mathrm{PSL}_2\mathbb{Z} : \overline{\Gamma}_0(N)]$ (aquí $\overline{\Gamma}_0(N)$ es la imagen de $\Gamma_0(N)$ bajo la proyección $\mathrm{SL}_2\mathbb{Z} \twoheadrightarrow \mathrm{PSL}_2\mathbb{Z}$), ν_2 (respectivamente ν_3) es la cantidad de clases de equivalencia (bajo la acción de $\overline{\Gamma}_0(N)$) de los puntos elípticos de orden 2 (respectivamente de orden 3) y ν_∞ es la cantidad de clases de equivalencias de puntos cúspidales.

Para calcular μ observamos que la imagen de la función

$$\Gamma_0(N) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \quad \text{definido por} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a+N\mathbb{Z} & b+N\mathbb{Z} \\ c+N\mathbb{Z} & d+N\mathbb{Z} \end{pmatrix}$$

es el conjunto de matrices de $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ de la forma:

$$\begin{pmatrix} a+N\mathbb{Z} & b+N\mathbb{Z} \\ 0 & a^{-1}+N\mathbb{Z} \end{pmatrix}.$$

Hay N posibles elecciones para tomar b y $\varphi(N)$ posibilidades para a (donde φ es la función de Euler). Por lo tanto el orden de la imagen de $\Gamma_0(N)$ es $N\varphi(N)$.

Por otro lado, el kernel de la función es el *subgrupo de congruencia principal de nivel* N:

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

Además $\Gamma(N)$ se realiza como el kernel del homomorfismo $\mathrm{SL}_2\mathbb{Z} \to \mathrm{SL}_2(\mathbb{Z}/N/ZZ)$. Por lo tanto $[\mathrm{SL}_2\mathbb{Z} : \Gamma(N)]$ □

0.1.1 Curvas modulares y espacios moduli

En esta sección definimos la curva $X_0(N)$ y vemos que parametriza ciertas clases de isomorfismo de curvas elípticas. Fijamos $N > 1$.

Sea E una curva elíptica sobre el campo $\mathbb{Q}(x)$ tal que $j(E) = x$. Sea $P \in E$ un punto de orden n y sea $C = \{O, P, 2P, \ldots, (N-1)P\}$ el subgrupo de E generado por P. Toma $K \subset \overline{\mathbb{Q}(x)}$ como el campo fijo del subgrupo $H = \{\sigma \in G_{\mathbb{Q}(x)} \mid \sigma(C) = C\}$.

Como $(G_{\mathbb{Q}(x)} : H) < \infty$ (porque C es finito), entonces K es una extensión finita de $\mathbb{Q}(x)$. En particular es una extensión de $\mathbb{Q}$ finitamente generada. Ahora, si $\overline{\mathbb{Q}} \cap K = \mathbb{Q}$ (estamos identificando a $\overline{\mathbb{Q}}$ con su inclusión en $\overline{K}$) entonces K es una extensión de $\mathbb{Q}$ finitamente generada de grado de trascendencia 1. De esta manera, como la categoría de curvas proyectivas suaves definidas sobre $\mathbb{Q}$ (con morfismos dominantes) y la categoría de extensiones de $\mathbb{Q}$ finitamente generadas de grado de trascendencia 1 (cf. [**?**, §1.6, corolario 6.12]), podemos asociar a K una curva proyectiva suave definida sobre $\mathbb{Q}$ que llamamos $X_0(N)$.

Hay que probar que la elección de $X_0(N)$ está bien definida, es decir que no depende de E ni de el subgrupo $C \subset E$ y además que efectivamente $\overline{\mathbb{Q}} \cap K = \mathbb{Q}$ para que K realmente sea un campo de funciones de una curva. Estas tres proposiciones se siguen del siguiente teorema:

Sea E una curva elíptica sobre $\mathbb{Q}$ y definimos a $\mathbb{Q}(E[N])$ como la extensión de Galois generada por las coordenadas afines de los puntos de $E[N]$. La acción natural $G_{\mathbb{Q}(E[N])} \curvearrowright E[N]$ induce una representación $\rho : G_{\mathbb{Q}(E[N])} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ (gracias a la estructura de $E[N]$ dada en la proposición **??**).

Teorema 7. *Sea E una curva elíptica definida sobre $k = \mathbb{Q}(x)$ tal que $j(E) = x$. Con la notación del párrafo anterior, la representación ρ es un isomorfismo, es decir:*

$$G_{\mathbb{Q}(x,E[N])} \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Además, $\overline{\mathbb{Q}} \cap \mathbb{Q}(x, E[N]) = \mathbb{Q}(\mu_N)$ donde $\mu_N \subset \mathbb{C}$ es el conjunto de las N-ésimas raices de la unidad.

Nota. Este resultado es una versión débil del caso $k = \mathbb{C}(x)$ donde el isomorfismo es $\mathrm{Gal}(\mathbb{Q}(x, E[N]) \mid \mathbb{Q}(x)) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ (cf. [**?**, capítulo III, §1, teorema 1 y su corolario])

Ahora explicamos porque la elección $X_0(N)$ está bien definida:

Corolario 8. *La curva elíptica $X_0(N)$ sobre $\mathbb{Q}$ existe y no depende de E ni del subgrupo C.*

Proof. Como mencionamos antes, basta robar que $\overline{\mathbb{Q}} \cap K = \mathbb{Q}$ para que K efectivamente sea una extensión finitamente generada sobre $\mathbb{Q}$ de grado de trascendencia 1. Sea $P \in E$ el generador de C. Observa que $\{P\} \subset E[N]$ se puede extender a una base ordenada de tal manera que el isomorfismo $G_{\mathbb{Q}(x,E[N])} \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ del teorema 6 hace que $H' := \{\sigma \in G_{\mathbb{Q}(x,E[N])} \mid \sigma(C) = C\}$ sea isomorfo a las matrices triangulares inferiores, i.e.

$$H \cong \left\{ \begin{pmatrix} a & 0 \\ b & d \end{pmatrix} : a, d \in (\mathbb{Z}/N\mathbb{Z})^*,\ b \in \mathbb{Z}/N\mathbb{Z} \right\}.$$

Ahora, la función determinante $\det : \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to (\mathbb{Z}/N\mathbb{Z})^*$ restringida a H sigue siendo sobre. Por lo tanto $\mathbb{Q}(\mu_N) \cap K = \mathbb{Q}$.... Si sustituimos la igualdad de la segunda parte del teorema 6 en esta fórmula obtenemos:

$$\mathbb{Q} = \left(\overline{\mathbb{Q}} \cap \mathbb{Q}(x, E[N])\right) \cap K = \mathbb{Q}(x, E[N]) \cap \left(\overline{\mathbb{Q}} \cap K\right) = \overline{\mathbb{Q}} \cap K$$

ya que $\overline{\mathbb{Q}} \cap K \subset \mathbb{Q}(x, E[N])$.

Ahora probamos que $X_0(N)$ es independiente de la elección de C. Cambiar de subgrupo C es cambiar de punto P de orden N. Sean $P' \in E$ otro punto de orden N, $C' \subset E[N]$ el subgrupo cíclico generado por P' y H' el subgrupo de $G_{\mathbb{Q}(x,E[N])}$ de fija a C'. De la misma manera extendemos $\{P'\}$ a otra base de $E[N]$. Este cambio de base modifica el isomorfismo $G_{\mathbb{Q}(x,E[N])} \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ mediante una conjugación por la matriz de cambio de base. En particular la imagen de H' en $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ es un conjugado de la imagen de H. Por lo tanto existe un $\sigma \in G_{\mathbb{Q}(x,E[N])}$ tal que $H' = \sigma H \sigma^{-1}$. Por lo tanto el campo fijo K' de H' es simplemente $\sigma(K)$, es decir $K \cong K'$. Gracias a la equivalencia de categorías mencionada al principio de la sección, $X_0(N)$ es isomorfo a cualquier curva proyectiva suave con campo de funciones K' y por lo tanto $X_0(N)$ es independiente de la elección de C.

Por último probamos que $X_0(N)$ es independiente de la elección de la curva $E/\mathbb{Q}(x)$.... □

Como consecuencia de este corolario, cada curva proyectiva $X_0(N)$ sobre $\mathbb{Q}$ tiene asociado una curva elíptica $E/\mathbb{Q}(x)$ (con $j(E) = x$) y un subgrupo cíclico $C \subset E$ de orden N tal que el campo de funciones K de $X_0(N)$ es el campo fijo de $H = \{\sigma \in G_{\mathbb{Q}(x)} \mid \sigma(C) = C\}$. La inclusión $\mathbb{Q}(x) \hookrightarrow K$ induce un morfismo de curvas $X_0(N) \to \mathbb{P}^1(\mathbb{Q})$. A un punto en la imagen inversa de $\infty \in \mathbb{P}^1(\mathbb{Q})$ se le llama una *cúspide* de $X_0(N)$.

También podemos considerar a $X_0(N)$ como una curva proyectiva sobre $\mathbb{C}$; en este caso su campo de funciones es $K \otimes_{\mathbb{Q}} \mathbb{C}$. Como en el párrafo anterior, la inclusión $\mathbb{C}(x) \hookrightarrow K \otimes \mathbb{C}$ determina un morfismo $X_0(N)(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$. Sea $S \subseteq \mathbb{P}^1(\mathbb{C})$ un subconjunto y S^{c} su complemento en $\mathbb{P}^1(\mathbb{C})$. Denotamos $X_0(N)(\mathbb{C})_S$ como la imagen inversa de S^{c} bajo $X_0(N)(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$.

Estamos en posición de estudiar cómo parametriza $X_0(N)$ a algunas curvas elípticas, pero primero debemos definir una categoría nueva. Los objetos son parejas (E, C) donde $E/\mathbb{C}$ es una curva elíptica y $C \subset E$ es un subgrupo cíclico de orden N. Los morfismos $(E, C) \to (E', C')$ son isomorfismos de curvas $\varphi : E \to E'$ tales que $\varphi(C) = C'$. A la clase de isomofismo de (E, C) la denotamos por $[E, C]$ y al conjunto de clases de isomorfismo lo denotamos por $\mathrm{El}_0(N)(\mathbb{C})$. Además, si $S \subseteq \mathbb{P}^1(\mathbb{C})$ entonces escribimos

$$\mathrm{El}_0(N)(\mathbb{C})_S := \{[E, C] \in \mathrm{El}_0(N)(\mathbb{C}) \mid j(E) \notin S\}.$$

Similarmente denotamos por $\mathrm{Toro}_0(N)$ al conjunto de clases de isomorfismo de parejas (T, C) donde T es un toro complejo de dimensión 1 (i.e. $T \cong \mathbb{C}/\Lambda$ para alguna retícula) y $C \subset T$ es un subgrupo cíclico de orden N.

Ahora, sea $x \in X_0(N)(\mathbb{C})$. Como $X_0(N)(\mathbb{C})$ es una curva suave, x determina un anillo de valoración discreta $\mathcal{O}_x \subset K \otimes \mathbb{C}$ con ideal maximal $\mathfrak{m}_x$. Si E tiene buena reducción en $\mathfrak{m}_x$, entonces la reducción módulo $\mathfrak{m}_x$ produce una curva elíptica $E_x/\mathbb{C}$. La restricción de la reducción módulo $\mathfrak{m}_x$ a $E[n] \to E_x[N]$ es inyectiva y así la reducción módulo $\mathfrak{m}_x$ del punto $P \in E[N]$ es un punto $P_x \in E_x[N]$ de orden N que genera un subgrupo cíclico $C_x \subset E_x$ de orden N.

Con estas consideraciones podemos enunciar el resultado más importante de esta sección:

Teorema 9. *Sean $E/\mathbb{Q}(x)$ una curva elíptica tal que $j(E) = x$, $S \subseteq \mathbb{P}^1(\mathbb{C})$ un subconjunto que contiene a todos los lugares donde E tiene mala reducción, $\{Q, P\}$ una $\mathbb{Z}/N\mathbb{Z}$-base de $E[N]$ y $C \subset E$ el subgrupo cíclico generado por P, entonces tenemos el siguiente diagrama conmutativo de funciones biyectivas:*

$$\begin{array}{ccc} X_0(N)(\mathbb{C})_S & \xrightarrow{(i)} & \mathrm{El}_0(N)(\mathbb{C})_S \\ \Big\downarrow{\scriptstyle (ii)} & & \Big\downarrow{\scriptstyle (iv)} \\ \mathbb{H}/\Gamma_0(N) & \xrightarrow[(iii)]{} & \mathrm{Toro}_0(N) \end{array}$$

donde las funciones están dadas por:

i) $x \mapsto [E_x, C_x]$.

ii) *La restricción del isomorfismo $X_0(N)(\mathbb{C}) \cong \mathbb{H}^*/\Gamma_0(N)$ de superficies de Riemann.*

iii) $[z] \mapsto [\mathbb{C}/\Lambda_z, \langle \frac{1}{N} + \Lambda_z \rangle]$ *donde $\Lambda_z := z\mathbb{Z} \oplus \mathbb{Z}$ es una retícula de $\mathbb{C}$.*

iv) $[E, C] \mapsto [E(\mathbb{C}), C]$.

Proof. La prueba de que (i) es biyectiva se sigue de [**?**, capítulo III, §1.3, proposición 1], la biyectividad de (ii) se sigue de [**?**, capítulo III, §1.10, proposición 6], la biyectividad de (iii) se sigue de [**?**, capítulo III, §1.10, proposición 7] y la biyectividad de (iv) se sigue de [**?**, capítulo III, §1.8, proposición 5]. □

Definición 10. Una curva elíptica $E/\mathbb{Q}$ es *modular* si existe una función holomorfa no constante $X_0(N) \to E$ para alguna N.