Rev.R.Acad.Cienc.Exact.Fis.Nat. (Esp)
Vol. 94, N.º 3, pp 309-322, 2000
Monográfico: Contribuciones al estudio algorítmico de problemas de moduli aritméticos

DOMINIOS FUNDAMENTALES MODULARES[1]

(homografías/grupos de congruencia/curvas modulares/dominios fundamentales)

M. ALSINA

Dept. Matemàtica Aplicada III. Universitat Politècnica de Catalunya. Av. Bases de Manresa, 61-73. Manresa. E-mail: montsea@bages.eupm.upc.es

ABSTRACT

The aim of this article is to apply the theory of isometric circles to construct fundamental domains of some modular curves, defined by congruence subgroups $\Gamma_0(p)$ of the modular group $\mathbf{SL}(2, \mathbb{Z})$, p prime. The fundamental domains obtained are highly symmetric. Their graphical representation and the computation of their invariants have been implemented in a MapleV package, for interactive use.

RESUMEN

En este artículo se aplica la teoría de los círculos de isometría a la construcción de dominios fundamentales de algunas curvas modulares, concretamente las definidas por los subgrupos de congruencia $\Gamma_0(p)$ del grupo modular $\mathbf{SL}(2, \mathbb{Z})$, con p un número primo. Los dominios fundamentales obtenidos tienen una gran simetría. Su representación gráfica y el cálculo de sus invariantes han sido implementados en un paquete de MapleV, para uso interactivo.

INTRODUCCIÓN

Los subgrupos de congruencia $\Gamma_0(p)$ del grupo modular $\mathbf{SL}(2, \mathbb{Z})$ actúan de forma propiamente discontínua en el semiplano de Poincaré $\mathcal{H}$, lo cual conduce al estudio de dominios fundamentales para dicha acción (cf. por ejemplo [1], [2]). En este artículo, contruimos dominios fundamentales de $\Gamma_0(p)$ a través de la teoría de los círculos de isometría de las homografías. Los dominios fundamentales obtenidos tienen una gran simetría. Damos una forma sistemática de obtener tanto la representación gráfica del dominio y sus características principales, como algunos invariantes asociados a dichos grupos modulares. Su representación gráfica y el cálculo de sus invariantes han sido implementados en un paquete de MapleV, para uso interactivo.

La sección 1 contiene las definiciones y propiedades básicas referidas a las homografías y a los puntos hiperbólicos, elípticos y parabólicos.

En la sección 2, se introducen los círculos de isometría asociados a las homografías y se resumen sus propiedades principales. Siguiendo a Ford [3], se describe el método de construcción del dominio fundamental estándar de un grupo de homografías a partir de sus círculos de isometría, y su adaptación para el caso en que no todos los elementos del grupo tengan círculos de isometría asociados.

En la sección 3, se aplican los métodos y resultados anteriores, de forma generalizada, al cálculo de los dominios fundamentales de los grupos $\Gamma_0(p)$. Uno de los resultados principales es el teorema 3.1 que describe el conjunto de círculos maximales de $\Gamma_0(p)$, concepto introducido en la sección anterior, que permite reducir el estudio del dominio fundamental al estudio de un número finito de círculos de isometría. Utilizando propiedades de los círculos de isometría, se construye de forma sistemática un dominio fundamental de $\Gamma_0(p)$ en el teorema 3.4, y se describen sus propiedades en la proposición 3.8 y el teorema 3.10. En particular, se obtienen fórmulas simplificadas para el número de vértices y ciclos de cada tipo, la expresión explícita de dichos vértices y ciclos, y las parejas de aristas identificadas dos a dos. Como consecuencia, en la proposición 3.13 se da una presentación del grupo de homografías definido por $\Gamma_0(p)$. Los casos $\Gamma_0(1) = \mathbf{SL}(2, \mathbb{Z})$ y $\Gamma_0(2)$ son casos especiales que requieren un trato aparte, utilizando también la teoría de círculos de isometría, y se han incluido por motivos de completitud.

En la última sección, se comenta la implementación en MapleV del algoritmo de construcción de los dominios fundamentales $\mathcal{D}(\Gamma_0(p))$ y se presentan ejemplos gráficos y resultados explícitos para ilustrar los datos computables.

[1] Con soporte parcial de DGES, PB96-0166.

1. HOMOGRAFÍAS

En esta sección se dan las definiciones y se describen resultados referentes a las homografías sobre el semiplano de Poincaré, $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. Como referencias principales citamos [4], [5], [6] y [7].

Una homografía es una aplicación biyectiva conforme, es decir que conserva la medida y la orientación de los ángulos, $t : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$, $z \mapsto \dfrac{az + b}{cz + d}$ con $a, b, c, d \in \mathbb{C}$, $ad - bc = 1$. El grupo de homografías se identifica con el grupo de matrices PSL(2, $\mathbb{C}$). Si nos restringimos al semiplano de Poincaré, las aplicaciones conformes son precisamente las homografías con a, b, c, d reales. Así, identificaremos el grupo de homografías de $\mathcal{H}$ con el grupo de matrices PSL(2, $\mathbb{R}$). Usualmente, abusando de la notación, escribiremos las homografías como elementos de $\mathbf{SL}(2, \mathbb{R})$.

A continuación, vamos a describir geométricamente una aplicación del plano complejo en sí mismo: la inversión del círculo. Aunque no es una aplicación conforme, nos permitirá interpretar geométricamente las aplicaciones conformes de $\mathcal{H}$. Sea C un círculo de radio r y centro un punto $o \in \mathbb{C}$. La inversión respecto del círculo C es la transformación geométrica que a cada punto z le asigna el punto w de la recta determinada por z y o, de forma que el producto escalar de oz con ow sea r^2. Si el círculo tiene ecuación $az\bar{z} + bz + \bar{b}\bar{z} + c = 0$, en términos de variable compleja, la expresión analítica de la transformación es $w = \dfrac{-\bar{b}\bar{z} - c}{a\bar{z} + b}$. Notemos que incluye el caso $a = 0$, en que C en realidad es un recta, y entonces la inversión es exactamente la reflexión respecto de dicha recta. La inversión del círculo es la composición de la conjugación compleja con una aplicación conforme (cambia la orientación de los ángulos pero conserva su magnitud). Se demuestra que toda homografía $\gamma \in \mathbf{SL}(2, \mathbb{R})$ se expresa como la composición de dos inversiones respecto círculos adecuados.

Definición 1.1. *Sea* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}(2, \mathbb{R})$ *una homografía distinta de* $\pm\mathrm{Id}$.

(a) Se dice que γ es una homografía hiperbólica si tiene dos puntos fijos distintos en $\mathbb{R} \cup \{\infty\}$, o equivalentemente si $(a + d)^2 > 4$, es decir $|\mathrm{tr}(\gamma)| > 2$.

(b) Se dice que γ es una homografía elíptica si tiene un punto fijo $z \in \mathcal{H}$ y el otro punto fijo es $\bar{z}$, o equivalentemente si $(a + d)^2 < 4$, es decir $|\mathrm{tr}(\gamma)| < 2$.

(c) Se dice que γ es una homografía parabólica si tiene únicamente un punto fijo en $\mathbb{R} \cup \{\infty\}$, o equivalentemente si $(a + d)^2 = 4$, es decir $|\mathrm{tr}(\gamma)| = 2$.

Sobre $\mathbb{C}$, cada matriz $\gamma \in \mathbf{SL}(2, \mathbb{R})$, $\gamma \neq \pm\mathrm{Id}$, es conjugada de una de las dos formas canónicas de Jordan siguientes: $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, con $\lambda_1 \neq \lambda_2$, o bien $\begin{pmatrix} \pm 1 & 1 \\ 0 & \pm 1 \end{pmatrix}$. Las matrices hiperbólicas y las elípticas son diagonalizables y les corresponde la primera forma de Jordan. Las matrices parabólicas son justamente aquellas que tienen la segunda forma de Jordan. De hecho, se puede definir el carácter parabólico, hiperbólico o elíptico a partir de los valores propios de la matriz, como se indica en la proposición siguiente.

Proposición 1.2. *Dada una homografía* $\gamma \in \mathbf{SL}(2, \mathbb{R})$, *sean* λ_1, λ_2 *sus valores propios sobre* $\mathbb{C}$ *y* $\mu := \dfrac{\lambda_1}{\lambda_2}$. *Entonces,*

(i) γ es hiperbólica si, y sólo si, μ es un número real positivo.

(ii) γ es elíptica si, y sólo si, μ es un número complejo con valor absoluto igual a 1. En este caso, si $\mu = e^{i\theta}$ con $0 < \theta < 2\pi$, se tiene $\lambda_1 + \lambda_2 = 2\cos\theta$.

(iii) γ es parabólica si, y sólo si, μ es igual a 1.

Para los casos no parabólicos, el valor μ se llama el multiplicador de γ, lo cual parece natural a partir de la interpretación geométrica siguiente. Consideremos la homografía γ dada por una cierta matriz M y el cambio de variables que transforma M en su forma de Jordan. Si γ es hiperbólica o elíptica, este cambio de variables lleva sus dos puntos fijos al 0 y al infinito, respectivamente. Con este cambio de variables, la homografía puede interpretarse geométricamente como una dilatación de módulo μ con centro en el origen para el caso hiperbólico, y como una rotación de ángulo igual al argumento de μ alrededor del origen para el caso elíptico. En el caso de una homografía parabólica, el cambio lleva su único punto fijo al infinito, y la homografía es geométricamente una traslación.

Observemos que las homografías elípticas con $\theta = \dfrac{p}{q}\pi$ con $p, q \in \mathbb{Z}$ tienen orden finito. Las homografías parabólicas siempre tienen orden infinito.

De ahora en adelante, sea $\Gamma \subset \mathbf{SL}(2, \mathbb{R})$ un grupo de homografías, que actúa en el semiplano de Poincaré $\mathcal{H}$. Se dice que Γ actúa de forma propia y discontinua en $\mathcal{H}$ si existen un punto z_0 y un número real $\varepsilon > 0$ tales que para todo $\gamma \in \Gamma$, $\gamma \neq \pm\mathrm{Id}$, se tiene $|\gamma(z_0) - z_0| > \varepsilon$; en este caso se dice que z_0 es un punto estándar. Como grupo de matrices, ello es equivalente a que Γ sea un subgrupo discreto de $\mathbf{SL}(2, \mathbb{R})$.

La acción de Γ en $\mathcal{H}$ da una relación de equivalencia entre sus puntos. Se dice que dos puntos, $z, z' \in \mathcal{H}$, son equivalentes respecto de Γ si $z' = \gamma(z)$ para algún $\gamma \in \Gamma$.

La clasificación de las homografías descrita anteriormente permite clasificar también los puntos de $\mathcal{H} \cup \mathbb{R} \cup \{\infty\}$ respecto de un grupo Γ.

Definición 1.3. *Un punto $x \in \mathbb{R} \cup \{\infty\}$ se llama punto parabólico, respectivamente hiperbólico, respecto de Γ si existe un elemento $\gamma \in \Gamma$ parabólico, respectivamente hiperbólico, tal que $\gamma(x) = x$. Un punto $z \in \mathcal{H}$ se llama punto elíptico respecto de Γ si existe un elemento $\gamma \in \Gamma$ elíptico tal que $\gamma(z) = z$.*

Definición 1.4. *El grupo de isotropía de un punto $z \in \mathcal{H}$ respecto de Γ es $\Gamma_z = \{\gamma \in \Gamma \mid \gamma(z) = z\}$.*

Si Γ es un subgrupo discreto de $\mathbf{SL}(2, \mathbb{R})$, se demuestra que el grupo de isotropía de un punto elíptico es un grupo cíclico finito, formado por matrices elípticas. De hecho, los únicos elementos no triviales de Γ de orden finito son precisamente las matrices elípticas.

Definición 1.5. *El orden de un punto elíptico $z \in \mathcal{H}$ respecto de Γ es el orden de su grupo de isotropía en $\Gamma/(\pm\mathrm{Id})$. Es decir, el orden del punto elíptico z es $k = |\Gamma_z|$, si $-\mathrm{Id} \notin \Gamma$, o $k = \frac{1}{2}|\Gamma_z|$, si $-\mathrm{Id} \in \Gamma$.*

Si z es un punto elíptico respecto de Γ, entonces se ve fácilmente que $\gamma(z)$, para todo $\gamma \in \Gamma$, es también un punto elíptico respecto de Γ. Además, dos puntos elípticos equivalentes tienen el mismo orden ya que $\Gamma_{\gamma(z)} = \gamma\Gamma_z\gamma^{-1}$.

Lema 1.6. *Sea $\Gamma \subset \mathbf{SL}(2, \mathbb{R})$ tal que para todo $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ se satisface $\gamma' := \begin{pmatrix} -a & b \\ c & -d \end{pmatrix} \in \Gamma$. Entonces:*

(i) Dos puntos son Γ-equivalentes si, y sólo si, sus simétricos respecto el eje imaginario también lo son.

(ii) Un punto $z \in \mathcal{H}$ es elíptico respecto de Γ si, y sólo si, su simétrico respecto el eje imaginario $-\bar{z}$ lo es; en tal caso, tienen el mismo orden.

Demostración. Sean $z, w \in \mathcal{H}$ tales que $\gamma(z) = w$, con $\gamma \in \Gamma$. Entonces tenemos $\gamma'(-\bar{z}) = -\bar{w}$, lo cual demuestra *(i)*.

Tomando en particular $z = w$ se obtiene *(ii)*. Notemos que γ y γ' tienen el mismo orden como homografías, es decir módulo $\pm$Id, por lo que los puntos, en el caso de ser elípticos, tienen también el mismo orden. □

Definición 1.7. *Un subconjunto cerrado conexo $\mathcal{D}$ de $\mathcal{H}$ es un dominio fundamental por la acción de Γ en $\mathcal{H}$ si los puntos del interior de $\mathcal{D}$ no son dos a dos Γ-equivalentes y cada punto de $\mathcal{H}$ es Γ-equivalente a algún punto de $\mathcal{D}$.*

Evidentemente, el dominio fundamental de un grupo Γ no es único. Por ejemplo, si $\mathcal{D}$ es un dominio fundamental de Γ, entonces $\gamma(\mathcal{D})$ también lo es, para cualquier $\gamma \in \Gamma$.

2. CÍRCULOS DE ISOMETRÍA

Aunque las homografías son aplicaciones conformes, no siempre conservan las longitudes y las áreas euclídeas. Por ejemplo, sea Γ un subgrupo discreto de $\mathbf{SL}(2, \mathbb{R})$ y sea $\gamma \in \Gamma$ una homografía que fija el infinito. Entonces se demuestra que γ es o bien una homotecia o bien una traslación. En el primer caso, γ altera todas las longitudes y áreas; en el segundo caso las deja todas invariantes. Notemos que en la expresión de γ en función de *a, b, c* y *d*, fijar el infinito es equivalente a $c = 0$. Si consideramos las aplicaciones que no fijan el infinito, el resultado es muy distinto. Ello nos permite definir los círculos de isometría.

En general, la definición de círculo de isometría se aplica a todas las homografías que no fijan el infinito. En este artículo, vamos a considerar básicamente homografías definidas por matrices de $\mathbf{SL}(2, \mathbb{R})$ y subgrupos discretos de $\mathbf{SL}(2, \mathbb{R})$, es decir grupos de homografías que actúan de forma propia y discontinua en $\mathcal{H}$. Para un enfoque más general veáse [3] y [7].

Definición 2.1. *Dada una homografía $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}(2, \mathbb{C})$ con $c \neq 0$, el círculo $I_\gamma := \{z \in \mathbb{C} : |cz + d| = 1\}$ se llama círculo de isometría de γ.*

Para cada círculo de isometría I_γ, denotamos por r_γ y o_γ el radio y el centro, respectivamente, y designaremos $\mathrm{int}(I_\gamma)$ y $\mathrm{ext}(I_\gamma)$ las regiones del plano complejo, interior y exterior, delimitadas por el círculo. Dado un conjunto G de homografías que no fijen el infinito, no necesariamente con estructura de grupo, ponemos $I_G = \{I_\gamma : \gamma \in G\}$.

Dada una homografía γ definida sobre $\mathbb{C} \cup \{\infty\}$, tenemos que $\dfrac{d\gamma}{dz} = \dfrac{1}{(cz + d)^2}$. Así, $z \in I_\gamma$ si, y sólo si, $|d\gamma| = |dz|$. Por lo tanto, el círculo I_γ puede pensarse como el lugar geométrico de los puntos alrededor de los cuales las longitudes y las áreas euclídeas no son alteradas en magnitud al aplicar la homografía γ. Del mismo modo, $z \in \mathrm{int}(I_\gamma)$ si, y sólo si, $|d\gamma| > |dz|$. Por lo tanto, para los puntos interiores al círculo I_γ las magnitudes aumentan al aplicar γ, y para los puntos exteriores, disminuyen.

Lema 2.2. *Sea $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}(2, \mathbb{R})$ con $c \neq 0$.*

(i) *Los centros y los radios de I_γ y $I_{\gamma^{-1}}$ son los números reales $o_\gamma = -d/c$, $o_{\gamma^{-1}} = a/c$, $r_\gamma = r_{\gamma^{-1}} = 1/|c|$.*

(ii) *La distancia entre o_γ y $o_{\gamma^{-1}}$ es $\left|\frac{a+d}{c}\right|$; además, $r_\gamma + r_{\gamma^{-1}} = \frac{2}{|c|}$.*

(iii) *Sea $\sigma \in \mathbf{SL}(2, \mathbb{R})$ tal que ni σ ni $\gamma\sigma$ fijan el infinito. Entonces,*

$$r_{\gamma\sigma} = \frac{r_\gamma r_\sigma}{|o_{\sigma^{-1}} - o_\gamma|}, \quad |o_{\gamma\sigma} - o_\gamma| = \frac{r_\sigma^2}{|o_{\sigma^{-1}} - o_\gamma|}.$$

(iv) *Tenemos $\gamma(I_\gamma) = I_{\gamma^{-1}}$ y $\gamma(\text{ext}(I_\gamma)) = \text{ext}(I_{\gamma^{-1}})$, de lo cual se deduce $\gamma(\text{int}(I_\gamma)) = \text{ext}(I_{\gamma^{-1}})$. Además, $\gamma(o_\gamma) = \infty$ y $\gamma(\infty) = o_{\gamma^{-1}}$.*

Proposición 2.3. *Para toda homografía $\gamma \in \mathbf{SL}(2, \mathbb{R})$ existe una recta, que denotaremos L_γ, tal que:*

(i) *γ es igual a la inversión del círculo I_γ seguida por la reflexión respecto la recta L_γ;*

(ii) *un círculo es invariante por γ si, y sólo si, es ortogonal a I_γ y tiene el centro en L_γ.*

Definición 2.4. *Fijado un conjunto $G \subseteq \mathbf{SL}(2, \mathbb{R})$, decimos que un círculo de isometría $I \in \mathcal{I}_G$ es maximal respecto G, si no existe ningún $I' \in \mathcal{I}_G$, $I' \neq I$, tal que $I \subseteq (\text{int}(I') \cup I')$.*

Denotaremos $\mathcal{I}_G^{\max} = \{I_\gamma : I_\gamma \text{ maximal en } G, \gamma \in G\}$. Es evidente que para cualquier conjunto G de homografías, $\bigcap_{I \in \mathcal{I}_G} \text{ext}(I) = \bigcap_{I \in \mathcal{I}_G^{\max}} \text{ext}(I)$.

Definición 2.5. *Sea Γ un subgrupo discreto de $\mathbf{SL}(2, \mathbb{R})$. Se dice que un punto de $\mathcal{H}$ es un punto límite respecto de Γ si es un punto de acumulación del conjunto $\{o_\gamma : \gamma \in \Gamma\}$. El resto de puntos de $\mathcal{H}$ se llaman puntos ordinarios respecto de Γ.*

Lema 2.6. *Sea Γ un subgrupo discreto de $\mathbf{SL}(2, \mathbb{R})$.*

(i) *El conjunto de puntos límite de Γ es cerrado por la acción de Γ.*

(ii) *Todos los puntos límite de Γ son reales.*

Aplicando las propiedades de los círculos de isometría recopiladas en el lema 2.2 y la interpretación geométrica de las homografías alrededor de los puntos fijos dada en la sección 1, se obtienen nuevas caracterizaciones de las homografías según sean hiperbólicas, elípticas o parabólicas.

Proposición 2.7. *Sea $\gamma \in \mathbf{SL}(2, \mathbb{R})$ una homografía hiperbólica con puntos fijos $x_1, x_2 \in \mathbb{R}$. Entonces,*

(i) *$I_\gamma \cap I_{\gamma^{-1}} = \varnothing$.*

(ii) *$I_{\gamma^n} \subset \text{ext}(I_{\gamma^{n-1}})$, para $n > 0$, por lo tanto I_γ es maximal respecto de $\{\gamma^n : n > 0\}$. Además, $\lim_{n \to \infty} r_{\gamma^n} = 0$. En particular, $\mathcal{I}_{\langle\gamma\rangle}^{\max} = \{I_\gamma, I_{\gamma^{-1}}\}$.*

(iii) *$\bigcap_{n>0} \text{int}(I_{\gamma^n}) = x_1$, $\bigcap_{n>0} \text{int}(I_{\gamma^{-n}}) = x_2$; x_1 y x_2 son puntos límite.*

(iv) *L_γ es el bisector del segmento que une los centros de I_γ e $I_{\gamma^{-1}}$.*

En la figura 1 se ilustra la posición relativa de los círculos de isometría correspondientes a una homografía hiperbólica $\gamma \in \mathbf{SL}(2, \mathbb{R})$, γ^{-1}, γ^2, γ^{-2}, γ^3 y γ^{-3}, así como la recta L_γ y los puntos fijos x_1 y x_2.

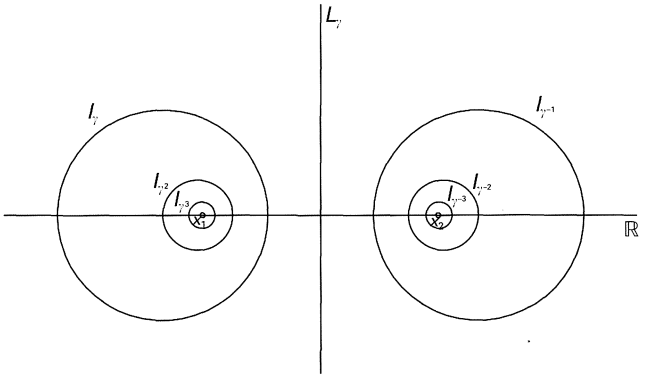

Figura 1. Círculos de isometría asociados a una homografía hiperbólica $\gamma \in \mathbf{SL}(2, \mathbb{R})$.

Proposición 2.8. *Sea $\gamma \in \mathbf{SL}(2, \mathbb{R})$ una homografía elíptica de orden k con puntos fijos $z \in \mathcal{H}$ y $\bar{z}$. Entonces,*

(i) *$\{z, \bar{z}\} \subseteq \bigcap_{n \in \mathbb{Z}} I_{\gamma^n}$.*

(ii) *Si $k = 2$, $I_{\gamma^{-1}} = I_\gamma$. Si $k > 2$, $I_\gamma \cap I_{\gamma^{-1}} = \{z, \bar{z}\}$.*

(iii) *El ángulo determinado por I_γ e $I_{\gamma^{-1}}$ en z es $\theta = 2\pi/k$.*

(iv) *L_γ es la recta determinada por z y $\bar{z}$. Si $k = 2$, L_γ es un diámetro de $I_\gamma = I_{\gamma^{-1}}$; si $k > 2$, L_γ es el bisector del segmento que une los centros de I_γ e $I_{\gamma^{-1}}$.*

En la figura 2 se ilustra la posición relativa de los círculos de isometría correspondientes a una homografía elíptica $\gamma \in \mathbf{SL}(2, \mathbb{R})$ de orden $k > 2$ y a γ^{-1}, así como la recta L_γ y los puntos fijos z y $\bar{z}$.

Proposición 2.9. *Sea $\gamma \in \mathbf{SL}(2, \mathbb{R})$ una homografía parabólica con punto fijo $x \in \mathbb{R}$. Entonces,*

(i) *$\bigcap_{n \in \mathbb{Z}} I_{\gamma^n} = \{x\}$.*

(ii) *Para $n > 0$, $I_{\gamma^n} \subseteq \text{int}(I_{\gamma^{n-1}})$; por tanto, I_γ es maximal respecto de $\{\gamma^n : n > 0\}$. Así, $\mathcal{I}_{\langle\gamma\rangle}^{\max} = \{I_\gamma, I_{\gamma^{-1}}\}$.*

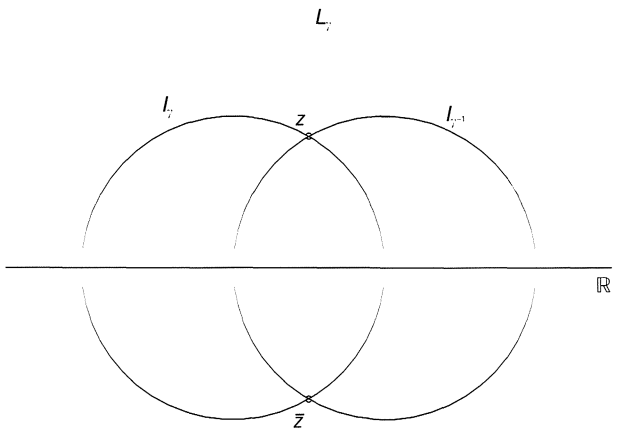

Figura 2. Círculos de isometría asociados a una homografía elíptica $\gamma \in \mathbf{SL}(2, \mathbb{R})$ de orden $k > 2$.

(iii) $r_{\gamma^n} = \dfrac{1}{|nc|} \to 0$ *para* $n \to \infty$; $o_{\gamma^n} = x - \dfrac{1}{nc} \in \mathbb{R}$ y x *es un punto límite.*

(iv) *La recta* L_γ *es la tangente común a los círculos* I_{γ^n} *en el punto* x *para todo* $n \neq 0$; L_γ *coincide con el bisector del segmento que une los centros de* I_γ *e* $I_{\gamma^{-1}}$.

En la figura 3 se ilustra la posición relativa de los círculos de isometría correspondientes a una homografía parabólica $\gamma \in \mathbf{SL}(2, \mathbb{R})$, γ^{-1}, γ^2, γ^{-2}, γ^3 y γ^{-3}, así como la recta L_γ y el punto fijo x.

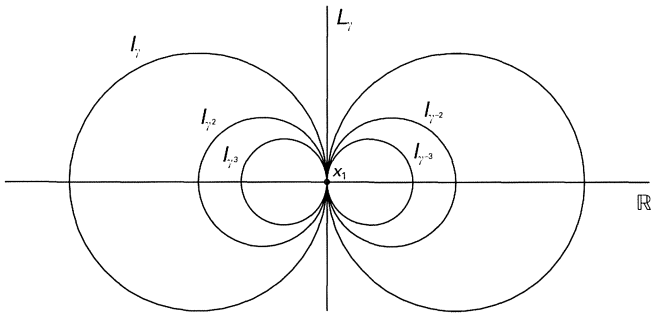

Figura 3. Círculos de isometría asociados a una homografía parabólica $\gamma \in \mathbf{SL}(2, \mathbb{R})\}$.

De las tres proposiciones anteriores deducimos el siguiente corolario.

Corolario 2.10. *Sea* $\gamma \in \mathbf{SL}(2, \mathbb{R})$ *que no fije el infinito. Entonces,*

(i) γ *es hiperbólica si, y sólo si,* $I_\gamma \cap I_{\gamma^{-1}} = \varnothing$.

(ii) γ *es elíptica si, y sólo si,* $\{z, \bar{z}\} \subseteq I_\gamma \cap I_{\gamma^{-1}}$, *para algún* $z \in \mathcal{H}$.

(iii) γ *es parabólica si, y sólo si,* $I_\gamma \cap I_{\gamma^{-1}} = \{x\} \in \mathbb{R}$.

Para los resultados del resto de la sección, se requerirá que el punto del infinito sea un punto estándar para el grupo Γ (cf. sección sección 1). Esta condición implica ya que los elementos de Γ distintos de la identidad no fijan el infinito, por lo que todos sus elementos tendrán un círculo de isometría asociado.

Proposición 2.11. *Sea* $\Gamma \subset \mathbf{SL}(2, \mathbb{C})$ *un grupo de homografías que actúa de forma propia y discontinua para el cual el infinito es un punto estándar. Entonces tenemos las propiedades siguientes.*

(i) *Los centros de los círculos de isometría estan a una distancia acotada del origen.*

(ii) *Para cada número real* $r \in \mathbb{R}$ *hay un número finito de círculos de isometría con radio mayor que* r. *Así, el conjunto de radios de los círculos de isometría está acotado.*

(iii) *El conjunto* $\bigcup_{\gamma \in \Gamma} \operatorname{int}(I_\gamma)$ *es un subconjunto acotado del plano complejo.*

(iv) *Homografías distintas tienen círculos de isometría distintos.*

Proposición 2.12. *Sea* Γ *un grupo de homografías que actúa de forma propia y discontinua en* $\mathcal{H}$, *es decir* Γ *es un subgrupo discreto de* $\mathbf{SL}(2, \mathbb{R})$. *Supongamos que el infinito es un punto estándar de* Γ. *Entonces,*

$$\mathcal{D}_{st}(\Gamma) := \overline{\mathcal{H} \cap \left(\bigcap_{\gamma \in \Gamma} \operatorname{ext}(I_\gamma)\right)}$$

es un dominio fundamental de Γ. *Este dominio se llama dominio fundamental estándar de* Γ.

Es fácil ver que dos puntos de $\mathcal{D}_{st}(\Gamma)$ no son Γ-equivalentes. Suponemos $\gamma(z_1) = z_2$, con $z_1 \in \mathcal{D}_{st}(\Gamma)$, $\gamma \in \Gamma$. En particular, z_1 es exterior al círculo de isometría I_γ. Aplicando el lema 2.2(iv), se tiene $z_2 \in \operatorname{int}(I_{\gamma^{-1}})$; por lo tanto $z_2 \notin \mathcal{D}_{st}(\Gamma)$. La demostración de que los transformados de $\mathcal{D}_{st}(\Gamma)$ recubren $\mathcal{H}$ (utilizando que el infinito es un punto estándar), se puede encontrar por ejemplo en [3] o [7].

Definición 2.13. *Los vértices del dominio fundamental* $\mathcal{D}_{st}(\Gamma)$ *son los puntos de la frontera del dominio que sean intersección de dos o más círculos de isometría distintos o que sean puntos elípticos de orden* 2. *Los vértices que no son puntos elípticos ni parabólicos se llaman vértices accidentales. Llamamos aristas de* $\mathcal{D}_{st}(\Gamma)$ *a los arcos de los círculos de isometría, es decir segmentos de rectas hiperbólicas, contenidos en la frontera del dominio delimitados por vértices.*

Observemos que los puntos elípticos y los parabólicos no pueden estar en el interior del dominio fundamental estándar, por 2.8 y 2.9. De hecho, siempre podemos su-

poner que los puntos elípticos y los parabólicos son vértices del dominio fundamental, aunque no todos los vértices son puntos elípticos o parabólicos. Asimismo notemos que un vértice tiene siempre dos aristas adyacentes. Como las homografías transforman círculos de isometría en círculos de isometría, se tiene también que transforman vértices en vértices.

Definición 2.14. *Una órbita de vértices de un dominio fundamental se llama ciclo. Se dice que un ciclo es elíptico de orden k si está formado por vértices elípticos de orden k. Se dice que el ciclo es accidental o parabólico, si está formado por vértices accidentales o parabólicos, respectivamente; convenimos en este caso que es de orden $k = 1$ o $k = \infty$, respectivamente.*

Propiedades 2.15. *Sea Γ un subgrupo discreto de* $\mathbf{SL}(2, \mathbb{R})$ *para el cual el infinito es un punto estándar y sea $\mathcal{D}_{st}(\Gamma)$ su dominio fundamental estándar.*

(i) Las aristas del dominio fundamental $\mathcal{D}_{st}(\Gamma)$ son equivalentes dos a dos por la acción de Γ. Es decir, existen $\gamma_j \in \Gamma$ tales que las aristas se disponen en pares disjuntos de la forma $\{l_j, \gamma_j(l_j)\}$.

(ii) Las aristas que son equivalentes tienen la misma longitud hiperbólica.

(iii) El conjunto de homografías $\gamma_j \in \Gamma$ que dan los pares de aristas, identificándolas dos a dos, forman un sistema de generadores del grupo Γ.

(iv) Cada ciclo de orden finito determina una relación entre los generadores. Sea $\{w_1, \ldots, w_m\}$ un ciclo de orden $k \in \mathbb{N}$. Consideramos las homografías $\gamma_j \in \Gamma$, $j = 1, \ldots, m$, tales que $\gamma_j(w_j) = w_{j+1}$ para $j = 1, \ldots, m-1$ y $\gamma_m(w_m) = w_1$. Entonces $(\gamma_m \gamma_{m-1} \ldots \gamma_1)^k = \pm \mathrm{Id}$.

(v) El conjunto de generadores de (iii) junto con las relaciones de (iv) forman una presentación del grupo Γ.

(vi) La suma de los ángulos en los vértices de un ciclo no parabólico es $2\pi/k$, donde k es el orden del ciclo. La suma de los ángulos en los vértices de un ciclo parabólico es 0.

Proposición 2.16. *Sea Γ un grupo que actúa de forma propia y discontinua en $\mathcal{H}$. Entonces existe un dominio fundamental de Γ que cumple las propiedades de* 2.15.

Demostración. Si el infinito es un punto estándar de Γ, se toma el dominio fundamental estándar $\mathcal{D}_{st}(\Gamma)$.

Supongamos ahora que el infinito no es un punto estándar de Γ. Cualquier grupo que actúe de forma propia y discontinua en el plano complejo tiene almenos un punto estándar z. Tomando una homografía $\sigma \in \mathbf{SL}(2, \mathbb{C})$ tal que $\sigma(z) = \infty$, obtenemos un transformado del grupo Γ, $\sigma\Gamma\sigma^{-1}$, que actúa sobre $\sigma\mathcal{H}$ y tiene el infinito como punto estándar. En ese caso se demuestra que los resultados enunciados para $\Gamma \in \mathbf{SL}(2, \mathbb{R})$ y $\mathcal{H}$, formulados de acuerdo con la nueva situación, también son válidos y se obtiene un dominio fundamental estándar con las propiedades de 2.15, $\mathcal{D}_{st}(\sigma\Gamma\,\sigma^{-1})$. Finalmente, $\sigma^{-1}(\mathcal{D}_{st}(\sigma\Gamma\sigma^{-1}))$ es un dominio fundamental de Γ que cumple las propiedades de 2.15. □

A continuación se describe la adaptación del método introducido por Ford para hallar un dominio fundamental para un grupo Γ que actúe de forma propia y discontinua y que tenga elementos que fijen el infinito que, a menudo, evita manejar transformados del grupo y del semiplano de Poincaré.

Denotamos Γ_∞ el subgrupo de Γ formado por los elementos que fijan el infinito. La proposición anterior nos asegura la existencia de un dominio fundamental de Γ_∞ con las propiedades enunciadas en 2.15. A menudo hay otras formas más directas de hallar un dominio para el grupo Γ_∞ con esas propiedades.

Denotaremos por Γ' el resto de elementos del grupo, $\Gamma' = \Gamma \backslash \Gamma_\infty$. Todos sus elementos tienen círculos de isometría, pero Γ' no es un grupo y no se pueden aplicar los resultados anteriores. Por ejemplo, puede que el conjunto de radios de los círculos de isometría no sea acotado, o que los círculos de isometría de homografías distintas sean iguales o que los centros de dichos círculos no estén en una región acotada (cf. sección 3). Estudiando la interrelación entre Γ_∞ y Γ', se demuestra que las transformaciones de Γ_∞ llevan círculos de isometría de Γ' a círculos de isometría de Γ', y se obtiene el siguiente resultado (cf. [3]).

Teorema 2.17. *Sea Γ un grupo de homografías que actúa de forma propia y discontinua. Sea $\mathcal{D}(\Gamma_\infty)$ un dominio fundamental de Γ_∞ que cumple las propiedades enunciadas en* 2.15. *Entonces, el conjunto siguiente*

$$\mathcal{D}(\Gamma) = \mathcal{D}(\Gamma_\infty) \cap \overline{\left(\bigcap_{\gamma \in \Gamma'} \mathrm{ext}(I_\gamma)\right)},$$

si es distinto del vacío, es un dominio fundamental del grupo Γ.

Corolario 2.18. *En las hipótesis del teorema anterior, el conjunto siguiente,*

$$\mathcal{D}(\Gamma) = \mathcal{D}(\Gamma_\infty) \cap \overline{\left(\bigcap_{I \in I_{\Gamma'}^{\max}} \mathrm{ext}(I)\right)},$$

si es distinto del vacío, es un dominio fundamental del grupo Γ.

Proposición 2.19. *El dominio fundamental $\mathcal{D}(\Gamma)$ satisface las propiedades listadas en* 2.15.

Notemos que debido a la intersección de la frontera de $\mathcal{D}(\Gamma_\infty)$ con los círculos de isometría de $I_{\Gamma'}^{\max}$ deben modi-

ficarse ligeramente los conceptos de vértice y arista definidos para el dominio fundamental estándar (cf. 2.13).

Definición 2.20. *El conjunto de vértices de $\mathcal{D}(\Gamma)$ está formado por los puntos de la frontera que cumplen una de las condiciones siguientes: son vértices de $\mathcal{D}(\Gamma_\infty)$; son intersección de dos o más círculos de isometría distintos; son puntos elípticos de orden 2, o son intersección de una arista de $\mathcal{D}(\Gamma_\infty)$ con uno o más círculos de isometría de Γ'. Los vértices que no son ni elípticos ni parabólicos reciben el nombre de accidentales. Las aristas de $\mathcal{D}(\Gamma)$ son los segmentos de rectas hiperbólicas, contenidos en la frontera, delimitados por vértices.*

3. CONSTRUCCIÓN DE UN DOMINIO FUNDAMENTAL DE $\Gamma_0(p)$ EN $\mathcal{H}$

Sea p un número primo o bien $p = 1$. Consideremos el grupo $\Gamma_0(p)$, que actúa de forma propiamente discontinua en el semiplano de Poincaré, donde

$$\Gamma_0(p) := \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z},\ ad - bc = 1,\ c \equiv 0 \bmod p\right\}.$$

$\Gamma_0(p)$ es un subgrupo de congruencia de nivel p de $\mathbf{SL}(2, \mathbb{Z})$. El caso $p = 1$ corresponde a $\Gamma_0(1) = \mathbf{SL}(2, \mathbb{Z})$.

Vamos a describir una forma sistemática de construir un dominio fundamental de $\Gamma_0(p)$, utilizando los resultados de las secciones anteriores.

En primer lugar, consideremos el subgrupo de $\Gamma_0(p)$ formado por los elementos que fijan el infinito. Se trata del conjunto de las matrices de la forma anterior que satisfacen las condiciones $c = 0$, $ad = 1$. De hecho no depende de p y lo denotaremos

$$\Gamma_\infty := \left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z}\right\} = \{T^b : b \in \mathbb{Z}\},\quad \text{con } T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Geométricamente, T actúa como una traslación de longitud 1. Por tanto, un dominio fundamental para Γ_∞ es

$$\mathcal{D}(\Gamma_\infty) = \left\{z \in \mathcal{H} \ :\ -\frac{1}{2} \le \operatorname{Re} z \le \frac{1}{2}\right\}.$$

Por otro lado, consideramos el resto de elementos del grupo $\Gamma_0(p)$, $\Gamma_0'(p) = \Gamma_0(p) \backslash \Gamma_\infty$. Para cada elemento de este conjunto tenemos un círculo de isometría asociado. Veamos qué características tienen y qué región de $\mathcal{H}$ delimitan.

Denotamos por $C(o, r)$ el círculo de centro o y radio r.

Teorema 3.1. *Sea p un número primo y consideramos el conjunto $\Gamma_0'(p)$. Entonces,*

(i) $I_{\Gamma_0'(p)} = \{C(k/sp,\ 1/sp) : k \in \mathbb{Z},\ s \in \mathbb{N},\ \operatorname{mcd}(k, ps) = 1\}$.

(ii) $I^{\max}_{\Gamma_0'(p)} = \{C(k/p,\ 1/p) : k \in \mathrm{Z},\ p \nmid k\}$.

Demostración. Sea $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0'(p)$. Entonces $I_\gamma = C(k/sp,\ 1/sp)$ con $s = \dfrac{|c|}{p} \in \mathbb{N}$ y $k = -d\dfrac{c}{|c|} \in \mathbb{Z}$. Por ser $ad - bc = 1$ se cumple $d \neq 0$ y $\operatorname{mcd}(k, sp) = \operatorname{mcd}(d, c) = 1$. Recíprocamente, sea $C(k/sp,\ 1/sp)$ un círculo cumpliendo $k \in \mathbb{Z}$, $s \in \mathbb{N}$ y $\operatorname{mcd}(k, sp) = 1$. Aplicando la identidad de Bézout, existen $a, b \in \mathbb{Z}$ tales que $-ak - bsp = 1$; entonces $\gamma = \begin{pmatrix} a & b \\ sp & -k \end{pmatrix} \in \Gamma_0'(p)$ y satisface $I_\gamma = C(k/sp,\ 1/sp)$, lo cual demuestra *(i)*.

El mayor radio posible de un círculo de isometría es $1/p$. Por tanto, los círculos $C(k/p,\ 1/p)$ con $k \in \mathbb{Z}$ y $\operatorname{mcd}(k, p) = 1$ son maximales respecto de $\Gamma_0'(p)$. Veamos que son los únicos círculos de isometría maximales. Sea $I \in I_{\Gamma_0'(p)}$, $I = C(k/sp,\ 1/sp)$ con $k \in \mathbb{Z}$, $s \in \mathbb{N}$, $\operatorname{mcd}(k, sp) = 1$ y $s > 1$. Puesto que k no es múltiplo de s, tenemos $\dfrac{1}{s} \le \dfrac{k}{s} - \left[\dfrac{k}{s}\right] \le \dfrac{s-1}{s}$. Por tanto, como $\dfrac{[k/s]}{p} \le \dfrac{k}{sp} \le \dfrac{[k/s]+1}{p}$, se verifican las dos desigualdades siguientes:

$$\left(\frac{k}{sp} + \frac{1}{sp}\right) - \frac{[k/s]}{p} \le \frac{1}{p} \quad \text{y} \quad \frac{[k/s]+1}{p} - \left(\frac{k}{sp} - \frac{1}{sp}\right) \le \frac{1}{p}.$$

De aquí se deduce que $I = C(k/sp, 1/sp)$ está contenido en los círculos $C\left(\frac{[k/s]}{p},\ 1/p\right)$ y $C\left(\frac{[k/s]+1}{p},\ 1/p\right)$. Puesto que $\left[\frac{k}{s}\right]$ y $\left[\frac{k}{s}\right] + 1$ no pueden ser simultáneamente múltiplos de p, como mínimo uno de estos círculos pertenece a $I_{\Gamma_0'(p)}$ (de hecho pertenece a $I^{\max}_{\Gamma_0'(p)}$ por tener radio $1/p$). Ello demuestra que I no es maximal, completando *(ii)*. □

De forma análoga, se demuestran los resultados correspondientes a $p = 1$.

Proposición 3.2. *Consideramos el conjunto $\Gamma_0'(1)$. Entonces,*

(i) $I_{\Gamma_0'(1)} = \{C(k/s,\ 1/s) : k \in \mathbb{Z},\ s \in \mathbb{N},\ \operatorname{mcd}(k, s) = 1\}$.

(ii) $I^{\max}_{\Gamma_0'(1)} = \{C(k,\ 1) : k \in \mathbb{Z}\}$.

Corolario 3.3. *Sea p un número primo o $p = 1$. La intersección de un círculo de isometría no maximal con un círculo de isometría maximal, si es diferente del vacío, se encuentra siempre en $\mathbb{R}$. Además, la intersección de tres círculos maximales distintos siempre es vacía.*

Para ilustrar los resultados anteriores véase la figura 4, que representa los círculos de isometría de $\Gamma'_0(3)$ para $s < 8$ y $\left|\frac{k}{3s}\right| < 1$.

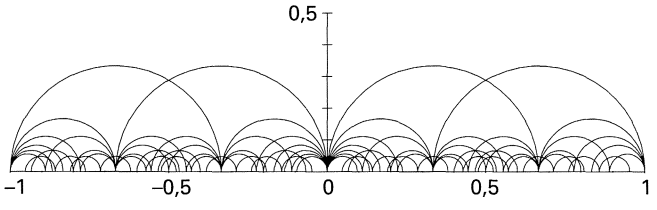

Figura 3. Círculos de isometría de $\Gamma_0'(3)$.

Notemos que no estamos en las hipótesis de la proposición 2.11; los radios son acotados, pero la distancia de los centros al 0 no está acotada, y un círculo puede ser círculo de isometría de homografías distintas. En general, el radio y el centro del círculo de isometría determinan los valores de c y d, excepto el signo. La condición que el determinante valga 1 nos da, entonces, una relación entre a y b, que tiene distintas soluciones.

Teorema 3.4. *Sea p un número primo, $p > 2$. Entonces,*

$$\mathcal{D}(\Gamma_0(p)) = \left\{ z \in \mathcal{H} : |\mathrm{Re}(z)| \le 1/2,\ \left| z - \frac{k}{p} \right| \ge \frac{1}{p},\ k \in \mathbb{Z},\ 0 < |k| \le \frac{p-1}{2} \right\}$$

es un dominio fundamental de $\Gamma_0(p)$ en $\mathcal{H}$.

Demostración. Consideramos el dominio fundamental de Γ_∞ calculado en el inicio de la sección y aplicamos 2.18, con lo cual obtenemos

$$\mathcal{D}(\Gamma_0(p)) = \{ z \in \mathcal{H} : |\mathrm{Re}(z)| \le 1/2 \} \cap \overline{\bigcap_{I \in I^{\max}_{\Gamma_0(p)}} \mathrm{ext}(I)}.$$

Completamos la demostración utilizando la descripción de los círculos de isometría maximales dada en el teorema anterior. Los únicos círculos de isometría maximales que tienen intersección significativa con $\mathcal{D}(\Gamma_\infty)$ son exactamente los círculos $C(k/p,\ 1/p)$ tales que $0 < |k| \le \frac{p-1}{2}$. □

Proposición 3.5. *Para los grupos $\Gamma_0(1)$ y $\Gamma_0(2)$, los dominios fundamentales son*

$$\mathcal{D}(\Gamma_0(1)) = \{ z \in \mathcal{H} : |\mathrm{Re}(z)| \le 1/2,\ |z| > 1 \},$$

$$\mathcal{D}(\Gamma_0(2)) = \left\{ z \in \mathcal{H} : |\mathrm{Re}(z)| \le 1/2, \left| z - \frac{k}{2} \right| \ge \frac{1}{2},\ k = \pm 1 \right\}.$$

Demostración. De forma análoga al teorema anterior, consideramos el dominio fundamental $\mathcal{D}(\Gamma_\infty)$ y aplicamos 2.18. Usando la descripción de los círculos de isometría maximales, es fácil ver que es suficiente considerar el círculo de isometría maximal $C(0,1)$ para el caso $p = 1$, y los círculos $C(-1/2, 1/2)$ y $C(1/2, 1/2)$ para $p = 2$.

Denotamos $\mathcal{J}(p)$ el conjunto de círculos de isometría maximales que determinan aristas del dominio fundamental $\mathcal{D}(\Gamma_0(p))$. Por los resultados anteriores, si p es un número primo $p > 2$, $\mathcal{J}(p) = \{ C(k/p,\ 1/p) : k \in \mathbb{Z},\ 0 < |k| \le \frac{p-1}{2},\ \mathrm{mcd}(k, p) = 1 \}$; el caso $p = 1$ da simplemente $\mathcal{J}(1) = \{ C(0, 1) \}$; para $p = 2$ obtenemos $\mathcal{J}(2) = \{ C(-1/2, 1/2), C(1/2, 1/2) \}$. Veamos que este conjunto de círculos maximales satisface una propiedad técnica, importante para obtener los principales resultados posteriores.

Lema 3.6. *Sea p un número primo o $p = 1$. Dado $I \in \mathcal{J}(p)$ existe una única homografía $\gamma \in \Gamma_0'(p)$ tal que $I = I_\gamma$ e $I_{\gamma^{-1}} \in \mathcal{J}(p)$.*

Demostración. Sea $I = C(k/p,\ 1/p) \in \mathcal{J}(p)$. Determinaremos de forma única una homografía $\gamma \in \Gamma_0'(p)$ tal que $I = I_\gamma \in \mathcal{J}(p)$ e $I_{\gamma^{-1}} \in \mathcal{J}(p)$. Cualquier $\gamma = \begin{pmatrix} a & b \\ p & -k \end{pmatrix}$, con $a, b \in \mathbb{Z}$ tales que $-ak - bp = 1$, satisface $\gamma \in \Gamma_0'(p)$ e $I = I_\gamma$. Debe escogerse una solución $\{a, b\}$ de $-ak - bp = 1$ tal que $I_{\gamma^{-1}} = C(a/p,\ 1/p)$ pertenezca a $\mathcal{J}(p)$. Si $p > 2$, tomamos la única solución con $|a| \le \frac{p-1}{2}$, $a \ne 0$. Si $p = 1$, tenemos $k = 0$ y tomamos $a = 0$ y $b = -1$ y se cumple $\gamma = \gamma^{-1}$, $I_\gamma = C(0, 1)$. Para $p = 2$, con $k = -1$ y $a = b = -1$ se tiene $I_\gamma = C(-1/2, 1/2)$, $I_{\gamma^{-1}} = C(1/2, 1/2)$. □

Notación 3.7. *Consideremos el dominio fundamental de $\Gamma_0(p)$, $\mathcal{D}(\Gamma_0(p))$. Denotamos $n(p)$ el número total de sus vértices. Denotamos $n_2(p)$, $n_3(p)$, $n_\infty(p)$ y $n_1(p)$ el número de vértices elípticos de orden 2, elípticos de orden 3, parabólicos y accidentales, respectivamente. Análogamente, $e_2(p)$, $e_3(p)$, $e_\infty(p)$ y $e_1(p)$ denotan el número de ciclos elípticos de orden 2, elípticos de orden 3, parabólicos y accidentales, respectivamente. Denotamos $V_h(p)$ el volumen hiperbólico de $\mathcal{D}(\Gamma_0(p))$.*

Proposición 3.8. *Sea p un número primo, $p > 2$. El dominio fundamental de $\Gamma_0(p)$, $\mathcal{D}(\Gamma_0(p))$, tiene las siguientes propiedades.*

(i) *Los puntos $z_j = \frac{2j - 2 - p}{2p} + \frac{\sqrt{3}}{2p} i$ para $j = 1, \ldots, \frac{p+1}{2} - 1$, $z_{\frac{p+1}{2}} = 0$, $z_j = \frac{2j - p}{2p} + \frac{\sqrt{3}}{2p} i$ para $j = \frac{p+1}{2} + 1, \ldots, p$ y $z_{p+1} = \infty$ son vértices de $\mathcal{D}(\Gamma_0(p))$.*

(ii) *El ángulo interior a $\mathcal{D}(\Gamma_0(p))$ en los vértices $z_{\frac{p+1}{2}} = 0$ y $z_{p+1} = \infty$ es 0; en los vértices z_1 y z_p es $\pi/3$ y en el resto de vértices z_j es $2\pi/3$.*

(iii) *$\mathcal{D}(\Gamma_0(p))$ es un polígono hiperbólico con un número par, $n(p) = p + 1 + n_2(p)$, de vértices y aristas.*

(iv) *El volumen hiperbólico de $\mathcal{D}(\Gamma_0(p))$ es $V_h(p) = (p + 1)\frac{\pi}{3}$.*

Demostración. Consideremos los puntos de $\mathcal{H}$ o $\mathbb{R}$ determinados por las intersecciones de los círculos de isometría maximales pertenecientes a $J(p)$, y las intersecciones de las dos semirectas $\mathrm{Re}(z) = -1/2$ y $\mathrm{Re}(z) = 1/2$ con dichos círculos. Todos ellos forman parte del conjunto de vértices del dominio fundamental. Denotaremos z_j, $j = 1,\ldots, p$ dichos vértices, según orden creciente de la parte real. Pongamos además $z_{p+1} = \infty$, vértice que proviene directamente de $\mathcal{D}(\Gamma_\infty)$. Un simple cálculo demuestra que, para $j = 2,\ldots, \frac{p+1}{2} - 1$, se tiene $z_j = C\left(\frac{2(j-1)-1-p}{2p}, \frac{1}{p}\right) \cap C\left(\frac{2j-1-p}{2p}, \frac{1}{p}\right) = \frac{2j-2-p}{2p} + \frac{\sqrt{3}}{2p}i$; el vértice $z_{\frac{p+1}{2}} = C(-1/p, 1/p) \cap C(1/p, 1/p) = 0$; y, para $j = \frac{p+1}{2} + 1, \ldots, p - 1$, se tiene $z_j = C\left(\frac{2j-1-p}{2p}, \frac{1}{p}\right) \cap C\left(\frac{2(j+1)-1-p}{2p}, \frac{1}{p}\right) = \frac{2j-p}{2p} + \frac{\sqrt{3}}{2p}i$. Finalmente, los vértices z_1 y z_p se obtienen intersecando los círculos de isometría correspondientes, $C\left(-\frac{p-1}{2p}, \frac{1}{p}\right)$ y $C\left(\frac{p-1}{2p}, \frac{1}{p}\right)$, con las semirectas $\mathrm{Re}(z) = -1/2$ y $\mathrm{Re}(z) = 1/2$, respectivamente. Estos dos vértices también pueden calcularse como la intersección de dos círculos de isometría maximales, $z_1 = C\left(-\frac{p+1}{2p}, \frac{1}{p}\right) \cap C\left(-\frac{p-1}{2p}, \frac{1}{p}\right)$, $z_p = C\left(\frac{p-1}{2p}, \frac{1}{p}\right) \cap C\left(\frac{p+1}{2p}, \frac{1}{p}\right)$, con $C\left(-\frac{p+1}{2p}, \frac{1}{p}\right)$ y $C\left(\frac{p+1}{2p}, \frac{1}{p}\right)$ no pertenecientes a $J(p)$. Observemos que es posible que z_j, $j = 1,\ldots, p + 1$, no sean todos los vértices del dominio fundamental, ya que no sabemos si contienen los puntos elípticos de orden 2 incluidos en la frontera del dominio fundamental $\mathcal{D}(\Gamma_0(p))$, considerados también vértices.

Para demostrar *(ii)*, denotemos θ_j el ángulo interior a $\mathcal{D}(\Gamma_0(p))$ en el vértice z_j. Claramente $\theta_{\frac{p+1}{2}} = \theta_{p+1} = 0$. Observemos que θ_j toma el mismo valor para $j = 2,\ldots, \frac{p+1}{2} - 1, \frac{p+1}{2} + 1,\ldots, p - 1$; denotémoslo θ. Tenemos además $\theta_1 = \theta_p = \theta/2$. Completamos la demostración de *(ii)* probando $\theta = 2\pi/3$. En efecto, tomando por ejemplo $j = \frac{p+1}{2} + 1$, los vectores directores de las rectas tangentes a los círculos $C(1/p, 1/p)$ y $C(2/p, 1/p)$ son $(-1, 1/\sqrt{3})$ y $(1, 1/\sqrt{3})$, respectivamente, y forman un ángulo $\theta = 2\pi/3$.

La figura resultante es un polígono hiperbólico de $\mathcal{H}$, ya que tanto los arcos de los círculos de isometría como el par de semirectas provinentes de $\mathcal{D}(\Gamma_\infty)$ son segmentos de rectas hiperbólicas. En el apartado *(i)* se han explicitado un número par de vértices, $p + 1$. Deben añadirse, si hay lugar, los puntos elípticos de orden 2 contenidos en la frontera de $\mathcal{D}(\Gamma_0(p))$, distintos de los anteriores. Ahora bien, gracias a 1.6 y a la simetría del dominio, el número de vértices elípticos es también par, con lo cual obtenemos que el número total de vértices sigue siendo par. A partir de la paridad del número de vértices, se deduce directamente que el número de aristas es también par, y coincide con el anterior, por tratarse de un polígono hiperbólico. Notemos que la existencia de vértices elípticos de orden 2, distintos de z_1 y z_p, incrementa el número de aristas en la misma cantidad en que se incrementan los vértices.

Vamos a precisar el número de vértices total. Recordemos que un ciclo de puntos elípticos de orden 2 tiene suma de ángulos en sus vértices igual a π, por 2.19. Notemos también que los vértices z_1 y z_p son equivalentes, ya que $T(z_1) = z_p$. Utilizando las dos afirmaciones anteriores y los ángulos calculados en *(ii)*, es obvio que, para $p > 2$, los vértices z_j no serán nunca elípticos de orden 2. Así, a los vértices anteriores deben añadirse exactamente $n_2(p)$ vértices, por lo que el número total de vértices será exactamente $p + 1 + n_2(p)$. Esto completa la demostración de *(iii)*.

Calculamos el volumen hiperbólico a partir de la expresión $V_h = (n(p) - 2)\pi - (\theta_1 + \cdots + \theta_n)$, donde $\theta_1,\ldots, \theta_{n(p)}$ son los ángulos en los vértices (cf. [4]). Consideremos, en primer lugar, los $p + 1$ vértices calculados en *(i)*. La suma de los ángulos en estos vértices es $(p - 2)\frac{2\pi}{3}$. Notemos que no es necesario considerar los vértices elípticos de orden 2, ya que el ángulo en cada uno de estos vértices es π por lo que no contribuyen al volumen del polígono hiperbólico. Así, $V_h(p) = (p + 1 - 2)\pi - \frac{2}{3}(p - 2)\pi = (p + 1)\frac{\pi}{3}$. □

Conservaremos la notación de los vértices z_j para el resto de la sección.

Lema 3.9 *Sea $z \in \mathcal{H}$, $z \in I$ con $I \in \mathcal{I}^{\max}_{\Gamma_0(p)}$. Entonces, z es un punto elíptico de orden 3 si, y sólo si, existe $\gamma \in \Gamma_0'(p)$ tal que $I = I_\gamma$ y $\{z\} = I_\gamma \cap I_{\gamma^{-1}}$.*

Demostración. Es inmediato ver que se trata de una condición suficiente. En efecto, si $\gamma \in \Gamma_0'(p)$ es una homografía tal que $z \in I_\gamma \cap I_{\gamma^{-1}}$, aplicando 2.10 y 2.8, se obtiene que γ es una homografía elíptica de orden 3 que tiene z como punto fijo en $\mathcal{H}$. Por tanto, z es elíptico de orden 3.

Recíprocamente, veamos que se trata de una condición necesaria. Sea z elíptico de orden 3, $z \in I$ con $I \in \mathcal{I}^{\max}_{\Gamma_0'(p)}$. Sea $\sigma \in \Gamma_0'(p)$ una homografía elíptica de orden 3 tal que $\sigma(z) = z$. Aplicando 2.8 se tiene $z \in I_\sigma \cap I_{\sigma^{-1}}$; en particular, z pertenece a los círculos de isometría I, I_σ e $I_{\sigma^{-1}}$, dos de ellos distintos como mínimo. Supongamos $I \neq I_{\sigma^{-1}}$. Como $z \in \mathcal{H}$, aplicando 3.3, se tiene que $I_{\sigma^{-1}} \in \mathcal{I}^{\max}_{\Gamma_0(p)}$. De aquí, I_σ también es maximal. Pero z no puede pertenecer a más de dos círculos de isometría maximales, por tanto $I = I_\sigma$. Así, tomamos $\gamma = \sigma$. Si fuera $I = I_{\sigma^{-1}}$, sería $I \neq I_\sigma$ y tomaríamos $\gamma = \sigma^{-1}$. □

Teorema 3.10. *Consideremos el grupo $\Gamma_0(p)$, $p > 2$, actuando sobre el semiplano de Poincaré. Entonces el dominio fundamental $\mathcal{D}(\Gamma_0(p))$ satisface:*

(i) $n_\infty(p) = e_\infty(p) = 2$.

Los ciclos parabólicos son $\{z_{\frac{p+1}{2}}\} = \{0\}$ y $\{z_{p+1}\} = \{\infty\}$.

(ii) $n_2(p) = e_2(p) = \begin{cases} 0 & si\ p \equiv 3 \mod 4, \\ 2 & si\ p \equiv 1 \mod 4. \end{cases}$

Si $p \equiv 1 \mod 4$, *los ciclos elípticos de orden* 2 *son*

$$\{w_{2,1}\} = \left\{\frac{-k_0}{p} + \frac{1}{p}i\right\}, \quad \{w_{2,2}\} = \left\{\frac{+k_0}{p} + \frac{1}{p}i\right\},$$

con $0 < k_0 \leq \frac{p-1}{2}$, $k_0^2 \equiv -1 \mod p$.

(iii) $n_3(3) = 2$ y $e_3(3) = 1$.

Para $p = 3$, *el ciclo elíptico de orden* 3 *es* $\{z_1, z_3\}$.

(iv) *Si* $p > 3$, $n_3(p) = e_3(p) = \begin{cases} 0 & si\ p \equiv 2 \mod 3, \\ 2 & si\ p \equiv 1 \mod 3. \end{cases}$

Si $p \equiv 1 \mod 3$, *los ciclos elípticos de orden* 3 son

$$\{w_{3,1}\} = \left\{\frac{-2k_1 - 1}{2p} + \frac{1}{p}i\right\}, \{w_{3,2}\} = \left\{\frac{2k_1 + 1}{2p} + \frac{1}{p}i\right\},$$

con $k_1 \in \mathbb{Z}$, $0 < k_1 \leq (p-1)/2$, $k_1^2 + k_1 + 1 \equiv 0 \mod p$.

(v) $n_1(p) = p - 1 - n_3(p)$ *y* $e_1(p) = \dfrac{p - 2 - e_3(p)}{3}$.

Demostración. En primer lugar, veamos que los vértices 0 y ∞ son parabólicos. Para el vértice ∞, que proviene de $\mathcal{D}(\Gamma_\infty)$, es obvio ya que es el punto fijo de la homografía parabólica T, considerada anteriormente. El vértice 0 corresponde a la intersección de los círculos de isometría maximales tangentes $C(-1/p, 1/p)$ y $C(1/p, 1/p)$. Tomando $\sigma = \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix}$ se tiene $I_\sigma = C(-1/p, 1/p)$ y $I_{\sigma^{-1}} = C(1/p, 1/p)$. Aplicando 2.10 y 2.9, se tiene que σ es parabólica y tiene el punto 0 como punto fijo; con la expresión explícita de σ se llega a la misma conclusión aplicando directamente las definiciones. Además se deduce, también de ambos modos, que $\sigma(z_{\frac{p+1}{2}-1}) = z_{\frac{p+1}{2}+1}$. El dominio $\mathcal{D}(\Gamma_0(p))$ no tiene otros vértices en $\mathbb{R}$, por lo que no hay otros vértices parabólicos. Finalmente, se comprueba que no son equivalentes, ya que $\gamma(0) = \infty$ implicaría $\det \gamma \neq 1$. Así, hay exactamente dos ciclos parabólicos, $\{z_{\frac{p+1}{2}}\} = \{0\}$ y $\{z_{p+1}\} = \{\infty\}$, lo cual completa la demostración de *(i)*.

Para demostrar *(ii)*, sea w un vértice de $\mathcal{D}(\Gamma_0(p))$ elíptico de orden 2. Recordemos que se ha probado que $w \neq z_j$, para todo $j = 1, \ldots, p$, $p > 2$. Entonces, existe un único círculo de isometría maximal $I \in \mathcal{J}(p)$ tal que $w \in I$, y el ángulo en w es π, cf. 2.8. Se deduce que los ciclos elípticos de orden 2 están formados por un solo vértice, y así $e_2(p) = n_2(p)$, que ya se ha visto que es un número par gracias a 1.6. Como el ciclo está formado por un solo vértice, las dos aristas adyacentes al vértice w se identifican entre sí, por lo que deben ser de igual longitud por 2.19; así w es el punto medio del arco de I que forma parte de la frontera del dominio fundamental. Por 3.1, tenemos $I = C(k/p, 1/p)$ para cierto k, $0 < |k| \leq \frac{p-1}{2}$ y por tanto $w = \frac{k}{p} + \frac{1}{p}i$. Veamos qué condiciones debe cumplir k para que w sea efectivamente un punto elíptico de orden 2 de $\Gamma_0(p)$. Observemos que $w \neq \in I'$ para cualquier círculo de isometría no maximal, $I' \in \mathcal{I}_{\Gamma_0'(p)} \backslash \mathcal{I}^{\max}_{\Gamma_0'(p)}$, por 3.3; es decir w sólo pertenece al círculo de isometría I. Así, por 2.8, w es elíptico de orden 2 si, y sólo si, $I = I_\gamma = I_{\gamma^{-1}}$, para cierta homografía elíptica de orden 2, $\gamma = \gamma^{-1}$. Como $I = C(k/p, 1/p)$, una tal homografía debe ser de la forma $\gamma = \begin{pmatrix} a & b \\ p & -k \end{pmatrix}$ para ciertos valores de $a, b \in \mathbb{Z}$ cumpliendo $-ak - bp = 1$ y $a = k$. Por tanto, w es elíptico de orden 2 si, y sólo si, $-k^2 - bp = 1$ tiene solución para algún $b \in \mathbb{Z}$. Por último, ello es equivalente a que -1 sea un residuo cuadrático módulo p, $\left(\dfrac{-1}{p}\right) = 1$, es decir $p \equiv 1 \mod 4$. En este caso, la ecuación $k^2 + bp = -1$ tiene dos únicas soluciones, k_0 y $-k_0$ con $0 < |k_0| \leq \frac{p-1}{2}$, que dan lugar a los dos vértices elípticos de orden 2 siguientes, claramente simétricos respecto al eje imaginario,

$$w_{2,1} = \frac{-k_0}{p} + \frac{1}{p}i, \quad w_{2,2} = \frac{k_0}{p} + \frac{1}{p}i.$$

Así pues, $e_2(p) = 2$ si $p \equiv 1 \mod 4$ y $e_2(p) = 0$ en caso contrario. Ello demuestra los resultados para los vértices elípticos de orden 2 enunciados en *(ii)*.

Consideremos a continuación los vértices elípticos de orden 3. Un ciclo de puntos elípticos de orden 3 tiene suma de ángulos en sus vértices igual a $2\pi/3$, por 2.19. Por tanto, utilizando 3.8 *(ii)*, un ciclo elíptico o bien está constituido por un solo vértice, entre $z_2, \ldots, z_{\frac{p+1}{2}-1}$, $z_{\frac{p+1}{2}+1}, \ldots, z_{p-1}$, o bien es el ciclo $\{z_1, z_p\}$.

Supongamos que z_1 es un punto elíptico de orden 3. Aplicando el lema 3.9, los círculos de isometría $C\left(-\frac{p+1/2}{p}, \frac{1}{p}\right)$ y $C\left(-\frac{p-1/2}{p}, \frac{1}{p}\right)$ corresponden a homografías inversas, lo cual da la ecuación $p^2 + 4bp = 3$, que sólo tiene solución para $p = 3$. Así, $\{z_1, z_p\}$ es un ciclo elíptico de orden 3 si, y sólo si, $p = 3$. En este caso, no hay más vértices que puedan ser elípticos de orden 3, por lo que tenemos $n_3(3) = 2$ y $e_3(3) = 1$, lo cual completa la demostración de *(iii)*.

Supongamos ahora $p > 3$, para demostrar *(iv)*. En primer lugar, recordemos que la homografía parabólica correspondiente al vértice 0 relacionaba los vértices $z_{\frac{p+1}{2}-1}$ y $z_{\frac{p+1}{2}+1}$, por lo que son equivalentes. De aquí se deduce que nunca son elípticos, porque sus ángulos suman $4\pi/3 > 2\pi/3$ (cf. 3.8). El mismo argumento de ángulos nos conduce a que los ciclos elípticos de orden 3 están formados por un solo vértice, por lo que $n_3(p) = e_3(p)$; además es un número par aplicando 1.6, de forma análoga al caso de orden 2.

Vamos a determinar de forma efectiva cuando hay vértices elípticos de orden 3. Supongamos que un vértice $z \in \mathcal{H}$, obtenido como intersección de dos círculos de isometría maximales consecutivos, es un punto elíptico de orden 3. Aplicando 3.9, estos dos círculos de isometría tienen que corresponder a aplicaciones inversas una de la otra, es decir $z = I_\gamma \cap I_{\gamma^{-1}}$, para cierta homografía elíptica $\gamma \in \Gamma_0'(p)$. La descripción explícita de $I^{\max}_{\Gamma_0'(p)}$ dada en 3.1 nos lleva a $I_\gamma = C(k/p, 1/p)$ y $I_{\gamma^{-1}} = C\big((k+1)/p, 1/p\big)$ para cierto valor de $k \in \mathbb{Z}$, $|k| \leq (p-1)/2$, $k \neq 0, -1$. Así, γ será de la forma $\begin{pmatrix} a & b \\ p & -k \end{pmatrix}$ cumpliendo $o_{\gamma^{-1}} = \dfrac{-a}{p} = \dfrac{k+1}{p}$; por lo tanto $a = -(k+1)$. Imponiendo $\det(\gamma) = 1$, obtenemos $-(k+1)k - bp = 1$ y reduciendo módulo p resulta $k^2 + k + 1 \equiv 0 \bmod p$, que tiene solución si, y sólo si, -3 es un residuo cuadrático módulo p. Esto demuestra que un vértice de $\mathcal{D}(\Gamma_0(p))$ es elíptico de orden 3 si, y sólo si, se obtiene de la forma $C(k/p, 1/p) \cap C\big((k+1)/p, 1/p\big)$ con $|k| \leq (p-1)/2$, $k^2 + k + 1 \equiv 0 \bmod p$. Por tanto, $e_3(p) = 0$ si $p \equiv 2 \bmod 3$ y $e_3(p) = 2$ si $p \equiv 1 \bmod 3$. En este último caso, los vértices elípticos son

$$w_{3,1} = \frac{-2k_1 - 1}{2p} + \frac{\sqrt{3}}{2p}\, i, \qquad w_{3,2} = \frac{2k_1 + 1}{2p} + \frac{\sqrt{3}}{2p}\, i,$$

donde $k_1 \in \mathbb{Z}$, $0 < k_1 \leq (p-1)/2$ es una solución de $k^2 + k + 1 \equiv 0 \bmod p$. Esto demuestra *(iv)*.

Los vértices accidentales son los vértices que no son ni elípticos ni parabólicos y se encuentran forzosamente entre los vértices z_j calculados en 3.8. Así, $n_1(p) = n(p) - n_\infty(p) - n_2(p) - n_3(p) = p - 1 - n_3(p)$. Teniendo en cuenta que la suma de ángulos en cada ciclo accidental tiene que ser 2π (cf. 3.8), obtenemos que los ciclos accidentales están formados por 3 vértices, excepto el ciclo accidental al que pertenecen z_1 y z_p, para $p > 3$, que tendrá 4. Por tanto $e_1(p) = \dfrac{p - 2 - e_3(p)}{3}$. □

Observación 3.11. *El dominio fundamental $\mathcal{D}(\Gamma_0(p))$, para $p > 3$, satisface que los ciclos elípticos y parabólicos consisten en un sólo vértice y que no hay vértices accidentales en $\mathbb{R}$.*

Notación 3.12. *Sea p un número primo fijado, $p > 2$. Para cada $k \in \mathbb{Z}$ con $0 < |k| \leq \frac{p-1}{2}$, denotamos*

$$\gamma_k = \begin{pmatrix} a & b \\ p & -k \end{pmatrix} \in \Gamma_0(p),$$

donde $a, b \in \mathbb{Z}$ vienen determinados unívocamente por las condiciones $-ak - bp = 1$ y $0 < |a| \leq \frac{p-1}{2}$. Notemos que $\gamma_{-1} = \gamma_1^{-1}$.

Proposición 3.13. *Sea p un número primo, $p > 2$. El grupo de homografías definido por $\Gamma_0(p)$ está generado por T, γ_1 y las homografías γ_k tales que $|a| \geq |k|$ si $|k| > 1$. Las relaciones entre dichos generadores son las siguientes:*

(i) $\gamma_{k_0}^2 = \gamma_{-k_0}^2 = \mathrm{Id}$, *si* $k_0 > 0$ con $k_0^2 \equiv -1 \bmod p$;

(ii) $\gamma_{k_1}^3 = \gamma_{-k_1-1}^3 = \mathrm{Id}$, *si* $k_1 > 0$ con $k_1^2 + k_1 + 1 \equiv 0 \bmod p$;

(iii) *una relación del tipo* $\gamma_{t_3}^{\varepsilon_{t_3}} \gamma_{t_2}^{\varepsilon_{t_2}} \gamma_{t_1}^{\varepsilon_{t_1}} = \mathrm{Id}$ *para cada ciclo accidental de* $\mathcal{D}(\Gamma_0(p))$ de la forma $\{z_{j_1}, z_{j_2}, z_{j_3}\}$ con $\gamma_{t_i}^{\varepsilon_{t_i}}(z_{j_i}) = z_{j_i+1}$, $z_{j_4} = z_{j_1}$, $\varepsilon_{t_i} = \pm 1$;

(iv) *la relación* $T^{-1}\gamma_{s_2}^{\varepsilon_{s_2}}\gamma_{s_1}^{\varepsilon_{s_1}}\gamma_{\frac{1-p}{2}} = \mathrm{Id}$, *para* $p > 3$, *que proviene del único ciclo accidental de* $\mathcal{D}(\Gamma_0(p))$ *que contiene cuatro vértices* $\{z_1, z_{a_1}, z_{a_2}, z_p\}$, *con* $\gamma_{\frac{1-p}{2}}(z_1) = z_{a_1}$, $\gamma_{t_1}(z_{a_1}) = z_{a_2}$ y $\gamma_{t_2}(z_{a_2}) = z_p$, $\varepsilon_{s_i} = \pm 1$.

Demostración. El dominio fundamental $\mathcal{D}(\Gamma_0(p))$ es un polígono hiperbólico con un número par de aristas identificadas dos a dos y, por 2.19, las homografías que aparejan las aristas forman una familia de generadores.

La traslación T aparea las dos aristas que son semirectas verticales, que provienen de las aristas de $\mathcal{D}(\Gamma_\infty)$, por lo que forma parte de la familia de generadores.

El lema 3.6 nos asegura que dado $I \in \mathcal{J}(p)$ existe una única $\gamma \in \Gamma_0'(p)$ tal que $I = I_\gamma$ e $I_{\gamma^{-1}} \in \mathcal{J}(p)$. Aplicando las propiedades de los círculos de isometría y las homografías, cf. 2.3 y 2.7–2.9, es claro que la homografía γ aparea las aristas que forman parte de los círculos I_γ e $I_{\gamma^{-1}}$. Recordemos que $\mathcal{J}(p)$ es precisamente el conjunto de círculos de isometría que dan lugar a aristas de $\mathcal{D}(\Gamma_0(p))$. Así el conjunto de homografías correspondientes a los círculos de isometría de $\mathcal{J}(p)$, cuya expresión explícita se da en la demostración del lema 3.6 y coincide con γ_k, bastan para aparejar las aristas de $\mathcal{D}(\Gamma_0(p))$ que son arcos de círculos de isometría. Obviamente, deben evitarse las repeticiones causadas por una homografía y su inversa, lo cual se realiza añadiendo la condición $|a| \geq |k|$, para $|k| > 1$. La homografía γ_1 identifica las dos aristas que se intersectan en el punto 0, por lo que será también un generador y, al igual que T, será un elemento de orden infinito.

A nivel de relaciones, sólo cabe recordar que se obtiene una relación para cada ciclo no parabólico, cf. 2.19. Así, los ciclos elípticos de orden 2 y 3, si los hay, nos aportan las relaciones $\gamma_{k_0}^2 = \gamma_{-k_0}^2 = \mathrm{Id}$ y $\gamma_{k_1}^3 = \gamma_{-k_1-1}^3 = \mathrm{Id}$, donde $k_0 > 0$ cumple $k_0^2 \equiv -1 \bmod p$ y $k_1 > 0$ cumple $k_1^2 + k_1 + 1 \equiv 0 \bmod p$, respectivamente. A partir de cada ciclo accidental obtenemos una relación de la forma indicada. □

La presentación obtenida en la proposición anterior tiene $(p + 1 + e_2(p))/2$ generadores y $e_1(p) + e_2(p) + e_3(p)$ relaciones. En general, no será una presentación minimal. Una forma de disminuir el número de relaciones y de generadores sería disminuir el número de ciclos accidentales, que no es propiamente un invariante del grupo y que depende del tipo de dominio fundamental escogido. De todas formas, no se puede realizar de forma indis-

criminada para todos los ciclos accidentales, ya que hay repeticiones de generadores entre las diferentes relaciones.

Finalmente, para la completitud de los resultados, consideremos los casos $p \leq 2$. Los dominios fundamentales correspondientes a $p = 1$ y $p = 2$ se encuentran en 3.5. Vamos a recuperar sus características principales en las proposiciones siguientes, que se demuestran utilizando también argumentos derivados de las propiedades de los círculos de isometría.

Proposición 3.14. *Consideremos el dominio fundamental del grupo modular* $\mathbf{SL}(2, \mathbb{Z})$, $D(\Gamma_0(1))$. *Entonces,*

(i) $\mathcal{D}(\Gamma_0(1))$ *tiene* $n(1) = 4$ *vértices:* $z_1 = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$, $z_2 = \frac{1}{2} + \frac{\sqrt{3}}{2}i$, $z_3 = \infty$ *y* $w_{2,1} = i$.

(ii) *El ángulo interior a* $\mathcal{D}(\Gamma_0(1))$ *en los vértices* z_1 y z_2 *es* $\pi/3$, *y en el vértice* $w_{2,1}$, *es* π.

(iii) *El volumen hiperbólico de* $\mathcal{D}(\Gamma_0(1))$ *es* $V_h(1) = \frac{\pi}{3}$.

(iv) $n_\infty(1) = e_\infty(1) = 1$; *el vértice parabólico es* ∞.

(v) $n_2(1) = e_2(1) = 1$; *el vértice elíptico de orden 2 es* $w_{2,1}$.

(vi) $n_3(1) = 2$ *y* $e_3(1) = 1$; *los vértices elípticos de orden 3 son* z_1 *y* z_2.

(vii) $n_1(1) = e_1(1) = 0$; *es decir, no hay vértices accidentales.*

(viii) $\mathrm{SL}(2, \mathbb{Z})$ *está generado por*

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad y \quad S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

con la relación $S^2 = 1$.

Demostración. En este caso, $J(1) = \{C(0, 1)\}$. El círculo de isometría $C(0, 1) = I_\sigma$ para $\sigma \in \Gamma_0(1)$ tal que $c = \pm 1$, $d = 0$, $b = -c$ y $a \in \mathbb{Z}$. Así, es el círculo de isometría de las homografías

$$\sigma_a = \begin{pmatrix} a & 1 \\ -1 & 0 \end{pmatrix}, \quad a \in \mathbb{Z}.$$

Para $|a| > 2$, el centro del círculo $I_{\sigma_a^{-1}}$ es a; en este caso los círculos $I_{\sigma_a^{-1}}$ y I_{σ_a} no se cortan y σ_a y σ_a^{-1} son transformaciones hiperbólicas.

Se tiene que σ_a es elíptico si, y sólo si, $|a| < 2$. Para $a = 0$, obtenemos $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. En este caso $\sigma_a = \sigma_a^{-1}$, por lo que es una homografía elíptica de orden 2. El punto elíptico correspondiente es $w_{2,1} = i$. Para $a = \pm 1$, obtenemos $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$, y $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$, las dos de orden 3. Los puntos elípticos correspondientes son $z_1 = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$ y $z_2 = \frac{1}{2} + \frac{\sqrt{3}}{2}i$, respectivamente. Observemos que los 3 puntos elípticos son vértices del dominio fundamental que hemos encontrado. Se obtienen también directamente a partir del círculo de isometría, utilizando 2.8 y 2.19*(iv)*, como se ha hecho en el caso general. Explicitando las homografías que corresponden a los círculos, tenemos $w_{2,1} \in \mathrm{I}_S$, $z_1 = I_{ST} \cap I_{(ST)^{-1}} = C(-1, 1) \cap C(0, 1)$, $z_2 = I_{TS} \cap I_{(TS)^{-1}} = C(0, 1) \cap C(1, 1)$.

Las homografías S y T son las que identifican las aristas del dominio fundamental dos a dos; por lo tanto, forman una familia de generadores del grupo modular $\mathbf{SL}(2, \mathbb{Z})$, con la relación $S^2 = 1$. □

De forma análoga se demuestra la proposición siguiente, para el caso $p = 2$.

Proposición 3.15. *Sea* $\mathcal{D}(\Gamma_0(2))$ *el dominio fundamental de* $\Gamma_0(2)$ *en* $\mathcal{H}$. *Entonces,*

(i) $n(2) = 4$. *Explícitamente,* $z_1 = \frac{-1}{2} + \frac{1}{2}i$, $z_2 = 0$, $z_3 = \frac{1}{2} + \frac{1}{2}i$ y $z_4 = \infty$.

(ii) *El ángulo interior a* $\mathcal{D}(\Gamma_0(2))$ *en los vértices* z_1 y z_3 *es* $\pi/2$, *y en el vértice* z_2 es 0.

(iii) *El volumen hiperbólico de* $\mathcal{D}(\Gamma_0(2))$ *es* $V_h(2) = \pi$.

(iv) $n_\infty(2) = e_\infty(2) = 2$; *los ciclos parabólicos son* $\{0\}$ *y* $\{\infty\}$.

(v) $n_2(2) = 2$ *y* $e_2(2) = 1$; *el ciclo elíptico es* $\{z_1, z_3\}$.

(vi) $n_3(2) = 0$; *es decir, no hay vértices elípticos de orden 3.*

(vii) $n_1(2) = 0$; *es decir, no hay vértices accidentales.*

(viii) $\Gamma_0(2)$ *está generado por*

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad \gamma_1 = \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix},$$

con la relación $(\gamma_1 T)^2 = 1$.

4. EJEMPLOS

En esta sección, presentamos varios ejemplos con el espíritu de ilustrar las propiedades de los dominios fundamentales construidos para $\Gamma_0(p)$, que difieren de otros dominios fundamentales conocidos (cf. [2]). Quizás la principal diferencia sea su gran simetría y su construcción sistemática, fácilmente implementable.

De hecho, se ha implementado un paquete en MapleV, siguiendo los resultados de la sección 3. El paquete requiere como único dato de entrada el número primo p. Como aplicación principal, dicho paquete permite obtener la representación gráfica del dominio fundamental $\mathcal{D}(\Gamma_0(p))$.

Con ánimo de completitud, en el programa se han incluido también instrucciones para calcular algunos invariantes de la curva modular $X_0(p)$ asociada al grupo $\Gamma_0(p)$. Para ello se han usado las fórmulas simplificadas obtenidas en la sección anterior, a partir de las propiedades de los círculos de isometría y del dominio fundamental construido, aunque no dependen de éste.

El programa contiene instrucciones para obtener toda la información disponible referente al dominio fundamental $\mathcal{D}(\Gamma_0(p))$, para cualquier número primo p. Así, de forma interactiva, proporciona los cardinales de los conjuntos de vértices, aristas, vértices elípticos, vértices accidentales, ciclos elípticos, ciclos accidentales, etc. Los resultados sobre vértices y ciclos son explícitos: calcula todos los vértices, los clasifica y los organiza en ciclos. También permite obtener las parejas de aristas y las homografías que las aparejan.

A nivel de resultados sobre el grupo, se obtiene una presentación explícita de $\Gamma_0(p)$, con generadores y relaciones.

A continuación se incluyen ejemplos explícitos para algunos números primos p, seleccionados de forma que corresponden a curvas modulares de género 0, 1, 2 y 3.

Las figuras 5 y 6 reproducen el dominio fundamental para los grupos $\Gamma_0(3)$ y $\Gamma_0(13)$, respectivamente. Ambos dan lugar a curvas modulares de género 0, $X_0(3)$ y $X_0(13)$. En ambos casos se han señalado los vértices elípticos. El caso $p = 3$ es el único con $p > 2$ en que los vértices z_1 y z_p son elípticos. El caso $p = 13$ se incluye como ejemplo de dominio fundamental con el máximo número posible de ciclos elípticos. Para $p = 13$, se han recopilado los datos calculados en la tabla 1.

En la figura 7, se representa el dominio fundamental $\mathcal{D}(\Gamma_0(11))$, asociado a la curva modular $X_0(11)$ de género 1. Notemos que no posee ningún vértice elíptico. Los vértices y los ciclos accidentales, y una presentación del grupo, se explicitan en la tabla 2.

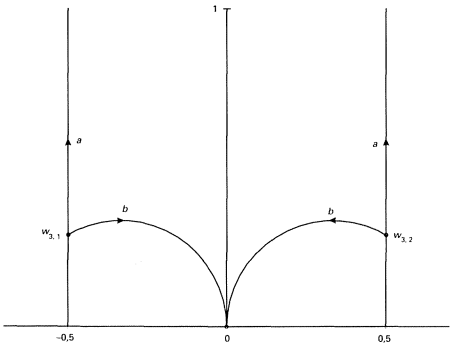

Figura 5. Dominio fundamental de $\Gamma_0(3)$.

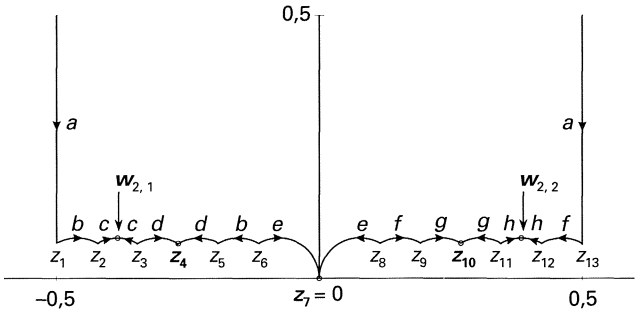

Figura 6. Dominio fundamental de $\Gamma_0(13)$.

Tabla 1. $\Gamma_0(13)/\pm\mathrm{Id}$

k	$n_k(13)$	$e_k(13)$	Ciclos de orden k de $\Gamma_0(13)$
∞	2	2	$\{0\}$, $\{\infty\}$
2	2	2	$\{w_{2,1}\} = \{\frac{-5}{13} + \frac{1}{13}i\}$, $\{w_{2,2}\} = \{\frac{5}{13} + \frac{1}{13}i\}$
3	2	2	$\{z_4\} = \{\frac{-7}{26} + \frac{\sqrt{3}}{26}i\}$, $\{z_{10}\} = \{\frac{7}{126} + \frac{\sqrt{3}}{26}i\}$
1	10	3	$\{z_1, z_{13}, z_8, z_6\}$, $\{z_2, z_3, z_5\}$, $\{z_{12}, z_{11}, z_9\}$

Generadores	Relaciones
$\gamma_5, \gamma_{-5}, \gamma_3, \gamma_{-3}$ $T, \gamma_1, \gamma_2, \gamma_{-2}$	$\gamma_5^2 = \gamma_{-5}^2 = \mathrm{Id}$, $\gamma_3^3 = \gamma_{-3}^3 = \mathrm{Id}$, $\gamma_{-2}\gamma_1\gamma_2^{-1}T = \mathrm{Id}$, $\gamma_{-2}\gamma_{-3}^{-1}\gamma_{-5} = \mathrm{Id}$, $\gamma_2\gamma_3^{-3}\gamma_5 = \mathrm{Id}$

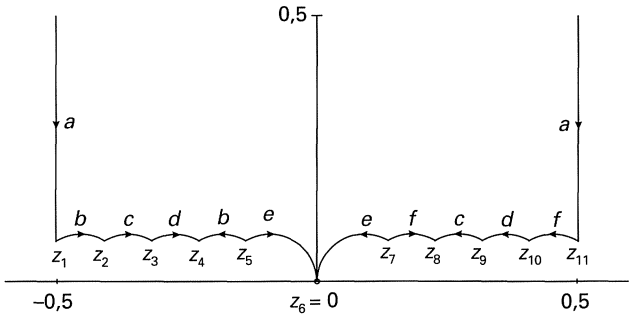

Figura 7. Dominio fundamental de $\Gamma_0(11)$.

Tabla 2. $\Gamma_0(11)/\pm\mathrm{Id}$

k	$n_k(11)$	$e_k(11)$	Ciclos de orden k de $\mathcal{D}(\Gamma_0(11))$
∞	2	2	$\{0\}$, $\{\infty\}$
2	0	0	
3	0	0	
1	10	3	$\{z_1, z_{11}, z_7, z_5\}$, $\{z_2, z_4, z_9\}$, $\{z_{10}, z_8, z_3\}$

Generadores	Relaciones
$T, \gamma_1, \gamma_2, \gamma_3, \gamma_{-2}, \gamma_{-3}$	$\gamma_{-2}\gamma_1\gamma_2^{-1}T = \mathrm{Id}$, $\gamma_3\gamma_{-3}\gamma_{-5}^{-1} = \mathrm{Id}$, $\gamma_3^{-3}\gamma_3\gamma_2^{-1} = \mathrm{Id}$

La figura 8 contiene la representación del dominio fundamental para el caso $p = 23$. Corresponde al menor valor de p, número primo, tal que $X_0(p)$ tiene género 2. Observemos que tampoco tiene ciclos elípticos. Los ciclos accidentales y una presentación del grupo se muestran en la tabla 3.

Finalmente, en la tabla 4 se muestran los datos referentes al grupo $\Gamma_0(41)$ y al dominio fundamental $\mathcal{D}(\Gamma_0(41))$, que corresponde a una curva modular de género 3.

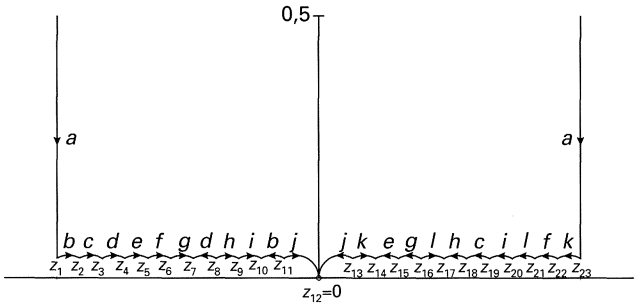

Figura 8. Dominio fundamental de $\Gamma_0(23)$.

Tabla 3. $\Gamma_0(23)/\pm\mathrm{Id}$

k	$n_k(23)$	$e_k(23)$	Ciclos de orden k de $\mathcal{D}(\Gamma_0(23))$
∞	2	2	$\{0\}$, $\{\infty\}$
2	0	0	
3	0	0	
1	22	7	$\{z_1, z_{23}, z_{13}, z_{11}\}$, $\{z_2, z_{10}, z_{19}\}$, $\{z_3, z_8, z_{18}\}$ $\{z_4, z_{15}, z_7\}$, $\{z_{22}, z_{14}, z_5\}$ $\{z_{21}, z_{16}, z_6\}$, $\{z_{20}, z_9, z_{17}\}$

Generadores	Relaciones
T, γ_1, γ_2, γ_3, γ_4, γ_5, γ_7 γ_{-2}, γ_{-3}, γ_{-4}, γ_{-5}, γ_{-7}	$\gamma_{-2}\gamma_1\gamma_2^{-1}T=\mathrm{Id}$, $\gamma_7\gamma_{-3}\gamma_{-2}^{-1}=\mathrm{Id}$, $\gamma_7\gamma_{-4}\gamma_{-5}^{-1}=\mathrm{Id}$, $\gamma_{-5}\gamma_4\gamma_3^{-1}=\mathrm{Id}$, $\gamma_{-7}\gamma_3\gamma_2^{-1}=\mathrm{Id}$, $\gamma_{-7}\gamma_4\gamma_5^{-1}=\mathrm{Id}$, $\gamma_5\gamma_{-4}\gamma_{-3}^{-1}=\mathrm{Id}$

Tabla 4. $\Gamma_0(41)/\pm\mathrm{Id}$

k	$n_k(41)$	$e_k(41)$	Ciclos de orden k de $\mathcal{D}(\Gamma_0(41))$
∞	2	2	$\{0\}$, $\{\infty\}$
2	2	2	$\{w_{2,1}\} = \{\frac{-9}{41} + \frac{1}{41}i\}$, $\{w_{2,2}\} = \{\frac{9}{41} + \frac{1}{41}i\}$
3	0	0	
1	40	13	$\{z_1, z_{20}, z_{22}, z_{41}\}$, $\{z_2, z_{34}, z_{19}\}$, $\{z_3, z_{37}, z_{33}\}$, $\{z_4, z_{10}, z_{36}\}$, $\{z_5, z_{39}, z_9\}$, $\{z_6, z_{32}, z_{38}\}$, $\{z_7, z_{24}, z_{31}\}$, $\{z_8, z_{40}, z_{23}\}$, $\{z_{11}, z_{18}, z_{35}\}$, $\{z_{12}, z_{13}, z_{17}\}$, $\{z_{14}, z_{27}, z_{16}\}$, $\{z_{15}, z_{28}, z_{26}\}$, $\{z_{25}, z_{29}, z_{30}\}$

Generadores	T, γ_1, γ_9, γ_{-9}, γ_2, γ_3, γ_5, γ_6, γ_{11}, γ_{12}, γ_{13}, γ_{16}, γ_{-2}, γ_{-3}, γ_{-4}, γ_{-5}, γ_{-6}, γ_{-11}, γ_{-12}, γ_{-13}, γ_{-16}
Relaciones	$\gamma_9^2 = \gamma_{-9}^2 = \mathrm{Id}$, $T^{-1}\gamma_2\gamma_1\gamma_2^{-1} = \mathrm{Id}$, $\gamma_{-2}\gamma_3^{-1}\gamma_{-13}^{-1} = \mathrm{Id}$, $\gamma_{13}\gamma_{-12}^{-1}\gamma_{-10}^{-1} = \mathrm{Id}$, $\gamma_{16}\gamma_{-11}\gamma_{12}^{-1} = \mathrm{Id}$, $\gamma_{-12}\gamma_{13}^{-1}\gamma_{-16} = \mathrm{Id}$, $\gamma_{16}^{-1}\gamma_{12}\gamma_{-11}^{-1} = \mathrm{Id}$, $\gamma_{11}\gamma_4\gamma_{-3}^{-1} = \mathrm{Id}$, $\gamma_3\gamma_{-2}^{-1}\gamma_{-13} = \mathrm{Id}$, $\gamma_{11}^{-1}\gamma_{-3}\gamma_4^{-1} = \mathrm{Id}$, $\gamma_{-4}\gamma_5\gamma_{-9} = \mathrm{Id}$, $\gamma_{-5}\gamma_6^{-1}\gamma_{-6}^{-1} = \mathrm{Id}$, $\gamma_6\gamma_{-5}^{-1}\gamma_{-6} = \mathrm{Id}$, $\gamma_{-4}^{-1}\gamma_9\gamma_5 = \mathrm{Id}$.

REFERENCIAS

1. T. M. Apostol (1976), *Modular functions and Dirichlet Series in Number Theory.* Springer.
2. P. Bayer & A. Travesa (eds.) (1992), *Corbes Modulars: Taules.* Seminari de Teoria de Nombres (UB-UAB-UPC), Barcelona. ISBN 84-604-3577-6.
3. Lester R. Ford (1951), *Automorphic functions.* Chelsea, 2nd edition.
4. C. L. Siegel (1971), *Topics in complex function theory v. II.* Wiley-Interscience.
5. H. Poincaré (1952), *Ouvres Completes.* Gauthier-Villlars.
6. G. Shimura (1971), *Introduction to the arithmetic theory of automorphic functions.* Princenton University Press.
7. J. Lehner (1964), *Discontinuous groups and automorphic functions.* Mathematical Surveys, **8**, American Mathematical Society.