Modularidad y conjetura *abc*

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

Resumen. En esta charla comenzaremos con un repaso de la teoría de formas modulares. Luego estudiaremos el problema de modularidad de curvas elípticas y finalizamos relacionando la modularidad con la conjetura *abc*.

1. Formas modulares

Recuérdese, de la charla anterior, la definición de subgrupo principal de congruencia $\Gamma_0(N)$, de la acción sobre el semiplano superior $\mathrm{SL}_2\,\mathbb{Z} \curvearrowright \mathfrak{h}$ y de las curvas modulares $X_0(N)$ e $Y_0(N)$.

Definición 1.1: Sea $\Gamma \leq \mathrm{SL}_2\,\mathbb{Z}$ un subgrupo y $k \in \mathbb{Z}$ un entero. Se dice que una función $f\colon \mathfrak{h}^* \to \mathbb{C}$ es una ***forma modular de peso k respecto a*** Γ (denotado $f \in \mathcal{M}_k(\Gamma)$) si:

1. f es holomorfa en $\mathfrak{h}$.
2. Para todo $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, se cumple que $f(\gamma \cdot \tau) = (c\tau + d)^k f(\tau)$.
3. f es holomorfa en las cúspides (i.e., en los puntos de $\mathbb{P}^1(\mathbb{Q})$).

Se dice que una forma modular f es ***cuspidal*** (denotado $f \in \mathcal{S}_k(\Gamma)$) si f se anula en las cúspides.

Observación 1.1.1: Considere el grupo de congruencia $\Gamma_0(N)$. Nótese que el elemento $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_0(N)$, por lo que, el axioma 2, implica que $f(\tau + 1) = f(T \cdot \tau) = f(\tau)$, es decir, f es 1-periódica y, por tanto, admite una expansión en serie de Fourier:

$$f(q) = \sum_{n=-\infty}^{\infty} a_n q^n, \qquad q = \exp(2\pi \mathrm{i}\,\tau).$$

Ahora bien, por el axioma 3, no puede poseer un polo en $\infty \in \mathfrak{h}^*$, de modo que $a_n = 0$ para todo $n < 0$. Si tomamos el límite $\tau \to \mathrm{i}\infty$, vemos que $q \to 0^+$, por lo que el valor de una forma modular en la cúspide $\infty \in \mathfrak{h}^*$ es a_0. En consecuencia, si f es cuspidal, se expande en serie de Fourier:

$$f(q) = \sum_{n=1}^{\infty} a_n q^n, \qquad q = \exp(2\pi \mathrm{i}\,\tau). \tag{1}$$

Fecha: 21 de junio de 2024.

Corolario 1.1.2: Para todo subgrupo $\Gamma \leq \mathrm{SL}_2\,\mathbb{Z}$ y $k \in \mathbb{Z}$ entero, los conjuntos $\mathcal{M}_k(\Gamma)$ y $\mathcal{S}_k(\Gamma)$ son $\mathbb{C}$-espacios vectoriales.

Lema 1.2.A: Sean $N \geq 1$, $k \in \mathbb{Z}$ enteros y sea $p \nmid N$ un número primo. Dada una forma modular $f \in \mathcal{M}_k\big(\Gamma_0(N)\big)$, la función

$$T_p(f) := \frac{1}{p}\sum_{j=0}^{p-1} f\left(\frac{\tau+j}{p}\right) + p^{k-1} f(p\tau) \tag{2}$$

es también una forma modular de peso k respecto a $\Gamma_0(N)$.

Demostración: Cfr. Serre [**3,** pág. 101], Prop. VII.11. □

Definición 1.2: Sean $N \geq 1$, $k \in \mathbb{Z}$ enteros y sea $p \nmid N$ un número primo. Se define el ***operador de Hecke*** $T_p\colon \mathcal{M}_k\big(\Gamma_0(N)\big) \to \mathcal{M}_k\big(\Gamma_0(N)\big)$ como la función dada por la fórmula (2). Definiendo $T_1 := \mathrm{Id}$, podemos dar la siguiente definición recursiva

$$T_{p^{r+1}} = T_p \circ T_{p^r} - p^{k-1} T_{p^{r-1}}.$$

Tratemos de hacer el cálculo explícito de $T_p f$ en términos de la expansión de Fourier, donde a_n denota el $\mathbb{C}$-funcional que extrae el n-ésimo coeficiente. Por linealidad nótese que podemos analizar un sumando a la vez:

$$a_n(p^{k-1} f(p\tau)) = a_n\left(p^{k-1}\sum_{n=0}^{\infty} a_n(f)(q^p)^n\right) = \begin{cases} p^{k-1} a_{n/p}(f), & p \mid n, \\ 0, & p \nmid n. \end{cases}$$

Para el otro sumando, vemos que

$$a_n\left(\frac{1}{p}\sum_{j=0}^{p-1} f\left(\frac{\tau+j}{p}\right)\right) = a_n\left(\frac{1}{p}\sum_{n=0}^{\infty} a_n(f) q^{n/p}\left(\sum_{j=0}^{p-1} e^{\frac{2\pi}{p}\mathrm{i}\, jn}\right)\right),$$

ahora bien, $e^{2\pi/p\mathrm{i}} =: \zeta_p$ es una raíz primitiva p-ésima de la unidad, o si se quiere, un generador del grupo $\mu_p \cong \mathbb{Z}/p\mathbb{Z}$. Hay dos casos: si $p \nmid n$, entonces ζ_p^n también es una raíz primitiva, luego la suma de ζ_p^{jn} recorre todas las raíces p-ésimas; o bien $p \mid n$, en cuyo caso $\zeta_p^n = 1$ y sumamos p veces 1. Así que

$$a_n\left(\frac{1}{p}\sum_{j=0}^{p-1} f\left(\frac{\tau+j}{p}\right)\right) = a_n\left(\sum_{\substack{m=0 \\ p\mid m}}^{\infty} a_m(f) q^{m/p}\right) = a_{np}(f).$$

Juntando ambos cálculos obtenemos:

Proposición 1.3: Sea $f \in \mathcal{M}_k\big(\Gamma_0(N)\big)$ con coeficientes en expansión de Fourier $a_n(f)$, entonces

$$(T_p f)(\tau) = \sum_{n=0}^{\infty} a_{np}(f) q^n + p^{k-1} \sum_{n=0}^{\infty} a_n(f) q^{np}. \tag{3}$$

Corolario 1.3.1: Sean $p \neq q$ primos distintos y $\alpha, \beta \geq 1$ enteros, entonces

$$T_{p^\alpha} \circ T_{q^\beta} = T_{q^\beta} \circ T_{p^\alpha}.$$

Definición 1.4: Dado $n \in \mathbb{N}$ coprimo a N, definimos $T_n \in \operatorname{End} \mathcal{M}_k(\Gamma_0(N))$ como

$$T_n := T_{p_1^{e_1}} \circ \cdots \circ T_{p_r^{e_r}},$$

donde $n = p_1^{e_1} \cdots p_r^{e_r}$.

Definición 1.5: Una ***forma propia*** (eng. *eigenform*) es un vector propio de $\mathcal{M}_k\big(\Gamma_0(N)\big)$ respecto a los operadores de Hecke, es decir, tal que existe $\lambda_n \in \mathbb{C}$ para cada $n \in \mathbb{N}$ tal que

$$T_n f = \lambda_n f.$$

Ejemplo. Sea f una forma propia, nos gustaría poder calcular los λ_n's. Si f no fuese cuspidal (i.e. $a_0 \neq 0$), entonces la fórmula (3) dice, mirando el $a_0(T_p f)$, que

$$\lambda_p = 1 + p^{k-1}.$$

Esto es un tanto decepcionante, en cuanto que no depende de la forma modular en cuestión. Si f sí fuese cuspidal y tuviera, por ejemplo, $a_1(f) \neq 0$, entonces por (3) vemos que $a_p(f) = a_1(T_p f) = a_1(\lambda_p f) = \lambda_p a_1(f)$, de modo que $\lambda_p = a_p(f)/a_1(f)$. Similarmente, los otros casos también dependen del valor del primer coeficiente no nulo y de los otros coeficientes.

1.1. Dimensiones. Ya vimos en la charla anterior que $X_0(N)(\mathbb{C})$ es una curva compleja proyectiva, por tanto, posee un $\mathbb{C}$-espacio vectorial de dimensión finita de diferenciales, ¿podemos describirlos explícitamente? Una forma diferencial sobre $X_0(N)(\mathbb{C})$ debe ser una forma diferencial $f(\tau)\,\mathrm{d}\tau$ sobre $\mathfrak{h}$ que es $\Gamma_0(N)$-invariante y que es holomorfa en las cúspides; esto, *per ser*, tiene un sabor a formas modulares. Recíprocamente, si $f \in \mathcal{M}_2\big(\Gamma_0(N)\big)$ y $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, entonces

$$\begin{aligned} f(\gamma \cdot \tau)\,\mathrm{d}(\gamma \cdot \tau) &= (c\tau + d)^2 f(\tau)\,\mathrm{d}\left(\frac{a\tau + b}{c\tau + d}\right) \\ &= (c\tau + d)^2 f(\tau)\,\frac{a(c\tau + d) - c(a\tau + b)}{(c\tau + d)^2}\,\mathrm{d}\tau = f(\tau)\,\mathrm{d}\tau. \end{aligned}$$

Más aún, el cambio de variables $q = \exp(2\pi\mathrm{i}\,\tau)$ tiene $\mathrm{d}q = (2\pi\mathrm{i})q\,\mathrm{d}\tau$, de modo que

$$f(\tau)\,\mathrm{d}\tau = \frac{1}{2\pi\mathrm{i}}\frac{f(q)}{q}\,\mathrm{d}q,$$

por lo que, para que f sea integrable en $X_0(N)(\mathbb{C})$ se requiere que $f(q) \to 0$ cuando $q \to 0$. En consecuencia:

Proposición 1.6: $\dim \mathcal{S}_2\big(\Gamma_0(N)\big) = \dim_{\mathbb{C}} \Gamma(X_0(N), \Omega^1_{X_0(N)/\mathbb{C}}) = p_g\big(X_0(N)\big)$.

Donde p_g denota el *género geométrico* de la curva $X_0(N)$.

Para $k \neq 2$ uno puede hacer un análisis similar y emplear teoremas de curvas, como Riemann-Roch y la fórmula de Riemann-Hurwitz (vid. Diamond y Shurman [**1,** págs. 83 ss.]) para obtener las siguientes fórmulas:

Teorema 1.7: Fijemos $N \geq 2$ entero. Entonces:

$$\dim\big(\mathcal{M}_k\big(\Gamma_0(N)\big)\big) = \frac{N^2}{12}\prod_{p|N}\left(1 - \frac{1}{p^2}\right)k + O(1) \asymp k,$$
$$\dim\big(\mathcal{M}_k\big(\Gamma_0(N)\big)\big) = \dim\big(\mathcal{S}_k\big(\Gamma_0(N)\big)\big) + O(1).$$

Demostración: En el capítulo 3 de [**1,** págs. 65-108] véanse las fórmulas de los teoremas 3.1.1, 3.5.1, 3.6.1 y la primera fórmula en la pág. 107. □

Corolario 1.7.1: Los $\mathbb{C}$-espacios vectoriales $\mathcal{M}_k\big(\Gamma_0(N)\big)$ y $\mathcal{S}_k\big(\Gamma_0(N)\big)$ tienen dimensión finita.

2. Teoría de Atkin-Lehner

Definición 2.1: Se define la siguiente forma hermitiana

$$\begin{aligned}\langle -,-\rangle\colon \mathcal{S}_k\big(\Gamma_0(N)\big) \times \mathcal{S}_k\big(\Gamma_0(N)\big) &\longrightarrow \mathbb{C}\\ (f,g) &\longmapsto \int_{X_0(N)(\mathbb{C})} f(\tau)\cdot\overline{g(\tau)}\,\mathrm{Im}(\tau)^k\,\frac{\mathrm{d}x\,\mathrm{d}y}{y^2},\end{aligned}$$

donde $\tau = x + \mathrm{i}y$ y donde $\mathrm{d}x \wedge \mathrm{d}y/y^2$ es un diferencial sobre $\mathbb{C}$ que es $\mathrm{SL}_2(\mathbb{Z})$-invariante. A ésta se le llama el ***producto interno de Petersson***.

Ejemplo. Cuando $k = 2$, el producto de Petersson coincide con la forma hermitiana del espacio de Hilbert $\mathscr{L}^2(X_0(N)(\mathbb{C}); \mathbb{C})$:

$$\langle f, g\rangle = \int_{X_0(N)(\mathbb{C})} f(\tau)\overline{g(\tau)}\,\mathrm{d}x\,\mathrm{d}y.$$

Proposición 2.2: Sobre $\mathcal{S}_k\big(\Gamma_0(N)\big)$, se cumple que $\langle T_p f, g\rangle = \langle f, T_p g\rangle$; en consecuente, T_p es un operador *autoadjunto* sobre $\mathcal{S}_k\left(\Gamma_0(N)\right)$.

Sumado al hecho de que $\mathcal{S}_k\big(\Gamma_0(N)\big)$ es un $\mathbb{C}$-espacio vectorial de dimensión finita, tenemos la siguiente aplicación de álgebra lineal:

Corolario 2.2.1: Los operadores $\{T_p\}_{p\nmid N}$ sobre $\mathcal{S}_k\big(\Gamma_0(N)\big)$ son *simultáneamente diagonalizables*. Es decir, existe una base $f_1, \ldots, f_m$ de $\mathcal{S}_k\big(\Gamma_0(N)\big)$ tales que cada f_j es un vector propio relativo a todos los T_p's.

Demostración: El teorema espectral para formas hermitianas (cfr. Lang **[2,** págs. 581-584], Thm. XV.6.7) dice que cada T_p es diagonalizable por si solo. Luego, nótese que T_p y T_q conmutan por el corolario 1.3.1, y es un ejercicio (vid. **[2,** págs. 568-569], Exr. XIV.13(d)) verificar que una familia de operadores que conmutan se puede diagonalizar simultáneamente. □

2.1. Espacios viejos y nuevos. Sean $M \mid N$ naturales, entonces hay un epimorfismo de anillos $\mathbb{Z}/N\mathbb{Z} \twoheadrightarrow \mathbb{Z}/M\mathbb{Z}$. Recuérdese que $\Gamma_0(N)$ es el núcleo de la proyección $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, por lo que tenemos el diagrama:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Gamma_0(N) & \longrightarrow & \mathrm{SL}_2(\mathbb{Z}) & \longrightarrow & \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \iota} & & \| & & \downarrow & & \\ 0 & \longrightarrow & \Gamma_0(M) & \longrightarrow & \mathrm{SL}_2(\mathbb{Z}) & \longrightarrow & \mathrm{SL}_2(\mathbb{Z}/M\mathbb{Z}) & \longrightarrow & 0 \end{array}$$

que conmuta y tiene filas exactas, de modo que $\Gamma_0(N) \leq \Gamma_0(M)$ y, en particular, $\mathcal{S}_k\big(\Gamma_0(M)\big) \leq \mathcal{S}_k\big(\Gamma_0(N)\big)$. Ahora bien, sea $r \mid N/M$, entonces

$$\varphi_r \colon \mathcal{S}_k\big(\Gamma_0(M)\big) \longrightarrow \mathcal{S}_k\big(\Gamma_0(N)\big), \qquad f(\tau) \longmapsto f(r\tau) \tag{4}$$

es una transformación $\mathbb{C}$-lineal inyectiva.

Definición 2.3: El ***espacio viejo*** de $\mathcal{S}_k\big(\Gamma_0(N)\big)$, denotado $\mathcal{S}_k\big(\Gamma_0(N)\big)^{\mathrm{old}}$ es la imagen de cada φ_r dado por (4), donde M recorre los divisores de N distintos de sí mismo. El complemento ortogonal del espacio viejo se llama el ***espacio nuevo*** y se denota $\mathcal{S}_k\big(\Gamma_0(N)\big)^{\mathrm{new}}$.

Una ***newform*** f de $\mathcal{S}_k\big(\Gamma_0(N)\big)$ es un elemento del espacio nuevo que es una forma propia y tal que $a_1(f) = 1$.

Teorema 2.4: Las newforms conforman una base para el espacio nuevo $\mathcal{S}_k\big(\Gamma_0(N)\big)^{\mathrm{new}}$.

Demostración: Cfr. **[1,** pág. 196], Thm. 5.8.2. □

Como corolario, uno puede, inductivamente, probar que hay una base para $\mathcal{S}_k\big(\Gamma_0(N)\big)$ donde todos los elementos son imágenes, mediante φ_r de newforms en niveles inferiores. Para más detalle véase **[1],** Thm. 5.8.3.

Referencias

1. Diamond, F. y Shurman, J. *A First Course in Modular Forms Graduate Texts in Mathematics* **228** (Springer-Verlag, 2010).
2. Lang, S. *Algebra* (Springer-Verlag New York, 2002).
3. Serre, J.-P. *A course in arithmetic* (Springer-Verlag, 1973).

Correo electrónico: mnalvarado1@mat.uc.cl

Departamento de Matemáticas, Pontificia Universidad Católica de Chile. Facultad de Matemáticas, 4860 Av. Vicuña Mackenna, Macul, RM, Chile
Correo electrónico: josecuevasbtos@uc.cl