POLINOMIO MODULAR

JAVIER REYES

1. Recordatorio y Motivación

Fijemos $m \in \mathbb{N}$. Una idea de este capítulo y el anterior es estudiar la relación entre las funciones $j(\tau)$ y $j(m\tau)$. Nombramos $\sigma_0 = \left(\begin{smallmatrix} m & 0 \\ 0 & 1 \end{smallmatrix}\right)$ con tal que $j(m\tau) = j(\sigma_0\tau)$. Al intentar comparar ambas funciones surge un "problema" y una "ambigüedad".

Problema: $j(\tau)$ es $\mathrm{SL}(2,\mathbb{Z})$-invariante pero no necesariamente lo es $j(\sigma_0\tau)$, a pesar de si ser $\Gamma_0(m)$ invariante. Si intentáramos hacer el cambio $\tau \mapsto \gamma\tau$, $\gamma \in \mathrm{SL}(2,\mathbb{Z})$ estaríamos variando sobre las funciones $j((\sigma_0\gamma)\tau)$. La observación clave es que la acción por la derecha de $\mathrm{SL}(2,\mathbb{Z})$ preserva determinante y gcd de las entradas de las matrices, lo que nos motiva a definir

$$\Delta_m^* = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{Z}) \mid ad - bc = m,\ \gcd(a,b,c,d) = 1 \right\}$$

La nos dice que $\sigma_0 \,\mathrm{SL}(2,\mathbb{Z}) \subseteq \Delta_m^*$, por lo que nos reducimos a estudiar $j(\sigma\tau)$, con $\sigma \in \Delta_m^*$.

Ambigüedad: Ya que $j(\gamma\sigma\tau) = j(\sigma\tau)$, esto nos dice que solo nos interesa estudiar las distintas órbitas de Δ_m^* bajo la acción por la izquierda de $\mathrm{SL}(2,\mathbb{Z})$, por lo que basta encontrar un conjunto de representantes de estas clases.

Lema 1.1. *Se define*

$$C(m) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_{2\times 2}(\mathbb{Z}) \mid ad = m, \quad 0 \le b < d, \quad \gcd(a,b,d) = 1 \right\}.$$

Este es un conjunto de representantes de $\mathrm{SL}(2,\mathbb{Z})$*-equivalencia por la izquierda.*

La siguiente pregunta natural es ¿no sobrarán elementos de Δ_m^* que no tenemos por qué estudiar?

Lema 1.2. *La acción por la derecha de* $\mathrm{SL}(2,\mathbb{Z})$ *en las clases de* $\mathrm{SL}(2,\mathbb{Z})$*-equivalencia de* Δ_m^* *es transitiva. (En otras palabras,* $\Delta_m^* = \Gamma\sigma_0\Gamma$*).*

Demostración: Sea $\sigma \in C(m)$. Como $\sigma_0^{-1}\,\mathrm{SL}(2,\mathbb{Z})\sigma \cap \mathrm{SL}(2,\mathbb{Z})$ es una clase lateral de $\Gamma_0(m)$, en particular se tiene

$$\mathrm{SL}(2,\mathbb{Z})\sigma \cap \sigma_0\,\mathrm{SL}(2,\mathbb{Z}) \neq \varnothing$$

□

La vez sesión pasada se probó una correspondencia entre prueba que exuste una correspondecia entre estos representantes y clases laterales derechas de $\Gamma_0(m)$, dada por asignarle a $\sigma \in C(m)$ el conjunto

$$\left(\sigma_0^{-1}\,\mathrm{SL}(2,\mathbb{Z})\sigma\right) \cap \mathrm{SL}(2,\mathbb{Z})$$

Enumerando las clases laterales de $\Gamma_0(m)$ como $\Gamma_0(m)\gamma_i$, $i = 1, \ldots, |C(m)|$, se define

$$\Phi_m(X,\tau) = \prod_{i=1}^{|C(m)|} (X - j(m\gamma_i\tau)) = \prod_{\sigma\in C(m)} (X - j(\sigma\tau))$$

Dado que multiplicación por la derecha por elementos de $\mathrm{SL}(2,\mathbb{Z})$ es una permutación en las clases de $\mathrm{SL}(2,\mathbb{Z})$-equivalencia, entonces cada coeficiente de $\Phi_m(X,\tau)$ es $\mathrm{SL}(2,\mathbb{Z})$-invariante. Se prueba también que los coeficientes son meromofros en las cúspides, por lo tanto son funciones holomorfas modulares y así polinomios en $j(\tau)$, es decir existe

$$\Phi_m(X,Y) \in \mathbb{C}[X,Y]$$

llamado el polinomio modular, que cumple

$$\Phi_m(X, j(\tau)) = \prod_{\sigma\in C(m)} (X - j(\sigma\tau)).$$

Teorema 2.1. *Sea m entero positivo. Entonces*

1. $\Phi_m(X,Y) \in \mathbb{Z}[X,Y]$.
2. $\Phi_m(X,Y)$ *es irreducible visto como polinomio en* X.
3. *Si* $m > 1$, *entonces* $\Phi_m(X,Y) = \Phi_m(Y,X)$.
4. *Si* m *no es un entero perfecto, entonces* $\Phi_m(X,X)$ *es un polinomio de grado mayor estricto a* 1 *cuyo coeficiente lider es* ± 1.
5. *(Congruencia de Kronecker) Si* $m = p$ *es primo, entonces* $\Phi_p(X,Y) \equiv (X^p - Y)(X - Y^p)$ mód $p\mathbb{Z}[X,Y]$.

Para esto primero veremos un lema útil:

Lema 2.2 (Principio de la q-expansión de Hasse)**.** *Sea $A \subseteq \mathbb{C}$ un subgrupo aditivo y $f(\tau)$ una función modular holomorfa. Si la q-expansión de f es*

$$f(\tau) = \sum_{n=-M}^{\infty} a_n q^n$$

con $a_n \in A$ para todo $n \leq 0$, entonces $f(\tau)$ es un polinomio en $j(\tau)$ con coeficientes en A.

Demostración: Por inducción en M, cuando $M \leq 0$, entonces $f(\tau)$ converge hacia infinito, por lo tanto es constante e igual a $a_0 \in A$.

Si la q-expansión de f comienza con $a_{-M}q^{-M}$, $M > 0$, consideramos

$$g(\tau) = f(\tau) - a_{-M}(j(\tau))^M.$$

Dado que $j(\tau) = 1/q + \sum_{n=0}^{\infty} c_n q^n$, $c_n \in \mathbb{Z}$, entonces $g(\tau)$ es otra función modular holomorfa cuya q-expansión empieza con orden $-(M-1)$, y además sus coeficientes no positivos están en A.

Entonces $g(\tau) = P(j(\tau))$ con $P(x) \in A[x]$ y así, $f(\tau) = a_{-M}j(\tau)^M + P(j(\tau))$. □

Ahora para el teorema:

Demostración:

1. Primero recordamos que los coeficientes de $\Phi(X, j(\tau))$ son polinomios simétricos en los $j(\sigma\tau)$. Comenzamos estudiando la q-expansión de $j(\sigma\tau)$. Si

$$\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(m)$$

se sigue que

$$q(\sigma\tau) = e^{2\pi i(a\tau+b)/d} = e^{2\pi ib/d}(e^{2\pi i\tau})^{a/d} = \zeta_m^{ab}(q^{1/m})^{a^2}$$

y evaluando en j se obtiene

$$j(\sigma\tau) = \frac{\zeta_m^{-ab}}{(q^{1/m})^{a^2}} + \sum_{n=0}^{\infty} c_n \zeta_m^{abn}(q^{1/m})^{a^2 n} \tag{2.1}$$

en particular, $j(\sigma\tau) \in \mathbb{Z}[\zeta_m]((q^{1/m})) \subseteq \mathbb{Q}(\zeta_m)((q^{1/m}))$. El grupo de Galois de $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ actúa de manera natural en $\mathbb{Q}(\zeta_m)((q^{1/m}))$. Sea $\psi \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ con $\psi(\zeta_m) = \zeta_m^k$, donde k es coprimo a m. Luego

$$\psi(j(\sigma\tau)) = \frac{\zeta_m^{-a(bk)}}{(q^{1/m})^{a^2}} + \sum_{n=0}^{\infty} c_n \zeta_m^{a(bk)n}(q^{1/m})^{a^2 n} = j(\sigma_k\tau),$$

donde

$$\sigma_k = \begin{pmatrix} a & bk \\ 0 & d \end{pmatrix}.$$

Esta matriz es $\mathrm{SL}(2,\mathbb{Z})$-equivalente a alguna otra $\sigma' \in C(m)$, es decir, $j(\sigma_k\tau) = j(\sigma'\tau)$, lo que muestra que la acción del Galois permuta los $j(\sigma\tau)$. Si $f(\tau)$ es un coeficiente de $\Phi_m(X, j(\tau))$ al ser simétrico, es invariantes bajo el Galois, por lo tanto tiene coeficientes racionales. Recordando que $j(\sigma\tau)$ tiene coeficientes en $\mathbb{Z}[\zeta_m]$, obtenemos

$$f(\tau) \in \mathbb{Z}[\zeta_m]((q^{1/m})) \cap \mathbb{Q}((q^{1/m})) = \mathbb{Z}((q^{1/m}))$$

También recordamos la conclusión de que $f(\tau)$ es una función modular para $\mathrm{SL}(2,\mathbb{Z})$, es decir, su q-expansión realmente está en términos de q:

$$f(\tau) \in \mathbb{C}((q)) \cap \mathbb{Z}((q^{1/m})) = \mathbb{Z}((q))$$

Aplicando directamente el principio de la q-expansión de Hasse para $A = \mathbb{Z}$, sabemos que existe un polinomio $P(Y) \in \mathbb{Z}[Y]$ tal que $f(\tau) = P(j(\tau))$, probando así que $\Phi_m(X, Y) \in \mathbb{Z}[X, Y]$.

2. Sesión pasada usando Teoría de Galois.
3. Sea
$$\sigma = \begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix} \in C(m).$$
de modo que $\sigma\tau = \tau/m$. Ya que para todo τ se tiene
$$\Phi_m(j(\tau/m), j(\tau)) = \Phi_m(j(\sigma\tau), j(\tau)) = 0,$$
haciendo el reemplazo $\tau \mapsto m\tau$, obtenemos
$$\Phi_m(j(\tau), j(m\tau)) = 0$$
para todo τ. Esto implica que $j(m\tau)$ es una raíz de $\Phi_m(j(\tau), X)$, pero como $\Phi_m(X, j(\tau))$ es su polinomio minimal (sobre $\mathbb{C}(j(\tau))$), entonces
$$\Phi_m(X, j(\tau)) \mid \Phi_m(j(\tau), X),$$
Como j es sobreyectiva (alternativamente trascendental sobre $\mathbb{Z}$), se tiene $\Phi_m(X, Y) \mid \Phi_m(Y, X)$, es decir, existe $g(X, Y) \in \mathbb{Z}[X, Y]$ tal que
$$\Phi_m(Y, X) = g(X, Y)\Phi(X, Y)$$
y así
$$\Phi_m(Y, X) = g(X, Y)g(Y, X)\Phi(Y, X)$$
concluyendo que $g(X, Y)g(Y, X) = 1$, por lo que g es constante e igual a ± 1. Si $g = -1$, entonces tendríamos
$$\Phi_m(j(\tau), j(\tau)) = -\Phi_m(j(\tau), j(\tau))$$
lo que implicaría que $j(\tau)$ es raíz de $\Phi_m(X, j(\tau))$, pero para $m > 1$, este polinomio tiene grado > 1 y es irreducible, lo que sería contradictorio. Luego $g = 1$ probando la igualdad.
4. Viendo la construcción en el principio de la q-expansión de Hasse, si consideramos un una función modular como polinomio en $j(\tau)$, su término lider corresponde al coeficiente más negativo de su q-expansión. Por esto, estudiaremos la q-expansión de $\Phi_m(j(\tau), j(\tau))$.

   Tal expresión es
$$\Phi_m(j(\tau), j(\tau)) = \prod_{\sigma \in C(m)} (j(\tau) - j(\sigma\tau)),$$
y expandiendo los términos
$$j(\tau) - j(\sigma\tau) = \frac{1}{q} - \frac{\zeta_m^{-ab}}{q^{a/d}} + \sum_{n=0}^{\infty} d_n (q^{1/m})^n$$
para algunos $d_i \in \mathbb{C}$. Dado que $ad = m$ no es un cuadrado, entonces $a \neq d$ para todo σ, por lo que el término más negativo de $j(\tau) - j(\sigma\tau)$ es siempre una raíz de la unidad (ya sea 1 cuando $a < d$ o $-\zeta_m^{-ab}$ en otro caso).

   En consecuencia, el producto sobre todos los σ tiene una raíz de la unidad como coeficiente más negativo, por lo tanto el término líder de $\Phi_m(X, X)$ es una raíz de la unidad. Por la parte 1, tal raíz debe ser entera, es decir ± 1.

   El grado es mayor que uno pues la potencia más negativa de q en la expresión anterior es siempre menor o igual a -1, en particular, $\deg \Phi_m(X, X) \geq |C(m)|$.
5. Enumeramos explícitamente los elementos de $C(p)$:
$$\sigma_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_i = \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix}, i = 0, \ldots, p-1$$
Trabajando en $\mathbb{Z}[\zeta_p]((q^{1/p}))$, notamos que para $i = 0, \ldots, p-1$
$$j(\sigma_i\tau) = \frac{\zeta_p^{-i}}{q^{1/p}} + \sum_{n=0}^{\infty} c_n \zeta_p^{in} (q^{1/p})^n \equiv \frac{1}{q^{1/p}} + \sum_{n=0}^{\infty} c_n (q^{1/p})^n \mod 1 - \zeta_p$$
y que la última expresión es igual a $j(\sigma_0\tau)$. Esto prueba que
$$\prod_{i=0}^{p-1} (X - j(\sigma_i\tau)) \equiv (X - j(\sigma_0\tau))^p \equiv X^p - j(\sigma_0\tau)^p \mod 1 - \zeta_p$$

donde la última congruencia viene dada porque $1-\zeta_p$ divide a p. También se tiene

$$j(\sigma_0\tau)^p = \left(\frac{1}{q^{1/p}} + \sum_{n=0}^{\infty} c_n q^{n/p}\right)^p \equiv \frac{1}{q} + \sum_{n=0}^{\infty} c_n^p q^n \equiv \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n \equiv j(\tau) \quad \text{mód } 1-\zeta_p$$

Ahora para σ_p, se tiene

$$j(\sigma_p\tau) = \frac{1}{q^p} + \sum_{n=0}^{\infty} c_n q^{pn} \equiv \frac{1}{q^p} + \sum_{n=0}^{\infty} c_n^p q^{pn} \equiv \left(\frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n\right)^p \equiv (j(\tau))^p \quad \text{mód } 1-\zeta_p.$$

Se concluye entonces que

$$\Phi_p(X, j(\tau)) \equiv (X^p - j(\tau))(X - j(\tau)^p) \quad \text{mód } (1-\zeta_p)\mathbb{Z}[\zeta_p]((q^{1/p}))[X]$$

Dado que ambos lados están en $\mathbb{Z}((q))[X]$ su diferencia es una serie en q de coeficientes enteros divisibles por $1-\zeta_p$. Como cada entero divisible por $1-\zeta_p$ es divisible también por p, podemos reescribir la congruencia ahora módulo p:

$$\Phi_m(X, j(\tau)) - (X^p - j(\tau))(X - j(\tau)^p) \in p\mathbb{Z}((q))[X]$$

Usando el principio de la q-expansión de Hasse para $A = p\mathbb{Z}$, obtenemos que la expresión arriba es un polinomio en $j(\tau)$ con coeficientes divisibles por p, es decir,

$$\Phi_m(X, Y) - (X^p - Y)(X - Y^p) \in p\mathbb{Z}[X, Y]$$

□

3. Relación con Látices

Dado un Látice (normalizado) $L = [1, \tau] \subseteq \mathbb{C}$, El conjunto de sublátices se puede obtener mediante matrices enteras de la siguiente forma. Si

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{Z}),$$

el látice

$$L' = [c\tau + d, a\tau + b] = (c\tau + d)[1, \gamma\tau]$$

es un sublátice de L. Hay que notar que no es una acción directamente en los látices, ya que depende de la elección de base.

Los resultados importantes son

- $\mathrm{SL}(2, \mathbb{Z})$ "actúa" cambiando de base, y a cada base le corresponde un elemento de $\mathrm{SL}(2, \mathbb{Z})$. En particular deja el látice invariante.
- El grupo L/L' tiene orden $\det \gamma$.
- El grupo L/L' es cíclico si y sólo si $\gcd(a, b, c, d) = 1$.

¡Resulta que los elementos de $C(m)$ corresponden a sublátices cíclicos de orden m! De hecho por medio de esta construcción, codifican una manera canónica de escoger bases para sublátices.

Lema 3.1. *Sea $\tau \in \mathfrak{h}$, y $L' \subseteq [1, \tau]$ sublátice cíclico de orden m. Luego existe un único $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in C(m)$ tal que $L' = d[1, \sigma\tau]$.*

Demostración: Escribiendo $L' = [c\tau + d, a\tau + b]$, por los resultados anteriores, se tiene que $\rho = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Delta_m^*$, por lo tanto es $\mathrm{SL}(2, \mathbb{Z})$-equivalente a algún $\sigma = \left(\begin{smallmatrix} a' & b' \\ 0 & d' \end{smallmatrix}\right) \in C(m)$, es decir,

$$\rho = \gamma\sigma, \quad \gamma \in \mathrm{SL}(2, \mathbb{Z})$$

entonces la diferencia entre ambos látices es símplemente un cambio de base, por lo tanto $L' = d'[1, \sigma\tau]$.

La unicidad viene de que si σ y σ' definen el mismo sublátice, sería posible cambiar de base entre ellos, es decir, $\sigma = \gamma\sigma'$ para $\gamma \in \mathrm{SL}(2, \mathbb{Z})$. Por construcción de $C(m)$, necesariamente $\sigma = \sigma'$. □

Teorema 3.2. *Sea $m \in \mathbb{N}$, y $u, v \in \mathbb{C}$. Luego $\Phi_m(u, v) = 0$ si y solo si existen látices $L' \subseteq L$ tal que L/L' es cíclico de orden m, $u = j(L')$, $v = j(L)$*

Demostración: Si $j(\tau) = j([1, \tau])$, los ceros de $\Phi_m(X, j(\tau))$ son $j(\sigma\tau) = j([1, \sigma\tau]) = j(d[1, \sigma\tau])$ □

Email address: jereyes4@uc.cl