Más sobre j Parte II

Marcos Morales

Sea $m \in \mathbb{Z}$, definimos $\Gamma_0(m) \subset SL_2(\mathbb{Z})$, como

$$\Gamma_0(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \, mod \, (m) \right\}.$$

Notemos que $\Gamma_0(1) = SL_2(\mathbb{Z})$. Una función modular para $\Gamma_0(m)$, es una función $f : \mathbb{H} \to \mathbb{C}$, que satisface las siguientes condiciones

(i) f es meromorfa en $\mathbb{H}$.
(ii) f es invariante bajo $\Gamma_0(m)$.
(iii) f es meromorfa en las cúspides.

La parte (ii), quiere decir que $f(\gamma\tau) = \tau$, para todo $\tau \in \mathbb{H}$ y todo $\gamma \in \Gamma_0(m)$. Más tarde explicaremos lo que significa (iii). Notemos que, si $f(\tau)$ satisface (i) y (ii), y $\gamma \in SL_2(\mathbb{Z})$, entonces $f(\gamma\tau)$ tiene periodo m, en efecto, se tiene que $\tau + m = U\tau$, donde $U = \left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right)$. además notemos que, si $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, entonces

$$\gamma U \gamma^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad - acm - bc & -ab + a^2 m + ab \\ -mc^2 & -bc + cma + da \end{pmatrix} \in \Gamma_0(m)$$

Con esto, obtenemos que

$$f(\gamma(\tau + m)) = f(\gamma U \tau) = f(\gamma U \gamma^{-1} \gamma\tau) = f(\gamma\tau)$$

Lo último, es debido a que $f(\tau)$ es $\Gamma_0(m)$-invariante. Sean entonces $f : \mathbb{H} \to \mathbb{C}$ que cumpla tanto (i) como (ii) y $\gamma \in SL_2(\mathbb{Z})$, escribimos el mapeo, $\Phi : \mathbb{H} \to D(0,1) \setminus \{0\}$, donde $\Phi(\tau) = e^{\frac{2\pi i \tau}{m}}$, podemos definir entonces $\phi : D(0,1) \to \mathbb{C}$, dada por, $\phi(x) = f(\gamma\tau)$, donde τ es una de las pre-imágenes de x bajo la función Φ, tenemos que ϕ esta bien definido, pues si τ y τ' se mapean a x, entonces $\frac{2\pi i \tau}{m} = \frac{2\pi i \tau'}{m} + 2k\pi i$, donde $k \in \mathbb{Z}$, luego $\tau = \tau' + km$, y de esta forma, $f(\gamma\tau) = f(\gamma\tau')$. Por otra parte, se tiene que

$$\phi'(x) = \frac{d}{dx} f(\gamma\tau) = \frac{d}{d\gamma\tau} f(\gamma\tau) \frac{d\gamma\tau}{dx} = \frac{d}{d\gamma\tau} f(\gamma\tau) \frac{d\gamma\tau}{d\tau} \frac{d\tau}{dx} = \frac{m}{2\pi i e^{\frac{2\pi i \tau}{m}}} \frac{d}{d\gamma\tau} f(\gamma\tau) \frac{d\gamma\tau}{d\tau}.$$

Luego ϕ es meromorfa en $D(0,1)$ y por lo tanto tiene una serie de Laurent alrededor del cero, si escribimos $q = e^{2\pi i \tau}$, entonces la serie es de la forma

$$f(\gamma\tau) = \sum_{n=-\infty}^{\infty} a_n q^{n/m}.$$

La cual llamaremos, la q-expansión de $f(\gamma\tau)$. Entonces, diremos que $f(\tau)$ es meromorfa en las cúspides si para todo $\gamma \in SL_2(\mathbb{Z})$, la q-expansión de $f(\gamma\tau)$ tiene sólo un número finito de coeficientes para exponentes negativos.

Un ejemplo básico de este tipo de funciones es la función j. Por lo visto en la charla CM 8, la función j es holomorfa en $\mathbb{H}$, invariante bajo $SL_2(\mathbb{Z})$ y meromorfa en las cúspides. Entonces, $j(\tau)$ es una función modular para $SL_2(\mathbb{Z}) = \Gamma_0(1)$. Con las definiciones anteriores, el resultado principal de esta sección es el siguiente

Teorema 1.0: *Sea m entero positivo, entonces*

i) $j(\tau)$ es una función modular para $SL_2(\mathbb{Z})$, y toda función modular para $SL_2(\mathbb{Z})$ es una función racional en $j(\tau)$.
ii) $j(\tau)$ y $j(m\tau)$ son funciones modulares para $\Gamma_0(m)$, y toda función modular para $\Gamma_0(m)$ es una función racional en $j(\tau)$ y $j(m\tau)$.

Demostración: (i) Ya vimos que $j(\tau)$ es una función modular para $SL_2(\mathbb{Z})$. Para ver la otra parte empezaremos con una definición, diremos que una función modular es holomorfa en ∞ si su q-expansión tiene sólo potencias no negativas de q, con esta definición podemos establecer el siguiente lema.

Lema 1.1:

i) Una función modular holomorfa para $SL_2(\mathbb{Z})$ que es holomorfa en ∞ es contante.
ii) Una función modular holomorfa para $SL_2(\mathbb{Z})$ es un polinomio en $j(\tau)$.

Demostración:(i) Supongamos que f es una función modular holomorfa para $SL_2(\mathbb{Z})$. Notemos que, como f es holomorfa en ∞, entonces $\lim f(\tau)$, cuando $Im(\tau) \to \infty$, existe como número complejo. La idea es probar que $f(\mathbb{H} \cup \{\infty\})$ es compacto, pues de esta forma, el principio del módulo máximo implicaría que f es constante.
Sea $f(\tau_k)$ una secuencia de puntos en $f(\mathbb{H})$. Como f es $SL_2(\mathbb{Z})$- invariante, podemos asumir que los τ_k están en la región $R = \{\tau \in \mathbb{H} \ / \ |Re(\tau)| \leq 1/2,\ Im(\tau) \geq 1/2\}$. Si las partes imaginarias de los τ_k no están acotadas, entonces por lo dicho anterirormente hay una subsecuencia τ_{k_n}, tal que $f(\tau_{k_n})$ converge a $f(\infty)$. Si por lo contrario, las partes imaginarias de los τ_k están acotadas, entonces los τ_k están en un subconjunto compacto de $\mathbb{H}$, por lo tanto, hay una subsucesión τ_{k_n} que converge a un elemento $\tau \in \mathbb{H}$, como f es continua se tiene que los $f(\tau_{k_n})$ convergen a $f(\tau)$. Esto prueba (i).

(ii) Sea f función modular holomorfa para $SL_2(\mathbb{Z})$. Entonces su q-expansión tiene sólo finitos términos con potencias negativas de q. Como la q-expansión de j comienza con $1/q$, podemos encontrar un polinomio $A(x)$, tal que $f(\tau) - A(j(\tau))$ sea holomorfa en ∞, como también es holomorfa en $\mathbb{H}$, entonces es constante. Concluimos que $f(\tau)$ es un polinomio en $j(\tau)$. Esto concluye con la demostración del lema. □

La idea ahora es encontrar un polinomio B, tal que $B(j(\tau))f(\tau)$ sea holomorfa, entonces usando el lema tendríamos (i), como f tiene una q-expansión meromorfa, entonces f tiene finitos polos en la región $R = \{\tau \in \mathbb{H} \ / \ |Re(\tau)| \leq 1/2,\ Im(\tau) \geq 1/2\}$, y como f es $SL_2(\mathbb{Z})$- invariante, entonces cada polo de f es $SL_2(\mathbb{Z})$-equivalente a un elemento en R. De esta forma, si podemos encontrar B, tal que, $B(j(\tau))f(\tau)$ no tiene polos, tendríamos el resultado pedido.

Supongamos que f tiene un polo de orden m en $\tau_0 \in R$. Si $j'(\tau_0) \neq 0$, entonces $(j(\tau) - j(\tau_0)^m f(\tau))$ es holomorfa en τ_0. Siguiendo este método podemos encontrar B tal que $B(j(\tau))f(\tau)$ no tiene polos en R, excepto posiblemente en los puntos donde $j'(\tau_0) = 0$. El teorema 10,0 de CM 8, nos permite asumir que $\tau_0 = i$ o $\omega = e^{2\pi i/3}$. Cuando $\tau_0 = i$, afirmamos que m es par. Para ver esto, notamos que en una vecindad de i, f puede ser escrita de la forma

$$f(\tau) = \frac{g(\tau)}{(\tau - i)^m}.$$

Donde $g(\tau)$ es holomorfa y $g(i) \neq 0$. Ahora $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ fija a i fija i, por lo tanto

$$f(\tau) = f(\tfrac{-1}{\tau}) = \frac{g(-1/\tau)}{(-1/\tau - i)^m}.$$

Comparando estas dos igualdades, se concluye que

$$g(-1/\tau) = \frac{1}{(i\tau)^m} g(\tau).$$

Evaluando en $\tau = i$, implica que $g(i) = (-1)^m g(i)$ y como $g(i) \neq 0$, se sigue que m es par. Por el teorema 1.0 parte (iv)de la sección CM 8, $j(\tau) - 1728$ tiene un polo de orden 2 en i, por lo tanto $(j(\tau) - 1728)^{m/2} f(\tau)$ es holomorfa en i. El argumento para $\tau_0 = \omega$ es similar y se deja para la versión final. Esto prueba la parte (i) de teorema 1.0.

(ii) probar que j es una función modular para $\Gamma_0(m)$ es trivial. Por otra parte, tenemos que $j(m\tau)$ es holomorfa, sea entonces $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(m)$. Entonces

$$j(m\gamma\tau) = j\left(\frac{m(a\tau + b)}{c\tau + d}\right) = j\left(\frac{am\tau + bm}{c/m\, m\tau + d}\right).$$

Como $\gamma \in \Gamma_0(m)$, se sigue que $\gamma' = \left(\begin{smallmatrix} a & bm \\ c/m & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. Así

$$j(m\gamma\tau) = j(\gamma' m\tau) = j(m\tau).$$

Lo cual prueba que $j(m\tau)$ es $\Gamma_0(m)$-invariante.

Sea ahora

$$C(m)\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbb{Z}) \;\middle|\; ad = m,\, a > 0,\, 0 \leq b < d,\, mcd(a, b, d) = 1 \right\}.$$

Entonces, la matriz $\sigma_0 = \left(\begin{smallmatrix} m & 0 \\ 0 & 1 \end{smallmatrix}\right) \in C(m)$ y tiene dos propiedades importantes, primero $\sigma_0\tau = m\tau$ y segundo

$$\Gamma_0(m) = (\sigma_0^{-1} SL_2(\mathbb{Z})\sigma_0) \cap SL_2\mathbb{Z}.$$

Para ver esto último, notemos que para $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, se tiene que

$$\sigma_0^{-1}\gamma\sigma = \begin{pmatrix} 1/m & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b/m \\ mc & d \end{pmatrix}. \quad (1)$$

Ahora, si $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(m)$ entonces considerando $\gamma' = \left(\begin{smallmatrix} a & bm \\ c/m & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ y entonces $\sigma_0^{-1}\gamma'\sigma_0 = \gamma$, concluimos que $\gamma \in (\sigma_0^{-1} SL_2(\mathbb{Z})\sigma_0) \cap SL_2\mathbb{Z}$. Por otra parte, si $\gamma \in (\sigma_0^{-1} SL_2(\mathbb{Z})\sigma_0) \cap SL_2(\mathbb{Z})$, entonces usando (1), se conluye directamente que $\gamma \in \Gamma_0(m)$.

Más generalmente, tenemos el siguiente lema.

Lema 1.2: Para $\sigma \in C(m)$, el conjunto

$$(\sigma_0^{-1} SL_2(\mathbb{Z})\sigma) \cap SL_2\mathbb{Z}.$$

Es una clase lateral por la derecha de $\Gamma_0(m)$ en $SL_2(\mathbb{Z})$. Esto induce una correspondencia 1-1 entre clases laterales derechas de $\Gamma_0(m)$ y elementos de $C(m)$.

Demostración: Tenemos que $(\sigma_0^{-1} SL_2(\mathbb{Z})\sigma) \cap SL_2\mathbb{Z} = (\sigma_0^{-1} SL_2(\mathbb{Z})\sigma_0)(\sigma_0^{-1}\sigma) \cap SL_2\mathbb{Z} = \Gamma_0(m)\sigma_0^{-1}\sigma \cap SL_2\mathbb{Z}$, pero si $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, entonces

$$\sigma_0^{-1}\sigma = \begin{pmatrix} a/m & b/m \\ 0 & d \end{pmatrix}.$$

Como $\sigma \in C(m)$, entonces $ad = m$.

Este lema implica que $[SL_2(\mathbb{Z}) : \Gamma_0(m)] = |C(m)|$. Además, se puede probar el siguiente lema

Lema 1.3: Sea m entero positivo, entonces

$$|C(m)| = m \prod_{p|m} \left(1 + \frac{1}{p}\right).$$

Demostración: Fijemos $d|m$, entonces $a = m/d$ queda fijo, por la definición de $C(m)$, los b que completan el trío deben cumplir que $0 \leq b < d$ y $(a, b, d) = (b, d, m/d) = 1$, recordemos que $(b, d, m/d) = (b, (d, m/d))$, luego dividimos el intervalo $(0, d)$ en intervalos de largo $d/(d, m/d)$, en estos intervalos hay exactamente $\phi((d, m/d))$ opciones para b, luego la cantidad de b que sirven son

$$\frac{d}{(d, m/d)} \phi((d, m/d)).$$

De esta forma

$$|C(m)| = \sum_{d|m} \frac{d}{(d, m/d)} \phi((d, m/d)).$$

Notemos que si $m = p^r$ entonces

$$\begin{aligned} |C(p^r)| &= \sum_{k=0}^{r} \frac{p^r}{(p^k, p^{r-k})} \phi((p^k, p^{r-k})) \\ &= \sum_{k=1}^{r-1} \frac{p^r}{(p^k, p^{r-k})} \phi((p^k, p^{r-k})) + p^r + 1 \\ &= \sum_{k=1}^{r-1} (p^k - p^{k-1}) + p^r + 1 \\ &= p^r + p^{r-1}. \end{aligned}$$

Notemos además que si m_1, m_2 son enteros positivos con $(m_1, m_2) = 1$, entonces

$$|C(m_1 m_2)| = \sum_{d_1|m_1, d_2|m_2} \frac{d_1 d_2}{(d_1 d_2, m_1 m_2/d_1 d_2)} \phi((d_1 d_2, m_1 m_2/d_1 d_2)).$$

Como $(m_1, m_2) = 1$, se tiene que $(d_1 d_2, m_1 m_2/d_1 d_2) = (d_1, m_1/d_1)(d_2, m_2/d_2)$, luego

$$\begin{aligned} |C(m_1 m_2)| &= \sum_{d_1|m_1, d_2|m_2} \frac{d_1 d_2}{(d_1, m_1/d_1)(d_2, m_2/d_2)} \phi((d_1, m_1/d_1)) \phi((d_2, m_2/d_2)) \\ &= \sum_{d_1|m_1} \sum_{d_2|m_2} \frac{d_1 d_2}{(d_1, m_1/d_1)(d_2, m_2/d_2)} \phi((d_1, m_1/d_1)) \phi((d_2, m_2/d_2)) \quad = C(m_1) C(m_2). \end{aligned}$$

Lo cuál demuestra que $|C(m)|$ es multiplicativa, usando estos últimos resultados se concluye el lema. □

Ahora podemos calcular la q-expansión. Sea $\gamma \in SL_2(\mathbb{Z})$, escogemos $\sigma \in C(m)$ tal que γ está en la clase lateral derecha correspondiente a σ en el lema 1,2. Esto significa que $\sigma_0 \gamma = \overline{\gamma} \sigma$ para algún $\overline{\gamma} \in SL_2(\mathbb{Z})$, y por lo tanto $j(m\gamma\tau) = j(\sigma_0 \gamma \tau) = j(\overline{\gamma} \sigma \tau) = j(\sigma\tau)$, pues j es $SL_2(\mathbb{Z})$-invariante. Se sigue que

$$j(m\gamma\tau) = j(\sigma\tau).$$

Supongamos que $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$. Sabemos del la charla CM 8, que la q-expansión de j es

$$j(\tau) = \frac{1}{q} + \sum_{n=0}^{\infty} c(n) q^n, \text{ donde } c_n \in \mathbb{Z}.$$

Como $\sigma\tau = (a\tau + b)/d$, se sigue que

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

Si escribimos $\zeta_m = e^(2\pi i/m)$ y recordando que $ab = m$, entonces

$$q(\sigma\tau) = \zeta_m^{ab}(q^{1/m})^{a^2}.$$

Esto nos da la q-expansión

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

Hay sólo un número finito de exponentes negativos de q. lo cuál demuestra que $j(m\tau)$ es meromorfa en las cúspides, concluimos que, $j(m\tau)$ es una función modular para $\Gamma_0(m)$.

Ahora bien, sean $\Gamma_0(m)$ γ_i, i = 1,...,$|C(m)|$ las clases laterales de $\Gamma_0(m)$ en $SL_2(\mathbb{Z})$. Consideramos el polinomio en X

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

Afirmamos que $\Phi_m(X,\tau)$ es un polinomio en X y $j(\tau)$. Consideremos los coeficientes de $\Phi_m(X,\tau)$, al ser polinomios simétricos en los coeficientes $j(m\gamma_i\tau)$ entonces son holomorfos. Sea ahora $\gamma \in SL_2(\mathbb{Z})$, entonces las clases laterales $\Gamma_0(m)\gamma_i\gamma$ son permutaciones de las clases $\Gamma_0(m)\gamma_i$ y como $j(m\tau)$ es invariante por $\Gamma_0(m)$, los $j(m\gamma_i\gamma\tau)$ son permutaciones de los $j(m\gamma_i\tau)$. Esto muestra que los coeficientes de $\Phi_m(X,\tau)$ son invariantes por $SL_2(\mathbb{Z})$. Por último, ya probamos que $j(m\gamma_i\tau) = j(\sigma\tau)$ para algún $\sigma \in C(m)$ y entonces (2) muestra que $j(m\gamma_i\tau)$ tiene sólo finitos exponentes negativos. Como los coeficientes son polinomios en los $j(m\gamma_i\tau)$, entonces son meromorfos en las cúspides.

Lo anterior prueba que los coeficientes de $\Phi(X,\tau)$ son funciones modulares holomorfas y por lo tanto por el lema 1.1 se sigue que son polinomios en $j(\tau)$. luego existe un polinomio $\Phi_m(X,Y) \in \mathbb{C}(X,Y)$, tal que

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

A la ecuación $\Phi_m(X,Y) = 0$ le llamamos la ecuación modular, y a $\Phi_m(X,Y)$ le llamamos el polinomio modular, este polinomio cumple el siguiente lema

Lema 1.4: Sea m entero positivo, entonces $\Phi_m(X,Y)$ es irreducible como polinomio en X.

*Demostración:*Sea $\mathcal{F}_m = \mathbb{C}(j(\tau), j(m\tau))$. Como $\Phi_m(X, j(\tau)) \in \mathbb{C}(j(\tau))[X]$ y $j(m(\tau))$ es raiz, se sigue que $[\mathcal{F}_m : \mathbb{C}(j(\tau))] \leq deg(\Phi(X, j(\tau)))$. Si pudieramos probar la otra desigualdad estaríamos listos, pue sentonces $j(m\tau)$ sería el polinomio minimal de $j(m\tau)$ sobre $\mathbb{C}(j(\tau))$.

Sea entonces $\mathcal{F}$ el cuerpo de todas las funciones meromorfas en $\mathbb{H}$, el cuál contiene a $\mathcal{F}_m$. Para $\gamma \in SL_2(\mathbb{Z})$, sea $\phi_\gamma : \mathcal{F}_m \to \mathcal{F}$, definido por, $\phi_\Gamma(f)(\tau) = f(\gamma\tau)$. Entonces ϕ_γ es una incrustación y es la identidad en $\mathbb{C}(j(\tau))$, pues j es invariante por $SL_2(\mathbb{Z})$. Además, si γ_i y γ_j con $i \neq j$, son dos representantes de clases laterales distintas, se tiene que por (2) $j(m\gamma_i\tau) \neq j(m\gamma_j\tau)$ por lo tanto las incrustaciones son distintas para distintos γ_i, se concluye que $[\mathcal{F}_m : \mathbb{C}(j(\tau))] \geq deg(\Phi(X, j(\tau)))$ lo cual termina la demostración. □

Notemos que, cada $j(\gamma_i\tau)$ puede ser escrita como $j(\sigma\tau)$ para un único $\sigma \in C(m)$. Así también podemos escribir el polinomio modular como

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

Notemos que $j(m\tau)$ siempre es uno de los $j(\sigma\tau)$, ya que $\left(\begin{smallmatrix} m & 0 \\ 0 & 1 \end{smallmatrix}\right) \in C(m)$, por lo tanto $\Phi_m(j(m\tau), j(\tau)) = 0$, la cual es una propiedad importante de la ecuación modular, también notemos que el grado de $\Phi_m(X, Y)$ respecto a X es $|C(m)|$.

Sea ahora $f(\tau)$ una función modular arbitraria para $\Gamma_0(m)$. Consideremos la función

$$G(X, \tau) = \Phi_m(X, j(\tau)) \sum_{i=1}^{|C(m)|} \frac{f(\gamma_i)}{X - j(m\gamma_i\tau)}.$$

Este es un polinomio en X y afirmamos que sus coeficientes son funciones modulares para $SL_2(\mathbb{Z})$, en efecto, tenemos que los coeficientes son sumas de la forma $f(\gamma_r\tau)p_r(\tau)$, donde los p_r, son polinomios simétricos en $j(\gamma_i\tau)$ con $i \neq r$, por lo tanto son meromorfos en $\mathbb{H}$, usando el hecho de que f es invarinate por $\Gamma_0(m)$ y el mismo razonamiento usado anteriormente para el polinomio modular, se concluye que los coeficientes son invarinates por $SL_2(\mathbb{Z})$, por último como f es función modular para $SL_2(\mathbb{Z})$ entonces $f(\gamma_i\tau)$ tiene q-expansión con finitos coeficientes para potencias negativas de q para cada i, se conluye que, los coeficinetes tienen q-expansiones con finitas potencias negativas y por lo tanto son funciones modulares para $SL_2(\mathbb{Z})$. Pero, al ser funciones modulares para $SL_2(\mathbb{Z})$, entonces son funciones racionales para $j(\tau)$, luego $G(X, \tau) = G(X, j(\tau)) \in \mathbb{C}(j(\tau))[X]$.

Podemos asumir que $\gamma_1 = Id$, por la regla del producto tenemos que

$$\frac{\partial \Phi_m}{\partial X}(j(m\tau), j(\tau)) = \prod_{i \neq 1} (j(m\tau) - j(m\gamma_i\tau)).$$

Sustituyendo $X = j(m\tau)$ en la definición de G, obtenemos

$$G(j(m\tau), j(\tau)) = f(\tau) \frac{\partial \Phi_m}{\partial X}(j(m\tau), j(\tau)).$$

Ahora $\Phi_m(X, Y)$ es irreducible y por lo tanto separable, se sigue que $\dfrac{\partial \Phi_m}{\partial X}(j(m\tau), j(\tau)) \neq 0$. Luego

$$f(\tau) = \frac{G(j(m\tau), j(\tau))}{\dfrac{\partial \Phi_m}{\partial X}(j(m\tau), j(\tau))}.$$

Lo cual prueba que f es una función racional en $j(\tau)$ y $j(m\tau)$. El teorema queda entonces demostrado.□