Seminario de modularidad de representaciones de Galois (2020-1)

Héctor Pastén

Pontificia Universidad Católica de Chile

2020/04/28

Contenido de hoy:

Voy a hacer un recuento de lo que hemos estudiado hasta ahora, pero no ordenado por complejidad sino que ordenado por tema.

- Curvas modulares.
- El caso de $\Gamma_0(N)$: Polinomios modulares.
- Formas modulares: $S_2(\Gamma) \simeq H^0(X_\Gamma, \Omega^1)$.
- El principio de q-expansión.
- Operadores y correspondencias de Hecke.
- Congruencia de Eichler-Shimura
- Teoría de Atkin-Lehner-Li.

Curvas modulares

Curvas modulares sobre $\mathbb{C}$

Sea $\Gamma_1(N) \leq \Gamma \leq \Gamma_0(N)$. Tenemos las curvas modulares afín y proyectiva

$$Y_\Gamma = \Gamma\backslash\mathfrak{h}, \quad X_\Gamma = \Gamma\backslash\mathfrak{h}^* \text{ (se agregan finitas cúspides).}$$

Son superficies de Riemann, pero además son espacios de moduli sobre $\mathbb{C}$:

- Y_Γ: curvas elípticas con Γ-estructura en su N-torsión.
- X_Γ: curvas elípticas generalizadas con Γ-estructura.

Para nosotros, los ejemplos más útiles de Γ-estructura:

- $\Gamma_0(N)$: Cualquiera de estos dos problemas de moduli equivalentes:
  - (E, C) con $E/\mathbb{C}$ curva elíptica y $C \leq E$ grupo cíclico de orden N.
  - (E, E', ϕ) con $E, E'/\mathbb{C}$ curvas elípticas y $\phi : E \to E'$ es isogenia con $\ker(\phi)$ cíclico de orden N.
- $\Gamma_1(N)$: El siguiente problema de moduli:
  - (E, P) con $E/\mathbb{C}$ curva elíptica y $P \in E$ un punto de orden N.

El problema del descenso a $\mathbb{Q}$.

Ejemplo no-modular. Las siguientes ecuaciones sobre $\mathbb{Q}$

$$X_1 : x^2 + y^2 + z^2 = 0, \quad X_2 : x^2 + y^2 - z^2 = 0$$

definen curvas suaves, proyectivas en $\mathbb{P}^2$ de género $g = 0$. Así que

$$X_1(\mathbb{C}) \simeq \mathbb{P}^1 \simeq X_2(\mathbb{C}).$$

Pero $X_1 \not\simeq X_2$ sobre $\mathbb{Q}$ dado que $X_1(\mathbb{Q}) = \emptyset$ y $[0 : 1 : 1] \in X_2(\mathbb{Q})$.

Problema del descenso a $\mathbb{Q}$ para X_Γ:

- ¿Es posible definir la curva X_Γ sobre $\mathbb{Q}$?
  Respuesta. Sí, para cualquier $\Gamma_1(N) \leq \Gamma \leq \Gamma_0(N)$.
- Y de ser así, ¿cuál es la "ecuación correcta"?
  Respuesta. El principio básico es "moduli determina los k-puntos". La estructura correcta sobre $\mathbb{Q}$ debe conseguir esto: "$X_\Gamma(k)$ clasifica curvas elípticas E/k con Γ-estructura sobre k."

Ejemplo fundamental: $\Gamma = SL_2(\mathbb{Z})$, $X(1) = X_{SL_2(\mathbb{Z})}$

Problema de moduli sobre k: E curva elíptica sobre k.

El invariante j de una E/k "casi" resuelve el problema de moduli: tenemos

$$j(E) = j(E') \Leftrightarrow E \otimes k^{alg} \simeq E' \otimes k^{alg}.$$

En el caso $k = \mathbb{C}$, la función $j(z) : X(1) \to \mathbb{C}$ dada por

$$j(\tau) = \text{ invariante } j \text{ de la curva elíptica compleja } \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$$

de hecho es holomorfa en $\mathfrak{h}$ con una bonita q-expansión (polo simple en $i\infty$) con coeficientes de Fourier en $\mathbb{Z}$ cuando se ve como $j : \mathfrak{h} \to \mathbb{C}$:

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + ..., \quad q = e^{e\pi i\tau}$$

Ejemplo fundamental: $\Gamma = SL_2(\mathbb{Z})$, $X(1) = X_{SL_2(\mathbb{Z})}$

Escribimos $X_\Gamma^{an} = \Gamma\backslash\mathfrak{h}^*$ para la superficie de Riemann y evitar confundirla con la curva algebraica.

Descenso a $\mathbb{Q}$: Declaramos que $X(1)_{/\mathbb{Q}} = \mathbb{P}^1_{\mathbb{Q}}$ en coordenadas $[1 : j]$.

- El campo de funciones sobre $\mathbb{Q}$ es $\mathbb{Q}(j)$.
- Dada una curva elíptica E sobre un campo $k/\mathbb{Q}$, le corresponde el punto k-racional $x_E = [1 : j_E] \in X(1)(k)$.
- Moduli: Notamos que $x_E = x_{E'}$ si y solo si $E \otimes k^{alg} \simeq E' \otimes k^{alg}$.
- Es modelo de la misma $X(1)^{an} = SL_2(\mathbb{Z})\backslash\mathfrak{h}^*$ de partida: Tenemos el isomorfismo $X(1)^{an} \to X(1)(\mathbb{C}) = \mathbb{P}^1(\mathbb{C})$ dado por $[\tau] \mapsto [1 : j(\tau)]$.
- $i\infty \in X(1)$ es $\mathbb{Q}$-racional: Dado que $j : \mathfrak{h} \to \mathbb{C}$ tiene un polo en $i\infty$ tenemos que $i\infty \mapsto [1 : j(i\infty)] = [1 : \infty] = [0 : 1] \in X(1)(\mathbb{Q})$.

Caso clave para la teoría: $\Gamma = \Gamma_0(N)$, $X_0(N) = X_{\Gamma_0(N)}$

Lema. Sean E, E' sobre $\mathbb{C}$. Si existen $\phi, \psi : E \to E'$ isogenias N-cícilcas no isomorfas, entonces E tiene CM (tiene endomorfismos "raros" que no son del tipo $[m] : E \to E$).
Demostración. Tomar $\theta = \psi^\vee \circ \phi : E \to E$. Entonces $\theta \in End(E)$ tiene grado N^2. Si E no tiene CM, obtendríamos $\theta = [\pm N]$, así que $\psi = \pm\phi$, pero no se puede porque ϕ y ψ son isogenias no-isomorfas. □

Entonces, sobre $\mathbb{C}$, los siguientes problemas de moduli son idénticos salvo un conjunto numerable (omitir los $j(E)$ con CM):

- (E, E', ϕ) con $E, E'/\mathbb{C}$ curvas elípticas y $\phi : E \to E'$ es isogenia con $\ker(\phi)$ cíclico de orden N.
- (E, E') con $E, E'/\mathbb{C}$ curvas elípticas que admiten alguna isogenia $E \to E'$ con kernel cíclico de orden N.

Las curvas $\mathbb{C}/\mathbb{Z} + \mathbb{Z} \cdot \tau$ y $\mathbb{C}/\mathbb{Z} + \mathbb{Z} \cdot (N\tau)$ tiene una N-isogenia cíclica. Se deduce que el segundo problema es resuelto por $(j(\tau), j(N\tau))$.

Caso clave para la teoría: $\Gamma = \Gamma_0(N)$, $X_0(N) = X_{\Gamma_0(N)}$

Sea Y_N^{an} la curva plana imagen de $\tau \mapsto (j(\tau), j(N\tau))$.

- Teorema (cálculo con matrices): Hay un polinomio $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$ que define a Y_N. Se obtiene como ecuación minimal entre $j(z)$ y $j_N(\tau) := j(N\tau)$, así que cumple $\Phi_N(j, j_N) = 0$.
- Por moduli, $X_0(N)^{an}$ e Y_N^{an} son isomorfas salvo un conjunto numerable. Entonces son birracionales: isomorfas salvo finitos puntos
- Por lo tanto $X_0(N)^{an}$ admite un modelo plano birracional sobre $\mathbb{Q}$:

$$\Phi_N(X, Y) = 0.$$

- El modelo plano, salvo finitos puntos, resuelve el problema de moduli. Su desingualización proyectiva resuelve el problema de moduli.
- En particular, la $\mathbb{Q}$-estructura correcta para $X_0(N)^{an}$ es determinada por declara que su campo de funciones es $\mathbb{Q}(j, j_N)$.
- La cúspide $i\infty$ es $\mathbb{Q}$-racional: $[i\infty] \in X_0(N)(\mathbb{Q})$.

Modelos sobre $\mathbb{Z}$

Modelos sobre $\mathbb{Z}$ para $\Gamma_0(N)$

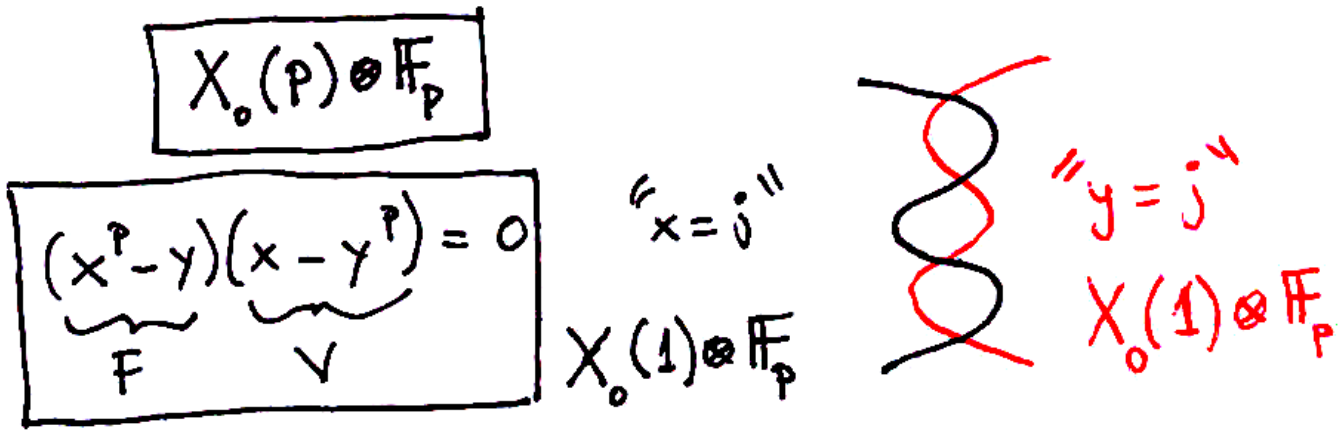
La ecuación $\Phi_N(X, Y) = 0$ define una curva sobre $\mathbb{Z}$. Se puede reducir mod p para todo primo (desingularización proyectiva, etc.)
¿Es la forma correcta de definir $X_0(N)/\mathbb{F}_p$? Es decir, ¿ La curva sobre $\mathbb{F}_p$ dada por $\Phi_N(X, Y)$ mod p, tiene interpretación de moduli?

- **Caso bueno** $p \nmid N$: las isogenias N-cíclicas de curvas elípticas en característica p se comportan igual de bien que en característica 0. Todo lo anterior se adapta y obtenemos que $\Phi_N(X, Y)$ mod p tiene buena interpretación de moduli (salvo tomar desingularización proyectiva).

  Por lo tanto la misma $X_0(N)/\mathbb{Q}$ que construimos se reduce mod p al objeto correcto. Es igual de buena: irreducible, proyectiva, suave.

Modelos sobre $\mathbb{Z}$ para $\Gamma_0(N)$

- **Caso malo fácil** $p = N$: Solo hay dos tipos de p-isogenias: Frobenius $F : E \to E'$ y su dual Verschiebung $V : E' \to E$. Notar que $j(E') = j(E)^p$. Entonces hay 2 tipos de puntos en $X_0(p)^{moduli}/\mathbb{F}_p$: los (j, j^p) y los (j^p, j). En ambas familias el parámetro $j \in X_0(1)/\mathbb{F}_p$ es suficiente, y puede ocurrir $E \simeq E'$ en cuyo caso esas dos copias de $X_0(1)/\mathbb{F}_p$ se cortan. Así que en términos de moduli, lo correcto es:



Esto coincide con tomar nuestra $X_0(p)/\mathbb{Q}$ y reducir mod p:
Teorema. (Kronecker) Se tiene $\Phi_p(X, Y) \equiv (x^p - y)(x - y^p) \bmod p$.

Modelos sobre $\mathbb{Z}$ para $\Gamma_0(N)$

- **Caso malo igual de fácil** $p||N$: muy parecido a $p = N$, pero las dos curvas son copias de $X_0(N/p)$.
- **Caso pésimo** $p^2|N$: complicadísimo, pero hay modelos adecuados (Deligne-Rapoport, Katz-Mazur, Edixhoven, Conrad, etc.).

Caso $\Gamma_1(N) \leq \Gamma \leq \Gamma_0(N)$. Algunos detalles técnicos

El caso general es más complicado. Uno quiere $i\infty \in X_\Gamma(\mathbb{Q})$ para trabajar con q-expansiones. La idea es la siguiente:

- Para $X_1(N)$, mejor usar otro problema de moduli: pares (E, i) donde $i : \mu_N \to E$ es una incrustación cerrada de esquemas de grupo.
- Esto determina un modelo sobre $\mathbb{Q}$ que escribimos $X_1^\mu(N)$. Hay que construirlo a mano y chequear que funciona...
  Es como con $\Gamma_0(N)$: el $\Phi_N(X, Y)$ permite la construcción, y después uno chequea que resuelve el problema de moduli.
- Para X_Γ^{an}: dado que $\Gamma_1(N) \trianglelefteq \Gamma$, el grupo finito $\bar{\Gamma} = \Gamma/\Gamma_1(N)$ actúa en $X_1^\mu(N)$ y se define $X_\Gamma^\mu = \bar{\Gamma}\backslash X_1^\mu(N)$. Con esto, $i\infty \in X_\Gamma^\mu(\mathbb{Q})$.
- El problema de moduli modificado permite obtener modelos enteros decentes (planos=“flat”) sobre $\mathbb{Z}$ que son suaves sobre $\mathbb{Z}[1/N]$.
- Con $\Gamma = \Gamma_0(N)$ estos detalles técnicos no importan. Se obtiene $X_0^\mu(N) \simeq X_0(N)$ sobre $\mathbb{Q}$ y sobre $\mathbb{Z}[1/N]$. Sobre $\mathbb{Z}$ hay discrepancia para $p|N$: solo se cumple $(X_0(N)/\mathbb{Z})^0 \simeq X_0^\mu(N)/\mathbb{Z}$.

El principio de la q-expansión

El principio de la q-expansión, versión para campos

Recordamos que si $f \in S_2(\Gamma)$ entonces

$$\omega_f := 2\pi i f(z)dz = f(z)\frac{dq}{q} = (a_1(f)q + a_2(f)q^2 + ...)\frac{dq}{q} \in H^0(X_\Gamma^{an}, \Omega^1)$$

y esto define un isomorfismo de $\mathbb{C}$-e.v. $S_2(\Gamma) \simeq H^0(X_\Gamma^{an}, \Omega^1)$. Básicamente, q es un parámetro local analítico en $i\infty \in X_\Gamma^{an}$ y la q-expansión de f se convierte en la expansión de Taylor de ω_f en $i\infty$.

Teorema. Sea $\Gamma_1(N) \leq \Gamma \leq \Gamma_0(N)$. Sea $k \subseteq \mathbb{C}$ un campo. Sea $S_2(\Gamma, k) \subseteq S_2(\Gamma)$ el subgrupo formado por aquellas formas modulares f con $a_n(f) \in k$ para todo n. La regla $f \mapsto \omega_f = 2\pi i f(z)dz = f\frac{dq}{q}$ determina un isomorfismo de k-e.v. $S_2(\Gamma, k) \simeq H^0(X_\Gamma^\mu \otimes k, \Omega^1)$.

Idea. Recordar $j = q^{-1} + ... \in \mathbb{Q}(X_\Gamma^\mu)$ y que $i\infty \in X_\Gamma^\mu$. Es posible expresar q en $\mathbb{Q}[[1/j]]$, y al sustituir en $a_1(f)q + a_2(f)q^2 + ...$ se obtiene lo pedido porque $j \in \mathbb{Q}(X_\Gamma^\mu) \subseteq k(X_\Gamma^\mu)$.

El principio de la q-expansión, versión para anillos

Teorema. Sea $\Gamma_1(N) \leq \Gamma \leq \Gamma_0(N)$. Sea A un anillo plano sobre $\mathbb{Z}$, o bien con $N \in A^\times$. Sea $S_2(\Gamma, \mathbb{Z}) \subseteq S_2(\Gamma)$ el subgrupo formado por aquellas formas modulares f con $a_n(f) \in \mathbb{Z}$ para todo n, y sea $S_2(\Gamma, A) := S_2(\Gamma, \mathbb{Z}) \otimes A$. La regla $f \mapsto \omega_f = 2\pi i f(z)dz = f\frac{dq}{q}$ determina un isomorfismo de A-módulos

$$S_2(\Gamma, A) \simeq H^0(X_\Gamma^\mu/A, \Omega^1).$$

Idea. Usar la geometría que $X_\Gamma^\mu/\mathbb{Z}$ con cambio de base plano, o bien de $X_\Gamma^\mu/\mathbb{Z}[1/N]$ donde hay buena reducción y ya no importa si el cambio de base no es plano. En ambos casos, la q-expansión no es otra cosa que la imagen de f en la completación formal a lo largo de $i\infty \in X_\Gamma^\mu/\mathbb{Z}$.

Comentario bien técnico. Uno de verdad necesita X_Γ^μ. Por ejemplo, **no** es verdad que $S_2(\Gamma_0(N), \mathbb{Z}) = H^0(X_0(N)/\mathbb{Z}, \Omega^1)$. El problema es que $\omega \in H^0(X_0(N)/\mathbb{Z}, \Omega^1)$ no tiene denominadores en ninguna parte, en particular en ninguna cúspide, sin embargo $f \in S_2(\Gamma_0(N), \mathbb{Z})$ bien podría tener denominadores al mirar su expansión de Fourier en otras cúspides. Pero esos denominadores solo son divisibles por primos $p|N$. En otros primos $X_0(N)/\mathbb{F}_p \simeq X_0^\mu(N)/\mathbb{F}_p$.

¿Sirven de algo estos tecnicismos?

Corolario. Sea $\Gamma_1(N) \leq \Gamma \leq \Gamma_0(N)$. Se tiene lo siguiente:

(i) $\dim_{\mathbb{Q}} S_2(\Gamma, \mathbb{Q}) = \dim_{\mathbb{C}} S_2(\Gamma)$.

(ii) $S_2(\Gamma, \mathbb{Z})$ es un $\mathbb{Z}$-módulo libre de rango igual a $\dim_{\mathbb{C}} S_2(\Gamma)$.

(iii) $S_2(\Gamma)$ admite una $\mathbb{C}$-base de formas modulares con coeficientes de Fourier en $\mathbb{Z}$.

Idea. El género de una curva sobre $\mathbb{Q}$ no cambia al pasar a $\mathbb{C}$:

$$\dim_{\mathbb{Q}} S_2(\Gamma, \mathbb{Q}) = \dim_{\mathbb{Q}} H^0(X_\Gamma^\mu/\mathbb{Q}, \Omega^1) = \dim_{\mathbb{C}} H^0(X_\Gamma^{an}, \Omega^1) = \dim_{\mathbb{C}} S_2(\Gamma).$$

$\mathbb{C}$ es plano sobre $\mathbb{Z}$ así que $S_2(\Gamma, \mathbb{Z}) \otimes \mathbb{C} = S_2(\Gamma)$ obteniendo (iii).

Usando la geometría de $X_\Gamma^\mu/\mathbb{Z}$ se deduce que $H^0(X_\Gamma^\mu/\mathbb{Z}, \Omega)$ es libre, y su rango se mantiene por cambio de base plano. Eso demuestra (ii).

Operadores y correspondencias de Hecke

Correspondencias

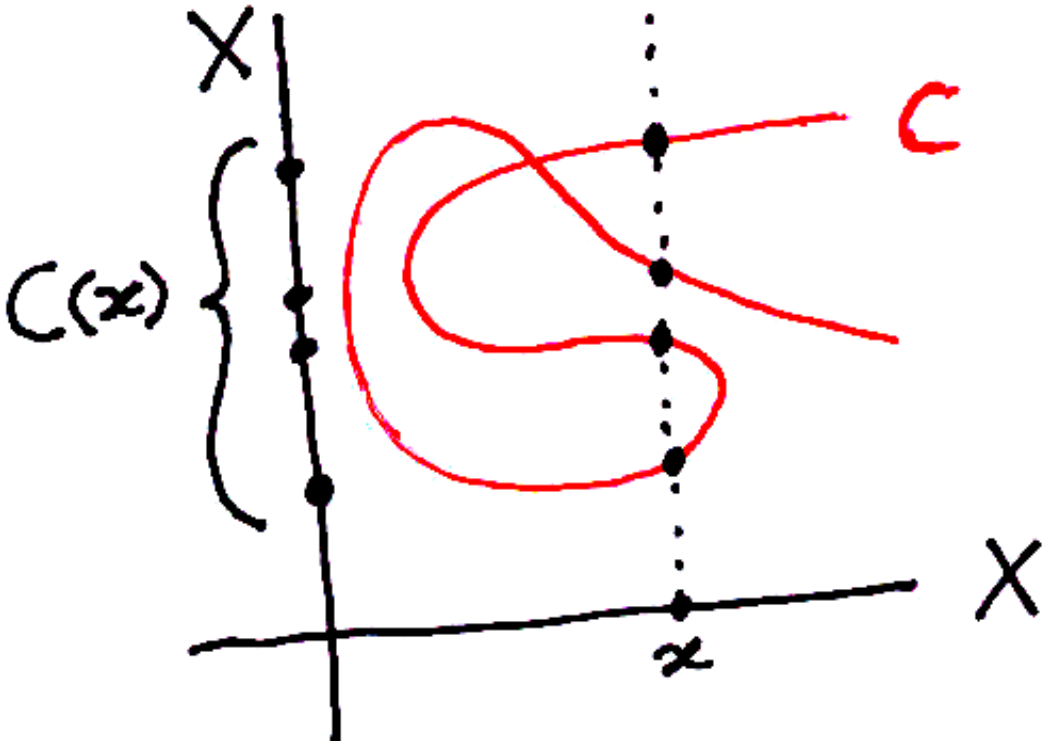
Sea X una curva. Una *correspondencia* C en X es un divisor en $X \times X$.

Parece una definición bien pobre, pero se puede hacer muchas cosas:

- "funciones" con valores en divisores. Las funciones $f : X \to X$ usuales son el caso cuando C es el gráfico de f.
- funciones $Div(X) \to Div(X)$ y $Div^0(X) \to Div^0(X)$.
- Componer correspondencias (como uno haría composición de funciones, pero con las componentes irreducibles de los divisores y $\mathbb{Z}$-linealmente). Entonces las correspondencias forman anillos.
- Actuar en diferenciales de X
- Actuar en J_X
- Actuar en $V_\ell J_X$
- si lo anterior es sobre $\mathbb{Z}$, reducir $\bmod p$ y hacer todo sobre $\mathbb{F}_p$, etc.

Correspondencias

Una función multivaluada $C : X \vdash X$ a partir de una correspondencia $C \subseteq X \times X$:



Correspondencias de Hecke T_p para $\Gamma_0(N)$ con $p \nmid N$

Sea $p \nmid N$. Hay 2 morfismos $\alpha_p, \beta_p : X_0(Np) \to X_0(N)$ bien naturales

- $[E, G] \mapsto [E, C_N]$ con C_N el único subgrupo de G de orden N.
- $[E, G] \mapsto [E/C_p, G/C_p]$ con C_p el único subgrupo de G de orden p.

La **correspondencia de Hecke** T_p (con $p \nmid N$) es la imagen de

$$(\alpha_p, \beta_p) : X_0(Np) \to X_0(N) \times X_0(N).$$

Viendo T_p como función multivaluada $x \mapsto \beta_p(\alpha_p^*(x))$:

- En términos de moduli con $[E, C] \in X_0(N)$.

$$T_p([E, C]) = \sum_{\phi : E \to E'} [E', \phi(C)], \text{ suma sobre } \textbf{todas} \text{ las } p\text{-isogenias } \phi.$$

- Analíticamente con $[\tau] \in X_0(N)$:

$$T_p([\tau]) = [p\tau] + \left[\frac{\tau}{p}\right] + \left[\frac{\tau+1}{p}\right] + \ldots + \left[\frac{\tau+p-1}{p}\right].$$

Correspondencias de Hecke T_p para $\Gamma_0(N)$ con $p \nmid N$

Propiedades de T_p:

- La correspondencia T_p no solo es un divisor: es *irreducible* porque es la imagen de una curva.
- T_p es definida sobre $\mathbb{Q}$ gracias a su interpretacion de moduli.
- T_p es definida sobre $\mathbb{Z}[1/N]$ porque estamos usando el problema (E, C) en lugar de (E, E', ϕ). Eso no es grave, se puede arreglar.
- Entonces T_p mod ℓ es una correspondencia en $X_0(N)_{\mathbb{F}_\ell}$ para cada primo $\ell \nmid N$. (En particular, podríamos tomar T_p mod p.)
- La reducción T_p mod ℓ coincide con la correspondencia obtenida en $X_0(N)_{\mathbb{F}_\ell}$ directamente copiando la definición por moduli.

T_p actuando en $H^0(X_0(N), \Omega^1)$

Es un hecho general que el pull-back de un diferencial regular es un diferencial regular, ya sea que usemos un morfismo o una correspondencia.

Recordamos que para $[\tau] \in X_0(N)$

$$T_p([\tau]) = [p\tau] + \sum_{j=0}^{p-1} \left[\frac{\tau + j}{p} \right].$$

Entonces en un diferencial $f(z)dz$ (con $f \in S_2(\Gamma_0(N))$) tenemos

$$\begin{aligned} T_p^*(f(z)dz) &= pf(pz)dz + \frac{1}{p} \sum_{j=0}^{p-1} f((z+j)/p)dz \\ &= p \sum_n a_n q^{pn} dz + \sum_m \left(\frac{1}{p} \sum_{j=0}^{p-1} e^{2\pi i m \cdot j/p} \right) a_m q^{m/p} dz \\ &= p \sum_n a_n q^{pn} dz + \sum_n a_{pn} q^n dz. \end{aligned}$$

T_p actuando en $S_2(\Gamma_0(N))$

En formas modulares usamos la acción de T_p en $H^0(X_0(N), \Omega^1)$ via el isomorfismo $S_2(\Gamma_0(N)) \simeq H^0(X_0(N), \Omega^1)$. Omitiremos el símbolo de pull-back, porque es la única acción de T_p que usaremos.

Así, es gratuito que la correspondencia T_p define una función

$$T_p : S_2(\Gamma_0(N)) \to S_2(\Gamma_0(N))$$

y se cumple la fórmula

$$T_p(f) = \sum_n a_{pn} q^n + p \sum_n a_n q^{pn}.$$

- ¡De la fórmula no para nada claro que $T_p(f)$ sea una forma modular! pero de la teoría de correspondencias es obvio.
- De la fórmula es obvio que T_p preserva $S_2(\Gamma_0(N), \mathbb{Z})$, y por ende, preserva $S_2(\Gamma_0(N), A) = S_2(\Gamma_0(N), \mathbb{Z}) \otimes A$ para todo anilo A.

Congruencia de Eichler-Shimura

Eichler-Shimura: calcular T_p mod p

Sea $p \nmid N$. Tenemos $T_p : X_0(N) \vdash X_0(N)$ definido sobre $\mathbb{Z}[1/N]$ por

$$T_p([E, C]) = \sum_{\phi: E \to E'} [E', \phi(C)], \quad p\text{-isogenias.}$$

Sobre k de característica p, las curvas elípticas tienen p-isogenias bien limitadas: el Frobenius $F_E : E \to E^{(p)}$ o su dual $V_E : E^{(p)} \to E$. Queremos *todas* las p-isogenias *desde* E, esto nos da

$$(T_p \otimes \mathbb{F}_p)([E, C]) = [E^{(p)}, F_E(C)] + \sum_{E_0 : E_0^{(p)} = E} [E_0, V_{E_0}(C)]$$

(Notar $V_{E_0} : E \to E_0$). Sea $Frob \subseteq X_0(N)_{\mathbb{F}_p} \times X_0(N)_{\mathbb{F}_p}$ el gráfico del Frobenius en $X_0(N)_{\mathbb{F}_p}$ y sea Ver su traspuesta. Entonces

$$\boxed{T_p \otimes \mathbb{F}_p = Frob + Ver} \quad \text{como correspondencias en } X_0(N)_{\mathbb{F}_p}.$$

Una primera aplicación sencilla: $X = X_0(11)$

Tenemos $g(X) = 1$ con $i\infty \in X(\mathbb{Q})$. ¡Es una curva elíptica!

Sea $f = q - 2q^2 - q^3 + 2q^4 + q^5 + \ldots \in S_2(\Gamma_0(11))$ la única forma modular, salvo escalar. Demostraremos $|a_p(f)| < 2\sqrt{p}$ para todo $p \neq 11$.

- Como dim $= 1$, automáticamente f es vector propio de todos los T_p.
- El valor propio es $a_p(f)$ porque $\lambda_p q + \ldots = \lambda_p f = T_p f = a_p q + \ldots$.
- T_p actúa en $H^0(X, \Omega^1) \simeq S_2(\Gamma_0(11))$ como multiplicación por $a_p(f)$.
- T_p actúa en $J_X = X$ como multiplicación por $a_p(f)$. Esto viendo X como toro complejo $\mathbb{C}/\Lambda$ y el típico cálculo "$d(\alpha z) = \alpha d(z)$".
- T_p actúa en $X[\ell^n]$ como multiplicación por $a_p(f)$ para todo n.
- T_p actúa en $V_\ell X$ como multiplicación por $a_p(f)$ (fijar $\ell \nmid 11p$).
- X tiene buena reducción en $p \neq 11$. Así que $V_\ell X \simeq V_\ell(X_{\mathbb{F}_p})$ y T_p actúa como la correspondencia $T_p \bmod p = Frob + Ver$.
- $2a_p(f) = Tr(T_p \bmod p) = Tr(Frob) + Tr(Ver) = 2a_p(X) \in \mathbb{Q}_\ell$. □

Teoría de Atkin-Lehner

Teoría de Atkin-Lehner

Tenemos una descomposición ortogonal (por producto de Petersson):

$$S_2(\Gamma_0(N)) = S_2(\Gamma_0(N))^{old} \oplus S_2(\Gamma_0(N))^{new}$$

donde $S_2(\Gamma_0(N))^{old}$ es generado por formas $f(rz)$ con $f(z) \in S_2(\Gamma_0(m))$ para $m < N$ tal que $mr|N$.

¿Para qué?

- Los T_n son todos simultaneamaente diagonalizables en $S_2(\Gamma_0(N))^{new}$. Esta diagonalización es *única* si pedimos que las f usadas cumplan $a_1(f) = 1$. Se llaman *newforms*.
- Esas newforms son vectores propios de la involución de Atkin-Lehner $w_N : X_0(N) \to X_0(N)$ definida por $z \mapsto -1/(Nz)$.
- Los valores propios de esas newforms son sus coeficientes de Fourier:

$$\lambda q + \lambda a_2 q^2 + \ldots = \lambda_p f = T_p(f) = a_p q + \ldots. \Rightarrow \boxed{\lambda_p = a_p}.$$

Teoría de Atkin-Lehner

Una aplicación es que las newforms tienen una excelente teoría de funciones L:

$$L(f,s) = \sum_{n=1}^{\infty} \frac{a_n(f)}{n^s}.$$

- Modularidad de $f \Rightarrow$ continuación meromorfa de $L(f,s)$ y ecuación funcional relativa a otra forma modular.
- f cuspidal $\Rightarrow$ $L(f,s)$ es entera: no tiene polos.
- f forma propia de $\mathbb{T} \Rightarrow$ $L(f,s)$ admite producto de Euler, gracias a recurrencias de los operadores de Hecke, que se hereda a una recurrencia en sus valores propios, y por ende en los $a_n(f)$.
- f forma propia para $w_N \Rightarrow$ la ecuación funcional de $L(f,s)$ la relaciona con ella misma:

$$L(f,s) = \pm(*)L(f,2-s)$$

donde $(*)$ es un producto de funciones Gamma y exponenciales.

continuación del ejemplo: $X = X_0(11)$

Recordar: Tenemos $g(X) = 1$ con $i\infty \in X(\mathbb{Q})$. ¡Es una curva elíptica!

Sea $f = q - 2q^2 - q^3 + 2q^4 + q^5 + \ldots \in S_2(\Gamma_0(11))$ la única forma modular, salvo escalar. Demostraremos $|a_p(f)| < 2\sqrt{p}$ para todo $p \neq 11$.

- Demostramos $a_p(f) = a_p(X)$ para todo $p \neq 11$.
- Uno chequea a mano que $a_{11}(f) = 1 = a_{11}(X)$.
- Entonces $L(f, s) = L(X, s)$ (mismo producto de Euler). En particular, $L(X, s)$ tiene continuación analítica y ecuación funcional.