# Formes Modulars

**Un introducció a la cinquena operació bàsica**

Marc Masdeu

2024-02-05

# Contingut

# Prefaci

La referència bàsica d'aquests apunts és el llibre Serre [2]. Si voleu aprofundir més, podeu consultar Diamond i Shurman [1].

Tipografiat amb Quarto. Per saber més, vegeu https://quarto.org/docs/books.

# 1 Primer dia

Abans d'introduir els objects que estudiarem, és natural preguntar-nos per què els estudiem (a més del fet que són objectes matemàtics extremadament bonics).

Resulta que molts problemes en la teoria de nombres (i en altres ciències) tracten de *comptar* certs objectes. Per exemple, podem comptar el nombre de particions d'un enter $n$ (maneres d'obtenir $n$ com a suma de naturals positius ordenats), o el nombre de solucions mòdul $n$ de l'equació $y^2 + y = x^3 - x^2$, o bé el nombre de maneres d'escriure $n$ com a suma de 2 quadrats,... Doncs resulta que per tots els problemes anteriors (i molts d'altres) aquests recomptes donen, un cop escrits en forma de sèrie de potències, una forma modular.

El fet anterior ja seria de per si interessant, ja que estudiar formes modulars ens permetria estudiar tots aquests problemes a la vegada. El que és encara més sorprenent és que resulta que les formes modulars constitueixen espais vectorials de dimensió finita, i això fa que si podem construir suficients exemples, podem descobrir identitats sorprenents. Com a mostra, podem enunciar alguns teoremes que aprofiten aquest fet:

**Teorema 1.1.** *Per a tot primer $p$, es té:*

$$\#\{(x,y) \in \mathbb{Z}/p \times \mathbb{Z}/p : y^2 + y = x^3 - x^2\} = p - a_p,$$

*on $a_p$ és el coeficient de $q^p$ de la sèrie formal*

$$q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 + \cdots.$$

**Teorema 1.2** (Fermat)**.** *El nombre de maneres d'escriure $n$ com a suma de 2 quadrats és*

$$4\sum_{\substack{0<d|n\\ d\equiv 1 \mod 4}} d - 4\sum_{\substack{0<d|n\\ d\equiv 3 \mod 4}} d.$$

**Teorema 1.3.** *Sigui $a_p$ el nombre d'arrels del polinomi $x^3 - x - 1$ a $\mathbb{Z}/p\mathbb{Z}$. Aleshores per tot primer $p \neq 23$, $a_p - 1$ és el coeficient de $q^p$ de la sèrie formal*

$$q\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n}).$$

**Teorema 1.4** (Ramanujan)**.** *Sigui $\tau(n)$ el coeficient de $q^n$ de la sèrie formal*

$$\Delta(q) = q\prod_{n\geq 1}(1-q^n)^{24}.$$

*Aleshores per a tot $n \geq 1$,*

$$\tau(n) \equiv \sum_{d|n} d^{11} \pmod{691}.$$

## 1.1 Definicions bàsiques

Considerem el semiplà superior de Poincaré,

$$\mathbb{H} = \{z \in \mathbb{C} : \mathfrak{I}(z) > 0\}$$

i el grup $\mathrm{SL}_2(\mathbb{R})$, definit com

$$\mathrm{SL}_2(\mathbb{R}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{R}) : ad - bc = 1 \right\}.$$

Aquest grup actua en els complexos (de fet, a $\mathbb{C} \cup \{\infty\}$) mitjançant les anomenades *transformacions lineals fraccionàries*:

$$g \cdot z = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot z = \frac{az+b}{cz+d}.$$

Es té una fórmula senzilla per la part imaginària d'aquesta quantitat:

$$\mathfrak{I}(gz) = \frac{\mathfrak{I}(z)}{|cz+d|^2}.$$

Per tant, veiem que $\mathrm{SL}_2(\mathbb{R})$ actua a $\mathbb{H}$. Com que $-1$ actua trivialment, de fet tenim una acció del quocient $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm 1\}$, que de fet és *fidel*.

*Observació* 1.1. De fet, el grup $\mathrm{PSL}_2(\mathbb{R})$ és el grup d'automorfismes analítics d'$\mathbb{H}$.

**Definició 1.1.** El grup $G = \mathrm{PSL}_2(\mathbb{R})$ s'anomena el *grup modular*. Sovint confondrem una matriu $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ amb la seva imatge a $G$.

## 1.2 El domini fonamental

Considerem dos elements a $G$ que jugaran un paper important:

$$S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), \quad T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right).$$

Actuen enviant $z$ a $Sz = -1/z$ i $Tz = z + 1$. A més, satisfan les relacions (a $G$)

$$S^2 = 1, \quad (ST)^3 = 1.$$

Considerem ara el conjunt $D \subseteq \mathbb{H}$ definit com

$$D = \{z \in \mathbb{H} : |\Re(z)| \leq 1/2, |z| \geq 1\}.$$

Es té el següent:

**Teorema 1.5.**

1. *Per cada $z \in \mathbb{H}$ hi ha algun $g \in G$ tal que $gz \in D$.*
2. *Siguin $z, z' \in D$ congruents mòdul $G$. Aleshores o bé $\Re(z) = \pm 1/2$ i $z = z' \pm 1$, o bé $|z| = 1$ i $z' = -1/z$.*
3. *Sigui $z \in D$, i considerem $G_z = \{g \in G : gz = z\}$. Aleshores $G_z = 1$ excepte si:*
   a. *$z = i$, i aleshores $G_i = \{1, S\}$.*
   b. *$z = \rho = e^{2\pi i/3}$, i aleshores $G_\rho = \{1, ST, (ST)^2\}$.*
   c. *$z = -\bar{\rho} = e^{\pi i/3}$, i aleshores $G_{-\bar{\rho}} = \{1, (TS), (TS)^2\}$.*
4. *El grup $G$ està generat per $S$ i $T$. De fet, es té $G = \langle S, T | S^2 = (ST)^3 = 1 \rangle$.*

Considerem $G' = \langle S, T \rangle$. Donat $z \in \mathbb{H}$, trobarem $g' \in G'$ tal que $g'z \in D$. Escrivim $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ un element de $G'$ arbitrari, i observem que hi ha un nombre finit de parelles $(c, d)$ tals que $|cz + d| < M$ (per qualsevol $M$ fixat): si escrivim $z = x + iy$, aleshores $|cz + d| > |cx + d|$ i $|cz + d| > |cy|$ i, per tant, hi ha un nombre finit de $c$ i de $d$ que el fan més petit. Aleshores per la fórmula

$$\Im(gz) = \frac{\Im(z)}{|cz + d|^2}$$

veiem que hi ha algun $g \in G'$ que maximitza $\Im(gz)$. Triem ara $n \in \mathbb{Z}$ tal que $T^n gz$ tingui part real entre $-1/2$ i $1/2$. Aleshores és fàcil veure que $z' = T^n gz$ és a $D$ (si no ho fos, seria perquè $|z'| < 1$, però aleshores $-1/z'$ tindria part imaginària més gran, contradicció).

Per demostrar el segon punt, suposem que $z$ i $gz$ pertanyen a $D$. Per simetria, podem assumir que $\Im(gz) \geq \Im(z)$, és a dir,

$$|cz + d|^2 = (cx + d)^2 + (cy)^2 \leq 1, \quad z = x + iy.$$

Com que $y^2 \geq 3/4$, això implica que $|c| \leq 1$. Analitzant els diferents casos $c = 0$, $c = 1$ i $c = -1$ obtenim el que quedava per demostrar, excepte el fet que $G = G'$.

Sigui ara $g \in G$ un element arbitrari, i prenem $z_0$ a l'interior de $D$. Considerem $z = gz_0$, i trobarem $g' \in G'$ tal que $g'z$ pertanyi a $D$. Pel què hem vist $g'z = z_0$ i d'aquí obtenim $g'g = 1$, i per tant $g$ pertany a $G'$.

**Corol · lari 1.1.** *L'aplicació de pas al quocient $D \longrightarrow \mathbb{H}/G$ és exhaustiva, i la seva restricció a l'interior de $D$ és injectiva.*

## 1.3 Formes modulars

### 1.3.1 Definicions

**Definició 1.2.** Diem que una funció $f$ meromorfa a $\mathbb{H}$ és *dèbilment modular* de pes $k \in \mathbb{Z}$ si

$$f(gz) = (cz + d)^k f(z), \forall g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}).$$

És convenient introduir aquí la notació "slash": definim $f|_k g$ com la funció (que depèn de $k$, encara que no ho posem a la notació)

$$(f|_k g)(z) = (cz + d)^{-k} f(z).$$

Aleshores veiem que $f$ és dèbilment modular si, i només si, $f|_k g = f$ per a tot $g \in \mathrm{SL}_2(\mathbb{Z})$.

Com que $G$ està generat pels elements $S$ i $T$, aquesta condició és equivalent a demanar que, per a tot $z \in \mathbb{H}$,

$$f(z + 1) = f(z), \quad f(-1/z) = z^k f(z).$$

*Observació* 1.2. Aplicant la definició a $-1 \in \mathrm{SL}_2(\mathbb{Z})$ obtenim que $f(z) = (-1)^k f(z)$. Per tant, si $k$ és senar només la funció 0 és dèbilment modular. Demanarem doncs, d'aquí en endavant, que $k$ sigui parell.

Fixem-nos que, si $f(z + 1) = f(z)$ per a tot $z \in \mathbb{H}$, aleshores podem composar amb el canvi $q = e^{2\pi i z}$ i obtenir una funció $\tilde{f}(q)$ definida a

$$\tilde{\mathbb{H}} = \{q \in \mathbb{C} : 0 < |q| < 1\}.$$

Aleshores, $\tilde{f}$ tindrà una sèrie de Laurent al voltant de $q = 0$:

$$\tilde{f}(q) = \sum_{n=-\infty}^{\infty} a_n q^n.$$

Direm aleshores que $f$ és *meromorfa a l'infinit* si $\tilde{f}$ és meromorfa a $q = 0$ ($a_n = 0$ per $n << 0$). També direm que $f$ és *holomorfa a l'infinit* si $a_n = 0$ per $n < 0$, i $f$ s'anul·la a l'infinit si $a_n = 0$ per $n \leq 0$.

**Definició 1.3.** Una *forma modular* de pes $k$ és una funció dèbilment modular que és holomorfa a tot arreu, incloent l'infinit. Si aquesta s'anul·la a l'infinit, l'anomenarem una *forma cuspidal*. Denotem per $M_k$ el $\mathbb{C}$-espai vectorial de les formes modulars de pes $k$, i per $S_k \subseteq M_k$ el subespai de les formes cuspidals.

Resumint, una forma modular de pes $k$ ve donada per una sèrie

$$f(z) = \sum_{n=0}^{\infty} a_n q^n = \sum_{n=0}^{\infty} a_n e^{2\pi i n z},$$

que convergeix per a tot $z \in \mathbb{H}$, i que satisfà $f(-1/z) = z^k f(z)$.

*Observació* 1.3. Si multipliquem una forma modular $f$ de pes $k$ amb una $f'$ de pes $k'$ obtindrem una forma $ff'$ de pes $k + k'$. Obtenim així un anell graduat $M = \bigoplus_{k \in \mathbb{Z}} M_k$.

### 1.3.2 Sèries d'Eisenstein

Per ara els únics exemples que tenim de formes modulars són les constants, que són formes modulars de pes zero (de fet, són les úniques formes modulars de pes zero). Si considerem una funció holomorfa $h$ qualsevol, aleshores una manera de construir una funció modular és "simetritzar-la", és a dir, considerar $\sum_{g \in G} h|_k g$. El problema és que en general aquesta suma no té per què convergir. Una segona idea seria considerar una funció que ja sigui invariant per algun subgrup de $H \leq G$, i aleshores només simetritzar per $G/H$. La versió més senzilla d'aquest principi és considerar la funció constant 1. Si $H = \{\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)\}$, veiem que $1|_k h = 1$ per a tot $h \in H$. Per tant, podem considerar

$$\tilde{G}_k(z) = \sum_{\gamma \in H \backslash \mathrm{SL}_2(\mathbb{Z})} 1|_k \gamma = \sum_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in H \backslash \mathrm{SL}_2(\mathbb{Z})} \frac{1}{(cz+d)^k}.$$

Fixem-nos que, donada una matriu $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, la classe lateral $H\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ està formada per totes les matrius de la forma $\left(\begin{smallmatrix} a' & b' \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. És a dir, les classes laterals venen indexades per parelles $(c, d) \in \mathbb{Z}^2$ amb $\gcd(c, d) = 1$. És més comú considerar *totes* les parelles diferents de $(0, 0)$, i definir

$$G_k(z) = \sum_{(c,d) \neq (0,0)} \frac{1}{(cz+d)^k}.$$

La relació entre $G_k$ i $\tilde{G}_k$ és un factor de $\zeta(k)$ (exercici).

**Proposició 1.1.** *Si $k > 2$, la funció $G_k(z)$ és una forma modular de pes $k$. El seu valor a l'infinit és $2\zeta(k)$, on $\zeta$ és la funció zeta de Riemann.*

Per demostrar la proposició anterior ens calen dos lemes auxiliars.

**Lema 1.1.** *Si $k > 2$, la sèrie*

$$\sum_{(c,d)\neq(0,0)} \max(c,d)^{-k}$$

*convergeix absolutament.*

*Demostració.* Considerem la suma parcial de la sèrie en la caixa $\{|c| \leq N, |d| \leq N\}$. Podem calcular explícitament que aquesta val

$$\sum_{n=1}^{N}(2n+1)n^{-k}.$$

Aquesta suma convergeix, de fet al valor $\zeta(k) + 2\zeta(k-1)$. □

**Lema 1.2.** *Donats $A > 0$ i $B > 0$ reals positius, considerem el compacte*

$$\Omega = \{z \in \mathbb{H} : |\Re(z)| \leq A, \Im(z) \geq B\}.$$

*Aleshores existeix una constant $C = C_{A,B}$ tal que*

$$|z+\delta| > L\max(1,|\delta|), \quad \forall \delta \in \mathbb{R}.$$

*Demostració.* Si $|\delta| < 1$, aleshores $|z+\delta| \geq B = B\max(1,|\delta|)$. Si $1 \leq |\delta| \leq 10A$, aleshores si $\Im(z) > A$ tenim

$$|z+\delta| > A \geq \frac{|\delta|}{10},$$

i si $B \leq \Im z \leq A$ aleshores la funció

$$\left|\frac{z+\delta}{\delta}\right|$$

té un mínim absolut $m$ en el compacte $1 \leq |\delta| \leq 10A$ i $B \leq \Im z \leq A$.

Finalment, si $|\delta| > 10A$, aleshores

$$|z+\delta| \geq |\delta| - |z| > |\delta| - A > \frac{9}{10}|\delta|.$$

□

*de la proposició.* Ens cal primer veure la convergència de la sèrie per tot $z$. Per simplificar la notació, ens restringim a les parelles en el primer quadrant. Si restringim suma doble a parelles a la caixa $\{0 \leq c, d \leq N\}$, per una banda tenim

$$\sum_{d=1}^{N} d^{-k} + \sum_{c=1}^{N} \sum_{d=1}^{N} (cz+d)^{-k}.$$

El primer summand està fitat per $\zeta(k)$ i el podem obviar. Si restringim $z$ al compacte $\Omega_{A,B}$, el segon summand el podem reescriure com

$$\begin{aligned} \sum_{c=1}^{N} \sum_{d=1}^{N} c^{-k}|z+d/c|^{-k} &\leq \sum_{c=1}^{N} \sum_{d=1}^{N} c^{-k} L^k \max(1, d^{-k}/c^{-k}) \\ &= L^k \sum_{c=1}^{N} \sum_{d=1}^{N} \max(c,d)^{-k}. \end{aligned}$$

Pel primer lema, aquesta sèrie convergeix absolutament. Hem vist que la sèrie convergeix absolutament en compactes que recobreixen tot $\mathbb{H}$, i per tant en deduïm la convergència a una funció holomorfa.

Per calcular $G_k(\infty)$, prenem el límit quan $\Im(z) \longrightarrow \infty$, i això ho podem fer mantenint $z$ a $D$. En aquest cas, gràcies a la convergència uniforme de la sèrie podem prendre el límit terme a terme. Els termes que tenen $c \neq 0$ tots van a 0, i només ens queda

$$\lim G_k(z) = \sum_{n \neq 0} n^{-k} = 2\zeta(k).$$

□

Podem normalitzar $G_k$ per tal que prengui el valor 1 a l'infinit, i obtenim $E_k(z) = \frac{1}{2\zeta(k)} G_k(z)$. Aleshores podem fer combinacions de sèries d'Eisenstein per obtenir altres formes modulars. Per exemple,

$$\Delta(z) = \frac{E_4^3 - E_6^2}{1728}$$

és una forma cuspidal de pes 12, anomenada la funció discriminant (més endavant veurem per què hem dividit per 1728).

*Observació* 1.4. Definim, per $\tau \in \mathbb{H}$ i $w \in \mathbb{C}$, la funció $\wp$ de Weierstrass, com

$$\wp_\tau(w) = \frac{1}{w^2} + \sum_{(c,d) \neq (0,0)} \left( \frac{1}{(w - c\tau - d)^2} - \frac{1}{(c\tau + d)^2} \right).$$

Aleshores la sèrie de Laurent de $\wp_\tau$ és fàcil de calcular, i resulta que les sèries d'Eisenstein apareixen com a coeficients d'aquesta sèrie:

$$\wp_\tau(w) = \frac{1}{w^2} + \sum_{k=2}^{\infty} (2k-1) G_{2k}(\tau) w^{2k-2}.$$

De fet, si definim $x = \wp_\tau(w)$ i $y = \wp'_\tau(w)$ (la derivada respecte $w$), tenim

$$y^2 = 4x^3 - 60G_4(\tau)x - 140G_6(\tau),$$

que és una corba el · líptica amb discriminant justament $16\Delta(\tau)$, que per tant és diferent de zero.

## 1.4 L'espai de les formes modulars

### 1.4.1 Zeros i pols d'una funció modular

Sigui $f \neq 0$ una funció meromorfa a $\mathbb{H}$, i sigui $\tau \in \mathbb{H}$. Escrivim $v_\tau(f)$ com l'enter tal que $(z-\tau)^{-v_\tau(f)} f(z)$ és holomorfa i diferent de zero a $z = \tau$ (l'ordre de $f$ a $\tau$).

Si $f$ és una funció modular de pes $k$, aleshores $v_\tau(f) = v_{g\tau}(f)$, perquè $cz + d$ és holomorfa i diferent de zero a tot $\mathbb{H}$. També podem definir $v_\infty(f) = n_0$ si $\tilde{f}(q) = \sum_{n \geq n_0} a_n q^n$ amb $a_{n_0} \neq 0$.

**Teorema 1.6** (fórmula de la valència)**.** *Si $f \neq 0$ és una funció dèbilment modular de pes $k$, es té*

$$v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{\tau \in G\backslash\mathbb{H}} v_\tau(f) = \frac{k}{12},$$

*on la suma recorre les òrbites de punts de $\mathbb{H}$ diferents de $i$, $\rho$ i $-\bar{\rho}$.*

*Observació* 1.5. La suma només conté un nombre finit de termes no nuls. En efecte, com que $f$ és meromorfa tenim que $\tilde{f}$ no té cap zero ni pol al disc $0 < |q| < r$ per algun $r > 0$. Per tant, $f$ no té zeros ni pols a la regió $\Im(z) > \frac{\log(1/r)}{2\pi}$ i, llavors $f$ té tots els zeros i pols de $D$ a la regió compacta $D \cap \Im(z) < \frac{\log(1/r)}{2\pi}$, on només n'hi pot haver un nombre finit.

El teorema es demostra aplicant el teorema del residu a un contorn adequat, i no el farem en aquestes notes.

### 1.4.2 L'àlgebra de formes modulars

Escrivim $M_k$ com el $\mathbb{C}$-espai vectorial format per les formes modulars de pes $k$, i $S_k$ com el subespai format per les formes cuspidals. Com que $S_k = \ker(f \mapsto f(\infty))$, tenim $\dim M_k/S_k \leq 1$. A més, quan $k \geq 4$ les sèries d'Eisenstein són de $M_k \smallsetminus S_k$ i, per tant $M_k = \mathbb{C}G_k \oplus S_k$.

Aplicarem la fórmula de la valència a alguns casos senzills. Per exemple, si $f$ és una funció holomorfa, aleshores tots els termes que apareixen a l'esquerra són positius o zero, i per tant

$M_k = 0$ per $k < 0$. Per $k = 2$, veiem que no hi ha manera d'obtenir $1/6$ sumant múltiples de 1, $1/2$ i $1/3$, i per tant $M_2 = 0$.

Ara, apliquem la fórmula a $G_4$. Podem escriure $1/3 = 0 + 1/2 \cdot 0 + 1/3 \cdot 1 + 0$ (i només d'aquesta manera), i per tant $G_4(\rho) = 0$ (amb ordre 1), i no s'anul · la enlloc més. De forma semblant, $v_i(G_6) = 1$ i aquest és l'únic punt on s'anul · la $G_6$. Observem llavors que $\Delta(i) \neq 0$ i que, per tant $\Delta \neq 0$. A més, per construcció $v_\infty(\Delta) \geq 1$. Per tant, la fórmula de la valència ens diu que $\Delta$ no s'anul · la a $\mathbb{H}$, i té un zero simple a l'infinit.

Finalment, sigui $f$ un element de $S_k$, i definim $g = f/\Delta$. Aleshores $g$ té pes $k - 12$, i $v_\tau(g) \geq 0$ per a tot $\tau$. Per tant $g \in M_{k-12}$.

Podem acabar calculant per $k \leq 10$ els espais $M_k$. En aquest cas, $k - 12 < 0$ i $S_k = 0$. Per tant, $\dim M_k \leq 1$. Com que $1, G_4, G_6, G_8, G_{10}$ són elements de $M_k$ per $k = 0, 4, 6, 8, 10$, formen una base de l'espai corresponent.

Resumim el què hem demostrat:

**Teorema 1.7.**

1. *$M_k = 0$ per $k < 0$ i $k = 2$.*
2. *$M_0 = \mathbb{C} \cdot 1$, $M_4 = \mathbb{C} \cdot G_4$, $M_6 = \mathbb{C} \cdot G_6$, $M_8 = \mathbb{C} \cdot G_8$ i $M_{10} = \mathbb{C} \cdot G_{10}$. En aquests casos, $S_k = 0$.*
3. *La multiplicació per $\Delta$ indueix un isomorfisme $M_{k-12} \cong S_k$.*

*En particular,* $\dim M_k = \lfloor k/12 \rfloor$ *si* $k \equiv 2 \pmod{12}$, *i* $\dim M_k = \lfloor k/12 \rfloor + 1$ *si* $k \neq 2 \pmod{12}$.

**Corol · lari 1.2.** *L'espai $M_k$ té com a base el conjunt de monomis $G_4^i G_6^j$, on $i, j \geq 0$ són enters amb $4i + 6j = k$.*

*Demostració.* Veiem primer que generen, cosa que és clara per $k \leq 6$. Per $k \geq 8$, fem inducció en $k$. Triem enters positius $i, j$ tals que $4i + 6j = k$, i considerem $g = G_4^i G_6^j$, que no s'anul · la a l'infinit. Si $f \in M_k$, aleshores $f - \lambda g \in S_k$ per algun $\lambda \in \mathbb{C}$. Per aquest $\lambda$, tenim $f - \lambda g = \Delta h$ amb $h \in M_{k-12}$. Apliquem ara la hipòtesi d'inducció a $h$, i ja estem.

Si aquests monomis no fossin linealment independents, la funció $G_4^3/G_6^2$ satisfaria un polinomi amb coeficients a $\mathbb{C}$ i, per tant, seria constant. Però això no pot ser, perquè $G_4$ s'anul · la a $\rho$ i $G_6$ no, per exemple. □

*Observació* 1.6. Es pot resumir l'anterior dient que $M = \bigoplus_{k \in \mathbb{Z}} M_k \cong \mathbb{C}[G_4, G_6]$.

# 2 Segon dia

## 2.1 q-expansió de les sèries d'Eisenstein

### 2.1.1 Els nombres de Bernoulli

Es defineixen com els coeficients de la sèrie de Taylor de

$$\frac{t}{e^t-1}=\sum_{k=0}^{\infty}B_k\frac{t^k}{k!}.$$

Es poden calcular de manera recursiva, calculant el terme de grau $n$ de l'expansió

$$t=\sum_{k=0}^{\infty}B_k\frac{t^k}{k!}\sum_{\ell=1}^{\infty}\frac{t^\ell}{\ell!}.$$

De fet, veiem que $B_0=1$, $B_1=-1/2$, i $B_k=0$ per a tot $k\geq 3$ senar. També podem calcular $B_2=1/6$, $B_4=-1/30$,…

L'interès en els nombres de Bernoulli prové del fet que són la "part racional" dels valors de la funció zeta de Riemann en els enters parells (per exemple, $\zeta(2)=\pi^2/6$, $\zeta(4)=\pi^4/90$,…).

**Proposició 2.1.** *Si $n\geq 2$ és un enter parell,*

$$\zeta(n)=\frac{2^{n-1}\pi^n|B_n|}{n!}$$

*Demostració.* Substituint $t=2iz$ a la definició dels nombres de Bernoulli obtenim la fórmula

$$z\cot z=\sum_{k=0}^{\infty}|B_{2k}|\frac{2^{2k}z^{2k}}{(2k)!}.$$

D'altra banda, de la famosa fórmula

$$\sin(z)=z\prod_{n=1}^{\infty}\left(1-\frac{z^2}{n^2\pi^2}\right)$$

n'obtenim, fent la derivada logarítmica,

$$z\cot z=1+2\sum_{n=1}^{\infty}\frac{z^2}{z^2-n^2\pi^2}=1-2\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{z^{2k}}{n^{2k}\pi^{2k}}.$$

Arribem al resultat comparant el terme de $z^{2k}$ de cada equació. □

### 2.1.2 Expansions de les sèries d'Eisenstein

Observem que, de la igualtat

$$z\cot z = 1 + 2\sum_{n=1}^{\infty} \frac{z^2}{z^2 - n^2\pi^2}$$

en podem deduir

$$\pi\cot(\pi z) = \frac{1}{z} + \sum_{m=1}^{\infty}\left(\frac{1}{z+m} - \frac{1}{z-m}\right).$$

D'altra banda,

$$\pi\cot(\pi z) = \pi\frac{\cos(\pi z)}{\sin(\pi z)} = i\pi\frac{q+1}{q-1} = i\pi - \frac{2i\pi}{1-q} = i\pi - 2\pi i\sum_{n=0}^{\infty} q^n.$$

Comparant les dues expressions, obtenim la igualtat bàsica

$$\frac{1}{z} + \sum_{m=1}^{\infty}\left(\frac{1}{z+m} + \frac{1}{z-m}\right) = i\pi - 2\pi i\sum_{n=0}^{\infty} q^n.$$

Derivant-la successivament, obtenim el que es coneix com la **fórmula de Lipschitz**:

$$\sum_{m\in\mathbb{Z}} \frac{1}{(z+m)^k} = \frac{(-1)^k(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty} n^{k-1}q^n, \quad k \geq 2.$$

**Proposició 2.2.** *Per cada $k \geq 4$ parell, tenim*

$$G_k(z) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n.$$

*Demostració.* Expandim $G_k(z)$ com

$$G_k(z) = \sum_{(m,n)\neq(0,0)} \frac{1}{(mz+n)^k} = 2\zeta(k) + 2\sum_{m=1}^{\infty}\sum_{n\in\mathbb{Z}}\frac{1}{(mz+n)^k}.$$

Aplicant la igualtat bàsica anterior amb $mz$ en comptes de $z$, tenim

$$\begin{aligned} G_k(z) &= 2\zeta(k) + 2\frac{(-1)^k(2\pi i)^k}{(k-1)!}\sum_{d=1}^{\infty}\sum_{a=1}^{\infty} d^{k-1}q^{ad} \\ &= 2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n. \end{aligned}$$

□

**Corol · lari 2.1.** *Tenim $G_k(z) = 2\zeta(k)E_k(z)$, amb*

$$E_k(z) = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n.$$

Per exemple,

$$E_4 = 1 + 240\sum_{n\geq 1}\sigma_3(n)q^n, \qquad E_6 = 1 - 504\sum_{n\geq 1}\sigma_5(n)q^n,$$
$$E_8 = 1 + 480\sum_{n\geq 1}\sigma_7(n)q^n, \qquad E_{10} = 1 - 264\sum_{n\geq 1}\sigma_9(n)q^n,$$
$$E_{12} = 1 + \frac{65520}{691}\sum_{n\geq 1}\sigma_{11}(n)q^n, \qquad E_{14} = 1 - 24\sum_{n\geq 1}\sigma_{13}(n)q^n.$$

### 2.1.3 Una primera aplicació

Ja hem vist que $M_8$, $M_{10}$ i $M_{14}$ tenen dimensió 1. Per tant, $E_4^2 = E_8$, $E_4E_6 = E_{10}$ i $E_4E_{10} = E_{14}$. Comparant coeficients de les corresponents expansions, obtenim les identitats

$$\sigma_7(n) = \sigma_3(n) + 120\sum_{m=1}^{n-1}\sigma_3(m)\sigma_3(n-m),$$
$$11\sigma_9(n) = 21\sigma_5(n) - 10\sigma_3(n) + 5040\sum_{m=1}^{n-1}\sigma_3(m)\sigma_5(n-m), i$$
$$\sigma_{13}(n) = 11\sigma_9(n) - 10\sigma_3(n) + 2640\sum_{m=1}^{n}\sigma_3(n)\sigma_9(n-m).$$

## 2.2 L'expansió de la funció discriminant

Volem donar una fórmula per $\Delta(z) = \frac{E_4(z)^3 - E_6(z)^2}{1728}$. Per això, considerem $\tilde{\Delta} = q\prod_{n=1}^{\infty}(1-q^n)^{24}$ a on, com sempre, $q = e^{2\pi i z}$. Veurem que aquestes dues funcions coincideixen. Per fer-ho, prenem primer la derivada logarítmica de $\tilde{\Delta}$, i obtenim (fixem-nos que $\operatorname{dlog} q = 2\pi i$)

$$\operatorname{dlog}\tilde{\Delta} = 2\pi i + 24\sum_{n=1}^{\infty}\frac{-2\pi i n q^n}{1-q^n} = 2\pi i\left(1 - 24\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n}\right).$$

Observem que

$$\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n} = \sum_{n=1}^{\infty}n\sum_{m=1}^{\infty}q^{nm} = \sum_{n\geq 1}\sigma_1(n)q^n,$$

i per tant obtenim

$$\operatorname{dlog}\tilde{\Delta} = 2\pi i\left(1 - 24\sum_{n\geq 1}\sigma_1(n)q^n\right).$$

### 2.2.1 La sèrie d'Eisenstein de pes 2

Considerem la funció

$$G_2(z) = \sum_{m=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^2},$$

on si $m = 0$ hem d'ometre el terme $n = 0$ (a partir d'ara això no ho direm). Podem separar el terme $m = 0$ i obtenir:

$$G_2(z) = 2\zeta(2) + \sum_{m\neq 0} \sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)^2}.$$

Igual que hem fet amb les series d'Eisenstein de pes $k \geq 4$, podem calcular els coeficients de Fourier de $G_2$, i obtenim

$$G_2(z) = 2\zeta(2) - 8\pi^2 \sum_{n=1}^{\infty} \sigma_1(n) q^n = \frac{\pi^2}{3} E_2(z),$$

amb

$$E_2(z) = 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n.$$

És clar, doncs, que $G_2(z+1) = G_2(z)$. Ara bé, si intentem calcular $G_2(-1/z)$ trobarem un comportament curiós:

$$G_2(-1/z) = \sum_{m=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} \frac{z^2}{(nz+m)^2} = z^2 \sum_{n=-\infty}^{\infty} \sum_{m=-\infty}^{\infty} \frac{1}{(mz+n)^2}.$$

Fixem-nos que l'ordre dels sumatoris està canviat! Per relacionar-ho altra vegada amb $G(z)$, ens cal primer poder-la escriure com la suma d'una sèrie absolutament convergent.

**Lema 2.1.** *Es pot escriure*

$$G_2(z) = 2\zeta(2) + \sum_{m\neq 0, n\in\mathbb{Z}} \frac{1}{(mz+n)^2(mz+n+1)},$$

*on la sèrie és absolutament convergent.*

*Demostració.* Només cal calcular

$$\begin{aligned} \sum_{m\neq 0} \sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)(mz+n+1)} &= \sum_{m\neq 0} \sum_{n\in\mathbb{Z}} \left( \frac{1}{mz+n} - \frac{1}{mz+n+1} \right) \\ &= \sum_{m\neq 0} 0 = 0. \end{aligned}$$

Per tant, podem restar el terme general de la sèrie que defineix $G_2(z)$, per obtenir

$$\begin{aligned} G_2(z) &= 2\zeta(2) + \sum_{m\neq 0}\sum_{n\in\mathbb{Z}} \left( \frac{1}{(mz+n)^2} - \frac{1}{(mz+n)(mz+n+1)} \right) \\ &= 2\zeta(2) + \sum_{m\neq 0}\sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)^2(mz+n+1)}. \end{aligned}$$

□

Ara podem veure com es transforma $G_2$:

$$\begin{aligned} z^{-2}G_2(-1/z) - G_2(z) &= \sum_{n\in\mathbb{Z}}\sum_{m\neq 0} \left( \frac{1}{(mz+n)^2} - \frac{1}{(mz+n)^2(mz+n+1)} \right) \\ &= \sum_{n\in\mathbb{Z}}\sum_{m\neq 0} \frac{1}{(mz+n)(mz+n+1)} \\ &= \sum_{n\in\mathbb{Z}}\sum_{m\neq 0} \left( \frac{1}{mz+n} - \frac{1}{mz+n+1} \right) \end{aligned}$$

Aquesta última suma la podem calcular explícitament:

$$\begin{aligned} \sum_{n=-N}^{N-1}\sum_{m\neq 0} \left( \frac{1}{mz+n} - \frac{1}{mz+n+1} \right) &= \sum_{m\neq 0}\sum_{n=-N}^{N-1} \left( \frac{1}{mz+n} - \frac{1}{mz+n+1} \right) \\ &= \sum_{m\neq 0} \left( \frac{1}{mz-N} - \frac{1}{mz+N} \right) \\ &= \frac{2}{N} + \frac{-2\pi}{z}\cot(\pi N/z). \end{aligned}$$

Per poder calcular el límit, observem que

$$\lim_{N\longrightarrow\infty} \cot(\pi N/z) = \lim_{N\longrightarrow\infty} i(1 - 2\sum_{m=0}^{\infty} e^{2\pi m N/z}) = i.$$

Resumint, hem trobat:

**Teorema 2.1.** *La funció $G_2$ satisfà, per a tot $z \in \mathbb{H}$,*

$$G_2(z+1) = G_2(z), \quad G_2(-1/z) = z^2 G_2(z) - 2\pi i z.$$

*De fet, per a tot $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$,*

$$G_2(\gamma z) = (cz+d)^2 G_2(z) - 2\pi i c(cz+d).$$

*En termes de la funció normalitzada $E_2(z)$, tenim*

$$E_2(-1/z) = z^2 E_2(z) + \frac{12z}{2\pi i},$$

*i per $\gamma$ qualsevol:*

$$E_2(\gamma z) = (cz+d)^2 E_2(z) + \frac{12}{2\pi i} c(cz+d).$$

### 2.2.2 Relació amb la funció delta

Els càlculs que hem fet fins ara ens demostren que

$$\operatorname{dlog} \tilde{\Delta} = 2\pi i E_2.$$

Podem calcular, per a tot $z \in \mathbb{H}$,

$$\begin{aligned}\operatorname{dlog}\left(z^{-12}\tilde{\Delta}(-1/z)\right) &= \frac{-12}{z} + \operatorname{dlog}\tilde{\Delta}(-1/z) \\ &= \frac{-12}{z} + 2\pi i(z^{-2}E_2(-1/z)) \\ &= 2\pi i E_2(z) = \operatorname{dlog}\tilde{\Delta}(z).\end{aligned}$$

Per tant, $z^{-12}\tilde{\Delta}(-1/z) = C\tilde{\Delta}(z)$, per certa constant $C$. Evaluant a $z = i$ podem veure que $C = 1$ (ja que $\Delta(i) \neq 0$) i que, per tant $\tilde{\Delta}$ és una forma modular de pes 12. És doncs un múltiple de $\Delta(z)$, que ha de ser 1 perquè ambdues sèries de Fourier comencen per $q + O(q^2)$.

### 2.2.3 La funció tau de Ramanujan

Calculant els primers termes del producte $\tilde{\Delta} = q\prod_{n=1}^{\infty}(1-q^n)^{24}$, de seguida veiem que

$$\begin{aligned}\tilde{\Delta} &= \sum_{n\geq 1}\tau(n)q^n \\ &= q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 \\ &\quad - 6048q^6 - 16744q^7 + O(q^8).\end{aligned}$$

Ramanujan va ser el primer a estudiar la funció $\tau(n)$ el 1916, i va conjecturar que:

1. $\tau(n)\tau(m) = \tau(nm)$ si $(n,m) = 1$.
2. $\tau(p^{k+1}) = \tau(p)\tau(p^k) - p^{11}\tau(p^{k-1})$, per a tot primer $p$ i $k \geq 1$; i
3. $|\tau(p)| \leq 2p^{11/2}$ per a tot primer $p$.

També va observar (sense demostrar-les) tot de congruències que satisfà:

1. $\tau(n) \equiv n^2\sigma_7(n) \pmod{27}$
2. $\tau(n) \equiv n\sigma_3(n) \pmod{7}$
3. $\tau(n) \equiv \sigma_{11}(n) \pmod{691}$.

Tot això, vist un segle després, és relativament fàcil de demostrar amb la teoria de les formes modulars. El proper dia veurem que $|\tau(p)| = O(p^6)$, però per veure la fita més fina conjecturada per Ramanujan hauríem de fer servir resultats molt més profunds de P.Deligne (1974).

Vegem aquí una d'aquestes congruències:

**Teorema 2.2.** *Per a tot $n \geq 1$, es té*

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}.$$

*Demostració.* Treballarem a $M_{12}$, i amb les formes $\Delta$, $E_{12}$, $E_4^3$ i $E_6^2$. Resulta que

$$E_{12} = 1 + \frac{65520}{691}\sum_{n\geq 1}\sigma_{11}(n)q^n.$$

Igualant els dos primers coeficients, trobem la igualtat

$$691E_{12} = 441E_4^3 + 250E_6^2.$$

Per altra banda, recordem que

$$1728\Delta = E_4^3 - E_6^2.$$

Per tant, tenim

$$441 \cdot 1728\Delta = 441E_4^3 - 441E_6^2 = 691E_{12} - 691E_6^2.$$

Mirant el terme $n$ d'aquesta expressió obtenim

$$441 \cdot 1728\tau(n) = 65520\sigma_{11}(n) - 691a_n(E_6^2).$$

Com que $E_6$ té tots els coeficients enters i $441 \cdot 1728 \equiv 566 \equiv 65520 \pmod{691}$, obtenim el resultat. □

## 2.3 L'operador diferencial de Ramanujan-Serre

Considerem l'operador diferencial $D = q\frac{d}{dq} = \frac{1}{2\pi i}\frac{d}{dz}$ actuant en les funcions diferenciables.

**Definició 2.1.** L'operador diferencial de Ramanujan-Serre és $\theta_k$:

$$\theta_k(f) = Df - \frac{k}{12}E_2 f.$$

Aquest operador $\theta_k$ és lineal i satisfà la regla del producte, però el motiu que l'estudiem aquí és el següent:

**Proposició 2.3.** *$\theta_k$ porta formes modulars de pes $k$ a formes modulars de pes $k+2$, i preserva els subespais de formes cuspidals.*

*Demostració.* Holomorfia a $\mathbb{H}$ i a $i\infty$ és automàtica, per la definició. Només cal comprovar que $\theta_k(f)$ és dèbilment modular de pes $k$, i això és un simple exercici. □

Definim, per comoditat $P = E_2$, $Q = E_4$ i $R = E_6$ (aquesta és la notació original de Ramanujan).

**Proposició 2.4.** *Es té:*

1. $DP = \frac{1}{12}(P^2 - Q)$.
2. $DQ = \frac{1}{3}(PQ - R)$,
3. $DR = \frac{1}{2}(PR - Q^2)$, *i*

*Demostració.* Les dues últimes identitats són equivalents a $\theta_4(Q) = -\frac{1}{3}R$ i $\theta_6(R) = -\frac{1}{2}Q^2$, respectivament. La demostració és automàtica, tenint en compte que $M_6$ i $M_8$ tenen dimensió 1. Per veure la primera afirmació, només cal comprovar que $H = DP - \frac{1}{12}P^2$ és una forma modular de pes 4, i això es veu directament fent servir la propietat de transformació de $P$:

$$P'(-1/z)z^{-2} = 2zP(z) + z^2P'(z) + \frac{6}{i\pi}.$$

Definim $H(z) = \frac{1}{2\pi i}P'(z) - \frac{1}{12}P^2(z)$, aleshores podem comprovar:

$$H(-1/z) = \frac{1}{2\pi i}P'(-1/z) - \frac{1}{12}P(-1/z)^2 = (\cdots) = z^4H(z).$$

□

Amb aquestes identitats ja podem demostrar més resultats de Ramanujan. Per exemple:

**Proposició 2.5.** *Per a tot $n \geq 1$, es té $\tau(n) \equiv n\sigma_3(n) \pmod 7$.*

*Demostració.* Com que $1728 \equiv 6 \pmod 7$, tenim

$$6\Delta = Q^3 - R^2.$$

D'altra banda, $Q^2 = E_8 \equiv P \pmod 7$, perquè $480 \equiv -24 \pmod 7$ i $n^7 \equiv n \pmod 7$. A més, com que $504 \equiv 0 \pmod 7$, tenim $R \equiv 1 \pmod 7$. Aleshores:

$$6\Delta = Q^3 - R^2 \equiv PQ - 1 \equiv 3DQ \implies 2\Delta \equiv DQ \pmod 7.$$

Finalment, observem que $DQ = 240\sum_{n\geq 1} n\sigma_3(n)q^n$. Com que $240 \equiv 2 \pmod 7$, en deduïm

$$\Delta = \sum_{n\geq 1} \tau(n)q^n \equiv \sum_{n\geq 1} n\sigma_3(n)q^n.$$

□

**Proposició 2.6.** *Per a tot $n \geq 1$, es té $\tau(n) \equiv n^2\sigma_7(n) \pmod{27}$.*

*Demostració.* Aplicant les fórmules que hem trobat per $D$ i la regla del producte, arribem a

$$D^2(Q^2) = \frac{1}{2}P^2Q^2 + \frac{5}{18}Q^3 - PQR + \frac{2}{9}R^2.$$

Fent servir que

$$\frac{5}{18}Q^3 = \frac{5}{18}(Q^3 - R^2) + \frac{5}{18}R^2 = 480\Delta + \frac{5}{18}R^2,$$

obtenim

$$D^2(Q^2) = 480\Delta + \frac{1}{2}P^2Q^2 - PQR + \frac{1}{2}R^2.$$

Fent servir que $PQ = 3DQ + R$, obtenim

$$\begin{aligned}(PQ)^2 + R^2 - 2PQR &= (3DQ + R)^2 + R^2 - 2R(3DQ + R)\\ &= 9(DQ)^2,\end{aligned}$$

i per tant

$$D^2(Q^2) = 480\Delta + \frac{9}{2}(DQ)^2.$$

Com que $D^2(Q^2) = 480\sum_{n\geq 1}\sigma_7(n)q^n$, per acabar només hem d'obervar que $DQ \equiv 0 \pmod 9$ i en deduïm que

$$160\sum_{n\geq 1}\sigma_7(n)q^n \equiv 160\sum_{n\geq 1}\tau(n)q^n \pmod{27}.$$

Com que $7 \nmid 160$, ja hem acabat. □

# 3 Tercer dia

## 3.1 Operadors de Hecke

### 3.1.1 Definició

Sigui $f$ una forma dèbilment modular de pes $k$ (és a dir, meromorfa i satisfent la simetria corresponent per $\mathrm{SL}_2(\mathbb{Z})$). Per cada $n \geq 1$, definim

$$(T_n f)(z) = n^{k-1} \sum_{e \geq 1, ed=n} \sum_{0 \leq b < d} d^{-k} f\left(\frac{ez+b}{d}\right).$$

En particular, si $n = p$ és un primer, tenim

$$(T_p f)(z) = \frac{1}{p}\left(\sum_{b=0}^{p-1} f(\frac{z+b}{p}) + f(pz)\right).$$

**Proposició 3.1.** *La funció $T_n f$ és dèbilment modular de pes $k$. Si $f$ és holomorfa, també ho és $T_n f$. A més:*

1. *$T_m T_n = T_n T_m = T_{nm}$ si $(m,n) = 1$.*
2. *$T_{p^{r+1}} = T_p T_{p^r} - p^{k-1} T_{p^{r-1}}$ si $p$ és primer i $n \geq 1$.*

Podem calcular l'efecte d'aquests operadors en les $q$-expansions, obtenint:

**Proposició 3.2.** *Si $f(z) = \sum_{m \in \mathbb{Z}} a_m(f) q^m$ és meromorfa l'infinit, aleshores $T_n f(z) = \sum_{m \in \mathbb{Z}} a_m(T_n f) q^m$ també ho és, i*

$$a_m(T_n f) = \sum_{d | (m,n)} d^{k-1} a_{mn/d^2}(f).$$

*En particular, $a_0(T_n f) = \sigma_{k-1}(n) a_0(f)$, $a_1(T_n f) = a_n(f)$ i, si $n = p$ és un primer,*

$$a_m(T_p f) = a_{pm}(f) + p^{k-1} a_{m/p}(f),$$

*on entenem que $a_{m/p}(f) = 0$ si $p$ no divideix $m$.*

**Corol · lari 3.1.** *Els operadors $T_n$ actuen a $M_k$ i $S_k$, i commuten entre si.*

### 3.1.2 Formes pròpies

Suposem ara que $f = \sum_{n\geq 0} a_n(f)q^n$ és una forma modular de pes $k > 0$, que és pròpia per tots els $T_n$. És a dir, per cada $n \geq 1$ tenim $T_n f = \lambda_n f$, per algun $\lambda_n \in \mathbb{C}$.

**Teorema 3.1.** *Si $f$ és pròpia, $a_1(f) \neq 0$. Si $f$ està normalitzada de manera que $a_1(f) = 1$, aleshores $a_n(f) = \lambda_n$.*

*Demostració.* Hem vist que $a_1(T_n f) = a_n(f)$. Com que $f$ és pròpia, $a_1(T_n f) = \lambda_n a_1(f)$. Per tant, $a_n(f) = \lambda_n a_1(f)$. Si suposem que $a_1(f) = 0$, aleshores tindríem $a_n(f) = 0$ per a tot $n \geq 1$, i per tant $f$ seria una constant. Però $k > 0$, i per tant arribem a contradicció. □

**Corol · lari 3.2.** *Si $f$ i $g$ són formes pròpies per tot $T_n$ amb els mateixos valors propis, aleshores són proporcionals.*

**Corol · lari 3.3.** *Si $f$ és pròpia i està normalitzada, aleshores*

$$a_m(f)a_n(f) = a_{mn}(f), \textit{ si } (m,n) = 1, \textit{ i}$$

$$a_{p^{r+1}}(f) = a_p(f)a_{p^r}(f) - p^{k-1}a_{r-1}(f).$$

### 3.1.3 Aplicació a la tau de Ramanujan

Recordem $\Delta(q) = q\prod_{n\geq 1}(1-q^n)^{24}$. Com ja hem vist, $S_{12} = \mathbb{C}\Delta$ i per tant $\Delta$ és trivialment una forma pròpia per tots els operadors de Hecke, que a més ja està normalitzada. Per tant:

**Corol · lari 3.4.** *Tenim:*

$$\tau(nm) = \tau(n)\tau(m), \quad (n,m) = 1,$$

*i*

$$\tau(p)\tau(p^n) = \tau(p^{n+1}) + p^{11}\tau(p^{n-1}), \quad \forall p \textit{ primer}, n \geq 1.$$

Es tenen resultats anàlegs per tots els espais $S_k$ de dimensió 1, que són exactament $k = 12, 16, 18, 20, 22, 26$. El generador és, en cada cas, $\Delta E_{k-12}$.

## 3.2 Creixement dels coeficients

Més endavant ens interessarà tenir fites per l'ordre de creixement dels coeficients de Fourier de les formes modulars.

**Proposició 3.3.** *Si $f = E_k$, aleshores $a_n \approx n^{k-1}$. És a dir, que hi ha constants $A, B > 0$ tals que*

$$An^{k-1} \leq |a_n| \leq Bn^{k-1}.$$

*Demostració.* Tenim $|a_n| = A\sigma_{k-1}(n) \geq An^{k-1}$. D'altra banda,

$$\frac{|a_n|}{n^{k-1}} = A\sum_{d|n} \frac{1}{d^{k-1}} \leq A\sum_{d=1}^{\infty} \frac{1}{d^{k-1}} = A\zeta(k-1) < \infty.$$

□

El creixement de les formes cuspidals és més lent:

**Teorema 3.2** (Hecke)**.** *Si $f$ és una forma cuspidal de pes $k$, llavors $a_n = O(n^{k/2})$.*

*Demostració.* Primer de tot, com que $a_0 = 0$, podem escriure $f(z) = q\sum_{n\geq 1} a_n q^{n-1}$ i, per tant,

$$|f(z)| = O(q) = O(e^{-2\pi\Im(z)}), \quad q \longrightarrow 0.$$

Escrivim $z = x + iy$, i definim $\phi(z) = |f(z)|y^{k/2}$. La modularitat de $f$ fa que la funció $C^\infty$ (no-holomorfa) $\phi$ sigui invariant per $\mathrm{SL}_2(\mathbb{Z})$, i $\phi(z) \longrightarrow 0$ quan $\Im(z) \longrightarrow \infty$. Per tant, $\phi$ és fitada: hi ha alguna constant $M$ tal que

$$|f(z)| \leq My^{-k/2}, \quad z \in \mathbb{H}.$$

Per com es calculen els coeficients de Fourier, tenim

$$a_n = \int_0^1 f(x+iy)e^{-2\pi in(x+iy)}dx,$$

i per tant

$$|a_n| \leq Me^{2\pi ny}\int_0^1 y^{-k/2}e^{-2\pi inx}dx = My^{-k/2}e^{2\pi iny}.$$

Aquesta igualtat és vàlida per tot $y > 0$. En particular, per $y = 1/n$ dona

$$|a_n| \leq e^{2\pi}Mn^{k/2}.$$

□

**Corol · lari 3.5.** *Si $f$ no és cuspidal, aleshores $a_n \approx n^{k-1}$.*

*Demostració.* Escrivim $f = \lambda E_k + h$ amb $\lambda \neq 0$ i $h$ cuspidal, i apliquem els resultats anteriors. Com que els coeficients de $E_k$ creixen molt més ràpid que els de $h$, el creixement de $f$ és igual que el de $E_k$. □

*Observació* 3.1. Un teorema molt profund de Deligne (1973) demostra, de fet, que $a_n = O(n^{(k-1)/2}\sigma_0(n)) = O(n^{(k-1)/2-\epsilon})$ per a tot $\epsilon > 0$. Abans del resultat de Deligne, aquest fet es coneixia com la conjectura de Petersson, que generalitzava una conjectura famosa de Ramanujan sobre la funció $\tau(n)$.

## 3.3 La funció-L associada a una forma modular

Podem empaquetar tota la informació que hem trobat de manera analítica, mitjançant la funció-L. Sigui

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

Observem que convergeix per a tot $\Re(s) > k$ gràcies a que controlem el creixement dels $a_n(f)$. Si $f$ és cuspidal, aleshores sabem que la sèrie convergeix a $\Re(s) > k/2 + 1$.

### 3.3.1 El producte d'Euler i l'equació funcional

**Proposició 3.4.** *Si $f$ és una forma pròpia normalitzada, aleshores la funció $L(f,s)$ té un producte d'Euler:*

$$L(f,s) = \prod_{p \text{ primer}} \frac{1}{1 - a_p(f)p^{-s} + p^{k-1-2s}}.$$

*Demostració.* Els coeficients $a_n(f)$ formen una successió multiplicativa i, per tant,

$$L(f,s) = \prod_{p} \sum_{r=0}^{\infty} a_{p^r}(f) p^{-rs}.$$

Per tant, si escrivim $T = p^{-s}$, hem de demostrar

$$\sum_{r=0}^{\infty} a_{p^r}(f) T^r = \left(1 - a_p(f)T + p^{k-1}T^2\right)^{-1}.$$

Equivalentment, podem demostrar

$$\left(1 - a_p(f)T + p^{k-1}T^2\right) \sum_{r=0}^{\infty} a_{p^r}(f) T^r = 1.$$

El coeficient de $T$ és $a_p(f) - a_p(f) = 0$. El de $T^{r+1}$ és, per a tot $r \geq 1$,

$$a_{p^{r+1}} - a_p a_{p^r} + p^{k-1} a_{p^{r-1}},$$

que ja sabem que és 0. □

*Observació* 3.2. El recíproc també és cert, i la demostració és essentialment el mateix argument fet a l'inrevés.

Per escriure l'equació funcional, escrivim $\Lambda(f,s) = (2\pi)^{-s}\Gamma(s)L(f,s)$, on

$$\Gamma(s) = \int_0^\infty t^s e^{-t} \frac{dt}{t}.$$

Podem trobar una formula integral per $\Lambda(f,s)$:

$$\begin{aligned}\Lambda(f,s) &= (2\pi)^{-s} \int_0^\infty t^s e^{-t} \frac{dt}{t} \sum_{n=1}^\infty a_n n^{-s} \\ &= \sum_{n=1}^\infty a_n \int_0^\infty \left(\frac{t}{2\pi n}\right)^s e^{-t} \frac{dt}{t}.\end{aligned}$$

Si fem el canvi de variables $t \mapsto t/(2\pi n)$ al terme $n$-èssim, obtenim

$$\sum_{n=1}^\infty a_n \int_0^\infty t^s e^{-2\pi n t} \frac{dt}{t} = \int_0^\infty \left(\sum_{n=1}^\infty a_n e^{-2\pi n t}\right) t^s \frac{dt}{t}.$$

Per tant, hem vist:

**Proposició 3.5.** $\Lambda(f,s) = \int_0^\infty (f(it) - a_0) t^s \frac{dt}{t}$.

Volem extendre $\Lambda(f,s)$ a tot el pla complex, però la integral tal i com la tenim té problemes de convergència prop de $t = 0$. Suposem, per simplicar, que $a_0 = 0$. Podem trencar la integral

$$\int_0^\infty f(it) t^s \frac{dt}{t} = \int_0^1 (\cdots) + \int_1^\infty (\cdots)$$

i, fent servir que $f(i/t) = i^k t^k f(it)$ trobem, fent el canvi $t \mapsto 1/t$,

$$\int_0^1 f(it) t^s \frac{dt}{t} = (-1)^{k/2} \int_1^\infty f(it) t^{k-s} \frac{dt}{t}.$$

Per tant,

$$\Lambda(f,s) = \int_1^\infty f(it)(t^s + (-1)^{k/2} t^{k-s}) \frac{dt}{t}.$$

Aquesta expressió convergeix per tot $s \in \mathbb{C}$. A més a més, obtenim l'equació funcional, que relaciona $s$ amb $k - s$:

$$\Lambda(f, k-s) = (-1)^{k/2} \Lambda(f,s).$$

*Observació* 3.3. Si $f \in M_k$ no és cuspidal, aleshores $\Lambda(f,s)$ no té una continuació holomorfa (només meromorfa), però l'equació funcional es segueix satisfent.

Hi ha un teorema recíproc, que no demostrarem.

**Teorema 3.3** (Weil)**.** *Sigui $L(\{a_n\},s) = \sum_{n=1}^{\infty} a_n n^{-s}$ una sèrie de Dirichlet associada a una successió $\{a_n\}_{n\geq 1}$ tal que $|a_n| = O(n^K)$ per $K$ suficientment gran. Suposem que la funció $\Lambda(\{a_n\},s)$ associada tingui continuació analítica a tot $s \in \mathbb{C}$, fitada en conjunts $\{\sigma_1 \leq \Re(s) \leq \sigma_2\}$ i que tingui una equació funcional com l'anterior. Aleshores la funció $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ és una forma cuspidal de pes $k$.*

### 3.3.2 Funció-L de les sèries d'Eisenstein

Sigui $k \geq 4$ un enter, i considerem la sèrie d'Eisenstein $E_k = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$.

**Proposició 3.6.** *Per a tot $p$ primer i tot $k \geq 4$ es té*

$$T_p(E_k) = (1 + p^{k-1}) E_k.$$

*Demostració.* Ho comprovem coeficient a coeficient. Si $p \nmid n$, hem de comprovar que

$$\sigma_{k-1}(pn) = (1 + p^{k-1})\sigma_{k-1}(n).$$

Per altra banda, si $n = p^e m$ amb $p \nmid m$ i $e \geq 1$, hem de veure que

$$\sigma_{k-1}(p^{e+1}m) + p^{k-1}\sigma_{k-1}(p^{e-1}m) = (1 + p^{k-1})\sigma_{k-1}(p^e m).$$

La primera equació es comprova fàcilment, i la segona es fa per inducció en $e$. □

Podem ara calcular ara la seva sèrie de Dirichlet:

$$\begin{aligned}\sum_{n=1}^{\infty} \sigma_{k-1}(n) n^{-s} &= \sum_{a,d\geq 1} \frac{a^{k-1}}{a^s d^s} \\ &= \left(\sum_{d\geq 1} d^{-s}\right)\left(\sum_{a\geq 1} a^{k-s-1}\right) \\ &= \zeta(s)\zeta(s-k+1).\end{aligned}$$

De manera alternativa, podem veure que l'invers del terme $p$-èssim del producte d'Euler és

$$\begin{aligned}1 - \sigma_{k-1}(p)p^{-s} + p^{k-1-2s} &= 1 - p^{-s} - p^{k-1-s} + p^{k-1-2s} \\ &= (1 - p^{-s})(1 - p^{k-1-s}),\end{aligned}$$

que coincideix amb el producte dels inversos dels factors d'Euler de $\zeta(s)\zeta(s-k+1)$. Resumint, obtenim la factorització

$$L(E_k, s) = \zeta(s)\zeta(s-k+1).$$

## 3.4 El producte de Petersson

Per estudiar més a fons els espais $S_k$, els hem de dotar de més estructura que la d'espai vectorial complex. Podem definir un producte escalar hermític, de la següent manera: donades $f, g \in S_k$, considerem

$$\phi_{f,g} = f(z)\overline{g(z)}y^k.$$

Si $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, podem veure fàcilment que $\phi_{f,g}(\gamma z) = \phi_{f,g}(z)$. Per tant, és una funció ben definida a $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. Podem doncs considerar la integral

$$\langle f, g\rangle = \frac{3}{\pi}\int_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}} f(z)\overline{g(z)}y^{k-2}dxdy,$$

ja que $\frac{dxdy}{y^2}$ és una mesura $\mathrm{SL}_2(\mathbb{Z})$-invariant a $\mathbb{H}$. Respecte aquesta mesura, el domini fonamental de $\mathrm{SL}_2(\mathbb{Z})$ té volum $\frac{\pi}{3}$, i per això escollim la normalització anterior.

**Proposició 3.7.** *El producte $\langle\cdot,\cdot\rangle$ és hermític i definit positiu. És a dir: 1. $\langle a_1 f_1 + a_2 f_2, g\rangle = a_1\langle f_1, g\rangle + a_2\langle f_2, g\rangle$, #. $\langle g, f\rangle = \overline{\langle f, g\rangle}$, i #. $\langle f, f\rangle \geq 0$, amb igualtat només si $f = 0$.*

*A més, per a tot $n \geq 1$, tenim*

$$\langle T_n f, g\rangle = \langle f, T_n g\rangle.$$

Com a conclusió, els operadors de Hecke $T_n$ formen una família d'operadors normals respecte el producte de Petersson. Per tant, $S_k$ conté una base ortogonal de formes pròpies per **tots** els operadors de Hecke simultàniament. Es diu que $S_k$ satisfà "multiplicitat-1": donat una col · lecció de valors propis $\{\lambda_n\}_{n\geq 1}$, hi ha com a molt una forma cuspidal pròpia $f \in S_k$ tal que $T_n(f) = \lambda_n f$. A més, pel teorema de Cayley-Hamilton tenim que els valors propis dels operadors de Hecke són nombres algebraics reals!

## 3.5 Formes modulars amb nivell

Fins ara hem considerat formes modulars que es transformen bé pel grup modular $\mathrm{PSL}_2(\mathbb{Z})$. És natural generalitzar la definició a altres subgrups de $\mathrm{PSL}_2(\mathbb{R})$ que actuin bé (de manera discreta) a $\mathbb{H}$ Una família important la formen els coneguts com a *grups de Hecke*, indexada per enters $N \geq 1$:

$$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq \mathrm{SL}_2(\mathbb{Z}),$$

definits com

$$\Gamma(N) = \{\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) : \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1\end{smallmatrix}\right) \pmod N\},$$
$$\Gamma_1(N) = \{\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) : \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1\end{smallmatrix}\right) \pmod N\},$$
$$\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) : \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & * \\ 0 & *\end{smallmatrix}\right) \pmod N\}.$$

La definició de formes modulars de nivell $\Gamma$ (on $\Gamma$ és un d'aquests grups) és bastant natural:

**Definició 3.1.** Una funció holomorfa $f\colon \mathbb{H} \longrightarrow \mathbb{C}$ és una forma modular de pes $k$ i nivell $\Gamma$ si:

1. $f(\gamma z) = (cz+d)^k f(z)$, per a tot $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$,
2. $(cz+d)^{-k} f(\gamma z)$ és holomorfa a l'infinit, per a tot $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

*Observació* 3.4. Fixem-nos que la definició demana que $f(\gamma z)$ sigui holomorfa a l'infinit per a tota $\gamma$ de $\mathrm{SL}_2(\mathbb{Z})$. Quan $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ aquesta condició només l'hem de comprovar per $f(z)$, però ara cal imposar més condicions.

Es té un anàleg per la fórmula de la valència, valid per tots aquests grups. Si escrivim $M_k(\Gamma)$ (resp. $S_k(\Gamma)$) per les formes modulars (resp. cuspidals) de pes $k$ i nivell $\Gamma$, es demostra de manera semblant que aquests espais són de dimensió finita. També es té una teoria d'operadors de Hecke i de producte de Petersson.

## 3.6 Corbes el · líptiques i modularitat

En aquesta secció enunciarem una versió del famós teorema de modularitat, que va jugar un paper central a la demostració de l'Últim teorema de Fermat.

Una corba el · líptica es pot pensar com una equació del tipus

$$E\colon \quad y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}, \Delta = -16(4a^3 - 27b^2) \neq 0.$$

Hem d'entendre aquesta equació com la part afí d'una corba dins el pla projectiu, així que hi ha un punt de més, $\mathcal{O} = (0:1:0)$, amb les coordenades $x = X/Z$, $y = Y/Z$.

Quan reduïm els coeficients mòdul $p$, obtenim una corba definida sobre $\mathbb{F}_p$. A les corbes sobre cossos finits se'ls pot associar una funció "zeta":

$$Z_p(E,T) = \exp\left(\sum_{m=1}^{\infty} \frac{\#E(\mathbb{F}_{p^m})}{m} T^m\right).$$

Resulta que, al ser $E$ una corba el · líptica, es té

$$\prod_p Z_p(E, p^{-s}) = \frac{\zeta(s)\zeta(s-1)}{L(E,s)},$$

on

$$L(E,s) = \prod_p L_p(E,s)^{-1}, \quad L_p(E,s) = \begin{cases} 1 - a_p p^{-s} + p^{1-2s} & p \nmid \Delta, \\ 1 - a_p p^{-s} & p \parallel N, \end{cases}$$

on $a_p$ es defineix com $p + 1 - \#E(\mathbb{F}_p)$.

Als anys 70 del segle passat, Eichler i Shimura van demostrar el següent resultat profund:

**Teorema 3.4** (Eichler-Shimura)**.** *Sigui $f \in S_2(\Gamma_0(N))$ una forma modular pròpia de pes 2,nivell $N$ i coeficients $a_n \in \mathbb{Z}$. A més, suposem que $f$ és "nova", és a dir que no "ve" de cap grup $\Gamma_0(M)$ amb $M \mid N$. Aleshores existeix una corba el·líptica $E_f$ de conductor $N$ tal que*

$$L(E_f, s) = L(f, s).$$

El recíproc d'aquest teorema es coneixia com la conjectura de Shimura-Taniyama-Weil, i la seva demostració va dur Andrew Wiles a la portada del New York Times perquè als anys 90 del segle passat ja es sabia que un cas particular (quan el "conductor" d'$E$ és lliure de quadrats) implicava l'Últim Teorema de Fermat. El teorema complet va ser demostrat finalment el 2002.

**Teorema 3.5** (Wiles, Taylor-Wiles, Breuil-Conrad-Diamond-Taylor)**.** *Sigui $E$ una corba el·líptica definida sobre els racionals, i de conductor $N$. Aleshores existeix una forma pròpia cuspidal $f_E \in S_2(\Gamma_0(N))$ tal que, per a tot $p \nmid N$,*

$$a_p(f) = p + 1 - \#E(\mathbb{F}_p).$$

*De fet, es té que $L(E, s) = L(f_E, s)$.*

**Exemple 3.1.** Considerem la corba amb etiqueta LMFDB 11.$a$3, que té per equació

$$E\colon \quad y^2 + y = x^3 - x^2.$$

No és de la forma anterior, però s'hi pot posar amb un canvi de variables, que faria els coeficients més grans. Si comptem els punts de la corba per uns quants primers obtenim, si calculem per cada primer $a_p = p + 1 - \#E(\mathbb{F}_p)$:

| $p$ | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $a_p$ | $-2$ | $-1$ | 1 | $-2$ | 1 | 4 | $-2$ | 0 | $-1$ | 0 | 7 |

Per altra banda, tenim la forma modular $f(z) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2$, que té una expansió

$$\begin{aligned} f(z) = q&-2q^2-q^3+2q^4+q^5+2q^6-2q^7-2q^9-2q^{10}+q^{11}-2q^{12} \\ &+4q^{13}+4q^{14}-q^{15}-4q^{16}-2q^{17}+4q^{18}+2q^{20}+2q^{21}-2q^{22} \\ &-q^{23}-4q^{25}-8q^{26}+5q^{27}-4q^{28}+2q^{30}+7q^{31}+O(q^{32}) \end{aligned}$$

i podem veure que els coeficients coincideixen amb els obtinguts de la corba el·líptica.

## 3.7 La funció j de Klein

Definim la següent funció modular de pes 0:

$$j = E_2^3/\Delta.$$

Veiem que $j$ té un holomorfa a tot $\mathbb{H}$, perquè $\Delta$ no s'anul · la. A més, té un pol simple a l'infinit, provinent del zero simple de $\Delta$.

**Proposició 3.8.** *L'aplicació $z \mapsto j(z)$ identifica $\mathrm{PSL}_2(\mathbb{R})\backslash\mathbb{H}$ amb $\mathbb{C}$.*

*Demostració.* Com que $j$ és invariant per $G$, obtenim una funció ben definida $G\backslash\mathbb{H} \longrightarrow \mathbb{C}$. Hem de veure que, per a tot $\lambda\mathbb{C}$, existeix un únic $z \in G\backslash\mathbb{H}$ tal que $j(z) = \lambda$ o, el què és el mateix, que la funció $f_\lambda(z) = E_2(z)^3 - \lambda\Delta(z)$ té un únic zero mòdul $G$. Aplicant la fórmula de la valència a $f_\lambda$ (que té pes 12) veiem que hem de descomposar 1 de la forma $a + b/2 + c/3$ amb $a, b, c \geq 0$. Les úniques possibilitats són $(1, 0, 0)$, $(0, 2, 0)$, $(0, 0, 3)$, i per tant hi ha un únic zero de $f_\lambda$ a $G\backslash\mathbb{H}$. □

De fet, la funció $j$ dona lloc a totes les funcions modulars de pes zero:

**Proposició 3.9.** *Tota funció modular de pes zero és una funció racional en $j$.*

*Demostració.* Sigui $f$ una funció modular. Multiplicant-la per un polinomi en $j$, posem suposar que és holomorfa a $\mathbb{H}$. D'altra banda, com que $\Delta$ té un zero simple a l'infinit, podem multiplicar $f$ per $\Delta^n$ de manera que $g = \Delta^n f$ sigui holomorfa també a l'infinit. Aleshores $g$ és una forma modular de pes $12n$, que podem escriure com un polinomi (4,6)-homogeni en $E_4$ i $E_6$, de grau $12n$. Per linealitat, n'hi ha prou amb veure que $f = E_4^i E_6^j/\Delta^n$ és una funció racional en $j$. Observem però que, com que $4i + 6j = 12n$, tant $p = i/3$ com $q = j/2$ són enters i, per tant,

$$f = E_4^{3p} E_6^{2q}/\Delta^{p+q} = (\frac{E_4^3}{\Delta})^p (\frac{E_6^2}{\Delta})^q.$$

Però tant $E_4^3/\Delta$ com $E_6^2/\Delta$ són funcions racionals en $j$, i ja estem. □

*Observació* 3.5. A partir de les $q$-expansions de les sèries d'Eisenstein podem obtenir la de $j$:

$$j(z) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots$$

Els coeficients són tots enters, que a més satisfan $n \equiv 0 \pmod{p^i} \implies c(n) \equiv 0 \pmod{p^i}$ per $p = 2, 3, 5, 7, 11$ (per $p = 2, 3, 5$ la divisilitat de $c(n)$ és per $2^{3i+8}$, $3^{2i+3}$ i $5^{i+1}$, respectivament).

El següent teorema és sorprenent: ens diu que la funció transcendent $j(z)$ pren valors algebraics quan l'argument és quadràtic.

**Teorema 3.6.** *Si $\tau \in \mathbb{H}$ genera un cos quadràtic, aleshores $j(\tau)$ és algebraic.*

*Demostració.* Suposem que $A\tau^2 + B\tau + C = 0$, amb $A \neq 0$. Aleshores la matriu $M = \left(\begin{smallmatrix} B & C \\ -A & 0 \end{smallmatrix}\right)$ té determinant $N = AC$ i fixa $\tau$. El grup $\Gamma = \mathrm{SL}_2(\mathbb{Z}) \cap M^{-1}\,\mathrm{SL}_2(\mathbb{Z})M$ és d'índex finit a $\mathrm{SL}_2(\mathbb{Z})$, i tant $j(z)$ com $j(Nz)$ són formes modulars meromorfes pel grup $\Gamma$. Per tant, són algebraicament dependents: hi ha un polinomi $P(X,Y) \in \mathbb{C}[X,Y]$ tal que $P(j(z), j(Nz)) = 0$. Mirant la $q$-expansió de $j(z)$ i $j(Nz)$ es veu que $\mathbb{Q}[X,Y]$. Resulta aleshores que $j(\tau)$ és arrel del polinomi $P(X,X) \in \mathbb{Q}[X]$. □

Per exemple, es pot demostrar que $j(\frac{1+\sqrt{-163}}{2}) = (640320)^3$. D'aquí se'n dedueix la famosa "identitat"

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999250072597\ldots$$

De fet, la funció $j$ ens permet apropar-nos al somni de joventut de Kronecker. Kronecker i Weber van demostrar el 1884 el següent teorema:

**Teorema 3.7** (Kronecker-Weber)**.** *Sigui $H$ una extensió abeliana de $\mathbb{Q}$. Aleshores existeix $n \geq 1$ tal que $H \subseteq \mathbb{Q}(e^{2\pi i/n})$.*

Es van preguntar si les extensions abelianes d'altres cossos diferents de $\mathbb{Q}$ també es poden obtenir adjuntant valors "especials" d'alguna funció anàloga a l'exponencial. Doncs bé, tenim:

**Teorema 3.8** (Kronecker, Weber, Takagi, Hasse)**.** *Sigui $H$ una extensió abeliana d'un cos quadràtic imaginari $K$. Aleshores existeix un $n \geq 1$ i un $\tau$ quadràtic tal que*

$$H \subseteq K(e^{2\pi i/n}, j(\tau), j(n\tau)).$$

# 4 Quart dia

Avui veurem les formes modulars $p$-àdiques des del punt de vista de J.-P. Serre, i com ens permeten una construcció alternativa de la funció $p$-àdica de Kubota–Leopoldt.

Recordem les congruències de Clausen–von Staudt pels nombres de Bernoulli

**Teorema 4.1** (Clausen–von Staudt)**.** *Si $k \geq 2$ és parell, aleshores*

$$B_k + \sum_{p-1|k} \frac{1}{p} \in \mathbb{Z}.$$

La demostració és relativament elemental, i no la farem en aquestes notes. Una conseqüència fàcil és que

**Corol · lari 4.1.** *Per a tot primer $p$ es té*

$$k \equiv 0 \pmod{(p-1)p^\alpha} \implies \frac{k}{B_k} \equiv 0 \pmod{p^{\alpha+1}}.$$

*Demostració.* Com que $p-1$ divideix $k$, del teorema obtenim que $v_p(B_k) = -1$. Per tant,

$$v_p(\frac{k}{B_k}) = v_p(k) - v_p(B_k) \geq \alpha - (-1) = \alpha + 1.$$

□

Recordem les sèries d'Eisenstein $E_k$,

$$E_k(q) = 1 - \frac{2k}{Bk} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

El corol · lari anterior ens diu que, per a tot $r \in \mathbb{Z}$ i $\alpha \geq 0$, tenim $E_{r(p-1)p^\alpha} \equiv 1 \pmod{p^{\alpha+1}}$. En particular, $E_{p-1} \equiv 1 \pmod{p}$. Aquí, les congruències són de $q$-expansions, és a dir, estem dient que la sèrie $E_{p-1} - 1$ té tots els coeficients divisibles per $p$.

Escrivim $\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \ : \ v_p(x) \geq 0\}$ (s'anomena l'anell dels $p$-enters), i considerem els espais

$$M_k(\mathbb{Z}_{(p)}) = M_k \cap \mathbb{Z}_{(p)}[[q]],$$

és a dir el subanell format per les formes modulars de pes $k$ tals que els coeficients de la seva $q$-expansió són tots $p$-enters. Tenim una aplicació de reducció

$$\mathrm{red}\colon M_k(\mathbb{Z}_{(p)}) \longrightarrow \mathbb{F}_p[[q]], \quad f \mapsto \overline{f}.$$

La imatge d'aquesta aplicació l'anomenarem $M_k(\mathbb{F}_p)$. Fixem-nos que, com que $\bar{E}_{p-1} = 1$, tenim inclusions

$$M_k(\mathbb{F}_p) \subseteq M_{k+(p-1)}(\mathbb{F}_p) \subseteq \cdots \subseteq M_{k+t(p-1)}(\mathbb{F}_p) \cdots$$

i per tant té sentit considerar la unió de tots aquests anells. Per cada $i \in \mathbb{Z}/(p-1)\mathbb{Z}$, definim

$$M^i(\mathbb{F}_p) = \bigcup_{k \equiv i \pmod{p-1}} M_k(\mathbb{F}_p).$$

Finalment, també considerem $M(\mathbb{F}_p) \subseteq \mathbb{F}_p[[q]]$ com la suma de tots els $M_k(\mathbb{F}_p)$, i de manera anàloga considerem també $M(\mathbb{Z}_{(p)})$. El morfisme de reducció dona lloc a un morfisme d'anells $M(\mathbb{Z}_{(p)}) \longrightarrow M(\mathbb{F}_p)$. Fixem-nos que $E_{p-1} - 1 \in M(\mathbb{Z}_{(p)})$ és al nucli d'aquesta aplicació. Escrivim $A = E_{p-1}$, i recordem que escrivim $Q = E_4$ i $R = E_6$. Sabem que $A$ es pot escriure com un cert polinomi "homogeni" en $Q, R$, que denotarem com $A = A(Q, R)$.

**Teorema 4.2** (Swinnerton-Dyer)**.**

1. *Si $p \geq 5$, aleshores* $\ker \mathrm{red} = A - 1$. *Per tant,* $M(\mathbb{F}_p) \cong \mathbb{F}_p[X, Y]/(\bar{A}(X, Y) - 1)$. *A més,*

$$M(\mathbb{F}_p) = \bigoplus_{i \in \mathbb{Z}/(p-1)\mathbb{Z}} M^i(\mathbb{F}_p).$$

2. *Per $p = 2, 3$, tenim* $M(\mathbb{F}_p) = M^0(\mathbb{F}_p) = \mathbb{F}_p(\bar{\Delta})$.

**Teorema 4.3.** *Sigui $p \geq 3$, i siguin $f \in M_k(\mathbb{Z}_{(p)})$ i $f' \in M_{k'}(\mathbb{Z}_{(p)})$ dues formes modulars de pesos $k$ i $k'$ respectivament. Aleshores*

$$f \equiv f' \pmod{p^m} \implies k \equiv k' \pmod{(p-1)p^{m-1}}.$$

*Si $p = 2$, aleshores es té*

$$f \equiv f' \pmod{2^m} \implies k \equiv k' \pmod{2^{m-2}}.$$

Més endavant veurem la demostració d'aquests resultats. Però fixem-nos que en podem treure alguna conseqüència fàcil:

**Proposició 4.1** (Congruències de Kummer per a=1)**.** *Si $k \equiv k' \not\equiv 0 \pmod{p-1}$ aleshores* $\frac{B_k}{k} \equiv \frac{B_{k'}}{k'} \pmod{p}$.

*Demostració.* Sabem que $\sigma_{k-1}(n) \equiv \sigma_{k'-1}(n) \pmod{p}$ per a tot $n$. Les congruències de Clausen–von Staudt ens diuen que $G_k$ i $G_{k'}$ viuen a $M_k(\mathbb{Z}_{(p)})$. Per tant, la reducció $\bar{G}_k - \bar{G}_{k'}$ viu a $M^k(\mathbb{F}_p)$. Però els termes no-constants de la $q$-expansió s'anul · len tots, i per tant en deduim que

$$\frac{B_k}{k} - \frac{B_{k'}}{k'} \in M^k(\mathbb{F}_p).$$

Essent la diferència de dues constants, també viuen a $M^0(\mathbb{F}_p)$ i , per tant, com que $p-1 \nmid k$, el teorema de Swinnerton-Dyer ens diu que aquesta diferència és 0. □

## 4.1 Formes modulars p-àdiques

Considerem l'anell de les formes modulars amb coeficients racionals $M(\mathbb{Q})$. Podem definir-hi una valoració $p$-àdica (que indueix una norma) definint

$$v_p(f) = \inf_n v_p(a_n), \quad f(q) = \sum_{n\geq 0} a_n q^n.$$

Aquesta definició té sentit, perquè les formes modulars tenen denominadors fitats: són polinomis "homogenis" en $Q$ i $R$ a coeficients racionals, i $Q$ i $R$ tenen denominadors enters.

**Definició 4.1.** L'anell $M(\mathbb{Q}_p) \subseteq \mathbb{Q}_p[[q]]$ és la completació de $M(\mathbb{Q})$ respecte la norma induida per $v_p$. Més concretament, una $q$-expansió $f \in \mathbb{Q}_p[[q]]$ és de $M(\mathbb{Q}_p)$ si, i només si, existeix una successió de formes modulars $(f_m)_m \subseteq M(\mathbb{Q})$ tals que $\lim_m f_m = f$ (convergència uniforme).

Considerem ara $f = \lim_m f_m$ una forma modular $p$-àdica, i suposem que $f_m$ té pes $k_m$. Pel teorema de la secció anterior, la successió d'enters $\{k_m\}_m$ convergeix $p$-àdicament a un element $\kappa \in \mathfrak{X}$, on

$$\mathfrak{X} = \varprojlim_m \mathbb{Z}/(p-1)p^m\mathbb{Z} \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p.$$

Direm que $f$ té pes $\kappa$, i escriurem $M_\kappa(\mathbb{Q}_p)$ pel subespai de formes modulars $p$-àdiques de pes $\kappa$.

*Observació* 4.1. El conjunt $\mathfrak{X}$, que s'anomena "l'espai de pesos", el podem pensar com un espai de caràcters. Fixem-nos que $\mathbb{Z}_p^\times \cong \mu_{p-1} \times (1+p\mathbb{Z}_p)$ (on $\mu_{p-1}$ és el grup cíclic format per les arrels $(p-1)$-èssimes de la unitat), via $x \mapsto \omega(x)\langle x\rangle$. Els caràcters multiplicatius de $1+p\mathbb{Z}_p$ són tots de la forma $\alpha \mapsto \alpha^\kappa$, per $\kappa \in \mathbb{Z}_p$. Per tant, els caràcters de $\mathbb{Z}_p^\times$ són de la forma $(u,\alpha) \mapsto \chi_{(h,\kappa)}(u,\alpha) = (u^h, \alpha^\kappa)$. Així,

$$\mathfrak{X} = \mathrm{Hom}_{\mathrm{cont}}(\mathbb{Z}_p^\times, \mathbb{Z}_p^\times), \quad (h,\kappa) \mapsto \chi_{(h,\kappa)}.$$

El teorema de la secció anterior es pot formular en termes de formes modulars $p$-àdiques:

**Teorema 4.4.** *Siguin $f$ i $f'$ formes modulars p-àdiques de pesos $\kappa$ i $\kappa'$, respectivament. Suposem que $v_p(f-f') \geq v_p(f)+m$ per algun $m \geq 1$. Aleshores, si $p \geq 3$,*

$$\kappa \equiv \kappa' \pmod{(p-1)p^{m-1}}.$$

*(Per $p=2$ cal canviar l'exponent $m-1$ per $m-2$).*

## 4.2 El terme constant a partir dels altres termes

Per les sèries d'Eisenstein, l'únic terme "interessant" és el constant, ja que la resta de termes estan formats per funcions ben conegudes. El següent resultat ens permet deduir propietats del terme constant a partir de conèixer els termes d'ordre més alt.

**Proposició 4.2.**

1. *Sigui $f = \sum_n a_n q^n \in M_\kappa(\mathbb{Q}_p)$ una forma modular p-àdica de pes $\kappa \in \mathfrak{X}$. Si $\kappa \not\equiv 0 \pmod{(p-1)p^m}$ per algun $m \geq 0$, aleshores*

$$v_p(a_0)+m \geq \inf_{n\geq 1} v_p(a_n).$$

2. *Sigui $(f_m)_m \subseteq M(\mathbb{Q}_p)$ una successió de formes modulars p-adiques de pesos $\{\kappa_m\}_m$. Escrivim $f_m = \lim_n f_m^{(n)}$, on $f_m^{(n)} = \sum_n a_n^{(m)} q^n$. Suposem que $\lim_m a_n^{(m)} = a_n$ uniformement en $n$ i que $\lim \kappa_m = \kappa \neq 0$. Aleshores $\lim_m a_0^{(m)} = a_0$, i $f = \sum_n a_n q^n$ és una forma modular p-àdica de pes $\kappa$.*

*Demostració.* Per demostrar (1), observem primer que si $a_0 = 0$ aleshores ja estem. Si no, $a_0 \in M_0(\mathbb{Q}_p)$ i per tant tenim, per la proposició anterior, que

$$v_p(f-a_0) < v_p(f)+m+1.$$

Per tant,

$$v_p(a_0)+m \geq v_p(f)+m \geq \inf_{n\geq 1} v_p(a_n).$$

Per demostrar (2), prenem un $m$ prou gran tal que $\kappa \not\equiv 0 \pmod{(p-1)p^m}$. Aleshores podem trobar $t \in \mathbb{Z}$ tal que, per $i$ suficientment gran,

$$v_p(a_n^{(i)}) \geq t, \quad \forall n \geq 1.$$

L'apartat anterior ens dona doncs que $v_p(a_0^{(i)}) > t-m$ per a tot $i$ suficientment gran. Com que $p^{t-m}\mathbb{Z}_p$ és compacte, hi ha una subsuccessió de $(a_0^{(i)})_i$ convergint a $a_0$, i $f = \sum_{n\geq 0} a_n q^n \in M_\kappa(\mathbb{Q}_p)$. Si $a_0'$ fos el límit d'una altra subsuccessió, aleshores obtindríem una altra $f'$, i

$$f - f' = a_0 - a_0' \in M_\kappa(\mathbb{Q}_p) \cap M_0(\mathbb{Q}_p) = 0.$$

Per tant $(a_0^{(i)})_i$ convergeix a $a_0$. □

## 4.3 La funció zeta p-àdica

Recordem la modificació $p$-àdica de la funció de divisors

$$\sigma_k^*(n) = \sum_{d|n, p\nmid d} d^k = \sigma_k(n) - p^k\sigma_k(n/p),$$

on entenem que $\sigma_k(n/p) = 0$ si $p \nmid n$. Si $k \equiv k' \pmod{(p-1)p^{m-1}}$, aleshores

$$\sigma_k^*(n) \equiv \sigma_{k'}^*(n) \pmod{p^m}.$$

Sigui ara $(k_i)_i \subseteq \mathbb{Z}$ una successió d'enters amb $k_i \longrightarrow \kappa$ $p$-àdicament, i tals que $k_i \longrightarrow \infty$ en sentit arquimedià. Suposem que $\kappa$ és parell i diferent de zero. Aleshores $\sigma_{k_i}^*(n) \longrightarrow \sigma_\kappa^*(n)$ de manera uniforme en $n$. Obtenim de la proposició anterior que hi ha una forma modular $p$-àdica $G_\kappa^* = a_0 + \sum_{n\geq 1}\sigma_\kappa^*(n)q^n$, on

$$\zeta^*(1-k) := a_0 = \lim_{i\longrightarrow\infty} \frac{-B_{k_i}}{2k_i} = \frac{1}{2}\lim_{i\longrightarrow\infty}\zeta(1-k_i).$$

Obtenim així una funció $\zeta^*(\kappa)$, definida per elements senars $\kappa \in \mathfrak{X}\setminus\{1\}$. La segona part de la proposició anterior ens diu que $\zeta^*$ és contínua (perquè els coeficients $\kappa \mapsto \sigma_\kappa(n)$ ho són).

Suposem que $\kappa \in \mathbb{Z}_{\geq 2}$ és un enter. Aleshores podem calcular

$$\zeta^*(1-\kappa) = \lim_{i\longrightarrow\infty}\zeta(1-k_i) = \lim_{i\longrightarrow\infty}\prod_\ell \frac{1}{1-\ell^{k_i-1}} = \prod_{\ell\neq p}\frac{1}{1-\ell^{k-1}} = (1-p^{k-1})\zeta(1-k).$$

Com que $\zeta^*$ és contínua i interpola en un conjunt dens, ha de ser la funció de Kubota–Leopoldt que ja hem vist. És a dir, que obtenim (assumim $p \neq 2$ per simplicitat):

**Teorema 4.5.** *Si $p \neq 2$ i $(s,u) \in \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} \cong \mathfrak{X}$, tenim*

$$\zeta^*(s,u) = L_p(s\omega^{1-u}).$$

# Bibliografia

[1] Fred Diamond i Jerry Michael Shurman. *A first course in modular forms*. Vol. 228. Springer, 2005.

[2] Jean-Pierre Serre. *A course in arithmetic*. Vol. 7. Springer Science & Business Media, 2012.