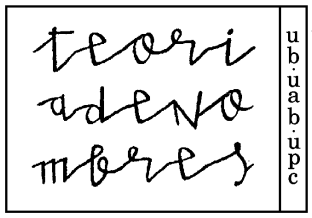
**NOTES DEL SEMINARI**




# MONOGRÀFIC SOBRE TREBALLS

# DE

# DON ZAGIER

**Barcelona, 2009**

# 18

# Notes del Seminari de Teoria de Nombres (UB-UAB-UPC)

# MONOGRÀFIC SOBRE TREBALLS DE

# DON ZAGIER

Edició a cura de

Pilar Bayer

Amb contribucions de

P. Bayer A. Cámara T. Crespo

A. Rio A. Travesa X. Xarles

P. Bayer

Facultat de Matemàtiques, UB
Gran Via de les Corts Catalanes, 585
E-08007 Barcelona
bayer@ub.edu



Classificació AMS
*Primària*: 11E25, 11F25, 11F37, 11G05, 11G20
*Secundària*: 11D25, 11F11, 11F33, 11F67, 11F72, 11M41, 11Y50

Barcelona, 2009
Amb suport parcial de

MTM 2006-04895, MRTN-CT-2006-035495
MTM 2006-11391
MTM 2006-15038-C02-01, 2005SGR 00443

ISBN: 978-84-934244-8-0

# Prefaci

Aquestes notes versen sobre les exposicions que, sota el títol *Monogràfic sobre treballs de Don Zagier*, foren presentades en l'edició 22 del Seminari de Teoria de Nombres (UB-UAB-UPC), celebrada a l'Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú, del 28 de gener a l'1 de febrer de 2008.

Zagier és un dels autors més originals, alhora que prolífics en idees, dels nostres dies, la qual cosa justifica amb escreix que el seminari dediqués un monogràfic a la seva obra. Qui llegeixi aquestes exposicions, però, s'adonarà que molts resultats fonamentals de la producció de Zagier no hi són reflectits. En la selecció dels temes, s'ha optat per presentar-ne de més nous enfront d'altres que, per la seva temàtica, podien ser-nos més familiars. Si, després de donar un cop d'ull a aquests escrits, sentiu la necessitat d'apropar-vos als treballs originals en què es basen, podrem dir que el monogràfic ha acomplert la seva funció.

Pilar Bayer

Barcelona, 22 de gener de 2009

# Índex

# Capítol 1

# Aperitiu: sumes de dos quadrats

A. Cámara

## Introducció

Pierre de Fermat fou un advocat francès que visqué al segle XVII i que tingué una gran afició per les matemàtiques. Aquesta afició fou prou gran com perquè habitualment hom acrediti Fermat com el més gran dels matemàtics *amateurs* de tots els temps.

L'anomenat teorema dels dos quadrats de Fermat afirma que un primer $p$ senar és igual a la suma de dos quadrats enters si, i només si, $p \equiv 1 \pmod 4$, i és un dels pocs resultats dels quals en coneixem una demostració feta pel propi Fermat.

La demostració donada per Fermat utilitza la tècnica del *descens infinit* (vegeu [2], capítol VI, paràgraf III, secció C). A part d'aquesta prova, més de cinquanta demostracions diferents d'aquest resultat clàssic han estat publicades al llarg del temps.

Segurament tota persona que hagi estudiat un primer curs d'iniciació a l'aritmètica s'haurà trobat aquest teorema. Les demostracions més freqüents acostumen a utilitzar o bé la factorialitat de l'anell $\mathbb{Z}[i]$ dels enters de Gauss, o bé el teorema d'aproximació dio-

fantina de Dirichlet. Tant en aquests dos casos com en la gran majoria de les proves conegudes, s'utilitza en algun punt el fet que si $p \equiv 1 \pmod 4$ aleshores $-1$ té arrel quadrada mòdul $p$.

La demostració de Zagier que exposem en aquest treball no utilitza aquest fet. Es tracta d'una simplificació d'una demostració donada per Roger Heath-Brown [1], basada en l'acció de grups sobre conjunts. La demostració de Heath-Brown, al seu torn, està inspirada en una demostració donada per Liouville [3].

## 1.1 Una demostració d'una sola frase

Don Zagier va publicar una nota [4], a l'*American Mathematical Monthly*, el febrer de 1990, que porta per títol:

*A One-Sentence Proof That Every Prime* $p \equiv 1 \pmod 4$ *Is a Sum of Two Squares.*

La demostració d'una sola frase de la qual parla Zagier és la següent:

*Com que la involució en el conjunt finit*

$$S = \{(x, y, z) \in \mathbb{N}^3; x^2 + 4yz = p\}$$

*definida per*

$$(1.1)\quad (x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & \text{si } x < y - z, \\ (2y - x, y, x - y + z) & \text{si } y - z < x < 2y, \\ (x - 2y, x - y + z, y) & \text{si } x > 2y; \end{cases}$$

*té un únic punt fix,* $\#S$ *és senar i la involució* $(x, y, z) \mapsto (x, z, y)$ *també té un punt fix.* $\square$

Només cal fer algunes comprovacions per completar la demostració, que Zagier deixa al lector.

D'entrada, $S$ és un conjunt finit ja que una terna $(x, y, z)$ de naturals que satisfaci $x^2 + 4yz = p$ no pot tenir cap component més gran que $p$.

En primer lloc, l'aplicació descrita per (1.1) està ben definida, perquè les desigualtats exposades no exclouen cap element de $S$: en

cas d'haver-hi una igualtat obtindríem immediatament divisors no trivials de $p$. En segon lloc, les imatges dels punts de $S$ són elements de $S$ perquè

$$(x+2z)^2+4z(y-x-z) = x^2+4xz+4z^4+4yz-4xz-4z^2 = p,$$
$$(2y-x)^2+4y(x-y+z) = 4y^2-4xy+x^2+4xy-4y^2+4yz = p,$$
$$(x-2y)^2+4(x-y+z)y = x^2-4xy+4y^2+4xy-4y^2+4yz = p.$$

Comprovem que (1.1) defineix una involució:

Si $x < y-z$, aleshores se satisfà que $x+2z > 2z$ i, per tant,

$$(x+2z, z, y-x-z) \mapsto (x+2z-2z, x+2z-z+y-x-z, z) = (x, y, z).$$

Si estem en la situació en què $y-z < x < 2y$, aleshores $y-(x-y+z) < 2y-x < 2y$ i, per tant,

$$(2y-x, y, x-y+z) \mapsto (2y-2y+x, y, 2y-x-y+x-y+z) = (x, y, z).$$

En el tercer cas, en què $x > 2y$, tenim que $x-2y < x-y+z-y$, de forma que

$$(x-2y, x-y+z, y) \mapsto (x-2y+2y, y, x-y+z-x+2y-y) = (x, y, z).$$

Suposem ara que $(x, y, z)$ és un punt fix per la involució (1.1). Es comprova ràpidament que només pot ser

$$(x, y, z) = (2y-x, y, x-y+z), \tag{1.2}$$

ja que les altres possibilitats porten a contradicció. Obtenim que $x = y = 1$ fent servir (1.2), per la primera igualtat, i fent servir que $p = x^2+4yz = x(x+4z)$, per la segona igualtat. Per tant, l'únic punt fix per (1.1) és $(1, 1, k)$, on $k$ és tal que $p = 4k+1$. Notem que aquí utilitzem que $p \equiv 1 \pmod 4$.

Si tenim una involució sobre un conjunt finit amb un únic punt fix, aleshores podem deduir que el cardinal del conjunt és senar, ja que la involució emparella cada punt amb la seva imatge. Un cop sabem que $\#S$ és senar, pel mateix motiu deduïm que tota involució sobre $S$ té, com a mínim, un punt fix. Finalment, un punt fix de la involució $(x, y, z) \mapsto (x, z, y)$ ens proporciona una manera d'escriure $p$ com a suma de dos quadrats.

## 1.2 Observacions

Cal dir que la demostració que acabem de veure no és constructiva: en cap cas obtenim un mètode per expressar $p$ com a suma de dos quadrats. En aquest sentit, succeeix un fenòmen similar al que succeeix en l'anàlisi matemàtica o en la topologia amb els teoremes de punt fix.

El principi bàsic que hem usat és que el cardinal d'un conjunt finit i el del seu conjunt de punts fixos per una involució són de la mateixa paritat. En aquest sentit, estem usant un anàleg discret d'un resultat de topologia: la característica d'Euler d'un espai topològic i la del seu subespai de punts fixos per una involució contínua són de la mateixa paritat.

# Bibliografia

[1] Heath-Brown, D. R.: Fermat's two-squares theorem, *Invariant*, 1984. p. 3-5.

[2] Mahoney, M. S.: *The Mathematical Career of Pierre de Fermat 1601-1665*. 2a ed. Princeton University Press: Princeton, 1994

[3] Uspensky, J. V.; Heaslet, M. A.: *Elementary Number Theory*, McGraw-Hill: New York, 1939.

[4] Zagier, D.: A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ Is a Sum of Two Squares. *Amer. Math. Monthly*, 97 (1990), no. 2, p. 144.

A. Cámara

School of Mathematical Sciences

University of Nottingham

University Park, Nottingham

NG7 2RD, United Kingdom

**alberto.camara.math@gmail.com**

# Capítol 2

# Construcció de corbes planes amb molts punts

A. Rio

## Introducció

Quan tractem amb corbes afins, en contrast amb les corbes completes, podem diferenciar entre punts enters i punts racionals. El teorema de Siegel (1929) sobre punts enters estableix que en una corba afí de gènere positiu, definida sobre un cos de nombres $K$, hi pot haver únicament un nombre finit de punts $K-$enters. Aquest teorema pot considerar-se el primer resultat important sobre equacions diofantines que depèn únicament del gènere, i no de cap forma algebraica especial de les equacions.

Per al cas de corbes el·líptiques definides sobre el cos dels nombres racionals, Zagier aborda a [17] la qüestió de cercar eficientment punts enters grans d'una corba donada i la de construir corbes el·líptiques que tinguin algun punt enter gran. Dóna tres respostes a la primera qüestió, totes de complexitat $O(\log\log B)$ per obtenir solucions enteres amb $|x|, |y| < B$.

Amb finançament parcial de MTM2006-15038-C02-01 i 2005SGR 00443.

## 2.1 Corbes sobre cossos de nombres

Per a gènere $g > 1$, el teorema de Siegel va ser finalment superat pel resultat de Faltings, conegut prèviament com a conjectura de Mordell:

**2.1.1 Teorema. (Faltings, 1983)** *Una corba no singular de gènere $g \geq 2$ definida sobre un cos de nombres $K$ té només un nombre finit de punts $K-$racionals.*

En plantejar-se la variació d'aquest nombre de punts racionals quan es consideren famílies de corbes, Caporaso, Harris i Mazur (cf. [4] i [5]) arriben a la formulació de les dues conjectures següents:

**2.1.2 Conjectura. (d'uniformitat)** *Siguin $K$ un cos de nombres i $g \geq 2$ un enter. Existeix un nombre $B(K, g)$ tal que per a tota corba no singular $X$ de gènere $g$ definida sobre $K$ se satisfà que*

$$|X(K)| < B(K, g).$$

**2.1.3 Conjectura. (d'afitació universal)** *Sigui $g \geq 2$ un enter. Existeix un nombre $N(g)$ tal que per a qualsevol cos de nombres $K$ existeix només un nombre finit (de classes de $K-$isomorfisme) de corbes de gènere $g$ definides sobre $K$ amb més de $N(g)$ punts $K-$racionals.*

En el segon dels treballs citats anteriorment, els autors proven que aquestes conjectures d'uniformitat són conseqüència de les conjectures diofantines de Lang, conjectures que provenen d'un intent de generalitzar el teorema de Faltings a varietats de dimensió superior:

**2.1.4 Conjectura. (de Lang feble)** *Sigui $X$ una varietat de tipus general definida sobre $K$. El conjunt dels punts $K-$racionals de $X$ no és Zariski-dens a $X$.*

**2.1.5 Conjectura. (de Lang forta)** *Sigui $X$ una varietat de tipus general definida sobre $K$. Existeix una subvarietat tancada pròpia $Y$ de $X$ tal que per a qualsevol cos de nombres $L \supseteq K$ tots els punts $L-$racionals de $X$ estan continguts en $Y$ amb excepció d'un nombre finit.*

Així doncs, a [5] es demostren els dos teoremes següents:

**Teorema d'afitació uniforme.**

Conjectura de Lang feble ⇒ Conjectura d'uniformitat.

**Teorema d'afitació genèrica universal.**

Conjectura de Lang forta ⇒ Conjectura d'afitació universal.

En aquest punt resulta oportú esmentar també el resultat obtingut per Abramovich i Pacelli (cf. [1] i [9]), que demostren que si $B(K, g)$ existeix, aleshores només depèn del grau $[K : \mathbb{Q}]$.

Amb l'objectiu de promoure la discussió al voltant d'aquestes qüestions, Caporaso, Harris i Mazur publiquen a [4] una recopilació de resultats relatius a $B(\mathbb{Q}, g)$ i $N(g)$. El punt de partida són resultats per a gèneres petits: Brumer ha obtingut $B(\mathbb{Q}, 2) \geq 144$ i $B(\mathbb{Q}, 3) \geq 72$, i Elkies $B(\mathbb{Q}, 4) \geq 126$ i $B(\mathbb{Q}, 3) \geq 132$. A continuació descriuen un mètode per obtenir corbes no singulars amb un bon nombre de punts racionals, amb el qual proven les fites inferiors següents:

**2.1.6 Teorema. (Caporaso, Harris, Mazur)**

$$B(\mathbb{Q}, g) \geq \begin{cases} 6g + 38 & si\ g \equiv 7 \mod 8 \\ 6g + 26 & si\ g \equiv 1 \mod 8 \\ 6g + 30 & si\ g \equiv 5 \mod 6 \\ 6g + 18 & si\ g \equiv 1 \mod 6 \\ 6g + 12 & si\ g \equiv 2 \mod 6 \\ 6g + 14 & si\ g\ senar \\ 6g + 10 & en\ general \end{cases}$$

La seccions següents es dediquen a demostrar que $N(3) \geq 72$ i $N(2) \geq 128$, usant en ambdós casos la superfície quàrtica de $\mathbb{P}^3$ definida en coordenades homogènies per l'equació $X(X^3 - Y^3) = Z(Z^3 - W^3)$. En la part final del treball es cerquen estimacions per a $N(g)$ amb $g$ arbitràriament gran. Usant en principi superfícies de $\mathbb{P}^3$ de la forma $F(X, Y) - F(Z, W) = 0$, amb $F(X, Y)$ polinomi homogeni, obtenen la taula següent:

| $g$ | 6 | 10 | 15 | 21 | 28 | 36 | 45 | 55 | 153 | 171 |
|---|---|---|---|---|---|---|---|---|---|---|
| $N(g) \geq$ | 145 | 180 | 217 | 256 | 261 | 320 | 781 | 864 | 1501 | 1600 |

Amb una segona tècnica arriben a un resultat general: $N(g) \geq 8g + 14$ per a tot $g$. Cal observar que aquesta fitació no millora els valors obtinguts a la taula anterior. A la darrera secció del treball es descriu un mètode de Mestre de construcció explícita de corbes hiperel·líptiques de gènere $g$ que exhibeix directament $8g + 12$ punts $K-$racionals, essent $K$ un cos de nombres qualsevol. Per al cas $K = \mathbb{Q}$, la fita $B(\mathbb{Q}, g) \geq 8g+12$ millora els resultats del teorema anterior, excepte per a un nombre finit de valors de $g$.

El treball [3] de Caporaso es presenta com una actualització de l'article que acabem de descriure, amb una recopilació de rècords vigents en aquell moment i una descripció del mètode de Brumer, que millora el resultat anterior amb la fitació $N(g) \geq 16(g + 1)$ per a tot $g$.

Pel que fa als rècords, en gènere 2 la corba

$$y^2 = 278271081\, x^2(x^2 - 9)^2 - 229833600\, (x^2 - 1)^2$$

obtinguda per Kulesz, permet afirmar que $B(\mathbb{Q}, 2) \geq 588$. Val a dir que aquesta corba té com a mínim 12 automorfismes, i que si restringim el problema a corbes sense automorfismes extra, aleshores tenim l'exemple de Stahlke

$$\begin{aligned} y^2 \;\; = \;\; & 9703225\, x^6 - 9394700\, x^5 + 152200\, x^4 + 1124745\, x^3 \\ & +119526\, x^2 - 42957\, x + 2061 \end{aligned}$$

que té almenys 306 punts racionals. En gènere 3, Keller i Kulesz obtenen $B(\mathbb{Q}, 3) \geq 112$ amb

$$y^2 = 48397950000\, (x^2 + 1)^4 - 939127350499\, (x^3 - x)^2,$$

una corba que té almenys 16 automorfismes. Quant a les fites inferiors per a $N(g)$, Elkies troba les que figuren en aquesta taula:

| $g$ | 3 | 4 | 5 | 9 | 10 | 45 |
|---|---|---|---|---|---|---|
| $N(g) \geq$ | 100 | 126 | 146 | 180 | 192 | 781 |

Les fites de Brumer s'obtenen amb corbes hiperel·líptiques que tenen un grup d'automorfismes gran. Considerem la família de corbes hiperel·líptiques de gènere $g$

$$C_{a,b} : \; y^2 = a\, (x^{g+1} + 1)^2 - b\, x^{g+1},$$

on $a, b \neq 0$ són del cos base, que suposem que és $\mathbb{Q}$. A més de la involució hiperel·líptica, s'observen dos tipus d'automorfismes: la involució

$$(x, y) \longrightarrow \left(\frac{1}{x}, \frac{y}{x^{g+1}}\right)$$

i les $g + 1$ *rotacions*

$$(x, y) \longrightarrow \left(\zeta^i x, y\right),$$

on $\zeta$ és una arrel primitiva $(g + 1)-$èsima de la unitat, i per consegüent $|\operatorname{Aut}(C_{a,b})| \geq 4(g + 1)$. A més, tots aquests automorfismes estan definits sobre l'extensió ciclotòmica $\mathbb{Q}(\zeta)$. Si trobem $m$ punts $\mathbb{Q}-$racionals, automàticament l'òrbita pel grup d'automorfismes ens proporcionarà $4m(g + 1)$ punts $\mathbb{Q}(\zeta)-$racionals.

D'altra banda, si $(x_i, y_i)$ són $m-$punts racionals, podem considerar les equacions $y_i^2 = a(x_i^{g+1} + 1)^2 + b\, x_i$ com un sistema lineal en $a, b$ i l'únic que cal és imposar que sigui compatible. Amb $m = 3$ s'obté una cònica del pla projectiu sobre $\mathbb{Q}(x_1, x_2, x_3)$, que tè un punt racional evident: el que correspon a la solució $b = 0$. Per tant, en té una infinitud, i una tria genèrica de nombres racionals $x_1, x_2, x_3$ proporciona infinits parells $(a, b)$ tal que $C_{a,b}$ té 3 punts racionals. En el cas $m = 4$, la condició rang $= 2$ dóna lloc a dues equacions en $y_1, y_2, y_3, y_4$ que s'interpreten com a quàdriques de l'espai projectiu sobre $\mathbb{Q}(x_1, x_2, x_3)$. La corba intersecció és una corba el·líptica que té alguns punts racionals obvis: $y_i = \pm(x_i^{g+1} + 1)$. Les addicions d'aquests punts proporcionen nous punts racionals, que donen lloc a corbes $C_{a,b}$ amb almenys 4 punts racionals. Finalment es prova que aquest mètode produeix una infinitat de corbes no isomorfes sobre $\overline{\mathbb{Q}}$ i així s'obté la fita esmentada anteriorment: $N(g) \geq 16(g + 1)$.

## 2.2 Punts ciclotòmics

El problema de trobar *punts ciclotòmics*, és a dir, punts de coordenades arrels de la unitat, d'una corba $f(x, y) = 0$ és tractat per Beukers i Smyth a [2]. Si $f(x, y) = \sum a_{ij} x^i y^j \in \mathbb{C}[x, y]$, el seu suport es defineix com $\operatorname{supp}(f) = \{(i, j) \in \mathbb{Z}^2 \mid a_{ij} \neq 0\}$. L'envolupant convexa de $\operatorname{supp}(f)$ s'anomena *politop de Newton* de $f$. La seva àrea la denotem $V(f)$.

El cos de coeficients de $f$ és l'extensió de $\mathbb{Q}$ generada per totes les raons $a_{ij}/a_{i'j'}$ entre coeficients diferents de zero. Denotem $\mathbb{Q}^{ab}$ l'extensió abeliana maximal de $\mathbb{Q}$.

Direm que $f$ és un polinomi *recíproc* si $f(x,y) = \lambda x^a y^b \bar{f}(1/x, 1/y)$ per a alguna constant no nul·la $\lambda$ i enters $a, b \geq 0$, on $\bar{f}$ denota el conjugat complex.

**2.2.1 Teorema. (Beukers, Smyth)** *Amb les notacions prèvies:*

- *$f$ té com a molt $22V(f)$ punts ciclotòmics o en té infinits.*
- *Si en té infinits, ha de tenir un factor de la forma $x^a y^b - \omega$, amb $\omega$ arrel de la unitat i $a, b$ enters no tots dos zero.*
- *Si cap factor absolutament irreductible de $f$ és recíproc, $f$ té com a molt $4V(f)$ punts ciclotòmics.*
- *Si cap dels cossos de coeficients dels factors absolutament irreductibles de $f$ és un subcòs de $\mathbb{Q}^{ab}$, aleshores $f$ té com a molt $2V(f)$ punts ciclotòmics.*
- *En els enunciats anteriors, la constant 22 no pot rebaixar-se per sota de 16 i les constants 4 i 2 són òptimes.*

En particular, si $f(x,y)$ és un polinomi de grau $m$, aleshores el seu politop de Newton està contingut en un triangle d'àrea $m^2/2$; i si tots els seus factors absolutament irreductibles són no recíprocs, tindrem la fita $2m^2$ per al nombre de punts ciclotòmics. Per exemple, si $\varphi_m(x) = 1 + x + x^2 + \cdots + x^m$ i

$$f(x,y) = \varphi_m(x) + \varphi_m(y) - 1$$

aleshores les arrels comunes de $f(x,y)$ i $f^*(x,y) = x^m y^m f(1/x, 1/y)$ són:

$$\begin{array}{ll} (\omega_{m+1}^i, \omega_m^j) & i = 1, \ldots, m;\ j = 1, \ldots, m-1 \\ (\omega_m^i, \omega_{m+1}^j) & i = 1, \ldots, m-1;\ j = 1, \ldots, m \\ (\omega_{2m+1}^i, \omega_{2m+1}^{-i}) & i = 1, \ldots, 2m \end{array}$$

on en cada cas $\omega_r$ indica una arrel primitiva $r-$èsima de la unitat. Això prova que tots els factors absolutament irreductibles són no recíprocs i dóna una família de $2m^2$ punts ciclotòmics de la corba $f(x,y) = 0$.

## 2.3 Corbes sobre cossos finits

Per a una corba completa no singular absolutament irreductible de gènere $g$ definida sobre un cos finit de $q$ elements, el resultat arquetípic sobre el nombre $N$ dels seus punts racionals prové de la hipòtesi de Riemann, que estableix $|N - (q+1)| \leq 2gq^{1/2}$. Hasse [7] va provar aquest resultat per a corbes el·líptiques i Weil [16] va donar-ne la primera demostració general. La fita que se n'obté,

$$N \leq q + 1 + 2g\sqrt{q}\,,$$

es coneix com a fita de Weil o de Hasse-Weil. Aquesta fita és la millor possible en el sentit que si fixem el gènere $g$ i deixem variar el cos base, llavors $2g$ no pot substituir-se per cap constant menor. Però, d'altra banda hi ha diversos casos en què la fita de Hasse-Weil pot millorar-se. Per començar, cal tenir en compta la remarca de Serre:

$$N \leq q + 1 + g\,[2\sqrt{q}],$$

una fita que alguns autors anomenen de Hasse-Weil-Serre o de Weil-Serre. Segons [6], aquesta va ser considerada *essencialment optimal* fins que el 1981 Manin i Ihara van trobar fites que són significativament millors quan $g$ és gran comparat amb $q$.

Entre 1981 i 1983, Ihara, Drinfeld-Vladut i Serre (cf. [7]) van investigar fites per a $A(q) = \limsup |C(\mathbb{F}_q)|/g(C)$, on el límit es pren sobre totes les corbes completes no singulars absolutament irreductibles definides sobre el cos finit $\mathbb{F}_q$, obtenint que $0 \leq A(q) \leq \sqrt{q} - 1$ per a tot $q$ i que si $q$ és un quadrat, llavors s'assoleix el valor màxim $\sqrt{q}-1$. Si $g > \frac{1}{2}(q - \sqrt{q}\,)$, aleshores es pot millorar la fita de Weil.

Stöhr i Voloch es plantejen al treball [15] abordar de manera general aquesta qüestió de millora de la fita proporcionada per la hipòtesi de Riemann.

**2.3.1 Teorema. (Stöhr, Voloch)** *Sigui $\mathbb{F}_q$ un cos finit de $q$ elements i de característica $p > 2$.*

(1) *Sigui $f \in \mathbb{F}_q[x, y]$ un polinomi absolutament irreductible de grau $d$, amb $1 < d < p$. Aleshores el nombre $N$ de solucions de*

*l'equació* $f(x,y)=0$ *a* $\mathbb{F}_q^2$ *satisfà que*

$$N \leq \frac{1}{2}\, d\,(d+q-1)\,.$$

(2) *Sigui* $C$ *una corba algebraica projectiva no singular de gènere* $g \geq 3$*, definida sobre* $\mathbb{F}_q$*. Sigui* $N$ *el nombre dels seus punts racionals. Si* $p \geq 2g-1$*, aleshores*

$$N \leq 2q + g\,(g-1)\,.$$

(3) *Sigui* $C$ *una corba algebraica projectiva no singular de gènere* $g \geq 3$*, definida sobre* $\mathbb{F}_q$*. Sigui* $N$ *el nombre dels seus punts racionals. Si* $g \leq \frac{1}{2}\,(p+3)$ *i* $C$ *no és hiperel·líptica, aleshores*

$$N \leq \frac{2g-3}{g-2}\, q + g\,(g-2)\,.$$

Per a una corba de no-hiperel·líptica de gènere 3, la immersió canònica és una immersió plana de grau 4. Per a $g=3$ i $p \geq 5$, els dos primers apartats del teorema anterior proporcionen la mateixa fita i exemples de Serre mostren que aquesta és òptima per a $q = 5, 7, 11, 13, 17, 19$ i 25. Per a $q = 23$ i corbes de gènere 3, Serre prova que el màxim nombre de punts racionals és 48.

## 2.4 Corbes planes amb molts punts enters

En aquesta secció descrivim el treball [10] de Rodríguez-Villegas i Voloch en què es basa el treball posterior amb D. Zagier que dóna títol a aquest capítol. En ell defineixen una família de polinomis de grau creixent i amb moltes solucions enteres.

Segons descriuen els autors, aquests polinomis van aparèixer en el decurs d'una altra recerca: l'estudi de l'equació de Picard-Fuchs d'un període d'una diferencial holomorfa de la família de varietats donada per $(x_1 + \cdots + x_N)(x_1^{-1} + \cdots + x_N^{-1}) = \lambda$, amb $\lambda \in \mathbb{C}$. L'equació de Picard-Fuchs es relaciona amb l'equació de $J_0^N$, on $J_0$ indica la funció de Bessel estàndard, i aquesta equació pot obtenir-se recursivament. Com a coeficients de major ordre de la recurrència apareixen

els polinomis $T_k$:

$$(2.1)\qquad \begin{cases} T_0 &= 1\,, \\ T_1 &= y\,, \\ T_{k+1} &= y\,T_k + k\,(x+k-1)\,T_{k-1}\,, \qquad \forall k \geq 1. \end{cases}$$

Per exemple, tenim

$$\begin{aligned} T_2 &= x + y^2\,, \\ T_3 &= 3yx + y^3 + 2y\,, \\ T_4 &= 3x^2 + 6y^2x + 6x + y^4 + 8y^2\,, \\ T_5 &= 15yx^2 + 10y^3x + 50yx + y^5 + 20y^3 + 24y\,. \end{aligned}$$

De la recurrència que defineix la família $T_k(x,y)$ es dedueix que

$$T_k(x,-y) = (-1)^k\,T_k(x,y)\,, \quad \text{per a tot } k \geq 0.$$

Si considerem els subíndexs parells, aleshores la família de polinomis $P_d \in \mathbb{Z}[x,y]$ queda definida per la igualtat següent:

$$(2.2)\qquad T_{2d}(x,y) = P_d(-x,y^2).$$

Els primers polinomis de la família $P_d$ són

$$\begin{aligned} P_1 &= y - x\,, \\ P_2 &= 3x^2 - 6yx - 6x + y^2 + 8y \\ &= 3(y-x)(y-x+2) - 2y(y-1)\,, \\ P_3 &= -15x^3 + 45yx^2 + 90x^2 - 15y^2x - 210yx - 120x + y^3 \\ &\quad +40y^2 + 184y. \end{aligned}$$

La recurrència (2.1) mostra que $T_k$ és un polinomi de grau $k$, amb coeficients enters no negatius i tal que el coeficient de $y^k$ és 1. D'altra banda, si per a un polinomi $H \in \mathbb{Z}[x,y]$ es defineix $\|H\|_1$ com la suma dels valors absoluts dels seus coeficients, aleshores

$$\|T_k\|_1 = T_k(1,1).$$

Si posem $c_k = T_k(1,1)$, de la recurrència (2.1) obtenim ara

$$c_0 = 1, \quad c_1 = 1, \quad c_{k+1} = c_k + k^2 c_{k-1},$$

d'on es dedueix que

$$\|T_k\|_1 = k!.$$

Tot això comporta per als polinomis $P_d$ les propietats recollides a la proposició següent.

**2.4.1 Proposició.** *Sigui $P_d(x,y)$ el polinomi definit per* (2.2).

(1) *$P_d$ té grau $d$.*

(2) *Els coeficients de $P_d(-x,y)$ són enters $\geq 0$ relativament primers.*

(3) $\|P_d\|_1 = (2d)!$.

El resultat principal del treball [10] consisteix d'una banda en provar la irreductibilitat dels polinomis $P_d$ i d'altra banda en trobar famílies de zeros de coordenades enteres.

**2.4.2 Teorema.** *Sigui $P_d(x,y)$ el polinomi definit a partir de* (2.2).

(1) *$P_d$ és absolutament irreductible*

(2) *$P_d$ s'anul·la en els $d^2+2d+3$ punts enters de les quatre famílies següents:*

(I) $(n,0),(n,2^2),(n,4^2)\ldots(n,n^2)$, *amb* $0 \leq n \leq 2d-1$ *i $n$ parell,*

(II) $(n,1^2),(n,3^2),(n,5^2)\ldots(n,n^2)$, *amb* $0 \leq n \leq 2d-1$ *i $n$ senar,*

(III) $(4d,2^2),(4d,6^2),(4d,10^2)\ldots(4d,4(2d-1)^2)$,

(IV) $(8d+1,3^2)$, $(2d-4,-6d+4)$, $(2d-3,-2d+1)$.

Els autors també presenten dades experimentals sobre altres punts de les corbes $P_d = 0$, per a $3 \leq d \leq 12$. Per exemple, l'equació $P_3 = 0$ defineix una corba el·líptica d'equació de Weierstrass minimal

$$y^2 + xy + y = x^3 - x^2 - 62705x + 5793697$$

i conductor $N = 2\cdot 3^2\cdot 5^2\cdot 11\cdot 6007 = 29734650$. Una cerca exhaustiva de punts amb $|x| < 1000$ proporciona un total de 25 punts $(x,y)$ de coordenades enteres, 7 d'ells no provinents de les famílies descrites anteriorment:

$$(-14,-56),(-4,-20),(-1,-9),(1,1),(16,144),(67,25),(345,1225).$$

## 2.5 Corbes planes amb molts punts

En l'article comentat a la secció anterior, trobem la remarca següent:

> Don Zagier suggested to us a simpler way to study the properties of the polynomials $T_k$. One may define the polynomials by means of the generating series
>
> $$H(\lambda) = (1-\lambda)^x(1+\lambda)^y = \sum_{k\geq 0} T_k(-x-y,-x+y)\,\frac{\lambda^k}{k!}$$
>
> which satisfies the differential equation
>
> $$\frac{dH/d\lambda}{H} = -\frac{x}{(1-\lambda)} + \frac{y}{1+\lambda}$$
>
> giving the recursion of the $T_k$. As an example of this approach, $P_d$ clearly vanishes at the points (I) and (II) of the theorem, since $H$ is a polynomial of degree $x+y$ for $x, y \in \mathbb{N}$.

Aquesta remarca sembla ser l'origen de l'article objecte d'estudi en el capítol: *Constructions of plane curves with many points* de F. Rodríguez Villegas, J.F. Voloch i D. Zagier, publicat a la revista *Acta Arithmetica* l'any 2001 ([11]). En aquest treball s'investiguen corbes planes amb molts punts sobre $\mathbb{Q}$, cossos finits i cossos ciclotòmics. Concretament, es troben:

- polinomis a $\mathbb{Q}[x,y]$ de grau arbitràriament gran amb molts zeros racionals;
- polinomis amb el màxim nombre possible de zeros ciclotòmics i de zeros sobre cossos finits;
- valors de $d$ per als quals els polinomis $P_d$ tenen més zeros que els de les quatre famílies descrites anteriorment.

### 2.5.1 Variacions d'una construcció de Schaefer

Si considerem un polinomi $f(x) \in \mathbb{Z}[x]$ amb arrels enteres diferents $\alpha_1, \ldots, \alpha_n$, aleshores el polinomi $f(x) + \lambda f(y)$ és genèricament irreductible, té grau $d = n$ i $n^2 = d^2$ arrels enteres a $(x,y) = (\alpha_i, \alpha_j)$.

Per millorar això considerem $\lambda = -1$ i treiem el factor lineal $x-y$. El polinomi

$$\frac{f(x)-f(y)}{x-y}$$

té grau $d = n-1$ i $n^2-n = d^2+d$ arrels enteres. Si suposem, a més, que $f$ és parell, aleshores podem considerar el polinomi

$$\frac{f(x)-f(y)}{x^2-y^2},$$

que té grau $d = n-2$ i $n^2-2n = d^2+2d$ arrels enteres. Observem que aquest nombre de zeros és proper al nombre $d^2+2d+3$ trobat abans per als polinomis $P_d$.

Una generalització d'aquesta construcció s'obté en substituir la condició $f$ *parell* per la condició $f$ *invariant per la subtitució* $x \to \zeta x$, amb $\zeta$ arrel $k-$èsima de la unitat, i passant a treballar sobre un cos $K$ que contingui les arrels $k-$èsimes de la unitat. Posem

$$f(x) = \prod (x^k - \alpha_i^k)\,,$$

on $\alpha_1, \ldots, \alpha_r \in K^*$ són elements tals que les seves potències $k-$èsimes són diferents. Aleshores,

$$P(x,y) = \frac{f(x)-f(y)}{x^k-y^k}$$

té grau $d = k(r-1)$ i $k^2r(r-1) = d^2+kd$ arrels a $(\zeta\alpha_i, \zeta'\alpha_j)$, on $\zeta,\ \zeta'$ són arrels $k-$èsimes de la unitat i $i \neq j$.

Suposem ara que $K = \mathbb{F}_p$ i que $k$ és un divisor de $p-1$, tal que $k < \dfrac{p-1}{2}$. Si prenem $r = \dfrac{p-1}{k} - 1$, la construcció anterior dóna lloc a un polinomi de grau $d = k(r-1) = p-1-2k$ amb

$$k^2r(r-1) = d^2+kd = \frac{1}{2}d(d+p-1)$$

arrels a $\mathbb{F}_p$. És a dir, s'assoleix la fita de Stöhr i Voloch. Val a dir que encara falta considerar la irreductibilitat absoluta del polinomi $P(x,y)$, cosa que es farà tot seguit per al cas

$$f(x) = \frac{x^{(m+2)k}-1}{x^k-1}. \tag{2.3}$$

### 2.5.2 Els polinomis $G_m$

Per a cada $m \geq 1$, considerem el polinomi homogeni de grau $m$

$$G_m(x,y,z) = \sum_{\substack{i,j,k \geq 0 \\ i+j+k=m}} x^i y^j z^k.$$

Si fem ús de la fórmula de sumació d'una sèrie geomètrica, obtenim

$$G_m(x,y,z) = \frac{1}{x-y}\left(\frac{x^{m+2}-z^{m+2}}{x-z} - \frac{y^{m+2}-z^{m+2}}{y-z}\right). \tag{2.4}$$

En particular,

$$\begin{aligned} G_m(x^k,y^k,1) &= \frac{1}{x^k-y^k}\left(\frac{x^{(m+2)k}-1}{x^k-1} - \frac{y^{(m+2)k}-1}{y^k-1}\right) \\ &= \frac{f(x)-f(y)}{x^k-y^k} = P(x,y), \end{aligned}$$

amb $f(x)$ com a (2.3).

**2.5.1 Teorema.** *Per a cada $m \geq 1$, la corba projectiva plana de grau $m$ definida per*

$$G_m(x,y,z) = 0$$

*és no singular en característica zero o característica $p \nmid (m+1)(m+2)$ i té zeros a $2m^2$ punts de coordenades $x,y,z$ arrels de la unitat.*

Fent ús de l'expressió (2.4) trobem de manera immediata els $2m^2$ punts ciclotòmics següents:

- $m^2+m = (m+1)^2-(m+1)$ arrels $(\zeta,\zeta',1)$, amb $\zeta,\zeta'$ arrels $m+2$ de la unitat, $\zeta \neq \zeta'$ i $\zeta,\zeta' \neq 1$;

- $m^2-m$ arrels $(\zeta,\zeta',1)$, amb $\zeta,\zeta'$ arrels $m+1$ de la unitat, $\zeta \neq \zeta'$ i $\zeta,\zeta' \neq 1$.

Cal remarcar que $2m^2$ és el màxim nombre de punts ciclotòmics per a un polinomi no recíproc de grau $m$ a coeficients en $\mathbb{Q}$, i que un polinomi de $\mathbb{Q}[x,y]$ no singular i que no s'anul·la a l'origen és no recíproc.

Estudiem ara la no singularitat de les corbes d'equació $G_m = 0$. Per fer-ho, primer reescrivim la igualtat (2.4) de la manera següent:

$$G_m = \frac{D_{m+2}}{D_2}\,, \quad \text{amb} \quad D_n(x,y,z) = \left| \begin{pmatrix} 1 & 1 & 1 \\ z & x & y \\ z^n & x^n & y^n \end{pmatrix} \right|,$$

considerem la $m$ fixada i simplifiquem la notació amb $G = G_m(x,y,1)$ i $D = D_{m+2}(x,y,1)$. El polinomi $D_2(x,y,1)$ és $(x-1)(y-1)(y-x)$. Deixant de banda els punts tals que $D_2 = 0$, que són fàcils d'estudiar per separat, tenim que

$$\left.\begin{aligned} G &= 0 \\ \frac{\partial G}{\partial y} &= 0 \end{aligned}\right\} \quad \Leftrightarrow \quad \left.\begin{aligned} D &= 0 \\ \frac{\partial D}{\partial y} &= 0 \end{aligned}\right\}.$$

Atès que $D = \det(v(1), v(x), v(y))$, amb $v(x) = (1, x, x^{m+2})^t$, tenim

$$\frac{\partial D}{\partial y} = \det(v(1), v(x), v'(y))$$

i $v'(y) = (0, 1, (m+2)y^{m+1})^t$. Si $x \neq 1$, els vectors $v(1)$ i $v(x)$ no són mai proporcionals i el rang de la matriu $(v(1), v(x), v(y), v'(y))$ és $\geq 2$. L'anul·lació dels dos determinants $D$ i $\partial D/\partial y$ vol dir que aquest rang és 2. I llavors també $\det(v(1), v(y), v'(y)) = 0$. Per tant, l'anul·lació simultània de $G$ i $\partial G/\partial y$ vé donada per les arrels del polinomi

$$\begin{aligned} g(y) &= \det(v(1), v(y), v'(y)) = \left| \begin{pmatrix} 1 & 1 & 0 \\ 1 & y & 1 \\ 1 & y^{m+2} & (m+2)y^{m+1} \end{pmatrix} \right| \\ &= \sum_{j=0}^{m} (j+1)y^j = G(y,y). \end{aligned}$$

Explícitament, cada zero de $G = \partial G/\partial y = 0$ té com a segona coordenada una arrel de $g$ i cada arrel $y_i$ de $g$ és segona coordenada

d'exactament $m-1$ zeros de $G = \partial G/\partial y = 0$, essent les abscisses les arrels del polinomi

$$\frac{x^{m+2} - (m+2)y_i^{m+1}x + (m+1)y_i^{m+2}}{(x-1)(x-y_i)^2}\,.$$

Amb això hem provat que

$$\mathrm{Res}_x(G, \partial G/\partial y) = g(y)^{m-1},$$

on $\mathrm{Res}_x$ indica la resultant com a polinomis en $x$. En principi, la igualtat és a menys de constants, però observant els termes de grau màxim es comprova que aquesta constant val 1.

Per tal de trobar les singularitats hem de buscar arrels comunes de $G$, $\partial G/\partial y$ i $\partial G/\partial x$; és a dir, de $g(y)$ i $\partial G/\partial x$. Raonant de manera anàloga a l'anterior, trobem que $v(1)$, $v(x)$, $v'(x)$, $v(y)$ i $v'(y)$ han d'estar al mateix espai de dimensió 2, que té complement ortognal generat per $w(y) = ((m+1)y^{m+2}, -(m+2)y^{m+1}, 1)$. Per simetria, aquest complement ortogonal també ha d'estar generat per $w(x)$, de manera que ambdós vectors han d'ésser iguals. En restar-los, tenim

$$(m+1)(x^{m+2} - y^{m+2}) = 0 \quad \text{i} \quad (m+2)(x^{m+1} - y^{m+1}) = 0,$$

la qual cosa és impossible si $m+1$ i $m+2$ són $\neq 0$.

### 2.5.3 Construcció de corbes amb molts punts sobre $\mathbb{Q}$

**2.5.2 Teorema.** *Per a tot $d$ enter divisible per 6 existeixen infinits polinomis $F_d(x,y) \in \mathbb{Q}[x,y]$, de grau $d$, que s'expressen de la forma*

$$F_d(x,y) = \frac{f(h(x)) - f(h(y))}{h(x) - h(y)}$$

*i tals que la corba $F_d(x,y) = 0$ és no singular i té almenys $d^2 + 6d$ punts racionals*

Considerem $h(x) = x^6 - 2x^4 + x^2$ i

$$C(\lambda) = \frac{(\,\lambda(\lambda-1)(\lambda+1)(2\lambda-1)(\lambda-2))^2}{(\lambda^2-\lambda+1)^6}\,.$$

Aleshores,

$$h(x) - C(\lambda) = \prod_{\alpha \in S(\lambda)} (x - \alpha)$$

amb

$$S(\lambda) = \left\{ \pm\frac{\lambda^2 - 1}{\lambda^2 - \lambda + 1}, \pm\frac{\lambda^2 - 2\lambda}{\lambda^2 - \lambda + 1}, \pm\frac{2\lambda - 1}{\lambda^2 - \lambda + 1} \right\}.$$

Prenem $\lambda_1, \ldots, \lambda_n$ nombres racionals tals que els valors $C(\lambda_i)$ siguin tots diferents i definim

$$f(X) = \prod_i (X - C(\lambda_i)) \quad \text{i} \quad F(x,y) = \frac{f(h(x)) - f(h(y))}{h(x) - h(y)}\,.$$

El polinomi $F$ té grau $d = 6n - 6$ i s'anul·la en tots els punts $(x, y)$, amb

$$x \in S(\lambda_i)\,, \quad y \in S(\lambda_j) \qquad (1 \le i \ne j \le n)\,,$$

és a dir, en $36n(n-1) = d^2 + 6d$ punts racionals.

La corba definida per $F(x, y) = 0$ és no singular llevat d'un nombre finit de $(\lambda_1, \ldots, \lambda_n) \in \mathbb{Q}^n$ atès que el conjunt de $n-$ples complexes per a les quals la corba és no singular formen un obert per la topologia de Zariski.

### 2.5.4 Els polinomis $P_d$

Ara, els mateixos polinomis $P_d$ de la secció (2.5) s'estudien des d'un altre punt de vista. Recordem que $P_d(-X, Y^2) = T_{2d}(X, Y)$ i que els polinomis $T_k$ s'havien definit mitjançant una recurrència. Doncs bé, ara considerem que aquests polinomis provenen de la funció generatriu

$$H(t) := (1-t)^r (1+t)^s = \sum_{k \ge 0} T_k(-r-s, -r+s)\frac{t^k}{k!}\,.$$

Si fem l'expansió dels binomis, obtenim

$$T_k(-r-s, -r+s) = k! \sum_{n=0}^{k} (-1)^n \binom{r}{n}\binom{s}{k-n}\,.$$

Aquesta interpretació permetrà mostrar 10 construccions de famílies de solucions enteres de $P_d(x, y) = 0$, que resumim en la taula següent:

| Família | Condició | ♯ Zeros |
|---|---|---|
| I | $r, s$ petits | $d^2+d$ |
| II | $x = 4d$ | $d$ |
| III | $y = 9$ | 1 |
| IV | $x = 2d-3$ o $2d-4$ | 2 |
| V | $x = 4d-3$ | [odd] |
| VI | $r = 2$ | $2\epsilon_{16d+1}$ |
| VII | $r = 3, 4, 5$ | $2\epsilon_{48d+1}$ |
| VIII | $x = 2d+2$ | $2\epsilon_{2d+2}$ |
| IX | $x = 2d+3$ | $2\epsilon_{6d+7}$ |
| X | $x = 2d-5$ o $2d-6$ | |

on [odd]= 1 si $d$ és senar i 0 altrament, i $\epsilon_n = 1$ si $n$ és un quadrat i 0 altrament.

L'objectiu final serà cercar polinomis $P_d$ que satisfacin simultàniament les condicions de les famílies I-VII, i que tinguin, per tant, com a mínim $d^2+2d+8$ arrels enteres.

**Família I.** Si $r$ i $s$ són enters no negatius, aleshores el polinomi $H(t) = (1-t)^r(1+t)^s$ té grau $r+s$. Per tant, en el seu desenvolupament el coeficient de $t^k$ és zero per a tot $k > r+s$, és a dir,

$$T_k(-r-s, -r+s) = 0, \qquad \text{si } k > r+s.$$

Posem $r+s = n$ i $-r+s = m$. Les condicions $r, s$ enters $\geq 0$ i $r+s < 2d$ es tradueixen en $0 \leq m \leq n \leq 2d-1$, i $n \equiv m \mod 2$. Així obtenim $d(d+1)$ zeros enters $(x, y) = (n, m^2)$ de $P_d(x, y) = 0$.

**Família II.** Si $r$ i $s$ són enters senars positius i posem $r+s = 2k$, aleshores

$$H\left(\frac{1}{t}\right) = \left(1-\frac{1}{t}\right)^r \left(1+\frac{1}{t}\right)^s = \frac{(t-1)^r(t+1)^s}{t^{r+s}} = -H(t)t^{-2d}.$$

D'aquesta antisimetria deduïm que el coeficient central ha d'ésser zero: $H_k(-2k, -r+s) = 0$. Si agafem $s = 2d+n$ i $r = 2d-n$, amb $0 < n < 2d$ i $n$ senar, aleshores $H_{2d}(-4d, 2n) = 0$ i obtenim els $d$ zeros enters $(x, y) = (4d, 4n^2)$ de $P_d(x, y) = 0$.

**Família III.** Si prenem $r = 4d-1$ i $s = 4d+2$, aleshores podem escriure $H(t) = (1+t)^3(1-t^2)^{4d-1}$ i veure que el coeficient de $t^{2d}$ serà igual a

$$(-1)^d \left[ \binom{4d-1}{d} - 3\binom{4d-1}{d-1} \right],$$

que val zero. Per tant, $H_{2d}(-8d+1, 3) = 0$ i així tenim un zero més: $P_d(8d-1, 9) = 0$.

**Família IV.** La derivada logarítmica de $H(t) = 1-t)^r(1+t)^s$ és

$$\frac{H'(t)}{H(t)} = -\frac{r}{1-t} + \frac{s}{1+t},$$

d'on s'obté la fórmula recursiva

$$T_{k+1} = Y\,T_k + k\,(X+k-1)\,T_{k-1}$$

per als polinomis $T_k(X, Y)$. Per a la subfamília $P_d(x, y) = T_{2d}(-x, \sqrt{y}\,)$, això dóna lloc a la recurrència

$$\begin{aligned} P_{d+1} \;=\; & [y-(4d+1)x+8d^2]P_d \\ & -[2d(2d-1)(x-2d+1)(x-2d+2)]P_{d-1}. \end{aligned}$$

Els dos coeficients s'anul·len si $x = 2d-1$ o $2d-2$ i $y = (4d+1)x - 8d^2$ i tenim dos zeros més amb coordenades enteres.

**Família V.** Ara considerem $r = d-1$ i $s = 3d-2$, de manera que $H(t) = (1-t^2)^{d-1}(1+t)^{2d-1}$ i el coeficient de $t^{2d}$ és

$$\sum_{n=1}^{d-1} (-1)^{d-n} \binom{d-1}{d-n} \binom{2d-1}{2n},$$

que s'anul·la si $d$ és senar, perquè els termes per a $n$ i $d-n$ es cancel·len. Així doncs, $H_{2d}(-4d+3, 2d-1) = 0$ si $d$ és senar i, per tant, en aquest cas $P_d(4d-3, (2d-1)^2) = 0$.

**Família VI.** Si $r = 2$, llavors

$$H(t) = (1+t)^{s+2} - 4t(1+t)^s$$

i

$$T_k(-s-2,s-2) = k!\left[\tbinom{s+2}{k} - 4\tbinom{s}{k-1}\right] \\ \frac{1}{4}s(s-1)\dots(s-k+3)[(2s-k+3)^2-(8k+1)]\,.$$

Els zeros $s = 0, 1, \dots, k-3$ ja s'han obtingut en la família I, però si $k = 2d$ i $16d+1 = a^2$ per a algun enter $a$, aleshores trobem un nou punt enter

$$x = \left(\frac{a+1}{2}\right), \quad y = \left(\frac{a+5}{2}\right)^2\left(\frac{a-3}{2}\right)^2$$

de $P_d(x,y) = 0$. De fet, obtenim dos punts, atès que podem canviar $a$ per $-a$.

**Família VII.** Si fixem $r$, i prenem $k \geq r$, aleshores podem reescriure

$$T_k(-r-s,-r+s) = \binom{k}{r}^{-1}\binom{s}{k-r}Q_r(k,s)\,,$$

on

$$Q_r(k,s) = r!\sum_{n=0}^{r}(-1)^n\binom{k}{n}\binom{r+s-k}{r-n} \in \mathbb{Z}[k,s]$$

és un polinomi de grau $r$. Si $r$ és senar, posem $\tilde{Q}_r(k,s) = Q_r(k,s)/(r+s-2k)$, per eliminar zeros que ja han estat considerats a la família II.

Fixant $r = 3$, trobem

$$4\tilde{Q}_3(k,s) = (2s-4k+3)^2 - (24k+1).$$

Prenent $k = 2d$, si $24k+1 = 48d+1$ és un quadrat, aleshores hi ha dos zeros enters de $P_d(x,y) = 0$.

Per a $r = 4, 5$, tenim

$$\begin{aligned} Q_4(k,t+2k-4) &= 3(2k-t^2+t-1)^2 - (2t^4-2t^2+3), \\ 3\tilde{Q}_5(k,t-2k-5) &= 5(6k-t^2+3t-5)^2 - (2t^4-10t^2+53) \end{aligned}$$

i només un nombre finit de valors $d$ que proporcionin solucions $(k = 2d, s)$, atès que corresponen als punts enters d'una corba el·líptica definida sobre $\mathbb{Q}$ i de rang positiu.

**Família VIII.** Una altra família de zeros enters de $P_d(x,y)=0$, per a valors especials de $d$, ve donada per

$$d=2c^2-1, \quad x=y=4c^2\,,$$

amb $c$ enter positiu. Això correspon a $r=2c^2-c$ i $s=2c^2+c$. El coeficient de $t^{2d}=t^{4c^2-2}=t^{r+s-2}$ en $H(t)=(1-t)^r(1+t)^s$ és, a menys de signe,

$$\frac{s(s-1)}{2}-rs+\frac{r(r-1)}{2}$$

i s'anul·la en aquest cas.

**Família IX.** Ens fixem ara en el coeficient de $t^{r+s-3}$ en $H(t)$ que, novament llevat del signe, és

$$\frac{r(r-1)(r-2)}{6}+\frac{rs(s-r)}{2}-\frac{s(s-1)(s-2)}{6},$$

és a dir,

$$\frac{1}{6}(r-s)\left(r^2-2sr-3r+s^2-3s+2\right)$$

Si $s=2d-r-3$ i $6d+7$ és un quadrat, la forma quadràtica $r^2-2sr-3r+s^2-3s+2$ s'anul·la per a

$$r=\frac{1}{2}\left(3+2d\pm\sqrt{6d+7}\right).$$

Així doncs, si $6d+7$ és un quadrat, aleshores $P_d(2d+3,6d+7)$.

**Família X.** Si fixem $x=2d-2\nu-1$ o $x=2d-2\nu-2$, amb $\nu\geq 1$, aleshores $k=2d>x=r+s$ i estem en les condicions de la família I, on ja hem trobat $d-\nu$ solucions de l'equació de grau $d$ determinada per $P_d(x,\cdot)=0$. El cas $\nu=1$ correspon a la família IV, mentre que si prenem $\nu=2$, per trobar les arrels que falten estarem considerant les possibles arrels d'un polinomi de grau 2. En concret, tenim

$$\begin{aligned} 6d^2-9d+4=e^2 \quad &\Rightarrow \quad P_d(2d-5,5-6d\pm 2e)=0\\ 10d^2-15d+9=f^2 \quad &\Rightarrow \quad P_d(2d-6,10-10d\pm 2f)=0 \end{aligned}$$

En cada cas, les condicions sobre $d$ són equacions de tipus Pell amb infinites solucions. Les primeres són $d=4,33,320,3161,\ldots$ i $d=8,33,144,637,\ldots$, respectivament.

Un cop fet aquest estudi exhaustiu podem demostrar el resultat següent.

**2.5.3 Teorema.** *Per a infinits valors de d, l'equació $P_d(x, y) = 0$, de grau d, té almenys $d^2 + 2d + 8$ solucions enteres.*

Per a un valor de $d$ senar, les famílies I-V proporcionen un total de $d^2 + 2d + 4$ solucions enteres de $P_d(x, y) = 0$. Per trobar valors de $d$ per als quals tinguem 4 solucions addicionals, considerarem les condicions de les famílies $VI$ i $VII$ simultàniament:

$$\begin{cases} 16d + 1 &= a^2\,, \\ 48d + 1 &= b^2. \end{cases}$$

Aquestes condicions donen lloc a l'equació de Pell

$$3a^2 - b^2 = 2\,,$$

les solucions positives de la qual venen donades per

$$b + a\sqrt{3} = (1 + \sqrt{3})(2 + \sqrt{3})^n\,, \qquad \text{amb } n \geq 0. \tag{2.5}$$

Aleshores,

$$d = \frac{a^2 - 1}{16} = \frac{b^2 - 1}{48} \tag{2.6}$$

és enter si $n \equiv 0, 3 \mod 4$ i senar si

$$n \equiv 3, 4 \mod 8.$$

En resum, si anem donant valors $n \equiv 3, 4 \mod 8$, calculem el valor de $a$ (o de $b$) usant (2.5) i llavors la fórmula (2.6) anirà proporcionant els valors de $d$ per als quals l'equació $P_d(x, y) = 0$ té $d^2 + 2d + 8$ solucions enteres.

Per exemple,

- $n = 3 \Rightarrow a = 41,\ b = 71 \Rightarrow d = 105\,,$
- $n = 4 \Rightarrow a = 153,\ b = 265 \Rightarrow d = 1463\,,$
- $n = 11 \Rightarrow a = 1542841,\ b = 2672279 \Rightarrow d = 148772396955\,,$

- $n = 12 \Rightarrow a = 5757961,\ b = 9973081 \Rightarrow d = 2072132179845\,,$
- $n = 19 \Rightarrow a = 58063278153 \Rightarrow d = 210709016867040443213\,.$

Aquest conjunt de valors enters $d$, tot i no ser gaire dens, és certament infinit, i tenim doncs demostrat el teorema anterior.

Per acabar, cal remarcar que altres combinacions de parells de condicions també donen lloc a equacions de Pell amb infinites solucions, però únicament $d^2 + 2d + 7$ solucions enteres. I no es possible combinar tres condicions, per exemple VI, VII i VIII, perquè això correspondria a trobar punts enters en una corba el·líptica definida sobre $\mathbb{Q}$ i en tindríem únicament un nombre finit.

# Bibliografia


[1] Abramovich, D.: Uniformité des points rationnels des courbes algébriques sur les extensions quadratiques et cubiques. *C. R. Acad. Sci. Paris Sér. I Math.* 321 (1995), 755–758.

[2] Beukers, F.; Smyth, C. J.: Cyclotomic points on curves. *Number Theory for the Millenium I (Proceedings of the Millennial Conference on Number Theory, Urbana May 21-26, 2000).* A. K. Peters, 2002, 67–85.

[3] Caporaso, L.: Counting rational points on algebraic curves. *Rend. Sem. Mat. Univ. Pol. Torino* 53 (1995), no. 3, 223–229.

[4] Caporaso, L.; Harris, J.; Mazur, B.: How many rational points can a curve have? *Proceedings of the Texel Conference.* Progress in Mathematics, Vol. 129. Birkhäuser, 1995, 13–31.

[5] Caporaso, L.; Harris, J.; Mazur, B.: Uniformity of Rational Points. *J. Amer. Math. Soc.* 10 (1997), no. 1, 1–35.

[6] Elkies, N. D.; Howe, E. W.; Kresch, A.; Poonen, B.; Wetherell, J. L.; Zieve, M. E.: Curves of every genus with many points, II: Asymptotically good families. *Duke Math. J.* 122 (2004), no. 2, 399–422.

[7] Hasse, H.: Zur Theorie der abstraktenelliptischen Funktionenkorper. *J. Reine Angew. Math.* 175 (1936), 55–62, 69–88, 193–208.

[8] Lang, S.: Hyperbolic and Diophantine analysis. *Bull. Amer. Math. Soc.* 14 (1986), no. 2, 159–205.

[9] Pacelli, P. L.: Uniform boundedness for rational points. *Duke Math. J.* 88 (1997), no. 1, 77–102.

[10] Rodríguez-Villlegas, F.; Voloch, J.: On certain plane curves with many integral points. *Experiment. Math.* 8 (1999), 57–62.

[11] Rodríguez-Villlegas, F.; Voloch, J. ; Zagier, D.: Constructions of plane curves with many points. *Acta Arith.* 99 (2001), no. 1, 85–96.

[12] Serre, J.-P.: Nombre des points des courbes algebrique sur $\mathbb{F}_q$. *Sem. Theor. Nombres Bordeaux* 22 (1983).

[13] Serre, J.-P.: Sur le nombre des points rationnels d'une courbe algebrique sur un corps fini. *C. R. Acad Sci. Paris Ser. I Math.* 296 (1983), 397–402.

[14] Siegel, C. L.: Über einige Anwendungen diophantischer Approximationen. *Abh. Preuss. Akad. Wiss., Phys.-Math. Kl.* 1 (1929), 1–41. (Gesammelte Abhandlungen I, 209–266, Springer Verlag 1966.)

[15] Stöhr, K. O.; Voloch, J. F.: Weierstrass points and curves over finite fields. *Proc. London Math. Soc.* 52 (1986), 1–19.

[16] Weil, A.: Courbes algébriques et variétés abéliennes. Sur les courbes algébriques et les varietés qui s'en deduisent. Hermann, 1948. (Segona edició combinada: Hermann, 1971.)

[17] Zagier, D.: Large integral points on elliptic curves. *Math. Comp.* 48 (1987), 425 – 436.

A. Rio

Departament de Matemàtica Aplicada II

Universitat Politècnica de Catalunya

Edifici Omega. Jordi Girona, 1–3

E-08034, Barcelona

**ana.rio@upc.edu**

# Capítol 3

# Formes modulars i operadors diferencials

T. Crespo

## Introducció

La derivada d'una forma modular no és una forma modular. Tanmateix existeixen operadors diferencials que envien formes modulars a formes modulars. R. A. Rankin en donà una descripció general a [4]. L'objectiu de l'article [6] és estudiar aquests operadors de Rankin tant des del punt de vista diferencial com algebraic.

## 3.1 Preliminars

Recordem la definició de forma modular (cf. [5]). Considerem l'acció de $\mathrm{SL}(2,\mathbb{R})$ sobre $\widetilde{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ donada per

$$\gamma(z) = \frac{az+b}{cz+d}, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R}), z \in \widetilde{\mathbb{C}}.$$

Amb finançament parcial de MTM2006-04895 i MRTN-CT-2006-035495.

Es fàcil comprovar la fòrmula

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

que dóna que el semiplà superior de Poincaré

$$\mathbb{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$$

és estable per l'acció de $\mathrm{SL}(2,\mathbb{R})$. A més $-1 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ actúa trivialment sobre $\mathbb{H}$. Tenim doncs una acció de $\mathrm{PSL}(2,\mathbb{R})$ sobre $\mathbb{H}$, que es pot provar que és fidel.

Anomenem *grup modular* el grup $\Gamma = \mathrm{SL}(2,\mathbb{Z})/\{\pm 1\}$. És generat per les matrius

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Una *funció feblement modular de pes k* és una funció meromorfa $f$ sobre $\mathbb{H}$ que compleix

$$f(\gamma(\tau)) = (c\tau+d)^k f(\tau), \quad \text{per a tot } \gamma \in \Gamma. \tag{3.1}$$

En particular $f$ compleix que $f(\tau+1) = f(\tau)$, i per tant es pot expressar com una funció $\widetilde{f}$ de $q = e^{2\pi i\tau}$, que és meromorfa sobre el disc perforat $0 < |q| < 1$. Si $\widetilde{f}$ es pot estendre a una funció meromorfa (resp. holomorfa) a l'origen, diem que $f$ és meromorfa (resp. holomorfa) a $\infty$. Aleshores $\widetilde{f}$ admet un desenvolupament en sèrie de Laurent a l'entorn de l'origen

$$\widetilde{f}(q) = \sum_{n=r}^{\infty} a_n q^n.$$

Una *funció modular* és una funció feblement modular que és meromorfa a l'infinit.

Si $f$ és holomorfa a l'infinit, el seu valor a l'infinit és $f(\infty) = \widetilde{f}(0)$.

Una *forma modular* és una funció modular que és holomorfa a tot arreu (inclòs a l'infinit). Si s'anul·la a l'infinit, s'anomena *forma parabòlica*.

Exemples de funcions modulars són les sèries d'Eisenstein. Per a un enter $k > 1$, considerem la sèrie

$$G_k(z) = \sum_{m,n}{}' \frac{1}{(mz+n)^{2k}},$$

on $m, n$ són enters i el símbol $\sum'$ indica que la suma es fa sobre els parells d'enters $(m, n)$ diferents de $(0, 0)$. Per a $k$ enter $> 1$, la sèrie d'Eisenstein $G_k(z)$ és una forma modular de pes $2k$. Es té que $G_k(\infty) = 2\zeta(2k)$, on $\zeta$ indica la funció zeta de Riemann. El desenvolupament en sèrie de potències de $q$ de $G_k$ és

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

on $\sigma_k(n) = \sum_{d|n} d^k$ és la suma de les potències $k$-èsimes dels divisors positius de $n$. Es defineix la sèrie d'Eisenstein normalitzada de pes $2k$ com

$$E_k(z) = G_k(z)/2\zeta(2k).$$

En particular, tenim les sèries d'Eisenstein nomalitzades de pesos 4 i 6:

$$E_2 = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n, \quad E_3 = 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n.$$

Es pot definir anàlogament la sèrie d'Eisenstein normalitzada $E_1$ de pes 2 però no és una forma modular.

Més en general, es poden definir formes modulars respecte d'un subgrup $G$ de $\Gamma$, és a dir complint la relació (3.1) per a $\gamma \in G$. Dos punts $z_1, z_2$ de $\mathbb{H}$ són $G$-equivalents si existeix un element $\gamma \in G$ tal que $z_2 = \gamma z_1$. Un *domini fonamental* per al grup $G$ és un conjunt obert $D$ que conté exactament un punt de cada classe de $G$-equivalència. Els punts de compactificació de $D$ sobre la frontera de $\mathbb{H}$ s'anomenen *puntes*. En la definició de funció modular (resp. forma modular) respecte de $G$ s'exigeix la condició de meromorfia (resp. holomorfia) a totes les puntes (cf. [3], [1]).

A l'article de Zagier [6], es consideren formes modulars respecte d'un subgrup fixat $\Gamma$ de $\mathrm{PSL}(2, \mathbb{R})$, però quin és aquest subgrup no juga cap paper en els resultats que s'hi obtenen.

## 3.2 El claudàtor de Rankin-Cohen

Siguin $f(\tau), g(\tau)$ formes modulars de pes $k$ i $l$ respecte d'un grup $\Gamma \subset \mathrm{PSL}(2,\mathbb{R})$. Considerem l'operador diferencial

$$D := \frac{1}{2\pi i}\frac{d}{d\tau} = q\frac{d}{dq} \quad (q = e^{2\pi i\tau}).$$

El *n-èsim claudàtor de Rankin-Cohen* de $f$ i $g$ es defineix per

(3.2)
$$[f,g]_n(\tau) = \sum_{r+s=n} (-1)^r \binom{n+k-1}{s}\binom{n+l-1}{r} f^{(r)}(\tau) g^{(s)}(\tau).$$

Veurem que $[f,g]_n(\tau)$ és una forma modular de pes $k+l+2n$ sobre el grup $\Gamma$.

L'espai vectorial graduat $M_*(\Gamma)$ té, a més de l'estructura d'anell graduat commutatiu corresponent al claudàtor 0-èsim, un conjunt infinit d'operacions bilineals

$$[\ ,\ ]_n : M_* \otimes M_* \to M_{*+*+2n}.$$

Associem a la forma modular $f(\tau)$ la sèrie de potències formals

$$\widetilde{f}(\tau, X) = \sum_{n=0}^{\infty} \frac{f^{(n)}(\tau)}{n!(n+k-1)!}(2\pi i X)^n \tag{3.3}$$

introduïda per Kuznetsov i Cohen.

Aleshores,

$$\widetilde{f}(\tau,-X)\widetilde{g}(\tau,X) = \sum_{n=0}^{\infty} \frac{[f,g]_n(\tau)}{(n+k-1)!(n+l-1)!}(2\pi i X)^n \tag{3.4}$$
$$(f \in M_k, g \in M_l).$$

D'altra banda,

$$\widetilde{f}\left(\gamma(\tau), \frac{X}{(c\tau+d)^2}\right) = (c\tau+d)^k e^{cX/(c\tau+d)}\widetilde{f}(\tau,X) \tag{3.5}$$
$$\left(\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, \gamma(\tau) := \frac{a\tau+b}{c\tau+d}\right).$$

La identitat (3.5) és equivalent per comparació dels coeficients a la sèrie d'identitats

$$\frac{f^{(n)}(\gamma(\tau))}{n!(n+k-1)!} = \sum_{m=0}^{n} \frac{c^{n-m}(c\tau+d)^{k+n+m}}{(2\pi i)^{n-m}(n-m)!} \; \frac{f^{(m)}(\tau)}{m!(m+k-1)!} \quad (n \geq 0),$$

que es prova per inducció sobre $n$. Per a $n = 0$, tenim que $f(\gamma(\tau)) = (c\tau+d)^k f(\tau)$.

Ara, la identitat (3.5) i la fórmula corresponent per a $\widetilde{g}$ impliquen que el producte $\widetilde{f}(\tau,-X)\widetilde{g}(\tau,X)$ queda multiplicat per $(c\tau+d)^{k+l}$ quan s'aplica la transformació $(\tau,X) \mapsto (\gamma(\tau),(c\tau+d)^{-2}X)$ i això dóna que el coeficient de $X^n$ en aquest producte es transforma com una forma modular de pes $k+l+2n$ per a tot $n$, per tant per l'igualtat (3.4) el mateix és cert per a $[f,g]_n(\tau)$. Com la holomorfia en les puntes es dedueix de la seva definició, obtenim que $[f,g]_n(\tau)$ és una forma modular de pes $k+l+2n$ per a tot $n$.

Es pot donar una prova alternativa en termes de funcions theta i polinomis esfèrics. Aquesta segona prova dóna que l'operador $[\cdot,\cdot]_n$ és l'únic operador diferencial de grau $2n$ que envia formes modulars a formes modulars.

## 3.3 Propietats algebraiques dels claudàtors de Rankin-Cohen

Els claudàtors de Rankin-Cohen satisfan unes quantes identitats algebraiques

$$[f,g]_n = (-1)^n [g,f]_n,$$

per a tot $n$. El claudàtor 0-èsim és la multiplicació usual, per tant satisfà

$$[[f,g]_0,h]_0 = [f,[g,h]_0]_0$$

i dota $(M_*,[\ ,\ ]_0)$ d'una estructura d'àlgebra commutativa i associativa. Tenim també

$$[f,1]_0 = [1,f]_0 = f, \quad [f,1]_n = [1,f]_n = 0 \quad (n>0).$$

El primer claudàtor, donat per

$$[f,g]_1 = -[g,f]_1 = kfg' - lf'g \in M_{k+l+2} \quad (f \in M_k, g \in M_l),$$

satisfà l'identitat de Jacobi

$$[[f,g]_1,h]_1+[[g,h]_1,f]_1+[[h,f]_1,g]_1=0,$$

i dota $M_{*-2}$ d'una estructura d'àlgebra de Lie graduada.

Els dobles claudàtors $[[\ ,\ ]_0,\ ]_1$ i $[[\ ,\ ]_1,\ ]_0$ satisfan les identitats

$$[[f,g]_0,h]_1+[[g,h]_0,f]_1+[[h,f]_0,g]_1=0$$

i

$$m[[f,g]_1,h]_0+k[[g,h]_1,f]_0+l[[h,f]_1,g]_0=0$$

$$(f\in M_k, g\in M_l, h\in M_m),$$

així com també les relacions barrejades

$$\begin{aligned}[[f,g]_0,h]_1 &= [[g,h]_1,f]_0-[[h,f]_1,g]_0\\ &= [[g,h]_1,f]_0+[[f,h]_1,g]_0,\\ (k+m+l)[[f,g]_1,h]_0 &= k[[h,f]_0,g]_1-l[[g,h]_0,f]_1.\end{aligned}$$

La primera d'aquestes relacions indica que el claudàtor de Lie amb un element fixat de $M_*$ actúa com una derivació respecte de l'estructura d'àlgebra associativa donada per $[,]_0$, i.e. $M_*$ és una àlgebra de Poisson.

Les relacions anteriors, que no són totes independents, descriuen totes les identitats que relacionen els claudàtors de nivell 0 i 1. Les relacions del segon claudàtor

$$[f,g]_2=\tbinom{k+1}{2}fg''-(k+1)(l+1)f'g'+\tbinom{l+1}{2}f''g\in M_{k+l+4}$$

$$(f\in M_k, g\in M_l)$$

ja són bastant complicades. Amb $f,g,h\in M_k,M_l,M_m$ (resp.), podem escriure nou expressions trilineals de pes $k+l+m+4$, que són

$$[[f,g]_0,h]_2,\quad [[f,g]_1,h]_1,\quad [[f,g]_2,h]_0$$

i les seves permutacions cícliques. (Les transposicions donen el mateix element tret del signe). L'espai que generen té dimensió 3 i una base

ve donada pel primer o l'últim grup, que es relacionen mútuament per

$$(k+1)(l+1)[[f,g]_0,h]_2 = -m(m+1)[[f,g]_2,h]_0$$

$$+(k+1)(k+l+1)[[g,h]_2,f]_0 + (l+1)(k+l+1)[[h,f]_2,g]_0,$$

$$(k+l+m+1)(k+l+m+2)[[f,g]_2,h]_0 = -(k+1)(l+1)[[f,g]_0,h]_2$$

$$+(l+1)(k+l+1)[[g,h]_0,f]_2 + (k+1)(k+l+1)[[h,f]_0,g]_2,$$

mentre que el segon grup (que és linealment dependent per la identitat de Jacobi) s'expressa en termes d'aquests per

$$[[f,g]_1,h]_1 = [[g,h]_0,f]_2 - [[h,f]_0,g]_2 + [[g,h]_2,f]_0 - [[h,f]_2,g]_0.$$

## 3.4 Operadors de Rankin-Cohen i formes del tipus de Jacobi

Fixem un subgrup $\Gamma$ de $\mathrm{PSL}(2,\mathbb{R})$. Per a cada enter $k > 0$, sigui $J_k = J_k(\Gamma)$ el conjunt de totes les funcions holomorfes $\phi(\tau, X)$ sobre $\mathbb{H} \times \mathbb{C}$ ($\mathbb{H}$= semiplà superior) satisfent

$$\phi\left(\gamma(\tau), \frac{X}{(c\tau+d)^2}\right) = (c\tau+d)^k e^{cX/(c\tau+d)}\phi(\tau,X) \qquad \left(\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma\right), \tag{3.6}$$

i.e. l'equació (3.5) amb $\phi$ en lloc de $\widetilde{f}$ així com les condicions d'holomorfia usuals en les puntes. Anomenem el elements de $J_k$ *de tipus de Jacobi de pes* $k$.

Clarament la restricció d'una forma de tipus de Jacobi a $X = 0$ és una forma de pes $k$ sobre $\Gamma$ i el nucli de l'aplicació $J_k \to M_k = M_k(\Gamma)$, $\phi(\tau, X) \mapsto \phi(\tau, 0)$ és justament $X \cdot J_{k+2}(\Gamma)$.

L'equació funcional (3.5) indica que tenim una secció canònica $f \mapsto (k-1)!\widetilde{f}$ de $J_k \to M_k$, de forma que la successió

$$0 \to J_{k+2}(\Gamma) \to J_k(\Gamma) \to M_k(\Gamma) \to 0$$

és exacta i escindeix canònicament.

Si escrivim $\phi(\tau, X) \in J_k(\Gamma)$ com $\sum_{n=0}^{\infty} \phi_n(\tau)(2\pi i X)^n$, aleshores comparant coeficients de $X^n$ a (3.6) s'obtenen les equacions funcionals

$$(3.7) \quad (c\tau + d)^{-k-2n}\phi_n(\gamma(\tau)) = \sum_{m=0}^{n} \frac{1}{m!}\left(\frac{1}{2\pi i}\,\frac{c}{c\tau+d}\right)^m \phi_{n-m}(\tau)$$

i, recíprocament, qualsevol successió de funcions holomorfes $\phi_n(\tau)$ satisfent (3.7) i una condició de creixement a les puntes defineix un element de $J_k(\Gamma)$. Les equacions (3.7) són al seu torn equivalents a la sèrie de lleis de transformació

$$\phi_0 \in M_k, \quad k\phi_1 - \phi_0' \in M_{k+2},$$

$$2(k+2)(k+1)\phi_2 - 2(k+1)\phi_1' + \phi_0'' \in M_{k+4}, \ldots$$

(recordem $D = \dfrac{1}{2\pi i}\,\dfrac{d}{d\tau}$) i, en general,

$$(3.8) \quad h_n := \sum_{m=0}^{n} (-1)^m \frac{(2n-m+k-2)!}{m!}\,\phi_{n-m}^{(m)} \in M_{k+2n} \quad (n \geq 0).$$

L'igualtat (3.8) es pot invertir per escriure

$$(3.9) \qquad \phi_n(\tau) = \sum_{r+m=n} \frac{2m+k-1}{r!(r+2m+k-1)!}\,h_m^{(r)}(\tau)$$

o, equivalentment, com

$$\phi(\tau, X) = \sum_{n=0}^{\infty} (2n+k-1)\widetilde{h}_n(\tau, X)(2\pi i X)^n$$

i aleshores la modularitat de $h_n$ se segueix inductivament de la igualtat

$$(3.10) \qquad \widetilde{f}\left(\gamma(\tau), \frac{X}{(c\tau+d)^2}\right) = (c\tau+d)^k e^{cX/(c\tau+d)}\,\widetilde{f}(\tau, X)$$

aplicada a $\widetilde{h}_{n'}, n' < n$, i de la propietat de tipus Jacobi de $\phi$.

Les equacions (3.8) i (3.9) proporcionen una bijecció entre $J_k(\Gamma)$ i $\prod_n M_{k+2n}(\Gamma)$.

Ara podem obtenir més relacions satisfetes pels claudàtors de Rankin-Cohen considerant els aixecaments $\widetilde{f}(\tau, X)$, $\widetilde{g}(\tau, Y)$ de Cohen-Kuznetsov de dues formes modulars $f \in M_k$, $g \in M_l$ i una família de polinomis homogenis auxiliars en quatre variables

$$H_n(k, l; X, Y) = \sum_{r+s=n} (-1)^r \binom{n+k-1}{s} \binom{n+l-1}{r} X^r Y^s.$$

L'equació que defineix $[f, g]_n$ es pot escriure de nou com

$$[f, g]_n = H_n(k, l; D_{\tau_1}, D_{\tau_2})(f(\tau_1)g(\tau_2))|_{\tau_1=\tau_2=\tau}.$$

Obtenim

**3.4.1 Proposició.** *Per a $f \in M_k(\Gamma), g \in M_l(\Gamma)$, $h \in M_m(\Gamma)$ i $\alpha, \beta, \gamma \in \mathbb{C}$, l'expressió*

$$\sum_{n=0}^{r} c_n(k, l; \alpha, \beta) c_{r-n}(k + l + 2n, m; \alpha + \beta, \gamma)[[f, g]_n, h]_{r-n}$$

*que dóna un element de $M_{k+l+m+2r}(\Gamma)(r \in \mathbb{Z}_{\geq 0})$ és simètrica per l'acció de les permutacions de $(f, k, \alpha), (g, l, \beta), (h, m, \gamma)$, on $c_n$ ve donat per*

$$c_n(k, l; \alpha, \beta) = (2n + k - 1) \frac{n!(n + k + l - 2)!}{(n + k - 1)!(n + l - 1)!} H_n(k, l; \alpha, \beta).$$

Variant $r$ i comparant coeficients dels diferents monomis en $\alpha, \beta$ i $\gamma$, obtenim sistemàticament identitats universals satisfetes pels claudàtors de Rankin-Cohen del tipus estudiat abans.

## 3.5 Operadors de Rankin-Cohen i operadors pseudodiferencials

Sigui $D = (2\pi i)^{-1} d/d\tau$. Per *operador pseudodiferencial* formal entendrem una sèrie de potències formal $\sum_{n=0}^{\infty} g_n(\tau) D^{-n}$, on els $g_n$ són funcions holomorfes en el semiplà superior. Estenent la fórmula per a la multiplicació d'operadors diferencials implicada per la regla de

Leibniz als operadors pseudodiferencials, obtenim que dos d'aquests es poden multiplicar amb la fórmula

$$(\sum_{m=0}^{\infty} f_m(\tau)D^{-m})(\sum_{n=0}^{\infty} g_n(\tau)D^{-n}) =$$

$$\sum_{m,r,n\geq 0} \binom{-m}{r} f_m(\tau)g_n^{(r)}(\tau)D^{-m-r-n},$$

on $\binom{-m}{r} = (-m)(-m-1)\dots(-m-r+1)/r!$.

Per un canvi de coordenades $\tau \mapsto \widetilde{\tau}$, l'operador de diferenciació $D$ es transforma en $\widetilde{D} = j^{-1}D$, on $j = d\widetilde{\tau}/d\tau$, i a aquesta transformació li correspon una acció sobre els operadors pseudodiferencials. Si el canvi de coordenades és $\widetilde{\tau} = \gamma(\tau) = \dfrac{a\tau+b}{c\tau+d}$ amb $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{C})$, aleshores $j = (c\tau+d)^{-2}$ i obtenim

$$\begin{aligned} \widetilde{D}^{-n} &= [(c\tau+d)^2 D]^{-n} \\ &= \sum_{r=0}^{\infty} r! \binom{-n}{r}\binom{-n-1}{r} (c/2\pi i)^r (c\tau+d)^{2r+n} D^{r-n}. \end{aligned}$$

Tenim doncs una acció de $\Gamma$ sobre els operadors pseudodiferencials, per a un grup modular $\Gamma$ que opera sobre el semiplà superior, per tant té sentit dir qu'un operador diferencial $\sum_{n=0}^{\infty} g_n(\tau)D^{-n}$ és $\Gamma$-invariant. Si $n_0$ és l'índex més petit amb $g_{n_0} \not\equiv 0$ per a un tal operador, llavors obtenim

$$g_{n_0} \in M_{2n_0}, g_{n_0+1} + \frac{1}{2}(n_0+1)g'_{n_0} \in M_{2n_0+2}, \dots$$

que recorda a les equacions (3.8). En efecte, obtenim que la sèrie de potències

$$\sum_{n=n_0}^{\infty} \frac{g_n(\tau)}{n!(n-1)!}(-2\pi i X)^{n-n_0}$$

pertany a $J_k(\Gamma)$, establint una correspondència bijectiva entre operadors diferencials invariants de la forma $\sum_{n=0} g_n(\tau)D^{-n}$ i formes del tipus de Jacobi de pes $k$.

Combinant aquesta correspondència amb l'aixecament de Kuznetsov-Cohen que envia una forma modular $f$ a la sèrie de potències $\widetilde{f}$, trobem que hi ha un aixecament canònic

$$f(\tau) \mapsto \mathcal{D}[f] = \sum_{r=0}^{\infty} (-1)^r \frac{(r+k/2)!(r+k/2-1)!}{r!(r+k-1)!} f^{(r)}(\tau) D^{-r-k/2}$$
$$(f \in M_k, k > 0 \text{ parell})$$

de formes modulars a operadors pseudodiferencials, i que reciprocament qualsevol operador pseudodiferencial $\Gamma$-invariant es pot desenvolupar en suma d'aixecaments. En particular, com que el producte de dos operadors pseudodiferencials $\Gamma$-invariants n'és un altre, podem associar a un parell de formes modulars $f \in M_k, g \in M_l$ una successió de formes modulars $\{h_n\}_{n\geq 0}$ via

$$\mathcal{D}[f] \cdot \mathcal{D}[g] = \sum_{n=0}^{\infty} \mathcal{D}[h_n] \quad (h_n \in M_{k+l+2n}).$$

Per la unicitat dels claudàtors de Rankin-Cohen, ha de ser

$$h_n = t_n(k,l)[f,g]_n$$

per a un cert factor universal $t_n = t_n(k,l)$. La fórmula per a $t_n(k,l)$ així com també altres aspectes de la connexió entre operadors pseudodiferencials i formes modulars es troba a ([2]).

## 3.6 Àlgebres de Rankin-Cohen

Definim una *àlgebra de Rankin-Cohen* (o àlgebra RC) sobre un cos $K$ com un $K$-espai vectorial graduat $M_* = \oplus_{k\geq 0} M_k$ (amb $M_0 = K.1$ i $\dim_K M_k$ finita per a tot $k$) junt amb operacions bilineals

$$[\,,\,]_n : M_k \otimes M_l \to M_{k+l+2n} \quad (k,l,n \geq 0)$$

que satisfan totes les identitats algebraiques satisfetes pels claudàtors de Rankin-Cohen.

Suposarem car $K = 0$.

*Exemple 1.*

**3.6.1 Definició.** Sigui $R_*$ una àlgebra commutativa graduada amb unitat sobre $K$ junt amb una derivació $D : R_* \to R_*$ de grau 2 (i.e. $D(R_k) \subset R_{k+2}$ per a tot $k$ i $(fg)' = f'g + fg'$), i definim $[,]_{D,n}$ per

$$[f,g]_{D,n} = \sum_{r+s=n} (-1)^r \binom{n+k-1}{s}\binom{n+l-1}{r} f^{(r)}g^{(s)} \in R_{k+l+2n}$$

$$(f \in R_k, g \in R_l).$$

Aleshores $(R_*, [,]_{D,n})$ és una àlgebra RC que anomenem l'*àlgebra RC estàndard sobre* $(R_*, D)$.

*Exemple 2.* $M_*(\Gamma)$ amb el claudàtor de Rankin-Cohen no és una àlgebra estàndard ja que no és tancada per l'acció de $D = (2\pi i)^{-1}d/d\tau$. Busquem una àlgebra RC estàndard no massa gran que la contingui. Considerem primer el cas $\Gamma = \mathrm{PSL}(2,\mathbb{Z})$. Aquí $M_*(\Gamma) = \mathbb{C}[E_2, E_3]$, on $E_2$ i $E_3$ són les sèries d'Eisenstein normalitzades de pesos 4 i 6. Les seves derivades venen donades per $E_2' = \frac{1}{3}(E_1E_2 - E_3)$ i $E_3' = \frac{1}{2}(E_1E_3 - E_2^2)$, on $E_1$ és la sèrie d'Eisenstein normalitzada de pes 2, i com que també tenim $E_1' = \frac{1}{12}(E_1^2 - E_2)$, això vol dir que $M_*(\Gamma)$ està continguda a l'àlgebra RC estàndard sobre$(\mathbb{C}[E_1, E_2, E_3], D)$.

Sigui $K$ un cos de característica 0 i definim una derivació sobre $K[E_1, E_2, E_3]$

$$D : K[E_1, E_2, E_3]_* \to K[E_1, E_2, E_3]_{*+2},$$

on $E_1, E_2, E_3$ tenen graus 2,4,6, per

$$D = \frac{E_1^2 - E_2}{12}\frac{\partial}{\partial E_1} + \frac{E_1E_2 - E_3}{3}\frac{\partial}{\partial E_2} + \frac{E_1E_3 - E_2^2}{2}\frac{\partial}{\partial E_3};$$

aleshores la subàlgebra generada per $E_2$ i $E_3$ és tancada per l'acció dels operadors $[,]_n = [,]_{D,n}$ per a tot $n \geq 0$.

*Exemple 3.* Observem que tenim també una derivació $\partial$ de grau 2 sobre la subàlgebra $M_* = K[E_2, E_3]$ de $R_* = K[E_1, E_2, E_3]$ definida en termes de $D$ per

$$\partial f = Df - \frac{k}{12}E_1 f \in M_{k+2} \qquad (f \in M_k) \tag{3.11}$$

o directament per

$$\partial = -\frac{E_3}{3}\frac{\partial}{\partial E_2} - \frac{E_2^2}{2}\frac{\partial}{\partial E_3} : M_* \to M_{*+2}.$$

Podem reconstruir $(R_*, D)$ a partir de $(M_*, \partial)$ usant (3.11) per definir $Df$ per a $f \in M_k$ i definint $D(E_1)$ com $\frac{1}{12}(E_1^2 - E_2)$.

**3.6.2 Proposició.** *Sigui $M_*$ una $K$-àlgebra graduada commutativa i associativa amb $M_0 = K.1$ junt amb una derivació $\partial : M_* \to M_{*+2}$ de grau 2, i sigui $\psi \in M_4$. Definim claudàtors $[\ ]_{\partial,\psi,n} (n \geq 0)$ a $M_*$ per*

$$[f,g]_{\partial,\psi,n} = \sum_{r+s=n} (-1)^r \binom{n+k-1}{s}\binom{n+l-1}{r} f_r g_s \in M_{k+l+2n}$$

*per a $f \in M_k, g \in M_l$, on $f_r \in M_{k+2r}, g_s \in M_{l+2s} (r,s \geq 0)$ es defineixen recursivament per*

$$f_{r+1} = \partial f_r + r(r+k-1)\psi f_{r-1},\ g_{s+1} = \partial g_s + s(s+l-1)\psi g_{s-1},\ (r,s \geq 0)$$

*amb condicions inicials $f_0 = f, g_0 = g$ (per tant $f_1 = \partial f, f_2 = \partial^2 f + k\psi f$ i similarment per a $g_s$). Aleshores $(M_*, [\ ]_{\partial,\psi,n})$ és una álgebra RC.*

**3.6.3 Definició.** Una àlgebra RC s'anomena *canònica* si els seus claudàtors estan donats com a la proposició 3.6.2 per a alguna derivació $\partial : M_* \to M_*$ de grau $+2$ i algun element $\psi \in M_4$.

*Idea de la prova.* L'única manera de comprovar que quelcom és una àlgebra RC és immergir-lo en una àlgebra RC estàndard $(R_*, [,]_{D,*})$ per a algun anell graduat més gran $R_*$ amb derivació $D$. Prenem $R_* = M[\phi]_* := M_* \otimes_K K[\phi]$, on $\phi$ te grau 2, i definim $D$ per

(3.12)
$$D(f) = \partial(f) + k\phi f \in R_{k+2} \quad (f \in M_k), \quad D(\phi) = \psi + \phi^2 \in R_4.$$

Aleshores provem que $[f,g]_{D,n} = [f,g]_{\partial,\psi,n}$, per a $f$ i $g$ a $M_*$ i és clar que $M_*$ és tancat per l'acció dels claudàtors $[\ ]_{\partial,\psi,n}$.

## 3.7 Un teorema d'estructura per a les àlgebres de Rankin-Cohen

Donada una RC algebra $M_*$ sobre un cos $K$, volem realitzar els seus claudàtors com els claudàtors $[\ ,\ ]_{\partial,\psi,n}$ per a alguna derivació $\partial$ de grau 2 i algun element $\psi$ de grau 4. Com que el claudàtor 0-èsim dóna a $M_*$ una estructura d'àlgebra commutativa, tenim estructura d'anell. Suposem que aquest anell és íntegre o, com a mínim que existeix un element homogeni $F$ de grau positiu $N$ que no és divisor de zero i sigui $\widehat{M}_*$ el cos de fraccions de $M_*$ o $M[1/F]_*$, respectivament. La compatibilitat dels claudàtors en el cas d'una àlgebra RC estàndard implica que podem estendre els claudàtors canònicament a $\widehat{M}_*$. Definirem ara una derivació $\partial : \widehat{M}_* \to \widehat{M}_{*+2}$ i un element $\psi \in \widehat{M}_4$ per

$$\partial(f) = \frac{[F,f]_1}{NF}\ (F \in \widehat{M}_*), \quad \psi = \frac{[F,F]_2}{N^2(N+1)F^2}.$$

Es pot provar que els claudàtors $[\ ,\ ]_{\partial,\psi,n}$ associats a $\partial$ i $\psi$ coincideixen amb els claudàtors donats a $\widehat{M}_*$. Per tant qualsevol àlgebra RC $\widehat{M}_*$ que contingui al menys un element homogeni $F$ de grau positiu que no sigui divisor de zero és una subàlgebra d'una àlgebra RC canònica i, per tant, també una subàlgebra RC d'una àlgebra estàndard, l'àlgebra $(\widehat{M}_*[\phi], [\ ,\ ]_{D,*})$ amb $\phi$ de grau 2 i $D : \widehat{M}[\phi]_* \to \widehat{M}[\phi]_{*+2}$ definida per (3.12).

El teorema següent dóna un criteri per a què una àlgebra RC sigui canònica que es pot comprovar en temps finit.

**3.7.1 Teorema.** *Sigui $(M_*, [\ ,\ ]_*)$ una àlgebra RC finitament generada sobre un cos de característica 0. Aleshores les propietats següents són equivalents.*

(a) *$(M_*, [\ ,\ ]_*)$ és canònica.*

(b) *Per a cada element homogeni $F \in M_*$ existeix un element $G \in M_{*+2}$ tal que*

  (i) *$[F,f]_1 \equiv kfG \pmod F$ per a tot $k \geq 0$ i tot $f \in M_k$.*

  (ii) *$[F,F]_2 \equiv (N+1)G^2 - (N+1)[F,G]_1 \pmod{F^2}$, on $N = \deg F$.*

(c) *La propietat (b) es compleix per a algun $F \in M_*$ homogeni, no divisor de zero.*

*Específicament, si $(F, G)$ és un parell d'elements satisfent (i) i (ii), i amb $F \in M_N$ no divisor de zero, aleshores el claudàtor sobre $M_*$ coincideix amb el claudàtor canònic associat a*

$$\partial_{F,G}(f) := \frac{[F, f]_1 - kfG}{NF} \quad (f \in M_k),$$

$$\psi_{F,G} := \frac{[F, F]_2 + (N+1)([F, G]_1 - G^2)}{N^2(N+1)F^2}.$$

Finalment, Zagier fa notar que les àlgebres de Rankin-Cohen tenen similaritats amb altres objectes que apareixen de forma natural en diferents contextos matemàtics. Aquests són àlgebres d'invariants, els operadors de Moyal de la teoria quàntica i les àlgebres d'operadors de vèrtexs.

# Bibliografia


[1] Atkin, A. O. L.; Lehner, J.: Hecke operators on $\Gamma_0(m)$. *Math. Ann.* 185 (1970), 134–160.

[2] Cohen, P. B.; Manin, Y.; Zagier, D.: *Automorphic pseudodifferential operators, Algebraic aspects of integrable systems*, 17–47. Progr. Nonlinear Differential Equations Appl., 26. Birkhäuser Boston, Boston, MA, 1997.

[3] Gunning, R. C.: *Lectures on modular forms*. Princeton University Press, 1962.

[4] Rankin, R. A.: The construction of automorphic forms from the derivatives of a given form. *J. Indian Math. Soc.* 20 (1956), 103–116.

[5] Serre, J-P.: *Cours d'arithmétique*. PUF, 1977.

[6] Zagier, D.: Modular forms and differential operators. *Proc. Indian Acad. Sci. Math. Sci.* 104 (1994), no. 1, 57–75.



T. Crespo

Departament d'Àlgebra i Geometria

Universitat de Barcelona

Gran Via de les Corts Catalanes 585

E-08007, Barcelona

**teresa.crespo@ub.edu**

# Capítol 4

# Càlcul d'invariants $j$ supersingulars

A. Travesa

Aquest capítol correspon a l'exposició que tingué lloc el dia 30 de gener de 2008 a Vilanova i la Geltrú, en la quarta de les sis sessions dedicades al tema "Monogràfic sobre treballs de Don Zagier" dins el marc del 22è Seminari de Teoria de Nombres (UB-UAB-UPC). L'objectiu era donar compte de l'article següent que, alhora, correspon a una exposició dels seus autors que tingué lloc l'any 1995 a Chicago i que citaré [K-Z] (cf. [4]):

[K-Z] Kaneko, M.; Zagier, D.: Supersingular $j$-invariants, hypergeometric series, and Atkin's orthogonal polynomials. *Computational perspectives on Number Theory*, 97-126, AMS/IP Stud. Adv. Math., **7**, Amer. Math. Soc., Providence, RI, 1998.

## 4.1 Introducció

L'article [K-Z] és una revisió i una posada al dia de la part dels treballs clàssics de M. Deuring [1] i de H. Hasse [3] en què es fa l'estudi dels

Amb finançament parcial de MTM2006-04895 i MRTN-CT-2006-035495.

invariants supersingulars. Començaré per fer una descripció breu del seu contingut sense entrar, en aquest moment, en el detall precís dels resultats.

Kaneko i Zagier consideren el polinomi supersingular en característica $p$, polinomi que anomenen $ss_p(j)$ i que pertany a $\mathbb{F}_p[j]$, i es plantegen com a problema donar polinomis canònics de $\mathbb{Q}[j]$ per als quals la reducció mòdul $p$ tingui sentit i proporcioni $ss_p(j)$. Amb aquest objectiu, construeixen polinomis de tres maneres diferents i, així, obtenen:
(a) polinomis que provenen de formes modulars;
(b) els polinomis ortogonals d'Atkin; i
(c) altres polinomis ortogonals que provenen de sèries hipergeomètriques.

(a) Dels polinomis que provenen de formes modulars en donen quatre per a cada $p \geq 5$. Per a això, comencen per ensenyar com associar polinomis a formes modulars i, a continuació, es dediquen a construir quatre formes modulars, de les quals consideraran els polinomis associats.

(b) Pel que fa als polinomis ortogonals d'Atkin, els autors els defineixen a partir del producte escalar d'Atkin, del qual donen fins a quatre descripcions diferents; això els permet donar, també, quatre descripcions diferents dels polinomis d'Atkin.

(c) També proporcionen quatre polinomis diferents associats a sèries hipergeomètriques, la reducció mòdul $p$ dels quals coincideix amb el polinomi supersingular.

L'article conté demostracions autocontingudes de la majoria dels resultats que els autors utilitzen, de manera que la seva exposició es pot pensar com una teoria sobre els invariants supersingulars.

De fet, en aquesta exposició, només comentarem amb detall tot allò que fa referència a formes modulars i als polinomis ortogonals d'Atkin, i ens limitarem a enunciar els resultats que es relacionen amb les sèries hipergeomètriques.

## 4.2 Una mica d'història

Abans d'entrar en el detall del contingut de [K-Z], convé destacar quins són els resultats clàssics sobre els quals tracta el tema. Comencem per la definició d'invariant supersingular, tal com es dóna en [K-Z].

**4.2.1 Definició.** (Cf. [4], p. 97) Es diu que una corba el·líptica $E$ definida sobre un cos $k$ de característica un nombre primer $p$ és supersingular si el grup de $p$-torsió de $E$ sobre una clausura algebraica $\overline{k}$ de $k$ és trivial; o sigui, si $E(\overline{k})$ no té elements d'ordre $p$.

Com que l'invariant $j$ de la corba el·líptica, $j(E) \in \overline{k}$, només depèn de la classe d'isomorfisme de $E$ sobre $\overline{k}$, el fet que una corba el·líptica sigui supersingular o no només depèn del valor $j(E)$. Podem parlar, doncs, dels invariants $j$ supersingulars: són els elements de $\overline{k}$ que es corresponen amb les classes d'isomorfisme de corbes el·líptiques supersingulars.

La definició clàssica d'invariant supersingular que dóna Deuring fa ús dels cossos de funcions el·líptiques. Concretament:

**4.2.2 Definició.** (Cf. [1], p. 249 i p. 198-199) Sigui $K$ un cos de funcions el·líptiques de característica $p$, de cos de constants algebraicament tancat $\overline{k}$, i d'invariant $j(K) \in \overline{k}$. Es diu que $j(K)$ és supersingular si $K$ té multiplicació per un ordre d'una àlgebra de quaternions sobre $\mathbb{Q}$.

En l'article de Deuring [1] es demostra que, obligatòriament, l'ordre és maximal, que l'àlgebra de quaternions només ramifica en $p$ i $\infty$, i que aquesta definició només depèn de $j(K)$. Denotem aquesta àlgebra per $Q_{p\,\infty}$. Disposem, doncs, de dues definicions del concepte d'invariant supersingular; Deuring mateix demostra que totes dues són equivalents.

**4.2.3 Teorema.** (Cf. [1], p. 251-252 i p. 200) *Per a un invariant supersingular $j$ de característica $p$, el cos el·líptic $K$ d'invariant $j$ no té cap classe de divisors d'ordre $p$.*

*També val, recíprocament*:

*Si $K$ no té cap classe de divisors d'ordre $p$, aleshores $K$ té un ordre maximal de $Q_{p\infty}$ com a anell de multiplicadors. L'invariant $j$ corresponent és, per tant, supersingular.* □

Altres teoremes clàssics de [1] asseguren que, fixat un nombre primer $p$, els invariants supersingulars associats a cossos $k$ de característica $p$ són nombres algebraics sobre el cos primer $\mathbb{F}_p$, independentment de quin sigui el cos $k$ sobre el qual considerem les corbes el·líptiques; a més a més, tots són de grau 1 o bé 2, és a dir, pertanyen a $\mathbb{F}_p$ o bé a $\mathbb{F}_{p^2}$, i si $j_0 \in \mathbb{F}_{p^2} - \mathbb{F}_p$ és un invariant supersingular, el seu altre conjugat galoisià també ho és.

Com a conseqüència, només hi ha una quantitat finita d'invariants supersingulars, i té sentit que en [K-Z] es consideri el polinomi

$$ss_p(j) := \prod_{j_0 \text{ supersingular}} (j - j_0) \in \mathbb{F}_p[j].$$

Anomenarem aquest polinomi el polinomi supersingular en característica $p$. Notem que, per definició, aquest polinomi no té arrels múltiples.

En [1] es demostra que el nombre d'invariants supersingulars en característica $p$, o sigui, el grau del polinomni $ss_p(j)$, coincideix amb el nombre de classes de l'àlgebra $Q_{p\infty}$; i, per a aquest nombre, que prèviament havia calculat Eichler (cf. [2]), en dóna l'expressió

$$h = \begin{cases} 1, & \text{per a } p = 2, \ p = 3, \\ \dfrac{p-1}{12}, & \text{per a } p \equiv 1 \pmod{12}, \\ \dfrac{p-5}{12} + 1, & \text{per a } p \equiv 5 \pmod{12}, \\ \dfrac{p-7}{12} + 1, & \text{per a } p \equiv 7 \pmod{12}, \\ \dfrac{p-11}{12} + 2, & \text{per a } p \equiv 11 \pmod{12}. \end{cases} \tag{4.1}$$

Per a $p = 2$ i per a $p = 3$, l'únic invariant supersingular és $j = 0 = 1728$; en particular, $ss_2(j) = j \in \mathbb{F}_2[j]$ i $ss_3(j) = j \in \mathbb{F}_3[j]$. Per a $p \geq 5$, Deuring atribueix a Hasse (cf. [1], [3]) l'expressió següent per a un invariant $A$ l'anul·lació del qual en un valor concret de $j$ equival a dir que aquest valor de $j$ és supersingular:

$$A = \begin{cases} \Delta^{\frac{p-1}{12}} P(j), & \text{per a } p \equiv 1 \pmod{12}, \\ g_2 \Delta^{\frac{p-5}{12}} P(j), & \text{per a } p \equiv 5 \pmod{12}, \\ g_3 \Delta^{\frac{p-7}{12}} P(j), & \text{per a } p \equiv 7 \pmod{12}, \\ g_2 g_3 \Delta^{\frac{p-11}{12}} P(j), & \text{per a } p \equiv 11 \pmod{12}, \end{cases}$$

on $g_2$ i $g_3$ són els coeficients d'una equació definidora

$$y^2 = 4x^3 - g_2 x - g_3 \tag{4.2}$$

de la corba el·líptica en forma normal de Weierstraß, $\Delta$ és el discriminant

$$\Delta = g_2^3 - 27 g_3^2,$$

i $P(j)$ denota un polinomi de l'invariant $j$ "del qual se sap com a mínim que el seu grau és com a màxim igual a l'exponent de la potència de $\Delta$ que el precedeix" (cf. [1]). Deuring demostra que el polinomi $P(j)$ té efectivament el grau màxim possible, conjecturat per Hasse, i, en conseqüència, que no té arrels múltiples, perquè el nombre d'arrels de $A$ coincideix exactament amb el nombre de classes $h$.

No només això, Deuring també proporciona la fórmula explícita següent per al càlcul de l'invariant $A$:

En el cas que es disposi de l'equació de Weierstrass (4.2) de més amunt,

$$A = \begin{cases} (-1)^{\frac{p-1}{4}} 3^{-\frac{p-1}{4}} \Delta^{\frac{p-1}{12}} \left(\frac{p-1}{2}\right)! \Phi_p(j), & \text{si } p \equiv 1 \pmod{12}, \\ 2^2 (-1)^{\frac{p-1}{4}} 3^{-\frac{p-5}{4}} \Delta^{\frac{p-5}{12}} g_2 \left(\frac{p-1}{2}\right)! \Phi_p(j), & \text{si } p \equiv 5 \pmod{12}, \\ 2^4 (-1)^{\frac{p-3}{4}} 3^{-\frac{p-7}{4}} \Delta^{\frac{p-7}{12}} g_3 \left(\frac{p-1}{2}\right)! \Phi_p(j), & \text{si } p \equiv 7 \pmod{12}, \\ 2^6 (-1)^{\frac{p-3}{4}} 3^{-\frac{p-11}{4}} \Delta^{\frac{p-11}{12}} g_2 g_3 \left(\frac{p-1}{2}\right)! \Phi_p(j), & \text{si } p \equiv 11 \pmod{12}, \end{cases} \tag{4.3}$$

on

$$\Phi_p(j) = j^{[\frac{p}{12}]} \sum_{0\le i<\frac{p}{12}} \frac{\left(-\frac{4}{27}\right)^i (1-2^6\cdot 3^3\cdot j^{-1})^i}{(2i)!\left(\frac{p-1}{4}-3i\right)!\left(\frac{p-1}{4}+i\right)!},$$

si $p \equiv 1 \pmod 4$; i

$$\Phi_p(j) = j^{[\frac{p}{12}]} \sum_{0\le i<\frac{p}{12}} \frac{\left(-\frac{4}{27}\right)^i (1-2^6\cdot 3^3\cdot j^{-1})^i}{(2i+1)!\left(\frac{p-7}{4}-3i\right)!\left(\frac{p+1}{4}+i\right)!},$$

si $p \equiv -1 \pmod 4$.

En el cas que es disposi de la forma normal de Legendre

$$y^2 = x(x-1)(x-\lambda), \tag{4.4}$$

$$A = (-1)^{\frac{p-1}{2}} \sum_{i=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i}^2 \lambda^i, \quad \text{per a} \quad p \ge 3, \tag{4.5}$$

on $\lambda$ és una qualsevol de les sis arrels de

$$j = 2^8 \frac{(1-\lambda(1-\lambda))^3}{\lambda^2(1-\lambda)^2}.$$

Com a conseqüència, i si tenim en compte que els valors de $j$ que corresponen a $g_2 = 0$ i a $g_3 = 0$ són $j = 0$ i $j = 1728$, respectivament, obtenim una expressió explícita del polinomi $ss_p(j)$.

**4.2.4 Proposició.** *Sigui $p \ge 5$ un nombre primer. Llavors,*

$$ss_p(j) = j^\delta (j-1728)^\varepsilon \Phi_p(j) \in \mathbb{F}_p[j],$$

*on $\delta = 0$, si $p \equiv 1 \pmod 6$, $\delta = 1$, si $p \equiv -1 \pmod 6$, $\varepsilon = 0$, si $p \equiv 1 \pmod 4$, $\varepsilon = 1$, si $p \equiv -1 \pmod 4$, i el polinomi $\Phi_p(j)$, donat més amunt, no s'anul·la per a $j = 0$ ni per a $j = 1728$. A més a més, $ss_2(j) = j \in \mathbb{F}_2[j]$, i $ss_3(j) = j \in \mathbb{F}_3[j]$.* □

Notem que els polinomis $\Phi_p(j)$ són, de fet, polinomis de coeficients racionals $p$-enters, de manera que el polinomi $ss_p(j) \in \mathbb{F}_p[j]$ és reducció mòdul $p$ d'un polinomi explícit de coeficients racionals $p$-enters. L'objectiu de l'article [K-Z] és donar explícitament altres polinomis canònics de $\mathbb{Q}[j]$ tals que la seva reducció mòdul $p$ tingui sentit i proporcioni els polinomis $ss_p(j) \in \mathbb{F}_p[j]$.

## 4.3 Polinomis supersingulars i formes modulars

Els primers polinomis que es consideren a [K-Z] que redueixen als polinomis supersingulars s'obtenen a partir de formes modulars; per això convé fixar les notacions de la teoria clàssica, de la qual podem trobar més detalls en [5], [6] i [7], d'acord amb les emprades a [K,Z].

Sigui $\mathcal{H} := \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$ el semiplà superior complex. Una funció modular de pes $k$ per a $\mathbf{PSL}(2,\mathbb{Z})$ és una aplicació meromorfa $f : \mathcal{H} \longrightarrow \mathbb{C} \cup \{\infty\}$ tal que

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau),$$

per a tota matriu $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{SL}(2,\mathbb{Z})$ i tot $\tau \in \mathcal{H}$, i que també és meromorfa en infinit; és a dir, que admet un desenvolupament en sèrie de Fourier de la forma

$$f(\tau) = \sum_{n \geq n_0} a_n q^n, \qquad q = e^{2\pi i \tau}, \qquad n_0 \in \mathbb{Z}.$$

És clar que si $f$, $g$, són funcions modulars de pesos $k$ i $k'$, respectivament, el seu producte $fg$ és una funció modular de pes $k + k'$.

Una forma modular de pes $k$ és una funció modular de pes $k$ holomorfa a tot arreu, inclòs $\infty$ (és a dir, $n_0 \geq 0$); i una forma parabòlica és una forma modular que s'anul·la en $\infty$ (és a dir, $n_0 \geq 1$). Per a tot nombre enter $k \geq 0$, denotarem per $M_k$ l'espai vectorial complex de les formes modulars de pes $k$ per al grup $\mathbf{PSL}(2,\mathbb{Z})$, i per $S_k$ el subespai de les formes parabòliques.

El resultat fonamental del qual se segueixen la majoria de propietats bàsiques de les formes modulars per a $\mathbf{PSL}(2,\mathbb{Z})$ es pot escriure de la manera següent.

**4.3.1 Proposició.** *Si $f$ és una funció modular per a $\mathbf{PSL}(2,\mathbb{Z})$, de pes $k$ i no nul·la, se satisfà la fórmula*

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_P{}' v_P(f) = \frac{k}{12}, \tag{4.6}$$

*on la suma* $\sum_P{}'$ *s'estén a tots els elements* $P$ *d'un conjunt de representants de les òrbites de l'acció de* $\mathbf{PSL}(2,\mathbb{Z})$ *en* $\mathcal{H}\cup\mathbb{Q}\cup\{\infty\}$ *diferents de les òrbites de* $i$, $\rho := \dfrac{-1+i\sqrt{3}}{2}$ $i$ $\infty$, $i$ *on* $v_P(f)$ *denota l'ordre de la funció meromorfa* $f(\tau)$ *en el punt* $P$. $\square$

Notem que, en particular, si $f \in M_k$, és a dir, si $f$ és una forma modular, tots els nombres enters $v_\infty(f)$, $v_i(f)$, $v_\rho(f)$, i $v_P(f)$ són no negatius. Si escrivim la fórmula anterior en la forma

$$12v_\infty(f) + 6v_i(f) + 4v_\rho(f) + \sum_P{}'12v_P(f) = k, \tag{4.7}$$

obtenim immediatament que per a tot $k$ senar i per a $k = 2$ és $M_k = (0)$, i també que $M_0 = \mathbb{C}$, perquè tota funció holomorfa sense zeros és constant. Més avall veurem que els espais vectorials $M_k$ i $S_k$ són de dimensió finita.

Els primers exemples, i molt importants, de formes modulars són les sèries d'Eisenstein. Denotem per $B_k$ els nombres de Bernoulli, definits pel desenvolupament en sèrie de potències

$$\frac{T}{e^T-1} = \sum_{k\geq 0}\frac{B_k}{k!}T^k \in \mathbb{Q}[[T]];$$

i, per a tota parella de nombres enters $r \geq 0$, $n \geq 1$, sigui

$$\sigma_r(n) := \sum_{d|n} d^r$$

la suma de les potències $r$-èsimes dels divisors naturals de $n$. Per a tot nombre enter parell $k \geq 0$, el desenvolupament en sèrie de Fourier de la $k$-èsima sèrie d'Eisenstein normalitzada és

$$E_k(\tau) := 1 - \frac{2k}{B_k}\sum_{n\geq 1}\sigma_{k-1}(n)q^n, \qquad q = q(\tau) = e^{2\pi i\tau}. \tag{4.8}$$

Clarament, és $E_0 = 1$; i, per exemple,

$$E_2(\tau) = 1 - 24\sum_{n\geq 1}\sigma_1(n)q^n \in \mathbb{Z}[[q]], \tag{4.9}$$

$$E_4(\tau) = 1 + 240 \sum_{n\geq 1} \sigma_3(n) q^n \in \mathbb{Z}[[q]], \tag{4.10}$$

$$E_6(\tau) = 1 - 504 \sum_{n\geq 1} \sigma_5(n) q^n \in \mathbb{Z}[[q]]. \tag{4.11}$$

En general, $E_k(\tau) \in \mathbb{Q}[[q]]$, però $E_k(\tau) \notin \mathbb{Z}[[q]]$; per exemple,

$$E_{12}(\tau) = 1 + \frac{65520}{691} \sum_{n\geq 1} \sigma_{11}(n) q^n. \tag{4.12}$$

Per a $k \geq 2$, parell, la sèrie $E_k(\tau)$ és convergent en $\mathcal{H}$ i, per a $k \geq 4$, defineix una forma modular de pes $k$ per al grup $\mathbf{PSL}(2,\mathbb{Z})$, no parabòlica. En particular, per a $k \geq 4$, parell, és $M_k \neq (0)$. En canvi, per a $k = 2$, malgrat que la sèrie és convergent i que, d'acord amb la definició que hem donat, se satisfà la llei de transformació $E_2(\tau + 1) = E_2(\tau)$, $E_2$ no és una forma modular de pes 2, perquè se satisfà la llei de transformació

$$E_2\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^2 E_2(\tau) + \frac{12}{2\pi i} c(c\tau + d), \tag{4.13}$$

per a $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{SL}(2,\mathbb{Z})$, que té el sumand extra $\dfrac{12}{2\pi i} c(c\tau + d)$.

Si apliquem la fórmula (4.7) a les sèries d'Eisenstein $E_4(\tau)$ i $E_6(\tau)$, obtenim que $E_4(\tau)$ només té un zero, i és simple, en els punts de l'òrbita de $\tau = \rho$; i que $E_6(\tau)$ només té un zero, i és simple, en els punts de l'òrbita de $\tau = i$.

Un primer exemple, i el més important, de forma modular parabòlica el proporciona la funció $\Delta(\tau)$, que es pot definir per

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

Escrivim els primers termes del desenvolupament de Fourier de $\Delta(\tau)$:

$$\Delta(\tau) := q - 24q^2 + 252q^3 + \cdots \in \mathbb{Z}[[q]], \qquad q = q(\tau) = e^{2\pi i \tau}. \tag{4.14}$$

La funció $\Delta$ és una forma modular de pes 12, i no nul·la; i, de nou a partir de (4.7), només té un zero, i és simple, en els punts de l'òrbita de $\tau = \infty$; és, doncs, una forma parabòlica de pes 12.

Com a exemple important de funció modular de pes zero i no constant, tenim l'invariant modular $j(\tau)$; es pot definir com

$$j(\tau) := \frac{E_4(\tau)^3}{\Delta(\tau)}. \tag{4.15}$$

Escrivim els primers termes del desenvolupament de Fourier de $j(\tau)$:

$$j(\tau) := q^{-1} + 744 + 196884q + \cdots \in \mathbb{Z}[[q]], \qquad q = q(\tau) = e^{2\pi i\tau}. \tag{4.16}$$

Com que la funció $j$ és quocient de dues formes modulars del mateix pes, és una funció modular de pes zero; és holomorfa en $\mathcal{H}$, només té un zero, i és triple, en els punts de l'òrbita de $\tau = \rho$, i només té un pol, i és simple, en els punts de l'òrbita de $\tau = \infty$. Per la seva importància, citem el resultat següent, que es pot obtenir com a conseqüència de la proposició que establirem a continuació.

**4.3.2 Corol·lari.** *El cos $\mathbb{C}(j)$ és el cos de les funcions modulars de pes zero.* □

Aquests exemples d'aplicació de la fórmula (4.7) es poden dur més enllà; s'obté el resultat següent.

**4.3.3 Proposició.** *Sigui $k \geq 4$ un nombre parell. Existeixen nombres enters $m \geq 0$, $\delta \in \{0,1,2\}$, $\varepsilon \in \{0,1\}$, únics tals que $k = 12m + 4\delta + 6\varepsilon$. L'espai vectorial $M_k$ és de dimensió $m+1$, i tota forma modular $f \in M_k$ es pot escriure de manera única com un producte*

$$f(\tau) = \Delta(\tau)^m E_4(\tau)^\delta E_6(\tau)^\varepsilon \tilde{f}(j(\tau)), \tag{4.17}$$

*on $\tilde{f}(j)$ és un polinomi de grau menor o igual que $m$, el coeficient de $j^m$ del qual és igual al terme constant del desenvolupament de $f(\tau)$ en sèrie de Fourier (de potències de $q = e^{2\pi i\tau}$). Més generalment, si tots els coeficients de Fourier de $f(\tau)$ pertanyen a un mateix subanell $K \subseteq \mathbb{C}$, llavors $\tilde{f}(j) \in K[j]$.*

Demostració. La demostració de l'existència i la unicitat de $m$, $\delta$ i $\varepsilon$ és immediata a partir de la classe de congruència de $k$ mòdul 12. D'altra banda, si $f \in M_k$ és una forma parabòlica no nul·la, llavors

és divisible per $\Delta$ de manera que $f\Delta^{-1} \in M_{k-12}$ i, per tant, $S_k = \Delta M_{k-12}$. Com que, per a $k \neq 2$, parell, $S_k$ és de codimensió 1 en $M_k$, i $E_k$ en genera un suplementari, tenim que $\dim M_k = \dim S_k + 1 = \dim M_{k-12} + 1$. Així, tant la dimensió de $M_k$ com el valor de $m$ augmenten d'una unitat quan $k$ augmenta de 12 unitats. El resultat sobre les dimensions es redueix, doncs, a veure que $M_0 = \mathbb{C}$, i que $M_k = E_k\mathbb{C}$, per a $k = 4$, 6, 8, 10, i 14; equivalentment, que, per a aquests valors de $k$, és $\dim S_k = 0$. Però la fórmula (4.7) ens diu que qualsevol forma parabòlica no nul·la és de pes més gran o igual que 12, i diferent de 14, perquè $v_\infty(f) \geq 1$ i $v_P(f) \geq 0$, per a tot $P$.

Resta veure la descomposició. Sigui, doncs, $f \in M_k$ una forma modular no nul·la. De nou el fet que tots els nombres $v_P(f)$ siguin enters no negatius obliga que $f$ tingui un zero d'ordre més gran o igual que $\delta$ en $\tau = \rho$ i un zero d'ordre més gran o igual que $\varepsilon$ en $\tau = i$; per tant, $f$ és divisible pel producte $E_4^\delta E_6^\varepsilon$ i el quocient és una forma modular de pes $12m$. Si dividim aquesta nova forma per $\Delta^m$, resulta una funció modular de pes 0 (meromorfa) que té pols, com a màxim, en $\tau = \infty$, i d'ordre menor o igual que $m$. Per tant, és un polinomi en $j$, de grau menor o igual que $m$ i de coeficient del monomi de grau $m$ el mateix que el coeficient del terme constant del desenvolupament de Fourier de $f$, perquè la divisió pel producte $E_4^\delta E_6^\varepsilon$ no fa variar aquest coeficient del desenvolupament, i la divisió per $\Delta^m$ el deixa com a coeficient de $q^{-m}$. $\square$

Aquesta proposició ens ensenya a associar, a cada forma modular $f \in M_k$, un polinomi $\tilde{f}(j) \in K[j]$, on $K \subseteq \mathbb{C}$ és l'anell generat pels coeficients de Fourier de $f(\tau)$.

Per exemple, podem considerar, per a tot nombre enter parell $k \geq 4$, la forma modular $E_k(\tau)$ i el seu polinomi associat $\tilde{E}_k(j) \in \mathbb{Q}[j]$. Notem que $\tilde{E}_4(j)$, $\tilde{E}_6(j) \in \mathbb{Z}[j]$ i que, de fet, $\tilde{E}_4(j) = \tilde{E}_6(j) = 1$.

**4.3.4 Corol·lari.** *L'àlgebra graduada de les formes modulars és isomorfa a l'anell de polinomis en dues indeterminades $E_4$, $E_6$; és a dir, $\bigoplus_{k\geq 0} M_k \simeq \mathbb{C}[E_4E_6]$, on $E_4$ és de grau 4 i $E_6$ de grau 6.*

Demostració. En efecte, si en la demostració anterior se substitueix $j$ per $\dfrac{E_4^3}{\Delta}$ en el polinomi $\tilde{f}(j)$, i després es multiplica tot per $\Delta^m$,

s'obté una expressió de $f$ com un polinomi en $E_4$, $E_6$ i $\Delta = \dfrac{E_4^3 - E_6^2}{1728}$; és a dir, com un polinomi en $E_4$, $E_6$. I la unicitat de l'expressió (4.17) equival a la independència algebraica de $E_4$ i $E_6$. □

**4.3.5 Observació.** Sigui $p \geq 5$ un nombre primer, posem $k := p-1$, i escrivim $k$ en la forma $k = 12m+4\delta+6\varepsilon$, com en la proposició (4.3.3). El valor $\delta = 2$ no és possible, perquè seria $p = k+1 = 12m+6\varepsilon+9 \equiv 0 \pmod 3$. De les fórmules de Deuring (4.3) es dedueix immediatament que el grau del polinomi $ss_p(j) \in \mathbb{F}_p[j]$ és exactament $m + \delta + \varepsilon$ i que $ss_p(j)$ és divisible per $j^\delta(j - 1728)^\varepsilon$. [K-Z] proporciona una demostració alternativa d'aquest fet.

Ara disposem de les eines necessàries per a definir tres dels polinomis que cerquem. Un d'ells és el polinomi $\tilde{E}_k(j)$, associat a la sèrie d'Eisenstein $E_k(\tau)$, per a tot valor parell de $k \geq 4$; en particular, associat a un nombre primer $p \geq 5$, el polinomi $\tilde{E}_{p-1}(j)$. La definició de dos polinomis més és conseqüència del resultat següent.

**4.3.6 Proposició.** *Sigui $k \geq 4$, parell, i escrivim $k = 12m+4\delta+6\varepsilon$, amb $m \geq 0$, $\delta \in \{0,1,2\}$, i $\varepsilon \in \{0,1\}$. Definim el polinomi*

$$H_k(E_4, E_6) \in \mathbb{Z}[E_4, E_6], \tag{4.18}$$

*com el coeficient de $X^k$ en el polinomi*

$$(1 - 3E_4X^4 + 2E_6X^6)^{k/2} \in \mathbb{Z}[E_4, E_6][X],$$

*i el polinomi*

$$G_k(E_4, E_6) \in \mathbb{Z}[1/2][E_4, E_6], \tag{4.19}$$

*com el coeficient de $X^k$ en la sèrie de potències*

$$(1 - 3E_4X^4 + 2E_6X^6)^{-1/2} \in \mathbb{Z}[1/2][E_4, E_6][[X]].$$

*Llavors, $H_k(E_4(\tau), E_6(\tau))$, $G_k(E_4(\tau), E_6(\tau))$ són formes modulars de pes $k$.*

Demostració. Podem substituir $T$ per $-3E_4X^4 + 2E_6X^6$ en el polinomi $(1 + T)^{k/2} \in \mathbb{Z}[T]$ i en la sèrie $(1 + T)^{-1/2} \in \mathbb{Z}[1/2][[T]]$; obtenim que

$$(1 - 3E_4X^4 + 2E_6X^6)^{k/2} \in \mathbb{Z}[E_4, E_6][X]$$

i que

$$(1 - 3E_4X^4 + 2E_6X^6)^{-1/2} \in \mathbb{Z}[1/2][E_4, E_6][[X]].$$

Donem pesos 4 a $E_4$, 6 a $E_6$, i $-1$ a $X$; llavors, $1 - 3E_4X^4 + 2E_6X^6$ és un polinomi isobàric de pes 0. Per tant, el polinomi i la sèrie

$$(1 - 3E_4X^4 + 2E_6X^6)^{k/2}, \qquad (1 - 3E_4X^4 + 2E_6X^6)^{-1/2},$$

són isobàrics de pes 0 i els coeficients respectius de $X^k$,

$$H_k(E_4, E_6) \in \mathbb{Z}[E_4, E_6], \qquad G_k(E_4, E_6) \in \mathbb{Z}[1/2][E_4, E_6],$$

són polinomis isobàrics de pes $k$ en $E_4$, $E_6$. Això ens diu que

$$H_k(\tau) := H_k(E_4(\tau), E_6(\tau)) \qquad \text{i} \qquad G_k(\tau) := G_k(E_4(\tau), E_6(\tau))$$

són formes modulars de pes $k$. □

**4.3.7 Definició.** Per a tot $k \geq 4$, parell, escriurem $\tilde{E}_k(j)$, $\tilde{H}_k(j)$, $\tilde{G}_k(j)$, els polinomis associats a les formes modulars de pes $k$

$$E_k(\tau), \qquad H_k(\tau), \qquad G_k(\tau).$$

En particular, per a $p \geq 5$, primer, obtenim els polinomis $\tilde{E}_{p-1}(j)$, $\tilde{H}_{p-1}(j)$, i $\tilde{G}_{p-1}(j)$.

Per a la definició del quart dels polinomis que cerquem, cal parlar de la derivació de formes modulars. La derivació de funcions modulars o de formes modulars no produeix, en general, ni funcions modulars ni formes modulars. Per exemple, se satisfan les relacions

$$\frac{1}{2\pi i} D(E_2, \tau) = \frac{E_2(\tau)^2 - E_4(\tau)}{12}, \tag{4.20}$$

$$\frac{1}{2\pi i} D(E_4, \tau) = \frac{E_2(\tau)E_4(\tau) - E_6(\tau)}{3}, \tag{4.21}$$

$$\frac{1}{2\pi i} D(E_6, \tau) = \frac{E_2(\tau)E_6(\tau) - E_4(\tau)^2}{2}, \tag{4.22}$$

$$\frac{1}{2\pi i} D(\Delta, \tau) = E_2(\tau)\Delta(\tau), \tag{4.23}$$

on $D := \dfrac{d}{d\tau}$ és la derivació habitual. Però es pot definir un operador de derivació de formes modulars que augmenta el pes en dues unitats.

**4.3.8 Proposició.** *L'assignació* $f \mapsto \vartheta_k(f, \cdot)$ *donada per*

$$\vartheta_k(f,\tau) := \frac{1}{2\pi i} D(f,\tau) - \frac{k}{12} E_2(\tau) f(\tau) \tag{4.24}$$

*defineix una aplicació* $\mathbb{C}$*-lineal* $\vartheta_k : M_k \longrightarrow M_{k+2}$ *tal que si* $g \in M_{k'}$*, llavors*

$$\vartheta_{k+k'}(fg,\tau) = \vartheta_k(f,\tau) g(\tau) + f(\tau)\vartheta_{k'}(g,\tau). \square$$

Notem que si $f_0(q)$ és el desenvolupament en sèrie de Fourier de $f$, és a dir, si $f_0(q)$ és la sèrie de potències tal que $f(\tau) = f_0(q(\tau))$, on $q(\tau) = e^{2\pi i \tau}$, llavors és $\dfrac{1}{2\pi i} D(f,\tau) = q(\tau) D(f_0, q(\tau))$.

**4.3.9 Proposició.** *Sigui* $k \geq 4$ *un nombre enter parell tal que* $k \not\equiv 2 \pmod 3$*. L'equació diferencial*

$$\vartheta_{k+2}\vartheta_k(F_k,\tau) = \frac{k(k+2)}{144} E_4(\tau) F_k(\tau) \tag{4.25}$$

*té una solució* $F_k \in M_k$*, única llevat de multiplicació per escalars, i no parabòlica.*

**4.3.10 Observació.** L'espai de solucions de l'equació diferencial és de dimensió 2, perquè es tracta d'una equació diferencial lineal homogènia d'ordre 2. La proposició assegura que la intersecció de l'espai de solucions amb $M_k$ és un espai de dimensió 1. D'altra banda, notem que si $k = p - 1$ per a un nombre primer $p \geq 5$, les condicions $k \geq 4$, $k$ parell i $k \not\equiv 2 \pmod 3$ se satisfan automàticament.

Obtindrem aquest resultat com a conseqüència del següent.

**4.3.11 Proposició.** *Sigui* $k \geq 4$ *un nombre enter parell tal que* $k \not\equiv 2 \pmod 3$*. L'assignació*

$$f \mapsto \phi_k(f) := \frac{\vartheta_{k+2}\vartheta_k f}{E_4}$$

*defineix un endomorfisme* $\phi_k : M_k \longrightarrow M_k$*, que diagonalitza en una base de vectors propis de valors propis* $\kappa_{k-12i}$*,* $0 \leq i \leq \dim M_k - 1$*, on* $\kappa_r := \dfrac{r(r+2)}{144}$*.*

DEMOSTRACIÓ. Si $k \geq 4$ és un nombre parell, i $k \not\equiv 2 \pmod 3$, llavors $k+4 \not\equiv 0 \pmod 3$, de manera que, en escriure $k+4 = 12m + 4\delta + 6\varepsilon$, amb $\delta \in \{0,1,2\}$, $\varepsilon \in \{0,1\}$, $m \in \mathbb{Z}$, resulta que $\delta \neq 0$. Per tant, tota forma modular de pes $k+4$ té un zero en $\tau = \rho$ i, en conseqüència, és el producte de $E_4$ per una forma modular de pes $k$. Això implica que podem considerar l'endomorfisme $\mathbb{C}$-lineal $\phi_k : M_k \longrightarrow M_k$ donat per $\phi_k(f) := \dfrac{\vartheta_{k+2}\vartheta_k f}{E_4}$. Ara, si $F_k \in M_k$, i si considerem el seu desenvolupament en sèrie de Fourier

$$F_k(\tau) = \sum_{n \geq 0} a_n q^n, \qquad q = e^{2\pi i \tau},$$

podem calcular el terme constant del desenvolupament en sèrie de Fourier de $\phi_k(F_k)$, que resulta ésser $\kappa_k a_0$, on $\kappa_k := \dfrac{k(k+2)}{144}$. Com a conseqüència, l'espai $S_k$ de les formes parabòliques és invariant per $\phi_k$ i, a més a més, en l'espai quocient $M_k/S_k$, que és de dimensió 1, $\phi_k$ indueix la multiplicació per $\kappa_k$. En particular, si $M_k$ és de dimensió 1, llavors $\kappa_k$ és un valor propi de $\phi_k$, i qualsevol funció no nul·la $F_k \in M_k$ és pròpia de valor propi $\kappa_k$ i, per tant, és una solució de l'equació diferencial, no parabòlica perquè en aquest cas és $S_k = (0)$.

Anem a provar, per inducció, que $M_k$ admet una base de funcions pròpies de valors propis $\kappa_{k-12i}$, $0 \leq i \leq m$, diferents. De la fórmula (4.23) es dedueix que $\vartheta_{12}(\Delta, \tau) = 0$, de manera que els operadors diferencials $\vartheta_k$ commuten amb la multiplicació per les potències de $\Delta(\tau)$; és a dir, se satisfà que $\vartheta_k(\Delta^i f, \tau) = \Delta(\tau)^i \vartheta_{k-12i}(f, \tau)$, per a $0 \leq i \leq m$ (notem que $k = 12m + 4(\delta - 1) + 6\varepsilon$). Així, si prenem una funció pròpia no nul·la $F_{k-12i} \in M_{k-12i}$ de valor propi $\kappa_{k-12i}$ per a $\phi_{k-12i}$, $1 \leq i \leq m$, resulta que el producte $F_{k-12i}\Delta^i \in M_k$ és funció pròpia no nul·la de $\phi_k$ de valor propi $\kappa_{k-12i} \neq \kappa_k$. Inductivament, obtenim una base de $S_k$ de funcions pròpies de $\phi_k$ de valors propis $\kappa_{k-12i}$, $1 \leq i \leq m$, diferents. Ara, com que en $M_k/S_k$, de dimensió 1, $\phi_k$ és una homotècia de raó $\kappa_k$ i en $S_k$, que és un subespai invariant per $\phi_k$, hi ha una base de funcions pròpies de valors propis diferents de $\kappa_k$, existeix una funció pròpia $F_k \in M_k$, $F_k \notin S_k$, de valor propi $\kappa_k$; és a dir, existeix una solució de l'equació diferencial en $M_k$, que és única llevat del producte per un factor escalar. □

Ara disposem de les eines necessàries per a definir el darrer dels quatre polinomis que cerquem.

**4.3.12 Definició.** Siguin $p \geq 5$ un nombre primer, posem $k := p-1$, i escrivim $k = 12m + 4\delta + 6\varepsilon$, amb $m \geq 0$, $\delta \in \{0,1,2\}$, $\varepsilon \in \{0,1\}$. Llavors, $k \not\equiv 2 \pmod 3$ i podem considerar la forma modular $F_k$, de pes $k = p-1$, solució de l'equació diferencial que proporciona la proposició **4.3.9**, normalitzada de manera que el coeficient constant del seu desenvolupament en sèrie de Fourier sigui $(-1)^m \binom{\frac{k-5}{6}}{m}$. I podem considerar el polinomi $\tilde{F}_{p-1}(j) \in \mathbb{C}[j]$ associat a la forma modular $F_{p-1}(\tau)$.

**4.3.13 Observació.** Notem que $\dfrac{k-5}{6}$ no és un nombre enter, perquè $k$ és parell; de manera que cal considerar

$$\binom{\frac{k-5}{6}}{m} := \frac{\frac{k-5}{6}\left(\frac{k-5}{6}-1\right)\cdots\left(\frac{k-5}{6}-m+1\right)}{m!}.$$

Un cop definits els polinomis $\tilde{E}_{p-1}(j)$, $\tilde{F}_{p-1}(j)$, $\tilde{G}_{p-1}(j)$, i $\tilde{H}_{p-1}(j)$, per a $p \geq 5$, primer, ja podem enunciar el primer dels resultats principals de l'article [K-Z].

**4.3.14 Teorema.** *Sigui $p \geq 5$ un nombre primer i posem $p-1 = 12m + 4\delta + 6\varepsilon$, amb $m \geq 0$, $\delta \in \{0,1\}$, i $\varepsilon \in \{0,1\}$. Sigui $\tilde{f}(j) \in \{\tilde{E}_{p-1}(j),\ \tilde{F}_{p-1}(j),\ \tilde{G}_{p-1}(j),\ \tilde{H}_{p-1}(j)\}$ un qualsevol dels polinomis que acabem de definir. Llavors, els coeficients de $\tilde{f}(j)$ són nombres racionals p-enters i se satisfan les congruències*

$$\begin{aligned}
\tilde{E}_{p-1}(j) &\equiv \tilde{F}_{p-1}(j) && \pmod p,\\
\tilde{G}_{p-1}(j) &\equiv \tilde{H}_{p-1}(j) && \pmod p,\\
\tilde{E}_{p-1}(j) &\equiv (-1)^{\delta+\varepsilon}\tilde{H}_{p-1}(j) && \pmod p,\\
ss_p(j) &\equiv j^{\delta}(j-1728)^{\varepsilon}\tilde{E}_{p-1}(j) && \pmod p.
\end{aligned}$$

Abans de demostrar el teorema, diguem que en [K-Z] es proporcionen exemples concrets per a $k = 28$. Notem que els coeficients no són enters, llevat dels de $\tilde{H}_{28}(j)$, així com també la simplicitat creixent dels coeficients dels polinomis, amb l'ordenació donada $E$, $G$, $H$, $F$.

$$\tilde{E}_{28}(j) = j^2 - \frac{5699870640000}{3392780147}j + \frac{1180807372800000}{3392780147},$$
$$\tilde{G}_{28}(j) = \frac{3304503}{2048}j^2 - \frac{8394435}{4}j + 176359680,$$
$$\tilde{H}_{28}(j) = 6608316j^2 - 23558895360j - 1434705592320,$$
$$\tilde{F}_{28}(j) = \frac{391}{72}j^2 - 11424j + 4644864.$$

I, per a $p = 29$, [K-Z] fan notar les congruències

$$\tilde{E}_{28}(j) \equiv \tilde{F}_{28}(j) \equiv -\tilde{G}_{28}(j) \equiv -\tilde{H}_{28}(j)$$
$$\equiv j^2 + 2j + 21 \equiv \frac{ss_p(j)}{j} \pmod{p}.$$

A fi de provar el teorema, convé començar per recordar el criteri per a decidir si una corba el·líptica sobre un cos finit és o no supersingular.

**4.3.15 Proposició.** *Siguin $p \geq 5$ un nombre primer, $q = p^r$, $r \geq 1$, $E$ la corba el·líptica sobre $\mathbb{F}_q$ donada per una equació $y^2 = f(x)$, on $f \in \mathbb{F}_q[x]$ és un polinomi de grau 3, i sigui $a_p \in \mathbb{F}_q$ el coeficient de $x^{p-1}$ del polinomi $f(x)^{\frac{p-1}{2}}$. Llavors, $\#E(\mathbb{F}_q) \equiv 1 - N_{\mathbb{F}_q|\mathbb{F}_p}(a_p)$ (mod $p$). La corba el·líptica $E$ és supersingular si, i només si, $a_p = 0$.*

Demostració. Donat un element qualsevol $z \in \mathbb{F}_q$, tenim que $z^{\frac{q-1}{2}} \in \{0, 1, -1\}$, segons que sigui $z = 0$, $z \in \mathbb{F}_q^{*\,2}$, o bé $z \in \mathbb{F}_q^* - \mathbb{F}_q^{*\,2}$; per tant, si escrivim $\left(\frac{z}{p}\right) \in \{0, 1, -1\} \subseteq \mathbb{Z}$ l'únic nombre enter tal que $\left(\frac{z}{p}\right) \equiv z^{\frac{q-1}{2}} \pmod{p}$, tenim que el nombre de solucions $(y, z)$ de l'equació $y^2 = z$ en $\mathbb{F}_q \times \mathbb{F}_q$ és exactament $1 + \left(\frac{z}{p}\right)$. Per tant, per a tot $x \in \mathbb{F}_q$, el nombre de solucions de $y^2 = f(x)$ és $1 + \left(\frac{f(x)}{p}\right)$; així, en tenir en compte el punt de l'infinit, obtenim que

$$\#E(\mathbb{F}_q) \equiv 1 + \sum_{x \in \mathbb{F}_q} (1 + f(x)^{\frac{q-1}{2}}) \pmod{p}.$$

Ara bé,

$$\sum_{x\in\mathbb{F}_q} x^j = \begin{cases} -1, & \text{si } q-1 \text{ divideix } j \neq 0, \\ 0, & \text{altrament;} \end{cases}$$

per tant, per a $0 \leq j \leq 3\dfrac{q-1}{2}$, és

$$\sum_{x\in\mathbb{F}_q} x^j = \begin{cases} -1, & \text{si } j = q-1, \\ 0, & \text{altrament.} \end{cases}$$

Com a conseqüència, si $a_q \in \mathbb{F}_q$ és el coeficient de $x^{q-1}$ del polinomi $f(x)^{\frac{q-1}{2}}$, obtenim que $\#E(\mathbb{F}_q) = 1 - a_q \in \mathbb{F}_q$, de manera que $\#E(\mathbb{F}_q) \equiv 1 - a_q \pmod{p}$, perquè la igualtat anterior diu, en particular, que $a_q \in \mathbb{F}_p$.

Ara, tinguem en compte que $\dfrac{q-1}{2} = \dfrac{p-1}{2}(1+p+p^2+\cdots+p^{r-1})$; si designem per $f^{(p^j)}(x)$ el polinomi que s'obté de $f(x)$ en elevar a la potència $p^j$ els coeficients de $f(x)$, obtenim la igualtat

$$f(x)^{\frac{q-1}{2}} = f(x)^{\frac{p-1}{2}} \cdot f^{(p)}(x^p)^{\frac{p-1}{2}} \cdots f^{(p^{r-1})}(x^{p^{r-1}})^{\frac{p-1}{2}},$$

de manera que si $a_p$ és el coeficient de $x^{p-1}$ del polinomi $f(x)^{\frac{p-1}{2}}$, tenim que

$$a_q = a_p^{1+p+p^2+\cdots+p^{r-1}} = N_{\mathbb{F}_q|\mathbb{F}_p}(a_p).$$

Per tant, $\#E(\mathbb{F}_q) \equiv 1 - a_q = 1 - N_{\mathbb{F}_q|\mathbb{F}_p}(a_p) \pmod{p}$, com calia veure.

Vegem, finalment, la qüestió relativa a la supersingularitat de la corba $E$. Notem que si $a_p = 0$, llavors $\#E(\mathbb{F}_{p^r}) \equiv 1 \not\equiv 0 \pmod{p}$, per a tot $r \geq 1$; per tant, $E$ no té punts d'ordre múltiple de $p$ sobre cap cos $\mathbb{F}_{q^r}$; o sigui, no té $p$-torsió sobre $\overline{\mathbb{F}}_p$. I si $a_p \neq 0$, llavors per a $n$ múltiple de l'ordre de l'element $N_{\mathbb{F}_q|\mathbb{F}_p}(a_p) \in \mathbb{F}_p^*$, és $\#E(\mathbb{F}_{q^n}) \equiv 1 - N_{\mathbb{F}_q|\mathbb{F}_p}(a_p)^n \equiv 0 \pmod{p}$, de manera que $E$ té $p$-torsió sobre el cos $\mathbb{F}_{q^n}$. □

Podem procedir ara a la demostració del teorema **4.3.14** per al cas del polinomi $\tilde{H}_{p-1}(j)$; més concretament, provarem el resultat següent.

**4.3.16 Proposició.** *Sigui $p \geq 5$ un nombre primer i posem $p - 1 = 12m + 4\delta + 6\varepsilon$, amb $m \geq 0$, $\delta \in \{0, 1\}$, i $\varepsilon \in \{0, 1\}$. Els coeficients de*

*$\tilde{H}_{p-1}(j)$ són nombres enters i se satisfà la congruència*

$$ss_p(j) \equiv (-1)^{\delta+\varepsilon} j^\delta (j-1728)^\varepsilon \tilde{H}_{p-1}(j) \pmod{p}.$$

Demostració. Considerem l'àlgebra de polinomis $\mathbb{Z}[x, Q, R]$ en tres indeterminades $x$, $Q$, $R$, i donem pesos 2 a $x$, 4 a $Q$ i 6 a $R$. Llavors, $x^3 - 3Qx + 2R$ és un polinomi isobàric de pes 6, de manera que $(x^3 - 3Qx + 2R)^{\frac{p-1}{2}}$ és isobàric de pes $3(p-1)$ i, en conseqüència, el coeficient de $x^{p-1}$ d'aquest polinomi, que podem denotar com $H_{p-1}(Q, R) \in \mathbb{Z}[Q, R]$, és un polinomi isobàric de pes $p-1$.

Si canviem $x$ per $\dfrac{1}{X^2}$ i ho multipliquem tot per $X^6$, el polinomi $x^3 - 3Qx + 2R$ es transforma en el polinomi $1 - 3E_4X^4 + 2E_6X^6$ que hem usat en la definició de la forma modular $H_{p-1}(\tau)$ (cf. la proposició **4.3.6**); d'aquí obtenim que

$$H_{p-1}(E_4(\tau), E_6(\tau)) = H_{p-1}(\tau).$$

I, com hem fet en la proposició **4.3.3**, però ara en $\mathbb{Z}[Q, R]$, podem escriure aquest polinomi en la forma

$$H_{p-1}(Q, R) = \Delta^m Q^\delta R^\varepsilon \tilde{H}_{p-1}(j),$$

per a un cert polinomi $\tilde{H}_{p-1} \in \mathbb{Z}[j]$, on ara es posa

$$\Delta := \frac{Q^3 - R^2}{1728}, \qquad j := \frac{Q^3}{\Delta},$$

i on $m = \left[\dfrac{p}{12}\right]$,

$$\delta = \begin{cases} 0, & \text{si } p \equiv 1 \pmod 3, \\ 1, & \text{si } p \equiv 2 \pmod 3, \end{cases} \qquad \varepsilon = \begin{cases} 0, & \text{si } p \equiv 1 \pmod 4, \\ 1, & \text{si } p \equiv 3 \pmod 4, \end{cases}$$

són els nombres definits per la igualtat $p - 1 = 12m + 4\delta + 6\varepsilon$. Notem que se satisfà la igualtat $m = \left[\dfrac{p}{12}\right]$ perquè $p - 1 \not\equiv 2 \pmod 3$.

Sigui, ara, $E$ una corba el·líptica sobre $\overline{\mathbb{F}}_p$. Com que $p \geq 5$, $E$ és isomorfa a la corba donada per una equació de Weierstraß de la forma $y^2 = x^3 - 3Q(E)x + 2R(E)$, amb $Q(E)$, $R(E) \in \overline{\mathbb{F}}_p$. L'invariant $j$ de la corba $E$, per a aquesta equació, és donat per $j(E) = \dfrac{Q(E)^3}{\Delta(E)}$,

on $\Delta(E) = \dfrac{Q(E)^3 - R(E)^2}{1728}$. Per tant, $j(E) = 0$ si, i només si, $Q(E) = 0$, i $j(E) = 1728$ si, i només si, $R(E) = 0$.

D'altra banda, el coeficient de $x^{p-1}$ en $(x^3 - 3Q(E)x + 2R(E))^{\frac{p-1}{2}}$ és

$$H_{p-1}(Q(E), R(E)) = \Delta(E)^m Q(E)^\delta R(E)^\varepsilon \tilde{H}_{p-1}(j(E));$$

la caracterització de les corbes el·líptiques supersingulars donada en la proposició **4.3.15** ens assegura que $E$ és supersingular si, i només si,

$$j(E)^\delta (j(E) - 1728)^\varepsilon \tilde{H}_{p-1}(j(E)) = 0.$$

Per tant, $ss_p(j)$ divideix el polinomi $j^\delta (j - 1728)^\varepsilon \tilde{H}_{p-1}(j) \in \mathbb{F}_p[j]$ i, a més a més, $ss_p(j)$ té les mateixes arrels que $j^\delta (j - 1728)^\varepsilon \tilde{H}_{p-1}(j)$. Com que, per definició, el polinomi $ss_p(j)$ no té arrels múltiples, si veiem que $j^\delta (j - 1728)^\varepsilon \tilde{H}_{p-1}(j)$ no té arrels múltiples, tindrem que els dos polinomis coincideixen llevat d'un factor constant, i només restarà calcular aquesta constant.

En aquest punt, en [K-Z] s'observa que el resultat (abans de la determinació de la constant) es dedueix immediatament de la fórmula de Deuring (4.1) sobre el grau de $ss_p(j)$,

$$\deg(ss_p(j)) = m + \delta + \varepsilon;$$

però se'n dóna una altra demostració. En efecte; és suficient provar que totes les arrels del polinomi $j^\delta (j - 1728)^\varepsilon \tilde{H}_{p-1}(j)$ són simples.

- Cas $j = 0$.

Notem que, en $\mathbb{Z}[x, Q, R]$, se satisfà una identitat de la forma

$$(x^3 - 3Qx + 2R)^{\frac{p-1}{2}} = (x^3 + 2R)^{\frac{p-1}{2}} - 3\frac{p-1}{2} Qx (x^3 + 2R)^{\frac{p-3}{2}} + O(Q^2),$$

on $O(Q^2)$ indica un polinomi múltiple de $Q^2$. El càlcul del coeficient de $x^{p-1}$ proporciona que

$$H_{p-1}(Q, R) = \binom{\frac{p-1}{2}}{\frac{p-1}{3}} (2R)^{\frac{p-1}{6}} + O(Q),$$

si $p \equiv 1 \pmod 3$, i que

$$H_{p-1}(Q, R) = -3\frac{p-1}{2} \binom{\frac{p-3}{2}}{\frac{p-2}{3}} (2R)^{\frac{p-5}{6}} Q + O(Q^2),$$

si $p \equiv 2 \pmod 3$. Per tant, per a $R \neq 0$, $Q = 0$ no n'és arrel, si $p \equiv 1 \pmod 3$, i n'és una arrel simple si $p \equiv 2 \pmod 3$.

Ara bé, per a una corba el·líptica $E$, tenim que $\Delta(E) \neq 0$, de manera que si $Q(E) = 0$, llavors $R(E) \neq 0$; i, a més a més, $j(E) = 0$ si, i només si, $Q(E) = 0$. Així, $j = 0$ és una arrel de $\tilde{H}_{p-1}(j)$ si, i només si, $Q = 0$ és una arrel de $H_{p-1}(Q, R)$; però això només succeeix per a $p \equiv 2 \pmod 3$ i, en aquest cas, és $\delta = 1$, de manera que el polinomi $\tilde{H}_{p-1}(j) \in \mathbb{F}_p[j]$ no s'anul·la en cap dels dos casos per a $j = j(E) = 0$ i, si $j = 0$ és arrel de $j^\delta(j - 1728)^\varepsilon \tilde{H}_{p-1}(j)$, n'és arrel simple.

- Cas $j = 1728$.

En l'article [K-Z], només es diu que es fa de manera similar. Fet l'exercici, resulta que en $\mathbb{Z}[x, Q, R]$ se satisfà una identitat de la forma

$$(x^3 - 3Qx + 2R)^{\frac{p-1}{2}} = (x^3 - 3Qx)^{\frac{p-1}{2}} + 2\frac{p-1}{2}R(x^3 - 3Qx)^{\frac{p-3}{2}} + O(R^2),$$

on $O(R^2)$ indica un polinomi múltiple de $R^2$. El càlcul del coeficient de $x^{p-1}$ proporciona que

$$H_{p-1}(Q, R) = \binom{\frac{p-1}{2}}{\frac{p-1}{4}} (-3Q)^{\frac{p-1}{4}} + O(R),$$

si $p \equiv 1 \pmod 4$, i que

$$H_{p-1}(Q, R) = 2\frac{p-1}{2} \binom{\frac{p-3}{2}}{\frac{p+1}{4}} (-3Q)^{\frac{p-7}{4}} R + O(R^2),$$

si $p \equiv 3 \pmod 4$. Per tant, per a $Q \neq 0$, $R = 0$ no n'és arrel, si $p \equiv 1 \pmod 4$, i n'és una arrel simple si $p \equiv 3 \pmod 4$.

De nou, per a una corba el·líptica $E$, tenim que $\Delta(E) \neq 0$, de manera que si $R(E) = 0$, llavors $Q(E) \neq 0$; i, a més a més, $j(E) = 1728$ si, i només si, $R(E) = 0$. Així, $j = 1728$ és una arrel de $\tilde{H}_{p-1}(j)$ si, i només si, $R = 0$ és una arrel de $H_{p-1}(Q, R)$; però això només succeeix per a $p \equiv 3 \pmod 4$ i, en aquest cas, és $\varepsilon = 1$, de manera que el polinomi $\tilde{H}_{p-1}(j) \in \mathbb{F}_p[j]$ no s'anul·la en cap dels dos casos per a $j = j(E) = 1728$ i, si $j = 1728$ és arrel de $j^\delta(j - 1728)^\varepsilon \tilde{H}_{p-1}(j)$, n'és arrel simple.

• Cas $j \neq 0$, 1728.

Més endavant (cf. el teorema **4.5.10**, a) veurem que el polinomi $\tilde{H}_{p-1}(j)$ satisfà una equació diferencial lineal de segon ordre de coeficients polinòmics i coeficient dominant el polinomi $j(j-1728)$. Això implica que qualsevol arrel comuna diferent de $j = 0$ i de $j = 1728$ en $\overline{\mathbb{F}}_p$ de $\tilde{H}_{p-1}(j)$ i el seu polinomi derivat també ho seria del derivat segon i, per inducció, de tots els derivats successius; per tant, obtindríem un zero de multiplicitat infinita, contradicció. Notem que l'argument també és vàlid en el nostre cas, en què la característica és $p$, perquè el polinomi no és un polinomi en $j^p$, fet trivial perquè el polinomi és de grau $m = \left[\dfrac{p-1}{12}\right] < p$.

Per a acabar la demostració de la proposició, resta determinar la constant de proporcionalitat i veure que és $(-1)^{\delta+\varepsilon}$; és a dir, cal veure que el coeficient del monomi de grau màxim de $\tilde{H}_{p-1}(j)$ mòdul $p$ és $(-1)^{\delta+\varepsilon}$.

El coeficient del terme de grau màxim del polinomi $\tilde{f}(j) \in \mathbb{C}[j]$ associat a una forma modular no nul·la $f(\tau) \in M_k$ coincideix amb el terme constant del desenvolupament de Fourier de $f(\tau)$ (cf. la proposició **4.3.3**); en particular, el coeficient dominant del polinomi $\tilde{f}(j) \in \mathbb{C}[j]$ associat a un polinomi isobàric de pes $k$, $f(E_4, E_6) \in \mathbb{C}[E_4, E_6]$, s'obté en substituir $E_4 = E_6 = 1$ en el polinomi $f(E_4, E_6)$. Per tant, cal calcular $H_{p-1}(1,1)$ i reduir mòdul $p$. Notem que $E_4 = E_6 = 1$ no correspon a cap corba el·líptica $E$, perquè seria $\Delta(E) = 0$; però no hi ha cap inconvenient a substituir les indeterminades pels nombres que vulguem.

Ja hem vist que $H_{p-1}(Q, R)$ és el coeficient de $x^{p-1}$ del polinomi $(x^3 - 3Qx + 2R)^{\frac{p-1}{2}} \in \mathbb{Z}[x, Q, R]$; o sigui, el coeficient de $X^{p-1}$ del polinomi $(1 - 3QX^4 + 2RX^6)^{\frac{p-1}{2}} \in \mathbb{Z}[X, Q, R]$. Per tant, $H_{p-1}(1,1)$ és el coeficient de $X^{p-1}$ del polinomi $(1 - 3X^4 + 2X^6)^{\frac{p-1}{2}} \in \mathbb{Z}[X]$.

Ara bé, com que $1-3X^4+2X^6=(1-X^2)^2(1+2X^2)$, tenim que

$$\begin{aligned}
&(1-3X^4+2X^6)^{\frac{p-1}{2}}\\
=&(1-X^2)^{p-1}(1+2X^2)^{\frac{p-1}{2}}\\
=&\frac{(1-X^2)^p}{1-X^2}((1+2X^2)^{\frac{p-1}{2}}-3^{\frac{p-1}{2}}+3^{\frac{p-1}{2}})\\
\equiv&\frac{1-X^{2p}}{1-X^2}((1+2X^2)^{\frac{p-1}{2}}-3^{\frac{p-1}{2}}+3^{\frac{p-1}{2}}) \pmod p\\
=&(1-X^{2p})\frac{(1+2X^2)^{\frac{p-1}{2}}-3^{\frac{p-1}{2}}}{1-X^2}+\left(\frac{3}{p}\right)\frac{1-X^{2p}}{1-X^2},
\end{aligned}$$

ja que, d'una banda, $\left(\frac{3}{p}\right)\equiv 3^{\frac{p-1}{2}} \pmod p$ i, de l'altra, els polinomis $(1+2X^2)^{\frac{p-1}{2}}-3^{\frac{p-1}{2}}$ i $1-X^{2p}$ són divisibles pel polinomi $1-X^2$. A més a més, el quocient

$$\frac{(1+2X^2)^{\frac{p-1}{2}}-3^{\frac{p-1}{2}}}{1-X^2}$$

és un polinomi de grau $p-3$, de manera que el polinomi

$$(1-X^{2p})\frac{(1+2X^2)^{\frac{p-1}{2}}-3^{\frac{p-1}{2}}}{1-X^2}$$

no té monomis de grau $p-1$; com que

$$\frac{1-X^{2p}}{1-X^2}=1+X^2+X^4+\cdots+X^{2p-2},$$

obtenim que per al coeficient del monomi de grau $p-1$ del polinomi

$$\left(\frac{3}{p}\right)\frac{1-X^{2p}}{1-X^2}$$

se satisfà la congruència

$$H_{p-1}(1,1)\equiv\left(\frac{3}{p}\right)=(-1)^{\delta+\varepsilon} \pmod p,$$

com calia veure. □

A partir d'aquest resultat, no és gaire complicat demostrar el teorema **4.3.14** per al polinomi $\tilde{G}_{p-1}(j)$; ho fem en la forma següent.

**4.3.17 Proposició.** *Sigui $p \geq 5$ un nombre primer. Els coeficients de $\tilde{G}_{p-1}(j)$ són nombres racionals p-enters i se satisfà la congruència*

$$\tilde{G}_{p-1}(j) \equiv \tilde{H}_{p-1}(j) \pmod{p}.$$

Demostració. Recordem que $H_{p-1}(E_4, E_6)$ i $G_{p-1}(E_4, E_6)$ són els coeficients de $X^{p-1}$ en el polinomi $(1-3E_4X^4+2E_6X^6)^{\frac{p-1}{2}}$ i en la sèrie $(1-3E_4X^4+2E_6X^6)^{\frac{-1}{2}}$, respectivament. Ara bé, com a sèries de $\mathbb{Z}[1/2][E_4, E_6][[X]]$, se satisfà que

$$\begin{aligned}\frac{(1-3E_4X^4+2E_6X^6)^{\frac{p-1}{2}}}{(1-3E_4X^4+2E_6X^6)^{\frac{-1}{2}}} &= (1-3E_4X^4+2E_6X^6)^{\frac{p}{2}} \\ &\equiv 1+O(X^p) \pmod{p},\end{aligned}$$

perquè la sèrie $(1+T)^{\frac{p}{2}}$ té els seus coeficients en $\mathbb{Z}[1/2]$ i els coeficients dels termes de grau $k$, $1 \leq k \leq p-1$, són divisibles per $p$.

En conseqüència, les dues sèries

$$(1-3E_4X^4+2E_6X^6)^{\frac{p-1}{2}}, \qquad (1-3E_4X^4+2E_6X^6)^{\frac{-1}{2}}$$

tenen, mòdul $p$, el mateix coeficient de $X^{p-1}$; és a dir, se satisfà la congruència $H_{p-1}(E_4, E_6) \equiv G_{p-1}(E_4, E_6) \pmod{p}$ i, per tant, se satisfà la congruència $\tilde{G}_{p-1}(j) \equiv \tilde{H}_{p-1}(j) \pmod{p}$ que calia provar. □

La demostració del teorema **4.3.14** per al polinomi $\tilde{E}_{p-1}(j)$ s'obté en el resultat següent.

**4.3.18 Proposició.** *Sigui $p \geq 5$ un nombre primer i posem $p-1 = 12m+4\delta+6\varepsilon$, amb $m \geq 0$, $\delta \in \{0,1\}$, i $\varepsilon \in \{0,1\}$. Els coeficients de $\tilde{E}_{p-1}(j)$ són nombres racionals p-enters i se satisfà la congruència*

$$\tilde{E}_{p-1}(j) \equiv (-1)^{\delta+\varepsilon}\tilde{G}_{p-1}(j) \pmod{p}.$$

Demostració. Sigui $E_{|\mathbb{C}}$ la corba el·líptica associada al tor $\mathbb{C}/(\mathbb{Z}\tau+\mathbb{Z})$, d'invariant $j(\tau)$, per a la qual podem prendre l'equació de Weierstraß

$$y^2 = x^3 - 3E_4(\tau)x + 2E_6(\tau).$$

Aquesta corba admet la parametrització analítica $x = P(u)$, $y = \dfrac{-1}{2}D(P,u)$, on

$$P(u) := u^{-2} - \sum_{n\geq 4,\ \text{parell}} \frac{12^{n/2}B_n}{n(n-2)!}E_n(\tau)u^{n-2}$$

és una renormalització de la funció $\wp$ de Weierstraß a fi que els coeficients siguin racionals.

Per a tot nombre enter parell $k \geq 4$, la definició de la forma modular $G_k(\tau)$ s'ha fet de manera que

$$G_k(\tau) = \operatorname*{Res}_{X=0} \frac{dX}{X^{k+1}\sqrt{1-3E_4(\tau)X^4+2E_6(\tau)X^6}}.$$

El canvi de variable $X = P(u)^{-1/2} = u + \cdots$ proporciona la igualtat $G_k(\tau) = \operatorname{Res}_{u=0} P(u)^{\frac{k+1}{2}}du$, de manera que tenim

$$\begin{aligned} G_k(\tau) &= \operatorname*{Res}_{u=0} P(u)^{\frac{k+1}{2}}du \\ &= \operatorname*{Res}_{u=0}\left(1 - \sum_{n\geq 4,\text{parell}} \frac{12^{n/2}B_n}{n(n-2)!}E_n(\tau)u^n\right)^{\frac{k+1}{2}} \frac{du}{u^{k+1}} \\ &= \text{coeficient de } u^k \text{ en } \left(1 - \sum_{n\geq 4,\text{parell}} \frac{12^{n/2}B_n}{n(n-2)!}E_n(\tau)u^n\right)^{\frac{k+1}{2}}. \end{aligned}$$

Calculem, per a $k = p-1$, la reducció mòdul $p$ del coeficient de $u^{p-1}$ de la sèrie

$$\left(1 - \sum_{n\geq 4,\text{parell}} \frac{12^{n/2}B_n}{n(n-2)!}E_n(\tau)u^n\right)^{\frac{p}{2}};$$

o sigui, de la sèrie

$$\left(1 - \sum_{n=4,\text{parell}}^{p-3} \frac{12^{n/2}B_n}{n(n-2)!}E_n(\tau)u^n - \frac{12^{\frac{p-1}{2}}B_{p-1}}{(p-1)(p-3)!}E_{p-1}(\tau)u^{p-1}\right)^{\frac{p}{2}},$$

sèrie que admet l'expressió

$$\sum_{r\geq 0}\binom{\frac{p}{2}}{r}\left(-\sum_{n=4,\text{parell}}^{p-3}\frac{12^{n/2}B_n}{n(n-2)!}E_n(\tau)u^n - \frac{12^{\frac{p-1}{2}}B_{p-1}}{(p-1)(p-3)!}E_{p-1}(\tau)u^{p-1}\right)^r.$$

Per a $r > \dfrac{p-1}{4}$, tots els termes de la potència $r$-èsima del parèntesi contenen una potència de $u$ d'exponent més gran que $p-1$; Això permet limitar-nos a una suma finita.

El sumand que correspon a $r=0$ és 1, i no hi ha termes en $u^{p-1}$.

Per a $r=1$, el coeficient de $u^{p-1}$ és exactament

$$-\frac{12^{\frac{p-1}{2}}pB_{p-1}}{2(p-1)(p-3)!}E_{p-1}(\tau),$$

on ja s'ha inclòs el nombre $\binom{\frac{p}{2}}{r}$. Ara, el teorema de Clausen-von Staudt ens diu que el nombre $\dfrac{pB_{p-1}}{(p-1)!}$ és $p$-enter i que $\dfrac{pB_{p-1}}{(p-1)!}\equiv 1 \pmod p$, per tant,

$$-\frac{12^{\frac{p-1}{2}}pB_{p-1}}{2(p-1)(p-3)!}\equiv 12^{\frac{p-1}{2}}\equiv\left(\frac{12}{p}\right)=\left(\frac{3}{p}\right)=(-1)^{\delta+\varepsilon}\pmod p,$$

i la reducció mòdul $p$ del coeficient de $u^{p-1}$ per al sumand que correspon a $r=1$ és $(-1)^{\delta+\varepsilon}\tilde{E}_{p-1}(\tau)$.

Finalment, observem que per a $n<p-1$, el nombre $\dfrac{B_n}{n!}$ és $p$-enter (de nou, teorema de Clausen-von Staudt) i que, per tant,

$$\frac{B_nE_n(\tau)}{n!}=\frac{B_n}{n!}-\frac{2}{(n-1)!}\sum_{\nu\geq 1}\sigma_{n-1}(\nu)q^\nu$$

és un polinomi en $E_4(\tau)$, $E_6(\tau)$ de coeficients $p$-enters. En particular, té sentit la seva reducció mòdul $p$ i, per a $1<r\leq\dfrac{p-1}{4}$, el coeficient

de $u^{p-1}$ coincideix amb el de

$$\binom{\frac{p}{2}}{r}\left(-\sum_{n=4,\text{parell}}^{p-3}\frac{12^{n/2}B_n}{n(n-2)!}E_n(\tau)u^n\right)^r,$$

que porta incorporat el factor $\binom{\frac{p}{2}}{r}\equiv 0 \pmod p$. Doncs, per al coeficient de $u^{p-1}$ mòdul $p$ és

$$G_{p-1}(\tau)\equiv(-1)^{\delta+\varepsilon}E_{p-1}(\tau) \pmod p,$$

com calia veure. □

Per a acabar la demostració del teorema **4.3.14**, només resta el cas del polinomi $\tilde{F}_{p-1}$. S'obté en el resultat següent.

**4.3.19 Proposició.** *Sigui $p\geq 5$ un nombre primer. Els coeficients de $\tilde{F}_{p-1}(j)$ són nombres racionals $p$-enters i se satisfà la congruència*

$$\tilde{F}_{p-1}(j)\equiv\tilde{E}_{p-1}(j) \pmod p.$$

Demostració. Recordem que $F_{p-1}(\tau)$ s'ha definit com l'única, llevat el producte per una constant, forma modular de pes $p-1$ del nucli de l'operador lineal $\vartheta_{p+1}\vartheta_{p-1}-\kappa_{p-1}E_4$. Dit d'una altra manera, $F_{p-1}$ és l'únic, llevat del producte per una constant, polinomi isobàric de pes $p-1$ en $E_4$, $E_6$, anul·lat per l'operador $\vartheta_{p+1}\vartheta_{p-1}-\kappa_{p-1}E_4$. Notem que, aquí, l'operador no és un endomorfisme, perquè transforma polinomis isobàrics de pes $p-1$ en polinomis isobàrics de pes $p+3$.

Considerem l'espai de formes modulars de pes $p-1$ mòdul $p$; és a dir, l'espai dels polinomis en $E_4$, $E_6$ i coeficients en $\mathbb{F}_p$ que són reducció mòdul $p$ de formes modulars de pes $p-1$ i coeficients $p$-enters. Els valors propis $\kappa_{p-1-12i}$, $0\leq i<\dfrac{p}{12}$, de $E_4^{-1}\vartheta_{p+1}\vartheta_{p-1}$ són $p$-enters i diferents mòdul $p$. Per tant, la caracterització de $F_{p-1}$ que hem donat resta vàlida mòdul $p$.

Com que $E_{p-1}(q)\equiv 1 \pmod p$ (de nou, el teorema de Clausen-von Staudt), la constant 1 és una forma modular de pes $p-1$ mòdul $p$; a més a més, anul·la la reducció mòdul $p$ de l'operador

$$(\vartheta_{p+1}\vartheta_{p-1}-\kappa_{p-1}E_4)f=f''-\frac{p}{6}E_2f'+\frac{p(p-1)}{12}E_2'f,$$

on $f'(\tau) := \dfrac{df(\tau)}{2\pi i d\tau} = q\dfrac{df}{dq}$. Per tant, $F_{p-1}$ i $E_{p-1}$ són proporcionals mòdul $p$. I com que hem definit $F_{p-1}$ de manera que el terme constant del desenvolupament de Fourier de $F_{p-1}(\tau)$ és

$$(-1)^m \binom{\frac{p-6}{6}}{m} \equiv 1 \pmod{p},$$

obtenim que $\tilde{F}_{p-1}(j) \equiv \tilde{E}_{p-1}(j) \pmod{p}$, com calia veure. □

## 4.4 Els polinomis ortogonals d'Atkin

En l'article [K-Z] es fa una descripció, deguda originalment a Atkin però no publicada, dels polinomis supersingulars. Comencem per un repàs de polinomis ortogonals.

Donat un cos qualsevol $K$, considerem $V := K[X]$ com a $K$-espai vectorial, una forma lineal $\phi : V \longrightarrow K$, i el producte escalar en $V$ donat per $(f, g) := \phi(fg)$.

**4.4.1 Lema.** (Mètode de Gram-Schmidt aplicat a la base $\{X^n\}_{n\geq 0}$) *La successió de polinomis donada recursivament per*

$$P_n(X) = X^n - \sum_{m=0}^{n-1} \frac{(X^n, P_m)}{(P_m, P_m)} P_m(X)$$

*proporciona una base ortogonal de polinomis mònics $P_n$, de grau $n$, sempre que per a tot $n \geq 0$ sigui $(P_n, P_n) \neq 0$.* □

**4.4.2 Observació.** Si $K$ és un subcòs de $\mathbb{R}$ i la forma lineal $\phi$ és donada en la forma

$$\phi(f) := \int_a^b f(X)\omega(X)dX,$$

per a certs nombres reals $a < b$ i alguna funció $\omega(X)$ positiva en l'interval obert $(a, b)$, la condició de no-degeneració del producte escalar se satisfà automàticament; és a dir, $(f, f) > 0$, per a tot $f \in V$, $f \neq 0$.

En [K-Z] es proporciona una altra manera general de caracteritzar i calcular els polinomis $P_n(X)$, sempre que sigui $(P_n, P_n) \neq 0$, per a tot $n \geq 0$; en particular, quan el producte escalar és definit positiu.

**4.4.3 Proposició.** *Siguin $K$ un cos, $V := K[X]$, $\phi : V \longrightarrow K$ una forma lineal, i posem $(f, g) := \phi(fg)$ per al producte escalar definit per $\phi$. Suposem que per a tot $n \geq 0$ és $(P_n(X), P_n(X)) \neq 0$ i considerem la base de polinomis ortogonals $\{P_n(X)\}_{n\geq 0}$ obtinguda pel mètode de Gram-Schmidt. Definim*

$$b_n := \frac{(P_n(X), P_n(X))}{(P_{n-1}(X), P_{n-1}(X))} \neq 0, \qquad g_n := (X^n, 1) = \phi(X^n).$$

*Llavors,*
(a) *Per als polinomis $P_n(X)$ se satisfan relacions de recurrència de la forma*

$$P_{n+1}(X) = (X - a_n)P_n(X) - b_n P_{n-1}(X), \quad a_n \in K, \quad n \geq 1,$$

*amb*

$$P_0(X) := 1, \qquad P_1(X) := X - \frac{\phi(X)}{\phi(1)} = X - \frac{g_1}{g_0}.$$

(b) *Per a la successió $\{Q_n(X)\}_{n\geq 0}$ definida per aquesta relació, però a partir de $Q_0(X) = 0$, $Q_1(X) = g_0 = \phi(1)$, se satisfà que*

$$\frac{Q_n(X)}{P_n(X)} = \Phi(X) + O(X^{-2n-1}) \in K[[X^{-1}]], \text{ on } \Phi(X) := \sum_{n\geq 0} g_n X^{-n-1}.$$

*Aquesta propietat caracteritza unívocament els polinomis $P_n(X)$ i $Q_n(X)$, si imposem, a més a més, que els polinomis $P_n(X)$ siguin mònics i de grau $n$.*
(c) *Definim nombres $\lambda_n \in K$ per l'expressió*

$$g_0 + g_1 x + g_2 x^2 + \cdots = \cfrac{g_0}{1 - \cfrac{\lambda_1 x}{1 - \cfrac{\lambda_2 x}{1 - \cdots}}} \in K[[x]]. \tag{4.26}$$

*Llavors, tots els $\lambda_n$ són no nuls i*

$$a_n = \lambda_{2n} + \lambda_{2n+1}, \qquad b_n = \lambda_{2n-1}\lambda_{2n}, \qquad n \geq 1.$$

DEMOSTRACIÓ. (a) Com que els polinomis $P_n(X)$ són mònics i de grau $n$, existeixen constants $a_{n,m} \in K$, $0 \leq m \leq n$, tals que

$$XP_n(X) = P_{n+1}(X) + a_{n,n}P_n(X) + a_{n,n-1}P_{n-1}(X) + \cdots + a_{n,0}P_0(X).$$

Per a $0 \leq m \leq n-1$, podem calcular els productes escalars

$$a_{n,m}(P_m(X), P_m(X)) = (XP_n(X), P_m(X)) = (P_n(X), XP_m(X)),$$

la segona igualtat perquè el producte escalar només depèn del producte dels polinomis, i la primera perquè els polinomis $P_n(X)$ són ortogonals. Ara bé, de nou per l'ortogonalitat dels $P_n(X)$, obtenim que

$$\begin{cases} (P_n(X), XP_m(X)) = 0, & \text{per a } 0 \leq m \leq n-2, \\ (P_n(X), XP_{n-1}(X)) = (P_n(X), P_n(X)), & \text{per a } m = n-1. \end{cases}$$

Com que, per a tot $m \geq 0$, és $(P_m(X), P_m(X)) \neq 0$, obtenim que

$$a_{n,m} = \begin{cases} 0, & \text{si } 0 \leq m \leq n-2, \\ \dfrac{(P_n(X), P_n(X))}{(P_{n-1}(X), P_{n-1}(X))} = b_n, & \text{si } m = n-1, \end{cases}$$

d'on s'obté la igualtat

$$XP_n(X) = P_{n+1}(X) + a_{n,n}P_n(X) + b_nP_{n-1}(X),$$

equivalent a la demanada amb $a_n := a_{n,n}$.

(b) Definim $\Phi(X) := \sum_{k\geq 0} g_k X^{-k-1} \in K[[X^{-1}]]$. Llavors, per a un polinomi qualsevol de grau $n$, $f(X) = \sum_{m=0}^{n} c_m X^m \in K[X]$, $c_m \in K$, el producte $f(X)\Phi(X) \in K((X^{-1}))$, que és la suma d'un polinomi de grau $n-1$ en $X$ i una sèrie de potències de $X^{-1}$ sense terme constant, es pot escriure com a sèrie de Laurent de $X^{-1}$ en la forma

$$f(X)\Phi(X) = \sum_{m=0}^{n}\sum_{k\geq 0} c_m g_k X^{m-k-1} = \sum_{k\geq -n}\left(\sum_{m=0}^{n} c_m g_{m+k}\right) X^{-k-1}.$$

Com que, a més a més,

$$(1, f(X)) = \phi(f(X)) = \sum_{m=0}^{n} c_m g_m,$$

el producte escalar $(1, f(X))$ coincideix amb el coeficient de $X^{-1}$ en la sèrie $f(X)\Phi(X)$. I, més generalment, per a dos polinomis qualssevol $f(X), g(X) \in K[X]$, el producte escalar $(g(X), f(X))$ coincideix amb el coeficient de $X^{-1}$ en la sèrie $f(X)g(X)\Phi(X)$.

Si apliquem això al polinomi $f(X) = P_n(X)$ i tenim en compte l'ortogonalitat de $P_n(X)$ amb tots els monomis de grau menor que $n$, $g(X) = X^m$, $0 \leq m \leq n-1$, obtenim que el coeficient de $X^{-m-1}$ en el producte $P_n(X)\Phi(X)$ s'anul·la; és a dir, hi ha una igualtat de la forma

$$P_n(X)\Phi(X) = Q_n(X) + O(X^{-n-1}),$$

per a algun polinomi $Q_n(X) \in K[X]$, de grau $n-1$. Recíprocament, una igualtat com aquesta per a certes famílies de polinomis $P_n(X)$, $Q_n(X)$ de graus $n$ i $n-1$, ens indica que el producte escalar de $P_n(X)$ amb qualsevol polinomi de grau menor que $n$ és nul, de manera que els polinomis $P_n(X)$ són ortogonals i de grau $n$; per tant, si són mònics, són els polinomis ortogonals obtinguts pel mètode de Gram-Schmidt. Dit d'una altra manera, els polinomis $P_n(X)$ són els únics polinomis mònics i de grau $n$ per als quals existeix una família de polinomis de grau $n-1$, $Q_n(X)$, tals que

$$P_n(X)\Phi(X) = Q_n(X) + O(X^{-n-1})$$

o, equivalentment,

$$\frac{Q_n(X)}{P_n(X)} = \Phi(X) + O(X^{-2n-1}).$$

Finalment, aquesta propietat, juntament amb el fet que per als polinomis $P_n(X)$ se satisfà la relació de recurrència de (a), permet calcular

$$\begin{aligned} Q_{n+1}(X) - (X - a_n)Q_n(X) + b_nQ_{n-1}(X) = \\ \big(P_{n+1}(X) - (X - a_n)P_n(X) + b_nP_{n-1}(X)\big)\Phi(X) + O(X^{-n}) = \\ O(X^{-n}); \end{aligned}$$

però $Q_{n+1}(X) - (X - a_n)Q_n(X) + b_nQ_{n-1}(X)$ és un polinomi, de manera que $Q_{n+1}(X) - (X - a_n)Q_n(X) + b_nQ_{n-1}(X) = 0$ i, en conseqüència, per als polinomis $Q_n(X)$ se satisfan les mateixes relacions de recurrència que per als $P_n(X)$, només que, ara, a partir de $Q_0(X) = 0$, $Q_1(X) = g_0 = \phi(1)$.

(c) Modifiquem l'espai vectorial $V = K[X]$ i considerem $V^* := K[Y]$, amb producte escalar $(f(X), g(X)) := \psi(f(X)g(X))$, on la forma lineal $\psi$ es defineix per $\psi(X^{2m+1}) = 0$, per a $n = 2m+1$, senar, i $\psi(X^{2m}) := g_m$, per a $n = 2m$, parell. Notem que, amb la identificació $X = Y^2$, $V$ és el subespai vectorial de $V^*$ format pels polinomis en $Y^2$; és a dir, pels polinomis parells.

En particular, per a $V^*$, podem considerar, com abans, la base de polinomis ortogonals $P_n^*(Y)$ obtinguda pel mètode de Gram-Schmidt a partir de la base $Y^n$. De la definició del producte escalar, és obvi que els monomis de grau senar són ortogonals als monomis de grau parell; per tant, per inducció, obtenim que els polinomis $P_{2m}^*(Y)$ són polinomis parells (és a dir, polinomis en $Y^2$) i els polinomis $P_{2m+1}^*(Y)$ són polinomis senars (és a dir, productes de $Y$ per polinomis en $Y^2$).

Ara, per als polinomis $P_n^*(Y)$ se satisfan les propietats anàlogues a les (a) i (b) anteriors; però el fet que els polinomis siguin alternativament parells i senars obliga que la recursió de (a) sigui de la forma més senzilla

$$P_{n+1}^*(Y) = YP_n^*(Y) - \lambda_n P_{n-1}^*(Y), \tag{4.27}$$

per a certs elements $a_n^* = 0$ i $b_n^* = \lambda_n = \dfrac{(P_n^*(Y), P_n^*(Y))}{(P_{n-1}^*(Y), P_{n-1}^*(Y))} \in K^*$. Els polinomis $Q_n^*(Y)$, obtinguts igual que en (b), són de paritat oposada a la paritat dels $P_n^*(Y)$, perquè són de grau una unitat inferior i per a ells se satisfà la mateixa recursió que per als $P_n^*(Y)$,

$$Q_{n+1}^*(Y) = YQ_n^*(Y) - \lambda_n Q_{n-1}^*(Y). \tag{4.28}$$

I, també com en (b), les funcions racionals $\dfrac{Q_n^*(Y)}{P_n^*(Y)}$ són les millors aproximacions a la sèrie $\displaystyle\sum_{k\geq 0} g_k Y^{-2k-1}$, en el sentit que

$$\frac{Q_n^*(Y)}{P_n^*(Y)} = \sum_{k\geq 0} g_k Y^{-2k-1} + O(Y^{-2n-1}).$$

Per inducció, s'obté la fórmula matricial

$$\begin{bmatrix} Q_{n+1}^*(Y) & Q_n^*(Y) \\ P_{n+1}^*(Y) & P_n^*(Y) \end{bmatrix} = \begin{bmatrix} g_0 & 0 \\ Y & 1 \end{bmatrix} \begin{bmatrix} Y & 1 \\ -\lambda_1 & 0 \end{bmatrix} \cdots \begin{bmatrix} Y & 1 \\ -\lambda_n & 0 \end{bmatrix}, \tag{4.29}$$

de la qual, per un càlcul estàndard (cf. **4.4.4**, més avall), s'obté l'expressió

$$\cfrac{g_0 Y^{-1}}{1-\cfrac{\lambda_1 Y^{-2}}{1-\cfrac{\lambda_2 Y^{-2}}{\ddots\, 1-\lambda_n Y^{-2}}}} = \frac{Q_n^*(Y)}{P_n^*(Y)}.$$

Com que

$$\frac{Q_n^*(Y)}{P_n^*(Y)} = \frac{g_0}{Y} + \frac{g_1}{Y^3} + \cdots + \frac{g_n}{Y^{2n+1}} + O(\frac{1}{Y^{2n+3}}),$$

si multipliquem per $Y$, posem $x := Y^{-2}$, i fem tendir $n$ a infinit, obtenim l'expressió en fracció continuada (4.26) que volíem.

Per a acabar la prova, notem que la recurrència (4.27) que satisfan els polinomis $P_n^*(Y)$ es transforma en dues recurrències idèntiques

$$P_{n+2}^*(Y) = (Y^2 - \lambda_n - \lambda_{n+1})P_n^*(Y) - \lambda_n\lambda_{n-1}P_{n-2}^*(Y),$$

una entre els termes parells, i l'altra entre els termes senars, que només depenen dels primers dos termes, cadascuna. Com que amb la identificació de $V$ com a subespai de $V^*$ donada per $X = Y^2$, tenim que $P_{2n}^*(Y) = P_n(X)$, les relacions desitjades entre les constants $\lambda_n$, $a_n$ i $b_n$ s'obtenen en comparar la relació de recurrència per als $P_{2n}^*(Y)$ i la relació de recurrència per als $P_n(X)$ de (a). □

**4.4.4 Observació.** El càlcul, que ni es detalla ni del qual no hi ha cap referència en [K-Z], es pot fer de la manera següent. A partir d'una igualtat matricial sobre $K(Y)$ de la forma

$$\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix} = \begin{bmatrix}Y & 1\\ -\lambda & 0\end{bmatrix}\begin{bmatrix}\varepsilon & \zeta\\ \eta & \theta\end{bmatrix},$$

tenim que

$$Y^{-1}\frac{\delta}{\beta} = Y^{-1}\frac{-\lambda\zeta}{Y\zeta+\theta} = \frac{-\lambda Y^{-2}}{1+Y^{-1}\dfrac{\theta}{\zeta}};$$

per inducció, per al producte

$$\begin{bmatrix}\alpha_n & \beta_n\\ \gamma_n & \delta_n\end{bmatrix} = \begin{bmatrix}Y & 1\\ -\lambda_1 & 0\end{bmatrix}\cdots\begin{bmatrix}Y & 1\\ -\lambda_n & 0\end{bmatrix},$$

obtenim que

$$Y^{-1}\frac{\delta_n}{\beta_n} = \cfrac{-\lambda_1 Y^{-2}}{1 - \cfrac{\lambda_2 Y^{-2}}{\ddots\, 1 - \lambda_n Y^{-2}}},$$

de manera que, per ser

$$\begin{bmatrix} Q^*_{n+1}(Y) & Q^*_n(Y) \\ P^*_{n+1}(Y) & P^*_n(Y) \end{bmatrix} = \begin{bmatrix} g_0 & 0 \\ Y & 1 \end{bmatrix} \begin{bmatrix} \alpha_n & \beta_n \\ \gamma_n & \delta_n \end{bmatrix},$$

obtenim finalment la igualtat

$$\frac{Q^*_n(Y)}{P^*_n(Y)} = \frac{g_0\beta_n}{Y\beta_n + \delta_n} = \cfrac{g_0 Y^{-1}}{1 + Y^{-1}\cfrac{\delta_n}{\beta_n}} = \cfrac{g_0 Y^{-1}}{1 - \cfrac{\lambda_1 Y^{-2}}{1 - \cfrac{\lambda_2 Y^{-2}}{\ddots\, 1 - \lambda_n Y^{-2}}}}. \square$$

A partir d'aquestes consideracions generals sobre els polinomis ortogonals, en [K-Z] es donen fins a quatre descripcions d'un producte escalar que els autors atribueixen a Atkin. Comencem per la definició.

**4.4.5 Definició.** Considerem l'espai vectorial $V = \mathbb{C}[j]$ dels polinomis en una indeterminada $j$ i de coeficients complexos. Si pensem $j$ com l'invariant modular,

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

podem identificar $V$ amb l'espai vectorial de les funcions complexes que són holomorfes en $\mathcal{H}$, invariants per a l'acció de $\mathbf{PSL}(2,\mathbb{Z})$, i meromorfes en $\infty$ (és a dir, amb un creixement en $\infty$ com a màxim com $q^{-N}$, per a algun nombre $N > 0$). Ara, en lloc de $q(\tau) := e^{2\pi i\tau}$, podem prendre $j(\tau)^{-1}$ o bé

$$\Delta(\tau) = q - 24q^2 + 252q^3 + \cdots$$

com a paràmetre local d'uniformització en $\infty$ per a la superfície de Riemann $\Gamma\backslash(\mathcal{H}\cup\mathbb{Q}\cup\{\infty\})$. El producte escalar d'Atkin $(f,g)$, de dos elements $f, g \in V$, es pot definir com el terme constant del desenvolupament de $f(\tau)g(\tau)$ com a sèrie de Laurent de $\Delta(\tau)$. I els polinomis ortogonals d'Atkin són els polinomis ortogonals que corresponen al producte escalar d'Atkin. Els denotarem per $A_n(j)$, $n \geq 0$.

**4.4.6 Proposició.** *El producte escalar d'Atkin admet les quatre definicions equivalents següents:*
(a) $(f,g)$ = *terme constant de* $fg$ *com a sèrie de Laurent de* $\Delta$*;*
(b) $(f,g)$ = *terme constant de* $fg\dfrac{E_2E_4}{E_6}$ *com a sèrie de Laurent de* $j^{-1}$*;*
(c) $(f,g)$ = *terme constant de* $fgE_2$ *com a sèrie de Laurent de* $q$*;*
(d)

$$(f,g)=\frac{6}{\pi}\int_{\frac{\pi}{3}}^{\frac{\pi}{2}} f(e^{i\theta})g(e^{i\theta})d\theta.$$

*A més a més, el producte escalar restringit a* $V_{\mathbb{R}}:=\mathbb{R}[j]$ *és definit positiu.*

Demostració. De les fórmules (4.23), (4.15) i (4.21) s'obté immediatament la igualtat de formes diferencials

$$\begin{aligned}\frac{d\Delta(\tau)}{\Delta(\tau)}=2\pi iE_2(\tau)d\tau=E_2(\tau)\frac{dq(\tau)}{q(\tau)}&=-\frac{E_2(\tau)E_4(\tau)}{E_6(\tau)}\,\frac{dj(\tau)}{j(\tau)}\\&=\frac{E_2(\tau)E_4(\tau)}{E_6(\tau)}\,\frac{dj^{-1}(\tau)}{j^{-1}(\tau)},\end{aligned}\tag{4.30}$$

de manera que el càlcul dels residus permet relacionar les tres primeres fórmules immediatament i obtenir la seva equivalència. En efecte, el terme constant del desenvolupament d'una funció qualsevol $h(\tau)$ expressada com a sèrie de Laurent d'un paràmetre uniformitzador qualsevol $\delta(\tau)$ coincideix amb el coeficient de $\delta^{-1}$ en el desenvolupament de la funció $\dfrac{h(\tau)}{\delta(\tau)}$ en sèrie de Laurent de $\delta(\tau)$; és a dir, amb el residu en $\delta=0$ de la funció $\dfrac{h(\tau)}{\delta(\tau)}$, o sigui, amb el residu de la forma diferencial $\dfrac{h(\tau)}{\delta(\tau)}d\delta$. Ara, les igualtats (4.30) entre les formes diferencials associades als paràmetres uniformitzadors $\Delta(\tau)$, $q(\tau)$ i $j^{-1}(\tau)$ demostren immediatament l'equivalència de les fórmules (a), (b) i (c).

Per a la fórmula (d), en [K-Z] es fa servir la fórmula dels residus; és a dir, s'integra la forma diferencial $\dfrac{f(\tau)g(\tau)d\Delta(\tau)}{2\pi i\Delta(\tau)}=f(\tau)g(\tau)E_2(\tau)d\tau$ en el domini fonamental usual per a $\mathbf{PSL}(2,\mathbb{Z})$, truncat a una certa

altura $a > 1$; això és, en el domini format pels punts $\tau = x + yi \in \mathcal{H}$ tals que $x^2 + y^2 \geq 1$, $-\dfrac{1}{2} \leq x \leq \dfrac{1}{2}$, i $y \leq a$. Vegem-ne els detalls.

Per (c), el producte escalar $(f(\tau), g(\tau))$ coincideix amb la integral de la forma diferencial $f(\tau)g(\tau)E_2(\tau)d\tau$ sobre l'aresta superior del domini recorreguda en el sentit creixent de $x$. En efecte, si escrivim

$$f(\tau)g(\tau)E_2(\tau) =: \sum_{n>>-\infty} c_n q(\tau)^n = \sum_{n>>-\infty} c_n e^{2\pi i n\tau},$$

tenim que $(f(\tau), g(\tau)) = c_0$; d'altra banda, en l'aresta superior, $y = a$, és $\tau = x + ai$ i $d\tau = dx$; per tant,

$$\begin{aligned}\int_{y=a} f(x+ai)g(x+ai)E_2(x+ai)dx &= \sum_{n>>-\infty} c_n \int_{y=a} e^{2\pi i n(x+ai)}dx \\ &= \sum_{n>>-\infty} c_n e^{-2\pi na} \int_{x=-1/2}^{x=1/2} e^{2\pi i n x}dx = c_0,\end{aligned}$$

perquè

$$\int_{x=-1/2}^{x=1/2} e^{2\pi i n x}dx = \begin{cases} 0, & \text{si } n \neq 0, \\ 1, & \text{si } n = 0. \end{cases}$$

Com que la funció $f(\tau)g(\tau)E_2(\tau)$ és holomorfa en el semiplà superior, la seva integral sobre la vora del domini truncat s'anul·la; i com que és periòdica de període 1, les integrals sobre les arestes verticals del domini truncat, que es recorren en sentits contraris, sumen zero. Per tant, obtenim que el producte escalar $(f(\tau), g(\tau)) = c_0$ coincideix amb la integral de $f(\tau)g(\tau)E_2(\tau)d\tau$ sobre l'arc $\tau = e^{i\theta}$, recorregut en sentit decreixent de $\theta$ des de $\theta = \dfrac{2\pi}{3}$ fins a $\theta = \dfrac{2\pi}{6}$; és a dir,

$$c_0 = \int_{\theta=2\pi/3}^{\theta=2\pi/6} f(e^{i\theta})g(e^{i\theta})E_2(e^{i\theta})ie^{i\theta}d\theta.$$

Ara bé, el canvi de $\tau$ per $\dfrac{-1}{\tau}$ en la meitat esquerra de l'arc, o sigui, de $e^{i\theta}$ per $-e^{-i\theta}$ per a $\theta$ decreixent des de $\dfrac{2\pi}{3}$ fins a $\dfrac{2\pi}{4}$ (això és $\theta$ es canvia per $\pi - \theta$), proporciona l'altra meitat de l'arc recorreguda en sentit contrari; d'altra banda, la funció $f(\tau)g(\tau)$ és invariant per aquest canvi, perquè és modular, i la funció $E_2(\tau)$ es transforma en

$E_2(-1/\tau) = \tau^2 E_2(\tau) + \dfrac{6}{\pi i}\tau$ (cf. (4.13)); és a dir, $E_2(e^{i\theta})$ es transforma en $E_2(-e^{-i\theta}) = e^{2i\theta}E_2(e^{i\theta}) + \dfrac{6}{\pi i}e^{i\theta}$; per tant, s'obté que

$$-E_2(-e^{-i\theta})ie^{-i\theta}d(\pi-\theta) = E_2(e^{i\theta})ie^{i\theta}d\theta + \frac{6}{\pi}d\theta,$$

de manera que

$$c_0 = -\int_{\theta=2\pi/4}^{\theta=2\pi/6} f(e^{i\theta})g(e^{i\theta})\frac{6}{\pi}d\theta = \frac{6}{\pi}\int_{\theta=\pi/3}^{\theta=\pi/2} f(e^{i\theta})g(e^{i\theta})d\theta,$$

com calia veure.

Resta veure que la restricció del producte escalar a $\mathbb{R}[j]$ és un producte escalar definit positiu; però això es dedueix immediatament de (d), perquè per a $\dfrac{\pi}{3} \leq \theta \leq \dfrac{\pi}{2}$ és $j(e^{i\theta}) \in \mathbb{R}$ (i, a més a més, $0 \leq j(e^{i\theta}) \leq 1728$), de manera que per a qualsevol polinomi no nul de coeficients reals, $f(j) \in \mathbb{R}[j]$, és $f(j(e^{i\theta}))^2 \geq 0$ i, en conseqüència,

$$\int_{\pi/3}^{\pi/2} f(j(e^{i\theta}))^2 d\theta > 0. \,\square$$

**4.4.7 Observació.** En [K-Z] encara es dóna una altra fórmula per al càlcul del producte escalar d'Atkin. De fet, no es tracta d'una fórmula essencialment diferent, perquè només és conseqüència d'un canvi de variable a partir de la fórmula de (d) de la proposició **4.4.6**. Concretament,

$$(f,g) = \int_0^{1728} f(j)g(j)w(j)dj, \qquad w(j) := \frac{6}{\pi}\theta'(j),$$

on $\theta : [0, 1728] \longrightarrow [\pi/3, \pi/2]$ és la inversa de la funció creixent $\theta \mapsto j(e^{i\theta})$.

Dels resultats generals de més amunt i de la descripció del producte escalar d'Atkin s'obté immediatament el resultat següent.

**4.4.8 Corol·lari.** (a) *Existeix una família de polinomis $A_n(j) \in \mathbb{C}[j]$, $n \geq 0$, única tal que els polinomis són mònics, de grau $n$, i ortogonals per al producte escalar d'Atkin.*

(b) *El producte escalar de dos monomis $j^n$ i $j^m$ és $(j^n, j^m) = g_{n+m}$, on $g_n$ és el coeficient de $j(\tau)^{-n-1}$ en la sèrie*

$$\Phi(\tau) = \frac{E_2(\tau)E_4(\tau)}{E_6(\tau)j(\tau)} = q - 24q^2 + 196812q^3 + \cdots = \frac{1}{j(\tau)} + \frac{720}{j(\tau)^2} + \cdots$$

(c) *Els polinomis $A_n(j)$ són els denominadors de les millors aproximacions per funcions racionals de la sèrie $\Phi(j(\tau))$.*

(d) *Per als polinomis $A_n(j)$ se satisfan relacions de recursió de la forma*

$$A_{n+1}(j) = (j - (\lambda_{2n} + \lambda_{2n+1}))A_n(j) - \lambda_{2n-1}\lambda_{2n}A_{n-1}(j),$$

*on els nombres $\lambda_n$ són racionals i positius i definits per l'expressió en fracció continuada de $\Phi(j)$ respecte de $j^{-1}$.* □

**4.4.9 Observació.** Es poden calcular explícitament els primers coeficients; en [K-Z] es donen els valors

$$g_0 = 1, \quad g_1 = 720, \quad g_2 = 911520, \quad g_3 = 1301011200,$$
$$g_4 = 1958042030400,$$

i els valors

$$\lambda_1 = 720, \quad \lambda_2 = 546, \quad \lambda_3 = 374, \quad \lambda_4 = 475, \quad \lambda_5 = \frac{2001}{5}.$$

Anàlogament, els polinomis $A_n(j)$ es poden trobar pel mètode de Gram-Schmidt; en [K-Z] es donen els exemples

$$A_0(j) = 1,$$
$$A_1(j) = j - 720,$$
$$A_2(j) = j^2 - 1640j + 269280,$$
$$A_3(j) = j^3 - \frac{12576}{5}j^2 + 1526958j - 107765856,$$
$$A_4(j) = j^4 - 3384j^3 + 3528552j^2 - 1133263680j + 44184000960,$$

i els autors comenten que els seus coeficients són racionals i, per a nombres primers $p > 2n$, són $p$-enters (cf. el teorema **4.5.1**, (a), més avall). Això justifica que, si posem $n_p := \deg(ss_p(j))$, llavors el polinomi $A_{n_p}(j)$ es pugui reduir mòdul $p$, perquè $n_p$ és, aproximadament, $\frac{p}{12}$ i, per tant, menor que $\frac{p}{2}$.

Aquests resultats previs permeten enunciar els dos resultats següents, dels quals en [K-Z] es diu que foren descoberts, però no publicats, per Atkin.

**4.4.10 Teorema.** *Sigui $p$ un nombre primer. Aleshores,*

$$ss_p(j) \equiv A_{n_p}(j) \pmod{p}.$$

**4.4.11 Teorema.** *Existeix una forma lineal $\phi : V \longrightarrow \mathbb{C}$, única llevat d'un múltiple escalar, per a la qual tots els operadors de Hecke $T_n : V \longrightarrow V$ són autoadjunts respecte del producte escalar $(f, g) := \phi(fg)$. Aquest producte escalar és, llevat del canvi de $\phi$ per un múltiple escalar, el producte escalar d'Atkin.*

**4.4.12 Observació.** El teorema **4.3.14** proporciona, per a cada nombre primer $p \geq 5$, un polinomi (de fet, quatre polinomis) $\tilde{f}(j)$ de coeficients $p$-enters tals que $ss_p(j) \equiv j^\delta (j - 1728)^\varepsilon \tilde{f}(j) \pmod{p}$. En particular, el grau del polinomi $j^\delta (j-1728)^\varepsilon \tilde{f}$ depèn separadament de $m$, $\delta$, i $\varepsilon$ (on $p-1 = 12m+4\delta+6\varepsilon$). En canvi, en el teorema **4.4.10**, el grau del polinomi només depèn de $n = m+\delta+\varepsilon$ i, en conseqüència, serveix per a tots els nombres primers $p$ que proporcionen el mateix valor de $n$. Per exemple, per als nombres primers $p = 23$, 29, 31 i 37, és $n = 3$, de manera que els corresponents polinomis $ss_p(j)$ són la reducció mòdul $p$ del mateix polinomi d'Atkin,

$$A_3(j) = j^3 - \frac{12576}{5} j^2 + 1526958j - 107765856.$$

A continuació, presentem la demostració del teorema **4.4.11** que hi ha en [K-Z].

Demostració. Lluny de limitar-se a treballar en $V = \mathbb{C}[j]$, en [K-Z] els seus autors escriuen $V_0 := V$, defineixen $V_k$ com l'espai de les funcions holomorfes en $\mathcal{H}$ que es transformen com si fossin formes modulars de pes $k$ i que tenen creixement en $\infty$ com a màxim exponencial, i consideren l'àlgebra graduada $\mathbb{C}[E_4, E_6, \Delta^{-1}]$ de la qual $V_k$ és el subespai de grau $k$. Aquí, $k$ és un nombre enter arbitrari, positiu o negatiu, de manera que també treballen amb pesos negatius. Notem que, encara que no hi ha formes modulars de pes 2, és a dir, que $M_2 = (0)$, l'espai $V_2$ és no nul; per exemple, conté el quocient $\dfrac{E_4^2 E_6}{\Delta} \neq 0$; de fet, $V_2$ és l'espai de les derivades dels elements de $V$.

A continuació, es defineixen operadors de Hecke: per a tot nombre enter $k$ i tot nombre enter $n > 0$, els operadors de Hecke $T_n$ en $V_k$ són donats per la fórmula

$$(f|_k T_n)(\tau) := n^{k/2} \sum_{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma\backslash\mathcal{M}_n} \frac{1}{(c\tau+d)^k} f\left(\frac{a\tau+b}{c\tau+d}\right),$$

on $\mathcal{M}_n$ és el conjunt de les matrius de $\mathbf{M}(2,\mathbb{Z})$ de determinant $n > 0$, $f \in V_k$ és un element qualsevol, i $\Gamma := \mathbf{SL}(2,\mathbb{Z})$. En [K-Z] es diu que aquesta normalització només coincideix amb l'estàndard quan $k = 2$, però que és més convenient per a estudiar alhora pesos positius i pesos negatius. Aquesta fórmula només té sentit per a funcions $f \in V_k$, "perquè, si $f$ no fos modular, l'expressió $(c\tau+d)^{-k} f\left(\frac{a\tau+b}{c\tau+d}\right)$ no seria independent del representant elegit en $\Gamma\backslash\mathcal{M}_n$." Per a evitar aquest problema, es defineixen uns "operadors de Hecke en infinit", $T_n^\infty$, per la fórmula

$$(f|_k T_n^\infty)(\tau) := n^{k/2} \sum_{\substack{ad=n \\ a,d>0}} \sum_{b \bmod d} d^{-k} f\left(\frac{a\tau+b}{d}\right);$$

aquesta fórmula té sentit per a qualsevol funció 1-periòdica $f$ i coincideix amb $|_k T_n$, si $f \in V_k$, perquè les matrius $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, $0 \le b < d = \frac{n}{a}$, formen un sistema de representants de $\Gamma\backslash\mathcal{M}_n$.

Amb aquests previs, encara es defineix el residu en $\infty$ d'una funció $F$, holomorfa en $\mathcal{H}$ i 1-periòdica, com

$$\operatorname*{Res}_\infty(F) := \text{ residu en } \infty \text{ de } 2\pi i F(\tau) d\tau,$$

o sigui, com el terme constant del desenvolupament de $F(\tau)$ com a sèrie de Laurent en $q$, i es proven les fórmules

$$\operatorname*{Res}_\infty((f|_k T_n^\infty)\cdot h) = \operatorname*{Res}_\infty(f \cdot (h|_{2-k} T_n^\infty)), \qquad f, h \in \mathbb{C}((q)),$$

i

$$(gE_2)|_2 T_n^\infty = (g|_0 T_n)\cdot E_2 \pmod{V_2}, \qquad g \in V_0.$$

Per a la primera, s'observa que els operadors en infinit $T_n^\infty$ actuen sobre les sèries de Fourier per la fórmula

$$\left(\sum_r A_r q^r\right)|_k T_n^\infty = n^{k/2}\sum_{ad=n} d^{1-k}\sum_r A_{rd}q^{ar},$$

de manera que, per a

$$f =: \sum_r A_r q^r, \qquad h =: \sum_s B_s q^s,$$

es pot escriure

$$\begin{aligned}\operatorname*{Res}_\infty\big((f|_k T_n^\infty)h\big) &= n^{k/2}\sum_{ad=n}\sum_r d^{1-k}A_{dr}B_{-ar}\\ &= n^{1-k/2}\sum_{ad=n} a^{-1+k}\sum_s B_{as}A_{-ds}\\ &= \operatorname*{Res}_\infty\big(f(h|_{2-k}T_n^\infty)\big).\end{aligned}$$

Per a la segona, es comença per escriure la llei de transformació (4.13) en la forma equivalent

$$E_2(\tau) = E_2^*(\tau) + \frac{3}{\pi y}, \qquad \tau = x+yi, \qquad x,y\in\mathbb{R},$$

on la funció (no holomorfa) $E_2^*(\tau)$ es transforma com una forma modular de pes 2. Llavors, es considera l'espai $V_2^*$ de les funcions (no necessàriament holomorfes) que es transformen com si fossin formes modulars de pes 2, s'observa que $VV_2^*\subseteq V_2^*$, i es nota que l'operador $|_2T_n$ també actua en l'espai $V_2^*$; això permet escriure la igualtat

$$(gE_2)|_2T_n^\infty - (g|_0T_n)E_2 \equiv \frac{3}{\pi}\big((gy^{-1})|_2T_n^\infty - (g|_0T_n)y^{-1}\big) \pmod{V_2^*}$$

que, juntament amb el fet que

$$\begin{aligned}\big((gy^{-1})|_2T_n^\infty\big)(\tau) &= \sum_{\substack{ad=n\\ b \pmod d}} \frac{n}{d^2}g\left(\frac{a\tau+b}{d}\right)\operatorname{Im}\left(\frac{a\tau+b}{d}\right)^{-1}\\ &= y^{-1}(g|_0T_n)(\tau),\end{aligned}$$

igualtat que assegura que la dreta de la congruència s'anul·la, ens diu que $(gE_2)|_2T_n^\infty - (g|_0T_n)E_2 \in V_2$, ja que és una funció holomorfa.

Amb aquestes fórmules provades, i juntament amb la descripció (c) del producte escalar de la proposició **4.4.6** i els fets que $VV_2 \subseteq V_2$ i que $\mathrm{Res}_\infty$ s'anul·la en $V_2$, s'obté la fórmula d'adjunció per al producte escalar d'Atkin de la manera següent:

$$\begin{aligned}(f|_0T_n, g) &= \operatorname*{Res}_\infty \left((f|_0T_n^\infty)\cdot g\cdot E_2\right)\\ &= \operatorname*{Res}_\infty \left(f\cdot (gE_2)|_2T_n^\infty\right)\\ &= \operatorname*{Res}_\infty \left(f\cdot (g|_0T_n)\cdot E_2\right)\\ &= (f, g|_0T_n), \qquad f,g\in V.\end{aligned}$$

Per a veure la unicitat, en [K-Z] es diu que si $\Phi : V \longrightarrow \mathbb{C}$ és un operador lineal qualsevol per al qual se satisfà la conclusió del teorema, llavors els polinomis

$$\begin{aligned}h_n &:= j|_0T_n\cdot 1 - j\cdot 1|_0T_n, \qquad n\geq 2,\\ h^* &:= j^2|_0T_2\cdot j - j^2\cdot j|_0T_2\end{aligned}$$

pertanyen al nucli de $\Phi$ i generen un subespai de codimensió 1 de $V$, ja que $h_n$ és de grau $n$ i $h^*$ no és combinació lineal dels $h_n$. Per tant, $\Phi$ és determinat llevat d'un factor escalar, com calia veure. □

**4.4.13 Observació.** Encara s'afirma que es pot provar de la mateixa manera la fórmula d'adjunció més general

$$(f|_kT_n, g) = (f, g|_{-k}T_n), \qquad f\in V_k,\ g\in V_{-k},$$

on l'aparellament $(\ ,\ ) : V_k\otimes V_{-k}\longrightarrow \mathbb{C}$ és definit per

$$(f,g) = \operatorname*{Res}_\infty(fgE_2).$$

Tot això permet donar una demostració "modular" del teorema **4.4.10**; a la secció següent en donarem una altra, "hipergeomètrica".

Demostració. En primer lloc, recordem que disposem dels polinomis ortogonals d'Atkin, $A_n(j)$, i que les seves propietats estan resumides en el corol·lari **4.4.8**. En particular, per a $n = 1$ és

$A_1(j) = j - 720$, de manera que, per a $p = 2$ i per a $p = 3$, és $ss_p(j) = j \equiv j - 720 = A_1(j) \pmod{p}$, i el teorema és demostrat per a aquests dos valors de $p$.

Sigui, doncs, $p \geq 5$ un nombre primer. Per als desenvolupaments en sèries de potències de $q$ de les sèries d'Eisenstein se satisfan les congruències

$$E_{p-1}(q) \equiv 1 \pmod{p}, \qquad E_{p+1}(q) \equiv E_2(q) \pmod{p};$$

la primera, ja que el teorema de Clausen-von Staudt permet dir que $\dfrac{p-1}{B_{p-1}} \equiv 0 \pmod{p}$, i la segona en virtut de les congruències de Kummer que, en particular, ens diuen que $\dfrac{B_{p+1}}{p+1} \equiv \dfrac{B_2}{2} = \dfrac{1}{12} \pmod{p}$ (cf. [8]).

Com que podem substituir el paràmetre uniformitzador $q$ pel paràmetre uniformitzador $j^{-1}$ o bé a la inversa, tenim un isomorfisme $\mathbb{Z}_{(p)}[[q]] \simeq \mathbb{Z}_{(p)}[[j^{-1}]]$, entre els anells de sèries de coeficients nombres racionals $p$-enters; en reduir mòdul $p$, obtenim les congruències, ara com a sèries de potències de $j^{-1}$,

$$E_{p-1} \equiv 1 \pmod{p}, \qquad E_{p+1} \equiv E_2 \pmod{p}.$$

Això permet canviar, mòdul $p$, la funció racional $\Phi(j) = \dfrac{E_2(j)E_4(j)}{E_6(j)j}$ per la funció modular $\dfrac{E_{p+1}E_4}{E_{p-1}E_6 j}$ que, per ésser de pes 0, també és una funció racional de $j$; és a dir, obtenim la congruència

$$\Phi(j) = \frac{E_2(j)E_4(j)}{E_6(j)j} \equiv \frac{E_{p+1}(j)E_4(j)}{E_{p-1}(j)E_6(j)j} \pmod{p}.$$

Ara, la idea és que aquesta funció racional és una aproximació perfecta de si mateixa, de manera que és la millor possible i, en conseqüència, el seu denominador hauria d'ésser la reducció mòdul $p$ del polinomi d'Atkin corresponent. Però cal precisar els detalls d'aquest argument.

Podem escriure el pes $p-1$ en la forma $p - 1 = 12m + 4\delta + 6\varepsilon$, amb $m = \left[\dfrac{p}{12}\right]$,

$$\delta = \begin{cases} 0, & \text{si } p \equiv 1 \pmod{3}, \\ 1, & \text{si } p \equiv 2 \pmod{3}, \end{cases} \qquad \varepsilon = \begin{cases} 0, & \text{si } p \equiv 1 \pmod{4}, \\ 1, & \text{si } p \equiv 3 \pmod{4}. \end{cases}$$

Llavors, tenim que $p+1 = 12(m+\delta+\varepsilon-1)+4(2(1-\delta))+6(1-\varepsilon)$, on $m+\delta+\varepsilon-1$, $2(1-\delta)$, i $1-\varepsilon$, respectivament, són els nombres $m$, $\delta$ i $\varepsilon$ que corresponen al pes $p+1$. En virtut de la proposició **4.3.3**, obtenim les igualtats

$$E_{p-1} = \Delta^m E_4^\delta E_6^\varepsilon \tilde{E}_{p-1}, \qquad E_{p+1} = \Delta^{m+\delta+\varepsilon-1} E_4^{2(1-\delta)} E_6^{1-\varepsilon} \tilde{E}_{p+1},$$

que permeten calcular la reducció de $\Phi$ mòdul $p$, com a funcions de $j$, en la forma

$$\Phi = \frac{E_2E_4}{E_6 j} \equiv \frac{E_{p+1}E_4}{E_{p-1}E_6 j} = \frac{\Delta^{\delta+\varepsilon-1} E_4^{3(1-\delta)} \tilde{E}_{p+1}}{j E_6^{2\varepsilon} \tilde{E}_{p-1}} \pmod p$$

i, en tenir en compte que $j = \dfrac{E_4^3}{\Delta}$ i que $j-1728 = \dfrac{E_6^2}{\Delta}$, com

$$\Phi(j) \equiv \frac{\tilde{E}_{p+1}(j)}{j^\delta (j-1728)^\varepsilon \tilde{E}_{p-1}(j)} = \frac{\tilde{E}_{p+1}(j)}{ss_p(j)} \pmod p,$$

la darrera igualtat en virtut del teorema **4.3.14**.

Notem que el denominador de la darrera expressió és un polinomi de grau $n_p = m+\delta+\varepsilon = \mathrm{gr}(ss_p(j))$, mentre que el numerador és un polinomi de grau $m+\delta+\varepsilon-1 = n_p-1$. Però, per a tot $n$ i, en particular, per a $n = n_p$, tenim que

$$\Phi(j) = \frac{B_n(j)}{A_n(j)} + O(j^{-2n-1}),$$

per als polinomis d'Atkin $A_n(j)$ i certs polinomis $B_n(j)$ de grau $n-1$. Si convé, i per a $n = n_p$, multipliquem $A_n(j)$ i $B_n(j)$ per una mateixa potència de $p$ a fi que el polinomi $A_n(j)$ sigui de coeficients $p$-enters i, alhora, primitiu mòdul $p$, i denotem per $\overline{A}_n(j)$, $\overline{B}_n(j)$ les reduccions mòdul $p$ corresponents; obtenim una congruència

$$\frac{\tilde{E}_{p+1}(j)}{ss_p(j)} \equiv \Phi(j) \equiv \frac{\overline{B}_{n_p}(j)}{\overline{A}_{n_p}(j)} + O(j^{-2n_p-1}) \pmod p,$$

on els polinomis $\overline{A}_{n_p}(j)$, $\overline{B}_{n_p}(j) \in \mathbb{F}_p[j]$ són de grau menor o igual que $n_p$ i que $n_p-1$, respectivament. En multiplicar aquesta igualtat pel producte $ss_p(j)\overline{A}_{n_p}(j)$, obtenim que

$$\overline{B}_{n_p}(j) ss_p(j) - \overline{A}_{n_p}(j)\tilde{E}_{p+1}(j) \equiv O(j^{-1}) \pmod p$$

i, com que és un polinomi, que

$$\overline{B}_{n_p}(j)ss_p(j) - \overline{A}_{n_p}(j)\tilde{E}_{p+1}(j) \equiv 0 \pmod{p}.$$

Ara es tracta de veure que els polinomis $\tilde{E}_{p+1}(j) \pmod{p}$ i $ss_p(j)$ són primers entre si; així tindrem que el polinomi $ss_p(j)$ divideix $\overline{A}_{n_p}(j)$ i, en conseqüència, com que $A_n(j)$ és mònic de grau $n_p$, que el polinomi $A_n(j)$ és de coeficients $p$-enters i redueix a $ss_p(j)$ mòdul $p$, com volem demostrar.

I, per a demostrar que els polinomis $\tilde{E}_{p+1}(j) \pmod{p}$ i $ss_p(j)$ són primers entre si, n'hi ha prou si demostrem la congruència

$$\tilde{E}_{p+1}(j) \equiv -12\frac{d\,ss_p(j)}{dj} + 8\delta\frac{ss_p(j)}{j} + 6\varepsilon\frac{ss_p(j)}{j-1728} \pmod{p},$$

ja que el polinomi $ss_p(j)$ no té arrels múltiples. Notem que $\delta\dfrac{ss_p(j)}{j}$ i $\varepsilon\dfrac{ss_p(j)}{j-1728}$ són polinomis, perquè si $\delta \neq 0$, el polinomi $ss_p(j)$ és divisible per $j$, i si $\varepsilon \neq 0$, ho és per $j - 1728 \pmod{p}$.

Ara bé, de la definició de l'operador $\vartheta_{p-1}$ i de les congruències $E_{p-1} \equiv 1 \pmod{p}$ i $E_{p+1} \equiv E_2 \pmod{p}$, tenim que

$$12\vartheta_{p-1}E_{p-1} = 12q\frac{d}{dq}E_{p-1} - (p-1)E_2E_{p-1} \equiv E_2 \equiv E_{p+1} \pmod{p},$$

de manera que el polinomi $\tilde{E}_{p+1}(j)$ és, mòdul $p$, el polinomi associat a la forma modular $12\vartheta_{p-1}E_{p-1}$ per la proposició **4.3.3**. Si ara tenim en compte que la forma modular $\vartheta_{p-1}E_{p-1}$ és de pes $p+1$, i que s'escriu en la forma

$$\vartheta_{p-1}E_{p-1} = \Delta^{m+\delta+\varepsilon-1}E_4^{2(1-\delta)}E_6^{1-\varepsilon}(\vartheta E_{p-1})^{\sim}(j),$$

veiem que cal calcular el polinomi $12(\vartheta E_{p-1})^{\sim}(j)$.

A partir de la igualtat $E_{p-1} = \Delta^m E_4^\delta E_6^\varepsilon \tilde{E}_{p-1}$, i en tenir en compte que la família d'operadors $\vartheta_k$ es comporta com una derivació, tenim que

$$\vartheta_{p-1}E_{p-1} = \vartheta_{12m+4\delta+6\varepsilon}(\Delta^m E_4^\delta E_6^\varepsilon)\tilde{E}_{p-1} + \Delta^m E_4^\delta E_6^\varepsilon \vartheta_0(\tilde{E}_{p-1});$$

com que

$$\vartheta_{12m+4\delta+6\varepsilon}(\Delta^m E_4^\delta E_6^\varepsilon) = -\Delta^m \left(\frac{\delta}{3} E_4^{\delta-1} E_6^{1+\varepsilon} + \frac{\varepsilon}{2} E_4^{2+\delta} E_6^{\varepsilon-1}\right),$$

obtenim que

$$\begin{aligned}\vartheta_{p-1}E_{p-1} &= -\Delta^{m+\delta+\varepsilon-1} E_4^{2(1-\delta)} E_6^{1-\varepsilon}\cdot \\ &\quad \left(\frac{\delta E_4^{3\delta-3}E_6^{2\varepsilon}}{3\Delta^{\delta+\varepsilon-1}} + \frac{\varepsilon E_4^{3\delta}E_6^{2\varepsilon-2}}{2\Delta^{\delta+\varepsilon-1}} - \frac{E_4^{3\delta-2}E_6^{2\varepsilon-1}\vartheta_0}{\Delta^{\delta+\varepsilon-1}}\right)\tilde{E}_{p-1} \\ &= -\Delta^{m+\delta+\varepsilon-1} E_4^{2(1-\delta)} E_6^{1-\varepsilon} j^\delta (j-1728)^\varepsilon\cdot \\ &\quad \left(\frac{\delta}{3j} + \frac{\varepsilon}{2(j-1728)} - \frac{\Delta}{E_4^2 E_6}\vartheta_0\right)\tilde{E}_{p-1},\end{aligned}$$

en tenir en compte que $j = \dfrac{E_4^3}{\Delta}$ i que $j - 1728 = \dfrac{E_6^2}{\Delta}$. Finalment, com que $\vartheta_0 = q\dfrac{d}{dq} = q\dfrac{dj}{dq}\dfrac{d}{dj}$ i $q\dfrac{dj}{dq} = -\dfrac{E_4^2 E_6}{\Delta}$, obtenim l'expressió

$$\begin{aligned}\vartheta_{p-1}E_{p-1} = -\Delta^{m+\delta+\varepsilon-1} E_4^{2(1-\delta)} E_6^{1-\varepsilon} j^\delta (j-1728)^\varepsilon\cdot \\ \left(\frac{\delta}{3j} + \frac{\varepsilon}{2(j-1728)} + \frac{d}{dj}\right)\tilde{E}_{p-1}.\end{aligned}$$

Per tant, i com restava veure,

$$\begin{aligned}12(\vartheta E_{p-1})^\sim(j) &= -j^\delta (j-1728)^\varepsilon \left(\frac{4\delta}{j} + \frac{6\varepsilon}{(j-1728)} + \frac{12d}{dj}\right)\tilde{E}_{p-1} \\ &\equiv 8\delta\frac{ss_p(j)}{j} + 6\varepsilon\frac{ss_p(j)}{j-1728} - 12\frac{d\,ss_p(j)}{dj} \pmod p,\end{aligned}$$

ja que $ss_p(j) \equiv j^\delta (j-1728)^\varepsilon \tilde{E}_{p-1}(j) \pmod p$. □

## 4.5 Aspectes hipergeomètrics

Els autors de [K-Z] no es conformen amb la descripció que han donat dels polinomis ortogonals d'Atkin, i en donen tres més.

Encara que els polinomis d'Atkin es poden obtenir pel mètode de Gram-Schmidt, a partir d'una fórmula recursiva que utilitza tots

els polinomis anteriors, el corol·lari **4.4.8** proporciona una fórmula recursiva d'ordre 2 de coeficients polinomis de graus 1 i 0; aquesta fórmula recursiva es pot fer més explícita amb el càlcul dels coeficients $\lambda_n$. D'altra banda, els polinomis d'Atkin també es poden donar explícitament, de manera semblant a la fórmula de Hasse i Deuring. I, per a cada $n \geq 0$, es pot donar una equació diferencial d'ordre 4 i coeficients polinòmics l'únic polinomi mònic solució de la qual és el polinomi d'Atkin $A_n(j)$.

**4.5.1 Teorema.** *Siguin $A_n(j)$ els polinomis ortogonals d'Atkin.*

(a) (Fórmula recursiva) *Per a tot $n \geq 2$, se satisfà la relació recursiva*

$$\begin{aligned} A_{n+1}(j) = &\left(j - 24\frac{144n^2-29}{(2n+1)(2n-1)}\right) A_n(j) \\ &- 36\frac{(12n-13)(12n-7)(12n-5)(12n+1)}{n(n-1)(2n-1)^2} A_{n-1}(j), \end{aligned}$$

*definida a partir de*

$$A_0(j) = 1, \qquad A_1(j) = j - 720, \qquad A_2(j) = j^2 - 1640j + 269280.$$

(b) (Fórmula tancada) *Per a tot $n \geq 0$, $A_n(j)$ és el polinomi*

$$\sum_{i=0}^{n} 12^{3i} \left( \sum_{m=0}^{i} (-1)^m \frac{\binom{-\frac{1}{12}}{i-m}\binom{-\frac{5}{12}}{i-m}\binom{n+\frac{1}{12}}{m}\binom{n-\frac{7}{12}}{m}}{\binom{2n-1}{m}} \right) j^{n-i}.$$

(c) (Equació diferencial) *Posem $c := 1728 = 12^3$. Per a tot $n \geq 0$, $A_n(j)$ és l'únic polinomi mònic que és solució de l'equació diferencial d'ordre* 4

$$\begin{aligned} &j^2(j-c)^2(n^2j-144)D^4(A_n,j) \\ &+j(j-c)\big(6n^2j^2 - 144(36n^2+7)j + \frac{c^2}{3}\big)D^3(A_n,j) \\ &-\big((2n^4-7n^2)j^3 - 48(72n^4-245n^2-30)j^2 \\ &\qquad -4c(240n^2+413)j + 320c^2\big)D^2(A_n,j) \\ &-\big((2n^4-n^2)j^2 - 24(72n^4-13n^2-12)j \\ &\qquad +2c(192n^2-107)\big)D(A_n,j) \\ &+\big(n^6j - 24(18n^4-n^2)\big)A_n(j) \\ &= 0. \end{aligned}$$

Per a demostrar aquest teorema i donar una segona demostració del teorema **4.4.10**, hipergeomètrica, en [K-Z] es comença per recordar la definició de les sèries hipergeomètriques de Gauss.

**4.5.2 Definició.** S'anomenen sèries hipergeomètriques de Gauss les sèries $F = {}_2F_1$ definides per

$$F(a,b,c;x) := \sum_{n\geq 0} \frac{(a)_n(b)_n}{(c)_n} x^n = \sum_{n\geq 0} \frac{\binom{-a}{n}\binom{-b}{n}}{\binom{-c}{n}} (-x)^n,$$

on $(a)_n := a(a+1)\cdots(a+n-1)$, i $c$ o bé és un nombre no enter, o bé és un nombre enter positiu. Són convergents, com a mínim, en el disc $|x| < 1$. Notem que si $a$ o $b$ és un nombre enter no positiu, llavors la sèrie és, de fet, un polinomi.

**4.5.3 Definició.** Els autors de [K-Z] no en tenen prou amb les sèries hipergeomètriques i treballen amb sèries hipergeomètriques truncades. Per a tot $n \geq 0$, defineixen quatre polinomis mònics $U_n^\varepsilon$, $V_n^\delta$, $\delta$, $\varepsilon \in \{0,1\}$, les funcions hipergeomètriques truncades i amb canvis de variable, per les fórmules

$$\begin{aligned}
j^n F\left(\frac{1}{12},\frac{5}{12},1;\frac{1728}{j}\right) &=: U_n^0(j) + O(j^{-1}),\\
j^{n-1}(j-1728)F\left(\frac{7}{12},\frac{11}{12},1;\frac{1728}{j}\right) &=: U_n^1(j) + O(j^{-1}),\\
(j-1728)^n F\left(\frac{1}{12},\frac{7}{12},1;\frac{1728}{1728-j}\right) &=: V_n^0(j) + O(j^{-1}),\\
j(j-1728)^{n-1} F\left(\frac{5}{12},\frac{11}{12},1;\frac{1728}{1728-j}\right) &=: U_n^0(j) + O(j^{-1}).
\end{aligned}$$

Aquestes funcions els permeten expressar d'una altra manera, més adient per als seus propòsits, els polinomis $A_n(j)$.

**4.5.4 Proposició.** *Els polinomis $A_n(j)$ definits per la relació de recurrència i les condicions inicials donades en el teorema* **4.5.1** (a),

*admeten les expressions següents en funció dels polinomis* $U_n^\varepsilon(j)$, $V_n^\delta(j)$*:*

$$\begin{aligned} A_n(j) &= \sum_{m=0}^{n} (-12)^{3m} \binom{n+\frac{1}{12}}{m} \binom{n-\frac{7}{12}}{m} \binom{2n-1}{m}^{-1} U_{n-m}^0(j) \\ &= \sum_{m=0}^{n} (-12)^{3m} \binom{n-\frac{5}{12}}{m} \binom{n-\frac{13}{12}}{m} \binom{2n-1}{m}^{-1} U_{n-m}^1(j) \\ &= \sum_{m=0}^{n} 12^{3m} \binom{n+\frac{1}{12}}{m} \binom{n-\frac{5}{12}}{m} \binom{2n-1}{m}^{-1} V_{n-m}^0(j) \\ &= \sum_{m=0}^{n} 12^{3m} \binom{n-\frac{7}{12}}{m} \binom{n-\frac{13}{12}}{m} \binom{2n-1}{m}^{-1} V_{n-m}^1(j). \square \end{aligned}$$

**4.5.5 Observació.** Aquestes fórmules poden ésser invertides de manera que, per exemple, es té que

$$U_n^0(j) = \sum_{m=0}^{n} 12^{3m} \binom{n+\frac{1}{12}}{m} \binom{n-\frac{7}{12}}{m} \binom{2n-1}{m}^{-1} A_{n-m}(j).$$

La proposició **4.5.4** permet provar les relacions de congruència mòdul $p$ entre el polinomi supersingular i les sèries hipergeomètriques truncades, de manera que s'obtenen quatre descripcions més del polinomi supersingular.

**4.5.6 Proposició.** *Sigui* $p \geq 5$ *un nombre primer i posem* $p = 12m - 8\delta - 6\varepsilon + 1$*, amb* $m \geq 0$*,* $\delta$*,* $\varepsilon \in \{0, 1\}$*. Llavors,*

$$ss_p(j) \equiv U_m^\varepsilon(j) \equiv V_m^\delta(j) \pmod{p}. \square$$

**4.5.7 Observació.** Notem que, aquí, en [K-Z] se surt de la manera que s'ha usat habitualment per a escriure $k = p - 1 = 12m + 4\delta + 6\varepsilon$, i s'usa el fet que $-8 \equiv 4$, $-6 \equiv 6 \pmod{12}$, que pot fer variar els valors de $m$ i de $\delta$.

Com a corol·lari d'aquesta proposició, s'obté una segona demostració del teorema **4.4.10**. D'altra banda, com a corol·lari del teorema **4.5.1**, obtenen el resultat següent, que atribueixen a Atkin.

**4.5.8 Proposició.** *Es tenen els valors especials següents:*

$$(A_n, A_n) = -12^{6n-1}\frac{(-1/12)_n(5/12)_n(7/12)_n(13/12)_n}{(2n-1)!(2n)!},$$
$$A_n(0) = (-12)^{3n+1}\frac{(-1/12)_n(5/12)_n}{(2n-1)!},$$
$$A_n(1728) = -12^{3n+1}\frac{(-1/12)_n(7/12)_n}{(2n-1)!}.\ \square$$

A continuació, presentem algunes propietats hipergeomètriques de les formes modulars $F_k(\tau)$, per a $k \not\equiv 3 \pmod 3$, i dels seus polinomis associats, $\tilde{F}_k(j)$. Recordem que aquesta forma modular ha estat definida com l'única solució, normalitzada amb un factor constant, de l'equació diferencial de segon ordre

$$\vartheta_{k+2}\vartheta_k F_k - \frac{k(k+2)}{144}E_4F_k = 0.$$

**4.5.9 Definició.** Sigui $k \geq 4$ un nombre enter parell, i posem $k = 12m + 4\delta + 6\varepsilon$, amb $m \geq 0$, $\delta \in \{0,1,2\}$, $\varepsilon \in \{0,1\}$. Definim

$$\nu_0 := \frac{1-2\delta}{3}, \qquad \nu_1 := \frac{1-2\varepsilon}{2}, \quad \nu_\infty := \frac{k+1}{6},$$
$$X_0 := J := \frac{j}{1728}, \quad X_1 := 1-J, \quad X_\infty := -1,$$
$$Y_0 := E_4^3, \qquad Y_1 := -E_6^2, \qquad Y_\infty := -1728\Delta.$$

Notem que se satisfan les igualtats

$$\nu_0+\nu_1+\nu_\infty = 2m+1, \quad X_0+X_1+X_\infty = 0, \quad Y_0+Y_1+Y_\infty = 0.$$

**4.5.10 Teorema.** *Sigui $k \geq 0$, $k \not\equiv 2 \pmod 3$, un nombre enter parell, que escrivim en la forma $k = 12m+4\delta+6\varepsilon$, amb $\delta, \varepsilon \in \{0,1\}$.*

(a) (Equació diferencial) *El polinomi $\tilde{F}_k(j)$ és l'única solució polinòmica normalitzada de l'equació diferencial d'ordre 2*

$$\begin{aligned} &j(j-1728)D^2(\tilde{F},j)\\ +((1-\nu_1)j+(1-\nu_0)(j-1728))&D(\tilde{F}_k,j)\\ &+m(m-\nu_\infty)\tilde{F}_k(j) = 0. \end{aligned}$$

(b) (Fórmules tancades) *Sigui $\sigma$ qualsevol permutació de $\{0,1,\infty\}$. Se satisfan les igualtats*

$$\tilde{F}_k(j) = (\mathrm{sgn}(\sigma)\cdot 1728)^m \binom{m-\nu_{\sigma(\infty)}}{m} X_{\sigma(0)}^m \cdot F\left(-m, -m+\nu_{\sigma(0)}, 1-\nu_{\sigma(\infty)}; -\frac{X_{\sigma(\infty)}}{X_{\sigma(0)}}\right),$$

$$F_k(\tau) = \mathrm{sgn}(\sigma)^m E_4(\tau)^\delta E_6(\tau)^\varepsilon \cdot \sum_{l=0}^{m} (-1)^l \binom{m-\nu_{\sigma(0)}}{l}\binom{m-\nu_{\sigma(\infty)}}{m-l} Y_{\sigma(\infty)}^l Y_{\sigma(0)}^{m-l}.$$

(c) (Relació de recursió) *Per als polinomis $\tilde{F}_k(j)$ i per a $k \geq 12$ se satisfà que:*

$$\begin{aligned}(m+1)(m-\nu_\infty)(1-\nu_\infty)\tilde{F}_{k+12}(j) - \\ \nu_\infty\big((1+\nu_\infty)(1-\nu_\infty)j - \\ 1728(1-\nu_0)(\nu_0+\nu_1)+2m(m-\nu_\infty)\big)\tilde{F}_k(j) + \\ 1728^2(m-\nu_0)(m-\nu_1)(1+\nu_\infty)\tilde{F}_{k-12}(j) = 0.\end{aligned}$$

(d) (Funció generadora) *Per a tot $k \geq 0$, i tot $\alpha$, sigui $G_{k,\alpha}(\tau)$ el coeficient de $X^k$ en la sèrie $(1-3E_4(\tau)X^4+2E_6(\tau)X^6)^\alpha$. Llavors,*

$$F_k(\tau) = (-1)^{m+\delta} 2^{2m-\varepsilon} \binom{2m+\varepsilon}{m}\binom{\frac{1}{6}(k-2)}{m+\varepsilon} G_{k,\frac{k-2}{6}}(\tau). \square$$

**4.5.11 Observació.** La part (d) d'aquest teorema permet explicar per què les formes modulars $F_{p-1}$, $G_{p-1}$ i $H_{p-1}$ del teorema **4.3.14** proporcionen, llevat de factors escalars, un mateix polinomi mòdul $p$. En efecte, són les especialitzacions de $G_{p-1,\alpha}$ als tres valors $\frac{-1}{2}$, $\frac{p-1}{2}$, i $\frac{p-3}{6}$, que són congrus mòdul $p$.

**4.5.12 Observació.** La fórmula tancada per a $F_k$ es pot escriure com

$$F_k = \mathrm{sgn}(\sigma)^m E_4^\delta E_6^\varepsilon H_m(1-\nu_{\sigma(\infty)}, 1-\nu_\sigma(0), Y_{\sigma(\infty)}, Y_{\sigma(0)}),$$

on $H_n(k,l,X,Y) := \sum_{r+s=n} (-1)^r \binom{n+k-1}{s}\binom{n+l-1}{r} X^r Y^s$ és essencialment el símbol $3J$ (moment angular) de Wigner de la mecànica quàntica i està relacionat amb el claudàtor de Cohen de formes modulars.

No contents amb tot això, els autors de [K-Z] defineixen un altre producte escalar de manera que els polinomis ortogonals per a aquest producte proporcionen una altra visió del polinomi supersingular.

Considerem l'anell $W := \mathbb{C}[j^{1/3}, (j-1728)^{1/2}]$ identificat amb l'espai de les funcions holomorfes en $\mathcal{H}$ que són invariants per a l'acció del subgrup derivat $[\Gamma,\Gamma]$ de $\Gamma := \mathbf{PSL}(2,\mathbb{Z})$ i que tenen creixement com a màxim polinòmic en $q^{-1}$.

Per a tot $r \in \mathbb{Z}/6\mathbb{Z}$, sigui $\chi^r$ el caràcter del grup cíclic $\Gamma/[\Gamma,\Gamma]$ determinat unívocament per $\chi^r\left(\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix} \pmod{[\Gamma:\Gamma]}\right) := e^{\pi i r/3}$.

Sigui $W = \bigoplus_{r \bmod 6} W(r)$ la descomposició corresponent de $W$; o sigui, $W(r)$ és l'espai propi corresponent a $\chi^r$ per a l'acció de $\Gamma$.

Si es determinen $\delta$ i $\varepsilon$ per la congruència $2r \equiv 4\delta + 6\varepsilon \pmod{12}$, llavors $W(r)$ s'identifica amb $j^{\delta/3}(j-1728)^{\varepsilon/2}\mathbb{C}[j]$.

**4.5.13 Definició.** Definim en $W$ un producte escalar per

$$(f,g) := \int_0^{1728} \frac{f(j)g(j)}{j^{1/3}(j-1728)^{1/2}}dj, \qquad f,g \in W.$$

**4.5.14 Proposició.** *En $j^{\delta/3}(j-1728)^{\varepsilon/2}\mathbb{R}[j] \subseteq W(r)$, aquest producte escalar és definit positiu o definit negatiu, segons que sigui $\varepsilon = 0$ o $\varepsilon = 1$.* $\square$

Per tant, obtenim sis famílies de polinomis mònics $\{f_m^r\}_{m\geq 0}$, $f_m^r$ de grau $m$, tals que els polinomis $j^{\delta/3}(j-1728)^{\varepsilon/2}f_m^r$ són ortogonals per a aquest producte escalar.

**4.5.15 Definició.** Per a cada classe $2r \equiv 4\delta + 6\varepsilon \pmod{12}$, i cada $m \geq 0$, posem

$$\hat{F}_m^{(r)}(j) := j^m F\left(-m, -m+\nu_0, 1-\nu_\infty, \frac{1728}{j}\right),$$

on $\nu_0 := \dfrac{1-2\delta}{3}$ i $\nu_\infty := \dfrac{12m+4\delta+6\varepsilon+1}{6}$.

**4.5.16 Observació.** Si $2r \not\equiv 2 \pmod 3$ i $k = 12m + 4\delta + \varepsilon$, llavors $\hat{F}_m^{(r)}(j)$ només és el polinomi $\tilde{F}_k(j)$ renormalitzat a fi que sigui mònic.

**4.5.17 Teorema.** *Per a tot* $r \pmod 6$ *i tot* $m \geq 0$*, se satisfà que*

$$f_n^{(r)} = \hat{F}_n^{(r)}. \square$$

**4.5.18 Observació.** Llevat del factor 1728, aquest polinomi és essencialment un polinomi de Jacobi. Aquests darrers són polinomis $P_n^{(\alpha,\beta)}$ que generalitzen els polinomis de Txebychev, als quals els corresponen paràmetres $(1/2, 1/2)$ i s'apleguen en quatre tipus (parell i senar, primera i segona espècie) corresponents a la descomposició en quatre parts de $\mathbb{C}[x^{1/2}, (1-x)^{1/2}]$; els paràmetres dels polinomis de [K-Z] són $(1/3, 1/2)$, i hi ha 6, en lloc de 4, famílies.

L'article [K-Z] s'acaba amb algunes consideracions sobre els denominadors dels polinomis d'Atkin i sobre la relació entre els polinomis supersingulars i el polinomis modulars, que no comentarem aquí.

# Bibliografia


[1] Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörpern. *Abh. Math. Sem. Hamburg*, **14** (1941), 197–272.

[2] Eichler, M.: Über die Idealklassenzahl total definiter Quaternionenalgebren. *Math. Z.*, **43** (1938), 102–109.

[3] Hasse, H.: Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade $p$ über elliptischen Funktionenkörpern der Charakteristik $p$. *J. Reine Angew. Math.* , **172** (1934), 77–85. *Math. Abhandlungen*, **2**, 161–169.

[4] Kaneko, M.; Zagier, D.: Supersingular $j$-invariants, hypergeometric series, and Atkin's orthogonal polynomials. *Computational perspectives on Number Theory*, 97–126, AMS/IP Stud. Adv. Math., **7**, Amer. Math. Soc., Providence, RI, 1998.

[5] Koblitz, N.: *Introduction to Elliptic Curves and Modular Forms*. GTM 97, Springer-Verlag, 1984.

[6] Serre, J-P.: *Course d'Arithmétique*. Presses Universitaires de France, 1970.

[7] Serre, J-P.: Congruences et formes modulaires (d'après H. P. F. Swinnerton-Dyer). *Séminaire Bourbaki*, **416**, 1971–72; Œuvres, **95**, vol. III, 74–88.

[8] Travesa, A.: *Teoria de nombres*. Universitat de Barcelona, 1992. http://atlas.mat.ub.es/personals/travesa.

A. Travesa

Facultat de Matemàtiques

Universitat de Barcelona

Gran Via de les Corts Catalanes, 585

E-08007, Barcelona

**travesa@ub.edu**

# Capítol 5

# Funcions període per a formes d'ona de Maass

P. Bayer

## Introducció

Aquesta exposició proporciona una introducció a l'estudi de les formes d'ona de Maass i al de les seves funcions període. Les formes d'ona de Maass són certes funcions de variable complexa, no necessàriament meromorfes, de quadrat integrable, que estan lligades a l'espectre discret de l'operador de Laplace-Beltrami. La seva definició generalitza el concepte de forma automorfa. En el cas no meromorf, però, se'n coneixen pocs exemples explícits.

L'estudi de funcions període associades a formes de Maass s'inicia amb Lewis [4] i Lewis i Zagier [5]. Tal com fan aquests autors, tractarem les funcions període únicament en el cas del grup modular $\mathbf{SL}(2,\mathbb{Z})$.

Amb finançament parcial de MTM2006-04895 i MRTN-CT-2006-035495.

## 5.1 Introducció a les formes d'ona de Maass

### 5.1.1 L'operador de Laplace

L'operador de Laplace es troba en el centre de la teoria clàssica del potencial i de la teoria de Hodge. A $\mathbb{R}^n$, l'expressió d'aquest operador és

$$\Delta := \sum_{i=1}^{n} \frac{\partial^2}{\partial x_i^2}.$$

Es tracta, doncs, d'un operador diferencial de segon ordre, que és el·líptic. Les funcions de variable complexa que anul·len l'operador de Laplace són les funcions harmòniques.

L'operador de Laplace es generalitza a espais no euclidians i pot esdevenir un operador el·líptic o bé un operador hiperbòlic. Per exemple, en l'espai-temps de Minkowski, l'operador de Laplace dóna lloc a l'operador de D'Alembert,

$$\Box := \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2} - \frac{1}{c^2}\frac{\partial^2}{\partial t^2},$$

que és un operador hiperbòlic.

De fet, l'operador de Laplace pot ser definit sobre qualsevol varietat riemanniana o pseudo-riemanniana. En aquests casos, rep el nom d'operador de Laplace-Beltrami. La seva acció sobre les funcions diferenciables és donada per

$$\Delta f = \frac{1}{\sqrt{|\,g|}}\,\partial_i\left(\frac{\partial^2 f}{\partial u^i\,\partial u^j}\sqrt{|\,g|}g^{ij}\partial_j f\right),$$

on $(g^{ij})$ denota la matriu inversa de la matriu $g = (g_{ij})$ que defineix la mètrica. Se satisfà que

$$\Delta f = \text{div grad} f.$$

En coordenades locals, l'operador de Laplace-Beltrami s'expressa en termes del tensor $g$ i dels símbols de Christoffel $\{\Gamma_{ij}^k\}$:

$$\Delta f = g^{ij}\left(\frac{\partial^2 f}{\partial u^i\,\partial u^j} - \Gamma_{ij}^k\frac{\partial f}{\partial u^k}\right).$$

L'operador de Laplace intervé en la modelització de molts fenòmens físics. En mecànica ondulatòria és utilitzat per a estudiar la propagació de les ones. En termodinàmica és emprat per a estudiar el flux de la calor. En electrostàtica dóna lloc a les equacions de Laplace i de Poisson. En mecànica quàntica intervé en l'equació de Schrödinger.

### 5.1.2 Formes d'ona de Maass. Conjectura de Selberg. Llei de Weyl

En el semiplà superior complex $\mathcal{H}$, suposem donada la mètrica hiperbòlica,

$$ds = \frac{|\,dz|}{y}, \quad d\mu := \frac{1}{y^2}\,dz\,d\overline{z},$$

on $ds$ denota l'element d'arc i $d\mu$, l'element d'àrea. Ambdós elements són invariants per l'acció usual del grup $\mathbf{SL}(2,\mathbb{R})$ en $\mathcal{H}$.

En el pla hiperbòlic, l'operador de Laplace es defineix segons

$$\Delta = -y^2\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}\right),$$

i és, també, invariant per l'acció de $\mathbf{SL}(2,\mathbb{R})$. Es tracta d'un operador autoadjunt, per la qual cosa el seu espectre és real.

**5.1.1 Definició.** Donat un grup fuchsià cofinit $\Gamma$, una aplicació

$$u : \mathcal{H} \to \mathbb{C}$$

de classe $\mathcal{C}^\infty$ es diu que és una forma d'ona de Maass respecte de $\Gamma$ si satisfà les condicions següents:

(i) La funció $u$ és una funció pròpia de l'operador de Laplace: existeix una constant $\lambda \in \mathbb{R}$, $\lambda \geq 0$, tal que

$$\Delta u = \lambda u.$$

(ii) La funció $u$ és invariant per l'acció de $\Gamma$: per a tota $\gamma \in \Gamma$, es té que

$$u(\gamma z) = u(z).$$

(iii) La funció $u$ és de quadrat integrable en $\Gamma\backslash\mathcal{H}$:

$$\int_{\mathcal{F}} |u(z)|^2 \, d\mu(z) < \infty,$$

on la integral s'estén a un domini fonamental $\mathcal{F} = \mathcal{F}_\Gamma$ de $\Gamma$ en $\mathcal{H}$.

Per abreujar, parlarem de formes de Maass per a designar les formes d'ona de Maass.

*La conjectura de Selberg.* El paràmetre espectral $\lambda$ se sol escriure en la forma

$$\lambda = \frac{1}{4} + R^2.$$

Una conjectura deguda a Selberg afirma que si $\Gamma \subseteq \mathbf{SL}(2,\mathbb{Z})$ és un subgrup de congruència i $\lambda \neq 0$, aleshores $R \in [0,\infty)$; és a dir, no hi ha valors espectrals petits, atès que es tindria $\lambda \geq \frac{1}{4}$, per a tot valor propi no nul de $\Delta$.

Per a un grup fuchsià cofinit qualsevol, els valors propis $\lambda \in (0, \frac{1}{4})$ s'anomenen excepcionals.

Denotem per $\mathcal{M}(\Gamma,\lambda)$ l'espai de les formes de Maass per $\Gamma$ de valor espectral $\lambda$. Si $\Gamma$ és un grup de congruència, també es poden considerar formes de Maass amb caràcter (amb les definicions habituals); denotem per $\mathcal{M}(\Gamma,\chi,\lambda)$ l'espai corresponent.

**5.1.2 Proposició.** (i) *Els espais $\mathcal{M}(\Gamma,\lambda)$, $\mathcal{M}(\Gamma,\chi,\lambda)$ són de dimensió finita.*

(ii) *Si $\lambda > 0$, tota forma de Maass és cuspidal, en el sentit que en cada punta tendeix ràpidament a zero.*

(iii) *Les formes de Maass generen la part discreta de l'espectre de l'operador $\Delta$ de Laplace-Beltrami de $\Gamma\backslash\mathcal{H}$.*

(iv) *La part contínua de l'espectre de $\Delta$ és generada per sèries d'Eisenstein (cf. la secció (5.5)).*

Els espais $\mathcal{M}(\Gamma,\lambda)$, $\mathcal{M}(\Gamma,\chi,\lambda)$ estan dotats d'un producte escalar de Petersson,

$$(u,v) = \int_{\mathcal{F}} u(z)\overline{v(z)} d\mu(z),$$

per mitjà del qual esdevenen espais de Hilbert, de dimensió finita.

*Llei de Weyl.* Si $\Gamma$ és un grup de congruència i $\chi$ és un caràcter de Dirichlet mòdul $N$, els valors propis

$$0 = \lambda_0 < \lambda_1 \leq \lambda_2 \leq \ldots,$$

comptats amb les seves multiplicitats, formen una successió discreta de la qual se sap que satisfà un llei de Weyl general. En particular, si $\Gamma = \Gamma_0(N)$, i definim la funció comptadora espectral

$$N_{\Gamma_0(N)}(T) := \#\{\lambda_n \leq T : \lambda_n \text{ valor propi de } \Delta_{\Gamma_0(N)}\},$$

se satisfà la fórmula asimptòtica

$$N_{\Gamma_0(N)}(T) = \frac{\mu(\mathcal{F}_N)}{4\pi}\, T - \frac{2\kappa}{\pi}\sqrt{T}\ln\,\sqrt{T} + A\sqrt{T} + \mathrm{O}\left(\frac{\sqrt{T}}{\ln\sqrt{T}}\right),$$

on $A$ és una certa constant que depèn del nivell $N$ i $\kappa$ denota el nombre de puntes de $\Gamma_0(N)$ (cf. [8]).

Es creu que per a grups fuchsians $\Gamma$ no co-compactes, però cofinits i genèrics, l'espectre discret de l'operador de Laplace-Beltrami hauria de ser finit. És a dir, la presència de simetries aritmètiques o geomètriques seria la causa de la infinitud de l'espectre. Aquí el terme genèric s'empra en el sentit que els grups fuchsians excepcionals defineixen un subconjunt de mesura zero en determinats espais de deformacions d'aquestes estructures.

### 5.1.3 Primers exemples

(i) Les funcions $y^s, y^s x$, $s \in \mathbb{C}$, són valors propis de l'operador de Laplace de valor propi $s(1-s)$.

(ii) Les funcions

$$h(x+iy) := y^{1/2} K_{s-\frac{1}{2}}(2\pi|\,a|y) e^{2\pi i a x},$$

on $x, y \in \mathbb{R}$, $s \in \mathbb{C}$, $a \neq 0$, i $K_s(x)$ denota la funció de Bessel hiperbòlica de segona espècie, són formes de Maass de valor propi $s(1-s)$.

Avancem que les funcions $K_s(x)$ de l'expressió anterior mostren el comportament asimptòtic

$$K_s(x) \sim \sqrt{\frac{\pi}{2x}}\, e^{-x}, \quad x \to \infty;$$

per tant, són de decreixement ràpid a l'infinit. Per a més informació sobre aquestes funcions, vegeu la subsecció que segueix.

### 5.1.4 Funcions de Bessel

Les funcions de Bessel foren considerades per primera vegada per Daniel Bernoulli, l'any 1738, en una memòria sobre l'oscil·lació de cadenes pesades. Posteriorment, foren generalitzades per Bessel.

L'equació diferencial ordinària de segon ordre

$$x^2 \frac{d^2y}{dx^2} + x\frac{dy}{dx} + (x^2 - s^2)y = 0 \tag{5.1}$$

és coneguda amb el nom d'equació diferencial de Bessel. Té una singularitat regular en $x = 0$ i una singularitat irregular en $x = \infty$.

Donat un $s \in \mathbb{C}$, es defineix la funció de Bessel de primera espècie segons

$$J_s(x) := \frac{1}{2\pi i}\left(\frac{x}{2}\right)^s \int_{-\infty}^{(0+)} e^{\left(t - \frac{x^2}{4t}\right)}\, t^{-s-1}\, dt.$$

Per definició, el contorn de la primera integral parteix de $-\infty$, recorre la circumferència unitat en el sentit invers de les agulles del rellotge i retorna a $-\infty$. Si $s = n$ és enter, la definició se simplifica i es pot escriure

$$J_n(x) \quad := \frac{1}{2\pi i} \oint e^{\frac{x}{2}(t - t^{-1})} t^{-n-1}\, dt,$$

on el contorn de la integral encercla l'origen i el recorregut es pren en sentit invers de les agulles del rellotge. Quan $s = n$ és un enter positiu, es té la representació integral

$$J_n(x) = \frac{1}{\pi}\int_0^{\pi} \cos(n\theta - x\sin\theta)\, d\,\theta.$$

La funció de Bessel de segona espècie (dita, també, funció de Weber) es defineix per a valors de $s$ no enters segons

$$Y_s(x) := \frac{J_s(x)\cos(s\,\pi) - J_{-s}(x)}{\sin(s\pi)}.$$

I per a $s = n$, enter,

$$Y_n(x) := \lim_{s\to n} Y_s(x).$$

Les funcions de Bessel $\{J_s, Y_s\}$ formen un sistema independent de solucions de l'equació diferencial de Bessel (5.1). Per a $n$ enter, les funcions $J_n(x)$ són regulars en $x = 0$ mentre que les funcions $Y_n(x)$ presenten en $x = 0$ una singularitat logarítmica.

L'equació diferencial ordinària de segon ordre

$$x^2\frac{d^2y}{dx^2} + x\frac{dy}{dx} - (x^2 + s^2)y = 0 \tag{5.2}$$

és coneguda amb el nom d'equació diferencial de Bessel modificada.

Per a un $s \in \mathbb{C}$, es defineix la funció de Bessel modificada de primera espècie segons

$$I_s(x) := i^{-s}J_s(ix).$$

Per a $s = n$ enter, aquesta funció es pot representar com

$$I_n(x) := \frac{1}{2\pi i}\oint e^{\frac{x}{2}(t+t^{-1})}t^{-n-1}\,dt.$$

Per a un $s \in \mathbb{C}$, es defineix la funció de Bessel modificada de segona espècie segons

$$K_s(z) = \frac{\pi}{2}\frac{I_{-s}(z) - I_s(z)}{\sin(s\,\pi)}.$$

Per a $s = n$ enter, es té que

$$K_n(x) = \frac{1}{2}\int_0^\infty e^{-\frac{x}{2}(t+t^{-1})}t^{n-1}\,dt.$$

Les funcions de Bessel modificades $\{I_s(x),\, K_s(x)\}$ formen un sistema independent de solucions de l'equació diferencial de Bessel modificada (5.2). Per a $n$ enter, les funcions $I_n(x)$ són regulars en $x = 0$ mentre que les funcions $K_n(x)$ tenen en $x = 0$ una singularitat logarítmica. Les funcions de Bessel modificades també reben el nom de funcions de Bessel hiperbòliques.

### 5.1.5 Desenvolupaments de formes de Maass

En aquesta secció suposarem que $\Gamma = \Gamma_0(N)$.

**5.1.3 Notació.** Per a cada punta $p_j \in \mathbb{P}^1(\mathbb{Q})$ de $\Gamma_0(N)$, considerem un conjunt de matrius $\sigma_j \in \mathbf{SL}(2,\mathbb{R})$ tals que

(i) $\sigma_j(i\,\infty) = p_j$,

(ii) $\sigma_j S \sigma_j^{-1} = S_j$,

on $S(z) := z + 1$ és un generador del grup d'isotropia $\Gamma_\infty$ de la punta de l'infinit i $S_j$ és un generador del grup d'isotropia $\Gamma_{p_j}$ de la punta $p_j$. Aleshores, $\sigma_j$ està unívocament determinada llevat de translacions.

Posarem, també,

$$\kappa_n(y) = \kappa_n(R, y) := y^{1/2}\, K_{iR}(2\pi|\, n|y), \quad \lambda = \frac{1}{4} + R^2.$$

Observem que $\kappa_{-n}(y) = \kappa_n(y)$.

**5.1.4 Proposició.** *Siguin $\chi$ un caràcter de Dirichlet mòdul $N$ i $u \in \mathcal{M}(\Gamma_0(N), \chi, \lambda)$ una forma de Maass. Aleshores, a l'entorn de cada punta $p_j$, la forma $u$ admet un desenvolupament en sèrie de Fourier del tipus*

$$u_j(x + iy) = u_{|\sigma_j}(x + iy) = \sum_{|n|>1} c_j(n)\kappa_n(y)e^{2\pi i n x}, \quad 1 \le j \le \kappa.$$

### 5.1.6 L'operador de reflexió

Donades la matriu $J := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, i una matriu qualsevol $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, es defineix

$$M^* = JMJ^{-1} = \begin{bmatrix} a & -b \\ -c & d \end{bmatrix}.$$

Si $\chi$ és un caràcter de Dirichlet mòdul $N$, aleshores

$$\chi(M^*) = \chi(d) = \chi(M)$$

i la matriu $J$ defineix una involució en $\mathcal{M}(\Gamma_0(N), \chi, \lambda)$.

Una forma de Maass $u \in \mathcal{M}(\Gamma_0(N), \chi, \lambda)$ s'anomena parella, respectivament senar, si $u_{|\,J} := u(-\overline{z}) = u$, respectivament, si $u_{|\,J} = -u$. Si una forma de Maass és parella, el seu desenvolupament de Fourier només conté termes en cosinus; si és senar, només conté termes en sinus. És a dir,

$$u(z) = \sum_{n=1}^{\infty} a(n)\,\kappa_n(y)\cos(2\pi n x), \quad \text{si } u \text{ és parella,}$$

$$u(z) = \sum_{n=1}^{\infty} a(n)\,\kappa_n(y)\sin(2\pi n x), \quad \text{si } u \text{ és senar.}$$

Cal observar, però, que les formes $u_j$ en general no són diagonalitzables simultàniament respecte de $J$.

## 5.2 Formes de Maass-Hecke

### 5.2.1 Formes de Maass per a grups de congruència

Els operadors de Hecke actuen en els espais de formes de Maass i en aquest context es té una teoria de formes noves i de formes velles similar a la teoria d'Atkin-Lehner. Aquesta permet una descomposició

$$\mathcal{M}(\Gamma_0(N), \chi, \lambda) = \mathcal{M}^{\text{vell}}(\Gamma_0(N), \chi, \lambda) \oplus \mathcal{M}^{nou}(\Gamma_0(N), \chi, \lambda).$$

**5.2.1 Definició.** Una funció $u \in \mathcal{M}^{nou}(\Gamma_0(N), \chi, \lambda)$ es diu que és una forma de Maass-Hecke, nova i normalitzada, si $f$ és una funció pròpia de la involució $J$ i de tots els operadors de Hecke $T_n$ per als quals $\mathrm{mcd}(n, N) = 1$, i si, a més, el primer coeficient de Fourier de $u$ és 1; és a dir $c(1) = 1$, on

$$u(x + iy) = \sum_{n \neq 0} c(n)\, \kappa_n(y)\, e^{2\pi i n x},$$

és el desenvolupament de $u$ a l'entorn de la punta de l'infinit.

De manera similar al cas meromorf, se satisfà el teorema següent.

**5.2.2 Teorema.** *Sigui $u$ una forma de Maass nova i normalitzada tal que*

$$T_n(u) = \lambda(n)u, \quad u_{|\,J} = \varepsilon u,$$

*on $\varepsilon \in \{-1, 1\}$. Si el desenvolupament en sèrie de Fourier de $u$ és*

$$u(z) = \sum_{|\,n| \geq 1} c(n)\kappa_n(y)e^{2\pi i n x}, \quad c(1) = 1,$$

*se satisfà que*

$$c(n) = \lambda(n), \quad c(-n) = \varepsilon\lambda(n),$$

*per a tot $n \in \mathbb{Z}_{\geq 0}$. A més, se satisfan les relacions multiplicatives*

$$c(m)c(n) = \sum_{\substack{d \mid \mathrm{mcd}(m,n) \\ d>0}} \chi(d)c\left(\frac{mn}{d^2}\right), \quad \mathrm{mcd}(n, N) = 1, m \in \mathbb{Z},$$

$$c(m)c(p) = c(mp), \quad p|N,\ m \in \mathbb{Z}.$$

Notem que si $u$ és una forma nova, normalitzada, de valors propis $\lambda(n)$, aleshores $\varepsilon u$ també ho és. En general, es té que

$$T_n^* = \overline{\chi(n)}T_n, \quad \overline{\lambda(n)} = \overline{\chi(n)}\lambda(n), \quad \overline{c(n)} = \overline{\chi(n)}c(n),$$

sempre que $\mathrm{mcd}(n, N) = 1$. En particular, si $\chi(n) = -1$, $c(n)$ és purament imaginari. Si $\chi(n) = 1$, $c(n)$ és real.

Les primeres formes construïdes per Maass eren noves i de coeficients reals; per tant, tenien molts coeficients iguals a zero. Concretament, $c(n) = 0$, per a tots els $n \in \mathbb{Z}_{\geq 0}$ tals que $\mathrm{mcd}(n, N) = 1$ i $\chi(n) \neq 1$.

### 5.2.2 Formes de Maass de tipus MR

Sigui $F = \mathbb{Q}(\sqrt{m})$ un cos quadràtic real, on $m > 0$ és un enter lliure de quadrats i $m \equiv 1 \pmod 4$. Suposem que el nombre de classes restringit de $F$ és igual a 1. És a dir, que tot ideal de l'anell d'enters $\mathcal{O}_F$ és principal i generat per un element totalment positiu. Aleshores, $m$ ha de ser un nombre primer (cf. [7]). Per exemple, aquest és el cas si

$$m \in \{\, 5,\ 13,\ 17,\ 29,\ 37,\ 41,\ 53 \,\}.$$

Sigui $\eta \in \mathcal{O}_F^*$ la unitat fonamental per a la qual

$$N_{F/\mathbb{Q}}(\eta) = -1.$$

Per a cada $k \in \mathbb{Z}$, l'aplicació

$$\psi(\mathfrak{a}) := \left|\frac{x}{x'}\right|^{\pi i k/\log \eta}, \qquad \text{on } \mathfrak{a} = (x),\ x > 0,$$

defineix un caràcter de Hecke sobre els ideals de $\mathcal{O}_F$. Hem utilitzat $x'$ per a denotar el conjugat galoisià de $x$.

Considerem la sèrie $L$ de Hecke associada al caràcter $\psi$,

$$L(s,\psi) := \sum_{\mathfrak{a}\neq(0)} \frac{\psi(\mathfrak{a})}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1-\psi(\mathfrak{p})N(\mathfrak{p})^{-s}}.$$

Com és ben sabut, la sèrie completada

$$\Lambda(s,\psi) = \left(\frac{\sqrt{m}}{\pi}\right)^s \Gamma\left(\frac{s}{2} + \frac{i\pi k}{2\log\eta}\right) \Gamma\left(\frac{s}{2} - \frac{i\pi k}{2\log\eta}\right) L(s,\psi)$$

satisfà una equació funcional quan $s \mapsto 1 - s$.

**5.2.3 Proposició.** *Sigui $m > 1$ un enter lliure de quadrats, $m \equiv 1 \pmod 4$. Suposem que el nombre de classes restringit de $\mathbb{Q}(\sqrt{m})$ és igual a 1. Aleshores, la sèrie*

$$\varphi(x+iy) := \sum_{\mathfrak{a}} \psi(\mathfrak{a})\, y^{1/2}\, K_{iR}(2\pi N(\mathfrak{a})y)\cos(2\pi N(\mathfrak{a})x)$$

*és una forma de Maass per al grup de congruència $\Gamma(m)$ quan es pren*

$$R = \frac{\pi k}{\log \eta}, \quad k \neq 0.$$

*Més precisament,* $\varphi \in \mathcal{M}(\Gamma_0(m), \chi_m, \frac{1}{4}+R^2)$*, on* $\chi_m$ *denota el símbol de Kronecker.*

*Demostració.* (Indicació) Es comprova que per a tota matriu $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{SL}(2,\mathbb{Z})$, tal que $c \equiv 0 \pmod{m}$, es té que

$$\varphi\left(\frac{az+b}{cz+d}\right) = \left(\frac{m}{d}\right)\varphi(z).$$

A més,

$$\varphi\left(-\frac{1}{mz}\right) = \varphi(z).$$

□

**5.2.4 Exemple.** Per a les dades següents:

$$m = 5, \quad \eta = \frac{1}{2}(1+\sqrt{5}), \quad k = 3830, \quad R = 25004.164978...,$$

$$m = 5, \quad \eta = \frac{1}{2}(1+\sqrt{5}), \quad k = 15320, \quad R = 100016.659912...,$$

és $\mathcal{M}(\Gamma_0(5), \chi_5, \frac{1}{4}+R^2) \neq (0)$.

### 5.2.3 Relació amb la conjectura d'Artin

Donada una representació galoisiana, contínua i irreductible,

$$\rho: \ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbf{GL}(n,\mathbb{C}),$$

la conjectura d'Artin prediu que la seva funció $L$,

$$\begin{aligned} L(s,\rho) &:= \prod_{p}^{\infty} \det(1-\rho(\mathrm{Frob}_p)p^{-s})^{-1} \\ &= \sum_{n=1}^{\infty} \lambda_\rho(n) n^{-s}, \end{aligned}$$

definida inicialment per a $\mathrm{Re}(s) > 1$ i holomorfa en aquest semiplà, admet una prolongació analítica en una funció entera de $s \in \mathbb{C}$. Per

un teorema degut a Brauer, aquesta funció admet una prolongació meromorfa a tot $\mathbb{C}$ i satisfà una equació funcional. Però resta pendent la qüestió de si aquesta funció pot tenir pols a la banda crítica.

El teorema següent, degut a Booker (cf. [1], [2]), relaciona la conjectura d'Artin en dimensió 2 amb les formes de Maass.

**5.2.5 Teorema.** *Sigui $\rho$ una representació de Galois, continua, parella i de dimensió 2. Si la sèrie $L(s,\rho)$ s'estén a una funció entera, aleshores la funció*

$$\varphi(z) := \sum_{n=1}^{\infty} \lambda_\rho(n)\, y^{1/2}\, K_0(2\pi n y)\cos(2\pi n x), \quad z = x + iy,$$

*és una forma pròpia de Maass-Hecke respecte del grup principal de congruència $\Gamma(N)$, on $N$ denota el conductor d'Artin de $\rho$, de valor espectral,*

$$\lambda_\varphi = \frac{1}{4}.$$

El recíproc es creu que també és cert: tota forma pròpia de Maass-Hecke $\varphi$, parella, de valor espectral $\lambda_\varphi = \dfrac{1}{4}$, ha de provenir d'una representació galoisiana complexa de dimensió 2, irreductible i parella, segons el procediment anterior. Alguns resultats en aquesta direcció han estat obtinguts per Sarnak.

## 5.3 Funcions període

En aquest secció començarem a entrar en matèria. Les notacions són les de l'article de Lewis-Zagier [5].

Denotarem per $\Gamma$ el grup modular $\mathbf{SL}(2,\mathbb{Z})$. Una funció definida en $\mathcal{H}$ serà anomenada periòdica quan sigui invariant per la translació $z \mapsto z+1$.

Associarem a cada forma de Maass respecte del grup modular dues series $L$. Aplicant a aquestes sèries la inversa de la transformació de Mellin, obtindrem certes funcions holomorfes que satisfan una equació funcional de tres termes. Més endavant interpretem aquestes funcions com a funcions període associades a formes de Maass.

### 5.3.1 Solucions periòdiques de l'equació de Laplace

**5.3.1 Definició.** Donada una funció $u$ diferenciable, considerem les funcions

$$u_0(y) = \frac{1}{\sqrt{y}}\, u(iy), \quad u_1(y) = \frac{\sqrt{y}}{2\pi i}\, \frac{\partial u}{\partial x}(iy). \tag{5.3}$$

La funció $u_0$ és una renormalització de $u$ al llarg de l'eix imaginari. La funció $u_1$ és la derivada normal de $u$ restringida a l'eix imaginari.

**5.3.2 Proposició.** *Siguin $s$ un nombre complex, $\sigma = \Re(s)$, $\varepsilon \in \{0,1\}$. Les fórmules*

$$L_\varepsilon^*(\rho) = \int_0^\infty u_\varepsilon(y)\, y^{\rho-1}\, dy, \tag{5.4}$$

$$(2\pi)^{-\rho}\, \Gamma(\rho) L_\varepsilon(\rho - s + \frac{1}{2}) = \int_0^\infty (f(iy) - (-1)^\varepsilon f(-iy))\, y^{\rho-1}\, dy, \tag{5.5}$$

*estableixen una correspondència bijectiva entre les tres classes de funcions següents:*

(a) *Solucions periòdiques de $\Delta u = s(1-s)u$, definides en $\mathcal{H}$, que satisfan la condició de creixement*

$$u(x+iy) = \mathrm{O}(y^A), \quad y \to \infty,$$

*per a algun $A < \min\{\sigma, 1-\sigma\}$.*

(b) *Un parell de sèries de Dirichlet $L_\varepsilon(\rho)$, convergents en algun semiplà.*

(c) *Una funció periòdica $f(z)$ en $\mathbb{C}\backslash\mathbb{R}$ que satisfà*

$$f(z) = \mathrm{O}(|\Im(z)|^{-A}), \quad |\Im(z)| \to \infty,$$

*per a algun $A > 0$.*

*Demostració.* Per un teorema degut a Maass, se sap que l'equació

$$\Delta u = s(1-s)u,$$

juntament amb la periodicitat de $u$ i l'estimació del seu creixement imposats en (a) són equivalents a la representabilitat de $u$ per una sèrie de Fourier de la forma

$$u(z) = y^{1/2} \sum_{n\neq 0} A_n \, K_{s-\frac{1}{2}}(2|\pi|\, n|y) e^{2\pi i n x}, \quad z = x + iy,\ y > 0, \tag{5.6}$$

de coeficients $A_n \in \mathbb{C}$ de creixement polinòmic. La condició de creixement és necessària per a eliminar els termes exponencialment grans $y^{1/2}\, I_{s-\frac{1}{2}}(2\pi|n|y)e^{2\pi i n x}$ i el terme constant $\alpha y^s + \beta y^{1-s}$ en el desenvolupament de $u$.

Donada una funció $u$ com la d'abans, li associem dues sèries de Dirichlet $L_0$, $L_1$,

$$L_\varepsilon(\rho) := \sum_{n=1}^{\infty} \frac{A_{n,\varepsilon}}{n^\rho}, \quad \varepsilon \in \{0,1\}, \quad A_{n,\varepsilon} := A_n + (-1)^\varepsilon A_{-n}, \tag{5.7}$$

i la funció holomorfa $f$ definida en $\mathbb{C} \setminus \mathbb{R}$ segons

$$f(z) = \begin{cases} \displaystyle\sum_{n>0} n^{s-\frac{1}{2}}\, A_n\, e^{2\pi i n z}, & \text{si } \Im(z) > 0, \\ \\ \displaystyle -\sum_{n<0} |n|^{s-\frac{1}{2}}\, A_n\, e^{2\pi i n z}, & \text{si } \Im(z) < 0. \end{cases} \tag{5.8}$$

El creixement polimòmic dels coeficients $A_n$ implica que $L_0, L_1$ convergeixen en un semiplà i que $f(x+iy)$ és fitada per una potència de $|y|$ quan $|y| \to 0$.

Recíprocament, si comencem o bé per dues sèries de Dirichlet $L_0$, $L_1$, que són convergents en algun semiplà, o bé per una funció periòdica i holomorfa $f(z)$ en $\mathbb{C} \setminus \mathbb{R}$, que sigui $\mathrm{O}(|\Im(z)|^{-A})$ per a algun $A > 0$, aleshores el desenvolupament anterior defineix coeficients $\{A_n\}_{n\neq 0}$ que tenen un creixement polinòmic en $n$. Això és evident en el primer cas, i s'obté per un argument estàndard, degut a Hecke, en el segon. Després, si definim $u$, trobem que les funcions $u_\varepsilon$ corresponents posseeixen un desenvolupament en sèrie del tipus

$$u_\varepsilon(y) = \sum_{n=1}^{\infty} (ny)^\varepsilon\, A_{n,\varepsilon}\, K_{s-\frac{1}{2}}(2\pi n y),$$

per a $y > 0$ i on $\varepsilon \in \{0, 1\}$. Aquests fets, juntament amb la consideració de les transformades de Mellin

$$\int_0^\infty e^{-2\pi y}\, y^{\rho-1}\, dy = \frac{1}{(2\pi)^\rho}\,\Gamma(\rho),$$

$$\int_0^\infty K_{s-\frac{1}{2}}(2\pi y)\, y^{\rho-1}\, dy = \frac{1}{4\pi^\rho}\,\Gamma\left(\frac{\rho - s + \frac{1}{2}}{2}\right)\Gamma\left(\frac{\rho + s - \frac{1}{2}}{2}\right),$$

posen de manifest la relació que hi ha entre les funcions $L_\varepsilon$, $f$, i $u$ considerades.

Les fórmules anteriors condueixen a introduir el factor

$$\gamma_s(\rho) := \frac{1}{4\pi^\rho}\,\Gamma\left(\frac{\rho - s + \frac{1}{2}}{2}\right)\Gamma\left(\frac{\rho + s - \frac{1}{2}}{2}\right).$$

Precisem que

$$L_\varepsilon^*(\rho) = \gamma_s(\rho + \varepsilon) L_\varepsilon(\rho).$$

□

### 5.3.2 El cas parell i el cas senar

Els resultats de la secció anterior tenen versions més precises per a funcions parelles i per a funcions senars. Denotarem per $\mathbb{C}'$ el pla complex menys la semi-recta real negativa:

$$\mathbb{C}' = \mathbb{C} \setminus (-\infty, 0].$$

**5.3.3 Proposició.** (Cas parell) *Donada una successió de nombres complexos de creixement polinòmic $\{A_n\}_{n\geq 1}$, les afirmacions següents són equivalents:*

(a) *La funció*

$$u(z) := y^{1/2} \sum_{n=1}^{\infty} A_n\, K_{s-\frac{1}{2}}(2\pi n y)\cos(2\pi n x)$$

*és invariant per $z \mapsto -1/z$ i, per tant, és una forma de Maass parella.*

(b) *La funció*

$$\Lambda_s(\rho) := \gamma_s(\rho) \sum_{n=1}^{\infty} A_n \, n^{-\rho}$$

*és entera, d'ordre finit i és invariant per* $\rho \mapsto 1 - \rho$.

(c) *La funció*

$$f(z) := \pm \sum_{n=1}^{\infty} n^{s-1/2} A_n (e^{\pm 2\pi i n z} - z^{-2s} e^{\mp 2\pi i n/z})$$

*definida per a* $\Im(z) > 0$, *respectivament,* $\Im(z) < 0$, *s'estén a una funció holomorfa de tot* $\mathbb{C}'$ *i és fitada en el semiplà dret.*

**5.3.4 Proposició.** (Cas senar) *Sigui* $\{A_n\}_{n\geq 1}$ *una successió de nombres complexos de creixement polinòmic. Aleshores, les afirmacions següents són equivalents:*

(a) *La funció*

$$u(z) := y^{1/2} \sum_{n=1}^{\infty} A_n \, K_{s-\frac{1}{2}}(2\pi n y) \sin(2\pi n x)$$

*és invariant per* $z \mapsto -1/z$ *i, per tant, és una forma de Maass senar.*

(b) *La funció*

$$\Lambda_s(\rho) := \gamma_s(\rho + 1) \sum_{n=1}^{\infty} A_n \, n^{-\rho}$$

*és entera, d'ordre finit i és anti-invariant per* $\rho \mapsto 1 - \rho$.

(c) *La funció*

$$f(z) := \sum_{n=1}^{\infty} n^{s-1/2} A_n (e^{\pm 2\pi i n z} - z^{-2s} e^{\mp 2\pi i n/z})$$

*definida per a* $\Im(z) > 0$ *o bé* $\Im(z) < 0$ *s'estén holomòrficament a tot* $\mathbb{C}'$ *i és fitada en el semiplà dret.*

### 5.3.3 Una equació funcional de tres termes

En aquest apartat, relacionarem les formes de Maass $u$ amb solucions $\psi$ de certes equacions funcionals de tres termes. Recordem que $\Gamma = \mathbf{SL}(2, \mathbb{Z})$.

**5.3.5 Proposició.** *Siguin $\psi(z)$ una funció definida en $\mathcal{H}$ i $s \in \mathbb{C} \setminus \mathbb{Z}$ un nombre complex no enter. Aleshores, la funció $\psi(z)$ satisfà l'equació funcional*

$$\psi(z) = \psi(z+1) + (z+1)^{-2s}\psi(\frac{z}{z+1}), \quad z \in \mathbb{C}', \tag{5.9}$$

*si, i només si, la funció*

$$\psi(z) + z^{-2s}\psi\left(\frac{-1}{z}\right) \tag{5.10}$$

*és periòdica.*

*Més precisament, les fórmules*

$$c(s)\psi(z) = f(z) - z^{-2s} f\left(\frac{-1}{z}\right), \tag{5.11}$$

$$c^*(s)f(z) = \psi(z) + z^{-2s}\psi\left(\frac{-1}{z}\right), \tag{5.12}$$

*on $c(s)$, $c^*(s)$ són dues constants que satisfan*

$$c(s)\, c^*(s) = 1 - e^{-2\pi i s} \tag{5.13}$$

*estableixen una correspondència bijectiva entre les solucions $\psi$ de l'equació funcional* (5.9) *i les funcions periòdiques $f$ definides en el semiplà superior $\mathcal{H}$.*

*El mateix se satisfà en el semiplà inferior, però cal canviar la condició $c(s)$, $c^*(s)$ per*

$$c(s)\, c^*(s) = 1 - e^{2\pi i s}. \tag{5.14}$$

*Demostració.* Si la funció $\psi$ satisfà l'equació funcional de tres termes 5.9, es tindrà que

$$\left[\psi(z+1)+(z+1)^{-2s}\psi\left(\frac{-1}{z+1}\right)\right]-\left[\psi(z)+(z)^{-2s}\psi\left(\frac{-1}{z}\right)\right]$$

$$=\left[\psi(z+1)-\psi(z)+(z+1)^{-2s}\psi\left(\frac{z}{z+1}\right)\right]$$

$$-(z+1)^{-2s}\left[\psi\left(\frac{z}{z+1}\right)-\psi\left(\frac{-1}{z+1}\right)+\left(\frac{z+1}{z}\right)^{2s}\psi\left(\frac{-1}{z}\right)\right]$$

$$=0.$$

Per tant, la funció $f$ definida en (5.12) serà periòdica.

En relació amb les constants, Lewis i Zagier fan a [5] l'elecció següent:

$$c(s):=\frac{i\,\pi^{-s}}{\Gamma(1-s)},\quad c^*(s):=\pm\frac{2\pi^{s+1}}{\Gamma(s)}e^{\mp i\pi s},$$

on el signe + es pren en el semiplà superior i el signe −, en l'inferior. □

El teorema següent permetrà interpretar en seccions posteriors les funcions període $\psi$ associades a les formes de Maass.

**5.3.6 Teorema.** *Sigui $s$ un nombre complex tal que $\sigma:=\Re(s)>0$. Aleshores, existeix una correspondència canònica bijectiva entre els objectes següents:*

(a) *Les formes de Maass u cuspidals de valor propi $s(1-s)$.*

(b) *Les funcions holomorfes $\psi:\mathbb{C}'\to\mathbb{C}$ que satisfan les equacions funcionals de tres termes*

$$\psi(z)=\psi(z+1)+(z+1)^{-2s}\psi(\frac{z}{z+1}) \tag{5.15}$$

*i les estimacions*

$$\psi(z) \ll \begin{cases} |\Im(z)|^{-A}(1+|z|^{2A-2\sigma}), & \text{si } \Re(z) \le 0, \\ 1, & \text{si } \Re(z) \ge 0, |z| \le 1, \\ |z|^{-2\sigma}, & \text{si } \Re(z) \ge 0,\ |z| \ge 1. \end{cases} \tag{5.16}$$

*per a algun* $A > 0$.

*Demostració.* La demostració d'aquest teorema utilitza les funcions auxiliars i els resultats de les proposicions de les subseccions precedents. Una sèrie de càlculs acaben donant les implicacions dobles

$$u \leftrightarrow L_\varepsilon \leftrightarrow f \leftrightarrow \psi,$$

que permeten comparar la forma de Maass amb la seva funció període. □

## 5.4 Les funcions període com a transformades integrals

En aquesta secció donarem representacions integrals de la funció $\psi$ associada a una forma de Maass $u$. D'ací que aquestes funcions s'anomenin funcions període de les formes de Maass.

**5.4.1 Proposició.** *Donada una forma de Maass* $u$, *siguin* $u_0$ *la renormalització de* $u$ *i* $u_1$ *la derivada normal de* $u$ *restringida a l'eix imaginari, tal com han estat definides a* (5.3). *Aleshores, la funció*

$$\psi_1(z) := 2s\,z \int_0^\infty \frac{t^{s+1/2}\,u_0(t)}{(z^2+t^2)^{s+1}}\,dt \;-\; 2\pi i \int_0^\infty \frac{t^{s-1/2}u_1(t)}{(z^2+t^2)^s}\,dt,$$

*definida per a* $\Re(z) > 0$, *és proporcional a la funció període* $\psi(z)$ *associada a* $u$.

*Demostració.* La demostració procedeix per comparació de les transformades de Mellin de $\psi$ i de $\psi_1$. □

**5.4.2 Corol·lari.** *La funció $\psi_1$ satisfà les propietats d'una funció període de Maass: s'estén a una funció holomorfa de $\mathbb{C}'$, satisfà una equació funcional de tres termes i satisfà les condicions de creixement donades a* (5.16).

### 5.4.1 Formes diferencials de Green

Tot seguit interpretarem la funció període $\psi$ associada a una forma de Maass com a la integral de una 1-forma diferencial tancada. D'aquesta manera s'obté una segona demostració del corol·lari (5.4.2).

**5.4.3 Definició.** Donades funcions diferenciables $u(z)$, $v(z)$ de la variable complexa $z = x + iy$, es defineixen les 1-formes de Green $\{u, v\}(z)$, $[u, v](z)$ segons:

$$\{u, v\}(z) := \left( v \frac{\partial u}{\partial y} - u \frac{\partial v}{\partial y} \right) dx + \left( u \frac{\partial v}{\partial x} - v \frac{\partial u}{\partial x} \right) dy,$$

$$[u, v](z) := v \frac{\partial u}{\partial z}\, dz + u \frac{\partial v}{\partial \overline{z}}\, d\overline{z}.$$

**5.4.4 Lema.** *Les formes diferencials $\{u, v\}$, $[u, v]$ satisfan les propietats següents:*

(i) $[u, v] + [v, u] = d(u\, v), \quad [u, v] - [v, u] = -i\{u, v\}.$

(ii) *Si $u$, $v$ són funcions pròpies de l'operador de Laplace del mateix valor propi, aleshores les dues formes diferencials de Green associades són tancades.*

Les formes diferencials que ens interessaran portaran com a $u$ la forma de Maass i com a $v$ la potència $s$-èsima d'una funció auxiliar $R_\zeta$ que veurem a continuació.

**5.4.5 Proposició.** *Donat $\zeta \in \mathbb{C}$, sigui*

$$R_\zeta(z) := \frac{y}{(x - \zeta)^2 + y^2} = \frac{i}{2} \left( \frac{1}{z - \zeta} - \frac{1}{\overline{z} - \zeta} \right),$$

*on $z = x + iy \in \mathcal{H}$. La funció $R_\zeta$ satisfà les propietats següents:*

(i) $R_{g\,\zeta}(gz) = (c\,\zeta + d)^2 R_\zeta(z)$, *per a tota* $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{SL}(2,\mathbb{R})$.

(ii) $\Delta(R_\zeta^s) = s(1-s)\,R_\zeta^s$, *per a tot* $s \in \mathbb{C}$.

Observem que la potència $s$-èsima de $R_\zeta$ està ben definida si $\zeta \in \mathbb{R}$; en el cas general, cas restringir-se als arguments $z$ situats en el complementari en $\mathcal{H}$ d'algun camí que uneixi $\zeta$ amb $\overline{\zeta}$ i escollir la branca evident.

Un càlcul relativament senzill proporciona el corol·lari següent.

**5.4.6 Corol·lari.** *Si* $u : \mathcal{H} \to \mathbb{C}$ *és una funció pròpia de* $\Delta$ *de valor propi* $s(1-s)$*, aleshores*

(i) *La forma diferencial de Green* $\{u, R_\zeta^s\}$ *és tancada.*

(ii) *Se satisfà la igualtat*

$$\psi_1(\zeta) = \int_0^{i\infty} \{u, R_\zeta^s\}(z), \quad \Re(\zeta) > 0.$$

Donada una forma de Maass $u$, la representació integral anterior de la funció període $\psi_1$ permet obtenir la prolongació analítica d'aquesta funció en una funció analítica de $\mathbb{C}'$, així com també demostrar que $\psi_1$ satisfà l'equació funcional de tres termes.

### 5.4.2 Transformades de Hankel i de Laplace

Sigui $u$ una funció periòdica amb desenvolupament de Fourier

$$u(z) = y^{1/2} \sum_{n\neq 0} A_n\, K_{s-\frac{1}{2}}(2|\pi|\,n|y)\, e^{2\pi i n x}, \quad z = x + iy,\ y > 0,$$

en el qual suposarem que $A_n = \mathrm{O}(n^{1/2})$. Es defineix la seva transformada de Hankel segons

$$\phi(w) := w^{1-s} \int_0^\infty \sqrt{w\,t}\, J_{s-\frac{1}{2}}(w\,t)\, u(it)\, dt,$$

per a $\{w \in \mathbb{C} : |\Im(w)| < 2\pi|\}$.

La funció $\psi_1$ es pot recuperar com a transformada de Laplace de la transformada de Hankel $\phi$ de $u$:

$$\psi_1(z) \doteq \int_0^\infty e^{-zw} w^{2s-1} \phi(w)\, dw, \quad \Re(z) > 0.$$

Aquí, el símbol $\doteq$ denota que la igualtat té lloc llevat de factors que depenen únicament de $s$.

Alhora, la funció $\psi_1(z)$ admet un desenvolupament

$$\psi_1(z) \doteq \sum_{n=1}^{\infty} n^{s-1/2} A_n \, \mathcal{C}_s(2\pi n z),$$

on

$$\mathcal{C}_s(z) \doteq \int_0^\infty \frac{z t^{s+1/2}}{(z^2+t^2)^{s+1}} \, K_{s-1/2}(t)\, dt, \quad \Re(z) > 0.$$

La funció $\mathcal{C}_s$ és una de les funcions de Lommel. Ve a ser com una funció cosinus, que té la seva rèplica en una funció sinus, definida per

$$\mathcal{S}_s(z) \doteq \int_0^\infty \frac{t^{s+1/2}}{(z^2+t^2)^{s}} \, K_{s-1/2}(t)\, dt, \quad \Re(z) > 0.$$

Les representacions anteriors proporcionen els coeficients de Taylor de la funció $\psi$ donats en el teorema que segueix.

**5.4.7 Teorema.** *Sigui $u$ una funció de Maass parella, de valor propi $s(1-s)$ i sigui $\psi(z)$ la seva funció període associada. Aleshores, $\psi(z)$ és una funció infinitament diferenciable des de la dreta en $z = 0$. Se satisfà que*

(i) *Si $m$ és parell, $\psi^{(m)}(0) = 0$.*

(ii) *Si $m$ és senar,*

$$\psi^{(m)}(0) \doteq \frac{m!}{(2\pi i)^m} \, \Gamma(m+2s)\, L_0(m+s+\frac{1}{2}). \tag{5.17}$$

L'expressió (5.17) és l'anàleg del fet que la funció període associada a una forma modular holomorfa és un polinomi que té per coeficients múltiples senzills de valors especials de la seva $L$-sèrie (cf. la secció (5.6)).

### 5.4.3 Valors frontera de formes de Maass

En aquesta secció es tracta de comprendre com, a partir d'una forma de Maass $u$, podem deduir formalment la seva cohort de funcions associades:

$$u \mapsto \{L_\varepsilon,\ f,\ \psi,\ \phi\}.$$

Veurem que totes aquestes funcions s'expressen com a transformades integrals de tipus diversos (Poisson, Stieltjes, Laplace, Mellin) d'una única "funció automorfa" $U(t)$.

Les fórmules seran les següents:

$$u(z) = y^s \int_{-\infty}^{+\infty} |z-t|^{-2s}\, U(t)\, dt, \quad z \in \mathcal{H}, \tag{5.18}$$

$$f(z) = \int_{-\infty}^{+\infty} (z-t)^{-2s}\, U(t)\, dt, \quad z \in \mathbb{C} \setminus \mathbb{R}, \tag{5.19}$$

$$\psi(z) = \int_{-\infty}^{0} (z-t)^{-2s}\, U(t)\, dt, \quad z \in \mathbb{C}'. \tag{5.20}$$

Si, a més, se suposa que les integrals convergeixen suficientment bé, la funció $u$ esdevé una funció pròpia de l'operador de Laplace, de valor propi $s(1-s)$, i les funcions $f$, $\psi$ esdevenen funcions holomorfes en els dominis que s'indiquen.

Però aquesta presentació té un problema: la funció automorfa $U$ no existeix com a tal. Per a vèncer aquest petit obstacle, els autors transformen els arguments formals en rigorosos en interpretar $U$ com a un objecte $\Gamma$-invariant en un espai de distribucions. La distribució $U$ és invariant en el sentit següent:

$$U(t) = |ct+d|^{2s-2} U\left(\frac{at+b}{ct+d}\right),$$

per a tota $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$.

Per a fer els càlculs rigorosos, es defineix un espai de funcions test $\mathcal{V}_s$ en en el qual opera $\Gamma$ i el corresponent espai de distribucions al qual pertany $U$. L'espai $\mathcal{V}_s$ consta de les funcions $\varphi$ reals que tenen un desenvolupament asimptòtic

$$\varphi(t) \sim |t|^{-2s} \sum_{n\geq 0} c_n t^{-n}, \quad |t| \to \infty.$$

L'acció de $\Gamma$ en aquest espai és donada per

$$(\varphi|g)(x) := |cx+d|^{-2s} \varphi\left(\frac{ax+b}{cx+d}\right),$$

on $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$. La distribució $U$ és una aplicació lineal

$$\begin{aligned} U: \quad \mathcal{V}_s \quad &\to \mathbb{C} \\ \varphi \quad &\mapsto U[\varphi] := \sum_{n=1}^{\infty} n^{1/2-s} A_n \, \widehat{\varphi}(n). \end{aligned}$$

La sèrie convergeix ràpidament atès que $\widehat{\varphi}(n)$ decau quan $n \to \infty$ més de pressa que qualsevol potència de $n$. Això dóna sentit a la integral formal

$$U[\varphi] = \int_{-\infty}^{+\infty} U(t)\varphi(t)\, dt.$$

El sentit de l'automorfia es manifesta en la proposició següent.

**5.4.8 Proposició.** *Sigui $s \in \mathbb{C}$ amb $\Re(s) > 0$ i sigui $\{A_n\}_{n\geq 1}$ una successió de nombres complexos de creixement polinòmic. Aleshores, els $A_n$ són els coeficients de Fourier d'una forma de Maass u parella, de valor propi $s(1-s)$, si, i només si, l'aplicació lineal*

$$U : \mathcal{V}_s \to \mathbb{C}$$

*definida per*

$$U[\varphi] := \sum_{n=1}^{\infty} n^{1/2-s} A_n \widehat{\varphi}(n)$$

*és invariant per l'acció de $\Gamma$ en $\mathcal{V}_s$.*

De la representació integral donada per a les funcions anteriors, es dedueixen els desenvolupaments en sèrie per a $u$ i per a $f$ donats a (5.6) i a (5.8).

## 5.5 Formes de Maass no cuspidals

Les funcions tractades fins a aquí es corresponen amb formes de Maass cuspidals. Estendrem ara aquest concepte al cas no cuspidal.

**5.5.1 Definició.** Una aplicació $u : \mathcal{H} \to \mathbb{C}$ de classe $\mathcal{C}^\infty$ es diu que és una forma d'ona de Maass respecte de $\Gamma$ i de paràmetre espectral un nombre $s \in \mathbb{C}$ si satisfà les condicions següents:

(i) Existeix $\lambda \in \mathbb{R}$, $\lambda \geq 0$, tal que

$$\Delta u = s(1-s)u.$$

(ii) $u(\gamma z) = u(z)$, per a tota $\gamma \in \Gamma$.

(iii) La funció $u(z)$ creix per sota de la funció exponencial quan $y \to \infty$.

Aleshores, segons la definició anterior, les formes de Maass cuspidals de paràmetre espectral $s$ constitueixen un espai vectorial de codimensió 1 dins l'espai de totes les formes de Maass de paràmetre espectral $s$. Les funcions extra són donades pels múltiples escalars de la sèrie d'Eisenstein no holomorfa $E_s(z)$. Aquesta funció es defineix de la manera següent:

$$E_s(z) = \frac{1}{2} \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{y^s}{|mz+n|^{2s}}, \quad \Re(s) > 1,$$

i, per a un $s$ arbitrari, segons el desenvolupament en sèrie de Fourier

$$\begin{aligned} E_s(z) \quad &= \zeta(2s)\, y^s + \frac{\pi^{1/2}\Gamma(s-\frac{1}{2})}{\Gamma(s)}\, \zeta(2s-1) y^{1-s} \\ &+ \frac{4\pi^s}{\Gamma(s)}\, y^{1/2} \sum_{n=1}^{\infty} n^{1/2-s} \sigma_{2s-1}(n)\, K_{s-\frac{1}{2}}(2\pi n y)\, \cos(2\pi n x). \end{aligned}$$

Les sèries d'Eisenstein són formes de Maass parelles. El fet és que no hi ha formes de Maass respecte de $\Gamma$ que siguin senars i no cuspidals.

### 5.5.1 Les funcions període en el cas no cuspidal

El teorema següent dóna compte de com s'estén la teoria dels períodes a fi de cobrir el cas no cuspidal.

**5.5.2 Teorema.** *Sigui $s \in \mathbb{C}$ un nombre que satisfaci $\Re(s) > 0$, $s \notin \mathbb{Z}$.*

(a) *Si $u : \mathcal{H} \to \mathbb{C}$ és una funció invariant per $\Gamma$ amb desenvolupament de Fourier*

$$u(z) = c_0 y^s + c_1 y^{1-s} + 2y^{1/2} \sum_{n=1}^{\infty} A_n K_{s-\frac{1}{2}}(2\pi\, n\, y)\, \cos(2\pi n x), \tag{5.21}$$

*i definim una funció holomorfa i periòdica $f : \mathbb{C} \setminus \mathbb{R} \to \mathbb{C}$ per*

$$\pm f(z) = \frac{\pi^{\frac{1}{2}-s}}{\Gamma(\frac{1}{2}-s)}\, c_0 + \sum_{n=1}^{\infty} n^{s-\frac{1}{2}} A_n e^{\pm 2\pi i n\, z}, \quad \Im(z) > 0, \Im(z) < 0, \tag{5.22}$$

*aleshores, la solució $\psi$ de l'equació funcional de tres termes* (5.9) *definida per* (5.11) *s'estén a una funció holomorfa de $\mathbb{C}'$ que satisfà*

$$\psi(x) = \frac{\pi^{\frac{1}{2}}\Gamma(s+\frac{1}{2})}{\Gamma(s)} \frac{c_0}{x^{2s}} + \frac{c_1}{x} + \mathrm{O}(1), \quad x \to 0. \tag{5.23}$$

(b) *Recíprocament, sigui $\psi$ una solució analítica real de l'equació funcional de tres termes* (5.9)*, en $\mathbb{R}_+$, de creixement asimptòtic com a* (5.23)*. Aleshores $\psi$ s'estén holomòrficament a tot $\mathbb{C}'$, la funció $f$ definida per* (5.12) *admet un desenvolupament en sèrie de Fourier de la forma* (5.22) *i la funció $u$ definida per* (5.21) *és invariant per l'acció del grup modular $\Gamma$.*

Si $u = E_s$, aleshores la funció $\psi = \psi_s$ admet a l'entorn del 0 un desenvolupament asimptòtic donat per

$$\begin{aligned} \psi_s(x) \;&\sim \frac{\zeta(2s)}{2} x^{-2s} + \frac{\zeta(2s-1)}{2s-1}\, x^{-1} \\ &\quad + \sum_{\substack{m \geq 1 \\ m \text{senar}}} \binom{cm + 2s - 1}{m} \frac{B_{m+1}}{m+1}\, \zeta(m+2s) x^m, \end{aligned}$$

on $B_n$ denota el $n$-èsim nombre de Bernoulli.

## 5.6 Analogia entre el cas holomorf i el cas infinitament diferenciable

En aquesta secció analitzarem l'analogia entre les funcions període del cas holomorf i les funcions període del cas infinitament diferenciable.

### 5.6.1 Revisió de la teoria d'Eichler, Shimura i Manin

En aquesta secció veurem que les funcions període associades a les formes de Maass s'assemblen als polinomis de períodes associats a les formes modulars. En el cas especial en què el paràmetre espectral és enter, les dues teories no solament són anàlogues sinó que coincideixen en un cert sentit. En aquest cas, no hi ha formes de Maass cuspidals, però hi ha unes funcions pròpies $u$ de l'operador de Laplace que són "gairebé automorfes". Això permet associar a les formes $u(z)$ funcions període $\psi(z)$ i funcions holomorfes $f(z)$. Les funcions holomorfes $f(z)$ són formes modulars cuspidals de pes $2k$, on $s = k \in \mathbb{Z}_{\geq 0}$ és un enter positiu. Quan $s = 1 - k \in \mathbb{Z}_{\leq 0}$ és un enter, les funcions $\psi(z)$ són la integral d'Eichler d'aquesta forma.

La proposició següent resumeix la teoria clàssica dels períodes, deguda a Eichler, Shimura i Manin.

**5.6.1 Proposició.** *Sigui $f(z)$ una forma modular cuspidal (holomorfa) de pes $2k$ respecte de $\mathbf{SL}(2,\mathbb{Z})$. Sigui*

$$f(z) = \sum_{n=1}^{\infty} a_n q^n, \quad z \in \mathcal{H}, \quad q = e^{2\pi i z},$$

*el seu desenvolupament en sèrie de Fourier a l'entorn de la punta de l'infinit. Associat a la forma $f$, existeix un polinomi $r_f$ de grau $2k-2$, anomenat el polinomi dels períodes, que pot ésser definit de les tres maneres equivalents següents:*

(i) *Per mitjà de la identitat*

$$r_f(z) \doteq \widetilde{f}(z) - z^{2k-2}\widetilde{f}(-1/z), \quad z \in \mathcal{H}, \tag{5.24}$$

*on el signe $\doteq$ ara denota una igualtat llevat d'una constant que depèn únicament de $k$ i $\widetilde{f}$ denota la integral d'Eichler de la*

*forma $f$, definida pel desenvolupament de Fourier*

$$\widetilde{f}(z) = \sum_{n=1}^{\infty} \frac{a_n}{n^{2k-1}}\, q^n, \quad z \in \mathcal{H}. \tag{5.25}$$

(ii) *Per mitjà de la representació integral*

$$r_f(X) \doteq \int_0^{i\infty} f(\tau)(\tau - X)^{2k-2}\, d\tau, \tag{5.26}$$

*on la integral es pren sobre l'eix imaginari.*

(iii) *Per mitjà de la fórmula tancada*

$$r_f(X) \doteq \sum_{r=0}^{2k-2} \frac{(-2\pi i)^{-r}}{(2k-2-r)!}\, L_f(r+1)X^r, \tag{5.27}$$

*on $L_f(\rho) = \sum_{n=1}^{\infty} a_n n^{-\rho}$, i la seva continuació analítica, és la sèrie $L$ de Hecke associada a $f$.*

*Demostració.* (Indicació.) La demostració consisteix en una sèrie de càlculs que parteixen del fet que

$$D^{2k-1}(\widetilde{f}) = f,$$

on $D$ denota l'operador diferencial

$$D = \frac{1}{2\pi i}\frac{d}{dz} = q\frac{d}{dq}.$$

Un punt decisiu és que $D^{2k-1}$ és un operador diferencial que intercanvia l'acció del grup $\mathbf{SL}(2,\mathbb{R})$ en pesos $2-2k$ i $2k$. És a dir, es compleix que

$$D^{2k-1}(F|_{2-2k}g) = (D^{2k-1}F)|_{2k}g$$

per a tota transformació $g \in \mathbf{SL}(2,\mathbb{R})$ i per a tota funció diferenciable $F$. □

Ara es pot establir una analogia entre les fórmules que defineixen les funcions període de formes de Maass i les funcions període de funcions holomorfes. A la taula (5.1) es disposa cada fórmula amb la seva anàloga.

| |
|---|
| $r_f(z) \doteq \widetilde{f}(z) - z^{2k-2}\widetilde{f}\left(\dfrac{-1}{z}\right), \quad z \in \mathcal{H}$<br>formes modulars |
| $c(s)\psi(z) = f(z) - z^{-2s} f\left(\dfrac{-1}{z}\right), \quad z \in \mathbb{C} \setminus \mathbb{R}$<br>formes de Maass |
| $r_f(X) \doteq \displaystyle\int_0^{\infty} f(\tau)(\tau - X)^{2k-2}\, d\tau$<br>formes modulars |
| $\psi_1(\zeta) = \displaystyle\int_0^{i\infty} \{u, R_\zeta^s\}(z), \quad \Re(\zeta) > 0$<br>formes de Maass |
| $r_f(X) \doteq \displaystyle\sum_{m=0}^{2k-2} \frac{(-2\pi i)^{-m}}{(2k-2-m)!} L_f(m+1) X^m$<br>formes modulars |
| $\psi^{(m)}(0) \doteq \dfrac{m!}{(2\pi i)^m} \Gamma(m+2s)\, L_{u,0}(m+s+\frac{1}{2})$<br>formes de Maass |

Taula 5.1: Dues versions de les funcions període

### 5.6.2 Períodes i cocicles

Les analogies entre les dues teories de períodes, en el cas holomorf i en el cas infinitament diferenciable, encara es poden fer més precises. Per a tal fi, sigui

$$P_{2k-2} := \{F(X) \in \mathbb{C}[X] : \operatorname{gr}(F(X)) \leq 2k-2\}.$$

A l'espai anterior de polinomis considerem l'acció de $\mathbf{SL}(2,\mathbb{Z})$ donada per $|_{2k-2}$. A partir de les definicions, es té que el polinomi de períodes $r_f(X)$ associat a una forma modular cuspidal $f$ de pes $k$ pertany a l'espai

$$W_{2k-2} := \{F \in P_{2k-2} : F|(1+S) = F|(1+U+U^2) = 0\}.$$

Aquí, $S$ i $U = TS$ denoten els generadors del grup modular tals que

$$\Gamma = \langle S, U\rangle, \quad S^2 = -1, \quad U^3 = 1,$$

i l'acció de $\Gamma$ en $P_{2k-2}$ ha estat estesa per linealitat a tot l'anell de grup $\mathbb{Z}[\Gamma]$.

La proposició següent és ben coneguda.

**5.6.2 Proposició.** *Les funcions polinòmiques*

$$r_f(X), \quad \overline{r_f(\overline{X})}, \quad f \in S(\Gamma, 2k)$$

*generen un subespai de codimensió* 1 *en l'espai vectorial* $W_{2k-2}$.

*Les relacions que defineixen* $W_{2k-2}$ *posen de manifest que hi ha un* 1*-cocicle*

$$\gamma : \Gamma \to P_{2k-2}, \quad \gamma \mapsto \widetilde{f}|(1-\gamma).$$

*En particular,* $\gamma(T) = 0$, $\gamma(S) = r_f$,

En el context holomorf es dóna la situació següent.

**5.6.3 Proposició.** *Tot element* $F$ *de* $W_{2k-2}$ *és solució d'una equació funcional de tres termes del tipus*

$$F(X) = F(X+1) + (X+1)^{-2s} F\left(\frac{X}{X+1}\right),$$

*amb paràmetre* $s = 1-k$. *Recíprocament, si* $k > 1$, *tot polinomi amb les propietats d'una funció període de paràmetre* $s = 1-k$ *és un element de* $W_{2k-2}$.

*Demostració.* Considerem les matrius

$$T := US = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}, \qquad T' = U^2 S = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Aleshores, les relacions anteriors es tradueixen en les igualtats

$$F|(1 - T - T') = F|(1 + S) - F|(1 + U + U^2)|S = 0,$$

que és precisament l'equació funcional de tres termes. El recíproc és igualment senzill de comprovar. □

La proposició precedent mostra que quan el paràmetre és $s = 1 - k$, els polinomis de períodes de paràmetre $s = 1-k$ associats a formes holomorfes cuspidals de pes $2k$ produeixen solucions holomorfes d'una equació funcional de tres termes. Ara podem preguntar-nos: com encaixa aquesta situació en el camp de les formes de Maass? Veurem la resposta tot seguit.

Per a cada enter $h$, l'operador diferencial

$$\partial_h := D - \frac{ih}{2\pi y}$$

intercanvia l'acció de $\mathbf{SL}(2, \mathbb{R})$ en pesos $2h$ i $2h + 2$; és a dir,

$$\partial_h(F|_{2h} g) = \partial_h(F)|_{2h+2}\, g.$$

En particular, si $F$ és modular de pes $2h$, aleshores, $\partial_h F$ és modular de pes $2h + 2$. En iterar, veiem que la composició

$$\partial_h^n := \partial_{h+n-1} \circ \cdots \circ \partial_h$$

intercanvia les accions de $\mathbf{SL}(2, \mathbb{R})$ en pesos $2h$ i $2h+2n$. Així, aquest operador aplica formes modulars de pes $2h$ en formes modulars de pes $2h + 2n$. Per inducció es demostra que se satisfà la fórmula

$$\partial_h^n = \sum_{m=0}^{n} \frac{n!}{(n-m)!} \binom{n + 2h - 1}{m} \left(\frac{-1}{4\pi y}\right)^m D^{n-m}.$$

En el cas particular en què $h = 1 - k$ i $n = 2k - 1$, es té la igualtat

$$\partial_{1-k}^{2k-1} = D^{2k-1}.$$

L'operador $\partial_h^n$ preserva sempre la modularitat però, en general, destrueix l'holomorfia; l'operador $D^n$ preserva l'holomorfia però, en general, destrueix la modularitat. Per tant, quan tots dos coincideixen, es preserven la modularitat i l'holomorfia. Així la igualtat

$$D^{2k-1}(\widetilde{f}) = f$$

pot ser factoritzada en dos passos:

$$u := \partial_{1-k}^{k-1}(\widetilde{f}), \quad f = \partial_0^k(u).$$

Ara, a partir de la fórmula recurrent per al càlcul de $\partial_{1-k}^{k-1}$ aplicada a

$$\widetilde{f}(z) = \sum_{n=1}^{\infty} \frac{a_n}{n^{2k-1}}\, q^n, \quad z \in \mathcal{H},$$

s'obté l'expressió familiar

$$u(z) \doteq y^{1/2} \sum_{n\neq 0}^{\infty} A_n\, K_{k-\frac{1}{2}}(2|\pi|\, n|y) e^{2\pi i n x},$$

on els coeficients de Fourier $A_n$ són donats per

$$A_n = \begin{cases} n^{-k+1/2} a_n, & \text{per a } n > 0, \\ 0, & \text{per a } n < 0. \end{cases}$$

En particular, la funció $u$ definida a partir de $\widetilde{f}$ és una funció pròpia de l'operador de Laplace de valor propi $k(1-k)$, és $T$-invariant i decreix a l'infinit. Observem, però, que no és del tot $\Gamma$-invariant, atès que se satisfà que

$$u(z) - u(-1/z) \doteq \partial_{1-k}^{k-1}(r_f).$$

# Bibliografia


[1] Booker, A. R.: Poles of Artin L-function and the strong Artin conjecture. *Ann. Math.* 158 (2003), 1089–1098.

[2] Booker, A. R.: Artin conjecture, Turing's method and the Riemann hypothesis. arXiv:math.NT/0507502, v1, 25, Jul. 2005.

[3] Hejhal, D. A.; Strömbergsson, A.: On quantum chaos and Maass waveforms of CM-type. Invited papers dedicated to Martin C. Gutzwiller, Part IV. *Found. Phys.* 31 (2001), no. 3, 519–533.

[4] Lewis, J.: Eigenfunctions on symmetric spaces with distribution-valued boundary forms. *J. Func. Anal.* 29 (1978), 287–307.

[5] Lewis, J.; Zagier, D.: Period functions for Maass wave forms. I. *Ann. Math.* (2) 153 (2001), no. 1, 191–258.

[6] Maass, H.: Über eine neue Art von nichtanalytischen automorphen Funktionen und die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. *Math. Ann.* 121 (1949), 141–183.

[7] Narkiewicz, W.: *Elementary and analytic theory of algebraic numbers*. Third edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2004. xii+708 pp. ISBN: 3-540-21902-1.

[8] Risager, M. S.: Asymptotic densities of Maass newforms. *J. Number Theory* 109 (2004), 96-119.

[9] Sarnak, P.: Maass cusp forms with integer coefficients. *A panorama of number theory or the view from Baker's garden*, (Zürich, 1999), 121–127, Wüstholz (ed.), Cambridge Univ. Press, Cambridge, 2002.

[10] Sarnak, P.: Spectra of hyperbolic surfaces. *Bull. Amer. Math. Soc.* (N.S.) 40 (2003), no. 4, 441–478.

[11] Strömberg, F.: *Computational Aspects of Maass Waveforms.* Upsala Dissertations in Mathematics 39, 2005. ISBN: 91-506-1794-X.

[12] Whittaker, E. T. ; Watson, G. N.: *A course of modern analysis. An introduction to the general theory of infinite processes and of analytic functions; with an account of the principal transcendental functions.* Reprint of the fourth (1927) edition. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1996. vi+608 pp. ISBN: 0-521-58807-3.

P. Bayer

Facultat de Matemàtiques

Universitat de Barcelona

Gran Via de les Corts Catalanes 585

E-08007, Barcelona

**bayer@ub.edu**

# Capítol 6

# Valors multizeta

X. Xarles

## Introducció

Aquestes notes són, essencialment, les transparències que vaig presentar en una xerrada a Vilanova el dia 2 de febrer del 2008. En elles explico algunes idees de l'article del Kentaro Ihara, Masanobu Kaneko i Don Zagier "Derivation and double shuffle relations for multiple zeta values"[4], publicat l'any 2006, on diuen a l'introducció que *some of the results in this paper* (...) *originated in work which the third-named author did in the year 1988 - 1994 but never published.*

## 6.1 Apunt històric

L'any 1730, Leonhard Euler va demostrar un resultat espectacular, del qual sempre n'estaria ben orgullós:

$$\zeta(2) := \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Amb finançament parcial de MTM 2006-11391.

Seguidament va demostrar, si denotem com és usual ara

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s},$$

que

$$\zeta(4) = \frac{1}{90}\pi^4$$

i que

$$\zeta(2) = \frac{1}{6}\pi^2,\ \zeta(4) = \frac{1}{90}\pi^4,\ \zeta(6) = \frac{1}{945}\pi^6,\ \zeta(8) = \frac{1}{9450}\pi^8,$$

$$\zeta(10) = \frac{1}{93555}\pi^{10},\ \zeta(12) = \frac{691}{638512875}\pi^{12}, \cdots,$$

fins a

$$\zeta(26) = \frac{1315862}{11094481976030578125}\pi^{26}.$$

Finalment, un temps més tard, va demostrar que

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

i, per tant, que

$$\zeta(2n) = c_{2n}\zeta(2)^n, \quad c_{2n} \in \mathbb{Q}.$$

La seva demostració, ara prou ben entesa, tenia llacunes que es varen haver d'anar omplint amb el temps.

Tot i així, ens podríem preguntar si no hi ha una demostració elemental, sense passar per la fórmula amb els nombres de Bernoulli, de la racionalitat de $\zeta(2n)/\zeta(2)^n$.

Començarem per explicar una idea de Zagier de com provar aquesta relació. Aquesta està explicada en un article seu al primer Congrés Europeu de Matemàtiques [8].

**6.1.1 Observació.** Considerem

$$f(m,n) = \frac{2}{mn^3} + \frac{1}{m^2n^2} + \frac{2}{m^3n}.$$

És un exercici elemental veure que tenim la relació

$$f(m,n) - f(m,n+m) - f(m+n,n) = \frac{2}{m^2n^2}.$$

Així tenim com a conseqüència que

$$2\zeta(2)^2 = \sum_{m>0,n>0} \frac{2}{m^2n^2}$$

$$= \sum_{m>0,n>0} f(m,n) - \sum_{m>0,n>0} f(m,n+m) - \sum_{m>0,n>0} f(m+n,n)$$

$$= \sum_{m>0,n>0} f(m,n) - \sum_{n>m>0} f(m,n) - \sum_{m>n>0} f(m,n)$$

$$= \sum_{n>0} f(n,n) = \sum_{n>0} \left( \frac{2}{n^4} + \frac{1}{n^4} + \frac{2}{n^4} \right) = 5\zeta(4).$$

Seguint la mateixa idea podem demostrar el següent.

**6.1.2 Lema.** *Si considerem*

$$f(m,n) = \frac{2}{mn^{k-1}} + \frac{1}{m^2n^{k-2}} + \cdots + \frac{1}{m^{k-2}n^2} + \frac{2}{m^{k-1}n},$$

*aleshores*

$$f(m,n) - f(m,n+m) - f(m+n,n) = 2 \sum_{\substack{0<j<k \\ j_{parell}}} \frac{1}{m^j n^{k-j}}.$$

D'on es dedueix fàcilment que

**6.1.3 Corol·lari.**

$$(2n+1)\zeta(2n) = \sum_{m>0} f(m,m) = 2 \sum_{\substack{0<j<k \\ j_{parell}}} \zeta(j)\zeta(2n-j).$$

Per tant, per inducció, obtenim que

$$\zeta(2n) \in \zeta(2)^n \mathbb{Q}.$$

## 6.2 Preguntes, respostes i conjectures

Ja des dels resultats d'Euler, els matemàtics s'han fet varies preguntes sobre quins resultats podrien ser certs sobre els altres valors (en els senars) de la funció zeta. Per exemple, ens podríem preguntar

- Hi ha altres possibles relacions entre els valors de $\zeta(n)$, $n \in \mathbb{N}$?
- Podria ser que $\zeta(kn) \in \zeta(k)^n\mathbb{Q}$?
- Atès que

  $$\mathbb{Q}(\{\zeta(2n) \mid n = 1, 2, \dots\}) = \mathbb{Q}(\zeta(2)),$$

  amb grau de trascendencia 1 sobre $\mathbb{Q}$, què podem dir del grau de transcendència de

  $$\mathbb{Q}(\{\zeta(n) \mid n = 2, 3, 4, \dots\})?$$

- I del de $\mathbb{Q}(\{\zeta(n) \mid n = 2, 3, \cdots, k\})$?

I què sabem? La veritat, no sabem gairebé res.

Sabem que

**6.2.1 Teorema.**

- Apéry 1978 [1]: $\zeta(3)$ *és irracional.*
- Rivoal 2000 [6]: *Per a tot* $\epsilon > 0$*, existeix* $n_0$ *tal que per a tot* $n \geq n_0$

  $$\dim_{\mathbb{Q}} \mathbb{Q} + \zeta(3)\mathbb{Q} + \zeta(5)\mathbb{Q} + \cdots + \zeta(2n+1)\mathbb{Q} \geq \frac{1-\epsilon}{1+\log(2)} \log(n).$$

- Zudilin 2001 [9]:

  *Un com a mínim dels 4 nombres* $\zeta(5)$*,* $\zeta(7)$*,* $\zeta(9)$ *i* $\zeta(11)$ *és irracional.*

I també coneixem algunes petites millores dels resultats anteriors.

D'altra banda, què creiem que és cert? Doncs creiem que és certa la conjectura següent.

**6.2.2 Conjectura.**

- *Els nombres $\zeta(n)$ són sempre transcendents.*
- *Els nombres $\zeta(2n+1)$ són sempre algebraicament independents entre si.*
- grau $\text{trans}_{\mathbb{Q}}(\mathbb{Q}(\pi, \{\zeta(2n+1) \mid n = 1, 2, \cdots, k\})) = k + 1$.

## 6.3 Valors multizeta

Els valors multizeta apareixen per primer cop en una carta d'Euler a Goldbach. En ella es defineix, amb la notació actual, el valor

$$\zeta(n_1, n_2, \ldots, n_k) := \sum_{a_1 > \cdots > a_k > 0} \frac{1}{a_1^{n_1} \cdots a_k^{n_k}},$$

on $a_1, \ldots, a_n \in \mathbb{Z}_{\geq 1}$.

Aquesta serie està definida (o sigui és convergent) per a $n_1 > 1$ i $n_i \in \mathbb{Z}_{\geq 1}$.

Denotem per $k \geq 1$ la profunditat i per $n := n_1 + \cdots + n_k$ el pes de $\zeta(n_1, n_2, \ldots, n_k)$.

Euler mateix va demostrar alguns resultats. Concretament tenim el següent

**6.3.1 Teorema.** (Euler) *Si $k = 2$ i $n = n_1 + n_2$ és senar, aleshores $\zeta(n_1, n_2)$ és una combinació lineal amb coeficients racionals de $\zeta(n_1 + n_2)$ i de $\zeta(n_1 + n_2 - i)\zeta(i)$, variant $i$. A més es té que*

$$2\zeta(m, 1) = m\zeta(n+1) - \sum_{i=1}^{m-2} \zeta(n-i)\zeta(i+1),$$

$$\zeta(n) = \sum_{n_1 + n_2 = n} \zeta(n_1, n_2)$$

*i que*

$$\zeta(3) = \zeta(2, 1).$$

Aquests valors varen ser "oblidats" fins que, el 1988, Drinfeld els "retrobà" com a coeficients del seu "associador".

Cap els anys 90's, Zagier els "redescobrí" i es va posar a estudiar les relacions entre ells.

Comencem per introduir algunes notacions.

**6.3.2 Notació.** Definim

$$\mathcal{Z} := \langle \zeta(n_1, n_2, \ldots, n_k) \mid n_1 > 1, n_i \geq 1 \forall i = 1, \ldots, k, \forall k \geq 1 \rangle_{\mathbb{Q}} \subset \mathbb{R}.$$

Un punt clau que ara veuré és que $\mathcal{Z}$ és un sub-anell commutatiu (de $\mathbb{R}$). Definim, també,

$$\mathcal{Z}_n := \langle \zeta(n_1, n_2, \ldots, n_k) \mid n_1 + \cdots + n_k = n \ \forall k \geq 1 \rangle_{\mathbb{Q}} \subset \mathbb{R}.$$

En la secció següent, veurem que $\mathcal{Z}$ és un anell commutatiu, veient que el producte de valors multizeta és una suma de valors multizeta. I en la propera, que de fet ho és de dues formes diferents.

## 6.4 Producte harmònic

**6.4.1 Proposició.** (Producte harmònic)

$$\zeta(n_1, \ldots, n_k) \cdot \zeta(m_1, \ldots, m_{k'}) =$$

$$= \sum \textit{multizetes de pes } n_1 + \cdots + n_k + m_1 + \cdots + m_{k'}.$$

Per exemple, tenim que

$$\zeta(n) \cdot \zeta(m) = \zeta(n, m) + \zeta(m, n) + \zeta(n + m).$$

Això s'obté simplement reordenant la sèrie:

$$\sum_{0<a,b} \frac{1}{a^n b^m} = \left( \sum_{0<a<b} + \sum_{0<b<a} + \sum_{0<a=b} \right) \frac{1}{a^n b^m}.$$

La demostració de la proposició (i el seu enunciat!) és similar. Veuré l'enunciat més precís més endavant.

**6.4.2 Exemples.**

$$\zeta(n)^2 = 2\zeta(n,n) + \zeta(2n).$$

Per a $n = 2$, tenim:

$$\zeta(2) = \frac{\pi^2}{6},\ \zeta(4) = \frac{\pi^4}{90}.$$

Per tant,

$$\zeta(2,2) = \sum_{m>n\geq 1} \frac{1}{(mn)^2} = \frac{\pi^4}{120}.$$

Un altre exemple:

$$\zeta(2)\cdot\zeta(3) = \zeta(2,3) + \zeta(3,2) + \zeta(5).$$

De fet, el punt clau de tota la teoria és que

$$\zeta(n_1,\ldots,n_k)\cdot\zeta(m_1,\ldots,m_{k'}) =$$

$$= \sum \text{multiples racionals de multizetes de pes } n_1+\cdots+m_{k'},$$

de dues maneres diferents!

**6.4.3 Exemple.** Tenim que

$$\zeta(2)\cdot\zeta(3) = \zeta(2,3) + \zeta(3,2) + \zeta(5)$$

i que

$$\zeta(2)\cdot\zeta(3) = \zeta(2,3) + 3\zeta(3,2) + 6\zeta(4,1).$$

Aquest segon s'anomena producte escartejat (*shuffle*). Obtenim que

$$\zeta(5) = 2\zeta(3,2) + 6\zeta(4,1).$$

## 6.5 Producte escartejat

Per a poder definir-lo, primer necessitem una nova expressió dels valors multizeta, deguda a Drinfeld i Konsevich.

**6.5.1 Proposició.** (Drinfeld-Konsevich) *Si* $n = n_1 + \cdots + n_k$, *aleshores*

$$\zeta(n_1, \ldots, n_k) =$$

$$= \int_{\Delta_n} \frac{dt_1}{t_1}\frac{dt_2}{t_2}\cdots\frac{dt_{n_1}}{1-t_{n_1}}\cdots\frac{dt_{n-n_k+1}}{t_{n-n_k+1}}\frac{dt_{n-n_k+2}}{t_{n-n_k+2}}\cdots\frac{dt_n}{1-t_n},$$

*on*

$$\Delta_n = \{(t_1, \cdots, t_n) \in \mathbb{R} \mid 1 > t_1 > \cdots > t_n > 0\}.$$

Per exemple tenim el resultat següent degut a Leibniz

$$\zeta(3) = \int_{1>t_1>t_2>t_3>0} \frac{dt_1}{t_1}\frac{dt_2}{t_2}\frac{dt_3}{1-t_3}.$$

La demostració és fàcil: només cal desenvolupar en serie de potències les funcions de dins de la integral.

Per tal d'introduir el producte escartejat, utilitzarem un seguit de notacions, aparentment deslligades del problema original, que a la llarga ens seran molt útils.

**6.5.2 Notació.**

- Denotem per $\mathfrak{H} := \mathbb{Q}\langle x, y\rangle$ l'àlgebra de polinomis no commutatius en dues variables $x$ i $y$.
- Denotem per $\mathfrak{H}^1 := \mathbb{Q} + \mathfrak{H}y$ la subàlgebra generada per les paraules "acabades en $y$".
- Denotem per $\mathfrak{H}^0 := \mathbb{Q} + x\mathfrak{H}y$ la subàlgebra generada per les paraules "començades amb $x$ i acabades en $y$".
- Denotem per $\omega_x(t) = dt/t$, i per $\omega_y(t) = dt/(1-t)$.
- Denotem per $Z : \mathfrak{H}^0 \to \mathbb{R}$ l'únic morfisme $\mathbb{Q}$-lineal amb $Z(1) = 1$ que assigna, a cada paraula $u_1u_2\cdots u_k$ (on $u_i = x$ o $y$), la integral múltiple

$$Z(u_1u_2\cdots u_k) := \int_{\Delta_n} \omega_{u_1}\omega_{u_2}\cdots\omega_{u_k}.$$

Associem a cada $n_i \in \mathbb{N}$ el monomi no commutatiu $z_{n_i} = x^{n_i-1}y$, i a $\underline{n} = (n_1, \cdots, n_k)$ la paraula

$$z_{\underline{n}} := z_{n_1}\ldots z_{n_k} = x^{n_1-1}yx^{n_2-1}y\cdots x^{n_k-1}y.$$

Tenim aleshores que el teorema de Drinfeld ens diu que

$$Z(z_{\underline{n}}) = Z(x^{n_1-1}yx^{n_2-1}y\cdots x^{n_k-1}y) = \zeta(n_1,\cdots,n_k).$$

Així, $z_k$ correspon al valor de la funció zeta de Riemman $\zeta(k)$.

**6.5.3 Observació.** Observeu que $z_k = x^{k-1}y$, $k = 1, 2, 3, \cdots$ generen lliurement $\mathfrak{H}^1$, però amb $k = 2, 3, \cdots$ no generen $\mathfrak{H}^0$. Per exemple, la paraula $xy^2 \in \mathfrak{H}^0$ no està generada per les $z_k$'s.

A cada monomi de $\mathfrak{H}^1$ li associem el pes, que és el grau total, i la profunditat, que és el grau en $y$. Diem que un element de $\mathfrak{H}^1$ té pes (pur) $n$ si tots els monomis que el formen tenen pes $n$.

El producte escartejat que hem mencionat abans és fàcil de definir en paraules.

**6.5.4 Definició.** Un escartejament de dues paraules és una paraula obtinguda posant les lletres de cadascuna de les paraules tot mantenint l'ordre intern de cada paraula.

Per exemple, els escartejaments de *ab* i *cd* són

$$abcd\ ,\ acbd\ ,\ acdb\ ,\ cabd\ ,\ cadb\ ,\ cdab.$$

**6.5.5 Definició.** Si $w_1$ i $w_2$ són dues paraules qualssevol de $\mathfrak{H}$, definim el producte escartejat

$$w_1 \sqcup\!\sqcup w_2 = \sum \text{tots els escartejaments de } w_1 \text{ i } w_2.$$

**6.5.6 Exemple.** Vegem que

$$\zeta(2)\cdot\zeta(3) = \zeta(2,3) + 3\zeta(3,2) + 6\zeta(4,1)$$

Qui és $xy \sqcup\!\sqcup \mathbf{x^2y}$?

Els escartejaments són

$$xy\mathbf{x^2y}, x\mathbf{x}y\mathbf{xy}, x\mathbf{x^2}y\mathbf{y}, x\mathbf{x^2y}y, \mathbf{x}xy\mathbf{xy},$$
$$\mathbf{x}x\mathbf{xy}y, \mathbf{x}x\mathbf{xy}y, \mathbf{x^2}xy\mathbf{y}, \mathbf{x^2}x\mathbf{y}y, \mathbf{x^2y}xy,$$

d'on

$$xy \sqcup\!\sqcup x^2y = xyx^2y + 3x^2yxy + 6x^3y^2.$$

**6.5.7 Proposició.** *Propietats del producte escartejat*:

- $\mathfrak{H}$ *esdevé un anell commutatiu amb aquest producte, una* $\mathbb{Q}$*-àlgebra.*
- $\mathfrak{H}^1$ *i* $\mathfrak{H}^0$ *són subanells, sub-*$\mathbb{Q}$*-àlgebres.*
- *El producte escartejat de dues paraules de pes pur* $n$ *i* $m$ *té pes* $n+m$*.*
- $Z$ *és un morfisme d'anells, o sigui*

$$Z(w_1 \sqcup\!\sqcup w_2) = Z(w_1)Z(w_2).$$

Aquesta última propietat és una conseqüència "formal" de la definició, no depèn de com hem definit $\omega_x$ i $\omega_y$, només de si convergeix la integral.

A $\mathfrak{H}^1$ podem definir el producte harmònic inductivament per

$$1 * w = w * 1 = w,$$

$$z_k w_1 * z_l w_2 := z_k(w_1 * z_l w_2) + z_l(z_k w_1 * w_2) + z_{k+l}(w_1 * w_2),$$

per a totes $k, l \geq 1$, i per a totes les paraules $w, w_1, w_2 \in \mathfrak{H}^1$, i estenent-lo per $\mathbb{Q}$-bilinealitat. També es pot estendre a tot $\mathfrak{H} = \mathbb{Q}\langle x, y\rangle$.

**6.5.8 Proposició.** *Propietats del producte harmònic*:

- *El producte harmònic de dos elements de pes pur* $n$ *i* $m$ *té pes pur* $n+m$*.*
- $\mathfrak{H}^1$ *és una àlgebra commutativa per* $*$*, i* $\mathfrak{H}^0$ *és una subàlgebra.*
- $Z$ *és un morfisme d'anells també per* $*$*, o sigui,*

$$Z(w_1 * w_2) = Z(w_1)Z(w_2).$$

Per exemple, tenim que

$$z_k * z_l = z_k z_l + z_l z_k + z_{k+l}.$$

## 6.6 Relacions dobles finites

Donades dues paraules $w_1$ i $w_2$ de $\mathfrak{H}^0$, tenim, per tant, que

$$Z(w_1 \sqcup\!\sqcup w_2) = Z(w_1 * w_2).$$

Les relacions obtingudes s'anomenen les relacions dobles finites.

El primer exemple és

$$4\zeta(3,1) + 2\zeta(2,2) = 2\zeta(2,2) + \zeta(4) \quad (= \zeta(2)^2),$$

d'on tenim que $4\zeta(3,1) = \zeta(4)$.

**Observació important:** Hi ha altres relacions a més d'aquestes.

**6.6.1 Exemples.** Les igualtats $\zeta(2,1) = \zeta(3)$ i $4\zeta(2,2) = 3\zeta(4)$ no s'obtenen de les relacions d'abans.

Podem obtenir més relacions considerant elements de $\mathfrak{H}^1$, que corresponen a sumes divergents.

**6.6.2 Observació.** Si $w \in \mathfrak{H}^0$, aleshores

$$y * w = yw + w' \quad \text{amb} \quad w' \in \mathfrak{H}^0.$$

**6.6.3 Observació.** Si $w \in \mathfrak{H}^0$, aleshores

$$y \sqcup\!\sqcup w = yw + w'' \quad \text{amb} \quad w'' \in \mathfrak{H}^0$$

**6.6.4 Corol·lari.** *Per a tot $w \in \mathfrak{H}^0$, és $y \sqcup\!\sqcup w - y * w \in \mathfrak{H}^0$.*

**6.6.5 Teorema.** (Zagier) *Per a tot $w \in \mathfrak{H}^0$, és $Z(y \sqcup\!\sqcup w - y * w) = 0$.*

**Conseqüència:** Tenim més relacions entre els valors zeta múltiples.

**6.6.6 Conjectura.** *Les relacions següents:*

$$\begin{array}{ll} \text{per a tot } w_1, w_2 \in \mathfrak{H}^0, & Z(w_1 \sqcup\!\sqcup w_2 - w_1 * w_2) = 0, \\ \text{per a tot } w \in \mathfrak{H}^0, & Z(y \sqcup\!\sqcup w - y * w) = 0, \end{array}$$

*generen totes les relacions sobre $\mathbb{Q}$ que hi ha.*

**6.6.7 Exemple.** Prenem $w = xy$ en el teorema anterior. A partir de $y \sqcup xy = yxy + 2xy^2$ i de $y * xy = z_1 * z_2 = z_1z_2 + z_2z_1 + z_3 = yxy + xy^2 + x^2y$, tenim que

$$y \sqcup xy - y * xy = xy^2 - x^2y.$$

Com a conseqüència, $\zeta(2,1) = \zeta(3)$.

**6.6.8 Exemple.** Prenem $w = x^2y$ en el teorema anterior. A partir de $y \sqcup x^2y = yx^2y + xyxy + 2x^2y^2$ i de $y * x^2y = z_1 * z_3 = z_1z_3 + z_3z_1 + z_4 = yx^2y + x^2y^2 + x^3y$, tenim que $y \sqcup x^2y - y * x^2y = xyxy + x^2y^2 - x^3y$. Com a conseqüència, $\zeta(2,2) + \zeta(3,1) = \zeta(4)$.

**6.6.9 Exemple.** Prenem $w = xy^2$ en el teorema anterior. Obtenim que $\zeta(2,2) + \zeta(3,1) = \zeta(2,1,1)$.

**6.6.10 Corol·lari.** (dels exemples i de la irracionalitat) *La dimensió sobre $\mathbb{Q}$ de cadascun dels espais vectorials $\mathcal{Z}_n$ generats pels valors multizetes de pesos $n = 2, 3, 4$ és igual a 1, i estan generats per $\zeta(n)$.*

## 6.7 Relacions dobles generals

Anem a estudiar més relacions entre valors multizeta, aquest cop utilitzant series divergents sortint d'elements qualssevol de $\mathfrak{H}^1$, i no només els de la forma $y \sqcup \chi^0$. Per a fer-ho necessitem dos resultats sobre l'estructura de $\chi$ com a anell commutatiu, tant pel producte escartejat $\sqcup$ com pel producte harmònic $*$.

**6.7.1 Teorema.** (Reutenauer 1993 [5]) *Se satisfà que* $\mathrm{reg}^T_{\sqcup} : \mathfrak{H}^1_{\sqcup} \cong \mathfrak{H}^0_{\sqcup}[T]$, *com a $\mathbb{Q}$-àlgebres, en aplicar $y$ en $T$ i $\mathfrak{H}^0$ en ell mateix. O sigui,*

1. *Per a tot $w \in \mathfrak{H}^1$, $\exists n \geq 0$ tal que, per a tot $i = 0, \ldots, n$, existeix $w_i \in \mathfrak{H}^0$ tal que*
$$w = \sum_{i=0}^{n} w_i \sqcup y^{\sqcup i}.$$

*2. És morfisme d'anells, o sigui*

$$(\sum_{i=0}^{n} w_i \sqcup\!\sqcup y^{\sqcup\!\sqcup i}) \sqcup\!\sqcup (\sum_{j=0}^{m} u_j \sqcup\!\sqcup y^{\sqcup\!\sqcup j}) = \sum_{k=0}^{n+m} v_k \sqcup\!\sqcup y^{\sqcup\!\sqcup k},$$

*on* $v_k = \sum_{i+j=k} w_i \sqcup\!\sqcup u_j$.

**6.7.2 Observació.** $y^{\sqcup\!\sqcup n} = n!y^n$.

**6.7.3 Teorema.** (Hoffman 1997 [3]) $\mathrm{reg}_*^T : \mathfrak{H}_*^1 \cong \mathfrak{H}_*^0[T]$ *com a* $\mathbb{Q}$*-àlgebres, en aplicar* $y$ *en* $T$ *i* $\mathfrak{H}^0$ *en ell mateix.*

**Exercici:** $y^{*2} = 2y^2 + xy$, $y^{*3} = 6y^3 + 3yxy + 3xy^2 + x^2y$.

**6.7.4 Corol·lari.** *Existeixen dos morfismes d'anells*

$$Z^{\sqcup\!\sqcup} : \mathfrak{H}^1_{\sqcup\!\sqcup} \to \mathbb{R}[T],$$
$$Z^* : \mathfrak{H}^1_* \to \mathbb{R}[T]$$

*tals que apliquen* $y$ *en* $T$ *i estenen el morfisme* $Z : \mathfrak{H}^0 \to \mathbb{R}$.

El teorema del Zagier d'abans s'interpreta així:

$$Z^{\sqcup\!\sqcup}(w) = Z^*(w),$$

si $w = yw'$ amb $w' \in \mathfrak{H}^0$.

Potser podríem pensar que $Z^{\sqcup\!\sqcup}(w) = Z^*(w)$ és sempre cert per a tot $w \in \chi^1$. Però l'exemple següent ens mostra que això no és així.

**6.7.5 Exemple.**

$$y^{*2} = 2y^2 + xy \Rightarrow Z^*(y^2) = \frac{T^2}{2} - \frac{\zeta(2)}{2},$$
$$y^{\sqcup\!\sqcup 2} = 2y^2 \Rightarrow Z^{\sqcup\!\sqcup}(y^2) = \frac{T^2}{2}.$$

**6.7.6 Definició.** Considerem

$$A(u) := \exp\left(\sum_{n=2}^{\infty} \frac{(-1)^n}{n} \zeta(n) u^n\right) = \sum_{k=0}^{\infty} \gamma_k u^k \in \mathbb{R}[[T]].$$

Tenim que

$$A(u) = e^{\gamma u}\Gamma(1+u), \text{ per a } |u| < 1 \text{ i } \gamma \text{ la constant d'Euler.}$$

Tenim que $\gamma_0 = 1$, $\gamma_1 = 0$, $\gamma_2 = \frac{\zeta(2)}{2}$, $\gamma_3 = -\frac{\zeta(3)}{3}$, $\gamma_4 = \frac{\zeta(4)}{4} + \frac{\zeta(2)^2}{8}$,...

**6.7.7 Definició.** Considerem el morfisme $\mathbb{R}$-lineal $\rho : \mathbb{R}[T] \to \mathbb{R}[T]$ determinat per

$$\rho\left(\frac{T^n}{n!}\right) := \sum_{k=0}^{n} \gamma_k \frac{T^{n-k}}{(n-k)!}, \text{ o sigui } \rho(e^{Tu}) = A(u)e^{Tu}.$$

El teorema principal de l'article de Ihara, Kaneko i Zagier [4] és el següent.

**6.7.8 Teorema.** (Ihara-Kaneko-Zagier) *Se satisfà que*

$$Z^{\text{ш}}(w) = \rho(Z^*(w)).$$

**6.7.9 Exemple.** Tenim que

$$Z^{\text{ш}}(y^2xy) = \frac{\zeta(2)}{2}T^2 - 2\zeta(2,1)T + 3\zeta(2,1,1),$$

i que

$$Z^*(y^2xy) = \frac{\zeta(2)}{2}T^2 - (\zeta(3) + \zeta(2,1))T + \frac{\zeta(4)}{2} + \zeta(3,1) + \zeta(2,1,1).$$

D'altra banda,

$$\rho(T^2) = T^2 + \zeta(2),$$

i, per tant, deduïm del teorema que

$$\zeta(3) = \zeta(2,1)$$

i que

$$3\zeta(2,1,1) = \frac{\zeta(2)}{2} + \frac{\zeta(4)}{2} + \zeta(3,1) + \zeta(2,1,1).$$

La demostració del teorema 6.7.8 utilitza, entre altres coses, unes funcions de les quals Zagier té força resultats: els polilogaritmes.

## 6.8 Polilogaritmes

**6.8.1 Definició.** El polilogaritme associat a $(n_1, n_2, \ldots, n_k)$ és

$$\mathrm{Li}_{(n_1,n_2,\ldots,n_k)}(t) := \sum_{a_1>\cdots>a_k>0} \frac{t^{a_1}}{a_1^{n_1}\cdots a_k^{n_k}}.$$

**6.8.2 Lema.** (Representació integral) *Si* $n = n_1+\cdots+n_k$, *aleshores*

$$\mathrm{Li}_{(n_1,\ldots,n_k)}(t) = \int_{t>t_1>\cdots>t_n>0} \cdots \int \omega_1(t_1)\omega_2(t_2)\cdots\omega_n(t_n),$$

*on* $\omega_i(t) = dt/(1-t)$ *si* $i = n_1, n_1+n_2, \cdots, n$; $\omega_i(t) = dt/t$ *si no.*

**6.8.3 Observació.** 1. $\mathrm{Li}_1(t) = \log(1/(1-t))$.

2. $\mathrm{Li}_{(n_1,n_2,\ldots,n_k)}(1) = \zeta((n_1, n_2, \ldots, n_k))$, si $n_1 > 1$.

**6.8.4 Definició.** Definim el valor multizeta truncat fins a $M$ com

$$\zeta_M(n_1, n_2, \ldots, n_k) := \sum_{M>a_1>\cdots>a_k>0} \frac{1}{a_1^{n_1}\cdots a_k^{n_k}}.$$

Tenim aleshores que el producte harmònic s'estén als valors multizeta truncats, obtenint que

$$\zeta_M(\underline{n})\zeta_M(\underline{n'}) = \sum_{\text{certes } \underline{n''}} \zeta_M(\underline{n''}).$$

D'altra banda, pel producte escartejat tenim que el producte de polilogaritmes també s'expressa com a suma de polilogaritmes, seguint la regla del producte escartejat:

$$\mathrm{Li}_{\underline{n}}(t)\,\mathrm{Li}_{\underline{n'}}(t) = \sum_{\text{certes } \underline{n''}} \mathrm{Li}_{\underline{n''}}(t).$$

Això es relaciona amb els valors multizeta truncats utilitzant la fórmula següent:

$$\mathrm{Li}_{\underline{n}}(t) = (1-t)\sum_{M=1}^{\infty} \zeta_M(\underline{n})t^{M-1}.$$

Els dos lemmes següents són clau en la demostració del teorema 6.7.8.

**6.8.5 Lema.** *Es té que*

$$\zeta_M(\underline{n}) = Z^*(\underline{n})(\log(M)+\gamma) + O(M^{-1}\log^J(M)),$$
$$\mathrm{Li}_{\underline{n}}(t) = Z^{ш}(\underline{n})(\log(\frac{1}{1-t})) + O((1-t)\log^J(\frac{1}{1-t})).$$

**6.8.6 Lema.** *Si $P(T) \in \mathbb{R}[T]$ i $Q(T) = \rho(P(T))$, aleshores*

$$\sum_{M=1}^{\infty} P(\log(M)+\gamma)t^{M-1} = \frac{1}{1-t}Q(\log(\frac{1}{1-t})) + O(\log^J(\frac{1}{1-t}).$$

**6.8.7 Notació.** Definim les regularitzacions com

$$\mathrm{reg}^T_{ш} : \mathfrak{H}^1_{ш} \cong \mathfrak{H}^0_{ш}[T],$$
$$\mathrm{reg}_{ш} = \mathrm{reg}^T_{ш\,|T=0} : \mathfrak{H}^1_{ш} \to \mathfrak{H}^0,$$
$$\mathrm{reg}^T_* : \mathfrak{H}^1_* \cong \mathfrak{H}^0_*[T],$$
$$\mathrm{reg}_* = \mathrm{reg}^T_{*\,|T=0} : \mathfrak{H}^1_* \to \mathfrak{H}^0.$$

**6.8.8 Exemple.**

$$\mathrm{reg}^T_{ш}(y^2) = \frac{T^2}{2}\ ,\ \mathrm{reg}_{ш}(y^2) = 0,$$
$$\mathrm{reg}^T_*(y^2) = \frac{T^2}{2} - \frac{xy}{2}\ ,\ \mathrm{reg}_{ш}(y^2) = -\frac{xy}{2}.$$

**6.8.9 Proposició.** (Fórmules explícites per a les regularitzacions) *Per a tot $m \geq 0$ i tot $w_0'$ de $\mathfrak{H}^1$, tenim que*

$$\mathrm{reg}^T_{ш}(y^m x w_0') = \sum_{l=0}^{\infty}(-1)^l x(y^l \,ш\, w_0')\frac{T^{m-l}}{(m-l)!},$$
$$\mathrm{reg}_{ш}(y^m x w_0') = (-1)^m x(y^m \,ш\, w_0').$$

*Si $w_0 \in \mathfrak{H}^0$, tenim que*

$$\mathrm{reg}_{ш}(y^m w_0) = \sum_{i=0}^{m}(-1)^i y^i \,ш\, y^{m-i}w_0,$$
$$\mathrm{reg}_*(y^m w_0) = \sum_{i=0}^{m}\frac{(-1)^i}{i!}y^i * y^{m-i}w_0.$$

## 6.9 Equivalències

Un dels resultats principals de l'article de Ihara, Kaneko i Zagier és una llista de afirmacions equivalents a la fórmula del teorema 6.7.8.

**6.9.1 Teorema.** *Suposem sabudes les relacions dobles finites. Aleshores les següents propietats són equivalents*:

(1) $Z^{\text{ш}}(w) - \rho Z^*(w) = 0$, *per a tota* $w \in \mathfrak{H}^1$.

- $(Z^{\text{ш}}(w) - \rho Z^*(w))_{|T=0} = 0$, *per a tota* $w \in \mathfrak{H}^1$.

(2) $Z^{\text{ш}}(w_1 \sqcup\!\sqcup w_0 - w_1 * w_0) = 0$, *per a tota* $w_1 \in \mathfrak{H}^1$ *i* $w_0 \in \mathfrak{H}^0$.

(3) $Z(\mathrm{reg}_{\text{ш}}(w_1 \sqcup\!\sqcup w_0 - w_1 * w_0)) = 0$, *per a tota* $w_1 \in \mathfrak{H}^1$ *i* $w_0 \in \mathfrak{H}^0$.

(4) *El mateix canviant* $\sqcup\!\sqcup$ *per* $*$.

(5) $Z(\mathrm{reg}_{\text{ш}}(y^m * w_0)) = 0$, *per a tota* $w_0 \in \mathfrak{H}^0$.

Aquest resultat, de fet, es pot aplicar a qualssevol morfismes $Z^*$ i $Z^{\text{ш}}$ en un anell de característica zero.

D'aquest resultat es poden deduir alguns resultats coneguts, i d'altres menys coneguts. Un d'ells és l'anomenat teorema de la suma, que va ser demostrat per primer cop per Andrew Granville. És una generalització d'un resultat d'Euler 6.3.1, qui ho va demostrar per al cas $k = 2$.

**6.9.2 Proposició.** *Sigui* $S(m,k)$ *la suma de tots els monomis a* $\mathfrak{H}^0$ *de pes* $m$ *i profunditat* $k$. *Aleshores, si* $m > k+1 \geq 2$, *tenim que*

$$(-1)^k \,\mathrm{reg}_{\text{ш}}(y^k * x^{m-k-1}y) = S(m,k+1) - S(m,k).$$

Demostració.Tenim que

$$S(m,k) = (-1)^k x(y^k \sqcup\!\sqcup x^{m-k-2})y.$$

D'altra banda, tenim que

$$y^k * x^{m-k-1}y = \sum_{i=0}^{k} y^i x^{m-k-1} y^{k+1-i} + \sum_{j=0}^{k-1} y^j x^{m-k} y^{k-j}.$$

i, com que,

$$\mathrm{reg}_{ш}(y^a x^b y^c) = (-1)^a x(y^a \; ш \, x^{b-1} y^c),$$

obtenim el resultat.

**6.9.3 Corol·lari.** (El teorema de la suma de Granville [2]) *La suma de tots els valors multizeta de pes fixat $n$ i profunditat fixada $< n$ és igual a $\zeta(n)$. O sigui, fixada $k < n$ tenim que*

$$\sum_{n_1+\cdots+n_k=n} \zeta(n_1, \ldots, n_k) = \zeta(n).$$

**6.9.4 Exemple.** $\zeta(2,1) = \zeta(3)$,

$$\zeta(3,1) + \zeta(2,2) = \zeta(4) = \zeta(2,1,1).$$

Demostració. Per l'última de les equivalències, tenim que

$$Z((-1)^k \, \mathrm{reg}_{ш}(y^k * x^{m-k-1} y)) = 0.$$

Per tant,

$$Z(S(m,k+1)) = Z(S(m,k)) = \cdots = Z(S(m,1)) = \zeta(m).$$

**6.9.5 Conjectura.** *Les úniques relacions entre els valors de les funcions multizeta s'obtenen d'igualar*

$$Z^{ш}(w) = \rho(Z^*(w)), \text{ per a tot } w \in \mathfrak{H}^1.$$

*O bé, equivalentment, el nucli del morfisme*

$$Z : \mathfrak{H}^0 \to \mathcal{Z} := \langle \zeta(n_1, n_2, \ldots, n_k) \mid n_1 > 1, n_i \geq 1 \forall i, \forall k \geq 1 \rangle_{\mathbb{Q}}$$

*és igual a*

$$\ker(Z) = \{\mathrm{reg}_{ш}(y^m * w_0) \mid \forall w_0 \in \mathfrak{H}^0\}.$$

La conjectura 6.6.6 que hem anunciat abans és equivalent a

**6.9.6 Conjectura.** *Se satisfà que*

$$\ker(Z) = \{\mathrm{reg}_{ш}(y * w_0) \mid \forall w_0 \in \mathfrak{H}^0\}.$$

Com a conseqüències de qualsevol de les conjectures anteriors, obtenim les conjectures següents, que formen part del folklore.

**6.9.7 Conjectura.** *Dos valors multizeta de pesos diferents són linealment independents sobre* $\mathbb{Q}$*. O sigui,* $\mathcal{Z} = \bigoplus_n \mathcal{Z}_n$*, com a* $\mathbb{Q}$*-algebra.*

*Per tant, tenim que els valors* $\zeta(n_1, \ldots, n_k)$ *són sempre transcendents.*

*Per exemple,* $\zeta(2)^3$ *i* $\zeta(3)^2$ *són independents sobre* $\mathbb{Q}$*.*

## 6.10 Dimensions

Una de les últimes coses que fan en l'article és estudiar i demostrar alguna petita cosa sobre quines poden ser les dimensions de l'espai generat per les multizetes de pes fixat. El resultat que esperen provar ve donat per una conjectura famosa.

**6.10.1 Conjectura.** (Zagier, Broadhurst-Kreimer) *La dimensió sobre* $\mathbb{Q}$ *de* $\mathcal{Z}_n$ *és* $d_n$*, on* $d_0 = 1$*,* $d_1 = 0$*,* $d_2 = 1$ *i* $d_n = d_{n-2} + d_{n-3}$*.*

Aquesta conjectura va sorgir de l'estudi de les multizetes de profunditat $\leq 2$.

**6.10.2 Corol·lari.** *Suposem certa la conjectura* 6.10.1*. Aleshores, els valors següents són linealment independents sobre* $\mathbb{Q}$ *i generen* $\mathcal{Z}_{\leq 10}$*:*

$$\zeta(2),\ \zeta(3),\ \zeta(5),\ \zeta(9),$$

$$\zeta(6,8),\ \zeta(8,2).$$

De fet, hi ha una conjectura que, si fos certa, justificaria la conjectura 6.10.1, i que explicitaria una base per als espais $\mathcal{Z}_n$.

**6.10.3 Conjectura.** (La conjectura de la base (Hoffman)) *Tot valor multizeta pot ser escrit com a suma de múltiples racionals de valors multizeta que sols continguin 2 i 3.*

A diferència de la conjectura 6.10.1, aquesta conjectura pot ser atacada per a mètodes purament algebraics, estudiant com són els espais equivalents a $\mathfrak{H}^1$.

**6.10.4 Exemple.**

$$\zeta(7) = \frac{252}{151}\zeta(3,2,2) + \frac{672}{151}\zeta(2,3,2) + \frac{528}{151}\zeta(2,2,3).$$

Com a conseqüència de la conjectura de la base i de la dimensió tindríem que

**6.10.5 Conjectura.** *Els valors multizeta que sols contenen 2 i 3 són tots linealment independents sobre $\mathbb{Q}$ i generen $\mathcal{Z}$.*

Sobre la conjectura sobre les dimensions, tenim un resultat que ens dóna una de les desigualtats.

**6.10.6 Teorema.** (Goncharov, Terasoma [7])

$$\dim_{\mathbb{Q}}(\mathcal{Z}_n) \leq d_n.$$

Finalment, voldria mencionar un dels teoremes de Zagier sobre valors multizeta, que en certa manera generalitza el càlcul d'Euler.

**6.10.7 Teorema.** (Teorema de la paritat, Zagier) *Tot valor de les funcions multizeta amb pes $n$ i profunditat $k$, si $n \not\equiv k (mod\ 2)$, és combinació lineal de valors amb profunditat menor i productes de valors amb pes menor.*

# Bibliografia


[1] Apéry, R.: Irrationalité de $\zeta(2)$ et $\zeta(3)$. *Astérisque* 61 (1979), 11–13.

[2] Granville, A.: A decomposition of Riemann's zeta-function. *Analytic Number Theory*. London Mathematical Society Lecture Note Series 247, Y. Motohashi (ed.). Cambridge University Press, 1997, pp. 95–101.

[3] Hoffman, M.: The algebra of multiple harmonic series. *J. of Algebra* 194 (1997), 477–495.

[4] Ihara, K.; Kaneko, M; Zagier, D.: Derivation and double shuffle relations for multiple zeta functions. *Comp. Math.* 142 (2006), 307–338.

[5] Reutenauer, C.: *Free Lie Algebras*. Oxford Science Publications, 1993.

[6] Rivoal, T.: La fonction zêta de Riemann prend une infinité de valeurs irrationnelles aux entiers impairs. *C. R. A. S. Paris Sér. I Math.* 331.4 (2000), 267–270.

[7] Terasoma, T.: Mixed Tate motives and multiple zeta values, *Invent. Math.* 149 (2002), 339–369.

[8] Zagier, D.: Values of zeta functions and their applications. *First European Congress of Mathematics (Paris, 1992)*, Vol. II, A. Joseph et. al. (eds.). Birkhäuser, Basel, 1994, pp. 497–512.

[9] Zudilin, W.: One of the numbers $\zeta(5)$, $\zeta(7)$, $\zeta(9)$, $\zeta(11)$ is irrational. *Uspekhi Mat. Nauk* [Russian Math. Surveys] 56:4 (2001), 149–15.

X. Xarles

Departament de Matemàtiques

Universitat Autònoma de Barcelona

08193, Bellaterra

**xarles@mat.uab.cat**