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 ∞, 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. $\square$

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, Δ 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 Δ 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,

(4.3)

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

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 λ 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 ∞ (és a dir, $n_0 \geq 0$); i una forma parabòlica és una forma modular que s'anul·la en ∞ (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* ∞, *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 Δ 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, δ i ε 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 Δ 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 δ en $\tau = \rho$ i un zero d'ordre més gran o igual que ε 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 Δ^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 Δ^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 Δ^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* κ_{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 ϕ_k i, a més a més, en l'espai quocient M_k/S_k, que és de dimensió 1, ϕ_k indueix la multiplicació per κ_k. En particular, si M_k és de dimensió 1, llavors κ_k és un valor propi de ϕ_k, i qualsevol funció no nul·la $F_k \in M_k$ és pròpia de valor propi κ_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 κ_{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 ϑ_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 κ_{k-12i} per a ϕ_{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 ϕ_k de valor propi $\kappa_{k-12i} \neq \kappa_k$. Inductivament, obtenim una base de S_k de funcions pròpies de ϕ_k de valors propis κ_{k-12i}, $1 \leq i \leq m$, diferents. Ara, com que en M_k/S_k, de dimensió 1, ϕ_k és una homotècia de raó κ_k i en S_k, que és un subespai invariant per ϕ_k, hi ha una base de funcions pròpies de valors propis diferents de κ_k, existeix una funció pròpia $F_k \in M_k$, $F_k \notin S_k$, de valor propi κ_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, $\#E(\mathbb{F}_q) \equiv 1 - N_{\mathbb{F}_q|\mathbb{F}_p}(a_p) \pmod{p}$. 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 $x = P(u)$, $y = \frac{-1}{2}D(P,u)$, 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 ϕ 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 ϕ. 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 λ_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

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

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 ψ 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 λ_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

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

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 ∞ (és a dir, amb un creixement en ∞ 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 ∞ 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* Δ*;*
(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 δ^{-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 $x^2 + y^2 \geq 1$, $-\frac{1}{2} \leq x \leq \frac{1}{2}$, 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 θ des de $\theta = \frac{2\pi}{3}$ fins a $\theta = \frac{2\pi}{6}$; 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 τ per $\frac{-1}{\tau}$ en la meitat esquerra de l'arc, o sigui, de $e^{i\theta}$ per $-e^{-i\theta}$ per a θ decreixent des de $\frac{2\pi}{3}$ fins a $\frac{2\pi}{4}$ (això és θ 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 λ_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 ϕ 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, δ, i ε (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 ∞ 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^∞, 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 ∞ 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^∞ 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 $|_2 T_n$ també actua en l'espai V_2^*; això permet escriure la igualtat

$$(gE_2)|_2 T_n^\infty - (g|_0 T_n)E_2 \equiv \frac{3}{\pi}\big((gy^{-1})|_2 T_n^\infty - (g|_0 T_n)y^{-1}\big) \pmod{V_2^*}$$

que, juntament amb el fet que

$$\begin{aligned} \big((gy^{-1})|_2 T_n^\infty\big)(\tau) &= \sum_{\substack{ad=n \\ b \pmod d}} \frac{n}{d^2} g\left(\frac{a\tau+b}{d}\right) \operatorname{Im}\left(\frac{a\tau+b}{d}\right)^{-1} \\ &= y^{-1}(g|_0 T_n)(\tau), \end{aligned}$$

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 $\operatorname{Res}_\infty$ 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 Φ 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, Φ 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, δ i ε 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 Φ mòdul p, com a funcions de j, en la forma

$$\Phi = \frac{E_2E_4}{E_6 j} \equiv \frac{E_{p+1}E_4}{E_{p-1}E_6 j} = \frac{\Delta^{\delta+\varepsilon-1}E_4^{3(1-\delta)}\tilde{E}_{p+1}}{jE_6^{2\varepsilon}\tilde{E}_{p-1}} \pmod p$$

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 ϑ_{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 ϑ_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 λ_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*

$$A_{n+1}(j) = \left(j - 24\frac{144n^2-29}{(2n+1)(2n-1)}\right)A_n(j) - 36\frac{(12n-13)(12n-7)(12n-5)(12n+1)}{n(n-1)(2n-1)^2}A_{n-1}(j),$$

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^ε, V_n^δ, δ, $\varepsilon \in \{0,1\}$, 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* $m \geq 0$*,* δ*,* $\varepsilon \in \{0, 1\}$*. 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 δ.

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 σ 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 α, 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 χ^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 χ^r per a l'acció de Γ.

Si es determinen δ i ε 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 $\varepsilon = 1$.* □

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