(*March 9, 2021*)

14. *Elliptic modular forms*

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/~garrett/

[This document is
http://www.math.umn.edu/~garrett/m/complex/notes_2020-21/14_elliptic_modular_forms.pdf]

The coefficients g_2 and g_3 in the Weierstraß form

$$\wp_\Lambda'^2 \;=\; 4\wp_\Lambda^3 - g_2\wp_\Lambda - g_3$$

are simple examples of *modular forms*, as functions of the lattice Λ on which the elliptic functions $\wp_\Lambda$ and $\wp'_\Lambda$ live. Also, the cubic discriminant (up to a scalar multiple), Ramanujan's Δ-function

$$\Delta \;=\; \Delta_\Lambda \;=\; g_2^3 - 27g_3^2$$

is a modular form. It is the prototype of a *cuspform*, as explained below.

In this brief introduction, we necessarily omit some basic topics, for example, *Hecke operators*, *Poincaré series*, and *theta series*.

---

1. *Elliptic modular forms*

[1.1] Functions of lattices

The functions traditionally denoted $g_2 = g_2(\Lambda)$ and $g_3 = g_3(\Lambda)$ in Weierstraß' equation relating $\wp$ and $\wp'$ certainly depend on the lattice, or *module*, Λ. It is in this sense that they are *modular forms*. [1] That is, as they arose historically, *modular forms* are functions on the set of lattices in $\mathbb{C}$.

The functions g_2 and g_3 have the further property of *homogeneity*, meaning that for any non-zero complex number α

$$g_2(\alpha\cdot\Lambda) = \alpha^{-4}\,g_2(\Lambda) \qquad\text{and}\qquad g_3(\alpha\cdot\Lambda) = \alpha^{-6}\,g_3(\Lambda)$$

since

$$\sum_{0\neq\lambda\in\Lambda}\frac{1}{(\alpha\lambda)^{2k}} \;=\; \alpha^{-2k}\sum_{0\neq\lambda\in\Lambda}\frac{1}{\lambda^{2k}}$$

Thus, more precisely, *modular forms* are *homogeneous* functions on lattices in $\mathbb{C}$.

[1.2] From lattices to the upper half-plane

We would be happier if the inputs to these functions-of-lattices were more familiar, rather than *lattices*, since initially we might see no helpful structure on the set

[1] Why *form* rather than *function*? After all, these functions *are* literal functions (in our modern sense) on the set of lattices in $\mathbb{C}$. Certainly there was historical hesitancy to attempt to refer to functions on exotic spaces, since there was no completely abstract notion of *function* in the 19^{th} century.

of lattices. The homogeneity allows a more tangible viewpoint, as follows. Let F be a *homogeneous* function F of degree $-k$ on lattices, meaning that [2]

$$F(\alpha \cdot \Lambda) \;=\; \alpha^{-k} \cdot F(\Lambda)$$

For a $\mathbb{Z}$-basis ω_1, ω_2 for a lattice Λ, *ordered* so that $\omega_1/\omega_2 \in \mathfrak{H}$, *normalize* the second basis element to 1, by multiplying Λ by ω_2^{-1} and using basis $z = \omega_1/\omega_2$, 1 for the dilated-and-rotated lattice $\omega_2^{-1} \cdot \Lambda$. By homogeneity,

$$F(\omega_2^{-1} \cdot \Lambda) \;=\; \omega_2^k \cdot F(\Lambda)$$

allowing recovery of the value of F on the original lattice from the value on the adjusted one.

Further, a function of lattices does not depend upon *choice of ordered basis*. That is, for $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL_2(\mathbb{Z})$ [3] the new ordered basis

$$\begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix} \;=\; \begin{bmatrix} a\omega_1 + b\omega_2 \\ c\omega_1 + d\omega_2 \end{bmatrix} \;=\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

gives the same lattice, that is,

$$\mathbb{Z} \cdot \omega_1' + \mathbb{Z} \cdot \omega_2' \;=\; \mathbb{Z} \cdot \omega_1 + \mathbb{Z} \cdot \omega_2$$

The normalization and change-of-basis can be combined, as follows. For $\mathbb{R}$-linearly-independent ω_1 and ω_2, and without loss of generality with ω_1/ω_2 in the upper half-plane $\mathfrak{H}$, let

$$z \;=\; \omega_1/\omega_2 \qquad\qquad (\text{in } \mathfrak{H})$$

Put

$$f(z) \;=\; F(\mathbb{Z} \cdot z + \mathbb{Z} \cdot 1)$$

For $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL_2(\mathbb{Z})$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{bmatrix} z \\ 1 \end{bmatrix} \;=\; \begin{bmatrix} az+b \\ cz+d \end{bmatrix}$$

Since change-of-basis does not alter the value of a function of lattices, using homogeneity,

$$f(z) \;=\; F(\mathbb{Z} \cdot z + \mathbb{Z} \cdot 1) \;=\; F(\mathbb{Z} \cdot (az+b) + \mathbb{Z} \cdot (cz+d))$$

$$=\; (cz+d)^{-k}\, F(\mathbb{Z} \cdot \frac{az+b}{cz+d} + \mathbb{Z} \cdot 1) \;=\; (cz+d)^{-k}\, f(\frac{az+b}{cz+d})$$

Thus, the action of $SL_2(\mathbb{Z})$ or $SL_2(\mathbb{C})$ by *linear fractional transformations* [4]

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (z) \;=\; \frac{az+b}{cz+d}$$

---

[2] Yes, g_2 is homogeneous of degree -4 and g_3 is homogeneous of degree -6. Yes, it would have been better if their indices matched their degrees of homogeneity, at least up to sign, but the tradition developed otherwise.

[3] As usual, for a commutative ring R, the group $SL_2(R)$ is the group of invertible 2-by-2 matrices with entries in R and determinant 1.

[4] Also dubiously called *Möbius* transformations. That this is a genuine group action, including associativity, is not obvious from an *ad hoc* presentation. In fact, as we see later, this action is descended from a reasonable *linear* action on *projective space*, giving a conceptual explanation for the good behavior. Indeed, in general, linear fractional transformations truly act on the *Riemann sphere*, that is, on complex projective one-space $\mathbb{P}^1$, which is $\mathbb{C}$ with an additional point.

arises through renormalization of generators for lattices.

[1.3] Modular forms of weight $2k$ The next incarnation of *modular forms* is as *elliptic modular forms of weight* $2k$: these are *holomorphic* function f of a complex variable z on $\mathfrak{H}$, meeting the *automorphy condition* [5]

$$f(\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z)) \;=\; (cz+d)^{2k}\; f(z) \qquad\qquad (\text{where } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),\; z\in\mathfrak{H})$$

For example, up to normalizations, the functions associated to g_2 and g_3 above fit into a family of explicitly-constructable elliptic modular forms

$$\text{Eisenstein series} \;=\; \sum_{c,d} \frac{1}{(cz+d)^k} \qquad\qquad (\text{summed over } c,d \text{ not both } 0)$$

Since $cz+d$ is complex, we must take $2k\in\mathbb{Z}$. This series converges for $2k>2$. The series is identically 0, by obvious cancellation, for $2k$ an odd integer. Verification of the automorphy condition is direct, and is really just repeating the conversion of homogeneous functions-of-lattices to functions on $\mathfrak{H}$:

$$\sum_{m,n} \frac{1}{(m\frac{az+b}{cz+d}+n)^{2k}} \;=\; (cz+d)^{2k} \sum_{m,n} \frac{1}{\big(m(az+b)+n(cz+d)\big)^{2k}}$$

$$=\; (cz+d)^{2k} \sum_{m,n} \frac{1}{\big((ma+nc)z+(mb+nd)\big)^{2k}} \;=\; (cz+d)^{2k} \sum_{m,n} \frac{1}{(m'z+n')^{2k}}$$

$$(\text{with } (m',n') = (ma+nc,\; mb+nd) = (m,\; n)\begin{pmatrix} a & b \\ c & d \end{pmatrix})$$

Since right multiplication by any element of $SL_2(\mathbb{Z})$ is a bijection of $\mathbb{Z}^2-\{0\}$ to itself, the sum is again exactly over pairs of integers not both 0, recovering the Eisenstein series.

[1.4] Normalizations of Eisenstein series In the sum $\sum_{c,d}\frac{1}{(cz+d)^{2k}}$ over all pairs $(c,d)\neq(0,0)$, we could take out *common divisors* $\ell=\gcd(c,d)$:

$$\sum_{c,d} \frac{1}{(cz+d)^{2k}} \;=\; \sum_{c,d} \frac{1}{\ell^{2k}} \frac{1}{(\frac{c}{\ell}z+\frac{d}{\ell})^{2k}} \;=\; \sum_{c,d} \frac{1}{\ell^{2k}} \frac{1}{(\frac{c}{\ell}z+\frac{d}{\ell})^{2k}} \;=\; \sum_{\ell\ge1} \frac{1}{\ell^{2k}} \sum_{c,d:\,\gcd(c,d)=\ell} \frac{1}{(\frac{c}{\ell}z+\frac{d}{\ell})^{2k}}$$

$$=\; \sum_{\ell\ge1} \frac{1}{\ell^{2k}} \sum_{c',d':\,\gcd(c',d')=1} \frac{1}{(c'z+d')^{2k}} \;=\; \zeta(2k) \sum_{c',d':\,\gcd(c',d')=1} \frac{1}{(c'z+d')^{2k}}$$

That is, up to the constant $\zeta(2k)$, the sum over *all* c,d gives the same thing as the sum over *coprime* c,d. Some sources create notations that attempt to distinguish these variations, but there is no universal notational convention.

[1.5] Group-theoretic version of Eisenstein series Further, noticing that for $2k\in 2\mathbb{Z}$ the pairs $\pm(c,d)$ give the same outcome $(cz+d)^{2k}$, we might declare the weight-$2k$ Eisenstein series to have a leading coefficient $\frac{1}{2}$:

$$\text{Eisenstein series} \;=\; \tfrac{1}{2} \sum_{\text{coprime } c,d} \frac{1}{(cz+d)^{2k}}$$

Indeed, this is exactly a *group-theoretic* version of an Eisenstein series: with $\Gamma_\infty = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \subset \Gamma$, the coset space $\Gamma_\infty\backslash\Gamma$ is in bijection with the set of coprime pairs (c,d) modulo ±1, by

$$\Gamma_\infty\cdot\begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\longrightarrow\; \{\pm1\}\cdot(c,d)$$

[5] The function $j(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z) = (cz+d)^{-2k}$ is a *cocycle*, because it satisfies the condition $j(\gamma\delta,z) = j(\gamma,\delta(z))j(\delta,z)$.

Indeed, since $ad - bc = 1$, necessarily the c, d in a lower row of an element of $SL_2(\mathbb{Z})$ are mutually prime. Conversely, given coprime c, d, there exist a, b such that $ad - bc = 1$, creating an element of $SL_2(\mathbb{Z})$. Thus, another presentation of an Eisenstein series, perhaps optimally explanatory:

$$E_{2k}(z) \;=\; \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} \frac{1}{(c_\gamma z + d_\gamma)^{2k}} \;=\; \tfrac{1}{2} \sum_{\text{coprime } c,d} \frac{1}{(cz+d)^{2k}} \qquad (\text{where } \gamma = \begin{pmatrix} * & * \\ c_\gamma & d_\gamma \end{pmatrix})$$

[1.6] Congruence subgroups

There are Eisenstein series with *congruence conditions*: for fixed positive integer N and integers c_o, d_o, define Eisenstein series with *congruence conditions*

$$E(z) \;=\; \sum_{(c,d)=(c_o,d_o) \bmod N} \frac{1}{(cz+d)^k} \qquad (c, d \text{ not both } 0)$$

This is an example of a modular form *of level* N, meaning that a condition such as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod N \quad (\text{elementwise})$$

is necessary to have[6] this Eisenstein series satisfy the *automorphy* condition

$$E(\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z)) \;=\; (cz+d)^k \, E(z)$$

The first examples were tacitly of level 1. Such considerations motivate attention to natural subgroups of $SL_2(\mathbb{Z})$, with traditional notations: for a positive integer N,

$$\begin{aligned} \Gamma(N) \;&=\; \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;:\; a = 1 \bmod N, b = 0 \bmod N, c = 0 \bmod N, d = 1 \bmod N\} \\ &=\; \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;:\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod N\} \\ \Gamma_0(N) \;&=\; \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;:\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \bmod N\} \\ \Gamma_1(N) \;&=\; \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;:\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \bmod N\} \end{aligned}$$

In particular, the frequently occurring subgroup $\Gamma(N)$ is also denoted Γ_N for reasons of economy:

$$\Gamma_N = \Gamma(N) = \textit{principal} \text{ congruence subgroup of level } N$$

With level $N > 1$, it is possible to have Eisenstein series and other modular forms of odd integer weight, hence the shift in notation from weight $2k$ to k.

[1.7] A less-elementary modular form

Up to a normalizing constant, the *discriminant*[7] of Weierstraß' cubic $4x^3 - g_2 x - g_3$ is $g_2^3 - 27g_3^2$. For the lattice $\Lambda_z = \mathbb{Z} \cdot z + \mathbb{Z} \cdot 1 \subset \mathbb{C}$, the discriminant is an elliptic modular

[6] Some choices of the data c_o, d_o modulo N may allow larger groups than $\Gamma(N)$. For example, $c_o = d_o = 0$ does not require any congruence condition at all (and yields N^{-k} times the simplest Eisenstein series $E(z) = \sum_{c,d} 1/(cz+d)^k$ summed over all c, d not both 0.

[7] The *discriminant* of a cubic $(x-\alpha)(x-\beta)(x-\gamma)$ is $\Delta = (\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$. Invariant under permutations of the roots, it is expressible in terms of the *elementary* symmetric functions $s_1 = \alpha+\beta+\gamma$, $s_2 = \alpha\beta+\beta\gamma+\gamma\alpha$, and $s_3 = \alpha\beta\gamma$. After some work (see the appendix), one finds

$$\Delta \;=\; (s_1^2 - 4s_2)s_2^2 + s_3(-4s_1^3 + 18s_1 s_2 - 27s_3)$$

For a cubic $x^3 + px + q$ this simplifies to the more-familiar $-4p^3 - 27q^2$.

form of weight 12, usually renormalized as

$$\Delta(z) \;=\; \frac{1}{(2\pi)^{12}}\,(g_2^3 - 27g_3^2)$$

We'll later prove the surprising factorization

$$\Delta(z) \;=\; e^{2\pi i z}\prod_{n=1}^{\infty}(1-e^{2\pi i n z})^{24}$$

This factorization suggests combinatorial applications, in light of the generating function identity

$$\prod_{n=1}^{\infty}\frac{1}{1-q^n} \;=\; \sum_{n=0}^{\infty} p(n)\cdot x^n$$

where $p(n)$ is the number of *partitions* $n_1 + \ldots + n_k = n$, with $n_1 \le n_2 \le \ldots \le n_k$. Even more profoundly, as it turns out, the Fourier expansion

$$\Delta(z) \;=\; e^{2\pi i z} + \sum_{n\ge 2}\tau(n)\,e^{2\pi i n z}$$

has coefficients $\tau(n)$ with properties conjectured by S. Ramanujan: *weak multiplicativity* $\tau(mn) = \tau(m)\tau(n)$ for coprime m, n was proven by L. J. Mordell soon after, but the estimate $|\tau(p)| \le 2p^{\frac{11}{2}+\varepsilon}$ for every $\varepsilon > 0$ was proven only in 1974 by P. Deligne, as a striking corollary of the Grothendieck-Deligne-*et al* proof of Weil's conjectures on Hasse-Weil zeta functions of algebraic varieties. E. Hecke had proven $|\tau(p)| \le 2p^{\frac{12}{2}}$ in fairly straightforward fashion decades earlier, but that last $\frac{1}{2}+\varepsilon$ was much larger, and more meaningful, than it may seem.

[1.8] Preview: the j-invariant and parametrization of elliptic curves As above, a reasonable notion of isomorphism of elliptic curves $\mathbb{C}/\Lambda$ leads to identifying the collection of isomorphism classes with the quotient $\Gamma\backslash\mathfrak{H}$, with $\Gamma = SL_2(\mathbb{Z})$.

The j-function is

$$j(z) \;=\; 1728\frac{g_2^3}{g_2^3 - 27g_3^2}$$

The numerator and denominator are both weight 12 level one modular forms, so $j(z)$ is weight 0, that is, *invariant* under $SL_2(\mathbb{Z})$.

We will see that $z \to j(z)$ *injects* the quotient $SL_2(\mathbb{Z})\backslash\mathfrak{H}$ to complex projective one-space $\mathbb{P}^1$, so $j(z)$ is a sufficient invariant for isomorphism classes of elliptic curves over $\mathbb{C}$.

---

2. *Automorphy, growth, Fourier expansion, cuspforms*

Now we give somewhat more careful definitions.

An *elliptic (holomorphic) modular form* of *level one* and *weight* $2k$ is a *holomorphic* function f on the upper half-plane $\mathfrak{H}$ meeting the *automorphy condition*

$$f(\gamma z) \;=\; (cz+d)^{2k}\cdot f(z) \qquad \text{(for } z\in\mathfrak{H} \text{ and } \gamma = \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in SL_2(\mathbb{Z}))$$

with $\gamma z = \frac{az+b}{cz+d}$, and meeting the *growth condition* that it is *bounded* on the closure of the standard fundamental domain (see appendix)

$$F \;=\; \{z\in\mathfrak{H} \;:\; |z|>1,\; |\mathrm{Re}(z)| < \tfrac{1}{2}\}$$

The function

$$j \;:\; SL_2(\mathbb{Z}) \times \mathfrak{H} \longrightarrow \mathbb{C}^\times \qquad \text{by} \qquad j(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z) \longrightarrow cz+d$$

is the *cocycle*. When context makes the details clear, the modifier *elliptic* is often dropped. [8]

$$f|_{2k}\gamma \;=\; f(\gamma z)\cdot (cz+d)^{-2k} \qquad (\text{with } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix})$$

for arbitrary complex-valued functions f on $\mathfrak{H}$, allowing the automorphy condition to be rewritten as

$$f|_{2k}\gamma \;=\; f \qquad (\text{for all } \gamma \in SL_2(\mathbb{Z}))$$

[2.1] Note: The holomorphic modular forms of weight $2k$ for $SL_2(\mathbb{Z})$ form a complex vector space under value-wise *sums*. Also, the *product* of a weight $2k$ form and a weight $2k'$ form gives a weight $2k+2k'$ form.

[2.2] Remark: The modifier *elliptic modular* refers to the fact that the function is on $\mathfrak{H}$, as opposed to some other homogeneous space, and is *holomorphic*, as opposed to meeting some other local analytic condition. *Level one* refers to the automorphy requirement for all $\gamma \in SL_2(\mathbb{Z})$ rather than some smaller or different subgroup of $SL_2(\mathbb{R})$.

[2.3] Remark: Boundedness in the closure of the fundamental domain does *not* imply boundedness on $\mathfrak{H}$, because modular forms are not quite *invariant* under $SL_2(\mathbb{Z})$, but only almost invariant, with the cocycle making things more complicated.

[2.4] Fourier expansions The upper-triangular element $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$ sends $z \to z+1$, and $j(\gamma, z) = 1$, so a level-one modular form f has the property

$$f(z+1) \;=\; f(\gamma z) \;=\; j(\gamma,z)^{2k}\cdot f(z) \;=\; 1^{2k}\cdot f(z) \;=\; f(z)$$

That is, modular forms are *periodic* in $x = \mathrm{Re}(z)$, with period 1. Thus, as functions of z, modular forms have *Fourier expansions* in x, with coefficients depending on $y = \mathrm{Im}(z)$:

$$f(x+iy) \;=\; \sum_{n\in\mathbb{Z}} c_n(y)\, e^{2\pi i n x}$$

Since f is *holomorphic*, it satisfies the Cauchy-Riemann equation

$$\Big(\frac{\partial}{\partial x} + i\frac{\partial}{\partial y}\Big) f(x+iy) \;=\; 0$$

Differentiating term-wise,

$$0 \;=\; \sum_{n\in\mathbb{Z}} \Big(\frac{\partial}{\partial x} + i\frac{\partial}{\partial y}\Big)\Big(c_n(y) e^{2\pi i n x}\Big) \;=\; \sum_{n\in\mathbb{Z}} \Big(2\pi i n c_n(y) e^{2\pi i n x} + i c_n'(y) e^{2\pi i n x}\Big)$$

By uniqueness of Fourier expansions,

$$2\pi i n c_n(y) + i c_n'(y) \;=\; 0 \qquad (\text{for all } n \in \mathbb{Z})$$

---

[8] Traditional terminology is that $f \to f|_{2k}\gamma$ is the *slash* operator, although this name fails to suggest any meaning other than reference to the notation itself. In fact, obviously $f(z) \to f(\gamma z)(cz+d)^{-2k}$ is a *left translation* operator, albeit complicated by the automorphy factor. That is, this is a *right* action of $SL_2(\mathbb{Z})$ on functions on $\mathfrak{H}$, while the group action of $SL_2(\mathbb{Z})$ on $\mathfrak{H}$ is written on the *left*.

This is a linear, constant-coefficient differential equation for $c_n(y)$:

$$c_n'(y) + 2\pi n c_n(y) \;=\; 0$$

Thus,

$$c_n(y) \;=\; \text{constant} \times e^{-2\pi n y}$$

and the Fourier expansion of a (holomorphic) modular form is of the form

$$f(z) \;=\; \sum_{n\in\mathbb{Z}} c_n\, e^{2\pi i n z} \qquad\qquad (\text{constants } c_n \in \mathbb{C})$$

[2.5] Remark: Fourier expansions of modular forms are sometimes called *q-expansions*, with $q = e^{2\pi i z}$.

[2.6] Fourier expansions and growth condition

Use the standard notation

$$A_n \;\ll\; B_n$$

for the assertion that $|A_n| \le C \cdot B_n$ for some constant C.

[2.7] Proposition: A modular form $f(z) = \sum_{n\in\mathbb{Z}} c_n e^{2\pi i n z}$ has $c_n = 0$ for $n < 0$, and $|c_n| \ll e^{2\pi n}$ for $n \ge 0$, with implied constant depending on f.

Proof: Let $|f(z)| \le C$ for z in the fundamental domain. Then the usual expression for the n^{th} Fourier component gives

$$|c_n|e^{-2\pi n y} \;=\; \Big|\int_{-\frac{1}{2}}^{\frac{1}{2}} e^{-2\pi i n x} f(x+iy)\; dx\Big| \;\le\; \int_{-\frac{1}{2}}^{\frac{1}{2}} \Big|e^{-2\pi i n x} f(x+iy)\Big|\; dx \;\le\; \int_{-\frac{1}{2}}^{\frac{1}{2}} 1 \cdot C\; dx \;\le\; C$$

That is,

$$|c_n| \;\le\; e^{2\pi n y} \cdot C$$

As $y \to +\infty$ with $z \in F$, we find $c_n = 0$ for $n < 0$. For $n \ge 0$, taking $y = 1$ gives the estimate. ///

[2.8] Remark: The estimate $|c_n| \ll e^{2\pi n}$ is very bad, but useful in preliminaries.

[2.9] Cuspforms A modular form with 0^{th} Fourier coefficient 0 is a *cuspform*.

This innocent cuspform condition, beyond holomorphy, automorphy, and the growth condition, has important ramifications.

[2.10] Theorem: *(Hecke)* A weight $2k$ holomorphic cuspform f has *exponential decay*

$$|f(x+iy)| \;\ll_f\; e^{-2\pi y} \qquad\qquad (\text{as } y \to +\infty)$$

with implied constant depending on f. The Fourier coefficients c_n of f satisfy

$$|c_n| \;\ll\; n^k$$

Proof: Using the preliminary bound $|c_n| \ll e^{2\pi n y}$ from above,

$$|f(z)| \;\ll\; \sum_{n\ge 1} e^{2\pi n}\, e^{-2\pi n y} \;=\; \sum_{n\ge 1} e^{-2\pi n (y-1)} \;=\; \frac{e^{-2\pi(y-1)}}{1 - e^{-2\pi(y-1)}}$$

by summing the geometric series, giving the exponential decay. Since

$$|\mathrm{Im}(\begin{pmatrix} a & b \\ c & d \end{pmatrix} z)| \;=\; \frac{\mathrm{Im}(z)}{|cz+d|^2}$$

the function $y^k \cdot |f(z)|$ is $SL_2(\mathbb{Z})$-*invariant*, rather than merely satisfying the automorphy condition. Due to the exponential decay in the fundamental domain, $y^k \cdot |f(z)|$ is surely *bounded* in the fundamental domain. By $SL_2(\mathbb{Z})$-invariance, $y^k \cdot |f(z)|$ is *bounded* on $\mathfrak{H}$.

For any $y > 0$,

$$|c_n \cdot e^{-2\pi n y}| \;\le\; \int_{-\frac{1}{2}}^{\frac{1}{2}} \Big| e^{-2\pi i n x}\, f(x+iy)\Big|\, dx \;\ll_f\; y^{-k}$$

That is, $|c_n| \ll_f y^{-k} e^{2\pi n y}$. The bounding expression blows up as $y \to 0^+$ and as $y \to +\infty$, but we can find its minimum: solve

$$0 \;=\; \frac{\partial}{\partial y}\Big(y^{-k} e^{2\pi n y}\Big) \;=\; -k y^{-k-1} e^{2\pi n y} + 2\pi n y^{-k} e^{2\pi n y} \;=\; (-k + 2\pi n y) y^{-k-1} e^{2\pi n y}$$

The minimizing $y = k/2\pi n$ gives

$$|c_n| \;\ll\; \Big(\frac{k}{2\pi n}\Big)^{-k} e^{2\pi n \cdot \frac{k}{2\pi n}} \;=\; n^k \cdot \Big(\frac{2\pi e}{k}\Big)^k$$

giving the asserted bound. ///

[2.11] Remark: [Hecke 1937]'s bound given above was improved by [Rankin 1939] and [Selberg 1940]. [Ramanujan 1916]'s and [Petersson 1930]'s conjecture that $|c_p| \le 2p^{k-\frac{1}{2}}$ for prime p and weight $2k$ cuspforms, was proven by [Deligne 1974] as application of his completion of proof of the *Weil conjectures*.

---

3. *Fourier expansions of holomorphic Eisenstein series*

Our normalization of *(holomorphic) Eisenstein series* is

$$E_{2k}(z) \;=\; \tfrac{1}{2} \sum_{\text{coprime } c,d} \frac{1}{(cz+d)^{2k}}$$

Legitimate analogues of an integral test show that this is absolutely convergent, and uniformly so for z in compacts, for $2k \ge 4$. Thus, E_{2k} is holomorphic. [9]

As earlier, direct computation shows that

$$E_{2k}(\gamma z) \;=\; (cz+d)^{2k} E_{2k}(z) \qquad\qquad (\text{with } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix})$$

Namely, with $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$,

$$E_{2k}(\gamma z) \;=\; \tfrac{1}{2} \sum_{\text{coprime } C,D} \frac{1}{(C\frac{az+b}{cz+d} + D)^{2k}} \;=\; (cz+d)^{2k} \sum_{\text{coprime } C,D} \frac{1}{(C(az+b) + D(cz+d))^{2k}}$$

[9] An infinite sum $\sum_{n\ge 1} f_n$ of holomorphic functions, if uniformly absolutely convergent on compacts, is again holomorphic, by basic corollaries of Cauchy's theorems.

$$= \ (cz+d)^{2k} \sum_{\text{coprime } C,D} \frac{1}{((Ca+Dc)z+(Cb+Dd))^{2k}}$$

and

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ = \ \begin{pmatrix} * & * \\ Ca+Dc & Cb+Dd \end{pmatrix}$$

Thus, the map $(C,D) \to (Ca+Dc, Cb+Dd)$ is a bijection on the set of coprime integers, and we have $(cz+d)^{2k}E_{2k}(z)$. [10]

As noted earlier, the leading fraction and the coprimality condition are elementary shadows of a more meaningful expression,

$$E_{2k}(z) \ = \ \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} \frac{1}{(cz+d)^{2k}} \qquad\qquad (\text{with } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix})$$

where $\Gamma = SL_2(\mathbb{Z})$, $\Gamma_\infty = \{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \in \Gamma\}$. Indeed, for integers c,d to be the lower row of an element $\gamma \in \Gamma$, necessarily c,d are coprime. With even integer $2k$, changing c,d for $-c,-d$ does not change $(cz+d)^{2k}$. And, given $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\begin{pmatrix} a' & b' \\ c & d \end{pmatrix}$ in Γ,

$$\begin{pmatrix} a' & b' \\ c & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \ = \ \begin{pmatrix} a' & b' \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \ = \ \begin{pmatrix} * & * \\ cd-dc & * \end{pmatrix} \ = \ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \ \in \ \Gamma_\infty$$

proving the bijection.

So $E_{2k}(z)$ satisfies the automorphy condition.

Thus, $E_{2k}(z)$ meets the holomorphy condition and the automorphy condition. Demonstration that it is bounded in the closure of the standard fundamental domain would complete proof that it is an elliptic modular form.

[3.1] Theorem: For weight $2k \geq 4$, the holomorphic Eisenstein series

$$E_{2k}(z) \ = \ \sum_{\text{coprime } c,d} \frac{1}{(cz+d)^{2k}}$$

has Fourier expansion

$$E_{2k}(z) \quad = \quad 1 \ + \ \frac{(-2\pi i)^{2k}}{(2k-1)!\,\zeta(2k)} \sum_{n\geq 1} \sigma_{2k-1}(n)\, e^{2\pi i n z}$$

where $\sigma_{2k-1}(n)$ is the sum of the $(2k-1)^{th}$ powers of the positive divisors of the integer n.

Before the important computation that determines the Fourier coefficients, two corollaries:

[3.2] Corollary: Given a modular form $f(z) = c_o + \sum_{n\geq 1} c_n\, e^{2\pi i n z}$, the difference $f - c_o \cdot E_{2k}$ is a *cuspform.*

---

[10] The same computation demonstrates the *cocycle relation* $j(gh,z) = j(g,hz)j(h,z)$ for $g,h \in SL_2(\mathbb{R})$ and $z \in \mathfrak{H}$. This certifies that the action $f \to f|_{2k}\gamma$ has the *associativity*

$$(f|_{2k}\gamma)|_{2k}\delta \ = \ f|_{2k}(\gamma\delta)$$

necessary for this to be a legitimate *right* action.

Proof: The leading Fourier coefficient of the Eisenstein series is 1, so the indicated subtraction exactly annihilates the leading Fourier coefficient. ///

[3.3] **Corollary:** For weight $2k \geq 4$, the holomorphic Eisenstein series $E_{2k}(z)$ is *bounded* in the standard fundamental domain, so is a elliptic modular form in the strongest sense.

Proof: The absence of negative-index Fourier terms, and an easy estimate

$$\sigma_{2k-1}(n) \;\leq\; \sum_{1\leq \ell\leq n} \ell^{2k-1} \;\leq\; (n+1)^{2k} \;\ll\; e^{2\pi n} \qquad\qquad (\text{as } n\to +\infty)$$

give

$$|E_{2k}(z) \;\ll\; 1+\sum_{n\geq 1} e^{2\pi n}\, e^{-2\pi n y} \;\leq\; 1+\frac{e^{-2\pi y}}{1-e^{-2\pi y}}$$

which is bounded for $y \geq \frac{\sqrt{3}}{2}$. ///

Proof: We directly compute the Fourier coefficients

$$c_n \;=\; e^{2\pi n y}\cdot \int_{-\frac{1}{2}}^{\frac{1}{2}} e^{-2\pi i n x}\; E^*_{2k}(x+iy)\; dx$$

of the renormalized Eisenstein series

$$E^*_{2k}(z) \;=\; \zeta(2k)\cdot E_{2k}(z) \;=\; \sum_{(c,d)\neq(0,0)} \frac{1}{(cz+d)^{2k}}$$

First, the subsum over $d \neq 0$ with $c = 0$ is literally $2\zeta(2k)$, and this is translation-invariant, so is part of the 0^{th} Fourier coefficient 0

Each subsum over $d\in\mathbb{Z}$ for fixed $c\neq 0$ is invariant under $z\to z+1$, so has a Fourier expansion, with n^{th} coefficient

$$e^{2\pi n y}\cdot \int_{-\frac{1}{2}}^{\frac{1}{2}} e^{-2\pi i n x}\; \sum_d \frac{1}{(cz+d)^{2k}}\; dx$$

The integral is

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} e^{-2\pi i n x}\; \sum_d \frac{1}{(cx+d+ciy)^{2k}}\; dx \;=\; c^{-2k}\int_{-\frac{1}{2}}^{\frac{1}{2}} e^{-2\pi i n x}\; \sum_d \frac{1}{(x+\frac{d}{c}+iy)^{2k}}\; dx$$

Aiming to *unwind* the sum-and-integral to have a simpler sum and an integral over $\mathbb{R}$, rewrite

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} e^{-2\pi i n x}\; \sum_d \frac{1}{(x+\frac{d}{c}+iy)^{2k}}\; dx \;=\; \int_{-\frac{1}{2}}^{\frac{1}{2}} e^{-2\pi i n x} \sum_{\ell\in\mathbb{Z}}\sum_{d \bmod c} \frac{1}{(x+\ell+\frac{d}{c}+iy)^{2k}}\; dx$$

and replace x by $x-\ell$, to obtain

$$\sum_{\ell\in\mathbb{Z}}\int_{-\frac{1}{2}+\ell}^{\frac{1}{2}+\ell} e^{-2\pi i n x}\; \sum_{d \bmod c} \frac{1}{(x+\frac{d}{c}+iy)^{2k}}\; dx \;=\; \int_{\mathbb{R}} e^{-2\pi i n x}\; \sum_{d \bmod c} \frac{1}{(x+\frac{d}{c}+iy)^{2k}}\; dx$$

$$=\; \sum_{d \bmod c} \int_{\mathbb{R}} e^{-2\pi i n x} \frac{1}{(x+\frac{d}{c}+iy)^{2k}}\; dx \;=\; \sum_{d \bmod c} e^{2\pi i n d/c} \int_{\mathbb{R}} e^{-2\pi i n x} \frac{1}{(x+iy)^{2k}}\; dx$$

by replacing x by $x - \frac{d}{c}$ in each integral. Now neither c nor d appears inside the integral, while neither x nor y appear in the sum.

The integral can be evaluated by residues, treating x itself as a complex variable, as follows. Fix y, the imaginary part of the original z. For $n \le 0$, the function $e^{2\pi i n x}$ is rapidly decreasing as x moves into the upper half-plane, so the indicated integral is the limit as $R \to +\infty$ of an integral left-to-right along $[-R, R]$ and then along an arc of a circle of radius R in the upper half-plane. This picks up residues of $x \to e^{-2\pi i n x}/(x+iy)^{2k}$ in the upper half-plane: there are none, so these Fourier coefficients are 0.

For $n > 0$, the integral can be evaluated by residues, using an arc of a circle in the *lower* half-plane, picking up $-2\pi i$ times the residue of $x \to e^{-2\pi i n x}/(x+iy)^{2k}$ at $-iy$, namely,

$$\frac{-2\pi i}{(2k-1)!} \cdot \Big(\frac{\partial}{\partial x}\Big)^{2k-1} e^{-2\pi i n x}\Big|_{x=-iy} \;=\; \frac{-2\pi i}{(2k-1)!} \cdot (-2\pi i n)^{2k-1} \cdot e^{-2\pi n y} \;=\; \frac{(2\pi i)^{2k}}{(2k-1)!}\, n^{2k-1}\, e^{-2\pi n y}$$

That is,

$$\int_{\mathbb{R}} e^{-2\pi i n x} \frac{1}{(x+iy)^{2k}}\, dx \;=\; \begin{cases} \dfrac{(2\pi i)^{2k}}{(2k-1)!}\, n^{2k-1}\, e^{-2\pi n y} & (\text{for } n \ge 1) \\[2ex] 0 & (\text{for } n \le 0) \end{cases}$$

The sum over $d \bmod c$ is a sum of the *character* $d \to e^{2\pi i n d/c}$ over the finite abelian group $\mathbb{Z}/c$. The *cancellation lemma* says this sum is 0 unless the character is *trivial*, in which case it is the cardinality of the group, namely, $|c|$. The character is trivial if and only $c|n$. Thus,

$$\sum_{d \bmod c} e^{2\pi i n d/c} \;=\; \begin{cases} |c| & (\text{for } c|n) \\[1ex] 0 & (\text{otherwise}) \end{cases}$$

In summary, the 0^{th} Fourier coefficient is $2\zeta(2k)$, the negative-index Fourier coefficients are 0, and for $n > 1$ the Fourier coefficient is

$$\sum_{c|n} \frac{1}{c^{2k}} \cdot |c| \;\times\; \frac{(2\pi i)^{2k}}{(2k-1)!}\, n^{2k-1} \qquad\qquad (\text{for } n > 1)$$

As c runs over positive and negative divisors of n, so does n/c, and the last expression can be simplified somewhat by doing so:

$$\sum_{c|n} \frac{c^{2k}}{n^{2k}} \Big|\frac{n}{c}\Big| \times \frac{(2\pi i)^{2k}}{(2k-1)!}\, n^{2k-1} \;=\; \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{0<c|n} c^{2k-1}$$

Often the sum of ℓ^{th} powers of positive divisors of an integer n is denoted $\sigma_\ell(n)$, so the Fourier expansion of the Eisenstein series can be written

$$2\zeta(2k) \cdot E_{2k}(z) \;=\; 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{n \ge 1} \sigma_{2k-1}(n)\, e^{2\pi i n z}$$

and

$$E_{2k}(z) \;=\; 1 \;+\; \frac{(2\pi i)^{2k}}{(2k-1)!\,\zeta(2k)} \sum_{n \ge 1} \sigma_{2k-1}(n)\, e^{2\pi i n z}$$

as claimed. ///

4. *Divisor/dimension formula, applications*

A useful relation on the *orders of vanishing* of an elliptic modular form f of weight $2k$ for $SL_2(\mathbb{Z})$ is produced via the *argument principle*, by path-integration of $f'(z)/f(z)$ around the boundary of a height-T truncation

$$F_T \;=\; \{|z|\ge 1,\ |\mathrm{Re}(z)|\le \tfrac{1}{2},\ \mathrm{Im}(z)\le T\}$$

of the standard fundamental domain F.

The *divisor* of a function is the set of it zeros, counting order-of-vanishing, that is, counting multiplicities. [11] Less usually, the *order of vanishing* at $i\infty$, $\nu_f(i\infty)$, of $f(z)=\sum_n c_n e^{2\pi i n z}$ is the smallest n_o such that $c_n=0$ for $n<n_o$. Still, this is consistent with the usual notion by viewing the Fourier expansion as a power series in $q=e^{2\pi i z}$.

[4.1] Theorem: Let $\nu_f(z)$ be the order of vanishing of not-identically-zero f at $z\in\mathfrak{H}$. Including only an *irredundant* collection of representatives for $SL_2(\mathbb{Z})\backslash\mathfrak{H}$,

$$\frac{\nu_f(i)}{2} \;+\; \frac{\nu_f(\rho)}{3} \;+\; \nu_f(i\infty) \;+\; \sum_{\text{other } z} \nu_f(z) \;=\; \frac{2k}{12}$$

where ρ is a cube root of unity in $\mathfrak{H}$ and f is weight $2k$. *(Proof in following section.)*

This divisor relation yields important corollaries.

[4.2] The first cuspform A small further preparation: Ramanujan's $\Delta(z)$-function is a non-zero constant multiple of $E_4^3-E_6^2$, which the proof of the following shows to be not identically zero. The choice of the multiplying constant is usually to make $\Delta(z)$ have Fourier expansion (with vanishing 0^{th} Fourier coefficient, and) 1^{st} Fourier coefficient 1:

$$\Delta(z) \;=\; 1\cdot e^{2\pi i z} + \sum_{n\ge 2} \tau(n)\, e^{2\pi i n z}$$

The higher Fourier coefficients are sometimes denoted $\tau(n)$ for reasons of tradition. When we compute the Fourier coefficients of E_{2k}, we will see that they are of the form

$$E_{2k}(z) \;=\; 1\cdot e^{2\pi i\cdot 0\cdot z} + \sum_{n\ge 1} c_n\, e^{2\pi i n z}$$

Granting this, since there are no negative-index Fourier components,

$$E_4(z)^3 - E_6(z)^2 \;=\; (1+\text{higher})^3 - (1+\text{higher})^2 \;=\; (1+\text{higher}) - (1+\text{higher})$$

$$=\; \text{vanishing } 0^{th} \text{ Fourier component} + \text{higher Fourier components}$$

Thus, granting this feature of the Fourier expension of Eisenstein series, the constant multiple $\Delta(z)$ of $E_4(z)^3-E_6(z)^2$ is indeed a *cuspform.*

[11] As usual in complex analysis, at a point $z_o\in\mathfrak{H}$, the *order of vanishing* $\nu_f(z_o)$ of a holomorphic function f is the smallest n_o so that the n_o^{th} power series coefficient of f at z_o is non-zero. That is, with

$$f(z) \;=\; \sum_{n=0}^{\infty} c_n\,(z-z_o)^n$$

the *order* (of vanishing) of f at z_o is the smallest n_o such that $c_{n_o}\ne 0$.

[4.3] Corollary: The spaces M_{2k} of modular forms of weight $2k$ for $SL_2(\mathbb{Z})$ are $\{0\}$ for $2k < 0$ or $2k$ an *odd* integer. In small non-negative weights: $M_0 = \mathbb{C}$ and $M_2 = \{0\}$, while for even integer weights $2k \geq 4$,

$$M_{2k} \;=\; \mathbb{C} \cdot E_{2k} \;\oplus\; \Delta \cdot M_{2k-12}$$

That is, for weights up through 22,

$$\begin{cases} M_0 &=& \mathbb{C} \\ M_2 &=& \{0\} \\ M_4 &=& \mathbb{C}\cdot E_4 \\ M_6 &=& \mathbb{C}\cdot E_6 \\ M_8 &=& \mathbb{C}\cdot E_8 \\ M_{10} &=& \mathbb{C}\cdot E_{10} \\ M_{12} &=& \mathbb{C}\cdot E_{12} \;\oplus\; \mathbb{C}\cdot\Delta \\ M_{14} &=& \mathbb{C}\cdot E_{14} \\ M_{16} &=& \mathbb{C}\cdot E_{16} \;\oplus\; \mathbb{C}\cdot\Delta E_4 \\ M_{18} &=& \mathbb{C}\cdot E_{18} \;\oplus\; \mathbb{C}\cdot\Delta E_6 \\ M_{20} &=& \mathbb{C}\cdot E_{20} \;\oplus\; \mathbb{C}\cdot\Delta E_8 \\ M_{22} &=& \mathbb{C}\cdot E_{22} \;\oplus\; \mathbb{C}\cdot\Delta E_{10} \end{cases}$$

Proof: For *odd* integers $2k$ (momentarily resisting the suggestion of the notation that it's an even integer), and $f \in M_{2k}$,

$$f(z) \;=\; f(\frac{-z+0}{0\cdot z - 1}) \;=\; f(\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} z) \;=\; (0\cdot z - 1)^{2k}\cdot f(z) \;=\; (-1)\cdot f(z)$$

so $f(z) = 0$.

For even integer $2k$, the point is that, for small non-negative even integers $2k$, it is not easy to meet the condition

$$\frac{n_i}{2} + \frac{n_\rho}{3} + n_{i\infty} + \sum_{\text{other } z} n_z \;=\; \frac{2k}{12}$$

with non-negative integers n_*.

To begin the more serious discussion, for $2k = 0$, all orders of vanishing must be 0, since they are non-negative integers. *Constants* are obviously in M_0. The trick is that, for a holomorphic modular form f of weight 0, $f(z) - f(z_o)$ vanishes at z_o for every $z_o \in \mathfrak{H}$. Thus, $f(z)$ is identically equal to $f(z_o)$, that is, is constant.

For $2k = 2$, there is *no* collection of orders of vanishing combining to give the required $2k/12 = 1/6$, so $M_2 = \{0\}$.

For $2k = 4$, on one hand, the only way to get $4/12 = 1/3$ is

$$\underbrace{\frac{0}{2}}_{\text{at } i} + \underbrace{\frac{1}{3}}_{\text{at } \rho} + \underbrace{0}_{\text{at } i\infty} + \sum_{\text{other } z} 0 \;=\; \frac{4}{12}$$

On the other hand, we are granting ourselves that the holomorphic Eisenstein series E_4 is in M_4, so evidently $E_4(\rho) = 0$, and the vanishing is just first-order. Given $f \in M_4$, take $z_o \in \mathfrak{H}$ not in the Γ-orbit of ρ, and consider

$$f_2 \;=\; f \;-\; \frac{f(z_o)}{E_4(z_o)} \cdot E_4$$

By design, f_2 vanishes at z_o:

$$f_2(z_o) \;=\; f(z_o) - \frac{f(z_o)}{E_4(z_o)} \cdot E_4(z_o) \;=\; 0$$

Such vanishing can occur only for f_2 identically zero, so f is a constant multiple of E_4.

Similarly, for $2k = 6, 8, 10$, there is only one way to satisfy the divisor relation:

$$\begin{cases} \underbrace{\frac{1}{2}}_{\text{at } i} + \underbrace{\frac{0}{3}}_{\text{at } \rho} + \underbrace{0}_{\text{at } i\infty} + \sum_{\text{other } z} 0 \;=\; \frac{6}{12} \\ \\ \underbrace{\frac{0}{2}}_{\text{at } i} + \underbrace{\frac{2}{3}}_{\text{at } \rho} + \underbrace{0}_{\text{at } i\infty} + \sum_{\text{other } z} 0 \;=\; \frac{8}{12} \\ \\ \underbrace{\frac{1}{2}}_{\text{at } i} + \underbrace{\frac{2}{3}}_{\text{at } \rho} + \underbrace{0}_{\text{at } i\infty} + \sum_{\text{other } z} 0 \;=\; \frac{10}{12} \end{cases}$$

and $E_{2k} \in M_{2k}$. The same argument as for M_4 shows that every element of M_6, M_8, M_{10} is a constant multiple of E_6, E_8, E_{10}.

Things change at M_{12}, since $12/12 = 1$: there is no numerical obstacle to vanishing at $i\infty$ and other points, in addition to the special points i and ρ. Still, E_{12} is present, and we are granting in advance that its Fourier expansion is of the form

$$E_{12}(z) \;=\; 1 \cdot e^{2\pi i \cdot 0 \cdot z} + \sum_{n \ge 1} a_n \, e^{2\pi i n z}$$

Given $f \in M_{12}$ with Fourier expansion

$$f(z) \;=\; \sum_{n \ge 0} b_n \, e^{2\pi i n z}$$

substract a multiple of E_{12} to make the 0^{th} Fourier coefficient 0: consider

$$f_2(z) \;=\; f(z) - b_0 \cdot E_{12}$$

Thus, $\nu_{f_2}(i\infty) = 1$, and f_2 is a *cuspform*, by definition. The divisor relation shows that f_2 has no *other* zeros, *unless* by mischance f_2 is identically 0.

To prove *existence* of a not-identically-zero cuspform of weight 12, note that $E_4^3 - E_6^2$ is weight 12, and has 0^{th} Fourier coefficient 0, so is a candidate. To show that $E_4^3 - E_6^2$ is not identically 0, recall from above that $E_4(\rho) = 0$ and does not vanish otherwise, while $E_6(i) = 0$ and does not vanish otherwise. Thus, $E_4^3 - E_6^2$ cannot vanish at either ρ or i, so is not identically 0. Up to normalizing constant, $\Delta = E_4^3 - E_6^2$.

By the divisor relation, Δ *only* vanishes at $i\infty$, and there to order 1. Now we will see that $M_{12} = \mathbb{C}E_{12} + \mathbb{C}\Delta$. Given $f \in M_{12}$, as before, subtract a multiple E_{12} to make the 0^{th} Fourier coefficient of $f_2 = f - cE_{12}$ be 0. Then *divide* f_2 by Δ, taking advantage of the fact that Δ does not vanish in $\mathfrak{H}$, and vanishes only to first order at $i\infty$. Thus, f_2/Δ is in $M_0 = \mathbb{C}$, proving that f_2 is a multiple of Δ, and $M_{12} = \mathbb{C}E_{12} + \mathbb{C}\Delta$.

Similarly, now that the non-zero cuspform Δ is identified, a similar argument gives the structure of M_{2k}, for $2k \ge 4$ so that Eisenstein series converge. Namely, given $f \in M_{2k}$, subtract a multiple of E_{2k} to obtain a cuspform of weight $2k$, and then divide by Δ to obtain a modular form of weight $2k - 12$. This shows that $M_{2k} = \mathbb{C}E_{2k} + \Delta M_{2k-12}$, as claimed. ///

For present purposes, an *isobaric* polynomial $P(X,Y) \in \mathbb{C}[X,Y]$ (with weights 4, 6) is a polynomial with the property that there is an integer $2k$ such that every monomial $X^a Y^b$ appearing has the property that $4a + 6b = 2k$. This has the effect that $P(E_4, E_6)$ is a modular form of weight 12.

[4.4] Corollary: Every holomorphic modular form for $SL_2(\mathbb{Z})$ is an isobaric polynomial in E_4, E_6.

Proof: The assertion is vacuously true for weight 0 since holomorphic modular forms of weight 0 are constants. Holomorphic modular forms of weight 2 are all identically 0. At weights 4 and 6, all modular forms are *multiples* of the respective Eisenstein series.

At weight 8, the only modular form is E_8, but also E_4^2 has weight 8. Both have 0^{th} Fourier coefficient 1, so $E_8 = E_4^2$. Similarly, $E_{10} = E_4 \cdot E_6$.

We already showed that Δ is a constant multiple of the isobaric polynomial $E_4^3 - E_6^2$. Since $E_{12} - E_4^3$ is a cuspform of weight 12, it is a multiple of Δ, proving that E_{12} has an isobaric polynomial expression in terms of E_4 and E_6.

Given $12 < 2k \in 2\mathbb{Z}$, find non-negative integers a, b such that $4a + 6b = 2k$. Then $E_{2k} - E_4^a E_6^b$ is a cuspform, and

$$\frac{E_{2k} - E_4^a E_6^b}{\Delta} \in M_{2k-12}$$

By induction, E_{2k} is an isobaric polynomial in E_4, E_6. Given $f \in M_{2k}$, subtract a multiple of E_{2k} to produce a cuspform f_2, allowing division by Δ to put f_2/Δ in M_{2k-12}, completing the induction. ///

[4.5] Corollary: For every weight $2k$, the space of holomorphic cuspforms is finite-dimensional.

Proof: The space of cuspforms of weight $2k$ is $\Delta \cdot M_{2k-12}$, and M_{2k-12} is cuspforms together with multiples of E_{2k-12}, for $2k - 12 \geq 4$. ///

[4.6] Remark: [Ramanujan 1916] conjectured that the n^{th} Fourier coefficient $\tau(n)$ of Δ satisfies

$$|\tau(p)| \leq 2p^{\frac{11}{2}} \qquad \text{(for prime } p\text{)}$$

and

$$\tau(mn) = \tau(m) \cdot \tau(n) \qquad \text{(for coprime } m, n\text{)}$$

and

$$\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1}) \qquad \text{(for prime } p\text{)}$$

[Mordell 1917] prove the latter two properties, using operators systematically investigated in [Hecke 1937], nowadays called *Hecke operators*. As noted earlier, [Deligne 1974] proved $|c_p| \leq 2p^{k-\frac{1}{2}}$ for prime p and weight $2k$ cuspforms, as consequence of his completion of proof of the *Weil conjectures*.

[4.7] Remark: In this context, *the modular function* or *modular invariant* $j(z)$ is defined to be a constant multiple of E_4^3/Δ, since now we know that $\Delta \neq 0$ in $\mathfrak{H}$, and that Δ has a simple pole at $i\infty$ and vanishes at ρ since $E_4(\rho) = 0$.

[4.8] Remark: Yes, there is some conflict with the notation that j can refer to the *cocycle*, as well as to the modular function, but context usually clarifies.

5. *Relations among Eisenstein series*

The divisor/dimension formula entails some relations among Eisenstein series, which entail relations among sum-of-divisors functions.

[5.1] Corollary: $E_4^2 = E_8$, $E_4 E_6 = E_{10}$, and $E_4 E_{10} = E_6 E_8 = E_{14}$.

Proof: In dimensions $8, 10, 14$ there are no holomorphic modular forms other than the corresponding Eisenstein series, and the leading Fourier coefficients are always 1. ///

[5.2] Corollary: Granting that $\zeta(2k)$ is a rational multiple of π^{2k}, the Fourier coefficients of Eisenstein series are *rational numbers*. ///

[5.3] Remark: The rationality of the Fourier coefficients of holomorphic Eisenstein series is significant in later developments. The following corollaries are slightly frivolous examples of proving number-theoretic identities by relations among automorphic forms. Nevertheless, more serious results do use the same proof mechanism of which these simple examples are prototypes.

[5.4] Corollary: For positive integers N,

$$\sigma_7(N) \;=\; 2\cdot \frac{7!\,\zeta(8)}{3!\,(2\pi i)^4\,\zeta(4)}\sigma_3(N) + \frac{7!\,\zeta(8)}{(3!)^2\,\zeta(4)^2}\sum_{m+n=N}\sigma_3(m)\,\sigma_3(n) \qquad (\text{with } m,n\ge 1)$$

$$\sigma_9(N) \;=\; \frac{9!\,\zeta(10)}{3!\,(2\pi i)^6\,\zeta(4)}\sigma_3(N) + \frac{9!\,\zeta(10)}{5!\,(2\pi i)^4\,\zeta(6)}\sigma_5(N) + \frac{9!\,\zeta(10)}{3!\,5!\,\zeta(4)\,\zeta(6)}\sum_{m+n=N}\sigma_3(m)\,\sigma_5(n) \qquad (m,n\ge 1)$$

Proof: The first identity comes from equating the Fourier coefficients of $E_4^2 = E_8$. A similar one arises from $E_4 E_6 = E_{10}$. Fourier expansions without negative-index terms multiply as

$$\sum_{m\ge 0} a_m\, e^{2\pi i m z}\;\cdot \sum_{n\ge 0} b_m\, e^{2\pi i n z} \;=\; \sum_{N\ge 0}\Big(\sum_{m+n=N} a_m\cdot b_n\Big)e^{2\pi i N z}$$

From $E_4^2 = E_8$, noting that the 0^{th} Fourier coefficients do not quite fit into the general pattern, for $N\ge 1$, equating the N^{th} coefficients of E_4^2 and E_8 gives

$$\frac{(2\pi i)^8}{7!\,\zeta(8)}\sigma_7(N) \;=\; 2\cdot\frac{(2\pi i)^4}{3!\,\zeta(4)}\sigma_3(N) \;+\; \Big(\frac{(2\pi i)^4}{3!\,\zeta(4)}\Big)^2\sum_{m+n=N}\sigma_3(m)\,\sigma_3(n)$$

Rearranging,

$$\sigma_7(N) \;=\; 2\cdot \frac{7!\,\zeta(8)}{3!\,(2\pi i)^4\,\zeta(4)}\sigma_3(N) + \frac{7!\,\zeta(8)}{(3!)^2\,\zeta(4)^2}\sum_{m+n=N}\sigma_3(m)\,\sigma_3(n)$$

The second computation is entirely analogous. ///

[5.5] Remark: Also, these frivolous relations completely determine $\zeta(4)$, $\zeta(6)$, $\zeta(8)$, and $\zeta(10)$, by looking at the relations for $N = 1, 2$. And since there are no cuspforms of weight 14, also $\zeta(14)$ is determined.

More generally, from [Gunning 1959/62] p. 55, Ramanujan proved the following, but with a worse error term, since Hecke's estimate on Fourier coefficients of cuspforms was not available. That is, in general, $E_{2k}\cdot E_{2\ell}$ is probably not exactly $E_{2k+2\ell}$, but it misses only by a cuspform:

[5.6] Corollary: For $2k \ge 4$ and $2\ell \ge 4$ and $N \ge 1$,

$$\sigma_{2k+2\ell-1}(N) \;=\; \frac{(2k+2\ell-1)!\,\zeta(2k+2\ell)}{(2\pi i)^{2\ell}\,(2k-1)!\,\zeta(2k-1)}\,\sigma_{2k-1}(N) + \frac{(2k+2\ell-1)!\,\zeta(2k+2\ell)}{(2\pi i)^{2k}\,(2\ell-1)!\,\zeta(2\ell)}\,\sigma_{2\ell-1}(N)$$

$$+\;\frac{(2k+2\ell-1)!\,\zeta(2k+2\ell)}{(2k-1)!\,(2\ell-1)!\,\zeta(2k)\,\zeta(2\ell)} \sum_{m+n=N} \sigma_{2k-1}(m)\cdot\sigma_{2\ell-1}(m) \;+\; O(n^{\frac{2k+2\ell}{2}}) \qquad \text{(with } m,n \ge 1)$$

Proof: Up to a cuspform, $E_{2k}\cdot E_{2\ell} = E_{2k+2\ell}$. Equating the N^{th} Fourier coefficients and multiplying through by $(2k+2\ell-1)!\,\zeta(2k+2\ell)/(2\pi i)^{2k+2\ell}$ gives the identity, with the big-O term arising from Hecke's estimate on the Fourier coefficients of the cuspform $= E_{2k+2\ell} - E_{2k}\cdot E_{2\ell}$. ///

[5.7] Remark: For weights $2k+2\ell$ among $8, 10, 14$, the divisor/dimension formula shows that there are no cuspforms, and the error term is exactly 0.

---

6. *Proof of divisor/dimension formula*

This proof of

$$\frac{n_i}{2} + \frac{n_\rho}{3} + n_{i\infty} + \sum_{\text{other } z} n_z \;=\; \frac{2k}{12}$$

is an application of the *argument principle*, exploiting the near-invariance of modular forms.

Proof: Let f be a not-identically-zero holomorphic modular form of weight $2k$. Let

$$F_T \;=\; \{|z| \ge 1,\ |\mathrm{Re}(z)| \le \tfrac{1}{2},\ \mathrm{Im}(z) \le T\}$$

be the truncation at height T of the standard fundamental domain F, and γ a path tracing its boundary.

On one hand, by the argument principle,

$$\int_\gamma \frac{f'(z)}{f(z)}\,dz \;=\; 2\pi i \sum_{z \text{ inside } F_T} \nu_f(z)$$

In fact, points on the boundary itself require special treatment, especially the points i and ρ. Treatment of this is postponed to the end of the proof.

On the other hand, the individual pieces of the path integral nearly cancel each other out, except for some manageable pieces, as follows.

The easiest part is that the integrals along the *upward* path along $\mathrm{Re}(z) = +\frac{1}{2}$ and *downward* path along $\mathrm{Re}(z) = -\frac{1}{2}$ *cancel* each other, because $f(z+1) = f(z)$.

Let $f(z) = \sum_{n\ge n_o} c_n\,e^{2\pi i n z}$, with $c_{n_o} \ne 0$. That is, $\nu_{i\infty}(f) = n_o$. The path-integral along the top of ∂F_T, from $\frac{1}{2} + iT$ to $-\frac{1}{2} + iT$ is an integral in the coordinate $q = e^{2\pi i n z}$ around a circle: letting $g(q) = f(z)$,

$$\int_{\frac{1}{2}}^{-\frac{1}{2}} \frac{f'(x+iT)}{f(x+iT)}\,dx \;=\; \int_{\frac{1}{2}+iT}^{-\frac{1}{2}+iT} \frac{g'(q)\cdot\frac{dq}{dz}}{g(q)}\,dz \;=\; \int_C \frac{g'(q)}{g(q)}\,dq$$

with C a circle of radius $e^{-2\pi T}$ at 0, traced *clockwise*. *The Fourier expansion of f in z is a power series expansion in q*, so by the *argument principle*, and by the convention about $\nu_f(i\infty)$,

$$\int_{\frac{1}{2}}^{-\frac{1}{2}} \frac{f'(x+iT)}{f(x+iT)}\,dx \;=\; -2\pi i\cdot\nu_f(i\infty) - 2\pi i \sum_{z:\mathrm{Im}\,(z)>T} \nu_f(z)$$

The path from the cube-root of unity ρ to i is mapped by $z \to -1/z$ to that running backward from the sixth root of unity to i, but these do not quite cancel each other, because f is not *invariant* under $z \to -1/z$. Rather, differentiating $f(-1/z) = z^{2k} \cdot f(z)$ gives

$$f'(-1/z) \cdot \frac{1}{z^2} \;=\; 2kz^{2k-1}f(z) + z^{2k}f'(z)$$

so

$$f'(-1/z) \;=\; 2kz^{2k+1}f(z) + z^{2k+2}f'(z)$$

and

$$\frac{f'(-1/z)}{f(-1/z)}d(-1/z) \;=\; \frac{2kz^{2k+1}f(z) + z^{2k+2}f'(z)}{z^{2k}f(z)}\frac{dz}{z^2} \;=\; \frac{2k}{z} + \frac{f'(z)}{f(z)}$$

Thus, the integral from the cube root of 1 to the sixth root of 1 cancel *except* for the $-2k/z$. Letting $z = e^{it}$ as t goes from $\frac{2}{3}\pi$ to $\frac{1}{2}\pi$,

$$\int_{\frac{2}{3}\pi}^{\frac{1}{2}\pi} \Big(\frac{f'(z)}{f(z)}\,dz \;-\; \frac{f'(-1/z)}{f(-1/z)}\Big)\,d(-1/z) \;=\; \int_{\frac{2}{3}\pi}^{\frac{1}{2}\pi} \frac{-2k}{e^{-it}}\,d(e^{it}) \;=\; \int_{\frac{2}{3}\pi}^{\frac{1}{2}\pi} -2ik\;dt \;=\; 2ik\cdot\frac{\pi}{6} \;=\; 2\pi i\cdot\frac{2k}{12}$$

Thus, *if there were no vanishing on the boundary*, evaluating the integral around the truncated fundamental domain in two ways gives

$$\sum_{z\;\mathrm{Im}\,(z)<T} \nu_f(z) \;\;=\;\; -\nu_f(i\infty) - \sum_{z:\mathrm{Im}\,(z)>T} \nu_f(z) \;+\; \frac{2k}{12}$$

or

$$\nu_f(i\infty) + \sum_{z\in F} \nu_f(z) \;\;=\;\; \frac{2k}{12}$$

Now we consider points on the boundary of F_T. Any vanishing on the top edge $\mathrm{Im}\,(z) = T$ can be avoided by adjusting T slightly. Any vanishing on the vertical edges $\mathrm{Re}\,(z) = \pm\frac{1}{2}$ can be easily accommodated by slightly deforming the contour γ *inward* on the *left* side $\mathrm{Re}\,(z) = -\frac{1}{2}$ to *exclude* a point z_o with $f(z_o) = 0$, and deforming the contour slightly *outward* on the right side $\mathrm{Re}\,(z) = \frac{1}{2}$ to *include* $z_o + 1$. Similarly, for any point on the bottom part of the boundary, except for i and ρ, at which f vanishes, the left half of that arc can be deformed slightly inward, and the right half outward, to avoid the points. [12] Thus, the ordinary argument principle is sufficient for these cases.

[6.1] Points i, ρ on the boundary

Unfortunately, there is no deformation of the contour to avoid the points i, ρ while counting order-of-vanishing. We first consider the situation at i.

To simplify the discussion, use the *Cayley map* $z \to \frac{z-i}{-iz+1}$ to convert the arc along $|z| = 1$ to a straight line segment σ along the real axis, and replace f by its composition g with the inverse $z \to \frac{z+i}{iz+1}$ to the Cayley map. This does not alter order-of-vanishing. In these coordinates modify σ traversing the interval $[-a, a]$ left-to-right to include a small semi-circular detour along $|z| = \varepsilon$ in the upper half-plane. That is, the modified path σ_ε goes along the interval $[-a, -\varepsilon]$ left-to-right, along the arc clockwise from $-\varepsilon$ to $+\varepsilon$, and left-to-right along the interval $[\varepsilon, a]$.

[12] One might reasonably worry that there might be infinitely-many points near F_T where f vanishes. However, the *compactness* of any slightly larger region containing F_T, and the holomorphy of f, assures that this cannot happen.

For $g(0) = 0$, the logarithmic derivative g'/g has a simple pole at 0, with Laurent expansion

$$\frac{g'(z)}{g(z)} \;=\; \frac{\nu_0(g)}{z} + (\text{holomorphic near } 0)$$

By continuity, the limit as $\varepsilon \to 0^+$ of the integral of a holomorphic function along the modified paths σ_ε is just the integral along the segment σ. This leaves us explicit computation of

$$\int_{\sigma_\varepsilon} \frac{dz}{z} \;=\; \int_{-a}^{-\varepsilon} \frac{dt}{t} + \int_{-\pi}^{0} \frac{d(\varepsilon e^{it})}{e^{it}} \int_{\varepsilon}^{a} \frac{dt}{t} \;=\; -(\log a - \log \varepsilon) - \pi i + (\log a - \log \varepsilon) \;=\; -\pi i$$

That is, the limit of the integrals over paths σ_ε *excluding* 0 produces $\frac{1}{2} \cdot 2\pi i \cdot \nu_g(0)$. Thus, the corresponding modification of the path around the boundary of F_T gives $-\frac{1}{2} \cdot 2\pi i \cdot \nu_f(i)$.

The point ρ is treated similarly, with slight further complications. One way to describe the outcome is to treat ρ and $\rho+1$ separately, as follows. Here, unlike at i, we cannot completely convert the path near ρ into straight line segments. Nevertheless, there is a well-defined angle to the boundary of F at ρ, namely, $\pi/3$. Modifying the path-integral along the boundary by indenting upward along a small arc of radius $\varepsilon > 0$, and taking a limit as $\varepsilon \to 0^+$, produces $-\frac{1}{6} \cdot 2\pi i \cdot \nu_f(\rho)$, rather than the full $-2\pi i \cdot \nu_f(\rho)$. Similarly, the limit of slightly-indented paths around $\rho + 1$ produces another $-\frac{1}{6} \cdot 2\pi i \cdot \nu_f(\rho)$, noting that $\nu_f(\rho+1) = \nu_f(\rho)$.

Thus, by integrating over the boundary of F_T modified by indentations of radius ε at i and ρ, and taking the limit as $\varepsilon \to 0^+$, we obtain

$$\nu_f(i\infty) + \sum_{z \in F} \nu_f(z) \;=\; -\frac{\nu_f(i)}{2} - \frac{\nu_f(\rho)}{3} + \frac{2k}{12}$$

Moving the suitably weighted orders of vanishing at i, ρ to the left-hand side gives the divisor/dimension formula. ///

[6.2] Remark: The idea that path integrals essentially running directly *through* a simple pole can be construed as giving *half* the residue, or half the negative, depending on the direction of indentation, can be legitimized as in the discussion of i above. The further idea, applied above to ρ and $\rho+1$, that path integrals along paths having a *corner* with angle θ at a simple pole, can be construed as producing $-\frac{\theta}{2\pi}$ of the residue, can likewise be legitimized. In all these cases, the underlying mechanism is that

$$\int_{\theta_1}^{\theta_2} \frac{d(\varepsilon e^{it})}{\varepsilon e^{it}} \;=\; \int_{\theta_1}^{\theta_2} i\; dt \;=\; (\theta_2 - \theta_1) i \qquad\qquad (\text{independent of } \varepsilon > 0)$$

---

7. *Automorphic L-functions*

[7.1] Euler product attached to $\Delta(z)$ A little later, we will prove two of the conjectures of Ramanujan proven by Mordell, in a form applicable to all holomorphic cuspforms of for $SL_2(\mathbb{Z})$. First, we examine the implications for Dirichlet series.

With $\Delta(z) = 1 \cdot e^{2\pi i n z} + \sum_{n \geq 1} \tau(n)\, e^{2\pi i n z}$ the unique cuspform of weight 12 for $SL_2(\mathbb{Z})$, the associated *Dirichlet series* is

$$L(s, \Delta) \;=\; \sum_{n \geq 1} \frac{\tau(n)}{n^s}$$

The Hecke estimate $|\tau(n)| \ll n^{\frac{12}{2}}$ shows that the series for $L(s, \Delta)$ is absolutely convergent for $\mathrm{Re}\,(s) > \frac{12}{2} + 1$.

The *weak multiplicativity* $\tau(mn) = \tau(m) \cdot \tau(n)$ for coprime m, n is equivalent to an *Euler factorization* of $L(s, \Delta)$:

$$L(s,\Delta) \;=\; \sum_{n\ge 1} \frac{\tau(n)}{n^s} \;=\; \prod_{p \text{ prime}} \Big(1 + \frac{\tau(p)}{p^s} + \frac{\tau(p^2)}{p^{2s}} + \frac{\tau(p^3)}{p^{3s}} + \ldots\Big)$$

The more peculiar relation

$$\tau(p^{n+1}) \;=\; \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1}) \qquad\qquad \text{(for prime } p\text{, for } n \ge 1)$$

gives a *recursion* for the $\tau(p^n)$: to simplify notation, let $X = p^{-s}$, observe that powers of p^{-s} do multiply like powers of X, and

$$1 \cdot \tau(p^{n+1})X^{n+1} \;-\; \tau(p)X \cdot \tau(p^n)X^n \;+\; p^{11}X^2 \cdot \tau(p^{n-1})X^{n-1} \;=\; 0 \qquad\qquad (\text{for } n \ge 1)$$

For $n \ge 1$, the left-hand side of the last equality is the $X^{n+1^{th}}$ term in

$$\Big(1 - \tau(p)X + p^{11}X^2\Big)\Big(1 + \tau(p)X + \tau(p^2)X^2 + \tau(p^3)X^3 + \ldots\Big)$$

The constant component of the latter product is 1. That is,

$$\Big(1 - \tau(p)X + p^{11}X^2\Big)\Big(1 + \tau(p)X + \tau(p^2)X^2 + \tau(p^3)X^3 + \ldots\Big) \;=\; 1$$

That is,

$$\Big(1 - \frac{\tau(p)}{p^s} + \frac{p^{11}}{p^{2s}}\Big)\Big(1 + \frac{\tau(p)}{p^s} + \frac{\tau(p^2)}{p^{2s}} + \frac{\tau(p^3)}{p^{3s}} + \ldots\Big) \;=\; 1$$

and

$$1 + \frac{\tau(p)}{p^s} + \frac{\tau(p^2)}{p^{2s}} + \frac{\tau(p^3)}{p^{3s}} + \ldots \;=\; \frac{1}{1 - \dfrac{\tau(p)}{p^s} + \dfrac{p^{11}}{p^{2s}}}$$

Thus,

$$\sum_n \frac{\tau(n)}{n^s} \;=\; \prod_p \frac{1}{1 - \dfrac{\tau(p)}{p^s} + \dfrac{p^{11}}{p^{2s}}}$$

This Euler product factorization partly justifies calling $\sum_n \frac{\tau(n)}{n^s}$ an *automorphic L-function.*

Further, the discriminant of the quadratic equation

$$X^2 - \tau(p)X + p^{11} \;=\; 0$$

is $\tau(p)^2 - 4p^{11}$. From the expression of Δ as a real constant multiple of $E_4^6 - E_6^2$, $\tau(p) \in \mathbb{R}$. Thus, the roots occur in complex conjugate pairs exactly when Ramanujan's conjectured, Deligne's proven, inequality $|\tau(p)| < 2p^{\frac{11}{2}}$ holds.

[7.2] Remark: We have given Hecke's proof of $|\tau(p)| \ll p^{\frac{12}{2}}$, but will not attempt to follow [Deligne 1974] to prove $|\tau(p)| < 2p^{\frac{11}{2}}$.

[7.3] Remark: We will show below that the space of weight $2k$ holomorphic cuspforms for $SL_2(\mathbb{Z})$ has a basis of cuspforms $f(z) = \sum_{n\ge 1} c_n\, e^{2\pi i n z}$ with $c_n = 1$ and whose associated Dirichlet series

$$L(s,f) \;=\; \sum_{n\ge 1} \frac{c_n}{n^s}$$

have Euler product factorizations

$$L(s,f) \;=\; \sum_{n\ge 1} \frac{c_n}{n^s} \;=\; \prod_p \frac{1}{1 - \dfrac{c_p}{p^s} + \dfrac{p^{2k-1}}{p^{2s}}}$$

Having an Euler product partly justifies calling $L(s,f)$ an *automorphic L-function* attached to f. The Hecke estimate $c_n \ll n^{\frac{2k}{2}}$ proves absolute convergence of $L(s,f)$ for $\mathrm{Re}(s) > \frac{2k}{2} + 1$.

[7.4] Analytic continuation and functional equation A holomorphic cuspform $f(z) = \sum_{n\ge 1} c_n\, e^{2\pi i n z}$ of weight $2k$ for $SL_2(\mathbb{Z})$ has associated Dirichlet series

$$L(s,f) \;=\; \sum_{n\ge 1} \frac{c_n}{n^s}$$

whether or not this has an Euler product.

[7.5] Remark: Merely copying Fourier coefficients to coefficients of a Dirichlet series accomplishes little, without further analytic features.

We do know that f is *rapidly decreasing* as $y \to +\infty$, and that $y^{\frac{2k}{2}} \cdot |f(z)|$ is *bounded* on $\mathfrak{H}$, so $|f(z)| \ll y^{-k}$ as $y \to 0^+$. Thus, for $\mathrm{Re}(s) > k$ we have absolute convergence of the *Mellin transform*

$$\int_0^\infty y^s\, f(iy)\, \frac{dy}{y}$$

In that range,

$$\int_0^\infty y^s\, f(iy)\, \frac{dy}{y} \;=\; \int_0^\infty y^s \sum_n c_n\, e^{-2\pi n y}\, \frac{dy}{y} \;=\; \sum_n c_n \int_0^\infty y^s\, e^{-2\pi n y}\, \frac{dy}{y}$$

$$= \sum_n \frac{c_n}{(2\pi n)^s} \cdot \int_0^\infty y^s\, e^{-y}\, \frac{dy}{y} \;=\; (2\pi)^{-s}\,\Gamma(s) \sum_n \frac{c_n}{n^s} \;=\; (2\pi)^{-s}\,\Gamma(s)\, L(s,f)$$

[7.6] Claim: $(2\pi)^{-s}\,\Gamma(s)\, L(s,f)$ has an analytic continuation to an *entire* function, satisfying

$$(2\pi)^{-(2k-s)}\,\Gamma(2k-s)\, L(2k-s,f) \;=\; (-1)^{\frac{2k}{2}} \cdot (2\pi)^{-s}\,\Gamma(s)\, L(s,f)$$

[7.7] Remark: This *integral representation* of $L(s,f)$, with Gamma-factor $(2\pi)^{-s}\,\Gamma(s)$ to *complete* it, plays the role for $L(s,f)$ as did the integral representation of the completed $\zeta(s)$ in terms of $\theta(z)$.

[7.8] Remark: With hindsight, seeing that the functional equation is with respect to $s \leftrightarrow 2k - s$, a contemporary choice would be to renormalize to have a functional equation $s \leftrightarrow 1 - s$, as we describe below. The latter convention is *not* universal.

Proof: The rapid decay of a cuspform $f(x+iy)$ as $y \to +\infty$ assures that part of the integral is *entire*:

$$\int_1^\infty y^s\, f(iy)\, \frac{dy}{y} \;=\; \text{entire}$$

Meanwhile, using the automorphy condition with $z \to -1/z$,

$$\int_0^1 y^s\, f(iy)\; \frac{dy}{y} \;=\; \int_0^1 y^s\, (iy)^{-2k}\cdot f(-1/iy)\; \frac{dy}{y} \;=\; (-1)^{\frac{2k}{2}} \int_0^1 y^{s-2k}\cdot f(-1/iy)\; \frac{dy}{y}$$

$$= \; (-1)^{\frac{2k}{2}} \int_1^\infty y^{2k-s}\cdot f(iy)\; \frac{dy}{y} \;=\; \text{entire}$$

Thus,

$$(2\pi)^{-s}\,\Gamma(s)\,L(s,f) \;=\; \int_1^\infty y^s\, f(iy)\; \frac{dy}{y} \;+\; (-1)^{\frac{2k}{2}} \int_1^\infty y^{2k-s}\, f(iy)\; \frac{dy}{y} \;=\; \text{entire}$$

and the behavior under $s \leftrightarrow 2k-s$ is clear. ///

[7.9] Remark: To translate so that the functional equation is $s \leftrightarrow 1-s$, instead of the natural but naive normalization above, put

$$L(s,f) \;=\; \sum_n \frac{c_n/n^{\frac{2k-1}{2}}}{n^s} \;=\; \sum_n \frac{c_n}{n^{s+\frac{2k-1}{2}}}$$

The corresponding integral representation becomes

$$(2\pi)^{-s-\frac{2k-1}{2}}\,\Gamma(s+\frac{2k-1}{2})\,L(s,f) \;=\; \int_0^\infty y^{s-\frac{1}{2}} \Big(f(iy)\cdot y^{\frac{2k}{2}}\Big)\; \frac{dy}{y}$$

Then one might further divide through by a constant so that the extra constant power of π disappears, giving functional equation

$$(2\pi)^{-(1-s)}\,\Gamma(1-s+\frac{2k-1}{2})\,L(1-s,f) \;=\; (-1)^k\cdot(2\pi)^{-s}\,\Gamma(s+\frac{2k-1}{2})\,L(s,f)$$

[7.10] Remark: Thus, we have shown that automorphic L-functions $L(f,s)$ arising from holomorphic cuspforms for $SL_2(\mathbb{Z})$ have analytic continuations and functional equations. Euler product factorizations are after a development of *Hecke operators*.

---

8. $\Delta(z) = q\prod(1-q^n)^{24}$

[Siegel 1954] showed a very simple, if somewhat unmotivated, argument for the product expansion of $\Delta(z)$. [Weil 1968] reproved the product expansion by a more complicated method related to the *converse theorems* in [Weil 1967], the latter arising as plausibility checks on the Taniyama-Shimura conjecture.

We reproduce both arguments. As expected, both make heavy use of various coincidences. Both use the one-dimensionality of the space of holomorphic cusp forms of weight 12 for $SL_2(\mathbb{Z})$ and generation of $SL_2(\mathbb{Z})$ by translation $z \to z+1$ and inversion $z \to -1/z$. A function of $e^{2\pi iz}$ is clearly invariant under $z \to z+1$. It remains to prove that the product expression must be proven to have the functional equation of a weight 12 modular form under $z \to -1/z$.

[8.1] Siegel's proof

Siegel's argument is simple but *ad-hoc*. With η the 24^{th} root of Δ, with $q = e^{2\pi iz}$, taking a logarithm,

$$\frac{1}{12}\pi iz - \log\eta(z) \;=\; -\sum_{\ell=1}^\infty \log(1-q^\ell) \;=\; \sum_{k,\ell\ge 1} \frac{1}{k} q^{k\ell} \;=\; \sum_{k\ge 1} \frac{1}{k}\cdot\frac{q^k}{1-q^k} \;=\; \sum_{k\ge 1}\frac{1}{k}\cdot\frac{1}{q^{-k}-1}$$

This suggests proving the functional equation in the form

$$\pi i\frac{z+z^{-1}}{12} + \tfrac{1}{2}\log\frac{z}{i} \;=\; \sum_{k=1}^\infty \frac{1}{k}\Big(\frac{1}{e^{-2\pi ikz}-1} - \frac{1}{q^{-2\pi ik/z}-1}\Big)$$

Let

$$f(w) \;=\; \cot w \cdot \cot w/z$$

and let ν run over values $(n+\frac{1}{2})\pi$ for $0 \le n \in \mathbb{Z}$. Then $f(\nu w)/w$ has *simple* poles at $w = \pm\pi k/\nu$ and at $w = \pm \pi k z/\nu$, with respective residues

$$\frac{1}{\pi k}\cot\frac{\pi k}{z} \qquad \text{and} \qquad \frac{1}{\pi k}\cot \pi k z \qquad (\text{for } k = 1,2,3,\ldots)$$

and a *triple* pole at at $w = 0$ with residue $-\frac{1}{3}(z+z^{-1})$. Let γ be the path tracing counter-clockwise the outline of the parallelogram with vertices $1, z, -1, -z$. By residues,

$$\pi\frac{z+z^{-1}}{12} + \int_\gamma f(\nu w)\frac{dw}{8w} \;=\; \frac{i}{2}\sum_{k\ge 1}\frac{1}{k}(\cot\pi k z + \cot \pi k/z) \;=\; \sum_{k=1}^\infty \frac{1}{k}\Big(\frac{1}{q^{-k}-1} - \frac{1}{q^{-k/z}-1}\Big)$$

The parameters n or ν only appear in the contour integral on the left-hand side. To evaluate it, let as $n \to +\infty$. In this limit, $f(\nu w)$ is uniformly bounded on γ, and has limiting values on the sides (excluding the vertices, where there are discontinuities) $1, -1, 1, -1$, respectively. The limit of the contour integral is

$$\int_\gamma f(\nu w)\frac{dw}{8w} \;=\; \Big(\int_1^z - \int_z^{-1} + \int_{-1}^{-z} - \int_{-z}^{1}\Big)\frac{dw}{w} \;=\; 4\,\log\frac{z}{i}$$

This gives the functional equation. ///

[8.2] Weil's proof

As in [Weil 1968], consider the Dirichlet series [13]

$$L(s) \;=\; \zeta(s)\cdot\zeta(s+1) \;=\; \sum_{m,n}\frac{1}{m}\frac{1}{(mn)^s} \;=\; \sum_{n=1}^\infty\Big(\sum_{d|n}\frac{1}{d}\Big)\frac{1}{n^s}$$

The *completed* version

$$\Lambda(s) \;=\; (2\pi)^{-s}\,\Gamma(s)\,L(s)$$

has functional equation inherited from $\zeta(s)$:

$$\Lambda(-s) \;=\; \Lambda(s)$$

Noting that $\zeta(2)/2\pi = \pi/12$,

$$\Lambda(s) \;=\; \frac{\pi/12}{s-1} - \frac{1}{2s^2} - \frac{\pi/12}{s+1} + (\text{holomorphic})$$

The power series in $q = e^{2\pi i z}$ with the same coefficients is

$$F(z) \;=\; \sum_{m,n}\frac{1}{m}q^{mn} \;=\; \sum_n\Big(\sum_m\frac{1}{m}\,(q^n)^m\Big) \;=\; -\sum_n \log(1-q^n)$$

Recall Dedekind's eta-function

$$\eta(z) \;=\; q^{1/24}\prod_{n\ge 1}(1-q^n)$$

[13] Weil was well aware that $L(s)$ is essentially the Mellin transform of the *constant coefficient* in the Laurent expansion in s at $s=1$ of the Eisenstein series $E_s = \sum \frac{y^s}{|cz|+d|^{2s}}$. The nature of that constant coefficient is part of the *Kronecker limit formula*.

Then

$$F(z) \;=\; -\Big(\frac{\log q}{24} + \sum_n \log(1-q^n)\Big) \;+\; \frac{\log q}{24} \;=\; -\log \eta \;+\; \frac{\pi i z}{12}$$

From the obvious Fourier-Mellin transform relation

$$\Lambda(s) \;=\; \int_0^\infty y^s\, F(iy)\, \frac{dy}{y} \qquad\qquad (\text{for } \mathrm{Re}\,(s) > 1)$$

Fourier-Mellin inversion gives

$$F(z) \;=\; \frac{1}{2\pi i}\int_{\sigma - i\infty}^{\sigma+i\infty} (z/i)^{-s}\, \Lambda(s)\, ds \qquad\qquad (\text{for } \sigma > 1)$$

Following Hecke and Weil, move the vertical line to $\mathrm{Re}\,(s) = -\sigma$, picking up residues at $1, 0, -1$:

$$\begin{aligned} F(z) \;&=\; \int_{-\sigma-i\infty}^{-\sigma+i\infty} (z/i)^{-s}\,\Lambda(s)\, ds + \Big(\frac{\pi}{12}\cdot (z/i)^{-1} + \tfrac{1}{2}\log(z/i) - \frac{\pi}{12}\cdot (z/i)\Big) \\ &=\; \int_{-\sigma-i\infty}^{-\sigma+i\infty} (z/i)^{-s}\,\Lambda(s)\, ds + \frac{\pi i}{12 z} + \tfrac{1}{2}\log(z/i) - \frac{\pi z}{12 i} \end{aligned}$$

The functional equation $\Lambda(-s) = \Lambda(s)$ allows conversion of the integral on $\mathrm{Re}\,(s) = -\sigma$ into

$$\frac{1}{2\pi i}\int_{-\sigma-i\infty}^{-\sigma+i\infty} (z/i)^{-s}\,\Lambda(-s)\, ds \;=\; \frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} \Big(\frac{-1}{z/i}\Big)^{-s}\,\Lambda(s)\, ds \;=\; F(-1/z)$$

That is,

$$F(z) \;=\; F(-1/z) + \frac{\pi i}{12 z} + \tfrac{1}{2}\log(z/i) - \frac{\pi z}{12 i}$$

Using $F(z) = \pi i z/12 - \log \eta(z)$, this is

$$\frac{\pi i z}{12} - \log\eta(z) \;=\; \frac{\pi i(-1/z)}{12} - \log \eta(-1/z) + \frac{\pi i}{12 z} + \tfrac{1}{2}\log(z/i) - \frac{\pi z}{12 i}$$

which simplifies to

$$\log \eta(z) \;=\; \log\eta(-1/z) - \tfrac{1}{2}\log(z/i)$$

Exponentiating and taking the 24^{th} power:

$$\eta^{24}(z) \;=\; \eta^{24}(-1/z)\cdot (z/i)^{-12}$$

or

$$\eta^{24}(-1/z) \;=\; z^{12}\cdot \eta^{24}(z)$$

That is, η^{24} has the two functional equations

$$\eta^{24}(z+1) \;=\; \eta^{24}(z) \qquad\qquad \eta^{24}(-1/z) \;=\; z^{12}\cdot\eta^{24}(z)$$

and goes to 0 as $\mathrm{Im}\,(z) \to +\infty$. Since $SL_2(\mathbb{Z})$ is generated by the matrices

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad\qquad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

giving the maps $z \to -1/z$ and $z \to z+1$, evidently η is a *holomorphic cuspform* of weight 12, with leading Fourier coefficient 1. Thus, it is $\Delta(z)$, and we have the product expansion

$$\Delta(z) \;=\; \eta^{24}(z) \;=\; e^{2\pi i z} \prod_{n\geq 1} (1 - e^{2\pi i n z})$$

[8.3] Remark: In fact, Weil's connection between a simple converse theorem and a product formula is anomalous.

---

9. *Appendix: fundamental domain for* $SL_2(\mathbb{Z})$

The simplest beginning choice of discrete subgroup Γ of $G = SL_2(\mathbb{R})$ is

$$\Gamma \;=\; SL_2(\mathbb{Z}) = \{\text{2-by-2 integer matrices with determinant 1}\}$$

Both for use below and to show that $SL_2(\mathbb{Z})$ is a large group, note:

[9.1] Claim: Given *relatively prime* integers c, d, there are integers a, b such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.

Proof: For *any* integers c, d, there are integers m, n such that

$$\text{greatest common divisor } c, d \;=\; m \cdot c + n \cdot d$$

Here the greatest common divisor is 1, so take $a = n$, $b = -m$, and then $ad - bc = 1$. ///

To be able to draw a picture of the quotient, we take an archaic approach which nevertheless succeeds in this case, namely, we find a *fundamental domain* for Γ on $\mathfrak{H}$, meaning to find a *nice* set of representatives for the quotient. Second, see how the edges of the fundamental domain are glued together when mapped to the quotient $\Gamma\backslash\mathfrak{H}$.

[9.2] Claim: Every Γ-orbit in $\mathfrak{H}$ has a representative in

$$\overline{F} \;=\; \{z \in \mathfrak{H} : |z| \geq 1,\; |\mathrm{Re}(z)| \leq \frac{1}{2}\}$$

More precisely, each orbit has a *unique* representative in the *standard fundamental domain*

$$F \;=\; \{z \in \mathfrak{H} : |z| > 1,\; -\frac{1}{2} \leq \mathrm{Re}(z) < \frac{1}{2}\} \cup \{z \in \mathfrak{H} : |z| = 1, \mathrm{Re}(z) \leq 0\}$$

Proof: From above, for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$

$$\mathrm{Im} \begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \frac{\mathrm{Im}\, z}{|cz+d|^2}$$

The set of complex numbers $cz + d$ is a subset of the lattice $\mathbb{Z} \cdot z + \mathbb{Z} \subset \mathbb{C}$. Since it is a discrete *subgroup*, it has (at least one) smallest (in absolute value) non-zero element.

Thus, $\inf |cz + d| = \min |cz + d| > 0$, taking the infimum or minimum over *relatively prime* c, d, which we have observed are exactly the lower rows of elements of Γ. Then

$$\sup \frac{1}{|cz+d|} = \max \frac{1}{|cz+d|} < \infty$$

Thus, for fixed $z \in \mathfrak{H}$,

$$\sup \operatorname{Im} \begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) \;=\; \sup \frac{\operatorname{Im} z}{|cz+d|^2} = \max \frac{\operatorname{Im} z}{|cz+d|^2} < \infty$$

Thus, in each Γ-orbit there is (at least one) point z assuming the maximum value of $\operatorname{Im} z$ on that orbit.

Since $\operatorname{Im} \begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \operatorname{Im} z/|cz+d|^2$, for z giving maximal $\operatorname{Im} z$ in its orbit, it must be that

$$|cz+d| \;\geq\; 1$$

for all c, d relatively prime. Thus, for example, for $d = 0$ there is the *inversion*

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}(z) \;=\; -1/z$$

Thus, $|1 \cdot z + 0| \geq 1$, so for $\operatorname{Im} z$ maximal in its Γ-orbit, $|z| \geq 1$.

We can adjust any $z \in \mathfrak{H}$ by

$$\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}(z) \;=\; z+n \qquad (\text{for } n \in \mathbb{Z})$$

to normalize $-1/2 \leq \operatorname{Re}(z) < 1/2$.

So take $|z| \geq 1$ and $|\operatorname{Re}(z)| \leq 1/2$ and show that $|cz+d| \geq 1$ for *all* c, d. Break z into its real and imaginary parts $z = x + iy$. Then

$$|cz+d|^2 \;=\; (cx+d)^2 + c^2y^2 \;=\; c^2(x^2+y^2) + 2cdx + d^2 \;\geq\; c^2(x^2+y^2) - |cd| + d^2$$

$$\geq\; c^2(|z|^2 - \frac{1}{4}) + \frac{c^2}{4} - |cd| + d^2 \;\geq\; c^2(|z|^2 - \frac{1}{4})$$

Thus, for $|c| \geq 2$, we have $|cz+d| > 1$ when $|z| \geq 1$ and $|x| \leq 1/2$.

For $c = 0$, necessarily $d = \pm 1$, and the only corresponding elements of Γ are

$$\begin{bmatrix} \pm 1 & n \\ 0 & \pm 1 \end{bmatrix}$$

The only z's with $|z| \geq 1$ and $|x| \leq 1/2$ that can be mapped to each other by such group elements are $-\frac{1}{2} + iy$ and $\frac{1}{2} + iy$. We whimsically keep the former as our chosen representative.

For $c = \pm 1$,

$$|cz+d|^2 \;=\; 2xd + d^2 + |z|^2 \geq -|d| + d^2 + 1 \;\geq\; 1 \qquad (\text{for } d \in \mathbb{Z})$$

In fact, for $|x| < 1/2$, there is a *strict* inequality

$$2xd + d^2 + |z|^2 \;>\; -|d| + d^2 + 1 \;\geq\; 1$$

so $|cz+d| > 1$. When $|x| = 1/2$, still $-|d| + d^2 + 1 > 1$, *except* for $d = 0, \pm 1$.

Thus, first without worrying about strictness of the inequalities, $|cz+d| \geq 1$ for $|z| \geq 1$ and $|x| \leq 1/2$, and the set $\overline{F}$ contains (at least one) representative for every orbit. What remains is to eliminate duplicates.

We have already observed that the only duplicates for $|z| > 1$ have $|x| = 1/2$, and $z \to z+1$ maps the $x = -1/2$ line to the $x = 1/2$ line.

Now consider $|z| = 1$. For $|x| < 1/2$, the only cases where $|cz + d| = 1$ are with $c = \pm 1$ and $d = 0$, which correspondes to matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{bmatrix} * & \pm 1 \\ \mp 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{bmatrix} \qquad \text{(for some } n \in \mathbb{Z}\text{)}$$

For $|z| = 1$, the inversion $z \to -1/z$ maps $z = x + iy$ to

$$-\frac{1}{z} = -\overline{z}/|z|^2 = -\overline{z} = -x + iy$$

Thus, for $|x| < 1/2$, the only one among these products that maps z back to the fundamental domain is exactly the inversion $z \to -1/z$. This inversion identifies the two arcs

$$\{|z| = 1 \text{ and } -\frac{1}{2} \le x \le 0\} \qquad \{|z| = 1 \text{ and } 0 \le x \le \frac{1}{2}\}$$

Thus, we should include only one or the other of these two arcs in the strict fundamental domain.

Last, with $|z| = 1$ and $|x| = 1/2$, there are exactly four group elements modulo $\pm 1_2$ (the center $\{\pm 1_2\}$ acts trivially) that map z to the closure of the fundamental region. These are: the identity, one of the translations $z \to z \pm 1$, the inversion $z \to -1/z$, and the *composite* of the translation and the inversion. That is, in addition to the identity,

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \ \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \ \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{map } -\frac{1}{2} + \frac{i\sqrt{3}}{2} \text{ to the boundary of } \overline{F}$$

and

$$\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, \ \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{map } \frac{1}{2} + \frac{i\sqrt{3}}{2} \text{ to the boundary of } \overline{F}$$

Thus, in the quotient $\Gamma\backslash\mathfrak{H}$, the identification of the sides $x = \pm 1$ creates a (topological) cyclinder, and the identification of the two arcs on the bottom closes the bottom of the cylinder. Thus, topologically, we have a cylinder closed at one end, which is a disk. But the non-euclidean geometry (if we were to pay more attention to details) suggests that the *top* of the cylinder is infinitely far away, and the radius of the cylinder goes to 0 as one goes toward the open top end, so it is more accurate to think of the quotient $\Gamma\backslash\mathfrak{H}$ as a raindrop shape. ///

[9.3] Claim: The inversion (long Weyl element) $w = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and translations $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ with $n \in \mathbb{Z}$ *generate* $\Gamma = SL_2(\mathbb{Z})$.

Proof: Again use the fact that $\mathbb{Z} \cdot z + \mathbb{Z}$ is a *lattice* in $\mathbb{C}$. In particular, there is *no* infinite sequence of decreasing sizes $|c_1 z + d_1| > |c_2 z + d_2| > \ldots$ with integers c_j, d_j. Thus, there is no infinite *increasing* sequence of heights

$$\frac{y}{|c_1 z + d_1|^2} < \frac{y}{|c_2 z + d_2|^2} < \ldots$$

Since $\mathrm{Im}\big(\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z)\big) = \dfrac{y}{|cz + d|^2}$, this implies that there is *no* infinite increasing sequence

$$\mathrm{Im}(\gamma_1 z) < \mathrm{Im}(\gamma_2 z) < \ldots \qquad \text{(for } \gamma_j \in \Gamma\text{)}$$

This promises that the following procedure does eventually put every point $z \in \mathfrak{H}$ inside the standard fundamental domain for Γ.

Given $z \in \mathfrak{H}$, translate z to z_1 satisfying $|\mathrm{Re}(z_1)| \le \frac{1}{2}$. If $|z_1| \ge 1$, stop: z_1 is in the fundamental domain. If $|z_1| < 1$, apply the inversion, noting

$$\mathrm{Im}\left(\frac{-1}{z_1}\right) \;=\; \frac{\mathrm{Im}(z_1)}{|z_1|^2} \;>\; \mathrm{Im}(z_1) \qquad\qquad (\text{since } |z_1| < 1)$$

Continue: translate $-1/z_1$ back to z_2 in the strip. If $|z_2| \ge 1$, stop. If $|z_2| < 1$, invert. Translate back to z_3 in the strip, and so on. The sequence $\mathrm{Im}(z_1) < \mathrm{Im}(z_2) < \ldots$ must be *finite*, so the process terminates after finitely many steps.

Thus, given $\gamma \in \Gamma$, take z in the *interior* of the fundamental domain, and let δ be a finite product of inversions and integer translations so that $\delta^{-1}\gamma z$ is back in the fundamental domain. Since z is in the interior, $\delta^{-1}\gamma = \pm 1_2$. Since $w^2 = -1_2$, necessarily γ is expressible in terms of inversions and integer translations. ///

[9.4] Remark: The number of steps require to move a given $z \in \mathfrak{H}$ into the fundamental domain is not simple to describe. This complication is visible in pictures of the tiling of the upper half-plane by images of the fundamental domain.

---

10. *Appendix: discriminants of cubics*

We give a reproducible derivation of the expression of the discriminant of a cubic in terms of the elementary symmetric polynomials:

[10.1] Claim: Given $(x-\alpha)(x-\beta)(x-\gamma) = x^3 - s_1x^2 + s_2x - s_3$, the *discriminant* is

$$\mathrm{disc} \;=\; (\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2 \;=\; (s_1^2 - 4s_2)s_2^2 + s_3(-4s_1^3 + 18s_1s_2 - 27s_3)$$

In particular, when $s_1 = 0$, as can be achieved by a linear change of variables, the discriminant is

$$\mathrm{disc} \;=\; -4s_2^3 - 27s_3^2$$

Thus, for $4x^3 - g_2x - g_3 = 4(x^3 - \frac{g_2}{4}x - \frac{g_3}{4}$, the discriminant is

$$\mathrm{disc} \;=\; -4\left(\frac{-g_2}{4}\right)^3 - 27\left(\frac{g_3}{4}\right)^2 \;=\; -\frac{1}{16}g_2^3 - \frac{27}{16}g_3^2$$

Proof: Imitating part of the proof that every symmetric polynomial is expressible in terms of the elementary ones, first set $\gamma = 0$, and observe that the discriminant degenerates into

$$(\alpha-\beta)^2\alpha^2\beta^2 \;=\; (\overline{s}_1^2 - 4\overline{s}_2)\overline{s}_2^2$$

where the $\overline{s}_j$ are the corresonding elementary symmetric functions $\overline{s}_1 = \alpha + \beta$ and $\overline{s}_2 = \alpha\beta$. Then $\mathrm{disc} - (s_1^2 - 4s_2)s_2^2$ is symmetric and vanishes at $\gamma = 0$, thus, vanishes at $s_3 = 0$. Since $\mathbb{Z}[s_1, s_2, s_3]$ is isomorphic to a polynomial ring in three variables, it is a unique factorization domain, by Gauss and Eisenstein. Thus, s_3 *divides* $\mathrm{disc} - (s_1^2 - 4s_2)s_2^2$.

The *homogeneity* properties

$$t\alpha+t\beta+t\gamma = t\cdot(\alpha+\beta+\gamma) \qquad (t\alpha)(t\beta)+(t\alpha)(t\gamma)+(t\beta)(t\gamma) = t^2\cdot(\alpha\beta+\alpha\gamma+\beta\gamma) \qquad (t\alpha)(t\beta)(t\gamma) = t^3\cdot\alpha\beta\gamma$$

of the elementary symmetric functions and of the discriminant shows that for some constants a, b, c

$$\frac{\mathrm{disc} - (s_1^2 - 4s_2)s_2^2}{s_3} \;=\; as_1^3 + bs_1s_2 + cs_3$$

that is,

$$\text{disc} \;=\; (s_1^2-4s_2)s_2^2 + (as_1^3 + bs_1s_2 + cs_3)s_3$$

Successive simple choices of α, β, γ give linear equations solvable for a, b, c.

First, $x^3-1 = (x-1)(x-\omega)(x-\omega^2)$ for cube root of unity ω conveniently makes $s_1 = s_2 = 0$ and $s_3 = 1$, so the expression for the discriminant directly gives

$$c \;=\; (1-\omega)^2(1-\omega^2)^2(\omega-\omega^2)^2 \;=\; -27$$

Second, $(x-1)^3 = x^3-3x^2+3x-1$ gives $s_1 = s_2 = 3$ and $s_3 = 1$, while the discriminant is 0. Thus,

$$0 \;=\; (s_1^2-4s_2)s_2^2 + (as_1^3 + bs_1s_2 + cs_3)s_3 \;=\; (3^2-4\cdot 3)3^2 + (a\cdot 3^3 + b\cdot 3\cdot 3 - 27)$$

Dividing through by 9 and rearranging,

$$6 \;=\; 3a+b$$

Third, to get another linear relation, use $(x^2+1)(x-1) = x^3-x^2+x-1$, so $s_1 = s_2 = s_3 = 1$. The discriminant is $(1-i)^2(1+i)^2(i+i)^2 = -16$, so

$$-16 \;=\; (s_1^2-4s_2)s_2^2 + (as_1^3 + bs_1s_2 + cs_3)s_3 \;=\; (1-4) + (a+b-27)$$

or

$$14 \;=\; a+b$$

Substituting $b = 14-a$ into $6 = 3a+b$ gives $6 = 3a+14-a$, so $-8 = 2a$, and $a = -4$. Thus, $b = 14-(-4) = 18$, and

$$\text{disc} \;=\; (s_1^2-4s_2)s_2^2 + (-4s_1^3 + 18s_1s_2 - 27s_3)s_3$$

///

[10.2] Remark: Another convenient data point is $(x^2-1)(x-1) = x^3-x^2-x+1$, with $s_1 = 1$, $s_2 = s_3 = -1$, to provide a check: the discriminant is 0, so we test whether or not

$$0 \;=\; (1-4(-1)) + (-4+18(-1)-27(-1))(-1) \qquad\qquad (?)$$

Indeed,

$$(1-4(-1)) + (-4+18(-1)-27(-1))(-1) \;=\; 5-(-4-18+27) \;=\; 5+4+18-27 \;=\; 0$$

as hoped.

Bibliography

[Deligne 1974] P. Deligne, *La conjecture de Weil, I*, Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273-307.

[Fricke-Klein 1897] R. Fricke, F. Klein, *Vorlesungen über die Theorie der automorphen Funktionen. Erster Band: Die gruppentheoretischen Grundlagen*, Teubner, Leipzig, 1897.

[Fricke-Klein 1912] R. Fricke, F. Klein, *Vorlesungen über die Theorie der automorphen Functionen. Zweiter Band: Die funktionentheoretischen Ausführungen und die Anwendungen. 1. Lieferung: Engere Theorie der automorphen Funktionen*, Teubner, Leipzig, 1897.

[Gunning 1959/62] R.C. Gunning, *Lectures on Modular Forms*, notes by A. Brumer, Princeton Univ. Press, 1962.

[Hecke 1937] E. Hecke, *Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklungen, I, II*, Math. Ann. **114** (1937) no. 1, 1-28, 316-351.

[Hurwitz 1881] A. Hurwitz, *[thesis]*, Math. Ann. **18** (1881), 528-592.

[Mordell 1917] L. J. Mordell, *On Mr. Ramanujan's empirical expansions of modular functions*, Proc. Camb. Phil. Soc. **19** (1917), 117-124.

[Petersson 1930] H. Petersson, *Theorie der automorphen Formen beliebiger reeler Dimension und ihre Darstellung durch eine neue Art Poincaréscher Reihen*, Math. Ann. **103** (1930, 369-436.

[Poincaré 1882] H. Poincaré, *Théorie des groupes fuchsiens*, Acta Math. **1** (1882), 1-62.

[Poincaré 1883] H. Poincaré, *Mémoire sur les groupes kleinéens*, Acta Math. **3** (1883), 49-92.

[Ramanujan 1916] S. Ramanujan, *On certain arithmetical functions*, Trans. Camb. Phil. Soc. **22** (1916), 136-162.

[Rankin 1939] R. Rankin, *Contributions to the theory of Ramanujan's function* $\tau(n)$ *and similar arithmetic functions I, II*, Proc. Cam. Phil. Soc. **35** (1939), 351-372.

[Selberg 1940] A. Selberg, *Bemerkungen über eine Dirichletsche Reihe, die mit der Theorie der Modulformen nahe verbunden ist*, Arch. Math. Naturvid **43** (1940), pp. 47-50.

[Siegel 1954] C.L. Siegel, *A simple proof of* $\eta(-1/\tau) = \eta(\tau)\sqrt{\tau/i}$, Mathematika **1** (1954), p. 4 (Ges. Abh. Bd. III, Springer 1966, p. 188).

[Weil 1967] A. Weil, *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Math. Ann. **168** (1967), 149-156.

[Weil 1968] A. Weil, *Sur une formule classique*, J. Math. Soc. Japan **20** (1968), 400-402. (*Oeuvres Sci.* Vol. III, Springer, New York, 1979, 198-200.)
