Introduction to Modular Forms

Pee Choon TOH

National Institute of Education
Nanyang Technological University
Singapore

16–21 July 2025
Arithmetic in Action: Number Theory
and its Applications to Cryptography and Coding Theory
Universitas Gadjah Mada

Outline

1. Fundamental domain of the modular group

2. Modular functions and modular forms

3. The space of modular forms

The modular group

Definition

- Let H denote the upper half plane of $\mathbb{C}$, i.e. $H = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$.
- Let $\tilde{\mathbb{C}}$ denote $\mathbb{C} \cup \{\infty\}$.
- Let $SL_2(\mathbb{R})$ denote the group of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $a, b, c, d \in \mathbb{R}$ and $ad - bc = 1$.

Action of $SL_2(\mathbb{R})$

Given $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$ and $z \in \tilde{\mathbb{C}}$, we define

$$gz := \frac{az + b}{cz + d}; \qquad g\infty := \frac{a}{c} = \lim_{z \to \infty} gz.$$

Correspondingly $g(-d/c) = \infty$ and if $c = 0$, $g\infty = \infty$.

Exercise 1

Check that g *is a group action on* $\tilde{\mathbb{C}}$, *i.e.* $g_1(g_2(z)) = g_1 \cdot g_2(z)$.

Exercise 2

Show that $\pm I = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *are the only elements of* $SL_2(\mathbb{R})$ *that acts trivially on* $\tilde{\mathbb{C}}$.

Thus $PSL_2(\mathbb{R}) := SL_2(\mathbb{R})/\{\pm I\}$ acts *faithfully*.

Exercise 3

Show that $\mathrm{Im}(gz) = |cz + d|^{-2}\mathrm{Im}(z)$.

Hence the action of $SL_2(\mathbb{R})$ preserves H.

Definition

Let $SL_2(\mathbb{Z})$ be the subgroup of $SL_2(\mathbb{R})$ with integer entries. Then $\Gamma := SL_2(\mathbb{Z})/\{\pm I\}$ is also called the modular group.

Fundamental domain

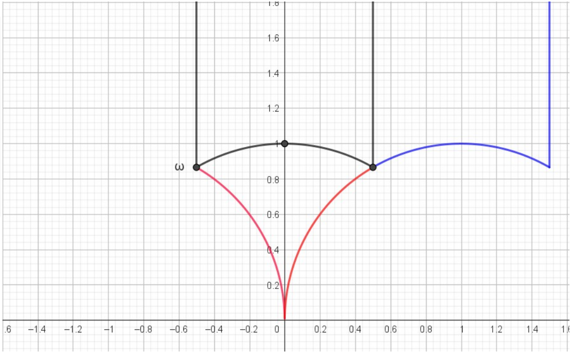
Definition

If G is a subgroup of Γ, we say two points $z_1, z_2 \in H$ are G-equivalent if there exists $g \in G$, such that $gz_1 = z_2$. A closed region F in H is called a fundamental domain for G if every $z \in H$ is G-equivalent to a point in F, but no two distinct points in the interior of F are G-equivalent.

Theorem 1

A fundamental domain for Γ is given by

$$D = \left\{ z \in H \,\middle|\, -\frac{1}{2} \leqslant \mathrm{Re}(z) \leqslant \frac{1}{2} \text{ and } |z| \geqslant 1 \right\}.$$



- What is the value of ω?
- Define $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Fundamental domain

Proof of Theorem 1: Let Γ' be the subgroup of Γ generated by S and T. We will prove that for any $z \in H, \exists g' \in \Gamma'$ such that $g'z \in D$.

Let $z \in H$ be fixed. If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma'$, then $\mathrm{Im}(gz) = \frac{\mathrm{Im}(z)}{|cz+d|^2}$. As c and d run through all possible integers, $|cz+d|$ is bounded away from 0. In other words, there are only finitely many pairs (c,d) such that $|cz+d|$ is less than a given number. So we can choose $g \in \Gamma'$ such that $\mathrm{Im}(gz)$ is maximum. We can choose a suitable integer n such that $z' = T^n(gz)$ has real part in the range $[-\frac{1}{2}, \frac{1}{2}]$, i.e. z' belongs to D. Note that we must have $|z'| \geqslant 1$, otherwise $S(z')$ would have a larger imaginary part. Thus $g' = T^n g$.

Next,we show that no two distinct points in the interior of D are Γ-equivalent. Suppose there exist $z \in D$ and $gz \in D$, and that $\mathrm{Im}(gz) \geqslant \mathrm{Im}(z)$. This would imply $|cz+d| \leqslant 1$. We have

$$1 \geqslant |cz+d| \geqslant |\mathrm{Im}(cz+d)| = |\mathrm{Im}(cz)| = |c|\mathrm{Im}(z).$$

So $c = 0$ or ± 1.

If $c = 0$, then $d = \pm 1$, i.e. $g = \begin{pmatrix} \pm 1 & b \\ 0 & \pm 1 \end{pmatrix}$. Since $gz \in D$, either $b = 0$ (i.e. $gz = z$) or $b = \pm 1$. This means z and gz have real parts $\pm\frac{1}{2}$.

Fundamental domain

Proof of Theorem 1 cont'd: If $c = 1$, i.e. $1 \geqslant |z + d| \geqslant |\mathrm{Re}(z + d)|$. This means $d = 0$ or ± 1.

If $d = 0$, $|z| \leqslant 1$, and so we must have $|z| = 1$. As $ad - bc = 1$, we have $b = -1$, i.e. $gz = a - \frac{1}{z}$. Since $gz \in D$, either $a = 0$ (i.e. $g = S$) or $a = 1$ (i.e. $z = -\overline{\omega}$, $g = TS$), or $a = -1$ (i.e. $z = \omega$, $g = T^{-1}S$).

If $d = 1$, $\mathrm{Re}(z) = -\frac{1}{2}$, i.e. $z = \omega$, $g = \begin{pmatrix} a & a-1 \\ 1 & 1 \end{pmatrix}$, so $g\omega = a - \frac{1}{1+\omega} = a + \omega$. Thus $a = 0$ ($g = ST$) or $a = 1$ ($g = -ST^{-1}S$).
If $d = -1$, $\mathrm{Re}(z) = \frac{1}{2}$, i.e. $z = -\overline{\omega}$.
Finally, if $c = -1$, just change the sign of a, b and d. □

Exercise 4

Verify that $T^{-1}S = (ST)^2$ *and* $(ST)^3 = -I$.

Corollary 2

Γ is generated by S and T, i.e. $\Gamma = \Gamma'$.

Proof: Let $g \in \Gamma$ and choose a point z_0 in the interior of D. Let $z = gz_0$, then there exists $g' \in \Gamma'$ such that $g'z \in D$. Hence z_0 and $g'z = g'gz_0$ are Γ-equivalent which means $g'g = I$, thus $g \in \Gamma'$. $\square$

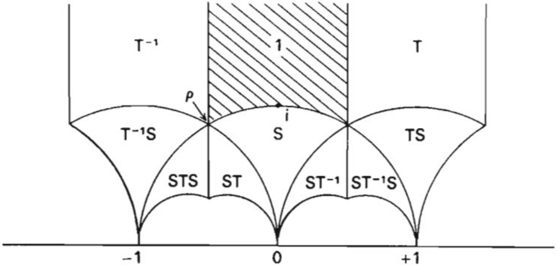


Figure: Serre [p. 78]

Remark: One can do the same calculations for subgroups of Γ, which will have “larger” fundamental domains. An example from Koblitz [p. 106] is $\Gamma(2)$ where $[\Gamma : \Gamma(2)] = 6$ with three cusps $\infty, 0, -1$.

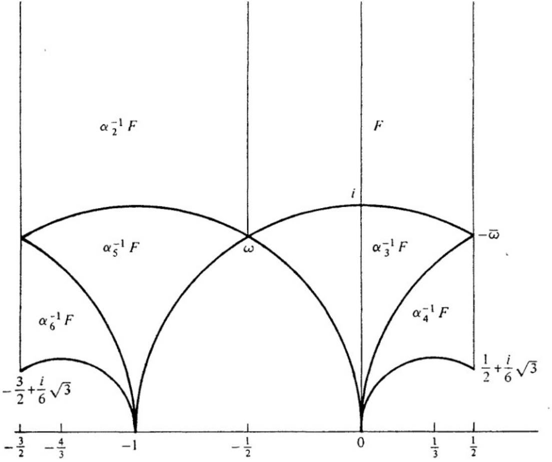


Figure III.3. A fundamental Domain $F(2)$ for $\Gamma(2)$.

Modular functions

Definition

Let k be an integer and $f(z)$ be meromorphic on H. Suppose $f(z)$ satisfies

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z), \qquad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$

Since Γ is generated by S and T, it suffices to check $f\left(-1/z\right) = z^k f(z)$ and $f(z+1) = f(z)$, i.e. $f(z)$ is periodic with period 1. We can express f as

$$f(z) = \sum_{n\in\mathbb{Z}} a_n q^n, \qquad \text{where } q = e^{2\pi i z}.$$

Suppose further that f is meromorphic at infinity, i.e. at most finitely many nonzero a_n for $n<0$, then we say $f(z)$ is a modular function of weight k for Γ.

Modular forms

Definition

A modular function which is holomorphic everywhere (including infinity) is called a modular form. A modular form of weight k for Γ is thus given by

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

which converges for $|q| < 1$, i.e. $\mathrm{Im}(z) > 0$ and satisfies $f(-1/z) = z^k f(z)$.

If $a_0 = 0$, then $f(z)$ is called a cusp-form.

Definition

$M_k(\Gamma)$ is defined to be the set of modular forms of weight k for Γ.
Correspondingly, $S_k(\Gamma)$ is defined to be the set of cusp-forms of weight k for Γ.

Ramanujan's τ function

Example

Ramanujan's τ function, a cusp form of weight 12, is defined by

$$\sum_{n=1}^{\infty} \tau(n) q^n = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 + \cdots .$$

ICM 2010

$|\tau(n)| \le n^{11/2} d(n)$

HYDERABAD • INDIA

आ नो भद्राः क्रतवो यन्तु विश्वतः।

MacDonald–Dyson formula

$$\tau(n) = \sum \frac{(a-b)(a-c)(a-d)(a-e)(b-c)(b-d)(b-e)(c-d)(c-e)(d-e)}{4!3!2!1!}$$

summed over integers a, b, c, d, e, with
$a, b, c, d, e \equiv 1, 2, 3, 4, 5 \pmod 5$,
$a + b + c + d + e = 0$,
$a^2 + b^2 + c^2 + d^2 + e^2 = 10n$.

Remarks on Modular functions

If k is an odd integer, there are no nonzero modular functions of weight k for Γ.

Applying $g = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ gives $f(z) = (-1)^k f(z)$.

The set of modular functions/forms of the same weight forms a complex vector space under addition and scalar multiplication. If f_1 and f_2 are modular functions/forms of weights k_1 and k_2 respectively, then the product $f_1 f_2$ is a modular function/form of weight $k_1 + k_2$.

Exercise 5

Check that if the transformation $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$ *holds for* g_1 *and* g_2*, then it holds for the product* $g_1 g_2$*.*

Hence it suffices to check the transformation holds for S and T.

Eisenstein series

Definition

Let k be an even integer greater than 2, for $z \in H$, define

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

where the sum is over all integers m, n not both zero.

Clearly, $G_k(z+1) = G_k(z)$. Next,

$$G_k(-1/z) = \sum_{m,n}{}' \frac{1}{(-\frac{m}{z}+n)^k} = \sum_{m,n}{}' \frac{z^k}{(-m+nz)^k} = z^k G_k(z).$$

So $G_k(z)$ satisfies the transformations for T and S.

Remark: Note we have switched the order of summation in the above and this is guaranteed by absolute convergence, i.e. $k > 2$.

Eisenstein series

Theorem 3

$G_k \in M_k(\Gamma)$.

Proof: Since $k \geqslant 4$, the double sum is absolutely convergent, and uniformly convergent in any compact subset of H. Hence $G_k(z)$ is holomorphic in H. We also need to check that $G_k(z)$ is holomorphic at infinity, i.e.

$$\lim_{z \to i\infty} \sum_{m,n}{}' \frac{1}{(mz+n)^k} = \sum_{n \neq 0} \frac{1}{n^k} = 2\zeta(k),$$

where ζ denote the Riemann zeta function. □

q-expansion of Eisenstein series

Theorem 4

Let $k \geqslant 2$ *be a positive integer and* $z \in H$. *Then*

$$G_{2k}(z) = 2\zeta(2k)\left(1 - \frac{4k}{B_{2k}}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n\right),$$

where $q = e^{2\pi iz}$, $\sigma_{2k-1}(n) = \sum_{d|n} d^{2k-1}$ *and the Bernoulli numbers,* B_k, *are defined by*

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

Exercise 6

Verify that $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$ *and* $B_4 = -\frac{1}{30}$. *[Cross multiply and compare coefficients.]*

Theorem 5

Let k *be a positive integer, then* $\zeta(2k) = \sum_{n\geqslant 1} \frac{1}{n^{2k}} = (-1)^{k+1}\frac{2^{2k-1}\pi^{2k}}{(2k)!}B_{2k}$.

Proof: Recall the formula $\sin(z) = z\prod_{n=1}^{\infty}\left(1-\frac{z^2}{\pi^2 n^2}\right)$. Taking the logarithmic derivative,

$$\frac{\cos(z)}{\sin(z)} = \frac{zi(e^{iz}+e^{-iz})}{e^{iz}-e^{-iz}} = \frac{1}{z} + \sum_{n\geqslant 1}\frac{1}{1-\frac{z^2}{\pi^2n^2}}\times\left(-\frac{2z}{\pi^2n^2}\right) = 1 - 2\sum_{n\geqslant 1}\frac{z^2}{\pi^2n^2-z^2}$$

$$\implies iz + \frac{2ize^{-iz}}{e^{iz}-e^{-iz}} = iz + \frac{2iz}{e^{2iz}-1} = 1 - 2\sum_{n\geqslant 1}\frac{z^2}{\pi^2n^2}\sum_{k\geqslant 0}\left(\frac{z^2}{\pi^2n^2}\right)^k$$

$$\implies iz + \sum_{k\geqslant 0}B_k\frac{(2iz)^k}{k!} = 1 - 2\sum_{n\geqslant 1}\sum_{k\geqslant 1}\left(\frac{z^2}{\pi^2n^2}\right)^k.$$

Comparing coefficients, $B_0 = 1$, $B_1 = -\frac{1}{2}$. Since right side is purely real, $B_{2j+1} = 0$, for $j \geqslant 1$, and the theorem follows from coefficients of z^{2k}. □

Exercise 7

Verify that $\zeta(2) = \frac{\pi^2}{6}$ *and* $\zeta(4) = \frac{\pi^4}{90}$.

Proof of Theorem 4: Replace z by πz and divide throughout by z in the cot formula to get

$$\pi i + \frac{2\pi i}{e^{2\pi i z} - 1} = \frac{1}{z} - \sum_{n \geqslant 1} \frac{2z}{(n-z)(n+z)} = \frac{1}{z} + \sum_{n \geqslant 1} \frac{1}{z+n} + \frac{1}{z-n}$$

$$\Longrightarrow \pi i - 2\pi i \sum_{n \geqslant 0} e^{(2\pi i z)n} = \frac{1}{z} + \sum_{n \geqslant 1} \frac{1}{z+n} + \frac{1}{z-n}.$$

Differentiating $2k-1$ times,

$$-(2\pi i)^{2k} \sum_{n \geqslant 1} n^{2k-1} e^{2\pi i n z} = (-1)^{2k-1}(2k-1)! \sum_{n \in \mathbb{Z}} \frac{1}{(z+n)^{2k}}.$$

Therefore (with z replaced by mz),

$$G_{2k}(z) = \sum_{m,n}{}' \frac{1}{(mz+n)^{2k}} = 2\zeta(2k) + 2\sum_{m=1}^{\infty} \sum_{n \in \mathbb{Z}} \frac{1}{(mz+n)^{2k}} = 2\zeta(k) + \frac{2(-1)^k (2\pi)^{2k}}{(2k-1)!} \sum_{m,n \geqslant 1} n^{2k-1} e^{2\pi i m n z}.$$

Proof of Theorem 4 cont'd: Replace $e^{2\pi iz}$ with q, we have

$$\begin{aligned} G_{2k}(z) &= 2\zeta(2k) - \frac{8k}{B_{2k}} \times \frac{(-1)^{k+1}2^{2k-1}\pi^{2k}B_{2k}}{(2k)!} \sum_{m,n\geqslant 1} n^{2k-1}q^{mn} \\ &= 2\zeta(2k)\left(1 - \frac{4k}{B_{2k}}\sum_{n\geqslant 1}\sigma_{2k-1}(n)q^n\right). \quad \square \end{aligned}$$

Normalized Eisenstein series

Definition

For $k \geqslant 2$, define the normalized Eisenstein series as

$$E_{2k} = 1 - \frac{4k}{B_{2k}} \sum_{n \geqslant 1} \sigma_{2k-1}(n) q^n.$$

We have

$$E_4(z) = 1 + 240 \sum_{n \geqslant 1} \sigma_3(n) q^n; \qquad E_{10}(z) = 1 - 264 \sum_{n \geqslant 1} \sigma_9(n) q^n;$$

$$E_6(z) = 1 - 504 \sum_{n \geqslant 1} \sigma_5(n) q^n; \qquad E_{12}(z) = 1 + \frac{65520}{691} \sum_{n \geqslant 1} \sigma_{11}(n) q^n;$$

$$E_8(z) = 1 + 480 \sum_{n \geqslant 1} \sigma_7(n) q^n; \qquad E_{14}(z) = 1 - 24 \sum_{n \geqslant 1} \sigma_{13}(n) q^n.$$

Exercise 8

Verify the first four terms of the q-expansions of E_4 and E_6 are

$$E_4 = 1 + 240q + 2160q^2 + 6720q^3 + \cdots \quad \text{and} \quad E_6 = 1 - 504q - 16632q^2 - 122976q^3 + \cdots .$$

Definition

The weight 12 cusp-form $\Delta(z)$ is defined as

$$\Delta(z) = \frac{(2\pi)^{12}}{1728} \left(E_4(z)^3 - E_6(z)^2 \right) .$$

Exercise 9

Compute the first two nonzero coefficients of $\Delta/(2\pi)^{12}$, i.e. coefficients of q and q^2.

Definition

Let f be meromorphic on H, not identically zero, and let p be a point in H. The order of f at p, denoted, $v_p(f)$, is defined as the integer n such that $f/(z-p)^n$ is holomorphic and nonzero at p.

When f is a modular function on Γ, $v_p(f) = v_{gp}(f)$ for $g \in \Gamma$, so it suffices to study the zeros and poles of f in $\Gamma \backslash H$, i.e. the fundamental domain with the Γ-equivalent boundary points identified.

Theorem 6 (Valence formula)

Let f be a nonzero modular function of weight k for Γ, then

$$v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\omega(f) + \sum_{p \in \Gamma \backslash H, p \neq i, \omega} v_p(f) = \frac{k}{12}.$$

Proof of Theorem 6: Suppose f has no zero or pole on the boundary of D, except possibly at i, ω and $-\overline{\omega}$. By the residue theorem,

$$\frac{1}{2\pi i}\int_\gamma \frac{f'(z)}{f(z)}dz = \sum_{p\in\Gamma\backslash H, p\neq i,\omega} v_p(f),$$

where γ is the contour indicated in the accompanying figure. Note that we can choose EA large enough that all the zeroes and poles lie below it. Specifically, $E = \frac{1}{2} + iT$ and $A = -\frac{1}{2} + iT$ and all zeroes and poles of f has imaginary parts less than T.

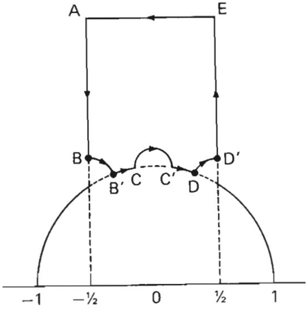


Figure: Serre, p. 86

(i) To evaluate the integral over EA, we change variables $q = e^{2\pi iz}$, so EA becomes a circle of radius $e^{-2\pi T}$ about the origin in a clockwise orientation. Hence

$$\frac{1}{2\pi i}\int_{EA} \frac{f'(z)}{f(z)}dz = -v_\infty(f).$$

Proof of Theorem 6 cont'd:

(ii) Since $f(z+1) = f(z)$, we have

$$\frac{1}{2\pi i}\int_{AB}\frac{f'(z)}{f(z)}dz + \frac{1}{2\pi i}\int_{D'E}\frac{f'(z)}{f(z)}dz = 0.$$

(iii) The integral over BB' approaches the integral (clockwise) of angle $\frac{2\pi}{6}$ about ω, i.e.

$$\frac{1}{2\pi i}\int_{BB'}\frac{f'(z)}{f(z)}dz \to -\frac{1}{6}v_\omega(f).$$

(iv) Similarly, we have

$$\frac{1}{2\pi i}\int_{CC'}\frac{f'(z)}{f(z)}dz \to -\frac{1}{2}v_i(f) \quad \text{and} \quad \frac{1}{2\pi i}\int_{DD'}\frac{f'(z)}{f(z)}dz \to -\frac{1}{6}v_\omega(f).$$

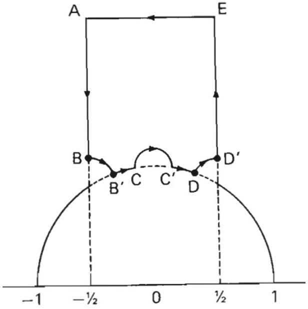


Figure: Serre, p. 86

Proof of Theorem 6 cont'd:

(v) It remains to show that

$$\frac{1}{2\pi i}\int_{B'C}\frac{f'(z)}{f(z)}dz + \frac{1}{2\pi i}\int_{C'D}\frac{f'(z)}{f(z)}dz \to \frac{k}{12}.$$

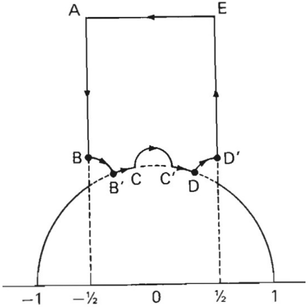


Figure: Serre, p. 86

S sends $B'C$ to DC'. (Note the orientation.) Since $f(Sz) = z^k f(z)$, we have

$$\frac{f'(Sz)}{f(Sz)}\frac{dSz}{dz} = \frac{k}{z} + \frac{f'(z)}{f(z)}.$$

$$\begin{aligned}\frac{1}{2\pi i}\int_{B'C}\frac{f'(z)}{f(z)}dz + \frac{1}{2\pi i}\int_{C'D}\frac{f'(z)}{f(z)}dz &= \frac{1}{2\pi i}\int_{B'C}\frac{f'(z)}{f(z)}dz - \frac{1}{2\pi i}\int_{B'C}\frac{f'(Sz)}{f(Sz)}dSz \\ &= \frac{1}{2\pi i}\int_{B'C} -\frac{k}{z}dz \to -k \times (-\frac{1}{12}).\end{aligned}$$

If f has zeros or poles on the boundary of D, we modify the contour accordingly. □

Corollary 7

The only modular forms of weight 0 for Γ are constant functions, i.e. $M_0(\Gamma) = \mathbb{C}$.

Proof: Let $f \in M_0(\Gamma)$ and c be a value taken by $f(z)$. If $f(z)$ is holomorphic but not a constant, at least one term $v_p(f) > 0$ in Theorem 6, giving rise to a contradiction. $\square$

Corollary 8

Let k be an even integer. If $k < 0$ or $k = 2$, then $M_k(\Gamma) = 0$.

Proof: The valence formula cannot hold in either case. $\square$

Corollary 9

$M_k(\Gamma)$ is one-dimensional, generated by E_k when $k = 4, 6, 8, 10$ or 14, i.e. $M_k(\Gamma) = \mathbb{C}E_k$.

Proof: When $k = 4$, $v_\omega(f) = 1$ and there are no other zeros. Therefore f/E_4 is weight 0 modular form, i.e. a constant. $\square$

Exercise 10

Complete the proof for Corollary 9.

Corollary 10

Let k be an even integer.
(i) If $k < 12$ or $k = 14$, then $S_k(\Gamma) = 0$;
(ii) $S_{12}(\Gamma) = \mathbb{C}\Delta$;
(iii) If $k > 14$, $S_k(\Gamma) = \Delta M_{k-12}(\Gamma)$;
(iv) $M_k(\Gamma) = S_k(\Gamma) \bigoplus \mathbb{C}E_k$ for $k > 2$.

Proof: For $f \in S_k(\Gamma)$, $v_\infty(f) > 0$ and the valence formula cannot hold if $k < 12$ or $k = 14$.

When $k = 12$, $v_\infty(f) = 1$ and there are no other zeros. Thus f/Δ is a modular form of weight 0. Hence statement (ii) follows.

This also shows that the only zero of Δ is at infinity, thus if $f \in S_k(\Gamma)$ for $k > 14$, $f/\Delta \in M_{k-12}(\Gamma)$.

To prove (iv), we note that E_k does not vanish at infinity. So given $f \in M_k(\Gamma)$, we can choose an appropriate value of c such that $f - cE_k$ vanishes at infinity. Thus $f - cE_k \in S_k(\Gamma)$. $\square$

Exercise 11

Let $j \geqslant 0$ be an integer. Show that

$$\dim(M_{2j}(\Gamma)) = \begin{cases} \left\lfloor \frac{j}{6} \right\rfloor, & j \equiv 1 \pmod 6 \\ \left\lfloor \frac{j}{6} \right\rfloor + 1, & j \not\equiv 1 \pmod 6 \end{cases}.$$

Theorem 11

Any $f \in M_k(\Gamma)$ can be written in the form

$$f(z) = \sum_{4i+6j=k} c_{i,j} E_4(z)^i E_6(z)^j.$$

Proof: By induction on k. E_4, E_6, E_4^2, $E_4 E_6$ and $E_4^2 E_6$ are in $M_k(\Gamma)$ for $k = 4, 6, 8, 10$ and 14 respectively. Since the dimension of $M_k(\Gamma)$ is 1 in each case, the result holds. For $k = 12$ or $k > 14$, there exist i and j such that $4i + 6j = k$ and also $E_4^i E_6^j \in M_k(\Gamma)$.

There exists c such that $f - cE_4^i E_6^j \in S_k(\Gamma)$. In other words,

$$f = cE_4^i E_6^j + \Delta f_1 = cE_4^i E_6^j + \frac{(2\pi)^{12}}{1728} \left(E_4(z)^3 - E_6(z)^2 \right) f_1,$$

where $f_1 \in M_{k-12}(\Gamma)$. Thus f is of the required form. □

Application to divisor sums

Corollary 12

Recall that $E_4^2 = E_8$. *Hence the following divisor sum identity holds:*

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m).$$

Proof: $E_4^2 \in M_8(\Gamma)$ which is spanned by E_8. The identity holds by comparing coefficients. Thus

$$\begin{aligned} 1 + 480 \sum_{n\geqslant 1} \sigma_7(n) q^n &= \left(1 + 240 \sum_{n\geqslant 1} \sigma_3(n) q^n\right)^2 \\ &= 1 + 480 \sum_{n\geqslant 1} \sigma_3(n) q^n + 240^2 \left(\sum_{m\geqslant 1} \sigma_3(m)\right)\left(\sum_{n\geqslant 1} \sigma_3(n)\right) q^{m+n}. \end{aligned}$$

The identity follows from simplification. □

Exercise 12

Show that $E_4E_6 = E_{10}$ and $E_6E_8 = E_4E_{10} = E_{14}$. Hence obtain divisor sum identities for $\sigma_9(n)$ and $\sigma_{13}(n)$.

Remark: These divisor sum identities are classical. One can study Eisenstein series for other levels and obtain analogous results. For example, define

$$\widetilde{\sigma}_s(n) = \sum_{d|n} (-1)^{d-1} d^s,$$

$$\widehat{\sigma}_s(n) = \sum_{d|n} (-1)^{\frac{n}{d}-1} d^s,$$

then in [T., 2011]

$$48 \sum_{m<n} \widehat{\sigma}_1(m)\widehat{\sigma}_1(n-m) = -4\widehat{\sigma}_1(n) + 5\sigma_3(n) - \widetilde{\sigma}_3(n).$$

References

- Serre, J. P., A course in Arithmetic, Springer (1973)
- Koblitz, N., Introduction to Elliptic Curves and Modular Forms, Second Ed., Springer (1993)
- Toh, P. C., Differential equations satisfied by Eisenstein series of level 2, Ramanujan J., 25, 2011, (179–194).